# Long solutions to small equations

Bogdan Grechuk, Eugene Go and Avraham Eisenberg

23 November 2026

**Abstract**

We give complete solutions of forty-nine Diophantine equations left open in Grechuk's 2024 monograph: twenty-five affine equations, five generalized Fermat equations, nine plane quartics, and ten further homogeneous equations. All proofs were generated by AI and require substantial computer algebra computations.

**Mathematics Subject Classification (2020).** 11D25, 11D41, 11G30, 11Y50.

**Keywords.** Diophantine equations; explicit descent; Chabauty method; Brauer–Manin obstruction.

hexagon:2610.00531v2

## Contents

**1 Introduction** **1**

**2 Shared tools and certificate lemmas** **6**

**3 Integral points on fifteen affine curves** **12**

**4 Ten further affine quartic equations** **71**

**5 Primitive generalized Fermat equations** **97**

**6 Rational points on nine plane quartics** **120**

**7 Homogeneous surfaces and diagonal quintics** **155**

**Reproducibility** **178**

## 1 Introduction

The theory of Diophantine equations contains many problems that are easy to state but exceptionally difficult to solve. Prominent examples include Fermat's Last Theorem, which asserts that $x^n + y^n = z^n$ has no solution in positive integers for any integer $n \geq 3$ [Wil95, TW95], and Mihăilescu's theorem, formerly Catalan's conjecture, which states that 8 and 9 are the only consecutive perfect powers greater than 1 [Mih04].

Grechuk's monograph [Gre24] develops a systematic approach to finding such problems among polynomial Diophantine equations

$$P(x_1, \dots, x_n) = 0, \tag{1}$$

where $P$ has integer coefficients. Write $P$ as a sum of distinct monomials with nonzero coefficients $a_1, \dots, a_k$ and total degrees $d_1, \dots, d_k$. Its size is defined by

$$H(P) = \sum_{i=1}^{k} |a_i| 2^{d_i}.$$

After identifying equations related by renaming variables, changing the signs of variables, or multiplying the equation by $-1$, and omitting variables that do not occur, there are only finitely many equations of any given size. This provides an ordering in which to study them systematically.

The same programme can be pursued within particular classes, such as equations in two variables, homogeneous equations, or generalized Fermat equations. The meaning of "solving" an equation depends on the class. An absolutely irreducible affine plane curve of positive genus has only finitely many integer points by Siegel's theorem [Gre24, Theorem 3.59]; the task is to determine all of them. For a generalized Fermat equation

$$ax^n + by^m = cz^r,$$

with fixed nonzero integer coefficients and positive integer exponents satisfying $1/n + 1/m + 1/r < 1$, Darmon and Granville [DG95] prove that the set of primitive integer solutions is finite. Here a solution is primitive if $\gcd(x, y, z) = 1$. A nonzero solution generates infinitely many solutions by weighted scaling, so the primitive solutions are the natural objects to classify. For a homogeneous equation, the zero vector is always a solution; one may instead ask whether a solution exists with at least one, or with every, coordinate nonzero. These two conditions are distinguished throughout.

In each class, the monograph resolves the relevant problem below a specified size and records the smallest outstanding cases. Subsequent progress is described in [Wil24, RG25, GR26, Gre26b, GA26, Gre26c]. We give AI-assisted proofs for forty-nine equations left open in the book. These comprise twenty-five affine curves, five generalized Fermat equations, nine plane quartics and ten further homogeneous equations.

For two-variable equations of size $H \leq 31$, Table 3.25 of [Gre24] contains thirty-one cases not resolved in that chapter. One is subsequently settled in Proposition 7.7 of the same book, leaving thirty open cases. Six were completed after book publication and before this paper [GG26, Wil24]. We determine the integer points on the other twenty-four. Table 1 thus gives the full solution sets for all thirty cases left open in the book.

Table 1: Completed two-variable equations of size $H \leq 31$ left open in [Gre24].

| $H$ | Equation | Solutions, $(x, y)$ | Reference |
|---|---|---|---|
| 28 | $x^4 - y^3 - x + y = 0$ | $(0, \pm 1), (0, 0), (1, 0), (1, \pm 1)$ | Thm. 3.1.1 |
| 28 | $x^4 - y^3 + x - y = 0$ | $(-1, 0), (0, 0), (1, 1)$ | Thm. 3.2.1 |
| 29 | $x^4 + y^3 + xy + 1 = 0$ | $(0, -1), (1, -1)$ | Thm. 3.3.1 |
| 29 | $x^4 + y^3 + xy - 1 = 0$ | $(-1, -1), (-1, 0), (-1, 1), (0, 1), (1, 0)$ | Thm. 4.18.1 |
| 30 | $x^4 - y^3 + xy + x = 0$ | $(-1, 0), (0, 0)$ | [Wil24] |
| 30 | $x^4 + y^3 - y^2 + x = 0$ | $(-4, -6), (-1, 0), (-1, 1), (0, 0), (0, 1), (1, -1)$ | Thm. 3.7.1 |
| 30 | $x^4 + y^3 + x - 2y = 0$ | $(-1, 0), (0, 0)$ | [GG26] |
| 30 | $x^4 + y^3 + x - y - 2 = 0$ | $(1, -1), (1, 0), (1, 1)$ | Thm. 4.13.1 |
| 30 | $x^4 + y^3 + x + y + 2 = 0$ | $(-1, -1), (0, -1)$ | Thm. 4.14.1 |
| 30 | $x^4 + y^3 + x + y - 2 = 0$ | $(-1, 1), (0, 1), (1, 0)$ | Thm. 4.17.1 |
| 30 | $x^4 + y^3 + x + 2y = 0$ | $(-1, 0), (0, 0)$ | Thm. 4.12.1 |
| 30 | $x^4 + y^3 + 2x - y = 0$ | $(-8, -16), (0, 0), (0, \pm 1)$ | Thm. 3.4.1 |
| 30 | $x^4 + y^3 + 2x + y = 0$ | $(0, 0), (8, -16)$ | Thm. 3.5.1 |
| 30 | $x^4 + y^3 + y^2 + x = 0$ | $(-1, -1), (-1, 0), (0, -1), (0, 0), (2, -3)$ | Thm. 3.6.1 |
| 30 | $x^4 + y^3 + xy - y = 0$ | $(0, \pm 1), (0, 0), (1, -1), (-1, 1)$ | [Wil24] |
| 30 | $x^4 + y^3 + xy + y = 0$ | $(-1, -1), (0, 0)$ | [Wil24] |
| 30 | $x^4 + y^3 + xy + x = 0$ | $(-1, \pm 1), (-1, 0), (0, 0), (1, -1)$ | [Wil24] |
| 31 | $x^4 - y^3 + xy + x + 1 = 0$ | $(0, 1)$ | Thm. 4.9.1 |
| 31 | $x^4 - y^3 + xy + x - 1 = 0$ | $(0, -1)$ | Thm. 3.12.1 |
| 31 | $x^4 + y^3 + x - 2y + 1 = 0$ | $(-1, 1), (0, 1)$ | [GG26] |

Continued on the next page.

Table 1: Completed two-variable equations of size $H \leq 31$ left open in the book (continued).

| $H$ | Equation | Solutions, $(x, y)$ | Reference |
|---|---|---|---|
| 31 | $x^4 + y^3 + x - 2y - 1 = 0$ | $(-1,-1), (0,-1), (1,1)$ | Thm. 4.16.1 |
| 31 | $x^4 + y^3 + x + 2y + 1 = 0$ | $(1,-1)$ | Thm. 4.15.1 |
| 31 | $x^4 + y^3 + 2x - y + 1 = 0$ | $(-1,\pm 1), (-1,0)$ | Thm. 3.8.1 |
| 31 | $x^4 + y^3 + 2x + y + 1 = 0$ | $(-1,0)$ | Thm. 3.9.1 |
| 31 | $x^4 + y^3 + 2x + y - 1 = 0$ | $(-1,1), (1,-1)$ | Thm. 3.10.1 |
| 31 | $x^4 + y^3 + xy - y - 1 = 0$ | $(\pm 1, 0)$ | Thm. 3.11.1 |
| 31 | $x^4 + y^3 + xy - 3 = 0$ | $(1,1)$ | Thm. 4.11.1 |
| 31 | $x^4 + y^3 + xy + y - 1 = 0$ | $(\pm 1, 0), (3,-4)$ | Thm. 3.13.1 |
| 31 | $x^4 + y^3 + xy + x + 1 = 0$ | $(0,-1)$ | Thm. 3.14.1 |
| 31 | $x^4 + y^3 + xy + x - 1 = 0$ | $(0,1)$ | Thm. 4.10.1 |

**Theorem 1.** *For each equation in the second column of Table 1, the integer solutions are exactly the pairs $(x, y)$ in the third column.*

*Proof.* See the references in the fourth column of Table 1. □

All equations in Table 1 have smooth projective models of genus 3. The smallest genus-two equation left open in the book is [Gre24, Equation (3.237)]

$$x^4 - x^2 + xy + y^3 = 0, \tag{2}$$

of size $H = 32$. Its plane model is singular, and its normalization has genus 2. We determine its integer solutions as well.

**Theorem 2.** *The only integer solutions to equation (2) are*

$$(x, y) = (0,0),\ (1,0),\ (-1,0),\ (-1,1),\ (-1,-1),\ (2,-2),\ (4,-6).$$

*Proof.* See Theorem 3.15.1. □

Open Question 4.52 of [Gre24] asks for all primitive solutions of the sixteen generalized Fermat equations in its Table 4.16. Table 2 gives their complete solution sets. Eight entries were resolved after publication of the book and before this paper: three in the appendix added to Wilcox [Wil24, Propositions A.2–A.4], two through Grechuk's reductions [Gre26a] to results of Bruin [Bru03] and Brown [Bro12], and three through the two separate papers [Eis26a, Eis26b]. The latter papers determine the primitive solutions of $x^4 + 3y^3 + 2z^3 = 0$ and $x^4 + 4y^3 + z^3 = 0$, respectively. The second also settles $2x^4 + 2y^3 + z^3 = 0$: parity forces $z = 2u$, and division by 2 gives $x^4 + 4u^3 + y^3 = 0$. This correspondence preserves primitivity, so the two presentations count as two table entries but require only one result.

Three further entries follow from results published before the book, by Zhang–Bai [ZB14], Bennett–Vatsal–Yazdani [BVY04], and Bennett–Ellenberg–Ng [BEN10]; their relevance is recorded in [Wil24, RG25]. The five proofs in Section 5 settle the five remaining entries. No entry of the book's Table 4.16 remains open.

**Theorem 3.** *For each equation in the second column of Table 2, the primitive integer solutions are exactly the triples $(x, y, z)$ in the third column.*

*Proof.* See the references in the fourth column. The row for $2x^4 + 2y^3 + z^3 = 0$ follows from [Eis26b] by the change of variables described above. □

Table 2: Completed generalized Fermat equations from [Gre24, Open Question 4.52]. All listed solutions are primitive.

| $H$ | Equation | Solutions, $(x, y, z)$ | Reference |
|---|---|---|---|
| 40 | $x^4 + 2y^3 + z^3 = 0$ | $(\pm 1, 0, -1), (\pm 1, -1, 1), (\pm 43, -203, 237)$ | [Gre26a] |
| 48 | $x^4 + 2y^3 + 2z^3 = 0$ | $\pm(0, 1, -1)$ | [Wil24, Prop. A.4] |
| 48 | $x^4 + 3y^3 + z^3 = 0$ | $(\pm 1, 0, -1), (\pm 895, -6202, 4199)$ | Thm. 5.1.1 |
| 48 | $2x^4 + y^3 + z^3 = 0$ | $\pm(0, 1, -1), (\pm 1, -1, -1)$ | [ZB14] |
| 48 | $x^4 - y^4 + 2z^3 = 0$ | $(\pm 1, \pm 1, 0)$ | [Wil24, Prop. A.2] |
| 48 | $x^4 + y^4 + 2z^3 = 0$ | $(\pm 1, \pm 1, -1)$ | [BVY04, Thm. 8.1] |
| 56 | $x^4 + 3y^3 + 2z^3 = 0$ | $(\pm 1, -1, 1)$ | [Eis26a] |
| 56 | $x^4 + 4y^3 + z^3 = 0$ | $(\pm 1, 0, -1)$ | [Eis26b] |
| 56 | $2x^4 + 2y^3 + z^3 = 0$ | $(\pm 1, -1, 0)$ | [Eis26b] |
| 56 | $x^4 - y^4 + 3z^3 = 0$ | $(\pm 1, \pm 1, 0)$ | [Wil24, Prop. A.3] |
| 56 | $2x^4 - y^4 + z^3 = 0$ | $(0, \pm 1, 1), (\pm 1, \pm 1, -1)$ | Thm. 5.2.1 |
| 56 | $x^5 + 2y^3 + z^3 = 0$ | $\pm(1, 0, -1), \pm(1, -1, 1)$ | [Gre26a] |
| 56 | $x^5 + y^4 - 2z^2 = 0$ | $(-1, \pm 1, 0), (1, \pm 1, \pm 1)$ | Thm. 5.3.1 |
| 56 | $x^5 + y^4 + 2z^2 = 0$ | $(-1, \pm 1, 0), (-3, \pm 1, \pm 11)$ | [BEN10, Thm. 1] |
| 60 | $x^5 + y^4 - 3z^2 = 0$ | $(-1, \pm 1, 0), (11, \pm 29, \pm 538)$ | Thm. 5.4.1 |
| 60 | $x^5 + y^4 + 3z^2 = 0$ | $(-1, \pm 1, 0)$ | Thm. 5.5.1 |

For homogeneous equations, Open Question 6.8 of [Gre24] asks whether the equation

$$x^4 + x^3y - y^4 + y^3z + z^4 = 0 \tag{3}$$

of size $H = 80$ has an integer solution other than $(0, 0, 0)$. We settle it by cubic reciprocity over the Eisenstein field.

**Theorem 4.** *Equation* (3) *has only the integer solution* $(0, 0, 0)$.

*Proof.* See Theorem 6.9.1. □

Open Question 6.9 of [Gre24] asks whether any of the three next-smallest equations in this category has a nonzero integer solution. We settle all three, as summarized in Table 3.

Table 3: Equations left open in [Gre24, Open Question 6.9]. Each has only the integer solution $(x, y, z, t) = (0, 0, 0, 0)$.

| $H$ | Equation | Reference |
|---|---|---|
| 96 | $x^3 + 2x^2y + y^3 + y^2z + xz^2 + z^3 + t^2x - t^2y - t^2z + tyz + t^3 = 0$ | Thm. 7.1.1 |
| 96 | $2x^3 + x^2y + xy^2 + y^3 + y^2z - 2xz^2 - z^3 + t^2y + tz^2 - t^3 = 0$ | Thm. 7.2.1 |
| 96 | $2x^3 + 2x^2y + 2y^3 + y^2z - 2xz^2 - z^3 + tz^2 - t^3 = 0$ | Thm. 7.3.1 |

**Theorem 5.** *Each equation in Table 3 has only the integer solution* $(x, y, z, t) = (0, 0, 0, 0)$.

*Proof.* See Theorems 7.1.1–7.3.1. □

Open Question 6.20 of [Gre24] concerns the five diagonal quintic equations in its Table 6.6: does any have a nonzero integer solution? Table 4 records our negative answer in each case, so none of these five questions remains open.

Table 4: Diagonal quintic equations left open in [Gre24, Open Question 6.20]. Each has only the integer solution $(x, y, z) = (0, 0, 0)$.

| $H$ | Equation | Reference |
|---|---|---|
| 704 | $14x^5 + 5y^5 + 3z^5 = 0$ | Thm. 7.5.1 |
| 832 | $17x^5 + 6y^5 + 3z^5 = 0$ | Thm. 7.7.1 |
| 928 | $14x^5 + 13y^5 + 2z^5 = 0$ | Thm. 7.9.1 |
| 960 | $21x^5 + 5y^5 + 4z^5 = 0$ | Thm. 7.6.1 |
| 992 | $17x^5 + 9y^5 + 5z^5 = 0$ | Thm. 7.8.1 |

**Theorem 6.** *Each equation in Table 4 has only the integer solution* $(x, y, z) = (0, 0, 0)$.

*Proof.* See Theorems 7.5.1–7.9.1. □

Open Question 6.21 of [Gre24] asks the analogous existence question for six diagonal quartic equations in four variables, all of size $H = 288$. Three were subsequently resolved by explicit nonzero solutions attributed to Eugene Go in [Gre26c, Sections 8.9–8.10]. We prove that a fourth has only the zero solution. Table 5 combines these four resolutions: a nonzero tuple is an existence witness, whereas the zero tuple is the complete solution set for its row. The two equations in Table 6 remain open; for each, the question is whether any nonzero integer solution exists.

Table 5: Resolved existence questions for diagonal quartics [Gre24, Open Question 6.21]. Nonzero rows give one witness each; the zero row gives all solutions.

| $H$ | Equation | Solutions, $(x, y, z, t)$ | Reference |
|---|---|---|---|
| 288 | $11x^4 + 4y^4 + 2z^4 - t^4 = 0$ | $(32519425, 30486957, 21147587, 63400357)$ | Go, [Gre26c, §8.10] |
| 288 | $8x^4 + 7y^4 + 2z^4 - t^4 = 0$ | $(0, 0, 0, 0)$ | Thm. 7.4.1 |
| 288 | $7x^4 + 5y^4 + 4z^4 - 2t^4 = 0$ | $(7337397, 6619385, 8035045, 12352344)$ | Go, [Gre26c, §8.9] |
| 288 | $8x^4 + 7y^4 + z^4 - 2t^4 = 0$ | $(60428235, 11074181, 51780065, 86883262)$ | Go, [Gre26c, §8.10] |

Table 6: Remaining open diagonal quartic equations from [Gre24, Open Question 6.21]. The question is the existence of a nonzero integer solution.

| $H$ | Equation |
|---|---|
| 288 | $7x^4 + 6y^4 + 4z^4 - t^4 = 0$ |
| 288 | $7x^4 + 6y^4 + 3z^4 - 2t^4 = 0$ |

**Theorem 7.** *The equation* $8x^4 + 7y^4 + 2z^4 - t^4 = 0$ *in Table 5 has only the integer solution* $(x, y, z, t) = (0, 0, 0, 0)$. *Each of the other three equations in that table has a nonzero integer solution.*

*Proof.* The nonexistence assertion is Theorem 7.4.1; the three displayed witnesses are verified by substitution. □

Open Question 6.28 of [Gre24] asks whether any of the eight plane quartics in its Table 6.10 has an integer solution with $xyz \neq 0$. Table 7 records a negative answer in every case. The cited theorems determine all integer solutions, including those with a zero coordinate, and no case in that table remains open.

Table 7: Plane quartics listed in [Gre24, Open Question 6.28]. None has an integer solution with $xyz \neq 0$.

| $H$ | Equation | Reference |
|---|---|---|
| 64 | $x^4 + x^3y + xy^3 - z^4 = 0$ | Thm. 6.1.1 |
| 64 | $x^4 + x^2y^2 + y^3z - yz^3 = 0$ | Thm. 6.3.1 |
| 64 | $x^4 - x^2y^2 + y^3z + yz^3 = 0$ | Thm. 6.5.1 |
| 64 | $x^4 + x^2y^2 + y^3z + z^4 = 0$ | Thm. 6.6.1 |
| 64 | $x^4 - y^4 + x^2yz + yz^3 = 0$ | Thm. 6.2.1 |
| 64 | $x^4 + y^4 + x^2yz - yz^3 = 0$ | Thm. 6.4.1 |
| 64 | $x^3z + y^3x + y^2z^2 - z^3y = 0$ | Thm. 6.7.1 |
| 64 | $x^4 - y^3z + xyz^2 + xz^3 = 0$ | Thm. 6.8.1 |

**Theorem 8.** *None of the equations in Table 7 has an integer solution with $xyz \neq 0$.*

*Proof.* See Theorems 6.1.1–6.8.1. □

Two related questions in four variables remain open. Open Question 6.32 of [Gre24] asks whether

$$x^4 + xy^3 + z^4 + t^4 = 0 \tag{4}$$

has an integer solution with $xyzt \neq 0$, and Open Question 6.33 asks the same question for

$$x^4 + y^4 + z^3t - zt^3 = 0. \tag{5}$$

Both equations have size $H = 64$ and remain open.

Finally, the book [Gre24] leaves open the existence of an integer solution with $xyz \neq 0$ to its equation (6.138), namely

$$4x^5 + 4y^5 + 11z^5 = 0, \tag{6}$$

of size $H = 608$. We determine its complete solution set.

**Theorem 9.** *The integer solutions to equation (6) are exactly $(x, y, z) = (n, -n, 0)$, where $n \in \mathbb{Z}$.*

*Proof.* See Theorem 7.10.1. □

The preceding discussion covers seventy-three entries explicitly left open in the book. We settle forty-nine here. Seventeen were resolved between publication of the book and this paper, and three follow from earlier literature. The four remaining entries in these families are the two diagonal quartics in Table 6 and the two four-variable equations (4) and (5). The seventeen earlier entries include the two equivalent presentations settled by [Eis26b] in Table 2. These counts concern the families discussed above, rather than every problem in the book. See the continuously updated arXiv preprint [Gre26c] for the full list of the current remaining open equations in this project.

Section 2 gives the shared certificate lemmas. Sections 3 and 4 determine the integral points on the affine curves. Section 5 treats the generalized Fermat equations. Section 6 determines the rational points on the plane quartics, including the cubic Brauer–Manin obstruction for (3). The remaining homogeneous equations are treated in Section 7. GPT-6.2 Astra, GPT-6 Astra Pro, GPT-5.6 Sol Ultra and Claude Opus 5.5 were used in developing, reviewing and editing the arguments. The computer-algebra computations used Magma and PARI/GP, together with the accompanying verification programs.

## 2 Shared tools and certificate lemmas

We cite standard theory at the point of use. For clarity, only the specializations needed to interpret the finite certificates are stated below. Proofs are retained for the elementary reductions and for consequences not quoted verbatim from a published theorem.

**Standard theory.** Explicit descent is used in the forms of Bruin–Poonen–Stoll [BPS16, Sections 6, 9 and 12], Poonen–Schaefer [PS97], Stoll [Sto01, Sections 4–5] and Simon [Sim02]. The deficiency correction to a genus-two rank bound is from Poonen–Stoll [PS99, Theorem 11 and Corollary 12]; two-cover descent is from [BS09]. Chabauty–Coleman integration and the residue-disk bounds are used as in [MP12, Sections 4–5], with Strassmann's theorem [Str28] when the prime or disk requires a coefficient calculation. Coleman–Gross heights [CG89], including tangent-vector normalization [Gro86, BB15], provide the quadratic Chabauty functions. The Mordell–Weil sieve is used as in [BS10].

For the Prym constructions we use [Bru08, Theorem 5.1 and Section 6] and [RR18, Theorem 1.1]. The determinant defining the genus-two curve uses the three-variable quadratic forms (their $3 \times 3$ matrices); the tangent calculation on a genus-five cover uses the $5 \times 5$ matrices of its defining quadrics. These two matrix constructions are distinct. In the ramified cases the rational maps used below are verified explicitly over the function field, including their quadratic twist. Torsion reduction is from [Kat81, Appendix], and extension across a smooth model uses the Néron mapping property [BLR90, Section 1.2].

For cyclic algebras we use local and global reciprocity [Neu99, Chapters V–VI]; for quadratic Hilbert symbols we use [Ser73, Chapter III, Sections 1–2]. The quintic arguments use modularity [BCDT01], level lowering in the form of [Sik12, Theorem 3 and Proposition 5.1], Mazur's torsion theorem [Maz77], and the Sturm bound [Stu87]. The calculations specific to the six Frey families are recorded once in the common Frey-curve argument below.

**Proposition A** (2-descent for plane quartics with a rational hyperflex)**.** *Let $C/\mathbb{Q}$ be a smooth plane quartic (genus 3), and let the rational point $O$ be a hyperflex; that is, the tangent line at $O$ meets $C$ at $O$ with multiplicity 4. Choose coordinates so that $O = (0:1:0)$ and its tangent line is $z = 0$. The other 27 bitangents do not pass through $O$, so they have the form $y = mx + b$. Suppose that these 27 slopes are the roots of a single irreducible polynomial $f \in \mathbb{Q}[m]$ of degree 27, and let $K = \mathbb{Q}[m]/(f)$. Then the following hold.*

*(1)* $J(\mathbb{Q})[2] = 0$.

*(2) From the generic bitangent $y = mx + b$ ($b \in K$) form $h = c\,(y - mx - b) \in K(C)$. The constant $c \in \mathbb{Q}^\times$ is chosen so that the leading coefficient at $O$ is 1 (the square class of the leading coefficient does not depend on the local parameter). Then $\operatorname{div} h = 2(P_m + Q_m - 2O)$ ($P_m, Q_m$ are the points of tangency). Sending a degree 0 divisor $\sum n_i P_i$ that avoids the zeros and poles of $h$ to $\prod h(P_i)^{n_i}$, and setting the value at $O$ to be 1, we obtain an injective homomorphism*

$$\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \hookrightarrow K^\times/K^{\times 2}, \qquad \delta([P - O]) = h(P)$$

*(3) Let $S = \{2\} \cup \{p : \ p \text{ is odd and the Tamagawa number } c_p(J) \text{ is even}\}$. The elements of the image of $\delta$ have norm in $\mathbb{Q}^{\times 2}$, and the image lies in*

$$K(S,2) = \{\alpha \in K^\times/K^{\times 2} : \text{ for every prime ideal } \mathfrak{p} \text{ not above } S,\ v_{\mathfrak{p}}(\alpha) \text{ is even}\}$$

*Moreover, at every prime $p \le \infty$, the local map $\delta_p : J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \to (K \otimes \mathbb{Q}_p)^\times/(K \otimes \mathbb{Q}_p)^{\times 2}$ defined by the same formula satisfies $\operatorname{res}_p \circ \delta = \delta_p \circ \operatorname{res}_p$.*

*(4) Hence, if we set*

$$\mathrm{Sel} = \{\alpha \in K(S,2) : \ N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}^{\times 2},\ \operatorname{res}_p(\alpha) \in \delta_p(J(\mathbb{Q}_p))\ (p \le \infty)\}$$

*then $\operatorname{rank} J(\mathbb{Q}) \le \dim_{\mathbb{F}_2} \mathrm{Sel}$. Here, if $K$ has signature $(r_1, r_2)$, then $\dim_{\mathbb{F}_2} K(S,2) = r_1 + r_2 + \#\{\mathfrak{p} \mid S\} + \dim_{\mathbb{F}_2} \mathrm{Cl}_S(K)[2]$, and the last term is 0 if $\mathrm{Cl}(K)[2] = 0$.*

*(5) (Local size) If $A$ is an abelian variety of dimension $g$ and $F$ is a finite extension of $\mathbb{Q}_p$, then*

$$\dim_{\mathbb{F}_2} A(F)/2A(F) = \begin{cases} \dim_{\mathbb{F}_2} A(F)[2], & p \neq 2, \\ \dim_{\mathbb{F}_2} A(F)[2] + g\,[F:\mathbb{Q}_2], & p = 2 \end{cases}$$

*and $\dim_{\mathbb{F}_2} A(\mathbb{R})/2A(\mathbb{R}) = \dim_{\mathbb{F}_2} A(\mathbb{R})[2] - g$, $A(\mathbb{C})/2A(\mathbb{C}) = 0$.*

*Outline of the proof of (1), of the injectivity in (2), and of $S$ in (3).* The 27 bitangents correspond to the 27 nonzero isotropic vectors of the odd quadratic refinement on $V = J[2] \cong \mathbb{F}_2^6$ (determined by the rational theta characteristic $2O$). The Weil pairing embeds $V$ into the permutation module $E = \mathbb{F}_2^{27}$, and the nonzero vectors of the image have weight 12 or 16 (this can be checked by enumerating all 64 vectors). Since $f$ is irreducible, the Galois image $G$ is transitive on the 27 bitangents, and so is its Sylow 3-subgroup $P$. Hence $E^P$ consists only of the constant vectors; the constant vector has weight 27, which is odd, so it is not in $V$, and therefore $V^P = 0$. Since $P$ has odd order, taking $P$-invariants is exact, so $(E/V)^G$ is generated by the image of the constant vector and $E^G \to (E/V)^G$ is surjective. By the long exact sequence, $H^1(\mathbb{Q}, V) \to H^1(\mathbb{Q}, E) = K^\times/K^{\times 2}$ is injective, and (1) follows from $V^G = 0$. $S$ in (3): if $c_p$ is odd at an odd prime $p$, then $J(\mathbb{Q}_p) = J^0(\mathbb{Q}_p) + 2J(\mathbb{Q}_p)$. On the connected Néron component $J^0$, $[2]$ is étale and surjective, so the Kummer classes of $J^0(\mathbb{Q}_p)$ are unramified, and their images have even valuation at every prime ideal above $p$. □

This is the rational-hyperflex specialization of [BPS16, Sections 6, 9 and 12]. The injectivity argument is included because it is essential to the rank bounds.

**Proposition B** (Explicit formula criterion for the 2-part of the class group)**.** *Let $K$ be a number field of degree $n$ and signature $(r_1, r_2)$, let $D \geq |d_K|$ (for example $D = |d_K|$, or $D = |\operatorname{disc} R|$ for an order $R \subseteq \mathcal{O}_K$ of rank $n$, since $\operatorname{disc} R = [\mathcal{O}_K : R]^2 d_K$), and let $\alpha = r_1/n$. Let $T > 0$, and let $v \geq 0$ be a nonzero step function supported on an interval of length $T$. Let $f$ be the normalized autocorrelation of $v$,*

$$f(x) = \frac{\int_{\mathbb{R}} v(t)v(t+x)\,dt}{\int_{\mathbb{R}} v(t)^2\,dt}$$

*For each prime power $q$, let $a(q)$ be the number of prime ideals of norm $q$, and let $k(q) \leq a(q)$ be the number of those whose classes have been proved to lie in $2\operatorname{Cl}(K)$ (for example, those proved to be principal). Set $c_m(q) = a(q)$ if $m \geq 1$ is even and $c_m(q) = 2k(q) - a(q)$ if $m$ is odd, and let*

$$C_\infty = \gamma + \log 4\pi + \alpha - \frac{\log D}{n}, \qquad W(x) = \frac{1}{\sinh x} + \frac{\alpha}{2\cosh^2(x/2)}$$

*($\gamma$ is Euler's constant). Then, if*

$$B^-(f) = C_\infty - \int_0^\infty (1 - f(x))W(x)\,dx + \frac{4}{n}\sum_{q^m < e^T} c_m(q)\frac{\log q}{q^m + 1} f(m\log q) > 0$$

*we have $\operatorname{Cl}(K)[2] = 0$. The sum runs over all prime powers $q$ and all $m \geq 1$ with $q^m < e^T$.*

*Proof.* $f$ is even, $f(0) = 1$, $f \geq 0$, and $f$ is a continuous piecewise linear function supported on $[-T, T]$. Moreover, its Fourier transform is $|\hat{v}|^2/\|v\|^2 \geq 0$. Suppose $\operatorname{Cl}(K)[2] \neq 0$. Then there is a quadratic character $\chi \neq 1$ of the class group, and by class field theory there is a quadratic extension $L/K$, unramified at all places (including the infinite places), with $\zeta_L = \zeta_K L(s, \chi)$. $L(s, \chi)$ is entire, its gamma factor is the same as that of $\zeta_K$, and its conductor is $|d_K|$. Writing the explicit formula for $L(s, \chi)$ with the test function $F(x) = f(x)/\cosh(x/2)$ and $\Phi(s) = \int_{\mathbb{R}} F(x)e^{(s-1/2)x}dx$, we get

$$\log|d_K| = n(\gamma + \log 8\pi) + \frac{r_1\pi}{2} - n\int_0^\infty \frac{1 - F(x)}{2}\Big(\frac{1}{\sinh(x/2)} + \frac{\alpha}{\cosh(x/2)}\Big)dx \\ + \sum_\rho \Phi(\rho) + 2\sum_{\mathfrak{p},\, m\geq 1} \frac{\chi(\mathfrak{p})^m \log N\mathfrak{p}}{N\mathfrak{p}^{m/2}} F(m\log N\mathfrak{p})$$

At a zero $\rho = \frac{1}{2} + b + it$ ($|b| \leq \frac{1}{2}$), the real part $\operatorname{Re}\Phi(\rho)$ equals the value at $t$ of the Fourier transform of $f(x)\cosh(bx)/\cosh(x/2)$. Since $f$ and $\cosh(bx)/\cosh(x/2)$ are both positive definite, this value is at least 0. So the sum over the zeros is at least 0, without any assumption on the location of the zeros. In the archimedean integral, the part corresponding to $f \equiv 1$ equals $\log 2 + \alpha\pi/2 - \alpha$, and the rest

is $\int_0^\infty (1-f)W$. Also $2F(m\log N\mathfrak{p})/N\mathfrak{p}^{m/2} = 4f(m\log N\mathfrak{p})/(N\mathfrak{p}^m+1)$. Therefore, dividing by $n$ and using $\log D \geq \log|d_K|$,

$$0 \geq C_\infty - \int_0^\infty (1-f)W + \frac{4}{n}\sum_{\mathfrak{p},\,m\geq 1}\chi(\mathfrak{p})^m \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m+1} f(m\log N\mathfrak{p}).$$

We have $f \geq 0$, and $\chi(\mathfrak{p})^m = 1$ if $m$ is even. If $m$ is odd, then $\chi(\mathfrak{p}) = 1$ at the prime ideals counted by $k(q)$ (a quadratic character is trivial on $2\,\mathrm{Cl}(K)$) and $\chi(\mathfrak{p}) \geq -1$ at the others. Hence the right-hand side is at least $B^-(f)$, which contradicts the assumption $B^-(f) > 0$. □

The explicit formula is from [Wei52, Poi77]; compare [Mil14, Sections 4–5] and [BDyDF08, Theorem 5.1]. The character bound and the partial-principality version are consequences proved here, not the statements of those references.

**Lemma C** (Strong induction on the norm)**.** *Let $K$ be a number field and $B \geq 2$. Suppose that for each prime ideal $\mathfrak{p}$ of norm at most $B$ an element $0 \neq g_\mathfrak{p} \in \mathfrak{p}$ is given such that, in the prime factorization $\prod q^{e_q}$ of $n_\mathfrak{p} = |N(g_\mathfrak{p})|/N\mathfrak{p}$, every $q^{e_q} < N\mathfrak{p}$. Then every prime ideal of norm at most $B$ is principal.*

*Proof.* $J = (g_\mathfrak{p})\mathfrak{p}^{-1}$ is an integral ideal of norm $n_\mathfrak{p}$. If a prime factor $\mathfrak{q}$ of $J$ lies above $q$, then $N\mathfrak{q} \leq q^{e_q} < N\mathfrak{p}$. Therefore, by strong induction on the norm, all prime factors of $J$ are principal, and hence $J$ and $\mathfrak{p}$ are principal. If $n_\mathfrak{p} = 1$, the induction starts immediately. □

This elementary certificate criterion is used to establish the input $k(q)$ in Proposition B.

**Proposition D** (Elliptic Chabauty over number fields)**.** *Let $K$ be a number field of degree $d \geq 2$, $E/K$ an elliptic curve, and $x : E \to \mathbb{P}^1$ a function defined over $K$; we want to determine $\mathcal{S} = \{P \in E(K) : x(P) \in \mathbb{P}^1(\mathbb{Q})\}$. Assume that $p$ is an odd prime unramified in $K$ and that $E$ has good reduction at every prime ideal above $p$, and let $K_p = K \otimes \mathbb{Q}_p$. Take $P_0 \in E(K)$ and $G_1, \ldots, G_r \in E(K)$ whose reductions are $0$ at all places above $p$, and let $P(n) = P_0 + \sum_i n_i G_i$ $(n \in \mathbb{Z}^r)$.*

*(1) Choose $f = x$ or $f = 1/x$, and assume that, at every place $v \mid p$, $f$ has no pole on the entire residue disk of $P_0$ (over an algebraic closure of $K_v$). For example, this holds for $f = x$ if $x$ has a well-defined reduction on each disk and $x(P_0)$ does not reduce to infinity. Then $n \mapsto f(P(n))$ extends to a power series with coefficients in $K_p$ that converges on $\mathbb{Z}_p^r$. The coefficients are determined by the formal group logarithm of $E$ (Lemma E) and the expansion of $f$ near $P_0$. The same disk condition is required when using $f = 1/x$.*

*(2) Under the hypothesis of (1), if $\lambda : K_p \to \mathbb{Q}_p$ is a $\mathbb{Q}_p$-linear map that vanishes on $\mathbb{Q}_p$, then $\theta_\lambda(n) = \lambda(f(P(n)))$ is $0$ at every $n$ with $P(n) \in \mathcal{S}$.*

*(3) Let $P_0 \in \mathcal{S}$. For $\lambda_1, \ldots, \lambda_r$ write $\Theta = (\theta_{\lambda_1}, \ldots, \theta_{\lambda_r})$ as $\Theta(n) = Bn + H(n)$ ($H$ of degree $\geq 2$). If $B$ is invertible over $\mathbb{Q}_p$, $p^s B^{-1} \in M_r(\mathbb{Z}_p)$, and all coefficients of $H$ lie in $p^{s+1}\mathbb{Z}_p$, then the only zero of $\Theta$ in $\mathbb{Z}_p^r$ is $n = 0$. Hence $\mathcal{S} \cap \{P(n) : n \in \mathbb{Z}^r\} = \{P_0\}$.*

The elliptic Chabauty setup is from [FW99, Bru03]. Since $p$ is odd and unramified in $K$, reduction to the origin puts each $G_i$ in the domain where the formal logarithm and exponential are inverse; see [Sil09, Chapter IV, Theorem 6.4]. In (3), if $v = \min_i v_p(n_i)$ and $n = -B^{-1}H(n) \neq 0$, then $v \geq s+1+2v-s > v$, a contradiction.

**Lemma E** (Logarithm of the formal group)**.** *Let $p$ be an odd prime, $\mathcal{A}/\mathbb{Z}_p$ an abelian scheme of relative dimension $g$ (e.g. a Jacobian with good reduction at $p$), and $z = (z_1, \ldots, z_g)$ formal parameters at the origin for which the formal group law $\mathcal{F}(X,Y)$ has coefficients in $\mathbb{Z}_p$.*

*(1) There is a unique $L \in \mathbb{Q}_p[[X]]^g$ with $L(X) \equiv X$ (modulo terms of degree $\geq 2$) and $L(\mathcal{F}(X,Y)) = L(X) + L(Y)$. The coefficients of the homogeneous part of degree $n$ of $L$ lie in $\frac{1}{n}\mathbb{Z}_p$. The coefficients of degree $n$ of the inverse $E = L^{-1}$ have valuation at least $-v_p(n!) \geq -\frac{n-1}{p-1}$.*

*(2) If $r \geq 1$, then $L$ and $E$ converge on $(p^r\mathbb{Z}_p)^g$ and are mutually inverse bijections of this set onto itself. If $\min_i v_p(X_i) = r$, then $L(X) \equiv X$, $E(X) \equiv X \pmod{p^{r+1}}$.*

(3) *If $Q \in \mathcal{A}(\mathbb{Z}_p)$ reduces to 0 and $r = \min_i v_p(z_i(Q)) \geq 1$, then for $m \in \mathbb{Z} \setminus \{0\}$ we have $z([m]Q) = E(m\,L(z(Q)))$ and*

$$z([m]Q) \equiv m\,z(Q) \pmod{p^{v_p(m)+r+1}}, \qquad \min_i v_p(z_i([m]Q)) = v_p(m) + r$$

*In particular, if $r = 1$, then $z([m]Q) \equiv m\,z(Q) \pmod{p^{v_p(m)+2}}$. The same formula $E(mL(z(Q)))$ defines $[m]Q$ for $m \in \mathbb{Z}_p$.*

For the formal logarithm and these coefficient estimates see [Haz78]; compare [Sil09, Chapter IV].

**Proposition F** (Size of local images and generation by points over finite fields)**.** *Let $C/\mathbb{Q}$ be a curve of genus $g$, $J = \mathrm{Jac}(C)$, and $p$ a prime.*

*(1) $\dim_{\mathbb{F}_2} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \dim_{\mathbb{F}_2} J(\mathbb{Q}_p)[2] + g \cdot [p = 2]$ (Proposition A(5)).*

*(2) If $p$ is odd and $C$ has a smooth model $\mathcal{C}/\mathbb{Z}_p$ at $p$, then reduction gives an isomorphism $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \cong J(\mathbb{F}_p)/2J(\mathbb{F}_p)$, and every point of $C(\mathbb{F}_p)$ lifts to $C(\mathbb{Q}_p)$.*

*(3) In addition to (2), assume that $O \in C(\mathbb{Q}_p)$ and $p + 1 > (8g-2)\sqrt{p}$ (for $g = 3$: $p \geq 487$). Then the classes $[\tilde{P} - \tilde{O}]$ for $\tilde{P} \in C(\mathbb{F}_p)$ generate $J(\mathbb{F}_p)/2J(\mathbb{F}_p)$. Hence the classes $[P - O]$, for lifts $P$ of the points of $C(\mathbb{F}_p)$, generate $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$, and the local image $\delta_p(J(\mathbb{Q}_p))$ (Theorems A, G) is generated by their values.*

*Proof.* (2) The reduction map is surjective, and its kernel is a pro-$p$ group consisting of points of the formal group (Lemma E). Since $p$ is odd, the kernel is uniquely divisible by 2. (3) Suppose they do not generate. Then there is a nonzero $\chi : J(\mathbb{F}_p) \to \mathbb{Z}/2$ that vanishes on all $[\tilde{P} - \tilde{O}]$. By class field theory, $\chi$ gives an unramified double cover $D \to C$, and $\tilde{P} \in C(\mathbb{F}_p)$ splits in $D$ exactly when $\chi([\tilde{P} - \tilde{O}]) = 0$. Since there is an $\mathbb{F}_p$-point above $\tilde{O}$, $D$ is geometrically irreducible, and by Riemann–Hurwitz its genus is $2g - 1$. Since all $\mathbb{F}_p$-points split, $\#D(\mathbb{F}_p) = 2\#C(\mathbb{F}_p)$, and by [Wei48], $2(p + 1 - 2g\sqrt{p}) \leq p + 1 + (4g-2)\sqrt{p}$, that is, $p + 1 \leq (8g-2)\sqrt{p}$. This contradicts the assumption. □

The local dimension is the standard local Kummer formula [Sto01, Section 4]. The finite-field generation criterion is a consequence of function-field class field theory [Ser88, Chapter VI] and the Weil bound [Wei48], as shown above.

**Proposition G** (Descent for a general bitangent algebra)**.** *In the situation of Proposition A, suppose that the slope polynomial $f$ of the 27 bitangents is squarefree but not necessarily irreducible. Let $f = \prod_i f_i$ be its factorization into irreducibles and $L = \mathbb{Q}[m]/(f) = \prod_i L_i$ ($L_i = \mathbb{Q}[m]/(f_i)$). Let $G$ be the Galois image on the 27 bitangents, $E = \mathbb{F}_2^{27}$ the permutation module, and $V = J[2] \hookrightarrow E$ the injection as in the proof of Proposition A. Then $H^1(\mathbb{Q}, E) = L^\times/L^{\times 2}$.*

*(1) $J(\mathbb{Q})[2] = V^G$. The map $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to L^\times/L^{\times 2}$ obtained by evaluating the normalized bitangent function $h$ componentwise is the composition of the Kummer map and $H^1(\mathbb{Q}, V) \to H^1(\mathbb{Q}, E)$. The kernel of the latter map is the quotient of $(E/V)^G$ by the image of $E^G$. In particular, if $E^G \to (E/V)^G$ is surjective, then $\delta$ is injective.*

*(2) The image of $\delta$ satisfies $N_{L/\mathbb{Q}}(\delta(x)) \in \mathbb{Q}^{\times 2}$, lies in $L(S, 2) = \prod_i L_i(S, 2)$ for the $S$ of Proposition A(3), and is compatible with the local images at all $p \leq \infty$. Hence, if $\delta$ is injective, then for $\mathrm{Sel} \subset L(S, 2)$ defined as in Proposition A(4) we have $\mathrm{rank}\, J(\mathbb{Q}) + \dim_{\mathbb{F}_2} V^G \leq \dim_{\mathbb{F}_2} \mathrm{Sel}$.*

*(3) If $G_p$ is the image of the decomposition group at $p$, then $\dim J(\mathbb{Q}_p)[2] = \dim V^{G_p}$, and the dimension of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$, an upper bound for that of the local image, is given by Proposition F(1).*

This is the reducible-bitangent-algebra form of [BPS16, Sections 6, 9 and 12]; the injectivity test is the cohomology exact sequence for $0 \to V \to E \to E/V \to 0$.

**Proposition H** (Explicit formula inequality for a single quadratic character)**.** *Use the notation of Proposition B ($n$, $r_1$, $D$, $\alpha$, $T$, $f$, $C_\infty$, $W$), and let $\chi : \mathrm{Cl}(K) \to \{\pm 1\}$ be a nontrivial character. Then*

$$C_\infty - \int_0^\infty (1 - f(x))W(x)\,dx + \frac{4}{n}\sum_{\mathfrak{p}} \sum_{m\geq 1:\ N\mathfrak{p}^m < e^T} \chi(\mathfrak{p})^m \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m + 1} f(m \log N\mathfrak{p}) \leq 0$$

This is the intermediate inequality in the proof of Proposition B; it is used when only a particular Selmer character has to be excluded.

**Proposition I** (2-descent by the 28 bitangents of a plane quartic)**.** *Let $C \subset \mathbb{P}^2$ be a smooth plane quartic over $\mathbb{Q}$ with Jacobian $J$, and let $V = J[2]$ with the Weil pairing $e_2$. Let $\Theta$ be the set of the 28 bitangents of $C$ with its Galois action, and let $K$ be the étale algebra of $\Theta$ (if the action is transitive, $K = \mathbb{Q}(\theta)$ for one bitangent $\theta$, a field of degree 28). Let $\ell$ be a linear form with coefficients in $K$ whose images under the 28 homomorphisms $K \to \overline{\mathbb{Q}}$ are linear forms $\ell_\theta$ defining the bitangents $\theta$; so $\mathrm{div}(\ell_\theta|_C) = 2D_\theta$ for an effective divisor $D_\theta$ of degree 2.*

*(1) The $D_\theta$ are the 28 odd theta characteristics of $C$, and $\theta \mapsto q_\theta$, $q_\theta(T) = h^0(D_\theta + T) + h^0(D_\theta) \bmod 2$, is a Galois-equivariant bijection from $\Theta$ onto the set of quadratic forms on $V$ with polar form $e_2$ and Arf invariant 1. Moreover $e_2(T, D_\theta - D_{\theta'}) = q_\theta(T) + q_{\theta'}(T)$. The image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Sp}(V) \cong \mathrm{Sp}_6(\mathbb{F}_2)$ acts faithfully on $\Theta$; so it is the Galois group of the polynomial whose roots are the slopes of the bitangents.*

*(2) Let $M = \mathbb{F}_2^\Theta / \mathbb{F}_2\mathbf{1}$ (as a Galois module, $\mathrm{Res}_{K/\mathbb{Q}}\,\mu_2/\mu_2$) and $\iota : V \to M$, $T \mapsto (e_2(T, D_\theta - D_{\theta_0}))_\theta$. Let $k \supseteq \mathbb{Q}$ be a field and $D = \sum n_P P$ a divisor of degree 0 over $k$ whose support avoids the points of contact. For a linear form $h$ over $k$ that vanishes at no point of the support, the class $\ell(D)$ of $\prod_P \big((\ell/h)(P)\big)^{n_P}$ in $(K \otimes k)^\times / k^\times$ does not depend on $h$, and $[D] \mapsto \ell(D)$ induces a homomorphism*

$$\delta_k : J(k)/2J(k) \to (K \otimes k)^\times / (K \otimes k)^{\times 2} k^\times.$$

*It is the composite of the Kummer map, $\iota_* : H^1(k, V) \to H^1(k, M)$, and the inverse of the injection $(K \otimes k)^\times / (K \otimes k)^{\times 2} k^\times \hookrightarrow H^1(k, M)$. The maps $\delta_k$ are compatible with restriction from $\mathbb{Q}$ to $\mathbb{Q}_v$, and $N_{K/\mathbb{Q}}(\delta_{\mathbb{Q}}(\xi)) \in \mathbb{Q}^{\times 2}$. The kernel of $\iota_*$ on $H^1(\mathbb{Q}, V)$ is the image of $(M/\iota V)^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$; in particular, if $(M/\iota V)^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} = 0$, then $\delta_{\mathbb{Q}}$ is injective. Also $J(\mathbb{Q})[2] = V^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$.*

*(3) (Odd primes) Let $p$ be an odd prime such that the Tamagawa number $c_p(J)$ is odd, and let $\xi \in J(\mathbb{Q}_p)$. Then $\delta_{\mathbb{Q}_p}(\xi)$ becomes trivial over $\mathbb{Q}_p^{\mathrm{nr}}$. Hence, if $\xi \in J(\mathbb{Q})$ and $\kappa \in K^\times$ represents $\delta_{\mathbb{Q}}(\xi)$, the vector $(v_{\mathfrak{p}}(\kappa) \bmod 2)_{\mathfrak{p}|p}$ is either 0 or $(e_{\mathfrak{p}} \bmod 2)_{\mathfrak{p}|p}$, where $e_{\mathfrak{p}}$ is the ramification index.*

For evaluation of functions in descent see [Sch98]; for the bitangent algebra and the fake descent target see [BPS16, Sections 6, 9 and 12]. The theta-characteristic description is standard [Dol12, Chapters 5–6].

**Proposition J** (Brauer–Manin obstruction from a cyclic algebra on a smooth cubic surface)**.** *Let $K$ be a number field, $X \subset \mathbb{P}^3_K$ a smooth cubic surface, $L/K$ a cyclic extension of prime degree $n$, and $\tau$ a generator of $\mathrm{Gal}(L/K)$; $\tau$ acts on $X_L = X \times_K L$ and on its divisors. For a divisor $D$ on $X_L$ put $N_{L/K}(D) = D + \tau D + \cdots + \tau^{n-1} D$, and for $\psi \in K(X)^\times$ let $\mathcal{B}_\psi = (L/K, \tau, \psi) \in \mathrm{Br}(K(X))$ be the cyclic algebra over the function field. For a field $K' \supseteq K$ and $c \in K'^\times$, $(L \otimes_K K'/K', \tau, c)$ is the cyclic algebra of [Neu99, Chapters V–VI] if $L \otimes_K K'$ is a field, and $0 \in \mathrm{Br}(K')$ if $L \otimes_K K' \cong K'^n$ (since $n$ is prime, there are no other cases).*

*(1) (Azumaya extension) If $\mathrm{div}(\psi) = N_{L/K}(D)$ for a divisor $D$ on $X_L$, then $\mathcal{B}_\psi$ lies in $\mathrm{Br}(X) \subseteq \mathrm{Br}(K(X))$. For $g \in K(X)^\times$ and $f \in L(X)^\times$, $\psi' = \psi\, g^n\, N_{L(X)/K(X)}(f)$ defines the same class. If $K' \supseteq K$ is a field and $P \in X(K')$ is a point at which such a $\psi'$ is regular and nonzero, then $\mathcal{B}_\psi(P) = (L \otimes_K K'/K', \tau, \psi'(P))$ in $\mathrm{Br}(K')$.*

*(2) (Local constancy) For every place $w$ of $K$ and every $\alpha \in \mathrm{Br}(X)$, the map $X(K_w) \to \mathbb{Q}/\mathbb{Z}$, $P \mapsto \mathrm{inv}_w\, \alpha(P)$, is locally constant.*

*(3) (Points of smooth reduction) Let $w$ be a finite place of $K$, with ring of integers $\mathcal{O}_w$, uniformizer $\pi$ and residue field $k$, at which $L/K$ is unramified. Let $\mathcal{X} \subset \mathbb{P}^3_{\mathcal{O}_w}$ be defined by an equation of $X$ with coefficients*

*in $\mathcal{O}_w$, not all in $\pi\mathcal{O}_w$, and assume that the special fibre $\mathcal{X}_k$ is geometrically integral. Let $\psi = G/(c\,\ell^d)$ with $\operatorname{div}(\psi) = N_{L/K}(D)$ as in (1), where $G$ is a form of degree $d$ and $\ell$ a linear form, both with coefficients in $\mathcal{O}_w$, $c \in K_w^\times$ with $n \mid v_w(c)$, and the reduction of $G$ does not vanish identically on $\mathcal{X}_k$. If $P \in X(K_w)$ reduces to a point $\bar{P} \in \mathcal{X}(k)$ at which $\mathcal{X}_k$ is smooth and $\ell(\bar{P}) \neq 0$, then $\operatorname{inv}_w \mathcal{B}_\psi(P) = 0$. In particular, if $\mathcal{X}_k$ is smooth and $n \mid d$, then $\operatorname{inv}_w \mathcal{B}_\psi(P) = 0$ for all $P \in X(K_w)$ (replace $\ell$ by a coordinate $\ell'$ with $\ell'(\bar{P}) \neq 0$; by (1), $G/(c\,\ell'^d) = \psi \cdot (\ell/\ell')^d$ defines the same class).*

*(4) (Reciprocity) If $\alpha \in \operatorname{Br}(X)$ and $P \in X(K)$, then $\sum_w \operatorname{inv}_w \alpha(P) = 0$, the sum over all places of $K$. Hence, if $\sum_w \operatorname{inv}_w \alpha(P_w) \neq 0$ for every family $(P_w)_w \in \prod_w X(K_w)$, then $X(K) = \varnothing$.*

*Outline of the proof of (1) and (3).* (1) Let $\chi$ be the character of $\operatorname{Gal}(L/K)$ with $\chi(\tau) = 1/n$. Since $\chi$ comes from the constant field, the residue of $\mathcal{B}_\psi$ at a prime divisor $E$ of $X$ is $v_E(\psi) \cdot \chi|_{K(E)} \in H^1(K(E), \mathbb{Q}/\mathbb{Z})$ (up to sign). If $E_L$ is not integral, then $L \otimes_K K(E)$ is split and $\chi|_{K(E)} = 0$. Otherwise $E_L$ is a prime divisor with $N_{L/K}(E_L) = nE$, so the coefficient $v_E(\psi)$ of $E$ in $N_{L/K}(D)$ is divisible by $n$. Hence all residues vanish, and since $X$ is smooth, $\mathcal{B}_\psi \in \operatorname{Br}(X)$ by purity. The algebras $(L/K, \tau, g^n)$ and $(L/K, \tau, N_{L(X)/K(X)}(f))$ are split, and the value of an Azumaya algebra at a point can be computed from any representative that is regular and nonzero there.

(3) If $L \otimes_K K_w \cong K_w^n$, the invariant is 0. Otherwise $L_w = L \otimes_K K_w$ is the unramified field extension of degree $n$; let $\mathcal{O}_{L_w}$ be its ring of integers and $R = \mathcal{O}_{\mathcal{X},\bar{P}} \otimes_{\mathcal{O}_w} \mathcal{O}_{L_w}$. Since $\bar{P}$ is $k$-rational and the residue field of $L_w$ is a field, $R$ is local. $R/\pi R$ is the local ring of the smooth surface $\mathcal{X}_k \otimes_k k_{L_w}$ at a rational point, so it is a regular local ring of dimension 2, in particular a domain, and $\pi$ is not a zero divisor in $R$; hence $R$ is a regular local ring of dimension 3, and by the Auslander–Buchsbaum theorem [Mat86, Theorem 20.3] it is a unique factorization domain. The function $g = G/\ell^d$ lies in $R$, and $\pi \nmid g$ because $\mathcal{X}_k \otimes_k k_{L_w}$ is integral and the reduction of $G$ does not vanish on it. The other height-one primes of $R$ are the closures of the prime divisors of $X_{L_w}$ that meet $\operatorname{Spec} R$, and each of them is principal. Writing the restriction of $D$ to $\operatorname{Spec} R$ as $\operatorname{div}(f)$ ($f \in \operatorname{Frac}(R)^\times$; $\ell$ is a unit of $R$), we obtain $g = u\,N_{L_w/K_w}(f)$ with $u \in R^\times$, and $u = g/N(f)$ lies in $K_w(X)$, hence in $\mathcal{O}^\times_{\mathcal{X},\bar{P}}$. By (1) over $K_w$, $\mathcal{B}_\psi = \mathcal{B}_{u/c}$, and $u/c$ is regular and nonzero at $P$, so $\mathcal{B}_\psi(P) = (L_w/K_w, \tau, u(P)/c)$ with $v_w(u(P)/c) = -v_w(c) \equiv 0 \pmod{n}$. By [Neu99, Chapters V–VI], its invariant is 0. □

The cyclic-algebra construction and its local evaluation are treated in [CTS21, Sections 1.4, 3.7 and Chapter 12] and [EJ12, Definition 4.9, Lemma 4.16 and Theorem 4.18]. The proof of (3) records the precise extension needed at smooth points of a possibly singular special fibre; the reciprocity obstruction is [Poo17, Section 8.2].

## 3 Integral points on fifteen affine curves

The first thirteen curves are treated by bitangent descent, followed by linear or quadratic Chabauty and a Mordell–Weil sieve. The last two use a Prym cover and the normalization of a nodal quartic, respectively.

### 3.1 $x^4 - y^3 - x + y = 0$ ($H = 28$)

**Theorem 3.1.1.** *The equation $x^4 - y^3 - x + y = 0$ has only the following integer solutions: $(x, y) = (0, -1), (0, 0), (0, 1), (1, -1), (1, 0), (1, 1)$.*

**Setup.** Let $J$ be the Jacobian of the smooth projective model of the curve. Setting $u = -x$, $v = -y$, the equation becomes

$$C: \quad F(u, v) = u^4 + v^3 + u - v = 0$$

and the integer solutions correspond bijectively to the integral points of $C$ via $(x, y) = (-u, -v)$. There is a single point at infinity, $O = (0 : 1 : 0)$. In the chart $t = U/V$, $w = W/V$ the equation is $t^4 + w + tw^3 - w^3 = 0$, so $O$ is a smooth rational hyperflex. An affine singular point in odd

characteristic satisfies $4u^3+1 = 3v^2-1 = 0$ and $12F - 3uF_u - 4vF_v = 9u - 8v = 0$; eliminating gives $4u^3+1 = 243u^2-64 = 0$, so the characteristic is a prime factor of the resultant $157 \cdot 64679$. In characteristic 2, $F_u \equiv 1$. At the two bad primes the reduction has only a single ordinary node, of thickness 1, so it is geometrically irreducible and the component group of the Jacobian is trivial (certificate 1.1.1a).

Denote the six known points by

$$A = (-1,-1),\ B = (-1,0),\ C_1 = (-1,1),\ D = (0,-1),\ E = (0,0),\ F_1 = (0,1)$$

(in the original coordinates these are $(1,1), (1,0), (1,-1), (0,1), (0,0), (0,-1)$, respectively). We abbreviate $[P-O] \in J(\mathbb{Q})$ to $P$. Since $\operatorname{div}(v-u) = A + 3E - 4O$, $\operatorname{div}(u+1) = A + B + C_1 - 3O$, $\operatorname{div}(u) = D + E + F_1 - 3O$, we have $A = -3E$, $C_1 = 3E - B$, $F_1 = -E - D$.

The proof runs as follows. Using 2-descent and the real points, we turn any excess in the Selmer group into a special quadratic character of the bitangent field (Steps 1–2), and with the explicit formula we show that no such character exists, which gives rank 3 (Step 3). At $p = 3, 5$, quadratic Chabauty reduces the possible $p$-adic positions of a new integral point to finitely many (Steps 4–6), and a Mordell–Weil sieve at 109, 233, 277 rules them all out (Step 7).

**Step 1: the bitangent field and 2-descent.** For a root $m$ of

$$p_K(z) = z^{27} - 480z^{19} - 1344z^{18} - 34560z^{11} + 70656z^{10} - 40704z^9 + 16384z^3 - 12288z - 4096$$

set $\eta = \dfrac{m(11m^{12} - 112m^4 + 112m^3)}{8(13m^9 + 16m + 8)}$, $a = m^3/2$, $b = (12m^2\eta - m^6)/8$. Then $F(u, mu+\eta) = (u^2 + au + b)^2$ and $a^2 - 4b \neq 0$. So $v = mu + \eta$ is a bitangent. The resultant with respect to $\eta$ of the two conditions $2ab = 3m\eta^2 - m + 1$, $b^2 = \eta^3 - \eta$ is $p_K(m)/4096$, so these 27 lines together with the tangent line at $O$ are all the bitangents. $p_K$ is irreducible, $K = \mathbb{Q}[m]/(p_K)$ has signature $(3, 12)$ and discriminant $D = 2^{24} \cdot 157^6 \cdot 64679^6$, and there is only one prime ideal above 2 ($e = 9$, $f = 3$) (certificate 1.1.1a). The descent value of an affine point is $mu + \eta - v$.

**Lemma 3.1.2.** *(1) $J(\mathbb{Q})[2] = 0$, the map $H^1(\mathbb{Q}, J[2]) \to K^\times/K^{\times 2}$ is injective, and the image of $\mathrm{Sel}^{(2)}(J/\mathbb{Q})$ lies in $K(\{2\}, 2)$. (2) $J(\mathbb{Q}_2)[2] = 0$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3$. (3) The 2-adic descent images of $E, B, D$ are independent. Hence these three form a basis of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$, the 2-adic descent map is injective on it, and $E, B, D$ are also independent in $J(\mathbb{Q})/2J(\mathbb{Q})$, so that $\operatorname{rank} J(\mathbb{Q}) \geq 3$.*

*Proof.* (1) is Proposition A, and $S = \{2\}$ because the component groups at the odd bad primes are trivial. (2) Since there is only one prime ideal above 2, $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ acts transitively on the 27 bitangents. A nonzero element of $J(\mathbb{Q}_2)[2]$ would have to give a codeword that is constant on the bitangents, that is, a codeword of weight 27, but the nonzero codewords have weight 12 or 16 only. Hence $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = g = 3$. (3) If we take as coordinates on $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ ($\mathfrak{p} \mid 2$, dimension 29) the parity of the exponent and the square class of the unit modulo $\mathfrak{p}^{19}$, then the images of $E, B, D$ have rank 3 (certificate 1.1.1b). □

**Step 2: real points and the strict character.** In the proof of Proposition A, $J[2]$ carries a quadratic form preserved by the Galois action, and it is isomorphic to $V = \mathbb{F}_2^6$ with $Q(v) = v_1v_2 + v_3v_4 + v_5v_6 + v_5 + v_6$; the finite bitangents correspond to $\Omega = \{w \neq 0 : Q(w) = 0\}$. Let $\langle v, w\rangle = Q(v+w) + Q(v) + Q(w)$.

**Lemma 3.1.3.** *For a subspace $U \leq V$ and a linear form $\lambda$, if $r = \#(U \cap \Omega)$, then $\sum_{w \in U\cap\Omega}(-1)^{\lambda(w)} \geq \kappa(r)$, where*

| $r$ | 0 | 1 | 2 | 3 | 5 | 7 | 9 | 11 | 15 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\kappa(r)$ | 0 | −1 | −2 | −3 | −3 | −5 | −3 | −5 | −5 | −5 |

*($r$ takes only these values).*

*Proof.* We check all 2825 subspaces and all 64 linear forms (certificate 1.1.1c). □

**Lemma 3.1.4.** *$C(\mathbb{R})$ is connected, and hence $J(\mathbb{R})/2J(\mathbb{R}) = 0$.*

*Proof.* $C$ is $g(u) = h(v)$ with $g(u) = u^4 + u$, $h(v) = v - v^3$. The minimum $m_0$ of $g$ satisfies $m_0 \le g(-\frac{1}{2}) = -\frac{7}{16}$, and since $(\frac{7}{16})^2 > \frac{4}{27}$, it is smaller than both critical values $\pm\frac{2}{3\sqrt{3}}$ of $h$. So $\{v : h(v) \ge m_0\}$ is a single half-line; on it, the two real roots of $g(u) = h(v)$ meet at the endpoint, and both tend to $O$ as $v \to -\infty$. Hence $C(\mathbb{R})$ is a single loop. The rest is [GH81]. □

**Lemma 3.1.5.** *If $\dim \mathrm{Sel}^{(2)}(J/\mathbb{Q}) > 3$, then there is a nontrivial character $\chi : \mathrm{Cl}(K) \to \{\pm 1\}$ of $\mathrm{Cl}(K)$ such that (i) $\chi = 1$ at prime ideals that are principal, and (ii) if $p \nmid \mathrm{disc}(p_K)$ and $r(p)$ is the number of roots of $p_K$ modulo $p$, then $\sum_{\mathfrak{p}|p,\, N\mathfrak{p}=p} \chi(\mathfrak{p}) \ge \kappa(r(p))$.*

*Proof.* Let $\gamma$ be a Selmer element outside the span of $\delta(E), \delta(B), \delta(D)$. By Lemma 3.1.2(3) there are $a, b, d \in \mathbb{F}_2$ such that $\gamma' = \gamma - a\delta(E) - b\delta(B) - d\delta(D)$ becomes trivial over $\mathbb{Q}_2$, and $\gamma' \neq 0$. At the real place $\gamma'$ is trivial (Lemma 3.1.4), and at odd primes it is unramified, since the reduction is good or the component group is trivial. By Lemma 3.1.2(1), the image $\epsilon \in K^\times/K^{\times 2}$ of $\gamma'$ is not 1, it is a square above 2 and positive at the real embeddings, and $K(\sqrt{\epsilon})/K$ is an unramified quadratic extension that splits at the real places. Its character is $\chi$. (ii) At $p$, $\gamma'$ is determined by the Frobenius $g \in \mathrm{GL}(V)$ and a cocycle value $c \in V$. The prime ideals of norm $p$ correspond to the $w \in \Omega$ fixed by $g$, and there $\chi = (-1)^{\langle c, w\rangle}$; so the sum is the sum of Lemma 3.1.3 for $U = \ker(g-1)$, $\lambda = \langle c, \cdot\rangle$. □

**Step 3: rank.**

**Lemma 3.1.6.** $\dim \mathrm{Sel}^{(2)}(J/\mathbb{Q}) = \mathrm{rank}\, J(\mathbb{Q}) = 3$.

*Proof.* Suppose not, and take $\chi$ as in Lemma 3.1.5. For a nontrivial quadratic character $\chi$ of $\mathrm{Cl}(K)$, the proof of Proposition B gives

$$0 \;\ge\; C_\infty - \int_0^\infty (1-f)W\,dx + \frac{4}{n}\sum_{\mathfrak{p},\, m\ge 1} \chi(\mathfrak{p})^m \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m + 1} f(m \log N\mathfrak{p}) \qquad (*)$$

We take $n = 27$, $\alpha = 1/9$, $D$ as above, $X = 10^{10}$, $T = \log X$, and let $f$ be the normalized autocorrelation of a symmetric step function (with positive integer heights) on 128 cells of width $T/128$. With $M = 10^7$ and $R = 1.1 \cdot 10^8$ we split the prime ideals into four groups. All the weights are nonnegative. (a) The 664,464 prime ideals with $N\mathfrak{p} \le M$ are all principal. For 588,850 of them this is proved with witnesses as in Lemma C, and for 75,614 with generators $g$ satisfying $|N(g)| = N\mathfrak{p}$ (certificate 1.1.1d). The sum over this part is computed from the counts per norm (certificate 1.1.1e). Norms $q \le 10^5$ are included exactly, together with all powers $q^m < X$; the larger norms are grouped into 9154 intervals, and the value at the right endpoint is used (the weight function is decreasing). The lower bound obtained in this way is $P_-$. (b) For the 9589 prime ideals with $M < N\mathfrak{p} < X$ and residue degree at least 2 we use $\chi \ge -1$ (sum $H$). (c) For $N\mathfrak{p} = p$, $M < p < R$ we use Lemma 3.1.5(ii). The distribution of $r(p)$ over the 5,638,730 primes in this range is (certificate 1.1.1e)

| $r$ | 0 | 1 | 2 | 3 | 5 | 7 | 9 | 11 | 15 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\#p$ | 2582146 | 1821326 | 563570 | 435372 | 176800 | 29325 | 26194 | 0 | 3878 | 119 |

and, using the value at the left endpoint of each interval, we obtain the lower bound $E$. (d) For $N\mathfrak{p} = p$, $R < p < X$ we use the lower bound $-5$ and Dusart's unconditional inequalities $\vartheta(x) < cx$, $\vartheta(R) > R(1 - \frac{1}{5\log^2 R})$ ($c = \frac{36261}{36260}$, [Dus10, Section 1]). By partial summation, $\sum_{R<p<X} \frac{\log p}{p+1} f(\log p) \le \mathcal{T}_R := c\int_{\log R}^T f + (c - 1 + \frac{1}{5\log^2 R}) f(\log R)$, so the contribution is at least $-\frac{20}{27}\mathcal{T}_R$. Since $M^2 > X$, the terms with $m \ge 2$ occur only in (a). All prime factors of $\mathrm{disc}(p_K) = 2^{312}3^{54}157^6\,64679^6\,333337^2\,172659335137^2$

are less than $M$ or greater than $X$, so (ii) can be used in (c) and (d). The values computed with 224-bit interval arithmetic are as follows (certificate 1.1.1f).

| $\mathcal{A}(f)$ | $P_-$ | $H$ | $E$ | $-\frac{20}{27}\mathcal{T}_R$ |
|---|---|---|---|---|
| $-1.0229409565\ldots$ | $1.1435757488\ldots$ | $-0.0000100075\ldots$ | $-0.0340749409\ldots$ | $-0.0598580721\ldots$ |

Their sum is $\mathcal{B} > 0.0266917716 > 0$. The right-hand side of $(*)$ is at least $\mathcal{B}$, a contradiction. Hence the Selmer dimension is at most 3, and the conclusion follows from Lemma 3.1.2(3) and $J(\mathbb{Q})[2] = 0$. □

**Step 4: $p$-adic heights.** Fix $p \in \{3, 5\}$ and use the Coleman–Gross height $h = \sum_v h_v$ ($\log_p p = 0$) of [CG89, BBM16]. When supports overlap we normalize by tangent vectors: at affine points we use the dual of $\omega = du/(3v^2 - 1) = -dv/(4u^3 + 1)$, and at $O$ the dual of $t = -u/v$.

**Lemma 3.1.7.** *For an integral point $P$ and a prime $\ell \neq p$ we have $h_\ell(P - O, P - O) = 0$, and for distinct $Q, Q'$ among $E, B, D$ we have $h_\ell(Q - O, Q' - O) = 0$.*

*Proof.* Since the two nodes have thickness 1, the plane model is regular over $\mathbb{Z}$; the integral sections do not pass through the nodes, and since all fibers are irreducible, the vertical correction is 0. On the smooth affine part one of $F_u$, $F_v$ is a unit, so the tangent vector dual to $\omega$ is primitive and $(P \cdot P)_\omega = 0$. Near $O$ we have $\operatorname{div}\omega = 4O$, the leading coefficient $-1$ is a unit, and $t$ is a relative parameter, so $(O \cdot O)_t = 0$. Integral points do not meet $O$. Any two of $E, B, D$ differ by $\pm 1$ in one coordinate, so their sections do not meet. □

**Lemma 3.1.8.** *Let $\omega_i = (1, u, v)\,\omega$ and $\eta_i = (5u^2v, 2uv, u^2)\,\omega$. The $\eta_i$ are differentials of the second kind with poles only at $O$, and the cup product matrix with respect to $\operatorname{Res}_O((\int \alpha)\beta)$ is $\left(\begin{smallmatrix} 0 & -I_3 \\ I_3 & 0 \end{smallmatrix}\right)$. For $P = (a, b)$, $\nu_P(Q) = \frac{v^2+bv+b^2-1}{u-a}\,\omega(Q)$ is a differential of the third kind with residue divisor $P - O$. Let $I_i(P) = \int_O^P \omega_i$, $J_i(P) = \int_O^P \eta_i$, $K(P, Q) = \int_O^Q \nu_P$ (normalized by the tangent vectors above). Then the local height at $p$ with respect to $W = \langle \eta_i \rangle$ is $h_p(P - O, Q - O) = H(P, Q) := K(P, Q) - \sum_i J_i(P) I_i(Q)$, and $\tau(P) = H(P, P)$ satisfies $d\tau = -2\sum_i \omega_i J_i$ on the affine disks on which $3v^2 - 1$ is a unit.*

*Proof.* Expanding at $O$ with $u = t^{-3}\rho$, $v = -t^{-4}\rho$, $\rho^2(\rho - 1) = -t^8 - t^9$, the leading terms of $\omega_0, \omega_1, \omega_2, \eta_0, \eta_1, \eta_2$ are $-t^4dt$, $-t\,dt$, $dt$, $5t^{-6}dt$, $2t^{-3}dt$, $-t^{-2}dt$, respectively, and the corrections start in degree 8; this gives the cup product matrix. On the curve, $(b - v)(v^2 + bv + b^2 - 1) = (u - a)(u^3 + u^2a + ua^2 + a^3 + 1)$, so the only poles of $\nu_P$ are $P$ and $O$. The bidifferential identity $d_P\nu_P(Q) - d_Q\nu_Q(P) = \sum_i(\eta_i(P)\omega_i(Q) - \omega_i(P)\eta_i(Q))$ holds, since after dividing both sides by $\omega(P)\omega(Q)$ each side becomes $5a^2b - 5u^2v + 2abu - 2auv + a^2v - bu^2$ (certificate 1.1.1g). At $O$, the coefficients of $t^0, t^1, t^4$ in $\nu_P = (-t^{-1} - at^2 + bt^3 - a^2t^5 + \cdots)dt$ are 0, so the de Rham class of $\nu_P - \sum_i J_i(P)\omega_i$ lies in $W$, and by the definition in [CG89, BBM16], $h_p = H$. Integrating the identity gives $d_P H(P, Q) = \nu_Q(P) - \sum_i \omega_i(P) J_i(Q)$. On the diagonal, the regular part $2 \cdot (-3bb'/\beta)\,da$ ($\beta = 3b^2 - 1$, $b' = db/da$) of $\nu_P(Q), \nu_Q(P)$ cancels against the $d\log\beta$ added by the tangent vector normalization, and we obtain $d\tau = -2\sum_i \omega_i J_i$. □

**Lemma 3.1.9.** *Let $I_B$ be the matrix with rows $I(E), I(B), I(D)$, let $H_B = (H(Q, Q'))_{Q,Q' \in \{E,B,D\}}$, and assume that $I_B$ is invertible. If $M = I_B^{-1} H_B (I_B^{\mathsf{T}})^{-1}$ and $q(P) = \tau(P) - I(P)\,M\,I(P)^{\mathsf{T}}$, then $q(P) = 0$ at every integral point $P$.*

*Proof.* $h$ is a symmetric bilinear form on $J(\mathbb{Q})$ ([CG89, BBM16]), and since the rank is 3, it is a quadratic form in log. By Lemma 3.1.7, $h = h_p$ among $E, B, D$, so its matrix is $M$, and at an integral point $P$ we have $h(P - O, P - O) = \tau(P)$. □

**Step 5: $p = 3$.** $C$ has good reduction at 3, and the only affine points modulo 3 are the six reductions of $A, \ldots, F_1$. We parametrize the disk with center $P_j = (a_j, b_j)$ by $u = a_j + 3s$, $s \in \mathbb{Z}_3$, and let $q_j(s) = q(P_j(s))$.

**Lemma 3.1.10.** *(1)* $I_B/3 \equiv \left(\begin{smallmatrix}1&1&0\\0&2&2\\1&1&2\end{smallmatrix}\right) \pmod 3$ *(the determinant is a unit), and* $\min v_3(M_{ij}) = -1$. *(2) The minimal valuation* $e_j$ *of the coefficients of* $q_j$ *and the reductions are as follows, and the roots of* $q_j/s$ *modulo 3 are all simple.*

| $P_j$ | $A$ | $B$ | $C_1$ | $D$ | $E$ | $F_1$ |
|---|---|---|---|---|---|---|
| $e_j$ | 2 | 1 | 1 | 1 | 1 | 1 |
| $3^{-e_j}q_j \bmod 3$ | $2s^2+2s^3$ | $2s+2s^2$ | $2s+s^2$ | $2s+2s^2$ | $s$ | $s^2$ |
| *extra roots* | 2 | 1 | 1 | 1 | 0 | 1 |

*(3) The positions* $s$ *of the six extra roots and their coordinates* $\mathbf{a}_i = I(P)I_B^{-1}$ *(basis* $E, B, D$*) are, modulo* $3^8$*, as follows.*

| $i$ | *disk* | $s$ | $\mathbf{a}_i$ | | |
|---|---|---|---|---|---|
| 0 | $A$ | 4680 | 5946 | 6246 | 1629 |
| 1 | $A$ | 1274 | 4511 | 1997 | 707 |
| 2 | $B$ | 5882 | 1542 | 2265 | 5452 |
| 3 | $C_1$ | 2620 | 1475 | 1164 | 2808 |
| 4 | $D$ | 1442 | 1405 | 250 | 6058 |
| 5 | $F_1$ | 5667 | 6218 | 5349 | 6041 |

*Proof.* Choose six functions $f_j$ in $L(7O)$ with $\operatorname{div} f_j = 4P_j + R_{j,1} + R_{j,2} + R_{j,3} - 7O$. The remaining zeros $R_{j,k}$ are simple modulo 3 and lie in three other disks. Writing the $R_{j,k}$ in terms of the disk centers and tiny integrals, the coefficient matrix of the principal divisor relations has determinant $3185 \in \mathbb{Z}_3^\times$. The right-hand sides are given exactly by Coleman reciprocity: for $\rho$ of the second kind it is $\operatorname{Res}_O(\log f_j \cdot \rho)$, and for $\nu_{P_i}$ of the third kind it is the $\log_3$ of the ratio of the leading coefficients with respect to the tangent vectors. Solving with precision $3^{20}$ determines $M$ modulo $3^{17}$ (certificate 1.1.1h). On a disk, $\tau(P_j(s)) = \tau(P_j) - 2\sum_i \int_0^s \omega_i(J_i(P_j) + \int \eta_i)$, and the expansion coefficients lie in $\mathbb{Z}_3$, so $v_3([s^n]q_j) \geq n - 1 - 2\lfloor \log_3 n \rfloor$. This is at least 3 for $n \geq 6$, so the reductions in the table take the tail into account. We have $q_j(0) = 0$, and (2), (3) follow from Hensel's lemma. The eight digits in the table are within the remaining precision. □

**Step 6:** $p = 5$**.** The affine points modulo 5 are the reductions of the six points and $(3, 2)$; the latter lifts to $P_6 = (3, \beta)$, $\beta^3 - \beta + 84 = 0$, $\beta \equiv 309087 \pmod{5^8}$. We parametrize by $u = a_j + 5s$.

**Lemma 3.1.11.** *(1)* $5^{-1}I_B \equiv \left(\begin{smallmatrix}3&3&2\\2&0&0\\1&3&0\end{smallmatrix}\right) \pmod 5$ *(the determinant is a unit), and* $\min v_5(M_{ij}) = -1$. *(2) The minimal valuation of the coefficients of every* $q_j$ *is 1, and*

| $P_j$ | $A$ | $B$ | $C_1$ | $D$ | $E$ | $F_1$ | $P_6$ |
|---|---|---|---|---|---|---|---|
| $5^{-1}q_j \bmod 5$ | $4s+s^2$ | $3s+2s^2$ | $3s+s^2$ | $3s+3s^2$ | $2s$ | $4s+3s^2$ | $4s+4s^2$ |
| *extra roots* | 1 | 1 | 1 | 1 | 0 | 1 | 2 |

*(*$P_6$ *is not a rational point, so both of its roots are extra roots). (3) The positions and the coordinates* $\mathbf{a}'_j$ *of the seven extra roots are, modulo* $5^8$*, as follows.*

| $j$ | *disk* | $s$ | $\mathbf{a}'_j$ | | |
|---|---|---|---|---|---|
| 0 | $A$ | 88061 | 182268 | 389041 | 117968 |
| 1 | $B$ | 51781 | 9880 | 216347 | 307132 |
| 2 | $C_1$ | 291387 | 125051 | 375010 | 46930 |
| 3 | $D$ | 332159 | 759 | 70457 | 158427 |
| 4 | $F_1$ | 49757 | 79377 | 350530 | 127046 |
| 5 | $P_6$ | 325535 | 352126 | 189681 | 390420 |
| 6 | $P_6$ | 235554 | 361850 | 252022 | 388570 |

*Proof.* As in Step 5. We use seven functions in $L(NO)$ over $\mathbb{Q}(\beta)$, $N = 6,7,7,7,7,7,9$, and the determinant of the relation matrix is $452 \in \mathbb{Z}_5^\times$. For the tail, $v_5([s^n]q_j) \geq n - 1 - 2\lfloor \log_5 n \rfloor$, which is at least 2 for $n \geq 3$ (certificate 1.1.1i). □

**Step 7: torsion, saturation, Mordell–Weil sieve.**

**Lemma 3.1.12.** *$J(\mathbb{Q})$ is torsion-free, and the index of $\Gamma = \langle E, B, D\rangle$ is prime to 30.*

*Proof.* $\#J(\mathbb{F}_3) = 91$ and $\#J(\mathbb{F}_5) = 226$ (certificate 1.1.1j) are coprime, so by [Kat81, Appendix] the torsion is 0. If a prime $\ell$ divides the index, then there is $R$ with $\ell R = a_1E + a_2B + a_3D$ where the $a_k$ are not all multiples of $\ell$. If $\ell = 2$, this contradicts Lemma 3.1.2(3). If $\ell = 3$: since $3 \nmid 91$, we have $\log J(\mathbb{Q}_3) \subset 3\mathbb{Z}_3^3$ (Lemma E), and since the rows of $I_B$ form a basis of $3\mathbb{Z}_3^3$ (Lemma 3.1.10(1)), we get $a_k/3 \in \mathbb{Z}_3$, a contradiction. The case $\ell = 5$ is the same. □

So every $R \in J(\mathbb{Q})$ can be written as $R = a_1E + a_2B + a_3D$ with $a_k \in \mathbb{Z}_{(2)} \cap \mathbb{Z}_{(3)} \cap \mathbb{Z}_{(5)}$, and at an auxiliary prime $q$ the projection of $R$ onto the $\{2,3,5\}$-primary part is determined by the residue classes of the $a_k$. Arithmetic in $J(\mathbb{F}_q)$ is done by Riemann–Roch computations with the basis $u^iv^j$ ($j \le 2$, $3i + 4j \le m$) of $L(mO)$, and elements are compared exactly by their reduced representatives. Minimality forces $h^0(D) = 1$: otherwise a section vanishing at $O$ would give a representative of smaller degree.

**Lemma 3.1.13.** *The only integral points of $C$ are $A, B, C_1, D, E, F_1$.*

*Proof.* If there is another integral point $P$, then by Lemmas 3.1.9, 3.1.10, 3.1.11, $P$ is a 3-adic extra root $i$ and also a 5-adic extra root $j$ (if it were the root at a center, it would be equal in $\mathbb{Q}_p$ to a known point). The coefficient vector $\mathbf{a}$ of $P - O$ is $\mathbf{a}_i$ modulo $3^8$ and $\mathbf{a}'_j$ modulo $5^8$. By [BS10], at each $q$ the reduction of $P$ is a point of $C(\mathbb{F}_q)$, and its primary projection must be the value determined by $\mathbf{a}$. The data for the primes used are as follows (certificate 1.1.1j).

| $q$ | $\#C(\mathbb{F}_q)$ | $\#C(\mathbb{F}_{q^2})$ | $\#C(\mathbb{F}_{q^3})$ | $\#J(\mathbb{F}_q)$ |
|---|---|---|---|---|
| 109 | 109 | 12243 | 1296898 | 1303500 |
| 233 | 259 | 54447 | 12648664 | 14102424 |
| 277 | 300 | 77454 | 21247200 | 23117400 |

Imposing the 3-primary and the 5-primary conditions on the same curve point at $q = 109, 277$, the values of $j$ that remain for each $i$ are as follows.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $q = 109$ | $\{2,6\}$ | $\{0,4,5\}$ | $\{0,2\}$ | $\{0,4,5\}$ | $\{0,2\}$ | $\{0,2\}$ |
| $q = 277$ | $\{4\}$ | $\varnothing$ | $\{2,6\}$ | $\varnothing$ | $\{4\}$ | $\{4\}$ |

The only remaining pair is $(2,2)$, and its coefficients are $\mathbf{a} \equiv (3,78,25) \pmod{81}$, $\mathbf{a} \equiv (51,10,55) \pmod{125}$. At $q = 233$ the 2-primary subgroup is $(\mathbb{Z}/2)^3$, and the projections of $E, B, D$ form a basis of it. The only curve points with matching 3-primary coordinates are $(20,173)$ and $(78,144)$, and their 2-primary coordinates are $B$ and 0, so $a_1 \equiv a_3 \equiv 0 \pmod 2$. At $q = 277$ the only curve point satisfying both conditions is $(44,20)$; the 2-primary subgroup is cyclic of order 8, generated by the projection $U$ of $E$, and $B \mapsto 4U$, $D \mapsto 5U$, $(44,20) - O \mapsto 3U$. Hence $a_1 + 4a_2 + 5a_3 \equiv 3 \pmod 8$, that is, $a_1 + a_3 \equiv 1 \pmod 2$, a contradiction. □

*Proof of Theorem 3.1.1.* Under $(x,y) = (-u,-v)$ the six points of Lemma 3.1.13 become the six solutions in the theorem. $J(\mathbb{Q}) \cong \mathbb{Z}^3$ follows from Lemmas 3.1.6, 3.1.12. □

## 3.2 $x^4 - y^3 + x - y = 0$ ($H = 28$)

**Theorem 3.2.1.** *The only integer solutions of $x^4 - y^3 + x - y = 0$ are $(x,y) = (-1,0), (0,0), (1,1)$.*

**Setup.** Setting $u = -y$, $z = x$, the equation becomes

$$C: \quad u^3 + u + z^4 + z = 0$$

The projective closure $z^4 + u^3w + uw^3 + zw^3 = 0$ is a smooth plane quartic (genus 3). At the point at infinity $\infty = (1:0:0)$ the tangent line $w = 0$ meets the curve with multiplicity 4, as $z^4 = 0$, so $\infty$ is a rational hyperflex. Theorem 3.2.1 follows immediately from the following proposition.

**Proposition 3.2.2.** $C(\mathbb{Q}) = \{\infty, (0,0), (0,-1), (-1,1)\}$.

Indeed, the affine points $(u,z) = (0,0), (0,-1), (-1,1)$ give $(x,y) = (z,-u) = (0,0), (-1,0), (1,1)$.

The proof has four steps. We determine the bitangent field $K$, show $\mathrm{Cl}(K)[2] = 0$ with Proposition B (Lemma 3.2.3), use this to show by 2-descent that the rank is at most 2 (Lemma 3.2.4), and finish with Chabauty–Coleman at $p = 3$ (Lemma 3.2.5).

**Step 1: the bitangent field.** The slopes of the 27 bitangents other than the tangent line at $\infty$ are the roots of

$$f(m) = m^{27} + 480m^{19} - 1344m^{18} - 34560m^{11} - 70656m^{10} - 40704m^9 - 16384m^3 + 12288m - 4096$$

$f$ is irreducible (certificate 1.1.2a), and $K = \mathbb{Q}[m]/(f)$ has signature $(3,12)$ and discriminant $D = 2^{24} \cdot 277^6 \cdot 66943^6$. The bad primes of the curve are 277 and 66943. At both of them the reduction has only one node, of thickness 1, so the Tamagawa number is 1, and hence the descent image is unramified at these two primes. Therefore $S = \{2\}$ suffices. There is only one prime ideal above 2 (ramification index 9, residue degree 3).

**Step 2: the class group.**

**Lemma 3.2.3.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (3,12)$, $D$ as above, and $T = \log 10^8$. The window is a step function on 256 cells of equal width, with positive integer heights (the input of certificate 1.1.2d). Two kinds of data are needed.

(i) There are 5,763,020 prime ideals of norm less than $10^8$ in total, and all the counts $a(q)$ by norm are computed (certificate 1.1.2b).

(ii) All 349,551 prime ideals of norm at most $5 \cdot 10^6$ have a witness as in Lemma C (certificate 1.1.2c). So we set $k(q) = a(q)$ if $q \le 5 \cdot 10^6$, and $k(q) = 0$ for larger $q$.

With these data, $B^-(f) > 0.000875203229\ldots > 0$ (certificate 1.1.2d). The computation uses exact rational coefficients and directed-rounding interval arithmetic (192 bits), so rounding errors cannot change the conclusion. By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.2.4.** $\operatorname{rank} J(\mathbb{Q}) \le 2$.

*Proof.* The hypotheses of Proposition A were checked above. So $J(\mathbb{Q})[2] = 0$ and $\delta$ is injective. Since $\mathrm{Cl}(K)[2] = 0$ by Lemma 3.2.3,

$$\dim_{\mathbb{F}_2} K(S,2) = (r_1 + r_2) + \#\{\mathfrak{p} \mid 2\} = 15 + 1 = 16$$

Indeed, 16 explicit elements supported on $S$ form a basis of this space. Their independence is checked with quadratic characters at the primes 487, 491, 499, 503, 509, 521, 523, 541 (certificate 1.1.2a).

We impose conditions on this 16-dimensional space one after another. After imposing the condition that the norm is a square, we impose the local conditions at the good primes 487, 491, 499, 503

in turn, and the dimension of the candidate space becomes $10, 6, 4, 3$. At 2 the bitangent orbit is transitive, of size 27. So, because the weights of the bitangent code are $12, 16$, we have $J(\mathbb{Q}_2)[2] = 0$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = g = 3$. The three 2-adic images are independent, so they fill this space, and this condition reduces the candidate dimension from 3 to 2. Since $J(\mathbb{Q})[2] = 0$, $\operatorname{rank} J(\mathbb{Q}) \leq 2$. □

**Step 4: Chabauty–Coleman at $p = 3$.** $C$ has good reduction at 3, because on the affine part $\partial F/\partial u = 3u^2 + 1 \equiv 1 \pmod 3$, and in the chart at infinity the derivative is also a unit. An integral basis of the regular differentials is

$$\omega_0 = \frac{dz}{3u^2+1}, \quad \omega_1 = \frac{z\,dz}{3u^2+1}, \quad \omega_2 = \frac{u\,dz}{3u^2+1}$$

$C(\mathbb{F}_3)$ consists of the four points $\infty, (0,0), (0,2), (2,1)$, so there are also four residue disks. The four known rational points lie one in each disk, since $(0,-1) \equiv (0,2)$ and $(-1,1) \equiv (2,1)$.

**Lemma 3.2.5.** $\operatorname{rank} J(\mathbb{Q}) = 2$. *Moreover, a 3-adic lift of the differential $\omega = 2\omega_0 + \omega_1 + \omega_2$ annihilates all logarithms of $J(\mathbb{Q})$, and it is nonzero modulo 3 on all four disks.*

*Proof.* For $P_0 = (0,0)$, $P_1 = (0,-1)$, explicit functions $h_i$ satisfy

$$\operatorname{div}(h_i) = 28P_i + E_i - 31\infty$$

Here $E_i$ is an irreducible divisor of degree 3. This identity is checked exactly through the pole order 31, the Taylor order 28 at $P_i$, and the norm identity $\operatorname{Res}_u(F, h_i) = c_i(z - z(P_i))^{28} d_i(z)$ (certificate 1.1.2e). $E_i$ is unramified at 3, and its $z$-coordinates reduce to the fibers $z = 1$ and $z = 0$, respectively. Both fibers are linearly equivalent to $3\infty$. Hence the 3-adic logarithm of

$$28[P_i - \infty] = -[E_i - 3\infty]$$

is computed as a sum (trace) of tiny integrals starting from the points of $E_i$, and dividing it by $-28$ gives the logarithm of $[P_i - \infty]$.

Computing modulo $3^{16}$ with 18 terms, the logarithms with respect to $(\omega_0, \omega_1, \omega_2)$ are, modulo $3^{10}$,

$$\log[P_0 - \infty] \equiv (57309, 48831, 7839), \qquad \log[P_1 - \infty] \equiv (40674, 56691, 3162)$$

(certificate 1.1.2e). The discarded $k$-th term has valuation at least $k - v_3(k)$, which is at least 17 for $k \geq 19$, so this precision is guaranteed. The two logarithms are linearly independent, so $\operatorname{rank} J(\mathbb{Q}) \geq 2$, and together with Lemma 3.2.4 we get $\operatorname{rank} J(\mathbb{Q}) = 2$. The components of the cross product of the two vectors have common valuation 2, and the primitive annihilator obtained by dividing by $3^2$ is $(2,1,1)$ modulo 3. The annihilator kills the subgroup generated by the two logarithms, and this subgroup has finite index in $J(\mathbb{Q})$, so $\omega$ kills all logarithms of $J(\mathbb{Q})$.

Finally we evaluate $\omega \bmod 3 = (2 + z + u)\,dz$ at the centers of the disks. It is 2 at $(0,0)$, 1 at $(0,2)$, and 2 at $(2,1)$. In the chart at infinity, with $t = z/u$, $w = 1/u$, the basis becomes $(-w, -t, -1)\,dt/(1 + 3(1+t)w^2)$, and the value at the center is $-1 \equiv 2$. All four values are nonzero. □

*Proof of Proposition 3.2.2.* Take one disk, and let $t$ be a local parameter that vanishes at the known rational point $P$ in it. At points of the disk $t \in 3\mathbb{Z}_3$, so we write $t = 3s$, $s \in \mathbb{Z}_3$. By Lemma 3.2.5, $\omega = \sum_{k \geq 0} a_k t^k\,dt$ with $a_0$ a 3-adic unit. Integrating from $P$ gives

$$\int \omega = \sum_{k \geq 1} \frac{a_{k-1}}{k} (3s)^k$$

and here the coefficient of the linear term in $s$ has valuation exactly 1. The coefficients of the terms with $k \geq 2$ have valuation at least $k - v_3(k) \geq 2$. The constant term is 0. By Strassmann's theorem this integral has at most one zero in the disk ($s = 0$). By [Col85, MP12], every rational point in the disk is a zero of this integral, so each disk contains at most one rational point. Each of the four disks contains one known point, so $C(\mathbb{Q})$ consists of these four points only. □

### 3.3 $x^4 + y^3 + xy + 1 = 0$ ($H = 29$)

**Theorem 3.3.1.** *The only integer solutions of* $x^4 + y^3 + xy + 1 = 0$ *are* $(x, y) = (0, -1), (1, -1)$.

**Setup.** Let $J$ denote the Jacobian of the smooth projective model of the curve. We do not change coordinates.

$$C: \quad F(x,y) = x^4 + y^3 + xy + 1 = 0, \qquad P_0 = (0,-1), \quad P_1 = (1,-1).$$

The projective closure $X^4 + Y^3Z + XYZ^2 + Z^4 = 0$ has a single point at infinity, $O = (0:1:0)$. In the chart $t = x/y$, $w = 1/y$ the equation is $t^4 + w + tw^2 + w^4 = 0$; at $O$ the derivative with respect to $w$ is 1, and the tangent line $w = 0$ meets the curve as $t^4 = 0$, so $O$ is a smooth rational hyperflex.

In characteristic other than 2, 3, 5, an affine singular point satisfies, from $F_x = 4x^3 + y = 0$, $F_y = 3y^2 + x = 0$, $F = 0$, the relations $y = -4x^3$, $x^5 = -1/48$, $x^4 = 3/5$, that is, $x = -5/144$. Hence the characteristic divides $3 \cdot 144^4 - 5^5 = 17^2 \cdot 4463467$ (4463467 is prime). In characteristics 2 and 3 the only point at which $F_x$, $F_y$ vanish is $(0,0)$, but $F(0,0) = 1$; in characteristic 5 and at infinity the curve is also smooth (certificate 1.1.3a). At the two bad primes the only singular point is the reduction of $(x_c, y_c) = (-5/144,\ -4x_c^3)$, and it is an ordinary node with unit Hessian. At a lift of the critical point the valuation of $F$ is 2 at 17 and 1 at 4463467, so the thickness of the node is 2 and 1, respectively (certificate 1.1.3a). A plane quartic with only one node is geometrically irreducible (two distinct components meet at least three times, counted with multiplicity). So at 4463467, where the node has thickness 1, the component group of the Jacobian is trivial. At 17 the component group may be nontrivial, so we put 17 into $S$.

The proof has four steps. We determine the bitangent field $K$ (Step 1), show $\mathrm{Cl}(K)[2] = 0$ (Step 2), obtain rank $J(\mathbb{Q}) \le 2$ by 2-descent (Step 3), and finish with Chabauty–Coleman at $p = 3$ (Step 4).

**Step 1: the bitangent field.** If the line $y = mx + b$ is a bitangent, then the slope $m$ is a root of

$$\begin{aligned} p_K(m) = {} & m^{27} - 48m^{22} + 144m^{17} + 17280m^{15} + 832m^{12} + 64512m^{10} \\ & - 2560m^7 + 27648m^5 - 110592m^3 - 1024m^2 + 4096 \end{aligned}$$

$p_K$ is irreducible, and for each root $m$ there is one $b \in \mathbb{Q}(m)$ for which $F(x, mx + b)$ is the square of a monic quadratic (certificate 1.1.3a). So the 27 finite bitangents form a single Galois orbit, and the remaining one is the tangent line at $O$. $K = \mathbb{Q}[m]/(p_K)$ has signature $(3, 12)$ and discriminant $D = 2^{20} \cdot 4463467^6$. The prime ideals above 2 have $(e, f)$ equal to $(1,1), (1,1), (5,1), (5,1), (5,1), (5,2)$, and there are 9 prime ideals above 17. The descent value of an affine point is $-(y - mx - b)$, and its leading coefficient at $O$ is 1.

**Step 2: the class group.**

**Lemma 3.3.2.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (3, 12)$, $D$ as above, and $T = \log 10^6$. The window is a symmetric step function on 64 cells of equal width, with positive integer heights. Two kinds of data are needed.

(i) There are 78,493 prime ideals of norm less than $10^6$ in total, and all the counts $a(q)$ by norm are computed (certificate 1.1.3b).

(ii) Each of the 1,260 prime ideals of norm at most $10^4$ contains some $g \in \mathfrak{p}$ with $|N(g)| = N\mathfrak{p}$ (certificate 1.1.3b). This is a witness for Lemma C with cofactor 1, so these ideals are principal. So we set $k(q) = a(q)$ if $q \le 10^4$, and $k(q) = 0$ for larger $q$.

Computing in 224-bit interval arithmetic gives $B^-(f) > 0.0642182715 > 0$ (certificate 1.1.3c). By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.3.3.** $\operatorname{rank} J(\mathbb{Q}) \leq 2$.

*Proof.* By Proposition A, $J(\mathbb{Q})[2] = 0$, and the descent map sends $J(\mathbb{Q})/2J(\mathbb{Q})$ injectively into the part of $K(S,2)$, $S = \{2, 17\}$, on which the norm is a square. By Lemma 3.3.2,

$$\dim_{\mathbb{F}_2} K(S,2) = (r_1 + r_2) + \#\{\mathfrak{p} \mid 2 \cdot 17\} = 15 + 15 = 30$$

There are 30 explicit elements whose ideals involve only prime ideals above 2 and 17, and the matrix formed by their valuation parities and their quadratic residue symbols at auxiliary primes has rank 30, so they form a basis (certificate 1.1.3d). We impose conditions on this space one after another.

(a) The condition that the norm is a square (sign, and parity of the valuations at 2 and 17) brings the dimension to 27.

(b) At a good prime $p$ the local image is the image of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \cong J(\mathbb{F}_p)/2J(\mathbb{F}_p)$, and for $p \geq 487$ it is generated by the images of the points of $C(\mathbb{F}_p)$. Otherwise there would be a connected étale double cover (of genus 5) in which all $\mathbb{F}_p$-points split, and the Weil bound ([Wei48]) would require $2(p + 1 - 6\sqrt{p}) \leq p + 1 + 10\sqrt{p}$, so $p < 484$. If a coordinate vanishes at a point of tangency with a bitangent, that coordinate is recovered from the condition that the norm is a square. Imposing the conditions at $p = 487, 491, 499, 503, 509, 521$ in turn, the dimension becomes $25, 22, 16, 14, 12, 7$ (certificate 1.1.3d).

(c) At 2. The orbits of the wild inertia group on the bitangents have size a power of 2 that divides the ramification index 1 or 5, so they have size 1. The action on the bitangents is faithful, so the inertia group is tame and cyclic, and its image has order 5. The nontrivial irreducible $\mathbb{F}_2$-representation of the cyclic group of order 5 is 4-dimensional, so the inertia-invariant subspace of $J[2]$ is 2-dimensional. The two bitangents corresponding to the two prime ideals with $(e, f) = (1, 1)$ are distinct nonzero vectors fixed by the decomposition group, so they span this 2-dimensional space. Hence $\dim J(\mathbb{Q}_2)[2] = 2$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3 + 2 = 5$. The images of the five 2-adic points, determined modulo $2^{44}$,

$$(2,\ 12109782689869), \quad (4,\ 6831052190827), \quad (3,\ 10504516484706),$$
$$(477564860141,\ 1), \quad (7164285329697,\ 3).$$

are independent. At each prime ideal $\mathfrak{p}$ above 2 the square class of a unit is determined modulo $\mathfrak{p}^{2e+1}$, and the valuation of the approximation error is greater than the valuation of the value plus $2e$, so these square classes are exact. Hence these five images span the whole local image, and this condition brings the dimension from 7 down to 2 (certificate 1.1.3d).

Since $J(\mathbb{Q})[2] = 0$, $\operatorname{rank} J(\mathbb{Q}) \leq 2$. □

**Step 4: Chabauty–Coleman at $p = 3$.** $C$ has good reduction at 3. An integral basis of the regular differentials is $(\omega_0, \omega_1, \omega_2) = (1, x, y)\,dx/(3y^2 + x)$, or $-(1, x, y)\,dy/(4x^3 + y)$ where the denominator vanishes. The only affine points modulo 3 are $(0, 2)$ and $(1, 2)$, which are the reductions of $P_0$ and $P_1$, respectively. Let $L_i = \log[P_i - O] \in \mathbb{Q}_3^3$.

**Lemma 3.3.4.** $\operatorname{rank} J(\mathbb{Q}) = 2$. *Moreover,* $L_0 \equiv (0, 6, 1) \pmod 9$, $v_3((L_0)_0) \geq 4$, *and there is a vector* $T$ *with* $3L_1 + L_0 + T = 0$, $T \equiv (0, 6, 0) \pmod 9$. *The vector* $\lambda = (L_0 \times T)/3$ *lies in* $\mathbb{Z}_3^3$, *satisfies* $\lambda \equiv (1, 0, 0) \pmod 3$, *and annihilates all logarithms of* $J(\mathbb{Q})$.

*Proof.* For the line $y = x/3 - 1$ we have $F(x, x/3 - 1) = x^3(x + 1/27)$, so its divisor is $3P_0 + Q - 4O$ with $Q = (-1/27, -82/81)$. Since $t(Q) = 3/82 \in 3\mathbb{Z}_3$, $Q$ lies in the disk of $O$, and $3L_0 = -\int_O^Q \omega$. In the chart at infinity, $\omega = -(w, t, 1)\,dt/(1 + 2tw + 4w^3)$ and $w \in -t^4 + t^5\mathbb{Z}_3[[t]]$, so the inverse of the denominator lies in $1 + t^5\mathbb{Z}_3[[t]]$. For $t \in 3\mathbb{Z}_3$ the integrated term of degree $n$ has valuation at least $n - v_3(n)$. So the first component consists only of terms of degree at least 5, and its valuation is at least 4 even after dividing by 3; modulo 9, the second component is $t(Q)^2/6 \equiv 6$ and the third is $t(Q)/3 = 1/82 \equiv 1$. The tangent line $y = -(3x + 1)/4$ at $P_1$ gives $F(x, -(3x + 1)/4) =$

$(x-1)^2(64x^2+101x+63)/64$. The roots of the quadratic factor lie in $\mathbb{Z}_3$, and $a_0 \equiv 0$, $a_1 \equiv 7 \pmod 9$. The corresponding points $A$, $B$ reduce to $P_0$, $P_1$, respectively. From $\operatorname{div} = 2P_1 + A + B - 4O$ we get $3L_1 + L_0 + T = 0$ with $T = \int_{P_0}^{A} \omega + \int_{P_1}^{B} \omega$. With the parameter $s = y + 1$ at $P_0$ we have $s(A) \equiv 3 \pmod 9$, and the constant term of the differential is $(1, 0, -1)\, ds$. With $s = x - 1$ at $P_1$ we have $s(B) \equiv 6 \pmod 9$, and the constant term is $(1, 1, -1)\, ds/4$. The higher coefficients lie in $\mathbb{Z}_3$, and $n - v_3(n) \geq 2$ for $n \geq 2$, so $T \equiv (0, 6, 0) \pmod 9$ (certificate 1.1.3e). Since $L_0 \times T \equiv (3, 0, 0) \pmod 9$, the vectors $L_0$ and $T$, and hence $L_0$ and $L_1$, are independent. So $\operatorname{rank} J(\mathbb{Q}) \geq 2$, and together with Lemma 3.3.3 the rank is 2. The three components of $L_0 \times T$ have valuations 1, 2, 3, so $\lambda \in \mathbb{Z}_3^3$ and $\lambda \equiv (1, 0, 0) \pmod 3$. $\lambda$ annihilates $L_0$ and $T$, and hence $L_1$. Since the rank is 2, $\lambda$ annihilates all logarithms of $J(\mathbb{Q})$. □

**Lemma 3.3.5.** *The only integral points of $C$ are $P_0$, $P_1$.*

*Proof.* An integral point reduces modulo 3 to an affine point, so it lies in the disk of $P_0$ or in the disk of $P_1$. On the disk of $P_0$ we have $F_x \equiv -1$, so $s = y + 1$ is an integral parameter; on the disk of $P_1$ we have $F_y \equiv 1$, so $s = x - 1$ is one. By Lemma 3.3.4, $\lambda \cdot \omega = (c_0 + c_1 s + \cdots)\, ds$ with $c_k \in \mathbb{Z}_3$, and $c_0$ is a unit, since it is $\lambda \cdot (1, 0, -1) \equiv 1$ at $P_0$ and $\lambda \cdot (1, 1, -1)/4 \equiv 1/4$ at $P_1$. Setting $s = 3z$, $z \in \mathbb{Z}_3$, and integrating from the center gives

$$\int \lambda \cdot \omega = 3c_0 z + \sum_{n \geq 2} \frac{3^n c_{n-1}}{n} z^n$$

and each term of the sum has valuation at least 2. After division by $3z$ we get a unit on all of $\mathbb{Z}_3$, so the only zero is $z = 0$. By [Col85, MP12], the rational points in a disk are zeros of this integral, so the only integral point in each disk is its center. □

*Proof of Theorem 3.3.1.* This follows from Lemma 3.3.5 and Lemma 3.3.4. Substitution shows that the two points are solutions. □

## 3.4 $x^4 + y^3 + 2x - y = 0$ ($H = 30$)

**Theorem 3.4.1.** *The only integer solutions of $x^4 + y^3 + 2x - y = 0$ are $(-8, -16)$, $(0, -1)$, $(0, 0)$ and $(0, 1)$.*

**Setup.** Let $J$ denote the Jacobian of the smooth projective model of the curve. Setting $u = -y$, $v = x$, the equation becomes

$$C: \quad F(u, v) = v^4 - u^3 + u + 2v = 0$$

and the integer solutions correspond bijectively to the integral points of $C$ via $(x, y) = (v, -u)$. The known points are

$$P_0 = (0, 0), \quad P_1 = (1, 0), \quad P_{-1} = (-1, 0), \quad P_* = (16, -8)$$

which in the original coordinates are $(0, 0)$, $(0, -1)$, $(0, 1)$, $(-8, -16)$, respectively. There is a single point at infinity, $O$. In the chart $t = v/u$, $w = 1/u$ the equation is $t^4 - w + (1 + 2t)w^3 = 0$, $w = t^4 + \cdots$, so $O$ is a smooth rational hyperflex. Let $G_i = [P_i - O]$. Since $\operatorname{div}(u + 2v) = 3P_0 + P_* - 4O$ and $\operatorname{div}(v) = P_{-1} + P_0 + P_1 - 3O$, we have $G_* = -3G_0$, $G_{-1} = -G_0 - G_1$.

In odd characteristic other than 3, an affine singular point satisfies $3u^2 = 1$, $2v^3 = -1$, $12F - 4uF_u - 3vF_v = 8u + 18v = 0$, and hence $243v^2 - 16 = 0$. We have $\operatorname{Res}(243v^2 - 16, 2v^3 + 1) = 14332523 = 83 \cdot 172681$. In characteristic 3, $F_u = 1 - 3u^2 \equiv 1$, and the point at infinity is smooth in every odd characteristic. At 83 and 172681 the only singular point is the reduction of $(u_c, v_c) = (2187/128, -243/32)$, which is an ordinary node, and since $F(u_c, v_c) = -3482803089/2097152$ has valuation 1, its thickness is 1. So the two fibers are geometrically irreducible and the component groups are trivial (certificate 1.1.4a). Modulo 2 the plane model is singular at $(1, 0)$. Therefore in Step 4 we use explicit analytic disks instead of 2-adic residue disks.

The proof has six steps. We determine the bitangent field (Step 1), show $\mathrm{Cl}(K)[2] = 0$ (Step 2), and show by 2-descent that the rank is at most 2 (Step 3). We fix 2-adic analytic disks covering the integral

points (Step 4), obtain from 2-adic logarithms that the rank is 2, together with the logarithm lattice (Step 5), and determine the integral points disk by disk (Step 6).

**Step 1: the bitangent field.** If the line $u = mv + \eta$ is a bitangent, then $m$ is a root of

$$p_K(m) = m^{27} - 480m^{19} + 2688m^{18} - 34560m^{11} - 141312m^{10} - 162816m^9 + 16384m^3 - 49152m + 32768$$

and for each root there is one $\eta \in \mathbb{Q}(m)$ for which $F(mv + \eta, v)$ is the square of a monic quadratic (certificate 1.1.4a). Since $p_K$ is irreducible, the 27 finite bitangents form a single Galois orbit, and the remaining one is the tangent line at $O$. $K = \mathbb{Q}[m]/(p_K)$ has signature $(3, 12)$ and discriminant $D = 2^{28} \cdot 83^6 \cdot 172681^6$, and the three prime ideals above 2 have $(e, f)$ equal to $(1, 1), (10, 1), (16, 1)$. The descent value is $u - mv - \eta$ (with leading coefficient 1 at $O$), and at $G_0$, $G_1$ it is $-\eta$, $1 - \eta$, respectively.

**Lemma 3.4.2.** *$J(\mathbb{Q})[2] = 0$, and $\mathrm{Sel}^{(2)}(J/\mathbb{Q})$ maps injectively into $K(\{2\}, 2)$. Moreover, $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)[2] \leq 1$ and $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \leq 4$.*

*Proof.* The first claim is Proposition A, and $S = \{2\}$ because the component groups at the odd bad primes are trivial. The codeword given by an element of $J(\mathbb{Q}_2)[2]$ is invariant under the decomposition group, so its support is a union of orbits, which have sizes $1, 10, 16$. Nonzero codewords have weight 12 or 16, so the only possibility is the single orbit of size 16. Hence there is at most one nonzero invariant element, and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = g + \dim J(\mathbb{Q}_2)[2] \leq 4$. □

**Step 2: the class group.**

**Lemma 3.4.3.** *$\mathrm{Cl}(K)[2] = 0$.*

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (3, 12)$, $D$ as above, and $T = \log(5 \cdot 10^8)$. The window is a symmetric step function on 64 cells of equal width, with positive integer heights. Two kinds of data are needed.

(i) There are 26,362,584 prime ideals of norm less than $5 \cdot 10^8$ in total, and all the counts $a(q)$ by norm are computed (certificate 1.1.4b).

(ii) All 150,219 prime ideals of norm at most $2.02 \cdot 10^6$ have a witness as in Lemma C (certificate 1.1.4c). So we set $k(q) = a(q)$ if $q \leq 2.02 \cdot 10^6$, and $k(q) = 0$ for larger $q$.

Computing with directed-rounding interval arithmetic gives $B^-(f) > 1.0015 \cdot 10^{-4} > 0$ (certificate 1.1.4d). By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.4.4.** *$\mathrm{rank}\, J(\mathbb{Q}) \leq 2$.*

*Proof.* By Lemma 3.4.3, $\dim K(\{2\}, 2) = r_1 + r_2 + 3 = 18$. There are 18 explicit elements whose ideals involve only prime ideals above 2, and their square classes in the three completions above 2 alone already have rank 18, so they form a basis (certificate 1.1.4e). We impose conditions on this space one after another. (a) Sign of the norm and parity of the 2-adic valuation of the norm: dimension 16. (b) Images of the points of $C(\mathbb{F}_p)$ at the good primes $p = 487, 491, 499, 503, 509, 521, 523$: dimensions $12, 9, 6, 4, 4, 4, 4$ (certificate 1.1.4e). For $p \geq 487$ the images of these points generate the whole local image. Otherwise there would be a connected étale double cover (of genus 5) in which all $\mathbb{F}_p$-points split, which contradicts the Weil bound ([Wei48]). The one coordinate that is missing at a point of tangency with a bitangent is recovered from the norm condition. (c) At 2: the images of the 2-adic points $(0, 0)$, $(1, 0)$, the point with $v = 2$ and $u$ even ($u \equiv 29760316588 \pmod{2^{36}}$), and the point with $t = 2$ in the chart at infinity ($w \equiv 59134464016 \pmod{2^{36}}$) are independent in the three completions above 2 (certificate 1.1.4e). In each approximation the valuation of the error is greater than the valuation of the value plus $2e$, so the square classes are exact. By Lemma 3.4.2 these four span the whole local image, and this condition brings the dimension from 4 down to 2. Since $J(\mathbb{Q})[2] = 0$, $\mathrm{rank}\, J(\mathbb{Q}) \leq 2$. □

**Step 4: 2-adic analytic disks.**

**Lemma 3.4.5.** *An integral point $(u, v)$ of $C$ lies in one of the three disks of (i), (ii) below. (i) and (ii) are analytic parametrizations that converge on a disk larger than the closed unit disk, and (iii) is one that converges on the open unit disk $|t| < 1$.*

*(i) Even disk: $v = 2t$, $t \in \mathbb{Z}_2$, $u = u_0(v)$. Here $u_0 \in \mathbb{Z}_2[[v]]$ is the solution of $u - u^3 = -2v - v^4$, $u_0(0) = 0$.*

*(ii) Odd disks ($\varepsilon = \pm 1$): $u = \varepsilon + 4r$, $v = 4t$, $t \in \mathbb{Z}_2$. Here $r = r_\varepsilon(t) \in \mathbb{Z}_2[[t]]$ is the solution of $r + 6\varepsilon r^2 + 8r^3 = t + 32t^4$, $r(0) = 0$, and $v_2([t^j]r) \geq j - 1$.*

*(iii) Disk at infinity: $t = v/u$, $w = 1/u$, and $w = w(t) \in t^4 + t^5\mathbb{Z}_2[[t]]$ is the solution of $t^4 - w + (1 + 2t)w^3 = 0$.*

*Proof.* Modulo 2, $v^4 \equiv u^3 - u \equiv 0$, so $v$ is even. If $u$ is even, the derivative of $u - u^3$ is a unit at $u \equiv 0$, so $u = u_0(v)$ by Hensel's lemma. If $u$ is odd, then $8 \mid u - u^3$, so $v^4 + 2v \equiv 0 \pmod 8$ gives $4 \mid v$. Dividing the equation by $-8$ gives the equation of (ii), and its derivative with respect to $r$ is a unit, so the solution is unique. The coefficient inequality follows by induction from $r = t + 32t^4 - 6\varepsilon r^2 - 8r^3$. (iii) holds because the derivative with respect to $w$ is $-1$. □

**Step 5: 2-adic logarithms.** We use $\omega = (\omega_0, \omega_1, \omega_2) = (1, v, u)\, dv/(1 - 3u^2)$ as a basis of the regular differentials, and let $L_i = \log G_i \in \mathbb{Q}_2^3$. All integrals below are computed as antiderivatives of power series on the analytic disks of Lemma 3.4.5, and their values equal the abelian integrals ([KRZB16, Section 3]).

**Lemma 3.4.6.** *(1) $v_2(L_0) = (1, 3, 4)$, $v_2(L_1) = (-1, 1, 1)$, and $\Delta = L_{0,0}L_{1,2} - L_{1,0}L_{0,2}$ has valuation 2. Hence* $\operatorname{rank} J(\mathbb{Q}) = 2$. *(2) The annihilating vector $a$ of $L_0, L_1$, normalized by $a_1 = 1$, lies in $\mathbb{Z}_2^3$, and $a \equiv (4, 1, 2) \pmod 8$. (3) $\log J(\mathbb{Q}) \subseteq \mathbb{Z}_2 L_0 + \mathbb{Z}_2 L_1$.*

*Proof.* (1) From $\operatorname{div}(u + 2v)$ we get $4L_0 = -\int_{P_0}^{P_*} \omega$, and $P_*$ lies in the same even disk as $P_0$ ($t = -4$). The function of pole order 10

$$g_{10} = -13043u^2 + (27304v^2 + 22862v + 19496)u - 5780v^3 - 47008v^2 - 16272v - 6453$$

satisfies $\operatorname{div} g_{10} = 7P_1 + Q_1 + Q_2 + Q_3 - 10O$. $Q_1$ lies in the odd disk of $P_1$, and $Q_2, Q_3$ are conjugate over a 2-adic quadratic extension and lie in the disk at infinity ($v_2(t) = 3/2$, $v_2(w) = 6$). Hence $8L_1 = -\left(\int_{P_1}^{Q_1} \omega + \operatorname{Tr} \int_O^{Q_2} \omega\right)$. Computing with the valuations of all discarded tails bounded, we obtain the valuations in (1) (certificate 1.1.4f). The two products in $\Delta$ have valuations 2 and 3, so $v_2(\Delta) = 2$, and $L_0, L_1$ are independent. So the rank is at least 2, and together with Lemma 3.4.4 it is 2. (2) is the same computation (certificate 1.1.4f). (3) In Step 3 (c) the 2-adic images of $G_0, G_1$ are independent, so the two are independent in $J(\mathbb{Q})/2J(\mathbb{Q})$. The torsion of $J(\mathbb{Q})$ has odd order ($J(\mathbb{Q})[2] = 0$) and the rank is 2, so $\langle G_0, G_1 \rangle$ has odd index modulo torsion. The logarithm of a torsion point is 0, so (3) follows. □

**Step 6: integral points.**

**Lemma 3.4.7.** *The only integral points in the even disk are $P_0$ and $P_*$.*

*Proof.* Let $E(t)$ be the integral from $t = 0$ of the pullback of $a \cdot \omega$. At rational points, $E(t) = a \cdot (\log[P(t) - O] - L_0) = 0$. The coefficients are

$$[t]E = 2a_0, \quad [t^2]E = 2a_1 - 4a_2, \quad [t^3]E = 32a_0, \quad [t^4]E = 48a_1 - 128a_2$$

and by Lemma 3.4.6(2) their valuations are $3, 1, 7, 4$. For $m \geq 5$, since the coefficients of $u_0$ are integers, $v_2([t^m]E) \geq m - v_2(m) \geq 5$. The minimal valuation occurs only in degree 2 (certificate 1.1.4g), so by Strassmann's theorem $E$ has at most two zeros in $\mathbb{Z}_2$. These two are $t = 0$ ($P_0$) and $t = -4$ ($P_*$). □

**Lemma 3.4.8.** *The only integral point in the odd disk $\varepsilon$ is $P_\varepsilon$.*

*Proof.* Since $1-3u^2 = -2D_\varepsilon$ with $D_\varepsilon = 1+12\varepsilon r+24r^2$, the pullback of $\omega$ is $-2(1,4t,\varepsilon+4r)\,dt/D_\varepsilon$, and $v_2([t^j]D_\varepsilon^{-1}) \geq j+1$ ($j \geq 1$). Let $H_\varepsilon$ ($H_\varepsilon(0)=0$) be the antiderivative of $a\cdot\omega$ divided by $-4$. Then $H_\varepsilon' = (C_\varepsilon/2 + 2a_1 t + 2a_2 r)/D_\varepsilon$ with $C_\varepsilon = a_0+\varepsilon a_2$, and $v_2(C_\varepsilon)=1$. So $[t]H_\varepsilon = C_\varepsilon/2$ and $[t^2]H_\varepsilon = a_1+a_2-3\varepsilon C_\varepsilon$ are odd, and for $m\geq 3$, $v_2([t^m]H_\varepsilon) \geq m - v_2(m) \geq 2$. That is, $H_\varepsilon \equiv t+t^2 \pmod 2$ (certificate 1.1.4g). By Strassmann's theorem and Hensel's lemma, the zeros of $H_\varepsilon$ in $\mathbb{Z}_2$ are one with $t$ even ($t=0$) and one with $t$ odd. Suppose that $P(t)$ is a rational point for an odd $t$. For $I = \int_{P_\varepsilon}^{P(t)}\omega$, the coefficient inequalities above give $I_0/(-2)\equiv t$, $I_2/(-2)\equiv \varepsilon t \pmod 2$, so $v_2(I_0)=v_2(I_2)=1$. By Lemma 3.4.6(3), $I = b_0L_0+b_1L_1$ with $b_k\in\mathbb{Z}_2$. But in Cramer's formula $b_0 = (I_0L_{1,2}-L_{1,0}I_2)/\Delta$ the two terms of the numerator have valuations 2 and 0, so $v_2(b_0)=0-2=-2$. This is a contradiction. □

*Proof of Theorem 3.4.1.* By Lemmas 3.4.5, 3.4.7, 3.4.8, the only integral points of $C$ are $P_0, P_1, P_{-1}, P_*$, and under $(x,y)=(v,-u)$ they become the four solutions in the theorem. The rank follows from Lemma 3.4.6(1). □

## 3.5 $x^4+y^3+2x+y=0$ ($H=30$)

**Theorem 3.5.1.** *The only integer solutions of $x^4+y^3+2x+y=0$ are $(x,y)=(0,0),(8,-16)$.*

**Setup.** Put $u=y$, $z=x$. Then the equation becomes

$$C: \quad F(u,z) = u^3+u+z^4+2z = 0$$

The projective completion $z^4+u^3w+uw^3+2zw^3=0$ is a smooth plane quartic over $\mathbb{Q}$ (genus 3). At the point at infinity $O=(1:0:0)$ the line $w=0$ meets the curve with multiplicity 4, since $z^4=0$; so $O$ is a rational hyperflex. Near $O$ put $t=z/u$, $w=1/u$. Then the equation is

$$w+t^4+(1+2t)w^3 = 0$$

The partial derivative with respect to $w$ is 1 at $(t,w)=(0,0)$, so $t$ is a local parameter, and $\operatorname{ord}_O z=-3$, $\operatorname{ord}_O u=-4$. $J$ is the Jacobian of $C$.

**Proposition 3.5.2.** *The only integral points of $C$ are $P=(0,0)$ and $R=(-16,8)$.*

Since $(x,y)=(z,u)$, the points $P,R$ are $(x,y)=(0,0),(8,-16)$, and Theorem 3.5.1 is equivalent to Proposition 3.5.2. This section does not determine all of $C(\mathbb{Q})$. Modulo 2 the point $(u,z)=(1,0)$ is singular, so $C$ has bad reduction at 2. Therefore we argue in a single 2-adic disk that contains all integral points.

The proof has five steps. We fix the bitangent field $K$, show $\mathrm{Cl}(K)[2]=0$ (Lemma 3.5.3), and obtain rank $J(\mathbb{Q})\leq 2$ by 2-descent (Lemma 3.5.4). Then we construct an annihilating differential from 2-adic logarithms (Lemma 3.5.5) and apply Strassmann's theorem on the disk that contains all integral points (Lemma 3.5.6).

**Step 1: the bitangent field and bad primes.** The 27 bitangents other than the tangent line at $O$ have the form $u=mz+b$, and the slope $m$ is a root of

$$g(m) = m^{27}+480m^{19}-2688m^{18}-34560m^{11}-141312m^{10} \\ -162816m^9-16384m^3+49152m-32768$$

The intercept $b$ is an explicit element of $\mathbb{Q}(m)$, and substituting $u=mz+b$ into $F$ gives the square of a monic quadratic with nonzero discriminant (certificate 1.1.5a). Since $g$ is irreducible, the 27 bitangents form one Galois orbit. The field $K=\mathbb{Q}[m]/(g)$ has signature $(3,12)$ and discriminant

$D = 2^{28} \cdot 14365291^6$. There are three prime ideals above 2; their ramification indices are $1, 10, 16$, and all residue degrees are 1.

We find the bad primes of $C$. Because of the identity

$$12F - 4uF_u - 3zF_z = 8u + 18z$$

a singular point in odd characteristic satisfies $u = -9z/4$. In characteristic 3 we have $F_u \equiv 1$, so there is no singular point. In characteristic different from 2 and 3, $F_u = 3u^2 + 1 = 0$ and $F_z = 4z^3 + 2 = 0$ give $z^2 = -16/243$, $z^3 = -1/2$, and hence $z = 243/32$. For this value to satisfy $z^2 = -16/243$, the number $243^3 + 2^{14} = 14365291$ must be 0. The number $q = 14365291$ is prime. Modulo $q$ the only singular point is the reduction of $(u_c, z_c) = (-2187/128, 243/32)$, and at this point the $q$-adic valuations of $(F, F_u, F_z, \det \mathrm{Hess}\, F)$ are $(1, 1, 1, 0)$. Hence the singular fiber has only one singular point, an ordinary double point (node) of thickness 1. This fiber is geometrically irreducible: if it were reducible, Bézout's theorem would force further intersection points between the components. The component group of the Néron model is trivial, so the descent image is unramified at $q$, and $S = \{2\}$ suffices in Proposition A.

**Step 2: the class group.**

**Lemma 3.5.3.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (3, 12)$, the $D$ above, and $T = \log 10^8$. The window is a step function on 64 cells of equal width, and its heights are positive integers, symmetric from left to right (the input of certificate 1.1.5d). Two pieces of data are needed.

(i) There are 5,764,533 prime ideals of norm less than $10^8$ in total, and we count the number $a(q)$ for every norm (certificate 1.1.5b).

(ii) Every one of the 412,122 prime ideals of norm at most $6 \cdot 10^6$ has a witness for Lemma C (certificate 1.1.5c). Therefore we set $k(q) = a(q)$ if $q \le 6 \cdot 10^6$, and $k(q) = 0$ otherwise.

With these data the computation gives $B^-(f) > 0.000226856 > 0$ (certificate 1.1.5d). The computation uses exact rational coefficients and directed interval arithmetic, so rounding errors cannot change the conclusion. By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.5.4.** $\mathrm{rank}\, J(\mathbb{Q}) \le 2$.

*Proof.* The hypotheses of Proposition A were checked in the setup and in Step 1. Hence $J(\mathbb{Q})[2] = 0$, and the bitangent function $h = -(u - mz - b)$, normalized to have leading coefficient 1 at $O$, gives an injective homomorphism $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^\times/K^{\times 2}$. By Lemma 3.5.3,

$$\dim_{\mathbb{F}_2} K(S, 2) = (r_1 + r_2) + \#\{\mathfrak{p} \mid 2\} = 15 + 3 = 18$$

Eighteen explicit elements supported on $S$ form a basis of this space, because the matrix formed from their 2-adic valuations and their quadratic characters at the primes 7, 11, 13, 17 has rank 18 (certificate 1.1.5a).

We impose conditions on this space one at a time. The condition that the norm is a square reduces the dimension to 16. Imposing in turn the local conditions at the good primes 487, 491, 499, 503 reduces the dimension to $11, 9, 6, 4$. At each prime the local image is generated by the values of $h$ computed at all points of $C(\mathbb{F}_p)$ (Proposition F).

At 2, the bitangent code maps $J[2]$ Galois-equivariantly and injectively into $\mathbb{F}_2^{27}$, and the nonzero codewords have weights 12 and 16. An element of $J(\mathbb{Q}_2)[2]$ goes to a codeword that is constant on each local orbit, and the local orbits have sizes $1, 10, 16$. Among the unions of these orbits, the only one of weight 12 or 16 is the single orbit of size 16. Hence $\dim J(\mathbb{Q}_2)[2] \le 1$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3 + \dim J(\mathbb{Q}_2)[2] \le 4$. The images of the following four local classes are independent (certificate 1.1.5a).

(a) $[P - O]$;

(b) $[Q - O]$ for the point $Q$ with $t = 2$ in the chart at infinity;

(c) $[D_1 - 2O]$, where $D_1$ is the sum of the $\mathbb{Q}_2(\sqrt{2})$-point with $z = \sqrt{2}$ and its conjugate;

(d) $[D_2 - 2O]$, where $\theta^2 + \theta + 1 = 0$ and $D_2$ is the sum of the $\mathbb{Q}_2(\theta)$-point with $z = \theta$ and its conjugate.

The coordinates of the points are Hensel lifts modulo $2^{36}$. The relative valuation that this error contributes to the values of $h$ exceeds twice the ramification index at each 2-adic prime ideal, so the local square classes are determined. The local image has dimension at most 4 and contains four independent elements, so the 2-adic local image is the space spanned by these four elements. In the 4-dimensional candidate space above, the subspace whose restriction at 2 lies in this image is 2-dimensional. Since $\delta$ is injective and $J(\mathbb{Q})[2] = 0$, we get $\operatorname{rank} J(\mathbb{Q}) \le 2$. □

**Step 4: 2-adic logarithms.** Let $D$ be the rational divisor of degree 2 defined by $z^2 - z + 1 = 0$, $u = 1 - z$. Since $F(1 - z, z) = (z^2 - z + 1)(z^2 + 2)$, the divisor $D$ lies on $C$. We use the basis of holomorphic differentials

$$\boldsymbol{\omega} = (\omega_0, \omega_1, \omega_2) = (1, z, u)\frac{dz}{3u^2 + 1}$$

The $P$-disk consists of the points with $|z|_2 < 1$, $u = u(z)$. Here $u(z) \in \mathbb{Z}_2[[z]]$ is the unique solution with $u(0) = 0$ ($F_u(0, 0) = 1$). On this disk the coefficients of $\boldsymbol{\omega}$ lie in $\mathbb{Z}_2$. On the $O$-disk we have $|t|_2 < 1$, $w = w(t) \in \mathbb{Z}_2[[t]]$, and $\boldsymbol{\omega} = -(w, t, 1)\, dt/(1 + 3(1 + 2t)w^2)$, so again the coefficients are integral. Both disks are analytic open disks, so Abelian integrals on them are equal to formal antiderivatives ([KRZB16, Section 3]). We write $\log X \in \mathbb{Q}_2^3$ for the logarithm of $X \in J(\mathbb{Q}_2)$.

**Lemma 3.5.5.** *(1)* $\operatorname{div}(u + 2z) = 3P + R - 4O$. *Moreover, there is a rational function* $h_D$ *with* $\operatorname{div}(h_D) = 14D + E_D - 31O$, *where* $E_D$ *is an effective divisor of degree 3, irreducible over* $\mathbb{Q}$.

*(2) Modulo* $2^{16}$, $L_P = \log[P - O]$ *and* $L_D = \log[D - 2O]$ *are*

$$L_P \equiv (510,\ 3064,\ 32784), \qquad L_D \equiv (12669,\ 59033,\ 38772)$$

*(3)* $\operatorname{rank} J(\mathbb{Q}) = 2$. *Moreover, there is a primitive vector* $\lambda = (a_0, a_1, a_2) \in \mathbb{Z}_2^3$ *with* $\lambda \equiv (0, 4, 1) \pmod 8$ *such that* $\lambda \cdot \boldsymbol{\omega}$ *annihilates all logarithms of* $J(\mathbb{Q})$.

*Proof.* (1) Substituting $u = -2z$ gives $F(-2z, z) = z^3(z - 8)$, and $u + 2z$ has a pole of order 4 at $O$. Hence the first equality holds. We find $h_D$ in the basis $z^a u^b$ ($b \le 2$, $3a + 4b \le 31$; 29 elements) of $L(31O)$ from the condition that it vanishes to order 14 at the two points of $D$; the solution space is 1-dimensional. The coefficient of $uz^9$, the unique monomial of weight 31, is nonzero, so the pole has order exactly 31. Further, $\operatorname{Res}_u(F, h_D) = c\,(z^2 - z + 1)^{14} q_D(z)$, where $q_D$ is an irreducible cubic. At the roots of $q_D$ the greatest common divisor of $F$ and $h_D$ is linear in $u$, so the $u$-coordinates of $E_D$ are also determined. Hence the divisor equality accounts for all zeros and poles (certificate 1.1.5e).

(2) $R$ is the point of the $P$-disk with $z = 8$. From the first equality in (1), $4[P - O] + [R - P] = 0$, so

$$L_P = -\tfrac{1}{4}\int_P^R \boldsymbol{\omega}$$

The three roots of $q_D$ have distinct 2-adic valuations $1, 2, -6$, so all of them lie in $\mathbb{Q}_2$. The first two points lie in the $P$-disk, and the third lies in the $O$-disk ($v_2(t) = 2$). The class of the base divisor $2P + O$ is $2[P - O]$. Let $T_D$ be the sum of the tiny integrals from $P, P, O$ to the three points of $E_D$. Then the second equality in (1) gives

$$14L_D = -T_D - 2L_P$$

The differentials in the charts have integral coefficients and the parameters of the endpoints have valuation at least 1, so the $n$th term of the integral series has valuation at least $n - v_2(n)$. We compute 60

terms; the discarded terms have valuation at least 55, and the values modulo $2^{16}$ above are determined even after division by 4 and by 14 (certificate 1.1.5e).

(3) The valuations of the components of $L_P$ are $(1,3,4)$, and those of $L_D$ are $(0,0,2)$. Since $L_P/2 \equiv (1,0,0)$ and $L_D \equiv (1,1,0) \pmod 2$ are independent, $[P-O]$ and $[D-2O]$ have infinite order and are independent. Together with Lemma 3.5.4, this gives $\operatorname{rank} J(\mathbb{Q}) = 2$. The cross product of $L_P/2$ and $L_D$ is an integral vector whose third component is a unit. Let $\lambda$ be this vector divided so that its third component is 1; then $\lambda \equiv (0,4,1) \pmod 8$ (certificate 1.1.5e). The vector $\lambda$ annihilates the two logarithms, the subgroup generated by the two classes has finite index in $J(\mathbb{Q})$, and the logarithm of a torsion element is 0. Therefore $\lambda \cdot \boldsymbol{\omega}$ annihilates all logarithms of $J(\mathbb{Q})$. □

**Step 5: the disk containing the integral points.**

**Lemma 3.5.6.** *All integral points of $C$ lie in the $P$-disk. That is, they can be written as $z = 2t$, $t \in \mathbb{Z}_2$, $u = u(2t)$.*

*Proof.* Since $u^3 + u \equiv u(u+1)^2 \equiv 0 \pmod 2$, we have $z^4 \equiv 0$ modulo 2, that is, $z$ is even. If $u$ is odd, then $u^3 + u = u(u^2+1) \equiv 2 \pmod 4$, while $z^4 + 2z \equiv 0 \pmod 4$, a contradiction. Hence both $u$ and $z$ are even. For each even $z$, the equation $F(u,z) = 0$ has only one even solution by Hensel's lemma ($F_u \equiv 1 \pmod 2$), and this solution is $u(z)$. □

*Proof of Proposition 3.5.2.* On the $P$-disk let

$$\Phi(t) = \int_P^{(u(2t),2t)} \lambda \cdot \boldsymbol{\omega} = \sum_{n \geq 1} c_n t^n$$

The constant term is 0. The exact Taylor expansion gives

$$c_1 = 2a_0, \qquad c_2 = 2a_1 - 4a_2, \qquad c_3 = -32a_0, \qquad c_4 = -48a_1 + 128a_2$$

(certificate 1.1.5f). Since $\lambda \equiv (0,4,1) \pmod 8$, their valuations are, in order, at least 4, exactly 2, at least 8, and exactly 6. Since the coefficients of $\boldsymbol{\omega}$ in $z$ are integral, for $n \geq 5$ the valuation of $c_n$ is at least $n - v_2(n) \geq 5$. Hence $c_2$ is the only coefficient of smallest valuation, and by Strassmann's theorem $\Phi$ has at most two zeros in $\mathbb{Z}_2$.

If an integral point $Q$ lies at $t = t_Q$, then $[Q-P] \in J(\mathbb{Q})$, and by [KRZB16, Section 3], $\Phi(t_Q)$ is equal to $\lambda \cdot \log[Q-P]$. By Lemma 3.5.5(3) this value is 0 (the argument of [Col85, MP12]). The points $P$ and $R$ give the distinct zeros $t = 0$ and $t = 4$. By Lemma 3.5.6 all integral points lie in this disk, so there are no other integral points. □

## 3.6 $x^4 + y^3 + y^2 + x = 0$ ($H = 30$)

**Theorem 3.6.1.** *The equation $x^4 + y^3 + y^2 + x = 0$ has only the following integer solutions: $(x,y) = (-1,-1), (-1,0), (0,-1), (0,0), (2,-3)$.*

**Setup.** Put $u = y$, $z = x$. Then the equation becomes

$$C: \quad F(u,z) = u^3 + u^2 + z^4 + z = 0$$

The projective completion $u^3w + u^2w^2 + z^4 + zw^3 = 0$ is a smooth plane quartic (genus 3), and the point at infinity $\infty = (1:0:0)$ is a rational hyperflex. With $t = z/u$, $w = 1/u$, the equation near $\infty$ is $w + w^2 + tw^3 + t^4 = 0$, and $t$ is a local parameter. $C$ has good reduction at 2, because $F_z = 1 + 4z^3$ is a unit in the affine chart and $F_w = 1 + 2w + 3tw^2$ is a unit in the chart at infinity. An integral basis of holomorphic differentials is

$$\boldsymbol{\omega} = (\omega_0, \omega_1, \omega_2) = (1,z,u)\frac{dz}{3u^2+2u} = -(1,z,u)\frac{du}{1+4z^3} = -(w,t,1)\frac{dt}{1+2w+3tw^2}$$

and in the last two expressions the denominators are units on the 2-adic residue disks.

**Proposition 3.6.2.** *$C(\mathbb{Q}) = \{\infty, P_0, P_1, A, B, R\}$, where $P_0 = (0,0)$, $P_1 = (0,-1)$, $A = (-1,0)$, $B = (-1,-1)$, $R = (-3,2)$.*

Since $(x,y) = (z,u)$, the five affine points are $(x,y) = (0,0), (-1,0), (0,-1), (-1,-1), (2,-3)$, and Theorem 3.6.1 follows directly from Proposition 3.6.2.

The proof has six steps. We obtain rank $J(\mathbb{Q}) \leq 2$ from $\mathrm{Cl}(K)[2] = 0$ (Lemma 3.6.3) and 2-descent (Lemma 3.6.4), and we compute 2-adic logarithms using principal divisors to obtain saturation at 2 and an annihilator (Lemmas 3.6.5, 3.6.6). 2-adic Chabauty reduces the candidates to 11 (Lemma 3.6.7), and a sieve modulo 23 eliminates the five that remain (Lemma 3.6.8).

**Step 1: the bitangent field and bad primes.** The 27 bitangents other than the tangent line at $\infty$ have the form $u = mz + \eta(m)$, where $m$ is a root of

$$\begin{aligned} f(M) = M^{27} &- 160M^{19} - 1344M^{18} + 1280M^{15} - 3840M^{11} \\ &+ 23552M^{10} - 40704M^9 + 4096M^7 - 8192M^6 - 4096M - 4096 \end{aligned}$$

The element $\eta \in \mathbb{Q}(m)$ is given explicitly, and we check exactly the two coefficient conditions which say that $z^4 + (mz+\eta)^3 + (mz+\eta)^2 + z$ is the square of a quadratic (certificate 1.1.6a). Since $f$ is irreducible, the 27 bitangents form one Galois orbit. The field $K = \mathbb{Q}[M]/(f)$ has signature $(3,12)$ and discriminant $D_K = 2^{24} \cdot 3^6 \cdot 601^6 \cdot 857^6$. There is one prime ideal above 2 (ramification index 9, residue degree 3), and there are eight above 3.

A singular point satisfies $F_u = u(3u+2) = 0$ and $F_z = 4z^3 + 1 = 0$. In characteristic 2 we have $F_z \equiv 1$. In characteristic different from 2 and 3, if $u = 0$ then $F = z(z^3+1) = 3z/4 \neq 0$. If $u = -2/3$ then $F = 4/27 + 3z/4$, so $z = -16/81$, and $\mathrm{Res}_Z(81Z + 16, 4Z^3 + 1) = 515057 = 601 \cdot 857$. At 601 and 857 the only singular point is the reduction of $(-2/3, -16/81)$. There the Hessian determinant $-2048/2187$ is a unit, and the value $-2060228/43046721$ of $F$ has valuation 1. Hence there is only one singular point, an ordinary node of thickness 1, the singular fiber is geometrically irreducible, and the component group is trivial. Therefore $S = \{2,3\}$ suffices in Proposition A.

**Step 2: the class group.**

**Lemma 3.6.3.** *$\mathrm{Cl}(K)[2] = 0$.*

*Proof.* We apply Proposition B with a window consisting of a single cell. That is, $v$ is the indicator function of an interval of length $T$, and $f(x) = (1 - |x|/T)_+$. We take $T = 13$ ($e^{13} = 442413.4\ldots$). Every one of the 37,489 prime ideals of norm at most 450,000 has an explicit generator $g$ with $(g) = \mathfrak{p}$ (certificate 1.1.6b; this is the case of Lemma C with cofactor 1). Hence $c_m(q) = a(q)$ in every term of the sum. For this window the archimedean term has a closed form, and

$$B^-(f) = B_0 + \frac{2}{T} \sum_{j \text{ odd}} \frac{e^{-jT}}{j^2} + \frac{2\alpha}{T} \log(1 + e^{-T}) > B_0,$$

where

$$B_0 = \gamma + \log 4\pi + \alpha - \frac{\pi^2}{4T} - \frac{2\alpha \log 2}{T} - \frac{\log D_K}{n} + \frac{4}{n} \sum_{q^m < e^T} a(q) \frac{\log q}{q^m + 1} \left(1 - \frac{m \log q}{T}\right)$$

With 192-bit interval arithmetic, $B_0 > 0.0264813 > 0$ (certificate 1.1.6c). By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.6.4.** *rank $J(\mathbb{Q}) \leq 2$.*

*Proof.* By Proposition A, $J(\mathbb{Q})[2] = 0$, and $h_m = -(u - mz - \eta(m))$, normalized to have leading coefficient 1 at $\infty$, gives an injective homomorphism $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^\times/K^{\times 2}$. By Lemma 3.6.3, $\dim K(S,2) = 15 + 9 = 24$. Twenty-four explicit elements supported on the nine prime ideals above $S$ form a basis. The support is checked by exact ideal equalities, and the independence by the rank 24 of the matrix formed from valuation characters and quadratic characters at good primes (certificate 1.1.6a).

The condition that the norm is a square (the sign, and the parity of the valuations at 2 and 3) reduces the dimension to 21. Imposing in turn the local conditions at the good primes 487, 491, 499, 503, 509, 521, 523 reduces the dimension to 18, 15, 12, 10, 8, 6, 5 (the local images have dimensions $1, 1, 1, 1, 0, 1, 2$, in this order). Each local image is generated by the values at all points of $C(\mathbb{F}_p)$ (Proposition F).

There is only one prime ideal above 2, so the decomposition group acts transitively on the 27 bitangents. An invariant codeword has weight 0 or 27, while the nonzero codewords have weights 12 and 16; hence $J(\mathbb{Q}_2)[2] = 0$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3$. Local square classes are determined by the parity of the valuation and by the characters of $(\mathcal{O}_K/\mathfrak{p}^{19})^\times$ ($2e + 1 = 19$). The images of the three $\mathbb{Q}_2$-points with $(u, z) \equiv (0, 0), (1, 398796270), (1, 823490285)$ modulo $2^{30}$ are independent. The approximation error contributes valuation at least 274 to the value of $h_m$, and the value itself has valuation $-2$, so the square class is determined. Hence these three images span the whole 2-adic local image, and the 5-dimensional space shrinks to dimension 2. Since $\delta$ is injective, $\operatorname{rank} J(\mathbb{Q}) \le 2$. □

**Step 4: principal divisors and 2-adic logarithms.** Let $D_i = [P_i - \infty]$ ($i = 0, 1$). The equalities $\operatorname{div}(z) = 2P_0 + A - 3\infty$, $\operatorname{div}(z+1) = 2P_1 + B - 3\infty$, $\operatorname{div}(u + z + 1) = 2A + P_1 + R - 4\infty$ are checked by substitution (the last one comes from $F(-z-1, z) = z^2(z-2)(z+1)$), and they give

$$[A - \infty] = -2D_0, \qquad [B - \infty] = -2D_1, \qquad [R - \infty] = 4D_0 - D_1$$

**Lemma 3.6.5.** *(1) For $i = 0, 1$ there is a polynomial $h_i(u, z)$ with $\operatorname{div}(h_i) = 35P_i + E_i - 38\infty$, where $E_i$ is an effective divisor of degree 3, irreducible over $\mathbb{Q}$.*

*(2) Modulo $2^{24}$,*

$$\log D_0 \equiv (15495542, 1371452, 14073150), \qquad \log D_1 \equiv (13080018, 15362130, 15080040).$$

*Proof.* (1) Among the combinations of the 36 basis elements $z^a u^b$ ($b \le 2$, $3a + 4b \le 38$) of $L(38\infty)$, those whose first 35 Taylor coefficients at $P_i$ vanish form a 1-dimensional space, and its element is $h_i$. Exact computation confirms the order 35 at $P_i$, the pole of order 38, and $\operatorname{Res}_u(F, h_i) = c_i(z - z(P_i))^{35} d_i(z)$. Here $d_i$ is an irreducible monic cubic, and in $\mathbb{Q}[z]/(d_i)$ the common factor of $F$ and $h_i$ is linear in $u$. Hence the divisor equality accounts for all zeros and poles, and $[E_i - 3\infty] = -35D_i$ (certificate 1.1.6d).

(2) The minimal polynomial $p_i$ of the $u$-coordinate of $E_i$ is integral at 2 and satisfies $p_i(U) \equiv U^2(U+1) \pmod 2$, and the $z$-coordinate is a polynomial in $u$ with even coefficients. Hence the three points of $E_i$ reduce modulo 2 to $P_0, P_0, A$. The class of the base divisor $2P_0 + A = \operatorname{div}(z) + 3\infty$ is 0, so $\log D_i$ is the sum of the tiny integrals from $P_0, P_0, A$ to the three points of $E_i$, divided by $-35$. We compute this sum by a trace in the cubic algebra $\mathcal{A}_i = \mathbb{Z}_2[U]/(p_i)$. Let $e$ be the idempotent lifting $U^2$ from modulo 2, and take the base coordinate $u = -e$ and $\delta = U + e$. Then $\delta^2 \in 2\mathcal{A}_i$, so the $k$th term of the integral has valuation at least $\lfloor k/2 \rfloor - v_2(k)$. We compute 80 terms modulo $2^{40}$; the discarded terms have valuation at least 34, and the division loses at most 6 digits, so the values modulo $2^{24}$ above are determined (certificate 1.1.6d). □

**Lemma 3.6.6.** $\operatorname{rank} J(\mathbb{Q}) = 2$, *and $H = \langle D_0, D_1 \rangle$ has odd index in $J(\mathbb{Q})$. Hence for each $X \in J(\mathbb{Q})$ there are unique $c_0, c_1 \in \mathbb{Z}_2$ with $\log X = c_0 \log D_0 + c_1 \log D_1$, and if $NX = aD_0 + bD_1$ with $N$ odd and $a, b$ integers, then $(c_0, c_1) = (a/N, b/N)$. Moreover, for the primitive vector $\mathbf{a}$ with $\mathbf{a} \equiv (699041, 3772347, 3371045) \pmod{2^{22}}$ and $\mathbf{a} \equiv (1, 1, 1) \pmod 2$, the differential $\omega = \mathbf{a} \cdot \boldsymbol{\omega}$ annihilates all logarithms of $J(\mathbb{Q})$.*

*Proof.* Since $\log D_0/2 \equiv (1, 0, 1)$ and $\log D_1/2 \equiv (1, 1, 0) \pmod 2$ are independent, $D_0, D_1$ are independent elements of infinite order, and together with Lemma 3.6.4 the rank is 2.

The numbers of points over $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ are $5, 9, 5$, and $\#J(\mathbb{F}_2) = 35$ (certificate 1.1.6d). If $X \in J(\mathbb{Q}_2)$, then $35X$ lies in the kernel of reduction, that is, in the formal group with parameters in $2\mathbb{Z}_2$. In the formal logarithm of an integral invariant differential, the coefficients of the homogeneous part of degree $n$ lie in $n^{-1}\mathbb{Z}_2$ (apply the Euler operator to the closed integral differential), so its value has valuation at least $n - v_2(n) \geq 1$. Since 35 is odd, $\log J(\mathbb{Q}_2) \subseteq 2\mathbb{Z}_2^3$.

If $X \in J(\mathbb{Q})$ and $2X = aD_0 + bD_1$, then $a \log D_0/2 + b \log D_1/2 = \log X \in 2\mathbb{Z}_2^3$. The matrix formed by the first two components of the two half-logarithms is invertible modulo 2, so $a, b$ are even, and $X - (a/2)D_0 - (b/2)D_1 \in J(\mathbb{Q})[2] = 0$. Hence $J(\mathbb{Q})/H$ has no element of order 2, and the index $N = [J(\mathbb{Q}) : H]$ is odd. The rest follows because the logarithm is a homomorphism and vanishes on torsion elements. The coefficients are obtained from the inverse over $\mathbb{Z}_2$ of the matrix of the first two logarithm components. The cross product of the two logarithms has common valuation 2, and after division by $2^2$ it is the primitive annihilator **a** (certificate 1.1.6d). □

**Step 5: 2-adic zeros.** $C(\mathbb{F}_2)$ consists of the five reductions of $P_0, P_1, A, B, \infty$, so there are also five residue disks, and each center has a known rational point. On the finite disks we use $t = u - u_0$, at $\infty$ we use $t = z/u$, and we put $t = 2s$, $s \in \mathbb{Z}_2$. The constant term of $G(s) = \int_0^{2s} \omega$ is 0, and by [Col85, MP12] and Lemma 3.6.6 every rational point of a disk is a zero of $G$.

**Lemma 3.6.7.** *On the five disks, $G$ has 11 zeros in total, exactly one in each ball of the table below. Here $(c_0, c_1)$ are the coefficients of Lemma 3.6.6.*

| *Disk* | *Ball of $s$* | $v$ | $s \bmod 2^{14}$ | $(c_0, c_1) \bmod 128$ | $70c_0 + c_1 \bmod 128$ | *Point* |
|---|---|---|---|---|---|---|
| $P_0$ | $1 + 2\mathbb{Z}_2$ | 2 | 11613 | $(106, 48)$ | 44 | – |
| $P_0$ | $2\mathbb{Z}_2$ | 2 | 0 | $(1, 0)$ | 70 | $P_0$ |
| $P_1$ | $2 + 4\mathbb{Z}_2$ | 4 | 10130 | $(124, 35)$ | 11 | – |
| $P_1$ | $4\mathbb{Z}_2$ | 4 | 0 | $(0, 1)$ | 1 | $P_1$ |
| $A$ | $7 + 8\mathbb{Z}_2$ | 7 | 16383 | $(4, 127)$ | 23 | $R$ |
| $A$ | $3 + 8\mathbb{Z}_2$ | 7 | 4595 | $(120, 79)$ | 31 | – |
| $A$ | $2 + 4\mathbb{Z}_2$ | 5 | 7586 | $(64, 104)$ | 104 | – |
| $A$ | $4\mathbb{Z}_2$ | 5 | 0 | $(126, 0)$ | 116 | $A$ |
| $B$ | $\mathbb{Z}_2$ | 1 | 0 | $(0, 126)$ | 126 | $B$ |
| $\infty$ | $1 + 2\mathbb{Z}_2$ | 2 | 529 | $(5, 65)$ | 31 | – |
| $\infty$ | $2\mathbb{Z}_2$ | 2 | 0 | $(0, 0)$ | 0 | $\infty$ |

*Proof.* We expand $G$ up to degree 40 over $\mathbb{Z}/2^{30}$ and divide each disk into balls $s = c + 2^d r$. After dividing by the minimal valuation $v$ of the coefficients: if only the constant term is a unit, then Strassmann's theorem gives no zero; if the linear coefficient is a unit and all higher coefficients are even, then Hensel's lemma and Strassmann's theorem give exactly one zero. Every ball ends in one of these two cases within depth 3. The only balls outside the table are $1 + 2\mathbb{Z}_2$ in the $P_1$-disk and $1 + 4\mathbb{Z}_2$ in the $A$-disk, and neither has a zero (certificate 1.1.6e). The error of the annihilator is divisible by $2^{22}$, and after the substitution $t = 2s$ the coefficient of degree $k$ acquires a factor of valuation $k - v_2(k) \geq 1$, so the error of $G$ is divisible by $2^{23}$. The terms of degree above 40 have valuation at least 36. Hence the error of a root $s$ has valuation $23 - v + d \geq 19$, and the coefficients $(c_0, c_1)$ are determined modulo $2^{11}$. Below we use them only modulo $2^7$. $R$ is the point of the $A$-disk with $s = -1$. □

**Step 6: a sieve modulo 23.**

**Lemma 3.6.8.** $\#J(\mathbb{F}_{23}) = 11392 = 2^7 \cdot 89$. *The element $H_1 = 89\overline{D_1}$ has order 128 and $H_0 = 89\overline{D_0} = 70H_1$, so the 2-primary part of $J(\mathbb{F}_{23})$ is the cyclic group generated by $H_1$. Moreover, as $Q$ runs through $C(\mathbb{F}_{23})$, the set of $r \in \mathbb{Z}/128$ with $89[Q - \infty] = rH_1$ is*

$$\mathcal{R} = \{0, 1, 2, 4, 6, 8, 23, 24, 33, 35, 52, 58, 70, 99, 101, 116, 117, 126, 127\}$$

*Proof.* We have $\#C(\mathbb{F}_{23}) = 22$, $\#C(\mathbb{F}_{23^2}) = 538$, $\#C(\mathbb{F}_{23^3}) = 12616$. Newton's identities and the functional equation give $L_{23}(T) = 1 - 2T + 6T^2 + 140T^3 + 138T^4 - 1058T^5 + 12167T^6$, and $\#J(\mathbb{F}_{23}) = L_{23}(1) = 11392$. The order, the relation $H_0 = 70H_1$, and the classes of the 22 points are computed exactly by Riemann–Roch divisor arithmetic over $\mathbb{F}_{23}$ (certificate 1.1.6f). □

*Proof of Proposition 3.6.2.* A point $X \in C(\mathbb{Q})$ lies in one of the five disks and is a zero of $G$, so it is one of the 11 zeros in the table. A ball that contains a known point contains only one zero, so if it lies in such a ball, $X$ is that known point. Otherwise $X$ is one of the other five zeros. By Lemma 3.6.6, $N[X - \infty] = aD_0 + bD_1$ with $N$ odd. Reducing modulo 23 and multiplying by 89 gives $89N\,\overline{[X - \infty]} = aH_0 + bH_1 = (70a + b)H_1$, and $N$ is invertible modulo 128, so $89\,\overline{[X - \infty]} = (70c_0 + c_1)H_1$. The reduction of $X$ is a point of $C(\mathbb{F}_{23})$, so by [BS10], we must have $70c_0 + c_1 \bmod 128 \in \mathcal{R}$. However, none of the values $44, 11, 31, 104, 31$ of the five zeros lies in $\mathcal{R}$. Therefore $C(\mathbb{Q})$ consists only of the six known points. □

## 3.7 $x^4 + y^3 - y^2 + x = 0$ ($H = 30$)

**Theorem 3.7.1.** *The equation $x^4 + y^3 - y^2 + x = 0$ has only the following integer solutions: $(x, y) = (-4, -6), (-1, 0), (-1, 1), (0, 0), (0, 1), (1, -1)$.*

**Setup.** Put $u = -y$, $z = -x$. Then $x^4 + y^3 - y^2 + x = -(u^3 + u^2 - z^4 + z)$, so the equation becomes

$$C: \quad F(u, z) = u^3 + u^2 - z^4 + z = 0$$

The projective completion $u^3w + u^2w^2 - z^4 + zw^3 = 0$ is a smooth plane quartic (genus 3), and the point at infinity $O = (1 : 0 : 0)$ is a rational hyperflex. With $t = z/u$, $w = 1/u$, the equation near $O$ is $w + w^2 + tw^3 - t^4 = 0$. $C$ has good reduction at 2 ($F_z = 1 - 4z^3$ and $F_w = 1 + 2w + 3tw^2$ are units), and an integral basis of holomorphic differentials is

$$\boldsymbol{\omega} = (1, z, u)\frac{dz}{3u^2 + 2u} = -(1, z, u)\frac{du}{1 - 4z^3} = -(w, t, 1)\frac{dt}{1 + 2w + 3tw^2}$$

At 3 the curve has bad reduction, since modulo 3 the point $(u, z) = (0, 1)$ is singular.

**Proposition 3.7.2.** $C(\mathbb{Q}) = \{O, (0, 0), (0, 1), (-1, 0), (-1, 1), (1, -1), (6, 4)\}$.

Since $(x, y) = (-z, -u)$, the six affine points are $(0, 0)$, $(-1, 0)$, $(0, 1)$, $(-1, 1)$, $(1, -1)$ and $(-4, -6)$, in this order, and Theorem 3.7.1 follows from Proposition 3.7.2. For $X \in C(\mathbb{Q})$ we write $D_X = [X - O]$, and we put $G_1 = D_{(0,1)}$, $G_2 = D_{(1,-1)}$.

The proof goes as follows. In Steps 1–3 we show $\operatorname{rank} J(\mathbb{Q}) \leq 2$; since 5 is a bad prime at which the component group has order 2, we determine the local image at 5 separately (Lemma 3.7.4). In Step 4 we show that the rank is 2 and that $\langle G_1, G_2 \rangle$ has odd index. In Steps 5 and 6, 2-adic and 3-adic Chabauty each reduce the candidates for new rational points to two, and in Step 7 a comparison modulo 509 and 293 eliminates all of them.

**Step 1: the bitangent field and bad primes.** The 27 bitangents other than the tangent line at $O$ have the form $u = mz + \eta(m)$, where $m$ is a root of

$$\begin{aligned} f(m) = {} & m^{27} - 160m^{19} - 1344m^{18} - 1280m^{15} - 3840m^{11} \\ & + 23552m^{10} - 40704m^9 - 4096m^7 + 8192m^6 - 4096m - 4096 \end{aligned}$$

The element $\eta \in \mathbb{Q}(m)$ is given explicitly, and we check exactly the two coefficient conditions which say that $F(mz + \eta, z)$ is $-1$ times the square of a quadratic (certificate 1.1.7a). The polynomial $f$ is irreducible, and $h = u - mz - \eta$ is $t^{-4}(1 + \cdots)$ at $O$, so it is normalized. The field $K = \mathbb{Q}[m]/(f)$ has signature $(3, 12)$ and discriminant $D_K = 2^{24} \cdot 3^6 \cdot 17^6 \cdot 1289^6$. There is one prime ideal above 2 ($e = 9$,

$f = 3$), there are four above 3, and five above 5. The prime 5 is unramified in $K$, with residue degrees $3, 6, 6, 6, 6$.

In characteristic different from 2 and 3, a singular point satisfies $F_u = u(3u + 2) = 0$ and $F_z = 1 - 4z^3 = 0$. If $u = 0$ then $F = 3z/4 \neq 0$; if $u = -2/3$ then $F = 4/27 + 3z/4$, so $z = -16/81$, and $|\operatorname{Res}(81z + 16, 4z^3 - 1)| = 547825 = 5^2 \cdot 17 \cdot 1289$. At 17 and 1289 the only singular point is the reduction of $(-2/3, -16/81)$, the Hessian is a unit, and the critical value has valuation 1. Hence it is a node of thickness 1, and the component group is trivial. At 5, too, the only singular point is $(u, z) \equiv (1, 4)$. However, at the approximate critical point $(-2/3, -16/81)$ the valuations of $F$ and $F_z$ are 2, $F_u = 0$, and the Hessian is a unit, and at the true critical point obtained by Hensel lifting the value of $F$ changes only modulo $5^4$. Hence the node at 5 has thickness 2, and the geometric component group is $\mathbb{Z}/2$ (the singular fiber is geometrically irreducible). Therefore we take $S = \{2, 3, 5\}$ in Proposition A.

**Step 2: the class group.**

**Lemma 3.7.3.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* As in the proof of Lemma 3.6.3, we apply Proposition B to the one-cell window $f(x) = (1 - |x|/T)_+$. Here $T = 8$ and $e^8 = 2980.96\ldots < 3000$. All 413 prime ideals of norm at most 3000 have explicit generators (certificate 1.1.7b), so $c_m(q) = a(q)$ in every term, and the same closed-form lower bound gives $B_0 > 0.0849899 > 0$ (certificate 1.1.7c). By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.7.4.** *The local image $\delta_5\big(J(\mathbb{Q}_5)/2J(\mathbb{Q}_5)\big)$ at 5 is the line spanned by $\delta_5([X_5 - O])$, where $X_5$ is the unique $\mathbb{Q}_5$-point with $u = 1$, $z \equiv 4 \pmod{25}$.*

*Proof.* The bitangent code embeds $J[2]$ Galois-equivariantly and injectively into $E = \mathbb{F}_2^{27}$, and $K$ is unramified at 5, so $J[2]$ is also unramified at 5. The Frobenius $\Phi$ at 5 preserves the quadratic form that the rational odd theta characteristic $2O$ defines on $J[2]$, so it lies in the orthogonal group $O_6^-(2)$ (of order 51840) of this form, and it has cycle type $(3, 6, 6, 6, 6)$ on the bitangents. Listing all such elements (certificate 1.1.7d), the only pairs consisting of $\dim J[2]^\Phi$ and the rank of the coinvariant map $J[2]/(\Phi - 1)J[2] \to E/(\Phi - 1)E$ are $(0, 0)$ (720 elements), $(1, 1)$ (4320 elements), and $(2, 0)$ (1440 elements). If $p \neq 2$, then $\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \dim J(\mathbb{Q}_p)[2] = \dim J[2]^\Phi$, so in the first two cases the local image has dimension at most 1.

In the third case, let $J^0(\mathbb{Q}_5)$ be the subgroup of points that reduce to the identity component of the Néron model. The special fiber of the identity component is a connected commutative algebraic group, on which multiplication by 2 is surjective and étale. Hence, by Hensel's lemma, the points of $J^0(\mathbb{Q}_5)$ are divisible by 2 over the maximal unramified extension, and their Kummer classes are unramified classes, that is, elements of $J[2]/(\Phi - 1)J[2]$. Since the coinvariant map has rank 0, $\delta_5(J^0(\mathbb{Q}_5)) = 0$. The quotient $J(\mathbb{Q}_5)/J^0(\mathbb{Q}_5)$ embeds into the component group $\mathbb{Z}/2$, so the local image has dimension at most 1. On the other hand, the image of $X_5$ is nonzero (checked exactly, including the margin for the approximation error, certificate 1.1.7d). Therefore the local image is that line. □

**Lemma 3.7.5.** $\operatorname{rank} J(\mathbb{Q}) \leq 2$.

*Proof.* By Proposition A, $J(\mathbb{Q})[2] = 0$ and $\delta$ is injective. By Lemma 3.7.3, $\dim K(S, 2) = 15 + 10 = 25$, and 25 explicit elements supported on the ten prime ideals above $S$ form a basis (rank 25 from valuation characters and quadratic characters at good primes). The conditions on the sign of the norm and on the parity of the valuations at 2, 3, 5 reduce the dimension to 21. The local conditions at the good primes 487, 491, 499, 503, 509, 521, 523 (local images of dimensions $1, 2, 1, 2, 3, 3, 1$) reduce the dimension to 18, 15, 13, 10, 7, 6, 6 (Proposition F). At 2, as in the proof of Lemma 3.6.4, $J(\mathbb{Q}_2)[2] = 0$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3$, and the images of the three points obtained by Hensel lifting from $(u, z) \equiv (1, 0), (2, 0), (0, 1)$ (the third is the rational point $(0, 1)$) are independent (approximation

modulo $2^{30}$; the relative error exceeds twice the ramification index). Hence the dimension drops to 3, and the condition of Lemma 3.7.4 makes it 2 (certificate 1.1.7a). Therefore rank $J(\mathbb{Q}) \le 2$. □

**Step 4: 2-adic logarithms and odd index.** Since $F(u,0) = F(u,1) = u^2(u+1)$ and $F(-z,z) = -z(z-1)(z+1)^2$, we have $\operatorname{div}(z) = 2(0,0) + (-1,0) - 3O$, $\operatorname{div}(z-1) = 2(0,1) + (-1,1) - 3O$, $\operatorname{div}(u+z) = (0,0) + (-1,1) + 2(1,-1) - 4O$, and

$$D_{(0,0)} = 2G_1 - 2G_2, \qquad D_{(-1,0)} = -4G_1 + 4G_2, \qquad D_{(-1,1)} = -2G_1$$

**Lemma 3.7.6.** *(1) For each of $X = (0,0), (0,1), (1,-1)$ there is a polynomial $h_X$ with $\operatorname{div}(h_X) = 35X + E_X - 38O$ ($E_X$ an effective divisor of degree 3), and modulo $2^{40}$*

| $X$ | $\log_0 D_X$ | $\log_1 D_X$ | $\log_2 D_X$ |
|---|---|---|---|
| $(0,0)$ | 714153886116 | 445000321592 | 1048252576132 |
| $(0,1)$ | 578889133504 | 570949811744 | 721623895966 |
| $(1,-1)$ | 771568004334 | 348449650948 | 747253421788 |

*(2)* $\operatorname{rank} J(\mathbb{Q}) = 2$, *$\#J(\mathbb{Q})_{\mathrm{tors}}$ divides 35, and $\langle G_1, G_2\rangle$ has odd index in $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$. Hence for each $Y \in J(\mathbb{Q})$ we have $NY = n_1G_1 + n_2G_2$ with $N$ odd and $n_1, n_2$ integers, and $(c_1, c_2) = (n_1/N, n_2/N) \in \mathbb{Z}_2^2$ is uniquely determined by the 0th and 2nd components of* $\log Y$.

*Proof.* (1) $h_X$ is the combination of the $z^iu^j$ ($j < 3$, $3i + 4j \le 38$) whose first 35 Taylor coefficients at $X$ vanish (the solution space is 1-dimensional). $\operatorname{Res}_u(F, h_X)$ is the product of a constant, $(z - z_X)^{35}$ and an irreducible cubic, and the order 35 and the pole of order 38 account for all zeros and poles. For $(0,1)$ the residual divisor lies in the $O$-disk (the roots have valuation $\ge 1/2$). For the other two, as in the proof of Lemma 3.6.5, the cubic algebra becomes $\mathbb{F}_2[u]/(u^2(u+1))$ modulo 2, and the base divisor is a full fiber of $z$ or of $z-1$, so its class is 0. Hence $\log D_X$ is the trace of the tiny integrals divided by $-35$. The integrated term of degree $n$ has valuation at least $\lfloor n/2 \rfloor - v_2(n)$; with 144 terms the tail has valuation at least 64, and the division in the computation modulo $2^{60}$ loses at most 7 digits, so the values modulo $2^{40}$ are determined (certificate 1.1.7e). The table agrees with $D_{(0,0)} = 2G_1 - 2G_2$ modulo $2^{40}$.

(2) From the point counts $5, 9, 5$ over $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ we get $\#J(\mathbb{F}_2) = 35$. By [Kat81, Appendix], torsion of odd order injects into $J(\mathbb{F}_2)$, and $J(\mathbb{Q})[2] = 0$, so $\#J(\mathbb{Q})_{\mathrm{tors}} \mid 35$. Since $\log G_1/2 \equiv (0,0,1)$ and $\log G_2/2 \equiv (1,0,0) \pmod 2$ are independent, the rank is 2. As in the proof of Lemma 3.6.6, $\log J(\mathbb{Q}_2) \subseteq 2\mathbb{Z}_2^3$. The submatrix formed by the 0th and 2nd components of the two half-logarithms has unit determinant. If the index were even, then for a basis $B_1, B_2$ of the free part we would have $(G_1, G_2) = (B_1, B_2)M$ with $\det M$ even; since the half-logarithms of the $B_i$ are integral, the determinant of this submatrix would then be even, a contradiction. The coefficients are read off using the inverse of this submatrix over $\mathbb{Z}_2$. □

**Step 5: 2-adic zeros.** For the five points of $C(\mathbb{F}_2)$ we take the rational points $O$, $(0,0)$, $(0,1)$, $(-1,0)$, $(-1,1)$ as the centers of the disks. On the finite disks we use $t = u - u_0$, at $O$ we use $t = z/u$, and we put $t = 2s$. Let $\omega$ be the primitive annihilator obtained from the cross product of the two logarithms, normalized by its middle coefficient (which is odd). Then the zeros of $G(s) = \int_0^{2s} \omega$ include all rational points of the disk ([Col85, MP12]).

**Lemma 3.7.7.** *On the five disks, $G$ has exactly nine zeros, and each of them lies in a ball that contains only this zero. Seven of them are known points ($(6,4)$ is at $s = 3$ in the $(0,0)$-disk, $(1,-1)$ is at $s = 1$ in the $(-1,1)$-disk, and the others are at the centers). The other two are*

| | *Disk* | $s \bmod 2^{20}$ | $c_1 \bmod 2^{16}$ | $c_2 \bmod 2^{16}$ |
|---|---|---|---|---|
| $Q_2$ | $(-1,0)$ | 902770 | 18122 | 35366 |
| $R_2$ | $O$ | 607280 | 38704 | 39424 |

*$Q_2, R_2$ are only local zeros in $C(\mathbb{Q}_2)$; this does not mean that they are rational points.*

*Proof.* We use the same ball decomposition as in the proof of Lemma 3.6.7. When we integrate up to degree 64, the discarded part is divisible by $2^{58}$ and the uncertainty of the annihilator by $2^{39}$; since we compute in $\mathbb{Z}/2^{50}$, the coefficients have an absolute precision of 39 digits. The valuation we divide by is at most 10 (depth 5), so the roots have a precision of at least $39-10+5=34$ digits, and since the half-logarithm submatrix is invertible, the coefficients are determined to 16 digits (certificate 1.1.7f). □

**Step 6: 3-adic logarithms and 3-adic zeros.**

**Lemma 3.7.8.** *(1) For $X=(0,0),(1,-1)$ we have $\operatorname{div}(h_X)=63X+E_X-66O$, and modulo $3^{24}$*

| $X$ | $3\log_0 D_X$ | $3\log_1 D_X$ | $3\log_2 D_X$ |
|---|---|---|---|
| $(0,0)$ | 265295843469 | 256546487256 | 167647527990 |
| $(1,-1)$ | 247088970603 | 249160065058 | 89859469233 |

*In the space of logarithms $G_1=G_2+D_{(0,0)}/2$; the cross product of $3\log G_1, 3\log G_2$ has common valuation 2, and the primitive annihilator is $(16280295932, 6711384369, 10302306500)$ modulo $3^{22}$ and $(2,0,2)$ modulo 3.*

*(2) Integrate the differential made from this annihilator on each 3-adic chart, starting from the rational point at the center. The resulting function has exactly nine zeros on all of $C(\mathbb{Q}_3)$, and each of them lies in a ball that contains only this zero. Seven of them are known points, and the coefficients of the remaining two, $Q_3, R_3$, are $(c_1,c_2)\equiv(2705,832),\ (1055,2942) \pmod{3^8}$.*

*(3) At all nine zeros, $c_1, c_2\in\mathbb{Z}_3$.*

*Proof.* (1) As in the 2-adic case, $h_X$ is found from the $z^iu^j$ ($j<3$, $3i+4j\le 66$) and checked with resultants. Both residual divisors lie in the $O$-disk, and the base divisor is $3O$. Since $t^3\in 3\mathcal{A}$, the traced term of degree $n$ has valuation at least $\lfloor n/3\rfloor - v_3(n)$; with 120 terms the tail has valuation at least 35, and the division in the computation in $\mathbb{Z}/3^{40}$ loses at most 5 digits. Hence the values modulo $3^{24}$ are determined. The bad reduction at 3 is not used; we use only the fact that the $O$-disk is an analytic disk ([KRZB16, Section 3]; certificate 1.1.7g).

(2) The rational points of the singular fiber modulo 3 are $O,(0,0),(1,-1),(-1,0),(-1,1),(0,1)$, and only $(0,1)$ is a singular point. At the five smooth points, $u-u_0$ ($z-1$ at $(-1,1)$, and $z/u$ at $O$) is a parameter that runs over $3\mathbb{Z}_3$. The points that reduce to $(0,1)$, written as $u=3a$, $z=1+3b$, satisfy $b+6b^2+12b^3+9b^4=a^2+3a^3$. For rational $0<r<1/4$ and $|a|\le 3^r$, the map $b\mapsto a^2+3a^3-6b^2-12b^3-9b^4$ is a contraction on $|b|\le 3^{2r}$, so the solution $b(a)$ is analytic on the open disk of radius $3^{1/4}>1$, and this disk contains all $a\in\mathbb{Z}_3$ ($(0,1)$ is $a=0$, and $(6,4)$ is $a=2$). On it $\omega=(1,1+3b,3a)\,da/(1+12b+36b^2+36b^3)$, and after integration the coefficient of $a^n$ has valuation at least $\lceil (n-1)/4\rceil - v_3(n)\ge 0$, and at least 28 if $n\ge 121$. By [KRZB16, Section 3], the antiderivative starting at $a=0$ is the Abelian integral on this whole chart. When we decompose the six charts into balls (smooth disks: $t=3s$ with 120 terms, coefficient error $3^{23}$, tail $3^{100}$; singular chart: error $3^{22}$, tail $3^{28}$), every ball ends with either 0 zeros or 1 simple root. The zeros are the seven known points, $Q_3$ (in the chart $u=-1+3s$, $s\equiv 273546 \pmod{3^{12}}$), and $R_3$ (in the singular chart, $a\equiv 397615 \pmod{3^{12}}$) (certificate 1.1.7g).

(3) Let $M$ be the matrix of the 1st and 2nd components of $3\log G_1, 3\log G_2$. Then $\det M=9\varepsilon$ with $\varepsilon\in\mathbb{Z}_3^\times$. If $U=\varepsilon^{-1}\operatorname{adj} M$, then for $v=3\log D$ at a zero we have $U(v_1,v_2)^{\mathsf{T}}=9(c_1,c_2)^{\mathsf{T}}$. At all nine zeros both components of the left-hand side are divisible by 9 (the error has valuation at least 11, certificate 1.1.7g). □

**Lemma 3.7.9.** *If the 3-adic coefficients of $Y\in C(\mathbb{Q})$ are $(c_1,c_2)\in\mathbb{Z}_3^2$, then at a good prime $\ell$, for the projection $\pi_3$ onto the 3-primary part of $J(\mathbb{F}_\ell)$, we have $\pi_3(\overline{D_Y})=\pi_3(c_1\overline{G_1}+c_2\overline{G_2})$. The same holds for the 2-primary part and the 2-adic coefficients of Lemma 3.7.6(2).*

*Proof.* The rank is 2 and the two 3-adic logarithms are independent, so $c_1, c_2$ are rational numbers, and by assumption their denominators are prime to 3. For a common denominator $d$ ($3\nmid d$), the element

$T = dD_Y - dc_1G_1 - dc_2G_2$ has logarithm 0, so it is a torsion element, and its order divides 35. Hence $\pi_3(\overline{T}) = 0$, and $d$ is invertible on the 3-primary part. For the 2-primary part the same argument works with an odd $N$. □

**Step 7: comparison modulo 509 and 293.** The point counts over three extensions determine the Weil polynomial and $\#J$ (certificate 1.1.7h).

| $p$ | $\#C(\mathbb{F}_p)$ | $\#C(\mathbb{F}_{p^2})$ | $\#C(\mathbb{F}_{p^3})$ | $\#J(\mathbb{F}_p)$ |
|---|---|---|---|---|
| 293 | 284 | 85720 | 25164212 | $24294816 = 2^5 \cdot 3^4 \cdot 7 \cdot 13 \cdot 103$ |
| 509 | 510 | 259528 | 131838318 | $131974656 = 2^9 \cdot 3 \cdot 11 \cdot 73 \cdot 107$ |

Multiplication by $257763 = \#J(\mathbb{F}_{509})/2^9, 759213 = \#J(\mathbb{F}_{293})/2^5, 299936 = \#J(\mathbb{F}_{293})/3^4$ is the projection onto the 2-primary or the 3-primary part.

**Lemma 3.7.10.** *(1)* $257763 \cdot 304\,\overline{G_1}$ *is not equal to* $257763\,[Q - O]$ *for any* $Q \in C(\mathbb{F}_{509})$.

*(2) The points* $Q \in C(\mathbb{F}_{293})$ *with* $759213\,[Q - O] = 759213\,(10\overline{G_1} + 6\overline{G_2})$ *are the nine points* $(u, z) = (0,0), (1,20), (47,88), (60,82), (68,67), (119,277), (124,164), (162,64), (197,60)$, *and for none of them is* $299936\,[Q - O]$ *equal to* $299936\,(32\overline{G_1} + 22\overline{G_2})$ *or to* $299936\,(2\overline{G_1} + 26\overline{G_2})$.

*Proof.* We compare all points by exact divisor arithmetic over $\mathbb{F}_\ell$ (certificate 1.1.7h). □

*Proof of Proposition 3.7.2.* Suppose that $Y \in C(\mathbb{Q})$ is not a known point. By Lemma 3.7.7, $Y$ is $Q_2$ or $R_2$ in $C(\mathbb{Q}_2)$. If $Y = R_2$, then its 2-adic coefficients are $(304, 0)$ mod 512, so by Lemma 3.7.9, $257763\,\overline{D_Y} = 257763 \cdot 304\,\overline{G_1}$; but the reduction of $Y$ is a point of $C(\mathbb{F}_{509})$, so this contradicts Lemma 3.7.10(1) ([BS10]). Hence $Y = Q_2$, its 2-adic coefficients are $(10, 6)$ mod 32, and the reduction of $Y$ modulo 293 is one of the nine points of Lemma 3.7.10(2). On the other hand, by Lemma 3.7.8, $Y$ is $Q_3$ or $R_3$, and its 3-adic coefficients lie in $\mathbb{Z}_3$ and are $(32, 22)$ or $(2, 26)$ modulo 81. Applying Lemma 3.7.9 with $\ell = 293$ gives a contradiction with Lemma 3.7.10(2). Therefore $C(\mathbb{Q})$ consists only of the seven known points. □

## 3.8 $x^4 + y^3 + 2x - y + 1 = 0$ $(H = 31)$

**Theorem 3.8.1.** *The only integer solutions of* $x^4 + y^3 + 2x - y + 1 = 0$ *are* $(-1,-1)$, $(-1,0)$ *and* $(-1,1)$.

**Setup.** Put $u = -y$, $z = x$. Then the equation becomes

$$C: \quad F(u,z) = -u^3 + u + z^4 + 2z + 1 = 0$$

The projective completion $-U^3W + UW^3 + Z^4 + 2ZW^3 + W^4 = 0$ is a smooth plane quartic (genus 3) (Step 1), and it has only one point at infinity, $O = [1:0:0]$. The tangent line $W = 0$ meets the curve at $O$ with multiplicity 4, since $Z^4 = 0$; so $O$ is a rational hyperflex. $J$ is the Jacobian of $C$. Theorem 3.8.1 is equivalent to the following proposition.

**Proposition 3.8.2.** *The only integer solutions of* $F(u,z) = 0$ *are* $P_0 = (0,-1)$, $P_1 = (1,-1)$, $P_2 = (-1,-1)$.

Since $(x,y) = (z,-u)$, the three points are $(x,y) = (-1,0), (-1,-1), (-1,1)$, respectively.

The proof has five steps. In Step 1 we fix the bitangent field $K$ and the bad primes. In Step 2 we show $\mathrm{Cl}(K)[2] = 0$ by Proposition B, and in Step 3 we show by 2-descent that the rank is at most 2. In Step 4 we construct an annihilating differential from 2-adic logarithms, and in Step 5 we count the zeros on the two 2-adic disks that cover the integral points. The curve has bad reduction at 2, so we use [KRZB16, Section 3] to identify the integrals on the disks with integrals of power series.

**Step 1: the bitangent field and bad primes.** The 27 bitangents other than the tangent line at $O$ have the form $u = mz + \eta$, and the slope $m$ is a root of

$$f(m) = m^{27} - 480m^{19} + 2688m^{18} + 17280m^{15} - 34560m^{11} - 141312m^{10} \\ - 162816m^9 + 165888m^7 + 221184m^6 - 94208m^3 - 49152m + 32768$$

The polynomial $f$ is irreducible. In $K = \mathbb{Q}[m]/(f)$ put

$$\eta = -\frac{11m^{13} - 112m^5 - 224m^4 + 192m}{8(13m^9 + 16m - 16)}$$

Then the identity

$$F(mz + \eta, z) = \Big(z^2 - \frac{m^3}{2}z - \frac{3m^2\eta}{2} - \frac{m^6}{8}\Big)^2$$

holds. $K$ has signature $(r_1, r_2) = (7, 10)$ and discriminant $D = 2^{30} \cdot 5^{10} \cdot 431^6 \cdot 659^6$. There are two prime ideals above 2, with $(e, f) = (8, 3), (1, 3)$ (certificate 1.1.8a).

The bad primes are as follows. The point $O$ is smooth in every characteristic (at $[1 : 0 : 0]$ the derivative in the $W$ direction is $-1$). In characteristic 3, $F_u \equiv 1$. In characteristic $p > 3$, an affine singular point satisfies

$$u^2 = 1/3, \qquad z^3 = -1/2, \qquad 4u + 9z + 6 = 0$$

The last equation comes from $12F - 4uF_u - 3zF_z = 2(4u + 9z + 6)$. In the critical algebra defined by the first two equations, the norm of the critical value $(4u + 9z + 6)/6$ is $-5^2 \cdot 431 \cdot 659/(2^8 \cdot 3^9)$. Hence the only odd bad primes are 5, 431, 659. The $z$-coordinates of the singular points are given by $z^2 + 3z + 4 \equiv 0 \pmod 5$ (two conjugate points), $z \equiv -6 \pmod{431}$, and $z \equiv -222 \pmod{659}$, respectively. The Hessian determinant $-72uz^2$ is a unit, so all of them are ordinary double points (nodes), and since the critical value has valuation exactly 1, their thickness is 1. A plane quartic with at most two nodes is geometrically irreducible (if it were reducible, then by Bezout the components would meet in at least three points). Therefore, at these three primes the special fiber of the regular model has one component, and the component group of the Jacobian is trivial. Then $J(\mathbb{Q}_p^{\mathrm{nr}})$ is divisible by 2, so the descent image is unramified at $p$. Therefore $S = \{\mathfrak{p} \mid 2\}$ suffices (certificate 1.1.8a).

**Step 2: the class group.**

**Lemma 3.8.3.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (7, 10)$, the $D$ above, and $T = \log 10^7$. The window is a step function on 48 cells of equal width, and its heights are positive integers, symmetric from left to right (the input of certificate 1.1.8d). Two pieces of data are needed.

(i) There are 665,664 prime ideals of norm less than $10^7$ in total, and we count the number $a(q)$ for every norm (certificate 1.1.8b).

(ii) All 9,432 prime ideals of norm at most $10^5$ are principal ideals. For each of these ideals we give a witness $g$ for Lemma C and check it in exact arithmetic (certificate 1.1.8c). Therefore we set $k(q) = a(q)$ if $q \le 10^5$, and $k(q) = 0$ otherwise. Since $(10^5)^2 > 10^7$, all terms with $m \ge 2$ receive a positive sign.

With these data the computation gives $B^-(f) > 0.0930446107 > 0$ (certificate 1.1.8d). In detail, $C_\infty = -0.7891595062\ldots$, the integral term is $0.0842206841\ldots$, and the prime term is $0.9664248011\ldots$. The computation uses exact rational coefficients and directed interval arithmetic (224 bits), so rounding errors cannot change the conclusion. By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: an upper bound for the rank.**

**Lemma 3.8.4.** $\operatorname{rank} J(\mathbb{Q}) \leq 2$.

*Proof.* The hypotheses of Proposition A (a rational hyperflex, irreducibility of $f$) were checked above. Hence $J(\mathbb{Q})[2] = 0$ and $\delta$ is injective. For an affine rational point $P$, $\delta(P - O)$ is the square class of $u(P) - mz(P) - \eta$. With $t = z/u$, $w = 1/u$ at $O$, the value of $t^4(u - mz - \eta)$ is 1, so this normalization is correct. By Step 1 the image lies in $K(S, 2)$, and by Lemma 3.8.3

$$\dim_{\mathbb{F}_2} K(S, 2) = (r_1 + r_2) + \#S = 17 + 2 = 19$$

Nineteen explicit elements form a basis of this space. We factor the principal divisors of 85 atomic elements exactly into 61 prime ideals to show that all 19 elements have even valuation outside 2, and we check that the matrix of quadratic characters has rank 19 (certificate 1.1.8e).

We impose conditions on this 19-dimensional space one at a time. Imposing the condition that the norm is a square (the sign and the parity of the 2-adic valuation) gives dimension 17. At the good primes 7, 11, 59, 83, the polynomial $f$ splits into three irreducible factors of degree 9. A Frobenius-invariant codeword has weight divisible by 9, while the nonzero codewords have weights 12 and 16. Hence $J(\mathbb{F}_p)[2] = 0$ and $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = 0$. That is, the quadratic characters at the three prime ideals above $p$ must all be 0. These conditions reduce the dimension to $15, 13, 11, 9$ in turn.

At 2, the bitangent orbits have sizes 24 and 3. The partial sums $0, 3, 24, 27$ do not include 12 or 16, so $J(\mathbb{Q}_2)[2] = 0$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = g = 3$. In the two components of $K \otimes \mathbb{Q}_2$, the spaces of square classes have dimensions 26 and 5. By Hensel's lemma every element of $1 + \mathfrak{p}^{2e+1}$ is a square, so a finite computation in the unit group gives the whole space of square classes. We use three local points: the rational points $P_0$, $P_1$, and the point with $t = 2$ in the disk at infinity. The last point is obtained by computing the root $w$ ($v_2(w) = 4$) of $t^4 - w + (1 + 2t)w^3 + w^4 = 0$ modulo $2^{80}$. The relative error caused by the approximation has valuation at least 648 and at least 81 in the two local fields, respectively, which is more than the depths 19 and 5 needed to determine the square classes. The three images are independent, so they make up the whole local image. Keeping only the elements of the 9-dimensional space that map into this image leaves the 2-dimensional space spanned by (in the numbering of the 19 basis elements)

$$e_3 + e_{14} + e_{19}, \qquad e_5 + e_{14}$$

(certificate 1.1.8e). Since $J(\mathbb{Q})[2] = 0$, $\operatorname{rank} J(\mathbb{Q}) \leq 2$. □

**Step 4: 2-adic logarithms and the annihilating differential.** Let $G_i = [P_i - O]$ ($i = 0, 1$), and take the basis of holomorphic differentials

$$\omega_\bullet = (\omega_0, \omega_1, \omega_2) = (1, z, u)\,\frac{dz}{1 - 3u^2}$$

**Lemma 3.8.5.** $\operatorname{rank} J(\mathbb{Q}) = 2$. *Moreover, there is a primitive vector $a = (a_0, a_1, a_2) \in \mathbb{Z}_2^3$ with $a \equiv (12, 14, 9) \pmod{16}$ such that $\omega = a_0\omega_0 + a_1\omega_1 + a_2\omega_2$ annihilates all 2-adic logarithms of $J(\mathbb{Q})$.*

*Proof.* There is a polynomial $h_i(u, z)$ of degree at most 2 in $u$ such that

$$\operatorname{div}(h_i) = 16P_i + E_i - 19O, \qquad \deg E_i = 3$$

This is checked exactly: the Taylor order at $P_i$ is 16, the maximum of the pole orders $3a + 4b$ of the terms $z^a u^b$ is exactly 19, and $\operatorname{Res}_u(F, h_i)$ is a constant times $(z + 1)^{16}$ times a squarefree cubic, and this cubic does not vanish at $z = -1$ (certificate 1.1.8f).

At the point at infinity put $t = z/u$, $w = 1/u$. Then the curve is $t^4 - w + (1 + 2t)w^3 + w^4 = 0$, and the derivative in the $w$ direction at $(0, 0)$ is $-1$, so there is only one branch, $w = t^4 + \cdots \in \mathbb{Z}_2[[t]]$. At the points of $E_i$, the characteristic polynomials of $t$ and of $w$ are monic with every coefficient

except the leading coefficient even (equivalently, each reduces to $T^3$ modulo 2), so $E_i$ lies in the residue disk of $O$ ($v_2(t) = 1/3, 1/3, 1/3$ on $E_0$, and $1, 1, 4$ on $E_1$). In this parameter the differential is $(w, t, 1)(1 - tw'/w)(w^2 - 3)^{-1}dt$, with 2-adically integral coefficients. Therefore

$$\log G_i = -\tfrac{1}{16} \operatorname{Tr}_{E_i} \int_0^t \omega_\bullet$$

and the trace is computed exactly from the Newton sums of the characteristic polynomial of $t$. We compute up to 156 terms with 44 digits. The discarded term of degree $n$ has valuation at least $\lfloor n/3 \rfloor - v_2(n) - 4 \geq 44$ ($n \geq 157$), and the finite computation loses at most 11 digits, so at least 33 digits are guaranteed (certificate 1.1.8f). Modulo $2^{12}$,

$$4 \log G_0 \equiv (3044,\ 434,\ 1012), \qquad 4 \log G_1 \equiv (4064,\ 481,\ 1506)$$

The two logarithms are linearly independent, so $\operatorname{rank} J(\mathbb{Q}) \geq 2$, and together with Lemma 3.8.4 this gives $\operatorname{rank} J(\mathbb{Q}) = 2$. The minimal valuation of the components of the cross product of the two vectors is $-2$, and multiplying it by 4 gives the primitive vector $a \equiv (12, 14, 9) \pmod{16}$. The subgroup generated by $G_0, G_1$ has finite index in $J(\mathbb{Q})$ modulo torsion, and the logarithm kills torsion, so $\omega$ kills all logarithms of $J(\mathbb{Q})$. □

**Step 5: two disks covering the integral points.** Modulo 2 we have $F \equiv z + 1$, so $z$ is odd at an integral point.

**Lemma 3.8.6.** *Among the integer solutions of $F(u, z) = 0$, the only one with $u$ even is $P_0$, and the only ones with $u$ odd are $P_1, P_2$.*

*Proof. The even disk.* If $u$ is even, substituting $z = -1 + 2t$ gives $4 \mid u$. Writing $u = 4a$, we get

$$a - 16a^3 = t - 6t^2 + 8t^3 - 4t^4$$

For each $t \in \mathbb{Z}_2$ this equation has only one solution $a \in \mathbb{Z}_2$, by the contraction mapping principle. More generally, for a rational number $r$ with $0 < r < 2/3$, if $|t| \leq 2^r$ then $a \mapsto t - 6t^2 + 8t^3 - 4t^4 + 16a^3$ is a contraction that preserves $|a| \leq 2^r$, so $a(t)$ is analytic on a disk of radius greater than 1. Dividing the pullback of $\omega$ by 4 gives

$$D_e(t)\, dt = \frac{(a_0 - a_1)/2 + a_1 t + 2a_2 a(t)}{1 - 48a(t)^2}\, dt$$

On these disks the denominator is a unit, $(a_0 - a_1)/2$ is a unit, and the remaining terms are smaller, so $|D_e| \leq 1$. Letting $r \uparrow 2/3$ in the Cauchy inequality, we get $v_2(d_j) \geq \lceil 2j/3 \rceil$ for the coefficients of $D_e = \sum d_j t^j$. Hence $H_e(t) = \int_0^t D_e$ satisfies

$$v_2([t^n] H_e) \geq \lceil 2(n-1)/3 \rceil - v_2(n) \geq 1 \qquad (n \geq 5)$$

The coefficients with $n \leq 4$ are determined by $a$ modulo 16, and their valuations are $0, 4, 2, 2$ (certificate 1.1.8g). Therefore $H_e \equiv t \pmod 2$, and by Strassmann's theorem the only zero of $H_e$ in $\mathbb{Z}_2$ is $t = 0$ ($P_0$).

*The odd disk.* Writing $u = 1 + 2t$, $z = -1 + 2b$, we get

$$b - 6b^2 + 8b^3 - 4b^4 = -t - 3t^2 - 2t^3$$

If $0 < r < 1/3$, then for $|t| \leq 2^r$ the fixed-point map is a contraction that preserves $|b| \leq 2^{2r}$ (the strongest constraint is $|4b^4| \leq 2^{8r-2} < 2^{2r}$), so $b(t)$ is analytic on a disk of radius greater than 1. The pullback of $\omega$ is

$$D_o(t)\, dt = \frac{a_0 - a_1 + a_2 + 2a_1 b(t) + 2a_2 t}{1 - 12b(t) + 24b(t)^2 - 16b(t)^3}\, dt$$

where the denominator is a unit and the numerator has absolute value at most 1. By the same argument, $H_o(t) = \int_0^t D_o$ satisfies

$$v_2([t^n]H_o) \geq \lceil (n-1)/3 \rceil - v_2(n) \geq 1 \qquad (n \geq 9)$$

The valuations of the first eight coefficients are $(0, 0, 4, 1, 3, 3, 4, 3)$ (certificate 1.1.8g). Therefore $H_o \equiv t + t^2 \pmod 2$, and by Strassmann's theorem there are at most two zeros. The points $t = 0$ ($P_1$) and $t = -1$ ($P_2$) are zeros. Indeed, $H_o(-1) = \int_{P_1}^{P_2} \omega$ is the value of $\omega$ on the logarithm of $[P_2 - P_1] \in J(\mathbb{Q})$, and hence it is 0.

Finally, the two parametrizations are analytic embeddings of open disks of radius greater than 1. By [KRZB16, Section 3], on these disks the Abelian integrals are equal to the power-series antiderivatives above. Therefore, if an integral point $P$ lies in the even disk, then $H_e(t(P)) = \frac{1}{4}\,\omega(\log[P - P_0]) = 0$, and if it lies in the odd disk, then $H_o(t(P)) = \omega(\log[P - P_1]) = 0$. The zeros counted above are all the zeros. □

*Proof of Proposition 3.8.2.* At an integer solution $z$ is odd, so every integer solution lies in one of the two disks. By Lemma 3.8.6, the only integer solutions are $P_0, P_1, P_2$, and these three points do satisfy $F = 0$. This argument involves no bound on the size of the coordinates. □

## 3.9 $x^4 + y^3 + 2x + y + 1 = 0$ ($H = 31$)

**Theorem 3.9.1.** *The only integer solution of $x^4 + y^3 + 2x + y + 1 = 0$ is $(x, y) = (-1, 0)$.*

**Setup.** We do not change the coordinates. The projective completion of

$$C: \quad F(x, y) = x^4 + y^3 + 2x + y + 1 = 0$$

is $X^4 + Y^3Z + 2XZ^3 + YZ^3 + Z^4 = 0$. It is a smooth plane quartic (genus 3) (Step 1), and it has only one point at infinity, $O = [0 : 1 : 0]$. The tangent line $Z = 0$ meets the curve at $O$ with multiplicity 4, since $X^4 = 0$; so $O$ is a rational hyperflex. Near the point at infinity we put $t = x/y$, $w = 1/y$; then the curve is $t^4 + w + (1 + 2t)w^3 + w^4 = 0$, and $w = -t^4 + \cdots$. $J$ is the Jacobian of $C$.

We use two rational divisor classes. For $P_0 = (-1, 0)$ let $G_0 = [P_0 - O]$. Let $D_{\text{eff}}$ be the effective divisor of degree 2 defined by $x^2 - 2x + 3 = 0$, $y = x - 2$, and let $D = [D_{\text{eff}} - 2O]$. By the identity

$$F(x, x - 2) = (x^2 - 2x + 3)(x^2 + 3x - 3)$$

$D_{\text{eff}}$ lies on the curve. Theorem 3.9.1 is equivalent to the following proposition.

**Proposition 3.9.2.** *The only affine integral point of $C$ is $P_0$.*

The proof has six steps. In Step 1 we fix the bitangent field $K$ and the bad primes. In Step 2 we show $\mathrm{Cl}(K)[2] = 0$ by Proposition B, and in Step 3 we show by 2-descent that the rank is exactly 2 and that $\langle G_0, D \rangle$ has odd index. In Step 4 we construct an annihilating differential from 2-adic logarithms. In Step 5 we show that a single 2-adic disk covering all integral points contains at most two zeros. One of them is $P_0$, and the other is excluded in Step 6 by a Mordell–Weil sieve at 23. The curve has bad reduction at 2, so we use [KRZB16, Section 3] to identify the integrals on the disk with integrals of power series.

**Step 1: the bitangent field and bad primes.** The 27 bitangents other than the tangent line at $O$ have the form $y = mx + \eta$, and the slope $m$ is a root of

$$\begin{aligned} f(m) = {} & m^{27} + 480m^{19} - 2688m^{18} + 17280m^{15} - 34560m^{11} - 141312m^{10} \\ & - 162816m^9 - 165888m^7 - 221184m^6 - 126976m^3 + 49152m - 32768 \end{aligned}$$

The polynomial $f$ is irreducible. In $K = \mathbb{Q}[m]/(f)$ put

$$\eta = \frac{11m^{13} + 112m^5 + 224m^4 + 192m}{8(13m^9 - 16m + 16)}$$

Then

$$F(x, mx + \eta) = \left(x^2 + \frac{m^3}{2}x + \frac{3m^2\eta}{2} - \frac{m^6}{8}\right)^2$$

$K$ has signature $(r_1, r_2) = (3, 12)$ and discriminant $D_K = 2^{30} \cdot 12527563^6$ (12527563 is prime). There are two prime ideals above 2, with $(e, f) = (8, 3), (1, 3)$ (certificate 1.1.9a).

The point $O$ is smooth in every characteristic (the derivative in the $w$ direction is 1). In characteristic 3, $F_y \equiv 1$. In characteristic $p > 3$, an affine singular point satisfies $x^3 = -1/2$, $y^2 = -1/3$, $9x + 4y + 6 = 0$ (the last equation comes from $12F - 3xF_x - 4yF_y = 2(9x + 4y + 6)$). The norm of the critical value $(9x + 4y + 6)/6$ is $12527563/(2^8 \cdot 3^9)$, so the only odd bad prime is $p = 12527563$. There the only singular point is $(x, y) \equiv (2189611, 4469046)$, and the Hessian determinant $72x^2y \equiv 4898948$ is a unit, so it is an ordinary node. The critical norm has valuation 1, so the thickness is 1. A plane quartic with only one node is geometrically irreducible, so the component group of the Jacobian is trivial, and the descent image is unramified at $p$. Therefore $S = \{\mathfrak{p} \mid 2\}$ suffices (certificate 1.1.9a).

**Step 2: the class group.**

**Lemma 3.9.3.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (3, 12)$, the $D_K$ above, and $T = \log 10^9$. The window is a step function on 96 cells of equal width, and its heights are positive integers, symmetric from left to right (the input of certificate 1.1.9d). Two pieces of data are needed.

(i) There are 50,851,991 prime ideals of norm less than $10^9$ in total, and we count the number $a(q)$ for every norm (certificate 1.1.9b). For the primes $p \le 31622$ and the primes of the polynomial discriminant we factor into prime ideals directly in the maximal order; for the remaining primes we count the prime ideals of degree 1 by $\deg \gcd(f, X^p - X)$.

(ii) All 879,491 prime ideals of norm at most $1.35 \cdot 10^7$ are principal ideals (certificate 1.1.9c). For 879,341 of them, $(g) = \mathfrak{p}$ is checked for a single element $g$ by an exact ideal equality. The remaining 150 are checked with a product $\prod_j \alpha_j^{e_j}$: we factor the principal divisor of each atomic element $\alpha_j$ exactly into prime ideals and add the exponents in integer arithmetic, and then the exponent of $\mathfrak{p}$ is 1 and all the others are 0. (certificate 1.1.9c constructs the witnesses anew, and in that case every ideal is verified by a single witness for Lemma C, without product witnesses.) Therefore we set $k(q) = a(q)$ if $q \le 1.35 \cdot 10^7$, and $k(q) = 0$ otherwise. Since $(1.35 \cdot 10^7)^2 > 10^9$, all terms with $m \ge 2$ receive a positive sign.

With these data the computation gives the integral term $0.0631019954\ldots$ and

$$B^-(f) = 3.3541015\ldots \cdot 10^{-5} > 0$$

(certificate 1.1.9d). The computation uses exact rational coefficients and directed interval arithmetic (288 bits), and the radius of the final interval is less than $10^{-61}$. Hence the sign is certain, even though the margin is small. By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: the rank and the index.**

**Lemma 3.9.4.** $J(\mathbb{Q})[2] = 0$ *and* $\operatorname{rank} J(\mathbb{Q}) = 2$. *Moreover,* $\langle G_0, D\rangle$ *has odd index in* $J(\mathbb{Q})$.

*Proof.* The hypotheses of Proposition A were checked above. Hence $J(\mathbb{Q})[2] = 0$, $\delta$ is injective, and at an affine point $\delta(P - O)$ is the square class of $mx(P) + \eta - y(P)$ (the value of $t^4(mx + \eta - y)$ at $O$ is 1). By Step 1 and Lemma 3.9.3, the image lies in the space of dimension

$$\dim_{\mathbb{F}_2} K(S, 2) = (r_1 + r_2) + \#S = 15 + 2 = 17$$

Seventeen explicit elements form a basis of this space. We factor the principal divisors of 161 atomic elements exactly into 141 prime ideals to show that all valuations outside 2 are even, and we check that the matrix of quadratic characters has rank 17 (certificate 1.1.9e).

We impose the conditions one at a time. The condition that the norm is a square reduces the dimension from 17 to 15. At a good odd prime $p$ the local image is the image of $V/(\mathrm{Frob}-1)V \to E/(\mathrm{Frob}-1)E$. Here $V = J[2]$, and $E = \mathbb{F}_2^{27}$ is the permutation module on the 27 bitangents. We bound its dimension from above as follows: among the elements of the orthogonal group (of order 51,840) that preserves the quadratic form on $V$, we take all $T$ that induce on the bitangents the same cycle type as Frobenius, compute for each the dimension of the image of $V/(T-1)V \to E/(T-1)E$, and take the maximum (certificate 1.1.9e). The images of points obtained by Hensel lifting points of $C(\mathbb{F}_p)$ attain this upper bound, so we know the local image exactly. The results are as follows.

| $p$ | degrees of the factors of $f$ mod $p$ | dimension of local image | remaining dimension |
|---|---|---|---|
| 13 | $(9,9,9)$ | 0 | 13 |
| 17 | $(3,12,12)$ | 0 | 11 |
| 43 | $(9,9,9)$ | 0 | 9 |
| 53 | $(9,9,9)$ | 0 | 7 |
| 59 | $(3,3,3,3,3,3,3,3,3)$ | 2 | 4 |
| 67 | $(2,5,5,5,10)$ | 1 | 3 |

At 2 the bitangent orbits have sizes 24 and 3, so $J(\mathbb{Q}_2)[2] = 0$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3$. The spaces of square classes of the two local components have dimensions 26 and 5. The images of three local divisor classes are independent, so they make up the whole local image. The first is $P_0$ ($\delta = \eta - m$). The second is the point with $t = 2$ in the disk at infinity, where $w$ is computed modulo $2^{80}$ ($v_2(w) = 4$). The third is the trace divisor $P + P^\sigma - 2O$ formed from the point $P = (d, y)$, $y \equiv d \pmod 2$ (Hensel; $F_y$ is a unit), over the unramified quadratic extension $\mathbb{Q}_2(d)$, $d^2 + d + 1 = 0$. For the second and the third, the relative error of the approximation has valuation at least 640 and at least 80 in the two local fields, which is more than the required depths 19 and 5. Keeping only the elements of the 3-dimensional space that map into this local image leaves the 2-dimensional space spanned by (in the numbering of the 17 basis elements)

$$e_3 + e_5, \qquad e_4 + e_5 + e_6 + e_{17}$$

Therefore $\mathrm{rank}\, J(\mathbb{Q}) \le 2$.

The lower bound and the index are as follows. We have $\delta(G_0) = \eta - m$, and at a point $Q$ of $D_{\mathrm{eff}}$, $mx + \eta - y = -(bx + a)$ ($a = -2 - \eta$, $b = 1 - m$), so $\delta(D) = a^2 + 2ab + 3b^2$. Computing the quadratic characters at the simple roots $m \equiv -1 \pmod 5$ and $m \equiv -21 \pmod{37}$ of $f$, the rows, in the order $(G_0, D)$, are $(1,1)$ and $(1,0)$ (certificate 1.1.9e). The determinant is 1, so $G_0, D$ are independent in $J(\mathbb{Q})/2J(\mathbb{Q})$. Since $J(\mathbb{Q})[2] = 0$, we have $\dim J(\mathbb{Q})/2J(\mathbb{Q}) = \mathrm{rank}\, J(\mathbb{Q}) \le 2$; hence the rank is 2, and $G_0, D$ generate $J(\mathbb{Q})/2J(\mathbb{Q})$. That is, the index of $\langle G_0, D\rangle$ is odd. □

**Step 4: 2-adic logarithms and the annihilating differential.** We take the basis of holomorphic differentials $\omega_\bullet = (\omega_0, \omega_1, \omega_2) = (1, x, y)\, dx/(1 + 3y^2)$.

**Lemma 3.9.5.** *There is a primitive vector $a = (a_0, a_1, a_2) \in \mathbb{Z}_2^3$ with $a \equiv (6, 10, 9) \pmod{16}$ such that $\omega = a_0\omega_0 + a_1\omega_1 + a_2\omega_2$ annihilates all 2-adic logarithms of $J(\mathbb{Q})$. The vector $a$ is known exactly to at least 50 digits.*

*Proof.* There are polynomials $h_0, h_D$ of degree at most 2 in $y$ such that

$$\mathrm{div}(h_0) = 16P_0 + E_0 - 19O, \qquad \mathrm{div}(h_D) = 8D_{\mathrm{eff}} + E_D - 19O, \qquad \deg E_0 = \deg E_D = 3$$

This is checked by exact Taylor expansions at the given points, by the pole orders (the maximum of the weights $3i + 4j$ of the terms $x^i y^j$ is 19, and the weights are all distinct), and by the factorization of the norm polynomials (certificate 1.1.9f). On $E_0$ and $E_D$, the valuations of the coefficients of the characteristic polynomial of $t$, from the lowest degree up, are $(1,3,3,0)$ and $(2,2,3,0)$, so $v_2(t) = 1/3$

and $2/3$. For the characteristic polynomial of $w$ they are $(4,7,4,0)$ and $(8,9,5,0)$, so $w$ also has positive valuation. Hence $E_0, E_D$ lie in the residue disk of $O$. There the differential is $(w,t,1)(1-tw'/w)(w^2+3)^{-1}dt$, with 2-adically integral coefficients, so

$$\log G_0 = -\tfrac{1}{16}\operatorname{Tr}_{E_0}\int_0^t \omega_\bullet, \qquad \log D = -\tfrac{1}{8}\operatorname{Tr}_{E_D}\int_0^t \omega_\bullet$$

We compute with 216 terms and 64 digits. The discarded term of degree $n$ satisfies $v_2(\operatorname{Tr}(t^n)/16n) \geq \lceil n/3\rceil - v_2(n) - 4 \geq 65$ ($n \geq 217$), and the finite computation loses at most 11 digits, so at least 53 digits are guaranteed (certificate 1.1.9f). Modulo $2^{12}$,

$$4\log G_0 \equiv (3988,\ 2194,\ 1012), \qquad 4\log D \equiv (1848,\ 3542,\ 3892)$$

The two logarithms are independent, and the minimal valuation of the components of their cross product is $-1$. Multiplying it by 2 gives the primitive vector $a \equiv (6,10,9) \pmod{16}$. By Lemma 3.9.4, $\langle G_0, D\rangle$ has finite index in $J(\mathbb{Q})$ modulo torsion, so $\omega$ kills all logarithms of $J(\mathbb{Q})$. □

**Step 5: the disk covering the integral points.** Modulo 2 we have $F \equiv x+1$, so $x$ is odd. Then $x^4+2x+1 \equiv 0 \pmod 4$. If $y$ is odd, then $y^3+y \equiv 2 \pmod 4$, a contradiction; if $y$ is even, then $y^3+y \equiv 0 \pmod 4$ gives $4 \mid y$. Hence every integral point can be written as

$$x = -1+2t, \qquad y = 4b, \qquad b+16b^3 = t-6t^2+8t^3-4t^4 \qquad (t,b \in \mathbb{Z}_2)$$

**Lemma 3.9.6.** *Let $H(t)$ be the antiderivative of $\omega$ starting at $P_0$ ($t=0$), divided by 8. The only zeros of $H$ in $\mathbb{Z}_2$ are $t=0$ and a single odd $t_*$, and $t_* \equiv 3{,}366{,}055{,}599 \pmod{2^{32}}$. The coordinates $(c_0, c_D)$ of the logarithm of the point $P(t_*)$ with respect to $\log G_0, \log D$ lie in $\mathbb{Z}_2$, and $(c_0, c_D) \equiv (11,10) \pmod{32}$.*

*Proof.* For every $R$ with $1 \leq R < 2^{2/3}$ and $|t| \leq R$, the map $b \mapsto t-6t^2+8t^3-4t^4-16b^3$ is a contraction that preserves $|b| \leq R$, so $b(t)$ is analytic on a disk of radius greater than 1, and $|b| \leq R$. Pulling back $\omega$ gives

$$H'(t) = \frac{(a_0-a_1)/4 + (a_1/2)t + a_2 b(t)}{1+48b(t)^2}, \qquad H(0) = 0$$

On this disk $|H'| \leq R$, so the Cauchy inequality gives

$$v_2([t^n]H) \geq \left\lceil \frac{2(n-2)}{3} \right\rceil - v_2(n)$$

This bound is at least 1 if $n \geq 3$ and $n \neq 4$. The remaining coefficients are exactly

$$[t]H = \frac{a_0-a_1}{4}, \qquad [t^2]H = \frac{a_1+2a_2}{4}, \qquad [t^4]H = 36a_0 - 42a_1 - 14a_2$$

and for $a \equiv (6,10,9) \pmod{16}$ the first two are odd and the last has valuation 1. Hence $H \equiv t+t^2 \pmod 2$, and by Strassmann's theorem there are at most two zeros. One of them is $t=0$, and since $H(t)/t \equiv 1+t \pmod 2$, Hensel's lemma gives exactly one odd zero $t_*$. Using $a$ to 50 digits and the antiderivative with 120 terms (the discarded terms have valuation at least 77), we get $t_* \equiv 3{,}366{,}055{,}599 \pmod{2^{32}}$ (certificate 1.1.9g).

The vector $\log[P(t_*) - O] = \log G_0 + \int_{P_0}^{P(t_*)} \omega_\bullet$ is annihilated by $\omega$, so it is a $\mathbb{Q}_2$-linear combination of $\log G_0, \log D$. When we solve for these coordinates with a minor of order 2, the entries of its inverse have valuation at least $-1$, and the $t$-derivative of the tiny integral is divisible by 2. Hence the error $2^{32}$ in $t_*$ changes the coordinates only by multiples of $2^{32}$. The result is $(c_0, c_D) \equiv (10{,}965{,}931,\ 8{,}513{,}226) \pmod{2^{24}}$, that is, $(11,10) \pmod{32}$ (certificate 1.1.9g). □

**Step 6: a sieve at 23.**

**Lemma 3.9.7.** *$P(t_*)$ is not a rational point.*

*Proof.* $C$ has good reduction at 23. The point counts are $\#C(\mathbb{F}_{23^k}) = 26, 622, 12044$ ($k = 1, 2, 3$), and $\#J(\mathbb{F}_{23}) = 14432 = 451 \cdot 32$ (certificate 1.1.9h). Suppose that $P = P(t_*)$ is a rational point. By Lemma 3.9.4 there is an odd $k$ with $k[P - O] = n_0 G_0 + n_D D + \tau$, where $\tau$ is torsion of odd order. Taking logarithms gives $n_0/k = c_0$ and $n_D/k = c_D$. In $J(\mathbb{F}_{23})$, multiplication by 451 kills the odd part and is invertible on the 2-part (of order 32), so we can divide by $k$ modulo 32. Therefore, in the form of [BS10],

$$451\,[\bar{P} - \bar{O}] = 451\,(11\,\bar{G}_0 + 10\,\bar{D}) \qquad (\text{in } J(\mathbb{F}_{23}))$$

must hold. Comparing, by exact Jacobian arithmetic, the right-hand side with the value of the left-hand side for all 26 points of $C(\mathbb{F}_{23})$ ($O$ and 25 affine points), we find no matching point (certificate 1.1.9h). This is a contradiction. □

*Proof of Proposition 3.9.2.* An integral point $P$ lies in the disk of Step 5. Its parametrization is an analytic embedding of an open disk of radius greater than 1, so by [KRZB16, Section 3], $8H(t(P)) = \omega(\log[P - P_0])$. Since $[P - P_0] \in J(\mathbb{Q})$, this value is 0 by Lemma 3.9.5. By Lemma 3.9.6, $t(P) = 0$ or $t(P) = t_*$, and by Lemma 3.9.7 the latter case does not occur. Therefore $P = P_0$. □

## 3.10 $x^4 + y^3 + 2x + y - 1 = 0$ ($H = 31$)

**Theorem 3.10.1.** *The only integer solutions of $x^4 + y^3 + 2x + y - 1 = 0$ are $(x, y) = (-1, 1), (1, -1)$.*

**Setup.** Let $J$ denote the Jacobian of the smooth projective model of the curve. We do not change coordinates. $C$ is the smooth plane quartic (genus 3; Step 1) defined by

$$X^4 + Y^3Z + 2XZ^3 + YZ^3 - Z^4 = 0, \qquad F(x, y) = x^4 + y^3 + 2x + y - 1$$

and $J$ is its Jacobian. The only point at infinity is $O = [0 : 1 : 0]$. The tangent line $Z = 0$ meets the curve there with multiplicity 4, since $X^4 = 0$, so $O$ is a rational hyperflex. Near $O$ we set $t = X/Y$, $w = Z/Y$; then the curve is $t^4 + w + 2tw^3 + w^3 - w^4 = 0$ and $w = -t^4 + O(t^{12})$. We write $A = (-1, 1)$, $B = (1, -1)$, and in $J(\mathbb{Q})$ we use the same letters for $[A - O]$, $[B - O]$.

The proof runs as follows. Unlike in other sections, we do not show $\mathrm{Cl}(K)[2] = 0$. Instead we show that an element of the 2-Selmer group outside $\langle A, B\rangle$ produces a quadratic class character with special properties (Lemma 3.10.5), and we exclude this character with the explicit formula (Proposition 3.10.8). Then the rank is 2. Next, Chabauty–Coleman at $p = 3, 5$ reduces the possible new points to two residue classes (Lemmas 3.10.9, 3.10.10), and the Mordell–Weil sieve excludes both (Lemma 3.10.11).

**Step 1: the bitangent field and descent.** In characteristic $p > 3$, an affine singular point satisfies $2x^3 + 1 = 0$ and $G(x) = 243x^2 - 324x + 124 = 0$, and $\mathrm{Res}(2x^3 + 1, G) = 31 \cdot 433 \cdot 2341$. In characteristic 3 we have $F_y \equiv 1$, and at $O$ the derivative in the $w$ direction is 1 in every characteristic. At each of the three primes there is exactly one singular point: $(x, y) \equiv (22, 14) \pmod{31}$, $(6, 421) \pmod{433}$, $(2236, 823) \pmod{2341}$. The Hessian determinant $72x^2y$ is a unit, so the point is an ordinary node. Lifting the gradient equations modulo $p^4$ shows that the critical value has valuation exactly 1, so the thickness is 1. Since there is only one node, the special fiber is geometrically irreducible (if it were reducible, Bezout would give at least three intersection points), and the component group is trivial. Hence the descent image is unramified at the odd primes (certificate 1.1.10a).

The 27 finite bitangents have the form $y = mx + \eta$, where $m$ is a root of

$$f(m) = m^{27} + 480m^{19} - 2688m^{18} - 17280m^{15} - 34560m^{11} - 141312m^{10} - 162816m^9 + 165888m^7 + 221184m^6 - 126976m^3 + 49152m - 32768.$$

$f$ is irreducible, and in $K = \mathbb{Q}[m]/(f)$ we have

$$\eta = \frac{m(11m^{12} + 112m^4 + 224m^3 - 192)}{8(13m^9 - 16m + 16)}, \qquad F(x, mx + \eta) = \left(x^2 + \frac{m^3}{2}x + \frac{12m^2\eta - m^6}{8}\right)^2.$$

For an arbitrary line $y = mx + z$, put $a = m^3/2$ and $b = (12m^2z - m^6)/8$. The remaining coefficient conditions are $2ab = 3mz^2 + m + 2$ and $b^2 = z^3 + z - 1$. Their resultant with respect to $z$ (left side minus right side, in this order) is $f(m)/4096$, so these are all the finite bitangents. $K$ has $n = 27$, $(r_1, r_2) = (3, 12)$, $D = 2^{30} \cdot 31^6 \cdot 433^6 \cdot 2341^6$, and there are two prime ideals above 2, with $(e, f) = (8, 3), (1, 3)$ (certificate 1.1.10a).

Equip $V = J[2]$ with the quadratic form $q$ determined by $O$. Then the 27 bitangents are indexed by $\Omega = \{w \in V : q(w) = 0,\ w \neq 0\}$, and the descent map is given by $\iota : V \to \mathbb{F}_2^\Omega$, $c \mapsto (\langle c, w\rangle)_{w\in\Omega}$. In suitable coordinates, $q(z) = z_1z_2 + z_3z_4 + z_5z_6 + z_5 + z_6$.

**Lemma 3.10.2.** *$J(\mathbb{Q})[2] = 0$, and $H^1(\mathbb{Q}, J[2]) \to K^\times/K^{\times 2}$ is injective. Composing with the Kummer map $\kappa : J(\mathbb{Q})/2J(\mathbb{Q}) \to H^1(\mathbb{Q}, J[2])$, for a rational point $P \neq O$ the image of $\kappa([P - O])$ is the square class of $mx(P) + \eta - y(P)$. The image of the 2-Selmer group* Sel *lies in*

$$K(\{2\}, 2) = \{[u] \in K^\times/K^{\times 2} : v_\mathfrak{p}(u) \text{ is even for every } \mathfrak{p} \text{ not above } 2\}.$$

*Proof.* Since $f$ is irreducible, the Galois group acts transitively on $\Omega$. Proposition A gives $J(\mathbb{Q})[2] = 0$. Its proof (the argument that a Sylow 3-subgroup containing a Sylow 3-subgroup of a point stabilizer is transitive on $\Omega$) gives injectivity not only on $J(\mathbb{Q})/2J(\mathbb{Q})$ but on all of $H^1(\mathbb{Q}, J[2])$. The value of $t^4(mx + \eta - y)$ at $O$ is 1, so the normalization is correct. A Selmer element maps to a local class that is unramified at every odd prime (at the bad primes, by the component group computation above), so its valuations away from 2 are even. □

**Step 2: the 2-adic image and 17 known classes.** The square class spaces of the two components of $K \otimes \mathbb{Q}_2$ have dimensions 26 and 5, and their sum $\mathcal{T}_2$ has dimension 31. The 2-adic bitangent orbits have sizes 3 and 24, so there is no invariant codeword of weight 12 or 16. Hence $J(\mathbb{Q}_2)[2] = 0$, and the image $\mathcal{I}_2 \subset \mathcal{T}_2$ of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$ is 3-dimensional.

**Lemma 3.10.3.** *There are explicit elements $u_1, \ldots, u_{17}$ of $K(\{2\}, 2)$ whose 2-adic images span a 17-dimensional space $\mathcal{L}_2$, and $\mathcal{L}_2 \cap \mathcal{I}_2$ is the 2-dimensional space spanned by the images of $[A - O]$ and $[B - O]$.*

*Proof.* Each $u_i$ is a product of some of 170 polynomials in $m$ with rational coefficients. We factor its principal ideal and check that all valuations away from 2 are even. The 2-adic images are computed from the parity of the valuations and the unit square class modulo $\mathfrak{p}^{2e+1}$ (elements of $1 + \mathfrak{p}^{2e+1}$ are squares), and they have rank 17. $\mathcal{I}_2$ is spanned by the images of three actual 2-adic points: the point lifting $y \equiv 0 \pmod 2$ at $x = -63$ ($F_y = 3y^2 + 1$ is odd), and the points lifting $x \equiv 1 \pmod 2$ at $y = -31, -29$ (the derivative $2x^3 + 1$ of $F(1 + 2u, y)/4 \in \mathbb{Z}_2[u]$ is odd). We compute each point modulo $2^{48}$; the valuation of the approximation error is larger than the valuation of the image plus $2e$, so the square classes are exact. The three images have rank 3. The 17 and the 3 together have rank 18, so $\dim(\mathcal{L}_2 \cap \mathcal{I}_2) = 2$. The images of $A$, $B$ lie in both spaces and are independent (certificate 1.1.10a). □

**Step 3: the localization image and strictification of Selmer classes.** Adding the three real places, we set $\mathcal{T} = \mathcal{T}_2 \oplus \bigoplus_{v \text{ real}} K_v^\times/K_v^{\times 2}$ (dimension 34), and give it the $\mathbb{F}_2$-valued pairing equal to the sum of the Hilbert symbols at the 2-adic and real places. Each local Hilbert pairing is nondegenerate, so this pairing is nondegenerate too.

**Lemma 3.10.4.** *Let $\mathcal{L}$ be the span of the images of $u_1, \ldots, u_{17}$ in $\mathcal{T}$. Then the image of $K(\{2\}, 2)$ in $\mathcal{T}$ is exactly $\mathcal{L}$. Moreover, the projection $\mathcal{L} \to \mathcal{T}_2$ is injective.*

*Proof.* If $u, v \in K(\{2\}, 2)$, then at the odd finite places both are units modulo squares, so their Hilbert symbol is 1; it is also 1 at the complex places. By Hilbert reciprocity, the image of $K(\{2\}, 2)$ is isotropic in $\mathcal{T}$. By Lemma 3.10.3, $\mathcal{L} \to \mathcal{T}_2$ is injective and $\dim \mathcal{L} = 17$. Since $\mathcal{L}$ is a 17-dimensional isotropic subspace of a 34-dimensional nondegenerate space, $\mathcal{L} = \mathcal{L}^\perp$. By reciprocity, the image of an element of $K(\{2\}, 2)$ is orthogonal to $\mathcal{L}$, so it lies in $\mathcal{L}$. □

**Lemma 3.10.5.** *Suppose* $\mathrm{Sel} \neq \langle \kappa(A), \kappa(B) \rangle$. *Then there is a nontrivial character* $\chi : \mathrm{Cl}(K) \to \{\pm 1\}$ *of the ordinary class group, and for every prime* $p > 15{,}000{,}000$ *there are a Frobenius* $g \in O(V, q)$ *and* $c \in V$ *such that*

$$\sum_{\mathfrak{p} \mid p,\ N\mathfrak{p} = p} \chi(\mathfrak{p}) = \sum_{w \in \Omega,\ gw = w} (-1)^{\langle c, w \rangle}.$$

*Proof.* Choose $\gamma \in \mathrm{Sel} \setminus \langle \kappa(A), \kappa(B) \rangle$. By Lemma 3.10.2, the image of $\gamma$ lies in $K(\{2\}, 2)$. Hence, by Lemma 3.10.4, its 2-adic image lies in $\mathcal{L}_2$, and by the Selmer condition it also lies in $\mathcal{I}_2$. By Lemma 3.10.3, there are $\epsilon, \epsilon' \in \mathbb{F}_2$ such that the 2-adic image of $\gamma' = \gamma - \epsilon\kappa(A) - \epsilon'\kappa(B)$ is 0. Then $\gamma' \neq 0$, and it is still a Selmer element. By Lemma 3.10.4, the image of $\gamma'$ in $\mathcal{T}$ lies in $\mathcal{L}$, and its 2-adic component is 0, so its real components are also 0. Let $u$ be the image of $\gamma'$. Then $u \neq 1$, and $K(\sqrt{u})/K$ is unramified at the odd places (even valuations) and split at the 2-adic and real places. Therefore its character $\chi$ is a nontrivial quadratic character of the ordinary class group.

If $p > 15{,}000{,}000$, then $C$ has good reduction at $p$ and $K$ is unramified at $p$. $\gamma'$ is unramified at $p$, so it is determined by its cocycle value $c$ at Frobenius. A degree-one prime ideal $\mathfrak{p} \mid p$ of $K$ corresponds to a $w \in \Omega$ fixed by $g$, and the quadratic character of $u$ there is the $w$-component $\langle c, w \rangle$ of $\iota(c)$. □

**Step 4: a lower bound for the character sum.**

**Lemma 3.10.6.** *For a subspace* $U \leq V = \mathbb{F}_2^6$, *let* $r(U) = \#\{w \in U \setminus 0 : q(w) = 0\}$. *For every* $c \in V$,

$$\sum_{w \in U,\ q(w) = 0,\ w \neq 0} (-1)^{\langle c, w \rangle} \geq \ell(r(U)),$$

| $r$ | 0 | 1 | 2 | 3 | 5 | 7 | 9 | 11 | 15 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\ell(r)$ | 0 | −1 | −2 | −3 | −3 | −5 | −3 | −5 | −5 | −5 |

*In particular, this sum is always at least* $-5$.

*Proof.* We examine all 2825 subspaces of $V$ (by dimension: $1, 63, 651, 1395, 651, 63, 1$) and all 64 vectors $c$ (certificate 1.1.10b). □

On the right-hand side of Lemma 3.10.5, $U = \ker(g - 1)$, and $r(U)$ is the number of roots of $f$ modulo $p$, $r(p) = \deg \gcd(f, z^p - z)$. The polynomial discriminant is

$$2^{390} 3^{54} 17^2\, 31^6\, 101^2\, 433^6\, 2341^6\, 2969^2\, 5227^2\, 924151^2,$$

and all its prime factors are smaller than 15,000,000. Hence for $p > 15{,}000{,}000$, $r(p)$ is exactly the number of degree-one prime ideals.

**Step 5: principal ideals.**

**Lemma 3.10.7.** *All* 971,856 *prime ideals of norm at most* $M = 15{,}000{,}000$ *are principal.*

*Proof.* We construct the prime ideals exhaustively as follows. For $p > \sqrt{M}$ not dividing the denominators of the integral basis, only degree-one prime ideals can have norm at most $M$, and for each root $r$ of $f$ modulo $p$ the kernel of $b_i \mapsto b_i(r)$ is a degree-one prime ideal. For the remaining $p$ we factor directly in the maximal order. For each $\mathfrak{p}$ we check an element $g \in \mathfrak{p}$ exactly. If $|N(g)| = N\mathfrak{p}$, then $(g) = \mathfrak{p}$. Otherwise we prove the prime factorization $|N(g)|/N\mathfrak{p} = \prod r^{e_r}$ and check that $r^{e_r} < N\mathfrak{p}$ for all $r$. By Lemma C, all of them are principal (certificate 1.1.10c). □

**Step 6: excluding the character, and the rank.**

**Proposition 3.10.8.** $\mathrm{Sel} = \langle \kappa(A), \kappa(B) \rangle$ *and* $\operatorname{rank} J(\mathbb{Q}) = 2$.

*Proof.* Suppose Sel is larger, and take $\chi$ as in Lemma 3.10.5. Set $X = 10^{11}$, $T = \log X$, $R = 765{,}000{,}000$, and use the normalized autocorrelation $f$ of a window with 128 cells of equal width and positive integer heights, symmetric left to right (we check that $f$ is decreasing on $[0, T]$). By Proposition H,

$$C_\infty - \int_0^\infty (1-f)W\,dx + \frac{4}{27}\sum_{\mathfrak{p}}\sum_{N\mathfrak{p}^m<X} \chi(\mathfrak{p})^m \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m+1} f(m\log N\mathfrak{p}) \le 0.$$

We bound the left-hand side from below.

(i) If $N\mathfrak{p} \le M$, then $\chi(\mathfrak{p}) = 1$ by Lemma 3.10.7. For the 27,293 prime ideals of norm at most $316{,}227 = \lfloor\sqrt{X}\rfloor$ we include all prime power terms exactly. The remaining 944,563 are grouped into 7,715 norm intervals, and each group is bounded by the value at the right endpoint. We call this sum $\Sigma_{\mathrm{pr}}$.

(ii) To the 26,759 prime ideals of degree at least 2 with norm in $(M, X)$ we assign $\chi = -1$ (sum $\Sigma_{\mathrm{hi}}$). Since $M^2 > X$, there are no terms with $m \ge 2$ for ideals of norm greater than $M$ (certificate 1.1.10d).

(iii) For the 38,465,791 primes with $M < p < R$, we bound the sum over the degree-one prime ideals by $\ell(r(p))$ from Lemma 3.10.6. The distribution of $r(p)$ is 17610407, 12425717, 3851583, 2971635, 1200580, 200672, 177984, 26479, 734 for $r = 0, 1, 2, 3, 5, 7, 9, 15, 27$ (certificate 1.1.10e). Since $x \mapsto \log x\, f(\log x)/(x+1)$ is decreasing, we use the value at the left endpoint of each interval (sum $\Sigma_{\mathrm{cen}}$).

(iv) For $R < p < X$ we use $-5$. Partial summation with $\vartheta(x) < (1 + \frac{1}{36260})x$ from [Dus10, Section 1] and $\vartheta(R) > R(1 - \frac{1}{5\log^2 R})$ gives

$$\sum_{R<p<X} \frac{\log p}{p+1} f(\log p) \le \Big(1 + \frac{1}{36260}\Big)\int_{\log R}^{T} f(s)\,ds + \Big(\frac{1}{36260} + \frac{1}{5\log^2 R}\Big) f(\log R) =: \mathcal{T}_R,$$

so the contribution of this range is at least $-\frac{20}{27}\mathcal{T}_R$. Since $R$ is composite, no prime is lost at the endpoint.

Computing with 224-bit interval arithmetic (certificate 1.1.10f), we obtain

$$C_\infty - \int (1-f)W = -1.4201612735\ldots, \quad \Sigma_{\mathrm{pr}} = 1.5354743490\ldots, \quad \Sigma_{\mathrm{hi}} = -8.78\ldots\cdot 10^{-6},$$

$$\Sigma_{\mathrm{cen}} = -0.0590216892\ldots, \qquad -\tfrac{20}{27}\mathcal{T}_R = -0.0489055193\ldots,$$

and their sum $\mathcal{B}$ is a lower bound for the left-hand side, with

$$0.00737708655431125 < \mathcal{B} < 0.00737708655431126.$$

$\mathcal{B} > 0$ contradicts the inequality above. Hence $\mathrm{Sel} = \langle \kappa(A), \kappa(B) \rangle$. The 2-adic images of $\kappa(A), \kappa(B)$ are independent, so $\dim \mathrm{Sel} = 2$. Since $J(\mathbb{Q})[2] = 0$, $\operatorname{rank} J(\mathbb{Q}) \le 2$, and since $A, B$ are independent, the rank is 2. □

**Step 7: Chabauty–Coleman at $p = 3, 5$.** Set $(\omega_0, \omega_1, \omega_2) = (1, x, y)\,dx/(3y^2+1)$, and use $L(P) = \int_O^P (\omega_0, \omega_1, \omega_2)$ as the abelian logarithm. At $O$ this basis is $-(w, t, 1)H_w^{-1}dt$ ($H_w = 1 + 6tw^2 + 3w^2 - 4w^3$), with integral coefficients. The plane model is smooth at 3 and 5. Since $\#C(\mathbb{F}_{3^k}) = 4, 10, 28$ and $\#C(\mathbb{F}_{5^k}) = 3, 23, 120$ ($k = 1, 2, 3$), we have $\#J(\mathbb{F}_3) = 28$, $\#J(\mathbb{F}_5) = 64$ (certificate 1.1.10g). By [Kat81, Appendix], the order of the rational torsion divides $\gcd(28, 64) = 4$, and since $J(\mathbb{Q})[2] = 0$, $J(\mathbb{Q})$ is torsion-free. Since $\#J(\mathbb{F}_p)$ is prime to $p$, multiplying an element of $J(\mathbb{Q}_p)$ by $\#J(\mathbb{F}_p)$ puts it in the kernel of reduction, and by Lemma E its logarithm lies in $p\mathbb{Z}_p^3$. Hence $L(J(\mathbb{Q}_p)) \subset p\mathbb{Z}_p^3$.

For integers $n, m$ set $N = n + m + 5$, and let $h_{n,m} \in L(NO)$ be the primitive integral generator of the kernel (which is 1-dimensional) of the linear conditions $\mathrm{ord}_A \geq n + 2$, $\mathrm{ord}_B \geq m$. The basis is $x^i y^j$ ($j \leq 2$, $3i + 4j \leq N$), and then $\mathrm{div}(h_{n,m}) = (n+2)A + mB + E_{n,m} - NO$ with $\deg E_{n,m} = 3$ (certificate 1.1.10h).

**Lemma 3.10.9.** *Modulo 81, $L(A) \equiv (0, 78, 51)$ and $L(B) \equiv (78, 15, 66)$. $A, B$ are independent, and the index of $\langle A, B\rangle$ is prime to 3. If there is a new rational point $P \notin \{O, A, B\}$, then the 3-adic coordinates of $[P - O] = nA + mB$ satisfy $(n, m) \equiv (6, 3)$ or $(3, 4) \pmod 9$, and in the latter case $P \equiv (0, 2) \pmod 3$.*

*Proof.* For $(n, m) = (3, 1), (2, 10)$, $E_{n,m}$ has one point in each of the residue disks of $A, B, O$ (the constant term of the local expansion is divisible by 3 and the linear term is a unit). Let $\tau_{n,m}$ be the sum of the three tiny integrals. Then $6L(A) + 2L(B) = -\tau_{3,1}$, $5L(A) + 11L(B) = -\tau_{2,10}$, and modulo 81, $\tau_{3,1} \equiv (6, 69, 48)$, $\tau_{2,10} \equiv (33, 12, 72)$. For a parameter $u \in 3\mathbb{Z}_3$ the integral is $a_0 u + a_1 u^2/2 + a_2 u^3/3$ modulo 81, and the terms with $k \geq 4$ have valuation $k - v_3(k) \geq 4$. The determinant 56 is a unit, so $L(A), L(B)$ are as stated (certificate 1.1.10h). $L(A)/3, L(B)/3$ are independent modulo 3, so $A, B$ are independent. If $3x = nA + mB$ ($x \in J(\mathbb{Q})$), then $L(x) \in 3\mathbb{Z}_3^3$ gives $nL(A)/3 + mL(B)/3 \equiv 0 \pmod 3$, so $n \equiv m \equiv 0 \pmod 3$; since $J(\mathbb{Q})$ is torsion-free, the index is prime to 3. Normalizing the cross product gives the annihilating differential $\alpha_3 = (a + bx + y)\omega_0$ with $(a, b) \equiv (26, 17) \pmod{27}$ (since the rank is 2, it kills all of $J(\mathbb{Q})$).

Among the points of $C(\mathbb{F}_3) = \{O, (2, 1), (1, 2), (0, 2)\}$, $\alpha_3 \bmod 3 = (2 + 2x + y)\omega_0$ is nonzero at $O$, $A \equiv (2, 1)$ and $(0, 2)$, and is zero at $B \equiv (1, 2)$. The antiderivative of a differential with unit constant term is injective on $3\mathbb{Z}_3$, so the disks of $O$ and $A$ contain only the known points.

In the disk of $B$, write $u = x - 1$ and $\alpha_3 = (f_0 + f_1 u + f_2 u^2 + \cdots)du$; then $(f_0, f_1, f_2) \equiv (24, 14, 12) \pmod{27}$. With $u = 3v$, the antiderivative starting at $B$ is $u$ times an analytic function, and this analytic function divided by 3 is $8 + 7v + 3v^2$ modulo 9 and $2 + v$ modulo 3. Hence there is exactly one zero other than $B$, with $v \equiv 1 \pmod 9$, $L(P) \equiv (18, 0, 18) \pmod{27}$, $(n, m) \equiv (6, 3) \pmod 9$.

In the disk of $(0, 2)$ we use the base point $C_0 = (\xi, -1)$, where $\xi^3 + \xi^2 + \xi + 3 = 0$, $\xi \in 3\mathbb{Z}_3$ ($\xi \equiv 42 \pmod{81}$). The line $y = -1$ cuts out $B + C_0 + R_1 + R_2 - 4O$, and $R_1, R_2$, given by the roots of $u^2 + (3 + \xi)u + (3 + 2\xi + \xi^2)$ in $u = x - 1$, lie in the disk of $B$ (Eisenstein, valuation $1/2$). The power sums $s_k = u(R_1)^k + u(R_2)^k$ satisfy $v_3(s_k) \geq \lceil k/2 \rceil$, so the terms with $k \leq 6$ determine the trace modulo 27, and $L(C_0) = -3L(B) - \tau \equiv (0, 24, 9) \pmod{27}$. With $u = x - \xi = 3v$ we get $\alpha_3(L(P))/3 \equiv 4 + 7v \pmod 9$, so there is exactly one zero, with $v \equiv 2 \pmod 9$, $L(P) \equiv (15, 24, 12) \pmod{27}$, $(n, m) \equiv (3, 4) \pmod 9$ (certificate 1.1.10h). A new rational point is one of these two zeros. □

**Lemma 3.10.10.** *Modulo 125, $L(A) \equiv (80, 60, 120)$ and $L(B) \equiv (115, 120, 110)$, and the index of $\langle A, B\rangle$ is prime to 5. A new rational point $P$ reduces to $B$ modulo 5, and $(n, m) \equiv (3, 3) \pmod 5$. Therefore $(n, m) \equiv (33, 3)$ or $(3, 13) \pmod{45}$.*

*Proof.* On the tangent line at $A$, $8F(x, (x + 3)/2) = (x + 1)^2(8x^2 - 15x + 31)$. Let $Q, Q'$ be the two points with $x = (15 \pm \sqrt{-767})/16$, $y = (x + 3)/2$. Then $2L(A) + L(Q) + L(Q') = 0$, and the quadratic field is unramified at 5. For $(n, m) = (3, 13), (7, 9)$, $E_{n,m}$ has one point near each of $Q, Q', O$, so $3L(A) + 13L(B) = -\tau_{3,13}$, $7L(A) + 9L(B) = -\tau_{7,9}$, and modulo 125, $\tau_{3,13} \equiv (15, 10, 85)$, $\tau_{7,9} \equiv (30, 0, 45)$ (the integrals are taken up to $a_0 u + a_1 u^2/2$; the terms with $k \geq 3$ have valuation $k - v_5(k) \geq 3$). The determinant $-64$ is a unit, so we get the values above. The normalized logarithms are independent modulo 5, so the index is prime to 5, and the annihilating differential is $\alpha_5 = (a' + b'x + y)\omega_0$, $(a', b') \equiv (11, 0) \pmod{25}$ (certificate 1.1.10h).

We have $C(\mathbb{F}_5) = \{O, (4, 1), (1, 4)\}$. $\alpha_5$ is a unit at $O$ and $A$, so their disks contain only the known points. At $B$ the constant coefficient is 15 modulo 25 and the linear coefficient is 4 modulo 5. Setting $u = x - 1 = 5v$ and dividing the antiderivative by $25v$ gives $3 + 2v$ modulo 5 (the terms with $k \geq 3$ satisfy $k - 2 - v_5(k) \geq 1$). Hence there is one more zero, with $v \equiv 1 \pmod 5$, $L(P) \equiv (10, 15, 15) \pmod{25}$, $(n, m) \equiv (3, 3) \pmod 5$. Combining this with Lemma 3.10.9, $(6, 3) \bmod 9$ becomes $(33, 3) \bmod 45$, and $(3, 4) \bmod 9$ becomes $(3, 13) \bmod 45$. □

**Step 8: Mordell–Weil sieve.**

**Lemma 3.10.11.** $C(\mathbb{Q}) = \{O, A, B\}$.

*Proof.* Suppose there is a new rational point $P$. The reduction is good at 3, 5, 11, 13, and $\#J(\mathbb{F}_{11}) = 2520$, $\#J(\mathbb{F}_{13}) = 2912$ ($\#C(\mathbb{F}_{11^k}) = 18, 146, 1296$, $\#C(\mathbb{F}_{13^k}) = 16, 216, 2128$). Arithmetic in $J(\mathbb{F}_p)$ is done exactly by solving Riemann–Roch with the basis $x^i y^j$ ($j \le 2$, $3i + 4j \le m \le 9$) of $L(mO)$, and the equality of two classes is decided by whether the effective representative of their difference is empty (certificate 1.1.10g). Following [BS10], we show the following in order.

(1) In $J(\mathbb{F}_5)$, $\operatorname{ord} B = 64$ and $A = 17B$. The characters of order 2 obtained by multiplying by 32 at 5 and by 1260 at 11 give the rows $(1,1)$, $(0,1)$ on $(A, B)$, so $\langle A, B\rangle$ is saturated at 2. Together with Lemmas 3.10.9, 3.10.10, the index is prime to 2, 3, 5, and the coordinates $(n, m)$ are integral at these primes. Since $P \equiv B \pmod 5$, $17n + m \equiv 1 \pmod{64}$.

(2) At 11, multiplication by 56 leaves the $\{3, 5\}$-part, of order 45. Of the two candidates, only $(3, 13)$ mod 45 matches the image of one of the 18 points of $C(\mathbb{F}_{11})$, and that point is $(3, 4)$. Hence $P \equiv (0, 2) \pmod 3$ and $P \equiv (3, 4) \pmod{11}$. Multiplication by 7 leaves the $\{2, 3, 5\}$-part, of order 360. Among the 8 pairs modulo 360 satisfying $(3, 13)$ mod 45 and $17n + m \equiv 1 \pmod 8$, only $(228, 13)$ has the same image as $(3, 4)$. Hence $n \equiv 4$, $m \equiv 5 \pmod 8$.

(3) The 7-parts of $J(\mathbb{F}_3)$ and $J(\mathbb{F}_{11})$ have order 7. Projecting by multiplication by 4 and by 360, respectively, and normalizing the image of $A$ to 1, the images of $B$ are 4 and 3, and the images required for the point are 2 at $(0, 2)$ and 1 at $(3, 4)$. The determinant is $6 \not\equiv 0 \pmod 7$, so the group is saturated at 7 as well, and $n \equiv 5$, $m \equiv 1 \pmod 7$.

(4) In $J(\mathbb{F}_{13})$, multiplication by 13 leaves the $\{2, 7\}$-part, of order 224. Reducing the conditions above modulo 32 and 7, there are four pairs modulo 224: $(68, 29)$, $(12, 85)$, $(180, 141)$, $(124, 197)$. None of their images equals the image of any of the 16 points of $C(\mathbb{F}_{13})$ (including $O$).

This is a contradiction. □

*Proof of Theorem 3.10.1.* By Proposition 3.10.8, $\operatorname{rank} J(\mathbb{Q}) = 2$, and as shown in Step 7, $J(\mathbb{Q})$ is torsion-free. By Lemma 3.10.11, $C(\mathbb{Q}) = \{O, A, B\}$. Since $O$ is the only point at infinity, the only integer solutions are $A = (-1, 1)$ and $B = (1, -1)$. □

## 3.11 $x^4 + y^3 + xy - y - 1 = 0$ ($H = 31$)

**Theorem 3.11.1.** *The only integer solutions of* $x^4 + y^3 + xy - y - 1 = 0$ *are* $(x, y) = (-1, 0), (1, 0)$.

**Setup.** Setting $u = -x$, $v = y$, the equation becomes

$$C: \quad G(u, v) := u^4 + v^3 - (u + 1)v - 1 = 0.$$

The projective completion $u^4 + v^3 w - (u + w)vw^2 - w^4 = 0$ is a smooth plane quartic (genus 3), and its only bad primes are 2 and $q_0 = 13839869$ (certificate 1.1.11a). At the point at infinity $O = (0 : 1 : 0)$ the line $w = 0$ meets the curve with multiplicity 4, since $u^4 = 0$, so $O$ is a rational hyperflex. Near $O$ we use $t = u/v$, $w = 1/v$. In this chart the curve is

$$t^4 + w - tw^2 - w^3 - w^4 = 0,$$

and the partial derivative with respect to $w$ is 1 at the origin, so $w = -t^4 + t^9 - t^{12} + \cdots \in \mathbb{Z}[[t]]$. Hence $u$ and $v$ have poles of order 3 and 4 at $O$, respectively.

**Proposition 3.11.2.** $C(\mathbb{Q}) = \{O, P_+, P_-\}$, *where* $P_+ = (1, 0)$, $P_- = (-1, 0)$.

Since $(u,v) = (1,0), (-1,0)$ correspond to $(x,y) = (-1,0), (1,0)$, Theorem 3.11.1 follows directly from this proposition. Since $G(-1,v) = v^3$, we have $\operatorname{div}(u+1) = 3P_- - 3O$, and $[P_- - O]$ is a torsion element.

The proof has five steps. We fix the bitangent field $K$ (Step 1), show $\mathrm{Cl}(K)[2] = 0$ with Proposition B (Lemma 3.11.3), and show by 2-descent that the rank is at most 1 (Lemma 3.11.4). Next we compute the 3-adic logarithm of $[P_+ - O]$ from one principal divisor and show that the rank is exactly 1 (Lemma 3.11.6). We finish with Chabauty–Coleman at $p = 3$.

**Step 1: the bitangent field.** If the line $v = mu + b$ is a bitangent, then $u^4 + (mu+b)^3 - (u+1)(mu+b) - 1 = (u^2 + c_1 u + c_0)^2$ with $c_1^2 \neq 4c_0$. The slopes of the 27 bitangents other than the line at infinity are the roots of

$$\begin{aligned} f(m) = {} & m^{27} + 48m^{22} - 480m^{19} + 144m^{17} - 17280m^{15} + 2304m^{14} - 832m^{12} - 34560m^{11} \\ & + 64512m^{10} + 18944m^9 - 168448m^7 - 49152m^6 - 27648m^5 + 8192m^4 - 94208m^3 \\ & + 1024m^2 - 4096m + 4096. \end{aligned}$$

$f$ is irreducible, and $K = \mathbb{Q}[m]/(f)$ has degree 27, signature $(3,12)$ and absolute discriminant $D = 2^{28} \cdot 13839869^6$ (certificate 1.1.11a). There are four prime ideals above 2, with (ramification index, residue degree) equal to $(5,1), (10,1), (2,1), (5,2)$. We normalize the bitangent function as $h_m = mu + b - v$. Since $v = -t^{-4} + \cdots$ at $O$, the coefficient of $t^{-4}$ in $h_m$ is 1.

At $q_0$ the reduction has only one singular point, $(u,v) \equiv (950455, 6126477) \pmod{q_0}$. At the integral lift $(950455, 4 \cdot 950455^3)$ the value of $G$ has $q_0$-adic valuation 1, and the Hessian $288u^5 - 1$ is a $q_0$-adic unit. So this point is an ordinary node of thickness 1. If the quartic split into several components, then by Bézout's theorem the components would have to meet at least three times, and if there were a multiple component, the singular points would not be isolated. Hence this fiber is geometrically irreducible, the Tamagawa number is 1, and the descent image is unramified at $q_0$. Therefore $S = \{2\}$ suffices.

**Step 2: the class group.**

**Lemma 3.11.3.** $\mathrm{Cl}(K)[2] = 0$.

*Proof.* We apply Proposition B with $n = 27$, $(r_1, r_2) = (3,12)$, the $D$ above, and $T = \log(5 \cdot 10^8)$. The window is a step function with 64 cells of equal width, and its heights are 64 positive integers, symmetric left to right (input of certificate 1.1.11d). Two pieces of data are needed.

(i) There are 26,350,721 prime ideals of norm less than $5 \cdot 10^8$ in total, and we count the number $a(q)$ for every norm (certificate 1.1.11b).

(ii) All 664,374 prime ideals of norm at most $10^7$ have a witness for Lemma C (certificate 1.1.11c). Hence we set $k(q) = a(q)$ if $q \leq 10^7$, and $k(q) = 0$ otherwise.

With these data we get $B^- > 0.00490937703090692\ldots > 0$ (certificate 1.1.11d). The knot values of the autocorrelation are computed as exact rationals, and the archimedean term and the prime sum are computed with directed-rounding interval arithmetic. So rounding errors cannot change the conclusion. By Proposition B, $\mathrm{Cl}(K)[2] = 0$. □

**Step 3: upper bound for the rank.**

**Lemma 3.11.4.** $\operatorname{rank} J(\mathbb{Q}) \leq 1$.

*Proof.* The hypotheses of Proposition A (smooth quartic, rational hyperflex $O$, irreducible $f$ of degree 27) were checked above. Hence $J(\mathbb{Q})[2] = 0$, the map $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^\times/K^{\times 2}$ is injective, and its image has square norm and lies in $K(S,2)$, $S = \{2\}$. By Lemma 3.11.3,

$$\dim_{\mathbb{F}_2} K(S,2) = (r_1 + r_2) + \#\{\mathfrak{p} \mid 2\} = 15 + 4 = 19.$$

There are 19 explicit elements supported on $S$ that form a basis of this space. Their independence is checked by the parities of the valuations at the prime ideals above 2 and by quadratic characters at auxiliary primes (certificate 1.1.11e).

We impose conditions on this 19-dimensional space one after another. The condition that the norm be a square (sign and 2-adic valuation) cuts it down to 17 dimensions. Imposing the local conditions at the good primes 487, 491, 499, 503 in turn, the dimension becomes $10, 7, 5, 4$. At each prime we use all points of $C(\mathbb{F}_p)$, and since $p > 484$, the images of these points generate the whole local image (Proposition F(3)).

At 2 the situation is as follows. The decomposition group at 2 acts on the 27 bitangents with orbits of sizes $5, 10, 2, 10$ (the values $ef$ above). Under $J[2] \hookrightarrow \mathbb{F}_2^{27}$, an element of $J(\mathbb{Q}_2)[2]$ maps to a codeword that is a union of these orbits. Nonzero codewords have weight 12 or 16. The only unions of orbits of size 12 or 16 are the two obtained by joining the orbit of size 2 with one orbit of size 10, and their sum has weight 20, so it is not a codeword. Hence $\dim J(\mathbb{Q}_2)[2] \le 1$, and by Proposition F(1), $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \le 1 + 3 = 4$. On the other hand, the 2-adic images of the following four divisors are independent (certificate 1.1.11e).

(a) $P_+ - O$.

(b) $R_1 - O$. $R_1$ is the 2-adic point with $u = 5$, $v = 8s$, where $s$ is a root of $\frac{1-u^4}{16} + \frac{u+1}{2}s - 32s^3 = 0$. The derivative with respect to $s$ is odd, so by Hensel's lemma there is a unique such root in $\mathbb{Z}_2$.

(c) $R_2 - O$. $R_2$ is the point in the disk of $O$ with $t = 2$. In the equation of the chart the derivative with respect to $w$ is a unit, so $w \in 2\mathbb{Z}_2$ is uniquely determined.

(d) $R_3 + \bar{R}_3 - 2O$. $R_3$ is the point over $\mathbb{Q}_2(\sqrt{2})$ with $t = \sqrt{2}$, and $\bar{R}_3$ is its conjugate.

The coordinates of the points are approximated to precision $2^{60}$, and we check that the error of each image has valuation greater than $2e_{\mathfrak{p}}$ at each prime ideal $\mathfrak{p}$ above 2. So the square classes are determined exactly. Therefore the four images generate the whole 2-adic local image. The elements of the preceding 4-dimensional space that map into this local image form a 1-dimensional space. Since $\delta$ is injective and $J(\mathbb{Q})[2] = 0$, $\operatorname{rank} J(\mathbb{Q}) \le 1$. □

**Step 4: a principal divisor and the 3-adic logarithm.** 3 is a good prime. We take the integral basis of regular differentials

$$\boldsymbol{\omega} = (\omega_0, \omega_1, \omega_2) = (1, u, v)\frac{du}{u + 1 - 3v^2} = (1, u, v)\frac{dv}{4u^3 - v}.$$

In the chart at $O$,

$$\boldsymbol{\omega} = (w, t, 1)\frac{dt}{1 - 2tw - 3w^2 - 4w^3},$$

and the three components are series with integer coefficients:

$$\omega_0 = (-t^4 + 3t^9 + \cdots)\,dt, \quad \omega_1 = (t - 2t^6 + 3t^9 + \cdots)\,dt, \quad \omega_2 = (1 - 2t^5 + 3t^8 + \cdots)\,dt.$$

Since $C(\mathbb{F}_3) = \{O, (1,0), (2,0)\}$, there are three residue disks, and each contains one of the known rational points $O$, $P_+$, $P_-$.

**Lemma 3.11.5.** *There is a polynomial $h \in \mathbb{Q}[u, v]$ of degree at most 2 in $v$ such that*

$$\operatorname{div}(h) = 21P_+ + E - 24O.$$

*Here $E$ is an effective divisor of degree 3 defined over $\mathbb{Q}$, and the $u$-coordinates of its three points are the roots of an irreducible cubic polynomial $U$.*

*Proof.* $h$ is a linear combination of the 22 monomials $u^i v^j$ with $3i + 4j \le 24$, $j \le 2$, and its coefficients are in the input of certificate 1.1.11f. Weight 24 occurs only for $u^8$, so $h$ has a pole of order exactly 24 at $O$. An exact computation verifies

$$\operatorname{Res}_v(G, h) = c\,(u - 1)^{21}U(u) \quad (c \in \mathbb{Q}^\times), \qquad \gcd\big(G(1, v), h(1, v)\big) = v.$$

Since $G_v(P_+) = -2 \neq 0$, $u - 1$ is a local parameter at $P_+$. So $h$ vanishes to order exactly 21 at $P_+$ and does not vanish at the other points above $u = 1$. The remaining three zeros lie above the roots of $U$, and their $v$-coordinates are given by a quadratic polynomial in $u$ with rational coefficients. Substituting these, we check $G = h = 0$. The total order of the zeros, $21 + 3$, equals the order 24 of the pole, so there are no other zeros. □

**Lemma 3.11.6.** *Let $L = (L_0, L_1, L_2)$ be the 3-adic logarithm of $[P_+ - O]$ with respect to $\boldsymbol{\omega}$. Then $L \equiv (0, 3, 6) \pmod 9$. Hence* rank $J(\mathbb{Q}) = 1$.

*Proof.* The characteristic polynomial $T(Z)$ of $t = u/v$ on $E$ is

$$T(Z) \equiv Z^3 + 36Z^2 + 9Z + 60 \pmod{81}.$$

It is 3-Eisenstein, so all three points of $E$ have $v_3(t) = 1/3$. The coefficients of the characteristic polynomial of $v$ on $E$ have 3-adic valuations $(-4, -1, 0, 0)$, and its Newton polygon is a single segment, so $v_3(v) = -4/3$, that is, $v_3(w) = 4/3 > 0$ (certificate 1.1.11f). Therefore the points of $E$, defined over a totally ramified cubic extension of $\mathbb{Q}_3$, lie in the residue disk of $O$, on the branch $w = w(t)$. By Lemma 3.11.5, $21[P_+ - O] = -[E - 3O]$, so

$$L = -\frac{1}{21} \operatorname{Tr} \int_0^{t(E)} \boldsymbol{\omega}.$$

The right-hand side is the sum of the tiny integrals to the three points of $E$.

The integrals up to degree 9 are

$$I_0 = -\frac{t^5}{5}, \qquad I_1 = \frac{t^2}{2} - \frac{2t^7}{7}, \qquad I_2 = t - \frac{t^6}{3} + \frac{t^9}{3}.$$

For $n \geq 10$, the degree-$n$ term $a\,t^n/n$ ($a \in \mathbb{Z}$) of the integral has valuation at least $n/3 - v_3(n) \geq 3$ at $v_3(t) = 1/3$. For $10 \leq n \leq 26$ this is checked directly, and for $n \geq 27$, $v_3(n) \leq \log_3 n \leq n/3 - 3$. Hence the trace of all the discarded terms lies in $27\mathbb{Z}_3$. The power sums $p_k$ of the roots of $T$ are

$$(p_1, \ldots, p_9) \equiv (45, 63, 63, 54, 27, 27, 0, 0, 0) \pmod{81}.$$

Therefore

$$\operatorname{Tr}(I_0, I_1, I_2) = \left(-\tfrac{p_5}{5},\ \tfrac{p_2}{2} - \tfrac{2p_7}{7},\ p_1 - \tfrac{p_6}{3} + \tfrac{p_9}{3}\right) \equiv (0, 18, 9) \pmod{27},$$

and dividing by $-21$ gives $L \equiv (0, 3, 6) \pmod 9$. Since $L \neq 0$, $[P_+ - O]$ has infinite order, and together with Lemma 3.11.4 this gives rank $J(\mathbb{Q}) = 1$. □

**Step 5: Chabauty–Coleman at $p = 3$.** Since $L_1/3$ is a 3-adic unit,

$$\eta_0 = \omega_0 - \frac{L_0}{L_1}\omega_1, \qquad \eta_2 = \omega_2 - \frac{L_2}{L_1}\omega_1$$

are integral differentials that annihilate $L$. From $L \equiv (0, 3, 6) \pmod 9$ we get $L_0/L_1 \equiv 0$, $L_2/L_1 \equiv 2 \pmod 3$, so

$$\eta_0 \equiv \omega_0, \qquad \eta_2 \equiv \omega_1 + \omega_2 \pmod 3.$$

Since the rank is 1 and $[P_+ - O]$ has infinite order, every element of $J(\mathbb{Q})$, after multiplication by a suitable integer, becomes the sum of an integer multiple of $[P_+ - O]$ and a torsion element. Hence $\eta_0$ and $\eta_2$ annihilate the logarithms of all of $J(\mathbb{Q})$.

*Proof of Proposition 3.11.2.* For each disk we choose the center and a local parameter $s$ as follows.

- $P_+$: $s = u - 1$. Since $G_v(P_+) = -2$ is a unit, $v \in \mathbb{Z}_3[[s]]$, and at the center $\boldsymbol{\omega}/ds = (1, 1, 0)/2$. The constant coefficient $1/2$ of $\eta_0$ is a unit.

- $P_-$: $s = v$. Since $G_u(P_-) = -4$ is a unit, $u \in \mathbb{Z}_3[[s]]$, and at the center $\omega/ds = (1,-1,0)/(-4)$. The constant coefficient $-1/4$ of $\eta_0$ is a unit.
- $O$: $s = t$. At the center $\omega/ds = (0,0,1)$, and the constant coefficient 1 of $\eta_2$ is a unit.

In all three cases the coefficients of the differentials lie in $\mathbb{Z}_3$, and the rational points of the disk correspond to $s \in 3\mathbb{Z}_3$. Let $\eta = \sum_{k\geq 0} c_k s^k\, ds$ ($c_0 \in \mathbb{Z}_3^\times$) be the chosen differential. Integrating from the center gives

$$I(3z) = \sum_{n\geq 1} \frac{c_{n-1}}{n}(3z)^n = 3z\Big(c_0 + \sum_{n\geq 2} \frac{c_{n-1}3^{n-1}}{n} z^{n-1}\Big).$$

For $n \geq 2$ we have $n - 1 - v_3(n) \geq 1$, so the expression in parentheses is a unit for every $z \in \mathbb{Z}_3$. So the only solution of $I(3z) = 0$ is $z = 0$. For a rational point $R$ in the disk, $[R - \text{center}] \in J(\mathbb{Q})$, so $I(s(R)) = 0$ by [Col85, MP12]. Hence the only rational point in each disk is its center. $C$ has good reduction at 3, so every rational point lies in one of the three disks. Therefore $C(\mathbb{Q}) = \{O, P_+, P_-\}$. □

## 3.12 $x^4 - y^3 + xy + x - 1 = 0$ ($H = 31$)

**Theorem 3.12.1.** *The only integer solution of $x^4 - y^3 + xy + x - 1 = 0$ is $(x, y) = (0, -1)$.*

**Setup.** Setting $u = -x$, $v = y$, the equation becomes

$$C: \quad G(u,v) := u^4 - v^3 - uv - u - 1 = 0.$$

The projective completion $u^4 - v^3w - uvw^2 - uw^3 - w^4 = 0$ is a smooth plane quartic (genus 3). The bad primes are $3, 5, 313, 14087$, and the curve has good reduction at 2 (certificate 1.1.12a). At the point at infinity $O = (0:1:0)$ the line $w = 0$ meets the curve with multiplicity 4, since $u^4 = 0$, so $O$ is a rational hyperflex. The parameter near $O$ is $t = u/v$, and $v = t^{-4} + \cdots$. At the point $P = (0,-1)$ we also have $G(u,-1) = u^4$, so the line $v = -1$ meets $C$ with multiplicity 4. Hence

$$\operatorname{div}(v+1) = 4P - 4O.$$

Since $G_v(P) = -3 \neq 0$, $u$ is a local parameter near $P$, and $v + 1 = u^4/3 - u^5/9 + \cdots$.

**Proposition 3.12.2.** *$J(\mathbb{Q}) = \langle [P - O] \rangle \cong \mathbb{Z}/4\mathbb{Z}$ and $C(\mathbb{Q}) = \{O, P\}$.*

Since $P = (0,-1)$ corresponds to $(x,y) = (0,-1)$, Theorem 3.12.1 follows from this proposition.

The proof has four steps. We determine the bitangent algebra and the Galois structure of $J[2]$ (Step 1), show that the class groups of two fields have no 2-torsion (Step 2), show by descent that the rank is 0 (Step 3), and then determine the torsion subgroup and the rational points (Step 4).

**Step 1: the bitangent algebra and $J[2]$.** If the line $v = mu + b$ is a bitangent, then $u^4 - (mu+b)^3 - u(mu+b) - u - 1$ is the square of a quadratic polynomial. The slopes of the 27 bitangents other than the line at infinity are $m = 0$ ($b = -1$, that is, the tangent line $v = -1$ at $P$) and the roots of

$$\begin{aligned} f_{10}(m) &= m^{10} - 24m^6 - 48m^2 - 16, \\ f_{16}(m) &= m^{16} + 24m^{12} + 48m^{11} + 624m^8 - 192m^7 + 160m^6 \\ &\quad - 1152m^4 - 2304m^3 + 960m^2 - 64m + 2304. \end{aligned}$$

Both polynomials are irreducible. Hence the bitangent algebra is $\mathcal{L} = \mathbb{Q} \times F_{10} \times F_{16}$, $F_d = \mathbb{Q}[m]/(f_d)$ (certificate 1.1.12a), and

$$F_{10}:\ (r_1,r_2) = (2,4),\ |D| = 2^8(5\cdot 313\cdot 14087)^2; \qquad F_{16}:\ (r_1,r_2) = (0,8),\ |D| = 2^{12}(5\cdot 313\cdot 14087)^4.$$

We take the bitangent function $h_m = v - mu - b$. Its coefficient of $t^{-4}$ at $O$ is 1.

We use the framework of Proposition G. $V = J[2]$ carries the quadratic form determined by $2O$, and in a suitable basis $V = \mathbb{F}_2^6$ and

$$q(z) = z_1z_2 + z_3z_4 + z_5z_6 + z_5 + z_6, \qquad B(a,b) = q(a+b) - q(a) - q(b).$$

The 27 bitangents other than the line at infinity correspond to the 27 nonzero isotropic vectors of $q$. The map $a \mapsto (B(a,w))_w$ is a Galois-equivariant injection $V \hookrightarrow E = \mathbb{F}_2^{27}$, and nonzero images have weight 12 or 16. Let $H$ be the subgroup of the orthogonal group fixing the vector $v_0$ corresponding to the rational bitangent $v = -1$. Then the Galois image $G$ is contained in $H$.

**Lemma 3.12.3.** *$G = H$ and $|H| = 1920$.*

*Proof.* First we do the following finite computation (certificate 1.1.12b). The transvections $z \mapsto z + B(z,a)a$ for $a$ with $q(a) = 1$, $B(a,v_0) = 0$ generate a group of order 1920, and this group has orbits of sizes $1, 10, 16$ on the 27 isotropic vectors. This group is all of $H$. Indeed, there are 16 isotropic vectors that form a hyperbolic pair with $v_0$, and the elements fixing one such pair act faithfully as permutations of the five nonzero isotropic vectors of the 4-dimensional orthogonal complement, so $|H| \le 16 \cdot 120$. The orbit of size 10 splits into five pairs $\{w, w+v_0\}$. The action $H \to S_5$ on these pairs is surjective, and its kernel $N$ is an elementary abelian group of order 16. The $H$-normal closure of every nonzero element of $N$ is $N$.

The orbits of $G$ are $\{v_0\}$, the 10 roots of $f_{10}$, and the 16 roots of $f_{16}$. The image $\bar{G}$ of $G$ in $S_5$ is transitive on the five pairs, so its order is a multiple of 5. 13 splits in $F_{10}$ with residue degrees $(1,1,2,6)$, so the Frobenius at 13 has order divisible by 3; since $N$ is a 2-group, the order of $\bar{G}$ is also divisible by 3. 3 splits in $F_{10}$, $F_{16}$ with residue degrees $(1,1,4,4)$, $(1,1,2,4,4,4)$, and every element of $H$ with this cycle type maps to a 4-cycle in $S_5$. Hence the order of $\bar{G}$ is a multiple of 60 and $\bar{G}$ contains an odd permutation, so $\bar{G} = S_5$. Since $N$ is abelian, the conjugation action on $N$ factors through $H/N \cong S_5$, and since $G \to S_5$ is surjective, $G \cap N$ is $H$-invariant. Hence $G \cap N$ is 0 or $N$. If it were 0, then $|G| = 120$; but there is an orbit of size 16, so $16 \mid |G|$, a contradiction. Therefore $N \subset G$ and $G = H$. □

**Lemma 3.12.4.** *$\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = 1$, and $H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, E)$ is injective. Hence $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathcal{L}^\times/\mathcal{L}^{\times 2}$ is injective.*

*Proof.* A finite computation gives $\dim V^H = 1$, $\dim E^H = 3$, $\dim(E/V)^H = 2$ (certificate 1.1.12b). So $E^H \to (E/V)^H$ is surjective. In the cohomology exact sequence of $0 \to V \to E \to E/V \to 0$, the kernel of $H^1(\mathbb{Q}, V) \to H^1(\mathbb{Q}, E)$ is the quotient of $(E/V)^G$ by the image of $E^G$, and by Lemma 3.12.3 this quotient is 0. Moreover, $J(\mathbb{Q})[2] = V^G = V^H$ is 1-dimensional. $\delta$ is the composition of the Kummer map with this map. □

At the bad primes 5, 313, 14087 the reduction has a single singular point, an ordinary node of thickness 1, and the fiber is geometrically irreducible (certificate 1.1.12a). So the Tamagawa number is 1, and the descent image is unramified at these primes. At 3 we do not use this criterion. Hence $S = \{2, 3\}$.

**Step 2: class groups.**

**Lemma 3.12.5.** *$\mathrm{Cl}(F_{10})[2] = \mathrm{Cl}(F_{16})[2] = 0$.*

*Proof.* We apply Proposition B to both fields. The window is a step function with a single cell, and its autocorrelation is the triangle $f(x) = (1 - |x|/T)_+$. In this case the archimedean term of Proposition B has the closed form

$$C_\infty - \frac{\pi^2}{4T} - \frac{2\alpha \log 2}{T} + \frac{2}{T} \sum_{j \text{ odd}} \frac{e^{-jT}}{j^2} + \frac{2\alpha}{T} \log(1 + e^{-T}).$$

For $F_{10}$ we take $n = 10$, $\alpha = 1/5$, $T = 6$. There are 94 prime ideals of norm less than $e^6$ (the largest norm is 401), and we verify exactly, with witnesses for Lemma C, that all of them are principal. So $k = a$, and $B^- > 0.0809177 > 0$ (certificate 1.1.12c).

For $F_{16}$ we take $n = 16$, $\alpha = 0$, $T = 16$. There are 596,471 prime ideals of norm at most $8.9 \cdot 10^6$ ($> e^{16}$) in total, and we count the number $a(q)$ for every norm (certificate 1.1.12d). For all 18,074 prime ideals of norm at most $2 \cdot 10^5$ we verify exactly, with witnesses for Lemma C, that they are principal (certificate 1.1.12e). Setting $k(q) = a(q)$ for $q \le 2 \cdot 10^5$ and $k(q) = 0$ otherwise, we get $B^- > 0.0745721 > 0$ (certificate 1.1.12e).

Both computations are done with 60-digit precision, and the margin is at least 0.07, so rounding errors do not affect the conclusion. By Proposition B, neither class group has 2-torsion. □

**Step 3: rank 0.**

**Lemma 3.12.6.** rank $J(\mathbb{Q}) = 0$.

*Proof.* By Lemma 3.12.4, $\delta$ is injective, and its image has square norm and lies in $\mathcal{L}(S,2) = \mathbb{Q}(S,2) \times F_{10}(S,2) \times F_{16}(S,2)$ (Proposition G). We have $\mathbb{Q}(S,2) = \langle -1, 2, 3\rangle$. There are $2+4$ prime ideals above 2 and 3 in $F_{10}$, and $3+6$ in $F_{16}$. By Lemma 3.12.5,

$$\dim F_{10}(S,2) = (2+4)+6 = 12, \qquad \dim F_{16}(S,2) = (0+8)+9 = 17,$$

and the whole space has dimension $3+12+17 = 32$. That explicit elements supported on $S$ form a basis of each space is checked by the rank of their valuation parities and quadratic characters (certificate 1.1.12f).

We impose conditions one after another. The condition that the norm be a square (sign, 2-adic valuation, 3-adic valuation) gives 29 dimensions. Imposing the local conditions at the good primes $487, 491, 499, 503, 509, 521, 523, 541$, the dimension becomes $26, 19, 17, 12, 12, 11, 9, 8$ in turn. At each prime we use all points of $C(\mathbb{F}_p)$, so this is the condition given by the whole local image (Proposition F(3)).

At 2 the extension is tame, and the orbit sizes on the bitangents in the $\mathbb{Q}$, $F_{10}$, $F_{16}$ components are $(1)$, $(5,5)$, $(1,5,10)$. The inertia group is cyclic of order 5, and Frobenius sends a generator of inertia to its square. Every subgroup of $H$ satisfying this condition and having these orbit sizes has order 20 and a 2-dimensional fixed space in $V$ (certificate 1.1.12b). Hence $\dim J(\mathbb{Q}_2)[2] = 2$, and by Proposition F(1), $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 2+3 = 5$. On the other hand, the following images are independent: those of the divisors obtained by subtracting $O$ from the point with $u = 0$ ($= P$), from the 2-adic points with $u = 2$ and $u = 4$, and from the point with $t = 2$ in the disk of $O$; and that of the divisor obtained by subtracting $2O$ from the sum of the point with $u = \sqrt{2}$ over $\mathbb{Q}_2(\sqrt{2})$ and its conjugate. The coordinates of the points are determined by Hensel's lemma, and we check that the error of each image has valuation greater than $2e_{\mathfrak{p}}$ at each prime ideal $\mathfrak{p}$ above 2. Therefore these five images generate the whole 2-adic local image.

At 3, $\mathcal{L}$ is unramified, so inertia at 3 acts trivially on $E$, and hence on $V$. The Frobenius at 3 has the cycle type above, and its fixed space in $V$ is 3-dimensional (certificate 1.1.12b). So $\dim J(\mathbb{Q}_3)/2J(\mathbb{Q}_3) = \dim J(\mathbb{Q}_3)[2] = 3$. The three images of the 3-adic points with $u = 0$ ($= P$), $u = 1$, $u = 3$ are independent, so they generate the whole 3-adic local image.

The elements of the preceding 8-dimensional space that map into both local images form a 1-dimensional space (certificate 1.1.12f). Since $\delta$ is injective, $\operatorname{rank} J(\mathbb{Q}) + \dim J(\mathbb{Q})[2] \le 1$, and since $\dim J(\mathbb{Q})[2] = 1$, the rank is 0. □

**Step 4: torsion and rational points.**

*Proof of Proposition 3.12.2.* By Lemma 3.12.6, $J(\mathbb{Q})$ is a finite group. The numbers of points of $C$ over $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ are $2, 4, 8$ (certificate 1.1.12g). Hence the numerator of the congruence zeta function is $1 - T - 4T^5 + 8T^6$, and $\#J(\mathbb{F}_2) = 1 - 1 - 4 + 8 = 4$. Since 2 is a good prime, by [Kat81, Appendix] the

odd-order torsion of $J(\mathbb{Q})$ injects into $J(\mathbb{F}_2)$. Hence $J(\mathbb{Q})$ is a 2-group. Since $J(\mathbb{Q})[2]$ is 1-dimensional, $J(\mathbb{Q})$ is cyclic.

Since $\operatorname{div}(v+1) = 4P - 4O$, we have $4[P-O] = 0$. If $2[P-O] = 0$, then $2P \sim 2O$, which contradicts [Har77, Section IV.5] since $P \neq O$. So $[P-O]$ has order 4. Moreover, $[P-O] \notin 2J(\mathbb{Q})$. Indeed, the $\mathbb{Q}$-component of $\delta([P-O])$ is computed with the rational bitangent function $h_0 = v+1$. Since $h_0$ has a zero of order 4 at $P$, its value at $P$ is taken to be the first coefficient $1/3$ with respect to the parameter $u$, and its normalized value at $O$ is 1. So this component is the square class of 3, which is not a square. If $J(\mathbb{Q})$ were cyclic of order at least 8, every element of order 4 would lie in $2J(\mathbb{Q})$; hence $J(\mathbb{Q}) = \langle [P-O] \rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Now let $R \in C(\mathbb{Q})$. Since the genus is positive, $R \mapsto [R-O]$ is injective, and $[R-O] = j[P-O]$ with $0 \leq j \leq 3$. If $j = 0, 1$, then $R = O, P$. If $j = 2$, then $R + O \sim 2P$, and if $j = 3$, then $R + P \sim 2O$. Since $O \neq P$, in either case two distinct effective divisors of degree 2 are linearly equivalent, which contradicts [Har77, Section IV.5]. Therefore $C(\mathbb{Q}) = \{O, P\}$. □

## 3.13 $x^4 + y^3 + xy + y - 1 = 0$ ($H = 31$)

**Theorem 3.13.1.** *The only integer solutions of* $x^4 + y^3 + xy + y - 1 = 0$ *are* $(x, y) = (-1, 0), (1, 0), (3, -4)$.

**Setup.** Setting $v = -y$, the equation becomes

$$C: \quad G(x, v) := x^4 - v^3 - (x+1)v - 1 = 0.$$

The projective completion $x^4 - v^3 w - (x+w)vw^2 - w^4 = 0$ is a smooth plane quartic (genus 3), and the bad primes are $2, 13, 17, 43, 257$ (certificate 1.1.13a). At the point at infinity $O = (0:1:0)$ the line $w = 0$ meets the curve with multiplicity 4, since $x^4 = 0$, so $O$ is a rational hyperflex. Near $O$ we use $t = x/v$, $w = 1/v$. In this chart the curve is

$$t^4 - w - tw^2 - w^3 - w^4 = 0,$$

and $w = t^4 - t^9 - \cdots \in \mathbb{Z}[[t]]$. Hence $x$ and $v$ have poles of order 3 and 4 at $O$, respectively. The known rational points are $O$ and

$$P_- = (-1, 0), \qquad P_1 = (1, 0), \qquad P_3 = (3, 4).$$

Since $G(-1, v) = -v^3$ and $G(x, 2x-2) = ((x-1)(x-3))^2$,

$$\operatorname{div}(x+1) = 3P_- - 3O, \qquad \operatorname{div}(v - 2x + 2) = 2P_1 + 2P_3 - 4O.$$

So $[P_- - O]$ is an element of order 3 and $[P_1 + P_3 - 2O]$ is an element of order 2. That both are nonzero follows from [Har77, Section IV.5].

**Proposition 3.13.2.** $C(\mathbb{Q}) = \{O, P_-, P_1, P_3\}$.

Since $(x, v) = (-1, 0), (1, 0), (3, 4)$ correspond to $(x, y) = (-1, 0), (1, 0), (3, -4)$, Theorem 3.13.1 follows directly from this proposition.

The proof has five steps: the bitangent algebra and the Galois structure of $J[2]$ (Step 1), the class groups of two fields (Step 2), the upper bound 1 for the rank (Step 3), the 3-adic logarithm computed from three principal divisors (Step 4), and the six residue disks at $p = 3$ (Step 5).

**Step 1: the bitangent algebra and $J[2]$.** If the line $v = mx + b$ is a bitangent, then $x^4 - (mx+b)^3 - (x+1)(mx+b) - 1$ is the square of a quadratic polynomial. The slopes of the 27 bitangents other than the line at infinity are $m = 2$ ($b = -2$, that is, the line $v = 2x - 2$ tangent at $P_1$ and $P_3$) and the roots of

$$\begin{aligned} f_{10}(m) &= m^{10} + 10m^9 + 48m^8 + 144m^7 + 288m^6 + 384m^5 + 344m^4 + 224m^3 + 96m^2 - 16, \\ f_{16}(m) &= m^{16} - 8m^{15} + 36m^{14} - 112m^{13} + 272m^{12} - 528m^{11} + 872m^{10} - 1264m^9 + 1920m^8 \\ &\quad - 3008m^7 + 4256m^6 - 4896m^5 + 4224m^4 - 2560m^3 + 768m^2 - 64m + 128. \end{aligned}$$

Both polynomials are irreducible. Hence the bitangent algebra is $\mathcal{L} = \mathbb{Q} \times K_{10} \times K_{16}$, $K_d = \mathbb{Q}[m]/(f_d)$ (certificate 1.1.13a), and

$$K_{10}:\ (r_1, r_2) = (2, 4),\ |D| = 2^8 \cdot 17^2 \cdot 43^2 \cdot 257^2; \qquad K_{16}:\ (r_1, r_2) = (0, 8),\ |D| = 2^{12} \cdot 17^4 \cdot 43^4 \cdot 257^4.$$

We take the bitangent function $h_m = v - mx - b$. Its coefficient of $t^{-4}$ at $O$ is 1.

As in Section 3.12, we use the framework of Proposition G. $V = J[2] = \mathbb{F}_2^6$, the quadratic form $q(z) = z_1z_2 + z_3z_4 + z_5z_6 + z_5 + z_6$, the correspondence between isotropic vectors and bitangents, the injection $V \hookrightarrow E = \mathbb{F}_2^{27}$, and the stabilizer $H$ of the vector $v_0$ of the rational bitangent ($|H| = 1920$, with $N$ the kernel of $H \to S_5$) are as in the proof of Lemma 3.12.3.

**Lemma 3.13.3.** *The Galois image $G$ equals $H$. Hence* $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = 1$ *($J(\mathbb{Q})[2]$ is generated by $[P_1 + P_3 - 2O]$), and $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathcal{L}^\times/\mathcal{L}^{\times 2}$ is injective.*

*Proof.* Let $\bar{G} \subset S_5$ be the image of $G$. Since $f_{10}$ is irreducible, $\bar{G}$ is transitive on the five pairs, and its order is a multiple of 5. 3 splits in $K_{10}$, $K_{16}$ with residue degrees $(2, 8)$, $(8, 8)$, and every element of $H$ with this cycle type maps to a 4-cycle in $S_5$. 5 splits with residue degrees $(4, 6)$, $(4, 12)$, and every element of $H$ with this cycle type maps to an element of cycle type $(2, 3)$ (certificate 1.1.13b). Hence the order of $\bar{G}$ is a multiple of 60 and $\bar{G}$ contains an odd permutation, so $\bar{G} = S_5$. As in the proof of Lemma 3.12.3, $G \cap N$ is 0 or $N$, and 0 contradicts the orbit of size 16. Therefore $G = H$. The rest is as in the proof of Lemma 3.12.4: since $\dim V^H = 1$, $\dim E^H = 3$, $\dim(E/V)^H = 2$, the group $J(\mathbb{Q})[2]$ is 1-dimensional and $H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, E)$ is injective. □

At the bad primes $17, 43, 257$ the reduction has a single singular point, an ordinary node of thickness 1, and the fiber is geometrically irreducible. So the Tamagawa number is 1, and the descent image is unramified at these primes. At 13 the node has thickness 2, so we keep 13 (certificate 1.1.13a). Hence $S = \{2, 13\}$.

**Step 2: class groups.**

**Lemma 3.13.4.** $\mathrm{Cl}(K_{10})[2] = \mathrm{Cl}(K_{16})[2] = 0$.

*Proof.* As in the proof of Lemma 3.12.5, we apply Proposition B with the triangular window $f(x) = (1 - |x|/T)_+$. For $K_{10}$ we take $T = 5$, and we verify exactly, with witnesses for Lemma C, that all 32 prime ideals of norm less than $e^5$ (the largest norm is 131) are principal. For $K_{16}$ we take $T = 8$, and the same holds for all 465 prime ideals of norm less than $e^8$ (the largest norm is 2957). In both cases $k = a$, and

$$B^-(K_{10}) > 0.3436681640333619, \qquad B^-(K_{16}) > 0.0228202034642712$$

(certificate 1.1.13c). The conclusion follows from Proposition B. □

**Step 3: upper bound for the rank.**

**Lemma 3.13.5.** $\operatorname{rank} J(\mathbb{Q}) \le 1$.

*Proof.* By Lemma 3.13.3, $\delta$ is injective, and its image has square norm and lies in $\mathcal{L}(S, 2)$ (Proposition G). We have $\mathbb{Q}(S, 2) = \langle -1, 2, 13 \rangle$. There are $2 + 2$ prime ideals above 2 and 13 in $K_{10}$, and $3 + 4$ in $K_{16}$. By Lemma 3.13.4,

$$\dim K_{10}(S, 2) = (2 + 4) + 4 = 10, \qquad \dim K_{16}(S, 2) = (0 + 8) + 7 = 15,$$

and the whole space has dimension $3 + 10 + 15 = 28$. The explicit bases are checked by valuation parities and quadratic characters (certificate 1.1.13d). The condition that the norm be a square (sign, 2-adic and 13-adic valuations) gives 25 dimensions, and imposing the local conditions given by the images of all points of $C(\mathbb{F}_p)$ at the good primes

$$487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593$$

gives 7 dimensions (Proposition F(3)).

At 2 the extension is tame, and the orbit sizes on the bitangents in the $\mathbb{Q}$, $K_{10}$, $K_{16}$ components are $(1)$, $(5,5)$, $(5,1,10)$. By the same computation as in the proof of Lemma 3.12.6, the decomposition group has order 20 and $\dim J(\mathbb{Q}_2)[2] = 2$ (certificate 1.1.13b). Hence $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 5$ (Proposition F(1)). The 2-adic images of the following five divisors are independent (certificate 1.1.13d).

(a) $P_1 - O$. Since $P_1$ lies on the rational bitangent $v = 2x - 2$, its component is computed, using the identity
$$(v - 2x + 2)\big((v + x - 1)^2 + 3x^2 - 5x + 4\big) = ((x-1)(x-3))^2$$
on $C$, as the value of $1/\big((v + x - 1)^2 + 3x^2 - 5x + 4\big)$.

(b) The divisor obtained by subtracting $O$ from the 2-adic point with $x = -3$.

(c) The divisor obtained by subtracting $O$ from the point with $t = 2$ in the disk of $O$.

(d) $D_1 - 2O$, for a divisor $D_1$ of degree 2 on the line $v = -5x - 7$.

(e) $D_2 - 2O$, for a divisor $D_2$ of degree 2 on the line $v = -5x - 5$.

In (d), (e), write the line as $v = kx + b_0$. Then $G(x, kx + b_0)$ splits in $\mathbb{Z}_2[x]$ as a product of two monic quadratic polynomials with odd resultant (we apply Hensel's lemma to the factorization modulo $2^{50}$). $D_i$ is the effective divisor of degree 2 over $\mathbb{Q}_2$ determined by one of these quadratics. We check that the approximation error has valuation greater than $2e_{\mathfrak{p}}$ at each prime ideal $\mathfrak{p}$ above 2, so the square classes are determined exactly. Therefore the five images generate the whole 2-adic local image. The elements of the preceding 7-dimensional space that map into this local image form a 2-dimensional space. Since $\delta$ is injective and $\dim J(\mathbb{Q})[2] = 1$, $\operatorname{rank} J(\mathbb{Q}) \le 2 - 1 = 1$. □

**Step 4: principal divisors and the 3-adic logarithm.** 3 is a good prime. We take the integral basis of regular differentials
$$\boldsymbol{\omega} = (\omega_0, \omega_1, \omega_2) = (1, x, v)\frac{dx}{3v^2 + x + 1} = (1, x, v)\frac{dv}{4x^3 - v}.$$
In the chart at $O$, $\boldsymbol{\omega} = -(w, t, 1)\, dt/(1 + 2tw + 3w^2 + 4w^3)$. Modulo 3, $C(\mathbb{F}_3)$ consists of the six points
$$O, \quad (2,0), \quad (1,0), \quad (0,1), \quad (1,1), \quad (1,2).$$
Above the first four lie the rational points $O, P_-, P_1, P_3$. Above the last two lie the $\mathbb{Q}_3$-points $Q_\pm = (1, \alpha_\pm)$, where $\alpha_\pm^2 = -2$, $\alpha_+ \equiv 1$, $\alpha_- \equiv 2 \pmod 3$; since $G(1, v) = -v(v^2 + 2)$, $Q_\pm$ are points over $\mathbb{Q}(\sqrt{-2})$.

**Lemma 3.13.6.** *There are $h_1 \in \mathbb{Q}[x, v]$ and $h_\pm \in \mathbb{Q}(\sqrt{-2})[x, v]$ such that*
$$\begin{aligned}
\operatorname{div}(h_1) &= 22P_1 + E_1 - 25O,\\
\operatorname{div}(h_+) &= P_- + 18P_1 + Q_+ + E_+ - 23O,\\
\operatorname{div}(h_-) &= 2P_- + 5P_1 + Q_- + E_- - 11O.
\end{aligned}$$
*Here $E_1, E_\pm$ are effective divisors of degree 3.*

*Proof.* The three functions are computed by certificate 1.1.13e directly, as the kernel of the vanishing conditions (the kernel is one-dimensional, so they are unique up to a constant). In each function there is only one monomial of largest weight ($x$ has weight 3, $v$ has weight 4), so the pole orders are exactly 25, 23, 11. We check the orders of the zeros by Taylor expansion at $P_-$ and $P_1$, and check by substitution that $h_\pm$ vanishes at $Q_\pm$ and not at its conjugate. The norm to the $x$-line is the product of the known factors and one irreducible cubic, and this cubic does not vanish at the known $x$-coordinates. The remaining three points are given by a cubic for the $v$-coordinate and by an expression of $x$ as a polynomial in $v$; substituting them, we check $G = h = 0$. The sum of the orders of the zeros equals the order of the pole, so there are no other zeros. □

**Lemma 3.13.7.** *Let $L = \log[P_1 - O]$. The 3-adic logarithms with respect to $\boldsymbol{\omega}$ are as follows modulo 27.*

| | $\omega_0$ | $\omega_1$ | $\omega_2$ |
|---|---|---|---|
| $L$ | 24 | 15 | 15 |
| $\log(Q_+ - O)$ | 12 | 9 | 12 |
| $\log(Q_- - O)$ | 18 | 3 | 0 |

*In particular, $v_3(L_0) = 1$, so* $\operatorname{rank} J(\mathbb{Q}) = 1$.

*Proof.* $[P_- - O]$ is a torsion element, so its logarithm is 0. From Lemma 3.13.6,

$$\begin{aligned} L &= -\frac{\log(E_1 - 3O)}{22}, \\ \log(Q_+ - O) &= -\log(E_+ - 3O) - 18L, \\ \log(Q_- - O) &= -\log(E_- - 3O) - 5L. \end{aligned}$$

Here 22 is a 3-adic unit.

The points of $E_1$ and $E_+$ are defined over the unramified cubic extension of $\mathbb{Q}_3$, and their $x$-coordinates are 1 and 0 modulo 3, respectively. Over $\mathbb{F}_3$ the fibers $x = 1$ and $x = 0$ consist of three distinct points, and $\operatorname{div}(x - c) = (\text{fiber } x = c) - 3O$. So, pairing each point $e$ of $E$ with the point $e'$ of the fiber in the same residue disk, we get $\log(E - 3O) = \sum_e \int_{e'}^{e} \boldsymbol{\omega}$. On these disks $3v^2 + x + 1$ is a unit, so $x - c$ is a parameter. Writing $\boldsymbol{\omega}(x_e + s) = \sum_{n\geq 0} a_n s^n \, ds$ ($a_n$ integral) and setting $\delta = x_e - c \in 3\mathcal{O}$, we have

$$\int_{e'}^{e} \boldsymbol{\omega} = \sum_{n\geq 0} \frac{(-1)^n a_n \delta^{n+1}}{n+1}.$$

The terms with $n + 1 \geq 6$ have valuation at least $(n + 1) - v_3(n + 1) \geq 5$. So if we compute the terms with $n + 1 \leq 5$ exactly in the cubic field and take the trace, the result is exact modulo 81.

The cubic satisfied by the $v$-coordinates of $E_-$ is 3-Eisenstein, so all three points have $v_3(v) = 1/3$, and $x$ reduces to $-1$. So $E_-$ lies in the disk of $P_-$. Since $3P_- \sim 3O$, we have $\log(E_- - 3O) = \operatorname{Tr} \int_{P_-}^{e} \boldsymbol{\omega}$, and with respect to the parameter $v$ the denominator of $\boldsymbol{\omega} = (1, x, v)\, dv/(4x^3 - v)$ is a unit. We use 18 terms of the integral; the remaining terms, of degree $n \geq 19$, have valuation at least $n/3 - v_3(n) \geq 6$.

The values obtained in this way are, modulo 81,

$$\log(E_1 - 3O) \equiv (39, 48, 21), \quad \log(E_+ - 3O) \equiv (69, 72, 69), \quad \log(E_- - 3O) \equiv (51, 57, 33)$$

(certificate 1.1.13f). Substituting them into the relations above gives the table. Since $L_0 \equiv 24 \pmod{27}$, $L \neq 0$, and together with Lemma 3.13.5 this gives $\operatorname{rank} J(\mathbb{Q}) = 1$. □

**Step 5: Chabauty–Coleman at $p = 3$.** Since $v_3(L_0) = 1 \leq v_3(L_1), v_3(L_2)$,

$$A = \left(-\frac{L_1}{L_0}, 1, 0\right), \qquad B = \left(-\frac{L_2}{L_0}, 0, 1\right)$$

are integral vectors that annihilate $L$. From the table, $A \equiv (5, 1, 0) \pmod 9$, $A \equiv (2, 1, 0)$, $B \equiv (2, 0, 1) \pmod 3$. Since the rank is 1 and $[P_1 - O]$ has infinite order, the differentials $A\boldsymbol{\omega}$ and $B\boldsymbol{\omega}$ annihilate the logarithms of all of $J(\mathbb{Q})$. Also, from the table,

$$A \cdot \log(Q_+ - O) \equiv 15, \qquad A \cdot \log(Q_- - O) \equiv 12 \pmod{27},$$

and both values have 3-adic valuation exactly 1.

*Proof of Proposition 3.13.2.* $C$ has good reduction at 3, so every rational point lies in one of the six residue disks. We write the points of each disk with a parameter $s \in 3\mathbb{Z}_3$.

The disks of $Q_\pm$. The parameter is $s = x - 1$, and at $Q_\pm$, $3v^2 + x + 1 = -4$ is a unit. If such a disk contains a rational point $R$, then, since $A\omega$ annihilates $J(\mathbb{Q})$,

$$0 = A \cdot \log(R - O) = A \cdot \log(Q_\pm - O) + \int_{Q_\pm}^{R} A\omega.$$

Modulo 3, $A\omega \equiv (2 + x)\,dx/(3v^2 + x + 1)$, which vanishes at $x = 1$. So the linear term of the integral has valuation at least 2, and the terms of degree $n \geq 2$ also have valuation at least 2, since $n - v_3(n) \geq 2$. Hence the integral lies in $9\mathbb{Z}_3$. On the other hand, $A \cdot \log(Q_\pm - O)$ has valuation 1, so the equality above cannot hold. These two disks contain no rational points.

The remaining four disks. The centers, the parameters and the differentials used are as follows.

| center | $O$ | $P_-$ | $P_1$ | $P_3$ |
|---|---|---|---|---|
| parameter | $t$ | $v$ | $x-1$ | $x-3$ |
| differential | $B\omega$ | $A\omega$ | $B\omega$ | $A\omega$ |
| coefficient at the center (modulo 3) | $-1$ | 2 | 1 | 2 |

All these coefficients are units, so by the same computation as in the proof of Proposition 3.11.2, the integral $I(3z)$ from the center has the form $3z \cdot (\text{unit})$. By [Col85, MP12], the rational points of a disk are zeros of this integral, so the center is the only one. Therefore $C(\mathbb{Q}) = \{O, P_-, P_1, P_3\}$. □

## 3.14 $x^4 + y^3 + xy + x + 1 = 0$ ($H = 31$)

**Theorem 3.14.1.** *The only integer solution of $x^4 + y^3 + xy + x + 1 = 0$ is $(x, y) = (0, -1)$.*

This equation has the same shape as those in Sections 3.1–3.13, but the method of solution is different. Instead of bitangent 2-descent, an elementary fourth-power descent turns it into a problem about the rational points of a genus 5 curve. From that curve we construct a Prym map to the Jacobian of a genus 2 curve, and we finish with a sieve modulo 7 and 7-adic Chabauty.

**Setup.** Setting $v = y + 1$, the equation becomes

$$x^4 + v\,(v^2 - 3v + x + 3) = 0 \tag{7}$$

(certificate 1.1.14a). In projective coordinates $(x : v : z)$ we use the three quadratic forms

$$q_1 = vz, \qquad q_2 = x^2, \qquad q_3 = -(v^2 - 3vz + xz + 3z^2);$$

then the projective completion of (7) is the smooth plane quartic $C : q_2^2 = q_1 q_3$. Let $(x : v : z : r : s)$ be coordinates on $\mathbb{P}^4$, and let $D$ be the intersection of the three quadrics

$$Q_1 = vz + 3r^2, \qquad Q_2 = x^2 + 3rs, \qquad Q_3 = q_3 + 3s^2. \tag{8}$$

On $D$ we have $q_1 = -3r^2$, $q_2 = -3rs$, $q_3 = -3s^2$, so $q_1 q_3 = q_2^2$. Hence $\pi(x : v : z : r : s) = (x : v : z)$ is a morphism $D \to C$ (if $x = v = z = 0$, then $r = s = 0$). A fixed point of the involution $\sigma : (r, s) \mapsto (-r, -s)$ must have $r = s = 0$, but then $x = 0$, $vz = 0$, $v^2 - 3vz + 3z^2 = 0$ force all coordinates to be 0. Hence $\pi$ is an unramified double cover. $D$ is smooth modulo 7, and hence also smooth over $\mathbb{Q}$ (certificate 1.1.14b). Therefore $D$ is a curve of genus 5. We use the two rational points

$$P_\pm = (0 : 0 : 1 : 0 : \pm 1)$$

of $D$. Theorem 3.14.1 follows from the descent in Step 1 and the following proposition.

**Proposition 3.14.2.** $D(\mathbb{Q}) = \{P_+, P_-\}$.

**Step 1: elementary descent.**

**Lemma 3.14.3.** *Integer solutions of (7) satisfy $v \le 0$, and if $v = 0$, then $x = 0$.*

*Proof.* Suppose $v \ge 1$. If $x \ge 0$, then $v^2 - 3v + x + 3 = (v-1)(v-2) + x + 1 \ge 1$, so the left-hand side is positive. If $x = -t$ with $t \ge 1$, then the left-hand side is $t^4 - tv + (v-1)^3 + 1$. If $1 \le v \le t^3$, then $t^4 - tv \ge 0$ and $(v-1)^3 + 1 \ge 1$. If $v \ge t^3 + 1$, then $(v-1)^2 \ge t^6 \ge t$, so $(v-1)^3 \ge t(v-1)$, and the left-hand side is at least $t^4 - t + 1 > 0$. In either case the left-hand side is nonzero. If $v = 0$, then $x^4 = 0$. □

**Lemma 3.14.4.** *If $(x, v)$ is an integer solution of (7) with $v < 0$, then there are integers $r, s$ such that $(x : v : 1 : r : s) \in D(\mathbb{Q})$.*

*Proof.* Set $n = -v > 0$; then $x^4 = n\,(n^2 + 3n + x + 3)$. If $x = 0$, then $n^2 + 3n + 3 = 0$, which is impossible; so $x \ne 0$, and both factors are positive. If a prime $p$ divides both factors, then $p \mid x$, and looking at the second factor modulo $p$ gives $p \mid 3$. Hence for $p \ne 3$ the exponent of $p$ in $n$ is a multiple of 4, and we can write

$$n = du^4, \qquad d \in \{1, 3, 9, 27\}, \quad u \in \mathbb{Z}_{>0}.$$

If $d = 1$, then $u^4 \mid x^4$, so we write $x = uw$. If $d = 3, 9, 27$, then $3 \mid x$. Writing $x = 3x'$, we get $u^4 \mid 9x'^4$, so $u \mid x'$, and we write $x = 3uw$. Cancelling the common fourth power gives the following equations.

| $d$ | integer equation |
|---|---|
| 1 | $w^4 = u^8 + 3u^4 + uw + 3$ |
| 3 | $9w^4 = 3u^8 + 3u^4 + uw + 1$ |
| 9 | $3w^4 = 27u^8 + 9u^4 + uw + 1$ |
| 27 | $w^4 = 243u^8 + 27u^4 + uw + 1$ |

$d = 1$: If $u, w$ are both prime to 3, then modulo 3 we get $1 \equiv 1 + uw$, a contradiction. If one of them is a multiple of 3, then by the equation so is the other, and modulo 9 we get $0 \equiv 3$, a contradiction.

$d = 9$: With $A = 2w^2 - 6u^4 - 1$, $B = 2w^2 + 6u^4 + 1 > 0$, the equation is equivalent to $3AB = 4uw + 1$ (certificate 1.1.14a). From $u^4 \ge u^2$ and $4|uw| \le 2u^2 + 2w^2$ we get $3B - |4uw + 1| \ge 4w^2 + 16u^2 + 2 > 0$. If $A \ne 0$, then $|3AB| \ge 3B > |4uw + 1|$; if $A = 0$, then $4uw + 1 = 0$ would be required. Both are impossible.

$d = 3, 27$: Set $r = u^2$ ($d = 3$), $r = 3u^2$ ($d = 27$); then $n = 3r^2$. $s = -x^2/(3r)$ is an integer, namely $-3w^2$ and $-w^2$, respectively. Now at $z = 1$ we have $Q_1 = -n + 3r^2 = 0$ and $Q_2 = x^2 + 3rs = 0$. Also $n^2 + 3n + x + 3 = x^4/n = x^4/(3r^2) = 3s^2$, so $Q_3 = -(n^2 + 3n + x + 3) + 3s^2 = 0$. □

**Step 2: the Prym map.** Let $M_1, M_2, M_3$ be the $5 \times 5$ symmetric matrices of $Q_1, Q_2, Q_3$ in (8) ($Q_i(X) = X^{\mathsf{T}} M_i X$). In the pencil of quadrics

$$Q_t = Q_1 - 2tQ_2 + t^2 Q_3 = (q_1 - 2tq_2 + t^2 q_3) + 3(r - ts)^2,$$

each $Q_t$ is a quadric of rank at most 4 with vertex $(0 : 0 : 0 : t : 1)$. Its discriminant is determined by the $(x, v, z)$ part. Indeed,

$$12 \det\big(M(q_1) - 2tM(q_2) + t^2 M(q_3)\big) = f(t) := 3t^6 - 18t^5 + 36t^3 + 6t$$

(certificate 1.1.14a; $M(q_i)$ is the $3 \times 3$ symmetric matrix of $q_i$). We have $f = 3t\,(t^5 - 6t^4 + 12t^2 + 2)$, and its discriminant is $-2^6 \cdot 3^{10} \cdot 19 \cdot 149 \cdot 3461$. Let

$$H : \ \eta^2 = f(t), \qquad J = \mathrm{Jac}(H)$$

be the genus 2 curve and its Jacobian. $H$ has good reduction at 5 and 7. If $f(t) \ne 0$, then $Q_t$ has rank exactly 4, and its two families of planes correspond to $\eta = \pm\sqrt{f(t)}$. $D_\infty$ denotes the sum of the two points at infinity of $H$ (a rational divisor).

The Bruin construction of [Bru08, RR18] gives a morphism $\phi : D \to J$ over $\mathbb{Q}$. Up to an overall sign, $\phi$ is the composition of $p \mapsto [2\sigma(p) - 2p] \in \mathrm{Prym}(D/C)$ with the isomorphism $\mathrm{Prym}(D/C) \cong J$; see [Bru08, Proposition 6.2 and Remark 6.3]. What the proof uses is the following tangent formula. Represent $p \in D$ by a vector $P$, and choose a vector $w$ that is tangent to $D$ at $p$ and not proportional to $P$ ($P^{\mathsf{T}} M_i w = 0$, $i = 1, 2, 3$). Then

$$a_p(t) = w^{\mathsf{T}} M_1 w - 2t\, w^{\mathsf{T}} M_2 w + t^2\, w^{\mathsf{T}} M_3 w \tag{9}$$

is nonzero. Replacing $w$ by $aw + bP$ ($a \neq 0$) only multiplies $a_p$ by $a^2$. At a $t$ with $a_p(t) = 0$, the tangent line at $p$ is contained in $Q_t$, and the family of planes containing this tangent line determines the sign of $\eta$. Let $D_p$ be the effective divisor of degree 2 on $H$ obtained in this way. Then

$$\phi(p) = [D_p - D_\infty].$$

In particular, the $t$-coordinates of $D_p$ are the roots of $a_p$. This Prym identification, including the quadratic twist, is independently checked by $L_p(D) = L_p(C)\, L_p(H)$ at $p = 5, 7, 11, 13, 17$ (certificate 1.1.14b).

**Lemma 3.14.5.** *$A_0 = (0, 0)$ and $B_0 = (24, 20748)$ are rational points of $H$, and $\phi(P_+) = \pm G$, where*

$$G = [B_0 - A_0] = \left(t^2 - 24t,\ \tfrac{1729}{2} t\right) \in J(\mathbb{Q})$$

*(Mumford representation).*

*Proof.* We have $f(0) = 0$ and $f(24) = 20748^2$ (certificate 1.1.14a). In the coordinate order $(x, v, z, r, s)$, the three gradient vectors at $P_+$ are $(0, 1, 0, 0, 0)$, $(0, 0, 0, 3, 0)$, $(-1, 3, -6, 0, 6)$, and $w = (1, 0, 0, 0, \frac{1}{6})$ is orthogonal to all three. Since $Q_1(w) = 0$, $Q_2(w) = 1$, $Q_3(w) = 3 \cdot \frac{1}{36} = \frac{1}{12}$,

$$a_{P_+}(t) = -2t + \tfrac{1}{12} t^2 = \tfrac{1}{12}\, t\,(t - 24).$$

The only point of $H$ above the root $t = 0$ is the Weierstrass point $A_0$, and the points above $t = 24$ are $(24, \pm 20748)$. Hence $D_{P_+} = A_0 + (24, \varepsilon \cdot 20748)$ with $\varepsilon = \pm 1$. Since $2A_0 \sim D_\infty$, $\phi(P_+) = [(24, \varepsilon \cdot 20748) - A_0]$. The hyperelliptic involution fixes $A_0$ and acts on $J$ as $-1$, so this is $\varepsilon G$. The Mumford representation is checked from $t(t - 24)$, $b(0) = 0$, $b(24) = 1729 \cdot 12 = 20748$. □

**Step 3: $J(\mathbb{Q})$.**

**Lemma 3.14.6.** *$J(\mathbb{Q}) \cong \mathbb{Z}$. If $H_0$ is a generator and $G = mH_0$, then $m$ is odd. Moreover, the image of the reduction modulo 7, $\rho_7 : J(\mathbb{Q}) \to J(\mathbb{F}_7)$, is $\{0, \bar{G}\}$.*

*Proof.* certificate 1.1.14c verifies the following by exact computation:

$$\#\mathrm{Sel}^{(2)}(J/\mathbb{Q}) = 2, \qquad \#J(\mathbb{F}_5) = 23, \qquad \#J(\mathbb{F}_7) = 32, \qquad \mathrm{ord}\, \bar{G} = 2, \qquad \bar{G} \notin 2J(\mathbb{F}_7).$$

By [Kat81, Appendix], torsion of order prime to 5 injects into $J(\mathbb{F}_5)$, and torsion of order prime to 7 injects into $J(\mathbb{F}_7)$. If there were a torsion point of prime order $\ell$, we would need $\ell \mid 23$ when $\ell \neq 5$ and $\ell \mid 32$ when $\ell \neq 7$; no such $\ell$ exists. Hence $J(\mathbb{Q})$ has no torsion, and in particular $J(\mathbb{Q})[2] = 0$. By [Sto01, PS97, PS99], $\#\mathrm{Sel}^{(2)} = 2$ gives $\mathrm{rank}\, J(\mathbb{Q}) \leq 1$. Since $G \neq 0$, the rank is 1 and $J(\mathbb{Q}) \cong \mathbb{Z}$. If $m$ were even, then $\bar{G} = m\bar{H}_0 \in 2J(\mathbb{F}_7)$, a contradiction. Since $\#J(\mathbb{F}_7) = 32$ and $m$ is odd, $\bar{H}_0$ and $\bar{G} = m\bar{H}_0$ generate the same subgroup, which is $\{0, \bar{G}\}$. □

**Step 4: sieve modulo 7.**

**Lemma 3.14.7.** *Every point of $D(\mathbb{Q})$ reduces modulo 7 to $\bar{P}_+$ or $\bar{P}_-$.*

*Proof.* $D(\mathbb{F}_7)$ has eight points, all with $z \neq 0$ (certificate 1.1.14c). Their coordinates $(x, v, r, s)$ normalized by $z = 1$, and the tangent polynomials $a_{\bar{p}}$ normalized to be monic, are as follows. Two points paired by $\sigma$ have the same $a_{\bar{p}}$.

| $(x,v,r,s) \bmod 7$ | | $a_{\bar{p}}(t)$ |
|---|---|---|
| $(0,0,0,1),\ (0,0,0,6)$ | $(= \bar{P}_+, \bar{P}_-)$ | $t^2+4t$ |
| $(0,4,1,0),\ (0,4,6,0)$ | | $t^2+t+4$ |
| $(4,2,2,2),\ (4,2,5,5)$ | | $t^2+t+4$ |
| $(5,2,2,4),\ (5,2,5,3)$ | | $t^2+t+4$ |

Take $p \in D(\mathbb{Q})$ and represent it by a primitive vector $P \in \mathbb{Z}_7^5$. Since $D$ is smooth over $\mathbb{Z}_7$, the $3 \times 5$ matrix $(P^{\mathsf{T}} M_i)_i$ has rank 3 also modulo 7. Its kernel is a saturated submodule of rank 2 containing $P$, so there is $w \in \mathbb{Z}_7^5$ that, together with $P$, forms a basis of the kernel. Then $\bar{w}$ is a tangent vector at $\bar{p}$ and is independent of $\bar{P}$. Hence the reduction modulo 7 of $a_p \in \mathbb{Z}_7[t]$ is a nonzero constant multiple of $a_{\bar{p}}$. Since $H$ has good reduction at 7, the reduction of $\phi(p) = [D_p - D_\infty]$ is $[\bar{D}_p - \bar{D}_\infty]$, where $\bar{D}_p$ is the effective divisor of degree 2 whose $t$-coordinates are the roots of $a_{\bar{p}}$.

If $a_{\bar{p}} = t^2 + t + 4$, its discriminant $1 - 16 \equiv 6$ is not a square modulo 7. So $\bar{D}_p$ consists of two conjugate points over $\mathbb{F}_{49}$ with distinct $t$-coordinates. $\bar{D}_p$ is not a fiber of $t$, so $[\bar{D}_p - \bar{D}_\infty] \neq 0$, and the first polynomial of its Mumford representation is $t^2 + t + 4$. The first polynomial of $\bar{G}$ is $t^2 - 24t \equiv t^2 + 4t$, so this class is not $\bar{G}$ either. On the other hand, by Lemma 3.14.6, $\rho_7(\phi(p)) \in \{0, \bar{G}\}$ ([BS10]). Hence $\bar{p} \in \{\bar{P}_+, \bar{P}_-\}$. □

**Step 5: 7-adic Chabauty in the two residue disks.** The differentials of $H$

$$\omega_0 = \frac{dt}{2\eta}, \qquad \omega_1 = \frac{t\,dt}{2\eta}$$

form a basis of the regular differentials on the $\mathbb{Z}_7$-model of $H$, and hence a basis of the invariant differentials of $J$ over $\mathbb{Z}_7$. Let $\lambda = (\lambda_0, \lambda_1) : J(\mathbb{Q}_7) \to \mathbb{Q}_7^2$ be the logarithm with respect to this basis, and write $\lambda_{\omega'}$ for the component with respect to a differential $\omega'$.

**Lemma 3.14.8.** *Write $\lambda(G) = (\ell_0, \ell_1)$. Then $v_7(\ell_0) = v_7(\ell_1) = 1$. $\beta = \ell_1/\ell_0$ is a unit of $\mathbb{Z}_7$ with $\beta \equiv 24 \pmod{49}$, in particular $\beta \equiv 3 \pmod 7$ (more precisely, $\beta \equiv 53924 \pmod{7^6}$). The differential*

$$\omega = \omega_1 - \beta\omega_0 = \frac{(t-\beta)\,dt}{2\eta}$$

*annihilates the logarithms of all of $J(\mathbb{Q})$.*

*Proof.* Since $f(24) \equiv 0$ and $f'(24) \equiv 1 \pmod 7$, by Hensel's lemma $f$ has a 7-adic root $\alpha$ with $\alpha \equiv 24 \pmod 7$ ($\alpha \equiv 24 \pmod{49}$, $\alpha \equiv 1641 \pmod{7^4}$). Let $W = (\alpha, 0)$. $A_0$ and $W$ are Weierstrass points, so $[W - A_0]$ is 2-torsion and its logarithm is 0. Hence $\lambda(G) = \lambda([B_0 - W])$. Since $20748 = 7 \cdot 2964$, $B_0$ lies in the same residue disk as $W$, and since $f'(\alpha)$ is a unit, $\eta$ is a local parameter on this disk. Since $t = \alpha + \eta^2/f'(\alpha) + O(\eta^4)$,

$$\omega_0 = \Big(\frac{1}{f'(\alpha)} + O(\eta^2)\Big)d\eta, \qquad \omega_1 = \Big(\frac{\alpha}{f'(\alpha)} + O(\eta^2)\Big)d\eta,$$

and all coefficients lie in $\mathbb{Z}_7$. By the tiny integrals of [Col85, MP12], $\ell_i = \int_W^{B_0} \omega_i$. The terms $\eta^{2k+1}/(2k+1)$ ($k \geq 1$) have valuation at least $2k + 1 - v_7(2k+1) \geq 3$ at $\eta = 20748$, so

$$\ell_0 \equiv \frac{20748}{f'(\alpha)}, \qquad \ell_1 \equiv \frac{20748\,\alpha}{f'(\alpha)} \pmod{7^3}.$$

Hence both have valuation 1, and $\beta \equiv \alpha \pmod{49}$. The precise value is computed by certificate 1.1.14e. Since $J(\mathbb{Q}) = \mathbb{Z}H_0$ and $G = mH_0$ with $m \neq 0$, we get $\lambda_\omega(H_0) = (\ell_1 - \beta\ell_0)/m = 0$. □

**Lemma 3.14.9.** *On the residue disk of $P_+$ (the points of $D(\mathbb{Q}_7)$ that reduce to $\bar{P}_+$ modulo 7), $x$ is a local parameter, and the points of the disk correspond bijectively to $x \in 7\mathbb{Z}_7$. On this disk,*

$$\phi^*\omega = g(x)\,dx, \qquad g \in \mathbb{Z}_7[[x]], \qquad g(0) = \mp\tfrac{\beta}{3} \in \mathbb{Z}_7^\times.$$

*Proof.* In the chart $z = 1$, the Jacobian determinant of $(Q_1, Q_2, Q_3)$ with respect to $(v, r, s)$ at $P_+$ is

$$\det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 3 & 0 & 6 \end{pmatrix} = 18,$$

a 7-adic unit. Hence, by Hensel's lemma (the implicit function theorem), $v, r, s \in \mathbb{Z}_7[[x]]$, and $x \in 7\mathbb{Z}_7$ corresponds bijectively to the points of the disk. The first few terms are as follows (certificate 1.1.14a, certificate 1.1.14f).

$$s = 1 + \tfrac{x}{6} - \tfrac{x^2}{72} + \tfrac{x^3}{432} + O(x^4), \quad r = -\tfrac{x^2}{3} + \tfrac{x^3}{18} - \tfrac{x^4}{72} + O(x^5), \quad v = -\tfrac{x^4}{3} + \tfrac{x^5}{9} + O(x^6).$$

*Integrality.* The $\mathbb{Z}_7$-model of $D$ is smooth, and $J$ is an abelian scheme over $\mathbb{Z}_7$. By the Néron mapping property ([BLR90, Section 1.2]), $\phi$ extends to a morphism over $\mathbb{Z}_7$. Since $\omega_0, \omega_1$ are invariant differentials of $J$ over $\mathbb{Z}_7$ and $\beta \in \mathbb{Z}_7$, $\phi^*\omega$ is a regular differential on the $\mathbb{Z}_7$-model of $D$. Since $x$ is a parameter at $\bar{P}_+$, $\phi^*\omega = g(x)\,dx$ with $g \in \mathbb{Z}_7[[x]]$.

*Constant term.* Substituting the tangent vector $w = (1, v', 0, r', s')$ at the point $p(x)$ of the disk into (9), the coefficients of $a_{p(x)}$ at $x = 0$ are $(0, -2, \frac{1}{12})$, and the two roots are

$$t_1 = \tfrac{2}{3}x^2 - \tfrac{1}{9}x^3 + O(x^4), \qquad t_2 = 24 - \tfrac{1729}{9}x^3 + O(x^4).$$

Since $f(t_1) = 4x^2 + O(x^3)$, we have $\eta_1 = \pm(2x + O(x^2))$ and $dt_1/(2\eta_1) = \pm(\frac{1}{3} + O(x))\,dx$. Since $dt_2/dx = O(x^2)$, the contribution of the second point is $O(x^2)\,dx$. Hence

$$\phi^*\omega = (t_1 - \beta)\frac{dt_1}{2\eta_1} + (t_2 - \beta)\frac{dt_2}{2\eta_2} = \mp\frac{\beta}{3}\,dx + O(x)\,dx.$$

By Lemma 3.14.8, $\beta/3 \equiv 1 \pmod 7$ is a unit. certificate 1.1.14f computes this expansion exactly up to degree 18 and shows that all coefficients up to degree 14 are 7-adic integers. □

*Proof of Proposition 3.14.2.* Let $R \in D(\mathbb{Q})$. By Lemma 3.14.7, $R$ lies in the residue disk of $P_+$ or of $P_-$. $\sigma$ preserves $D(\mathbb{Q})$ and interchanges $\bar{P}_+$ and $\bar{P}_-$, so we may assume that $R$ lies in the disk of $P_+$. Let $\xi = x(R) \in 7\mathbb{Z}_7$. An integral within the disk is a difference of logarithms ([Col85, MP12]), so

$$\int_{P_+}^{R} \phi^*\omega = \lambda_\omega\big(\phi(R) - \phi(P_+)\big) = 0.$$

This is because $\phi(R) - \phi(P_+) \in J(\mathbb{Q})$, and by Lemma 3.14.8, $\omega$ annihilates the logarithms of $J(\mathbb{Q})$. On the other hand, writing $g = \sum_{j\ge 0} c_j x^j$ as in Lemma 3.14.9,

$$\int_{P_+}^{R} \phi^*\omega = \sum_{j\ge 1} \frac{c_{j-1}}{j}\,\xi^j.$$

If $\xi \neq 0$, the first term has valuation $v_7(\xi)$, and the terms with $j \ge 2$ have valuation at least $jv_7(\xi) - v_7(j) > v_7(\xi)$ (since $(j-1)v_7(\xi) \ge j - 1 > v_7(j)$). Then the integral has finite valuation $v_7(\xi)$, so it cannot be 0. Hence $\xi = 0$, that is, $R = P_+$. □

*Proof of Theorem 3.14.1.* By Lemma 3.14.3, integer solutions have $v \le 0$, and if $v = 0$, then $(x, y) = (0, -1)$. This is indeed a solution. If there were a solution with $v < 0$, then by Lemma 3.14.4 it would give a rational point $(x : v : 1 : r : s) \in D(\mathbb{Q})$ with nonzero $v$-coordinate. The $v$-coordinates of $P_\pm$ are 0, so this contradicts Proposition 3.14.2. □

### 3.15 $x^4 - x^2 + xy + y^3 = 0$ ($H = 32$)

**Theorem 3.15.1.** *The equation $x^4 - x^2 + xy + y^3 = 0$ has only the following integer solutions: $(x, y) = (0, 0)$, $(1, 0)$, $(-1, 0)$, $(-1, 1)$, $(-1, -1)$, $(2, -2)$, $(4, -6)$.*

**Setup.** Unlike the other equations of Section 3, the plane quartic is singular: its lowest-degree part $-x^2 + xy = x(y - x)$ has two distinct factors, so the origin is a node, and the point $(0 : 1 : 0)$ at infinity is smooth. If $x = 0$, the equation gives $y = 0$. For $x \neq 0$ put

$$u = -\frac{y}{x}, \qquad v = -x.$$

Then $x^4 - x^2 + xy + y^3 = v^2(v^2 + u^3 v - u - 1)$, so the solutions with $x \neq 0$ lie on

$$C: \quad v^2 + u^3 v = u + 1, \qquad \text{equivalently} \qquad w^2 = u^6 + 4u + 4 \quad (w = 2v + u^3). \tag{10}$$

Put $J = \mathrm{Jac}(C)$, where $C$ denotes the smooth projective model of (10). Let $O$ and $E$ be the two points at infinity of (10), labelled so that $v \sim -u^3$ at $O$ and $v \sim u^{-2}$ at $E$; $O$ corresponds to the point $(0 : 1 : 0)$ of the quartic, and $E$ to one of the two branches at the origin. The functions

$$x = -v, \qquad y = uv, \qquad z = -u^2 v = y^2/x$$

have poles of orders $3, 4, 5$ at $O$ and no other poles. The affine curve $\mathcal{U} = C \setminus \{O\}$ has the integral model

$$y^2 = xz, \qquad x^3 - x + y(z + 1) = 0, \qquad z^2 + z = y(1 - x^2). \tag{11}$$

On it $x = 0$ forces $y = 0$ and $z \in \{0, -1\}$; these are the points $D = (0, 0, 0)$ and $E = (0, 0, -1)$, the two branches at the origin. Over $\mathbb{Q}$, (11) is covered by the chart $z + 1 \neq 0$, on which $u = (x^2 - 1)/(z + 1)$ and $v = -x$, and the chart $z \neq 0$, on which $s = y/z = x/y$ is a parameter at $E$. Integrally, the proof uses only three facts: every integer solution lifts to an integral point of (11) (Lemma 3.15.2); an integral point of (11) does not reduce to $O$ modulo any prime (Lemma 3.15.8); and the $\mathbb{Z}_2$-points of (11) are described by four residue disks (Step 6).

**Lemma 3.15.2.** *If $(x, y)$ is an integer solution with $x \neq 0$, then $x \mid y^2$, and $(x, y, y^2/x)$ is an integral point of (11).*

*Proof.* Let $\ell$ be a prime with $\alpha = v_\ell(x) > 0$, and $\beta = v_\ell(y)$. If $\beta \geq \alpha$, then $\alpha \leq 2\beta$. If $\beta < \alpha$, the four terms $x^4, x^2, xy, y^3$ have valuations $4\alpha, 2\alpha, \alpha + \beta, 3\beta$, and the smallest one must occur at least twice. Since $\alpha + \beta < 2\alpha < 4\alpha$, this forces $\alpha + \beta = 3\beta$, that is, $\alpha = 2\beta$. So $\alpha \leq 2\beta$ at every prime, and $x \mid y^2$. The three relations follow from the equation by substituting $z = y^2/x$. □

The seven solutions of the theorem give the following eight integral points of (11) (the origin gives $D$ and $E$). They are used as known points; that they satisfy (11) is checked by substitution.

| | $A$ | $B$ | $C_1$ | $D$ | $E$ | $F_1$ | $G$ | $H$ |
|---|---|---|---|---|---|---|---|---|
| $(x, y, z)$ | $(-1, -1, -1)$ | $(-1, 0, 0)$ | $(-1, 1, -1)$ | $(0, 0, 0)$ | $(0, 0, -1)$ | $(1, 0, 0)$ | $(2, -2, 2)$ | $(4, -6, 9)$ |
| $(x, y)$ | $(-1, -1)$ | $(-1, 0)$ | $(-1, 1)$ | $(0, 0)$ | $(0, 0)$ | $(1, 0)$ | $(2, -2)$ | $(4, -6)$ |

**Lemma 3.15.3.** *The discriminant of (10), normalized as usual for genus 2, is $2^{-12}\,\mathrm{disc}(u^6 + 4u + 4) = -8539$, and 8539 is prime. Modulo 8539, $f = u^6 + 4u + 4$ satisfies $\gcd(f, f') = u + 1709$ and $\gcd(f, f', f'') = 1$. Hence (10) has good reduction at every prime $p \neq 8539$ (in particular at 2), and at 8539 the fibre is geometrically irreducible with a single ordinary node of thickness 1. The model is regular, and integral sections do not pass through the node (certificate 1.1.15a).*

*Proof.* The four other roots of $f$ modulo 8539 are simple, so the fibre at 8539 has one ordinary double point and is geometrically irreducible; since 8539 divides the discriminant exactly once, the node has thickness 1. After an unramified extension the local equation at the node is $ab = 8539 \cdot (\text{unit})$; this is regular, and a section through the node would make both $a$ and $b$ divisible by 8539, which is impossible. □

So all fibres are irreducible, and local heights of divisors of degree 0 need no vertical correction. We abbreviate $[P - O] \in J(\mathbb{Q})$ to $P$.

The proof runs as follows. A 2-descent bounds the rank by 2 (Step 1). With explicit differentials of the second and third kind we write down the Coleman–Gross local height at $p = 2$ (Steps 2–3). Since the differential $\omega_1$ used to normalize the self-height vanishes at the non-Weierstrass point $E$, we add the cross-height with $E$; the local terms at odd primes of this combination vanish at every integral point (Step 4). All periods and the height matrix are obtained from two tiny integrals, and they show that the rank is exactly 2 (Step 5). Finally, on each of the four 2-adic residue disks the resulting quadratic Chabauty function has at most two zeros, and the two known points in each disk account for them (Step 6). This is the method of [CG89, BBM16], at $p = 2$ and with the cross-height term. The literature quoted for [CG89, BBM16] does not cover this setting verbatim (it is usually stated for odd $p$, and no second point at infinity enters); the facts about heights used here are those of [CG89, BB12, BB15], which hold at every prime of good reduction, and the local heights are identified in Steps 3 and 4.

**Step 1: upper bound for the rank.**

**Lemma 3.15.4.** rank $J(\mathbb{Q}) \leq 2$.

*Proof.* The 2-descent of [Sto01, PS97, PS99] for $w^2 = u^6 + 4u + 4$, computed with Magma's `RankBound`, gives the upper bound 2 (certificate 1.1.15a). The class groups used in the descent are computed with the proof bound set to the Minkowski bound, so the bound does not depend on GRH. Equality is proved in Lemma 3.15.12. □

**Step 2: differentials and principal divisors.** Put

$$\omega_1 = \frac{dx}{1+3z}, \qquad \omega_2 = \frac{y}{x}\,\omega_1, \qquad \eta_1 = 2y\,\omega_1, \qquad \eta_2 = x\,\omega_1$$

(where an apparent denominator vanishes, these are understood as their regular extensions). On (10), $\omega_1 = -du/(2v + u^3)$ and $\omega_2 = u\,du/(2v + u^3)$, so $\omega_1, \omega_2$ form a basis of the holomorphic differentials. As a section of the relative dualizing sheaf of the regular model, $\omega_1$ has divisor $E + O$, with no vertical component. At $O$ we use the parameter $t = -x/y = 1/u$, fixed once and for all:

$$x = t^{-3}\rho, \quad y = -t^{-4}\rho, \quad z = t^{-5}\rho, \qquad \rho^2 - \rho = t^5 + t^6, \quad \rho(0) = 1. \tag{12}$$

The leading terms of $\omega_1, \omega_2, \eta_1, \eta_2$ are $-t\,dt$, $dt$, $2t^{-3}dt$, $-t^{-2}dt$, and the next terms begin in degrees $6, 5, 2, 3$. Hence the $\eta_i$ are of the second kind with poles only at $O$, and with the convention $\langle [\alpha], [\beta] \rangle = \mathrm{Res}_O((\int \alpha)\beta)$ the cup product matrix of $\omega_1, \omega_2, \eta_1, \eta_2$ is $\left(\begin{smallmatrix} 0 & -I_2 \\ I_2 & 0 \end{smallmatrix}\right)$. So $W = \langle [\eta_1], [\eta_2] \rangle$ is an isotropic subspace of $H^1_{\mathrm{dR}}$ complementary to the holomorphic differentials.

**Lemma 3.15.5.** *The following divisors hold on $C$ (certificate 1.1.15b):*

$$\begin{aligned} \mathrm{div}(x) &= D + 2E - 3O, & \mathrm{div}(y) &= B + F_1 + D + E - 4O, \\ \mathrm{div}(y - x) &= A + 2D + E - 4O, & \mathrm{div}(x + 1) &= A + B + C_1 - 3O, \\ \mathrm{div}(x + y) &= C_1 + G + D + E - 4O, & \mathrm{div}(z - 2x - 1) &= 3A + C_1 + H - 5O. \end{aligned}$$

*Hence, in $J(\mathbb{Q})$,*

$$D = -2E, \quad B = E - F_1, \quad A = 3E, \quad C_1 = F_1 - 4E, \quad G = 5E - F_1, \quad H = -5E - F_1.$$

*Proof.* The orders of zero of the six functions at the eight points are computed from local expansions, and in each case their sum equals the pole order at $O$ (certificate 1.1.15b). The relations follow successively. □

**Step 3: the local height at 2.** For $P = (a, b, c)$ and $Q = (x, y, z)$ put

$$\nu_P(Q) = \frac{z + c + 1 + by/x}{x - a}\,\omega_1(Q).$$

This is a differential of the third kind with residue divisor $P - O$: on the other branches over $x = a$ the numerator vanishes, and with the normalized branches it extends to $\nu_D = \frac{z+1}{x}\omega_1$ and $\nu_E = \frac{z}{x}\omega_1$. At $O$,

$$\nu_P = \left(-t^{-1} - at^2 + bt^3 + \cdots\right) dt,$$

so the coefficients of $t^0$ and $t^1$ are 0. The bidifferential identity

$$d_P\nu_P(Q) - d_Q\nu_Q(P) = \sum_{i=1}^{2}\bigl(\eta_i(P)\omega_i(Q) - \omega_i(P)\eta_i(Q)\bigr) \tag{13}$$

holds: after division by $\omega_1(P)\omega_1(Q)$ both sides reduce to $2b - 2y + ay/x - xb/a$ on $C \times C$ (certificate 1.1.15b).

Take $p = 2$ and let $\log_2$ be the 2-adic logarithm with $\log_2 2 = 0$ (so also $\log_2(-1) = 0$); it is the 2-component $\chi_2$ of the cyclotomic idele class character of [CG89, BB12, BB15]. Put

$$I(P) = \Bigl(\int_O^P \omega_1, \int_O^P \omega_2\Bigr), \qquad J(P) = \Bigl(\int_O^P \eta_1, \int_O^P \eta_2\Bigr), \qquad K(P, Q) = \int_O^Q \nu_P,$$

with the following normalizations at the end points. $J_j(P) = \Phi_j(P)$, where $\Phi_j$ is the Coleman integral of $\eta_j$ whose Laurent expansion in $t$ at $O$ has constant term 0 (this depends on the parameter $t$, not only on $\partial_t$). $K(P, Q) = \Lambda_P(Q)$, where $\Lambda_P$ is the Coleman integral of $\nu_P$ with $\Lambda_P + \log_2 t \to 0$ at $O$ (this depends only on $\partial_t$). For $P \neq E$ let $v_P$ be the tangent vector at $P$ with $\omega_1(v_P) = 1$, and put $K(P, P) = \lim_{Q\to P}\bigl(\Lambda_P(Q) - \log_2 z_P(Q)\bigr)$ for a parameter $z_P$ at $P$ with $dz_P(v_P) = 1$; at $E$ we use $\partial_s$ and $z_E = s$, with $s = x/y$ as in (14) below. Define

$$\mathcal{H}(P, Q) = K(P, Q) - J(P)\, I(Q)^{\mathsf{T}}.$$

**Lemma 3.15.6.** *For $P, Q \in \mathcal{U}(\mathbb{Q}_2)$, with the tangent vector $\partial_t$ at $O$ and, if $Q = P$, the tangent vector $v_P$ (or $\partial_s$ if $P = E$) at $P$,*

$$\mathcal{H}(P, Q) = h_2(P - O, Q - O),$$

*where $h_2$ is the local height at 2 of [CG89, BB12, BB15] for $W$ and $\chi_2 = \log_2$.*

*Proof.* By [BB12, Section 2] we need the differential $\omega_{P-O}$ of the third kind with residue divisor $P - O$ and $\Psi(\omega_{P-O}) \in W$. Write $\Psi(\nu_P) = \sum_i a_i[\omega_i] + w$ with $w \in W$; by the cup product matrix, $\langle[\eta_j], \Psi(\nu_P)\rangle = a_j$. The global symbol of [BB12, Section 2] with $\nu = \nu_P$, $\beta = \eta_j$, $\Phi_\beta = \Phi_j$ has two terms: at $P$ the residue is $\Phi_j(P) = J_j(P)$, and at $O$ it is 0, because $\nu_P = (-t^{-1} + 0 + 0 \cdot t + O(t^2))\,dt$ while $\Phi_j$ has a pole of order at most 2 and constant term 0. So $a_j = J_j(P)$, and $\omega_{P-O} = \nu_P - \sum_i J_i(P)\omega_i$. Hence $\int_{Q-O}\omega_{P-O} = K(P, Q) - J(P)I(Q)^{\mathsf{T}}$, the integrals being regularized at $O$ (and at $P$ if $Q = P$) by the chosen tangent vectors, as in the definition of $K$. This regularized pairing is bi-additive, agrees with $h_2$ for disjoint supports, and satisfies $h_2(\operatorname{div} f, \mathfrak{a}) = \log_2 f[\mathfrak{a}]$ for divisors $\mathfrak{a}$ of degree 0, because $\omega_{\operatorname{div} f} = df/f$; by [Gro86, BB15] these properties determine $h_2$. □

Consistently with this, (13) says that the mixed derivative $d_P d_Q$ of $\mathcal{H}(P, Q) - \mathcal{H}(Q, P)$ vanishes, as it must since $h_2$ is symmetric for isotropic $W$; with the opposite sign of the term $J(P)I(Q)^{\mathsf{T}}$ it would not. Integrating (13), with $Q$ replaced by a variable point $R$, from $R = O$ to $R = Q$ gives

$$d_P\mathcal{H}(P, Q) = \nu_Q(P) - \sum_i \omega_i(P)J_i(Q).$$

The boundary term at $O$ vanishes: if $R \to O$ and $t = t(R)$, then $\nu_R(P) = -t^{-2}\omega_1(P) + t^{-1}\omega_2(P) + O(t)$ by (12), while $\Phi_1 = -t^{-2} + O(t^3)$ and $\Phi_2 = t^{-1} + O(t^4)$; and the normalization of $K(P, \cdot)$ at $O$ does not depend on $P$.

**Lemma 3.15.7.** *Put $\tau_*(P) = \mathcal{H}(P,P) + \mathcal{H}(P,E)$. Then*

$$d\mathcal{H}(P,P) = -2\sum_i \omega_i(P)J_i(P) - \nu_E(P), \qquad d\mathcal{H}(P,E) = \nu_E(P) - \sum_i \omega_i(P)J_i(E),$$

*so $d\tau_* = -\sum_i \omega_i\big(2J_i(P) + J_i(E)\big)$, and $\tau_*$ has no logarithmic singularity at $E$. Its value at $E$, defined by the regular extension, is $2\mathcal{H}(E,E) = 2h_2(E-O, E-O)$ with respect to $\partial_s$.*

*Proof.* On the diagonal the two regular parts of $\nu_P(Q)$ and $\nu_Q(P)$ combine with the term $d\log$ of the normalization by $v_P$. Let $\Delta = 1 + 3c$ and $b' = db/da$. Where $x$ is a parameter, the regular coefficient of $\nu_P$ on the diagonal is $r = (-3bb'/a + c/a)/\Delta$, and

$$2r + \frac{d}{da}\log\Delta = -\frac{c}{a\Delta},$$

which is the coefficient of $-\nu_E$; the identity extends to the other charts. This gives the first formula; the second is the formula for $d_P\mathcal{H}$ above. Near $E$ we use $s = x/y$:

$$z + s^5z^2 + 1 - s = 0, \quad z(0) = -1, \qquad x = s^2z, \quad y = sz, \quad \omega_1 = \frac{s\,ds}{1 + 2s^5z}. \tag{14}$$

Since $\omega_1$ vanishes to order 1 at $E$, $v_P$ degenerates as $P \to E$; the resulting term $-\log_2 s$ in the self-height and the term $+\log_2 s$ in the cross-height cancel, and since the leading coefficient is the unit 1, no constant arises. □

**Step 4: local heights away from 2.**

**Lemma 3.15.8.** *Let $\ell$ be an odd prime and $P \in \mathcal{U}(\mathbb{Z})$. With the tangent vectors $\partial_t$ at $O$, $v_P$ at $P$ and $\partial_s$ at $E$,*

$$h_\ell(P-O, P-O) + h_\ell(P-O, E-O) = 0,$$

*where for $P = E$ the left-hand side is $2h_\ell(E-O, E-O)$ with respect to $\partial_s$.*

*Proof.* Near the points at infinity use $T = 1/u$ and $R = vT^3$, with $R^2 + R = T^5 + T^6$; then $x = -R/T^3$ and $\omega_1 = T\,dT/(2R+1)$. The sections $\bar{O}$ and $\bar{E}$ are $T = 0$ together with $R = -1$, resp. $R = 0$; they are disjoint at every prime, and $T$ is a local equation of each, since $2R + 1 = \mp 1$ there.

(i) Integral points do not meet $\bar{O}$: if $P \in \mathcal{U}(\mathbb{Z})$ reduced to $\bar{O}$ modulo $\ell$, then $T(P) \in \ell\mathbb{Z}_\ell$ and $R(P) \in -1 + \ell\mathbb{Z}_\ell$, so $v_\ell(x(P)) \le -3$. They do not pass through the node at 8539 (Lemma 3.15.3), all fibres are irreducible, and $\chi_\infty = 0$.

(ii) By [CG89, (1.3)], (3), $h_\ell(\mathfrak{a}_1, \mathfrak{a}_2) = \chi_\ell(\ell)(\mathfrak{a}_1 \cdot \mathfrak{a}_2)_\ell = -(\mathfrak{a}_1 \cdot \mathfrak{a}_2)_\ell \log_2 \ell$, also for common support when the tangent vectors at the common points are integral (the self-intersection of a section then contributes 0), and replacing a tangent vector $t_x$ by $\alpha t_x$ adds $\chi_\ell(\alpha)\,\mathrm{ord}_x(\mathfrak{a}_1)\,\mathrm{ord}_x(\mathfrak{a}_2)$.

(iii) The tangent vectors $\partial_t$ at $O$ and $\partial_s$ at $E$ ($s = -T$) are integral. Let $P \neq E$ and $n = (P \cdot E)_\ell$. Since $\mathrm{div}\,\omega_1 = \bar{E} + \bar{O}$ with no vertical part and $\bar{P}$ meets the special fibre in a smooth point and avoids $\bar{O}$, the restriction of $\omega_1$ to $\bar{P}$ vanishes to order exactly $n$. Hence $\omega_1(t_P) \in \ell^n\mathbb{Z}_\ell^\times$ for an integral tangent vector $t_P$, and $v_P = \alpha t_P$ with $v_\ell(\alpha) = -n$ (the adjunction formula $(P \cdot P)_{v_P} = -(P \cdot \mathrm{div}\,\omega_1)_\ell$).

By (i)–(iii), $h_\ell(P-O, P-O) = \chi_\ell(\alpha) = n\log_2\ell$ and $h_\ell(P-O, E-O) = -(P \cdot E)_\ell \log_2 \ell = -n\log_2\ell$, while $h_\ell(E-O, E-O) = 0$ with respect to $\partial_s$. □

For the eight known points, the resulting decomposition $\mathcal{H}(P,Q) - I(P)MI(Q)^{\mathsf{T}} = \sum_{\ell\neq 2}(P \cdot Q)_\ell \log_2 \ell$ ($P \neq Q$) and $\mathcal{H}(P,P) = I(P)MI(P)^{\mathsf{T}}$, with $M$ of Lemma 3.15.12, was confirmed numerically to 310 bits for all 64 ordered pairs, including $E$; the right-hand side is nonzero only for $\{A, H\}$ at $\ell = 5$ and for $\{C_1, G\}$, $\{F_1, H\}$ at $\ell = 3$. No known point meets $E$ at an odd prime, so the case $n \neq 0$ of (iii) rests on the argument above.

**Lemma 3.15.9.** *Let $h$ be the global height pairing on $J(\mathbb{Q})$ of [CG89] for $W$. For every $P \in \mathcal{U}(\mathbb{Z})$,*

$$\tau_*(P) = h(P,P) + h(P,E) \qquad (\text{for } P = E\text{: } \tau_*(E) = 2h(E,E)).$$

*Proof.* The tangent vectors $\partial_t$ at $O$, $v_P$ at $P \neq E$ and $\partial_s$ at $E$ are $\mathbb{Q}$-rational, so by [CG89] $h(P,P) + h(P,E) = \sum_v \big(h_v(P-O,P-O) + h_v(P-O,E-O)\big)$. The term at 2 is $\tau_*(P)$ by Lemmas 3.15.6 and 3.15.7, the terms at odd $\ell$ vanish by Lemma 3.15.8, and there is no archimedean term. □

**Step 5: periods and the height matrix.** Write $\omega = (\omega_1, \omega_2)$, $\eta = (\eta_1, \eta_2)$, and $I_P = I(P)$, $J_P = J(P)$. Put

$$\delta_1 = \int_B^{F_1} \omega, \quad \delta_2 = \int_D^{G} \omega, \quad \epsilon_1 = \int_B^{F_1} \eta, \quad \epsilon_2 = \int_D^{G} \eta.$$

Each of these is a tiny integral within one 2-adic residue disk (Step 6).

**Lemma 3.15.10.**

$$I_E = \frac{\delta_1 + 2\delta_2}{13}, \quad I_{F_1} = \frac{7\delta_1 + \delta_2}{13}, \quad J_E = \frac{\epsilon_1 + 2\epsilon_2 + (4,0)}{13}, \quad J_{F_1} = \frac{7\epsilon_1 + \epsilon_2 + (2,0)}{13},$$

*and*

$$\begin{aligned} &I_A = 3I_E, && I_B = I_E - I_{F_1}, && I_D = -2I_E, \\ &J_A = 3J_E - (1,1), && J_B = J_E - J_{F_1}, && J_D = -2J_E, \\ &J_{C_1} = J_{F_1} - 4J_E + (1,1), && J_G = 5J_E - J_{F_1} + (-2,0). \end{aligned}$$

*Proof.* The relations for $I$ follow from Lemma 3.15.5 and the additivity of abelian integrals ($\sum_P \operatorname{ord}_P(f) I(P) = 0$ for every rational function $f$). For $J$ the constant terms coming from the second kind must be kept: if $f = ct^k(1 + O(t))$ at $O$ with $k = \operatorname{ord}_O f$, then

$$\sum_{P \neq O} \operatorname{ord}_P(f)\, J(P) = \operatorname{Res}_O\Big(\log_2 \frac{f}{ct^k}\, \eta\Big).$$

This is the global symbol identity $\sum_x \operatorname{Res}_x((df/f)\Phi_j) = \langle [\eta_j], \Psi(df/f)\rangle = 0$ of [BB12, Section 2], after an integration by parts at $O$ that uses the normalization of $\Phi_j$; the leading term $ct^k$ is divided out, since otherwise $\log_2 f$ would contain $\log_2 t$. For the six functions of Lemma 3.15.5, in the order listed there, the residue vectors are $(0,0), (0,0), (-1,-1), (0,0), (-1,1), (-4,0)$; only the coefficients of $t$ and $t^2$ of the normalized logarithms are needed, and they are read off from (12) (certificate 1.1.15b). Solving the resulting linear relations gives the formulas. □

The base divisors are $D - O$ and $F_1 - O$. The integral sections of $D$, $F_1$ and $E$ are pairwise disjoint at every prime, and none of them meets $\bar{O}$ (Lemma 3.15.8(i)). So $\omega_1$ is primitive at $D$ and $F_1$ (that is, $n = 0$ in Lemma 3.15.8(iii)), all local terms away from 2 of the heights among $D - O$ and $F_1 - O$ vanish, and by [CG89] the global heights among these two divisors equal $\mathcal{H}$.

**Lemma 3.15.11.** *For $P \in \{D, F_1\}$ put $k_1(P) = \int_B^{F_1} \nu_P$ and $k_2(P) = \int_D^{G} \nu_P$. Then*

$$K(P,E) = \frac{k_1(P) + 2k_2(P)}{13}, \qquad K(P,F_1) = \frac{7k_1(P) + k_2(P)}{13}, \qquad K(P,D) = -2K(P,E).$$

*Proof.* By [Gro86, BB15] and the symmetry of $h_2$, $\sum_Q \operatorname{ord}_Q(f) K(P,Q) = h_2(P - O, \operatorname{div} f) = \log_2\big(f[P]/f[O]\big)$, where $f[\cdot]$ is the value normalized by the chosen tangent vectors (the first equality holds because $\sum_Q \operatorname{ord}_Q(f) I(Q) = 0$). We use the functions $x$, $y/x$ and $(x+y)(y-x)y/((x+1)x^4)$, with divisors $D + 2E - 3O$, $B + F_1 - E - O$ and $G + F_1 - 5E + 3O$. For $P = D, F_1$ the ratio of the normalized value at $P$ to the leading coefficient at $O$ is always of the form $\pm 2^m$, so all these logarithms are 0, and the formulas follow as in Lemma 3.15.10. In the tiny integrals the poles are subtracted algebraically: on the disk of $D$, with $x = s$ and $y = sV$, $\nu_D - dx/x = -2V^2\omega_1$, and on the disk of $B$ and $F_1$, $\nu_{F_1} - dx/(x-1) = \frac{2y(x+1)}{z+1}\omega_1$; the subtracted logarithms take values $\log_2(\pm 2^m) = 0$. □

**Lemma 3.15.12.** *Let $L$ be the matrix with rows $I_D, I_{F_1}$, let $B_h = \big(K(P,Q) - J(P)I(Q)^{\mathsf T}\big)_{P,Q\in\{D,F_1\}}$, and $M = L^{-1}B_h(L^{-1})^{\mathsf T}$. Then $v_2(\det L) = 3$, $B_h$ is symmetric, and*

$$I_E \equiv (2,0), \quad I_{F_1} \equiv (2,22), \quad J_E \equiv (60,44), \quad J_{F_1} \equiv (62,30), \quad M \equiv \begin{pmatrix} 56 & 19 \\ 19 & 53 \end{pmatrix} \pmod{64}.$$

*In particular $M \in M_2(\mathbb{Z}_2)$, $I_E, I_{F_1} \in 2\mathbb{Z}_2^2$ and $J_E \in 4\mathbb{Z}_2^2$. Moreover* $\operatorname{rank} J(\mathbb{Q}) = 2$, *and $h(P,Q) = I(P)\,M\,I(Q)^{\mathsf T}$ for all $P, Q \in J(\mathbb{Q})$, where $I$ is extended additively to $J(\mathbb{Q})$.*

*Proof.* The values are computed by exact arithmetic modulo $2^{40}$ (certificate 1.1.15c); a 70-bit computation in Magma gives the same values (certificate 1.1.15d). Since $v_2(\det L) = 3$, the logarithms of $D$ and $F_1$ are independent, so $\operatorname{rank} J(\mathbb{Q}) \geq 2$, and with Lemma 3.15.4 the rank is 2. Then $\log\colon J(\mathbb{Q}) \otimes \mathbb{Q}_2 \to \mathbb{Q}_2^2$ is an isomorphism, and by [CG89] the bilinear form $h$ is determined by its values on $D, F_1$, which form the matrix $B_h$ by the remark before Lemma 3.15.11. No integral basis of $J(\mathbb{Q})$ and no saturation is needed. □

**Step 6: the quadratic Chabauty function on the four disks.** By Lemmas 3.15.9 and 3.15.12, the function

$$q(P) = \tau_*(P) - I(P)\,M\,I(P)^{\mathsf T} - I(P)\,M\,I_E^{\mathsf T}$$

vanishes at every $P \in \mathcal{U}(\mathbb{Z})$. It involves both the self-height and the cross-height with $E$. By Lemma 3.15.7,

$$dq = -\sum_{i=1}^{2} \omega_i \Big(2J_i(P) + J_i(E) + \sum_{j=1}^{2} M_{ij}\big(2I_j(P) + I_j(E)\big)\Big).$$

Solving (11) over $\mathbb{F}_2$ gives the four points $(1,1,1)$, $(1,0,0)$, $(0,0,0)$, $(0,0,1)$; so $\mathcal{U}(\mathbb{Z}_2)$ is the union of four residue disks, with centres and parameters

| centre $P_0$ | parameter $s$ | known points | $u$ of the second point ($s = 2u$) |
|---|---|---|---|
| $A$ | $y+1$ | $A,\ C_1$ | $1$ |
| $B$ | $x+1$ | $B,\ F_1$ | $1$ |
| $D$ | $x$ | $D,\ G$ | $1$ |
| $E$ | $x/y = y/z$ | $E,\ H$ | $-1/3$ |

Each parameter is primitive over $\mathbb{Z}_2$, and $s \in 2\mathbb{Z}_2$ describes the whole disk. The disk of $D$ is given by $V + sV^3 + s^2 - 1 = 0$, $V(0) = 1$, $x = s$, $y = sV$, $z = sV^2$, and the disk of $E$ by (14). On the disks of $A$ and $B$ the derivative of the equation with respect to $x$, resp. $y$, is odd, so Newton's method gives a unique series in $\mathbb{Z}_2[[s]]$. On all four disks $\omega_i/ds$ and $\eta_i/ds$ lie in $\mathbb{Z}_2[[s]]$.

Since the centres are integral points, $q(P_0) = 0$, and integrating $dq$ with constant term 0 gives

$$q_{P_0}(2u) = \sum_{n\geq 1} c_{P_0,n} u^n.$$

**Lemma 3.15.13.** *The first seven coefficients, modulo 32, are as follows (certificate 1.1.15c).*

| $P_0$ | $e$ | $c_1$ | $c_2$ | $c_3$ | $c_4$ | $c_5$ | $c_6$ | $c_7$ |
|---|---|---|---|---|---|---|---|---|
| $A$ | 2 | 20 | 28 | 16 | 16 | 16 | 0 | 0 |
| $B$ | 3 | 24 | 24 | 0 | 16 | 0 | 0 | 0 |
| $D$ | 2 | 20 | 12 | 0 | 16 | 16 | 0 | 0 |
| $E$ | 2 | 20 | 4 | 8 | 0 | 16 | 0 | 0 |

*Proof.* certificate 1.1.15c computes these values by polynomial arithmetic over $\mathbb{Z}/2^{40}\mathbb{Z}$ with series of length 64; every series that is inverted has odd constant term, and since the $n$-th term of an integral is $a_{n-1}2^n/n$, the 2-part of $n$ is split off first and only odd parts are inverted. No floating-point approximation is used. Write $\lambda(n)$ for the integer with $2^{\lambda(n)} \leq n < 2^{\lambda(n)+1}$. The terms omitted from the tiny integrals are those with $n \geq 62$, and their valuations are at least $n - v_2(n) \geq n - \lambda(n) \geq 57$.

The entries of $L^{-1}$ have valuation at least $-2$ and those of $B_h$ at least 2, so errors of valuation at least 40 in $L$ and $B_h$ change $M$ only in valuation at least 36: $L^{-1}(\delta B_h)(L^{-1})^{\mathsf{T}}$ has valuation at least $-2+40-2$, and $\delta(L^{-1}) = -L^{-1}(\delta L)L^{-1}$ has valuation at least 36 while $B_h(L^{-1})^{\mathsf{T}}$ has valuation at least 0. So at most four bits are lost, and the five bits needed for the table are guaranteed. □

**Lemma 3.15.14.** *On each of the four disks, $v_2(c_{P_0,n}) \geq n+1-v_2(n)-\lambda(n-1)$ for $n \geq 2$. In particular this bound is at least 4 for $n \geq 8$, and the series converges on $\mathbb{Z}_2$.*

*Proof.* The series coefficients of $\omega_i, \eta_i$ are integers. At the centres, $I(P_0) \in 2\mathbb{Z}_2^2$ and $J(P_0) \in \mathbb{Z}_2^2$, by Lemmas 3.15.10 and 3.15.12; moreover $M$ is integral, $I_E \in 2\mathbb{Z}_2^2$ and $J_E \in 2\mathbb{Z}_2^2$. Hence the constant term of the bracket in $dq$ lies in $2\mathbb{Z}_2$, and the non-constant terms are integral combinations of twice the integrals of integral series. In such an integral the denominator of the coefficient of degree $k \geq 1$ divides $k$, so the coefficient of $s^{n-1}$ in $dq/ds$ has valuation at least $1-\lambda(n-1)$. Integrating once more and substituting $s = 2u$ adds $n - v_2(n)$. If $n = 2^k$ with $k \geq 3$, the bound is $2^k + 2 - 2k \geq 4$; if $2^k < n < 2^{k+1}$, then $v_2(n) \leq k-1$ and the bound is at least $n+2-2k \geq 2^k+3-2k > 4$. □

**Lemma 3.15.15.** *Each of the four residue disks contains exactly two points of $\mathcal{U}(\mathbb{Z})$, namely the two known points of the table.*

*Proof.* By Lemmas 3.15.13 and 3.15.14, for the whole series

$$2^{-e}q_{P_0}(2u) \equiv u^2 + u \pmod 2, \qquad e_A = e_D = e_E = 2, \quad e_B = 3.$$

Write $2^{-e}q_{P_0}(2u) = \sum_{n\geq 1} b_n u^n$. Then $b_n \in \mathbb{Z}_2$, $b_n \to 0$, $b_1$ and $b_2$ are units and $b_n \in 2\mathbb{Z}_2$ for $n \geq 3$, so by [Str28] the series has at most two zeros in $\mathbb{Z}_2$. The two known points lie at $u \equiv 0$ and $u \equiv 1 \pmod 2$, and they are zeros of $q$. (The 70-bit computation certificate 1.1.15d gives the same exponents $e$ and reductions.) □

*Proof of Theorem 3.15.1.* By Lemma 3.15.15, $\mathcal{U}(\mathbb{Z}) = \{A, B, C_1, D, E, F_1, G, H\}$. By Lemma 3.15.2, every integer solution with $x \neq 0$ lifts to one of these points with $x \neq 0$, which gives $(-1,-1)$, $(-1,0)$, $(-1,1)$, $(1,0)$, $(2,-2)$, $(4,-6)$, and the only solution with $x = 0$ is $(0,0)$. The genus and the rank are Lemmas 3.15.3 and 3.15.12. □

## 4 Ten further affine quartic equations

Of the thirty equations in Table 1, six were settled in the literature cited there and fourteen in Section 3. The ten that remain open at this stage are listed in Table 8. We give them labels L1–L5 and R1–R5 for convenience.

Table 8: The ten equations from Table 1 treated in this section.

| | | | |
|---|---|---|---|
| L1 | $x^4+y^3+xy-1=0$ | R1 | $x^4-y^3+xy+x+1=0$ |
| L2 | $x^4+y^3+x+2y=0$ | R2 | $x^4+y^3+xy-3=0$ |
| L3 | $x^4+y^3+x-y-2=0$ | R3 | $x^4+y^3+x-2y-1=0$ |
| L4 | $x^4+y^3+x+y+2=0$ | R4 | $x^4+y^3+xy+x-1=0$ |
| L5 | $x^4+y^3+x+y-2=0$ | R5 | $x^4+y^3+x+2y+1=0$ |

We use a common bitangent descent on the ten Jacobians. Their ranks range from one to four, and the individual proofs are arranged in increasing order of rank.

| Notation | Meaning in the common descent |
|---|---|
| $O, J, V$ | the rational hyperflex, the Jacobian and its geometric 2-torsion |
| $K$, $h_K$, $\mathfrak{a}_2$ | bitangent field, its class number and an ideal representing a class of order two |
| $S, S_0$ | primes inspected for ramification, primes used for the finite local images |
| $L, W$ | product of local squareclass spaces and the image of global squareclasses in it |
| $d, j, k$ | local Kummer dimension, dimension modulo $W$, bound for the strict kernel |
| $R_0, m$ | regulator of the exhibited units and their index in the full unit group |

### 4.1 The curves and the bitangent descent

The rational hyperflex $O = (0 : 1 : 0)$ gives the embedding $P \mapsto [P - O]$ into each Jacobian. Table 9 records the rank bounds, including the contribution of global classes invisible to the local evaluations.

Write the original affine equation as $F = x^4 + \sigma y^3 + (ax + c)y + bx + d_0 = 0$. In the monic cubic in the ordinate $\sigma y$ put $(A, B, C, D) = (\sigma a, b, \sigma c, d_0)$. The line at infinity cuts out $4O$. An affine bitangent $\sigma y = mx + n$ cuts out twice a quadratic divisor, so that substitution gives the square $(x^2 + vx + w)^2$. Comparing coefficients gives

$$2v = m^3, \quad 2w = 3m^2n + Am - v^2, \quad 2vw = 3mn^2 + An + Cm + B, \quad w^2 = n^3 + Cn + D.$$

We use the bitangent evaluation of Proposition A and [BPS16]. Section 4.3 verifies the required cohomological injectivity. The 27 affine bitangents give one degree-27 field $K$. The attached data give its irreducible defining polynomial, a certified integral basis, and the elements $m, n$. Checking the displayed identities in $K$ verifies the bitangents, since $m$ has degree 27 and a smooth plane quartic has 28 odd theta characteristics. All the fields here have signature $(3, 12)$.

The rational Kummer map sends $J(\mathbb{Q})/2J(\mathbb{Q})$ injectively to $H^1(\mathbb{Q}, V)$ with $V = J[2]$. Let $S$ consist of 2 and the bad odd primes, and let $S_0$ consist of 2, augmented by 5 on R5. The coefficients in the table refer to the equations in their original coordinates.

| Curve | $(\sigma, a, b, c, d_0)$ | Odd primes of bad reduction | $S_0$ | $q_9$ |
|---|---|---|---|---|
| L1 | $(1, 1, 0, 0, -1)$ | $383, 3368011$ | $\{2\}$ | 3 |
| L2 | $(1, 0, 1, 2, 0)$ | $5, 347, 1246013$ | $\{2\}$ | 29 |
| L3 | $(1, 0, 1, -1, -2)$ | $11, 7333, 944077$ | $\{2\}$ | 17 |
| L4 | $(1, 0, 1, 1, 2)$ | $24571, 3669073$ | $\{2\}$ | 11 |
| L5 | $(1, 0, 1, 1, -2)$ | $94022627947$ | $\{2\}$ | 7 |
| R1 | $(-1, 1, 1, 0, 1)$ | $5, 41, 907, 6911$ | $\{2\}$ | 3 |
| R2 | $(1, 1, 0, 0, -3)$ | $3, 7, 5147, 8700121$ | $\{2\}$ | 61 |
| R3 | $(1, 0, 1, -2, -1)$ | $5, 1051, 237053$ | $\{2\}$ | 11 |
| R4 | $(1, 1, 1, 0, -1)$ | $31, 223, 199813$ | $\{2\}$ | 179 |
| R5 | $(1, 0, 1, 2, 1)$ | $5, 11, 31, 1662103$ | $\{2, 5\}$ | 13 |

Here $q_9$ is a good prime at which the degree-27 bitangent polynomial has three irreducible factors of degree nine. The bad primes are obtained by factoring the discriminant of the branch polynomial $-4(Ax + C)^3 - 27(x^4 + Bx + D)^2$ and testing the affine singular ideal $(F, F_x, F_y)$ at its prime divisors. The verifier also checks which fibers are smooth. At good odd primes the Kummer classes are unramified. The bad odd fibers outside $S_0$ are geometrically irreducible, with one ordinary node of thickness one. A single ordinary double point forces geometric irreducibility here. Two different components would have total intersection multiplicity at least three by Bézout, whereas one ordinary transverse node contributes at most one. A repeated component would give a positive-dimensional singular locus. Thus the regular semistable model has trivial component group. Over the maximal unramified extension, multiplication by two is onto on the connected smooth special fiber and on the formal kernel. Consequently their local Kummer classes are unramified in $H^1(\mathbb{Q}_p, V)$ even if inertia acts nontrivially on $V$. On the bitangent field this implies even valuations outside $S_0$. The projective closure is smooth at $O$ in every characteristic. The file of singular fibers supplies the node, nonzero Hessian determinant test and the lift test for the thickness.

On R5 at 5 the unique node reduces to $(1,4)$. Its Hessian determinant is nonzero modulo 5. Its critical lift is $(11,4)$ mod 25, and $F(11,4) \equiv 100 \pmod{125}$. The critical value has valuation two, giving a node of thickness two. The geometric component group is therefore $\mathbb{Z}/2\mathbb{Z}$; this accounts for the local condition at 5.

Put $L = \prod_{v|S_0,\infty} K_v^\times / K_v^{\times 2}$. The product of the local quadratic Hilbert symbols is a nondegenerate bilinear pairing on $L$. At an odd prime a pair of squareclasses of even valuation has trivial Hilbert symbol. Global reciprocity therefore puts the localizations of all elements of even valuation outside $S_0$ in a totally isotropic subspace of $L$. We exhibit half its dimension using units, generators of the primes above $S_0$ and, where specified, one generator of a squared ideal. Hence this exhibited space $W$ equals its orthogonal complement, and contains every possible global localization.

We check connectedness over the reals before computing the finite local images. On R1 the discriminant in the monic ordinate is $4x^3 - 27(x^4 + x + 1)^2 < 0$. For $0 \le x \le 1$ use $x^{3/2} \le 1$ and for $x \ge 1$ use $x^{3/2} \le x^4$. R4 has two simple folds in the $x$-projection. The cubic discriminant $-4x^3 - 27(x^4 + x - 1)^2$ has exactly two real roots in $(-17/13, -13/10)$ and $(-8/7, -25/22)$ by Sturm's rule. The constant terms of the cubic have opposite signs at the folds, so those folds join the middle branch to opposite outer branches. Only one point is added at infinity. For the separated equations one can project to the $y$-axis. The range of $x^4 + x$ is $[-3/4^{4/3}, \infty)$. On R5 and L2, $y^3 + 2y$ is strictly increasing. On R3 the local maximum of $y^3 - 2y - 1$ equals $\frac{4}{3}\sqrt{2/3} - 1 < 3/4^{4/3}$, so the admissible values again form one ray. The two real inverse branches of $x^4 + x$ join at its minimum. For L3 the two extrema of $y^3 - y - 2$ likewise lie below $3/4^{4/3}$, and on L4 and L5 the cubic in $y$ is strictly increasing. On R2 and L1 the discriminant has two simple folds with opposite signs of the constant term, as checked in Sections 4.11 and 4.18. Since a real curve with $s > 0$ components has $2^{s-1}$ components in its real Jacobian [GH81, Prop. 3.2(2)], all ten real Kummer images vanish.

At each $p \in S_0$ we evaluate rational local divisor classes using factors of $p$-adic line intersections. The functions and group computations below show that these account for the whole local Kummer space. Write $d$ for its dimension, summed over $S_0$, and $j$ for its image dimension modulo $W$. The visible global dimension is at most $d - j$. The remaining kernel consists of strict classes, whose evaluated characters are everywhere unramified and split at the real places and above $S_0$. The ideal-class pairing and the local calculations below bound this kernel.

## 4.2 The strict kernel

Let $V = J[2](\overline{\mathbb{Q}})$. The rational odd theta characteristic $2O$ determines a quadratic form $q$ of minus type on this six-dimensional $\mathbb{F}_2$-space. Its polarization is the Weil pairing $b$. The other odd theta characteristics correspond to the set $T = \{w \neq 0 : q(w) = 0\}$ of size 27. Write $M = \mathrm{Map}(T, \mathbb{F}_2)$ and

$$e : V \longrightarrow M, \qquad e(v)(w) = b(v, w).$$

If the contact divisor of the affine bitangent is $E$, then $\mathrm{div}(mx + n - \sigma y) = 2(E - 2O)$ and $[E - 2O] \in V$. Their evaluation on a divisor class is the Kummer cocycle followed by $e$ and Shapiro's identification $H^1(\mathbb{Q}, M) = H^1(K, \mathbb{F}_2)$. The leading coefficient at $O$ in the parameter $x/(\sigma y)$ is one. This is also obtained directly from the defining property of the Weil pairing.

**Lemma 4.2.1.** *For $j = 1, 2, 3$ the multilinear map $\mathrm{Tr}(e(v_1) \cdots e(v_j))$ is identically zero, where the product is coordinatewise and the trace sums the 27 coordinates.*

*Proof.* Sum $(1 + q(w)) \prod_i b(v_i, w)$ over all 64 vectors $w$. It has degree at most five in six binary variables. Every monomial misses a variable and its sum vanishes in $\mathbb{F}_2$. The term at zero vanishes as well. The argument below uses only these three degrees. For four factors the trace can equal one. In symplectic coordinates write $q = \sum_{i=1}^{3} x_i y_i + \ell$ with $\ell$ linear. The four linear forms $x_1, y_1, x_2, y_2$ are evaluations under the nondegenerate pairing $b$. In $(1 + q)x_1 y_1 x_2 y_2$ the monomial $x_1 y_1 x_2 y_2 x_3 y_3$ has coefficient one, so the sum over all vectors is one. □

**Lemma 4.2.2.** *Take a finite set $S$ of finite rational primes containing 2 and all ramified primes of $V$. Put $U = \mathrm{Spec}\, \mathbb{Z}[1/S]$, and $U_K = \mathrm{Spec}\, \mathcal{O}_K[1/S]$. Let $c, d \in H^1(U, V)$, and let $\chi = e_* c$, $\alpha = e_* d$ under Shapiro.*

*Suppose $\chi$ is unramified at all places and splits above $S$ and at the real places. Suppose $c$ is locally zero at 2 and at infinity. At each other prime of $S$ suppose either $c$ is locally zero or both $c, d$ are unramified as cocycles (their restrictions to inertia vanish in cohomology). If $(\alpha) = I^2$ on $U_K$, then $\chi(I) = 0$ in additive notation.*

*Proof.* Write $S_K$ for the places over $S$, together with the archimedean places. Since 2 is invertible on $U_K$ and all primes over 2 are removed, the comparison of étale and Galois cohomology for $S$-integers identifies the cohomology of our finite locally constant 2-primary sheaves with that of the Galois group unramified outside $S_K$. We use Tate cochains at real places in the compact-support sequence [Mil06, Ch. II, §§2–3]. Write cochains additively and identify $\mu_2$ with $\mathbb{F}_2$.

*The ideal pairing.* In the Kummer sequence $1 \to \mu_2 \to \mathbb{G}_m \xrightarrow{2} \mathbb{G}_m \to 1$, the class of $\alpha$ maps to the line bundle of $I$ or its inverse. Indeed, a local generator of $I$ removes the square of the local uniformizer factor from $\alpha$. The ratios of these generators are the transition functions of that bundle. The two choices have the same Chern class modulo two. Mapping the sequence $1 \to \mu_2 \to \mu_4 \xrightarrow{2} \mu_2 \to 1$ to the Kummer sequence by inclusion on the middle and right terms gives

$$\beta_\mu(\alpha) = c_1(I) \quad \text{in } H^2(U_K, \mu_2).$$

Since $\chi$ splits at $S_K$, fix a lift $\widetilde{\chi} \in H^1_c(U_K, \mathbb{F}_2)$. For a prime ideal away from $S_K$, its Chern class is the Gysin image of 1 over its residue field. The projection formula for the arithmetic trace identifies its pairing with $\widetilde{\chi}$ with evaluation of $\chi$ at Frobenius. Additivity on divisors gives

$$\mathrm{inv}_{U_K}(\widetilde{\chi} \smile c_1(I)) = \chi(I) \quad \text{in } \mathbb{F}_2.$$

This depends only on $\chi$. Equivalently, changing the lift adds boundary terms from local degree zero, paired with the restrictions of $c_1(I)$. Those restrictions vanish because a line bundle on a field is trivial.

*A cochain for the boundary.* On lifting a bit $a(\gamma)$ to 0 or 1 modulo four, the ordinary coboundary divided by two gives the carry $a(\gamma)a(\delta)$ in addition. The action on a fourth root of unity adds $[-1](\gamma)a(\delta)$. Thus $\beta_\mu(a) = a \smile a + [-1] \smile a$ in cohomology (compare [PR11]). To carry out the trace downstairs, use the finite étale map $U_K \to U$. Its direct image of $\mathbb{F}_2$ is the algebra $M$ with coordinatewise multiplication. Shapiro identifies products with products in this algebra, and corestriction is induced by the sum of the coordinates. Put $a = e(c)$, $n = e(d)$ for cocycle representatives, and let $z$ be the diagonal cocycle of $-1$. The Bockstein has representative $B(n) = n \smile n + z \smile n$ in $M$; this also follows by lifting the bits in each coordinate before permuting them. In particular $\mathrm{Tr}(a \smile B(n)) = 0$ as a cochain. The arguments entering each coordinatewise trace are evaluations of two or three vectors of $V$, after the Galois translates in the cup product. Lemma 4.2.1 applies to all such vectors.

*The boundary terms.* With $C^\bullet$ the global continuous cochains and $C_v^\bullet$ the local ones, the compact-support complex is the cone of $C^\bullet \to \bigoplus_v C_v^\bullet$, shifted by $-1$. In characteristic two a cochain of degree $i$ is $(a, (m_v))$ with $\deg m_v = i - 1$, and its differential is $(\delta a, (a_v + \delta m_v))$. Its right cup product with an ordinary cocycle $B$ is $(a \smile B, (m_v \smile B_v))$. Hence we may choose $\delta m_v = a_v$ and need only show that each $\mathrm{Tr}(m_v \smile B(n_v))$ has zero class locally. At a place where $c_v$ is a coboundary take $m_v$ to be the evaluation of a $V$-valued primitive. The trace vanishes term by term by the same lemma, including at real places.

At any remaining place $v$, inflation–restriction provides representatives $c'_v, d'_v$ inflated from the procyclic residue Galois group, with values in $V^{I_v}$. If $c'_v = c_v + \delta s$, replace $m_v$ by $m'_v = m_v + e(s)$. The change in its traced product is zero by the trace lemma. Also $\delta m'_v = e(c'_v)$, so inertia fixes $m'_v$. Write $n' = e(d'_v) = n_v + \delta b$ with $b$ the evaluation of a $V$-valued zero-cochain. The cochain identity

$$B(n') - B(n_v) = \delta L, \qquad L = b \smile n_v + n' \smile b + z_v \smile b$$

follows from the cup-product differential rule. Consequently the change of local term is the coboundary $\delta \,\mathrm{Tr}(m'_v \smile L)$: the other summand $\mathrm{Tr}(\delta m'_v \smile L)$ is zero, again by the two- and three-factor trace identities. Now $z_v$ is unramified because $v$ is odd. The resulting traced local two-cocycle is inflated from $\widehat{\mathbb{Z}}$, whose second cohomology with coefficients $\mathbb{F}_2$ is zero. Thus the global trace cochain vanishes and all its local components are coboundaries. Its compactly supported class is zero. Compatibility of the arithmetic invariant with corestriction proves $\chi(I) = 0$. □

In particular, suppose $|\mathrm{Cl}(K)| \leq 3$ and every prime above $S$ is principal. If a strict Kummer class $c$ gives a nonzero $\chi$, then $\mathrm{Cl}(K)$ has order two and $\chi$ identifies it with $\mathbb{F}_2$. Apply the lemma with $d = c$. It says the half-ideal of its squareclass is principal. Hence the squareclass is represented by a unit. An injective localization on the unit squareclasses then forces $\chi = 0$, because the class is locally trivial at the test places. Injectivity of $e_*$ on global cohomology forces $c = 0$.

**An explicitly visible ideal class of order two.** For L2 and R3 let $\mathfrak{a}_2$ be the exhibited ideal of norm 6410024 or 291495872421, respectively. It satisfies $\mathfrak{a}_2^2 = (g)$. Let $\chi_0$ be the exhibited everywhere-unramified quadratic character with $\chi_0(\mathfrak{a}_2) = 1$ in additive notation. Thus $[\mathfrak{a}_2]$ has exact order two. Every prime above $S$ has class in $\langle \mathfrak{a}_2 \rangle$. The generators of $W$ have one linear dependence after localization. The corresponding global squareclass gives $\chi_0$. If $h_K \leq 7$, take a strict $c$ whose character $\chi$ vanishes on $\mathfrak{a}_2$. If $\chi \neq 0$, it factors through $\mathrm{Cl}(K)/\langle \mathfrak{a}_2 \rangle$, which has order at most three and must therefore have order two. Its kernel on $\mathrm{Cl}(K)$ equals $\langle \mathfrak{a}_2 \rangle$. Also $\chi$ splits above all of $S$. Lemma 4.2.2, with $d = c$, shows that the half-ideal belongs to $\langle \mathfrak{a}_2 \rangle$ (discarding primes over $S$ changes it only by this subgroup). All valuations are even, so its squareclass is a unit times 1 or $g$ after division by a square. The units are already a basis modulo squares by the independent residue tests at exponent two. Such a class belongs to the explicit space. Its strict kernel is generated by $\chi_0$, which is nontrivial on $\mathfrak{a}_2$. It follows that strict classes inject under $\chi \mapsto \chi(\mathfrak{a}_2)$ and have dimension at most one.

### 4.3 The bitangent action and local dimensions

For a group $G$ acting on $0 \to V \to M \to M/e(V) \to 0$, the kernel on $H^1$ is the cokernel of $M^G \to (M/e(V))^G$. It depends only on the finite permutation action. Globally, irreducibility makes the 27-element action transitive. Factoring at a good prime supplies an element $g$ with three 9-cycles. Its action has order nine because $T$ spans $V$. Since 9 is odd, each $g$-fixed coset of $e(V)$ has a $g$-fixed representative. It is a union of 9-cycles. Up to adding the constant function, every nonconstant possibility is a single cycle.

Here and in the local calculation one can use

$$q(z) = z_1z_2 + z_3z_4 + z_5z_6 + z_5 + z_6.$$

Generate the full orthogonal group by the matrices $z \mapsto z + b(z, a)a$ for $q(a) = 1$. The list has size $51,840$, the order of $O_6^-(2)$. For each element with cycle pattern $(9, 9, 9)$, record each cycle indicator modulo the 64 evaluations. The resulting 2,880 cosets form one orbit of the full group, with stabilizer of order 18. A group transitive on 27 objects has order divisible by 27, so cannot fix any of these cosets. The kernel on global $H^1$ vanishes. The primes $q_9$ in Section 4.1 certify the required cycle type in all ten fields.

On R1, R2, R4 and L1 the four dyadic factors have degrees $2, 5, 10, 10$. The group fixes the two-element subset. The two pair stabilizers in the orthogonal group have orders 384 and 240, according to the pairing between the two points. The first cannot contain an element of order five. Among all 535 subgroups of the second, 15 have the required orbits. Each has $\dim V^G = 1$ and trivial kernel on $H^1$. To reproduce a kernel dimension using generators $g_1, \ldots, g_s$, form the binary matrices for $m \mapsto ((g_j - 1)m)_j$. Compute $\dim\{m : (g_j - 1)m \in e(V) \text{ for all } j\}$ and subtract $6 + \dim M^G - \dim V^G$.

For L2, L3, L4, L5, R3 and R5 there is a single prime of $K$ above 2, with ramification index 9 and residue degree 3. Each inertia orbit on $T$ has size nine. The normal wild 2-subgroup has equal-sized orbits inside such a transitive orbit, hence acts trivially. Tame inertia has cyclic image of order nine. Its action on $V$ has no fixed vector since the ninth cyclotomic polynomial has degree six and is irreducible over $\mathbb{F}_2$. The decomposition group is transitive on 27, and the preceding 9-cycle argument makes the local $H^1$ kernel zero. On R5 at 5 the decomposition group is cyclic, with orbit lengths $2, 5, 5, 5, 10$. Testing all elements of this cycle type gives kernel zero and $\dim V^G = 1$. Unramifiedness of its action follows from the certified field decomposition and the faithful permutation action. By Proposition A(5), $\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \dim V^G + 3 \cdot \mathbf{1}_{p=2}$.

The archive gives representatives of the local divisors and the exact binary matrices. Here is the calculation of each column. A local squareclass at $p$ is specified by valuation parities and the unit modulo squares in $(\mathcal{O}_K/\mathfrak{m})^\times$, with $\mathfrak{m} = 8\mathcal{O}_K$ at 2 and $\mathfrak{m} = 5\mathcal{O}_K$ at 5. Indeed $1 + 8\mathcal{O}_{K_v}$ consists of squares at a dyadic place. At an odd place $1 + p\mathcal{O}_{K_v}$ consists of squares. Real signs give three more coordinates. For local divisors take a power $t$ of $p$ and put $x = X/t^3$, $\sigma y = (\alpha X + \beta)/t^4$. Factor the resulting monic quartic to precision $p^{60}$. For a factor $f$ of degree $r$ with complementary factor $h$, the polynomial congruence lifts with accuracy at least $60 - v_p \operatorname{Res}(f, h)$ because $60 > 2v_p \operatorname{Res}(f, h)$. For the divisor of degree $r$ cut out by $f$, subtract $rO$. Since $t^4$ is a square, its bitangent evaluation modulo squares is

$$\prod_{f(s)=0} \big((tm - \alpha)s + t^4 n - \beta\big).$$

The valuation of the coefficient error is checked at every relevant prime of $K$, and exceeds the value of the product by more than $2v(2)$. The archived rows reach exactly the dimensions of the local Jacobian quotients, so give the full local images. Gaussian elimination gives Table 9. Here $d$ is the dimension of the local Kummer image at $S_0$, $j$ its dimension modulo $W$, and $k$ the upper bound for the kernel of localization. Thus the rank is bounded by $d - j + k$. On L1 all four local directions are realized by rational points, which gives $j = 0$; the upper bound $d = 4$ already suffices once $k = 0$. The order-two ideal, when needed, is denoted by $\mathfrak{a}_2$ for every field. In L2, L5 and R3 the seventeen exhibited global

Table 9: Descent dimensions and ranks for the curves in Table 8. The class-number column gives the bound used in the descent.

| Curve | $\dim L$ | $\dim W$ | $d$ | $j$ | $d - j$ | $k$ | $h_K \le$ | Rank |
|---|---|---|---|---|---|---|---|---|
| L1 | 38 | 19 | 4 | 0 | 4 | 0 | 7 | 4 |
| L2 | 32 | 16 | 3 | 2 | 1 | 1 | 7 | 2 |
| L3 | 32 | 16 | 3 | 1 | 2 | 0 | 3 | 2 |
| L4 | 32 | 16 | 3 | 1 | 2 | 0 | 3 | 2 |
| L5 | 32 | 16 | 3 | 1 | 2 | 1 | 7 | 3 |
| R1 | 38 | 19 | 4 | 3 | 1 | 0 | 3 | 1 |
| R2 | 38 | 19 | 4 | 3 | 1 | 0 | 7 | 1 |
| R3 | 32 | 16 | 3 | 1 | 2 | 1 | 6 | 3 |
| R4 | 38 | 19 | 4 | 3 | 1 | 0 | 2 | 1 |
| R5 | 42 | 21 | 4 | 2 | 2 | 0 | 3 | 2 |

generators have localized rank sixteen. Where used, reduction of the fourteen units and $-1$ at finite residue fields proves their independence modulo squares. Dirichlet's theorem then gives the full unit group modulo squares.

### 4.4 Certifying the auxiliary class numbers

Put $D = |\mathrm{disc}(K)|$, $h = |\mathrm{Cl}(K)|$, and $\kappa = \operatorname{Res}_{s=1} \zeta_K(s)$. Let $R_0$ be the regulator of the fourteen displayed units and $m$ their index in the free part of $\mathcal{O}_K^\times$. The real embeddings imply that the torsion subgroup is $\{\pm 1\}$. The class number formula gives

$$\frac{h}{m} = \frac{\kappa}{\kappa_0}, \qquad \kappa_0 = 4(2\pi)^{12} R_0 / \sqrt{D}.$$

The units have exact norm $\pm 1$. The regulator determinant is enclosed using isolated complex roots and 960-bit interval arithmetic. There are two ways to start this calculation. For L1, L2, R1, R3, R4 and R5 a preliminary bound on $h$ and a lower bound on $\kappa$ bound $m$. For L3, L4, L5 and R2 a smoothed partial zeta sum bounds $m$ directly (Section 4.5). Both routes finish with finite-field saturation of the units and an upper bound on $\kappa$. For every prime $\ell$ up to the certified upper bound for $m$, reduce the units into residue fields $\mathbb{F}_q$ with $q \equiv 1 \pmod{\ell}$. Discrete logarithms of their $(q-1)/\ell$ powers give a matrix of rank 14 modulo $\ell$, with rank 15 on including the torsion unit $-1$ when $\ell = 2$. This excludes each prime divisor of $m$ and shows $m = 1$. The upper residue bound can then be used to bound $h$ sharply.

| Row | $\kappa_0$ (approx.) | $\kappa >$ | $\kappa <$ | preliminary $h \le$ | $m <$ | final $h \le$ |
|---|---|---|---|---|---|---|
| L2 | .108441 | .0015575 | .82360 | 1,640 | 114,181 | 7 |
| R1 | 3.011344 | .04988 | 9.981 | 395 | 24,000 | 3 |
| R3 | .163791 | .00556 | 1.087 | 2,356 | 70,000 | 6 |
| R4 | 8.458898 | .01850 | 23.738 | 16 | 7,400 | 2 |
| R5 | 1.117216 | .002656 | 3.507 | 60 | 25,300 | 3 |

The preliminary Gaussian parameters $(X, c)$ are $(3,600,000,101)$ for R1, $(4,500,000,145)$ for R3, $(3,500,000,35)$ for R4 and $(1,200,000,50)$ for R5. The split-prime bounds for the degrees of the respective class fields are $395.798, 1178.369, 16.955, 60.215$. The residue calculations also use prime ideals without a splitting requirement, through $50,000,001$ for R1, $80,000,001$ for R3, $50,000,001$ for R4 and $12,000,000$ for R5. On L2, $3,304,745$ certified prime ideals through $X = 64,100,000$ give a quotient bound of $820.876$ at $c = 185$. The residue bounds use $X = 350,000,001$ for the lower endpoint and $120,000,001$ for the upper endpoint.

### 4.4.1 The preliminary class bound

Let $A_0$ be trivial on R1, R4 and R5, and $\langle [\mathfrak{a}_2] \rangle$ on R3 and L2. Take the subfield of the ordinary Hilbert class field corresponding to $A_0$. Its degree over $K$ is $H = h/|A_0|$. Its root discriminant and the proportion $1/9$ of real embeddings agree with those of $K$, and every prime ideal whose class lies in $A_0$ splits completely. Apply the Poitou explicit formula in its arbitrary-signature form to this field with $F(x) = e^{-(x/c)^2}/\cosh(x/2)$. The summed zero contribution is nonnegative across the whole critical strip. This follows from the positivity criterion underlying Miller [Mil14, Lemma 5.1]. For any certified set $\mathcal{P}$ of such prime ideals set

$$B = \gamma + \log(4\pi) + \tfrac{1}{9} - \tfrac{1}{27}\log D - \frac{(7/2)\zeta(3) + \pi^2/27}{c^2} + \frac{4}{27}\sum_{P\in\mathcal{P}}\sum_{q^k\le X}\frac{\log q}{q^k+1}e^{-(k\log q/c)^2}, \qquad q = N(P).$$

If $B > 0$, then $H \le 2c\sqrt{\pi}/(27B)$. The signature constants follow by integrating the two archimedean kernels with $F(x) = 1/\cosh(x/2)$. Replacing this by the Gaussian-weighted function costs at most the displayed $c^{-2}$ term, by $1 - e^{-s} \le s$. The two integrals of the error kernels are $\int_0^\infty x^2/\sinh x\,dx = 7\zeta(3)/2$ and $\int_0^\infty x^2/(2\cosh^2(x/2))\,dx = \pi^2/3$.

Each ideal certificate is an element $v \in P$. Either $(v) = P$ or $(v) = P\mathfrak{a}_2$, or each prime power dividing the positive integer $|N(v)|/N(P)$ is strictly smaller than $N(P)$ and within the certified base. Every prime ideal in $(v)/P$ has norm bounded by its corresponding rational prime power. Induction therefore proves $[P] \in A_0$. A subset above the completed base suffices for the displayed inequality, since all discarded terms are positive. The auxiliary norms bound a sum in a theorem about class numbers. The resulting rank bounds apply to integer points of every height.

### 4.4.2 The two-sided residue certificate

Define $G(s) = (\pi^{-s/2}\Gamma(s/2))^3((2\pi)^{-s}\Gamma(s))^{12}$ and $A(b) = (1+b)^{-1} + b^{-1} + \frac{1}{2}\log D + G'(1+b)/G(1+b)$. If $k_b(\rho) = \Re\big((1+b-\rho)^{-1}\big)$ and $x = k\log q$, the logarithmic derivative of the completed zeta function gives

$$\sum_\rho k_b(\rho) = A(b) - \sum_{P,k}\log(q)q^{-k}e^{-bx}.$$

Integration from 1 to $1+a$ gives the second exact identity

$$\log\kappa = \log(a(1+a)) + \frac{a}{2}\log D + \log\frac{G(1+a)}{G(1)} + \log\zeta_K(1+a) - \sum_\rho h_a(\rho), \quad h_a(\rho) = \log\left|\frac{1+a-\rho}{1-\rho}\right|.$$

The zeros include multiplicity. Both real-part sums converge absolutely. These are identities from the functional equation and the paired Hadamard product.

The coefficient files use rational $b$ and weights $w_b$. Write $K_w = \sum w_b k_b$ and $P_w(x) = \sum w_b e^{-bx}$. For an upper bound take $a = 3/10$. The verifier proves $K_w(\rho) + K_w(1-\bar{\rho}) \le h_a(\rho) + h_a(1-\bar{\rho})$ on the strip and $P_w(x) + e^{-ax}/x \le 0$ for $x \ge \log X$. Substitution in the identities then gives an upper bound using exactly the listed prime powers through $X$.

A separate rational certificate makes $K_w(\rho) + K_w(1-\bar{\rho}) \ge 0$ on the strip and strictly greater than a target in a small square adjacent to $s = 1$. The unknown Euler tail has $P_w(x) \ge 0$, and the explicit upper bound on $\sum_\rho K_w(\rho)$ is strictly less than the target. A zero in the square and its distinct reflected partner would violate this inequality. This proves the stated zero-free square without a hypothesis on the locations of other zeros. For R1, R3 and L2 another kernel majorizes the paired $h_a$ outside the excluded squares, with $P_w \ge 0$ on the unseen tail, giving the required lower residue bound. Alternatively, outside a square of radius $\delta$, $h_a \le C k_a$ for

$$v_\delta = 2a/\delta + (a/\delta)^2, \qquad C = a(1+v_\delta)\log(1+v_\delta)/v_\delta.$$

Indeed $h_a = \frac{1}{2}\log(1+z)$ where $z = a(2(1-\Re\rho)+a)/|1-\rho|^2 \le v_\delta$. Dividing by $k_a$ gives the indicated bound by monotonicity. This latter test suffices for R4 and R5.

For the strip bounds use harmonicity and reflection, checking the boundary $\Re\rho = 1$ and any edges of the excluded squares. At infinity the unscaled functions tend to zero uniformly. With $u = (\Im\rho)^2/(1+(\Im\rho)^2)$, each boundary kernel multiplied by $1+(\Im\rho)^2$ becomes $c/[c^2+(1-c^2)u]$ with $c = b$ or $1+b$. Adaptive interval subdivision and rational derivative bounds cover $0 \le u \le 1$. For the unknown prime tail put $z = e^{-x/100}$. The tests become polynomial inequalities on a compact interval after replacing $1/x$ by a one-sided bound where needed. The finite Euler contributions are rigorously enclosed by bins in $k\log q$. Each bin's integer multiplicity is weighted by $1/k$. The exact endpoint pairs, rational coefficients, prime norms and checking programs are in the supporting data. The approximate decimal bounds in the tables are rounded outwards.

For example, on L2 the coarse bound is $h \le 1640$. The lower residue bound and the regulator give $m \le 114180$. All 10804 primes up to 114180 are excluded as divisors of $m$ by 151257 independently checked residue evaluations. Thus $m = 1$. The upper residue bound gives $h \le 7$, and the kernel argument of Section 4.2 leaves at most one strict class. The same inequalities apply to the four other rows of this table. L1 uses this method with the parameters in Section 4.18.

## 4.5 Bounding the index of the units by a partial zeta function

Keep $D, h, \kappa_0$ and $m$ from Section 4.4 and put $U = \langle -1, \epsilon_1, \dots, \epsilon_{14}\rangle$. Choose an explicitly exhibited subgroup $B \subset \mathrm{Cl}(K)$ of order $b$. The point of restricting to this subgroup is that the residue of its partial zeta function contains $1/m$ and no unknown class number.

**Lemma 4.5.1.** *Put $0 < \delta \le 1/2$, $a > 0$, and $\lambda \in \mathbb{R}$. Suppose $Z \ge \zeta_K(1+\delta)$. Set*

$$S_B = \frac{1}{\sqrt{4\pi a}} \sum_{\substack{0 \ne I \subset \mathcal{O}_K \\ [I] \in B}} \frac{e^{-(\log NI - \lambda)^2/(4a)}}{NI}.$$

*Then $|S_B - b\kappa_0/m| \le E$, where*

$$C_\delta = \pi^{-3(1+2\delta)/2}(2\pi)^{-12(1+2\delta)} \left(\frac{\Gamma((1+\delta)/2)}{2\Gamma(1-\delta/2)}\right)^3 \left(\frac{\Gamma(1+\delta)}{\Gamma(2-\delta)}\right)^{12},$$

$$E = \frac{D^{1/2+\delta} Z C_\delta}{\pi} e^{a(1+\delta)^2 - (1+\delta)\lambda} \int_0^\infty e^{-at^2}(t+\delta)(t^2+\delta^2)^7(t^2+(1-\delta)^2)^6\,dt.$$

*Proof.* Average $L(1+s,\chi)$ over all characters of $\mathrm{Cl}(K)/B$. Character orthogonality selects precisely the ideals with class in $B$. On any vertical line $\Re(s) > 0$, termwise Gaussian Mellin inversion with

multiplier $e^{\lambda s+as^2}$ gives $S_B$. Move the line to $\Re(s) = -1-\delta$. The only pole crossed belongs to the trivial character at $s = 0$. Its averaged residue is $b\kappa_0/m$. The Gaussian decays like $e^{-a(\Im s)^2}$ on each bounded vertical strip, so the horizontal integrals tend to zero by the usual vertical-strip growth bound for Hecke $L$-functions.

An ordinary ideal-class character is unramified at every finite place and trivial at each archimedean connected factor and on each archimedean sign. Hence all these characters have the same gamma factor

$$G(z) = \{\pi^{-z/2}\Gamma(z/2)\}^3\{(2\pi)^{-z}\Gamma(z)\}^{12}.$$

The Hecke functional equation [RV99, Ch. VII, §4] and absolute convergence to the right of one give

$$|L(-\delta+it,\chi)| \le D^{1/2+\delta}Z\,|G(1+\delta-it)/G(-\delta+it)|\,.$$

For $0 < A \le B$, the beta integral gives $|\Gamma(A+iv)/\Gamma(B+iv)| \le \Gamma(A)/\Gamma(B)$, with equality of the ratios when $A = B$. Shift the real denominator once and the complex denominator twice by the gamma recurrence. Using $|\Gamma(A-iv)| = |\Gamma(A+iv)|$ gives the bound

$$C_\delta(t^2+\delta^2)^{15/2}(t^2+(1-\delta)^2)^6.$$

The beta comparisons apply because $(1+\delta)/2 \le 1-\delta/2$ and $1+\delta \le 2-\delta$. Finally $\sqrt{t^2+\delta^2} \le t+\delta$ for $t \ge 0$. Integrating the absolute value on the new line proves the claim. □

**Computing the upper error.** Take $s = 1+\delta$, $\delta = 1/10$, $a = 12$ and $T = 136$. Bound $\log\zeta_K(s)$ by starting with $27\log\zeta(s)$ and correcting every rational prime power $p^k \le X$. Its change in coefficient is $(\sum_{\mathfrak{p}\mid p,\ f_{\mathfrak{p}}\mid k} f_{\mathfrak{p}} - 27)/k \le 0$. Group these signed coefficients in bins $[j/2048, (j+1)/2048]$ of $k\log p$ and evaluate the decreasing exponential at the right endpoint. The omitted coefficients are nonpositive, so this gives an upper bound. The four cutoffs $X$ are 650000001, 1800000001, 1400000001, and 200000001, in the order L3, L4, L5, R2. All higher-degree or ramified contributions through the cutoff are obtained by exact prime ideal decomposition. At an unramified prime prime to the polynomial index with $p^2 > X$, only linear roots can contribute. The integral in Lemma 4.5.1 is evaluated by expanding the nonnegative polynomial and replacing $t^j$ by $\Gamma((j+1)/2)/(2a^{(j+1)/2})$.

**Computing a lower bound for the positive sum.** For L3 and L4 take $B = 1$. For L5 and R2 let $\mathfrak{a}_2$ be the ideal specified in Hermite normal form in the corresponding field record, of norm 24477393307123 and 153147525034248, respectively. The record gives $g$ with $\mathfrak{a}_2^2 = (g)$, and the unramified characters computed below show that $[\mathfrak{a}_2]$ has order two. Take $B = \langle[\mathfrak{a}_2]\rangle$ in these two fields. A finite list of certified prime ideals suffices. Begin with principal fractional ideals, each given by an element of $K$ in its integral basis. Factor them completely. When all primes over $p$ occur already, adjoin the relation furnished by $(p)$. In the two cases with $\mathfrak{a}_2$, check one further principal identity $(v) = \mathfrak{p}\mathfrak{a}_2$ and use $[\mathfrak{p}] = 0$ in the quotient by $B$. These integer relations present a group surjecting onto the subgroup of $\mathrm{Cl}(K)/B$ generated by their supported primes. Eliminate entries $\pm1$ by integral row and column operations. The remaining matrix has integer column Hermite normal form equal to the identity. Thus every supported prime has class in $B$. The initial numbers of supported primes are 850, 1048, 924, 1273, and the residual dimensions after the unit pivots are 65, 98, 87, 155.

Now use an ordered list of algebraic integers. At each step the principal ideal has just one as yet uncertified prime divisor, of valuation one. All its other prime divisors have already been certified, so induction proves that the new prime also belongs to $B$. The verifier evaluates the algebraic integers, factors their absolute norms, identifies degree-one factors by reduction when the norm valuation is one, and otherwise uses exact ideal valuations in the maximal order. For every rational prime $p$ the identity $\sum_{\mathfrak{p}\mid p} f_{\mathfrak{p}} v_{\mathfrak{p}}(v) = v_p(Nv)$ accounts for the full factorization. This proves 76580, 85204, 85024, 115352 additional ideal memberships, respectively.

Let $a_q$ count these prime ideals of norm $q$, set $H = 96$, and put $j_q = \lceil H\log q\rceil$. Expand, through degree $HT$,

$$\sum_\nu c_\nu X^\nu = \prod_q (1-X^{j_q}/q)^{-a_q} = \exp\left(\sum_q\sum_{k\ge1}\frac{a_q X^{kj_q}}{kq^k}\right).$$

Unique ideal factorization shows that $c_\nu$ is the sum of $1/NI$ over all included products in bin $\nu$. Since $H\log q \le j_q \le H\log q + 1$ and $q \ge 2$,

$$\frac{\nu/H}{1+1/(H\log 2)} \le \log NI \le \nu/H.$$

For each bin, use the endpoint farthest from $\lambda$ to obtain a lower Gaussian weight. Discard the positive contribution from all other ideals. The resulting lower sum $S_{\mathrm{low}}$ and upper error $E_{\mathrm{up}}$ give

$$m \le \frac{b\kappa_0}{S_{\mathrm{low}} - E_{\mathrm{up}}}.$$

The power series, transcendental functions and final division are enclosed in Arb ball arithmetic with 168-bit precision. The code uses interval endpoints before taking the final integer floor.

### 4.5.1 The upper residue certificates

For L3, L4 and L5, use the real-shift upper certificate of Section 4.4. For R2 use the same identity at $s = 1 + b + iv$ and its conjugate. The contribution of one zero is the mean

$$k_{b,v}(\rho) = \tfrac{1}{2}\Re\left((1+b+iv-\rho)^{-1} + (1+b-iv-\rho)^{-1}\right).$$

In the Euler sum the corresponding real exponential is $e^{-bx}\cos(vx)$. In the constant term replace $A(b)$ by the real part of $s^{-1} + (s-1)^{-1} + \frac{1}{2}\log D + G'(s)/G(s)$. The rational weights and vertical shifts are listed in the archive. For the term $(b,v) = (1/100, 0)$ subtract $10^{-6}$ from the stored weight.

Write $K_w = \sum w_{b,v}k_{b,v}$, $P_w(x) = \sum w_{b,v}e^{-bx}\cos(vx)$. To check the zero inequality, reflect in the critical strip, set $z = t^2/(1+t^2)$ on its boundary, and multiply by $1+t^2$. The two reflected kernels for a pair of shifts become the sum over $c = b, 1+b$ of

$$\frac{c\,q_c}{q_c^2 - 4v^2z(1-z)}, \qquad q_c = z + (c^2+v^2)(1-z).$$

The normalized reflected logarithmic kernel equals

$$\frac{\log(1+a^2(1-z)/z) + \log(1+a(2+a)(1-z))}{2(1-z)}.$$

The two quotients are enclosed on each interval by monotonicity or their continuous limits. The rational kernel is enclosed by Taylor expansion through degree five at each midpoint, with the remainder obtained by multiplying back by the quadratic denominator. This proves $K_w(\rho) + K_w(1-\bar\rho) \le h_a(\rho) + h_a(1-\bar\rho)$ on both boundaries. Both sides are harmonic inside the strip, their difference tends to zero uniformly as $|\Im\rho| \to \infty$, and the logarithmic singularities on the boundary have positive sign on the majorizing side. The minimum principle proves the inequality throughout the strip.

For $x \ge c_0 = \log X$, the upper bound $e^{-ax}/x \le e^{-ax}/c_0$ reduces the Euler-tail test to an exponential polynomial. Divide by its slowest exponential. Its constant is negative, and beyond 512 the absolute values of all other terms have sum smaller than its magnitude. On $[c_0, 512]$ a degree-five Taylor enclosure and a sixth-derivative absolute bound certify negativity. On the finite prime-power bins of width $1/16384$ the kernel is $e^{-(1+a)x} + x\sum w_{b,v}e^{-(1+b)x}\cos(vx)$. Use its value and first derivative at the midpoint, and bound the second derivative term by term. This checks 9,723 boxes for the strip and 95 for the infinite-tail argument up to 512. For $X = 3{,}000{,}000{,}001$ the finite log-residue error is below 0.000137. The residue is less than 13.0790.

| | L3 | L4 | L5 | R2 |
|---|---|---|---|---|
| Certified prime ideals | 77430 | 86252 | 85948 | 116625 |
| Gaussian center $\lambda$ | 82 | 83 | 83 | 90 |
| $10^6 S_{\mathrm{low}}$, rounded down | 43.0186 | 9.7226 | 14.4151 | 38.7960 |
| $10^6 E_{\mathrm{up}}$, rounded up | 10.3988 | 2.2664 | 2.8294 | 8.3934 |
| Upper bound on $m$ | 37187 | 59400 | 42102 | 109967 |
| $\kappa/\kappa_0$, rounded up | 3.9641 | 3.9794 | 7.7290 | 7.8240 |
| Upper bound on $h$ | 3 | 3 | 7 | 7 |

The last step uses the integer bound on $m$. For every rational prime $\ell$ up to that bound the certificate supplies residue characters of the units at unramified degree-one primes. Their matrix modulo $\ell$ has rank fourteen (fifteen at $\ell = 2$ with $-1$). An element of $U$ which is an $\ell$th power in $K$ maps to zero under every one of these characters. Full rank excludes $\ell \mid m$. Thus $m = 1$ in all four cases, $h = \kappa/\kappa_0$, and the integer bounds follow.

### 4.6 The strict classes on L3, L4 and L5

For L3, L4 and L5 the dyadic prime has ramification index 9 and residue degree 3, and $\dim W = 16$. The geometry and local dimensions are recorded in Sections 4.1 and 4.3.

The three dyadic Jacobian rows have rank one modulo $W$. Thus the visible part has dimension at most two. The nine-cycle test and the dyadic calculation from Section 4.3 give injective cohomological evaluation. On L3 and L4 every prime above the exceptional rational primes is principal and the localization of the units modulo squares is injective. Since $h \leq 3$, Section 4.2 gives trivial strict kernel. On L5 the stored ideal $\mathfrak{a}_2$ satisfies $(g) = \mathfrak{a}_2^2$. A product of the displayed squareclasses, numbered by mask 16390, gives an everywhere-unramified character nontrivial on $\mathfrak{a}_2$. All exceptional prime ideals have class in $\langle \mathfrak{a}_2 \rangle$. The localized explicit squareclass space has one relation and the corresponding character detects $\mathfrak{a}_2$. The strict-kernel argument of Section 4.2, using $h \leq 7$, gives dimension at most one. Section 4.5 gives the class-number inequalities used here.

### 4.7 Rational divisors and rank lower bounds

We first certify lower bounds by reduction modulo two on L2, R1, R3, R4 and R5. Write $D_P = [P - O]$ for the displayed affine points, ordered as in the corresponding theorem below. On R5 also use $D_E = [E - 2O]$, where $E$ is the quadratic pair cut out by $y = -x - 1$ and $x^2 - 2x - 2 = 0$. Substitution shows that $E$ lies on R5.

| Curve | Good prime $p$ | $\#J(\mathbb{F}_p)$ | Character rows on the chosen classes |
|---|---|---|---|
| L2 | 3 | 91 | 11, 01 |
| R1 | 3 | 81 | 1 |
| R3 | 11 | 1769 | 101, 100, 011 |
| R4 | 7 | 475 | 1 |
| R5 | 13 | 3759 | 10, 01 |

For R5 put $D_E$ last. On L2 the two columns correspond to $(-1, 0), (0, 0)$, and on R3 to $(-1, -1), (0, -1), (1, 1)$. Each binary string gives a character evaluated on the classes in that order. For a prime, slope and intercept $(p, m, n)$, evaluate $mx + n - \sigma y$ and take its squareclass in $\mathbb{F}_p^\times$. At a point of tangency the equivalent nonsingular expression is $\sigma F_y$. Indeed, substituting $\sigma y = mx + n$ in the curve equation produces a square, whose quotient by $mx + n - \sigma y$ is a unit specializing to $\sigma F_y$. For $D_E$ take the norm over the quadratic pair. The triples giving the rows above are

$$\begin{aligned} &\text{L2} : (17, 12, 5), (37, 4, 13), && \text{R1} : (11, 4, 7), \\ &\text{R3} : (13, 3, 0), (13, 3, 8), (41, 16, 14), && \text{R4} : (5, 1, 1), \\ &\text{R5} : (3, 2, 0), (17, 7, 8). \end{aligned}$$

Each matrix has full column rank modulo two. Reduction at the indicated odd good prime excludes rational 2-torsion. Thus the displayed classes are independent, achieve the upper rank bound and span modulo two. The subgroup they generate has finite odd index. On L3, L4 and L5 the independent 3-adic logarithms below give the lower bounds, on R2 one nonzero logarithm suffices, and on L1 four independent dyadic images give rank four. Throughout the sieves we use saturation only at the primes at which it is proved.

## 4.8 Abelian logarithms by a principal divisor

Use the holomorphic differentials $(\omega_0, \omega_1, \omega_2) = (1, x, \sigma y)\, dx/(\sigma F_y)$. With an affine point $P$ we associate the row of abelian logarithms $I(P) = \log(D_P)$ in this basis. An integral point lies in an affine residue disk at every prime of good reduction. In rank at most two a nonzero linear form vanishing on the rational logarithms gives a differential whose integral between two rational points is zero.

The logarithms can be computed entirely in one disk. Choose $g \in L(\mu O)$ whose intersection with the curve reduces to $\mu P$. Its pole order is $\mu$, and the monomials $x^i y^j$, $0 \le j < 3$, $3i + 4j \le \mu$, form a basis there. Reduce the Taylor coefficients at $P$ to find $g$. The resultant of $g$ and $F$ in the chosen disk parameter has leading coefficient a unit and all other coefficients divisible by $p$. Each root has valuation at least $1/\mu$. If $\omega = \sum_{n \ge 1} c_{n-1} s^{n-1} ds$ is integral in this parameter, the principal divisor of $g$ gives

$$\mu \int_O^P \omega = -\sum_{n \ge 1} c_{n-1} \frac{S_n}{n}, \qquad S_n = \sum_{g(Q)=0} s(Q)^n.$$

Newton's identities compute $S_n$ exactly from the resultant, with multiplicities. The valuation of the $n$th summand is at least $\lceil n/\mu \rceil - v_p(n)$. This gives the truncation bound in the following local computations.

**Lemma 4.8.1.** *Let $f(x) = \sum_{n \ge 0} a_n x^n \in \mathbb{Z}_2[[x]]$. If $a_0$ is odd and $a_1$ is even, then $\int_0^x f(s)\, ds$ has no zero in $2\mathbb{Z}_2$ other than $x = 0$.*

*Proof.* For $x \in 2\mathbb{Z}_2 \setminus \{0\}$, divide the integral by $x$. Its constant term is odd, while $a_1 x/2$ is even. For $n \ge 2$ the $n$th term has valuation at least $n - v_2(n+1) \ge 1$. The quotient is therefore a unit. □

**The dyadic trace for R1 and R4.** Write the equation in monic form $F(x, u) = 0$ and let $P = (0, u_0)$ be the centre of its affine residue disk. In both cases the line $u = u_0$ cuts out $P$ and the three points with $x^3 = -2$. Write $I(P)$ in the basis $(1, x, u)\, dx/F_u$. For $h = 1, x, u$, if $h\, dx/F_u = \sum_{n \ge 0} c_{h,n} x^n\, dx$, the corresponding coordinate of $4I(P)$ is

$$V_h = -\sum_{k \ge 1} \frac{(-2)^k}{k}\, c_{h,3k-1}.$$

Indeed, the power sum of the three nonzero roots is zero unless the exponent is $3k$, when it equals $3(-2)^k$. The coefficients are 2-adically integral because $F_u(P) = 3$. For $k \ge 5$ one has $k - v_2(k) \ge 4$, so the first four terms suffice modulo 16.

**Lifting a disk at 3 on L3 and L4.** In both equations $F_y$ is a unit at 3. An annihilating differential is obtained from the primitive cross product of two independent rows of abelian logarithms. In a disk centred at a known point $P$, set $x = x(P) + 3T$, solve for $y$ as a power series, and divide the integral from $P$ by $3T$. A term of degree $n - 1$ in the differential then contributes a coefficient divisible by $3^{n-1-v_3(n)}$. This bounds the omitted terms. After removal of common powers of 3, each possible root lifts through at most three residue classes at the next precision, all of which are tested. An invertible two-coordinate minor of the logarithm matrix after division by 3 recovers the coefficients in the Mordell–Weil generators.

## 4.9 R1. $x^4 - y^3 + xy + x + 1 = 0$ $(H = 31)$

**Theorem 4.9.1.** *The only integer solution of $x^4 - y^3 + xy + x + 1 = 0$ is $(x, y) = (0, 1)$.*

*Proof of Theorem 4.9.1.* Put $u = -y$. Then $F = x^4 + u^3 - xu + x + 1$ and every integral point reduces modulo two to the class of $P = (0, -1)$ in the $(x, u)$-coordinates. Write $u = -1 + w$. The equation in this disk is

$$3w - 3w^2 + w^3 - xw + 2x + x^4 = 0.$$

Here $x$ is a local parameter. For $\omega_0 = dx/F_u$ and $\omega_1 = x\,dx/F_u$, the trace in Section 4.8 gives $(V_1, V_x) \equiv (12, 4) \pmod{16}$, where the subscripts denote the functions 1 and $x$. The class $[P - O]$ spans the rank-one rational logarithm line by Section 4.7. Thus the differential

$$f(x)\,dx = (V_x\omega_0 - V_1\omega_1)/4$$

annihilates every rational class. The expansion $1/F_u = 1/3 - x/3 + O(x^2)$ shows that $f$ has odd constant coefficient and even linear coefficient. For an integral point $Q$ in the disk the integral from $P$ to $Q$ vanishes. Lemma 4.8.1 forces $x(Q) = 0$, whence $u = -1$ and $y = 1$. Conversely, $(0, 1)$ satisfies the original equation. □

## 4.10 R4. $x^4 + y^3 + xy + x - 1 = 0$ ($H = 31$)

**Theorem 4.10.1.** *The only integer solution of $x^4 + y^3 + xy + x - 1 = 0$ is $(x, y) = (0, 1)$. The smooth projective model has exactly two rational points, $(0 : 1 : 1)$ and $O = (0 : 1 : 0)$.*

*Proof of Theorem 4.10.1.* Let $F = x^4 + y^3 + xy + x - 1$ and $P = (0, 1)$. By Section 4.7, $[P - O]$ spans the rational logarithm line. The good fibre over $\mathbb{F}_2$ has just two points, the reductions of $P$ and $O$. In the disk of $P$ put $y = 1 + w$. The equation

$$3w + 3w^2 + w^3 + xw + 2x + x^4 = 0$$

makes $x$ a local parameter and gives $1/F_y = 1/3 + x/3 + O(x^2)$. In the basis $\boldsymbol{\omega} = (1, x, y)\,dx/F_y$, the dyadic trace of Section 4.8 gives

$$4I(P) = (V_1, V_x, V_y) \equiv (8, 8, 0) \pmod{16}.$$

In particular $(V_x - V_1 x)\,dx/(8F_y)$ annihilates the rational logarithm line. Its constant coefficient is odd and its linear coefficient is even. By Lemma 4.8.1, a rational point in this disk must have $x = 0$, and hence $y = 1$.

In the disk of $O$, write $t = X/Y$ and $z = Z/Y$. The equation gives $z = -t^4 + O(t^9)$. With indices $0, 1, 2$ on the three entries of $\boldsymbol{\omega}$, we have $\omega_2 = (-1 + O(t^5))\,dt$ and $\omega_0 = z\omega_2$, with integral coefficients. For $0 \neq t \in 2\mathbb{Z}_2$ the first and third components of $t^{-1}\int_O^Q \boldsymbol{\omega}$ reduce to $(0, 1)$ modulo two. The primitive direction of the rational logarithm line reduces to $(1, 1, 0)$, by the displayed trace, so this vector cannot lie on that line. The disk therefore contains only $O$ among the rational points. This proves both assertions. □

## 4.11 R2. $x^4 + y^3 + xy - 3 = 0$ ($H = 31$)

**Theorem 4.11.1.** *The only integer solution of $x^4 + y^3 + xy - 3 = 0$ is $(x, y) = (1, 1)$.*

Let $F = x^4 + y^3 + xy - 3$. The factor degrees at 61 are $(9, 9, 9)$, and the dyadic factor degrees are $2, 5, 10, 10$. Section 4.3 gives injectivity on global cohomology and local dimension four. Sturm division for $-4x^3 - 27(x^4 - 3)^2$ gives exactly two real simple roots, in $(-18/13, -11/8)$ and $(-54/43, -5/4)$. The values of $x^4 - 3$ there have opposite signs, so the two folds connect the three real branches.

### 4.11.1 The global and local squareclasses

Write $\mathfrak{a}_2$ for the integral ideal of norm 153147525034248 specified by its Hermite normal form. The exact identity $(g) = \mathfrak{a}_2^2$ and the Artin value below show that $\mathfrak{a}_2$ has order two. The four primes above 2 have classes $1, \mathfrak{a}_2, 1, \mathfrak{a}_2$ in order. The four corresponding identities $(v_i) = \mathfrak{p}_i\mathfrak{a}_2^{k_i}$ have $k = (0, 1, 0, 1)$. For every prime over a bad odd rational prime the verifier checks the analogous principal ideal identity. Thus all exceptional primes belong to $\langle \mathfrak{a}_2 \rangle$.

The global rows consist of fourteen units, $-1$, $g$, and the three products of the $v_i$ specified by the masks 1, 10 and 4 (decimal integers whose bit $i-1$ selects $v_i$). Their odd valuations are even and their dyadic valuation patterns generate the kernel of $k$. The dyadic squareclass space has dimension $27+2\cdot 4=35$, and the three real signs bring the total to 38. Localize all nineteen elements with the ideal-star coordinates of Section 4.3. Their nineteen independent rows give a maximal isotropic subspace $W$. Any global squareclass with even valuation at all odd places has localization orthogonal to these rows by reciprocity and is therefore in $W$.

The local Jacobian rows are obtained from integral factors of the quartics cut out by horizontal lines at $y=1,1,-1,-2$, respectively. For $y=1$ use the two different linear factors. The resultant valuations separating the selected factors from their complements are $0,0,0,1$. The computation lifts to precision 60 at 2, evaluates the bitangent on each factor, and maps the norm to the dyadic squareclass group. The four row bitmasks are

$$12516524032,\quad 18253611008,\quad 28963733504,\quad 10541629440.$$

They are independent. As the local dimension is four, these rows span the local image. Of its sixteen linear combinations, just 0 and mask 2 lie in $W$ with trivial real signs. The visible global dimension is at most one.

The sixteen explicit unit and half-ideal squareclasses have independent dyadic–real rows. Adjoining the four unramified dyadic directions gives exactly one nonzero ordinary unramified character among the sixteen classes, mask 16737. Its Artin values on $\mathfrak{a}_2$ and the four dyadic primes are $-1$ and $(1,-1,1,-1)$. Here character values are written multiplicatively. Since a dyadic prime represents $[\mathfrak{a}_2]$, a strict character $\chi$, which is trivial at the dyadic primes, has $\chi(\mathfrak{a}_2)=1$. If $\chi$ were nontrivial, its kernel would have even order since it contains $\mathfrak{a}_2$. The bound $h\le 7$ then forces $h=4$ and $\ker\chi=\langle\mathfrak{a}_2\rangle$. Apply Lemma 4.2.2 with the strict class in both slots. The half-ideal of its squareclass has Artin value $+1$, hence class in $\langle\mathfrak{a}_2\rangle$. Dividing by $g$ if needed and then by a square shows that the strict class is represented by the sixteen explicit squareclasses. Their localizations are injective, a contradiction. The strict kernel vanishes and rank $J(\mathbb{Q})\le 1$.

### 4.11.2 The integral at 3

*Proof of Theorem 4.11.1.* Modulo three the only affine points are $(0,0)$ and $(1,1)$. The first has no lift modulo nine, since every term of $x^4+y^3+xy$ would be divisible by nine. At $P=(1,1)$ set $X=x-1$, $U=y-1$. The function

$$f=-X+U-X^2-U^2+X^3+X^2U$$

has pole order 10 and its resultant with $F$ reduces to $-X^{10}$ up to the ordering sign. The intersection divisor is supported in the disk of $P$ modulo three. The 3-adic abelian logarithm on $J(\mathbb{Q}_3)$ is additive. Differences of points in this smooth disk map into the formal group, where integrating the regular differentials computes that logarithm on the smooth locus of the fiber. Since $F_y(P)=4$ is a unit, the power-series trace used in Section 4.8 gives $10I(P)=(3,6,3)$ mod 9. This also proves nontorsion, hence rank exactly one. The primitive logarithm vector reduces to $(1,2,1)$ and the tangent vector of the three forms reduces to $(1,1,1)$. They are independent. An integral linear functional on the differentials annihilates the rank-one logarithm line and is a unit on this tangent. In the disk $X=3T$, its integral divided by $3T$ has unit constant term and all higher terms divisible by 3 because $j-1-v_3(j)\ge 1$ for $j\ge 2$. It has exactly the central zero. This proves that $(1,1)$ is the only integer solution. □

## 4.12 L2. $x^4+y^3+x+2y=0$ ($H=30$)

**Theorem 4.12.1.** *The integer solutions of $x^4+y^3+x+2y=0$ are exactly*

$$(x,y)=(-1,0),\quad (0,0).$$

*Proof of Theorem 4.12.1.* Here $x^4+x=-y^3-2y$. Modulo two the two affine disks are centered at $P=(-1,0)$ and $Q=(0,0)$. Since $1+4x^3$ is odd, $y$ is a parameter in both. The trace computation

gives

$$I(P) = (248, 110, 2), \qquad I(Q) = (224, 86, 170) \pmod{256}.$$

The two bitangent characters of Section 4.7 prove 2-saturation. The first logarithm coordinate of every rational class is consequently in $8\mathbb{Z}_2$. The cross product of the two logarithms, divided by 16, gives a primitive annihilator with coefficients $(2, 1, 1)$ mod 4. These are coefficients of an actual annihilator over $\mathbb{Z}_2$.

In each disk $\omega_0 = -dy/(1 + 4x^3)$. The inverse factor is 1 mod 4 as an integral power series. For $y \in 2\mathbb{Z}_2$ each monomial integral $y^{n+1}/(n+1)$ lies in $2\mathbb{Z}_2$. Thus $\int_0^y \omega_0 \equiv -y \bmod 8$ and a rational point in either disk has $y \in 8\mathbb{Z}_2$. Set $y = 2T$, so $T \equiv 0 \bmod 4$.

For $y \neq 0$ divide the integral of the primitive annihilator from the center by $y$. At $P$ its expansion is $1 + T$ mod 2, and at $Q$ it is $2 + T + 2T^3$ mod 4. For instance, at $Q$ the implicit equation gives $x = -2y - y^3 + O(y^4)$, while at $P$ one has $x = -1 + (2/3)y + O(y^2)$. Terms with integrated index $n \geq 5$ vanish at the required precision since $v_2(2^{n-1}/n) \geq 2$. The expansions take values 1 modulo 2 and 2 modulo 4, respectively, on $T \equiv 0 \bmod 4$. Thus $y = 0$, and $x(x^3 + 1) = 0$ gives exactly $(-1, 0)$ and $(0, 0)$. □

## 4.13 L3. $x^4 + y^3 + x - y - 2 = 0$ ($H = 30$)

**Theorem 4.13.1.** *The integer solutions of* $x^4 + y^3 + x - y - 2 = 0$ *are exactly*

$$(x, y) = (1, -1), \quad (1, 0), \quad (1, 1).$$

*Proof of Theorem 4.13.1.* Take $P_1 = (1, 0)$ and $P_2 = (1, 1)$. The trace of Section 4.8 in the basis $(1, x, y)\, dx/F_y$ gives

$$I(P_1)/3 \equiv (2, 0, 2), \qquad I(P_2)/3 \equiv (2, 2, 2) \pmod{3}.$$

Since $\#J(\mathbb{F}_3) = 16$, all rational logarithms belong to $3\mathbb{Z}_3^3$. The two reduced rows are independent, so the rank bound in Table 9 is attained and the two classes are saturated at 3. The group orders 16 and 101 at 3 and 5 exclude rational torsion by reduction away from its order. A rational class thus has coefficients in $\mathbb{Z}_3$ in this basis.

The three affine disks modulo 3 are centred at $(1, 0), (1, 1), (1, -1)$. The corresponding classes sum to zero, since $x - 1$ cuts out these three points and has pole divisor $3O$. The primitive annihilator has coefficients $(674, 11286, 11908)$ mod $3^9$, up to a unit. In the first and third disks the divided integral of Section 4.8 has no root modulo 3. In the second disk every additional root gives the coefficient pair $(0, 64)$ mod 81.

Now $\#J(\mathbb{F}_{31}) = 36612 = 452 \cdot 81$. After multiplication by 452, the reduction of any candidate class is determined by its pair modulo 81. None of the 37 affine points over $\mathbb{F}_{31}$ has this image. The centres of the three disks therefore exhaust the integer solutions. □

## 4.14 L4. $x^4 + y^3 + x + y + 2 = 0$ ($H = 30$)

**Theorem 4.14.1.** *The integer solutions of* $x^4 + y^3 + x + y + 2 = 0$ *are exactly*

$$(x, y) = (-1, -1), \quad (0, -1).$$

*Proof of Theorem 4.14.1.* Set $P_1 = (-1, -1)$ and $P_2 = (0, -1)$. In the basis $(1, x, y)\, dx/F_y$, the trace of Section 4.8 gives

$$I(P_1)/3 \equiv (1, 2, 2), \qquad I(P_2)/3 \equiv (2, 2, 1) \pmod{3}.$$

Since $\#J(\mathbb{F}_3) = 28$, every rational logarithm belongs to $3\mathbb{Z}_3^3$. The independent rows attain the rank-two bound in Table 9 and prove saturation at 3. Reduction at $3, 5, 11$, where the group orders are $28, 140, 2493$, excludes rational torsion. Thus the basis coefficients of a rational class belong to $\mathbb{Z}_3$.

The affine residue classes at 3 are represented by $(-1,-1),(0,-1),(1,1)$. A primitive annihilator has coefficients $(18529, 3366, 15868)$ mod $3^9$, up to a unit. The lifting procedure of Section 4.8 gives no further root in the first disk. In the second, any additional root has generator coefficients $(17, 20)$ mod 27. In the third disk, take as centre the Hensel lift of $y \equiv 1 \pmod 3$ at $x = 1$. A function with pole divisor $28O$ whose zeros reduce to this centre computes its base logarithm. With $x = 1 + 3T$, the annihilating integral including its constant term has coefficients of minimum valuation one. After dividing by 3 it has just one possible root modulo $3^{11}$, namely $T \equiv 82468$. Its coefficient pair is $(8, 25)$ mod 27.

At 29 the group order is $19710 = 730 \cdot 27$. Multiplication by 730 makes the reduced class depend only on its coefficient pair modulo 27. Enumerating all 23 affine points over $\mathbb{F}_{29}$ gives no match for either pair. Thus only $P_1$ and $P_2$ remain. □

### 4.15 R5. $x^4 + y^3 + x + 2y + 1 = 0$ ($H = 31$)

**Theorem 4.15.1.** *The only integer solution of $x^4 + y^3 + x + 2y + 1 = 0$ is $(x, y) = (1, -1)$. The smooth projective model has exactly two rational points, $(1 : -1 : 1)$ and $O = (0 : 1 : 0)$.*

*Proof of Theorem 4.15.1.* Let $F = x^4 + y^3 + x + 2y + 1$ and $P = (1, -1)$, and let $D_P, D_E$ be as in Section 4.7, where $E$ is the pair cut out by $y = -x - 1$ and $x^2 - 2x - 2 = 0$. By that section $J(\mathbb{Q})$ has rank two and no 2-torsion, and $D_P, D_E$ span $J(\mathbb{Q})/2J(\mathbb{Q})$.

**Residue classes modulo 3.** The curve has good reduction at 3, and its affine points over $\mathbb{F}_3$ are $Q_n = (1, n + 2)$ for $n \in \mathbb{F}_3$, that is $Q_0 = (1, -1)$, $Q_1 = (1, 0)$ and $Q_2 = (1, 1)$. For every $n \in \mathbb{F}_3$,

$$F(x, 2x + n) \equiv x^4 + 2x^3 + 2x + 1 = (x - 1)^4 \pmod 3.$$

Thus the line $y = 2x + n$ meets $C_{\mathbb{F}_3}$ only at $Q_n$, with multiplicity four, and $g_n = 2x + n - y$ has divisor $4Q_n - 4O = 2(2Q_n - 2O)$. Its leading coefficient at $O$ in the parameter $x/y$ is 1. By Weil reciprocity, evaluation of $g_n$ on divisors gives a homomorphism

$$\chi_n \colon J(\mathbb{F}_3) \longrightarrow \mathbb{F}_3^\times / \mathbb{F}_3^{\times 2} = \mathbb{F}_2.$$

At $Q_n$ itself one uses the leading coefficient of $g_n$ in the parameter $x - 1$. Since $g_n \cdot \big(F(x, y) - F(x, 2x + n)\big)/(y - 2x - n) = (x - 1)^4$ on $C_{\mathbb{F}_3}$, this coefficient is $1/F_y(Q_n) = 1/2$, a non-square. As $g_n(Q_m) = n - m$ for $m \neq n$, the vector $\chi = (\chi_0, \chi_1, \chi_2)$ takes the values

$$\chi([Q_0 - O]) = (1, 0, 1), \qquad \chi([Q_1 - O]) = (1, 1, 0), \qquad \chi([Q_2 - O]) = (0, 1, 1).$$

Modulo 3 the polynomial $x^2 - 2x - 2$ becomes $(x - 1)^2$, so $E$ reduces to $2Q_2$. Hence $\chi(D_E) = 0$, while $\chi(D_P) = (1, 0, 1)$. A rational point $R$ satisfies $[R - O] \in aD_P + bD_E + 2J(\mathbb{Q})$ for some $a, b$, and reduction gives $\chi([\bar{R} - O]) \in \{0, (1, 0, 1)\}$. Thus a rational point reduces either to $Q_0$ or to $O$. Every integral point reduces to $Q_0$.

**The logarithms modulo 9.** Use $\omega = (1, x, y)\,dx/(3y^2 + 2)$ and the parameter $t = x - 1$. The line $x + y = 0$ cuts out $2P + B$, where $B$ is the pair $x^2 + x + 1 = 0$ on $y = -x$; both points of $B$ lie in the residue disk of $P$. The line $x + y + 1 = 0$ cuts out $E + E'$, where $E'$ is the pair $x^2 + x + 1 = 0$ on $y = -x - 1$; both pairs lie in the residue disk of $Q_2$. Let $P'$ be the point of that disk with $x = 1$. Then

$$4 \log D_P = -\sum_{Q \in B} \int_P^Q \omega, \qquad 2 \log D_E = \sum_{Q \in E} \int_{P'}^Q \omega - \sum_{Q \in E'} \int_{P'}^Q \omega.$$

In the parameter $t$ the pairs $B$ and $E'$ are the roots of $t^2 + 3t + 3$, and $E$ is the pair of roots of $t^2 - 3$. Write $\omega_j = \sum_{k \geq 1} c_{j,k-1} t^{k-1}\,dt$ with $c_{j,k} \in \mathbb{Z}_3$ in the relevant disk. Each sum of integrals over a pair equals $\sum_k c_{j,k-1} S_k/k$, where $S_k$ is the $k$th power sum of the two roots. As $v_3(S_k) \geq k/2$, the terms with

$k \geq 4$ vanish modulo 9. The three sums are $(3,6,3)$, $(0,6,3)$ and $(3,6,0)$ modulo 9 for $B$, $E$ and $E'$, respectively, whence

$$\log D_P \equiv (6,3,6), \qquad \log D_E \equiv (3,0,6) \pmod 9.$$

After division by 3 these vectors are independent modulo 3. The cross product of the two original logarithms, divided by 9, is a primitive vector $\lambda \in \mathbb{Z}_3^3$, which after scaling by a unit satisfies $\lambda \equiv (1,2,1) \pmod 3$. Since $J(\mathbb{Q})$ has rank two, the differential $\lambda \cdot \omega$ annihilates the logarithm of every rational class.

**The disk of $P$.** Write $x = 1 + 3T$ with $T \in \mathbb{Z}_3$. Since $F_y(P) = 5$ is a unit, $\lambda \cdot \omega = \sum_{k\geq 0} a_k t^k \, dt$ with $a_k \in \mathbb{Z}_3$ and $a_0 = \lambda \cdot (1,1,-1)/5 \equiv 1 \pmod 3$. For a rational point $R$ in this disk with $T \neq 0$, $\int_P^R \lambda \cdot \omega = 0$, and

$$\frac{1}{3T} \int_P^R \lambda \cdot \omega = \sum_{k\geq 0} a_k \frac{(3T)^k}{k+1}$$

has unit constant term, while its term of index $k \geq 1$ has valuation at least $k - v_3(k+1) \geq 1$. Hence $T = 0$ and $R = P$. Thus $(1,-1)$ is the only integer solution.

**The disk of $O$.** In $t = X/Y$ at $O$, the constant coefficient of $\lambda \cdot \omega$ is $-\lambda_2 \equiv 2 \pmod 3$, where $\lambda_2$ is the coefficient of the third differential. For $0 \neq t \in 3\mathbb{Z}_3$, dividing the integral from $O$ by $t$ preserves that unit constant term. The term of index $k \geq 1$ has valuation at least $k - v_3(k+1) \geq 1$. Thus $O$ is the only rational point in this disk, which completes the description of the rational points. □

*Remark.* An alternative descent on R4 and R5 uses the stronger result $h_K = 1$. The separate computations recorded in the working notes in `notes/` of the ancillary files bound the unit indices by 10890 and 31968 before saturation. With the full unit groups, signed explicit-formula bounds and degree-one prime counts through 165055000000 and 190055000000 give $h_K < 1.992610$ and $h_K < 1.999553$, respectively. Then ordinary $S$-units suffice and the visible bounds in Table 9 give ranks one and two directly. Theorems 4.10.1 and 4.15.1 use the bounds $h_K \leq 2$ and $h_K \leq 3$, respectively, from Section 4.4.

## 4.16 R3. $x^4 + y^3 + x - 2y - 1 = 0$ ($H = 31$)

**Theorem 4.16.1.** *The integer solutions of $x^4 + y^3 + x - 2y - 1 = 0$ are exactly*

$$(x,y) = (-1,-1), \quad (0,-1), \quad (1,1).$$

The equation is $F = x^4 + y^3 + x - 2y - 1 = 0$. Let $P_1 = (-1,-1)$, $P_2 = (0,-1)$ and $P_3 = (1,1)$. These are the centers of all three affine disks modulo three. Let $U$ have rows $I(P_i)$. Then

$$U/3 \equiv \begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 1 \\ 0 & 2 & 1 \end{pmatrix} \pmod 3, \qquad \#J(\mathbb{F}_3) = 28.$$

The matrix is invertible modulo three. Good reduction and $3 \nmid \#J(\mathbb{F}_3)$ put the logarithms of all rational classes in $3\mathbb{Z}_3^3$. The rows of $U/3$ form a basis over $\mathbb{Z}_3$, proving 3-saturation, and Section 4.7 gives 2-saturation. A rational class consequently has coefficients in $\mathbb{Z}_3^3$ and $\mathbb{Z}_2^3$ with respect to these three classes.

### 4.16.1 The height and its normalization

Use the Coleman–Gross height for $p = 3$ with $\log_3(3) = 0$. Normalize at an affine point by the tangent dual to $\omega = dx/(3y^2 - 2) = -dy/(4x^3 + 1)$ and at infinity by the parameter $t = -x/y$. The projective model is regular. At each odd bad prime it has one irreducible fiber with a thickness-one node, as in

Section 4.1. An integral section cannot pass through that node since the local smoothing parameter has valuation one. Away from 3, an integral section and $O$ are disjoint and their tangent parameters are integral units on the smooth loci. The vertical correction and the regularized self-intersection therefore give zero local self-height. For the three basis classes, the only intersection of two distinct affine sections is $P_1$ with $P_3$ at 2. Its multiplicity is one because $x(P_3) - x(P_1) = 2$ and $x$ is a smooth parameter there. The off-diagonal correction in entries $(1,3)$ and $(3,1)$ is $-\log_3(2)$.

Take $\eta = (5x^2y, 2xy, x^2)\omega$ for the second-kind forms, and let $J_j(P) = \int_O^P \eta_j$ with tangential normalization. To see the normalization explicitly, write $x = t^{-3}\rho$, $y = -t^{-4}\rho$. The equation gives $\rho^3(\rho - 1) = -2\rho t^8 - \rho t^9 + t^{12}$, so $\rho = 1 + O(t^8)$. The leading powers of the three holomorphic forms are $-t^4dt, -t\,dt, dt$ and those of $\eta$ are $5t^{-6}dt, 2t^{-3}dt, -t^{-2}dt$. Taking residues gives the dual pairing and the isotropic complement spanned by the $\eta_j$. For $P = (a, b)$ use the third-kind form

$$\nu_P(Q) = \frac{y^2 + by + b^2 - 2}{x - a}\,\omega(Q), \qquad Q = (x, y).$$

On $F = 0$ the numerator times $b - y$ equals $(x - a)(x^3 + ax^2 + a^2x + a^3 + 1)$. This gives its poles at $P, O$. Differentiating in the two arguments gives

$$d_P\nu_P(Q) - d_Q\nu_Q(P) = \sum_j \big(\eta_j(P)\omega_j(Q) - \omega_j(P)\eta_j(Q)\big).$$

For a direct check, divide by $\omega(P)\omega(Q)$ and reduce the difference using $F(P) = F(Q) = 0$. Both sides give $5a^2b - 5x^2y + 2abx - 2axy + a^2y - bx^2$.

For the height we use the isotropic complement $\langle \eta_j \rangle$ in de Rham cohomology and the tangent vectors specified above. This is the Coleman–Gross construction [CG89, BB15]; the relation with quadratic Chabauty is developed for hyperelliptic curves in [BBM16] and for general curves in [BMS25]. Here the hyperflex supplies the single base point and the parameter in which one takes the constant terms of primitives at $O$. The coefficients of $t^0, t^1, t^4$ in $\nu_P/dt$ vanish there. Pairing with the primitives of the $\eta_j$ as in Lemma 3.1.8 therefore gives the normalized third-kind form $\nu_P - \sum_j J_j(P)\omega_j$. If $K(P, Q) = \int_O^Q \nu_P$ is regularized at the two marked tangents, its local height is

$$H_3(P, Q) = K(P, Q) - \sum_j J_j(P) I_j(Q).$$

Integrate the preceding bidifferential identity in the second argument. On taking $Q \to P = (a, b)$, the sum of the two regular parts on the diagonal is $-6b\,(db/da)\,da/(3b^2 - 2)$. Changing to the tangent dual to $dx/(3y^2 - 2)$ contributes $d\log(3b^2 - 2)$ and cancels this term. Thus $\tau(P) = H_3(P, P)$ satisfies $d\tau = -2\sum_j \omega_j J_j$ on the three affine disks. The same calculation on L5 replaces $3b^2 - 2$ by $3b^2 + 1$.

Let $H$ be the matrix of the global height on the three generators, with the correction at 2 included. Since their classes span $J(\mathbb{Q}) \otimes \mathbb{Q}$ and $U$ is invertible, global bilinearity gives $M = U^{-1}HU^{-\mathsf{T}}$. Every integral point satisfies

$$q(P) = \tau(P) - I(P)MI(P)^{\mathsf{T}} = 0.$$

### 4.16.2 Roots and finite reductions

*Proof of Theorem 4.16.1.* The verifier computes $U$ and $J_j(P_i)$ by the principal-divisor trace and Coleman reciprocity. For a second-kind differential the contribution at infinity is $\mathrm{Res}_O(\log(g)\eta_j)$. For a third-kind differential one uses the logarithm of the ratio of the leading coefficients of $g$ at its two poles in the chosen tangent parameters. Subtract the trace of the integrals within the disk and divide by the pole order $\mu$ of $g$. The matrix of the local heights before the correction at 2 is

$$H_3 \equiv \begin{pmatrix} 85590 & 447150 & 355752 \\ 447150 & 47358 & 329019 \\ 355752 & 329019 & 512109 \end{pmatrix} \pmod{3^{12}}.$$

In a disk centered at $P_i = (a_i, b_i)$ put $x = a_i + 3T$. Integrate the formula for $d\tau$, subtract the quadratic form, and divide out the known zero $T = 0$. After division by their respective contents $3^2, 3, 3$, the three series begin modulo three with $2T + 2T^2$, $2 + 2T$, $1 + T$. The local series is computed through degree 35. For a term of integrated degree $n$ beyond that cutoff, denominators from the two integrations cost at most $2\lfloor \log_3 n \rfloor$ digits and $U^{-1}$ on the two sides of $H$ costs at most two more. Its valuation is at least $n - 2\lfloor \log_3 n \rfloor - 2 > 10$ for $n \geq 36$. Recursive lifting gives the following necessary classes. The finite precision in the table suffices for every subsequent comparison.

| Center | Modulus | $T$ | Coefficients in the three generators | Final exclusion |
|---|---|---|---|---|
| $P_1$ | $3^8$ | 5787 | $(1927, 378, 1161)$ | 433 |
| $P_1$ | $3^8$ | 986 | $(594, 5481, 6342)$ | 2 |
| $P_2$ | $3^9$ | 12566 | $(2425, 15912, 15114)$ | 83 |
| $P_3$ | $3^9$ | 1211 | $(1771, 18407, 14801)$ | 2 |

For the second restriction, use the two affine disks at 2. The determinant of the matrix of the three dyadic logarithms has valuation four. Thus it suffices to evaluate the local integrals modulo $2^9$ to determine all possible generator coefficients modulo $2^5$. In the two disks this gives 16 and 64 distinct triples respectively. The disjoint union has size 80.

For a given auxiliary prime $q$, let $N = \#J(\mathbb{F}_q)$. First compare the 3-primary projection of each reduced affine point with that of each of the four candidates. At $q = 3$ the disk already fixes the center. To use the dyadic triples, multiply by $N/2^{\min(5, v_2(N))}$ and compare each of the surviving points with the projected triple. There is no assumption that the unrestricted rational group has been saturated at other primes. Both projections are unaffected by denominators prime to their respective primary factors. The numbers of possible dyadic triples, in the order of the table above, are

| $q$ | $\#J(\mathbb{F}_q)$ | Surviving triples after this prime |
|---|---|---|
| 2 | 21 | $(80, 0, 80, 0)$ |
| 3 | 28 | $(24, 0, 24, 0)$ |
| 13 | 3168 | $(8, 0, 8, 0)$ |
| 83 | 657288 | $(8, 0, 0, 0)$ |
| 433 | 79249104 | $(0, 0, 0, 0)$ |

For $q = 433$ the curve has 423 points over $\mathbb{F}_{433}$ and 187949 over $\mathbb{F}_{433^2}$. The genus-three Weil bounds with these two counts allow one multiple of the order 39624552 of $[P_1 - O]$, namely 79249104. For the other four primes the verifier directly counts points over the first three extensions. All four extra classes are excluded. This proves that $P_1, P_2, P_3$ are all the integer points on R3. □

## 4.17 L5. $x^4 + y^3 + x + y - 2 = 0$ ($H = 30$)

**Theorem 4.17.1.** *The integer solutions of $x^4 + y^3 + x + y - 2 = 0$ are exactly*

$$(x, y) = (-1, 1), \quad (0, 1), \quad (1, 0).$$

*Proof of Theorem 4.17.1.* Use $P_1 = (-1, 1), P_2 = (0, 1), P_3 = (1, 0)$. They exhaust the affine residue classes modulo 3. The matrix with rows $I(P_j)/3$ is

$$\begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} \pmod 3.$$

It is invertible, and $\#J(\mathbb{F}_3) = 28$. Together with the rank upper bound this gives rank three and saturation at 3. For the Coleman–Gross height of Section 4.16, form the symmetric height matrix $H$ in these classes, the logarithm matrix $U$, and $M = U^{-1} H U^{-\mathsf{T}}$. The affine sections are pairwise disjoint at every prime. For the first and third sections their $y$-coordinates differ by one even at 2. The

regular model has irreducible fibers and a smooth rational section at infinity. With tangent vector dual to $dx/(3y^2+1)$, the local corrections away from 3 for these sections and for the integral self-height vanish as in Section 4.16. Every integral point satisfies

$$\tau(P) - I(P)MI(P)^{\mathsf{T}} = 0.$$

In the indicated order of the three generators the local height matrix is

$$H_3 \equiv \begin{pmatrix} 398160 & 323658 & 140334 \\ 323658 & 253314 & 203760 \\ 140334 & 203760 & 450693 \end{pmatrix} \pmod{3^{12}}.$$

Repeating the calculation with the contact functions $g+3$ in place of $g$ gives the same matrix modulo $3^{12}$ on both R3 and L5. The two functions have the same reduction at 3 and the same pole at $O$, but cut out different characteristic-zero divisors. The normalized second-kind differentials are $(5x^2y, 2xy, x^2)\,dx/(3y^2+1)$. The normalization at $O$ agrees with the one used for R3 because there is no $xy$ term and the first relative error is $O(t^8)$ in $t = -x/y$. The verifier evaluates the height and its single integrals by the trace formulas, checks symmetry to the specified precision, expands $d\tau = -2\sum_j \omega_j J_j$ on each disk, and computes the disk series. With $x = x(P_i) + 3T$, divide the height equation by $3T$ to remove the known central zero. The three reductions are $2+T$, $T$, and 2 modulo three, respectively. Lifting gives $T \equiv 14317, 9153 \pmod{3^9}$ in the first two disks and no root in the third. Their coordinates are as follows.

| Center | Coefficients modulo $3^9$ | Matches modulo 709 |
|---|---|---|
| $(-1,1)$ | $(4230, 8614, 3244)$ | none |
| $(0,1)$ | $(9396, 9235, 14175)$ | $(189, 575)$ |

Indeed $\#J(\mathbb{F}_{709}) = 342779445 = 215 \cdot 3^{13}$. The exact counts over $\mathbb{F}_{709}, \mathbb{F}_{709^2}$ give the Weil interval $[342773896, 342798434]$. The computed order of $[P_1 - O]$ is 114259815, and exactly one multiple lies in this interval. The multiplier $17415 = 215 \cdot 3^4$ makes the reduction depend only on the three coefficients modulo $3^9$. The enumeration checks all 680 affine points. Increasing the height precision gives the necessary triple $(10480752, 10086931, 6903225)$ mod $3^{15}$ in the second disk. The multiplier 215 uses the full 3-primary subgroup. The resulting image differs from that of $(189, 575)$, which eliminates the last extra candidate. The three listed points all satisfy the equation. □

## 4.18 L1. $x^4 + y^3 + xy - 1 = 0$ ($H = 29$)

**Theorem 4.18.1.** *The integer solutions of $x^4 + y^3 + xy - 1 = 0$ are exactly*

$$(x,y) = (-1,-1), \quad (-1,0), \quad (-1,1), \quad (0,1), \quad (1,0).$$

Put $C\colon x^4 + y^3 + xy = 1$. In this section let

$$P_1 = (-1,-1), \quad P_2 = (-1,0), \quad P_3 = (0,1), \quad P_4 = (1,0), \quad P_5 = (-1,1), \qquad D_i = [P_i - O].$$

The function $x+1$ has divisor $P_1 + P_2 + P_5 - 3O$, so $D_5 = -D_1 - D_2$. Write $J = \mathrm{Jac}(C)$.

### 4.18.1 A height bound for integral points

**Proposition 4.18.2.** *Every integral point $(x,y)$ on L1 satisfies $|x| < 10^{181}$.*

*Proof.* We express the abelian logarithm of an integral point using the four classes $D_1, \dots, D_4$ and a basis of the real period lattice.

**A finite-index subgroup and a simple Jacobian.** The 27 affine bitangents give the global injection of Section 4.3. The auxiliary field has an ideal $\mathfrak{a}_2$ of norm 153301239508 with $\mathfrak{a}_2^2 = (g)$. Among the fourteen units, $-1$ and $g$, the mask 16387 defines an ordinary unramified character that takes the value $-1$ on $\mathfrak{a}_2$ and the dyadic values $(-1, 1, -1, 1)$. The sixteen rows are independent after localization at the dyadic and real places. Every exceptional prime belongs to $\langle \mathfrak{a}_2 \rangle$. For the class-number bound, the ideal certificates put 664623 prime ideals of norm at most $10^7$ in this subgroup. The Gaussian in Section 4.4 with $c = 110$ yields $h/2 < 446.295$. For $X = 60000001$ the two-sided residue test gives $0.0649191 < \kappa < 6.76842$ and $0.96025 < \kappa_0 < 0.96027$. These numbers give $m \le 13194$. The residue characters have full rank for every prime through 13194. Hence $m = 1$, $h \le 7$, and the same Artin argument as on R2 gives zero strict kernel. Sturm division puts the only real roots of $-4x^3 - 27(x^4 - 1)^2$ in $(-11/10, -12/11)$ and $(-10/11, -9/10)$. The polynomial $x^4 - 1$ has opposite signs there, so the two folds join the three real branches as on R2. The real locus is connected. The dyadic factor degrees are $2, 5, 10, 10$. The visible part has dimension at most $d - j \le 4$. The strict kernel is zero, so the global Mordell–Weil rank is at most four. For the entry $\dim W = 19$ in Table 9, the sixteen independent localized classes above have even valuations at every dyadic prime. The four dyadic classes generate $\langle [\mathfrak{a}_2] \rangle$: they lie in it, and the displayed character is nontrivial on two of them. Three independent parity vectors of dyadic prime products therefore have principal representatives. Their valuations are independent of the sixteen even-valuation classes, giving nineteen independent rows. The four $D_i$ have independent dyadic Kummer images. The rank is four, and their subgroup $\Gamma$ has finite index $e$. The finite orders $24, 81, 332$ at $2, 3, 5$ exclude rational torsion, using a different residue characteristic for each possible torsion prime.

The good fiber at 17 has point counts $26, 248, 5024$ over its first three extensions. Its Frobenius polynomial is irreducible,

$$f(z) = z^6 + 8z^5 + 11z^4 - 46z^3 + 187z^2 + 2312z + 4913.$$

Divide $\operatorname{Res}_z(f(z), f(Tz))$ by $(T-1)^6$. The quotient of degree 30 has no cyclotomic factor. The verifier tests all $2 \le n \le 1800$ with $\varphi(n) \le 30$, sufficient because $\varphi(n)^2 \ge n/2$. Hence the ratios of distinct Frobenius roots are never roots of unity. All powers of a Frobenius root have six distinct conjugates. The good fiber stays simple over every finite extension, since each extended Frobenius polynomial is irreducible. Specialization of abelian subvarieties then gives geometric simplicity of $J$.

**Periods and normalized heights.** The regular integral plane model has irreducible fibers. The only bad fibers, at 383 and 3368011, each have one ordinary node of thickness one. These facts follow from the discriminant, the tangent cone and the smoothing coefficient, as in Section 4.1. Adjunction gives $\omega_{C/\mathbb{Z}} = \mathcal{O}_C(1)$ and an integral basis $\boldsymbol{\omega} = (1, x, y)\, dx/(3y^2 + x)$. Its first member generates the relative dualizing sheaf along every affine integral section. At $O$, the third member is a generator. A section cannot meet a thickness-one node. These statements specify the tangent vectors used in the heights and the differential lattice used in computing the Faltings height.

Here are details of the complex integrations. Project to $x$ and take an embedded star from $(5+7i)/16$ to the eight simple zeros of $-4x^3 - 27(x^4 - 1)^2$. Lift each small circuit on the star and subtract the two paths to the base fiber. The resulting graph has three vertices and eight edges. A neighborhood of the star lifts to a neighborhood of this graph. Its complement is a disk because the remaining branch point is totally ramified at infinity. The six nontree edges thus give an integral homology basis. The cyclic order at each vertex determines its intersection pairing. Contract a spanning tree, and count a signed intersection when the endpoints of two chords alternate. The computed alternating matrix has determinant one. Symplectic integer elimination yields periods $(A, B)$, a symmetric matrix $\tau = A^{-1}B$ and positive definite $Y = \Im\tau$. To certify integration, on a disk of radius $3|h|$ about a segment endpoint bound the three roots by $Y_0 = 2 + X_0 + X_0^4$, with $X_0$ an upper bound on $|x|$. The discriminant is the product of the three squared root differences. Thus $1/|F_y|$ is at most $2Y_0/\sqrt{|\operatorname{disc}_y F|}$. Bounding the discriminant from below by distances to the eight roots bounds each form on the disk. Taylor recurrence, Cauchy's geometric remainder and disjoint endpoint root enclosures continue the correct sheet. The interval computation also checks the six integral cycles, the symmetry relations and

positivity. Direct paths to the affine sections, and the real path $x = s^{-3}$, $y = -vs^{-4}$, $v^3 + s^5 v + s^{12} = 1$ from $s = 0$ to 1, give Abel coordinates $z_i = A^{-1} \int_O^{P_i} \boldsymbol{\omega}$.

The covolume of the complex period lattice in the real and imaginary coordinates of the integral differential basis is in $(22.65026, 22.65027)$. It also equals $|\det A|^2 \det Y$. The Faltings height obtained from the metric without a $\pi$ factor is $-\frac{1}{2}\log \mathrm{covol}$, and the convention subtracting $\log(\pi^{-3})/2$ gives 0.1570091 rounded up. In particular the convention in [GR25] gives $h_F(J) < 1$. The symmetric principal theta polarization has one section up to scalar. It is defined over $\mathbb{Q}$ using the theta characteristic $2O$, since $4O$ is canonical.

For clarity, the exact height calculation uses the following theta quotient. For an odd characteristic $\delta$ put

$$L(z) = \log|\theta[\delta](z,\tau)| - \pi \Im(z)^{\mathsf{T}} Y^{-1} \Im(z), \qquad g(Q) = |\nabla\theta[\delta](0)\, A^{-1}(1, x_Q, y_Q)^{\mathsf{T}}|.$$

At $O$ use $(0,0,1)$ in the last formula. Write $H_{ij}$ for the symmetric Néron–Tate bilinear form, with $H_{ii} = \widehat{h}_\Theta(D_i)$. The Faltings–Hriljac formula and the prime form [vBHM20, Fay73] give

$$\begin{aligned} 2H_{ii} &= \log g(P_i) + \log g(O) - 2L(z_i), \\ 2H_{ij} &= L(z_i - z_j) + \log g(O) - L(z_i) - L(z_j) - \log \gcd(|x_i - x_j|, |y_i - y_j|) \quad (i \neq j). \end{aligned}$$

Indeed the logarithm of the norm of the prime form differs from $L(z_P - z_Q)$ by a term in $P$ and a term in $Q$. These terms cancel in a pairing of degree-zero divisors. On taking the diagonal with the indicated tangent, the leading term is the directional derivative of the theta function, giving $g$. At finite places disjointness from $O$, integral tangents and irreducible fibers remove the self and vertical terms. For two distinct affine sections the intersection length gives the displayed gcd. The same diagonal formula applies to any affine integral point at which the displayed theta quotient is defined.

The intervals obtained from characteristic 9, in binary characteristic order, agree for 26 admissible odd characteristics. Rounding only for display,

$$H \simeq \begin{pmatrix} .532422 & -.225381 & .105805 & .126358 \\ -.225381 & .467263 & .034874 & -.228590 \\ .105805 & .034874 & .411606 & -.048574 \\ .126358 & -.228590 & -.048574 & .462141 \end{pmatrix}, \qquad \det H \in (.02560132, .02560134).$$

The leading principal minors of $H - I/10$ are positive. Gaudron–Rémond [GR25, Thm. 1.1, p. 706] bound the number of points of canonical height $\widehat{h}_L \leq 1/(256\, gD)$ over a number field of degree $D$ on a $g$-dimensional polarized abelian variety by

$$(200g)^{2g^2} D^g \max\{1, h_F, \log h^0(L), \log D\}^g.$$

Here $D = 1$, $g = 3$, $h^0(\Theta) = 1$ and $h_F(J) < 1$. The theorem gives at most $600^{18}$ points of height at most $1/768$. The computation below uses the smaller cutoff $256^{-3} < 1/768$. Choose representatives for $J(\mathbb{Q})/\Gamma$ in the half-open unit parallelepiped of $D_1, \ldots, D_4$. Divide each coordinate interval into 11956 equal parts. Two representatives in the same box differ by a point of height at most $16 \max H_{ii}/11956^2 < 256^{-3}$, by the triangle inequality for $\sqrt{\widehat{h}}$. Within each box, subtraction of a fixed representative is injective. Consequently

$$e \leq E := 11956^4\, 600^{18} < 2.076 \cdot 10^{66}.$$

**An explicit initial bound for integral points.** Write $H_X = |x|$. For $H_X \geq 64$, the equation forces $z = -y > 0$ with $H_X^{4/3}/2 < z < 2H_X^{4/3}$. This follows by substituting the endpoints into $z^3 + xz = H_X^4 - 1$. For a nonnegative $y$ and $x = -H_X$, either $y \leq H_X$ gives $x^4 + y^3 + xy \geq H_X^4 - H_X^2$, or $y > H_X$ gives $y^3 + xy > 0$. Set $t = x/z$, $w = 1/z$. The branch at infinity satisfies

$$w + tw^2 + w^4 = t^4, \qquad d = 1 + 2tw + 4w^3, \qquad \boldsymbol{\omega} = (-w, -t, 1)\, dt/d.$$

For $|t| \le 1/2$, evaluation at $t^4/2$ and $2t^4$ brackets the small positive branch. On this branch $7/8 \le d \le 5/4$. Thus the real Abel integral $u_P$ from $O$ on the infinity branch satisfies the componentwise bounds

$$|u_P| \le \left(\tfrac{16}{35}|t|^5,\ \tfrac{4}{7}|t|^2,\ \tfrac{8}{7}|t|\right), \qquad |t| \le 2H_X^{-1/3}.$$

Its first component has absolute value at least $2|t|^5/25$.

For $|t| \le 10^{-3}$ the displayed differential gives $u_P/t = (0,0,1) + [-2\cdot 10^{-3}, 2\cdot 10^{-3}]^3$. Write $z_P = A^{-1}u_P$. Integrate the theta derivative on the straight segment from 0 to $z_P$. Interval evaluation for characteristic 9 encloses the directional derivative in direction $A^{-1}u_P/t$ throughout the segment in one convex complex rectangle disjoint from the disk of radius $g(O)/2 > 0.6554$ about zero. Consequently $|\theta[\delta](z_P)| \ge |t|g(O)/2$. For $H_X \ge (2\cdot 10^3)^3$ the finite and infinite self-height formula above, $|t| \ge H_X^{-1/3}/2$, and $g(P) \le 2H_X^{4/3}\sum_j |(\nabla\theta[\delta](0)A^{-1})_j|$ give

$$\widehat{h}_\Theta([P-O]) \le \log H_X + 2.157 < \log H_X + 10.$$

Here the exponential correction in $L$ is bounded by $3\pi\|Y^{-1}\|_\infty(2\|A^{-1}\|_\infty 10^{-3})^2$. The enclosure is computed in `global_height.py`. Write $e[P-O] = \sum n_i D_i$ and $N = \max_i |n_i|$. Positivity of $H - I/10$ now yields

$$N \le E\sqrt{10(\log H_X + 10)}. \tag{†}$$

To get a first numerical bound, apply Gaudron [Gau06, Cor. 3.2] under hypothesis (1) of its §3.2. The details of this hypothesis matter for the three period entries. Choose centered real logarithms $v_i$ of $6D_i$ in a real period basis $\Omega_1, \Omega_2, \Omega_3$. There are integers $b_j$ with $6eu_P = \sum_i n_i v_i + \sum_j b_j \Omega_j$. The real inverse period matrix has infinity norm below two. Centering gives $|b_j| \le 2N + 12e$ on this branch. Put $c = (n_1, \dots, n_4, b_1, b_2, b_3)$, and use the fixed point $p = (6D_1, \dots, 6D_4, 0, 0, 0)$ in $A_* = J^7$, with logarithm $u = (v_1, \dots, v_4, \Omega_1, \Omega_2, \Omega_3)$. Define the homomorphism $\phi\colon A_* \to J$ by the integer coefficients $c$ and let $W_0 = \ker(d\phi)$. Since $[P-O]$ is nontorsion, $\phi(p) = 6e[P-O]$ is nontorsion and $W_0$ has codimension three.

In the additive quotient times $A_*$ the auxiliary point has additive component zero. Every connected algebraic subgroup is a product $V \times B$ of a vector subspace and an abelian subvariety. If it contains a nonzero multiple of the point then $\phi(B)$ contains a nontorsion point, and therefore equals the geometrically simple $J$. Thus $d\phi(t_B)$ is the entire tangent quotient. Modulo the graph, $(v, z)$ maps to $v - d\phi(z)$ after identifying the quotient with $t_J$. The image of $0 \times t_B$ already fills this quotient. Thus the subgroup tangent and the graph span the whole tangent space. This proves hypothesis (1) for every positive multiple. Take $B = 0$ as the parameter in Corollary 3.2 and $y = 1$.

For reference, the specialization of [Gau06, Cor. 3.2, Eq. (13)] used here is as follows. With one abelian variety, auxiliary abelian subvariety 0, and hypothesis (1) of its §3.2, the distance to the graph satisfies

$$\log d((0,u), W) \ \ge\ -c_7\, \mathfrak{a}^{1/t}(\log b + \mathfrak{a}\log\varepsilon)\left(1 + \frac{D\mathfrak{a}}{\log\varepsilon}\log a_1\right)^{g/t}, \qquad c_7 = (10(g+t))^{13(g+t)(1+g/t)}.$$

Here $W$ is the graph of $t_{A_*} \to t_{A_*}/W_0$. The parameters in the stated theorem take the following values.

| Parameter | Value or bound for L1 |
|---|---|
| Field, degree $D$, number of factors $n$ | $\mathbb{Q}$, 1, 1 (the single factor is $A_* = J^7$) |
| Polarization and dimension $g$ | product principal theta polarization, $g = 21$ |
| $W_0$, codimension $t$, auxiliary variety $B$, flag $y$ | $\ker d\phi$, 3, 0, 1 |
| $u_0$, $\log\varepsilon$, $\log a_1$ | 0, 1, 1000 |
| $\widehat{h}(p)$, $\|u\|^2$, $h_F(A_*)$ | $< 68$, $< 12$, $7h_F(J) < 7$ |
| $\mathfrak{a}$, $\log b$, $c_7$ | $\mathfrak{a} \le 1000$, $10 + 3\log\|c\|_2$, $240^{2496}$ |

For a column $v$ the squared Riemann norm is $(A^{-1}v)^* Y^{-1}(A^{-1}v)$. Summing over the seven entries gives the bounds in the table, so $\log a_1$ exceeds both $\widehat{h}(p)$ and $\varepsilon^2\|u\|^2/D$. In Eq. (9) of [Gau06],

$D = \log \varepsilon = 1$ and $h^0(A_*, L) = 1$, giving $\mathfrak{a} = 1 + \lfloor \max\{1, h_F(A_*), \log(1000)\} \rfloor \le 1000$. For Eq. (8), $d\phi$ maps the integral lattice onto $\gcd(c)\, t_J(\mathbb{Z})$, and the quotient norm is the norm on $t_J$ divided by $\|c\|_2$. Its degree is at most $10 + 3\log\|c\|_2$, since $|\widehat{\deg}(t_J)| < 10$ by the determinant of $(A^{-1})^* Y^{-1} A^{-1}$. All multiples of $u_0$ have height zero. Enlarging $\mathfrak{a}^{1/3}$ to 1000 gives $\mathcal{K} = 240^{2496}\, 1000(1+10^6)^7 < 10^{6100}$ and

$$\log d((0,u), W) \ge -\mathcal{K}\big(1010 + 3\log\|c\|_2\big).$$

The distance to the graph is at most the quotient norm of $6eu_P$, hence below $1000 E H_X^{-1/3}$. Also $\|c\|_2 \le 100E\sqrt{\log H_X + 10}$. If $T = \log H_X \ge 10^{6200}$, then

$$T \le 3\{\log(1000E) + \mathcal{K}[1010 + 3\log(100E\sqrt{T+10})]\} < T,$$

where division by $T$ makes the expression on the right decreasing on this range and the strict inequality is checked at the left endpoint. Thus $T < 10^{6200}$ and (†) gives $N < 10^{3168}$.

**Periods at 26000-bit precision.** To reduce this bound we give a second, faster construction of the needed periods. Deform $x^4 + y^3 = 1$ to $x^4 + y^3 + cxy = 1$ for $0 \le c \le 1$. The only possibly singular finite parameters satisfy $x^4 = -3/5$, $y^3 = -4/5$ and $|c| = 4(3/5)^{3/4}(5/4)^{1/3} > 1$. At $c = 0$ the inverse image of $[0,1]$ under $x^4$ is the bipartite graph on $(0,\eta)$ and $(\xi,0)$, where $\eta^3 = \xi^4 = 1$. Its complement is a disk since the point over infinity is totally ramified of index twelve. A spanning tree therefore gives an integral basis of six cycles. Take the tree edges with $\eta = 1$ or $\xi = 1$. Each of the other six cycles is conjugate to another, with its orientation preserved. The three sums of conjugate cycles form an integral basis of the conjugation-invariant lattice. Their integrals give the full real period lattice.

Write $a = (i+1)/4$, $b = (j+1)/3$. Orient an edge from $(0,\eta)$ to $(\xi,0)$. Set $x = \xi(sr)^{1/4}$, $y = \eta((1-s)r)^{1/3}$, $0 \le s \le 1$. The equation is $r + zr^{7/12} = 1$ with $z = c\xi\eta s^{1/4}(1-s)^{1/3}$. The branch $r(0) = 1$ in the variable $z$ continues for $|z| \le 1$ by inversion (its critical values have modulus $(12/7)(7/5)^{5/12} > 1$). The resulting paths continuously deform the original edges. Computing the residue differential in $(s,r)$, expanding by Lagrange inversion, then integrating Euler's beta integral gives

$$\int_{\eta\to\xi} x^i y^j \frac{dx}{F_y} = \frac{\xi^{i+1}\eta^{j+1}}{12} \sum_{k\ge 0} \frac{(-c\xi\eta)^k \Gamma(a + k/4)\Gamma(b + k/3)}{k!\,\Gamma(a + b - 5k/12)}.$$

Indeed the radial factor is $r^{a+b-1}/(1 + (7/12)zr^{-5/12})$, whose coefficient of $(-z)^k$ is $\binom{a+b-1+7k/12}{k}$. Reciprocal gamma zeros contribute zero. The ratio of terms twelve apart is rational at $c = 1$ after the root-of-unity factors cancel. For $k \ge 1000$ its absolute value is less than $2^{-18}$, using the three, four and five gamma-recurrence factors and the twelve factorial factors. Exact integer binary splitting and the first omitted term times two give directed bounds.

It remains to integrate from $P_2$ to $P_1$ and $P_5$. On the two paths use $y = s$, $x = -r$, where $r^4 - sr + s^3 - 1 = 0$ and $r(0) = 1$, for $-1 \le s \le 1$. The required forms are $(\psi_0, -\psi_1, s\psi_0)\, ds$, $\psi_j = r^j/(4r^3 - s)$. Implicit differentiation and polynomial reduction give the rational system $\Delta(s)\psi' = \mathcal{A}(s)\psi$ for $\psi = (\psi_0, \psi_1, \psi_2)$, where $\Delta = 256(s^3-1)^3 - 27s^4$. Its exact numerator matrix is reconstructed symbolically in `vertical_ode.py`. On a dyadic segment $s = a + hz$ expand $\Delta = \sum \Delta_j z^j$, $h\mathcal{A} = \sum \mathcal{A}_j z^j$. The Taylor coefficient $v_{n+1}$ is determined by

$$(n+1)\Delta_0 v_{n+1} = \sum_{j\ge 0} \big(\mathcal{A}_j - (n-j)\Delta_{j+1} I\big) v_{n-j}, \qquad v_k = 0 \quad (k < 0).$$

On each segment put $R = 4$ and define

$$d_0 = \frac{\sum_{j>0} |\Delta_j| R^j}{|\Delta_0|}, \qquad d_1 = \frac{R \max_a \sum_{b,j} |(\mathcal{A}_j)_{ab}| R^j}{|\Delta_0|}.$$

Subdivide until $d_0 + d_1 \le 4$ and $d_0 + d_1/16 \le 3/4$. Hence $\|v_n\| \le 50 \cdot 4^{16} 4^{-n}$ by induction. At a fixed binary scale a truncated division introduces at most one unit in the last place. Errors accumulate by

a factor at most four for the first sixteen steps and contract thereafter, yielding the explicit bound in `vertical.py`. The 60 segments give both integrals $h_-, h_+$. With $P_2$ as path origin, the real logarithms of $3D_2, 3D_1$ are $-h_- - h_+$ and $2h_- - h_+$. Add three times the corresponding edge path to $-h_- - h_+$ for $3D_3, 3D_4$. At 256 bits the two period constructions differ by a unimodular integral matrix and the two sets of logarithms agree modulo periods after allowing for their factors 3 and 6.

**The lattice reductions.** Center the four logarithms of $3D_i$ in the fundamental parallelepiped of the three real periods. Write their seven rows $u_1, \dots, u_7$. The period coefficients in $3eu_P = \sum_{i\le 4} n_i u_i + \sum_j b_j u_{4+j}$ satisfy $|b_j| \le \beta = 2N + 3E\|\Omega^{-1}\|_\infty \|u_P\|_\infty$. The inverse norm is below four. Given positive integer scales $s_j$, form the seven lattice rows in $\mathbb{Z}^7$ by adjoining $(\mathrm{round}(s_j u_{ij}))_{j=1}^3$ to the four unit rows and three zero rows in the first four coordinates. Each rounding is unique on its enclosing interval. For a point with $|x| \ge X$, let $(a_1, a_2, a_3)$ be the three component bounds above at $|t| = 2X^{-1/3}$. The resulting nonzero lattice vector has squared norm at most

$$4N^2 + \sum_{j=1}^{3} \left(3Es_j a_j + (4N + 3\beta)/2\right)^2 .$$

It is nonzero because its first four entries are the $n_i$. A unimodular reduction supplies a basis whose smallest squared Gram–Schmidt length exceeds this upper bound. Every nonzero lattice vector has length at least the smallest such length, by projecting onto the last nonzero Gram–Schmidt direction. These comparisons use exact rational arithmetic on the integer basis. The first pass takes $s_1 = s_2 = s_3 = 10^{7500}$ and excludes $X = 10^{14000}$. Reinsertion in (†) gives $N < 1.179 \cdot 10^{69}$. The next two passes, with scales adapted to the three decay exponents, exclude $X = 10^{182}$ and then $X = 10^{181}$. The archive gives all seven-row constructions and the outwardly rounded integer bounds for both sides of every comparison. We have proved $|x| < 10^{181}$ for every integral point. □

### 4.18.2 From the height bound to the integral points

*Proof of Theorem 4.18.1.* Let $P = (x, y)$ be an affine integral point. Proposition 4.18.2 gives $|x| < 10^{181}$. For each prime at which the subgroup generated by the four $D_i$ is saturated, the coordinates of $[P - O]$ in this basis lie in $\mathbb{Z}_\ell$. Its coefficient vector modulo $\ell^a$ therefore makes sense independent of the unknown index $e$. At 2 independence of the Kummer images proves saturation. At $3, 5, 11, 13$ the verifier exhibits four independent linear characters. For example, for $\ell = 3$ the primes $2, 3, 7, 17$ give slopes $(0,0,1,0), (1,2,0,1), (0,0,1,2), (0,1,2,0)$ modulo three. Each row comes from multiplying reductions by $\#J(\mathbb{F}_q)/\ell$ and taking a discrete logarithm in a cyclic group of order $\ell$. The existence of four independent rows shows that the generators map bijectively to $J(\mathbb{Q})/\ell J(\mathbb{Q})$.

**The first coefficient restrictions.** On the affine 2-adic disks evaluate the bitangent and the logarithms. Split a residue disk until changing the argument changes the bitangent value by an element of valuation more than its valuation plus twice the valuation of 2 at each dyadic prime. The resulting mask is constant. For the logarithms, expand $\omega$ in the smooth coordinate, integrate term by term and include the central logarithm from the principal-divisor trace. To compare triples of integrals, choose the three-by-three minor of the four basis rows having smallest valuation. Multiplication by its adjugate and division by its determinant gives coordinates in this local lattice. Intersect those coordinates with the bitangent mask. Of the $16^4$ coefficient vectors modulo 16, 768 pass the dyadic test. Finite reductions at 11 and 113 leave 568. At 3 the analogous logarithm computation gives 396 coefficient vectors modulo 9. For each candidate pair modulo 16 and 9 require its two projected reductions to occur at the same affine point in each finite field. The $568 \cdot 396$ pairs drop to 13196.

At $p = 5, 11, 13$ compute the logarithms on all the integral residue disks. One may do this without a global group basis for the disk centers. Choose functions of pole order at most 24 whose divisors modulo $p$ consist of the listed centers with multiplicities at most three. The multiplicity matrix is invertible modulo $p$. Hensel lifting its distinguished factors and taking traces of the local integrals

gives a linear system for all the central logarithms. Newton sums supply the power traces. For a factor of degree $h \le 3$ the tail of its $n$th integrated term has valuation at least $\lceil n/h \rceil - v_p(n)$, as in Section 4.8. The logarithm divided by $p$ varies modulo $p$ along the affine line through its central value in the tangent direction. Enumerate the four coefficients modulo $p$, applying this condition in each disk; then intersect with projected curve reductions in the finite Jacobians. Simultaneous matching uses both coordinates of the *same* residue point for all projections. The three finite lists join to 188 vectors modulo $M_0 = 16 \cdot 9 \cdot 5 \cdot 11 \cdot 13 = 102960$. At $q = 271,883,353$ their counts become $72, 40, 36$. All 36 are congruent, coordinate by coordinate, modulo $M_* = M_0/4 = 25740$ to exactly one of

$$k_1 = (1,0,0,0), \quad k_2 = (0,1,0,0), \quad k_3 = (0,0,1,0), \quad k_4 = (0,0,0,1), \quad k_5 = (-1,-1,0,0).$$

It follows that $[P - P_i] = M_* D$ for some $D \in J(\mathbb{Q})$ and one of the five indicated $i$. This divisibility holds in the full rational group because the four generators are saturated at every prime dividing $M_*$. The archive contains the finite lists, all disk relations and a replay from the curve equation.

**Refining the coefficient modulus.** For $\ell \in \{3,5,7\}$ write $D \equiv \sum t_j D_j \bmod \ell J(\mathbb{Q})$. To justify and constrain this description simultaneously, put $N_q = \#J(\mathbb{F}_q)$, $s = N_q / \gcd(N_q, M_* \ell)$. The reductions $sM_* D_j$ are killed by $\ell$. Use primes at which their span is cyclic of order $\ell$, take a generator $g$ and write $sM_* D_j = v_j g$. A possible coefficient vector must satisfy

$$s[P_i - O] + (v \cdot t)g \ \in \ \{s[R - O] : R \in C_{\mathrm{aff}}(\mathbb{F}_q)\}.$$

If $\sum t_j D_j$ is divisible by $\ell$ in the full rational group, its projection under $sM_*$ vanishes since $sM_* \ell$ annihilates the finite group. Thus every such relation is killed by each slope. The slope matrices have rank four. Equality of rank and saturation follow from the known rational rank and absence of torsion. Enumerating every $t \in \mathbb{F}_\ell^4$ therefore covers all rational possibilities. The 44 auxiliary tables give the following sizes, in the order $P_1$ through $P_5$.

| $\ell$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ |
|---|---|---|---|---|---|
| 3 | 18 | 3 | 24 | 18 | 54 |
| 5 | 5 | 9 | 1 | 1 | 5 |
| 7 | 2 | 3 | 2 | 6 | 2 |

The initial vectors specify the coefficients of $D$ modulo four. Apply the ordinary Chinese remainder theorem with moduli $4, 3, 5, 7$. Multiplication by $M_*$ and addition of $k_i$ give 7224 distinct necessary coefficient classes for $[P - O]$ modulo $M = 10810800$.

**An integer contact test.** For a center $Q = (a, b)$ put $u = x - a$, $v = y - b$. For each chosen pole bound $\mu$, use the monomials $u^i v^j$ with $0 \le j < 3$, $3i + 4j \le \mu$. They form a basis of $L(\mu O)$. Require the first $r = \mu - 3$ Taylor coefficients at $Q$ to vanish by substituting the formal solution $v = v(u)$ of the curve. Exact linear algebra supplies an integral polynomial $f_Q = \sum c_{ij} u^i v^j$. Define $C_Q = \sum |c_{ij}|\, 2^i 3^j$. If $H_0 = 10^{181}$, the curve equation implies $|y| \le 2H_0^{4/3}$ for $|x| \le H_0$, whence $|f_Q(P)|^3 \le C_Q^3 H_0^\mu$. If a prime $q \nmid 3b^2 + a$ has $P \equiv Q \pmod q$, the same formal series is integral at $q$ and converges on the residue disk. Thus $q^r \mid f_Q(P)$. For a product $\Pi$ of distinct such primes, the integer inequality

$$\Pi^{3r} > C_Q^3 H_0^\mu \quad \Longrightarrow \quad f_Q(P) = 0$$

proves an exact consequence of the height bound. Eliminate $y$ from $F = f_Q = 0$, factor the integer resultant in $x$, and test each integral root in $F(x, y)$ and $f_Q(x, y)$. Each of the five functions has just its own center as an integer zero on $C$. The chosen pole orders are $30, 30, 38, 30, 30$, respectively. The minimum sufficient integer products have $74, 73, 72, 73, 74$ decimal digits. The coefficients, the products and the rational polynomial operations are given in `l1_contact.py` and its data file.

**Closing every class.** For each surviving residue vector $v$ and each good prime $q$, put $s = N_q / \gcd(N_q, M)$. Compute every affine $R$ satisfying

$$s[R - O] = \sum_j v_j \, sD_j \quad \text{in } J(\mathbb{F}_q).$$

An empty fiber rules out the residue vector. A fiber consisting solely of its designated center modulo $q$ contributes $q$ to the contact product, provided $F_y$ is a unit there. Once the product passes the displayed threshold, the integer point must equal its center. Across 80 prime tables, empty fibers eliminate 7213 vectors and the contact inequality settles the other 11. After tables 11, 21, 31 and 41 there are respectively 768, 132, 24 and 4 vectors still to check. The last vector closes at $q = 35059$.

The finite arithmetic can be reconstructed directly. Represent a reduced divisor of degree at most three by its affine ideal in $\mathbb{F}_q[x, y]/(y^3 + xy + x^4 - 1)$, as a free module over $\mathbb{F}_q[x]$ with three monic generators having leading weights distinct modulo three. Products of the nine pairs generate the product ideal. Polynomial elimination over $\mathbb{F}_q[x]$ cancels equal leading weight residues by multiples of powers of $x$. The smallest-weight element $f$ in the product ideal $I$ determines the residual divisor via $(f) : I$. Compute this colon by reducing $hI$ modulo $f$ for each successive monomial $h$, keeping the independent residue columns and their first three leading relations. This gives the unique least-degree representative of the negative class. Repeating the residual operation negates it back to the sum. All affine points are enumerated: for $x = g^{2k+\epsilon}$, scale $y = g^k u$ and use the value table of $u^3 + g^\epsilon u$; treat $x = 0$ separately. The verifier checks the group orders, includes a comparison to the independent $L(14O - D)$ implementation of the divisor arithmetic [KM04], and recomputes the full fibers.

For the order check one may use the three real Frobenius traces $a_i \in [-2\sqrt{q}, 2\sqrt{q}]$. Their sum is $t = q + 1 - \#C(\mathbb{F}_q)$, their pair sum lies in $[(t^2 - 12q)/2, t^2/3]$ and their product has absolute value at most $8q^{3/2}$. This gives an interval for $\prod(q + 1 - a_i)$. Exact orders of curve classes constrain the group order to multiples of their least common multiple. When needed, $\#C(\mathbb{F}_{q^2})$ sharpens the interval, or the first three extension counts give the order outright by Newton's identities. The final verifier uses these certificates independently of how a candidate order was found. Thus every integral point is one of the five displayed pairs, and direct substitution verifies all five. □

# 5 Primitive generalized Fermat equations

Primitivity means $\gcd(x, y, z) = 1$. Each proof reduces to finitely many covering curves and then determines the relevant rational or number-field points. All signs in the lists below are independent.

## 5.1 $x^4 + 3y^3 + z^3 = 0$ **(**$H = 48$**)**

**Theorem 5.1.1.** *The only primitive integer solutions of* $x^4 + 3y^3 + z^3 = 0$*, that is, integer solutions with* $\gcd(x, y, z) = 1$*, are*

$$(x, y, z) = (\pm 1, 0, -1), \qquad (\pm 895, -6202, 4199).$$

**Setup.** Put $X = x$, $Y_0 = -y$, $Z_0 = -z$. Then the equation becomes

$$Z_0^3 + 3Y_0^3 = X^4$$

For a primitive solution, $X \neq 0$, $\gcd(Y_0, Z_0) = 1$ and $3 \nmid XZ_0$. Indeed, if $X = 0$, then $Z_0^3 = -3Y_0^3$ gives $Y_0 = Z_0 = 0$. A common prime factor of $Y_0, Z_0$ also divides $X$. If 3 divides one of $X$ and $Z_0$, then by the equation it divides both; then $27 \mid 3Y_0^3$, so $3 \mid Y_0$, a contradiction.

We use three fields.

- $K = \mathbb{Q}(\theta)$, $\theta^3 = 3$. The unit $\varepsilon = 4 + 3\theta + 2\theta^2$, $\varepsilon^{-1} = \theta^2 - 2$.
- $L = \mathbb{Q}(\theta, \xi)$, $\xi^2 = 3 - 2\theta$ (degree 6). $\xi$ is a root of $T^6 - 9T^4 + 27T^2 - 3$.

- $M = K(R_0, W)$, $R_0^2 = 9 + 6\theta + 4\theta^2 = \theta^2\varepsilon$, $W^2 = 6 + 2\theta + 2R_0$ (degree 12).

The proof runs as follows. A fourth-power descent over $K$ gives four plane quartic curves $C_j$ (Step 1). The even $j$ are settled by elliptic curves over $K$ (Step 2). The case $j = 1$ is eliminated by congruences, and $j = -1$ becomes the problem of finding the rational points of the genus 2 curve $v^2 = f(q)$ (Step 3). A two-cover descent on this curve (Step 4) lifts all its points to an elliptic curve $E$ over the degree 12 field $M$ (Step 5). We show $\mathrm{Cl}(M)[2] = 0$ (Step 6) and $\operatorname{rank} E(M) = 6$ (Step 7), and we obtain $q \in \{0, -8/3\}$ by a sieve at 661 (Step 8) and elliptic Chabauty (Step 9).

**The disk argument.** We first record a fact that is used repeatedly in this section and in Sections 5.2–5.3.

**Lemma 5.1.2.** *Let $p \geq 3$, and let $\Lambda(T) = a_0 T + \sum_{n\geq 2} a_{n-1} T^n/n$ with $a_0 \in \mathbb{Z}_p^\times$, $a_i \in \mathbb{Z}_p$. Then the only $T \in p\mathbb{Z}_p$ with $\Lambda(T) = 0$ is $T = 0$.*

*Proof.* If $T \neq 0$ and $n \geq 2$, then $v_p(a_{n-1}T^n/n) \geq nv_p(T) - v_p(n) > v_p(T) = v_p(a_0T)$, because $(n-1)v_p(T) \geq n - 1 > v_p(n)$. These valuations tend to infinity, so the sum of the tail has larger valuation than the linear term and cannot cancel it. □

In elliptic Chabauty (Proposition D), for a local parameter $T$ of a residue disk, we take $\Lambda$ to be the composition of a global annihilator with the elliptic logarithm. This $\Lambda$ vanishes at every rational point in the disk. Since $\Lambda'$ is the pullback differential, if the map and the differential are integral on the disk and $\Lambda'(0)$ is a unit, then by Lemma 5.1.2 the only rational point in the disk is its center.

**Step 1: descent over the cubic field.**

**Lemma 5.1.3.** *(1) $\mathcal{O}_K = \mathbb{Z}[\theta]$, $\operatorname{disc} K = -243$, $h(K) = 1$, $\mathcal{O}_K^\times = \{\pm\varepsilon^n\}$.*

*(2) For each primitive solution we have*

$$Z_0 + \theta Y_0 = \varepsilon^j \beta^4, \qquad j \in \{0, 1, 2, -1\}, \qquad \beta = a + b\theta + c\theta^2,$$
$$a, b, c \in \mathbb{Z}, \qquad \gcd(a, b, c) = 1, \qquad 3 \nmid N\beta.$$

*and $|X| = |N\beta|$. Hence $(a : b : c)$ is a rational point of the plane quartic curve $C_j$ : $[\varepsilon^j(a + b\theta + c\theta^2)^4]_{\theta^2} = 0$. Here $[\,\cdot\,]_{\theta^2}$ denotes the coefficient of $\theta^2$ in the basis $1, \theta, \theta^2$.*

*Proof.* (1) $T^3 - 3$ is Eisenstein at 3 and its discriminant is $-3^5$, so $\mathcal{O}_K = \mathbb{Z}[\theta]$. The Minkowski constant is $\frac{4}{\pi} \cdot \frac{3!}{3^3}\sqrt{243} < 4.42$, and the only prime ideals of norm 2, 3, 4 are $(\theta - 1)$, $(\theta)$, $(\theta^2 + \theta + 1)$, so $h(K) = 1$. The signature is $(1, 1)$, so the unit rank is 1. For a unit with $1 < \eta < \varepsilon$, the other two conjugates have absolute value less than 1, and solving for the coefficients from the three embeddings gives $\eta = a + b\theta + c\theta^2$ with $0 \leq a \leq 4$, $0 \leq b \leq 3$, $0 \leq c \leq 2$. In this range the only elements whose norm $a^3 + 3b^3 + 9c^3 - 9abc$ equals 1 are 1 and $\varepsilon$ (certificate 1.2.1a). Hence $\varepsilon$ is the fundamental unit.

(2) If a prime ideal $\mathfrak{p}$ above $p \neq 3$ divides $Z_0 + \theta Y_0$, then $\mathfrak{p} \nmid Y_0$ (otherwise $\mathfrak{p} \mid Z_0$), and $\theta \equiv -Z_0/Y_0 \pmod{\mathfrak{p}}$. Since $T^3 - 3$ has no repeated root modulo $p$, such a $\mathfrak{p}$ is the only one among the prime ideals above $p$, and it has residue degree 1. Therefore $v_\mathfrak{p}(Z_0 + \theta Y_0) = v_p(X^4)$ is a multiple of 4. Since $3 \nmid X$, $(\theta)$ does not divide it. Hence $(Z_0 + \theta Y_0)$ is the fourth power of an ideal, and by (1), $Z_0 + \theta Y_0 = \pm\varepsilon^j\beta^4$. The norm $X^4$ is positive, $N(-1) = -1$ and $N\varepsilon = 1$, so the sign is $+$. A prime dividing all of $a, b, c$ would divide $Y_0, Z_0$, so $\gcd(a, b, c) = 1$. We have $(N\beta)^4 = X^4$ and $3 \nmid X$. Finally, the $\theta^2$-coefficient of $Z_0 + \theta Y_0$ is 0. □

**Step 2: the even case.** For a point of $C_j$, define $Y_0, Z_0 \in \mathbb{Q}$ by $\varepsilon^j\beta^4 = Z_0 + \theta Y_0$, and put $n = N\beta$, $\nu = n/\beta^3$, $\lambda = (\theta Y_0 - Z_0)/(\theta Y_0 + Z_0)$. From $(Z_0 + \theta Y_0)(Z_0^2 - \theta Y_0 Z_0 + \theta^2 Y_0^2) = Z_0^3 + 3Y_0^3 = n^4$ we get $4\nu^4 = \varepsilon^{3j}(1 + 3\lambda^2)$, and hence

$$\varphi_j : C_j \longrightarrow E_j : V^2 = U^3 - 36\varepsilon^j U, \qquad (U, V) = (12\varepsilon^{-j}\nu^2,\ 36\lambda\nu)$$

is a map over $K$. Written in homogeneous coordinates, it has no base points at the primes used below.

**Lemma 5.1.4.** *$C_2(\mathbb{Q}) = \varnothing$ and $C_0(\mathbb{Q}) = \{(1:0:0), (0:1:0)\}$. The only primitive solutions coming from even $j$ are $(\pm 1, 0, -1)$.*

*Proof.* If $j$ is even, then $U^3 - 36\varepsilon^j U = U(U - 6\varepsilon^{j/2})(U + 6\varepsilon^{j/2})$, so all 2-torsion points of $E_j$ are $K$-rational. We carry out the full 2-descent of [Sim02, Sil09] with the square class generators $-1, \varepsilon, \theta - 1, \theta^2 + \theta + 1, \theta$. At the two places above 2 the local images have sizes 8 and 16, and at 3 the size is 4. Of the $32^2$ global candidate pairs, 16 survive for $E_0$ and 4 for $E_2$. On $E_0$, the 2-torsion and the two points

$$A = (-3, 9), \qquad B = (6\theta - 6\theta^2,\ 36 - 36\theta + 12\theta^2)$$

fill all 16. Hence $\operatorname{rank} E_0(K) = 2$, $\operatorname{rank} E_2(K) = 0$, and $\langle A, B, E_0[2]\rangle$ has odd index. Reduction at the primes 5, 11 ($E_0$) and 61, 67 ($E_2$) of residue degree 1 and [Kat81, Appendix] show that the torsion is just $E_j[2]$ (certificate 1.2.1a).

Since $\nu \neq 0$, a rational point of $C_2$ maps to a point with $U \neq 0$. For $U = \pm 6\varepsilon$ we would need $\pm\varepsilon^3/2$ to be a square in $K$, and it is not (certificate 1.2.1a). So the image is not a torsion point, which contradicts rank 0. Hence $C_2(\mathbb{Q}) = \varnothing$.

For $C_0$ we apply [BS10] with $p = 577$. The prime 577 splits completely with $\theta \equiv 260, 329, 565$, and all three reductions have $E_0(\mathbb{F}_{577}) \cong (\mathbb{Z}/24)^2$. The subgroup $H$ of the product generated by the reductions of $A, B, E_0[2]$ has order 576. Since $[8]A$, $[8]B$ are independent in the 3-torsion of the product, the index of $\langle A, B, E_0[2]\rangle$ is prime to 3; being odd, it is prime to the order $576^2 = 2^{12}3^4$ of the quotient. Hence the reduction of $E_0(K)$ is exactly $H$. A full scan of $\mathbb{P}^2(\mathbb{F}_{577})$ finds 572 points on $C_0$, and the only ones whose image under $\varphi_0$ lies in $H$ are the reductions of $(1:0:0)$ and $(0:1:0)$ (certificate 1.2.1b).

We apply Proposition D to the two remaining disks. Lifting the three roots $\theta$ modulo $577^3$ and computing the logarithm of $\omega = dU/(2V)$ (Lemma E), we get, modulo $577^2$,

$$\tfrac{1}{577}\log A \equiv (4351, 4351, 4351), \qquad \tfrac{1}{577}\log B \equiv (55622, 183530, 93777)$$

The cross product of the two normalized logarithms is an integral annihilator that kills all logarithms of $E_0(K)$; modulo 577 it is $(28, 304, 245)$. With the parameter $b/a$ at $(1:0:0)$ and $a/b$ at $(0:1:0)$, the coefficients of $\varphi_0^*\omega$ at the centers are $\theta$ and $-\theta^2/3$, respectively, and their combinations with the annihilator are 496 and 241 modulo 577 (certificate 1.2.1b). $C_0$ is smooth at 577, and the derivatives of the dependent coordinate are 4 and 12, which are units. By Lemma 5.1.2, each disk contains only its center.

The point $(0:1:0)$ gives $\beta = \theta$, $N\beta = 3$, which violates $3 \nmid N\beta$. The point $(1:0:0)$ gives $\beta = \pm 1$, $Z_0 + \theta Y_0 = 1$, so $(X, Y_0, Z_0) = (\pm 1, 0, 1)$, that is, $(x, y, z) = (\pm 1, 0, -1)$. □

**Step 3: the odd case and a genus 2 curve.** We use the following polynomials.

$$\begin{aligned}
P(m,n) &= -720m^6 + 1944m^5n - 1620m^4n^2 - 60m^3n^3 + 810m^2n^4 - 432mn^5 + 73n^6,\\
Y(m,n) &= 84m^4 - 216m^3n + 216m^2n^2 - 100mn^3 + 18n^4,\\
Z(m,n) &= -108m^4 + 312m^3n - 324m^2n^2 + 144mn^3 - 23n^4,\\
f(q) &= 16q^6 + 72q^5 + 180q^4 + 300q^3 + 270q^2 + 108q + 9.
\end{aligned}$$

We have $Z^3 + 3Y^3 = P^2$, and $f$ is irreducible with discriminant $2^{18}3^{25}$ (certificate 1.2.1c).

**Lemma 5.1.5.** *There is no primitive solution with $j = 1$. For a primitive solution with $j = -1$, there are coprime integers $m, n$ ($n > 0$, $2 \mid m$, $\gcd(n, 6) = 1$) and $w > 0$ such that*

$$w^2 = P(m,n), \qquad (x, y, z) = (\pm w,\ -Y(m,n),\ -Z(m,n))$$

*Moreover, if we put $q = (2n - 3m)/(2m - n)$ and $v = w/(2m - n)^3$, then $v^2 = f(q)$, and $q$ has even numerator and odd denominator.*

*Proof.* $j = 1$: Modulo 2 the equation of $C_1$ is $b^4 \equiv 0$, so $b$ is even. If $b$ is even, then modulo 8 we would need $2a^4 + 6a^2c^2 + 4c^4 \equiv 0$, but in the three cases where $a, c$ are not both even the values are $2, 4, 4$ (certificate 1.2.1c). This contradicts $\gcd(a, b, c) = 1$.

$j = -1$: We have $\varepsilon^{-1} = \theta^2 - 2$. Writing $\beta^2 = A + B\theta + C\theta^2$, the equation of $C_{-1}$ becomes the conic

$$A^2 - 4AC - 2B^2 + 6BC = 0$$

The integers $A, B, C$ are coprime. Indeed, if a prime $\ell$ other than 3 divides all of them, then $\beta$ is a nilpotent element of $\mathbb{Z}[\theta]/\ell$ (a reduced algebra), so $\ell \mid \beta$; and if 3 divides all of them, then $3 \mid N\beta$. If $A = 0$, then $B = 0$ or $B = 3C$, and then $N\beta^2$ is $\pm 9$ or $\pm 90$, which violates $3 \nmid N\beta$. If $A \neq 0$, the equation is linear in $C$, so putting $B/A = m/n$ (in lowest terms, $n > 0$) we get

$$(A : B : C) = (h_A : h_B : h_C) = \big(2n(3m - 2n) : 2m(3m - 2n) : 2m^2 - n^2\big)$$

The gcd $g$ of the three forms is 1 if $n$ is odd and 2 if $n$ is even, and $N(h_A + h_B\theta + h_C\theta^2) = -P(m, n)$. We have $\beta^2 = \pm g^{-1}(h_A + h_B\theta + h_C\theta^2)$, and $(N\beta)^2$ must be a perfect square. But if $n$ is even, then $\pm N(h/2) \equiv 2 \pmod 4$, and if $n, m$ are both odd, then $\pm N(h) \equiv 5, 3 \pmod 8$. Hence $m$ is even, $n$ is odd, and

$$\beta^2 = -(h_A + h_B\theta + h_C\theta^2), \qquad (N\beta)^2 = P(m, n)$$

From $P(m, n) \equiv n^6 \pmod 3$ and $3 \nmid N\beta$ we get $3 \nmid n$. Now $Z_0 + \theta Y_0 = (\theta^2 - 2)\beta^4 = Z(m, n) + \theta Y(m, n)$ and $X^4 = P(m, n)^2$, so with $w = |N\beta|$ we get $(x, y, z) = (X, -Y_0, -Z_0) = (\pm w, -Y(m, n), -Z(m, n))$.

With $\ell = 2m - n$, $k = 2n - 3m$ we have $(m, n) = (k + 2\ell, 2k + 3\ell)$, and the identity $P(k + 2\ell, 2k + 3\ell) = \ell^6 f(k/\ell)$ gives $v^2 = f(q)$. Since $n$ is odd and $m$ is even, $\ell$ is odd and $k$ is even. □

**Step 4: two-cover descent.** Put

$$r = \tfrac{1}{4}\big(-3 + \theta - \theta^2 + (3 + 3\theta + \theta^2)\xi\big), \qquad \delta = \tfrac{1}{2}(3 - 3\theta + \theta^2)(1 + \xi),$$
$$\pi_0 = \theta - 1, \qquad \pi_1 = -1 + \theta - \theta^2 + 2\theta\xi + \delta.$$

Then $f(r) = 0$.

**Lemma 5.1.6.** *The pair $(q, v)$ of Lemma 5.1.5 satisfies*

$$q - r = c\,\pi_1\gamma^2, \qquad c \in \mathbb{Q}^\times,\ \gamma \in L^\times$$

*Proof.* An integral basis of $L$ is $(1, \theta, \theta^2, \xi, \theta\xi, \delta)$, and $\operatorname{disc} L = 2^4 3^{11}$, $h(L) = 1$. Above 2 there are the prime ideals $(\pi_0)$, $(\pi_1)$ of norm 4, and $2/(\pi_0\pi_1^2)$ is a unit. The prime 3 is totally ramified as $(\xi)^6$. The square classes of units are generated by $-1$, $\theta^2 - 2$, $u_2 = -1 + \theta\xi + \delta$, $u_3 = \theta - 1 - \xi$, and the identity $3/\xi^6 = (\theta^2 - 2)(52 + 36\theta + 25\theta^2)^2$ holds (certificate 1.2.1d).

By [BS09], the class of $q - r$ in $L^\times/L^{\times 2}\mathbb{Q}^\times$ is unramified outside the primes 2, 3 dividing the leading coefficient and the discriminant of $f$. Since $N(q - r) = f(q)/16 = (v/4)^2$ and $(\xi)$ is the only prime ideal above 3 (of residue degree 1), $v_\xi(q - r)$ is even. Modulo $\mathbb{Q}^\times$ the classes of $-1$ and $\theta^2 - 2 \equiv 3$ disappear, and since $2 \equiv \pi_0 \cdot (\text{unit})$, the class of $\pi_0$ also becomes a unit class. Hence the global candidates are the eight classes $u_2^a u_3^b \pi_1^c$ $(a, b, c \in \{0, 1\})$.

By Lemma 5.1.5, $q \in 2\mathbb{Z}_2$. For $q_0 = 0$ and for $q_0 = 2$, the $(\pi_0, \pi_1)$-valuations of $q_0 - r$ are $(-1, -1)$, and those of $4/(q_0 - r)$ are $(3, 5)$, which exceed $2v(2) = (2, 4)$. By Hensel's lemma, the square class of $q - r$ is constant on $4\mathbb{Z}_2$ and on $2 + 4\mathbb{Z}_2$. We now compare the local square classes of $-r$ and $2 - r$ with the eight candidates multiplied by the scalars $\pm 1, \pm 2, \pm 5, \pm 10$ of $\mathbb{Q}_2$. The comparison is exact: we check against the 576 squares of units of $\mathcal{O}_L/8\mathcal{O}_L$. If $q \in 4\mathbb{Z}_2$, the only matching candidate is $\pi_1$; if $q \in 2 + 4\mathbb{Z}_2$, no candidate matches (certificate 1.2.1d). Hence $q \in 4\mathbb{Z}_2$ and the class of $q - r$ is $\pi_1$. □

**Step 5: an elliptic curve over the degree 12 field.** Let $\xi_1, \xi_2$ be the two roots of $T^2 - WT + R_0$. Put

$$R(T) = \tfrac{1}{16}(T^5 - T^4 - 12T^3 + 4T^2 + 39T - 15), \qquad \Pi(T) = \tfrac{1}{8}(T^5 - T^4 - 8T^3 + 8T^2 + 27T - 11)$$

Then $r = R(\xi)$ and $\pi_1 = \Pi(\xi)$. Put $r_i = R(\xi_i)$ and $D_* = \Pi(\xi_1)\Pi(\xi_2)$. Also put

$$d = -3 - 2\theta + 3\theta^2 + \big(\theta + \tfrac{5}{6}\theta^2\big)W + \big(1 - \tfrac{1}{2}\theta^2\big)W^2 - \tfrac{\theta}{12}W^3, \qquad E:\ y^2 = x^3 + 2dx^2 + 2d^2x$$

We have $c_4(E) = -32d^2$, $\Delta_E = -256d^6$, $j(E) = 128$, $N_M(d) = -5184 = -2^6 3^4$.

**Lemma 5.1.7.** *(1)* $[M : \mathbb{Q}] = 12$, *and* $M$ *has signature* $(2, 5)$.

*(2) All points of Lemma 5.1.6 lift to* $M$*-points* $(q, V)$, $q \in \mathbb{Q}$, *of the quartic curve*

$$\mathcal{Q}:\ V^2 = Q(q) := D_* \frac{f(q)}{(q - r_1)(q - r_2)}$$

*Here* $Q$ *is a separable quartic over* $M$, *and* $Q(0) = (2\theta^2)^2$.

*(3) Write* $Q(q) = a_4q^4 + a_3q^3 + a_2q^2 + a_1q + e^2$ *with* $e = 2\theta^2$, *and put*

$$X' = \frac{2e(V + e) + a_1q}{q^2}, \quad Y' = \frac{(X'^2 - 4e^2a_4)q - (a_1X' + 2e^2a_3)}{2e}, \quad x = \frac{X' - h_0}{s_0}, \quad y = \frac{Y'}{s_0e}$$

*(*$s_0 = 12\theta$, $h_0 = (2ds_0 - a_2)/3$*). Then* $\varphi : (q, V) \mapsto (x, y)$ *is a map* $\mathcal{Q} \to E$, *and* $\varphi^*\big(dx/(2y)\big) = -\theta^2\, dq/V$.

*(4) The two points* $(0, e)$, $(0, -e)$ *above* $q = 0$ *map to* $O$ *and to a point* $P$, *and the two points above* $q = -8/3$ *map to* $P_1$ *and* $P - P_1$. *Here* $P, P_1 \in E(M)$.

*Proof.* (1) $\varepsilon$ is not a square in $K$, because its residue at the prime ideal above 5 with $\theta \equiv 2$ is 3. $N_{K(R_0)/K}(W^2) = (6 + 2\theta)^2 - 4R_0^2 = -12\theta^2$ is negative at the real embedding of $K$, so $W^2$ is not a square in $K(R_0)$. Since $\varepsilon > 0$, $K(R_0)$ has two real embeddings, and the two values of $W^2$ at them have negative product, so exactly one of them is positive. Hence $M$ has 2 real embeddings.

(2) By the identity $T^6 - 9T^4 + 27T^2 - 3 = (T^2 - 3 + 2\theta)(T^2 - WT + R_0)(T^2 + WT + R_0)$, the maps $\xi \mapsto \xi_i$ are two embeddings $\sigma_i$ of $L$ into $\overline{M}$. Applying $\sigma_1, \sigma_2$ to the relation of Lemma 5.1.6 and multiplying gives $(q - r_1)(q - r_2) = D_*H^2$ with $H = c\,\sigma_1(\gamma)\sigma_2(\gamma)$. The elements $H$, $r_1 + r_2$, $r_1r_2$, $D_*$ are symmetric under $\xi_1 \leftrightarrow \xi_2$, so they lie in $M$. Hence $Q(q) = (v/H)^2$. From $r_1r_2 = \theta^2 D_*/4$ we get $Q(0) = 4 \cdot 9/\theta^2 = (2\theta^2)^2$.

(3), (4) By the standard Weierstrass formulas for a quartic, $Y'^2 = X'^3 + a_2X'^2 + (a_3a_1 - 4a_4e^2)X' + a_3^2e^2 + a_4a_1^2 - 4a_4a_2e^2$, and a change of coordinates gives $E$. All identities are checked by polynomial division in $M$. The coordinates of $P$, $P_1$ and the two limits are also checked by exact substitution (certificate 1.2.1e). □

**Step 6: the class group of $M$.**

**Lemma 5.1.8.** $\mathrm{Cl}(M)[2] = 0$.

*Proof.* We use twice the ambiguous class number formula for a quadratic extension $B/A$ ([Lem13, Theorem 1])

$$|\,\mathrm{Cl}(B)^{\mathrm{Gal}(B/A)}| = \frac{h(A)\,2^{t-1}}{[\mathcal{O}_A^\times : \mathcal{O}_A^\times \cap N_{B/A}B^\times]}$$

($t$ is the number of ramified places, infinite places included). If this value is odd, then $h(B)$ is odd as well. Indeed, the generator $\sigma$ acts as an involution on the $\mathbb{F}_2$-space $\mathrm{Cl}(B)[2]$, and an involution on a nonzero space has a nonzero fixed vector.

Put $F = K(\kappa)$, $\kappa = R_0/\theta$, $\kappa^2 = \varepsilon$. Since $\varepsilon$ is a unit and is positive at the real embedding, $F/K$ can ramify only at places above 2. At the dyadic place of degree 1 we have $\theta \equiv 3$ and $\varepsilon \equiv 7 \pmod 8$, and

at the dyadic place of degree 2 we have $\theta^2+3\theta+1\equiv 0$ and $\varepsilon\equiv 2+\theta \pmod 4$, which is not a square; so both places ramify. Hence $t=2$, $\mathcal{O}_F=\mathbb{Z}[\theta,\kappa]$ and $\operatorname{disc} F=2^6 3^{10}$. At the dyadic place of degree 1, $-1$ is not a norm from $\mathbb{Q}_2(\sqrt{7})$ ($a^2-7b^2\equiv -1 \pmod 4$ is impossible). So the unit norm index is at least 2, and the formula gives $1\cdot 2/2=1$. Hence $h(F)$ is odd.

We have $M=F(W)$. From an explicit integral basis of $M$ we get $\operatorname{disc} M=-2^{14}3^{21}$ (certificate 1.2.1e), so the norm of the relative discriminant of $M/F$ is $2^{14}3^{21}/(2^6 3^{10})^2=12$. A ramified dyadic quadratic extension has discriminant exponent at least 2, so the dyadic prime ideal of $F$ of norm 4 is unramified, and the dyadic place of norm 2 ramifies with exponent 2. The remaining factor 3 comes from the ramification of one place above 3. At the place above 3 with $\kappa\equiv 1$ we have $(\kappa+2)(\kappa-2)=\varepsilon-4=3\theta+2\theta^2$, so $v_\theta(\kappa+2)=2$, and $W^2=6-2\theta+2\theta(\kappa+2)$ has valuation 1. So the ramified 3-adic place is this one. Of the two real places of $F$, only the one with $\kappa<0$ becomes complex (see the proof of Lemma 5.1.7(1)). Therefore $t=3$. The units $-1$, $\kappa$ have norm obstruction vectors $(1,1)$, $(1,0)$ at the real place that becomes complex and at the ramified 3-adic place (a unit that is a local norm there has a square residue in the residue field $\mathbb{F}_3$), so the unit norm index is at least 4. Since squares of units are norms, this index is a power of 2; since the value $h(F)\cdot 4/[\,\cdot\,]$ of the formula is an integer and $h(F)$ is odd, the index is exactly 4. Hence $|\operatorname{Cl}(M)^{\mathrm{Gal}}|=h(F)$ is odd, and $\operatorname{Cl}(M)[2]=0$ (certificate 1.2.1f). □

**Step 7: the rank.** We use the 2-isogenous curve $E'\colon y^2=x^3-4dx^2-4d^2x$ and the isogenies $\phi$, $\hat\phi$ between $E$ and $E'$. The maps $\alpha: E(M)\to M^\times/M^{\times 2}$ and $\alpha': E'(M)\to M^\times/M^{\times 2}$ send a point to the square class of its $x$-coordinate, and $\alpha(T)=2$, $\alpha'(T')=-1$ ($T=(0,0)$, $T'=(0,0)$). By [Sim02, Sil09],

$$2^{\operatorname{rank} E(M)}=\frac{|\alpha(E(M))|\,|\alpha'(E'(M))|}{4}.$$

**Lemma 5.1.9.** $\operatorname{rank} E(M)=6$. *For points $G_1,\dots,G_4\in E(M)$ (their coordinates are in the input of certificate 1.2.1g) and $P,Q,T$, the subgroup $G=\langle G_1,G_2,G_3,G_4,P,Q,T\rangle$ has odd index. Moreover, $E(M)_{\mathrm{tors}}=\{O,T\}$.*

*Proof.* Both images consist of classes with even valuation outside 2, 3 ($N_M(d)=-2^6 3^4$). By Lemma 5.1.8, an ideal whose square is principal is itself principal. So the candidates are the $2^{12}=4096$ classes generated by 7 unit square classes (unit rank 6 for the signature $(2,5)$, together with $\pm 1$) and 5 generators of the prime ideals above 2 and 3. The decomposition of 2 is $(e,f)=(4,1),(2,2),(2,2)$, and that of 3 is $(6,1),(3,2)$. The sizes of the local images are as follows.

| Places | Local degree | $\lvert\alpha_v\rvert$ | $\lvert\alpha'_v\rvert$ |
|---|---|---|---|
| Three places above 2 | 4 | 16 | 4 |
| Two places above 3 | 6 | 2 | 2 |

At each place the product of the two sizes equals the value of the local isogeny quotient formula ($2^{4+2}$ at a dyadic place, 4 at an odd place), so these images, generated by local point witnesses, are complete. At the real places, $x^3+2dx^2+2d^2x=x\big((x+d)^2+d^2\big)$, so $x>0$ on $E$. The numbers of candidates remaining after each condition are as follows.

| Condition | $E$ | $E'$ |
|---|---|---|
| First dyadic place | 1024 | 256 |
| Second dyadic place | 256 | 16 |
| Third dyadic place | 64 | 8 |
| Two places above 3 | 64 | 8 |
| Two real places | 32 | 8 |

On the other hand, $\alpha(T),\alpha(G_1),\dots,\alpha(G_4)$ are independent, and for the points $Q_0, D'$ on $E'$, $\alpha'(T'),\alpha'(Q_0),\alpha'(D')$ are also independent (certificate 1.2.1g). These match the upper bounds, so $|\alpha(E(M))|=32$, $|\alpha'(E'(M))|=8$, and $2^{\mathrm{rank}}=32\cdot 8/4=64$.

The dual isogeny $\hat{\phi}(x,y) = \big((x - 4d - 4d^2/x)/4,\ y(1 + 4d^2/x^2)/8\big)$ sends $Q_0 \mapsto P$, $D' \mapsto Q$ and $T' \mapsto O$. Therefore $T, G_1, \dots, G_4$ generate $E(M)/\hat{\phi}E'(M)$, $P, Q$ generate $\hat{\phi}E'(M)/2E(M)$, and $G$ generates $E(M)/2E(M)$. Hence the index is odd. At the places $(p, \theta, d) = (23, 12, 9)$, $(83, 11, 12)$ of residue degree 1 the reductions have orders 28 and 90, so by [Kat81, Appendix] the order of the torsion divides 2. □

**Step 8: a sieve at 661.** The prime $p = 661$ splits completely in $M$. Listing the twelve embeddings as $(\theta, d) \bmod p$, we get

$$\begin{array}{cccc} (261,34) & (261,334) & (261,454) & (261,500) \\ (481,390) & (481,441) & (481,513) & (481,639) \\ (580,17) & (580,153) & (580,517) & (580,635) \end{array}$$

and in this order $\#E_i(\mathbb{F}_p)$ is $(628, 696, 628, 696, 696, 696, 628, 628, 696, 696, 696, 696)$. Here $628 = 4 \cdot 157$ and $696 = 8 \cdot 3 \cdot 29$.

**Lemma 5.1.10.** *If $q \in \mathbb{Q}$ and $(q, V) \in \mathcal{Q}(M)$, then $q \equiv 0$ or $q \equiv 438 \equiv -8/3 \pmod{661}$. The sign patterns of $V$ at the twelve embeddings are restricted to 64.*

*Proof.* The subgroup $H$ of the product generated by the reductions of $G$ has index $2^{22}3^2 29^2$. Its 2-primary part has order 1024 and index $2^{22}$. For odd primes $\ell$, the matrix of $\ell$-components of the free generators $G_1, \dots, G_4, P, Q$ is $8 \times 6$ of rank 6 for $\ell = 3$, $8 \times 6$ of rank 6 for $\ell = 29$, and $4 \times 6$ of rank 4 (the whole image) for $\ell = 157$. Since the column rank is full for $\ell = 3, 29$, no nonzero combination of the generators modulo $\ell$ can lie in $\ell E(M)$ (multiplying by $\#E_i(\mathbb{F}_p)/\ell$ in each factor would kill that combination). The torsion has order 2, so $[E(M) : G]$ is prime to 3 and 29; being odd, it is prime to the quotient order $2^{22}3^2 29^2$. Hence, by [BS10], the reduction of $E(M)$ is exactly $H$.

For each $q \in \mathbb{P}^1(\mathbb{F}_p)$ we run over all signs of the ordinates of $V^2 = Q(q)$ at the twelve embeddings (including zero ordinates and removable poles of the map). There are 27 values of $q$ with points in every factor, and 106512 sign patterns. After the 2-primary test 6146 remain, after the 3-primary test 1152, and after the 29-primary test 64. All 64 remaining patterns have $q \equiv 0$ or $q \equiv 438$ (certificate 1.2.1h). □

**Step 9: 661-adic logarithms.**

**Lemma 5.1.11.** *If $q \in \mathbb{Q}$ and $(q, V) \in \mathcal{Q}(M)$, then $q = 0$ or $q = -8/3$.*

*Proof.* At each embedding we use the logarithm of $\omega = dx/(2y)$. We pass to the short model $X = x + 2d/3$, $Y^2 = X^3 + \frac{2}{3}d^2X - \frac{20}{27}d^3$, and multiply a point $G$ by the order $N_i$ (prime to $p$) of its reduction to put it into the formal group. Since $\log \tau = \tau + O(\tau^5)$ for $\tau = -X/Y$, computing $\tau([N_i]G)$ modulo $p^3$ determines $\log(G)/p$ modulo $p^2$ (Lemma E). We compute with two kinds of arithmetic (projective scalar multiplication and division polynomials). The $6 \times 12$ matrix of the normalized logarithms of $G_1, \dots, G_4, P, Q$ reduced modulo $p$ has rank 6, and the minor of its first six columns is a unit. Therefore we can choose an integral basis $c^{(1)}, \dots, c^{(6)}$ of the kernel of the exact normalized logarithms whose last six columns form the identity matrix. The first row is

$$c^{(1)} \equiv (74, 2, 659, 439, 29, 256, 1, 0, 0, 0, 0, 0) \pmod{661}$$

(the full matrix and the logarithm of $P_1$ are in certificate 1.2.1i). Since $G$ has finite index, these six annihilators kill the logarithms of all points of $E(M)$.

For each pattern of Lemma 5.1.10 we take the center $q_0 = 0$ or $q_1 = -8/3$. The image of the center in factor $i$ is $O$ or $P_i$ for $q_0$, and $(P_1)_i$ or $P_i - (P_1)_i$ for $q_1$, so the normalized logarithm vector $\ell$ is determined. Writing $q = q_j + pT$ with $T \in \mathbb{Z}_p$, Lemma 5.1.7(3) gives the differential vector $D_i \equiv -\theta_i^2/V_i \pmod{p}$, and the ordinates of the centers are all units. If the disk contains a rational point, then for every $c^{(k)}$

$$c^{(k)} \cdot \ell + T\,(c^{(k)} \cdot D) \equiv 0 \pmod{p}$$

The terms of degree at least 2 in $pT$ are still 0 modulo $p$ after division by $p$, so this condition is necessary on the whole disk. For 60 of the 64 patterns, no $T$ satisfies these six equations simultaneously. The remaining four are, for each center, the two patterns with all signs equal (certificate 1.2.1i).

The centers of the four remaining disks are preimages of the actual global points $O$, $P$, $P_1$, $P - P_1$, so the annihilating logarithms vanish exactly there. The derivative coefficients for $c^{(1)}$ are as follows.

| Center | Sign on the side of $O$ or $P_1$ | Opposite sign |
|---|---|---|
| $q = 0$ | 592 | 69 |
| $q = -8/3$ | 266 | 395 |

All of them are nonzero. The map and the differential are integral on these smooth disks, so by Proposition D and Lemma 5.1.2 each disk contains only its center. Points above parameter infinity were already eliminated by the sieve of Step 8. □

*Proof of Theorem 5.1.1.* By Lemma 5.1.4, even $j$ gives $(\pm 1, 0, -1)$. There is no solution with $j = 1$. By Lemmas 5.1.5, 5.1.6 and 5.1.7, a primitive solution with $j = -1$ gives a point of $\mathcal{Q}(M)$, and by Lemma 5.1.11, $q \in \{0, -8/3\}$. If $q = 0$, then $2n = 3m$, so $3 \mid n$, which contradicts $\gcd(n, 6) = 1$. If $q = -8/3$, then $7m = 2n$, so $(m, n) = (2, 7)$, and

$$P(2,7) = 895^2, \qquad Y(2,7) = 6202, \qquad Z(2,7) = -4199$$

gives $(x, y, z) = (\pm 895, -6202, 4199)$. Substituting these values, we get $895^4 + 3(-6202)^3 + 4199^3 = 0$, and $\gcd(895, 6202, 4199) = 1$. □

## 5.2 $2x^4 - y^4 + z^3 = 0$ ($H = 56$)

**Theorem 5.2.1.** *The only primitive integer solutions* ($\gcd(x, y, z) = 1$) *of* $2x^4 - y^4 + z^3 = 0$ *are*

$$(x, y, z) = (0, \pm 1, 1), \qquad (\pm 1, \pm 1, -1)$$

*(with independent signs).*

**Setup.** The equation is $y^4 - 2x^4 = z^3$. For a primitive solution, $\gcd(x, y) = 1$ and $y, z$ are odd. Indeed, if $y$ were even, then $x$ would be odd and $v_2(y^4 - 2x^4) = 1$, which is impossible for a cube.

The ring $\mathbb{Z}[\sqrt{2}]$ is norm-Euclidean: rounding the two coefficients leaves a remainder $a + b\sqrt{2}$ with $|a|, |b| \le 1/2$ and $|a^2 - 2b^2| \le 1/2$. The units are $\pm(1 + \sqrt{2})^n$. A unit with $1 < \eta < 1 + \sqrt{2}$ has a conjugate of absolute value less than 1, so writing $\eta = a + b\sqrt{2}$ we get $a = 1$, $b \in \{0, 1\}$, which are the two endpoints of the interval.

We use the two polynomials

$$f(A, B) = A^3 + 6A^2B + 6AB^2 + 4B^3, \qquad g(A, B) = A^3 + 3A^2B + 6AB^2 + 2B^3$$

and $F(t) = f(t, 1)g(t, 1) = t^6 + 9t^5 + 30t^4 + 60t^3 + 60t^2 + 36t + 8$. We have $\operatorname{disc} F = 2^{26}3^6$. The two genus 2 curves

$$C_+ : \ w^2 = F(t), \qquad C_- : \ w^2 = -F(t)$$

are understood as their smooth projective models. $C_+$ has the points at infinity $\infty_+, \infty_-$.

The proof runs as follows. A cube descent over $\mathbb{Q}(\sqrt{2})$ gives $C_\pm$ (Step 1). Over the cubic field $K = \mathbb{Q}(h)$, a 2-adic two-cover descent eliminates $C_-$ and lifts the points of $C_+$ to an elliptic curve $E$ over $K$ (Steps 2–4). We show $\operatorname{rank} E(K) = 2$ (Step 5), and a sieve at 29 (Step 6) and elliptic Chabauty (Step 7) give $C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$.

**Step 1: cube descent.**

**Lemma 5.2.2.** *For each primitive solution, $y^2 + x^2\sqrt{2} = (1+\sqrt{2})^j(a+b\sqrt{2})^3$ with $j \in \{-1,0,1\}$ and $\gcd(a,b) = 1$. If $j = 0$, then $(x,y,z) = (0,\pm 1,1)$. If $j = \pm 1$ and $b \neq 0$, we get a finite rational point of $C_\pm$. Hence, if*

$$C_-(\mathbb{Q}) = \varnothing, \qquad C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$$

*then Theorem 5.2.1 holds.*

*Proof.* The norm of $y^2 \pm x^2\sqrt{2}$ is the odd number $z^3$, so both elements are units above 2; a common odd prime ideal would divide both $x$ and $y$, so the two elements are coprime. By unique factorization, $y^2 + x^2\sqrt{2}$ is a unit times a cube, and the sign of the unit and $(1+\sqrt{2})^{3k}$ are absorbed into the cube.

$j = 0$: $y^2 = a(a^2+6b^2)$ and $x^2 = b(3a^2+2b^2)$. Since $y$ is odd, $a > 0$ is odd and $b \geq 0$. If $b = 0$, primitivity gives $(x,y,z) = (0,\pm 1,1)$. If $b > 0$, then $\gcd(b, 3a^2+2b^2) \mid 3$. If $3 \nmid b$, then $b$ and $3a^2+2b^2$ are both squares, but the latter is 2 modulo 3. If $3 \mid b$, then $3a^2+2b^2$ has 3-adic valuation 1, so $b = 3v^2$. From $\gcd(a, a^2+6b^2) = 1$ we get $a = u^2$ and $(x/(3v))^2 = u^4 + 6v^4$. Then $X = u^2/v^2$, $Y = ux/(3v^3)$ is a rational point of $E_6 : Y^2 = X^3 + 6X$ with $X \neq 0$. But $E_6(\mathbb{Q}) = \{O, (0,0)\}$. In the 2-isogeny descent of [Sim02, Sil09], the image for $E_6$ lies in the positive classes $\{1,2,3,6\}$; the class 2 is excluded because $W^2 = 2U^4 + 3V^4$ is impossible modulo 16, and 3 is excluded after multiplying by 6, so the image is $\{1,6\}$. The image for the partner curve $Y^2 = X^3 - 24X$ contains $\{1,-6\}$, and the representatives $-1,-2,2$ of the other three cosets are excluded because $W^2 = -U^4 + 24V^4$, $-2U^4 + 12V^4$, $2U^4 - 12V^4$ are impossible modulo 16, 16, 32, respectively, for $(U,V)$ not both even. Hence $2^{\text{rank}} = 2 \cdot 2/4 = 1$. The reductions at 5, 7, 13 have orders 4, 8, 10, so the torsion has order 2 (certificate 1.2.3a).

$j = 1$: $y^2 = f(a,b)$ and $x^2 = g(a,b)$. $j = -1$: $y^2 = f(-a,b)$ and $x^2 = -g(-a,b)$. If $b \neq 0$, then $t = a/b$ or $-a/b$, together with $w = xy/b^3$, is a finite rational point of $C_+$ or $C_-$. If $b = 0$: for $j = -1$, $y^2 = -a^3$, $x^2 = a^3$ is incompatible with a primitive solution; for $j = 1$, $y^2 = x^2 = a^3$, so $a = 1$, that is, $(x,y,z) = (\pm 1, \pm 1, -1)$. □

**Step 2: the cubic field.** Put

$$K = \mathbb{Q}(h), \quad h^3 + 3h - 2 = 0, \quad e = 1 - h - h^2, \quad \rho = h - 1, \quad \pi = -3 - h - h^2,$$

$$r_f = -4 - h - h^2 = \frac{2}{h-1}, \qquad r_g = h - 1.$$

The elements $r_f, r_g$ are roots of $f(t,1), g(t,1)$. The two polynomials have discriminants $-864$, $-216$, and $\operatorname{Res}(f,g) = -512$.

**Lemma 5.2.3.** *$\mathcal{O}_K = \mathbb{Z}[h]$, $\operatorname{disc} K = -216$, $\operatorname{Cl}(K) = 0$, $\mathcal{O}_K^\times = \{\pm e^n\}$. The prime ideals above 2 are $(h)$, $(\rho)$, and the prime ideal above 3 is $(\pi)$. The square classes of elements with even valuation outside 2, 3 are generated by the ordered basis $\mathcal{B} = (-1, e, \rho, h, \pi)$.*

*Proof.* The polynomial $T^3 - 3T^2 + 6T - 6$ obtained by the substitution $h = T - 1$ is Eisenstein at 3, so $\mathbb{Z}[h]$ is maximal at 3. The polynomial discriminant is $-216 = -2^3 3^3$, so the only other candidate index prime is 2; but if the index were 2, the field discriminant would be $-54$, which violates the condition that a discriminant is 0 or 1 modulo 4 (Stickelberger). The signature is $(1,1)$, and the Minkowski constant $\frac{4}{\pi} \cdot \frac{3!}{3^3}\sqrt{216}$ is less than 5. Modulo 2, $h^3 + 3h - 2 \equiv h(h+1)^2$, and modulo 3, $h^3 + 3h - 2 \equiv (h+1)^3$, so the only prime ideals of norm less than 5 are $(h)$, $(\rho)$, $(\pi)$, of norms 2, 2, 3, and $\operatorname{Cl}(K) = 0$. We have $e^{-1} = 17 + 3h + 5h^2$ and $Ne = 1$. Using the real root $0.59 < r < 0.6$ and the interpolation formula, the coefficients of a unit with $1 < \eta < e^{-1}$ are bounded by $0 \leq a \leq 18$, $0 \leq b \leq 3$, $0 \leq c \leq 5$, and in this range the only elements of norm 1 are 1 and $e^{-1}$ (certificate 1.2.3b). □

The rational square classes $-1, 2, 3$ have the masks 1, 10, 19 with respect to $\mathcal{B}$. Indeed,

$$2 = h\rho^2/e, \qquad (1 - h + h^2)^2 = -3\pi e$$

(certificate 1.2.3b). In the rational basis $(-1,2,3)$, the norms of the elements of $\mathcal{B}$ are written as $(1,0,3,2,5)$.

**Step 3: 2-adic two-cover descent.**

**Lemma 5.2.4.** *$C_-(\mathbb{Q}) = \varnothing$. Every finite rational point of $C_+$ satisfies*

$$t - r_f = c\,a_1^2, \qquad t - r_g = c\,a_2^2, \qquad c \in \mathbb{Q}^\times,\ a_1, a_2 \in K^\times$$

*Proof.* Write a finite rational point of $C_\sigma$ ($\sigma = \pm 1$) as $t = A/B$ ($A, B$ coprime), and consider $(A - Br_f, A - Br_g) \in K^\times \times K^\times$. If a prime ideal outside 2, 3 divides one component, then $B$ is a unit there and the residue of the corresponding root is $A/B$, so this prime ideal has residue degree 1. By the discriminants and the resultant, it is the only contributing factor above its rational prime, and the product of the two norms is $\sigma$ times a square, so the valuation is even. Hence the classes of both components lie in the span of $\mathcal{B}$, and the rational class of the product of the norms is $\sigma$. This is the two-cover condition of [BS09]. Dividing by a common rational scalar and imposing the norm condition leaves 16 candidate pairs for each sign.

We impose the 2-adic local conditions. We have $K \otimes \mathbb{Q}_2 = \mathbb{Q}_2 \times \mathbb{Q}_2(\omega)$ with $\omega^2 = -6$, and the two embeddings of $h$ are $a_0$ (the even 2-adic root of $h^3 + 3h - 2$) and $-a_0/2 + \omega/(a_0^2 + 1)$. We record square classes of $\mathbb{Q}_2$ by the unit bits $(-1, 5)$ and a valuation bit, and square classes of $\mathbb{Q}_2(\omega)$ by the unit bits $1 + \omega, 1 + 2\omega, 1 + 3\omega$ and an $\omega$-valuation bit. The squares of units of $\mathbb{Q}_2(\omega)$ modulo 8, written as $A + B\omega$, are the four classes $(1,0)$, $(3,2)$, $(1,4)$, $(3,6)$, and since $v_\omega(8) = 6 > 2v_\omega(2) = 4$, squares modulo 8 lift to squares. The seven-bit labels of the elements of $\mathcal{B}$ are $(41, 49, 122, 13, 11)$.

For $t \in a + 2^n\mathbb{Z}_2$, the class of the $\mathbb{Q}_2$-component of $t - r$ is constant if $n - v_2(a - r) > 2$, and the class of the $\mathbb{Q}_2(\omega)$-component is constant if $2n - v_\omega(a - r) > 4$. Splitting balls repeatedly, we cover $\mathbb{Z}_2$ by 42 disjoint balls. On 40 of them all four classes are constant; on the two root balls $10 + 64\mathbb{Z}_2$, $45 + 64\mathbb{Z}_2$ only the scalar class of the vanishing factor varies, so we test all eight values. The remaining chart $u = 1/t \in 2\mathbb{Z}_2$ is covered by $u \equiv 0, 2, 4, 6 \pmod 8$, and there we use $1 - ur_f$, $1 - ur_g$. The admissible local labels, modulo a common $\mathbb{Q}_2$ scalar, are $\{0, 1032, 9328, 9715\}$ for $\sigma = +1$ and $\{1, 1160, 9329, 9714\}$ for $\sigma = -1$. Comparing the 16 global candidate pairs with these sets, only the trivial pair survives for $\sigma = +1$, and nothing survives for $\sigma = -1$ (certificate 1.2.3c). Since $C_-$ has leading coefficient $-1$, it has no rational point at infinity either. □

**Step 4: an elliptic curve over the cubic field.** By Lemma 5.2.4, $(t - r_f)(t - r_g)$ is a square in $K$. Let

$$q(t) = t^4 + (4 - h^2)t^3 + (8 + 2h - 2h^2)t^2 + (8 - 2h^2)t + 4$$

so that $(t - r_f)(t - r_g)q(t) = F(t)$. Then the finite rational points of $C_+$ lift to $K$-points ($t \in \mathbb{Q}$) of $v^2 = q(t)$. Put

$$k = 2 - \tfrac{1}{2}h^2, \quad m = 2 + \tfrac{3}{4}h + \tfrac{3}{8}h^2, \quad n = \tfrac{3}{2} - \tfrac{9}{2}h - \tfrac{21}{8}h^2, \quad r_1 = 6h + 3h^2, \quad d = 2 - h + h^2,$$

$$X = 2(v + t^2 + kt + m), \qquad Y = (2t + k)X + n, \qquad x_E = 4X - r_1, \qquad y_E = 8Y.$$

Then

$$E:\ y_E^2 = x_E(x_E - 12d)(x_E + 4d), \qquad \phi^* \frac{dx_E}{2y_E} = \frac{dt}{4v}$$

The two points at infinity with $v/t^2 \to +1, -1$ map to $O$ and to

$$Q = (-6h - 3h^2,\ -12 + 36h + 21h^2)$$

respectively. Writing $u = 1/t$, the formal square root of $u^4 q(1/u)$ begins with $1 + ku + mu^2 + \frac{1}{2}nu^3 + O(u^4)$. All identities are checked by polynomial division using $h^3 + 3h - 2 = 0$ and $v^2 = q(t)$ (certificate 1.2.3d).

**Step 5: the rank.**

**Lemma 5.2.5.** rank $E(K) = 2$ *and* $E(K)_{\mathrm{tors}} = E[2]$. *The subgroup* $G$ *generated by*

$$P = (-8h + 4h^2,\ -16 + 56h), \qquad Q = (-6h - 3h^2,\ -12 + 36h + 21h^2)$$

*and* $T_0 = (0, 0)$, $T_1 = (12d, 0)$ *has index prime to 6.*

*Proof.* We carry out the full 2-descent of [Sim02, Sil09] on the isomorphic model $y^2 = x(x - 3d)(x + d)$ with the Kummer map $\delta = (x, x - 3d)$. Its values at $T_0, T_1$ are $(-3d^2, -3d)$, $(3d, 12d^2)$. From the differences of the roots and $N(d) = 16$, all Kummer values have even valuation outside 2, 3, so the global candidates are the $32^2 = 1024$ pairs written in $\mathcal{B}$. The local images have dimensions 3 and 4 at the two places above 2 and dimension 2 above 3, and they are filled by the torsion and three local points $(x = -6 - 7h - 5h^2, -7 - 6h - 7h^2, -7 - 6h + 3h^2)$. At the real place the two signs must agree. Of the 1024 pairs, 16 remain. The mask pairs of $T_0, T_1, P, Q$ are $(18, 29)$, $(28, 19)$, $(24, 26)$, $(24, 24)$; they are independent, so they fill all 16 pairs (certificate 1.2.3e). Hence the rank is 2 and the index of $G$ is odd.

At the places $(13, h - 9)$, $(29, h - 6)$ of residue degree 1 the reductions have orders 16 and 36 ([Kat81, Appendix]), so the order of the torsion divides 4, and all 2-torsion points are rational.

We check coprimality to 3 at 29. The prime 29 splits completely with $h \equiv 6, 9, 14$, and in the first two factors the exponents of the groups are 18 and 12. Multiplying by one third of the exponent, we get $[6]P = [6]Q = (16, 28)$ at $h \equiv 6$, and $[4]P = (22, 17)$, $[4]Q = (22, 12) = -[4]P$ at $h \equiv 9$; all of these have order 3. If $aP + bQ \in 3E(K)$, then $a + b \equiv 0$ and $a - b \equiv 0 \pmod 3$, so $a \equiv b \equiv 0$. The torsion has no 3-part, so the index is prime to 3 (certificate 1.2.3f). □

**Step 6: a sieve at 29.**

**Lemma 5.2.6.** *If* $(t, w)$ *is a rational point of* $C_+$ *and* $t$ *is a 29-adic integer, we get a contradiction. Hence* $u = 1/t \in 29\mathbb{Z}_{29}$, *and the point lies in one of the two disks centered at the two points at infinity* $\infty_\pm$.

*Proof.* In the three factors, $\#E(\mathbb{F}_{29}) = 36, 24, 36$, the exponents are $18, 12, 18$, the orders of $P$ are $18, 12, 3$, and the orders of $Q$ are $9, 3, 9$. Adding $P, Q, T_0, T_1$ one at a time, the generated subgroups have sizes $36, 324, 648, 1296$, and the index in the product, of order $36 \cdot 24 \cdot 36$, is 24. By Lemma 5.2.5, the index of $G$ is prime to 24, so by [BS10] the reduction of $E(K)$ equals this subgroup $H$.

Suppose that $t$ is a 29-adic integer. By Lemma 5.2.4, $t - r_f$ and $t - r_g$ are the same $c$ times squares at all three embeddings. If $v_{29}(c)$ is odd, all six values $t - r$ must be divisible by 29; but the residues of the six roots, $(r_f)_i = (12, 22, 18)$ and $(r_g)_i = (5, 8, 13)$, are distinct, so this is impossible. Hence $v_{29}(c)$ is even, and the quadratic characters of the nonzero residues $t - r$ must all be equal. Testing all $t = 0, \dots, 28$, none satisfies this condition (certificate 1.2.3f). Therefore $u = 1/t \in 29\mathbb{Z}_{29}$. In this chart, $\hat{v} = u^2 v$ satisfies $\hat{v}^2 = u^4 q(1/u) \equiv 1$, so it reduces to $\pm 1$ at each of the three embeddings, and the corresponding elliptic reductions are the eight tuples whose components are $O$ or $Q_i$. Among them, only $(O, O, O)$ and $(Q_1, Q_2, Q_3)$ lie in $H$. That is, the three signs are all equal. □

**Step 7: 29-adic logarithms.**

**Lemma 5.2.7.** $C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$.

*Proof.* Lifting $h$ at the three embeddings modulo $29^3$ gives 13172, 14132, 21474. At each embedding we pass to a short model $y^2 = x^3 + Ax + B$, multiply points by the orders of their reductions to put them into the formal group, and use $\log \tau = \tau + O(\tau^5)$ with $\tau = -x/y$ (Lemma E). Computing by two methods, projective arithmetic and division polynomials, we find that the normalized logarithms of $\omega = dx_E/(2y_E)$ are, modulo $29^2$,

$$\tfrac{1}{29} \log P \equiv (647, 368, 410), \qquad \tfrac{1}{29} \log Q \equiv (672, 302, 764)$$

Modulo 29 they are $(9,20,4)$ and $(5,12,10)$, which are independent. The cross product $c$ of the two exact normalized logarithms is an integral annihilator, with $c \equiv (7,17,8) \pmod{29}$ and $c_1+c_2+c_3 \equiv 3$. Since $P, Q$ span the logarithm space and torsion points have logarithm 0, $c$ kills all logarithms of $E(K)$ (certificate 1.2.3g).

On the disks of Lemma 5.2.6, $\hat{v}$ is an integral power series whose constant term at each embedding is $\varepsilon = \pm 1$ (the same for all three embeddings), and $\phi^*(dx_E/2y_E) = -du/(4\hat{v})$. The constant term of the pullback differential combined with the annihilator is $-\varepsilon(c_1+c_2+c_3)/4 \equiv \mp 3/4$, that is, 21 or 8 modulo 29. Both are units. The centers $\infty_\pm$ of the disks map to the global points $O$, $Q$, so the annihilating logarithm vanishes there. By Proposition D and Lemma 5.1.2, each disk contains only its center. □

*Proof of Theorem 5.2.1.* By Lemmas 5.2.4 and 5.2.7, $C_-(\mathbb{Q}) = \varnothing$ and $C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$. By Lemma 5.2.2, the only primitive solutions are $(0,\pm 1,1)$ and $(\pm 1,\pm 1,-1)$. Substituting gives $0-1+1=0$ and $2-1-1=0$. □

## 5.3 $x^5+y^4=2z^2$ ($H=56$)

**Theorem 5.3.1.** *The only primitive integer solutions* ($\gcd(x,y,z)=1$) *of* $x^5+y^4=2z^2$ *are*

$$(x,y,z) = (-1,\pm 1,0), \qquad (1,\pm 1,\pm 1)$$

*(with independent signs).*

**Setup.** The three numbers of a primitive solution are pairwise coprime. Modulo 2, $x$ and $y$ have the same parity; if both were even, $2z^2$ would be a multiple of 16, so $z$ would be even as well. Hence $x, y$ are odd. If $z=0$, then $(x,y,z)=(-1,\pm 1,0)$. From now on $z \neq 0$.

Put $d=\sqrt{2}$ and $\varepsilon = 1+d$. The ring $\mathbb{Z}[d]$ is norm-Euclidean and its units are $\pm\varepsilon^n$ (for a unit with $1 < \eta < \varepsilon$, the $d$-coefficient $(\eta - N(\eta)/\eta)/(2d)$ would have to lie between 0 and 1). We use the following forms.

$$F = a^5+20a^3b^2+20ab^4, \quad G = 5a^4b+20a^2b^3+4b^5, \quad F_1 = F+2G, \quad F_2 = 3F+4G.$$

We have $(a+bd)^5 = F+Gd$. The quintic field is

$$L=\mathbb{Q}(\theta), \qquad g(\theta)=\theta^5+5\theta^3+5\theta-2=0$$

and we use the following elements.

$$\begin{aligned} u_1 &= 1-\theta-\theta^3, & u_2 &= 1-3\theta+\theta^2-\theta^3,\\ q &= -1+2\theta+2\theta^2+\theta^3, & \ell &= 1+\theta^2,\\ \eta &= -\theta^4-\theta^3-5\theta^2-4\theta-6, & \chi &= \theta^4+\theta^3+3\theta^2+6\theta-4,\\ \delta &= \theta^4+\theta^3+3\theta^2+3\theta-1. \end{aligned}$$

The proof runs as follows. A fifth-power descent over $\mathbb{Q}(\sqrt{2})$ splits the problem into five cases according to the unit exponent $j$ (Step 1). The case $j=0$ is settled by a rank 0 elliptic curve over $\mathbb{Q}$ (Step 2). The case $j=2$ is eliminated by a computation modulo 8 in $L$, and $j=1$ lifts to an elliptic curve $E$ over $L$ (Steps 3–4). We show $\operatorname{rank} E(L)=2$ (Step 5) and finish with a sieve at 751 (Step 6) and elliptic Chabauty (Step 7).

### Step 1: fifth-power descent.

**Lemma 5.3.2.** *For each primitive solution ($z \neq 0$) we have*

$$y^2+zd = \varepsilon^j(a+bd)^5, \qquad j\in\{-2,-1,0,1,2\}, \quad \gcd(a,b)=1, \quad a \text{ odd}, \qquad x=(-1)^{j+1}(a^2-2b^2)$$

*If $j=0,1,2$, then $y^2=F$, $y^2=F_1$, $y^2=F_2$, respectively. Taking conjugates changes $(j,a,b,z)$ into $(-j,(-1)^j a,(-1)^{j+1}b,-z)$, so it suffices to consider $j=0,1,2$.*

*Proof.* The product of $y^2 \pm zd$ is $-x^5$, and their norms are odd. A common prime ideal does not lie above 2, and if there were one, it would give a common prime factor of $y, z$. Hence the two elements are coprime, and by unique factorization $y^2 + zd$ is a unit times a fifth power. The sign of the unit is absorbed into the fifth power, since 5 is odd. Taking norms gives $-x^5 = (-1)^j(a^2 - 2b^2)^5$. Since $x$ is odd, $a$ is odd. The rational parts of $(1+d)(F+Gd)$ and $(3+2d)(F+Gd)$ are $F_1$ and $F_2$. Since $\bar{\varepsilon} = -\varepsilon^{-1}$, the rule for conjugation follows. □

**Step 2: $j = 0$.**

**Lemma 5.3.3.** *If $j = 0$, the only solutions are $(x, y, z) = (-1, \pm 1, 0)$. In particular, there is no solution with $z \neq 0$.*

*Proof.* We have $F = a(a^4 + 20a^2b^2 + 20b^4) = y^2$, and the second factor is positive, so $a > 0$. The gcd of the two factors divides 20, and $a$ is odd, so the gcd is 1 or 5. If $a = 5u^2$, then $F \equiv 5$ or $13 \pmod{16}$, which cannot be an odd square. Hence $a = u^2$ ($u$ odd, $\gcd(u, 5b) = 1$) and $c^2 = u^8 + 20u^4b^2 + 20b^4$.

Suppose $b \neq 0$. The positive integers $m, k = (u^4 + 10b^2 \pm c)/2$ satisfy $mk = 20b^4$ and are coprime. Indeed, a common prime factor divides $20b^4$ and $m + k = u^4 + 10b^2$; but it cannot be a prime factor of $b$, the sum is odd, and $5 \nmid u$. Up to order, the two factors have the form $(r^4, 20s^4)$ or $(5r^4, 4s^4)$ ($|b| = rs$, $\gcd(r, s) = 1$). In the second case, $u^4 = 5r^4 - 10r^2s^2 + 4s^4$ is impossible modulo 16. In the first case, $u^4 = r^4 - 10r^2s^2 + 20s^4$, and we get a rational point

$$(X, Y) = \Big(\frac{r^2}{s^2}, \frac{ru^2}{s^3}\Big), \quad X \neq 0, \qquad Y^2 = X^3 - 10X^2 + 20X$$

But the only rational points of this curve are $O$ and $(0, 0)$. In the 2-isogeny descent of [Sim02, Sil09], the partner curve is $Y^2 = X^3 + 20X^2 + 20X$, and the candidate classes for the two curves are $\pm 1, \pm 2, \pm 5, \pm 10$. The class 5 is given by $(0, 0)$. On the first curve, the negative classes are excluded by the sign, and the class 2 is excluded because $W^2 = 2U^4 - 10U^2V^2 + 10V^4$ is impossible modulo 25 for pairs primitive at 5. On the partner curve, the representatives $2, -2$ of the other two cosets are excluded modulo 25, and $-1$ is excluded because $W^2 = -U^4 + 20U^2V^2 - 20V^4$ is impossible modulo 16 for pairs primitive at 2. Both images are $\{1, 5\}$, so $2^{\text{rank}} = 2 \cdot 2/4 = 1$. The reductions at 3 and 7 have orders 2 and 10 ([Kat81, Appendix]), so the torsion has order 2 (certificate 1.2.4a). Hence $b = 0$, and $y^2 = a^5$ together with primitivity gives $a = 1, z = 0$. □

**Step 3: the quintic field and $j = 1, 2$.**

**Lemma 5.3.4.** $\mathcal{O}_L = \mathbb{Z}[\theta]$, $\operatorname{disc} L = 200000 = 2^6 5^5$, $\mathrm{Cl}(L) = 0$, $\mathcal{O}_L^\times / \mathcal{O}_L^{\times 2} = \langle -1, u_1, u_2 \rangle$.

*Proof.* $g(T+2) = T^5 + 10T^4 + 45T^3 + 110T^2 + 145T + 80$ is Eisenstein at 5. Modulo 2 we have $g = T(T^2 + T + 1)^2$, and $(g - T(T^2 + T + 1)^2)/2 = -T^4 + T^3 - T^2 + 2T - 1$ is coprime to $T^2 + T + 1$ modulo 2, so by Dedekind's criterion [Coh93, Section 6.1] $\mathbb{Z}[\theta]$ is also maximal at 2. Since $\operatorname{disc} g = 2^6 5^5$, we get $\mathcal{O}_L = \mathbb{Z}[\theta]$. Since $g'(T) = 5(T^4 + 3T^2 + 1) > 0$, the signature is $(1, 2)$. The Minkowski constant $(4/\pi)^2(5!/5^5)\sqrt{200000}$ is less than 29. The prime ideals of norm less than 29 above primes less than 29 are generated by $\theta$ (2), $q$ (4), $3 + \theta + 2\theta^2$ (3), $\ell$ (5), $3 + \theta^2$ (7), $-1 + 3\theta + 2\theta^3$ (11), $1 + \theta$ (13), $-1 + \theta + 4\theta^2 + \theta^4$ (17), $-1 + 2\theta - \theta^2 + \theta^3$ (23), and factoring $g$ modulo $p$ shows that this list is complete (certificate 1.2.4b). Hence $h(L) = 1$. We have $Nu_1 = Nu_2 = 1$, and at the places $(7, \theta - 5)$, $(17, \theta - 3)$ of residue degree 1 the rows of quadratic characters of $u_1, u_2$ are $(0, 1)$, $(1, 0)$. The unit rank is 2, and since $u_1, u_2$ are positive at the real embedding, the class of $-1$ is independent of them. □

The following norm identities hold (certificate 1.2.4b).

$$N(a - \eta b) = F_1(a, b), \qquad N(3a - \chi b) = 81F_2(a, b).$$

The minimal polynomials of $\eta$ and $\chi$ are $Z^5 + 10Z^4 + 20Z^3 + 40Z^2 + 20Z + 8$ and $Z^5 + 20Z^4 + 180Z^3 + 720Z^2 + 1620Z + 1296$, and their discriminants are $2^{22}5^5$ and $2^{22}3^{12}5^5$.

**Lemma 5.3.5.** *There is no primitive solution with $j = 2$. If $j = 1$, then $a - \eta b = w^2$ with $w \in \mathcal{O}_L$.*

*Proof.* First, $5 \nmid y$. Indeed, $F_1 \equiv (a-2b)^5$ and $F_2 \equiv 3(a-3b)^5 \pmod 5$; the values $F_1(2,1) = 560$, $F_2(3,1) = 4885$ at the roots have 5-adic valuation 1, and the partial derivatives with respect to $a$ are divisible by 5, so the valuation remains 1 when the root is lifted. This is incompatible with $y^2$.

Put $\gamma_1 = a - \eta b$ and $\gamma_2 = 3a - \chi b$. Outside the primes dividing the discriminant, a prime ideal dividing $\gamma_j$ has residue degree 1 and is the only one above its rational prime (its residue is $\eta = a/b$ or $\chi = 3a/b$). By the norm identities its valuation is even. Since $y$ is odd, $\gamma_j$ is a unit above 2, and by the previous paragraph it is also a unit above 5. For $\gamma_1$ the argument above also applies above 3. For $\gamma_2$: modulo 3 we have $g \equiv (T-1)(T^4+T^3-1)$, the element $\delta$ ($N\delta = 81$) generates the prime ideal $\mathfrak{p}_4$ of degree 4, and $\chi$ has $N\chi = -1296$, is a unit at the 3-adic place of degree 1, and has $v_{\mathfrak{p}_4}(\chi) = 1$. If $3 \mid b$, then $3 \nmid a$ and $v_{\mathfrak{p}_4}(\gamma_2) = 1$. If $3 \nmid b$, then $F_2(a,b)$ is a 3-adic unit, so the norm gives $v_{\mathfrak{p}_4}(\gamma_2) = 1$. In either case the valuation at the 3-adic place of degree 1 is even. Therefore, from the unit classes and the positivity of the norm ($N(-1) = -1$ in a field of odd degree),

$$\gamma_1 = u_1^i u_2^k w^2, \qquad \gamma_2 = \delta u_1^i u_2^k w^2, \qquad i,k \in \{0,1\},\ w \in \mathcal{O}_L$$

The ring $R = (\mathbb{Z}/8\mathbb{Z})[T]/(g)$ has 32768 elements and 336 distinct squares. For $a$ odd and $b$ mod 8, the residues of $\gamma_j$ take 32 values. Comparing them with the four sets $u_1^i u_2^k R^2$, $\delta u_1^i u_2^k R^2$, the sizes of the intersections in the order $(i,k) = (0,0),(1,0),(0,1),(1,1)$ are $2,0,0,0$ for $\gamma_1$ and $0,0,0,0$ for $\gamma_2$ (certificate 1.2.4c). The two residues of $\gamma_1$ have coefficients $(1,0,0,0,0)$ and $(1,0,4,4,4)$. □

**Step 4: the elliptic cover.** Suppose $j = 1$ and $b \neq 0$. Putting $t = a/b$ and $v = y/(b^2 w)$, we get

$$v^2 = q(t) = t^4 + At^3 + Bt^2 + Ct + D, \qquad q(t) = \frac{N(t-\eta)}{t-\eta}$$

where $A = 10 + \eta$, $B = 20 + 10\eta + \eta^2$, $C = 40 + 20\eta + 10\eta^2 + \eta^3$, $D = 20 + 40\eta + 20\eta^2 + 10\eta^3 + \eta^4$. Here $t \in \mathbb{Q}$ and $v \in L$. Put

$$U = 2v + 2t^2 + At, \quad V = 2\big(U + B - \tfrac{A^2}{4}\big)t + \tfrac{A}{2}U + C, \quad R_\theta = 2\theta^3 - 4, \quad \xi = \frac{U - R_\theta}{4}, \quad \zeta = \frac{V}{8}.$$

Then $(\xi, \zeta)$ is a point of

$$E:\ \zeta^2 = \xi^3 - 5\theta\xi^2 + 5\theta^2\xi$$

and for $\omega = d\xi/(2\zeta)$ we have $\phi^*\omega = dt/v$ ($dU/dt = V/v$). The two points at infinity with $v/t^2 \to +1$, $-1$ map to $O$ and to

$$P = \Big(\frac{-5\theta^4 - 25\theta^2 + 10\theta}{8},\ \frac{35\theta^4 - 5\theta^3 + 195\theta^2 - 20}{32}\Big)$$

respectively (certificate 1.2.4d).

**Step 5: the rank.** The partner curve is $E':\ \zeta^2 = \xi^3 + 10\theta\xi^2 + 5\theta^2\xi$. We use the 2-isogeny descent of [Sim02, Sil09]. For $E_{a,b}: y^2 = x^3 + ax^2 + bx$, the map $\alpha$ sends a point to the square class of $x$, and a class $\mu$ lies in the image if and only if $\mu W^2 = \mu^2 U^4 + a\mu U^2 V^2 + bV^4$ has a suitable nonzero point. If both curves have only one rational 2-torsion point (which holds, since $\sqrt{5} \notin L$), then

$$2^{\operatorname{rank} E(L)} = \frac{|\alpha(E(L))|\,|\alpha'(E'(L))|}{4}.$$

**Lemma 5.3.6.** $\operatorname{rank} E(L) = 2$ *and* $E(L)_{\mathrm{tors}} = \{O, T_0\}$ *($T_0 = (0,0)$). For*

$$Q = (4\theta + 4\theta^2 + 3\theta^3 + 2\theta^4,\ 12 - 24\theta - 7\theta^2 - 21\theta^3 - 3\theta^4)$$

*the subgroup $\langle P, Q, T_0\rangle$ has odd index.*

*Proof.* Outside the primes above 2 and 5, the $x$-coordinate has even valuation, so the candidates are the 64 classes generated by the ordered basis $(-1, u_1, u_2, \theta, q, \ell)$. We impose necessary conditions one after another.

- Real place: $x \geq 0$ on $E$.
- 5: Put $\lambda = \theta - 2$; then $v_\lambda(5) = 5$ and $\lambda^5/5 \equiv -1 \pmod{\lambda}$. For both curves, $a, b$ have valuation 5, and the normalized leading unit of $b$ is a square. If we take $U, V$ integral with one of them a unit, and take the representative of $\mu$ of valuation 0 or 1, then a class of even valuation must have a square unit part, and a class of odd valuation must have the class of $b$.
- 2: The 2-adic completions of $L$ are one of degree 1 and one of degree 4 (the even root of $g$ is 178 modulo 256, and the quartic factor is $T^4 + 2T^3 + 9T^2 + 2T + 9$ modulo 16). We scan the charts $V = 1$ ($U$ arbitrary) and $U = 1$ ($V$ a nonunit) completely, modulo 256 for the linear factor and modulo 16 for the quartic factor. The ring of the quartic factor has 65536 elements, 49152 units and 1648 distinct squares.

The numbers of remaining candidates, for $E$ and $E'$ respectively, are 16, 32 after the real place and 5; 16, 16 after the dyadic place of degree 1; and 4, 4 after the dyadic place of degree 4. In both cases the masks are $0, 6, 32, 38$, that is, $1, u_1u_2, \ell, u_1u_2\ell$. On the other hand, the images of $T_0, Q$ have masks $32, 38$, and the images of the point $T_0' = (0, 0)$ of $E'$ and of

$$S = (50 + 5\theta + 50\theta^2 + 10\theta^4,\ 380 + 100\theta + 320\theta^2 + 20\theta^3 + 60\theta^4)$$

are also $32, 38$ ($5\theta^2/\ell$, $\xi(Q)/(u_1u_2\ell)$, $\xi(S)/(u_1u_2\ell)$ are squares in $L$). Hence both images have exactly four elements, and rank $E(L) = 2$ (certificate 1.2.4e).

For the dual isogeny $\hat\phi(x', y') = \big((x' + 10\theta + 5\theta^2/x')/4,\ y'(5\theta^2 - x'^2)/(8x'^2)\big)$ we have $\hat\phi(S) = P + T_0$ and $\hat\phi(T_0') = O$. Since $T_0, Q$ generate $E(L)/\hat\phi E'(L)$ and $T_0', S$ generate $E'(L)/\phi E(L)$, the points $T_0, Q, P + T_0$, that is, $P, Q, T_0$, generate $E(L)/2E(L)$, and the index is odd. At the places $(3, \theta - 1)$, $(11, \theta - 5)$ of residue degree 1 the reductions of the two curves have orders 6 and 16 ([Kat81, Appendix]), so the torsion subgroups are $\{O, T_0\}$ and $\{O, T_0'\}$. □

**Step 6: a sieve at 751.**

**Lemma 5.3.7.** *For a point of $v^2 = q(t)$ ($t \in \mathbb{Q}$, $v \in L$), $t$ is not a 751-adic integer. So $u = 1/t \in 751\mathbb{Z}_{751}$, and the signs of $\hat v_i = u^2 v_i$ at the five embeddings are all equal.*

*Proof.* The prime $p = 751$ splits completely with $\theta \equiv 65, 168, 348, 386, 535$. Each reduction is $\mathbb{Z}/384 \times \mathbb{Z}/2$ (of order 768), and $T_0$ has coordinates $(192, 0)$ in every factor. The subgroup $H$ of the product of the five factors generated by $P, Q, T_0$ satisfies

$$|H| = 36864 = 2^{12}3^2, \qquad [\textstyle\prod_i E_i(\mathbb{F}_p) : H] = 2^{28}3^3$$

If $mP + nQ \in 3E(L)$, then multiplying by 128 and looking at the 3-components in each factor, we find that $(m, n)$ modulo 3 lies in the kernel of the matrix

$$\begin{pmatrix} 2 & 1 & 2 & 2 & 0 \\ 2 & 1 & 0 & 1 & 1 \end{pmatrix}^\top$$

This matrix has rank 2, so $m \equiv n \equiv 0 \pmod 3$. The torsion has no 3-part, so the index is prime to 3; being odd, it is prime to $2^{28}3^3$. Hence, by [BS10], the reduction of $E(L)$ is exactly $H$.

For each $t \in \mathbb{F}_p$ we check whether the five conjugate quartics $q_i(t)$ are squares, and we apply the map for all choices of signs of the ordinates. At $t = \infty$ we choose $O$ or $P_i$ independently in each factor. There are 57 parameter residues (including $\infty$) that are squares in every factor, and 1674 product points are tested; the only ones in $H$ are $(O, O, O, O, O)$ and $(P_1, \dots, P_5)$ at $t = \infty$ (certificate 1.2.4f). If $t$ is a $p$-adic integer, the reduction of the point is one of the finite tuples tested, so it is excluded. Otherwise $\hat v_i \equiv \pm 1$, and the sieve leaves only the two patterns with all signs equal. □

**Step 7: 751-adic logarithms.**

**Lemma 5.3.8.** *The curve $v^2 = q(t)$ has no finite point with $t \in \mathbb{Q}$.*

*Proof.* The five roots lift modulo $p^3 = 423564751$ to 30368252, 51283705, 229643381, 365409950, 170424214. We pass to the short model $Y^2 = X^3 - \frac{10}{3}\theta^2 X - \frac{25}{27}\theta^3$, and we multiply $P$ by $192, 192, 192, 192, 64$ and $Q$ by $384, 384, 128, 384, 384$ to put them into the formal group (all these numbers are prime to $p$). Since $\log \tau = \tau + O(\tau^5)$ (Lemma E), we get, modulo $p^2$,

$$\tfrac{1}{p}\log P \equiv (423722, 191178, 352807, 294331, 252200),$$
$$\tfrac{1}{p}\log Q \equiv (330447, 456587, 117975, 48293, 396869)$$

The first three coordinates are independent modulo $p$. Let $c$ be the cross product of the first three coordinates of the exact normalized logarithms, followed by two zeros. Then $c$ is an integral annihilator, and

$$c \equiv (626, 131, 473, 0, 0) \pmod{p}, \qquad \textstyle\sum_i c_i \equiv 479 \pmod{p}$$

(certificate 1.2.4g). Since $P, Q$ span $E(L) \otimes \mathbb{Q}$, $c$ kills all logarithms of $E(L)$.

On the remaining disks the common parameter is $u = 1/t$, and $\hat{v}_i^2 = 1 + A_i u + B_i u^2 + C_i u^3 + D_i u^4$. The sign at $u = 0$ fixes an integral analytic square root. Since $\phi^*\omega = dt/v = -du/\hat{v}$, the combined differential is $-\sum_i c_i\, du/\hat{v}_i$, and on the two disks with uniform signs its constant coefficients are $-\sum c_i$ and $\sum c_i$, that is, 272 and 479 modulo 751. Both are units. The centers map to the global points $O$, $P$, so the annihilating logarithm vanishes there. By Proposition D and Lemma 5.1.2, the disks contain only the center $u = 0$, and this is not a finite point. □

*Proof of Theorem 5.3.1.* By Lemmas 5.3.5 and 5.3.8, if $j = 1$ then $b = 0$. Then $y^2 = a^5$, $z = a^5$, and primitivity gives $a = 1$, so $(x, y, z) = (1, \pm 1, 1)$. By conjugation, $j = -1$ gives $(1, \pm 1, -1)$. By Lemma 5.3.5 there is nothing for $j = \pm 2$, and by Lemma 5.3.3, $j = 0$ gives only $(-1, \pm 1, 0)$. Substituting gives $-1 + 1 = 0$ and $1 + 1 = 2$. □

## 5.4 $x^5 + y^4 = 3z^2$ ($H = 60$)

**Theorem 5.4.1.** *The only primitive integer solutions* ($\gcd(x, y, z) = 1$) *of $x^5 + y^4 = 3z^2$ are*

$$(x, y, z) = (-1, \pm 1, 0), \qquad (11, \pm 29, \pm 538)$$

*(independent signs).*

**Setup.** The proof goes as follows. We perform a fifth-power descent in $\mathbb{Z}[\sqrt{3}]$ and eliminate the cases with unit exponent $j \neq 0$ by a square-class obstruction in a quintic field (Steps 1–2). The remaining case leads to the plane quartic curve

$$\mathcal{C}: \quad u^4 = r^4 - 15r^2s^2 + 45s^4$$

(Step 3). A fourth-power descent over $\mathbb{Q}(\sqrt{5})$ turns the points with $s \neq 0$ into points of the genus 2 curve

$$\mathcal{H}: \quad Y^2 = f(X) := X(X^2 + 30X + 45)(X^2 - 45)$$

with $X \in \mathbb{Q}^{\times 2} \cup -\mathbb{Q}^{\times 2}$ (Step 4). We lift these points by pointwise 2-descent to three elliptic curves over $K = \mathbb{Q}(\sqrt{5})$, and find them all using ranks, a coset sieve and elliptic Chabauty (Steps 5–8).

Let $K = \mathbb{Q}(d)$, $d = \sqrt{5}$, $e = (1 + d)/2$. Then $\mathcal{O}_K = \mathbb{Z}[e]$, $h_K = 1$ (Minkowski bound $\sqrt{5}/2 < 2$), the unit group is $\{\pm e^n\}$, and $N(e) = -1$. The primes 2 and 3 are inert, and $d$ is a prime element above 5. Further, putting

$$\rho = -15 + 6d = -21 + 12e, \qquad \tau = 3d = -3 + 6e,$$

we have $X^2 + 30X + 45 = (X - \rho)(X - \bar{\rho})$ and $X^2 - 45 = (X - \tau)(X + \tau)$.

**Step 1: descent in $\mathbb{Z}[\sqrt{3}]$.**

**Lemma 5.4.2.** *For a primitive solution, $x, y, z$ are pairwise coprime, $3 \nmid xy$, and $x \equiv 2 \pmod 3$. The parities of $y$ and $z$ differ, and $x$ is odd. Also $x, y \neq 0$, and if $z = 0$ then $(x, y) = (-1, \pm 1)$.*

*Proof.* If 3 divides $x$ and $y$, then $3^4 \mid x^5 + y^4 = 3z^2$, so $3 \mid z$. If another prime divides two of the variables, then by the equation it also divides the third. Hence they are pairwise coprime. Modulo 3, $3 \mid x$ implies $3 \mid y$ and conversely, so $3 \nmid xy$, and $x^5 \equiv -y^4 \equiv -1$ gives $x \equiv 2 \pmod 3$. If $y, z$ are both odd, then $v_2(y^4 - 3z^2) = 1$, which is impossible since $y^4 - 3z^2 = -x^5$. Therefore the parities differ and $x$ is odd. If $x = 0$, then $y^4 = 3z^2$ gives $y = z = 0$. If $y = 0$, then $x^5 = 3z^2$ gives $3 \mid x$. If $z = 0$, then $x^5 = -y^4$ gives $x = -1$, $y = \pm 1$. □

**Lemma 5.4.3.** *For every primitive solution there exist $j \in \{-2, -1, 0, 1, 2\}$ and integers $a, b$ such that*

$$y^2 + z\sqrt{3} = (2 + \sqrt{3})^j (a + b\sqrt{3})^5, \qquad \gcd(a, b) = 1, \quad a + b \text{ odd}, \quad 3 \nmid a, \quad x = 3b^2 - a^2.$$

*Proof.* $\mathbb{Z}[\sqrt{3}]$ is norm-Euclidean: rounding the two coefficients gives a remainder $A + B\sqrt{3}$ with $|A|, |B| \leq \frac{1}{2}$ and $|A^2 - 3B^2| \leq \frac{3}{4}$. The unit group is $\{\pm(2 + \sqrt{3})^n\}$. There is no unit of norm $-1$, by reduction modulo 3, and a unit of norm 1 between 1 and $2 + \sqrt{3}$ would have to have $\sqrt{3}$-coefficient between 0 and 1. The product of $y^2 \pm z\sqrt{3}$ is $y^4 - 3z^2 = -x^5$. The norms of the two factors are units at 2 and 3, and any other common prime factor would divide both $y$ and $z$. Hence the two factors are coprime, and $y^2 + z\sqrt{3} = \pm(2 + \sqrt{3})^m \gamma^5$. Absorbing $-1$ and $(2 + \sqrt{3})^5$ into $\gamma^5$, we get $j \in \{-2, \ldots, 2\}$. A common prime factor of the coefficients of $\gamma = a + b\sqrt{3}$ divides $y$ and $z$, so $\gcd(a, b) = 1$. Since $N(2 + \sqrt{3}) = 1$, comparing norms gives $a^2 - 3b^2 = -x$. Since $x$ is odd, $a + b$ is odd, and since $3 \nmid x$, $3 \nmid a$. □

**Step 2: elimination of $j \neq 0$.** Writing $(a + b\sqrt{3})^5 = F + G\sqrt{3}$, we have

$$F = a(a^4 + 30a^2b^2 + 45b^4), \qquad G = b(5a^4 + 30a^2b^2 + 9b^4).$$

Multiplying by $(2 + \sqrt{3})^1$ and $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, we get, for $j = 1, 2$,

$$y^2 = F_1(a, b) := 2F + 3G, \qquad y^2 = F_2(a, b) := 7F + 12G.$$

Taking conjugates changes $(j, b, z)$ into $(-j, -b, -z)$, so it suffices to eliminate $j = 1, 2$.

We use the quintic field $L = \mathbb{Q}(\vartheta)$, $g(\vartheta) = 0$, $g(T) = T^5 - 5T^3 + 5T - 4$. The following facts are checked by certificate 1.2.6a.

- $\operatorname{disc}(g) = 2^4 \cdot 3^2 \cdot 5^5$ and $\mathcal{O}_L = \mathbb{Z}[\vartheta]$ ($g(T - 1)$ is Eisenstein at 5, and at 2 and 3 we use Dedekind's criterion). The signature is $(1, 2)$.
- $h_L = 1$. The Minkowski bound is less than 43, and every prime ideal of norm less than 43 is generated by an element of the same norm.
- $e_1 = 1 - \vartheta + \vartheta^3$ and $e_2 = 1 + 2\vartheta^2 + 3\vartheta^3 + \vartheta^4$ are units of norm 1, and $-1, e_1, e_2$ form a basis of $\mathcal{O}_L^\times / \mathcal{O}_L^{\times 2}$.
- $\varpi = \vartheta - 2$ and $\kappa = \vartheta^2 + \vartheta - 1$ have norms 2 and 4, and $(2) = (\varpi)(\kappa)^2$. There is one prime ideal above 5, and its residue degree is 1.
- For $\mu_1 = \vartheta^4 + 2\vartheta^3 - 5\vartheta^2 - 8\vartheta + 1$ and $\mu_2 = -\vartheta^4 - \vartheta^3 + 3\vartheta^2 + 2\vartheta$,

$$N(2a - \mu_1 b) = 16F_1(a, b), \qquad N(2a - \mu_2(a + b)) = 8F_2(a, b).$$

  The discriminants of the minimal polynomials of $\mu_1$ and $\mu_2$ are $2^{24}3^{10}5^5$ and $2^{16}3^{10}5^5$.

**Lemma 5.4.4.** *In Lemma 5.4.3, $j = 0$.*

*Proof.* Suppose $j \in \{1,2\}$, and put $\gamma = 2a - \mu_1 b$ ($j = 1$) or $\gamma = 2a - \mu_2(a+b)$ ($j = 2$). Then $N(\gamma) = 16y^2$ or $8y^2$, and $y \neq 0$.

Suppose a prime ideal $\mathfrak{P}$ above $p \notin \{2,3,5\}$ divides $\gamma$. The coefficient of $\mu_1$ or $\mu_2$ ($b$ or $a+b$) is not a multiple of $p$; otherwise $p \mid 2a$, and $p$ divides both $a$ and $b$. Thus the residue of $\mu_1$ (or $\mu_2$) is determined as an element of $\mathbb{F}_p$. Since $p$ does not divide the discriminants of $\mathbb{Z}[\mu_1]$ and $\mathbb{Z}[\mu_2]$, only one prime ideal above $p$ divides $\gamma$, and its residue degree is 1. So $v_{\mathfrak{P}}(\gamma) = v_p(N\gamma)$ is even. At 3 we have $F_1 \equiv 2a^5$ and $F_2 \equiv a^5 \pmod 3$, so $N\gamma$ is a unit. There is one prime ideal above 5, of residue degree 1, so its valuation is also $v_5(N\gamma)$, which is even. At 2, $v_2(N\gamma) = v_\varpi(\gamma) + 2v_\kappa(\gamma)$, so $v_\varpi(\gamma) \equiv v_2(N\gamma) \equiv j - 1 \pmod 2$. Since $h_L = 1$,

$$\gamma = \varpi^{j-1} e_1^i e_2^k \kappa^\ell w^2, \qquad i,k,\ell \in \{0,1\},\ w \in \mathcal{O}_L.$$

The factor $-1$ does not appear, because $N(-1) = -1$ and the norms of all the other factors are positive. And $w$ is integral, because all the remaining valuations are even and nonnegative.

Now we compare in $\mathcal{O}_L/8\mathcal{O}_L = R = (\mathbb{Z}/8)[T]/(g)$. $R$ has $8^5 = 32768$ elements, and exactly 336 of them are squares. For $a, b$ mod 8 with $a+b$ odd, the left side $\gamma$ mod 8 takes 16 values for each of $j = 1,2$. The right side is, for each of the eight $(i,k,\ell)$, the set of elements $\varpi^{j-1} e_1^i e_2^k \kappa^\ell \cdot (\text{square})$. The intersection of the two sets is empty for $j = 1,2$ and all eight $(i,k,\ell)$ (certificate 1.2.6a). This is a contradiction. □

**Step 3: the quartic curve $\mathcal{C}$.**

**Lemma 5.4.5.** *The primitive solutions are obtained from integral points $(u,r,s)$ of $\mathcal{C}$ with $u, r > 0$, $s \geq 0$, $\gcd(r,s) = 1$, by*

$$x = 3r^2s^2 - u^4, \qquad y = \pm u(r^4 - 45s^4), \qquad z = \pm rs(5u^8 + 30u^4r^2s^2 + 9r^4s^4).$$

*The solutions with $z = 0$ come from $(u,r,s) = (1,1,0)$.*

*Proof.* By Lemma 5.4.4, $y^2 = aP$ with $P = a^4 + 30a^2b^2 + 45b^4 > 0$, and $z = b(5a^4 + 30a^2b^2 + 9b^4)$. A common prime factor of $a$ and $P$ divides $45b^4$, and since $3 \nmid a$, it can only be 5. Since $y \neq 0$, $a > 0$. If $5 \nmid a$, then $a = u^2$. If $5 \mid a$, then $v_5(P) = 1$, so $a = 5u^2$; but then $y^2 = aP \equiv a^5 \equiv a \equiv 2u^2 \equiv 2 \pmod 3$, a contradiction. Hence $a = u^2$, $c^2 := P(u^2, b) = u^8 + 30u^4b^2 + 45b^4$, and $\gcd(u,b) = \gcd(u,15) = 1$. If $u$ is even, then $b$ is odd and $c^2 \equiv 13 \pmod{16}$, which is impossible (certificate 1.2.6b). Therefore $u$ is odd, $b$ is even and $c$ is odd. If $b = 0$, then $u = 1$.

If $b \neq 0$, then $m = (u^4 + 15b^2 + c)/2$ and $k = (u^4 + 15b^2 - c)/2$ are positive integers with $mk = 45b^4$. A common prime factor would divide $45b^4$ and $u^4 + 15b^2$, which contradicts $\gcd(u,b) = \gcd(u,15) = 1$; and the sum is odd. Distributing the fourth powers, we get, up to order, $(m,k) = (r^4, 45s^4)$ or $(5r^4, 9s^4)$, with $|b| = rs$ and $\gcd(r,s) = 1$. In the latter case the sum is 2 modulo 3, which is impossible since $m + k \equiv u^4 \equiv 1$. In the former case, $r^4 + 45s^4 = u^4 + 15r^2s^2$ is $\mathcal{C}$, $c = |r^4 - 45s^4|$, and $y = \pm uc$. The remaining formulas follow by substituting $a = u^2$, $b = \pm rs$. □

**Lemma 5.4.6.** *Every primitive integral point ($\gcd(u,r,s) = 1$) of $\mathcal{C}$ satisfies $\gcd(r,s) = 1$, $\gcd(u,30) = 1$, $\gcd(r,15) = 1$, $\gcd(u,rs) = 1$. Moreover, there is no point with $u = 0$ or $r = 0$.*

*Proof.* A common prime factor of $r, s$ also divides $u$. Modulo 16, the right-hand side is 7 or 15 if $r, s$ are both odd, 13 if $4 \mid r$ and $s$ is odd, and 5 if $r$ is odd and $s \equiv 2 \pmod 4$. In the remaining cases ($r \equiv 2 \pmod 4$ and $s$ odd, or $r$ odd and $4 \mid s$) it is 1 (certificate 1.2.6b). Hence $u$ is odd. If $3 \mid u$, then $3 \mid r$, $3 \nmid s$, and the 3-adic valuation of the right-hand side is exactly 2. If $5 \mid u$, then in the same way the 5-adic valuation is exactly 1. If $3 \mid r$ or $5 \mid r$, then $u$ is also divisible by that prime. A common prime factor of $u$ and $r$ divides $45s^4$, so it is 3 or 5, or it divides $s$, a contradiction. A common prime factor of $u$ and $s$ divides $r$. If $u = 0$, then $r^2/s^2$ is a root of a quadratic polynomial of discriminant 45, and if $r = 0$, then $u^4 = 45s^4$; both are impossible. □

**Step 4: descent over $\mathbb{Q}(\sqrt{5})$.**

**Lemma 5.4.7.** *If a primitive integral point of $\mathcal{C}$ has $s \neq 0$, then there exist $\sigma \in \{\pm 1\}$ and $t \in \mathbb{Q}^\times$ such that $(X, Y) = (9\sigma t^2, Y)$ is a point of $\mathcal{H}(\mathbb{Q})$. In particular, $X \neq 0$ and $X \in \sigma\mathbb{Q}^{\times 2}$. Moreover, if $X = -9$, then $(u, r, s) = (\pm 1, \pm 2, \pm 1)$.*

*Proof.* Put $\alpha = r^2 + \frac{-15+3d}{2}s^2$. Then $N(\alpha) = u^4 > 0$, so the two real embeddings of $\alpha$ have the same sign. Call this sign $\sigma$. A common prime factor of $(\alpha)$ and $(\bar{\alpha})$ divides $3ds^2$. Those above 3 and 5 cannot divide $N\alpha = u^4$ because $\gcd(u, 15) = 1$, and one above a prime factor of $s$ would also divide $r$. Hence all valuations of $(\alpha)$ are multiples of 4, and $\alpha = \sigma e^j \beta^4$ with $j \in \{0, 2\}$. In the residue field $\mathbb{F}_9$ above 3 we have $\alpha \equiv r^2 \equiv 1$, the fourth powers are $\pm 1$, and $e^2 \notin \mathbb{F}_3$; hence $j = 0$. Writing $\beta^2 = A + Bd$, we get

$$\sigma(A^2 + 5B^2) = r^2 - \tfrac{15}{2}s^2, \qquad 4AB = 3\sigma s^2, \qquad A^2 - 5B^2 = u^2.$$

Then $B \neq 0$, and putting $t = s/(2B)$ we get $A = 3\sigma B t^2$ and

$$(r/B)^2 = \sigma(9t^4 + 5) + 30t^2, \qquad (u/B)^2 = 9t^4 - 5.$$

Then $X = 9\sigma t^2$ and $Y = 27tru/B^2$ satisfy $Y^2 = f(X)$ (certificate 1.2.6b). If $X = -9$, then $\sigma = -1$, $t^2 = 1$, and $|r/B| = 4$, $|u/B| = 2$, $|s/B| = 2$, so $(u, r, s) = (\pm 1, \pm 2, \pm 1)$. □

**Proposition 5.4.8.** *The only rational points of $\mathcal{H}$ with $X \in \mathbb{Q}^{\times 2} \cup -\mathbb{Q}^{\times 2}$ are $(X, Y) = (-9, \pm 216)$.*

**Step 5: pointwise descent and three elliptic curves.**

**Lemma 5.4.9.** *Let $(X, Y) \in \mathcal{H}(\mathbb{Q})$ with $X = \sigma q^2 \neq 0$. Then the class of $(X - \rho,\ X - \tau)$ in $K^\times/K^{\times 2}$ is $(1, 1)$ if $\sigma = 1$, and $(-3e, -6)$ or $(3ed, -3d)$ if $\sigma = -1$.*

*Proof.* We have $f(X) = X \cdot N(X - \rho) \cdot N(X - \tau)$. Since $\operatorname{disc}(f) = 2^{14}3^{20}5^{10}$, the five roots are distinct at prime ideals coprime to 30. At such a prime ideal, if $X$ is integral, then at most one of the five linear factors of $f$ has positive valuation, and that valuation is even. If $X$ is not integral, then all factors have valuation $v(X) = 2v(q)$, which is even. Therefore both classes are represented by subproducts of $(-1, e, 2, 3, d)$. Imposing the norm condition $\sigma N(X - \rho)N(X - \tau) \in \mathbb{Q}^{\times 2}$ leaves 256 pairs for each sign.

Now we compute the local classes of the two numbers for all $q \in \mathbb{Q}_2$ and $q \in \mathbb{Q}_3$. At 2, we test $q \in \mathbb{Z}_2$ modulo 16, and if $q \notin \mathbb{Z}_2$ we test $v = 1/q \in 2\mathbb{Z}_2$ modulo 16 (in the latter case we use the square-equivalent pair $(\sigma - \rho v^2, \sigma - \tau v^2)$). On each ball the valuations of the two factors are at most 2, and changing the representative by 16 changes the factors by multiples of 32. So the ratio of the normalized units is 1 modulo 8, and it is a square in the unramified quadratic extension of $\mathbb{Q}_2$. At 3, we test the balls $q$ mod 3 and $v \in 3\mathbb{Z}_3$; a change by 3 does not change the normalized residues. As a result, after the condition at 2, 4 pairs remain if $\sigma = 1$ and 8 pairs if $\sigma = -1$; after the condition at 3, 1 pair and 2 pairs remain, respectively. The remaining pairs are those above (certificate 1.2.6c). □

We define three elliptic curves

$$E_0 :\ \eta^2 = \xi(\xi - \rho)(\xi + \tau), \quad E_1 :\ \eta^2 = \xi(\xi + 2e\rho)(\xi - 2e\tau), \quad E_2 :\ \eta^2 = \xi(\xi - e\rho)(\xi - e\tau).$$

The three cases of Lemma 5.4.9 give, respectively, the point $\xi = X$ of $E_0$, the point $\xi = -2eX$ of $E_1$, and the point $\xi = eX$ of $E_2$. For example, in the middle case, if $X - \rho = -3ea_1^2$ and $X - \tau = -6a_2^2$, then taking conjugates gives $X + \tau = -6\bar{a}_2^2$, and $X(X - \rho)(X + \tau) = -2e(3qa_1\bar{a}_2)^2$. In general, if $X(X - r_1')(X - r_2') = \lambda V^2$, then $(\xi, \eta) = (\lambda X, \lambda^2 V)$ is a point on $\eta^2 = \xi(\xi - \lambda r_1')(\xi - \lambda r_2')$; here $\lambda = -2e$, and it is a point of $E_1$. In the third case, $X(X - \rho)(X - \tau) = e(3dqa_1a_2)^2$. Under the 2-descent map $\delta(\xi, \eta) = (\xi, \xi - r_1)$ (roots $0, r_1, r_2$), the classes of these points are $(2e, 6)$ on $E_1$ and $(-e, 3d)$ on $E_2$.

**Step 6: rank.**

**Lemma 5.4.10.** *The ranks of $E_0, E_1, E_2$ over $K$ are $0, 1, 1$, and their torsion subgroups are $E_i[2]$. For $P_1 = (18e, 72) \in E_1(K)$ and $P_2 = (1 - 2e, 5 - 5e) \in E_2(K)$, the subgroup $\langle P_i, E_i[2]\rangle$ has odd index. The points obtained in Step 5 lie in $P_1 + 2E_1(K)$ on $E_1$, and in $T_0 + 2E_2(K)$ on $E_2$ ($T_0 = (0, 0)$).*

*Proof.* We use the complete 2-descent of [Sim02, Sil09]. The differences of the roots are supported only above 2, 3, 5, so the candidates are the $32^2 = 1024$ pairs of classes of $(-1, e, 2, 3, d)$. The local images have dimensions $4, 2, 2$ at 2, 3, 5. At 3 and 5, the classes of the two torsion points span the local image. At 2, we add 2-adic points with the following $\xi$: $-1 - e$, $-4 + 4e$ on $E_0$; $-2 - e$, $1 + e$ on $E_1$; $e$, $1 - 2e$ on $E_2$. At each of these points the valuation of the right-hand side is even and the normalized unit is a square modulo 8, so by Hensel's lemma they are genuine local points. Imposing the conditions at 2, 3, 5 and at the two real places in turn, the numbers of remaining candidates are $64, 16, 4, 4, 4$ for $E_0$, and $64, 16, 8, 8, 8$ for $E_1$ and $E_2$. The remaining candidates are generated by the classes of the torsion points and of $P_1$, $P_2$ (certificate 1.2.6d). Since $\dim E_i(K)[2] = 2$, the ranks are $0, 1, 1$. Also $\langle P_i, E_i[2]\rangle + 2E_i(K) = E_i(K)$, so multiplication by 2 is surjective on the finitely generated abelian group $E_i(K)/\langle P_i, E_i[2]\rangle$, which is therefore finite of odd order.

Torsion: at the two prime ideals above 11, the orders of the reduced groups are $(8, 12)$ for $E_0, E_1$ and $(12, 16)$ for $E_2$; above 19 they are $(16, 12)$, $(16, 28)$, $(28, 24)$. By [Kat81, Appendix], the order of the prime-to-11 part of the torsion divides $\gcd(8, 12) = \gcd(12, 16) = 4$, and since the orders above 19 are not multiples of 11, the 11-part is trivial. Hence the torsion is $E_i[2]$ (certificate 1.2.6d).

On $E_1$ the root is $r_1 = -2e\rho = 18e - 24$, so $\delta(P_1) = (18e, 24) = (2e \cdot 3^2, 6 \cdot 2^2) \equiv (2e, 6)$. On $E_2$ we have $r_1 = e\rho$, $r_2 = e\tau$, and $\delta(T_0) = (r_1 r_2, -r_1) = \big((-e)(3d/e)^2, 3d(e-1)^2\big) \equiv (-e, 3d)$. The kernel of $\delta$ is $2E_i(K)$, so the last claim follows. □

The case $\sigma = 1$ does not occur, because $E_0(K) = E_0[2]$ and none of the $\xi$-coordinates $0, \rho, -\tau$ of the torsion points lies in $\mathbb{Q}^\times$.

**Step 7: coset sieve.**

**Lemma 5.4.11.** *The points of $E_1$ from Step 5 have $X \equiv -9 \pmod{89}$ and map to $\pm P_1$ in the two reductions above 89. The points of $E_2$ have $X \equiv 0 \pmod{11}$ and map to $T_0$ in the two reductions above 11.*

*Proof.* The roots of $e^2 - e - 1$ are $10, 80$ modulo 89 and $4, 8$ modulo 11. Let $H_i$ be the subgroup of the product of the two reductions generated by the images of $P_i$ and $E_i[2]$. For $E_1$, the two reduced groups above 89 have orders $80, 96$, and $|H_1| = 480$ (index 16); for $E_2$, the orders above 11 are $12, 16$, and $|H_2| = 96$ (index 2). Since these indices are powers of 2 and the global index is odd, the image of $E_i(K)$ under reduction is $H_i$. Therefore the reductions of the cosets of Lemma 5.4.10 are $P_1 + 2H_1$ (60 elements) and $T_0 + 2H_2$ (12 elements).

The $\xi$-coordinate of the point is $\lambda_i X$ ($\lambda_1 = -2e$, $\lambda_2 = e$, $X \in \mathbb{Q}$). Testing all residues $X$ and all signs of $\eta$ at the two embeddings, the only ones that land in the coset are $X \equiv 80 \equiv -9$ with the points $((2, 72), (16, 72))$ or $((2, 17), (16, 17))$, that is, $\pm P_1$, on $E_1$, and $X \equiv 0$ with the point $(T_0, T_0)$ on $E_2$ (certificate 1.2.6e). Since $\lambda_i$ is a unit, if $X$ is a pole then the point maps to $(O, O)$, which lies in neither coset. Therefore $X$ is integral at the prime in question. □

**Step 8: elliptic Chabauty.**

**Lemma 5.4.12.** *The only point from Step 5 on $E_1$ is the one with $X = -9$, and there is none on $E_2$.*

*Proof.* We apply Proposition D with $\omega = d\xi/(2\eta)$ and $p = 89$ ($E_1$), $p = 11$ ($E_2$). The two $p$-adic embeddings give a logarithm $\log : E_i(K) \to \mathbb{Q}_p^2$, and since the rank is 1, its image is generated by $\log P_i$. Put $\ell_i = \log(P_i)/p$ and $c_i = ((\ell_i)_2, -(\ell_i)_1)$; then $c_i$ kills the logarithms of all global points.

Multiplying $P_i$ by its finite orders $n$ (20, 24 at 89, 6, 8 at 11) to bring it into the formal group, and computing $t = -x_{\text{short}}/\eta$ modulo $p^3$ ($\log = t + O(t^3)$), we get

$$\ell_1 \equiv (2490, 2948) \pmod{89^2}, \quad c_1 \equiv (11, 2) \pmod{89},$$
$$\ell_2 \equiv (117, 76) \pmod{11^2}, \quad c_2 \equiv (10, 4) \pmod{11}$$

(certificate 1.2.6f). The $c_i$ are primitive.

$E_1$: by Step 7, the centers of the disks are $\pm P_1$, and $T = X + 9 \in 89\mathbb{Z}_{89}$. The pullback of $\omega$ is $\lambda_1\, dX/(\pm 144)$, and its coefficients for the positive sign at the two embeddings are $(32, 78)$ modulo 89. The dot product with $c_1$ is 63 or 26, a unit. Since $\eta \equiv \pm 72$ is a unit, the map and the differential have integral coefficients on the disk.

$E_2$: here $X = -q^2$ with $q \in 11\mathbb{Z}_{11}$, and the point maps to $T_0$ in both reductions. Resolving this double contact by $\xi = -eq^2$, $\eta = qW$, we get

$$W^2 = -e^3(q^2 + \rho)(q^2 + \tau) = 45 - (12 + 6e)q^2 - (1 + 2e)q^4.$$

The square roots of 45 modulo 11 are $\pm 1$, and we allow all four combinations of signs at the two embeddings. The pullback is $\omega = -(e/W)\, dq$, and for the sign combinations $(1,1), (1,-1), (-1,1), (-1,-1)$ of $W$ its dot products with $c_2$ are $5, 3, 8, 6$, all units (certificate 1.2.6f). Since $2W$ is a unit, each branch is an analytic function with integral coefficients, and the center is $T_0$, whose logarithm is 0.

On every disk the annihilating logarithm has the form $L(T) = vT + \sum_{n\geq 2} a_{n-1}T^n/n$ ($v \in \mathbb{Z}_p^\times$, $a_i \in \mathbb{Z}_p$, $T \in p\mathbb{Z}_p$), and it vanishes at the center and at all global points. If $T \neq 0$, then $v_p(a_{n-1}T^n/n) \geq nv_p(T) - v_p(n) > v_p(T)$, so $L(T) \neq 0$. Hence on $E_1$ only $X = -9$ remains, and on $E_2$ only $q = 0$ remains, which contradicts $X \neq 0$. □

*Proof of Proposition 5.4.8.* If there is a rational point with $X = \sigma q^2 \neq 0$, then by Lemma 5.4.9 it gives a point on one of $E_0, E_1, E_2$. The case $\sigma = 1$ ($E_0$) was eliminated at the end of Step 6, and $E_2$ is eliminated by Lemma 5.4.12. What remains is $X = -9$ on $E_1$, and $f(-9) = 46656 = 216^2$. □

*Proof of Theorem 5.4.1.* If $z = 0$, then the solution is $(-1, \pm 1, 0)$ by Lemma 5.4.2. If $z \neq 0$, then the point $(u, r, s)$ of Lemma 5.4.5 has $s \neq 0$, and it is primitive since $\gcd(r, s) = 1$. By Lemma 5.4.7 and Proposition 5.4.8, $X = -9$ and $(u, r, s) = (1, 2, 1)$. Substituting gives $x = 11$, $y = \pm(16 - 45) = \mp 29$, $z = \pm 2(5 + 120 + 144) = \pm 538$. The equation is invariant under $y \mapsto -y$ and $z \mapsto -z$, so all four sign combinations are solutions, and all of them are primitive. □

## 5.5 $x^5 + y^4 + 3z^2 = 0$ ($H = 60$)

**Theorem 5.5.1.** *The only primitive integer solutions* ($\gcd(x, y, z) = 1$) *of* $x^5 + y^4 + 3z^2 = 0$ *are* $(x, y, z) = (-1, 1, 0),\ (-1, -1, 0)$.

**Setup.** Put $n = -x$. Then the equation becomes

$$y^4 + 3z^2 = n^5.$$

The proof has three steps. A fifth-power descent in the Eisenstein integers leads to the plane quartic curve $u^4 = r^4 + 15r^2s^2 + 45s^4$ (Step 1). A fourth-power descent over $\mathbb{Q}(\sqrt{5})$ leads to rational points with $X \neq 0$ on the genus 2 curve

$$\mathcal{H}: \quad Y^2 = f(X) := X(X^2 - 30X + 45)(X^2 - 45)$$

(Step 2). Finally, we show $J(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$ for the Jacobian $J$ of $\mathcal{H}$, which gives $\mathcal{H}(\mathbb{Q}) = \{\infty, (0, 0)\}$ (Step 3).

**Step 1: descent in the Eisenstein integers.**

**Lemma 5.5.2.** *For a primitive solution, $n > 0$ and $n, y, z$ are pairwise coprime. Moreover, $3 \nmid ny$, the parities of $y$ and $z$ differ, and $n$ is odd. Also $y \neq 0$, and if $z = 0$ then $n = 1$, $y = \pm 1$.*

*Proof.* If $n \leq 0$, then $y = z = 0$ and $n = 0$, contradicting primitivity. If a prime $p$ divides $n$ and $y$, then $p \mid 3z^2$. If $p \neq 3$, then $p \mid z$. If $p = 3$, then $3^4 \mid n^5 - y^4 = 3z^2$, so again $3 \mid z$. If $p \mid n, z$, then $p \mid y^4$, and if $p \mid y, z$, then $p \mid n^5$. Hence they are pairwise coprime. Modulo 3, $3 \mid n$ implies $3 \mid y$, and $3 \mid y$ implies $3 \mid n$, so $3 \nmid ny$. If $y, z$ are both odd, then $y^4 + 3z^2 \equiv 4 \pmod 8$, so $v_2(n^5) = 2$, which is not a multiple of 5. Therefore the parities differ and $n$ is odd. If $y = 0$, then $3z^2 = n^5$ gives $3 \mid n$, a contradiction. If $z = 0$, then $y^4 = n^5$ and $\gcd(n, y) = 1$, so $n = 1$, $y = \pm 1$. □

Let $d_0 = \sqrt{-3}$, $\omega = (-1 + d_0)/2$, and put

$$F(a, b) = a^4 - 30a^2b^2 + 45b^4.$$

**Lemma 5.5.3.** *For every primitive solution there exist coprime integers $a, b$ of different parity ($3 \nmid a$) such that $y^2 + zd_0 = (a + bd_0)^5$. Hence*

$$n = a^2 + 3b^2, \qquad y^2 = a\,F(a, b), \qquad z = b(5a^4 - 30a^2b^2 + 9b^4).$$

*Proof.* $\mathbb{Z}[\omega]$ is norm-Euclidean (rounding the two coefficients gives a remainder of norm at most $3/4$). The product of $y^2 \pm zd_0$ is $n^5$. A common prime factor of the two factors divides $2y^2$ and $2zd_0$; since the norm $n^5$ is coprime to 6, it would divide both $y$ and $z$, a contradiction. Hence the two factors are coprime, and since all six units are fifth powers of units, $y^2 + zd_0 = \gamma^5$ ($\gamma \in \mathbb{Z}[\omega]$). In $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega] \cong \mathbb{F}_4$ we have $y^2 + zd_0 \equiv y^2 + z \equiv 1$, and $\mathbb{F}_4^\times$ has order 3, so $\gamma^5 = \gamma^2 = 1$ gives $\gamma \equiv 1 \pmod 2$. That is, the $\omega$-coefficient of $\gamma$ is even, $\gamma = a + bd_0$ ($a, b \in \mathbb{Z}$), and $a + b$ is odd. A common prime factor of $a, b$ divides $y^2$ and $z$, so $\gcd(a, b) = 1$. Comparing norms gives $n = a^2 + 3b^2$, and since $3 \nmid n$, $3 \nmid a$. The last two formulas come from expanding $(a + bd_0)^5$. □

**Lemma 5.5.4.** *In Lemma 5.5.3, $a = u^2$ and $F(u^2, b) = c^2$, with $\gcd(u, b) = \gcd(u, 15) = 1$. Moreover, $u, c$ are odd and $b$ is even.*

*Proof.* Since $y \neq 0$, $F \neq 0$. A common prime factor of $a$ and $F$ divides $45b^4$, and since $\gcd(a, b) = 1$ and $3 \nmid a$, it can only be 5.

If $5 \nmid a$, then $\gcd(a, F) = 1$ and $aF = y^2$, so $a = \pm u^2$, $F = \pm c^2$ (same sign). Since $F \equiv a^4 \equiv 1 \pmod 3$, $F = -c^2$ is impossible, and $a = u^2$.

We rule out the case $5 \mid a$. In this case $v_5(F) = v_5(45b^4) = 1$, so $a = \pm 5u^2$, $F = \pm 5c^2$ (same sign). Since $F \equiv 1 \pmod 3$ and $5c^2 \equiv 2c^2 \not\equiv 1 \pmod 3$, the sign is negative:

$$a = -5u^2, \qquad F = -5c^2.$$

We compare these two equations modulo 16. If $a$ is odd, then $b$ is even, $45b^4 \equiv 0$, $a^4 \equiv 1$, and $30a^2b^2 \equiv 0$ or $8 \pmod{16}$, so $F \equiv 1$ or 9. If $a$ is even, then $u$ is even by $a = -5u^2$, so $4 \mid a$; and $b$ is odd, so $F \equiv 45b^4 \equiv 13 \pmod{16}$. Hence $F \bmod 16 \in \{1, 9, 13\}$. On the other hand, $c^2 \bmod 16 \in \{0, 1, 4, 9\}$, so $-5c^2 \bmod 16 \in \{0, 3, 11, 12\}$. The two sets are disjoint, so this case does not occur (certificate 1.2.7a).

Therefore $a = u^2$, $c^2 = u^8 - 30u^4b^2 + 45b^4$, $\gcd(u, b) = 1$ and $\gcd(u, 15) = 1$. If $u$ is even, then $b$ is odd and $c^2 \equiv 45 \equiv 13 \pmod{16}$, a contradiction. Hence $u$ is odd, $b$ is even and $c$ is odd. □

**Lemma 5.5.5.** *If there is a primitive solution with $z \neq 0$, then there are integers $u, r, s$ with $\gcd(r, s) = 1$ and $urs \neq 0$ satisfying*

$$\mathcal{C}: \quad u^4 = r^4 + 15r^2s^2 + 45s^4.$$

*Proof.* If $z \neq 0$, then $b \neq 0$. For $u, b, c$ as in Lemma 5.5.4,

$$m = \frac{u^4 - 15b^2 + c}{2}, \qquad k = \frac{u^4 - 15b^2 - c}{2}$$

are integers with $mk = 45b^4$ and $m + k = u^4 - 15b^2$. A common prime factor of $m, k$ divides $45b^4$ and $u^4 - 15b^2$; if it is a prime factor of $b$ it also divides $u$, and if it is 3 or 5 it divides $u$, so this is impossible. Hence $m, k$ are coprime. Distributing the fourth powers, up to swapping $m$ and $k$, $\{m, k\}$ is $\{\pm r^4, \pm 45s^4\}$ or $\{\pm 9r^4, \pm 5s^4\}$ (same sign, $|b| = rs$, $\gcd(r, s) = 1$). Since $m + k \equiv u^4 \equiv 1 \pmod 3$, only $(r^4, 45s^4)$ and $(-9r^4, -5s^4)$ remain. In the latter case, after renaming $r, s$, we get $u^4 = -5r^4 + 15r^2s^2 - 9s^4$, and since exactly one of $r, s$ is even, the right-hand side is one of $3, 7, 11$ modulo 16. This contradicts $u^4 \equiv 1 \pmod{16}$ (certificate 1.2.7a). In the former case, $r^4 + 45s^4 = u^4 - 15r^2s^2$ is exactly $\mathcal{C}$. □

**Lemma 5.5.6.** *Every primitive integral point* ($\gcd(u, r, s) = 1$) *of* $\mathcal{C}$ *satisfies* $\gcd(r, s) = 1$, $\gcd(ur, 30) = 1$ *and* $4 \mid s$.

*Proof.* A common prime factor of $r, s$ also divides $u$, so $\gcd(r, s) = 1$. Modulo 16, the right-hand side is 5 or 13 if $r, s$ are both odd, 9 or 13 if $r$ is even, 13 if $r$ is odd and $s \equiv 2 \pmod 4$, and 1 if $r$ is odd and $4 \mid s$ (certificate 1.2.7a). Fourth powers are 0 or 1 modulo 16, so $u, r$ are odd and $4 \mid s$. If $3 \mid u$, then modulo 3 we get $3 \mid r$ and $3 \nmid s$, and the 3-adic valuation of the right-hand side is exactly 2, so it is not a fourth power. If $5 \mid u$, then in the same way the 5-adic valuation of the right-hand side is exactly 1. If $3 \mid r$ or $5 \mid r$, then, modulo 3 or 5, $u$ is also divisible by that prime, which gives the contradiction just seen. □

**Step 2: descent over $\mathbb{Q}(\sqrt{5})$.** Let $K = \mathbb{Q}(d)$, $d = \sqrt{5}$, $e = (1 + d)/2$. Then $\mathcal{O}_K = \mathbb{Z}[e]$, and since the Minkowski bound is $\sqrt{5}/2 < 2$, $h_K = 1$. The unit group is $\{\pm e^j\}$ (if there were a unit $\rho$ with $1 < \rho < e$, its $e$-coefficient $(\rho - N\rho/\rho)/\sqrt{5}$ would have to lie between 0 and 1). Since $N(e) = -1$, the totally positive units are the $e^{2j}$. The primes 2 and 3 are inert in $K$, and $d$ is a prime element above 5.

**Lemma 5.5.7.** *If a primitive integral point of* $\mathcal{C}$ *has* $s \neq 0$, *then there is a rational point* $(X, Y) \in \mathcal{H}(\mathbb{Q})$ *with* $X \neq 0$.

*Proof.* Put $\alpha = r^2 + \frac{15+3d}{2}s^2 = r^2 + (6 + 3e)s^2$. Then $N(\alpha) = r^4 + 15r^2s^2 + 45s^4 = u^4$, and $\alpha$ is totally positive. A common prime factor of $(\alpha)$ and $(\bar{\alpha})$ divides $\alpha - \bar{\alpha} = 3ds^2$. Prime ideals above 3 and 5 cannot divide $u^4 = N\alpha$, because $\gcd(u, 15) = 1$ by Lemma 5.5.6; and a prime ideal above a prime factor of $s$ would also divide $r^2$, contradicting $\gcd(r, s) = 1$. Hence all valuations of $(\alpha)$ are multiples of 4. Since $h_K = 1$ and $\alpha$ is totally positive, $\alpha = e^j\beta^4$ with $\beta \in \mathcal{O}_K$ and $j \in \{0, 2\}$. Above 3 the residue field is $\mathbb{F}_9$, $\alpha \equiv r^2 \equiv 1$, and $\beta$ is a unit. The fourth powers in $\mathbb{F}_9^\times$ are $\{\pm 1\}$, and $e^2 = e + 1 \notin \mathbb{F}_3$, so $j = 2$ is impossible. Hence $\alpha = \beta^4$.

Writing $\beta^2 = A + Bd$ ($A, B \in \mathbb{Q}$) and comparing coefficients and norms, we get

$$A^2 + 5B^2 = r^2 + \tfrac{15}{2}s^2, \qquad 4AB = 3s^2, \qquad A^2 - 5B^2 = u^2.$$

Since $s \neq 0$, $AB \neq 0$. Putting $t = s/(2B)$, we get $A = 3Bt^2$ and

$$(r/B)^2 = 9t^4 - 30t^2 + 5, \qquad (u/B)^2 = 9t^4 - 5.$$

Then for $(X, Y) = (9t^2,\ 27tru/B^2)$ we have $X^2 - 30X + 45 = 9(9t^4 - 30t^2 + 5)$ and $X^2 - 45 = 9(9t^4 - 5)$, so $Y^2 = f(X)$ and $X \neq 0$ (certificate 1.2.7a). □

**Step 3: a Jacobian of rank 0.**

**Proposition 5.5.8.** $J(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$ *and* $\mathcal{H}(\mathbb{Q}) = \{\infty, (0, 0)\}$.

*Proof.* We have $\operatorname{disc}(f) = 2^{14}3^{20}5^{10}$. The two quadratic factors are irreducible, with roots $\theta_2 = 15 + 6d$ and $\theta_3 = 3d$ (and their conjugates). Hence the algebra of $f$ is $\mathbb{Q} \times K \times K$, and a basis of $J(\mathbb{Q})[2]$ is $T_0 = [(0,0) - \infty]$, $T_1 = [(\theta_2, 0) + (\bar{\theta}_2, 0) - 2\infty]$.

We use the odd-degree 2-descent of [Sto01, PS97, PS99],

$$J(\mathbb{Q})/2J(\mathbb{Q}) \hookrightarrow \ker\left(N : \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times (K^\times/K^{\times 2})^2 \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right).$$

At finite points that are not Weierstrass points, this map is $(X, X - \theta_2, X - \theta_3)$. Outside 2, 3, 5 the valuations of the image are even, and since $h_K = 1$, the $K$-components are represented by subproducts of $(-1, e, 2, 3, d)$ (with norms $1, -1, 4, 9, -5$). The rational component $q \in \{\pm 1, \pm 5\}$ is determined by the norm condition, so there are $32^2 = 1024$ candidates.

The local images are as follows. Let $v_x = (x, x - \theta_2, x - \theta_3)$, and let the values at the torsion points be $v_0 = (-2025, -\theta_2, -\theta_3)$ and $v_1 = (45, -\theta_2(\theta_2^2 - 45), \theta_3^2 - 30\theta_3 + 45)$. At $p = 2, 3, 5$ the two quadratic factors are irreducible over $\mathbb{Q}_p$ as well, so $\dim J(\mathbb{Q}_p)[2] = 2$, and the local formula of [Sto01, PS97, PS99] gives $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 4$ and $\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = 2$ ($p = 3, 5$). At 2, $v_0, v_1, v_{-1}, v_{-1/3}$ span the local image, of size 16. Here $f(-1) = 2^4 \cdot 209$ and $f(-1/3) = 2^6 \cdot 3131/243$, and the normalized 2-adic units are 1 modulo 8, so $X = -1, -1/3$ are $X$-coordinates of points of $\mathcal{H}(\mathbb{Q}_2)$. At 3 and 5, $v_0, v_1$ span the local image, of size 4. Imposing the conditions at 2, 3, 5 on the 1024 candidates in turn leaves $64, 16, 4$ (certificate 1.2.7b). The remaining four are the images of $0, T_0, T_1, T_0 + T_1$. Hence $\dim J(\mathbb{Q})/2J(\mathbb{Q}) \le 2 = \dim J(\mathbb{Q})[2]$, and $\operatorname{rank} J(\mathbb{Q}) = 0$.

Torsion part: counting points gives $\#J(\mathbb{F}_7) = 20$ and $\#J(\mathbb{F}_{11}) = 144$ ($\#J(\mathbb{F}_p) = (\#\mathcal{H}(\mathbb{F}_p)^2 + \#\mathcal{H}(\mathbb{F}_{p^2}))/2 - p$, $\#\mathcal{H}(\mathbb{F}_7) = 2$, $\#\mathcal{H}(\mathbb{F}_{49}) = 50$, $\#\mathcal{H}(\mathbb{F}_{11}) = 12$, $\#\mathcal{H}(\mathbb{F}_{121}) = 166$; certificate 1.2.7c). The primes 7 and 11 are good. By [Kat81, Appendix], the order of the part of the torsion prime to 7 and 11 divides $\gcd(20, 144) = 4$; the 7-part embeds in $J(\mathbb{F}_{11})$ and the 11-part in $J(\mathbb{F}_7)$, so both are trivial. Therefore $J(\mathbb{Q}) = J(\mathbb{Q})[2] \cong (\mathbb{Z}/2)^2$.

Finally, if $P \in \mathcal{H}(\mathbb{Q})$ is a finite point, then $2[P - \infty] = 0$, so $2P - 2\infty$ is a principal divisor. At $\infty$, $X$ has a pole of order 2 and $Y$ a pole of order 5, so $L(2\infty) = \langle 1, X \rangle$. Hence $2P - 2\infty = \operatorname{div}(X - X(P))$, and the zeros of this function are $P + \iota(P)$; so $P = \iota(P)$, that is, $Y(P) = 0$. The only rational root of $f$ is 0, so $P = (0, 0)$. □

*Proof of Theorem 5.5.1.* Suppose there is a primitive solution with $z \neq 0$. By Lemma 5.5.5, there is a point of $\mathcal{C}$ with $urs \neq 0$; dividing by the common divisor gives a primitive integral point, still with $s \neq 0$. By Lemma 5.5.7, this gives a rational point of $\mathcal{H}$ with $X \neq 0$, contradicting Proposition 5.5.8. Hence $z = 0$, and by Lemma 5.5.2, $n = 1$ and $y = \pm 1$, that is, $(x, y, z) = (-1, \pm 1, 0)$. These two points are indeed primitive solutions. □

# 6 Rational points on nine plane quartics

The statements give all integer solutions, including those with a zero coordinate. For the five bielliptic quartics, the involution $x \mapsto -x$ leads to a genus-two Jacobian; the other three cases of size 64 use elliptic or bitangent descent. The quartic of size 80 requires a different argument, based on cubic Hilbert symbols.

## 6.1 $x^4 + x^3y + xy^3 = z^4$ ($H = 64$)

**Theorem 6.1.1.** *The only integer solutions of $x^4 + x^3y + xy^3 = z^4$ are $(0, y, 0)$ and $(x, 0, \pm x)$.*

**Setup.** Let $F = \mathbb{Q}(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$, and write $N = N_{F/\mathbb{Q}}$. Put

$$A = 3\alpha^2 + 1, \qquad g(t) = t^2 + \alpha t + \alpha^2 + 1, \qquad G(x, y) = y^2 + \alpha xy + (\alpha^2 + 1)x^2 = x^2 g(y/x).$$

The proof obtains four covers $Y^4 = (-\alpha)^k g(t)$ by a fourth-power descent on $y - \alpha x$ (Step 1), eliminates two of them locally at 3 and 13 (Step 2), regards the remaining two as rank 1 elliptic curves over $F$ (Steps 3–4), and finishes with a Mordell–Weil sieve and elliptic Chabauty at 47 (Steps 5–6).

**Lemma 6.1.2.** *The following hold (*certificate 1.3.1a*).*

*(i)* $\operatorname{disc}(T^3+T+1) = -31$ *is squarefree, so* $\mathcal{O}_F = \mathbb{Z}[\alpha]$. *$F$ has one real place.*

*(ii)* $h_F = 1$, $\mathcal{O}_F^\times = \{\pm\alpha^k\}$, *and* $N(\alpha) = -1$.

*(iii) The eight elements* $\pm\alpha^k$ $(0 \le k \le 3)$ *are distinct in* $\mathcal{O}_F^\times/\mathcal{O}_F^{\times 4}$. *The elements* $-1$, $\alpha$, $-\alpha$ *are not squares in $F$.*

*(iv)* $N(A) = 31$ *and* $31\mathcal{O}_F = \mathfrak{P}^2\mathfrak{Q}$ *with* $\mathfrak{P} = (A)$, $\mathfrak{Q} = (\alpha - 3)$, *both of degree 1.*

*(v)* $(t-\alpha)g(t) = t^3+t+1$, $N(y-\alpha x) = y^3 + x^2y + x^3 = (y-\alpha x)G(x,y)$, *and* $G(x,\alpha x) = Ax^2$. *The polynomial $g$ has no root in $F$.*

The class number is 1 directly from the Minkowski bound $\frac{4}{\pi}\cdot\frac{3!}{3^3}\sqrt{31} < 2$.

**Step 1: four covers.**

**Lemma 6.1.3.** *Let* $(x,y,z)$ *be a solution with* $\gcd(x,y) = 1$ *and* $z \neq 0$. *Then there exist* $\varepsilon = \pm 1$ *and* $a, b > 0$ *such that* $x = \varepsilon a^4$ *and* $N(y-\alpha x) = \varepsilon b^4$. *Moreover, there exist* $s = \pm 1$, $0 \le k \le 3$ *and* $\beta \in \mathcal{O}_F$ *such that*

$$y - \alpha x = \delta\beta^4, \qquad \delta = s\alpha^k, \qquad \varepsilon = N(\delta) = s(-1)^k.$$

*In particular,* $t = y/x \in \mathbb{Q}$ *and* $Y = b/(a^2\beta) \in F^\times$ *satisfy*

$$Y^4 = (-\alpha)^k\, g(t).$$

*Proof.* The equation is $z^4 = x(x^3 + x^2y + y^3) = x\,N(y-\alpha x)$, and $\gcd(x, N(y-\alpha x)) = \gcd(x, y^3) = 1$. Since $z \neq 0$, the two factors are coprime integers of the same sign, hence $x = \varepsilon a^4$ and $N(y-\alpha x) = \varepsilon b^4$.

We show that $(y-\alpha x)$ is the fourth power of an ideal. If a prime ideal $\mathfrak{R}$ divides both $y-\alpha x$ and $G(x,y)$, then $\mathfrak{R} \nmid x$ (if $\mathfrak{R} \mid x$, then $\mathfrak{R} \mid y$, contradicting $\gcd(x,y) = 1$). But $G(x,y) \equiv G(x,\alpha x) = Ax^2 \pmod{y-\alpha x}$, so $\mathfrak{R} \mid A$, that is, $\mathfrak{R} = \mathfrak{P}$. Hence, if $\mathfrak{R} \neq \mathfrak{P}$, then $v_{\mathfrak{R}}(y-\alpha x) = v_{\mathfrak{R}}(N(y-\alpha x)) = 4v_{\mathfrak{R}}(b) \equiv 0 \pmod 4$. Since $\mathfrak{P}$ and $\mathfrak{Q}$ have degree 1, $v_{\mathfrak{P}}(y-\alpha x) = 4v_{31}(b) - v_{\mathfrak{Q}}(y-\alpha x) \equiv 0 \pmod 4$. Since $h_F = 1$, $y - \alpha x = \delta\beta^4$ with $\delta = s\alpha^k$, and comparing norms gives $\varepsilon = N(\delta) = s(-1)^k$.

Since $x \neq 0$, $t = y/x$ is defined, and $x^2 g(t) = G(x,y) = N(y-\alpha x)/(y-\alpha x) = \varepsilon b^4/(\delta\beta^4)$. Since $x^2 = a^8$, we get $Y^4 = b^4/(a^8\beta^4) = (\delta/\varepsilon)g(t)$, and $\delta/\varepsilon = \alpha^k(-1)^k$. □

**Step 2: local elimination of $k = 2, 3$.** The two lemmas below treat the system

$$x = \varepsilon a^4, \qquad y - \alpha x = \delta\beta^4, \qquad \gcd(x,y) = 1, \qquad \varepsilon = N(\delta) \tag{$*$}$$

locally. The curve $Y^4 = (-\alpha)^k g(t)$ alone is not enough. For example, the curve $Y^4 = (\alpha+1)g(t)$ for $k = 3$ has the $F$-point $(t, Y) = (-1, 1)$ ($(\alpha+1)(\alpha^2 - \alpha + 2) = \alpha^3 + \alpha + 2 = 1$).

**Lemma 6.1.4.** *If* $\delta = s\alpha^3$, *then* $(*)$ *has no solution in* $\mathbb{Z}_3$.

*Proof.* Modulo 3, $T^3 + T + 1 = (T-1)(T^2 + T + 2)$. The residue field of $\mathfrak{P}_1 = (3, \alpha - 1)$ is $\mathbb{F}_3$, and the residue field of $\mathfrak{P}_2$, of degree 2, is $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$. We have $\mathbb{F}_9^{\times 4} = \mathbb{F}_3^\times$ and $\varepsilon = -s$. If $3 \mid x$, then $y$ is a unit and $y - \alpha x \equiv y \pmod{\mathfrak{P}_2}$, so we would need $y/(s\alpha^3) \in \mathbb{F}_3^\times$, that is, $\alpha^3 = -\alpha - 1 \in \mathbb{F}_3$, which is false. If $3 \nmid x$, then $x \equiv \varepsilon = -s \pmod 3$. Modulo $\mathfrak{P}_2$ we have $y - \alpha x = \lambda s\alpha^3 = -\lambda s(1+\alpha)$ ($\lambda \in \mathbb{F}_3^\times$), and comparing the coefficients of 1 and $\alpha$ gives $y = -\lambda s$, $x = \lambda s$. Hence $\lambda = -1$ and $y \equiv s \pmod 3$. Then at $\mathfrak{P}_1$ ($\alpha \equiv 1$) we get $(y - \alpha x)/\delta \equiv (s+s)/s = 2 \equiv -1$, which is not a square in $\mathbb{F}_3$ and so cannot be a fourth power. □

**Lemma 6.1.5.** *If* $\delta = s\alpha^2$, *then* $(*)$ *has no solution in* $\mathbb{Z}_{13}$.

*Proof.* Modulo 13, $T^3+T+1=(T-7)(T^2+7T+11)$. The residue field of $\mathfrak{P}_1=(13,\alpha-7)$ is $\mathbb{F}_{13}$, and that of $\mathfrak{P}_2$ is $\mathbb{F}_{169}$. We have $\mathbb{F}_{13}^{\times 4}=\{1,3,9\}$, and $w\in\mathbb{F}_{169}^{\times}$ is a fourth power if and only if its norm to $\mathbb{F}_{13}$ lies in $\{1,3,9\}$. At $\mathfrak{P}_2$ the norm of $\alpha$ is 11, and $\varepsilon=s$.

If $13\mid x$, then $y-\alpha x\equiv y$ at both prime ideals. At $\mathfrak{P}_1$, $y/(10s)\in\{1,3,9\}$, so $y/s$ is a square modulo 13. Taking norms at $\mathfrak{P}_2$ gives $(y/s)^2/4\in\{1,3,9\}$, so $y/s\in\{2,5,6,7,8,11\}$, that is, a nonsquare. This is a contradiction.

If $13\nmid x$, then $t=y/x\in\mathbb{Z}_{13}$ and $t-\alpha=\alpha^2(\beta/a)^4$. Taking norms at $\mathfrak{P}_2$ gives $(t^2+7t+11)/4\in\{1,3,9\}$. At $\mathfrak{P}_1$, $t\equiv 7$ or $(t-7)/10\in\{1,3,9\}$, so $t\in\{4,6,7,11\}$. For these four values, $(t^2+7t+11)/4\equiv 4,6,11,10$, and none of them lies in $\{1,3,9\}$. □

The conclusions of the two lemmas are also confirmed by an exhaustive check over the residue fields (certificate 1.3.1b). Therefore a solution with $z\neq 0$ and $\gcd(x,y)=1$ gives, for $t=y/x\in\mathbb{Q}$ and $Y\in F^{\times}$, a point on

$$G_0:\ Y^4=g(t)\quad(k=0)\qquad\text{or}\qquad G_1:\ Y^4=-\alpha\,g(t)\quad(k=1).$$

**Step 3: two elliptic curves.**

**Lemma 6.1.6.** *Smooth models of $G_0$ and $G_1$ are isomorphic over $F$ to*

$$E_0:\ y^2=x^3+(3\alpha^2+4)x,\qquad E_1:\ y^2=x^3+k_1x,$$
$$k_1=\frac{39936\alpha^2-205568\alpha+169216}{29791}=(3\alpha^2+\alpha+1)\Big(\frac{40\alpha^2-4\alpha+28}{31}\Big)^4,$$

*respectively. Hence each $F$-point $(t,Y)$ of $G_k$ corresponds to exactly one $R\in E_k(F)$, with $t(R)=t$. On $E_0$, $t=(3\alpha^2+4-2\alpha x-x^2)/(4x)$, and the only poles of this function are $O$ and $T=(0,0)$. On $E_1$, $t=(a_P(x)+b_P(x)y)/c_P(x)$ ($c_P$ monic of degree 4, $\deg a_P=3$, $\deg b_P=2$), and the points with $t=0$ are $O$ and*

$$R_1=\Big(\frac{264\alpha^2-324\alpha-212}{961},\ \frac{23104\alpha^2+33848\alpha+49008}{29791}\Big).$$

*Proof.* $G_0$: put $U=Y^2$, $m=U-t$, $x=2m-\alpha$. Then $U^2=g(t)$ gives $t=(3\alpha^2+4-2\alpha x-x^2)/(4x)$ and $Y^2=(x^2+3\alpha^2+4)/(4x)$, hence $(2xY)^2=x^3+(3\alpha^2+4)x$. Putting $y=2xY$ gives a point of $E_0$.

$G_1$: the conic $U^2=-\alpha g(t)$ has the point $(t,U)=(0,1)$ ($-\alpha(\alpha^2+1)=1$). Parametrizing by lines through this point gives $t=-(\alpha^2+2m)/(m^2+\alpha)$, $U=(\alpha-\alpha^2m-m^2)/(m^2+\alpha)$. Then $Y^2=U$ becomes $V^2=(\alpha-\alpha^2m-m^2)(m^2+\alpha)$ ($V=Y(m^2+\alpha)$), and this quartic takes the square value $(m_0^2+\alpha)^2$ at $m_0=-\alpha^2/2$. Substituting $m=m_0+1/s$ and dividing by $(m_0^2+\alpha)^2$ gives a monic quartic whose $s^2$-coefficient is 0, and the standard Weierstrass map of a monic quartic gives $E_1$. The second expression for $k_1$ shows that $E_1$ is isomorphic to $y^2=x^3+(3\alpha^2+\alpha+1)x$.

Each map in the chain is verified by identities in function fields: each map lands on the target curve, and the two compositions are the identity (certificate 1.3.1c). The function $t$ has degree 4 on $E_0$, $E_1$ and $G_k$, so each map $E_k\to G_k$ has degree 1; being a birational map between smooth projective curves, it is an isomorphism. The points of $G_1$ with $t=0$ are $(0,\pm 1)$, and they map to $O$ and $R_1$. □

**Step 4: Mordell–Weil groups.**

**Lemma 6.1.7.** *For $E\in\{E_0,E_1\}$, $E(F)\cong\mathbb{Z}\oplus\{O,T\}$. For $P=(-\alpha,2)\in E_0(F)$ and $R_1\in E_1(F)$, the index $[E(F):\langle P,T\rangle]$ (or $[E_1(F):\langle R_1,T\rangle]$) is prime to 2, 3, 47.*

*Proof.* Rank: in the 2-isogeny descent ([Sim02, Sil09]) between $E_A:y^2=x^3+Ax$ and $E'_A:y^2=x^3-4Ax$, we have $2^{\mathrm{rank}}=|\operatorname{Im}\alpha_A|\,|\operatorname{Im}\alpha'_A|/4$, and the two images lie in the Selmer groups. With $S=\{(2),\mathfrak{Q}\}$, the dimensions of the Selmer groups are $(2,1)$ for $E_0$ ($A=3\alpha^2+4$) and $(1,2)$ for $E_1$ ($A=3\alpha^2+\alpha+1$) (certificate 1.3.1d). Hence both curves have rank at most 1. On $E_0$, $\alpha_A(P)=-\alpha$ and $\alpha_A(T)=A$ fill $\mathrm{Sel}(\alpha)$.

Torsion: $\#E(\mathbb{F}_v) = 48$ at the three prime ideals above 47, and $\#E(\mathbb{F}_v) = 68$ at the three prime ideals above 67 (for both curves). By [Kat81, Appendix], the order of the torsion divides $\gcd(48, 68) = 4$. Torsion of order 4 occurs only if $A$ or $-A$ is a square in $F$, and this is not the case since $N(3\alpha^2 + 4) = 31$ and $N(k_1) = 2^{24}/31^3$. Hence the torsion is $\{O, T\}$, $P$ and $R_1$ have infinite order, and the rank is 1.

Index: if 2 divides the index, then $P$ or $P + T$ lies in $2E(F)$. But the halving quartic $(x^2 - A)^2 - 4x_R(x^3 + Ax)$ has no root in $F$ for $R = P$, $P + T$ (for example, for $P$ on $E_0$ it has no root modulo $(13, \alpha - 7)$, and for $P + T$ none modulo $(23, \alpha - 4)$). For an odd prime $\ell$: if there is a place $v$ of degree 1 such that $\ell \mid N = \#E(\mathbb{F}_v)$, $N/\ell$ is even and $(N/\ell)\bar{P} \neq O$, then $\ell$ does not divide the index. For $\ell = 3$ we take $v = (11, \alpha - 2)$, $N = 12$, and for $\ell = 47$ we take $v = (1879, \alpha - 342)$, $N = 1880$. The same places work for both curves (certificate 1.3.1d). □

**Step 5: Mordell–Weil sieve at 47.**

**Lemma 6.1.8.** *If $R \in E_k(F)$ and $t(R) \in \mathbb{P}^1(\mathbb{Q})$, then there is $R_0$, with $R_0 \in \{O, T\}$ on $E_0$ and $R_0 \in \{O, R_1\}$ on $E_1$, such that $R - R_0$ reduces to $O$ at all three prime ideals above 47.*

*Proof.* The prime 47 splits completely in $F$. At the three places $v_1, v_2, v_3$ we have $\alpha \equiv 25, 34, 35$. Both curves have good reduction at the three places, and $\#E(\mathbb{F}_{v_j}) = 48$. The function $t$ is well defined as a function on the reduced curve at each $v_j$; that is, at every reduced point there is an expression for $t$ whose numerator and denominator do not vanish simultaneously (on $E_0$ the formula above works as it is, since $A$ is a 47-adic unit; certificate 1.3.1e). Therefore, if $t(R) \in \mathbb{P}^1(\mathbb{Q})$, the values of $t$ at the three reductions are equal in $\mathbb{P}^1(\mathbb{F}_{47})$.

The exponent of $\prod_j E(\mathbb{F}_{v_j})$ divides 48, and $[E(F) : \langle P, T\rangle]$ is prime to 48. Hence $\bar{R} = n\bar{P} + e\bar{T}$ ($n$ mod 24, $e \in \{0, 1\}$). The orders of $\bar{P}$ are $24, 4, 12$ on $E_0$ and $24, 6, 6$ on $E_1$ ($P = R_1$). Among the 48 pairs $(n, e)$, the only ones with three equal $t$-values are $O$ and $T$ ($t = \infty$) on $E_0$, and $O$ and $R_1$ ($t = 0$) on $E_1$ (certificate 1.3.1e). This is the claim ([BS10]). □

**Step 6: Strassmann argument at 47.**

**Lemma 6.1.9.** *In Lemma 6.1.8, $R = R_0$.*

*Proof.* Let $Q = 24P$. Since the order of $\bar{P}$ divides 24 at the three places, $Q$ lies in the group $K_1$ of points that reduce to $O$ at all three places. $K_1$ is infinite cyclic ($T \notin K_1$), and by Lemma 6.1.7, $[K_1 : \langle Q\rangle]$ is prime to 47. Therefore $R - R_0 = sQ$ with $s \in \mathbb{Z}_{(47)}$, and for the three embeddings $\sigma_j : F \to \mathbb{Q}_{47}$ we have $\sigma_j(R) = \sigma_j(R_0) + [s]\sigma_j(Q)$ with the same $s$.

We use the framework of Proposition D. Put $f = 1/t$ on $E_0$ and $f = t$ on $E_1$, and let $\lambda_j = \log z(\sigma_j Q)$ ($z$ the formal group parameter). A computation gives $v(\lambda_j) = 1$. Put

$$h(s) = f\big(\sigma_1(R_0) + [s]\sigma_1 Q\big) - f\big(\sigma_2(R_0) + [s]\sigma_2 Q\big) = \sum_{n \geq 0} a_n s^n.$$

Then $h(s) = 0$ when $t(R) \in \mathbb{Q}$. Near $R_0$, $f$ lies in $\mathbb{Z}_{47}[[z]]$: at $O$ and $T$ on $E_0$ because $A$ is a 47-adic unit, and at $R_1$ on $E_1$ because $R_1$ is 47-adically integral and $c_P(x(R_1))$ is a 47-adic unit. The coefficients $e_n$ of the formal exponential satisfy $n!e_n \in \mathbb{Z}_{47}$, so $v(a_n) \geq n - (n-1)/46$.

$E_0$: $t$ is a function of $x$ alone, so $t(-R) = t(R)$, and $-T = T$. Hence $h(-s) = h(s)$, and since $f(O) = f(T) = 0$, $a_0 = a_1 = 0$. A computation gives $v(a_2) = 2$, and by the inequality above $v(a_n) > 2$ for $n \geq 3$. By Strassmann's theorem, $h$ has at most two zeros in $\mathbb{Z}_{47}$ counted with multiplicity, and since $s = 0$ is a double zero, there are no other zeros.

$E_1$: $a_0 = 0$, $v(a_1) = 1$, and $v(a_n) > 1$ for $n \geq 2$. Hence the only zero is $s = 0$.

In both cases $s = 0$, that is, $R = R_0$ (certificate 1.3.1f). □

*Proof of Theorem 6.1.1.* If $d = \gcd(x, y) > 1$, then $d^4 \mid z^4$, so $(x/d, y/d, z/d)$ is also a solution. Hence we may assume $\gcd(x, y) = 1$. If $z = 0$, then $x\,N(y - \alpha x) = 0$, and since $\alpha \notin \mathbb{Q}$, $N(y - \alpha x) \neq 0$ when $x \neq 0$. Therefore $x = 0$, and the solution is $(0, y, 0)$.

If $z \neq 0$, then by Lemmas 6.1.3, 6.1.4, 6.1.5 we get a point of $G_0$ or $G_1$, and by Lemma 6.1.6 there is $R \in E_k(F)$ with $t(R) = y/x$. By Lemmas 6.1.8 and 6.1.9, on $E_0$ we have $R \in \{O, T\}$ and $t(R) = \infty$, which is impossible since $x = \varepsilon a^4 \neq 0$. On $E_1$ we have $R \in \{O, R_1\}$ and $t = 0$, that is, $y = 0$, $x = \pm 1$, $z = \pm 1$. Returning to the original solution, we get $(x, 0, \pm x)$. □

## 6.2 $x^4 - y^4 + x^2yz + yz^3 = 0$ **($H = 64$)**

**Theorem 6.2.1.** *The only integer solutions of* $x^4 - y^4 + x^2yz + yz^3 = 0$ *are* $(0,0,n)$, $(0,n,n)$, $(n,n,0)$, $(-n,n,0)$ $(n \in \mathbb{Z})$.

**Setup.** Let $C \subset \mathbb{P}^2$ be the projective curve defined by the equation in the theorem. The partial derivatives of $F = x^4 - y^4 + x^2yz + yz^3$ are

$$F_x = 2x(2x^2 + yz), \qquad F_y = -4y^3 + x^2z + z^3, \qquad F_z = y(x^2 + 3z^2).$$

$F_z = 0$ gives $y = 0$ or $x^2 = -3z^2$. If $y = 0$, then $F_x = F_y = 0$ gives $x = z = 0$. If $x^2 = -3z^2$, then $F_x = 0$ gives $x = 0$ (and then $z = 0$, $y = 0$) or $y = 6z$, and in the latter case $F_y = -866z^3 = 0$. Hence $C$ is a smooth plane quartic curve (genus 3). The points with $xyz = 0$ are found directly. If $x = 0$, then $y(z^3 - y^3) = 0$ gives $(0:0:1), (0:1:1)$; if $y = 0$, then $x = 0$; and if $z = 0$, then $x^4 = y^4$ gives $(\pm 1 : 1 : 0)$. Hence the theorem is equivalent to the statement that there is no rational point with $xyz \neq 0$. Such points lie in the chart $x \neq 0$, so we work with

$$r = y/x, \qquad t = z/x, \qquad F(r,t) := 1 + rt + rt^3 - r^4 = 0, \qquad rt \neq 0.$$

The map $\iota(x : y : z) = (-x : y : z)$ is an involution of $C$. The Ritzenthaler–Romagny construction of [Bru08, RR18] maps the chart $x \neq 0$ into the intersection of the three quadrics in $\mathbb{P}^4$ (coordinates $(x_1 : x_2 : x_3 : u : v)$)

$$\begin{aligned} Q_1 &= -x_1x_2 - x_2^2 - x_1x_3 - u^2, \\ Q_2 &= -x_2^2 - x_1x_3 - uv, \\ Q_3 &= x_1x_2 + 2x_2^2 + 2x_1x_3 + x_2x_3 - v^2 \end{aligned} \tag{15}$$

by

$$V(r,t) = \big(r(t-r) : 1 : r^2 + rt + t^2 : r : t\big).$$

Indeed, $Q_1(V) = Q_2(V) = -F$ and $Q_3(V) = 2F$. Let $M_i$ be the $5 \times 5$ symmetric matrix of $Q_i$, and $M_i'$ its upper left $3 \times 3$ block. Then

$$h(s) := -4 \det(M_1' - 2sM_2' + s^2M_3') = 6s^6 + 22s^5 + 15s^4 - 14s^3 - 7s^2 + 6s - 1$$

(certificate 1.3.2a), $h = (2s^2 + 2s - 1)(3s^4 + 8s^3 + s^2 - 4s + 1)$, and the two factors are irreducible over $\mathbb{Q}$. By [Bru08, RR18], the Prym of the cover $C \to C/\iota$ is isogenous to the Jacobian of the genus 2 curve

$$H : \ \eta^2 = h(s), \qquad J = \mathrm{Jac}(H).$$

Let $D_\infty$ be the sum of the two points at infinity of $H$ (a rational divisor), and let $\kappa : J \to \mathcal{K} \subset \mathbb{P}^3$ be the Kummer map. In Kummer coordinates $\kappa(0) = (0:0:0:1)$, and the first three coordinates of $[(s_1, \eta_1) + (s_2, \eta_2) - D_\infty]$ are $(1 : s_1 + s_2 : s_1s_2)$. The proof below does not use the Prym identification itself. The required map $C \to J$ is obtained directly in Lemma 6.2.2 by a computation over the function field.

**Step 1: the map $\phi : C \to J$.** At a point $P$ of $C$ ($rt \neq 0$) we take the tangent direction

$$w = \frac{1}{2\Delta}\big(-N_1,\ 4r^3 - t^3 - t,\ -N_3,\ 2\Delta,\ 0\big), \qquad \Delta = r^4 - rt^3 + 1,$$

$$\begin{aligned} N_1 &= 2r^4t - 3r^2t^3 + r^2t + rt^4 - rt^2 + 4r - 2t, \\ N_3 &= 2r^4t + 4r^3t^2 + 3r^2t^3 - r^2t + rt^4 - rt^2 - 4r - t^5 - t^3 - 2t. \end{aligned}$$

The following hold (certificate 1.3.2c).

(i) $V^{\mathsf{T}} M_i w = 0$ $(i = 1,2,3)$, and the left $3 \times 3$ minor of the tangent matrix $(V^{\mathsf{T}} M_i)_i$ is $\Delta/4$.

(ii) On $C$, $\Delta = rt + 2$. If $rt = -2$, then multiplying $F = 0$ by $-r^2$ gives $r^6 + r^2 + 8 = 0$; so $\Delta \neq 0$ at rational points.

(iii) The fifth coordinate of $w$ is 0 and the fifth coordinate of $V$ is $t \neq 0$, so $w$ is not proportional to $V$.

Now put

$$q_i = w^{\mathsf{T}} M_i w \quad (i = 1,2,3), \qquad A_P(s) = q_1(P) - 2s\, q_2(P) + s^2 q_3(P).$$

The $q_i$ are rational functions on $C$ whose denominators are powers of $\Delta$. If we replace the tangent direction by $aw + bV$ $(a \neq 0)$, then, since $V^{\mathsf{T}} M_i V = 0$ and $V^{\mathsf{T}} M_i w = 0$, $A_P$ is only multiplied by $a^2$.

**Lemma 6.2.2.** *There is a map $\phi : C \to J$ over $\mathbb{Q}$ with the following properties.*

*(a) For $P \in C(\mathbb{Q})$ with $rt \neq 0$, $(q_1, q_2, q_3)(P) \neq (0,0,0)$ and $\phi(P) = [D_P - D_\infty]$. Here $D_P$ is an effective divisor of degree 2 on $H$, and its $s$-coordinates are the roots of the quadratic form $A_P$ (if $q_3(P) = 0$, one root is $\infty$).*

*(b) For the two quartics $\Phi_1, \Phi_2$ given in certificate 1.3.2a, certificate 1.3.2b, we have $\kappa(\phi(P)) \in \Gamma := \{\Phi_1 = \Phi_2 = 0\}$ for all $P \in C$.*

*Proof.* We compute over the function field $K = \mathbb{Q}(C)$ (certificate 1.3.2b). At the generic point, $A(s) = q_1 - 2sq_2 + s^2 q_3 \in K[s]$ is an irreducible quadratic. There are exactly two elements $\pm\phi_K$ of $J(K)$ whose Mumford representation has first polynomial $A/q_3$. Their Kummer images coincide, and the coordinates $(1 : 2q_2/q_3 : q_1/q_3 : k_4)$ satisfy $\Phi_1$, $\Phi_2$ and the equation of the Kummer surface.

We choose one $\phi_K$. Then $\phi_K \in J(K)$ is a rational map $C \dashrightarrow J$ over $\mathbb{Q}$. Since $C$ is a smooth projective curve and $J$ is a projective variety, it extends to a morphism $\phi : C \to J$. For the same reason, an effective divisor of degree 2 over $K$ representing $\phi_K$ gives a morphism $\psi : C \to \mathrm{Sym}^2 H$, and $\phi(P) = [\psi(P) - D_\infty]$. The composition of $\psi$ with the $s$-projection $\mathrm{Sym}^2 H \to \mathrm{Sym}^2 \mathbb{P}^1 = \mathbb{P}^2$ is $(q_1 : -2q_2 : q_3)$ at the generic point. Hence, at points where the three functions are regular and not all zero, it equals their value.

(a) At rational points with $rt \neq 0$ we have $\Delta \neq 0$, so the $q_i$ are regular. If $q_2(P) = q_3(P) = 0$, then the ideal memberships

$$(r-1)^2(r+1)^2(r^2+1)^2, \quad t - r^7 + r^3 \;\in\; \big(F,\ \mathrm{num}\, q_2,\ \mathrm{num}\, q_3\big) \subset \mathbb{Q}[r,t]$$

(certificate 1.3.2c) give $r = \pm 1$ and $t = r^7 - r^3 = 0$, a contradiction. Hence the $s$-coordinates of $D_P := \psi(P)$ are the roots of $A_P$.

(b) $\Phi_i \circ \kappa \circ \phi$ is a section of a line bundle on $C$ that vanishes at the generic point, so it is identically 0. □

**Step 2:** $J(\mathbb{Q})$**.**

**Lemma 6.2.3.** $J(\mathbb{Q}) = \langle T \rangle \oplus \langle G \rangle \cong \mathbb{Z}/2 \oplus \mathbb{Z}$, *where, in Mumford representation,*

$$T = \big(s^2 + s - \tfrac{1}{2},\ 0\big), \qquad G = \big(s^2 + 2s - 1,\ 2s - 1\big).$$

*Proof.* Since $h$ is the product of an irreducible quadratic and an irreducible quartic over $\mathbb{Q}$, $J(\mathbb{Q})[2] = \langle T \rangle \cong \mathbb{Z}/2$. The 2-Selmer group has order 8, and 2 is the only place at which $H$ is deficient. Since the number of deficient places is odd, $Ш(J)[2] \neq 0$, and by [Sto01, PS97, PS99], rank $J(\mathbb{Q}) \leq 3 - 1 - 1 = 1$. Since $G$ has infinite order, the rank is 1. That the torsion is only $\langle T \rangle$ and that $T, G$ generate all of $J(\mathbb{Q})$ is proved by a saturation computation using height constants ([CF96, Sto99, Sto02]). All of this is checked separately by certificate 1.3.2a and certificate 1.3.2d. □

**Step 3: Mordell–Weil sieve.** For $P \in C(\mathbb{Q})$ we write $\phi(P) = nG + eT$ ($n \in \mathbb{Z}$, $e \in \{0,1\}$). By Lemma 6.2.2(b), $\Phi_i(\kappa(nG + eT)) = 0$. Kummer coordinates are normalized to primitive integer vectors. $H$ has good reduction at 5, 29, 113.

**Lemma 6.2.4.** *$e = 0$ and $n \equiv 0, \pm 2, \pm 14 \pmod{31}$.*

*Proof.* Reduction is compatible with the group law and with the Kummer map, so $\kappa(n\bar{G} + e\bar{T}) \in \Gamma(\mathbb{F}_{29})$ ([BS10]). The order of $\bar{G} \in J(\mathbb{F}_{29})$ is 31. Testing all 62 pairs $(n \bmod 31, e)$ leaves only $(0,0), (2,0), (14,0), (17,0), (29,0)$ (certificate 1.3.2a). Here $17 \equiv -14$ and $29 \equiv -2$. (At $p = 5$ the order of $\bar{G}$ is also 31, and 13 classes remain. They contain all five classes above, so nothing more is removed.) □

**Lemma 6.2.5.** *$n \not\equiv \pm 14 \pmod{31}$.*

*Proof.* Put $Q = 31G$; then $\bar{Q} = 0$. Let $J^k$ be the kernel of reduction modulo $29^k$. Then $Q \in J^1$, and $z([29^k]Q) \equiv 29^k z(Q) \pmod{29^{k+2}}$ from Lemma E gives $[29^k]Q \in J^{k+1}$. Hence, if $n \equiv n' \pmod{31 \cdot 29^k}$, then $nG - n'G \in J^{k+1}$. Since the Kummer map is defined over $\mathbb{Z}_{29}$, the primitively normalized vectors $\kappa(nG)$ and $\kappa(n'G)$ agree modulo $29^{k+1}$ up to a unit multiple. Therefore $\Phi_i(\kappa(n'G)) \equiv 0 \pmod{29^{k+1}}$ must hold.

$k = 1$: if $n \equiv 14 \pmod{31}$, then among $n' = 14 + 31d$ ($0 \le d \le 28$) only 231 satisfies this condition. Similarly, from 17 only 668 remains. $k = 2$: among $231 + 899d$ ($0 \le d \le 28$) only 18211 remains, and among $668 + 899d$ only 7860 remains (certificate 1.3.2a). Hence $n \equiv 18211$ or $7860 \pmod{31 \cdot 29^2}$, and modulo $29^2$, $n \equiv 550$ or 291.

At $p = 113$ the order of $\bar{G}$ is $6728 = 2^3 \cdot 29^2$. For the 16 classes of $n$ mod 6728 with $n$ mod $841 \in \{291, 550\}$, none of the points $\kappa(n\bar{G})$ lies in $\Gamma(\mathbb{F}_{113})$ (certificate 1.3.2a). This is a contradiction. □

**Step 4: 29-adic isolation of the three remaining disks.**

**Lemma 6.2.6.** *$n \in \{0, 2, -2\}$.*

*Proof.* Let $z = (z_1, z_2)$ be the 29-adic formal group parameter of $J$; then $J^1$ corresponds to $z \in (29\mathbb{Z}_{29})^2$. Near the origin, writing the Kummer coordinates as $(\kappa_1 : \kappa_2 : \kappa_3 : 1)$, the $\kappa_j \in \mathbb{Z}_{29}[[z]]$ have no constant term. Since $\kappa \circ [-1] = \kappa$ and $[-1]z = -z + O(z^2)$, they have no linear term either. Hence $\kappa_j = B_j(z) + O(|z|^3)$ ($B_j$ quadratic forms). The primitive Kummer coordinates $(k_1, k_2, k_3, k_4)$ of $Q = 31G$ have valuations $(2, 2, 2, 0)$, and $(k_1, k_2, k_3) \equiv 29^2 \cdot (9, 10, 6) \pmod{29^3}$ (certificate 1.3.2a). Therefore $z(Q) = 29\zeta$ with $\zeta \in \mathbb{Z}_{29}^2$, and $B(\zeta) \equiv c\,(9, 10, 6) \pmod{29}$ ($c$ a unit).

(a) $n \equiv 0 \pmod{31}$: write $n = 31m$, $m = 29^e u \neq 0$ ($u$ a unit). By Lemma E, $z([m]Q) = 29^{1+e}(u\zeta + O(29))$, so

$$(\kappa_1, \kappa_2, \kappa_3)([m]Q) = 29^{2+2e}\big(u^2 B(\zeta) + O(29)\big).$$

Since $\Phi_i(k_1, k_2, k_3, 1)$ has no terms $k_4^4$, $k_4^3 k_j$, its lowest-order part is the quadratic form given by the coefficient of $k_4^2$:

$$L_1 = -336k_1k_2 + 540k_1k_3 - 135k_2^2 + 672k_3^2, \qquad L_2 = -192k_1k_2 + 388k_1k_3 - 97k_2^2 + 384k_3^2.$$

Hence $\Phi_1(\kappa([m]Q)) = 29^{4+4e}\big(u^4c^2 L_1(9, 10, 6) + O(29)\big)$. Since $L_1(9, 10, 6) \equiv 13 \not\equiv 0 \pmod{29}$ (and $L_2(9, 10, 6) \equiv 24$), the valuation is $4 + 4e$, which is finite. That is, if $m \neq 0$, then $\kappa(nG) \notin \Gamma$; so $n = 0$.

(b) $n \equiv 2 \pmod{31}$: write $n = 2 + 31m$, $m = 29^e u \neq 0$. In the patch $k_1 = 1$, $\kappa(2G) \equiv b = (1, 25, 2, 27) \pmod{29}$. Translation by $2G$ is an automorphism over $\mathbb{Z}_{29}$, so for $Y \in J^1$ we have $\kappa(2G + Y) = \kappa(2G) + \Lambda z(Y) + O(|z(Y)|^2)$ ($\Lambda$ a matrix over $\mathbb{Z}_{29}$). From the difference for $m = 1$ we get $\Lambda\zeta \equiv d = (0, 17, 9, 15) \pmod{29}$ (certificate 1.3.2a). Hence $\kappa(2G + [m]Q) = \kappa(2G) + 29^{1+e}\big(u\,d + O(29)\big)$. Since $\Phi_i(\kappa(2G)) = 0$,

$$\Phi_i\big(\kappa(2G + [m]Q)\big) = 29^{1+e}\big(u\,D_d\Phi_i(b) + O(29)\big),$$

and since $(D_d\Phi_1(b), D_d\Phi_2(b)) \equiv (23, 9) \pmod{29}$, the valuation is $1 + e$, which is finite. Hence $n = 2$.

(c) If $n \equiv -2 \pmod{31}$, then $\kappa(nG) = \kappa(-nG)$ and $-n \equiv 2 \pmod{31}$, so $-n = 2$ by (b). □

**Step 5: fibers over the three classes.**

**Lemma 6.2.7.** *For $P \in C(\mathbb{Q})$ with $rt \neq 0$, $\phi(P) \notin \{0, 2G, -2G\}$.*

*Proof.* (a) Suppose $\phi(P) = \pm 2G$. Since $\kappa(\pm 2G) = (32 : -128 : -52 : -441)$, the first Mumford polynomial of $\pm 2G$ is $s^2 + 4s - \frac{13}{8}$. In genus 2, the effective divisor $E$ of degree 2 in a nonzero class $[E - D_\infty]$ is unique, so $D_P$ of Lemma 6.2.2(a) is that divisor. Then $A_P$ is a constant multiple of $s^2 + 4s - \frac{13}{8}$, and at $P$

$$2q_2 + 4q_3 = 0, \qquad 8q_1 + 13q_3 = 0.$$

The lexicographic Gröbner basis of the ideal of $\mathbb{Q}[r, t]$ generated by these two equations (with denominators cleared) and $F$ is

$$r^4 - rt - 1, \qquad (r^2 - 1)t^2, \qquad t^3$$

(certificate 1.3.2e). Hence $t = 0$, contradicting $rt \neq 0$.

(b) Suppose $\phi(P) = 0$. Then $D_P \sim D_\infty$. The complete linear system of $D_\infty$ is the unique $g^1_2$ of $H$, that is, the fibers of $s$, so the $s$-image of $D_P$ is a single point. Hence the discriminant $q_2^2 - q_1 q_3$ of $A_P$ vanishes at $P$. The resultant with respect to $t$ of $F$ and the numerator of this discriminant is

$$\tfrac{1}{64}\, r^4 (r-1)^4 (r+1)^4 (r^2+1)^4 A_8(r) B_8(r) C_{24}(r),$$

where $A_8$, $B_8$, $C_{24}$ are irreducible polynomials over $\mathbb{Q}$ of degrees 8, 8, 24 (certificate 1.3.2c). For example, $A_8 = 27r^8 + 16r^6 - 19r^4 - 6r^2 - 1$ and $B_8 = 28r^8 + 16r^6 - 18r^4 + 2r^2 - 1$. Therefore $r \in \{0, \pm 1\}$. But $r \neq 0$, and $F(\pm 1, t) = \pm t(t^2 + 1)$ gives $t = 0$, a contradiction. □

*Proof of Theorem 6.2.1.* Suppose there is $P \in C(\mathbb{Q})$ with $xyz \neq 0$. Then $rt \neq 0$. By Lemma 6.2.3 we can write $\phi(P) = nG + eT$. By Lemmas 6.2.4, 6.2.5, 6.2.6, $\phi(P) \in \{0, \pm 2G\}$, which contradicts Lemma 6.2.7. The rational points with $xyz = 0$ are the four points found in the setup, and the integer solutions above them are the four forms in the theorem. □

At $(\pm 1 : 1 : 0)$, the tangent quadratic computed with a different tangent direction is proportional to $s^2 + 4s - \frac{13}{8}$, and the only elements of $J(\mathbb{Q})$ with this first polynomial are $\pm 2G$ (certificate 1.3.2a). So $\pm 2G$ necessarily survive the sieve; they are indeed the images of these two points.

## 6.3 $x^4 + x^2y^2 + y^3z - yz^3 = 0$ ($H = 64$)

**Theorem 6.3.1.** *The only integer solutions of $x^4 + x^2y^2 + y^3z - yz^3 = 0$ are $(0, 0, n)$, $(0, n, 0)$, $(0, n, n)$, $(0, n, -n)$ $(n \in \mathbb{Z})$.*

**Setup.** Let $C \subset \mathbb{P}^2$ be the projective curve defined by the equation in the theorem, and put $J_C = \mathrm{Jac}(C)$. $C$ is a smooth plane quartic curve (certificate 1.3.3a). Hence it has genus 3 and is not hyperelliptic. The map $\iota(x : y : z) = (-x : y : z)$ is an involution of $C$. Putting $x^2 = X$, we get $(2X + y^2)^2 = y^4 - 4y^3z + 4yz^3$, so the quotient curve $E = C/\langle \iota \rangle$ is $W^2 = y^4 - 4y^3z + 4yz^3$. $E$ has the rational point $(y : z : W) = (0 : 1 : 0)$ and is isomorphic over $\mathbb{Q}$ to the elliptic curve $Y^2 = X^3 - 16X + 16$ of conductor 37. The point $Q_0 = (0 : 0 : 1)$ is a rational fixed point of $\iota$. For $P \in C(\mathbb{Q})$ put

$$\delta_P = [P - \iota(P)] \in J_C(\mathbb{Q}).$$

Then $\delta_P = (1 - \iota_*)[P - Q_0]$, so $\delta_P$ is a rational point of the Prym variety $\mathrm{Prym}(C/E) = (1 - \iota_*)J_C$.

In the form of Ritzenthaler–Romagny,

$$C : \; x^4 - h_0 x^2 + f_0 g_0 = 0, \qquad f_0 = yz, \quad h_0 = -y^2, \quad g_0 = y^2 - z^2.$$

The matrix of coefficients of $(f_0, h_0, g_0)$ with respect to $(y^2, yz, z^2)$ and its inverse are

$$A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 1 & 0 & -1 \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix}.$$

Let $(a_i, b_i, c_i)$ be the rows of $A^{-1}$, and put $a(s) = a_1 + 2a_2 s + a_3 s^2$, and $b(s)$, $c(s)$ in the same way. Then $a = 2s$, $b = -(s^2+1)$, $c = -s^2$. By [Bru08, RR18], $\mathrm{Prym}(C/E)$ is isogenous over $\mathbb{Q}$ to the Jacobian $J_H$ of

$$H:\ \eta^2 = b(b^2 - ac) = -(s^2+1)(s^4 + 2s^3 + 2s^2 + 1)$$

(certificate 1.3.3a). This identification, including the quadratic twist, is confirmed by $L_p(C) = L_p(E)\,L_p(H)$ at all good primes $3 \le p \le 79$ (certificate 1.3.3b).

**Step 1: the rank of the Prym.**

**Lemma 6.3.2.** $\mathrm{rank}\, J_H(\mathbb{Q}) = 0$. *Hence* $\mathrm{Prym}(C/E)(\mathbb{Q})$ *is finite, and for every* $P \in C(\mathbb{Q})$, $\delta_P$ *is a torsion point of* $J_C(\mathbb{Q})$.

*Proof.* The 2-descent of [Sto01, PS97, PS99] gives the upper bound 0 for $\mathrm{rank}\, J_H(\mathbb{Q})$ (certificate 1.3.3a: the lower and upper bounds for the rank are both 0). In fact, $J_H(\mathbb{Q}) = \langle (s^2+1,\, 0) \rangle \cong \mathbb{Z}/2$ (certificate 1.3.3c). Isogenies preserve the rank, so $\mathrm{Prym}(C/E)(\mathbb{Q})$ is a finite group, and its element $\delta_P$ is torsion. □

**Step 2: the order of $\delta_P$.**

**Lemma 6.3.3.** *For every* $P \in C(\mathbb{Q})$, $2\delta_P = 0$.

*Proof.* $C$ has good reduction at 3 and 5, and

$$J_C(\mathbb{F}_3) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/14, \qquad J_C(\mathbb{F}_5) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/176$$

(certificate 1.3.3a). The orders are $L_3(1) = 28$ and $L_5(1) = 352$, respectively, where

$$L_3(T) = 1 + 27T^6, \qquad L_5(T) = 1 + 4T + 15T^2 + 32T^3 + 75T^4 + 100T^5 + 125T^6.$$

Let $\ell$ be a prime dividing the order of $\delta_P$. By [Kat81, Appendix], if $\ell \neq 3$ then $\ell \mid 28$, and if $\ell \neq 5$ then $\ell \mid 352$. If $\ell = 3$ we would need $3 \mid 352$, and if $\ell = 5$ we would need $5 \mid 28$; both are impossible. In the remaining cases $\ell \mid \gcd(28, 352) = 4$, so $\ell = 2$. Hence the order of $\delta_P$ is a power of 2, and by [Kat81, Appendix] the group generated by $\delta_P$ maps injectively into $J_C(\mathbb{F}_3)$. The 2-part of $J_C(\mathbb{F}_3)$ is $(\mathbb{Z}/2)^2$, which has exponent 2, so $2\delta_P = 0$. □

**Step 3: fixed points.**

*Proof of Theorem 6.3.1.* Let $P \in C(\mathbb{Q})$ with $P \neq \iota(P)$. By Lemma 6.3.3, $2[P - \iota(P)] = 0$. This contradicts [Har77, Section IV.5] ($C$ is a smooth plane quartic curve, so it is not hyperelliptic). Hence $P = \iota(P)$. The fixed points of $\iota$ are the points on the line $x = 0$ and $(1:0:0)$, and $(1:0:0)$ does not lie on $C$. If $x = 0$, then $yz(y-z)(y+z) = 0$, so $C(\mathbb{Q})$ consists of the four points $(0:0:1)$, $(0:1:0)$, $(0:1:1)$, $(0:-1:1)$. The integer solutions above these four points are the four forms in the theorem. □

## 6.4 $x^4 + y^4 + x^2yz - yz^3 = 0$ $(H = 64)$

**Theorem 6.4.1.** *The only integer solutions of* $x^4 + y^4 + x^2yz - yz^3 = 0$ *are* $(0, 0, n)$ *and* $(0, n, n)$ $(n \in \mathbb{Z})$.

**Setup.** Since the equation is homogeneous, it suffices to determine the rational points of the projective plane quartic curve

$$C:\quad X^4 + Y^4 + X^2YZ - YZ^3 = 0.$$

$C$ is smooth (certificate 1.3.4a). Hence it has genus 3 and, by [Har77, Section IV.5], it is not hyperelliptic. Theorem 6.4.1 follows directly from the next proposition, because a nonzero integer solution gives a rational point of $C$, and the integer solutions above the two points $(0:0:1)$, $(0:1:1)$ are $(0, 0, n)$, $(0, n, n)$.

**Proposition 6.4.2.** $C(\mathbb{Q}) = \{(0:0:1), (0:1:1)\}$.

The involution $\iota(X:Y:Z) = (-X:Y:Z)$ preserves $C$. The fixed points of $\iota$ in the plane are the line $X = 0$ and the point $(1:0:0)$, and $(1:0:0)$ does not lie on $C$. In the chart $Y = 1$, with $u = X/Y$, $t = Z/Y$, the curve $C$ is $u^4 + 1 + u^2t - t^3 = 0$. The functions $w = 4t$, $v = 4(2u^2 + t)$ satisfy

$$v^2 - (w^3 + w^2 - 64) = 64\,(u^4 + 1 + u^2t - t^3),$$

so the quotient curve $E = C/\iota$ is the elliptic curve $v^2 = w^3 + w^2 - 64$ (conductor 431). Let $P_C = \mathrm{im}(1 - \iota_*) \subset J_C$ be the Prym variety of the cover $C \to E$. It is an abelian variety of dimension 2, and $J_C$ is isogenous to $E \times P_C$.

Writing $C$ in the form $X^4 - hX^2 + fg = 0$, we have $f = Y(Y - Z)$, $h = -YZ$, $g = Y^2 + YZ + Z^2$. The matrix whose rows are the coefficients of $(Y^2, YZ, Z^2)$ in $f, h, g$, in this order, and its inverse are

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix}.$$

Forming $\alpha_1 + 2\alpha_2 s + \alpha_3 s^2$ from each column $(\alpha_1, \alpha_2, \alpha_3)^{\mathsf{T}}$ of $A^{-1}$ gives, in order, $a(s) = 1 - s^2$, $b(s) = 2s^2 - 2s - 1$, $c(s) = s^2$. By [Bru08, RR18], $P_C$ is isogenous over $\mathbb{Q}$ to the Jacobian $J_H$ of the genus 2 curve

$$H: \quad y^2 = f_H(s), \qquad \begin{aligned} f_H = b(b^2 - ac) &= 10s^6 - 26s^5 + 9s^4 + 18s^3 - 5s^2 - 6s - 1 \\ &= (2s^2 - 2s - 1)(5s^4 - 8s^3 - s^2 + 4s + 1). \end{aligned}$$

These polynomial identities are checked by certificate 1.3.4a. The same code also checks $L_p(C, T) = L_p(E, T)\, L_p(H, T)$ at the good primes $p = 5, 7, 11$. These finite comparisons check the formula and twist; the isogeny itself follows from the cited construction.

The proof has three steps. We show $\mathrm{rank}\, J_H(\mathbb{Q}) = 0$ (Lemma 6.4.3), show that the torsion of $J_C(\mathbb{Q})$ has order at most 2 (Lemma 6.4.4), and use these two facts to show that every rational point is a fixed point of $\iota$ (Lemma 6.4.5).

**Step 1: the rank of $J_H$.**

**Lemma 6.4.3.** $\mathrm{rank}\, J_H(\mathbb{Q}) = 0$. *Hence $P_C(\mathbb{Q})$ is a finite group.*

*Proof.* Let $D_\infty$ be the sum of the two points at infinity of $H$ (a rational divisor). For the two roots $\alpha, \bar{\alpha}$ of $2s^2 - 2s - 1$, the class $T = [(\alpha, 0) + (\bar{\alpha}, 0) - D_\infty]$, with Mumford representation $(s^2 - s - \frac{1}{2},\, 0)$, is an element of order 2 of $J_H(\mathbb{Q})$. Hence $\dim_{\mathbb{F}_2} J_H(\mathbb{Q})[2] \geq 1$.

The 2-Selmer group has 4 elements, that is, $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(\mathbb{Q}, J_H) = 2$ (certificate 1.3.4b). Moreover, the only place where $H$ is deficient, that is, where it has no $\mathbb{Q}_v$-rational divisor of degree 1, is $v = 2$ (certificate 1.3.4b). In particular, $H(\mathbb{Q}_2) = \emptyset$, because $f_H(s) \equiv 3, 7 \pmod 8$ if $s \in \mathbb{Z}_2$, and $s^{-6} f_H(s) \equiv 2 \pmod 4$ if $s \notin \mathbb{Z}_2$. On the other hand, at $\infty$ there are real points since the leading coefficient is $10 > 0$, and at the odd bad primes 3, 431 there are $\mathbb{Q}_p$-points. Since the number of deficient places is odd, the Poonen–Stoll version of [Sto01, PS97, PS99] gives $\mathrm{Sha}(J_H)[2] \neq 0$ and

$$\dim \mathrm{Sel}^2 \;\geq\; \mathrm{rank}\, J_H(\mathbb{Q}) + \dim J_H(\mathbb{Q})[2] + 1 \;\geq\; \mathrm{rank}\, J_H(\mathbb{Q}) + 2.$$

Therefore $\mathrm{rank}\, J_H(\mathbb{Q}) = 0$. Magma's `RankBounds` gives the same upper bound 0 (certificate 1.3.4a). The rank does not change under isogeny, so $\mathrm{rank}\, P_C(\mathbb{Q}) = 0$, and $P_C(\mathbb{Q})$ is a finite group. □

**Step 2: torsion of $J_C(\mathbb{Q})$.**

**Lemma 6.4.4.** *$J_C(\mathbb{Q})_{\mathrm{tors}}$ has order at most 2. In particular, every torsion element $x \in J_C(\mathbb{Q})$ satisfies $2x = 0$.*

*Proof.* $C$ has good reduction at 5, 7, 11, and the Jacobians of the reductions are

$$J_C(\mathbb{F}_5) \simeq \mathbb{Z}/110, \qquad J_C(\mathbb{F}_7) \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/140, \qquad J_C(\mathbb{F}_{11}) \simeq \mathbb{Z}/17 \oplus \mathbb{Z}/68$$

(certificate 1.3.4a). Their orders are $110 = 2 \cdot 5 \cdot 11$, $280 = 2^3 \cdot 5 \cdot 7$, $1156 = 2^2 \cdot 17^2$, respectively. Suppose an odd prime $\ell$ divides $\#J_C(\mathbb{Q})_{\mathrm{tors}}$. If $\ell \neq 5$, then $\ell \mid 110$ by [Kat81, Appendix], so $\ell = 11$. But $11 \nmid 280$, a contradiction at $p = 7$. If $\ell = 5$, then $5 \nmid 1156$ gives a contradiction at $p = 11$. Hence $J_C(\mathbb{Q})_{\mathrm{tors}}$ is a 2-group, and by [Kat81, Appendix] it injects into the 2-part $\mathbb{Z}/2$ of $J_C(\mathbb{F}_5)$. □

**Step 3: rational points are fixed points of $\iota$.**

**Lemma 6.4.5.** *For every $P \in C(\mathbb{Q})$, $\iota(P) = P$.*

*Proof.* $Q_0 = (0:0:1) \in C(\mathbb{Q})$ is a fixed point of $\iota$. For $P \in C(\mathbb{Q})$,

$$\delta_P = [P - \iota(P)] = (1 - \iota_*)[P - Q_0] \in P_C(\mathbb{Q}).$$

By Lemma 6.4.3, $\delta_P$ is a torsion element, and by Lemma 6.4.4, $2\delta_P = 0$, that is, $2P \sim 2\iota(P)$. If $P \neq \iota(P)$, this contradicts [Har77, Section IV.5]. Hence $P = \iota(P)$. □

*Proof of Proposition 6.4.2.* By Lemma 6.4.5, rational points are fixed points of $\iota$, and since $(1:0:0) \notin C$, we have $X = 0$. Substituting $X = 0$ gives

$$Y^4 - YZ^3 = Y(Y - Z)(Y^2 + YZ + Z^2) = 0.$$

Since $Y^2 + YZ + Z^2$ has discriminant $-3$, it has no rational root with $(Y, Z) \neq (0, 0)$. The remaining points are $(0:0:1)$ and $(0:1:1)$, and both lie on $C$. □

## 6.5 $x^4 - x^2y^2 + y^3z + yz^3 = 0$ ($H = 64$)

**Theorem 6.5.1.** *The only integer solutions of $x^4 - x^2y^2 + y^3z + yz^3 = 0$ are $(0, 0, n)$, $(0, n, 0)$, $(n, n, 0)$, $(-n, n, 0)$ $(n \in \mathbb{Z})$.*

**Setup.** The projective plane quartic curve

$$C: \quad F(X, Y, Z) = X^4 - X^2Y^2 + Y^3Z + YZ^3 = 0$$

is smooth modulo 3 (certificate 1.3.5a). Hence it is smooth over $\mathbb{Q}$ as well, has genus 3, and by [Har77, Section IV.5] is not hyperelliptic. Theorem 6.5.1 is equivalent to the following proposition.

**Proposition 6.5.2.** $C(\mathbb{Q}) = \{(0:0:1), (0:1:0), (1:1:0), (-1:1:0)\}$.

*Involution and Prym model.* Let $\iota(X:Y:Z) = (-X:Y:Z)$. In the chart $Y = 1$, with $r = X/Y$, $t = Z/Y$, $R = r^2$, the curve $C$ is $r^4 - r^2 + t + t^3 = 0$, and the quotient curve $E = C/\iota$ is $R^2 - R + t + t^3 = 0$ (an elliptic curve of conductor 91). Let $P_C = \mathrm{im}(1 - \iota_*) \subset J_C$ be the Prym variety of the cover $C \to E$. $C$ has the form $X^4 - hX^2 + fg = 0$ with $f = YZ$, $h = Y^2$, $g = Y^2 + Z^2$. Applying the construction of [Bru08, RR18] to these data, we obtain three quadratic forms in $(a, b, c)$

$$q_1 = b^2 + ac, \qquad q_2 = ab, \qquad q_3 = -b^2 - ac + bc$$

and the curve $D:\ q_1 = u^2,\ q_2 = uv,\ q_3 = v^2$ in $\mathbf{P}^4$. The map

$$\pi:\ C \to D, \qquad (X:Y:Z) \mapsto (a:b:c:u:v) = (YZ : X^2 : Y^2 + Z^2 : XY : XZ)$$

satisfies $q_1 - u^2 = F$, $q_2 - uv = 0$, $q_3 - v^2 = -F$, so it indeed maps to $D$. On $X \neq 0$, $\pi$ is an isomorphism onto its image, and the image lies in the smooth part $U$ of $D$ ($b = X^2 \neq 0$; [Bru08, RR18]). On $C$, $Y = 0$ implies $X = 0$, so the points with $X \neq 0$ lie in the chart $Y = 1$.

Let $N_i$ be the $3 \times 3$ symmetric matrix of $q_i$, and let $M_i$ be the $5 \times 5$ symmetric matrices of the three equations $q_1 - u^2$, $q_2 - uv$, $q_3 - v^2$ of $D$. The genus 2 curve is

$$\begin{aligned} H: \quad y^2 &= -4 \det(N_1 - 2sN_2 + s^2 N_3) \\ &= -s^6 - 2s^5 + 3s^4 + 2s^3 - 3s^2 + 1 \\ &= -(s^2 - 1)(s^4 + 2s^3 - 2s^2 + 1). \end{aligned}$$

(certificate 1.3.5b), and the prime factors of its discriminant are 2, 7, 13. $D_\infty$ is the sum of the two points at infinity of $H$ (a rational divisor). At a smooth point $\mathbf{v}$ of $D$ (viewed as a vector), the three rows $\mathbf{v}^{\mathsf{T}} M_i$ have rank 3, and their common kernel $W_{\mathbf{v}}$ is a 2-dimensional space containing $\mathbf{v}$. For $\mathbf{w} \in W_{\mathbf{v}} \setminus \mathbb{Q}\mathbf{v}$ we call

$$\tau_{\mathbf{v}}(s) = \mathbf{w}^{\mathsf{T}} (M_1 - 2sM_2 + s^2 M_3)\, \mathbf{w}$$

the *tangent quadratic* at $\mathbf{v}$. Since $\mathbf{v}^{\mathsf{T}} M_i \mathbf{v} = \mathbf{v}^{\mathsf{T}} M_i \mathbf{w} = 0$, replacing $\mathbf{w}$ by $\alpha\mathbf{w} + \beta\mathbf{v}$ only multiplies $\tau_{\mathbf{v}}$ by $\alpha^2$. In the chart $Y = 1$, at the image $\mathbf{v}_{\mathrm{gen}} = (t : R : 1 + t^2 : r : rt)$ of the generic point of $C$, the tangent quadratic is proportional to $A_2 s^2 + Bs + A_0$, formed from

$$\begin{aligned} A_2 &= -R^4 + 4R^3 t - 2R^3 - R^2 + 12Rt^2 - 4Rt - 4R - 4t^2, \\ B &= 2(3R^2 t^2 + 7R^2 + 3Rt^2 - 5R + 4t), \\ A_0 &= -4R^3 t + 13R^2 t - 12Rt^2 - Rt + 4R + 3t^2 - 1 \end{aligned}$$

(certificate 1.3.5b).

*Kummer surface.* Let $\kappa : J_H \to K_H \subset \mathbf{P}^3$ be the Kummer map in Cassels–Flynn coordinates $(k_1 : k_2 : k_3 : k_4)$. Then $\kappa(0) = (0 : 0 : 0 : 1)$, and $\kappa(x) = \kappa(y)$ is equivalent to $x = \pm y$. For an effective divisor $P_1 + P_2$, $P_i = (x_i, y_i)$, that is not a hyperelliptic fiber, $\kappa([P_1 + P_2 - D_\infty]) = (1 : x_1 + x_2 : x_1 x_2 : *)$. $\Phi_1, \Phi_2 \in \mathbb{Z}[k_1, \ldots, k_4]$ are the two quartic forms given in certificate 1.3.5b (28 terms each). In the chart $k_4 = 1$, $\Phi_1$ has no constant or linear term, and

$$\Phi_1 = 512k_1k_2 - 992k_1k_3 + 248k_2^2 + 512k_2k_3 + (\text{terms of degree 3 and 4})$$

(certificate 1.3.5d).

The proof goes as follows. We construct a map $\varphi : C \to J_H$ over $\mathbb{Q}$ from the tangent quadratic (Lemma 6.5.3), determine $J_H(\mathbb{Q})$ (Lemma 6.5.4), and show $\varphi(C(\mathbb{Q})) \subset \{0, \pm 4G\}$ by a sieve modulo 3 and 3-adic analysis (Lemma 6.5.10). Finally, we determine the two fibers (Lemmas 6.5.11, 6.5.12).

**Step 1: the map $\varphi$.**

**Lemma 6.5.3.** *There is a map $\varphi : C \to J_H$ defined over $\mathbb{Q}$ such that the following hold.*

*(i) For all $P \in C$, $\Phi_1(\kappa(\varphi(P))) = \Phi_2(\kappa(\varphi(P))) = 0$.*

*(ii) If $Y(P) \neq 0$ and $(A_2, B, A_0)(P) \neq (0, 0, 0)$, then $\varphi(P) = [D_P - D_\infty]$. Here $D_P$ is an effective divisor of degree 2 on $H$, and its $x$-image is the zero set in $\mathbf{P}^1$ of $A_2(P)s^2 + B(P)s + A_0(P)$.*

*(iii) If $X(P) \neq 0$ and $\varphi(P) = 0$, then $2[P - \iota(P)] = 0$.*

*Proof.* Over the function field $\mathbb{Q}(C) = \mathbb{Q}(r, t)$, certificate 1.3.5b checks the following. The generic point $\mathbf{v}_{\mathrm{gen}} = (t : R : 1 + t^2 : r : rt)$ lies on $D$, and $\dim W_{\mathbf{v}_{\mathrm{gen}}} = 2$. The tangent quadratic has degree 2, is irreducible over $\mathbb{Q}(C)$, and is proportional to $A_2 s^2 + Bs + A_0$. There are exactly two points $\pm\varphi_{\mathrm{gen}}$ of $J_H(\mathbb{Q}(C))$ whose Mumford polynomial is the monic version of this quadratic, and their common Kummer point satisfies $\Phi_1 = \Phi_2 = 0$ and $k_2 A_2 + k_1 B = 0$, $k_3 A_2 - k_1 A_0 = 0$.

$\varphi_{\mathrm{gen}} \in J_H(\mathbb{Q}(C))$ is a rational map $C \dashrightarrow J_H$ defined over $\mathbb{Q}$. Since $C$ is a smooth projective curve and $J_H$ is a projective variety, it extends to a morphism $\varphi : C \to J_H$. Likewise, the effective divisor of degree 2 determined by the Mumford representation of $\varphi_{\mathrm{gen}}$ is a $\mathbb{Q}(C)$-point of $\mathrm{Sym}^2 H$, and it extends to a morphism $\psi : C \to \mathrm{Sym}^2 H$. The two maps $\varphi$ and $P \mapsto [\psi(P) - D_\infty]$ agree at the generic point, hence everywhere. Put $D_P = \psi(P)$.

(i) $\kappa \circ \varphi$ is a morphism, and $\Phi_i \circ \kappa \circ \varphi$ vanishes at the generic point. Since zero sets are closed, it vanishes on all of $C$.

(ii) The composition of $\psi$ with $\mathrm{Sym}^2 H \to \mathrm{Sym}^2 \mathbf{P}^1 \simeq \mathbf{P}^2$ (the coefficients of the quadratic form of the $x$-image) is a morphism $C \to \mathbf{P}^2$, and it equals $(A_2 : B : A_0)$ at the generic point. In the chart $Y \neq 0$, $A_2, B, A_0$ are polynomials in $R, t$, so at points where the three values are not all 0, the value of this morphism is $(A_2(P) : B(P) : A_0(P))$.

(iii) By [Bru08, RR18], on the smooth part $U$ of $D$ the map given by the tangent construction is $\lambda \circ d$. Here $d(Q) = [2\iota(Q) - 2Q]$ is the map to the Prym scheme $P'$ of $D$ (the identity component of the kernel of the norm in $\mathrm{Pic}^0 D$), and $\lambda : P' \to J_H$ is an isomorphism over $\mathbb{Q}$. At the generic point, the value of this map is the class whose Mumford polynomial is the tangent quadratic, so it is $\pm\varphi_{\mathrm{gen}}$. Hence $\varphi = \pm\lambda \circ d \circ \pi$ on $\pi^{-1}(U) \supset \{X \neq 0\}$. Moreover, the pullback $\nu : P' \to P_C \subset J_C$ under the normalization $C \to D$ is an isogeny, and $\nu(d(\pi(P))) = 2[\iota(P) - P]$. Therefore, if $X(P) \neq 0$ and $\varphi(P) = 0$, then $d(\pi(P)) = 0$ and $2[P - \iota(P)] = 0$. □

**Step 2:** $J_H(\mathbb{Q})$.

**Lemma 6.5.4.** *$J_H(\mathbb{Q}) = \langle T \rangle \oplus \langle G \rangle \simeq \mathbb{Z}/2 \oplus \mathbb{Z}$, where, in Mumford representation,*

$$T = (s^2 - 1,\ 0) = [(1,0) + (-1,0) - D_\infty], \qquad G = (s^2 + s,\ -s - 1) = [(0,-1) + (-1,0) - D_\infty],$$

*and $\kappa(4G) = (32 : 16 : -12 : 73)$.*

*Proof.* certificate 1.3.5b computes this with Magma's `MordellWeilGroupGenus2`. The rank upper bound from 2-descent ([Sto01, PS97, PS99]) is 1, the torsion subgroup is $\langle T \rangle$, and $G$ has infinite order. That $\langle T, G \rangle$ is saturated is proved using bounds for the canonical height ([CF96, Sto99, Sto02]), and both proof flags are true. The same code also computes $\kappa(4G)$. □

**Step 3: sieve modulo 3.** $H$ has good reduction at 3. The order of $\bar{G}$ in $J_H(\mathbb{F}_3)$ is 5. Put $S = 5G$; then $S$ lies in the kernel $J_1$ of reduction modulo 3.

**Lemma 6.5.5.** *If $P \in C(\mathbb{Q})$ and $\varphi(P) = eT + nG$ ($e \in \{0,1\}$, $n \in \mathbb{Z}$), then $e = 0$ and $n \equiv 0, 1, 4 \pmod 5$. Hence, for some $m \in \mathbb{Z}$, $\kappa(\varphi(P)) = \kappa([m]S)$ or $\kappa(\varphi(P)) = \kappa(4G + [m]S)$.*

*Proof.* By Lemma 6.5.3(i), the primitive integer coordinates of $\kappa(\varphi(P))$ satisfy $\Phi_1 = \Phi_2 = 0$, and so do their reductions modulo 3. Reduction modulo 3 commutes with the Kummer map ([BS10]), so the Kummer point of $\overline{\varphi(P)} = e\bar{T} + n\bar{G}$ must satisfy $\Phi_1 \equiv \Phi_2 \equiv 0 \pmod 3$. Among the 10 classes $e\bar{T} + n\bar{G}$ ($e \in \{0,1\}$, $0 \leq n < 5$) of $J_H(\mathbb{F}_3)$, only $(e,n) = (0,0), (0,1), (0,4)$ satisfy this (certificate 1.3.5c). If $n = 5m$, then $\varphi(P) = [m]S$; if $n = 4 + 5m$, then $\varphi(P) = 4G + [m]S$. If $n = 1 + 5m'$, then $-\varphi(P) = 4G + [-1 - m']S$, and $\kappa(-x) = \kappa(x)$. □

**Step 4: 3-adic analysis.** $J_H$ extends to an abelian scheme over $\mathbb{Z}_3$, and $J_1$ is identified with $(3\mathbb{Z}_3)^2$ through the formal group $\hat{F}$ with integral formal parameter $z = (z_1, z_2)$. By Lemma E, the formal logarithm $L$ and its inverse Ex are mutually inverse bijections of $(3\mathbb{Z}_3)^2$ that preserve valuations. Moreover, $L([m]Q) = mL(Q)$ ($m \in \mathbb{Z}_3$), and $\partial^\alpha \mathrm{Ex}(0) \in \mathbb{Z}_3^2$ for every multi-index $\alpha$. The Kummer map also extends over $\mathbb{Z}_3$ ([BS10]). So, if $B \in J_H(\mathbb{Q})$ and $k_j$ is a 3-adic unit in the primitive integer coordinates of $\kappa(B)$, then on the disk $B + J_1$ the function $Q \mapsto (k_i/k_j)(\kappa(B + Q))$ is a power series in $z(Q)$ with coefficients in $\mathbb{Z}_3$. This is because translation by $B$ is an automorphism of the abelian scheme over $\mathbb{Z}_3$. The next two lemmas hold for any odd prime $p$ and any abelian scheme of dimension $g$ over $\mathbb{Z}_p$. We use the same symbols $z = (z_1, \ldots, z_g)$, $J_1$, $\hat{F}$, $L$, Ex.

**Lemma 6.5.6** (Formal translation). *Let $S \in J_1(\mathbb{Q}_p)$, $\mathcal{F} \in \mathbb{Z}_p[[z]]$, and $f(m) = \mathcal{F}(z([m]S))$ ($m \in \mathbb{Z}_p$). Put $a_j = \sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} f(k)$. Then $v_p(a_j) \geq j$, and $f(m) = \sum_{j \geq 0} a_j \binom{m}{j}$ for all $m \in \mathbb{Z}_p$.*

*Proof.* We have $z_S = z(S) \in (p\mathbb{Z}_p)^g$. In the formal group law $\hat{F}(z,w)$, all terms other than $z$ have $w$ as a factor, so $\hat{F}(z,z_S) = z + p\,h(z)$ with $h \in \mathbb{Z}_p[[z]]^g$. For $\mathcal{G} \in \mathbb{Z}_p[[z]]$ put $\tau\mathcal{G}(z) = \mathcal{G}(\hat{F}(z,z_S))$. In the Taylor expansion

$$\tau\mathcal{G} - \mathcal{G} = \sum_{\beta \neq 0} \frac{\partial^\beta \mathcal{G}}{\beta!}(z)\, p^{|\beta|} h(z)^\beta$$

we have $\partial^\beta \mathcal{G}/\beta! \in \mathbb{Z}_p[[z]]$, so $\tau\mathcal{G} - \mathcal{G} \in p\,\mathbb{Z}_p[[z]]$. Iterating gives $(\tau-1)^j\mathcal{F} \in p^j\mathbb{Z}_p[[z]]$. Since $z([k]S) = \hat{F}(z([k-1]S), z_S)$, we have $(\tau^k\mathcal{F})(0) = f(k)$, and hence $a_j = ((\tau-1)^j\mathcal{F})(0) \in p^j\mathbb{Z}_p$. The series $\sum a_j\binom{m}{j}$ converges in $\mathbb{Z}_p$ and equals $f(m)$ for $m \in \mathbb{Z}_{\geq 0}$ (Newton's forward difference formula). Both sides are continuous in $m$ ($[p^k]S \to 0$), so they agree on all of $\mathbb{Z}_p$. □

**Lemma 6.5.7** (Logarithmic coordinates)**.** *Suppose $\kappa \in \mathbb{Z}_p[[z]]$ satisfies $\kappa(0) = 0$ and $\kappa \circ [-1] = \kappa$. Then $\kappa(\mathrm{Ex}(\ell)) = \sum_{n\geq 2,\ n\ \mathrm{even}} \kappa_n(\ell)$, where $\kappa_n$ is homogeneous of degree $n$ and its coefficients have valuation at least $-(n-1)/(p-1)$. Hence, if $Q \in J_1(\mathbb{Q}_p)$, $\ell_Q = L(z(Q))$, $m \in \mathbb{Z}_p$ and $e = v_p(m)$, then*

$$\kappa([m]Q) = m^2\kappa_2(\ell_Q) + \varepsilon, \qquad v_p(\varepsilon) \geq 4(e+1) - \frac{3}{p-1}.$$

*Proof.* Since $L \circ [-1] = -L$, we have $\mathrm{Ex}(-\ell) = [-1]\mathrm{Ex}(\ell)$, so $\kappa \circ \mathrm{Ex}$ is an even function. Since $\kappa(0) = 0$, it has no constant term. By the chain rule and $\partial^\alpha \mathrm{Ex}(0) \in \mathbb{Z}_p^g$, we have $\partial^\alpha(\kappa \circ \mathrm{Ex})(0) \in \mathbb{Z}_p$. Therefore the coefficient of $\ell^\alpha$ lies in $\mathbb{Z}_p/\alpha!$, and $v_p(\alpha!) \leq (|\alpha|-1)/(p-1)$. Since $v_p(\ell_Q) \geq 1$, the valuation of $L([m]Q) = m\ell_Q$ is at least $e+1$, and $z([m]Q) = \mathrm{Ex}(m\ell_Q)$. The term of degree $n$, $m^n\kappa_n(\ell_Q)$, has valuation at least $n(e+1) - (n-1)/(p-1)$. This bound increases with $n$, so all terms with $n \geq 4$ have valuation at least $4(e+1) - 3/(p-1)$. □

Now we use $\kappa_i = k_i/k_4$ ($i = 1,2,3$) on the disk of the origin. These functions are $[-1]$-invariant, vanish at the origin, and lie in $\mathbb{Z}_3[[z]]$.

**Lemma 6.5.8.** *If $m \in \mathbb{Z}$ and $\Phi_1(\kappa([m]S)) = 0$, then $m = 0$.*

*Proof.* Put $f(m) = \Phi_1(\kappa_1, \kappa_2, \kappa_3, 1)([m]S)$. Since $\Phi_1$ has integer coefficients, Lemma 6.5.6 applies.

The case $3 \nmid m$. By certificate 1.3.5d, the Mahler coefficients are $a_0 = 0$, $v_3(a_1) = v_3(a_2) = 5$, $v_3(a_3) = 7$, $v_3(a_4) = 8$, $v_3(a_5) = 7$, with $a_1/3^5 \equiv 1$ and $a_2/3^5 \equiv 2 \pmod 3$. For $j \geq 6$, $v_3(a_j) \geq j \geq 6$. Hence

$$3^{-5}f(m) \equiv \binom{m}{1} + 2\binom{m}{2} = m^2 \pmod 3,$$

and $f(m) \neq 0$ if $3 \nmid m$.

The case $m = 3^e a$, $e \geq 1$, $3 \nmid a$. We apply Lemma 6.5.7 with $p = 3$ to the $\kappa_i$, and write $\kappa_{i,2}$ for the quadratic part of $\kappa_i \circ \mathrm{Ex}$. The error has valuation at least $4e + \frac{5}{2}$, and hence, since valuations are integers, at least $4e+3$. By certificate 1.3.5d, the valuations of $\kappa_1(3S), \kappa_2(3S), \kappa_3(3S)$ are $6, 5, 4$, and dividing them by $3^6, 3^5, 3^4$, respectively, gives 1 modulo 3. For $m = 3$ the error is a multiple of $3^7$, so $v_3(\kappa_{i,2}(\ell_S)) = 4, 3, 2$ ($i = 1,2,3$), and the normalized residues are all 1. For general $e \geq 1$ we have $\kappa_i([m]S) = 3^{2e}a^2\kappa_{i,2}(\ell_S) + O(3^{4e+3})$, and since $4e+3 > 2e+4$,

$$v_3(\kappa_1) = 2e+4, \quad v_3(\kappa_2) = 2e+3, \quad v_3(\kappa_3) = 2e+2,$$

with normalized residues $a^2 \equiv 1$. The numbers $512 = 2^9$, $992 = 2^5 \cdot 31$, $248 = 2^3 \cdot 31$ are 3-adic units. In the quadratic part of $\Phi_1$, the valuation of $512\kappa_2\kappa_3$ is exactly $4e+5$, those of $992\kappa_1\kappa_3$ and $248\kappa_2^2$ are $4e+6$, and that of $512\kappa_1\kappa_2$ is $4e+7$. The terms of degree 3 and higher have valuation at least $3(2e+2) > 4e+5$. Hence $v_3(f(m)) = 4e+5$ and $f(m) \neq 0$. □

**Lemma 6.5.9.** *If $m \in \mathbb{Z}$ and $\Phi_1(\kappa(4G + [m]S)) = 0$, then $m = 0$.*

*Proof.* In $\kappa(4G) = (32 : 16 : -12 : 73)$ the coordinate 32 is a 3-adic unit, so we use the chart $k_1 = 1$ on the whole disk $4G + J_1$. Then Lemma 6.5.6 applies to $h(m) = \Phi_1(1, k_2/k_1, k_3/k_1, k_4/k_1)(\kappa(4G + [m]S))$. By certificate 1.3.5d, the Mahler coefficients satisfy

$$a_0 = 0, \qquad 3^{-2}a_1 \equiv 2, \qquad 3^{-2}a_2 \equiv 2, \qquad 3^{-3}a_3 \equiv 1 \pmod 3,$$

and $v_3(a_j) \geq j$ for $j \geq 3$. The Mahler coefficients $b_j = a_j/9$ of $g = h/9$ satisfy $b_1 \equiv b_2 \equiv 2 \pmod 3$ and $v_3(b_j) \geq j - 2$ $(j \geq 3)$.

(a) Modulo 3, $g(m) \equiv 2\binom{m}{1} + 2\binom{m}{2} = m(m+1)$, so $g(m) \neq 0$ if $m \equiv 1 \pmod 3$.

(b) Suppose $m \equiv 2 \pmod 3$. Choose $r \in \{2, 5, 8\}$ with $r \equiv m \pmod 9$. By certificate 1.3.5d, $v_3(h(r)) = 3$, that is, $v_3(g(r)) = 1$. By the Vandermonde identity,

$$g(m) - g(r) = \sum_{j \geq 1} b_j \sum_{i=1}^{j} \binom{m-r}{i}\binom{r}{j-i},$$

and $v_3\binom{m-r}{i} \geq 2 - v_3(i)$. If $j \leq 2$, then $v_3(i) = 0$, and if $j \geq 3$, then $v_3(b_j) \geq j - 2 \geq v_3(i)$. Hence $g(m) \equiv g(r) \not\equiv 0 \pmod 9$.

(c) Suppose $m \equiv 0 \pmod 3$, $m \neq 0$, and $e = v_3(m)$. Then

$$\frac{h(m)}{9m} = \frac{a_1}{9} + \frac{a_2}{9} \cdot \frac{m-1}{2} + \frac{a_3}{27} \cdot \frac{(m-1)(m-2)}{2} + \frac{1}{9m} \sum_{j \geq 4} a_j \binom{m}{j}.$$

Since $\binom{m}{j} = \frac{m}{j}\binom{m-1}{j-1}$, for $j \geq 4$ we have $v_3(a_j\binom{m}{j}) \geq j + e - v_3(j) \geq e + 3$, so the tail is 0 modulo 3. If $m \equiv 0$, then $(m-1)/2 \equiv 1$ and $(m-1)(m-2)/2 \equiv 1 \pmod 3$, so $h(m)/(9m) \equiv 2 + 2 + 1 \equiv 2 \pmod 3$. Hence $h(m) \neq 0$. □

**Lemma 6.5.10.** *For every $P \in C(\mathbb{Q})$, $\varphi(P) \in \{0,\ 4G,\ -4G\}$.*

*Proof.* Applying Lemma 6.5.3(i) and Lemmas 6.5.8, 6.5.9 to the two cases of Lemma 6.5.5 gives $m = 0$. Hence $\kappa(\varphi(P))$ is $\kappa(0)$ or $\kappa(4G)$, and $\varphi(P) = 0$ or $\pm 4G$. □

**Step 5: the two fibers.**

**Lemma 6.5.11.** *If $P \in C(\mathbb{Q})$, $Y(P) \neq 0$ and $\varphi(P) = \pm 4G$, then $P = (\pm 1 : 1 : 0)$.*

*Proof.* In the chart $Y \neq 0$ of $C$, the only point with $A_2 = B = 0$ is $(R, t) = (0, 0)$, and there $A_0 = -1$ (certificate 1.3.5e). Therefore, by Lemma 6.5.3(ii), $\varphi(P) = [D_P - D_\infty]$, and the $x$-image of $D_P$ is the zero set of $A_2(P)s^2 + B(P)s + A_0(P)$. Since the class $\pm 4G$ is nonzero, by Riemann–Roch there is only one effective divisor in the class $\pm 4G + [D_\infty]$. Since $\kappa(4G) = (32 : 16 : -12 : 73)$, the two $x$-coordinates of that divisor satisfy $x_1 + x_2 = \frac{1}{2}$, $x_1 x_2 = -\frac{3}{8}$. That is, the $x$-image is the zero set of $8s^2 - 4s - 3$, and the same holds for $-4G$. Hence $(A_2 : B : A_0)(P) = (8 : -4 : -3)$, that is,

$$2B + A_2 = 0, \qquad 8A_0 + 3A_2 = 0$$

hold at $(R, t) = (r^2, t)$. The Gröbner basis of the ideal $(R^2 - R + t + t^3,\ 2B + A_2,\ 8A_0 + 3A_2)$ of $\mathbb{Q}[R, t]$ is $\{R - 1,\ t\}$ (certificate 1.3.5e). Therefore $R = 1$, $t = 0$, $r = \pm 1$, and $P = (\pm 1 : 1 : 0)$. □

**Lemma 6.5.12.** *If $P \in C(\mathbb{Q})$ and $\varphi(P) = 0$, then $X(P) = 0$.*

*Proof.* Suppose $X(P) \neq 0$. By Lemma 6.5.3(iii), $2P \sim 2\iota(P)$. On the other hand, $P \neq \iota(P)$, because the only fixed points of $\iota$ are the line $X = 0$ and $(1 : 0 : 0) \notin C$. This contradicts [Har77, Section IV.5]. □

*Proof of Proposition 6.5.2.* Let $P \in C(\mathbb{Q})$. If $X(P) \neq 0$, then $Y(P) \neq 0$, and by Lemma 6.5.12, $\varphi(P) \neq 0$. By Lemma 6.5.10, $\varphi(P) = \pm 4G$, and by Lemma 6.5.11, $P = (\pm 1 : 1 : 0)$. If $X(P) = 0$, then $YZ(Y^2 + Z^2) = 0$, so $P = (0 : 0 : 1)$ or $(0 : 1 : 0)$. All four points lie on $C$. □

## 6.6 $x^4 + x^2y^2 + y^3z + z^4 = 0$ $(H = 64)$

**Theorem 6.6.1.** *The only integer solutions of $x^4 + x^2y^2 + y^3z + z^4 = 0$ are $(0, n, 0)$ and $(0, n, -n)$ $(n \in \mathbb{Z})$.*

**Setup.** The projective plane quartic curve

$$C: \quad F(X, Y, Z) = X^4 + X^2Y^2 + Y^3Z + Z^4 = 0$$

has good reduction at $5, 7, 11, 13, 47$ (certificate 1.3.6a). Hence it is smooth over $\mathbb{Q}$, has genus 3, and by [Har77, Section IV.5] is not hyperelliptic. Theorem 6.6.1 is equivalent to the following proposition.

**Proposition 6.6.2.** $C(\mathbb{Q}) = \{(0:1:0), (0:1:-1)\}$.

*Involution and Prym model.* The quotient curve $E = C/\iota$ by $\iota(X:Y:Z) = (-X:Y:Z)$ is $w^2 = Y^4 - 4Y^3Z - 4Z^4$, and it is isomorphic to the elliptic curve $y^2 = x^3 + 16x - 64$ (conductor 248). Let $P_C = \mathrm{im}(1 - \iota_*) \subset J_C$ be the Prym variety of the cover $C \to E$. $C$ has the form $X^4 - hX^2 + fg = 0$ with $f = Z(Y + Z)$, $h = -Y^2$, $g = Y^2 - YZ + Z^2$. Applying the construction of [Bru08, RR18], we obtain three quadratic forms in $(a, b, c)$

$$q_1 = -(b^2 + ac), \qquad q_2 = \tfrac{1}{2}(ab - b^2 - ac - bc), \qquad q_3 = \tfrac{1}{2}(ab + b^2 + ac + bc)$$

and the curve $D:\ q_1 = u^2,\ q_2 = uv,\ q_3 = v^2$ $(\subset \mathbf{P}^4)$. The map

$$\pi:\ C \to D, \qquad (X:Y:Z) \mapsto (a:b:c:u:v) = \big(Z(Y+Z) : X^2 : Y^2 - YZ + Z^2 : XY : XZ\big)$$

satisfies $q_1 - u^2 = -F$, $q_2 - uv = -\frac{1}{2}F$, $q_3 - v^2 = \frac{1}{2}F$, so it maps to $D$. On $X \neq 0$, $\pi$ is an isomorphism onto its image, and the image lies in the smooth part $U$ of $D$ ($b = X^2 \neq 0$; [Bru08, RR18]). With $N_i$ the $3 \times 3$ symmetric matrix of $q_i$, the genus 2 curve is

$$\begin{aligned} H: \quad y^2 &= -16 \det(N_1 - 2sN_2 + s^2N_3) \\ &= 2s^5 + 6s^4 - 4s^3 - 10s^2 + 12s - 4 \\ &= 2(s^2 + 2s - 2)(s^3 + s^2 - 2s + 1). \end{aligned}$$

(certificate 1.3.6a). The Ritzenthaler–Romagny model $y^2 = -\frac{1}{2}(s^2 - 2s - 2)(s^3 - s^2 - 2s - 1)$ of [Bru08, RR18] becomes $H$ under $s \mapsto -s$, $y \mapsto y/2$. The prime factors of the discriminant of $H$ are 2, 3, 31. $H$ has one point at infinity $\infty$, and we put $D_\infty = 2\infty$. certificate 1.3.6a also checks $L_p(C, T) = L_p(E, T)\, L_p(H, T)$ at $p = 5, 7, 11, 13, 47$. The tangent quadratic is defined as in Section 6.5, using the $5 \times 5$ symmetric matrices $M_i$ of the three equations of $D$.

*Kummer surface.* $\kappa : J_H \to K_H \subset \mathbf{P}^3$ is the Kummer map in Cassels–Flynn coordinates $(k_1 : k_2 : k_3 : k_4)$, and $\kappa(0) = (0:0:0:1)$. $\Phi_1, \Phi_2 \in \mathbb{Z}[k_1, \dots, k_4]$ are the two primitive quartic forms printed by certificate 1.3.6a (28 terms each). In the chart $k_4 = 1$, neither has a constant or linear term, and their quadratic parts are

$$Q_1 = 48k_1^2 - 4k_1k_3 + k_2^2 + 24k_2k_3, \qquad Q_2 = -48k_1^2 + 240k_1k_3 - 60k_2^2 - 24k_2k_3$$

(certificate 1.3.6a).

The proof goes as in Section 6.5. We construct a map $\varphi : C \to J_H$, determine $J_H(\mathbb{Q})$, show $\varphi(C(\mathbb{Q})) = \{0\}$ by a sieve modulo 47 and 47-adic analysis, and then determine the zero fiber.

### Step 1: the map $\varphi$.

**Lemma 6.6.3.** *There is a map $\varphi : C \to J_H$ defined over $\mathbb{Q}$ such that the following hold.*

*(i) For all $P \in C$, $\Phi_1(\kappa(\varphi(P))) = \Phi_2(\kappa(\varphi(P))) = 0$.*

*(ii) If $X(P) \neq 0$ and $\varphi(P) = 0$, then $2[P - \iota(P)] = 0$.*

*Proof.* Over the function field $\mathbb{Q}(C)$, certificate 1.3.6a checks the following. At the image $\pi(X:Y:Z)$ of the generic point, the tangent quadratic has degree 2 and is irreducible. There are exactly two points $\pm\varphi_{\mathrm{gen}}$ of $J_H(\mathbb{Q}(C))$ whose Mumford polynomial is its monic version, and their common Kummer point satisfies $\Phi_1 = \Phi_2 = 0$. The rest is as in the proof of Lemma 6.5.3. $\varphi_{\mathrm{gen}}$ extends to a morphism $\varphi : C \to J_H$, and (i) holds because a closed condition holds at the generic point. (ii) follows from [Bru08, RR18]. On the smooth part of $D$, the map given by the tangent construction is $\lambda \circ d$, where $d(Q) = [2\iota(Q) - 2Q]$ is the map to the Prym scheme $P'$ and $\lambda : P' \to J_H$ is an isomorphism. Therefore $\varphi = \pm\lambda \circ d \circ \pi$ on $\{X \neq 0\}$. The isogeny $\nu : P' \to P_C$ given by the normalization sends $d(\pi(P))$ to $2[\iota(P) - P]$. □

**Step 2:** $J_H(\mathbb{Q})$.

**Lemma 6.6.4.** *$J_H(\mathbb{Q}) = \langle T\rangle \oplus \langle G\rangle \simeq \mathbb{Z}/2 \oplus \mathbb{Z}$, where, in Mumford representation,*

$$T = (s^2 + 2s - 2,\ 0) = [(\alpha, 0) + (\bar{\alpha}, 0) - 2\infty], \qquad G = (s + \tfrac{5}{2},\ -\tfrac{9}{4}) = [(-\tfrac{5}{2}, -\tfrac{9}{4}) - \infty],$$

*and $\alpha, \bar{\alpha}$ are the two roots of $s^2 + 2s - 2$.*

*Proof.* certificate 1.3.6a computes this with Magma. The rank upper bound from 2-descent ([Sto01, PS97, PS99]) is 1, and $G$ has infinite order, so the rank is 1. The torsion subgroup is $\langle T\rangle \simeq \mathbb{Z}/2$. `MordellWeilGroupGenus2` proves, using bounds for the canonical height ([CF96, Sto99, Sto02]), that $\langle T, G\rangle$ is all of $J_H(\mathbb{Q})$, and both proof flags are true. □

**Step 3: sieve modulo 47.** $H$ and $C$ have good reduction at 47. In $J_H(\mathbb{F}_{47})$, $\bar{T}$ has order 2 and $\bar{G}$ has order 28. Put $R = 28G$; then $R$ lies in the kernel $J_1$ of reduction modulo 47.

**Lemma 6.6.5.** *For every $P \in C(\mathbb{Q})$ there is $m \in \mathbb{Z}$ such that $\varphi(P) = [m]R$.*

*Proof.* Write $\varphi(P) = eT + nG$ ($e \in \{0,1\}$, $n \in \mathbb{Z}$). By Lemma 6.6.3(i), the primitive integer coordinates of $\kappa(\varphi(P))$ satisfy $\Phi_1 = \Phi_2 = 0$, and reduction modulo 47 commutes with the Kummer map ([BS10]). Among the 56 classes $e\bar{T} + n\bar{G}$ ($e \in \{0,1\}$, $0 \le n < 28$) of $J_H(\mathbb{F}_{47})$, the only one whose Kummer point satisfies $\Phi_1 = \Phi_2 = 0$ modulo 47 is $(e, n) = (0, 0)$ (certificate 1.3.6a). Hence $e = 0$ and $28 \mid n$. □

**Step 4: 47-adic analysis.** $J_H$ extends to an abelian scheme over $\mathbb{Z}_{47}$, and $\kappa_i = k_i/k_4$ ($i = 1, 2, 3$) are power series with coefficients in $\mathbb{Z}_{47}$ in the integral formal parameters on the disk $J_1$ of the origin ([BS10]). These functions are $[-1]$-invariant and vanish at the origin. By certificate 1.3.6a, the 47-adic valuations of the primitive integer coordinates of $\kappa(R)$ are $(2, 2, 2, 0)$, and

$$\kappa_i(R)/47^2 \equiv (24,\ 7,\ 1)_i \pmod{47}, \qquad Q_1(24,7,1) \equiv 39, \quad Q_2(24,7,1) \equiv 8 \pmod{47}.$$

**Lemma 6.6.6.** *If $m \in \mathbb{Z}$ and $m \neq 0$, then $\Phi_1(\kappa([m]R)) \neq 0$. More precisely, $v_{47}\big(\Phi_1(\kappa_1, \kappa_2, \kappa_3, 1)([m]R)\big) = 4v_{47}(m) + 4$.*

*Proof.* We apply Lemma 6.5.7 with $p = 47$ to the $\kappa_i$, and let $\kappa_{i,2}$ be the quadratic part of $\kappa_i \circ \mathrm{Ex}$. Writing $e = v_{47}(m)$ and $m = 47^e u$, the error has valuation at least $4(e+1) - \frac{3}{46}$, that is, at least $4e + 4$. For $m = 1$ we have $\kappa_i(R) = \kappa_{i,2}(\ell_R) + O(47^4)$, so $\kappa_{i,2}(\ell_R) = 47^2(d_i + O(47^2))$ with $(d_1, d_2, d_3) \equiv (24, 7, 1) \pmod{47}$. For general $m$,

$$\kappa_i([m]R) = m^2\kappa_{i,2}(\ell_R) + O(47^{4e+4}) = 47^{2e+2}\big(u^2 d_i + O(47)\big).$$

Since $\Phi_1$ has integer coefficients,

$$\Phi_1(\kappa_1, \kappa_2, \kappa_3, 1)([m]R) = 47^{4e+4}\big(u^4 Q_1(d) + O(47)\big) + O(47^{6e+6}).$$

Since $Q_1(d) \equiv 39 \not\equiv 0 \pmod{47}$ and $6e + 6 > 4e + 4$, the valuation is exactly $4e + 4$. □

**Step 5: the zero fiber.**

**Lemma 6.6.7.** *For every $P \in C(\mathbb{Q})$, $X(P) = 0$.*

*Proof.* By Lemma 6.6.5, $\varphi(P) = [m]R$, and by Lemma 6.6.3(i) and Lemma 6.6.6, $m = 0$, that is, $\varphi(P) = 0$. Suppose $X(P) \neq 0$. By Lemma 6.6.3(ii), $2P \sim 2\iota(P)$. The only fixed points of $\iota$ are the line $X = 0$ and $(1 : 0 : 0) \notin C$, so $P \neq \iota(P)$, and this contradicts [Har77, Section IV.5]. □

*Proof of Proposition 6.6.2.* By Lemma 6.6.7, $X = 0$. Substituting gives

$$Y^3Z + Z^4 = Z(Y + Z)(Y^2 - YZ + Z^2) = 0.$$

Since $Y^2 - YZ + Z^2$ has discriminant $-3$, it has no rational root with $(Y, Z) \neq (0, 0)$. The remaining points are $(0 : 1 : 0)$ and $(0 : 1 : -1)$, and both lie on $C$. □

## 6.7 $x^3z + y^3x + y^2z^2 - z^3y = 0$ $(H = 64)$

**Theorem 6.7.1.** *The only integer solutions of $x^3z + y^3x + y^2z^2 - z^3y = 0$ are $(n, 0, 0)$, $(0, n, 0)$, $(0, 0, n)$, $(0, n, n)$ $(n \in \mathbb{Z})$.*

**Setup.** Let $C \subset \mathbb{P}^2$ be the curve defined by the equation in the theorem, and put $J = \mathrm{Jac}(C)$. Denote the following rational points by

$$P_1 = (1 : 0 : 0), \quad P_2 = (0 : 1 : 0), \quad P_3 = (0 : 0 : 1), \quad P_4 = (0 : 1 : 1),$$

and set $G = [P_3 - P_1]$. Write $F = x^3z + y^3x + y^2z^2 - z^3y$. The proof runs as follows. $C$ is a smooth plane quartic with bad primes $2, 11, 41269$, $J(\mathbb{Q})$ is torsion-free and $G$ has infinite order (Step 1). The 28 bitangents of $C$ are conjugate; their field of definition $K$ has degree 28, and their Galois group is $\mathrm{Sp}_6(\mathbb{F}_2)$ (Step 2). The descent map of Proposition I by the bitangents is then injective, with image in $K(2, S)$ modulo $\mathbb{Q}^\times$ (Step 3). The class number of $K$ is odd, proved without GRH with Proposition B (Step 4), so $K(2, S)$ is spanned by 29 explicit $S$-units (Step 5). The local conditions at 2 and 11 cut the image down to dimension 1, so $\mathrm{rank}\, J(\mathbb{Q}) = 1$ (Step 6), and Chabauty–Coleman at $p = 3$ shows that each of the four residue disks of $C(\mathbb{F}_3)$ contains only one rational point (Step 7). Proposition A does not apply here: no bitangent of $C$ is rational, so $C$ has no rational hyperflex.

**Step 1: the curve.**

**Lemma 6.7.2.** *$C$ is smooth over $\mathbb{Q}$, so it has genus 3. The plane model $\mathcal{C} = \{F = 0\} \subset \mathbb{P}^2_{\mathbb{Z}}$ is smooth over $\mathbb{Z}_p$ for every prime $p \notin \{2, 11, 41269\}$. For $p \in \{2, 11, 41269\}$ the reduction has exactly one singular point over $\overline{\mathbb{F}}_p$; it is $\mathbb{F}_p$-rational and an ordinary double point, and $v_p(F) = 1$ at an integral lift (certificate 1.3.7a):*

| $p$ | *node* | *type* |
|---|---|---|
| 2 | $(1 : 1 : 1)$ | *split* |
| 11 | $(1 : 1 : 7)$ | *non-split* |
| 41269 | $(1 : 12101 : 2748)$ | *split* |

*For $p = 11, 41269$ the model $\mathcal{C}_{\mathbb{Z}_p}$ is regular with geometrically irreducible special fibre, and the Tamagawa number $c_p(J)$ is 1; at every prime $p \notin \{2, 11, 41269\}$ also $c_p(J) = 1$.*

*Proof.* In each of the three affine charts let $R_1, R_2, R_3$ be the resultants, with respect to one variable, of the pairs $(f, f_x)$, $(f, f_y)$, $(f_x, f_y)$ of the dehomogenized polynomial and its partial derivatives, and take the three pairwise resultants of the $R_i$ with respect to the other variable. In each chart some of these integers are 0 (in the charts $z = 1$ and $x = 1$, $R_1$ and $R_2$ have the common factor $x$, resp. $y^2$), but their greatest common divisor is $2 \cdot 11 \cdot 41269$. A singular point over $\overline{\mathbb{F}}_p$ in some chart makes $p$ divide all three integers of that chart, and a singular point over $\overline{\mathbb{Q}}$ would make them all 0. At $p = 2, 11, 41269$

the singular points were found from the gcds of $f, f_x, f_y$; there is one, with nonzero discriminant of the quadratic part (certificate 1.3.7a). At $p = 11, 41269$, the linear part of $F$ at an integral lift of the node vanishes modulo $p$ and $F(\text{lift}) \notin p^2\mathbb{Z}_p$, so $F \notin \mathfrak{m}^2$ and the model is regular there. The special fibre is reduced, and it is geometrically irreducible: two components $C', C''$ would meet only at the node, with $i(C', C'') = \deg C' \deg C'' \geq 3$ by Bézout, whereas each contains exactly one of the two branches there, which meet with multiplicity 1. By Raynaud's theorem [BLR90, 9.6, Theorem 1] the component group of the Néron model is trivial. □

**Lemma 6.7.3.** *(1) The points of $C$ with $xyz = 0$ are $P_1, \dots, P_4$: $F(0,y,z) = yz^2(y-z)$, $F(x,0,z) = x^3z$, $F(x,y,0) = xy^3$. (2)* $\operatorname{div}(z) = 3P_1 + P_2$, $\operatorname{div}(y) = P_1 + 3P_3$, $\operatorname{div}(x) = 2P_2 + P_3 + P_4$. *Hence $[P_2 - P_1] = 3G$ and $[P_4 - P_1] = -4G$. (3) The numbers $N_k = \#C(\mathbb{F}_{p^k})$, the L-polynomials and $\#J(\mathbb{F}_p) = L_p(1)$ are (certificate 1.3.7a)*

| $p$ | $(N_1, N_2, N_3)$ | $L_p(T)$ | $\#J(\mathbb{F}_p)$ |
|---|---|---|---|
| 3 | $(4, 10, 37)$ | $1 + 3T^3 + 27T^6$ | 31 |
| 5 | $(6, 26, 171)$ | $1 + 15T^3 + 125T^6$ | $141 = 3 \cdot 47$ |
| 7 | $(10, 66, 313)$ | $1 + 2T + 10T^2 + 7T^3 + 70T^4 + 98T^5 + 343T^6$ | $531 = 3^2 \cdot 59$ |
| 17 | $(30, 308, 4884)$ | $1 + 12T + 81T^2 + 386T^3 + 1377T^4 + 3468T^5 + 4913T^6$ | $10238 = 2 \cdot 5119$ |

*(4)* $J(\mathbb{Q})_{\text{tors}} = 0$, *and $G$ has infinite order.*

*Proof.* (2) $\operatorname{div}(z/y) = 2P_1 + P_2 - 3P_3$ and $\operatorname{div}(x/y) = 2P_2 + P_4 - P_1 - 2P_3$. (3) With $s_k = p^k + 1 - N_k$, $L_p(T) = 1 + a_1T + a_2T^2 + a_3T^3 + pa_2T^4 + p^2a_1T^5 + p^3T^6$ with $a_1 = -s_1$, $a_2 = (s_1^2 - s_2)/2$, $a_3 = -(s_1^3 - 3s_1s_2 + 2s_3)/6$. (4) Since $\gcd(141, 10238) = 1$, [Kat81, Appendix] gives $J(\mathbb{Q})_{\text{tors}} = 0$. Since $P_3 \neq P_1$ and the genus is positive, $G \neq 0$, so $G$ has infinite order. □

**Step 2: the bitangents and the field $K$.** Let

$$\begin{aligned} B(m) &= m^{28} - 208m^{26} - 1024m^{25} + 9344m^{24} - 33792m^{22} - 83636m^{21} + 32256m^{20} + 131816m^{19} \\ &\quad - 44352m^{17} - 23872m^{15} + 87462m^{14} + 28512m^{12} + 5968m^{10} - 3828m^7 - 504m^5 + 1, \\ g(w) &= w^{28} - 288w^{21} - 1028w^{19} - 1440w^{17} - 960w^{15} - 346w^{14} - 256w^{13} - 748w^{12} \\ &\quad - 528w^{10} - 128w^8 - 56w^7 - 68w^5 - 16w^3 + 1, \end{aligned}$$

and $K = \mathbb{Q}(w)$ with $g(w) = 0$. Put $n = -1/w^2$, and let $a \in K$ be the degree-27 polynomial in $w$ recorded in `data/a.txt` of certificate 1.3.7b.

**Lemma 6.7.4.** *The following hold (certificate 1.3.7b).*

*(1) The line $y = mx + nz$ is a bitangent of $C$ only if $B(m) = 0$. $B$ is irreducible over $\mathbb{Q}$ and squarefree.*

*(2) $B(a) = 0$, so $K = \mathbb{Q}(a)$, and $F(x, ax + nz, z) = a^3(x^2 + uxz + vz^2)^2$ for some $u, v \in K$. So $\ell = y - ax - nz$ defines a bitangent, and its 28 conjugates are the 28 bitangents of $C$.*

*(3) The maximal order of $K$ is certified without GRH; $d_K = 2^{42} \cdot 11^6 \cdot 41269^6$, and $K$ has signature $(4, 12)$. $a$ is a unit, and $-n = w^{-2}$ is a square.*

*(4) The prime ideals of $K$ above 2, 11, 41269 have $(e, f)$*

$$2: \ (4,1), (2,3), (2,3), (4,3); \qquad 11: \ (1,1), (1,3), (1,6), (1,6), (2,6);$$
$$41269: \ (2,2), (2,4), (1,8), (1,8).$$

*Let $S$ be the set of these 13 prime ideals.*

*Proof.* Substituting $y = mx + nz$ gives $F(x, mx + nz, z) = \sum_k c_k x^k z^{4-k}$ with $c_4 = m^3$, $c_3 = 1 + 3m^2n$, $c_2 = m^2 + 3mn^2$, $c_1 = n^3 + (2n-1)m$, $c_0 = n^2 - n$. This is $c_4(x^2 + uxz + vz^2)^2$ if and only if $u = c_3/(2c_4)$, $v = (4c_2c_4 - c_3^2)/(8c_4^2)$, $8c_1c_4^2 = c_3(4c_2c_4 - c_3^2)$ and $64c_0c_4^3 = (4c_2c_4 - c_3^2)^2$, and the resultant of the last two with respect to $n$ is $m^{24}B(m)$ up to a constant. For $m = 0$ the line $y = nz$ meets $C$ in $z(x^3 + n^3xz^2 + (n^2 - n)z^3)$, which vanishes to odd order at $P_1$. The rest is exact arithmetic in $K$; the 28 conjugates of $(a, n)$ have distinct slopes, and a smooth plane quartic has exactly 28 bitangents. □

**Lemma 6.7.5.** *The Galois group of $B$ is $\mathrm{Sp}_6(\mathbb{F}_2)$. In particular, $K$ has no quadratic subfield.*

*Proof.* By Proposition I(1) the Galois group $\Gamma$ of $B$ is a subgroup of $\mathrm{Sp}_6(\mathbb{F}_2)$. $B$ is squarefree modulo 13, 29 and 3, with factors of degrees $(3,5,5,15)$, $(7,7,7,7)$ and $(1,9,9,9)$ (certificate 1.3.7b), so $\Gamma$ contains elements of orders 15, 7 and 9. The maximal subgroups of $\mathrm{Sp}_6(\mathbb{F}_2)$ are $U_4(2)$:2, $S_8$, $2^5$:$S_6$, $U_3(3)$:2, $2^6$:$L_3(2)$, 2.$[2^6]$:$(S_3 \times S_3)$, $S_3 \times S_6$ and $L_2(8)$:3 [CCN+85, p. 46], of orders $2^7 3^4 5$, $2^7 3^2 5 \cdot 7$, $2^9 3^2 5$, $2^6 3^3 7$, $2^9 3 \cdot 7$, $2^9 3^2$, $2^5 3^3 5$, $2^3 3^3 7$. Only $S_8$ has order divisible by $5 \cdot 7$, and $S_8$ has no element of order 9. So $\Gamma = \mathrm{Sp}_6(\mathbb{F}_2)$, which is simple; hence it has no subgroup of index 2, and $K$ contains no quadratic field. □

**Step 3: the descent map.** We use Proposition I with $\ell = y - ax - nz$. Since $\ell(1,0,0) = -a$, for $P \in C(k)$ not on a bitangent the class $\delta_k([P - P_1])$ is represented by $\ell(\tilde{P})\, a$ for any coordinate vector $\tilde{P}$ of $P$. In particular $\delta(G) = \ell(P_3)/\ell(P_1) = (-n)/(-a) \equiv a$, because $-n$ is a square.

**Lemma 6.7.6.** *Let $V = \mathbb{F}_2^6$ with the standard symplectic form, $\Theta$ the 28 quadratic forms of Arf invariant 1, $\Gamma = \mathrm{Sp}_6(\mathbb{F}_2)$, $M = \mathbb{F}_2^\Theta / \mathbb{F}_2\mathbf{1}$ and $\iota(T) = (q(T))_{q \in \Theta}$. Then for $T \neq 0$ exactly 12 forms satisfy $q(T) = 0$, the 63 sets $\{q : q(T) = 0\}$ are distinct, $\iota$ is injective, $V^\Gamma = 0$ and $(M/\iota V)^\Gamma = 0$ (certificate 1.3.7c). Hence $J(\mathbb{Q})[2] = 0$ and $\delta = \delta_\mathbb{Q}$ is injective.*

*Proof.* The 63 transvections generate a permutation group of order $1451520 = \#\mathrm{Sp}_6(\mathbb{F}_2)$ on $\Theta$, and the space of $m \in \mathbb{F}_2^{28}$ with $\gamma m - m \in \mathbb{F}_2\mathbf{1} + \iota V$ for all 63 generators $\gamma$ has dimension $7 = \dim(\mathbb{F}_2\mathbf{1} + \iota V)$. The conclusion follows from Proposition I(1), (2) and Lemma 6.7.5. □

Since $J(\mathbb{Q})[2] = 0$, injectivity gives $\operatorname{rank} J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \Sigma$ for every subgroup $\Sigma$ containing $\delta(J(\mathbb{Q})/2J(\mathbb{Q}))$.

**Lemma 6.7.7.** *Every class in $\delta(J(\mathbb{Q})/2J(\mathbb{Q}))$ has a representative in*

$$K(2,S) = \{\kappa \in K^\times / K^{\times 2} :\ v_\mathfrak{p}(\kappa) \equiv 0 \pmod 2 \text{ for all prime ideals } \mathfrak{p} \notin S\},$$

*and the image of $K(2,S)$ in $K^\times/K^{\times 2}\mathbb{Q}^\times$ is $K(2,S)/\mathbb{Q}(2,S)$, where $\mathbb{Q}(2,S) = \langle -1, 2, 11, 41269\rangle$ has dimension 4. Moreover, for such a representative, $(v_\mathfrak{p}(\kappa) \bmod 2)_{\mathfrak{p}|11} \in \{0, (1,1,1,1,0)\}$ and $(v_\mathfrak{p}(\kappa) \bmod 2)_{\mathfrak{p}|41269} \in \{0, (0,0,1,1)\}$.*

*Proof.* At $p \notin \{2, 11, 41269\}$, $K/\mathbb{Q}$ is unramified and $c_p = 1$, so by Proposition I(3) all $v_\mathfrak{p}(\kappa)$, $\mathfrak{p} \mid p$, have the same parity; multiplying $\kappa$ by suitable powers of these finitely many $p$ gives a representative in $K(2,S)$. At $p = 11, 41269$, $c_p = 1$ (Lemma 6.7.2), and Proposition I(3) gives the two conditions, with $(e_\mathfrak{p} \bmod 2)$ read off from Lemma 6.7.4(4). If $c \in \mathbb{Q}^\times$ lies in $K(2,S)K^{\times 2}$, then $v_p(c)$ is even for $p \notin \{2, 11, 41269\}$, so $c \in \mathbb{Q}(2,S)\mathbb{Q}^{\times 2}$; and $\mathbb{Q}(2,S) \to K^\times/K^{\times 2}$ is injective because $K$ has no quadratic subfield. □

**Step 4: the class group of $K$.**

**Lemma 6.7.8.** *Every prime ideal of $\mathcal{O}_K$ of norm $< e^{13}$ (that is, of norm $\leq 442413$) is principal. There are 37,155 of them (certificate 1.3.7d).*

*Proof.* The prime ideals were enumerated with `idealprimedec` and independently counted by Dedekind–Kummer from the factorization of $g$ modulo $p$ for $p \nmid [\mathcal{O}_K : \mathbb{Z}[w]] = 2^{24} \cdot 717344179 \cdot 9625055309383932097$; the counts agree. For each prime ideal $\mathfrak{p}$ a generator $g_\mathfrak{p}$ was proposed by `bnfisprincipal` (used only as a proposer), and it was checked exactly that $g_\mathfrak{p} \in \mathcal{O}_K$, $|N(g_\mathfrak{p})| = N\mathfrak{p}$ and $v_\mathfrak{p}(g_\mathfrak{p}) \geq 1$. Then $(g_\mathfrak{p}) \subseteq \mathfrak{p}$ are integral ideals of the same norm, so $(g_\mathfrak{p}) = \mathfrak{p}$; the matching between generators and prime ideals is one-to-one. The check was run twice, with PARI 2.17.4 and with an independent GP script under GP 2.15.4. □

**Lemma 6.7.9.** *The class number of $K$ is odd; in particular $\mathrm{Cl}(K)[2] = 0$.*

*Proof.* Apply Proposition B with $n = 28$, $r_1 = 4$, $D = 2^{42}11^6 41269^6$, $T = 13$, $v$ the indicator function of $[0, T]$ (so $f(x) = (1 - |x|/T)_+$), and $k(q) = a(q)$ for all $q < e^{13}$ (Lemma 6.7.8). Since $1 - f(x) \le x/T$ for $x \ge 0$, $\int_0^\infty (1-f)W \le \frac{1}{T}\int_0^\infty xW(x)\,dx = \frac{\pi^2}{4T} + \frac{2\alpha\log 2}{T}$. Hence $B^-(f) \ge B_0(13)$, where

$$B_0(T) = C_\infty - \frac{\pi^2}{4T} - \frac{2r_1\log 2}{nT} + \frac{4}{n}\sum_{\mathfrak{p},\ m\ge 1:\ N\mathfrak{p}^m < e^T} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m + 1}\Big(1 - \frac{m\log N\mathfrak{p}}{T}\Big).$$

The sum involves 25,333 distinct pairs $(N\mathfrak{p}, m)$, that is, 37,333 pairs $(\mathfrak{p}, m)$. In ball arithmetic (256 bits),

$$C_\infty - \frac{\pi^2}{52} - \frac{2\cdot 4\log 2}{28\cdot 13} = -0.78489255426850599306\ldots,$$
$$B_0(13) = 0.030369049276711976553657615 8681 \pm 1.4\cdot 10^{-32} > 0$$

(certificate 1.3.7d; the GP script of certificate 1.3.7d gives the same value in floating point). □

**Step 5: $S$-units.**

**Lemma 6.7.10.** *Let $u_1, \ldots, u_{15}$ and $\pi_1, \ldots, \pi_{13}$ be the elements recorded in `data/paper_C2.json` of certificate 1.3.7e. Then $-1, u_1, \ldots, u_{15}, \pi_1, \ldots, \pi_{13}$ is an $\mathbb{F}_2$-basis of $K(2,S)$, which has dimension 29.*

*Proof.* Each $u_i$ is integral with norm $\pm 1$, so it is a unit. Each $\pi_j$ is integral, and the ideals $(\pi_1), \ldots, (\pi_{13})$ are the 13 prime ideals of $S$, in the order of Lemma 6.7.4(4) (certificate 1.3.7e). By Dirichlet's $S$-unit theorem, $\mathcal{O}_{K,S}^\times \cong \{\pm 1\} \times \mathbb{Z}^{r_1+r_2-1+\#S} = \{\pm 1\} \times \mathbb{Z}^{28}$ ($K$ has a real place, so its only roots of unity are $\pm 1$), hence $\dim \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2} = 29$. The 29 elements are independent in $K^\times/K^{\times 2}$: their quadratic characters at the 29 degree-one prime ideals $(q, w - r)$ with

$$(q,r) = (3,2), (5,1), (7,5), (19,10), (23,14), (23,16), (37,32), (41,10), (43,11), (47,15),$$
$$(47,18), (59,29), (67,18), (71,20), (79,38), (89,54), (103,29), (103,94), (107,92), (109,5),$$
$$(109,39), (113,76), (131,89), (137,16), (157,84), (157,116), (167,98), (173,9), (181,38)$$

form an invertible $29 \times 29$ matrix over $\mathbb{F}_2$. So they form a basis of $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$. Finally $0 \to \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2} \to K(2,S) \to \mathrm{Cl}(\mathcal{O}_{K,S})[2] \to 0$ is exact, and $\mathrm{Cl}(\mathcal{O}_{K,S})$ is a quotient of $\mathrm{Cl}(K)$, which has odd order (Lemma 6.7.9). □

**Step 6: local images and the rank.**

**Lemma 6.7.11.** $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \le 4$.

*Proof.* By Proposition A(5), $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3 + \dim J(\mathbb{Q}_2)[2]$. The orbits of the image $\Delta$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ on $\Theta$ correspond to the prime ideals above 2, so they have sizes $4, 6, 6, 12$. By Proposition I(1) and Lemma 6.7.6, a nonzero $T \in J[2]$ is fixed by $\Delta$ if and only if the 12-element set $\{\theta : q_\theta(T) = 0\}$ is $\Delta$-stable (these sets determine $T$), that is, a union of orbits: the 12-orbit or the union of the two 6-orbits. So $J(\mathbb{Q}_2)[2] = J[2]^\Delta$ has at most two nonzero elements, hence at most one, and $\dim J(\mathbb{Q}_2)[2] \le 1$. □

To compute in $(K \otimes \mathbb{Q}_2)^\times/(K \otimes \mathbb{Q}_2)^{\times 2} = \prod_{\mathfrak{p}|2} K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ we use, for each $\mathfrak{p} \mid 2$ with ramification index $e$, a uniformizer $\pi_\mathfrak{p}$ and record $v_\mathfrak{p}(x)$ modulo 2, together with the discrete-logarithm coordinates modulo 2 of the unit $x\pi_\mathfrak{p}^{-v_\mathfrak{p}(x)}$ in $(\mathcal{O}_K/\mathfrak{p}^{2e+1})^\times$. This is an isomorphism $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2} \to \mathbb{F}_2^{2+ef}$, because a unit that is a square modulo $\mathfrak{p}^{2e+1}$ is a square (Hensel's lemma). Together they give an isomorphism $\mathrm{loc}_2 : (K \otimes \mathbb{Q}_2)^\times/(\text{squares}) \to \mathbb{F}_2^{36}$, under which the images of $-1, 2, 5$ are independent.

**Lemma 6.7.12.** *Let $Q_1, \dots, Q_4 \in C(\mathbb{Q}_2)$ be the points $(x_0 : y_0 : 1)$ with*

$$\begin{aligned}(x_0, y_0) = (&-40,\ 591131412711573423326720 + O(2^{84})),\\ (&-38,\ 864734735839869549293544 + O(2^{80})),\\ (&-38,\ 273263295199333829574543 + O(2^{81})),\\ (&-36,\ 648823393722996630116800 + O(2^{80})).\end{aligned}$$

*Let $W_2^+ \subseteq \mathbb{F}_2^{36}$ be the span of $\mathrm{loc}_2(\ell(Q_i)a)$ $(i = 1, \dots, 4)$ and of $\mathrm{loc}_2(-1), \mathrm{loc}_2(2), \mathrm{loc}_2(5)$. Then $\dim W_2^+ = 7$, and $W_2^+$ is the full preimage in $\mathbb{F}_2^{36}$ of $\delta_{\mathbb{Q}_2}(J(\mathbb{Q}_2)/2J(\mathbb{Q}_2))$ (certificate 1.3.7f).*

*Proof.* For an integer $x_0$ and $h(Y) = F(x_0, Y, 1)$, an integer $Y$ with $v_2(h(Y)) > 2v_2(h'(Y))$ determines a unique root $y_0 \in \mathbb{Z}_2$ with $v_2(y_0 - Y) \geq N = v_2(h(Y)) - v_2(h'(Y))$. The exact element $(Y - ax_0 - n)a$ is used only when $Ne_{\mathfrak{p}} \geq v_{\mathfrak{p}}((Y - ax_0 - n)a) + 2e_{\mathfrak{p}} + 1$ for every $\mathfrak{p} \mid 2$, so that it has the same square class as $\ell(Q)a$. The seven vectors span a space of dimension 7, and the last three span $\mathrm{loc}_2(\mathbb{Q}_2^\times)$. So the classes $\delta_{\mathbb{Q}_2}([Q_i - P_1])$ span a space of dimension 4 in the image of $\delta_{\mathbb{Q}_2}$, which has dimension at most 4 by Lemma 6.7.11. All 82 points of $C(\mathbb{Q}_2)$ with $x_0 \in [-40, 40]$, and the four displayed points, give the same space. □

Let $\Sigma \subseteq K(2, S)/\mathbb{Q}(2, S)$ consist of the classes $\kappa$ satisfying only

$$(v_{\mathfrak{p}}(\kappa) \bmod 2)_{\mathfrak{p} \mid 11} \in \{0, (1, 1, 1, 1, 0)\}, \qquad \mathrm{loc}_2(\kappa) \in W_2^+.$$

These conditions are independent of the representative modulo $\mathbb{Q}(2, S)$. By Lemmas 6.7.7 and 6.7.12, this space contains $\delta(J(\mathbb{Q})/2J(\mathbb{Q}))$.

**Lemma 6.7.13.** $\dim_{\mathbb{F}_2} \Sigma = 1$, *and $\Sigma$ is spanned by $\delta(G) = [a]$. Hence* $\mathrm{rank}\, J(\mathbb{Q}) = 1$ *and* $J(\mathbb{Q}) \cong \mathbb{Z}$.

*Proof.* In the 29-element basis of Lemma 6.7.10, the two local conditions give an $\mathbb{F}_2$-linear system whose kernel has dimension 5. It contains the four-dimensional space $\mathbb{Q}(2, S)$ and the class of $a$, which is independent of that space (certificate 1.3.7h, the computation using only $p = 2$ and $p = 11$). Thus $\Sigma = \langle [a] \rangle$ has dimension 1. The descent map is injective and $J(\mathbb{Q})$ is torsion-free, so the rank is at most 1; the nonzero class $G$ has infinite order, so the rank is exactly 1. □

**Step 7: Chabauty–Coleman at $p = 3$.** By Lemma 6.7.2, $C$ has good reduction at 3, and $C(\mathbb{F}_3) = \{\bar{P}_1, \bar{P}_2, \bar{P}_3, \bar{P}_4\}$. $\#J(\mathbb{F}_3) = 31$, so $31G$ reduces to 0. Since $J(\mathbb{Q}) \cong \mathbb{Z}$, every element of $J(\mathbb{Q})$ has a nonzero multiple in $\mathbb{Z} \cdot 31G$; so if $\eta$ is a regular differential with $\int_{31G} \eta = 0$, then $\int_{P_i}^{P} \eta = 0$ for all $P \in C(\mathbb{Q})$ ([MP12, Sections 4–5]).

The differential $\Omega = (x\,dy - y\,dx)/F_z = (y\,dz - z\,dy)/F_x = (z\,dx - x\,dz)/F_y$ is well defined on $C$, and $\omega_x = x\Omega$, $\omega_y = y\Omega$, $\omega_z = z\Omega$ form a basis of the regular differentials, regular on the plane model at every good prime. We use the local parameters $t = y/x$ at $P_1$, $t = z/y$ at $P_2$, and $t = x/z$ at $P_3$ and $P_4$. At these points the relevant partial derivative ($F_z$, $F_x$, $F_y$, $F_y$) is $\pm 1$, so the remaining affine coordinate is a power series in $t$ with integer coefficients ($z = -t^3 + \cdots$ at $P_1$, $x = -t^2 + \cdots$ at $P_2$, $y = t^3 + \cdots$ at $P_3$, $y = 1 - t + \cdots$ at $P_4$), and $\Omega = w_\Omega(t)\,dt$ with $w_\Omega$ a unit of $\mathbb{Z}[[t]]$. All series were computed exactly to $O(t^{140})$; after the substitution $t = 3s$ the coefficient of $s^j$ in $\int_0^t \omega$ has valuation at least $j - \log_3 j$.

**Lemma 6.7.14.** *Let $E$ be the effective divisor of degree 3 consisting of the three points $(x : V(x) : 1)$, where $x$ runs over the roots of*

$$80621568x^3 + 19551871x^2 - 576258756x + 551007360, \qquad V(x) = \tfrac{27648}{10517}x^2 + \tfrac{154341055}{30667572}x - \tfrac{31989800}{2555631}.$$

*Then $E \sim P_1 + P_2 + P_3 + 31G$. The three points of $E$ are $\mathbb{Q}_3$-rational and lie in the residue disks of $P_1$, $P_3$, $P_2$, with $v_3(t) = 3, 1, 5$ respectively (certificate 1.3.7i).*

*Proof.* The forms of degree 12 in the 46 monomials not divisible by $xy^3$ (a basis of $\mathbb{Q}[x,y,z]_{12}/(F)$) that vanish to order at least 44 at $P_1$ and at least 1 at $P_3$ form a space of dimension 1; let $\Gamma$ be a generator. The resultant $\mathrm{Res}_y(F(x,y,1),\Gamma(x,y,1))$ is $x$ times the cubic above (up to a constant), and the gcd of $F(x,y,1)$ and $\Gamma(x,y,1)$ over $\mathbb{Q}[x]/(\text{cubic})$ is $y - V(x)$. Since $\deg \operatorname{div}\Gamma = 48 = 44+1+3$, $\operatorname{div}\Gamma = 44P_1 + P_3 + E$, and $\operatorname{div}(\Gamma/(y^{11}z)) = E + 30P_1 - 32P_3 - P_2$, that is, $E \sim P_2 + 32P_3 - 30P_1 = P_1 + P_2 + P_3 + 31(P_3 - P_1)$. The cubic has three roots in $\mathbb{Q}_3$, and the points reduce to $P_1, P_3, P_2$. □

**Lemma 6.7.15.** *With $L_\bullet = \int_{31G} \omega_\bullet$, which is a sum of three tiny integrals by Lemma 6.7.14,*

$$L_x \equiv 642322739790, \qquad L_y \equiv 657631671201, \qquad L_z \equiv 233976154908 \pmod{3^{25}},$$

*with valuations $2,4,1$; the values are known modulo $3^{55}$. The same computation for $62G$ (forms of degree 22 vanishing to order 85 at $P_1$) gives $2(L_x, L_y, L_z)$ (certificate 1.3.7i).*

The differentials $\eta_1 = L_z\omega_x - L_x\omega_z$ and $\eta_2 = L_z\omega_y - L_y\omega_z$ annihilate $J(\mathbb{Q})$ and are independent ($L_z \neq 0$). For $Q$ in the disk of $P_i$ with $t(Q) = 3s$ put $I_k(s) = \int_{P_i}^{Q} \eta_k = \sum_j c_j^{(k)} s^j$.

**Lemma 6.7.16.** *(1) In the disks of $P_1$, $P_2$, $P_4$ one of $I_1, I_2$ has Strassmann bound 1, so $P_i$ is the only rational point in its disk. (2) In the disk of $P_3$, $I_1$ has Strassmann bound 2; its zeros in $\mathbb{Z}_3$ are $s = 0$ and $s = U^* \equiv 589926054506 \pmod{3^{25}}$, and $v_3(I_2(U^*)) = 6$. So $P_3$ is the only rational point in its disk (certificate 1.3.7i).*

*Proof.* The valuations of $c_1, \dots, c_8$ ($\infty$ means that the coefficient is 0) are:

| disk | differential | $v_3(c_1), \dots, v_3(c_8)$ | bound |
|---|---|---|---|
| $P_1$ | $\eta_1$ | $2, \infty, \infty, 6, \infty, 6, \infty, 10$ | 1 |
| $P_2$ | $\eta_2$ | $2, 6, \infty, \infty, \infty, 7, 9, 10$ | 1 |
| $P_3$ | $\eta_1$ | $3, 3, \infty, 6, 6, \infty, 10, 10$ | 2 |
| $P_3$ | $\eta_2$ | $5, \infty, \infty, 5, \infty, \infty, 9, 13$ | 4 |
| $P_4$ | $\eta_2$ | $2, 3, 4, 5, 6, 7, 8, 12$ | 1 |

All $c_j$ with $j \leq 140$ were computed, and the bounds take all of them into account; for $j > 140$ the tail bound gives $v_3(c_j) \geq j - \log_3 j > 130$. The errors from knowing $L_\bullet$ modulo $3^{55}$ have valuation at least 55. This proves (1) and the bound in (2), by [Str28]. For (2), $J_1(s) = I_1(s)/s$ satisfies $v_3(J_1(s_0)) = 43 > 2v_3(J_1'(s_0)) = 6$ at the Newton approximation $s_0$, so by Hensel's lemma it has a unique zero $U^* \equiv s_0 \pmod{3^{40}}$, and $U^* \not\equiv 0 \pmod 3$. Since the coefficients of $I_2$ are integral, $I_2(U^*) \equiv I_2(s_0) \equiv 168750803736 \pmod{3^{25}}$, of valuation 6. So $U^*$ is not a common zero of $I_1, I_2$, while every rational point of the disk satisfies $I_1 = I_2 = 0$. □

*Proof of Theorem 6.7.1.* Every point of $C(\mathbb{Q})$ lies in one of the four residue disks of $C(\mathbb{F}_3)$, and by Lemma 6.7.16 (which uses Lemma 6.7.13) each disk contains only its centre. So $C(\mathbb{Q}) = \{P_1, P_2, P_3, P_4\}$. An integer solution $(x,y,z) \neq (0,0,0)$ is $d$ times a primitive coordinate vector of one of these points, $d = \gcd(x,y,z)$, which gives the four forms in the theorem. $J(\mathbb{Q}) \cong \mathbb{Z}$ is Lemma 6.7.13. □

## 6.8 $x^4 - y^3z + xyz^2 + xz^3 = 0$ ($H = 64$)

**Theorem 6.8.1.** *The only integer solutions of $x^4 - y^3z + xyz^2 + xz^3 = 0$ are $(0,n,0)$, $(0,0,n)$, $(-n,0,n)$ $(n \in \mathbb{Z})$.*

**Setup.** Let $C \subset \mathbb{P}^2$ be the curve defined by the equation in the theorem, and put $J = \mathrm{Jac}(C)$. Write

$$\infty = (0:1:0), \qquad P_0 = (0:0:1), \qquad P_1 = (-1:0:1).$$

Write $F = x^4 - y^3z + xyz^2 + xz^3$ and, in the chart $z = 1$, $f = F(x,y,1) = x^4 - y^3 + xy + x$, so that $C$ is $y^3 = x^4 + xy + x$ there. Put $T = [P_0 - \infty]$ and $G_1 = [P_1 - \infty]$ in $J(\mathbb{Q})$. The line $z = 0$ meets $C$ only at $\infty$, with multiplicity 4, so $\infty$ is a rational hyperflex and the 2-descent of Proposition A applies. The

proof runs as follows. $C$ is smooth, its odd bad primes are 11 and 652081, all odd Tamagawa numbers are 1, $J(\mathbb{Q})_{\mathrm{tors}} = \langle T \rangle \cong \mathbb{Z}/3$, and $G_1$ has infinite order (Step 1). The other 27 bitangents are conjugate, with field of definition $K$ of degree 27 (Step 2). The descent map is injective, with image in the totally positive part of $K(\{2\}, 2)$ (Step 3). The class group of $K$ has odd order, proved without GRH with Proposition B (Step 4); so $K(\{2\}, 2)$ is spanned by 19 explicit $S$-units, and the condition at 2 cuts the image down to dimension 1, so rank $J(\mathbb{Q}) = 1$ (Step 5). Chabauty–Coleman at $p = 3$ shows that each of the three residue disks of $C(\mathbb{F}_3)$ contains only one rational point (Step 6).

**Step 1: the curve.**

**Lemma 6.8.2.** *The points of $C$ with $x = 0$ are $\infty$ and $P_0$; with $y = 0$ they are $P_0$, $P_1$ and the two points $(\zeta : 0 : 1)$ with $\zeta^2 - \zeta + 1 = 0$; with $z = 0$ only $\infty$. So $\infty, P_0, P_1$ are the only rational points of $C$ with a zero coordinate.*

*Proof.* $F(0, y, z) = -y^3 z$, $F(x, 0, z) = x(x + z)(x^2 - xz + z^2)$, $F(x, y, 0) = x^4$. □

**Lemma 6.8.3.** *(1) $C$ is smooth over $\mathbb{Q}$, so it has genus 3. (2) For an odd prime $p$, $C$ has good reduction at $p$ unless $p \in \{11, 652081\}$. (3) For $p \in \{11, 652081\}$ the reduction has exactly one singular point over $\overline{\mathbb{F}}_p$, namely $(x_0 : y_0 : 1)$ with $y_0 \equiv -9/5$, $x_0 \equiv 3y_0^2 \pmod p$; it is an ordinary node, and the scheme $\{F = 0\} \subset \mathbb{P}^2_{\mathbb{Z}_p}$ is regular. (4) For every odd prime $p$ the Tamagawa number $c_p(J)$ is 1 (certificate 1.3.8a).*

*Proof.* On $z = 0$ the only point is $\infty$, and $F_z(0, 1, 0) = -1$, so $\infty$ is a smooth point of every reduction. For affine points, $f_x = 4x^3 + y + 1$ and $f_y = x - 3y^2$, and for odd $p$ Euler's identity shows that an affine point is singular if and only if $f = f_x = f_y = 0$. Over $\mathbb{F}_3$ and $\mathbb{F}_5$ the ideal $(f, f_x, f_y)$ has Gröbner basis $\{1\}$. For $p \neq 3$, $f_y = 0$ gives $x = 3y^2$, and then $f_x = 108y^6 + y + 1$ and $f = y^2(81y^6 + 2y + 3)$. If $y = 0$, then $x = 0$ and $f_x = 1$. Otherwise $4(81y^6 + 2y + 3) - 3(108y^6 + y + 1) = 5y + 9$, so for $p \neq 5$ a singular point has $y = -9/5$, and then $108y^6 + y + 1 = 57383128/5^6 = 2^3 \cdot 11 \cdot 652081/5^6$. This proves (1), (2) and the first part of (3). At $p = 11$ the node is $(4, 7)$, the Hessian determinant $f_{xx}f_{yy} - f_{xy}^2$ is $9 \not\equiv 0$, and $f(4, 7) \equiv 66 \not\equiv 0 \pmod{11^2}$; at $p = 652081$ the node is $(573841, 521663)$, the Hessian determinant is $217362 \not\equiv 0$, and $f(x_0, y_0) \equiv 91909512788 \not\equiv 0 \pmod{p^2}$. Since $f_x, f_y$ vanish at the node modulo $p$, the Taylor expansion shows that $f \in \mathfrak{m}^2$ ($\mathfrak{m} = (p, x - x_0, y - y_0)$) if and only if $f(x_0, y_0) \equiv 0 \pmod{p^2}$; so $f \notin \mathfrak{m}^2$, and the local ring at the node is regular. (4) The special fibre at $p = 11, 652081$ is reduced and geometrically irreducible: components would meet with total intersection number at least 3 (Bézout), only at singular points, but there is only one singular point, an ordinary node, where two branches meet with multiplicity 1. By Raynaud's theorem [BLR90, 9.6, Theorem 1] the component group of the Néron model is trivial. □

**Lemma 6.8.4.** *The numbers $N_k = \#C(\mathbb{F}_{p^k})$, the coefficients of the L-polynomials and $\#J(\mathbb{F}_p) = L_p(1)$ are as follows (certificate 1.3.8a).*

| $p$ | $(N_1, N_2, N_3)$ | *coefficients of* $L_p(t)$ | $\#J(\mathbb{F}_p)$ |
|---|---|---|---|
| 3 | $(3, 9, 27)$ | $1, -1, 0, 0, 0, -9, 27$ | $18 = 2 \cdot 3^2$ |
| 5 | $(5, 29, 119)$ | $1, -1, 2, -4, 10, -25, 125$ | $108 = 2^2 \cdot 3^3$ |
| 7 | $(7, 67, 352)$ | $1, -1, 9, -6, 63, -49, 343$ | $360 = 2^3 \cdot 3^2 \cdot 5$ |
| 17 | $(29, 313, 4856)$ | $1, 11, 72, 329, 1224, 3179, 4913$ | $9729 = 3^2 \cdot 23 \cdot 47$ |
| 29 | $(27, 871, 23904)$ | $1, -3, 19, -210, 551, -2523, 24389$ | $22224 = 2^4 \cdot 3 \cdot 463$ |

*Moreover $C(\mathbb{F}_3) = \{\bar{\infty}, \bar{P}_0, \bar{P}_1\}$.*

**Lemma 6.8.5.** *$J(\mathbb{Q})_{\mathrm{tors}} = \langle T \rangle \cong \mathbb{Z}/3$, and $G_1$ has infinite order.*

*Proof.* By [Kat81, Appendix], the torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}}$ injects into $J(\mathbb{F}_p)$ for every odd prime $p$ of good reduction; $\#J(\mathbb{F}_{17})$ is odd and $\gcd(108, 360, 9729, 22224) = 3$, so $\#J(\mathbb{Q})_{\mathrm{tors}}$ divides 3. The line $x = 0$ meets $C$ in $3P_0 + \infty$ and $z = 0$ in $4\infty$, so $\mathrm{div}(x/z) = 3P_0 - 3\infty$ and $3T = 0$; $T \neq 0$ since the genus is positive. The function $x/z$ has a pole of order exactly 3 at $\infty$, and $\dim L(3\infty) \leq 2$, so

$L(3\infty) = \langle 1, x/z \rangle$. If $G_1$ were torsion, then $3G_1 = 0$ and some $a + b\,x/z$ would have divisor $3P_1 - 3\infty$; vanishing at $P_1$ forces $a = b$, but $F(-z, y, z) = -yz(y^2 + z^2)$ shows that $(x + z)/z$ has only a simple zero at $P_1$. □

**Lemma 6.8.6.** *$C(\mathbb{R})$ is connected. Hence $J(\mathbb{R})/2J(\mathbb{R}) = 0$ (certificate 1.3.8a).*

*Proof.* For real $x$, the cubic $y^3 - xy - (x^4 + x)$ has discriminant $x^2\big(4x - 27(x^3 + 1)^2\big)$. The second factor has no real root and is $-27$ at $x = 0$, so the discriminant is negative for $x \neq 0$, and for $x = 0$ the cubic is $y^3$. So for every real $x$ there is exactly one real $y$, depending continuously on $x$; the affine real locus is a graph over $\mathbb{R}$, and $C(\mathbb{R})$ is its closure. The rest is [GH81]. □

**Step 2: the bitangents and the field $K$.** Let

$$B(m) = m^{27} - 48m^{22} + 1344m^{18} + 144m^{17} - 3264m^{13} + 832m^{12} - 40704m^9 \\ - 4608m^8 - 2560m^7 - 39936m^4 - 15360m^3 - 1024m^2 + 4096,$$

let $\theta$ be a root, and $K = \mathbb{Q}(\theta)$.

**Lemma 6.8.7.** *(1) $B$ is irreducible, and*

$$\operatorname{disc}(B) = 2^{318} \cdot 11^6 \cdot 41^2 \cdot 198839^2 \cdot 652081^6 \cdot 177432992570285462298592$$

*(all factors prime). (2) For the line $y = mx + k$ write $f(x, mx + k) = x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$. It is the square of $x^2 + ux + v$ if and only if $u = c_3/2 = -m^3/2$, $v = (c_2 - u^2)/2 = (m - 3m^2k - u^2)/2$, $E_1 := c_1 - 2uv = 0$ and $E_2 := c_0 - v^2 = 0$. The resultant of $E_1, E_2$ with respect to $k$ is $B(m)/4096$ (equivalently, that of the primitive integer polynomials $8E_1$, $64E_2$ is $512B(m)$), and the leading coefficient of $E_2$ in $k$ is $-1$; so $E_1(m_0, k)$ and $E_2(m_0, k)$ have a common root if and only if $B(m_0) = 0$. Over $K$ the gcd of $E_1(\theta, k)$ and $E_2(\theta, k)$ is linear in $k$, with root $k(\theta) \in K$ (recorded in `descent/k_paper.gp` of certificate 1.3.8b), and $f(x, \theta x + k(\theta)) = (x^2 + u(\theta)x + v(\theta))^2$ in $K[x]$. (3) The 28 bitangents of $C$ are $z = 0$ and the 27 lines $\ell_\theta : \ y = \theta x + k(\theta)z$, $\theta$ running over the roots of $B$ (certificate 1.3.8b).*

*Proof.* (3) A line through $\infty$ other than $z = 0$ is $x = cz$; it meets $C$ at $\infty$ with multiplicity 1, so it is not a bitangent. Every other line is $y = mx + kz$, and by (2) it is a bitangent if and only if $B(m) = 0$ and $k = k(m)$. These are 27 distinct lines. □

**Lemma 6.8.8.** *$K$ has signature $(3, 12)$ and discriminant $d_K = 2^{34} \cdot 11^6 \cdot 652081^6$; its maximal order is certified without GRH. The prime 2 factors as $2\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2^{10}\mathfrak{p}_3^5\mathfrak{p}_4^5$ with residue degrees $1, 1, 1, 2$; equivalently, $B$ factors over $\mathbb{Q}_2$ into irreducible factors of degrees $2, 10, 5, 10$ (certificate 1.3.8b, certificate 1.3.8c).*

**Step 3: the descent map.** For each root $\theta$ of $B$ put $h_\theta = (y - \theta x - k(\theta)z)/z$. At $\infty$ the function $X = x/y$ is a uniformizer, $z/y = X^4 + O(X^9)$ and $h_\theta = X^{-4}(1 + O(X))$, so $h_\theta$ is normalized as in Proposition A(2), and for an affine point $P = (x : y : 1)$ that is not a point of contact,

$$\delta([P - \infty]) = y - \theta x - k(\theta) \in K^\times / K^{\times 2}.$$

In particular $\delta(G_1) = \theta - k(\theta)$ and $\delta(T) = -k(\theta)$.

**Lemma 6.8.9.** *For a root $\theta$ of $B$ let $D_\theta$ be the contact divisor of $\ell_\theta$ (so $\operatorname{div} h_\theta = 2D_\theta - 4\infty$) and $w_\theta = [D_\theta - 2\infty] \in J[2]$. Then $\iota : J[2] \to \mathbb{F}_2^{27}$, $\varepsilon \mapsto (e_2(\varepsilon, w_\theta))_\theta$, is injective, and the nonzero vectors of $V = \iota(J[2])$ have weight 12 (36 vectors) or 16 (27 vectors); in particular $\mathbf{1} \notin V$ (certificate 1.3.8d).*

*Proof.* $q(w) = h^0(2\infty + w) + h^0(2\infty) \bmod 2$ is a quadratic form on $J[2]$ with polar form $e_2$, whose zeros are 0 and the 27 classes $w_\theta$; so it has Arf invariant 1, and $\iota(\varepsilon)_\theta = e_2(\varepsilon, w_\theta)$. All quadratic forms of Arf invariant 1 on $\mathbb{F}_2^6$ are equivalent, so it suffices to enumerate the 64 vectors for $q(a) = a_1a_2 + a_3a_4 + a_5^2 + a_5a_6 + a_6^2$. □

This is the computation behind Proposition A(1), (2).

**Lemma 6.8.10.** *$J(\mathbb{Q})[2] = 0$, and $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^\times/K^{\times 2}$ is injective. Every element of $\delta(J(\mathbb{Q}))$ lies in*

$$K(2,S) = \{a \in K^\times/K^{\times 2} : \ v_{\mathfrak{p}}(a) \text{ even for all } \mathfrak{p} \notin S\}, \qquad S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\},$$

*and is totally positive.*

*Proof.* $B$ is irreducible of degree 27, so Proposition A(1), (2) give the first statement. Since $c_p(J) = 1$ for all odd $p$ (Lemma 6.8.3), the set $S$ of Proposition A(3) is $\{2\}$. At the real place, $\delta_{\mathbb{R}}$ is defined on $J(\mathbb{R})/2J(\mathbb{R}) = 0$ (Lemma 6.8.6) and is compatible with restriction (Proposition A(3)). □

**Step 4: the class group of $K$.**

**Lemma 6.8.11.** *Every prime ideal of $K$ of norm $\leq 10^6$ is principal. There are 77,813 of them (77,583 of degree 1, 193 of degree 2, 18 of degree 3, 15 of degree 5, 3 of degree 6, 1 of degree 10) (certificate 1.3.8e).*

*Proof.* For each prime ideal $\mathfrak{p}$ a generator $g$ was proposed by `bnfisprincipal` (used only as a proposer). The checker, which does not use PARI's class group functions, enumerates the prime ideals itself (for $p > 1000$ not dividing $\operatorname{disc} B$ through the roots $r$ of $B$ modulo $p$, $\mathfrak{p} = (p, \theta - r)$; otherwise with `idealprimedec` in the certified maximal order), and verifies for each $\mathfrak{p}$: $g \in \mathcal{O}_K$ ($g$ is stored as a polynomial in $\theta$ divided by an integer, and its coordinates on the certified integral basis computed by the running PARI are integers; the check was run with PARI 2.15.4 and with PARI 2.17.4), $g \in \mathfrak{p}$, and $|N_{K/\mathbb{Q}}(g)| = N\mathfrak{p}$, where $N(g)$ is computed exactly as a resultant. Then $(g) \subseteq \mathfrak{p}$ and both have the same norm, so $(g) = \mathfrak{p}$. Each generator is used for exactly one prime ideal. □

**Lemma 6.8.12.** *Let $R = 5 \cdot 10^8$. There are 26,365,548 prime ideals of $K$ of norm $< R$, with 14,287,575 distinct norms (certificate 1.3.8f).*

*Proof.* For $p \leq \sqrt{R}$ and for $p \mid \operatorname{disc} B$ the prime ideals are computed with `idealprimedec` in the certified maximal order. For the other $p < R$ only prime ideals of degree 1 can have norm $< R$, and since $p \nmid \operatorname{disc} B$ their number is the number of roots of $B$ modulo $p$ (Dedekind–Kummer), computed as $\deg \gcd(B, x^p - x)$ over $\mathbb{F}_p$ by exact integer arithmetic. The root counts were confirmed with FLINT for 299,996 primes spread over the range and with PARI for 5,905 of them, and for all $p \leq 10^6$ by the checker of certificate 1.3.8e. □

**Lemma 6.8.13.** *$\mathrm{Cl}(K)$ has odd order. Consequently $\mathrm{Cl}(\mathcal{O}_{K,S})[2] = 0$.*

*Proof.* Apply Proposition B with $n = 27$, $(r_1, r_2) = (3, 12)$, $D = 2^{34}11^6652081^6$, $T = \log(5 \cdot 10^8) = 20.0301\ldots$, $k(q) = a(q)$ for $q \leq 10^6$ (Lemma 6.8.11) and $k(q) = 0$ for $10^6 < q < 5 \cdot 10^8$ (Lemma 6.8.12), and the step function $v$ with 64 equal cells on $[0, T]$ and the integer heights

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 307 | 385 | 444 | 494 | 541 | 584 | 626 | 667 | 704 | 738 | 769 | 799 | 827 | 853 | 876 | 898 |
| 917 | 935 | 949 | 962 | 971 | 977 | 982 | 986 | 990 | 993 | 995 | 997 | 998 | 999 | 1000 | 1000 |
| 1000 | 1000 | 999 | 998 | 997 | 995 | 993 | 990 | 986 | 982 | 977 | 971 | 962 | 949 | 935 | 917 |
| 898 | 876 | 853 | 827 | 799 | 769 | 738 | 704 | 667 | 626 | 584 | 541 | 494 | 444 | 385 | 307 |

In ball arithmetic (certificate 1.3.8g),

$$C_\infty = -1.16146083530\ldots,$$
$$C_\infty - \int_0^\infty (1-f)W = -1.215796113312597138688\ldots,$$
$$\frac{4}{n}\sum c_m(q)\frac{\log q}{q^m+1} f(m\log q) = 1.268980762763662101585\ldots,$$
$$B^-(f) \in [0.053184649451064962897026614594 4 \pm 4.6 \cdot 10^{-32}];$$

the prime sum has positive part $1.3389143385\ldots$ and negative part $-0.0699335757\ldots$. Therefore $B^-(f) > 0$ and $\mathrm{Cl}(K)[2] = 0$. $\mathrm{Cl}(\mathcal{O}_{K,S})$ is a quotient of $\mathrm{Cl}(K)$. □

The window was chosen as the top eigenvector of the symmetric Toeplitz matrix $\Lambda$ with $B^-(f) = \mathbf{h}^{\mathsf{T}}\Lambda\mathbf{h}/\mathbf{h}^{\mathsf{T}}\mathbf{h}$ for the vector $\mathbf{h}$ of heights (certificate 1.3.8g, floating point; this only selects the window). If $f$ has knots $f_k = f(k\delta)$ ($\delta = T/64$), then $f = \sum_k w_k(1-|x|/k\delta)_+$ with $w_k = k(f_{k-1} - 2f_k + f_{k+1})$, and $C_\infty - \int_0^\infty (1-f)W = \sum_k w_k A(k\delta)$ with

$$A(a) = C_\infty - \frac{\pi^2}{4a} - \frac{2\alpha\log 2}{a} + \frac{2}{a}\Big(\mathrm{Li}_2(e^{-a}) - \frac{\mathrm{Li}_2(e^{-2a})}{4}\Big) + \frac{2\alpha}{a}\log(1+e^{-a}).$$

**Step 5: $S$-units, the local image at 2, and the rank.**

**Lemma 6.8.14.** *Let $\varepsilon_1,\dots,\varepsilon_{14}$ and $\pi_1,\dots,\pi_4$ be the 14 units and 4 $S$-units recorded in* `descent/paper_sunits.json` *of* certificate 1.3.8i. *Then $-1,\varepsilon_1,\dots,\varepsilon_{14},\pi_1,\dots,\pi_4$ is a basis of $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ and of $K(2,S)$, and $\dim_{\mathbb{F}_2} K(2,S) = 19$ (certificate 1.3.8h, certificate 1.3.8i).*

*Proof.* Each $\varepsilon_i$ is integral with $N(\varepsilon_i) = \pm 1$, and each $\pi_j$ is integral with $N(\pi_j) \in \{\pm 2, \pm 4\}$, so all are $S$-units. Their quadratic characters at the 400 degree-one prime ideals $(q, \theta - r)$ with $q \le 2791$, $q \nmid \operatorname{disc} B$, form a matrix of rank 19 over $\mathbb{F}_2$, so the 19 elements are independent in $K^\times/K^{\times 2}$. By Dirichlet's $S$-unit theorem, $\mathcal{O}_{K,S}^\times \cong \{\pm 1\} \times \mathbb{Z}^{r_1+r_2-1+\#S} = \{\pm 1\} \times \mathbb{Z}^{18}$, so $\dim \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2} = 19$. The exact sequence $0 \to \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2} \to K(2,S) \to \mathrm{Cl}(\mathcal{O}_{K,S})[2] \to 0$ and Lemma 6.8.13 give $K(2,S) = \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$. □

**Lemma 6.8.15.** $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)[2] \le 1$, *so* $\dim_{\mathbb{F}_2} \delta_{\mathbb{Q}_2}(J(\mathbb{Q}_2)) \le 4$. *The four points $P = (x,y) \in C(\mathbb{Q}_2)$ with*

| $x$ | $y \bmod 2^{60}$ |
|---|---|
| $-40$ | 177036671367769442 |
| $-39$ | 271477316397691054 |
| $-37$ | 408928458825745180 |
| $-35$ | 1073474074041454754 |

*have classes $\delta_{\mathbb{Q}_2}([P-\infty])$ that span a subspace $W_2 \subset \prod_{\mathfrak{p}\mid 2} K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ of dimension 4. Hence $\delta_{\mathbb{Q}_2}(J(\mathbb{Q}_2)) = W_2$ (certificate 1.3.8d, certificate 1.3.8h).*

*Proof.* $J(\mathbb{Q}_2)[2] \cong V^D$ (Lemma 6.8.9), where $D$ is the image of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$; its orbits on the 27 coordinates have sizes $2,5,10,10$ (Lemma 6.8.8). A $D$-invariant vector is a union of orbits, of weight in $\{0,2,5,7,10,12,15,17,20,22,25,27\}$, so by Lemma 6.8.9 a nonzero invariant vector of $V$ has weight $12 = 2+10$; there are at most two such unions, and their sum has weight 20, which does not occur. So $\dim V^D \le 1$, and by Proposition A(5) $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3 + \dim J(\mathbb{Q}_2)[2] \le 4$.

The values $y$ are the roots in $\mathbb{Z}_2$ of $y^3 - xy - (x^4+x)$, computed to precision $2^{80}$. For each $\mathfrak{p} \mid 2$ with ramification index $e$, the class of $a \in K_\mathfrak{p}^\times$ modulo squares is determined by $v_\mathfrak{p}(a) \bmod 2$ and by the class of the unit $a\pi^{-v(a)}$ in $(\mathcal{O}_K/\mathfrak{p}^{2e+1})^\times$ modulo squares, read off from the discrete logarithm; the number of even cyclic factors of $(\mathcal{O}_K/\mathfrak{p}^{2e+1})^\times$ is $1 + [K_\mathfrak{p} : \mathbb{Q}_2]$ in all four cases, as it must be. This gives coordinates in $\mathbb{F}_2^{35}$. The integer $Y \equiv y \pmod{2^{80}}$ satisfies $v_\mathfrak{p}(Y-y) - v_\mathfrak{p}(Y-\theta x-k) \ge 2e+1$ for all $\mathfrak{p} \mid 2$, so $Y - \theta x - k$ has the same square class as $y - \theta x - k$. The four class vectors have rank 4. (All 47 points of $C(\mathbb{Q}_2)$ with $x \in \mathbb{Z} \cap [-40,40]$, and the four points with $x = -24,-23,-21,-19$, give classes in $W_2$.) □

Let $\Sigma = \{a \in K(2,S) : a \text{ is totally positive and } (a)_{\mathfrak{p}\mid 2} \in W_2\}$. By Lemmas 6.8.10 and 6.8.15, $\operatorname{rank} J(\mathbb{Q}) = \dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) \le \dim_{\mathbb{F}_2} \Sigma$.

**Lemma 6.8.16.** $\dim_{\mathbb{F}_2} \Sigma = 1$, *and $\Sigma$ is generated by $\theta - k(\theta) = \delta(G_1)$. Hence* $\operatorname{rank} J(\mathbb{Q}) = 1$, *and $J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3$.*

*Proof.* In the basis of Lemma 6.8.14, $\Sigma$ is the kernel of an explicit $\mathbb{F}_2$-linear map: the three real signs (computed with rigorous isolation of the real roots of $B$ in ball arithmetic, and confirmed by PARI's `nfeltsign`) and the 35 coordinates at $\mathfrak{p} \mid 2$ taken modulo $W_2$. The kernel has dimension 1 (certificate 1.3.8h); in this basis it is generated by $\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4$, which equals $\theta - k(\theta)$ modulo squares: both lie in

$K(2,S)$ ($\theta - k(\theta)$ has even valuation at every prime ideal outside $S$), and their quadratic characters agree at 399 prime ideals (certificate 1.3.8i). So rank $J(\mathbb{Q}) \le 1$, and by Lemma 6.8.5 rank $J(\mathbb{Q}) \ge 1$ and $J(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/3$. (Consistently, $\theta - k(\theta)$ is totally positive with local class in $W_2$, and $\delta(T) = -k(\theta)$ is a square in $K$.) □

The condition at 2 alone already gives the bound: in the coordinates of Lemma 6.8.14 and on the basis of $W_2$ given by the four points of Lemma 6.8.15, the condition $(a)_{\mathfrak{p}|2} \in W_2$ is a homogeneous system of 35 linear equations over $\mathbb{F}_2$ in $19+4$ unknowns of rank 22, and the four basis vectors of $W_2$ are independent; so $\{a \in K(2,S) : (a)_{\mathfrak{p}|2} \in W_2\}$ has dimension 1 (certificate 1.3.8h). Hence Lemma 6.8.16 holds without the sign condition, and without the norm condition of Proposition A(4).

**Step 6: Chabauty–Coleman at $p = 3$.** By Lemma 6.8.3, $C$ has good reduction at 3, and by Lemma 6.8.4, $C(\mathbb{Q}_3)$ is the union of the three residue disks $U_\infty, U_{P_0}, U_{P_1}$ of the points of $C(\mathbb{F}_3)$, where $U_R$ is the set of points of $C(\mathbb{Q}_3)$ that reduce to $\bar{R}$; for a finite extension $M$ of $\mathbb{Q}_3$, $U_R(M)$ denotes the set of points of $C(M)$ that reduce to $\bar{R}$.

Let $\Omega = dx/f_y(x,y)$ and $w_L = L\,\Omega$ for $L \in \{z, x, y\}$. These form a $\mathbb{Z}_3$-basis of the regular differentials of the smooth model over $\mathbb{Z}_3$, and $w_L$ vanishes exactly where $L$ does. In the chart $y = 1$, with $X = x/y$ and $Z = z/y$, $F(X,1,Z) = X^4 - Z + XZ^2 + XZ^3$, and the equation $Z = X^4 + XZ^2 + XZ^3$ has a unique solution $Z(X) \in X^4\mathbb{Z}[[X]]$; so $w_L = \phi_L(X)\,dX$ with $\phi_L \in \mathbb{Z}[[X]]$:

$$\phi_z = X^4 + \cdots, \qquad \phi_x = X + 2X^6 + \cdots, \qquad \phi_y = 1 + 2X^5 + \cdots.$$

**Lemma 6.8.17.** *Let $\lambda = \log(-9G_1) \in \mathbb{Q}_3^3$ be the vector of the abelian integrals of $w_z, w_x, w_y$ over $-9G_1$. Then $v_3(\lambda) = (5,2,6)$, and $3^{-2}\lambda$ is, up to a unit, congruent to $(432,1,81)$ modulo $3^6$. In particular, modulo 3, $\log G_1$ is proportional to $(0,1,0)$ (certificate 1.3.8j).*

*Proof.* The functions $x^i y^j$ ($j \le 2$, $3i + 4j \le 14$; $x, y$ have poles of orders 3 and 4 at $\infty$) form a basis of $L(14\infty)$. With the parameter $s = x + 1$ at $P_1$ (where $f_y = -1$) and $y(s) \in \mathbb{Z}[[s]]$, the condition $\mathrm{ord}_{P_1} \ge 9$ cuts out a 3-dimensional subspace, which contains

$$\begin{aligned} g = {} & 49412858216 + 191259723096x + 291125394027x^2 \\ & + 206187126854x^3 + 56908597707x^4 + 37163261480y \\ & + 102426117246xy + 100459295010x^2y + 35217797652x^3y + 836804043y^2 + 36xy^2, \end{aligned}$$

with $\mathrm{ord}_{P_1} g = 9$ exactly and pole order 13 at $\infty$; its reduction modulo 3 is nonzero with pole order exactly 9 at $\bar{\infty}$. So $\operatorname{div} g = 9P_1 + \mathcal{E} - 13\infty$ with $\mathcal{E}$ effective of degree 4, and $\operatorname{div} \bar{g} = 9\bar{P}_1 - 9\bar{\infty}$; since divisors specialize on the smooth model, $\mathcal{E}$ reduces to $4\bar{\infty}$. Thus $[\mathcal{E} - 4\infty] = -9G_1$. The $X$-coordinates of the points of $\mathcal{E}$ are the roots of the irreducible polynomial $\mathrm{Res}_Z(F(X,1,Z), Z^4 g(X/Z, 1/Z))/X^3$,

$$\begin{aligned} \mathcal{E}(X) = {} & 26889542662770715798711613338841 6X^4 + 32033763811651723720409184304589 1X^3 \\ & + 21967286057390851966863135827974 8X^2 + 15789457700179064657071966647590 4X \\ & + 85988850899990436755428562963712, \end{aligned}$$

whose four roots all have 3-adic valuation $3/4$ (the coefficients of $X^0, \ldots, X^4$ have valuations $3, 3, 2, 5, 0$); their $Z$-coordinates have valuation 3. Since $3/4$ has denominator 4, $\mathcal{E}(X)$ is irreducible over $\mathbb{Q}_3$, and any of its roots generates a totally ramified extension $M$ of $\mathbb{Q}_3$ of degree 4. So the four points of $\mathcal{E}$ are conjugate over $\mathbb{Q}_3$ and lie in $U_\infty(M)$, where $X$ takes values in the maximal ideal of $\mathcal{O}_M$. The divisor $\mathcal{E} - 4\infty$ is defined over $\mathbb{Q}_3$, and by [KRZB16, Section 3]

$$\lambda_L = \sum_{Q \in \mathcal{E}} \int_\infty^Q w_L = \mathrm{Tr}_{M/\mathbb{Q}_3} \int_\infty^{Q_1} w_L = \sum_{k \ge 0} \frac{\phi_{L,k}}{k+1}\, p_{k+1}, \qquad p_j = \sum_{Q \in \mathcal{E}} X(Q)^j,$$

where $Q_1$ is any one of the four points and $p_j \in \mathbb{Q}$ is computed exactly by Newton's identities from $\mathcal{E}(X)$. Since $v_3(p_j) \ge 3j/4$, the terms with $k \ge 159$ have valuation greater than 115. As a check, the same computation with $\mathrm{ord}_{P_1} \ge 18$ in $L(23\infty)$ (a function of pole order 22, again with $\deg \mathcal{E} = 4$) gives $\log(-18G_1) = 2\lambda$ to precision $3^{114}$. □

**Lemma 6.8.18.** *Each residue disk $U_\infty, U_{P_0}, U_{P_1}$ contains exactly one rational point (certificate 1.3.8j).*

*Proof.* Since $\operatorname{rank} J(\mathbb{Q}) = 1$ and $G_1$ has infinite order (Lemma 6.8.16), every $\omega = c_z w_z + c_x w_x + c_y w_y$ with $c \cdot \lambda = 0$ satisfies $\int_R^P \omega = 0$ for all $P, R \in C(\mathbb{Q})$ ([MP12, Sections 4–5]). By Lemma 6.8.17, $\lambda/9$ has unit $x$-coordinate, so for any $c_z, c_y \in \mathbb{Z}_3$ there is a unique $c_x \in \mathbb{Z}_3$ with $c \cdot \lambda = 0$, and then $c_x \equiv 0 \pmod 3$.

Let $R \in \{\infty, P_0, P_1\}$ and let $t$ be the local parameter $X$, $y$, $x+1$ respectively (at $P_0$, $f_x = 1$ and $x(y) \in y^3\mathbb{Z}[[y]]$; at $P_1$, $f_y = -1$ and $y(s) \in \mathbb{Z}[[s]]$). The map $Q \mapsto t(Q)$ is a bijection $U_R \to 3\mathbb{Z}_3$, and every regular differential is $(a_0 + a_1 t + \cdots)\,dt$ with $a_k \in \mathbb{Z}_3$ and $a_0 \equiv (\text{unit}) \cdot (c_z, c_x, c_y) \cdot (z, x, y)(R) \pmod 3$. The reductions $(z, x, y)(R) \bmod 3$ are $(0,0,1)$, $(1,0,0)$, $(1,2,0)$. Taking $(c_z, c_y) = (0,1)$ for $R = \infty$ and $(1,0)$ for $R = P_0, P_1$ gives annihilating differentials with $a_0 \not\equiv 0 \pmod 3$ (in fact $a_0 \equiv 1, -1, 41849 \pmod{3^{10}}$). For $Q \in U_R \cap C(\mathbb{Q})$ write $t(Q) = 3s$; then

$$0 = \frac{1}{3}\int_R^Q \omega = a_0 s + \sum_{k \geq 1} a_k \frac{3^k}{k+1} s^{k+1},$$

and $v_3(3^k/(k+1)) = k - v_3(k+1) \geq 1$ for $k \geq 1$. By [Str28] this power series has at most one zero in $\mathbb{Z}_3$, namely $s = 0$. So $Q = R$. □

*Proof of Theorem 6.8.1.* $C(\mathbb{Q}) \subseteq U_\infty \cup U_{P_0} \cup U_{P_1}$, and by Lemma 6.8.18 each disk contains only its centre. So $C(\mathbb{Q}) = \{\infty, P_0, P_1\}$. An integer solution $(x, y, z) \neq (0,0,0)$ is $\gcd(x,y,z)$ times a primitive coordinate vector of one of these points, which gives the three forms in the theorem. $J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3$ is Lemma 6.8.16. □

## 6.9 $x^4 + x^3y - y^4 + y^3z + z^4 = 0$ ($H = 80$)

Let $F = x^4 + x^3y - y^4 + y^3z + z^4$ and let $C$ be the projective plane curve $F = 0$. The equation is Open Question 6.8 of [Gre24] and equation (18) of [Gre26c]. Its five quartic monomials give $H(F) = 80$.

**Theorem 6.9.1.** *The curve $C$ has no rational point. The only integer solution of $F = 0$ is $(0,0,0)$.*

A nonzero integral solution gives a projective rational point, and denominators of a rational point can be cleared. We exhibit a class of order three in $\mathrm{Br}(C)$ whose local invariants have nonzero sum on every adelic point. The construction uses cubic Hilbert symbols over $K = \mathbb{Q}(\omega)$, where $\omega^2 + \omega + 1 = 0$. The arithmetic certificate specifies the functions in those symbols and the cube witnesses that verify their residues. Tables 11 and 12 give the functions, constants and weights.

### 6.9.1 Cubic Hilbert symbols

Let $K = \mathbb{Q}(\omega)$, $\mathcal{O}_K = \mathbb{Z}[\omega]$ and $\lambda = 1 - \omega$, so that $3 = -\omega^2\lambda^2$ and $\lambda$ is the place above 3. For a place $w$ of $K$ and $a, b \in K_w^\times$, the cubic Hilbert symbol $(a,b)_{w,3}$ is a cube root of unity, and we write

$$(a,b)_{w,3} = \omega^{\beta_w(a,b)}, \qquad \beta_w(a,b) \in \mathbb{Z}/3. \tag{16}$$

We use the following standard facts: (K1)–(K3) are in [Neu99, Ch. V, §3], (K4) is the product formula [Neu99, Ch. VI, §8], and (K5) relates the symbol to cyclic algebras [Ser79, Ch. XIV] and corestriction to local invariants [CTS21].

(K1) $\beta_w$ is bi-additive, $\beta_w(b,a) = -\beta_w(a,b)$, and $\beta_w(a,b)$ depends only on the classes of $a, b$ modulo $K_w^{\times 3}$. Note that $-1 = (-1)^3$ is a cube.

(K2) If $w$ is complex, $\beta_w = 0$. The field $K$ has one complex place.

(K3) Let $w \nmid 3$, let $\pi$ be a uniformiser and $q$ the order of the residue field. For $a = \pi^e u$ and $b = \pi^f v$ with units $u, v$,

$$\beta_w(a,b) = e\,\chi_w(v) - f\,\chi_w(u), \qquad \text{where } u^{(q-1)/3} \equiv \omega^{\chi_w(u)} \pmod w. \tag{17}$$

A unit congruent to 1 modulo $w$ is a cube, by Hensel's lemma, since $3 \nmid q$.

(K4) (Product formula) For $a, b \in K^\times$, $\beta_w(a,b) = 0$ for all but finitely many $w$, and $\sum_w \beta_w(a,b) = 0$.

(K5) The cyclic algebra $(a,b)_\omega$ over $K_w$ has invariant $\varepsilon\,\beta_w(a,b)/3 \in \frac{1}{3}\mathbb{Z}/\mathbb{Z}$, with a sign $\varepsilon = \pm 1$ that does not depend on $w$. For a place $v$ of $\mathbb{Q}$ and $\alpha \in \mathrm{Br}(K \otimes \mathbb{Q}_v)$, $\mathrm{inv}_v(\mathrm{Cor}\,\alpha) = \sum_{w|v} \mathrm{inv}_w(\alpha_w)$. We write $\iota\colon \frac{1}{3}\mathbb{Z}/\mathbb{Z} \longrightarrow \mathbb{Z}/3$ for the isomorphism $a/3 \bmod \mathbb{Z} \mapsto a \bmod 3$.

The opposite sign convention for (17) is also common; it changes the sign of every $\beta_w$ and does not affect the argument. For example, at the place above 7 where $\omega \equiv 2$, $\chi(2) = 2$ since $2^2 \equiv \omega^2$, so $\beta(7,2) = 2$ and $\beta(2,7) = 1$ there.

**Lemma 6.9.2** (the place $\lambda$). *Every element of $1 + 9\mathcal{O}_\lambda$ is a cube in $K_\lambda$. Hence, if $x, x' \in K_\lambda^\times$ and $v_\lambda(x - x') \geq v_\lambda(x) + 4$, then $x$ and $x'$ have the same class in $K_\lambda^\times / K_\lambda^{\times 3}$. For $a, b \in K^\times$,*

$$\beta_\lambda(a,b) = -\sum_{w \neq \lambda} \beta_w(a,b),$$

*where the sum is over the finitely many finite places $w \neq \lambda$ dividing $ab$, and each term is given by (17).*

*Proof.* For $t \in \mathcal{O}_\lambda$, $(1+3t)^3 = 1 + 9(t + 3t^2 + 3t^3)$. The derivative of $t + 3t^2 + 3t^3$ is a unit, so by Hensel's lemma every element of $1 + 9\mathcal{O}_\lambda$ is of this form. Since $v_\lambda(9) = 4$, the condition gives $x'/x \in 1 + 9\mathcal{O}_\lambda$. The last formula is (K4), with (K2) at the complex place and (K3) at the places $w \nmid 3ab$, where $a$ and $b$ are units. □

Every unit of $\mathcal{O}_\lambda$ is congruent modulo 9 to $\pm\omega^a 4^b (1+3\omega)^c$ for unique $a, b, c \in \{0,1,2\}$ (a check of the 54 units of $\mathcal{O}_\lambda/9$), and the cubes of units are congruent to $\pm 1$ modulo 9. So, by Lemma 6.9.2, the classes of $\lambda$, $\omega$, 4 and $1+3\omega$ form a basis of $K_\lambda^\times / K_\lambda^{\times 3} \cong (\mathbb{Z}/3)^4$; the class of an element is determined by its valuation and the residue of its unit part modulo 9; and $\beta_\lambda$ is the bilinear form whose matrix on this basis is given by the last formula of Lemma 6.9.2:

$$\big(\beta_\lambda(g,h)\big)_{g,h \in (\lambda, \omega, 4, 1+3\omega)} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The entries follow by applying the tame formula at the prime divisors of the four generators and then using reciprocity.

### 6.9.2 The curve

**Lemma 6.9.3.** *(i) $C$ is smooth over $\mathbb{Z}_p$ for every prime $p \notin \{149, 283, 163991\}$; in particular $C$ is smooth over $\mathbb{Q}$ and has good reduction at 2, 3 and 7. For each of the three primes the reduction has a single singular point over $\bar{\mathbb{F}}_p$, which is $\mathbb{F}_p$-rational: an ordinary double point for $p = 149$ and 163991, and a cusp for $p = 283$. The reduction is geometrically integral, and the model $\mathrm{Proj}\,\mathbb{Z}_p[x,y,z]/(F)$ is regular.*

*(ii) $C(\mathbb{R})$ and all $C(\mathbb{Q}_p)$ are non-empty. Moreover $C(\mathbb{F}_2) = \{(1:0:1)\}$ and $C(\mathbb{F}_3) = \{(1:1:1)\}$.*

*(iii) $C$ has the cubic points*

$$P_a\colon x^3 - x^2 + 1 = 0, \quad y = x^2 - x, \quad z = 1,$$
$$P_b\colon x^3 - x^2 - 2x - 1 = 0, \quad y = -x^2 + x + 1, \quad z = 1.$$

*Proof.* (i) The Macaulay resultant of the cubics $F_x, F_y, F_z$, computed as $\det M / \det M'$ from the $36 \times 36$ matrix $M$ of Macaulay in degree 7 and its $9 \times 9$ extraneous minor $M'$ ($\det M' = -2^{18}$), is

$$\mathrm{Res}(F_x, F_y, F_z) = -2^{14} \cdot 149 \cdot 283^2 \cdot 163991.$$

For odd $p$, the identity $4F = xF_x + yF_y + zF_z$ shows that the reduction is singular exactly when $p$ divides this number. Modulo 2, $F_z \equiv y^3$, $F_x \equiv x^2 y$ and $F_y \equiv x^3 + y^2 z$, so a common zero has $y = x = 0$,

and then $F = z^4 \neq 0$. For the three odd primes, let $f = F(x,y,1)$; the greatest common divisor of $\mathrm{Res}_y(f,f_y)$, $\mathrm{Res}_y(f_x,f_y)$ and $\mathrm{Res}_y(f,f_x)$ has a single root modulo $p$, above which $f$, $f_x$, $f_y$ have a single common root, and there is no singular point on $z=0$ (there $F_z = y^3$, and $(1:0:0) \notin C$). The singular points are $(99:17:1)$, $(0:213:1)$ and $(54470:146028:1)$. At 149 and 163991 the Hessian of $f$ is non-zero at the singular point. At 283 the quadratic part of $f$ at the singular point is the square of a linear form which does not divide the cubic part, so the singularity is a cusp. A cusp has one branch, and an ordinary double point is not a point where two components of degrees $d$ and $d'$ with $dd' \geq 3$ meet; so in all three cases the reduction is irreducible (a reducible or non-reduced quartic has at least two singular points, or a singular point of intersection multiplicity at least 3). Finally $F(\tilde{P})/p \not\equiv 0 \pmod{p}$ for the integral lifts $\tilde{P}$ of the singular points. As all partial derivatives vanish there modulo $p$, $F$ does not lie in the square of the maximal ideal of the local ring of $\mathbb{P}^2_{\mathbb{Z}_p}$ at the singular point, and the model is regular there. At the other points of the special fibre it is smooth over $\mathbb{Z}_p$.

(ii) $F(0,1,1) = 1$ and $F(0,2,1) = -7$, so $C(\mathbb{R}) \neq \emptyset$. For every $p < 60$ and for the three primes of (i) there are smooth points of $C$ modulo $p$, found by enumeration (for 163991, the point $(1:36060:1)$); for the other primes they exist by the Weil bound $\#C(\mathbb{F}_p) \geq p + 1 - 6\sqrt{p} > 0$, valid for $p \geq 37$. Smooth points lift to $C(\mathbb{Q}_p)$ by Hensel's lemma. The sets $C(\mathbb{F}_2)$ and $C(\mathbb{F}_3)$ are found by enumeration. (iii) is a direct substitution. □

There are 6 points in $C(\mathbb{F}_7)$; they are listed in Table 10.

### 6.9.3 Projective graphs of order 3

Let $H_i \in \mathcal{O}_K[x,y,z]$, $i \in V$, be primitive forms of degrees $d_i \in \{1,2,3\}$, let $E$ be a set of pairs $(i,j)$, $i<j$, with weights $e_{ij} \in \{1,2\}$, and let $c_i \in K^\times$. Put $\rho_{ij} = e_{ij}$ and $\rho_{ji} = -e_{ij}$ for $(i,j) \in E$, $\rho_{ij} = 0$ for non-adjacent $i,j$, and

$$G_i = c_i \prod_j H_j^{\rho_{ij}}.$$

The vertices are of four types: lines (type L), conics through $P_a$ (type A), conics through $P_b$ (type B), and cubics through both $P_a$ and $P_b$ (type K). The *residual scheme* $Z_i$ is the intersection of $C$ with $H_i = 0$, minus $P_a$ for type A, minus $P_b$ for type B, and minus $P_a + P_b$ for type K. We consider the following conditions.

(H) $\sum_j \rho_{ij} d_j \equiv 0 \pmod 3$ for every $i$, and $\prod_i c_i^{d_i} \in K^{\times 3}$.

(V) Every $Z_i$ is reduced (all its intersection multiplicities are 1), and $G_i(Q)$ is a non-zero cube in $\kappa(Q)$ at each closed point $Q$ of $Z_i$. The neighbouring forms are required to be nonzero there.

(P) For $s = a, b$, the curves through $P_s$ meet $C$ transversally there, the other vertices do not vanish at $P_s$, and

$$R_s = \prod_{(i,j)\in E} T_{ij}^{e_{ij}} \prod_{i:\, H_i(P_s)=0} c_i^{-1} \in \kappa(P_s)^{\times 3},$$

where $T_{ij}$ is $u_i/u_j$, $1/u_j$, $u_i$ or 1 according as both, only $H_i$, only $H_j$ or neither of $H_i, H_j$ vanish at $P_s$. Here $u_i = J_i/J_0$ if $H_i(P_s) = 0$, with $J_i = \partial_x H_i\, \partial_y F - \partial_y H_i\, \partial_x F$ at the point of Lemma 6.9.3(iii) and $J_0$ the same quantity for a fixed curve through $P_s$, and $u_i = H_i(P_s)$ otherwise.

In (V), $G_i(Q)$ is evaluated at coordinates of $Q$ in $\kappa(Q)$; by the first part of (H) its class modulo cubes does not depend on the choice of coordinates.

**Proposition 6.9.4.** *Assume (H), (V) and (P). For every linear form $\ell$ the class*

$$\beta = \sum_{(i,j)\in E} e_{ij} \big(H_i/\ell^{d_i}, H_j/\ell^{d_j}\big)_\omega + \sum_i \big(H_i/\ell^{d_i}, c_i\big)_\omega \in \mathrm{Br}\big(K(C)\big)[3]$$

*lies in $\mathrm{Br}(C_K)$ and does not depend on $\ell$. For every place $w$ of $K$ and every $P \in C(K_w)$ at which no $H_i$ vanishes, $\iota(\mathrm{inv}_w\, \beta(P)) = \varepsilon B_w(P)$, where*

$$B_w(P) = \sum_{(i,j)\in E} e_{ij}\, \beta_w\big(H_i(P), H_j(P)\big) + \sum_i \beta_w\big(H_i(P), c_i\big) \in \mathbb{Z}/3$$

*for any coordinates of $P$.*

*Proof.* We write $(f,g)$ for $(f,g)_\omega$. If $\ell$ is replaced by $\ell'$ and $u = \ell/\ell'$, bilinearity, $(a,b) = -(b,a)$ and $(u,u) = (u,-1) = 0$ show that $\beta$ changes by $\sum_i \big(\sum_j \rho_{ij} d_j\big)(H_i/\ell^{d_i}, u) + (u, \prod_i c_i^{d_i})$, which vanishes by (H). The same computation with (K1) shows that $B_w(\mu P) = B_w(P)$ for $\mu \in K_w^\times$.

A class of $\mathrm{Br}(K(C))[3]$ lies in $\mathrm{Br}(C_K)$ if its residue in $\kappa(Q)^\times/\kappa(Q)^{\times 3}$ vanishes at every closed point $Q$ of $C_K$ [CTS21, Ch. 3]. Choose $\ell$ with $\ell(Q) \neq 0$ and put $f_i = H_i/\ell^{d_i}$. The residue of $(f,g)$ at $Q$ is the class of $(-1)^{v(f)v(g)} f^{v(g)}/g^{v(f)}$ evaluated at $Q$, up to a sign that depends only on the normalisation [GS06, Ch. 6], and $-1$ is a cube. If no $H_i$ vanishes at $Q$, all terms are units at $Q$ and the residue is trivial. If $Q \in Z_i$, then $v_Q(f_i) = 1$ since $Z_i$ is reduced, $f_j(Q) \neq 0$ for the neighbours $j$ of $i$ by the nonvanishing check in (V), and the terms containing $f_i$ contribute $G_i(Q)^{-1}$. If $Q$ also lies on residual schemes of other vertices, these are pairwise non-adjacent by the same argument, and their contributions multiply. So the residue is a cube by (V). At $P_s$ take $\ell = z$ and write $f_i = \pi u_i$ for the curves through $P_s$, where $\pi = f_0$ is the fixed one; then $u_i(P_s) = J_i/J_0$, since both functions vanish simply, and the residue is the class of $R_s$, a cube by (P). Hence $\beta$ is unramified on $C_K$. At a point $P$ at which the $f_i$ are defined and non-zero, $\beta(P)$ is the sum of the cyclic algebras of the values, and (K5) gives the formula for $B_w$. □

### 6.9.4 The certificate

Our graph has 33 vertices: 17 lines, 8 conics of type A, 7 conics of type B and the cubic

$$H_K = \lambda x^2 y + x^2 z - (1+3\omega)xy^2 + \lambda xyz + \lambda xz^2 + \omega^2 y^3 + y^2 z - (1+2\omega)yz^2 + z^3,$$

and it has 183 edges, 99 of weight 1 and 84 of weight 2. Every vertex has between 6 and 20 neighbours. All coefficients of the vertex forms are of the form $a + b\omega$ with $|a|, |b| \leq 3$. The constants are products of

$$\omega, \quad \lambda = 1 - \omega, \quad 2, \quad \bar{\pi}_7 = -1 + 2\omega,$$

of norms 1, 3, 4, 7; 24 of the 33 constants are non-trivial, and the constant of $H_K$ is $2^2$. The full graph is given in Tables 11 and 12. Let $\beta$ be the class of Proposition 6.9.4 and, for a place $v$ of $\mathbb{Q}$ and $P \in C(\mathbb{Q}_v)$ at which no $H_i$ vanishes, put

$$B_v(P) = \sum_{w|v} B_w(P) \in \mathbb{Z}/3.$$

**Proposition 6.9.5.** *The graph satisfies (H), (V) and (P). Every residual scheme $Z_i$ is a single closed point of $C_K$, of degree* 4, 5, 5 *and* 6 *over $K$ for the types L, A, B and K. Hence $\beta \in \mathrm{Br}(C_K)[3]$, and no vertex vanishes at a rational point of $C$.*

*Proof.* (H) is a check of the exponents of the weights and of the constants; the constants are cubes exactly when all exponents of the four generators are divisible by 3, since the generators are a unit that is not a cube and three pairwise non-associate primes. For (V), the record `cert_unram.json` gives, for each vertex, a closed point $Q$ of $C_K$ by its field $\kappa(Q)$ and its coordinates, together with a cube root $r_i$ of $G_i(Q)$. One checks that $Q$ lies on $C$ and on $H_i = 0$, that the coordinates generate $\kappa(Q)$ over $K$, that $C$ and $H_i = 0$ meet transversally at $Q$, and that the degree of $Q$ over $K$ is $4d_i$ minus 3 for each special point on $H_i$; at the special points the intersection is transversal as well, by (P) below. By Bézout's theorem $Q$ is then the whole residual scheme $Z_i$, and $Z_i$ is reduced. Finally we check $r_i^3 = G_i(Q)$ using signed representatives $0, 1, -1$ of the weights and constant exponents. Changing any representative multiplies the evaluated expression by an explicit cube. For (P), the fields $\kappa(P_s)$ have degree 3 over $K$; the curves through $P_s$ are the 8 conics of type A and $H_K$ for $s = a$, and the 7 conics of type B and $H_K$ for $s = b$; all of them are transversal to $C$ at $P_s$, and $R_s$ has a cube root in $\kappa(P_s)$, again checked exactly. So $\beta \in \mathrm{Br}(C_K)$ by Proposition 6.9.4. A rational point of $C$ is a closed point of $C_K$ of degree 1. The zeros of $H_i$ on $C_K$ are $Z_i$ and the special points $P_a$, $P_b$, of degrees at least 4 and 3, so no $H_i$ vanishes at a rational point. □

### 6.9.5 Places outside $S = \{2, 3, 7\}$

**Proposition 6.9.6.** *$B_\infty = 0$ on $C(\mathbb{R})$, and $B_p = 0$ on $C(\mathbb{Q}_p)$ for every prime $p \notin \{2, 3, 7\}$.*

*Proof.* The only place of $K$ above $\infty$ is complex, so $B_\infty = 0$ by (K2).

Let $p \notin \{2, 3, 7\}$, and let $w \mid p$ be a place of $K$, with ring of integers $\mathcal{O}_w$. Since $p \neq 3$, $K_w/\mathbb{Q}_p$ is unramified. Let $\mathcal{X} = \operatorname{Proj} \mathbb{Z}_p[x, y, z]/(F)$ and $\mathcal{Y} = \mathcal{X} \otimes_{\mathbb{Z}_p} \mathcal{O}_w$. By Lemma 6.9.3(i), $\mathcal{X}$ is regular, so $\mathcal{Y}$ is regular (it is étale over $\mathcal{X}$); it is proper and flat over $\mathcal{O}_w$, with generic fibre $C_{K_w}$ and special fibre $\mathcal{Y}_k$, which is integral since the reduction of $C$ is geometrically integral (Lemma 6.9.3(i)). All $c_i$ are units at $w$, since their norms involve only 2, 3 and 7. Each $H_i$ is primitive, so its reduction is a non-zero form of degree at most 3, which does not vanish identically on the integral quartic $\mathcal{Y}_k$. Take for $\ell$ a coordinate; it does not vanish identically on $\mathcal{Y}_k$ either. Then every $H_i/\ell^{d_i}$ and every $c_i$ is a unit at the generic point of $\mathcal{Y}_k$, and the residue of $\beta$ along $\mathcal{Y}_k$ is trivial. The residues along the other prime divisors of $\mathcal{Y}$, the closures of the closed points of $C_{K_w}$, are trivial by Proposition 6.9.5. Since $\mathcal{Y}$ is regular of dimension 2 and 3 is invertible on $\mathcal{Y}$, purity [CTS21, Ch. 3] gives $\beta \in \operatorname{Br}(\mathcal{Y})$. By properness, $P \in C(\mathbb{Q}_p) \subseteq C(K_w)$ extends to a point of $\mathcal{Y}(\mathcal{O}_w)$, so $\beta(P) \in \operatorname{Br}(\mathcal{O}_w) = 0$. Hence $\operatorname{inv}_w \beta(P) = 0$ for every $w \mid p$, and $B_p(P) = 0$ by Proposition 6.9.4. □

### 6.9.6 The places in $S$

The values at 2, 3 and 7 are computed by covering $C(\mathbb{Q}_p)$ with small discs on which $B_p$ is visibly constant. The following lemma uses only the properties (K1)–(K3) of the symbols.

**Lemma 6.9.7** (discs)**.** *At a prime $p \in \{2, 3, 7\}$, let $\bar{P} \in C(\mathbb{F}_p)$, let $\ell$ be a coordinate which does not vanish at $\bar{P}$, $s$ a coordinate with $F_s(\bar{P}) \not\equiv 0 \pmod p$, and $u$ the third coordinate. Every point of $C(\mathbb{Q}_p)$ which reduces to $\bar{P}$ can be written $P(U)$ with $\ell = 1$, $u = u_0 + pU$, $U \in \mathbb{Z}_p$, and $s = s(U)$, where $s(U) - s(U') \in p(U - U')\mathbb{Z}_p$. Let $D = \{U \in \mathbb{Z}_p : U \equiv U_0 \pmod{p^k}\}$, $P_0 = P(U_0)$, and let $w \mid p$ be a place of $K$.*

*(a) If $w \neq \lambda$ and $k \geq v_w(H_i(P_0))$, or if $w = \lambda$ and $2k \geq v_\lambda(H_i(P_0)) + 2$, then $H_i(P)/H_i(P_0)$ is a cube in $K_w$ for all $P \in D$.*

*(b) Let $I$ be the set of vertices for which (a) does not apply. If no edge joins two vertices of $I$, and $G_i(P_0) \in K_w^{\times 3}$ for every $i \in I$, then $B_w$ is constant on $D$ (at the points where it is defined), equal to*

$$\sum_{(i,j)\in E,\ i,j\notin I} e_{ij}\, \beta_w\big(H_i(P_0), H_j(P_0)\big) + \sum_{i\notin I} \beta_w\big(H_i(P_0), c_i\big).$$

*(c) Suppose that $D$ contains a point $Q$ of $P_s$, that (a) applies to the vertices which do not vanish at $P_s$, and that for those which vanish at $P_s$, with $J_i = \partial_u H_i\, \partial_s F - \partial_s H_i\, \partial_u F$ at $Q$, $k \geq v_w(J_i) + 1$ if $w \neq \lambda$, and $2k \geq v_\lambda(J_i) + 4$ if $w = \lambda$. Then $B_w$ is constant on $D$, equal to the value at $P_0$ of the graph in which every $H_i$ which vanishes at $P_s$ is replaced by $H_i/H_{i_0}$, for a fixed such $i_0$.*

*Proof. Parametrisation.* Let $\tilde{P} \in \mathbb{Z}^3$ be the lift of $\bar{P}$ with $\ell = 1$ and coordinates $u_0$, $s_0$, and let $e_u$, $e_s$ be the unit vectors of the coordinates $u$, $s$. Since $F(\tilde{P}) \equiv 0 \pmod p$, the polynomial $\Phi(U, S) = p^{-1}F(\tilde{P} + p(Ue_u + Se_s))$ has coefficients in $\mathbb{Z}_p$, and $\partial_S \Phi \equiv F_s(\bar{P})$ is a unit modulo $p$. So Newton's method converges in the Tate algebra $\mathbb{Z}_p\langle U\rangle$ to $S(U)$ with $\Phi(U, S(U)) = 0$, and $s = s_0 + pS(U)$; by Hensel's lemma these are all the points of $C(\mathbb{Q}_p)$ reducing to $\bar{P}$. Elements of $\mathbb{Z}_p\langle U\rangle$ satisfy $|S(U) - S(U')| \leq |U - U'|$. Since the $H_i$ have integral coefficients, $|H_i(P(U)) - H_i(P(U'))|_w \leq |p|\,|U - U'|$. On $D$ we use the chart $\ell = 1$, so that the functions $H_i/\ell^{d_i}$ of Proposition 6.9.4 are the values $H_i(P)$.

(a) For $w \neq \lambda$ the bound gives $H_i(P)/H_i(P_0) \in 1 + w\mathcal{O}_w$ when $k \geq v_w(H_i(P_0))$, and this is a cube by (K3). For $w = \lambda$, $v_\lambda(p) = 2$, so $v_\lambda\big(H_i(P) - H_i(P_0)\big) \geq 2k + 2 \geq v_\lambda(H_i(P_0)) + 4$, and Lemma 6.9.2 applies.

(b) As $I$ contains no edge, every edge touching $i \in I$ joins $i$ to a vertex outside $I$, and bilinearity and $\beta_w(a,b) = -\beta_w(b,a)$ give, at every $P \in D$ at which no $H_j$ vanishes,

$$B_w(P) = B_w^I(P) + \sum_{i \in I} \beta_w\big(H_i(P), G_i(P)\big),$$

where $B_w^I$ is the displayed sum with $P$ in place of $P_0$, made of the edges and constants which do not touch $I$. The factors of $G_i$ are the neighbours of $i$, which are not in $I$, so by (a) $G_i(P)$ is a cube times $G_i(P_0)$, hence a cube; so the second sum vanishes on $D$. By (a), $B_w^I$ is constant on $D$.

(c) Let $T$ be the set of vertices through $P_s$ and $g_i = H_i/H_{i_0}$ for $i \in T$. Substituting $H_i = H_{i_0} g_i$ and expanding bilinearly, using $\beta_w(a,a) = \beta_w(a,-1) = 0$, gives $B_w(P) = B'_w(P) + \beta_w\big(H_{i_0}(P), R(P)\big)$, where $B'_w$ is the sum for the modified graph and $R$ is the product built from the $g_i$, $i \in T$, and the $H_j$, $j \notin T$, in the same way as $R_s^{-1}$ is built in (P) from the $u_i$. Write $Q = P(U_Q)$. Since $H_i(P(U_Q)) = 0$, we have $H_i(P(U)) = p(U - U_Q)D_i(U)$ with $D_i \in \mathcal{O}_w\langle U\rangle$ and $D_i(U_Q) = J_i/F_s(Q)$, where $F_s(Q)$ is a unit. The condition on $k$ gives $D_i(U)/D_i(U_Q) \in K_w^{\times 3}$ on $D$, as in (a), so the $g_i$ are constant modulo cubes on $D$, and they extend continuously to $Q$, where $g_i(Q) = J_i/J_{i_0}$. So $R$ is constant modulo cubes on $D$, and $R(Q)$ is the image of $R_s^{-1}$ in $K_w$ (computed with $J_0 = J_{i_0}$; $R_s$ does not depend on this choice), a cube by (P). Hence $\beta_w(H_{i_0}(P), R(P)) = 0$ on $D$, and $B'_w$ is constant on $D$ by (a) and the constancy of the $g_i$. □

At $w \neq \lambda$ the values in (b) and (c) are computed with (17), and at $\lambda$ with the bilinear form of Section 6.9.1. The centre $P_0$ is computed modulo $p^{60}$, which is far more than needed; if some $H_i$ vanishes to high order at a chosen centre, another point of the disc is taken as centre.

**Proposition 6.9.8.** *For $p = 2, 3, 7$ the function $B_p$ is constant on $C(\mathbb{Q}_p)$, with the values*

$$B_2 = 2, \qquad B_3 = 0, \qquad B_7 = 2.$$

*Proof.* For each point $\bar{P} \in C(\mathbb{F}_p)$ the computation starts with the disc $k = 0$ (the whole residue disc), applies Lemma 6.9.7, and splits a disc into $p$ discs of level $k+1$ whenever none of (a)–(c) settles it. The process stops for every disc. Table 10 lists, for each $\bar{P}$, the number of final discs, the largest level and the value; at each prime all values agree. The cubic points have the following points over $\mathbb{Q}_p$, $p \in S$: $P_a$ has one point in $C(\mathbb{Q}_7)$, in the residue disc of $(4:5:1)$, and $P_b$ has one point in $C(\mathbb{Q}_3)$, in the disc of $(1:1:1)$. Neither has a point in $C(\mathbb{Q}_2)$, as both cubics are irreducible modulo 2. The discs which contain these points are settled by (c), at the levels 1 and 3 respectively. The residual points $Z_i$ may also have points over $\mathbb{Q}_p$; near them (a) fails for $H_i$, and the discs are settled by (b), since $G_i$ is a cube at $Q \in Z_i$ by (V). □

| $p$ | $\bar{P} \in C(\mathbb{F}_p)$ | discs | largest level | settled by (c) | $B_p$ |
|---|---|---|---|---|---|
| 2 | $(1:0:1)$ | 5 | 3 | – | 2 |
| 3 | $(1:1:1)$ | 67 | 5 | $P_b$, level 3 | 0 |
| 7 | $(0:2:1)$ | 13 | 2 | – | 2 |
| | $(1:3:1)$ | 13 | 2 | – | 2 |
| | $(2:6:1)$ | 19 | 2 | – | 2 |
| | $(4:5:1)$ | 13 | 2 | $P_a$, level 1 | 2 |
| | $(5:2:1)$ | 25 | 3 | – | 2 |
| | $(5:1:0)$ | 19 | 2 | – | 2 |

Table 10: The local values of Proposition 6.9.8: for each point of $C(\mathbb{F}_p)$, the number of final discs of Lemma 6.9.7 covering its residue disc in $C(\mathbb{Q}_p)$, the largest level $k$ among them, the disc containing a point of $P_a$ or $P_b$, and the value of $B_p$. In total there are 5, 67 and 102 discs at $p = 2, 3, 7$.

*Proof of Theorem 6.9.1.* Let $P = (x : y : z) \in C(\mathbb{Q})$. By Proposition 6.9.5, no $H_i$ vanishes at $P$, so all the values $H_i(P)$ are in $K^\times$. By the product formula (K4), applied to each symbol in the definition of $B_w$,

$$\sum_w B_w(P) = 0,$$

where the sum is over all places of $K$; equivalently $\sum_v B_v(P) = 0$, the sum over the places of $\mathbb{Q}$. By Propositions 6.9.6 and 6.9.8,

$$\sum_v B_v(P) = B_2(P) + B_3(P) + B_7(P) = 2 + 0 + 2 = 4 \not\equiv 0 \pmod 3,$$

a contradiction. Hence $C(\mathbb{Q}) = \emptyset$, and $F = 0$ has only the integer solution $(0, 0, 0)$. □

By (K5) and Proposition 6.9.4, $\mathcal{A} = \mathrm{Cor}_{K/\mathbb{Q}}\,\beta \in \mathrm{Br}(C)[3]$ satisfies $\iota(\mathrm{inv}_v\,\mathcal{A}(P)) = \varepsilon B_v(P)$, and the computation shows that $\sum_v \mathrm{inv}_v\,\mathcal{A}(P)$ is the constant $\varepsilon/3 \neq 0$ on $\prod_v C(\mathbb{Q}_v)$. So $\mathcal{A}$ gives a Brauer–Manin obstruction.

*Remark.* The local symbol calculations use (K1)–(K5) and Hensel's lemma. Proposition 6.9.4 uses the residue formula for a symbol and purity for the Brauer group of a smooth curve. Proposition 6.9.6 uses prime-to-residue-characteristic purity on a regular surface and the vanishing of $\mathrm{Br}(\mathcal{O}_w)$. The geometric checks use the Weil bound and Bézout's theorem (Lemma 6.9.3 and Proposition 6.9.5). Newton iteration in a Tate algebra gives the disc parametrizations in Lemma 6.9.7. Once the local values are known, the contradiction follows directly from cubic reciprocity (K4), independently of the Mordell–Weil group of the Jacobian.

### 6.9.7 The forms, constants and weights

The vertices are numbered from 1 to 33. Vertices 1–17 are the lines, 18–25 the conics of type A, 26–32 the conics of type B, and 33 is the cubic $H_K$ of Section 6.9.4. Coefficients are written $a + b\omega$. The constant $c_i$ is a product of the generators $\omega$, $\lambda = 1 - \omega$, 2 and $\bar{\pi}_7 = -1 + 2\omega$.

Table 11: Vertex forms and constants of the cubic obstruction.

| $i$ | type | $H_i$ | $c_i$ |
|---|---|---|---|
| 1 | L | $x - y + z$ | $1$ |
| 2 | L | $x + \omega y + z$ | $\omega \cdot \lambda$ |
| 3 | L | $x - \omega y + z$ | $1$ |
| 4 | L | $(-1 - \omega)x + y$ | $\omega^2 \cdot 2$ |
| 5 | L | $-\omega x + z$ | $\omega^2 \cdot \lambda$ |
| 6 | L | $(1 + \omega)x + z$ | $\omega^2$ |
| 7 | L | $\omega x + z$ | $1$ |
| 8 | L | $x + y$ | $\omega^2 \cdot 2^2$ |
| 9 | L | $x$ | $\omega^2$ |
| 10 | L | $-x + (-1 - \omega)y + z$ | $\omega^2$ |
| 11 | L | $-\omega y + z$ | $\omega \cdot 2^2 \cdot \bar{\pi}_7^2$ |
| 12 | L | $z$ | $\omega^2$ |
| 13 | L | $x + z$ | $\omega$ |
| 14 | L | $-\omega x + (-1 - \omega)y + z$ | $\lambda^2$ |
| 15 | L | $-y + 2z$ | $2 \cdot \bar{\pi}_7$ |
| 16 | L | $(1 + \omega)x + y$ | $\omega^2 \cdot 2^2$ |
| 17 | L | $-\omega x + y$ | $\omega^2$ |
| 18 | A | $\omega x^2 + (-1 - \omega)xz - y^2 - \omega yz + z^2$ | $\lambda^2 \cdot 2$ |
| 19 | A | $(-1 - \omega)x^2 + \omega xz - y^2 + (1 + \omega)yz + z^2$ | $\lambda$ |
| 20 | A | $-x^2 - xy - y^2 + yz$ | $1$ |
| 21 | A | $-x^2 + \omega xy + (1 + \omega)xz + \omega y^2 + yz$ | $\omega$ |
| 22 | A | $\omega x^2 + (1 + \omega)xy + \omega y^2 - \omega yz + z^2$ | $\omega$ |
| 23 | A | $xy + xz + y^2$ | $1$ |
| 24 | A | $-x^2 + xy + xz + yz + z^2$ | $1$ |
| 25 | A | $x^2 + (2 + \omega)xy + \omega xz + (1 + \omega)y^2 - yz + z^2$ | $1$ |

| $i$ | type | $H_i$ | $c_i$ |
|---|---|---|---|
| 26 | B | $xy + y^2 + z^2$ | $\omega$ |
| 27 | B | $x^2 + xy + (1+\omega)xz + (-1-\omega)y^2 + yz$ | 1 |
| 28 | B | $x^2 + 2xy + y^2 + yz + z^2$ | 1 |
| 29 | B | $-\omega x^2 + (1-\omega)xy + y^2 - \omega yz + z^2$ | $\lambda^2$ |
| 30 | B | $x^2 + xy + yz$ | $\omega$ |
| 31 | B | $x^2 + 2xy + xz + yz + z^2$ | $\omega \cdot \lambda^2$ |
| 32 | B | $(-1-\omega)x^2 - \omega xy - \omega xz + (1+\omega)y^2 + (-1-\omega)yz + z^2$ | $\omega \cdot 2$ |
| 33 | K | $(1-\omega)x^2y + x^2z + (-1-3\omega)xy^2 + (1-\omega)xyz + (1-\omega)xz^2 + (-1-\omega)y^3 + y^2z + (-1-2\omega)yz^2 + z^3$ | $2^2$ |

Each edge $(i, j)$, $i < j$, is listed once, in the row of $i$, under its weight $e_{ij}$; it contributes $e_{ij}\,\beta_w(H_i(P), H_j(P))$ to $B_w(P)$.

Table 12: Edges of the cubic obstruction, grouped by initial vertex and weight.

| $i$ | $e_{ij} = 1$ | $e_{ij} = 2$ |
|---|---|---|
| 1 | 9, 20, 30, 32 | 6, 10, 15, 19, 24 |
| 2 | 4, 5, 6, 9, 19 | 13, 24, 29, 30, 31 |
| 3 | 11, 20, 23, 25, 26, 29 | 12, 19, 21, 27, 28, 30, 33 |
| 4 | 6, 18, 23, 27, 32 | 16, 17, 19, 26, 30 |
| 5 | 11, 14, 16, 18, 20, 27 | 8, 13, 25, 26, 30, 33 |
| 6 | 13, 17, 19, 20, 22 | 23, 29 |
| 7 | 9, 11, 17, 21, 30 | 19, 20 |
| 8 | 15, 18, 23, 28, 29 | 19, 24, 25, 26, 32 |
| 9 | 19, 20, 27, 31, 32 | 12, 21, 23, 28 |
| 10 | 26, 29 | 14, 19, 30 |
| 11 | 15, 17, 18, 19, 20, 26, 29 | 24, 30, 32 |
| 12 | 14, 17, 18, 24, 25, 26 | 19, 31, 32 |
| 13 | 14, 15, 16, 22, 24, 26, 28 | – |
| 14 | 22, 31, 33 | 16, 26, 29 |
| 15 | 20, 28, 30 | 18, 19 |
| 16 | 23, 28, 33 | 30, 31 |
| 17 | 28 | 26 |
| 18 | 19, 27, 31 | 32, 33 |
| 19 | 28, 33 | 20, 23, 24, 26, 32 |
| 20 | 21 | 22, 24, 26, 27, 29 |
| 21 | 22, 33 | 23, 29 |
| 22 | 27, 29 | 26, 30 |
| 23 | 31, 33 | 27, 28 |
| 24 | 27, 31, 33 | 30, 32 |
| 25 | 30 | 26 |
| 26 | 27, 33 | 29, 31 |
| 27 | 33 | – |
| 29 | 31 | 32, 33 |
| 31 | 32 | 33 |

# 7 Homogeneous surfaces and diagonal quintics

The first three cubic surfaces are excluded by cubic reciprocity, and the diagonal quartic by Hilbert reciprocity. The remaining six equations use the common Frey-curve framework below.

## 7.1 $x^3 + 2x^2y + y^3 + y^2z + xz^2 + z^3 + t^2x - t^2y - t^2z + tyz + t^3 = 0$ **(**$H = 96$**)**

**Theorem 7.1.1.** *The only integer solution of*

$$F(x, y, z, t) := x^3 + 2x^2y + y^3 + y^2z + xz^2 + z^3 + t^2x - t^2y - t^2z + tyz + t^3 = 0$$

*is* $(0,0,0,0)$.

**Setup.** Let $S \subset \mathbb{P}^3$ be the cubic surface $F = 0$. We prove that $S(\mathbb{Q}) = \varnothing$ by a Brauer–Manin obstruction of order 3 (Proposition J). Let

$$K = \mathbb{Q}(s), \quad s^2 = -23, \qquad h(T) = T^3 - T + 1, \qquad L = K(a), \quad h(a) = 0,$$

let $\tau(a) = -\big(23a + s(6a^2 + 9a - 4)\big)/46 \in L$ (by Lemma 7.1.2(i), $a \mapsto \tau(a)$ defines a generator $\tau$ of $\mathrm{Gal}(L/K)$), and let $G$ be the cubic form

$$\begin{aligned} G = {} & (102 - 18s)x^2y - (281 + 13s)x^2z - (119 + 19s)x^2t + 288xy^2 + (124 - 4s)xyz - (416 - 32s)xyt \\ & + (75 - 9s)y^3 + (107 - 41s)y^2z + (112 - 16s)y^2t \\ & + (59 - 89s)(xz^2 + xt^2 + yzt - yt^2 + z^3 - zt^2 + t^3). \end{aligned}$$

We write $G = G_0 + sG_1$ with $G_0, G_1 \in \mathbb{Z}[x,y,z,t]$. If a prime $p$ splits in $K$, then for each of the two places $w \mid p$ of $K$ we have $K_w = \mathbb{Q}_p$, $s \mapsto \sigma_w \in \mathbb{Z}_p$ with $\sigma_w^2 = -23$, and we put $G^{(w)} = G_0 + \sigma_w G_1 \in \mathbb{Z}_p[x,y,z,t]$; $\bar{w}$ denotes the other place above $p$. Points of $S(\mathbb{Q}_p)$ are always given by primitive coordinates in $\mathbb{Z}_p^4$, and $\bar{P}$ is the reduction of $P$ modulo $p$. Local invariants $\mathrm{inv}_w$ and Frobenius elements $\mathrm{Frob}_w \in \mathrm{Gal}(L/K)$ are those of [Neu99, Chapters V–VI].

The proof goes as follows. We construct a twisted cubic $C \subset S_L$ with $\mathrm{div}_S(G) = C + \tau C + \tau^2 C$ (Step 2), so that the cyclic algebra $\mathcal{B} = (L/K, \tau, G/(288x^3))$ lies in $\mathrm{Br}(S_K)$ (Step 3). After determining the reduction of $S$ modulo all primes (Step 4), we show that for every prime $p$ and every $P \in S(\mathbb{Q}_p)$ the sum of the local invariants of $\mathcal{B}(P)$ at the places above $p$ is 0 if $p \neq 3$ (Step 5) and $2/3$ if $p = 3$ (Step 6). At a rational point the sum over all places would be 0 (Step 7).

**Step 1: the fields.**

**Lemma 7.1.2.** *(i) $h$ is irreducible over $K$. Put $\tau^2(a) := -\big(23a - s(6a^2 + 9a - 4)\big)/46$ (the expression for $\tau(a)$ with $s$ replaced by $-s$). Then $a, \tau(a), \tau^2(a)$ are the three roots of $h$ in $L$, and the $K$-automorphism $\tau$ of $L$ with $a \mapsto \tau(a)$ maps $\tau(a)$ to $\tau^2(a)$ and $\tau^2(a)$ to $a$. Hence $L/K$ is cyclic of degree 3 and $\mathrm{Gal}(L/K) = \langle\tau\rangle$.*

*(ii) Let $w$ be a place of $K$ above a prime $p$. If $p$ is inert in $K$ or $p = 23$, then $h$ splits into linear factors over $K_w$, so $L \otimes_K K_w \cong K_w^3$. If $p$ splits in $K$, then either $h \bmod p$ has three distinct roots and $L \otimes_K K_w \cong K_w^3$, or $h \bmod p$ is irreducible; in the latter case $L_w := L \otimes_K K_w$ is the unramified cubic extension of $K_w = \mathbb{Q}_p$, $\mathrm{Frob}_w = \tau^e$ and $\mathrm{Frob}_{\bar{w}} = \tau^{-e}$ for some $e \in \{1,2\}$. In particular $L/K$ is unramified at all places.*

*(iii) The primes $2, 3, 29, 31$ split in $K$, and $h$ is irreducible modulo each of them; $59$ splits in $K$, and $h$ has the roots $17, 46, 55$ modulo $59$; $7, 337, 9013$ are inert in $K$. Let $w_+$ and $w_-$ be the places of $K$ above 3 with $\sigma_{w_+} \equiv 2$ and $\sigma_{w_-} \equiv -2 \pmod{27}$. Then $\mathrm{Frob}_{w_+} = \tau$ and $\mathrm{Frob}_{w_-} = \tau^2$.*

*Proof.* (i) $h(\pm 1) \neq 0$, so $h$ is irreducible over $\mathbb{Q}$, and a root in the quadratic field $K$ would generate a cubic subfield. That $\tau(a)$ is a root of $h$ and that $\tau(\tau(a)) = \tau^2(a)$, $\tau(\tau^2(a)) = a$ are identities in $L$ (certificate 1.4.1a).

(ii) We have $\mathrm{disc}\, h = -23$. Let $p \neq 2, 23$, and let $\delta = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$ for the roots $r_i$ of $h \bmod p$ in $\bar{\mathbb{F}}_p$. Then $\delta^2 = -23 \neq 0$, and the Frobenius $u \mapsto u^p$ maps $\delta$ to $\pm\delta$ according to the parity of the permutation it induces on the roots. Hence $h \bmod p$ has exactly one root if $\left(\frac{-23}{p}\right) = -1$, and three roots or none if $\left(\frac{-23}{p}\right) = 1$. If $p$ is inert, Hensel's lemma gives $h = (T - r)g(T)$ over $\mathbb{Z}_p$, and $\mathrm{disc}\, g \cdot g(r)^2 = \mathrm{disc}\, h = -23$ shows that $g$ splits over $K_w = \mathbb{Q}_p(\sqrt{-23})$. Modulo 23 we have $h \equiv (T - 20)(T - 13)^2$ with coprime factors, and the same argument applies, with $g(r) \equiv (20 - 13)^2 \equiv 3 \pmod{23}$ a unit. If $p$ splits and $h \bmod p$ has three roots, they lift to $\mathbb{Z}_p$. If $h \bmod p$ is irreducible, $L \otimes_K K_w \cong \mathbb{Q}_p[T]/(h)$ ($a \mapsto T$, $s \mapsto \sigma_w$) is the unramified cubic extension of $\mathbb{Q}_p$, and $\tau$ acts on it as the automorphism $\alpha_w \colon T \mapsto P(T, \sigma_w)$, $P(T,s) = -(23T + s(6T^2 + 9T - 4))/46$; $\alpha_w \neq 1$ because $\tau(a) \neq a$. By (i), $P(P(a,s),s) = \tau^2(a) = P(a,-s)$, so $\alpha_{\bar{w}} = \alpha_w^2$ on $\mathbb{Q}_p[T]/(h)$. If

$\alpha_w = \varphi^k$ for the Frobenius $\varphi$ of $\mathbb{Q}_p[T]/(h)$, then $\mathrm{Frob}_w = \tau^e$ with $e \equiv k^{-1}$ and $\mathrm{Frob}_{\bar{w}} = \tau^{e'}$ with $e' \equiv (2k)^{-1} \equiv -e \pmod 3$. For $p = 2$ we have $-23 \equiv 1 \pmod 8$, so 2 splits in $K$, and $h$ mod 2 has no root, so it is irreducible. Finally, $L \otimes_K K_w$ is unramified over $K_w$ for $p \neq 23$ because $h$ mod $p$ is separable, and for $p = 23$ because it is split.

(iii) The splitting data are computed by certificate 1.4.1a. In $\mathbb{F}_{27} = \mathbb{F}_3[T]/(h)$ we have $P(T,2) \equiv T + 2 \equiv T^3$ and $P(T,-2) \equiv T + 1 \equiv T^9$ (certificate 1.4.1a), so $\alpha_{w_+} = \varphi$ and $\alpha_{w_-} = \varphi^2$. □

**Step 2: the twisted cubic.** Let $q_0, q_1, q_2$ be the three quadratic forms over $L$ recorded in `data/cubic_a_quadrics.json` of certificate 1.4.1b. Every monomial of $q_0$ and of $q_1$ contains $x$ or $y$, so on the plane $(x, y) = (\lambda w, \mu w)$ we have

$$q_k(\lambda w, \mu w, z, t) = w\,\big(A_k w + B_k z + C_k t\big) \qquad (k = 0, 1),$$

with binary forms $A_k$ of degree 2 and $B_k, C_k$ of degree 1 in $(\lambda, \mu)$. Put

$$W = B_0 C_1 - C_0 B_1, \qquad Z = C_0 A_1 - A_0 C_1, \qquad T = A_0 B_1 - B_0 A_1,$$
$$\phi\colon \mathbb{P}^1_L \to \mathbb{P}^3_L, \qquad (\lambda : \mu) \mapsto (\lambda W : \mu W : Z : T),$$

so that $W$ is a quadratic and $Z, T$ are cubic binary forms; $(W : Z : T)$ is the common zero of the two linear forms $A_k w + B_k z + C_k t$ $(k = 0, 1)$, and $\phi(\lambda : \mu)$ lies on the plane $\mu x = \lambda y$ through the line $x = y = 0$. For $j = 1, 2$ let $\tau^j\phi$ be the map obtained by applying $\tau^j$ to the coefficients of $\phi$, so that $(\tau^j\phi)(\mathbb{P}^1) = \tau^j(\phi(\mathbb{P}^1))$.

**Lemma 7.1.3.** *(i)* $\phi^* q_0 = \phi^* q_1 = \phi^* q_2 = 0$, $\phi^* F = 0$ *and* $\phi^* G = 0$.

*(ii) The four binary cubics* $\lambda W, \mu W, Z, T$ *are linearly independent over* $L$. *Hence* $C := \phi(\mathbb{P}^1_L)$ *is a twisted cubic: a smooth, geometrically integral curve of degree 3 and genus 0. It lies on* $S_L$, *on the cubic surface* $G = 0$ *and on the three quadrics* $q_k = 0$.

*(iii) For* $j = 1, 2$ *the binary form* $q_0(\tau^j\phi)$ *is not* 0. *Hence* $\tau C$ *and* $\tau^2 C$ *do not lie on the quadric* $q_0 = 0$, *and* $C$, $\tau C$, $\tau^2 C$ *are pairwise distinct. The line* $x = y = 0$ *meets* $C$ *in* $P_0 = (0 : 0 : a : 1)$ *and* $P_1 = (0 : 0 : \tau(a) : 1)$, *and* $P_2 = (0 : 0 : \tau^2(a) : 1) \notin C$.

*(iv)* $\mathrm{div}_S(G) = C + \tau C + \tau^2 C$.

*Proof.* (i)–(iii) are exact computations in $L[\lambda, \mu]$ (certificate 1.4.1b). In (ii), four linearly independent binary cubics form a basis of the space of binary cubics, so $\phi$ is the composition of $(\lambda : \mu) \mapsto (\lambda^3 : \lambda^2\mu : \lambda\mu^2 : \mu^3)$ with a projective linear transformation. In (iii), if $\tau C = C$ then $\tau^2 C = C$, which is excluded, and $\tau^2 C \neq \tau C$ follows by applying $\tau$. The points: $\mathrm{Res}(W, Z - aT) = \mathrm{Res}(W, Z - \tau(a)T) = 0$, $\mathrm{Res}(W, Z - \tau^2(a)T) \neq 0$ and $\mathrm{Res}(W, T) \neq 0$ (certificate 1.4.1b).

(iv) $F$ and $G$ have coefficients in $K$, so by (i) all three curves $\tau^j C$ lie on $S$ and on $G = 0$. The coefficient of $x^3$ is 1 in $F$ and 0 in $G \neq 0$, so $G$ is not a multiple of $F$ and does not vanish on the irreducible surface $S$. By Bézout's theorem [Har77, Theorem I.7.7], $\mathrm{div}_S(G)$ (the divisor of $G/\ell^3$ plus three times the plane section $\ell = 0$, for any linear form $\ell$) is an effective divisor of degree $3 \cdot 3 = 9$. It contains the three distinct prime divisors $C, \tau C, \tau^2 C$ of degree 3, so it is their sum. □

**Step 3: the Brauer class.** For a linear form $\ell$ over $K$ let $H_\ell$ be the plane section $\ell = 0$ of $S$. Put $\psi = G/(288x^3) \in K(S)^\times$. By Lemma 7.1.3(iv),

$$\mathrm{div}_S(\psi) = C + \tau C + \tau^2 C - 3H_x = N_{L/K}(C - H_x),$$

so by Proposition J(1) the cyclic algebra $\mathcal{B} = (L/K, \tau, \psi)$ lies in $\mathrm{Br}(S_K)$. Since $G/(288\ell^3) = \psi \cdot (x/\ell)^3$, Proposition J(1) also gives: for every field $K' \supseteq K$, every linear form $\ell$ over $K$ and every $P \in S(K')$ with $G(P)\,\ell(P) \neq 0$ (so that $P$ is not on $C \cup \tau C \cup \tau^2 C \cup H_\ell$),

$$\mathcal{B}(P) = \big(L \otimes_K K'/K',\ \tau,\ G(P)/(288\,\ell(P)^3)\big). \tag{18}$$

**Step 4: reduction modulo primes.**

**Lemma 7.1.4.** *(i) $S$ is smooth. For every prime $p \notin \{2, 3, 23, 31, 59, 9013\}$ the surface $\bar{S}_p\colon F \equiv 0 \pmod p$ is smooth over $\bar{\mathbb{F}}_p$, hence geometrically integral; $\bar{S}_3$ is smooth as well.*

*(ii) Over $\bar{\mathbb{F}}_{31}$, the only singular point of $\bar{S}_{31}$ is $P_{31} = (1 : 23 : 28 : 12)$, and $\bar{S}_{31}$ is geometrically integral. The square roots of $-23$ modulo 31 are 15 and 16, and $G(P_{31}) \equiv 6$ for $s = 15$, $G(P_{31}) \equiv 16$ for $s = 16 \pmod{31}$.*

*(iii) $\bar{S}_p$ is singular for $p = 2, 23, 31, 59, 9013$. Hence these are exactly the primes of bad reduction of $S$.*

*Proof.* (i) For an order of the variables, the Macaulay matrix in degree 5 of the four partial derivatives of $F$ has its 56 rows indexed by the monomials of degree 5, and the column of a monomial $m$ is the coefficient vector of $(m/v^2)\,\partial F/\partial v$, where $v$ is the first variable in the given order with $v^2 \mid m$. If $\xi \in \bar{\mathbb{F}}_p^4 \setminus \{0\}$ is a common zero of the partial derivatives modulo $p$, then the vector $(m(\xi))_m \neq 0$ is in the left kernel of the matrix modulo $p$, so $p$ divides its determinant. For the orders $(x, y, z, t)$ and $(x, y, t, z)$ the determinants are

$$2^6 \cdot 3^{17} \cdot 7 \cdot 23 \cdot 29 \cdot 31 \cdot 59^2 \cdot 337 \cdot 9013^2 \quad \text{and} \quad 2^6 \cdot 3^{19} \cdot 23 \cdot 31 \cdot 59^3 \cdot 73 \cdot 9013^2$$

(certificate 1.4.1c), with greatest common divisor $2^6 \cdot 3^{17} \cdot 23 \cdot 31 \cdot 59^2 \cdot 9013^2$. For $p \neq 3$, Euler's identity $3F = \sum_v v\,\partial F/\partial v$ shows that a singular point of $\bar{S}_p$ is a common zero of the partial derivatives, so $\bar{S}_p$ is smooth for $p \notin \{2, 3, 23, 31, 59, 9013\}$; over $\bar{\mathbb{Q}}$ the same argument shows that $S$ is smooth. A cubic surface that is reducible or non-reduced over $\bar{\mathbb{F}}_p$ is singular along a curve (all partial derivatives of $F_1F_2$ vanish on $V(F_1) \cap V(F_2)$), so a cubic surface with finitely many singular points is geometrically integral.

For $p \in \{3, 31\}$ consider the $\mathbb{F}_p$-linear map $(g_0, g_1, \ldots, g_4) \mapsto g_0F + \sum_i g_i\,\partial F/\partial v_i$ from (forms of degree 2)$\times$(forms of degree 3)$^4$ to the 56-dimensional space of forms of degree 5. A common zero $\xi \neq 0$ of $F$ and its partial derivatives over $\bar{\mathbb{F}}_p$ gives the nonzero linear form "evaluation at $\xi$" on the forms of degree 5, which vanishes on the image, and two distinct points of $\mathbb{P}^3(\bar{\mathbb{F}}_p)$ give two linearly independent linear forms. The rank of the map is 56 for $p = 3$ and 55 for $p = 31$, and $F$ and its partial derivatives vanish at $P_{31}$ modulo 31 (certificate 1.4.1c). This proves the claims on $\bar{S}_3$ and the first claim of (ii); the values of $G$ are computed by certificate 1.4.1c.

(iii) $F$ and its partial derivatives vanish modulo $p$ at $(1 : 18 : 3 : 10)$, $(1 : 23 : 28 : 12)$, $(1 : 47 : 12 : 14)$, $(1 : 7636 : 7996 : 3944)$ for $p = 23, 31, 59, 9013$, and modulo 2 at the three points $(1 : r^3 + r : r^5 : r)$ over $\mathbb{F}_8$, $r^3 + r^2 + 1 = 0$ (certificate 1.4.1c). □

**Step 5: the places not above 3.**

**Lemma 7.1.5.** *Let $p \neq 3$ be a prime and $P \in S(\mathbb{Q}_p)$. Then $\sum_{w \mid p} \mathrm{inv}_w\, \mathcal{B}(P) = 0$, and for $p \neq 2$ each term is 0. At the complex place $w_\infty$ of $K$, $\mathrm{inv}_{w_\infty}\, \mathcal{B}(P) = 0$ for every $P \in S(\mathbb{C})$.*

*Proof.* $\mathrm{Br}(\mathbb{C}) = 0$. If $L \otimes_K K_w \cong K_w^3$, which by Lemma 7.1.2(ii) is the case when $p$ is inert in $K$, when $p = 23$, and when $p$ splits and $h$ mod $p$ has three roots (for example $p = 59$), then $\mathcal{B}(P)$ is split at $w$ ([Neu99, Chapters V–VI]). It remains to treat the primes $p$ that split in $K$ with $h$ mod $p$ irreducible. Then $L_w/\mathbb{Q}_p$ is the unramified cubic extension, $\mathrm{Frob}_w = \tau^e$ and $\mathrm{Frob}_{\bar{w}} = \tau^{-e}$.

$p = 2$. Choose $\ell \in \{x, y, z, t\}$ with $\ell(P) \in \mathbb{Z}_2^\times$. For every primitive solution of $F \equiv 0 \pmod{32}$, $G^{(w)}$ has 2-adic valuation 1 if $\sigma_w \equiv 5 \pmod 8$ and 4 if $\sigma_w \equiv 3 \pmod 8$ (certificate 1.4.1d); since these valuations are less than 5, the same holds at $P$. In particular $G(P) \neq 0$, and by (18) the algebra $\mathcal{B}(P)$ at $w$ is $(L_w/\mathbb{Q}_2, \tau, c_w)$ with $v_2(c_w) = v_2(G^{(w)}(P)) - v_2(288) \in \{-4, -1\}$, so $v_2(c_w) \equiv v_2(c_{\bar{w}}) \equiv 2 \pmod 3$. By [Neu99, Chapters V–VI], $\mathrm{inv}_w\, \mathcal{B}(P) + \mathrm{inv}_{\bar{w}}\, \mathcal{B}(P) = \big(2e + 2(-e)\big)/3 = 0$.

$p \geq 5$ (this covers $p = 29$, $p = 31$ and all primes of good reduction with $h$ mod $p$ irreducible). By Lemma 7.1.4, $\bar{S}_p$ is geometrically integral, and $\bar{P}$ is a smooth point of $\bar{S}_p$ unless $p = 31$ and $\bar{P} = P_{31}$. The reduction of $G^{(w)}$ does not vanish on $\bar{S}_p$: otherwise it would be a multiple of $F$ mod $p$, hence 0 (compare the coefficients of $x^3$), but its coefficient of $xy^2$ is $288 \not\equiv 0$. If $\bar{P}$ is a smooth point, Proposition J(3) (with

$\psi = G/(288\ell^3)$, $\ell$ a coordinate with $\ell(\bar{P}) \neq 0$, and $v_p(288) = 0$) gives $\mathrm{inv}_w \mathcal{B}(P) = 0$. If $p = 31$ and $\bar{P} = P_{31}$, then $x(P)$ is a unit and $G^{(w)}(P) \equiv G^{(w)}(P_{31}) \equiv 6$ or $16 \pmod{31}$ is a unit (Lemma 7.1.4(ii)), so by (18) with $\ell = x$ and [Neu99, Chapters V–VI], $\mathrm{inv}_w \mathcal{B}(P) = e \cdot 0/3 = 0$. □

**Step 6: the places above 3.**

**Lemma 7.1.6.** *For every $P \in S(\mathbb{Q}_3)$ we have $v_3(G^{(w_+)}(P)) = 0$, $v_3(G^{(w_-)}(P)) = 1$, and*

$$\mathrm{inv}_{w_+} \mathcal{B}(P) + \mathrm{inv}_{w_-} \mathcal{B}(P) = \tfrac{2}{3}.$$

*Proof.* The primitive coordinates of $P$ reduce to one of the 10,206 primitive solutions of $F \equiv 0 \pmod{27}$. For each of them, with $\sigma_{w_+} \equiv 2$ and $\sigma_{w_-} \equiv 25 \pmod{27}$, the value of $G^{(w_+)}$ has 3-adic valuation 0 and that of $G^{(w_-)}$ has valuation 1 (certificate 1.4.1e; the same holds for the 275,562 primitive solutions modulo 81). Valuations less than 3 are determined modulo 27, which proves the first claim. Choose $\ell \in \{x, y, z, t\}$ with $\ell(P) \in \mathbb{Z}_3^\times$, and put $c = G(P)/(288\ell(P)^3)$; since $v_3(288) = 2$, $v_{w_+}(c) = -2$ and $v_{w_-}(c) = -1$. By (18), Lemma 7.1.2(iii) and [Neu99, Chapters V–VI],

$$\mathrm{inv}_{w_+} \mathcal{B}(P) = \frac{1 \cdot (-2)}{3} \equiv \frac{1}{3}, \qquad \mathrm{inv}_{w_-} \mathcal{B}(P) = \frac{2 \cdot (-1)}{3} \equiv \frac{1}{3} \pmod{1}.$$

(With the opposite sign convention for the invariants the sum is $1/3$; it is nonzero in either case.) □

**Step 7: conclusion.**

*Proof of Theorem 7.1.1.* Suppose $P \in S(\mathbb{Q})$. Then $P \in S(K)$, and by Proposition J(4), $\sum_w \mathrm{inv}_w \mathcal{B}(P) = 0$, the sum over all places of $K$. Grouping the places by the primes below them, Lemmas 7.1.5 and 7.1.6 give $\sum_w \mathrm{inv}_w \mathcal{B}(P) = 2/3$, a contradiction. Hence $S(\mathbb{Q}) = \varnothing$. A nonzero integer solution would give a rational point of $S$. □

*Remark.* $S$ has points over $\mathbb{R}$ and over every $\mathbb{Q}_p$: at $p = 2, 23, 31, 59, 9013$ the points $(1:0:1:1)$, $(1:0:0:6)$, $(1:0:0:20)$, $(1:0:1:10)$, $(1:0:0:8363)$ are smooth points of $\bar{S}_p$, at $p = 3$ the point $(1:0:0:1)$ is a smooth point of $\bar{S}_3$ (certificate 1.4.1f), at the other primes $\bar{S}_p$ is smooth and has an $\mathbb{F}_p$-point by the Chevalley–Warning theorem, and all of them lift by Hensel's lemma; $F(1,0,0,t) = t^3 + t^2 + 1$ has a real root. So the obstruction is not local. In terms of $\mathcal{A} = \mathrm{Cor}_{K/\mathbb{Q}} \mathcal{B} \in \mathrm{Br}(S)$, whose local invariant at $P \in S(\mathbb{Q}_p)$ is $\sum_{w|p} \mathrm{inv}_w \mathcal{B}(P)$, Steps 5 and 6 say that $\sum_p \mathrm{inv}_p \mathcal{A}(P_p) = 2/3$ for every adelic point $(P_p)$; so $S(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}} = \varnothing$, and the class of $\mathcal{A}$ in $\mathrm{Br}(S)/\mathrm{Br}(\mathbb{Q})$ has order 3.

## 7.2 $2x^3 + x^2y + xy^2 + y^3 + y^2z - 2xz^2 - z^3 + t^2y + tz^2 - t^3 = 0$ ($H = 96$)

**Theorem 7.2.1.** *The only integer solution of*

$$F(x,y,z,t) = 2x^3 + x^2y + xy^2 + y^3 + y^2z - 2xz^2 - z^3 + t^2y + tz^2 - t^3 = 0$$

*is $(x,y,z,t) = (0,0,0,0)$.*

**Setup.** Since $F$ is homogeneous, it suffices to show that the cubic surface $S : F = 0$ in $\mathbb{P}^3$ has no rational point. Let $K = \mathbb{Q}(s)$ with $s^2 = -23$, let $h(T) = T^3 - T + 1$, let $L$ be the splitting field of $h$ over $\mathbb{Q}$, and let $q \in L$ be a root of $h$. Put

$$\ell_\pm = (-1 \pm s)x + 4y, \qquad \rho = -\frac{(s-1)q^2 + 8}{4(3q^2 - 1)}.$$

The plane $\ell_+ = 0$ meets $S$ in three lines that are defined over $L$ and permuted cyclically by $\mathrm{Gal}(L/K)$ (Step 2). For a rational point $P$ of $S$ we put $\psi = \ell_+(P)/\ell_-(P) \in K^\times$ and compute the local invariants $\mathrm{inv}_w(\psi)$ of the cyclic cubic extension $L/K$ ([Neu99, Chapters V–VI]). They vanish at every place of

$K$ except the two places above 2 (Steps 3–4), and there they are equal and nonzero (Step 5), which contradicts the reciprocity law.

For a place $w$ of $K$ we write $K_w$ for the completion and $v_w$ for the normalized valuation. Complex conjugation $c$ is the nontrivial automorphism of $K$, and $c(w)$ is the place with $v_{c(w)}(c(\alpha)) = v_w(\alpha)$. Since $P$ is rational, $c(\ell_+(P)) = \ell_-(P)$ and $c(\psi) = \psi^{-1}$.

**Step 1: the fields.**

**Lemma 7.2.2.** *(i) $h$ is irreducible over $\mathbb{Q}$ and $\operatorname{disc}(h) = -23$. $L = K(q) \cong K[T]/(h)$, $[L : K] = 3$, and $\operatorname{Gal}(L/K)$ is cyclic, generated by the automorphism $\tau$ with $\tau(q) = \big(-q + s/h'(q)\big)/2$. Every element of $\operatorname{Gal}(L/\mathbb{Q})$ outside $\operatorname{Gal}(L/K)$ conjugates $\tau$ to $\tau^{-1}$.*

*(ii) Let $w$ be a place of $K$ above a prime $p$. If $h$ has a simple root modulo $p$, then $L \otimes_K K_w \cong K_w^3$, that is, $L/K$ is split at $w$. This is the case for $p = 23$ ($h \equiv (T-13)^2(T-20)$), for every $p$ that is inert in $K$, and for every $p$ that splits in $K$ and modulo which $h$ has a root.*

*(iii) If $p$ splits in $K$ and $h$ has no root modulo $p$, then $K_w = \mathbb{Q}_p$, $L \otimes_K K_w$ is the unramified extension of $\mathbb{Q}_p$ of degree 3, $w$ is unramified in $L$, and its Frobenius element generates $\operatorname{Gal}(L/K)$. This is the case for $p = 2$ and $p = 3$.*

*(iv) Every prime $p$ falls under (ii) or (iii).*

*Proof.* (i) $\pm 1$ are not roots of $h$, so $h$ is irreducible, and $\operatorname{disc}(h) = -4(-1)^3 - 27 = -23$. Let $q_1, q_2, q_3$ be the roots of $h$ in $L$ and $\delta = (q_1 - q_2)(q_1 - q_3)(q_2 - q_3)$; then $\delta^2 = -23$, so $K = \mathbb{Q}(\delta) \subseteq L$. The group $\operatorname{Gal}(L/\mathbb{Q})$ acts faithfully and transitively on the roots, and the elements that fix $\delta$ are the even permutations; since $\delta \notin \mathbb{Q}$, $\operatorname{Gal}(L/\mathbb{Q}) \cong S_3$ and $\operatorname{Gal}(L/K) \cong A_3$ is cyclic of order 3. Hence $L = K(q)$, and $L \cong K[T]/(h)$ since $h$ is irreducible over $K$. The transpositions invert the 3-cycles. The element $(-q + s/h'(q))/2$ is a root of $h$ different from $q$ (we have $(q - q_2)(q - q_3) = h'(q)$ and $(q_2 - q_3)^2 = -23/h'(q)^2$), and the $K$-automorphism $\tau$ that maps $q$ to it has order 3 (certificate 1.4.2b).

(ii) We have $L \otimes_K K_w \cong K_w[T]/(h)$, and this is the product of the completions of $L$ at the places above $w$, which are all isomorphic since $L/K$ is Galois. A simple root modulo $p$ lifts to a root in $\mathbb{Z}_p \subseteq K_w$ by Hensel's lemma, so one factor is $K_w$, and hence all of them are. Modulo 23, $h \equiv (T-13)^2(T-20)$ and 20 is a simple root. If $p$ is inert in $K$, then $p \neq 2$ ($-23 \equiv 1 \pmod 8$, so 2 splits) and $p \neq 23$, so the roots $\theta_1, \theta_2, \theta_3$ of $h$ in $\overline{\mathbb{F}}_p$ are distinct, and $\bar\delta = \prod_{i<j}(\theta_i - \theta_j)$ satisfies $\bar\delta^2 = -23$, which is not a square in $\mathbb{F}_p$. So $x \mapsto x^p$ maps $\bar\delta$ to $-\bar\delta$, and it permutes the roots by an odd permutation, that is, by a transposition. Hence exactly one root lies in $\mathbb{F}_p$, and it is simple. If $p$ splits in $K$, then $p \neq 23$, and the roots of $h$ modulo $p$ are simple.

(iii) Since $p$ splits, $K_w = \mathbb{Q}_p$. Since $h$ has no root modulo $p$, it is irreducible over $\mathbb{F}_p$, so $K_w[T]/(h)$ is the unramified extension of $\mathbb{Q}_p$ of degree 3. Hence $w$ is unramified in $L$, there is only one place of $L$ above $w$, and the decomposition group is all of $\operatorname{Gal}(L/K)$, generated by the Frobenius element. We have $-23 \equiv 1$ modulo 8 and modulo 3, so 2 and 3 split in $K$, and $h$ has no root modulo 2 or modulo 3.

(iv) A prime is ramified in $K$ (only $p = 23$), inert, or split, and in the last case $h$ has a root modulo $p$ or not. □

The computations are certificate 1.4.2a. In particular $L/K$ is unramified at every place, so $L$ is contained in the Hilbert class field of $K$; since $h_K = 3$ (the reduced forms of discriminant $-23$ are $(1,1,6)$, $(2,\pm1,3)$), $L$ is the Hilbert class field of $K$. We do not use this.

**Step 2: the plane section.**

**Lemma 7.2.3.** *(i) As polynomials in $x, z, t$ with coefficients in $L$,*

$$F\Big(x, \frac{(1-s)x}{4}, z, t\Big) = -\prod_{i=0}^{2}\big(t - \tau^i(\rho)\,x - \tau^i(q)\,z\big).$$

*(ii) The determinant of the matrix with rows* $\big(-\tau^i(\rho), -\tau^i(q), 1\big)$ *(*$i = 0, 1, 2$*) is* $(s-1)/2$*, and* $N_{K/\mathbb{Q}}\big((s-1)/2\big) = 6$*.*

*(iii)* $q$ *is an algebraic integer,* $4(3q^2-1)\rho = (1-s)q^2 - 8$ *is integral, and* $N_{\mathbb{Q}(q)/\mathbb{Q}}(3q^2-1) = 23$*. Hence* $\tau^i(\rho)$ *and* $\tau^i(q)$ *are integral at every place of* $L$ *not above* 2 *or* 23*.*

*Proof.* (i) and (ii) are identities in the ring $\mathbb{Q}[q,s]/(h(q), s^2+23)$, with $\tau(q) = -q/2 + s(-6q^2 - 9q + 4)/46$. They are verified by certificate 1.4.2b, which also verifies (i) a second time without $\tau$: the product over the three roots $\theta$ of $h$ of $4(3\theta^2-1)(t-\theta z) + ((s-1)\theta^2 + 8)x$ is the resultant with $h$, and it equals $-64 \cdot 23 \cdot F(x, (1-s)x/4, z, t)$. (iii) $N(3q^2-1) = N(h'(q)) = -\operatorname{disc}(h) = 23$. □

**Lemma 7.2.4.** *If* $P = (x, y, z, t)$ *is a rational point of* $S$*, then* $\ell_+(P) \neq 0$ *and* $\ell_-(P) \neq 0$*.*

*Proof.* Since $s \notin \mathbb{Q}$, $\ell_\pm(P) = 0$ implies $x = y = 0$, and then $F(0,0,z,t) = -(z^3 - z^2t + t^3) = 0$. If $t = 0$, then $z = 0$. Otherwise $z/t$ is a rational root of $T^3 - T^2 + 1$, but $\pm 1$ are not roots (certificate 1.4.2b). □

**Step 3: the places not above 2 and 3.** From now on $P$ is a rational point of $S$, written with coprime integer coordinates, and $\psi = \ell_+(P)/\ell_-(P) \in K^\times$ (Lemma 7.2.4).

**Lemma 7.2.5.** $\operatorname{inv}_w(\psi) = 0$ *for every place* $w$ *of* $K$ *that does not lie above 2 or 3.*

*Proof.* At the complex place, and at every place of type (ii) of Lemma 7.2.2, $L/K$ is split, so $\operatorname{inv}_w(\psi) = 0$ by [Neu99, Chapters V–VI]. By Lemma 7.2.2(iv) it remains to treat a place $w$ above a prime $p \geq 5$ that splits in $K$ and modulo which $h$ has no root. By Lemma 7.2.2(iii), $K_w = \mathbb{Q}_p$ and there is a unique place $\mathfrak{W}$ of $L$ above $w$; hence $\tau(\mathfrak{W}) = \mathfrak{W}$ and $v_{\mathfrak{W}} \circ \tau = v_{\mathfrak{W}}$.

We show that $v_w(\ell_+(P)) = 0$. Suppose $v_w(\ell_+(P)) > 0$, and put $y_0 = (1-s)x/4$. Then $y - y_0 = \ell_+(P)/4$ has positive valuation, so $F(x, y_0, z, t) \equiv F(x, y, z, t) = 0$ modulo $\mathfrak{W}$. Put $m_i = t - \tau^i(\rho)x - \tau^i(q)z$. By Lemma 7.2.3(i), (iii), $\prod_i m_i$ has positive $\mathfrak{W}$-valuation and every $m_i$ is $\mathfrak{W}$-integral, so $v_{\mathfrak{W}}(m_i) > 0$ for some $i$. Since $x, z, t \in \mathbb{Q}$, we have $m_i = \tau^i(m_0)$, and therefore $v_{\mathfrak{W}}(m_0) = v_{\mathfrak{W}}(m_1) = v_{\mathfrak{W}}(m_2) > 0$. If $M$ is the matrix of Lemma 7.2.3(ii), then $M\,(x, z, t)^{\mathsf{T}} = (m_0, m_1, m_2)^{\mathsf{T}}$, and $\det M = (s-1)/2$ is a unit at $\mathfrak{W}$ since $p \nmid 6$. Hence $x, z, t \equiv 0$ modulo $\mathfrak{W}$, that is, $p \mid x, z, t$, and then $4y = \ell_+(P) - (-1+s)x$ gives $p \mid y$. This contradicts the coprimality of the coordinates.

The place $c(w)$ is of the same type, so also $v_{c(w)}(\ell_+(P)) = 0$, that is, $v_w(\ell_-(P)) = v_w(c(\ell_+(P))) = 0$. Hence $v_w(\psi) = 0$, and $\operatorname{inv}_w(\psi) = 0$ by [Neu99, Chapters V–VI]. □

For $5 \leq p < 500$ the conclusion is also confirmed directly: for each of the 32 such primes and both square roots of $-23$ modulo $p$, the plane cubic $F(x, (1-s)x/4, z, t)$ has no zero in $\mathbb{P}^2(\mathbb{F}_p)$ (certificate 1.4.2d).

**Step 4: the places above 2 and 3.** Let $s_2 \in \mathbb{Z}_2$ be the root of $s^2 = -23$ with $s_2 \equiv 1 \pmod 4$; then $s_2 \equiv 45 \pmod{256}$. Let $s_3 \in \mathbb{Z}_3$ be the root with $s_3 \equiv 1 \pmod 3$; then $s_3 \equiv 25 \pmod{81}$ ($s_3 \equiv 187 \pmod{243}$). Let $w_2$ and $w_3$ be the places of $K$ given by $s \mapsto s_2$ and $s \mapsto s_3$. The other places above 2 and 3 are $c(w_2)$ and $c(w_3)$.

**Lemma 7.2.6.** *For every* $(x, y, z, t) \in \mathbb{Z}_2^4$*, not all even, with* $F(x, y, z, t) = 0$*, the pair* $(v_2(\ell_+), v_2(\ell_-))$ *(with* $s = s_2$*) is* $(2,1)$*,* $(5,1)$ *or* $(2,4)$*, according as* $(x, y, z, t)$ *is congruent modulo 2 to* $(1,0,0,0)$*,* $(1,1,1,1)$ *or* $(0,1,1,1)$*. In particular* $v_{w_2}(\psi) \equiv 1 \pmod 3$*.*

*Proof.* Modulo 2, $F \equiv x^2y + xy^2 + y^3 + y^2z + z^3 + t^2y + tz^2 + t^3$, whose only projective zeros are the three residues of the statement. Moreover, modulo 16 every solution with $x, y, z, t$ odd has $y \equiv 13x$, and every solution with $x$ even and $y, z, t$ odd has $x \equiv 6y$ (certificate 1.4.2c). We have $(s_2 - 1)/4 \equiv 11 \pmod{64}$ and $(s_2+1)/2 \equiv 23 \pmod{128}$, so $v_2(s_2 - 1) = 2$ and $v_2(s_2 + 1) = 1$.

If $x$ is odd and $y$ is even, then $v_2(\ell_+) = v_2((s_2-1)x) = 2$ and $v_2(\ell_-) = v_2(-(s_2+1)x) = 1$. If $x, y, z, t$ are odd, then $v_2(\ell_-) = 1$, and $\ell_+/4 = \frac{s_2-1}{4}x + y \equiv 11x + 13x = 24x \pmod{16}$ has valuation 3,

so $v_2(\ell_+) = 5$. If $x$ is even and $y, z, t$ are odd, then $v_2(\ell_+) = 2$, and $\ell_-/4 = y - \frac{s_2+1}{2} \cdot \frac{x}{2} \equiv y - 23 \cdot 3y = -68y \pmod 8$ has valuation 2, so $v_2(\ell_-) = 4$. In each case $v_2(\ell_+) - v_2(\ell_-) \equiv 1 \pmod 3$, and $v_{w_2}(\psi) = v_2(\ell_+(P)) - v_2(\ell_-(P))$. □

The lemma is also confirmed by the complete residue tree of all primitive 2-adic points modulo $2^8$ (49152 normalized classes; every pair is determined from $2^6$ on) and by a direct enumeration of all primitive solutions modulo $2^6$ (certificate 1.4.2c).

**Lemma 7.2.7.** *For every $(x, y, z, t) \in \mathbb{Z}_3^4$, not all divisible by 3, with $F(x, y, z, t) = 0$, the pair $(v_3(\ell_+), v_3(\ell_-))$ (with $s = s_3$) is $(3, 0)$ if $(x, y, z, t)$ is congruent to a multiple of $(1, 0, 0, -1)$ modulo 3, and $(0, 0)$ otherwise. In particular $v_{w_3}(\psi) \equiv 0 \pmod 3$.*

*Proof.* Since $s_3 \equiv 1 \pmod 3$, we have $\ell_+ \equiv y$ and $\ell_- \equiv x + y \pmod 3$. The projective zeros of $F$ modulo 3 are $(1, 0, 0, -1)$, $(1, 1, 1, 0)$, $(1, 1, -1, 0)$, $(0, 1, 0, -1)$ (certificate 1.4.2c), and at the last three both forms are units. At the first one, scale to $x = 1$ and write $y = 3Y$, $z = 3Z$, $t = -1 + 3T$. Then

$$\tfrac{1}{3}F = 1 + 2Y - 3T + 3Y^2 - 6TY + 9\big(-T^3 + T^2Y + T^2 + TZ^2 + Y^3 + Y^2Z - Z^3 - Z^2\big).$$

Modulo 3 this gives $Y \equiv 1$, and then modulo 9, with $Y = 1 + 3Y_1$, it gives $6(1 + Y_1) \equiv 0$, so $Y \equiv 7 \pmod 9$. With $Y = 7 + 9Y_2$, the equation modulo 27 becomes $9(2Y_2 + 1 + 2T^2 + TZ^2 - Z^2) \equiv 0$, that is, $Y_2 \equiv 1 + 2T^2 + TZ^2 + 2Z^2 \pmod 3$, and $2T^2 + TZ^2 + 2Z^2 \in \{0, 2\}$ modulo 3 for all $T, Z$. Hence $Y \equiv 7$ or $16 \pmod{27}$. Now $\ell_+ = (s_3 - 1) + 12Y \equiv 12(Y + 2) \pmod{81}$ has valuation $1 + 2 = 3$, and $\ell_- \equiv 1 \pmod 3$ is a unit. □

The lemma is also confirmed by the complete residue tree modulo $3^5$ (26244 classes; every pair is determined from $3^4$ on) and by a direct enumeration of all primitive solutions modulo $3^4$ (certificate 1.4.2c).

**Step 5: reciprocity.**

*Proof of Theorem 7.2.1.* Suppose that $S$ has a rational point $P$, and let $\psi$ be as in Step 3. By [Neu99, Chapter VI, Section 5], $\sum_w \mathrm{inv}_w(\psi) = 0$, and by Lemma 7.2.5 only the places $w_2, c(w_2), w_3, c(w_3)$ can contribute. They are unramified in $L$ with Frobenius elements generating $\mathrm{Gal}(L/K)$ (Lemma 7.2.2(iii)). Write $\mathrm{Frob}_{w_2} = \tau^m$ with $m \in \{1, 2\}$. By Lemma 7.2.2(i), the hypothesis of [Neu99, Chapters V–VI] holds (with $k = \mathbb{Q}$), and $c(\psi) = \psi^{-1}$; so $\mathrm{inv}_{c(w)}(\psi) = \mathrm{inv}_w(\psi)$ for $w = w_2, w_3$. By [Neu99, Chapters V–VI] and Lemma 7.2.7, $\mathrm{inv}_{w_3}(\psi) = 0$, since $v_{w_3}(\psi) \equiv 0 \pmod 3$. By [Neu99, Chapters V–VI] and Lemma 7.2.6, $\mathrm{inv}_{w_2}(\psi) = m\, v_{w_2}(\psi)/3 \equiv m/3 \pmod 1$. Hence

$$\sum_w \mathrm{inv}_w(\psi) = 2\,\mathrm{inv}_{w_2}(\psi) = \frac{2m}{3} \not\equiv 0 \pmod 1,$$

a contradiction. Therefore $S(\mathbb{Q}) = \varnothing$. A nonzero integer solution would give a rational point of $S$, so the only integer solution is $(0, 0, 0, 0)$. □

## 7.3 $2x^3 + 2x^2y + 2y^3 + y^2z - 2xz^2 - z^3 + tz^2 - t^3 = 0$ ($H = 96$)

**Theorem 7.3.1.** *The only integer solution of*

$$F(x, y, z, t) = 2x^3 + 2x^2y + 2y^3 + y^2z - 2xz^2 - z^3 + tz^2 - t^3 = 0$$

*is $(x, y, z, t) = (0, 0, 0, 0)$.*

**Setup.** The proof is the same as that of Section 7.2, with a different decisive prime. It suffices to show that the cubic surface $S : F = 0$ in $\mathbb{P}^3$ has no rational point. Let $K = \mathbb{Q}(s)$ with $s^2 = -11$, let $g(U) = U^3 - 4U - 4$, let $L$ be the splitting field of $g$ over $\mathbb{Q}$, let $u \in L$ be a root of $g$, and put $q = u/2$, so that $2q^3 - 2q - 1 = 0$. (The field $\mathbb{Q}(u)$ is also generated by a root $v$ of $h_C(V) = V^3 - V^2 - V - 1$: $u = v^2 - 1$ and $v = u^2/2 - 1$; and $L$ is the splitting field of $h_C$.) Put

$$\ell_\pm = (2 \pm s)y + 3t, \qquad \rho = \frac{s + 2 - 6q^2}{6(3q^2 - 1)}.$$

The plane $\ell_+ = 0$ meets $S$ in three lines permuted cyclically by $\mathrm{Gal}(L/K)$ (Step 2). For a rational point $P$ we put $\psi = \ell_+(P)/\ell_-(P) \in K^\times$; its local invariants for $L/K$ ([Neu99, Chapters V–VI]) vanish at every place of $K$ except the two places above 3 (Steps 3–4), where they are equal and nonzero (Step 5). The notation $K_w$, $v_w$, $c$, $c(w)$ is as in Section 7.2; again $c(\psi) = \psi^{-1}$.

**Step 1: the fields.**

**Lemma 7.3.2.** *(i) $g$ is irreducible over $\mathbb{Q}$ and $\mathrm{disc}(g) = -176 = -11 \cdot 4^2$. $L = K(u) \cong K[U]/(g)$, $[L : K] = 3$, and $\mathrm{Gal}(L/K)$ is cyclic, generated by the automorphism $\tau$ with $\tau(u) = \big(-u + 4s/g'(u)\big)/2$. Every element of $\mathrm{Gal}(L/\mathbb{Q})$ outside $\mathrm{Gal}(L/K)$ conjugates $\tau$ to $\tau^{-1}$.*

*(ii) Let $w$ be a place of $K$ above a prime $p$. If $g$ has a simple root modulo $p$, then $L/K$ is split at $w$. This is the case for $p = 11$ ($g \equiv (U-4)^2(U-3)$), for every odd $p$ that is inert in $K$, and for every $p$ that splits in $K$ and modulo which $g$ has a root.*

*(iii) If $p$ splits in $K$ and $g$ has no root modulo $p$, then $K_w = \mathbb{Q}_p$, $L \otimes_K K_w$ is the unramified extension of $\mathbb{Q}_p$ of degree 3, $w$ is unramified in $L$, and its Frobenius element generates $\mathrm{Gal}(L/K)$. This is the case for $p = 3$.*

*(iv) The prime 2 is inert in $K$: $K_w = \mathbb{Q}_2(s)$ is the unramified quadratic extension of $\mathbb{Q}_2$, and with $\omega = (1+s)/2$ ($\omega^2 - \omega + 3 = 0$) we have $2 + s = 1 + 2\omega$ and $2 - s = 3 - 2\omega$. Every odd prime falls under (ii) or (iii).*

*Proof.* As for Lemma 7.2.2. The rational roots of $g$ would divide 4, and $\pm1, \pm2, \pm4$ are not roots. $\mathrm{disc}(g) = -4(-4)^3 - 27 \cdot 16 = -176$, and $K = \mathbb{Q}(\sqrt{-176})$. Since $u$ has two conjugates with $(u_2 - u_3)^2 = -176/g'(u)^2$, $\tau(u)$ is a root of $g$ different from $u$, and $\tau$ has order 3 (certificate 1.4.3b). Modulo 11, $g \equiv (U-4)^2(U-3)$. If $p$ is odd, $p \neq 11$, the roots of $g$ modulo $p$ are distinct, and the argument with $\bar\delta^2 = -176$ shows that $g$ has exactly one root modulo $p$ if $p$ is inert in $K$, and 0 or 3 roots if $p$ splits. The prime 3 splits ($-11 \equiv 1 \pmod 3$), and $g \equiv U^3 - U - 1$ has no root modulo 3. The prime 2 is inert since $-11 \equiv 5 \pmod 8$. These facts are checked by certificate 1.4.3a. □

In fact $h_C(V+1) = V^3 + 2V^2 - 2$ is Eisenstein at 2, so $L/K$ is totally (and tamely) ramified at the place above 2, and unramified at every other place; the field discriminant of $\mathbb{Q}(u)$ is $-44$ (certificate 1.4.3a). We do not use this: at 2 the argument of Lemma 7.3.6 works for any cubic extension.

**Step 2: the plane section.**

**Lemma 7.3.3.** *(i) As polynomials in $x, y, z$ with coefficients in $L$,*

$$F\Big(x, y, z, -\frac{(2+s)y}{3}\Big) = 2\prod_{i=0}^{2}\big(x - \tau^i(\rho)\,y - \tau^i(q)\,z\big).$$

*(ii) The determinant of the matrix with rows $\big(1, -\tau^i(\rho), -\tau^i(q)\big)$ ($i = 0, 1, 2$) is 2.*

*(iii) $u$ is an algebraic integer, $3q^2 - 1 = (3u^2 - 4)/4$, and $N_{\mathbb{Q}(u)/\mathbb{Q}}(3u^2 - 4) = -\mathrm{disc}(g) = 176$. Hence $\tau^i(\rho)$ and $\tau^i(q)$ are integral at every place of $L$ not above 2, 3 or 11.*

*Proof.* (i) and (ii) are identities in $\mathbb{Q}[u, s]/(g(u), s^2 + 11)$, with $\tau(u) = -u/2 + s(-6u^2 + 9u + 16)/22$ (certificate 1.4.3b); (i) is also verified through the resultant of $g$ with the numerator $6(3u^2 - 4)(x - uz/2) - 4(s + 2 - \frac{3}{2}u^2)y$. (iii) $\rho = 4(s + 2 - \frac{3}{2}u^2)/(6(3u^2 - 4))$. □

**Lemma 7.3.4.** *If $P$ is a rational point of $S$, then $\ell_\pm(P) \neq 0$.*

*Proof.* $\ell_\pm(P) = 0$ implies $y = t = 0$, and then $F(x,0,z,0) = 2x^3 - 2xz^2 - z^3 = 0$. If $x = 0$, then $z = 0$. Otherwise $r = z/x$ is a rational root of $r^3 + 2r^2 - 2$, but $\pm1, \pm2$ are not roots (certificate 1.4.3b). □

**Step 3: the places not above 2 and 3.** From now on $P$ is a rational point of $S$ with coprime integer coordinates, and $\psi = \ell_+(P)/\ell_-(P) \in K^\times$.

**Lemma 7.3.5.** $\mathrm{inv}_w(\psi) = 0$ *for every place $w$ of $K$ that does not lie above 2 or 3.*

*Proof.* At the complex place and at the places of type (ii) of Lemma 7.3.2, $L/K$ is split. It remains to treat a place $w$ above a prime $p \geq 5$ that splits in $K$ (so $p \neq 11$) and modulo which $g$ has no root; there is a unique place $\mathfrak{W}$ of $L$ above $w$, and $v_{\mathfrak{W}} \circ \tau = v_{\mathfrak{W}}$. Suppose $v_w(\ell_+(P)) > 0$. With $t_0 = -(2+s)y/3$ we have $t - t_0 = \ell_+(P)/3$, so $F(x,y,z,t_0) \equiv 0$ modulo $\mathfrak{W}$. By Lemma 7.3.3(i), (iii), some, and hence every, $m_i = x - \tau^i(\rho)y - \tau^i(q)z = \tau^i(m_0)$ has positive $\mathfrak{W}$-valuation. The determinant 2 of Lemma 7.3.3(ii) is a unit at $\mathfrak{W}$, so $p \mid x, y, z$, and then $3t = \ell_+(P) - (2+s)y$ gives $p \mid t$, a contradiction. Hence $v_w(\ell_+(P)) = 0$, and likewise $v_{c(w)}(\ell_+(P)) = 0$, that is, $v_w(\ell_-(P)) = 0$. So $v_w(\psi) = 0$ and $\mathrm{inv}_w(\psi) = 0$ by [Neu99, Chapters V–VI]. □

For the 32 such primes $5 \leq p < 500$ the plane cubic $F(x,y,z,-(2+s)y/3)$ has no zero in $\mathbb{P}^2(\mathbb{F}_p)$ for either square root of $-11$ modulo $p$ (certificate 1.4.3d).

**Step 4: the places above 2 and 3.** Let $s_3 \in \mathbb{Z}_3$ be the root of $s^2 = -11$ with $s_3 \equiv 1 \pmod 3$; then $s_3 \equiv 31 \pmod{81}$. Let $w_3$ be the place of $K$ given by $s \mapsto s_3$; the other place above 3 is $c(w_3)$. Let $w_2$ be the place above 2.

**Lemma 7.3.6.** *Every $(x,y,z,t) \in \mathbb{Z}_2^4$, not all even, with $F(x,y,z,t) = 0$ has $y$ odd and $t$ even. Consequently $\ell_+(P) \equiv \ell_-(P) \equiv 1$ modulo $2\mathcal{O}_{K_{w_2}}$, $\psi \in 1 + 2\mathcal{O}_{K_{w_2}}$, and $\mathrm{inv}_{w_2}(\psi) = 0$.*

*Proof.* Modulo 2, $F \equiv y^2z + z^3 + tz^2 + t^3$. If $y$ is even and $t$ is odd, then $F \equiv z(y^2 + z^2 + tz) + t^3 \equiv z^3 + z^2 + 1 \not\equiv 0$; so if $y$ is even, then $t$ and $z$ are even and $x$ is odd, and then $F \equiv 2x^2(x+y) \equiv 2 \pmod 4$. If $t$ is odd, then $F \equiv z^3 + z^2 + y^2z + 1 \pmod 2$ forces $z$ odd and then $y$ odd; with $y^2 \equiv z^2 \equiv t^2 \equiv 1 \pmod 8$ we get $F \equiv 2(x^3 + x^2y + y - x) \pmod 8$, which is $\equiv 4y \equiv 4 \pmod 8$ if $x$ is odd and $\equiv 2(y - x) \equiv 2 \pmod 4$ if $x$ is even. Hence $y$ is odd and $t$ is even (certificate 1.4.3c checks all primitive solutions modulo 8). By Lemma 7.3.2(iv), $\ell_\pm \equiv y + t \equiv 1$ modulo $2\mathcal{O}_{K_{w_2}}$, so $\psi \equiv 1$. By Hensel's lemma ($X^3 - \psi$ at $X = 1$; 3 is a unit) $\psi = b^3$ with $b \in K_{w_2}$, and $b^3$ is the norm of $b$ from every cubic extension of $K_{w_2}$. Hence $\psi$ is a local norm and $\mathrm{inv}_{w_2}(\psi) = 0$ by [Neu99, Chapters V–VI]. (Equivalently, by [Neu99, Chapters V–VI]: the residue of $\psi$ is 1, a cube in $\mathbb{F}_4^\times$.) □

**Lemma 7.3.7.** *For every $(x,y,z,t) \in \mathbb{Z}_3^4$, not all divisible by 3, with $F(x,y,z,t) = 0$, the pair $(v_3(\ell_+), v_3(\ell_-))$ (with $s = s_3$) is $(1,3)$ if $(x,y,z,t)$ is congruent to a multiple of $(1,0,0,-1)$ modulo 3, and $(1,0)$ otherwise. In particular $v_{w_3}(\psi) \equiv 1 \pmod 3$.*

*Proof.* The projective zeros of $F$ modulo 3 are $(1,0,0,-1)$, $(1,1,0,0)$, $(1,-1,0,1)$, $(0,1,0,-1)$ (certificate 1.4.3c). Since $2 + s_3 \equiv 33$ and $2 - s_3 \equiv -29 \pmod{81}$, we have $\ell_+ \equiv 3(11y + t)$ modulo 81, and $\ell_- \equiv y \pmod 3$. At the last three points, $3 \nmid y$ and $2y + t \not\equiv 0 \pmod 3$, so the pair is $(1,0)$. At the first point, scale to $t = 1$ and write $x = -1 + 3X$, $y = 3Y$, $z = 3Z$. Then

$$\tfrac{1}{3}F = 18X^3 + 18X^2Y - 18X^2 - 12XY - 18XZ^2 + 6X + 18Y^3 + 9Y^2Z + 2Y - 9Z^3 + 9Z^2 - 1.$$

Reducing modulo 3 and 9 gives $Y \equiv 5 \pmod 9$, and with $Y = 5 + 9Y_2$ the equation modulo 27 gives $Y_2 \equiv Z^2(X+1) - X^2 - X - 1 \pmod 3$. For $X \equiv 0, 1, -1$ this is $Z^2 - 1, -Z^2, -1$, so it is 0 or 2, never 1; hence $Y \equiv 5$ or $23 \pmod{27}$. Now $\ell_+ = 3\big((2+s_3)Y + 1\big) \equiv 3(33Y + 1)$ has valuation 1, and $\ell_- = 3\big((2-s_3)Y + 1\big) \equiv 3(1 - 29Y) \pmod{3^4}$, where $1 - 29Y \equiv 18$ or $9 \pmod{27}$ has valuation 2. So the pair is $(1,3)$. □

The lemma is also confirmed by the complete residue tree modulo $3^4$ (2916 normalized classes; the pairs are determined at $3^4$) and by a direct enumeration of all primitive solutions modulo $3^4$ (certificate 1.4.3c).

**Step 5: reciprocity.**

*Proof of Theorem 7.3.1.* Suppose that $S$ has a rational point $P$, and let $\psi$ be as in Step 3. By Lemmas 7.3.5 and 7.3.6, only $w_3$ and $c(w_3)$ can contribute to $\sum_w \mathrm{inv}_w(\psi)$, which is 0 by [Neu99, Chapter VI, Section 5]. These places are unramified in $L$, and $\mathrm{Frob}_{w_3} = \tau^m$ with $m \in \{1,2\}$ (Lemma 7.3.2(iii)). By [Neu99, Chapters V–VI] and $c(\psi) = \psi^{-1}$, $\mathrm{inv}_{c(w_3)}(\psi) = \mathrm{inv}_{w_3}(\psi)$, and by [Neu99, Chapters V–VI] and Lemma 7.3.7, $\mathrm{inv}_{w_3}(\psi) = m\, v_{w_3}(\psi)/3 \equiv m/3 \pmod 1$. Hence $\sum_w \mathrm{inv}_w(\psi) = 2m/3 \not\equiv 0 \pmod 1$, a contradiction. Therefore $S(\mathbb{Q}) = \varnothing$, and the only integer solution is $(0,0,0,0)$. □

## 7.4 $8x^4 + 7y^4 + 2z^4 - t^4 = 0$ ($H = 288$)

**Theorem 7.4.1.** *The only integer solution of $8x^4 + 7y^4 + 2z^4 = t^4$ is $(x,y,z,t) = (0,0,0,0)$.*

**Setup.** Suppose that there is a nonzero solution. Dividing by the greatest common divisor, we get a solution with $\gcd(x,y,z,t) = 1$, which we fix. Put

$$f = 7y^2 + 2z^2 - 3t^2, \qquad g = 7y^2 + 2z^2 + 3t^2, \qquad A_\pm = 2x^2 \pm 2xz + z^2.$$

We show that the Hilbert symbols $c_v = (-7, f)_v\,(7, A_+)_v$ satisfy $c_p = 1$ for every prime $p$ and $c_\infty = -1$, which contradicts Hilbert's product formula ([Ser73, Chapter III, Sections 1–2]). For a prime $p$ and an integer $a$ prime to $p$, $(a/p)$ is the Legendre symbol.

**Step 1: identities and signs.**

**Lemma 7.4.2.** *(i) $-fg = 72x^4 + 14(y^2 - z^2)^2 = 2\big(36x^4 + 7(y^2 - z^2)^2\big)$, which is twice the norm of $6x^2 + (y^2 - z^2)\sqrt{-7}$ from $\mathbb{Q}(\sqrt{-7})$.*

*(ii) $t^4 - 7y^4 = 2A_+A_-$, where $A_+A_- = 4x^4 + z^4$, and $t^4 - 7y^4$ is the norm of $t^2 + y^2\sqrt{7}$ from $\mathbb{Q}(\sqrt{7})$.*

*(iii) $g > 0$, $A_+ > 0$, $f < 0$.*

*Proof.* As polynomial identities, $-fg - 72x^4 - 14(y^2 - z^2)^2 = -9(8x^4 + 7y^4 + 2z^4 - t^4)$ and $t^4 - 7y^4 - 2A_+A_- = -(8x^4 + 7y^4 + 2z^4 - t^4)$ (certificate 1.4.4a); this gives (i) and (ii). (iii) $g = 0$ forces $y = z = t = 0$ and then $x = 0$. $A_+ = x^2 + (x+z)^2 = 0$ forces $x = z = 0$, and then $t^4 = 7y^4$ forces $y = t = 0$. By (i), $f \le 0$, and $f = 0$ forces $x = 0$ and $y^2 = z^2$, so $t^4 = 9y^4$, $t^2 = 3y^2$, $y = t = 0$. □

**Step 2: odd primes other than 3 and 7.**

**Lemma 7.4.3.** *Let $p \neq 2, 3, 7$ be a prime. If $(-7/p) = -1$, then $v_p(f)$ is even. If $(7/p) = -1$, then $v_p(A_+)$ is even.*

*Proof.* Suppose $(-7/p) = -1$ and $p \mid f$. If also $p \mid g$, then $p \mid g - f = 6t^2$, so $p \mid t$, and $36x^4 + 7(y^2 - z^2)^2 \equiv 0 \pmod p$ by Lemma 7.4.2(i). Since $-7$ is not a square modulo $p$, this forces $y^2 \equiv z^2$ and then $x \equiv 0$. Then $f \equiv 7y^2 + 2y^2 = 9y^2$, so $p \mid y$ and $p \mid z$, which contradicts $\gcd(x,y,z,t) = 1$. Hence $p \nmid g$, and $v_p(f) = v_p(-fg) = v_p\big(N(6x^2 + (y^2 - z^2)\sqrt{-7})\big)$ is even, because $p$ is inert in $\mathbb{Q}(\sqrt{-7})$.

Suppose $(7/p) = -1$ and $p \mid A_+$. Then $p \mid t^4 - 7y^4$, and since 7 is not a square modulo $p$, $p \mid y$ and $p \mid t$. If also $p \mid A_-$, then $p \mid A_+ - A_- = 4xz$ and $p \mid A_+ + A_- = 4x^2 + 2z^2$, so $p \mid x$ and $p \mid z$, a contradiction. Hence $p \nmid A_-$, and $v_p(A_+) = v_p(t^4 - 7y^4) = v_p\big(N(t^2 + y^2\sqrt{7})\big)$ is even, because $p$ is inert in $\mathbb{Q}(\sqrt{7})$. □

**Step 3: the prime 3.**

**Lemma 7.4.4.** $v_3(f) \in \{0, 2\}$.

*Proof.* Modulo 3, $f \equiv y^2 - z^2$ and $8x^4 + 7y^4 + 2z^4 - t^4 \equiv 2x^4 + y^4 + 2z^4 - t^4$. If $3 \mid f$, then $y^4 \equiv z^4$, so $2x^4 \equiv t^4$, which forces $3 \mid x$ and $3 \mid t$; then $y, z$ are units (if $3 \mid y$, then $3 \mid z$). In this case put $r = (z/y)^2 \in \mathbb{Z}_3$, so $r \equiv 1 \pmod 3$. Since $3^4$ divides $8x^4$ and $t^4$, we get $7 + 2r^2 \equiv 0 \pmod{81}$, and hence

$$(7 + 2r)(7 - 2r) = 49 - 4r^2 = 63 - 2(7 + 2r^2) \equiv 63 \pmod{81}.$$

Since $7 - 2r \equiv 2 \pmod 3$ is a unit, $v_3(7 + 2r) = v_3(63) = 2$. Finally $f/y^2 = 7 + 2r - 3(t/y)^2$ and $v_3(3(t/y)^2) \geq 3$, so $v_3(f) = 2$. The residue facts are checked by certificate 1.4.4b. □

**Step 4: the prime 2.**

**Lemma 7.4.5.** *$x, y, z, t$ are odd, $A_+ \equiv 1$ or $5 \pmod 8$, and $f \equiv 6 \pmod 8$.*

*Proof.* A fourth power is $\equiv 0$ or $1 \pmod{16}$, according as the number is even or odd. Hence $8x^4 + 7y^4 + 2z^4 - t^4 \equiv 8a + 7b + 2c - d \pmod{16}$, where $a, b, c, d \in \{0, 1\}$ are the parities of $x, y, z, t$. Among the sixteen choices, only $a = b = c = d = 0$ and $a = b = c = d = 1$ give $0 \pmod{16}$, and the first is excluded by $\gcd(x, y, z, t) = 1$. For odd $x, z$ we have $A_+ \equiv 2 + 2xz + 1 \equiv 1$ or $5 \pmod 8$, and for odd $y, z, t$ we have $f \equiv 7 + 2 - 3 = 6 \pmod 8$ (certificate 1.4.4b). □

**Step 5: the prime 7.**

**Lemma 7.4.6.** *$f$ and $A_+$ are prime to 7, and $(f/7) = (A_+/7)$.*

*Proof.* If 7 divides $x, z, t$, then $y$ is prime to 7 and $7y^4 = t^4 - 8x^4 - 2z^4$ has 7-adic valuation 1 on the left and at least 4 on the right. Hence $(x, z, t) \not\equiv (0, 0, 0) \pmod 7$, and modulo 7 the equation reads $x^4 + 2z^4 \equiv t^4$, while $f \equiv 2z^2 - 3t^2$. The fourth powers modulo 7 are $0, 1, 2, 4$. If $z \equiv 0$, then $x^4 \equiv t^4 \not\equiv 0$, and $A_+ \equiv 2x^2$, $f \equiv -3t^2 \equiv 4t^2$ are nonzero squares ($2 \equiv 3^2$). If $z \not\equiv 0$, put $r = x/z$, $s = t/z$; then $r^4 + 2 \equiv s^4$, and the possibilities are

| $r$ | $s$ | $A_+/z^2$ | $f/z^2$ |
|---|---|---|---|
| 0 | $\pm 2$ | 1 | 4 |
| 2 | $\pm 3$ | 6 | 3 |
| $-2$ | $\pm 3$ | 5 | 3 |

In each row $A_+/z^2$ and $f/z^2$ are both squares or both nonsquares modulo 7 (certificate 1.4.4b). □

**Step 6: Hilbert symbols.**

*Proof of Theorem 7.4.1.* By Lemma 7.4.2(iii), $f, A_+ \neq 0$, so the symbols are defined. We use the formulas of [Ser73, Chapter III, Sections 1–2].

$p \neq 2, 3, 7$: $-7$ and 7 are $p$-adic units, so $(-7, f)_p = (-7/p)^{v_p(f)}$ and $(7, A_+)_p = (7/p)^{v_p(A_+)}$. By Lemma 7.4.3, both are 1.

$p = 3$: $(-7, f)_3 = (-7/3)^{v_3(f)} = (-1)^{v_3(f)} = 1$ by Lemma 7.4.4, and $(7, A_+)_3 = (7/3)^{v_3(A_+)} = 1$ since $7 \equiv 1 \pmod 3$.

$p = 2$: $-7 \equiv 1 \pmod 8$ is a square in $\mathbb{Q}_2$, so $(-7, f)_2 = 1$. Since 7 and $A_+$ are 2-adic units and $A_+ \equiv 1 \pmod 4$ (Lemma 7.4.5), $(7, A_+)_2 = (-1)^{\varepsilon(7)\varepsilon(A_+)} = 1$.

$p = 7$: $f$ and $A_+$ are 7-adic units (Lemma 7.4.6) and $v_7(-7) = v_7(7) = 1$, so $(-7, f)_7 = (f/7)$ and $(7, A_+)_7 = (A_+/7)$, and $c_7 = (f/7)(A_+/7) = 1$ by Lemma 7.4.6.

$v = \infty$: $-7 < 0$ and $f < 0$, so $(-7, f)_\infty = -1$, while $(7, A_+)_\infty = 1$ since $7 > 0$.

Hence $\prod_v (-7, f)_v \cdot \prod_v (7, A_+)_v = \prod_v c_v = -1$. By Hilbert's product formula ([Ser73, Chapter III, Sections 1–2]) both products are 1, a contradiction. Therefore there is no nonzero solution. □

The local conclusions $c_2 = c_3 = c_7 = 1$ are also confirmed by evaluating the two symbols, with the formulas of [Ser73, Chapter III, Sections 1–2], on the complete residue trees of all primitive points over $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_7$ modulo $2^5$, $3^4$, $7^2$, and by a direct enumeration of all primitive solutions modulo $3^4$ and $7^2$ (certificate 1.4.4c).

### The common Frey-curve argument

Each of these six equations has the form $Ax^5 + By^5 + Cz^5 = 0$, and we use the modular method with exponent 5: a primitive solution gives a Frey curve $E$ whose 5-torsion $E[5]$ (an $\mathbb{F}_5[G_\mathbb{Q}]$-module of dimension 2, $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) is irreducible, so by modularity and level lowering ([Sik12, Theorem 3 and Proposition 5.1]) it is congruent modulo a prime above 5 to a newform of weight 2 and of a small level; the newforms of that level are then excluded by comparing their Hecke eigenvalues with the traces that $E$ can have at a few auxiliary primes. The lemmas below are used by all six sections. We write $v_\ell$ for the $\ell$-adic valuation, $\Delta_{\min}$ for the minimal discriminant, $f_\ell(E)$ for the exponent of $\ell$ in the conductor $N_E$, $a_\ell(E) = \ell + 1 - \#\widetilde{E}(\mathbb{F}_\ell)$ for a prime $\ell$ of good reduction, and $\chi_5$ for the cyclotomic character modulo 5. For a newform $f = \sum_{n\geq 1} a_n(f) q^n$ we write $K_f = \mathbb{Q}(a_n(f) : n \geq 1)$ for its coefficient field; the $a_n(f)$ are algebraic integers.

**Lemma 7.4.7.** *Let $A, B, C$ be pairwise coprime nonzero integers with $v_p(A), v_p(B), v_p(C) \leq 4$ for every prime $p$, and let $(x, y, z)$ be a primitive solution ($\gcd(x, y, z) = 1$) of $Ax^5 + By^5 + Cz^5 = 0$.*

*(1) If $z = 0$, then $|A| = |B| = |x| = |y| = 1$; similarly if $x = 0$ or $y = 0$.*

*(2) If $xyz \neq 0$, the three integers $Ax^5$, $By^5$, $Cz^5$ are pairwise coprime, and exactly one of them is even.*

*Proof.* (1) If $z = 0$, then $\gcd(x, y) = 1$ and $Ax^5 = -By^5$. Since $\gcd(A, B) = \gcd(x, y) = 1$, we get $|A| = |y|^5$ and $|B| = |x|^5$, and since no prime divides $A$ or $B$ to the fifth power, $|A| = |B| = 1$ and $|x| = |y| = 1$.

(2) Suppose that a prime $p$ divides two of the three terms; then it divides the third as well, since their sum is 0. Since $A, B, C$ are pairwise coprime, $p$ divides at most one coefficient. If $p \nmid ABC$, then $p$ divides $x$, $y$ and $z$. If, say, $p \mid A$, then $p \nmid BC$, so $p \mid y$ and $p \mid z$; then $p^5$ divides $By^5 + Cz^5 = -Ax^5$, and since $v_p(A) \leq 4$, also $p \mid x$. The cases $p \mid B$ and $p \mid C$ are the same. Each case contradicts $\gcd(x, y, z) = 1$. Hence the terms are pairwise coprime, so at most one of them is even, and they cannot all be odd, because their sum is 0. □

In the situation of Lemma 7.4.7(2), let $t_j$ be the even term and $t_i$, $t_k$ the two odd terms, in an order fixed in each section, and put

$$(u, v, w) = \varepsilon\,(t_i, t_j, t_k), \qquad \varepsilon \in \{\pm 1\} \text{ such that } u \equiv -1 \pmod 4.$$

Then $u, v, w$ are pairwise coprime and nonzero, $u + v + w = 0$, $u \equiv -1 \pmod 4$ and $v$ is even. The *Frey curve* of the solution is

$$E = E_{u,v}: \quad Y^2 = X(X - u)(X + v), \qquad c_4 = 16(u^2 + uv + v^2), \qquad \Delta = 16u^2v^2w^2.$$

Its 2-torsion points $(0, 0)$, $(u, 0)$, $(-v, 0)$ are rational. The other possible choice, with $t_k$ in place of $t_i$, gives a curve isomorphic to $E$ if $v_2(v) \geq 2$ (then it is $(-w, -v, -u)$), and the twist of $E$ by $-1$ if $v_2(v) = 1$ (then it is $(w, v, u)$), by Lemma 7.4.8(3); nothing below depends on this choice.

**Lemma 7.4.8.** *Let $u, v, w$ be pairwise coprime nonzero integers with $u + v + w = 0$, $u \equiv -1 \pmod 4$ and $v$ even, and put $r = v_2(v)$.*

*(1) At an odd prime $\ell$, $E_{u,v}$ has good reduction if $\ell \nmid uvw$, and multiplicative reduction with $v_\ell(\Delta_{\min}) = 2v_\ell(uvw)$ if $\ell \mid uvw$.*

(2) *At 2, the Kodaira type, $f_2(E_{u,v})$ and $v_2(\Delta_{\min})$ are*

| $r$ | 1 | 2 | 3 | 4 | $\geq 5$ |
|---|---|---|---|---|---|
| *type* | III | $\mathrm{I}_1^*$ | $\mathrm{III}^*$ | $\mathrm{I}_0$ | $\mathrm{I}_{2r-8}$ |
| $f_2$ | 5 | 3 | 3 | 0 | 1 |
| $v_2(\Delta_{\min})$ | 6 | 8 | 10 | 0 | $2r-8$ |

(3) *The curves $E_{u',v'}$ obtained from the other orderings $(u',v',w')$ of $(u,v,w)$ and of $(-u,-v,-w)$ are isomorphic over $\mathbb{Q}$ to $E_{u,v}$ or to its quadratic twist by $-1$, and for $a \in \mathbb{Q}^\times$ the curve $E_{au,av}$ is the quadratic twist of $E_{u,v}$ by $a$.*

*Proof.* The displayed $c_4$ and $\Delta$ give (1). Applying Tate's algorithm [Tat75, Sil94] to $a_2 = v-u$, $a_4 = -uv$ gives the table in (2), with the normalized model

$$S^2 + RS = R^3 + \frac{v-u-1}{4}R^2 - \frac{uv}{16}R$$

when $r \geq 4$; certificate 1.4qa checks every residue class needed for the other rows. In (3), translation permutes the three roots, changing all their signs gives the twist by $-1$, and scaling them by $a$ gives the twist by $a$. □

The congruences and the model used in (2) are checked by certificate 1.4qa, which also compares the table with PARI's implementation of Tate's algorithm on all residue classes of $u$ and $v/2^r$ modulo $2^7$, for $r \leq 12$. For $u \equiv 1 \pmod 4$ the exponents are different ($f_2 = 4$ for every $r \geq 2$); this is why the sign is normalized.

**Lemma 7.4.9.** *In the situation of Lemma 7.4.7(2), let $E$ be the Frey curve, $c_j$ the coefficient of the even term $t_j$ and $s_j$ its variable, so that $r = v_2(t_j) = v_2(c_j) + 5v_2(s_j)$. Then $E$ is semistable at every odd prime, and its level of [Sik12, Theorem 3 and Proposition 5.1] for $p = 5$,*

$$N_5 = N_E \Big/ \prod_{\ell \,\|\, N_E,\ 5 \mid v_\ell(\Delta_{\min})} \ell,$$

*is $N_5 = 2^\alpha \prod_{\ell \mid ABC,\ \ell \text{ odd}} \ell$, where $\alpha = f_2(E)$ from Lemma 7.4.8(2), except that $\alpha = 0$ if $r \geq 5$ and $r \equiv 4 \pmod 5$. Moreover, if $5 \nmid ABC$, then $E$ has good reduction at 5 or multiplicative reduction with $5 \mid v_5(\Delta_{\min})$; if $5 \mid ABC$, then $E$ has multiplicative reduction at 5 with $5 \nmid v_5(\Delta_{\min})$.*

*Proof.* Up to sign, $uvw = ABC(xyz)^5$, and every prime divides at most one of the three terms. Let $\ell$ be odd. By Lemma 7.4.8(1), $E$ is good at $\ell$ if $\ell \nmid uvw$, and otherwise multiplicative with $v_\ell(\Delta_{\min}) = 2v_\ell(c) + 10v_\ell(s)$, where $c$ and $s$ are the coefficient and the variable of the term divisible by $\ell$. If $\ell \mid ABC$, then $1 \leq v_\ell(c) \leq 4$, so $5 \nmid v_\ell(\Delta_{\min})$ and $\ell$ divides $N_5$ exactly once. If $\ell \nmid ABC$, then $5 \mid v_\ell(\Delta_{\min})$, so $\ell \nmid N_5$. At 2, Lemma 7.4.8(2) gives $f_2(E)$; the prime 2 is removed only if $f_2(E) = 1$, that is $r \geq 5$, and $5 \mid 2r-8$, that is $r \equiv 4 \pmod 5$. The statement at 5 is the case $\ell = 5$ above. □

Since $r \equiv v_2(c_j) \pmod 5$, the exception $\alpha = 0$ with $r \geq 5$ occurs only when $v_2(c_j) = 4$ (Section 7.9). The resulting levels for each equation are printed by certificate 1.4.5a–certificate 1.4.10a.

**Lemma 7.4.10.** *Let $E/\mathbb{Q}$ be an elliptic curve which is semistable at every odd prime $\ell \neq 5$, with $f_2(E) \leq 5$. If $E[5]$ is reducible, then $a_q(E) \equiv \pm 2 \pmod 5$ for every prime $q \equiv 1 \pmod 5$ at which $E$ has good reduction.*

*Proof.* Let $L \subset E[5]$ be a $G_\mathbb{Q}$-stable line, with character $\psi\colon G_\mathbb{Q} \to \mathbb{F}_5^\times$; by the Weil pairing, $G_\mathbb{Q}$ acts on $E[5]/L$ by $\psi' = \chi_5\psi^{-1}$. At an odd prime $\ell \neq 5$ of good reduction, $E[5]$ is unramified; at an odd prime $\ell \neq 5$ of multiplicative reduction, the semisimplification of $E[5]$ is trivial on the inertia group ([Sil94, Chapter V]). In both cases $\psi$ is unramified at $\ell$. At 5, the image of inertia under $\psi$ has order prime to 5, so $\psi$ is tamely ramified there, of conductor exponent at most 1. At 2, the Artin conductor exponents satisfy $a_2(\psi) + a_2(\psi') \leq a_2(E[5]) \leq f_2(E)$. Indeed, the Swan conductor is additive in the

exact sequence $0 \to L \to E[5] \to E[5]/L \to 0$, and the codimension of the inertia invariants of $E[5]$ is at least the sum of those of $L$ and $E[5]/L$; and $f_2(E) = \delta + \epsilon$, where $\delta$ is the Swan conductor of $E[5]$ and $\epsilon = 0, 1, 2$ according as the reduction is good, multiplicative or additive [Sil94, Section IV.10], and $\epsilon$ is at least the codimension of the inertia invariants of $E[5]$ (in the multiplicative case because inertia fixes the line coming from $\mu_5$, [Sil94, Chapter V]). Since $\chi_5$ is unramified at 2, $a_2(\psi') = a_2(\psi)$, so $a_2(\psi) \leq 2$. By the Kronecker–Weber theorem, $\psi$ is a Dirichlet character of conductor dividing $2^2 \cdot 5 = 20$. Let $q \equiv 1 \pmod 5$ be a prime of good reduction. Then $q^2 \equiv 1 \pmod{20}$, so $\psi(q) = \pm 1$, and the trace of $\mathrm{Frob}_q$ on $E[5]$ is $\psi(q) + q\psi(q)^{-1} \equiv 2\psi(q) \pmod 5$. It equals $a_q(E) \bmod 5$. □

**Lemma 7.4.11.** *Let $E/\mathbb{Q}$ be an elliptic curve with $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2)^2$, semistable at every odd prime, with $f_2(E) \leq 3$, and with good reduction at 5 or multiplicative reduction at 5 with $5 \mid v_5(\Delta_{\min})$. Then $E[5]$ is irreducible.*

*Proof.* Suppose that $L$, $\psi$, $\psi' = \chi_5\psi^{-1}$ are as in the proof of Lemma 7.4.10. As there, $\psi$ and $\psi'$ are unramified at every odd prime $\ell \neq 5$, and $2a_2(\psi) \leq f_2(E) \leq 3$. A character of $G_{\mathbb{Q}_2}$ of conductor exponent at most 1 corresponds, by local class field theory, to a character of $\mathbb{Q}_2^\times$ trivial on $1 + 2\mathbb{Z}_2 = \mathbb{Z}_2^\times$, so it is unramified; hence $\psi$ and $\psi'$ are unramified at 2. By [Ser87, Section 4.1], $E[5]$ is finite flat at 5, and by [Ray74, TO70] so are $L$ and $E[5]/L$, and the inertia group at 5 acts on each of them trivially or through $\chi_5$. Since $\psi\psi' = \chi_5$ is ramified at 5, one of $\psi, \psi'$ is unramified at 5, hence unramified everywhere, hence trivial, as $\mathbb{Q}$ has no nontrivial unramified extension. If $\psi = 1$, then $L \subset E(\mathbb{Q})$, and $E(\mathbb{Q})$ contains $(\mathbb{Z}/2)^2 \times \mathbb{Z}/5 \cong \mathbb{Z}/2 \times \mathbb{Z}/10$. If $\psi' = 1$, let $\phi\colon E \to E' = E/L$ be the isogeny of degree 5 over $\mathbb{Q}$. Then $\phi(E[5]) \cong E[5]/L$ is a subgroup of order 5 of $E'(\mathbb{Q})$, and since $\deg\phi$ is odd, $\phi$ maps $E[2]$ isomorphically onto $E'[2]$, so $E'(\mathbb{Q})$ contains $\mathbb{Z}/2 \times \mathbb{Z}/10$. Both cases contradict [Maz77]. □

For a prime $q \nmid 10ABC$ we define the *trace set* $T_q = T_q(A, B, C) \subseteq \mathbb{F}_5$: it consists of the residues modulo 5 of $\pm a_q(E_{Aa^5,Bb^5})$ for every point $(a : b : c) \in \mathbb{P}^2(\mathbb{F}_q)$ of $Aa^5 + Bb^5 + Cc^5 = 0$ with $abc \neq 0$, where

$$a_q(E_{u,v}) = -\sum_{X \in \mathbb{F}_q} \left(\frac{X(X-u)(X+v)}{q}\right) \qquad (u, v, u+v \in \mathbb{F}_q^\times),$$

together with the residues of $\pm(q+1)$ if the curve has a point over $\mathbb{F}_q$ with $abc = 0$. The sets used in Sections 7.5–7.10 are computed by certificate 1.4.5b, certificate 1.4.6b, certificate 1.4.7b, certificate 1.4.8b, certificate 1.4.9a and certificate 1.4.10a, each with two implementations: character sums as above, and point counting for all twelve signed orderings of the three terms and all scalings of $(a, b, c)$, which also confirms that these give only the two traces $\pm a_q$.

**Lemma 7.4.12.** *In the situation of Lemma 7.4.7(2), let $E$ be the Frey curve and $N_5$ its level from Lemma 7.4.9, and let $q \nmid 10ABC$ be a prime.*

*(1) If $q \nmid xyz$, then $E$ has good reduction at $q$ and $a_q(E) \bmod 5 \in T_q$. If $q \mid xyz$, then $q \parallel N_E$, $q \nmid N_5$, and $\pm(q+1) \bmod 5 \in T_q$.*

*(2) If $q \equiv 1 \pmod 5$, $T_q \cap \{2, 3\} = \emptyset$ and $f_2(E) \leq 5$, then $E[5]$ is irreducible.*

*(3) If $E[5]$ is irreducible, there are a newform $f \in S_2(\Gamma_0(N_5))$ and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_q(f) \bmod \lambda \in T_q$ for every prime $q \nmid 10ABC$.*

*Proof.* (1) Let $(a : b : c)$ be the reduction of $(x : y : z)$ modulo $q$, so $(x, y, z) \equiv \mu(a, b, c)$ with $\mu \in \mathbb{F}_q^\times$. If $q \nmid xyz$, then $q \nmid uvw$, so $E$ is good at $q$ (Lemma 7.4.8(1)); its reduction is, by Lemma 7.4.8(3), isomorphic to $E_{Ax^5,By^5}$ or its twist by $-1$, and $E_{Ax^5,By^5} \equiv E_{\mu^5 Aa^5,\mu^5 Bb^5}$ is the twist of $E_{Aa^5,Bb^5}$ by $\mu^5$. Quadratic twists over $\mathbb{F}_q$ change the trace at most by sign, so $a_q(E) = \pm a_q(E_{Aa^5,Bb^5})$. If $q \mid xyz$, then $q$ divides exactly one of $x, y, z$ (Lemma 7.4.7(2)), $(a : b : c)$ has a zero coordinate, and by the proof of Lemma 7.4.9, $q \parallel N_E$ and $q \nmid N_5$.

(2) By (1), $q \nmid xyz$, since $\pm(q+1) \equiv \pm 2 \pmod 5$. So $E$ is good at $q$ and $a_q(E) \not\equiv \pm 2 \pmod 5$. By Lemma 7.4.9, $E$ is semistable at every odd prime, and Lemma 7.4.10 applies.

(3) By [Sik12, Theorem 3 and Proposition 5.1] with $p = 5$ there are $f$ and $\lambda$ with $a_q(f) \equiv a_q(E) \pmod{\lambda}$ if $q \nmid 5N_E N_5$, and $a_q(f) \equiv \pm(q+1) \pmod{\lambda}$ if $q \nmid 5N_5$ and $q \parallel N_E$. Since $N_5$ divides $2^5ABC$, every prime $q \nmid 10ABC$ is in one of these two cases, and (1) gives the claim. □

The newforms of the levels $N_5$ are computed with PARI/GP (`mfinit`, `mfeigenbasis`). For each Galois orbit with coefficient field $K_f = \mathbb{Q}[y]/(P)$ the codes compute the maximal order of $K_f$ (`nfinit`, certified by `nfcertify`) and test every prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ separately: the pair (orbit, $\lambda$) is excluded at the first test prime $q$ for which $v_\lambda(a_q(f) - t) = 0$ for every $t \in T_q$. No coefficient field is discarded for being non-rational. The dimensions of the new subspaces are confirmed by the genus formula for $X_0(N)$ (certificate 1.4qb), and the characteristic polynomials of the Hecke operators $T_q$ used, by modular symbols (certificate 1.4qc).

**Lemma 7.4.13.** *Let $p$ be an odd prime and $\ell$ a prime ($\ell = p$ is allowed). Let $E_1, E_2/\mathbb{Q}_\ell$ be elliptic curves with multiplicative reduction such that $p \nmid v_\ell(\Delta_{\min}(E_1))\, v_\ell(\Delta_{\min}(E_2))$, and let $\phi\colon E_1[p] \to E_2[p]$ be an isomorphism of $\mathbb{F}_p[G_{\mathbb{Q}_\ell}]$-modules. Let $d \in \mathbb{F}_p^\times$ be defined by $e_2(\phi P, \phi Q) = e_1(P,Q)^d$, where $e_1, e_2$ are the Weil pairings. Then $d$ and $v_\ell(\Delta_{\min}(E_2))/v_\ell(\Delta_{\min}(E_1))$ have the same class in $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$.*

*Consequently, if $E, G/\mathbb{Q}$ are elliptic curves with $E[p] \cong G[p]$ as $\mathbb{F}_p[G_{\mathbb{Q}}]$-modules, and $\ell_1, \ell_2$ are primes at which both curves have multiplicative reduction with minimal discriminant valuations prime to $p$, then $v_{\ell_1}(\Delta_{\min}(G))/v_{\ell_1}(\Delta_{\min}(E))$ and $v_{\ell_2}(\Delta_{\min}(G))/v_{\ell_2}(\Delta_{\min}(E))$ are both squares or both nonsquares modulo $p$.*

*Proof.* Since $\phi^* e_2$ is again a nondegenerate alternating pairing with values in $\mu_p$ and the alternating forms on $E_1[p]$ form a space of dimension 1, $d$ is well defined. By [Sil94, Chapter V], $E_i$ is the twist by an unramified character $\varepsilon_i$ of the Tate curve $E_{q_i}$, with $v_\ell(q_i) = v_\ell(\Delta_{\min}(E_i)) \not\equiv 0 \pmod{p}$. Then $q_i$ is not a $p$th power, so the extension $0 \to \mu_p \to E_{q_i}[p] \to \mathbb{Z}/p \to 0$ does not split, and $\varepsilon_i \mu_p$ is the only $G_{\mathbb{Q}_\ell}$-stable line of $E_i[p]$. Hence $\phi$ maps $\varepsilon_1\mu_p$ to $\varepsilon_2\mu_p$, so $\varepsilon_1 = \varepsilon_2$ ($-1 \neq 1$ in $\mathbb{F}_p$), and twisting both curves by $\varepsilon_1$ changes neither $\phi$ nor the Weil pairings. So we may assume $E_i = E_{q_i}$. In the bases $(\zeta, Q_i)$ of [Sil94, Chapter V], written multiplicatively, $\phi(\zeta) = \zeta^a$ and $\phi(Q_1) = \zeta^b Q_2^{d'}$ with $a, d' \in \mathbb{F}_p^\times$. Comparing $\phi(\sigma Q_1)$ and $\sigma\phi(Q_1)$ gives $a\kappa_1(\sigma) + b = b\chi_p(\sigma) + d'\kappa_2(\sigma)$, so the cocycles $a\kappa_1$ and $d'\kappa_2$ differ by the coboundary of $\zeta^b$, and $q_1^a q_2^{-d'} \in \mathbb{Q}_\ell^{\times p}$. Taking valuations, $a\, v_\ell(q_1) \equiv d' v_\ell(q_2) \pmod{p}$. Finally $e_2(\phi\zeta, \phi Q_1) = e_2(\zeta, Q_2)^{ad'} = \zeta^{ad'} = e_1(\zeta, Q_1)^{ad'}$, so $d = ad' = (a/d')\, d'^2$, and $a/d' = v_\ell(q_2)/v_\ell(q_1)$.

For the consequence, take a $G_{\mathbb{Q}}$-isomorphism $\phi\colon E[p] \to G[p]$; its multiplier $d$ is the same for the restrictions to $G_{\mathbb{Q}_{\ell_1}}$ and $G_{\mathbb{Q}_{\ell_2}}$, and the first part applies at $\ell_1$ and at $\ell_2$. □

## 7.5 $14x^5 + 5y^5 + 3z^5 = 0$ ($H = 704$)

**Theorem 7.5.1.** *The only integer solution of $14x^5 + 5y^5 + 3z^5 = 0$ is $(x, y, z) = (0, 0, 0)$.*

**Setup.** We use the common framework of Section 7 (Lemmas 7.4.7–7.4.13). A primitive solution gives a Frey curve $E$ with $E[5]$ irreducible, and a newform of level 210 or 3360 congruent to it (Steps 1–2). A sieve with twelve auxiliary primes leaves only two rational newforms of level 3360 (Step 3). They are the newforms of the elliptic curves

$$G_+ :\ Y^2 = X^3 + X^2 - 890X - 10200, \qquad G_- :\ Y^2 = X^3 - X^2 - 890X + 10200$$

($G_-$ is the twist of $G_+$ by $-1$), and they are excluded by comparing the Weil pairings at 3 and at 5 (Step 4).

### Step 1: the Frey curve.

**Lemma 7.5.2.** *Let $(x, y, z)$ be a primitive solution. Then $xyz \neq 0$, the terms $14x^5, 5y^5, 3z^5$ are pairwise coprime, and $y, z$ are odd. Let $\varepsilon = \pm 1$ with $3\varepsilon z^5 \equiv -1 \pmod{4}$, and let $E = E_{u,v}$ with $(u, v, w) = \varepsilon(3z^5, 14x^5, 5y^5)$.*

*Then $E$ is semistable at every odd prime, it has multiplicative reduction at 3, 5, 7 with*

$$v_3(\Delta_{\min}) = 2 + 10v_3(z), \qquad v_5(\Delta_{\min}) = 2 + 10v_5(y), \qquad v_7(\Delta_{\min}) = 2 + 10v_7(x),$$

*and $f_2(E) = 5$ if $x$ is odd, while $f_2(E) = 1$ and $v_2(\Delta_{\min}) = 10v_2(x) - 6$ if $x$ is even. The level of Lemma 7.4.9 is $N_5 = 3360 = 2^5 \cdot 3 \cdot 5 \cdot 7$ if $x$ is odd and $N_5 = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ if $x$ is even.*

*Proof.* The coefficients $14 = 2 \cdot 7, 5, 3$ are pairwise coprime, every prime divides them at most once, and none is $\pm 1$. By Lemma 7.4.7, $xyz \neq 0$ and the three terms are pairwise coprime; $14x^5$ is even, so it is the even term, and $y$, $z$ are odd. Here $r = v_2(14x^5) = 1 + 5v_2(x)$. If $x$ is odd, then $r = 1$, and Lemma 7.4.8(2) gives $f_2 = 5$. If $x$ is even, then $r \geq 6$, $f_2 = 1$ and $v_2(\Delta_{\min}) = 2r - 8 = 10v_2(x) - 6 \equiv 4 \pmod 5$, so 2 divides $N_5$. The odd primes and $N_5$ are given by Lemma 7.4.9: the odd prime divisors of $14 \cdot 5 \cdot 3$ are $3, 5, 7$, and $v_\ell(\Delta_{\min}) = 2v_\ell(uvw)$ (certificate 1.4.5a; the 2-adic data are also checked with PARI's Tate algorithm on all residue classes of $x$ and $z$ modulo $2^6$ in certificate 1.4.5c). □

**Step 2: irreducibility and level lowering.** The trace sets $T_q = T_q(14, 5, 3)$ of the common framework are, for the primes $q$ used below (certificate 1.4.5b),

| $q$ | $T_q$ | $q$ | $T_q$ | $q$ | $T_q$ |
|---|---|---|---|---|---|
| 11 | $\{0, 2, 3\}$ | 41 | $\mathbb{F}_5^\times$ | 131 | $\{0, 2, 3\}$ |
| 13 | $\mathbb{F}_5^\times$ | 61 | $\mathbb{F}_5^\times$ | 151 | $\mathbb{F}_5^\times$ |
| 17 | $\mathbb{F}_5^\times$ | 71 | $\{2, 3\}$ | 181 | $\mathbb{F}_5^\times$ |
| 31 | $\{0, 1, 4\}$ | 101 | $\mathbb{F}_5^\times$ | 191 | $\mathbb{F}_5^\times$ |

For example, modulo 31 the curve $14a^5 + 5b^5 + 3c^5 = 0$ has 50 points, none with a zero coordinate, and the traces of the curves $E_{14a^5, 5b^5}$ at these points are 0 and $\pm 4$.

**Lemma 7.5.3.** *$E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(N_5))$, with $N_5$ as in Lemma 7.5.2, and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_q(f) \bmod \lambda \in T_q$ for the twelve primes $q$ of the table.*

*Proof.* We have $31 \equiv 1 \pmod 5$, $T_{31} \cap \{2, 3\} = \emptyset$ and $f_2(E) \leq 5$, so $E[5]$ is irreducible by Lemma 7.4.12(2). Since no $q$ in the table divides $10 \cdot 14 \cdot 5 \cdot 3$, Lemma 7.4.12(3) gives $f$ and $\lambda$. □

**Step 3: the sieve.**

**Lemma 7.5.4.** *(1) $S_2(\Gamma_0(210))^{\text{new}}$ has dimension 5 and consists of five rational newforms. None of them satisfies the conditions of Lemma 7.5.3 (with $\lambda = 5$).*

*(2) $S_2(\Gamma_0(3360))^{\text{new}}$ has dimension 48 and 36 Galois orbits of newforms: 26 rational, 8 with quadratic and 2 with cubic coefficient fields, which give 38 pairs (orbit, $\lambda \mid 5$). Exactly two pairs satisfy the conditions of Lemma 7.5.3; they are two rational newforms $f_+$, $f_-$ with $\lambda = 5$.*

*Proof.* This is a finite computation (certificate 1.4.5c). At level 210, three forms are excluded at $q = 11$, one at $q = 61$ and one at $q = 71$. At level 3360, the numbers of pairs that remain after $q = 11, 13, 17, 31$ are $12, 8, 6, 2$, and the two remaining pairs satisfy the conditions at all twelve primes. The prime 5 is inert in the coefficient fields of six of the quadratic orbits and ramified in the other two (whose field is $\mathbb{Q}(\sqrt{5})$), and it has two prime ideals, of residue degrees 1 and 2, in the two cubic fields; every one of these prime ideals is tested. The dimensions are also given by the genus formula (certificate 1.4qb), and the Hecke polynomials at the twelve primes agree with those computed by modular symbols (certificate 1.4qc). □

**Step 4: the two remaining newforms.**

**Lemma 7.5.5.** *The newform $f$ of Lemma 7.5.3 is neither $f_+$ nor $f_-$.*

*Proof.* The curves $G_\pm$ have conductor 3360 and minimal discriminant $2^6 \cdot 3^6 \cdot 5^2 \cdot 7^4$, and $c_4(G_\pm) = 2^4 \cdot 2671$ is prime to 15, so they have multiplicative reduction at 3 and 5, with $v_3(\Delta_{\min}) = 6$ and $v_5(\Delta_{\min}) = 2$. By [BCDT01] their newforms lie in $S_2(\Gamma_0(3360))$. The index of $\Gamma_0(3360)$ in $\mathrm{SL}_2(\mathbb{Z})$ is 9216, so the Sturm bound is $9216/6 = 1536$, and the coefficients $a_0, \dots, a_{1536}$ of $f_+$ and $f_-$ are those of $G_+$ and $G_-$, respectively, that is, $a_0 = 0$ and the coefficients $a_n(G_\pm)$ of $L(G_\pm, s)$, which are those of the newforms of $G_\pm$ by [BCDT01] (certificate 1.4.5d). By [Stu87], $f_\pm$ is the newform of $G_\pm$.

Suppose that $f = f_\pm$. By [Sik12, Section 5], $E[5] \cong G_\pm[5]$ as $\mathbb{F}_5[G_\mathbb{Q}]$-modules. Both $E$ and $G_\pm$ have multiplicative reduction at 3 and at 5, with discriminant valuations prime to 5: by Lemma 7.5.2, $v_3(\Delta_{\min}(E)) \equiv v_5(\Delta_{\min}(E)) \equiv 2 \pmod 5$. The ratios are

$$\frac{v_3(\Delta_{\min}(G_\pm))}{v_3(\Delta_{\min}(E))} \equiv \frac{6}{2} \equiv 3, \qquad \frac{v_5(\Delta_{\min}(G_\pm))}{v_5(\Delta_{\min}(E))} \equiv \frac{2}{2} = 1 \pmod 5,$$

and 3 is not a square modulo 5, while 1 is. This contradicts Lemma 7.4.13 with $p = 5$, $\ell_1 = 3$, $\ell_2 = 5$. □

The ratio $v_3(\Delta_{\min})/v_5(\Delta_{\min})$ is a nonsquare modulo 5 for all four curves isogenous to $G_+$ (certificate 1.4.5d), as it must be, since the argument does not depend on the choice of the curve in its isogeny class.

*Proof of Theorem 7.5.1.* If there is a solution other than $(0,0,0)$, dividing it by the greatest common divisor of its coordinates gives a primitive solution. By Lemmas 7.5.2 and 7.5.3 there is a newform $f$ of level 210 or 3360 with the conditions of Lemma 7.5.3. By Lemma 7.5.4, $f$ is $f_+$ or $f_-$, which contradicts Lemma 7.5.5. □

## 7.6 $21x^5 + 5y^5 + 4z^5 = 0$ ($H = 960$)

**Theorem 7.6.1.** *The only integer solution of* $21x^5 + 5y^5 + 4z^5 = 0$ *is* $(x, y, z) = (0, 0, 0)$.

**Setup.** We use the common framework of Section 7 (Lemmas 7.4.7–7.4.12). A primitive solution gives a Frey curve $E$ with $E[5]$ irreducible and a newform of level 210 or 840 congruent to it (Steps 1–2); the sieve of Step 3 excludes all newforms of these levels, using only the auxiliary primes 11, 31, 41 and 61.

### Step 1: the Frey curve.

**Lemma 7.6.2.** *Let $(x, y, z)$ be a primitive solution. Then $xyz \neq 0$, the terms $21x^5, 5y^5, 4z^5$ are pairwise coprime, and $x$, $y$ are odd. Let $\varepsilon = \pm 1$ with $\varepsilon x \equiv 3 \pmod 4$, and let $E = E_{u,v}$ with $(u, v, w) = \varepsilon(21x^5, 4z^5, 5y^5)$. Then $E$ is semistable at every odd prime, with multiplicative reduction and $v_\ell(\Delta_{\min}) \equiv 2 \pmod 5$ at $\ell = 3, 5, 7$. If $z$ is odd, then $E$ has type $\mathrm{I}_1^*$ at 2, $f_2(E) = 3$ and $N_5 = 840 = 2^3 \cdot 3 \cdot 5 \cdot 7$. If $z$ is even, then $f_2(E) = 1$, $v_2(\Delta_{\min}) = 10v_2(z) - 4$ and $N_5 = 210$.*

*Proof.* The coefficients $21 = 3 \cdot 7, 5, 4 = 2^2$ are pairwise coprime, with exponents at most 2, and none is $\pm 1$. By Lemma 7.4.7, $xyz \neq 0$, the terms are pairwise coprime, and since $4z^5$ is even, $x$ and $y$ are odd. As $x^5 \equiv x$ and $21 \equiv 1 \pmod 4$, $u = 21\varepsilon x^5 \equiv \varepsilon x \equiv -1 \pmod 4$. Here $r = v_2(4z^5) = 2 + 5v_2(z)$. If $z$ is odd, then $r = 2$ and Lemma 7.4.8(2) gives type $\mathrm{I}_1^*$, $f_2 = 3$, $v_2(\Delta_{\min}) = 8$. If $z$ is even, then $r \geq 7$, $f_2 = 1$, and $v_2(\Delta_{\min}) = 2r - 8 = 10v_2(z) - 4 \equiv 1 \pmod 5$, so 2 divides $N_5$. At $\ell = 3, 5, 7$, $v_\ell(\Delta_{\min}) = 2 + 10v_\ell(xyz)$, and Lemma 7.4.9 gives $N_5$ (certificate 1.4.6a; the 2-adic data are also checked with PARI on all residue classes of $\varepsilon x$ and $z$ modulo $2^6$ in certificate 1.4.6c). □

**Step 2: irreducibility and level lowering.** The trace sets $T_q = T_q(21,5,4)$ are (certificate 1.4.6b)

| $q$ | $T_q$ | $q$ | $T_q$ | $q$ | $T_q$ |
|---|---|---|---|---|---|
| 11 | $\{1,4\}$ | 41 | $\mathbb{F}_5^\times$ | 151 | $\{0,2,3\}$ |
| 13 | $\mathbb{F}_5^\times$ | 61 | $\{2,3\}$ | 181 | $\{2,3\}$ |
| 17 | $\mathbb{F}_5^\times$ | 101 | $\mathbb{F}_5^\times$ | 211 | $\mathbb{F}_5^\times$ |
| 31 | $\{0,1,4\}$ | 131 | $\mathbb{F}_5^\times$ | | |

**Lemma 7.6.3.** *$E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(N_5))$, with $N_5 \in \{210, 840\}$ as in Lemma 7.6.2, and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_q(f) \bmod \lambda \in T_q$ for the eleven primes $q$ of the table.*

*Proof.* As $31 \equiv 1 \pmod 5$, $T_{31} \cap \{2,3\} = \emptyset$ and $f_2(E) \le 5$, Lemma 7.4.12(2) applies; then Lemma 7.4.12(3) gives $f$ and $\lambda$, since no $q$ of the table divides $10 \cdot 21 \cdot 5 \cdot 4$. □

**Step 3: the sieve.**

**Lemma 7.6.4.** *No newform of level 210 or 840 satisfies the conditions of Lemma 7.6.3. More precisely, $S_2(\Gamma_0(210))^{\text{new}}$ consists of five rational newforms, two excluded at $q = 11$, two at $q = 31$ and one at $q = 61$; $S_2(\Gamma_0(840))^{\text{new}}$ has dimension 12 and 11 Galois orbits, ten rational and one with coefficient field $\mathbb{Q}(\sqrt{2})$, in which 5 is inert; of these 11 pairs (orbit, $\lambda$), five are excluded at $q = 11$, one at $q = 31$, two at $q = 41$ and three at $q = 61$.*

*Proof.* This is a finite computation (certificate 1.4.6c); the dimensions and the Hecke polynomials are confirmed by certificate 1.4qb and certificate 1.4qc. □

*Proof of Theorem 7.6.1.* A solution other than $(0,0,0)$ gives a primitive one, and then, by Lemmas 7.6.2 and 7.6.3, a newform of level 210 or 840 that Lemma 7.6.4 excludes. □

## 7.7 $17x^5 + 6y^5 + 3z^5 = 0$ ($H = 832$)

**Theorem 7.7.1.** *The only integer solution of $17x^5 + 6y^5 + 3z^5 = 0$ is $(x,y,z) = (0,0,0)$.*

**Setup.** Modulo 3 the equation gives $3 \mid x$, and with $x = 3X$ it becomes

$$1377X^5 + 2y^5 + z^5 = 0, \qquad 1377 = 3^4 \cdot 17.$$

We apply the common framework of Section 7 (Lemmas 7.4.7–7.4.12) to this equation: a primitive solution gives a Frey curve $E$ with $E[5]$ irreducible and a newform of level 102 or 1632 (Steps 1–2), and the auxiliary primes 41, 11 and 131 exclude all of them (Step 3).

**Step 1: the Frey curve.**

**Lemma 7.7.2.** *Let $(x,y,z)$ be a primitive solution. Then $x = 3X$, $(X,y,z)$ is a primitive solution of $1377X^5 + 2y^5 + z^5 = 0$, $Xyz \neq 0$, the terms $1377X^5$, $2y^5$, $z^5$ are pairwise coprime, and $X$, $z$ are odd. Let $\varepsilon = \pm 1$ with $\varepsilon X \equiv 3 \pmod 4$, and let $E = E_{u,v}$ with $(u,v,w) = \varepsilon(1377X^5, 2y^5, z^5)$. Then $E$ is semistable at every odd prime, with multiplicative reduction at 3 and 17, $v_3(\Delta_{\min}) = 8 + 10v_3(X)$, $v_{17}(\Delta_{\min}) = 2 + 10v_{17}(X)$, and $5 \nmid N_5$. If $y$ is odd, then $f_2(E) = 5$ and $N_5 = 1632 = 2^5 \cdot 3 \cdot 17$; if $y$ is even, then $f_2(E) = 1$, $v_2(\Delta_{\min}) = 10v_2(y) - 6$ and $N_5 = 102 = 2 \cdot 3 \cdot 17$.*

*Proof.* Modulo 3, $17x^5 + 6y^5 + 3z^5 \equiv 2x^5$, so $3 \mid x$; dividing $17 \cdot 3^5X^5 + 6y^5 + 3z^5 = 0$ by 3 gives the new equation. A common prime factor of $X, y, z$ would divide $x, y, z$, so $(X,y,z)$ is primitive. The coefficients $3^4 \cdot 17$, 2, 1 are pairwise coprime with exponents at most 4, and only one of them is $\pm 1$. By Lemma 7.4.7, $Xyz \neq 0$, the terms are pairwise coprime, and since $2y^5$ is even, $X$ and $z$ are odd. As $1377 \equiv 1 \pmod 4$, $u \equiv \varepsilon X \equiv -1 \pmod 4$. Here $r = 1 + 5v_2(y)$; Lemma 7.4.8(2) gives $f_2 = 5$ if $y$ is odd, and $f_2 = 1$, $v_2(\Delta_{\min}) = 2r - 8 = 10v_2(y) - 6 \equiv 4 \pmod 5$ if $y$ is even. Lemma 7.4.9 gives the odd primes and $N_5$; $5 \nmid 1377 \cdot 2$ (certificate 1.4.7a; the 2-adic data are also checked with PARI in certificate 1.4.7c). □

**Step 2: irreducibility and level lowering.** The trace sets $T_q = T_q(1377, 2, 1)$ are (certificate 1.4.7b)

| $q$ | 11 | 31 | 41 | 131 | 241 |
|---|---|---|---|---|---|
| $T_q$ | $\{2,3\}$ | $\{0,1,4\}$ | $\{0\}$ | $\{0,2,3\}$ | $\{0,2,3\}$ |

For example, modulo 41 the curve has 25 points, none with a zero coordinate, and the traces at these points are $\pm 10$.

**Lemma 7.7.3.** *$E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(N_5))$, with $N_5 \in \{102, 1632\}$ as in Lemma 7.7.2, and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_q(f) \bmod \lambda \in T_q$ for the five primes $q$ of the table.*

*Proof.* As $31 \equiv 1 \pmod 5$, $T_{31} \cap \{2,3\} = \emptyset$ and $f_2(E) \le 5$, Lemma 7.4.12(2) applies (so does $q = 41$); Lemma 7.4.12(3) gives $f$ and $\lambda$, since no $q$ of the table divides $10 \cdot 1377 \cdot 2$. □

**Step 3: the sieve.**

**Lemma 7.7.4.** *No newform of level 102 or 1632 satisfies the conditions of Lemma 7.7.3. More precisely, $S_2(\Gamma_0(102))^{\text{new}}$ consists of three rational newforms, one excluded at $q = 41$ and two at $q = 11$. $S_2(\Gamma_0(1632))^{\text{new}}$ has dimension 32 and 20 Galois orbits: 12 rational, four quadratic and four cubic, in whose coefficient fields 5 is inert, so there are 20 pairs (orbit, $\lambda$). The condition at $q = 41$ leaves 8 pairs and the condition at $q = 11$ leaves two rational newforms, with $(a_{41}, a_{11}) = (-5, 3)$ and $(-5, -3)$; their coefficients $a_{131} = 9$ and $-9$ are 4 and 1 modulo 5, not in $T_{131}$.*

*Proof.* This is a finite computation (certificate 1.4.7c); the dimensions and the Hecke polynomials are confirmed by certificate 1.4qb and certificate 1.4qc. □

*Proof of Theorem 7.7.1.* A solution other than $(0,0,0)$ gives a primitive one, and then, by Lemmas 7.7.2 and 7.7.3, a newform of level 102 or 1632 that Lemma 7.7.4 excludes. □

## 7.8 $17x^5 + 9y^5 + 5z^5 = 0$ ($H = 992$)

**Theorem 7.8.1.** *The only integer solution of $17x^5 + 9y^5 + 5z^5 = 0$ is $(x, y, z) = (0, 0, 0)$.*

**Setup.** We use the common framework of Section 7 (Lemmas 7.4.7–7.4.12). Here the Frey curve is semistable everywhere, the only level is 510 (Steps 1–2), and the auxiliary primes 41 and 11 exclude all newforms of that level (Step 3).

**Step 1: the Frey curve.**

**Lemma 7.8.2.** *Let $(x, y, z)$ be a primitive solution. Then $xyz \neq 0$, the terms $17x^5$, $9y^5$, $5z^5$ are pairwise coprime, and exactly one of $x, y, z$ is even. Let $t_j$ be the even term, $t_i$ the first and $t_k$ the second of the two odd terms in the order $17x^5, 9y^5, 5z^5$, $\varepsilon = \pm 1$ with $\varepsilon t_i \equiv -1 \pmod 4$, and $E = E_{u,v}$ with $(u, v, w) = \varepsilon(t_i, t_j, t_k)$. Then $E$ is semistable, with multiplicative reduction at $2, 3, 5, 17$,*

$$v_2(\Delta_{\min}) = 10e - 8 \quad (e = v_2(xyz) \ge 1),$$
$$v_3(\Delta_{\min}) = 4 + 10v_3(y), \qquad v_5(\Delta_{\min}) = 2 + 10v_5(z), \qquad v_{17}(\Delta_{\min}) = 2 + 10v_{17}(x),$$

*and $N_5 = 510 = 2 \cdot 3 \cdot 5 \cdot 17$.*

*Proof.* The coefficients $17$, $9 = 3^2$, $5$ are pairwise coprime, with exponents at most 2, and none is $\pm 1$. By Lemma 7.4.7, $xyz \neq 0$, the terms are pairwise coprime and exactly one is even; as the coefficients are odd, exactly one variable is even, and $r = 5e$ with $e = v_2(xyz) \ge 1$. By Lemma 7.4.8(2), $f_2 = 1$ and $v_2(\Delta_{\min}) = 2r - 8 = 10e - 8 \equiv 2 \pmod 5$, so 2 divides $N_5$. The odd primes and $N_5$ are given by Lemma 7.4.9 (certificate 1.4.8a; the 2-adic data are also checked with PARI for each choice of the even variable in certificate 1.4.8c). □

**Step 2: irreducibility and level lowering.** The trace sets $T_q = T_q(17,9,5)$ are (certificate 1.4.8b)

| $q$ | 11 | 31 | 41 | 71 |
|---|---|---|---|---|
| $T_q$ | $\{2,3\}$ | $\{2,3\}$ | $\{0\}$ | $\{2,3\}$ |

Modulo 41 the curve has 25 points, none with a zero coordinate, and the traces at these points are $\pm 10$.

**Lemma 7.8.3.** *$E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(510))$ and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_q(f) \bmod \lambda \in T_q$ for $q = 11, 31, 41, 71$.*

*Proof.* As $41 \equiv 1 \pmod 5$, $T_{41} \cap \{2,3\} = \emptyset$ and $f_2(E) = 1$, Lemma 7.4.12(2) applies; Lemma 7.4.12(3) gives $f$ and $\lambda$. □

**Step 3: the sieve.**

**Lemma 7.8.4.** *No newform of level 510 satisfies the conditions of Lemma 7.8.3. More precisely, $S_2(\Gamma_0(510))^{\text{new}}$ has dimension 9 and 8 Galois orbits, seven rational and one with coefficient field $\mathbb{Q}(\sqrt{6})$, in which 5 splits; this gives 9 pairs (orbit, $\lambda$). The condition at $q = 41$ leaves three pairs: two rational newforms, with $a_{11} = 0$ and 4, and one prime ideal $\lambda \mid 5$ of $\mathbb{Q}(\sqrt{6})$, at which $a_{41} = 2\sqrt{6} + 2 \equiv 0$ and $a_{11} = 0$. None of $0, 4, 0$ lies in $T_{11}$.*

*Proof.* This is a finite computation (certificate 1.4.8c); the dimension and the Hecke polynomials are confirmed by certificate 1.4qb and certificate 1.4qc. □

*Proof of Theorem 7.8.1.* A solution other than $(0,0,0)$ gives a primitive one, and then, by Lemmas 7.8.2 and 7.8.3, a newform of level 510 that Lemma 7.8.4 excludes. □

## 7.9 $14x^5 + 13y^5 + 2z^5 = 0$ ($H = 928$)

**Theorem 7.9.1.** *The only integer solution of $14x^5 + 13y^5 + 2z^5 = 0$ is $(x,y,z) = (0,0,0)$.*

**Setup.** Modulo 2 the equation gives $2 \mid y$, and with $y = 2Y$ it becomes

$$7x^5 + 208Y^5 + z^5 = 0, \qquad 208 = 2^4 \cdot 13.$$

We apply the common framework of Section 7 (Lemmas 7.4.7–7.4.12) to this equation. The Frey curve has good or multiplicative reduction at 2 with $5 \mid v_2(\Delta_{\min})$, so the prime 2 disappears from the level, which is 91 (Step 1). Irreducibility follows from Mazur's theorem (Step 2), and the single auxiliary prime 11 excludes all newforms of level 91 (Step 3).

**Step 1: the Frey curve.**

**Lemma 7.9.2.** *Let $(x,y,z)$ be a primitive solution. Then $y = 2Y$, $(x,Y,z)$ is a primitive solution of $7x^5 + 208Y^5 + z^5 = 0$, $xYz \neq 0$, the terms $7x^5$, $208Y^5$, $z^5$ are pairwise coprime, and $x$, $z$ are odd. Let $\varepsilon = \pm 1$ with $\varepsilon x \equiv 1 \pmod 4$, and let $E = E_{u,v}$ with $(u,v,w) = \varepsilon(7x^5, 208Y^5, z^5)$. Then $E$ is semistable, with multiplicative reduction at 7 and 13, $v_7(\Delta_{\min}) = 2 + 10v_7(x)$, $v_{13}(\Delta_{\min}) = 2 + 10v_{13}(Y)$; at 2 it has good reduction if $Y$ is odd, and multiplicative reduction with $v_2(\Delta_{\min}) = 10v_2(Y)$ if $Y$ is even; at 5 it has good reduction, or multiplicative reduction with $5 \mid v_5(\Delta_{\min})$. Its level is $N_5 = 91 = 7 \cdot 13$.*

*Proof.* Modulo 2, $14x^5 + 13y^5 + 2z^5 \equiv y^5$, so $y = 2Y$, and dividing by 2 gives the new equation; a common prime factor of $x, Y, z$ would divide $x, y, z$. The coefficients $7$, $2^4 \cdot 13$, $1$ are pairwise coprime with exponents at most 4, and only one is $\pm 1$. By Lemma 7.4.7, $xYz \neq 0$, the terms are pairwise coprime, and since $208Y^5$ is even, $x$ and $z$ are odd. As $7 \equiv -1 \pmod 4$, $u = 7\varepsilon x^5 \equiv -\varepsilon x \equiv -1 \pmod 4$. Here $r = v_2(208Y^5) = 4 + 5v_2(Y)$. If $Y$ is odd, then $r = 4$ and $E$ has good reduction at 2 by Lemma 7.4.8(2). If $Y$ is even, then $r \geq 9$, the reduction is multiplicative and $v_2(\Delta_{\min}) = 2r - 8 = 10v_2(Y)$; since $r \equiv 4 \pmod 5$, 2 does not divide $N_5$ (Lemma 7.4.9). The rest is Lemma 7.4.9, with $5 \nmid 7 \cdot 208$ (certificate 1.4.9a; the 2-adic data are also checked with PARI in certificate 1.4.9b). □

**Step 2: irreducibility and level lowering.**

**Lemma 7.9.3.** *$E[5]$ is irreducible, and there are a newform $f \in S_2(\Gamma_0(91))$ and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_{11}(f) \bmod \lambda \in T_{11}(7, 208, 1)$.*

*Proof.* By Lemma 7.9.2, $E$ has full rational 2-torsion, is semistable at every odd prime, has $f_2(E) \le 1$, and has good reduction at 5 or multiplicative reduction with $5 \mid v_5(\Delta_{\min})$. Lemma 7.4.11 gives irreducibility, and Lemma 7.4.12(3) gives $f$ and $\lambda$ ($11 \nmid 10 \cdot 7 \cdot 208$). □

**Lemma 7.9.4.** *Every point of $7a^5 + 208b^5 + c^5 = 0$ over $\mathbb{F}_{11}$ has $a = 0$ and $bc \neq 0$. Hence $11 \mid x$, $11 \nmid yz$, and $T_{11}(7, 208, 1) = \{2, 3\}$.*

*Proof.* The nonzero fifth powers modulo 11 are $\pm 1$, and $208 \equiv -1 \pmod{11}$. If $abc \neq 0$, then $7a^5 - b^5 + c^5 \equiv 7 \pm 1 \pm 1$ or $-7 \pm 1 \pm 1$, which is one of $\pm 5, \pm 7, \pm 9$ and is not 0 modulo 11. If $b = 0$ and $ac \neq 0$, or $c = 0$ and $ab \neq 0$, the two remaining terms add up to $\pm 7 \pm 1 \not\equiv 0$, and two vanishing coordinates force the third to vanish. So $a = 0$, and then $b^5 = c^5$ with $bc \neq 0$: the five points $(0 : 1 : c)$ with $c \in \{1, 3, 4, 5, 9\}$. All of them have a zero coordinate, so $T_{11} = \{\pm 12 \bmod 5\} = \{2, 3\}$ (certificate 1.4.9a). □

**Step 3: the newforms of level 91.**

**Lemma 7.9.5.** *$S_2(\Gamma_0(91))^{\text{new}}$ has dimension 7 and four Galois orbits, of dimensions $1, 1, 2, 3$. The minimal polynomials of their eigenvalues $a_{11}$ are*

$$T, \qquad T + 6, \qquad T^2 - 18, \qquad T^3 - 2T^2 - 6T + 8.$$

*None of them has 2 or 3 as a root modulo 5.*

*Proof.* The newforms are computed with PARI/GP (certificate 1.4.9b; the dimension and the Hecke polynomial are confirmed by certificate 1.4qb and certificate 1.4qc). The values of the four polynomials at $T = 2$ and $T = 3$ are $(2, 3)$, $(3, 4)$, $(1, 1)$ and $(1, 4)$ modulo 5. □

*Proof of Theorem 7.9.1.* Suppose that there is a solution other than $(0, 0, 0)$, and take a primitive one. By Lemmas 7.9.3 and 7.9.4, there is a newform $f$ of level 91 with $a_{11}(f) \equiv 2$ or $3 \pmod{\lambda}$ for a prime ideal $\lambda \mid 5$. The minimal polynomial of $a_{11}(f)$ has integer coefficients and vanishes at $a_{11}(f)$, so its reduction modulo 5 vanishes at 2 or 3, contrary to Lemma 7.9.5. □

## 7.10 $4x^5 + 4y^5 + 11z^5 = 0$ ($H = 608$)

**Theorem 7.10.1.** *The integer solutions of $4x^5 + 4y^5 + 11z^5 = 0$ are exactly $(x, y, z) = (n, -n, 0)$, $n \in \mathbb{Z}$.*

**Setup.** Modulo 4 the equation gives $2 \mid z$, and with $z = 2w$ it becomes

$$x^5 + y^5 + 88w^5 = 0, \qquad 88 = 2^3 \cdot 11.$$

The solutions with a zero coordinate are elementary (Step 1). For the others we apply the common framework of Section 7 (Lemmas 7.4.7–7.4.12): the Frey curve gives a newform of level 22 or 88, irreducibility follows from Mazur's theorem (Step 2), and the single auxiliary prime 3 excludes all newforms of these levels (Step 3).

**Step 1: reduction and the solutions with a zero coordinate.**

**Lemma 7.10.2.** *If $(x,y,z)$ is a primitive solution, then $z = 2w$ and $(x,y,w)$ is a primitive solution of $x^5+y^5+88w^5=0$. If moreover $xyz=0$, then $(x,y,z)=\pm(1,-1,0)$. Hence the integer solutions with $xyz=0$ are the $(n,-n,0)$, $n\in\mathbb{Z}$.*

*Proof.* Modulo 4, $11z^5\equiv 0$, so $z$ is even; dividing $4x^5+4y^5+11\cdot 2^5w^5=0$ by 4 gives the new equation, and a common prime factor of $x,y,w$ would divide $x,y,z$. The coefficients $1,1,2^3\cdot 11$ are pairwise coprime with exponents at most 3. By Lemma 7.4.7(1), $x=0$ would force $|1|=|88|=1$, and so would $y=0$; hence a zero coordinate can only be $w=0$, and then $(x,y)=\pm(1,-1)$. Every nonzero solution is a multiple of a primitive one, and $(n,-n,0)$ is a solution for every $n$. □

**Lemma 7.10.3.** *Let $(x,y,z)$ be a primitive solution with $xyz\neq 0$, and $z=2w$. Then the terms $x^5$, $y^5$, $88w^5$ are pairwise coprime, and $x$, $y$ are odd. Let $\varepsilon=\pm1$ with $\varepsilon x\equiv 3 \pmod 4$, and let $E=E_{u,v}$ with $(u,v,w')=\varepsilon(x^5,88w^5,y^5)$. Then $E$ is semistable at every odd prime, with multiplicative reduction at 11 and $v_{11}(\Delta_{\min})=2+10v_{11}(w)$, and it has good reduction at 5 or multiplicative reduction with $5\mid v_5(\Delta_{\min})$. If $w$ is odd, then $E$ has type $\mathrm{III}^*$ at 2, $f_2(E)=3$ and $N_5=88=2^3\cdot 11$; if $w$ is even, then $f_2(E)=1$, $v_2(\Delta_{\min})=10v_2(w)-2$ and $N_5=22=2\cdot 11$.*

*Proof.* By Lemma 7.4.7(2) applied to $x^5+y^5+88w^5=0$, the terms are pairwise coprime, and $88w^5$ is the even one. Here $r=v_2(88w^5)=3+5v_2(w)$. If $w$ is odd, then $r=3$ and Lemma 7.4.8(2) gives type $\mathrm{III}^*$, $f_2=3$, $v_2(\Delta_{\min})=10$. If $w$ is even, then $r\geq 8$, $f_2=1$ and $v_2(\Delta_{\min})=2r-8=10v_2(w)-2\equiv 3 \pmod 5$. The rest is Lemma 7.4.9, with $5\nmid 88$ (certificate 1.4.10a; the 2-adic data are also checked with PARI in certificate 1.4.10b). □

**Step 2: irreducibility, level lowering and the prime 3.**

**Lemma 7.10.4.** *$E[5]$ is irreducible, and there are a newform $f\in S_2(\Gamma_0(N_5))$, $N_5\in\{22,88\}$ as in Lemma 7.10.3, and a prime ideal $\lambda\mid 5$ of $\mathcal{O}_{K_f}$ such that $a_3(f) \bmod \lambda \in T_3(1,1,88)$.*

*Proof.* $E$ has full rational 2-torsion, is semistable at every odd prime, has $f_2(E)\leq 3$, and has good reduction at 5 or multiplicative reduction with $5\mid v_5(\Delta_{\min})$ (Lemma 7.10.3). Lemma 7.4.11 gives irreducibility, and Lemma 7.4.12(3) gives $f$ and $\lambda$ ($3\nmid 10\cdot 88$). □

**Lemma 7.10.5.** $T_3(1,1,88)=\{0,1,4\}$.

*Proof.* Over $\mathbb{F}_3$ we have $a^5=a$ and $88\equiv 1$, so the curve is the line $a+b+c=0$, with the four points $(1:1:1)$, $(1:2:0)$, $(1:0:2)$, $(0:1:2)$. At $(1:1:1)$ the curve $E_{1,1}$ is $Y^2=X(X-1)(X+1)=X^3-X$, which has four points over $\mathbb{F}_3$, so its trace is 0. The other three points have a zero coordinate and contribute $\pm(3+1)\equiv\pm 4$. Hence $T_3=\{0,4,1\}$ (certificate 1.4.10a). □

**Step 3: the newforms of levels 22 and 88.**

**Lemma 7.10.6.** *$S_2(\Gamma_0(22))^{\mathrm{new}}=0$. $S_2(\Gamma_0(88))^{\mathrm{new}}$ has dimension 3 and two Galois orbits, of dimensions 1 and 2, and the minimal polynomials of their eigenvalues $a_3$ are $T+3$ and $T^2-T-4$. Neither has a root in $\{0,1,4\}$ modulo 5.*

*Proof.* The newforms are computed with PARI/GP (certificate 1.4.10b; the dimensions and the Hecke polynomial are confirmed by certificate 1.4qb and certificate 1.4qc). The values of $T+3$ at $0,1,4$ are $3,4,2$ modulo 5, and those of $T^2-T-4$ are $1,1,3$; in fact $T^2-T-4$ is irreducible modulo 5, its discriminant 17 being a nonsquare. □

*Proof of Theorem 7.10.1.* By Lemma 7.10.2, it suffices to show that there is no primitive solution with $xyz\neq 0$. For such a solution, Lemma 7.10.4 gives a newform of level 22 or 88; there is none of level 22, and for one of level 88, $a_3(f) \bmod \lambda\in\{0,1,4\}$ by Lemma 7.10.5, so the reduction modulo 5 of the minimal polynomial of $a_3(f)$ would have a root in $\{0,1,4\}$, contrary to Lemma 7.10.6. □

## Reproducibility

The ancillary files under `anc/` contain the programs, exact witnesses and reference outputs for the computations. From the extracted submission root, run `python3 anc/unpack_reproducibility.py` to verify the bundles and restore the working directories. The source of this paper compiles directly with pdfLaTeX and BibTeX. Section and equation labels in the restored historical records refer to the corresponding original proof files.

The directory `v1/anc/` contains the case-by-case certificate map for the first thirty-eight proofs. In `ten/`, the left-column curves correspond to indices 1–5 and the right-column curves to 6–10. Run `python3 verify.py summary` for the solution lists and numerical endpoints, or `python3 verify.py all` for the full arithmetic replay, including the prime-ideal counts. The stages `l1-rank`, `l1-height` and `l1-sieve` check the rank-four argument separately. The local height computations are in `work/heights.py` for L5 and `previous/work/heights.py` for R3. Independent checks of local integrals and finite sieves, including the R5 hyperflex characters, are in `checks/`. For the quartic of size 80, `quartic80/` contains the graph, the residual fields and cube roots, and the programs for the local values. The instructions in `anc/README.json` specify the commands and software for each family. The proof of the ternary quartic given here uses the printed graph and these finite calculations.

## References


[BB12] Jennifer S. Balakrishnan and Amnon Besser, *Computing local p-adic height pairings on hyperelliptic curves*, International Mathematics Research Notices. IMRN (2012), no. 11, 2405–2444.

[BB15] _____, *Coleman–Gross height pairings and the p-adic sigma function*, Journal für die reine und angewandte Mathematik **698** (2015), 89–104.

[BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller, *Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves*, Journal für die reine und angewandte Mathematik **720** (2016), 51–79, https://doi.org/10.1515/crelle-2014-0048.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, Journal of the American Mathematical Society **14** (2001), no. 4, 843–939, https://doi.org/10.1090/S0894-0347-01-00370-8.

[BDyDF08] Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Mathematics of Computation **77** (2008), no. 262, 1185–1197, https://doi.org/10.1090/S0025-5718-07-02003-0.

[BEN10] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng, *The Diophantine equation* $A^4 + 2^\delta B^2 = C^n$, International Journal of Number Theory **6** (2010), no. 2, 311–338, https://doi.org/10.1142/S1793042110002971.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990, https://doi.org/10.1007/978-3-642-51438-8.

[BMS25] Amnon Besser, J. Steffen Müller, and Padmavathi Srinivasan, *p-adic adelic metrics and quadratic Chabauty I*, Journal für die reine und angewandte Mathematik **828** (2025), 223–305.

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum of Mathematics, Sigma **4** (2016), e6, https://doi.org/10.1017/fms.2016.1.

[Bro12] David Brown, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, International Mathematics Research Notices **2012** (2012), no. 2, 423–436, https://doi.org/10.1093/imrn/rnr022.

[Bru03] Nils Bruin, *Chabauty methods using elliptic curves*, Journal für die reine und angewandte Mathematik **562** (2003), 27–49.

[Bru08] _____, *The arithmetic of Prym varieties in genus 3*, Compositio Mathematica **144** (2008), 317–338, https://doi.org/10.1112/S0010437X07003314.

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Mathematics of Computation **78** (2009), no. 268, 2347–2370, https://doi.org/10.1090/S0025-5718-09-02255-8.

[BS10] _____, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS Journal of Computation and Mathematics **13** (2010), 272–306, https://doi.org/10.1112/S1461157009000187.

[BVY04] Michael A. Bennett, Vinayak Vatsal, and Soroosh Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compositio Mathematica **140** (2004), no. 6, 1399–1416, https://doi.org/10.1112/S0010437X04000983.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Oxford, 1985.

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996.

[CG89] Robert F. Coleman and Benedict H. Gross, *p-adic heights on curves*, Algebraic number theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, Academic Press, Boston, MA, 1989, pp. 73–81.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Mathematical Journal **52** (1985), no. 3, 765–770, https://doi.org/10.1215/S0012-7094-85-05240-8.

[CTS21] Jean-Louis Colliot-Thélène and Alexei N. Skorobogatov, *The Brauer–Grothendieck group*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 71, Springer, Cham, 2021.

[DG95] Henri Darmon and Andrew Granville, *On the equations* $z^m = f(x, y)$ *and* $ax^p + by^q = cz^r$, Bulletin of the London Mathematical Society **27** (1995), no. 6, 513–543, https://doi.org/10.1112/blms/27.6.513.

[Dol12] Igor V. Dolgachev, *Classical algebraic geometry: A modern view*, Cambridge University Press, Cambridge, 2012.

[Dus10] Pierre Dusart, *Estimates of some functions over primes without R.H.*, 2010.

[Eis26a] Avraham Eisenberg, *Primitive integer solutions of* $x^4 + 3y^3 + 2z^3 = 0$, Hexagon preprint 2609.00132v1, September 2026, Version 1, 29 September 2026. https://hexagonmath.org/2609.00132v1.

[Eis26b] _____, *Primitive integer solutions of* $x^4 + 4y^3 + z^3 = 0$, Hexagon preprint 2609.00130v1, September 2026, Version 1, 29 September 2026. https://hexagonmath.org/2609.00130v1.

[EJ12] Andreas-Stephan Elsenhans and Jörg Jahnel, *On the order three Brauer classes for cubic surfaces*, Central European Journal of Mathematics **10** (2012), no. 3, 903–926, arXiv:1110.2086. https://doi.org/10.2478/s11533-012-0042-6.

[Fay73] John D. Fay, *Theta functions on Riemann surfaces*, Lecture Notes in Mathematics, vol. 352, Springer, 1973.

[FW99] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Mathematica **100** (1999), no. 4, 519–533.

[GA26] Bogdan Grechuk and Jamal Agbanwa, *On the polynomial values represented by binary quadratic forms*, International Journal of Number Theory (2026), Published online 30 October 2026. https://doi.org/10.1142/S1793042126501460.

[Gau06] Éric Gaudron, *Formes linéaires de logarithmes effectives sur les variétés abéliennes*, Annales scientifiques de l'École Normale Supérieure **39** (2006), 699–773.

[GG26] Bogdan Grechuk and Eugene Go, *Certifying non-existence of integer points on curves*, arXiv:2610.18916, 2026, https://arxiv.org/abs/2610.18916.

[GH81] Benedict H. Gross and Joe Harris, *Real algebraic curves*, Annales scientifiques de l'École Normale Supérieure (4) **14** (1981), no. 2, 157–182, https://doi.org/10.24033/asens.1401.

[GR25] Éric Gaudron and Gaël Rémond, *Nombre de petits points sur une variété abélienne*, Journal of the Institute of Mathematics of Jussieu **24** (2025), 705–761.

[GR26] Bogdan Grechuk and Ashleigh Ratcliffe, *On the shortest open cubic equations*, International Journal of Number Theory **22** (2026), no. 9, 2117–2127, https://doi.org/10.1142/S1793042126501058.

[Gre24] Bogdan Grechuk, *Polynomial Diophantine equations: A systematic approach*, Springer, Cham, 2024, https://doi.org/10.1007/978-3-031-62949-5.

[Gre26a] _____, *Answer to "what are the primitive solutions to $x^3 + 2y^3 = z^4$?"*, MathOverflow, question 484736, 2026, Answer dated 10 July 2026; includes the reduction for exponent 5. https://mathoverflow.net/questions/484736/.

[Gre26b] _____, *Cubic Diophantine equations: integer solutions beyond direct search*, To appear in The American Mathematical Monthly, 2026.

[Gre26c] _____, *A systematic approach to Diophantine equations: open problems*, 2026, https://arxiv.org/abs/2404.08518.

[Gro86] Benedict H. Gross, *Local heights on curves*, Arithmetic Geometry (Storrs, Conn., 1984) (Gary Cornell and Joseph H. Silverman, eds.), Springer, New York, 1986, pp. 327–339.

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, 2006.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[Haz78] Michiel Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, vol. 78, Academic Press, New York, 1978.

[Kat81] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Inventiones Mathematicae **62** (1981), no. 3, 481–502, https://doi.org/10.1007/BF01394256.

[KM04] Kamal Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Mathematics of Computation **73** (2004), 333–357.

[KRZB16] Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Uniform bounds for the number of rational points on curves of small Mordell–Weil rank*, Duke Mathematical Journal **165** (2016), no. 16, 3189–3240, https://doi.org/10.1215/00127094-3673558.

[Lem13] Franz Lemmermeyer, *The ambiguous class number formula revisited*, Journal of the Ramanujan Mathematical Society **28** (2013), no. 4, 415–421.

[Mat86] Hideyuki Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986, Translated from the Japanese by M. Reid.

[Maz77] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'IHÉS **47** (1977), 33–186, https://doi.org/10.1007/BF02684339.

[Mih04] Preda Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, Journal für die reine und angewandte Mathematik **572** (2004), 167–195, https://doi.org/10.1515/crll.2004.048.

[Mil06] James S. Milne, *Arithmetic duality theorems*, 2 ed., BookSurge, 2006, https://www.jmilne.org/math/Books/ADTnot.pdf.

[Mil14] John C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arithmetica **164** (2014), no. 4, 381–397, https://doi.org/10.4064/aa164-4-4.

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory: rational points and Diophantine equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 99–117.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999.

[Poi77] Georges Poitou, *Sur les petits discriminants*, Séminaire Delange–Pisot–Poitou, Théorie des nombres **18** (1976/77), no. 1, 1–17, Exposé no. 6.

[Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017.

[PR11] Bjorn Poonen and Eric Rains, *Self cup products and the theta characteristic torsor*, Mathematical Research Letters **18** (2011), no. 6, 1305–1318.

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, Journal für die reine und angewandte Mathematik **488** (1997), 141–188.

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Annals of Mathematics (2) **150** (1999), no. 3, 1109–1149, https://doi.org/10.2307/121064.

[Ray74] Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bulletin de la Société Mathématique de France **102** (1974), 241–280.

[RG25] Ashleigh Ratcliffe and Bogdan Grechuk, *Generalised Fermat equation: a survey of solved cases*, Expositiones Mathematicae **43** (2025), no. 4, 125688, https://doi.org/10.1016/j.exmath.2025.125688.

[RR18] Christophe Ritzenthaler and Matthieu Romagny, *On the Prym variety of genus 3 covers of genus 1 curves*, Épijournal de Géométrie Algébrique **2** (2018), Article No. 2, https://doi.org/10.46298/epiga.2018.volume2.3663.

[RV99] Dinakar Ramakrishnan and Robert J. Valenza, *Fourier analysis on number fields*, Graduate Texts in Mathematics, vol. 186, Springer, 1999.

[Sch98] Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Mathematische Annalen **310** (1998), no. 3, 447–471.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York, 1973.

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer, 1979.

[Ser87] ———, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Mathematical Journal **54** (1987), no. 1, 179–230, https://doi.org/10.1215/S0012-7094-87-05413-5.

[Ser88] ———, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988.

[Sik12] Samir Siksek, *The modular approach to Diophantine equations*, Explicit Methods in Number Theory: Rational Points and Diophantine Equations, Panoramas et Synthèses, vol. 36, Société Mathématique de France, Paris, 2012, pp. 151–179.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, New York, 1994, https://doi.org/10.1007/978-1-4612-0851-8.

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, New York, 2009, https://doi.org/10.1007/978-0-387-09494-6.

[Sim02] Denis Simon, *Computing the rank of elliptic curves over number fields*, LMS Journal of Computation and Mathematics **5** (2002), 7–17, https://doi.org/10.1112/S1461157000000668.

[Sto99] Michael Stoll, *On the height constant for curves of genus two*, Acta Arithmetica **90** (1999), no. 2, 183–201, https://doi.org/10.4064/aa-90-2-183-201.

[Sto01] ———, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arithmetica **98** (2001), no. 3, 245–277, https://doi.org/10.4064/aa98-3-4.

[Sto02] ———, *On the height constant for curves of genus two, II*, Acta Arithmetica **104** (2002), no. 2, 165–182, https://doi.org/10.4064/aa104-2-6.

[Str28] Reinhold Straßmann, *Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen*, Journal für die reine und angewandte Mathematik **159** (1928), 13–28, https://doi.org/10.1515/crll.1928.159.13.

[Stu87] Jacob Sturm, *On the congruence of modular forms*, Number Theory (New York, 1984–1985), Lecture Notes in Mathematics, vol. 1240, Springer, Berlin, 1987, pp. 275–280.

[Tat75] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV (Antwerp, 1972), Lecture Notes in Mathematics, vol. 476, Springer, Berlin, 1975, pp. 33–52.

[TO70] John Tate and Frans Oort, *Group schemes of prime order*, Annales Scientifiques de l'École Normale Supérieure (4) **3** (1970), 1–21.

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics (2) **141** (1995), no. 3, 553–572, https://doi.org/10.2307/2118560.

[vBHM20] Raymond van Bommel, David Holmes, and J. Steffen Müller, *Explicit arithmetic intersection theory and computation of Néron–Tate heights*, Mathematics of Computation **89** (2020), 395–410.

[Wei48] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann et Cie., Paris, 1948.

[Wei52] _____, *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Sém. Math. Univ. Lund (1952), 252–265, Volume dédié à Marcel Riesz; Œuvres scientifiques II, 48–61.

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics (2) **141** (1995), no. 3, 443–551, https://doi.org/10.2307/2118559.

[Wil24] Ashleigh Wilcox, *A systematic approach to Diophantine equations: two thousand solved examples*, https://arxiv.org/abs/2404.08719, 2024.

[ZB14] Zhongfeng Zhang and Meng Bai, *On Diophantine equation* $x^3 + y^3 = 2z^{2n}$, Journal of Southwest China Normal University (Natural Science Edition) **39** (2014), no. 6, 14–16, In Chinese. https://doi.org/10.13718/j.cnki.xsxb.2014.06.004.