

Long solutions to small equations

Bogdan Grechuk, Eugene Go and Avraham Eisenberg

23 October 2026

Abstract

We give complete solutions of thirty-eight Diophantine equations left open in Grechuk's 2024 monograph: fifteen affine equations, five generalized Fermat equations, eight 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.

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]. In this paper we present AI-assisted proofs for thirty-eight equations explicitly left open in the book: fifteen affine equations, five generalized Fermat equations, eight 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 publication of the book and before this paper [GG26, Wil24]; we prove fourteen more, leaving ten open. Tables 1 and 2 list the twenty completed cases and the ten remaining ones. In all tables, signs within a tuple vary independently; a sign before an entire tuple changes all its coordinates simultaneously.

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
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	$x^4 + y^3 + 2x - y = 0$	$(-8, -16), (0, 0), (0, \pm 1)$	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. 3.12.1
31	$x^4 + y^3 + x - 2y + 1 = 0$	$(-1, 1), (0, 1)$	[GG26]
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	$x^4 + y^3 + xy + y - 1 = 0$	$(\pm 1, 0), (3, -4)$	Thm. 3.13.1
31	$x^4 + y^3 + xy + x + 1 = 0$	$(0, -1)$	Thm. 3.14.1

Table 2: Remaining open two-variable equations of size $H \leq 31$.

H	Equation	H	Equation
29	$x^4 + y^3 + xy - 1 = 0$	31	$x^4 - y^3 + xy + x + 1 = 0$
30	$x^4 + y^3 + x + 2y = 0$	31	$x^4 + y^3 + xy - 3 = 0$
30	$x^4 + y^3 + x - y - 2 = 0$	31	$x^4 + y^3 + x - 2y - 1 = 0$
30	$x^4 + y^3 + x + y + 2 = 0$	31	$x^4 + y^3 + xy + x - 1 = 0$
30	$x^4 + y^3 + x + y - 2 = 0$	31	$x^4 + y^3 + x + 2y + 1 = 0$

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 Tables 1 and 2 have smooth projective models of genus 3. The smallest genus-two equation left open in the book is [Gre24, Equation (3.237)]

$$x^4 - x^2 + xy + y^3 = 0, \quad (2)$$

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 3 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 4 settle the five remaining entries. No entry of the book’s Table 4.16 remains open.

Table 3: 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. 4.1.1
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. 4.2.1
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. 4.3.1
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. 4.4.1
60	$x^5 + y^4 + 3z^2 = 0$	$(-1, \pm 1, 0)$	Thm. 4.5.1

Theorem 3. *For each equation in the second column of Table 3, 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. □

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

$$x^4 + x^3y - y^4 + y^3z + z^4 = 0 \quad (3)$$

of size $H = 80$ has an integer solution other than $(0,0,0)$. This question remains open. 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 4.

Table 4: 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. 6.1.1
96	$2x^3 + x^2y + xy^2 + y^3 + y^2z - 2xz^2 - z^3 + t^2y + tz^2 - t^3 = 0$	Thm. 6.2.1
96	$2x^3 + 2x^2y + 2y^3 + y^2z - 2xz^2 - z^3 + tz^2 - t^3 = 0$	Thm. 6.3.1

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

Proof. See Theorems 6.1.1–6.3.1. □

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 5 records our negative answer in each case, so none of these five questions remains open.

Table 5: 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. 6.5.1
832	$17x^5 + 6y^5 + 3z^5 = 0$	Thm. 6.7.1
928	$14x^5 + 13y^5 + 2z^5 = 0$	Thm. 6.9.1
960	$21x^5 + 5y^5 + 4z^5 = 0$	Thm. 6.6.1
992	$17x^5 + 9y^5 + 5z^5 = 0$	Thm. 6.8.1

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

Proof. See Theorems 6.5.1–6.9.1. □

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 6 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 7 remain open; for each, the question is whether any nonzero integer solution exists.

Table 6: 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. 6.4.1
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 7: 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 6. *The equation $8x^4 + 7y^4 + 2z^4 - t^4 = 0$ in Table 6 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 6.4.1; the three displayed witnesses are verified by substitution. $\square$

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 8 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 8: 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. 5.1.1
64	$x^4 + x^2y^2 + y^3z - yz^3 = 0$	Thm. 5.3.1
64	$x^4 - x^2y^2 + y^3z + yz^3 = 0$	Thm. 5.5.1
64	$x^4 + x^2y^2 + y^3z + z^4 = 0$	Thm. 5.6.1
64	$x^4 - y^4 + x^2yz + yz^3 = 0$	Thm. 5.2.1
64	$x^4 + y^4 + x^2yz - yz^3 = 0$	Thm. 5.4.1
64	$x^3z + y^3x + y^2z^2 - z^3y = 0$	Thm. 5.7.1
64	$x^4 - y^3z + xyz^2 + xz^3 = 0$	Thm. 5.8.1

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

Proof. See Theorems 5.1.1–5.8.1. $\square$

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

$$x^4 + xy^3 + z^4 + t^4 = 0 \quad (4)$$

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

$$x^4 + y^4 + z^3t - zt^3 = 0. \quad (5)$$

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

Proof. See Theorem 6.10.1. □

The preceding discussion covers seventy-three entries explicitly left open in the book. Thirty-eight are proved here, seventeen are classified as completed after publication of the book and before this paper, three follow from pre-book literature, and fifteen remain open. The seventeen earlier entries include the two equivalent presentations settled by [Eis26b] in Table 3. 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.

The rest of the paper provides proofs for each of the thirty-eight equations. Shared results are collected in Section 2; the proofs for affine curves, generalized Fermat equations, plane quartics, and the remaining homogeneous equations appear in Sections 3–6, respectively. Established methods are cited where used, and the equation-specific computations have certificate identifiers linked to the accompanying reproducibility material. 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 3×3 matrices); the tangent calculation on a genus-five cover uses the 5×5 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 $\text{div } h = 2(P_m + Q_m - 2O)$ (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

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

(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 δ 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 $p \leq \infty$, the local map $\delta_p : J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \rightarrow (K \otimes \mathbb{Q}_p)^\times / (K \otimes \mathbb{Q}_p)^{\times 2}$ defined by the same formula satisfies $\text{res}_p \circ \delta = \delta_p \circ \text{res}_p$.

(4) Hence, if we set

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

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

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

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

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

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 $E^G \rightarrow (E/V)^G$ is surjective. By the long exact sequence, $H^1(\mathbb{Q}, V) \rightarrow H^1(\mathbb{Q}, E) = K^\times / K^{\times 2}$ 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 . $\square$

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 $D = |\text{disc } R|$ for an order $R \subseteq \mathcal{O}_K$ of rank n , since $\text{disc } R = [\mathcal{O}_K : R]^2 d_K$), 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 $2\text{Cl}(K)$ (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

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

(γ 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 $\text{Cl}(K)[2] = 0$. 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 $\text{Cl}(K)[2] \neq 0$. 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 ζ_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

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

At a zero $\rho = \frac{1}{2} + b + it$ ($|b| \leq \frac{1}{2}$), the real part $\text{Re } \Phi(\rho)$ 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 $2\text{Cl}(K)$) and $\chi(\mathfrak{p}) \geq -1$ at the others. Hence the right-hand side is at least $B^-(f)$, which contradicts the assumption $B^-(f) > 0$. $\square$

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. $\square$

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 $x : E \rightarrow \mathbb{P}^1$ 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 $G_1, \dots, G_r \in E(K)$ 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 $\lambda : K_p \rightarrow \mathbb{Q}_p$ 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 $\lambda_1, \dots, \lambda_r$ write $\Theta = (\theta_{\lambda_1}, \dots, \theta_{\lambda_r})$ as $\Theta(n) = Bn + H(n)$ (H of degree ≥ 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 Θ 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 $z = (z_1, \dots, z_g)$ 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 ≥ 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 $z([m]Q) = E(mL(z(Q)))$ and*

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

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 , $J = \text{Jac}(C)$, 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 $\chi : J(\mathbb{F}_p) \rightarrow \mathbb{Z}/2$ that vanishes on all $[\tilde{P} - \tilde{O}]$. By class field theory, χ gives an unramified double cover $D \rightarrow C$, 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. $\square$

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 $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow L^\times / L^{\times 2}$ obtained by evaluating the normalized bitangent function h componentwise is the composition of the Kummer map and $H^1(\mathbb{Q}, V) \rightarrow H^1(\mathbb{Q}, E)$. The kernel of the latter map is the quotient of $(E/V)^G$ by the image of E^G . In particular, if $E^G \rightarrow (E/V)^G$ is surjective, then δ is injective.
- (2) The image of δ 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 δ is injective, then for $\text{Sel} \subset L(S, 2)$ defined as in Proposition A(4) we have $\text{rank } J(\mathbb{Q}) + \dim_{\mathbb{F}_2} V^G \leq \dim_{\mathbb{F}_2} \text{Sel}$.
- (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 $0 \rightarrow V \rightarrow E \rightarrow E/V \rightarrow 0$.

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 $\chi : \text{Cl}(K) \rightarrow \{\pm 1\}$ 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 Θ be the set of the 28 bitangents of C with its Galois action, and let K be the étale algebra of Θ (if the action is transitive, $K = \mathbb{Q}(\theta)$ for one bitangent θ , a field of degree 28). Let ℓ be a linear form with coefficients in K whose images under the 28 homomorphisms $K \rightarrow \overline{\mathbb{Q}}$ are linear forms ℓ_θ defining the bitangents θ ; so $\text{div}(\ell_\theta|_C) = 2D_\theta$ for an effective divisor D_θ of degree 2.*

- (1) The D_θ 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 Θ 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\text{Sp}(V) \cong \text{Sp}_6(\mathbb{F}_2)$ acts faithfully on Θ ; 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, $\text{Res}_{K/\mathbb{Q}} \mu_2 / \mu_2$) and $\iota : V \rightarrow M, T \mapsto (e_2(T, D_\theta - D_{\theta_0}))_\theta$. 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 $\prod_P ((\ell/h)(P))^{n_P}$ in $(K \otimes k)^\times / k^\times$ does not depend on h , and $[D] \mapsto \ell(D)$ induces a homomorphism

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

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

- (3) (Odd primes) Let p be an odd prime such that the Tamagawa number $c_p(J)$ is odd, and let $\xi \in J(\mathbf{Q}_p)$. Then $\delta_{\mathbf{Q}_p}(\xi)$ becomes trivial over $\mathbf{Q}_p^{\text{nr}}$. Hence, if $\xi \in J(\mathbf{Q})$ and $\kappa \in K^\times$ represents $\delta_{\mathbf{Q}}(\xi)$, the vector $(v_p(\kappa) \bmod 2)_{p|p}$ is either 0 or $(e_p \bmod 2)_{p|p}$, where e_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, $X \subset \mathbb{P}_K^3$ a smooth cubic surface, L/K a cyclic extension of prime degree n , and τ a generator of $\text{Gal}(L/K)$; τ acts on $X_L = X \times_K L$ and on its divisors. For a divisor D on X_L put $N_{L/K}(D) = D + \tau D + \dots + \tau^{n-1} D$, and for $\psi \in K(X)^\times$ let $\mathcal{B}_\psi = (L/K, \tau, \psi) \in \text{Br}(K(X))$ 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 $0 \in \text{Br}(K')$ if $L \otimes_K K' \cong K'^n$ (since n is prime, there are no other cases).*

- (1) (Azumaya extension) *If $\text{div}(\psi) = N_{L/K}(D)$ for a divisor D on X_L , then $\mathcal{B}_\psi$ lies in $\text{Br}(X) \subseteq \text{Br}(K(X))$. 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 ψ' is regular and nonzero, then $\mathcal{B}_\psi(P) = (L \otimes_K K'/K', \tau, \psi'(P))$ in $\text{Br}(K')$.*
- (2) (Local constancy) *For every place w of K and every $\alpha \in \text{Br}(X)$, the map $X(K_w) \rightarrow \mathbf{Q}/\mathbf{Z}$, $P \mapsto \text{inv}_w \alpha(P)$, is locally constant.*
- (3) (Points of smooth reduction) *Let w be a finite place of K , with ring of integers $\mathcal{O}_w$, uniformizer π and residue field k , at which L/K is unramified. Let $\mathcal{X} \subset \mathbb{P}_{\mathcal{O}_w}^3$ 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 $\text{div}(\psi) = N_{L/K}(D)$ as in (1), where G is a form of degree d and ℓ 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 $\text{inv}_w \mathcal{B}_\psi(P) = 0$. In particular, if $\mathcal{X}_k$ is smooth and $n \mid d$, then $\text{inv}_w \mathcal{B}_\psi(P) = 0$ for all $P \in X(K_w)$ (replace ℓ by a coordinate ℓ' with $\ell'(\bar{P}) \neq 0$; by (1), $G/(c \ell'^d) = \psi \cdot (\ell/\ell')^d$ defines the same class).*
- (4) (Reciprocity) *If $\alpha \in \text{Br}(X)$ and $P \in X(K)$, then $\sum_w \text{inv}_w \alpha(P) = 0$, the sum over all places of K . Hence, if $\sum_w \text{inv}_w \alpha(P_w) \neq 0$ for every family $(P_w)_w \in \prod_w X(K_w)$, then $X(K) = \emptyset$.*

Outline of the proof of (1) and (3). (1) Let χ be the character of $\text{Gal}(L/K)$ with $\chi(\tau) = 1/n$. Since χ comes from the constant field, the residue of $\mathcal{B}_\psi$ at a prime divisor E of X is $v_E(\psi) \cdot \chi|_{K(E)} \in H^1(K(E), \mathbf{Q}/\mathbf{Z})$ (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, $\mathcal{B}_\psi \in \text{Br}(X)$ 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 $R = \mathcal{O}_{\mathcal{X}, P} \otimes_{\mathcal{O}_w} \mathcal{O}_{L_w}$. 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 π 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 $\text{Spec } R$, and each of them is principal. Writing the restriction of D to $\text{Spec } R$ as $\text{div}(f)$ ($f \in \text{Frac}(R)^\times$; ℓ 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 $\mathcal{O}_{\mathcal{X}, \bar{P}}^\times$. 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. $\square$

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

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

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 $\text{div}(v - u) = A + 3E - 4O$, $\text{div}(u + 1) = A + B + C_1 - 3O$, $\text{div}(u) = D + E + F_1 - 3O$, 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 $\eta = \frac{m(11m^{12} - 112m^4 + 112m^3)}{8(13m^9 + 16m + 8)}$, $a = m^3/2$, $b = (12m^2\eta - m^6)/8$. 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 η 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 $H^1(\mathbb{Q}, J[2]) \rightarrow K^\times / K^{\times 2}$ is injective, and the image of $\text{Sel}^{(2)}(J/\mathbb{Q})$ 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 $\text{rank } J(\mathbb{Q}) \geq 3$.

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, $\text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2)$ 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). $\square$

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 λ , 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). $\square$

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 $m_0 \leq g(-\frac{1}{2}) = -\frac{7}{16}$, 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 $\{v : h(v) \geq m_0\}$ 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 $v \rightarrow -\infty$. Hence $C(\mathbb{R})$ is a single loop. The rest is [GH81]. $\square$

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

Proof. Let γ 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 γ' 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 γ' 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 χ . (ii) At p , γ' is determined by the Frobenius $g \in \text{GL}(V)$ 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 $U = \ker(g - 1)$, $\lambda = \langle c, \cdot \rangle$. $\square$

Step 3: rank.

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

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

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

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 $N\mathfrak{p} \leq M$ 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 $q \leq 10^5$ 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 $\chi \geq -1$ (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, $\sum_{R < p < X} \frac{\log p}{p+1} f(\log p) \leq \mathcal{T}_R := c \int_{\log R}^T f + (c-1 + \frac{1}{5 \log^2 R}) f(\log R)$, so the contribution is at least $-\frac{20}{27} \mathcal{T}_R$. Since $M^2 > X$, the terms with $m \geq 2$ occur only in (a). All prime factors of $\text{disc}(p_K) = 2^{312} 3^{54} 157^6 64679^6 333337^2 172659335137^2$ 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...	1.1435757488...	-0.0000100075...	-0.0340749409...	-0.0598580721...

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

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 ω is primitive and $(P \cdot P)_\omega = 0$. Near O we have $\text{div } \omega = 4O$, 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 ± 1 in one coordinate, so their sections do not meet. $\square$

Lemma 3.1.8. *Let $\omega_i = (1, u, v) \omega$ and $\eta_i = (5u^2v, 2uv, u^2) \omega$. The η_i are differentials of the second kind with poles only at O , and the cup product matrix with respect to $\text{Res}_O((\int \alpha) \beta)$ is $\begin{pmatrix} 0 & -I_3 \\ I_3 & 0 \end{pmatrix}$. For $P = (a, b)$, $v_P(Q) = \frac{v^2 + bv + b^2 - 1}{u - a} \omega(Q)$ is a differential of the third kind with residue divisor $P - O$. Let $I_i(P) = \int_O^P \omega_i$, $J_i(P) = \int_O^P \eta_i$, $K(P, Q) = \int_O^Q v_P$ (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 $-t^4 dt$, $-t dt$, 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, $(b - v)(v^2 + bv + b^2 - 1) = (u - a)(u^3 + u^2 a + u a^2 + a^3 + 1)$, so the only poles of v_P are P and O . The bidifferential identity $d_P v_P(Q) - d_Q v_Q(P) = \sum_i (\eta_i(P) \omega_i(Q) - \omega_i(P) \eta_i(Q))$ holds, since after dividing both sides by $\omega(P) \omega(Q)$ each side becomes $5a^2 b - 5u^2 v + 2abu - 2auv + a^2 v - bu^2$ (certificate 1.1.1g). At O , the coefficients of t^0, t^1, t^4 in $v_P = (-t^{-1} - at^2 + bt^3 - a^2 t^5 + \dots) dt$ are 0, so the de Rham class of $v_P - \sum_i J_i(P) \omega_i$ lies in W , and by the definition in [CG89, BBM16], $h_p = H$. Integrating the identity gives $d_P H(P, Q) = v_Q(P) - \sum_i \omega_i(P) J_i(Q)$. On the diagonal, the regular part $2 \cdot (-3bb'/\beta) da$ ($\beta = 3b^2 - 1$, $b' = db/da$) of $v_P(Q), v_Q(P)$ cancels against the $d \log \beta$ added by the tangent vector normalization, and we obtain $d\tau = -2 \sum_i \omega_i J_i$. $\square$

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 $M = I_B^{-1} H_B (I_B^T)^{-1}$ and $q(P) = \tau(P) - I(P) M I(P)^T$, then $q(P) = 0$ at every integral point P .

Proof. h is a symmetric bilinear form on $J(Q)$ ([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 $h(P - O, P - O) = \tau(P)$. $\square$

Step 5: $p = 3$. C has good reduction at 3, and the only affine points modulo 3 are the six reductions of $A, \dots, F_1$. 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) $I_B/3 \equiv \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 2 \\ 1 & 1 & 2 \end{pmatrix} \pmod{3}$ (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
$3^{-e_j} q_j \pmod{3}$	$2s^2 + 2s^3$	$2s + 2s^2$	$2s + s^2$	$2s + 2s^2$	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 $\text{div } f_j = 4P_j + R_{j,1} + R_{j,2} + R_{j,3} - 7O$. 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 ρ of the second kind it is $\text{Res}_O(\log f_j \cdot \rho)$, and for v_{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. $\square$

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) $5^{-1}I_B \equiv \begin{pmatrix} 3 & 3 & 2 \\ 2 & 0 & 0 \\ 1 & 3 & 0 \end{pmatrix} \pmod{5}$ (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 $\mathbb{Q}(\beta)$, $N = 6, 7, 7, 7, 7, 9$, 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). $\square$

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 ℓ 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 ℓ . 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. $\square$

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 $u^i v^j$ ($j \leq 2, 3i + 4j \leq m$) 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
$q = 109$	$\{2, 6\}$	$\{0, 4, 5\}$	$\{0, 2\}$	$\{0, 4, 5\}$	$\{0, 2\}$	$\{0, 2\}$
$q = 277$	$\{4\}$	$\emptyset$	$\{2, 6\}$	$\emptyset$	$\{4\}$	$\{4\}$

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. $\square$

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. $\square$

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

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

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 ∞ 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 $\text{Cl}(K)[2] = 0$ 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 ∞ 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. $\text{Cl}(K)[2] = 0$.

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 $q \leq 5 \cdot 10^6$, and $k(q) = 0$ for larger q .

With these data, $B^-(f) > 0.000875203229 \dots > 0$ (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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: an upper bound for the rank.

Lemma 3.2.4. $\text{rank } J(\mathbb{Q}) \leq 2$.

Proof. The hypotheses of Proposition A were checked above. So $J(\mathbb{Q})[2] = 0$ and δ is injective. Since $\text{Cl}(K)[2] = 0$ 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 $J(\mathbb{Q})[2] = 0$, $\text{rank } J(\mathbb{Q}) \leq 2$. $\square$

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. $\text{rank } J(\mathbb{Q}) = 2$. 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

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

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 $\text{Res}_u(F, h_i) = c_i(z - z(P_i))^{28} d_i(z)$ (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∞ . 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} ,

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

(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 $\text{rank } J(\mathbb{Q}) \geq 2$, and together with Lemma 3.2.4 we get $\text{rank } J(\mathbb{Q}) = 2$. 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 ω 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. $\square$

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. $\square$

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.

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

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 $\text{Cl}(K)[2] = 0$ (Step 2), obtain $\text{rank } J(\mathbb{Q}) \leq 2$ 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. $\text{Cl}(K)[2] = 0$.

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 $q \leq 10^4$, 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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: an upper bound for the rank.

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

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

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. $\text{rank } J(\mathbb{Q}) = 2$. 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 $\text{div} = 2P_1 + A + B - 4O$ 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 $\text{rank } J(\mathbb{Q}) \geq 2$, 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 $\lambda \equiv (1, 0, 0) \pmod{3}$. λ annihilates L_0 and T , and hence L_1 . Since the rank is 2, λ 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, $\lambda \cdot \omega = (c_0 + c_1s + \dots) ds$ 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

$$\int \lambda \cdot \omega = 3c_0z + \sum_{n \geq 2} \frac{3^n c_{n-1}}{n} z^n$$

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

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

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 $t^4 - w + (1 + 2t)w^3 = 0, w = t^4 + \dots$, so O is a smooth rational hyperflex. Let $G_i = [P_i - O]$. Since $\text{div}(u + 2v) = 3P_0 + P_* - 4O$ and $\text{div}(v) = P_{-1} + P_0 + P_1 - 3O$, 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 $\text{Res}(243v^2 - 16, 2v^3 + 1) = 14332523 = 83 \cdot 172681$. 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 $\text{Cl}(K)[2] = 0$ (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 $\text{Sel}^{(2)}(J/\mathbb{Q})$ 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 $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = g + \dim J(\mathbb{Q}_2)[2] \leq 4$. $\square$

Step 2: the class group.

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

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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: an upper bound for the rank.

Lemma 3.4.4. $\text{rank } J(\mathbb{Q}) \leq 2$.

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 $J(\mathbb{Q})[2] = 0$, $\text{rank } J(\mathbb{Q}) \leq 2$. $\square$

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 . $\square$

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 $\text{rank } J(\mathbb{Q}) = 2$. (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 $\text{div}(u + 2v)$ 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 $\text{div } g_{10} = 7P_1 + Q_1 + Q_2 + Q_3 - 10O$. 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 $8L_1 = -(\int_{P_1}^{Q_1} \omega + \text{Tr} \int_O^{Q_2} \omega)$. Computing with the valuations of all discarded tails bounded, we obtain the valuations in (1) (certificate 1.1.4f). The two products in Δ 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. $\square$

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_*). $\square$

Lemma 3.4.8. *The only integral point in the odd disk ε is P_ε .*

Proof. Since $1 - 3u^2 = -2D_\varepsilon$ with $D_\varepsilon = 1 + 12\varepsilon r + 24r^2$, the pullback of ω 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_ε ($H_\varepsilon(0) = 0$) be the antiderivative of $a \cdot \omega$ divided by -4 . Then $H'_\varepsilon = (C_\varepsilon/2 + 2a_1t + 2a_2r)/D_\varepsilon$ 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_ε 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. $\square$

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). $\square$

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

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

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 $\text{ord}_O z = -3$, $\text{ord}_O u = -4$. 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 $\text{Cl}(K)[2] = 0$ (Lemma 3.5.3), and obtain $\text{rank } J(\mathbb{Q}) \leq 2$ 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 $(F, F_u, F_z, \det \text{Hess } F)$ 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. $\text{Cl}(K)[2] = 0$.

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 $q \leq 6 \cdot 10^6$, 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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: an upper bound for the rank.

Lemma 3.5.4. $\text{rank } J(\mathbb{Q}) \leq 2$.

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 $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow K^\times/K^{\times 2}$. 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 $\dim J(\mathbb{Q}_2)[2] \leq 1$ and $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3 + \dim J(\mathbb{Q}_2)[2] \leq 4$. 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 δ is injective and $J(\mathbb{Q})[2] = 0$, we get $\text{rank } J(\mathbb{Q}) \leq 2$. $\square$

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

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

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 ω lie in $\mathbb{Z}_2$. On the O -disk we have $|t|_2 < 1$, $w = w(t) \in \mathbb{Z}_2[[t]]$, and $\omega = -(w, t, 1) dt / (1 + 3(1 + 2t)w^2)$, 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) $\text{div}(u + 2z) = 3P + R - 4O$. Moreover, there is a rational function h_D with $\text{div}(h_D) = 14D + E_D - 31O$, 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

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

(3) $\text{rank } J(\mathbb{Q}) = 2$. 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 $\lambda \cdot \omega$ 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 $z^a u^b$ ($b \leq 2, 3a + 4b \leq 31$; 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, $\text{Res}_u(F, h_D) = c(z^2 - z + 1)^{14} q_D(z)$, 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

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

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 $\text{rank } J(\mathbb{Q}) = 2$. The cross product of $L_P/2$ and L_D is an integral vector whose third component is a unit. Let λ 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 λ 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 $\lambda \cdot \omega$ annihilates all logarithms of $J(\mathbb{Q})$. $\square$

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 $u(z)$. $\square$

Proof of Proposition 3.5.2. On the P -disk let

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

The constant term is 0. The exact Taylor expansion gives

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

(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 ω 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 Φ 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. $\square$

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

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

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 ∞ 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

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

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 $\text{rank } J(\mathbb{Q}) \leq 2$ from $\text{Cl}(K)[2] = 0$ (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 ∞ have the form $u = mz + \eta(m)$, where m is a root of

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

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 $\text{Res}_Z(81Z + 16, 4Z^3 + 1) = 515057 = 601 \cdot 857$. 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. $\text{Cl}(K)[2] = 0$.

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 $T = 13$ ($e^{13} = 442413.4\dots$). 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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: an upper bound for the rank.

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

Proof. By Proposition A, $J(\mathbb{Q})[2] = 0$, and $h_m = -(u - mz - \eta(m))$, normalized to have leading coefficient 1 at ∞ , gives an injective homomorphism $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow K^\times/K^{\times 2}$. 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 δ is injective, $\text{rank } J(\mathbb{Q}) \leq 2$. $\square$

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

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

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

(2) Modulo 2^{24} ,

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

Proof. (1) Among the combinations of the 36 basis elements $z^a u^b$ ($b \leq 2, 3a + 4b \leq 38$) 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 $\text{Res}_u(F, h_i) = c_i(z - z(P_i))^{35} d_i(z)$. 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 $2P_0 + A = \text{div}(z) + 3\infty$ 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). $\square$

Lemma 3.6.6. *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 $\omega = \mathbf{a} \cdot \omega$ 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 $\mathbf{a}$ (certificate 1.1.6d). $\square$

Step 5: 2-adic zeros. $C(\mathbb{F}_2)$ consists of the five reductions of P_0, P_1, A, B, ∞ , 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 ∞ 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
∞	$1 + 2\mathbb{Z}_2$	2	529	(5, 65)	31	—
∞	$2\mathbb{Z}_2$	2	0	(0, 0)	0	∞

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 $s = -1$. $\square$

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). $\square$

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 $89N[X - \infty] = aH_0 + bH_1 = (70a + b)H_1$, and N is invertible modulo 128, so $89[X - \infty] = (70c_0 + c_1)H_1$. 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. $\square$

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

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

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

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

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 $\text{rank } J(\mathbb{Q}) \leq 2$; 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 $t^{-4}(1 + \dots)$ 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 $|\text{Res}(81z + 16, 4z^3 - 1)| = 547825 = 5^2 \cdot 17 \cdot 1289$. 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. $\text{Cl}(K)[2] = 0$.

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 $e^8 = 2980.96 \dots < 3000$. 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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: an upper bound for the rank.

Lemma 3.7.4. *The local image $\delta_5(J(\mathbb{Q}_5)/2J(\mathbb{Q}_5))$ 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 Φ 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 $J[2]/(\Phi - 1)J[2] \rightarrow E/(\Phi - 1)E$ 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. $\square$

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

Proof. By Proposition A, $J(\mathbb{Q})[2] = 0$ and δ 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 $\text{rank } J(\mathbb{Q}) \leq 2$. $\square$

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 $\text{div}(z) = 2(0, 0) + (-1, 0) - 3O$, $\text{div}(z - 1) = 2(0, 1) + (-1, 1) - 3O$, $\text{div}(u + z) = (0, 0) + (-1, 1) + 2(1, -1) - 4O$, and

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

Lemma 3.7.6. (1) *For each of $X = (0, 0), (0, 1), (1, -1)$ there is a polynomial h_X with $\text{div}(h_X) = 35X + E_X - 38O$ (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) $\text{rank } J(\mathbb{Q}) = 2$, $\#J(\mathbb{Q})_{\text{tors}}$ divides 35, and $\langle G_1, G_2 \rangle$ has odd index in $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$. 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 $z^i u^j$ ($j < 3, 3i + 4j \leq 38$) whose first 35 Taylor coefficients at X vanish (the solution space is 1-dimensional). $\text{Res}_u(F, h_X)$ 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 $\geq 1/2$). 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 $\#J(\mathbb{Q})_{\text{tors}} \mid 35$. 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 $\mathbb{Z}_2$. $\square$

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 ω 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). $\square$

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

Lemma 3.7.8. (1) For $X = (0, 0), (1, -1)$ we have $\text{div}(h_X) = 63X + E_X - 66O$, 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 $z^i u^j$ ($j < 3, 3i + 4j \leq 66$) 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 $|a| \leq 3^r$, the map $b \mapsto a^2 + 3a^3 - 6b^2 - 12b^3 - 9b^4$ is a contraction on $|b| \leq 3^{2r}$, 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 $\lceil (n-1)/4 \rceil - v_3(n) \geq 0$, and at least 28 if $n \geq 121$. 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 $U(v_1, v_2)^\top = 9(c_1, c_2)^\top$. 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). $\square$

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 ℓ , for the projection π_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 $T = dD_Y - dc_1 G_1 - dc_2 G_2$ 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 . $\square$

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). $\square$

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 $(304, 0) \bmod 512$, 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 $(10, 6) \bmod 32$, 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. $\square$

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

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

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 $\text{Cl}(K)[2] = 0$ 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

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

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

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

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 $J(\mathbb{Q}_p^{\text{nr}})$ is divisible by 2, so the descent image is unramified at p . Therefore $S = \{p \mid 2\}$ suffices (certificate 1.1.8a).

Step 2: the class group.

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

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 $q \leq 10^5$, and $k(q) = 0$ otherwise. Since $(10^5)^2 > 10^7$, all terms with $m \geq 2$ receive a positive sign.

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

Step 3: an upper bound for the rank.

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

Proof. The hypotheses of Proposition A (a rational hyperflex, irreducibility of f) were checked above. Hence $J(\mathbb{Q})[2] = 0$ and δ 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)

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

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

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. $\text{rank } J(\mathbb{Q}) = 2$. 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

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

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 $\text{Res}_u(F, h_i)$ 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, $w = t^4 + \dots \in \mathbb{Z}_2[[t]]$. 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

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

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} ,

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

The two logarithms are linearly independent, so $\text{rank } J(\mathbb{Q}) \geq 2$, and together with Lemma 3.8.4 this gives $\text{rank } J(\mathbb{Q}) = 2$. 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 ω kills all logarithms of $J(\mathbb{Q})$. $\square$

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 ω 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

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

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 ω 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

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

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 ω 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. $\square$

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. $\square$

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

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

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 $w = -t^4 + \dots$. 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_{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_{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 $\text{Cl}(K)[2] = 0$ 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 $S = \{p \mid 2\}$ suffices (certificate 1.1.9a).

Step 2: the class group.

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

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 $p \leq 31622$ 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 α_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 $q \leq 1.35 \cdot 10^7$, and $k(q) = 0$ otherwise. Since $(1.35 \cdot 10^7)^2 > 10^9$, all terms with $m \geq 2$ receive a positive sign.

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

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

(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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: the rank and the index.

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

Proof. The hypotheses of Proposition A were checked above. Hence $J(\mathbb{Q})[2] = 0$, δ 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 $V/(\text{Frob} - 1)V \rightarrow E/(\text{Frob} - 1)E$. 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 $V/(T - 1)V \rightarrow E/(T - 1)E$, 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 $f \bmod p$	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)	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)

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

Therefore $\text{rank } J(\mathbb{Q}) \leq 2$.

The lower bound and the index are as follows. We have $\delta(G_0) = \eta - m$, and at a point Q of D_{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 $\dim J(\mathbb{Q})/2J(\mathbb{Q}) = \text{rank } J(\mathbb{Q}) \leq 2$; 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. $\square$

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

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

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

$$\log G_0 = -\frac{1}{16} \text{Tr}_{E_0} \int_0^t \omega_\bullet, \quad \log D = -\frac{1}{8} \text{Tr}_{E_D} \int_0^t \omega_\bullet.$$

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

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

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 ω kills all logarithms of $J(\mathbb{Q})$. $\square$

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

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

Lemma 3.9.6. *Let $H(t)$ be the antiderivative of ω 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 ω gives

$$H'(t) = \frac{(a_0 - a_1)/4 + (a_1/2)t + a_2b(t)}{1 + 48b(t)^2}, \quad H(0) = 0$$

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

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

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 ω , 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). $\square$

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 $k[P - O] = n_0G_0 + n_D D + \tau$, where τ 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],

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

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. $\square$

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 $P = P_0$. $\square$

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

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

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 $\text{Cl}(K)[2] = 0$. 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 $\text{Res}(2x^3 + 1, G) = 31 \cdot 433 \cdot 2341$. 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

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

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 $\iota : V \rightarrow \mathbb{F}_2^\Omega$, $c \mapsto (\langle c, w \rangle)_{w \in \Omega}$. 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 $H^1(\mathbb{Q}, J[2]) \rightarrow K^\times / K^{\times 2}$ is injective. Composing with the Kummer map $\kappa : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow H^1(\mathbb{Q}, J[2])$, 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 Ω . 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 Ω) 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. $\square$

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 $u_1, \dots, u_{17}$ 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). $\square$

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 $u_1, \dots, u_{17}$ in $\mathcal{T}$. Then the image of $K(\{2\}, 2)$ in $\mathcal{T}$ is exactly $\mathcal{L}$. Moreover, the projection $\mathcal{L} \rightarrow \mathcal{T}_2$ 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, $\mathcal{L} \rightarrow \mathcal{T}_2$ 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 $\mathcal{L}$. $\square$

Lemma 3.10.5. *Suppose $\text{Sel} \neq \langle \kappa(A), \kappa(B) \rangle$. Then there is a nontrivial character $\chi : \text{Cl}(K) \rightarrow \{\pm 1\}$ 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 $\gamma \in \text{Sel} \setminus \langle \kappa(A), \kappa(B) \rangle$. By Lemma 3.10.2, the image of γ 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 γ' 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 γ' . 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 χ 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 . γ' 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 $\iota(c)$. $\square$

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 $c \in V$,*

$$\sum_{w \in U, q(w)=0, w \neq 0} (-1)^{\langle c, w \rangle} \geq \ell(r(U)), \quad \begin{array}{c|cccccccccccc} r & 0 & 1 & 2 & 3 & 5 & 7 & 9 & 11 & 15 & 27 \\ \hline \ell(r) & 0 & -1 & -2 & -3 & -3 & -5 & -3 & -5 & -5 & -5 \end{array}$$

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). $\square$

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). $\square$

Step 6: excluding the character, and the rank.

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

Proof. Suppose Sel is larger, and take χ 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,

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

We bound the left-hand side from below.

- (i) If $N\mathfrak{p} \leq M$, 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 Σ_{pr} .
- (ii) To the 26,759 prime ideals of degree at least 2 with norm in (M, X) we assign $\chi = -1$ (sum Σ_{hi}). Since $M^2 > X$, there are no terms with $m \geq 2$ 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 Σ_{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

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

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

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

$$\Sigma_{\text{cen}} = -0.0590216892\dots, \quad -\frac{20}{27}\mathcal{T}_R = -0.0489055193\dots,$$

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 $\text{Sel} = \langle \kappa(A), \kappa(B) \rangle$. The 2-adic images of $\kappa(A), \kappa(B)$ are independent, so $\dim \text{Sel} = 2$. Since $J(\mathbb{Q})[2] = 0$, $\text{rank } J(\mathbb{Q}) \leq 2$, and since A, B are independent, the rank is 2. $\square$

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 $\text{ord}_A \geq n + 2$, $\text{ord}_B \geq m$. The basis is $x^i y^j$ ($j \leq 2, 3i + 4j \leq N$), and then $\text{div}(h_{n,m}) = (n + 2)A + mB + E_{n,m} - NO$ 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 $a_0u + a_1u^2/2 + a_2u^3/3$ 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 $C(\mathbb{F}_3) = \{O, (2, 1), (1, 2), (0, 2)\}$, $\alpha_3 \pmod{3} = (2 + 2x + y)\omega_0$ 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 $\alpha_3 = (f_0 + f_1u + f_2u^2 + \dots)du$; 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. $\square$

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 $a_0u + a_1u^2/2$; 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 $C(\mathbb{F}_5) = \{O, (4, 1), (1, 4)\}$. α_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, $(6, 3) \pmod{9}$ becomes $(33, 3) \pmod{45}$, and $(3, 4) \pmod{9}$ becomes $(3, 13) \pmod{45}$. $\square$

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 $x^i y^j$ ($j \leq 2, 3i + 4j \leq m \leq 9$) 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 $J(\mathbb{F}_5)$, $\text{ord } B = 64$ 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 $(3, 13) \pmod{45}$ 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 $(3, 13) \pmod{45}$ 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. $\square$

Proof of Theorem 3.10.1. By Proposition 3.10.8, $\text{rank } J(\mathbb{Q}) = 2$, 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 $B = (1, -1)$. $\square$

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

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

The projective completion $u^4 + v^3w - (u + w)vw^2 - w^4 = 0$ 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 $w = -t^4 + t^9 - t^{12} + \dots \in \mathbb{Z}[[t]]$. 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 $\text{div}(u + 1) = 3P_- - 3O$, and $[P_- - O]$ is a torsion element.

The proof has five steps. We fix the bitangent field K (Step 1), show $\text{Cl}(K)[2] = 0$ 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 $u^4 + (mu + b)^3 - (u + 1)(mu + b) - 1 = (u^2 + c_1u + c_0)^2$ 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 $v = -t^{-4} + \dots$ 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. $\text{Cl}(K)[2] = 0$.

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 $B^- > 0.00490937703090692 \dots > 0$ (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, $\text{Cl}(K)[2] = 0$. $\square$

Step 3: upper bound for the rank.

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

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 $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow K^\times/K^{\times 2}$ 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 $\dim J(\mathbb{Q}_2)[2] \leq 1$, and by Proposition F(1), $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \leq 1 + 3 = 4$. 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 $2e_p$ 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 δ is injective and $J(\mathbb{Q})[2] = 0$, $\text{rank } J(\mathbb{Q}) \leq 1$. $\square$

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

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

In the chart at O ,

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

and the three components are series with integer coefficients:

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

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 $3i + 4j \leq 24$, $j \leq 2$, 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

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

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. $\square$

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

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

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

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

The integrals up to degree 9 are

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

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

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

Therefore

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

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 $\operatorname{rank} J(\mathbb{Q}) = 1$. $\square$

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

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

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

$$\eta_0 \equiv \omega_0, \quad \eta_2 \equiv \omega_1 + \omega_2 \pmod{3}.$$

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 η_0 and η_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 $\omega/ds = (1, 1, 0)/2$. The constant coefficient $1/2$ of η_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 η_0 is a unit.
- O : $s = t$. At the center $\omega/ds = (0, 0, 1)$, and the constant coefficient 1 of η_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

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

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 $C(\mathbb{Q}) = \{O, P_+, P_-\}$. $\square$

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 $v = t^{-4} + \dots$. 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

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

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

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

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

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

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

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 $|H| \leq 16 \cdot 120$. The orbit of size 10 splits into five pairs $\{w, w + v_0\}$. The action $H \rightarrow S_5$ 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 $G \rightarrow S_5$ 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 $16 \nmid |G|$, a contradiction. Therefore $N \subset G$ and $G = H$. $\square$

Lemma 3.12.4. $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = 1$, and $H^1(\mathbb{Q}, J[2]) \rightarrow H^1(\mathbb{Q}, E)$ is injective. Hence $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow \mathcal{L}^\times / \mathcal{L}^{\times 2}$ 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 $E^H \rightarrow (E/V)^H$ is surjective. In the cohomology exact sequence of $0 \rightarrow V \rightarrow E \rightarrow E/V \rightarrow 0$, the kernel of $H^1(\mathbb{Q}, V) \rightarrow H^1(\mathbb{Q}, E)$ 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. δ is the composition of the Kummer map with this map. $\square$

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. $\text{Cl}(F_{10})[2] = \text{Cl}(F_{16})[2] = 0$.

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 $q \leq 2 \cdot 10^5$ 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. $\square$

Step 3: rank 0.

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

Proof. By Lemma 3.12.4, δ 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,

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

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 $2e_p$ 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 δ is injective, $\text{rank } J(\mathbb{Q}) + \dim J(\mathbb{Q})[2] \leq 1$, and since $\dim J(\mathbb{Q})[2] = 1$, the rank is 0. $\square$

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 $\text{div}(v+1) = 4P - 4O$, 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 $C(\mathbb{Q}) = \{O, P\}$. $\square$

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 $x^4 - v^3w - (x+w)vw^2 - w^4 = 0$ 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 $w = t^4 - t^9 - \dots \in \mathbb{Z}[[t]]$. Hence x and v have poles of order 3 and 4 at O , respectively. The known rational points are O and

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

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

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

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

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

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 $H \rightarrow S_5$) 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 $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow \mathcal{L}^\times / \mathcal{L}^{\times 2}$ 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 $H^1(\mathbb{Q}, J[2]) \rightarrow H^1(\mathbb{Q}, E)$ is injective. $\square$

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. $\text{Cl}(K_{10})[2] = \text{Cl}(K_{16})[2] = 0$.

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

$$B^-(K_{10}) > 0.3436681640333619, \quad B^-(K_{16}) > 0.0228202034642712$$

(certificate 1.1.13c). The conclusion follows from Proposition B. $\square$

Step 3: upper bound for the rank.

Lemma 3.13.5. $\text{rank } J(\mathbb{Q}) \leq 1$.

Proof. By Lemma 3.13.3, δ 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,

$$\dim K_{10}(S, 2) = (2 + 4) + 4 = 10, \quad \dim K_{16}(S, 2) = (0 + 8) + 7 = 15,$$

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

$$(v - 2x + 2)((v + x - 1)^2 + 3x^2 - 5x + 4) = ((x - 1)(x - 3))^2$$

on C , as the value of $1 / ((v + x - 1)^2 + 3x^2 - 5x + 4)$.

- (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 $2e_p$ 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 δ is injective and $\dim J(\mathbb{Q})[2] = 1$, $\text{rank } J(\mathbb{Q}) \leq 2 - 1 = 1$. $\square$

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

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

In the chart at O , $\omega = -(w, t, 1) dt / (1 + 2tw + 3w^2 + 4w^3)$. 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. $\square$

Lemma 3.13.7. *Let $L = \log[P_1 - O]$. The 3-adic logarithms with respect to ω are as follows modulo 27.*

	ω_0	ω_1	ω_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 $\log(E - 3O) = \sum_e \int_{e'}^e \omega$. On these disks $3v^2 + x + 1$ is a unit, so $x - c$ is a parameter. Writing $\omega(x_e + s) = \sum_{n \geq 0} a_n s^n ds$ (a_n integral) and setting $\delta = x_e - c \in 3\mathcal{O}$, we have

$$\int_{e'}^e \omega = \sum_{n \geq 0} \frac{(-1)^n a_n \delta^{n+1}}{n+1}.$$

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 $\log(E_- - 3O) = \operatorname{Tr} \int_{P_-}^e \omega$, and with respect to the parameter v the denominator of $\omega = (1, x, v) dv / (4x^3 - v)$ 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 $\operatorname{rank} J(\mathbb{Q}) = 1$. $\square$

Step 5: Chabauty–Coleman at $p = 3$. Since $v_3(L_0) = 1 \leq v_3(L_1), v_3(L_2)$,

$$A = \left(-\frac{L_1}{L_0}, 1, 0\right), \quad B = \left(-\frac{L_2}{L_0}, 0, 1\right)$$

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 $A\omega$ and $B\omega$ annihilate the logarithms of all of $J(\mathbb{Q})$. Also, from the table,

$$A \cdot \log(Q_+ - O) \equiv 15, \quad A \cdot \log(Q_- - O) \equiv 12 \pmod{27},$$

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

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

$$q_1 = vz, \quad q_2 = x^2, \quad q_3 = -(v^2 - 3vz + xz + 3z^2);$$

then the projective completion of (7) is the smooth plane quartic $C : q_2^2 = q_1q_3$. Let $(x : v : z : r : s)$ be coordinates on $\mathbb{P}^4$, and let D be the intersection of the three quadrics

$$Q_1 = vz + 3r^2, \quad Q_2 = x^2 + 3rs, \quad Q_3 = q_3 + 3s^2. \tag{8}$$

On D we have $q_1 = -3r^2$, $q_2 = -3rs$, $q_3 = -3s^2$, so $q_1q_3 = q_2^2$. Hence $\pi(x : v : z : r : s) = (x : v : z)$ is a morphism $D \rightarrow C$ (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 π 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 $v \leq 0$, and if $v = 0$, then $x = 0$.

Proof. Suppose $v \geq 1$. If $x \geq 0$, then $v^2 - 3v + x + 3 = (v - 1)(v - 2) + x + 1 \geq 1$, so the left-hand side is positive. If $x = -t$ with $t \geq 1$, then the left-hand side is $t^4 - tv + (v - 1)^3 + 1$. If $1 \leq v \leq t^3$, then $t^4 - tv \geq 0$ and $(v - 1)^3 + 1 \geq 1$. If $v \geq t^3 + 1$, then $(v - 1)^2 \geq t^6 \geq t$, so $(v - 1)^3 \geq t(v - 1)$, 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 $x^4 = 0$. $\square$

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 $x \neq 0$, 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 $p \neq 3$ the exponent of p in n is a multiple of 4, and we can write

$$n = du^4, \quad d \in \{1, 3, 9, 27\}, \quad u \in \mathbb{Z}_{>0}.$$

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 $u^4 \geq u^2$ and $4|uw| \leq 2u^2 + 2w^2$ we get $3B - |4uw + 1| \geq 4w^2 + 16u^2 + 2 > 0$. If $A \neq 0$, then $|3AB| \geq 3B > |4uw + 1|$; 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 $Q_3 = -(n^2 + 3n + x + 3) + 3s^2 = 0$. $\square$

Step 2: the Prym map. Let M_1, M_2, M_3 be the 5×5 symmetric matrices of Q_1, Q_2, Q_3 in (8) ($Q_i(X) = X^T M_i X$). In the pencil of quadrics

$$Q_t = Q_1 - 2tQ_2 + t^2Q_3 = (q_1 - 2tq_2 + t^2q_3) + 3(r - ts)^2,$$

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,

$$12 \det(M(q_1) - 2tM(q_2) + t^2M(q_3)) = f(t) := 3t^6 - 18t^5 + 36t^3 + 6t$$

(certificate 1.1.14a; $M(q_i)$ is the 3×3 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

$$H : \eta^2 = f(t), \quad J = \text{Jac}(H)$$

be the genus 2 curve and its Jacobian. H has good reduction at 5 and 7. If $f(t) \neq 0$, then Q_t has rank exactly 4, and its two families of planes correspond to $\eta = \pm \sqrt{f(t)}$. D_∞ denotes the sum of the two points at infinity of H (a rational divisor).

The Bruin construction of [Bru08, RR18] gives a morphism $\phi : D \rightarrow J$ over $\mathbb{Q}$. Up to an overall sign, ϕ is the composition of $p \mapsto [2\sigma(p) - 2p] \in \text{Prym}(D/C)$ with the isomorphism $\text{Prym}(D/C) \cong J$; 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 ($P^\top M_i w = 0, i = 1, 2, 3$). Then

$$a_p(t) = w^\top M_1 w - 2t w^\top M_2 w + t^2 w^\top M_3 w \quad (9)$$

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 η . 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

$$G = [B_0 - A_0] = (t^2 - 24t, \frac{1729}{2}t) \in J(\mathbb{Q})$$

(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 $Q_1(w) = 0$, $Q_2(w) = 1$, $Q_3(w) = 3 \cdot \frac{1}{36} = \frac{1}{12}$,

$$a_{P_+}(t) = -2t + \frac{1}{12}t^2 = \frac{1}{12}t(t - 24).$$

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 εG . The Mumford representation is checked from $t(t - 24)$, $b(0) = 0$, $b(24) = 1729 \cdot 12 = 20748$. $\square$

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, $\rho_7 : J(\mathbb{Q}) \rightarrow J(\mathbb{F}_7)$, is $\{0, \bar{G}\}$.

Proof. certificate 1.1.14c verifies the following by exact computation:

$$\#\text{Sel}^{(2)}(J/\mathbb{Q}) = 2, \quad \#J(\mathbb{F}_5) = 23, \quad \#J(\mathbb{F}_7) = 32, \quad \text{ord } \bar{G} = 2, \quad \bar{G} \notin 2J(\mathbb{F}_7).$$

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 ℓ , we would need $\ell \mid 23$ when $\ell \neq 5$ and $\ell \mid 32$ when $\ell \neq 7$; no such ℓ exists. Hence $J(\mathbb{Q})$ has no torsion, and in particular $J(\mathbb{Q})[2] = 0$. By [Sto01, PS97, PS99], $\#\text{Sel}^{(2)} = 2$ gives $\text{rank } J(\mathbb{Q}) \leq 1$. 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 $\{0, \bar{G}\}$. $\square$

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 σ have the same $a_{\bar{p}}$.

$(x, v, r, s) \bmod 7$	$a_{\bar{p}}(t)$
$(0, 0, 0, 1), (0, 0, 0, 6) \quad (= \bar{P}_+, \bar{P}_-)$	$t^2 + 4t$
$(0, 4, 1, 0), (0, 4, 6, 0)$	$t^2 + t + 4$
$(4, 2, 2, 2), (4, 2, 5, 5)$	$t^2 + t + 4$
$(5, 2, 2, 4), (5, 2, 5, 3)$	$t^2 + t + 4$

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 3×5 matrix $(P^T M_i)_i$ 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 $\bar{p} \in \{\bar{P}_+, \bar{P}_-\}$. $\square$

Step 5: 7-adic Chabauty in the two residue disks. The differentials of H

$$\omega_0 = \frac{dt}{2\eta}, \quad \omega_1 = \frac{t dt}{2\eta}$$

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 $\lambda = (\lambda_0, \lambda_1) : J(\mathbb{Q}_7) \rightarrow \mathbb{Q}_7^2$ be the logarithm with respect to this basis, and write $\lambda_{\omega'}$ for the component with respect to a differential ω' .

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 α 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, η is a local parameter on this disk. Since $t = \alpha + \eta^2/f'(\alpha) + O(\eta^4)$,

$$\omega_0 = \left(\frac{1}{f'(\alpha)} + O(\eta^2) \right) d\eta, \quad \omega_1 = \left(\frac{\alpha}{f'(\alpha)} + O(\eta^2) \right) d\eta,$$

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

$$\ell_0 \equiv \frac{20748}{f'(\alpha)}, \quad \ell_1 \equiv \frac{20748\alpha}{f'(\alpha)} \pmod{7^3}.$$

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 $\lambda_\omega(H_0) = (\ell_1 - \beta\ell_0)/m = 0$. $\square$

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,*

$$\phi^*\omega = g(x) dx, \quad g \in \mathbb{Z}_7[[x]], \quad g(0) = \mp \frac{\beta}{3} \in \mathbb{Z}_7^\times.$$

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).

$$s = 1 + \frac{x}{6} - \frac{x^2}{72} + \frac{x^3}{432} + O(x^4), \quad r = -\frac{x^2}{3} + \frac{x^3}{18} - \frac{x^4}{72} + O(x^5), \quad v = -\frac{x^4}{3} + \frac{x^5}{9} + O(x^6).$$

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]), ϕ extends to a morphism over $\mathbb{Z}_7$. Since ω_0, ω_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

$$t_1 = \frac{2}{3}x^2 - \frac{1}{9}x^3 + O(x^4), \quad t_2 = 24 - \frac{1729}{9}x^3 + O(x^4).$$

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. $\square$

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_- . σ 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

$$\int_{P_+}^R \phi^*\omega = \lambda_\omega(\phi(R) - \phi(P_+)) = 0.$$

This is because $\phi(R) - \phi(P_+) \in J(\mathbb{Q})$, and by Lemma 3.14.8, ω annihilates the logarithms of $J(\mathbb{Q})$. On the other hand, writing $g = \sum_{j \geq 0} c_j x^j$ as in Lemma 3.14.9,

$$\int_{P_+}^R \phi^*\omega = \sum_{j \geq 1} \frac{c_{j-1}}{j} \xi^j.$$

If $\xi \neq 0$, the first term has valuation $v_7(\xi)$, and the terms with $j \geq 2$ have valuation at least $jv_7(\xi) - v_7(j) > v_7(\xi)$ (since $(j-1)v_7(\xi) \geq j-1 > v_7(j)$). Then the integral has finite valuation $v_7(\xi)$, so it cannot be 0. Hence $\xi = 0$, that is, $R = P_+$. $\square$

Proof of Theorem 3.14.1. By Lemma 3.14.3, integer solutions have $v \leq 0$, 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. $\square$

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

$$u = -\frac{y}{x}, \quad v = -x.$$

Then $x^4 - x^2 + xy + y^3 = v^2(v^2 + u^3v - u - 1)$, so the solutions with $x \neq 0$ lie on

$$C : v^2 + u^3v = u + 1, \quad \text{equivalently} \quad w^2 = u^6 + 4u + 4 \quad (w = 2v + u^3). \quad (10)$$

Put $J = \text{Jac}(C)$, 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

$$x = -v, \quad y = uv, \quad z = -u^2v = y^2/x$$

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

$$y^2 = xz, \quad x^3 - x + y(z + 1) = 0, \quad z^2 + z = y(1 - x^2). \quad (11)$$

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 ℓ 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 $z = y^2/x$. $\square$

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 $2^{-12} \text{disc}(u^6 + 4u + 4) = -8539$, 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. $\square$

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 ω_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. $\text{rank } J(\mathbb{Q}) \leq 2$.

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. $\square$

Step 2: differentials and principal divisors. Put

$$\omega_1 = \frac{dx}{1+3z}, \quad \omega_2 = \frac{y}{x} \omega_1, \quad \eta_1 = 2y \omega_1, \quad \eta_2 = x \omega_1$$

(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 ω_1, ω_2 form a basis of the holomorphic differentials. As a section of the relative dualizing sheaf of the regular model, ω_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:

$$x = t^{-3}\rho, \quad y = -t^{-4}\rho, \quad z = t^{-5}\rho, \quad \rho^2 - \rho = t^5 + t^6, \quad \rho(0) = 1. \quad (12)$$

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 η_i are of the second kind with poles only at O , and with the convention $\langle [\alpha], [\beta] \rangle = \text{Res}_O((\int \alpha)\beta)$ the cup product matrix of $\omega_1, \omega_2, \eta_1, \eta_2$ is $\begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix}$. So $W = \langle [\eta_1], [\eta_2] \rangle$ is an isotropic subspace of H_{dR}^1 complementary to the holomorphic differentials.

Lemma 3.15.5. *The following divisors hold on C (certificate 1.1.15b):*

$$\begin{aligned} \text{div}(x) &= D + 2E - 3O, & \text{div}(y) &= B + F_1 + D + E - 4O, \\ \text{div}(y - x) &= A + 2D + E - 4O, & \text{div}(x + 1) &= A + B + C_1 - 3O, \\ \text{div}(x + y) &= C_1 + G + D + E - 4O, & \text{div}(z - 2x - 1) &= 3A + C_1 + H - 5O. \end{aligned}$$

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. $\square$

Step 3: the local height at 2. For $P = (a, b, c)$ and $Q = (x, y, z)$ put

$$v_P(Q) = \frac{z + c + 1 + by/x}{x - a} \omega_1(Q).$$

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 $v_D = \frac{z+1}{x} \omega_1$ and $v_E = \frac{z}{x} \omega_1$. At O ,

$$v_P = (-t^{-1} - at^2 + bt^3 + \dots) dt,$$

so the coefficients of t^0 and t^1 are 0. The bidifferential identity

$$d_P v_P(Q) - d_Q v_Q(P) = \sum_{i=1}^2 (\eta_i(P) \omega_i(Q) - \omega_i(P) \eta_i(Q)) \quad (13)$$

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 χ_2 of the cyclotomic idele class character of [CG89, BB12, BB15]. Put

$$I(P) = \left(\int_O^P \omega_1, \int_O^P \omega_2 \right), \quad J(P) = \left(\int_O^P \eta_1, \int_O^P \eta_2 \right), \quad K(P, Q) = \int_O^Q v_P,$$

with the following normalizations at the end points. $J_j(P) = \Phi_j(P)$, where Φ_j is the Coleman integral of η_j whose Laurent expansion in t at O has constant term 0 (this depends on the parameter t , not only on ∂_t). $K(P, Q) = \Lambda_P(Q)$, where Λ_P is the Coleman integral of v_P with $\Lambda_P + \log_2 t \rightarrow 0$ at O (this depends only on ∂_t). For $P \neq E$ let v_P be the tangent vector at P with $\omega_1(v_P) = 1$, and put $K(P, P) = \lim_{Q \rightarrow P} (\Lambda_P(Q) - \log_2 z_P(Q))$ for a parameter z_P at P with $dz_P(v_P) = 1$; at E we use ∂_s and $z_E = s$, with $s = x/y$ as in (14) below. Define

$$\mathcal{H}(P, Q) = K(P, Q) - J(P) I(Q)^\top.$$

Lemma 3.15.6. For $P, Q \in \mathcal{U}(\mathbb{Q}_2)$, with the tangent vector ∂_t at O and, if $Q = P$, the tangent vector v_P (or ∂_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 ω_{P-O} of the third kind with residue divisor $P - O$ and $\Psi(\omega_{P-O}) \in W$. Write $\Psi(v_P) = \sum_i a_i [\omega_i] + w$ with $w \in W$; by the cup product matrix, $\langle [\eta_j], \Psi(v_P) \rangle = a_j$. The global symbol of [BB12, Section 2] with $v = v_P$, $\beta = \eta_j$, $\Phi_\beta = \Phi_j$ has two terms: at P the residue is $\Phi_j(P) = J_j(P)$, and at O it is 0, because $v_P = (-t^{-1} + 0 + 0 \cdot t + O(t^2)) dt$ while Φ_j has a pole of order at most 2 and constant term 0. So $a_j = J_j(P)$, and $\omega_{P-O} = v_P - \sum_i J_i(P) \omega_i$. Hence $\int_{Q-O} \omega_{P-O} = K(P, Q) - J(P) I(Q)^\top$, 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 $h_2(\operatorname{div} f, a) = \log_2 f[a]$ for divisors a of degree 0, because $\omega_{\operatorname{div} f} = df/f$; by [Gro86, BB15] these properties determine h_2 . $\square$

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 $J(P) I(Q)^\top$ it would not. Integrating (13), with Q replaced by a variable point R , from $R = O$ to $R = Q$ gives

$$d_P \mathcal{H}(P, Q) = v_Q(P) - \sum_i \omega_i(P) J_i(Q).$$

The boundary term at O vanishes: if $R \rightarrow O$ and $t = t(R)$, then $v_R(P) = -t^{-2} \omega_1(P) + t^{-1} \omega_2(P) + O(t)$ 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

$$d\mathcal{H}(P, P) = -2 \sum_i \omega_i(P) J_i(P) - v_E(P), \quad d\mathcal{H}(P, E) = v_E(P) - \sum_i \omega_i(P) J_i(E),$$

so $d\tau_* = -\sum_i \omega_i(2J_i(P) + J_i(E))$, and τ_* 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 ∂_s .

Proof. On the diagonal the two regular parts of $v_P(Q)$ and $v_Q(P)$ 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 v_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 $-v_E$; 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 $s = x/y$:

$$z + s^5 z^2 + 1 - s = 0, \quad z(0) = -1, \quad x = s^2 z, \quad y = sz, \quad \omega_1 = \frac{s ds}{1 + 2s^5 z}. \quad (14)$$

Since ω_1 vanishes to order 1 at E , v_P degenerates as $P \rightarrow E$; 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. $\square$

Step 4: local heights away from 2.

Lemma 3.15.8. Let ℓ be an odd prime and $P \in \mathcal{U}(\mathbb{Z})$. With the tangent vectors ∂_t at O , v_P at P and ∂_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 ∂_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 ℓ , then $T(P) \in \ell\mathbb{Z}_\ell$ and $R(P) \in -1 + \ell\mathbb{Z}_\ell$, so $v_\ell(x(P)) \leq -3$. 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), $h_\ell(a_1, a_2) = \chi_\ell(\ell)(a_1 \cdot a_2)_\ell = -(a_1 \cdot a_2)_\ell \log_2 \ell$, 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 αt_x adds $\chi_\ell(\alpha) \text{ord}_x(a_1) \text{ord}_x(a_2)$.

(iii) The tangent vectors ∂_t at O and ∂_s at E ($s = -T$) are integral. Let $P \neq E$ and $n = (P \cdot E)_\ell$. Since $\text{div } \omega_1 = \bar{E} + \bar{O}$ with no vertical part and $\bar{P}$ meets the special fibre in a smooth point and avoids $\bar{O}$, the restriction of ω_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 $(P \cdot P)_{v_P} = -(P \cdot \text{div } \omega_1)_\ell$).

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 ∂_s . $\square$

For the eight known points, the resulting decomposition $\mathcal{H}(P, Q) - I(P)MI(Q)^\top = \sum_{\ell \neq 2} (P \cdot Q)_\ell \log_2 \ell$ ($P \neq Q$) and $\mathcal{H}(P, P) = I(P)MI(P)^\top$, 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 $P \in \mathcal{U}(\mathbb{Z})$,

$$\tau_*(P) = h(P, P) + h(P, E) \quad (\text{for } P = E: \tau_*(E) = 2h(E, E)).$$

Proof. The tangent vectors ∂_t at O , v_P at $P \neq E$ and ∂_s at E are $\mathbb{Q}$ -rational, so by [CG89] $h(P, P) + h(P, E) = \sum_v (h_v(P - O, P - O) + h_v(P - O, E - O))$. The term at 2 is $\tau_*(P)$ by Lemmas 3.15.6 and 3.15.7, the terms at odd ℓ vanish by Lemma 3.15.8, and there is no archimedean term. $\square$

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 ($\sum_P \text{ord}_P(f)I(P) = 0$ 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 $k = \text{ord}_O f$, then

$$\sum_{P \neq O} \text{ord}_P(f) J(P) = \text{Res}_O \left(\log_2 \frac{f}{ct^k} \eta \right).$$

This is the global symbol identity $\sum_x \text{Res}_x((df/f)\Phi_j) = \langle [\eta_j], \Psi(df/f) \rangle = 0$ of [BB12, Section 2], after an integration by parts at O that uses the normalization of Φ_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. $\square$

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 ω_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 $k_1(P) = \int_B^{F_1} v_P$ and $k_2(P) = \int_D^G v_P$. Then

$$K(P, E) = \frac{k_1(P) + 2k_2(P)}{13}, \quad K(P, F_1) = \frac{7k_1(P) + k_2(P)}{13}, \quad K(P, D) = -2K(P, E).$$

Proof. By [Gro86, BB15] and the symmetry of h_2 , $\sum_Q \text{ord}_Q(f)K(P, Q) = h_2(P - O, \text{div } f) = \log_2(f[P]/f[O])$, where $f[\cdot]$ is the value normalized by the chosen tangent vectors (the first equality holds because $\sum_Q \text{ord}_Q(f)I(Q) = 0$). 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 $y = sV$, $v_D - dx/x = -2V^2\omega_1$, and on the disk of B and F_1 , $v_{F_1} - dx/(x - 1) = \frac{2y(x+1)}{z+1}\omega_1$; the subtracted logarithms take values $\log_2(\pm 2^m) = 0$. $\square$

Lemma 3.15.12. Let L be the matrix with rows I_D, I_{F_1} , let $B_h = (K(P, Q) - J(P)I(Q)^\top)_{P, Q \in \{D, F_1\}}$, and $M = L^{-1}B_h(L^{-1})^\top$. 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 $\text{rank } J(Q) = 2$, and $h(P, Q) = I(P) M I(Q)^\top$ for all $P, Q \in J(Q)$, where I is extended additively to $J(Q)$.

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 $\text{rank } J(Q) \geq 2$, and with Lemma 3.15.4 the rank is 2. Then $\log: J(Q) \otimes \mathbb{Q}_2 \rightarrow \mathbb{Q}_2^2$ 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 $J(Q)$ and no saturation is needed. $\square$

Step 6: the quadratic Chabauty function on the four disks. By Lemmas 3.15.9 and 3.15.12, the function

$$q(P) = \tau_*(P) - I(P) M I(P)^\top - I(P) M I_E^\top$$

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,

$$dq = - \sum_{i=1}^2 \omega_i \left(2J_i(P) + J_i(E) + \sum_{j=1}^2 M_{ij}(2I_j(P) + I_j(E)) \right).$$

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 ω_i/ds and η_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 : $L^{-1}(\delta B_h)(L^{-1})^\top$ has valuation at least $-2 + 40 - 2$, and $\delta(L^{-1}) = -L^{-1}(\delta L)L^{-1}$ has valuation at least 36 while $B_h(L^{-1})^\top$ has valuation at least 0 . So at most four bits are lost, and the five bits needed for the table are guaranteed. $\square$

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 ω_i, η_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 $n + 2 - 2k \geq 2^k + 3 - 2k > 4$. $\square$

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

$$2^{-e}q_{P_0}(2u) \equiv u^2 + u \pmod{2}, \quad e_A = e_D = e_E = 2, \quad e_B = 3.$$

Write $2^{-e}q_{P_0}(2u) = \sum_{n \geq 1} b_n u^n$. Then $b_n \in \mathbb{Z}_2$, $b_n \rightarrow 0$, 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.) $\square$

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. $\square$

4 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.

4.1 $x^4 + 3y^3 + z^3 = 0$ ($H = 48$)

Theorem 4.1.1. *The only primitive integer solutions of $x^4 + 3y^3 + z^3 = 0$, that is, integer solutions with $\gcd(x, y, z) = 1$, are*

$$(x, y, z) = (\pm 1, 0, -1), \quad (\pm 895, -6202, 4199).$$

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). ξ 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 $\text{Cl}(M)[2] = 0$ (Step 6) and $\text{rank } E(M) = 6$ (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 4.2–4.3.

Lemma 4.1.2. *Let $p \geq 3$, and let $\Lambda(T) = a_0T + \sum_{n \geq 2} a_{n-1}T^n/n$ 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. $\square$

In elliptic Chabauty (Proposition D), for a local parameter T of a residue disk, we take Λ to be the composition of a global annihilator with the elliptic logarithm. This Λ vanishes at every rational point in the disk. Since Λ' is the pullback differential, if the map and the differential are integral on the disk and $\Lambda'(0)$ is a unit, then by Lemma 4.1.2 the only rational point in the disk is its center.

Step 1: descent over the cubic field.

Lemma 4.1.3. (1) $\mathcal{O}_K = \mathbb{Z}[\theta]$, $\text{disc } K = -243$, $h(K) = 1$, $\mathcal{O}_K^\times = \{\pm\varepsilon^n\}$.

(2) For each primitive solution we have

$$\begin{aligned} Z_0 + \theta Y_0 &= \varepsilon^j \beta^4, & j \in \{0, 1, 2, -1\}, & \beta = a + b\theta + c\theta^2, \\ a, b, c &\in \mathbb{Z}, & \gcd(a, b, c) &= 1, & 3 \nmid N\beta. \end{aligned}$$

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 θ^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 $(\theta - 1)$, (θ) , $(\theta^2 + \theta + 1)$, 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 ε (certificate 1.2.1a). Hence ε 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 $v_{\mathfrak{p}}(Z_0 + \theta Y_0) = v_{\mathfrak{p}}(X^4)$ is a multiple of 4. Since $3 \nmid X$, (θ) 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 θ^2 -coefficient of $Z_0 + \theta Y_0$ is 0. $\square$

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

$$\varphi_j : C_j \longrightarrow E_j : V^2 = U^3 - 36\varepsilon^j U, \quad (U, V) = (12\varepsilon^{-j}\nu^2, 36\lambda\nu)$$

is a map over K . Written in homogeneous coordinates, it has no base points at the primes used below.

Lemma 4.1.4. $C_2(\mathbb{Q}) = \emptyset$ 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

$$A = (-3, 9), \quad B = (6\theta - 6\theta^2, 36 - 36\theta + 12\theta^2)$$

fill all 16. Hence $\text{rank } E_0(K) = 2$, $\text{rank } E_2(K) = 0$, 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 $C_2(\mathbb{Q}) = \emptyset$.

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 φ_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 θ modulo 577^3 and computing the logarithm of $\omega = dU/(2V)$ (Lemma E), we get, modulo 577^2 ,

$$\frac{1}{577} \log A \equiv (4351, 4351, 4351), \quad \frac{1}{577} \log B \equiv (55622, 183530, 93777)$$

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 θ 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 4.1.2, 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, $(x, y, z) = (\pm 1, 0, -1)$. $\square$

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 4.1.5. *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*

$$w^2 = P(m, n), \quad (x, y, z) = (\pm w, -Y(m, n), -Z(m, n))$$

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 ℓ other than 3 divides all of them, then β 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 ± 9 or ± 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

$$(A : B : C) = (h_A : h_B : h_C) = (2n(3m - 2n) : 2m(3m - 2n) : 2m^2 - n^2)$$

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

$$\beta^2 = -(h_A + h_B\theta + h_C\theta^2), \quad (N\beta)^2 = P(m, n)$$

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, ℓ is odd and k is even. $\square$

Step 4: two-cover descent. Put

$$\begin{aligned} r &= \frac{1}{4}(-3 + \theta - \theta^2 + (3 + 3\theta + \theta^2)\xi), & \delta &= \frac{1}{2}(3 - 3\theta + \theta^2)(1 + \xi), \\ \pi_0 &= \theta - 1, & \pi_1 &= -1 + \theta - \theta^2 + 2\theta\xi + \delta. \end{aligned}$$

Then $f(r) = 0$.

Lemma 4.1.6. *The pair (q, v) of Lemma 4.1.5 satisfies*

$$q - r = c \pi_1 \gamma^2, \quad c \in \mathbb{Q}^\times, \gamma \in L^\times$$

Proof. An integral basis of L is $(1, \theta, \theta^2, \xi, \theta\xi, \delta)$, and $\text{disc } L = 2^4 3^{11}, h(L) = 1$. 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 (ξ) 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 π_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 4.1.5, $q \in 2\mathbb{Z}_2$. For $q_0 = 0$ and for $q_0 = 2$, the (π_0, π_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 π_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 π_1 . $\square$

Step 5: an elliptic curve over the degree 12 field. Let ξ_1, ξ_2 be the two roots of $T^2 - WT + R_0$. Put

$$R(T) = \frac{1}{16}(T^5 - T^4 - 12T^3 + 4T^2 + 39T - 15), \quad \Pi(T) = \frac{1}{8}(T^5 - T^4 - 8T^3 + 8T^2 + 27T - 11)$$

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

$$d = -3 - 2\theta + 3\theta^2 + (\theta + \frac{5}{6}\theta^2)W + (1 - \frac{1}{2}\theta^2)W^2 - \frac{\theta}{12}W^3, \quad E : y^2 = x^3 + 2dx^2 + 2d^2x$$

We have $c_4(E) = -32d^2$, $\Delta_E = -256d^6$, $j(E) = 128$, $N_M(d) = -5184 = -2^6 3^4$.

Lemma 4.1.7. (1) $[M : \mathbb{Q}] = 12$, and M has signature $(2, 5)$.

(2) All points of Lemma 4.1.6 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 $\mathcal{Q} \rightarrow E$, and $\varphi^*(dx/(2y)) = -\theta^2 dq/V$.

(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) ε 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 σ_i of L into $\overline{M}$. Applying σ_1, σ_2 to the relation of Lemma 4.1.6 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). $\square$

Step 6: the class group of M .

Lemma 4.1.8. $\text{Cl}(M)[2] = 0$.

Proof. We use twice the ambiguous class number formula for a quadratic extension B/A ([Lem13, Theorem 1])

$$|\text{Cl}(B)^{\text{Gal}(B/A)}| = \frac{h(A)2^{t-1}}{[\mathcal{O}_A^\times : \mathcal{O}_A^\times \cap N_{B/A}B^\times]}$$

(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 σ acts as an involution on the $\mathbb{F}_2$ -space $\text{Cl}(B)[2]$, and an involution on a nonzero space has a nonzero fixed vector.

Put $F = K(\kappa)$, $\kappa = R_0/\theta$, $\kappa^2 = \varepsilon$. Since ε 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 $\text{disc } F = 2^6 3^{10}$. 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 $\text{disc } M = -2^{14} 3^{21}$ (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 4.1.7(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 $|\text{Cl}(M)^{\text{Gal}}| = h(F)$ is odd, and $\text{Cl}(M)[2] = 0$ (certificate 1.2.1f). $\square$

Step 7: the rank. We use the 2-isogenous curve $E' : y^2 = x^3 - 4dx^2 - 4d^2x$ and the isogenies $\phi, \hat{\phi}$ between E and E' . The maps $\alpha : E(M) \rightarrow M^\times / M^{\times 2}$ and $\alpha' : E'(M) \rightarrow M^\times / M^{\times 2}$ 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],

$$2^{\text{rank } E(M)} = \frac{|\alpha(E(M))| |\alpha'(E'(M))|}{4}.$$

Lemma 4.1.9. $\text{rank } E(M) = 6$. 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, $E(M)_{\text{tors}} = \{O, T\}$.

Proof. Both images consist of classes with even valuation outside 2, 3 ($N_M(d) = -2^6 3^4$). By Lemma 4.1.8, 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 ± 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	$ \alpha_v $	$ \alpha'_v $
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, $x^3 + 2dx^2 + 2d^2x = x((x+d)^2 + d^2)$, 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 $2^{\text{rank}} = 32 \cdot 8/4 = 64$.

The dual isogeny $\hat{\phi}(x, y) = ((x - 4d - 4d^2/x)/4, y(1 + 4d^2/x^2)/8)$ 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. $\square$

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 4.1.10. *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 $2^{22}3^229^2$. Its 2-primary part has order 1024 and index 2^{22} . For odd primes ℓ , the matrix of ℓ -components of the free generators $G_1, \dots, G_4, P, Q$ is 8×6 of rank 6 for $\ell = 3$, 8×6 of rank 6 for $\ell = 29$, and 4×6 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 ℓ 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 $2^{22}3^229^2$. 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). $\square$

Step 9: 661-adic logarithms.

Lemma 4.1.11. *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 6×12 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 4.1.10 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 ℓ is determined. Writing $q = q_j + pT$ with $T \in \mathbb{Z}_p$, Lemma 4.1.7(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 4.1.2 each disk contains only its center. Points above parameter infinity were already eliminated by the sieve of Step 8. $\square$

Proof of Theorem 4.1.1. By Lemma 4.1.4, even j gives $(\pm 1, 0, -1)$. There is no solution with $j = 1$. By Lemmas 4.1.5, 4.1.6 and 4.1.7, a primitive solution with $j = -1$ gives a point of $\mathcal{Q}(M)$, and by Lemma 4.1.11, $q \in \{0, -8/3\}$. 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

$$P(2, 7) = 895^2, \quad Y(2, 7) = 6202, \quad Z(2, 7) = -4199$$

gives $(x, y, z) = (\pm 895, -6202, 4199)$. Substituting these values, we get $895^4 + 3(-6202)^3 + 4199^3 = 0$, and $\gcd(895, 6202, 4199) = 1$. $\square$

4.2 $2x^4 - y^4 + z^3 = 0$ ($H = 56$)

Theorem 4.2.1. *The only primitive integer solutions ($\gcd(x, y, z) = 1$) of $2x^4 - y^4 + z^3 = 0$ are*

$$(x, y, z) = (0, \pm 1, 1), \quad (\pm 1, \pm 1, -1)$$

(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 $|a|, |b| \leq 1/2$ and $|a^2 - 2b^2| \leq 1/2$. 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

$$f(A, B) = A^3 + 6A^2B + 6AB^2 + 4B^3, \quad g(A, B) = A^3 + 3A^2B + 6AB^2 + 2B^3$$

and $F(t) = f(t, 1)g(t, 1) = t^6 + 9t^5 + 30t^4 + 60t^3 + 60t^2 + 36t + 8$. We have $\text{disc } F = 2^{26}3^6$. The two genus 2 curves

$$C_+ : w^2 = F(t), \quad C_- : w^2 = -F(t)$$

are understood as their smooth projective models. C_+ has the points at infinity ∞_+, ∞_- .

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 $\text{rank } E(K) = 2$ (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 4.2.2. *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*

$$C_-(\mathbb{Q}) = \emptyset, \quad C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$$

then Theorem 4.2.1 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, $(x, y, z) = (\pm 1, \pm 1, -1)$. $\square$

Step 2: the cubic field. Put

$$K = \mathbb{Q}(h), \quad h^3 + 3h - 2 = 0, \quad e = 1 - h - h^2, \quad \rho = h - 1, \quad \pi = -3 - h - h^2,$$

$$r_f = -4 - h - h^2 = \frac{2}{h-1}, \quad r_g = h - 1.$$

The elements r_f, r_g are roots of $f(t, 1), g(t, 1)$. The two polynomials have discriminants $-864, -216$, and $\text{Res}(f, g) = -512$.

Lemma 4.2.3. $\mathcal{O}_K = \mathbb{Z}[h]$, $\text{disc } K = -216$, $\text{Cl}(K) = 0$, $\mathcal{O}_K^\times = \{\pm e^n\}$. The prime ideals above 2 are $(h), (\rho)$, and the prime ideal above 3 is (π) . 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 $\text{Cl}(K) = 0$. 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). $\square$

The rational square classes $-1, 2, 3$ have the masks 1, 10, 19 with respect to $\mathcal{B}$. Indeed,

$$2 = h\rho^2/e, \quad (1 - h + h^2)^2 = -3\pi e$$

(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 4.2.4. $C_-(\mathbb{Q}) = \emptyset$. Every finite rational point of C_+ satisfies

$$t - r_f = c a_1^2, \quad t - r_g = c a_2^2, \quad c \in \mathbb{Q}^\times, \quad a_1, a_2 \in K^\times$$

Proof. Write a finite rational point of C_σ ($\sigma = \pm 1$) 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 σ 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 σ . 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 ω -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. $\square$

Step 4: an elliptic curve over the cubic field. By Lemma 4.2.4, $(t - r_f)(t - r_g)$ 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

$$k = 2 - \frac{1}{2}h^2, \quad m = 2 + \frac{3}{4}h + \frac{3}{8}h^2, \quad n = \frac{3}{2} - \frac{9}{2}h - \frac{21}{8}h^2, \quad r_1 = 6h + 3h^2, \quad d = 2 - h + h^2,$$

$$X = 2(v + t^2 + kt + m), \quad Y = (2t + k)X + n, \quad x_E = 4X - r_1, \quad y_E = 8Y.$$

Then

$$E : y_E^2 = x_E(x_E - 12d)(x_E + 4d), \quad \phi^* \frac{dx_E}{2y_E} = \frac{dt}{4v}$$

The two points at infinity with $v/t^2 \rightarrow +1, -1$ 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 4.2.5. $\text{rank } E(K) = 2$ and $E(K)_{\text{tors}} = E[2]$. The subgroup G generated by

$$P = (-8h + 4h^2, -16 + 56h), \quad Q = (-6h - 3h^2, -12 + 36h + 21h^2)$$

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). $\square$

Step 6: a sieve at 29.

Lemma 4.2.6. 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 4.2.5, 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 4.2.4, $t - r_f$ 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 ± 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. $\square$

Step 7: 29-adic logarithms.

Lemma 4.2.7. $C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$.

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 ,

$$\frac{1}{29} \log P \equiv (647, 368, 410), \quad \frac{1}{29} \log Q \equiv (672, 302, 764)$$

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 4.2.6, $\hat{v}$ 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 4.1.2, each disk contains only its center. $\square$

Proof of Theorem 4.2.1. By Lemmas 4.2.4 and 4.2.7, $C_-(\mathbb{Q}) = \emptyset$ and $C_+(\mathbb{Q}) = \{\infty_+, \infty_-\}$. By Lemma 4.2.2, the only primitive solutions are $(0, \pm 1, 1)$ and $(\pm 1, \pm 1, -1)$. Substituting gives $0 - 1 + 1 = 0$ and $2 - 1 - 1 = 0$. $\square$

4.3 $x^5 + y^4 = 2z^2$ ($H = 56$)

Theorem 4.3.1. *The only primitive integer solutions ($\gcd(x, y, z) = 1$) of $x^5 + y^4 = 2z^2$ are*

$$(x, y, z) = (-1, \pm 1, 0), \quad (1, \pm 1, \pm 1)$$

(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

$$L = \mathbb{Q}(\theta), \quad g(\theta) = \theta^5 + 5\theta^3 + 5\theta - 2 = 0$$

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 $\text{rank } E(L) = 2$ (Step 5) and finish with a sieve at 751 (Step 6) and elliptic Chabauty (Step 7).

Step 1: fifth-power descent.

Lemma 4.3.2. *For each primitive solution ($z \neq 0$) we have*

$$y^2 + zd = \varepsilon^j(a + bd)^5, \quad j \in \{-2, -1, 0, 1, 2\}, \quad \gcd(a, b) = 1, \quad a \text{ odd}, \quad x = (-1)^{j+1}(a^2 - 2b^2)$$

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. $\square$

Step 2: $j = 0$.

Lemma 4.3.3. *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

$$(X, Y) = \left(\frac{r^2}{s^2}, \frac{ru^2}{s^3} \right), \quad X \neq 0, \quad Y^2 = X^3 - 10X^2 + 20X$$

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 $a = 1, z = 0$. $\square$

Step 3: the quintic field and $j = 1, 2$.

Lemma 4.3.4. $\mathcal{O}_L = \mathbb{Z}[\theta]$, $\text{disc } L = 200000 = 2^6 5^5$, $\text{Cl}(L) = 0$, $\mathcal{O}_L^\times / \mathcal{O}_L^{\times 2} = \langle -1, u_1, u_2 \rangle$.

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 $\text{disc } g = 2^6 5^5$, 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 θ (2), q (4), $3 + \theta + 2\theta^2$ (3), ℓ (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. $\square$

The following norm identities hold (certificate 1.2.4b).

$$N(a - \eta b) = F_1(a, b), \quad N(3a - \chi b) = 81F_2(a, b).$$

The minimal polynomials of η and χ 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 4.3.5. *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 γ_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, γ_j is a unit above 2, and by the previous paragraph it is also a unit above 5. For γ_1 the argument above also applies above 3. For γ_2 : modulo 3 we have $g \equiv (T - 1)(T^4 + T^3 - 1)$, the element δ ($N\delta = 81$) generates the prime ideal $\mathfrak{p}_4$ of degree 4, and χ 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),

$$\gamma_1 = u_1^i u_2^k w^2, \quad \gamma_2 = \delta u_1^i u_2^k w^2, \quad i, k \in \{0, 1\}, \quad w \in \mathcal{O}_L$$

The ring $R = (\mathbb{Z}/8\mathbb{Z})[T]/(g)$ has 32768 elements and 336 distinct squares. For a odd and $b \pmod{8}$, the residues of γ_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 γ_1 and 0, 0, 0, 0 for γ_2 (certificate 1.2.4c). The two residues of γ_1 have coefficients $(1, 0, 0, 0, 0)$ and $(1, 0, 4, 4, 4)$. $\square$

Step 4: the elliptic cover. Suppose $j = 1$ and $b \neq 0$. Putting $t = a/b$ and $v = y/(b^2 w)$, we get

$$v^2 = q(t) = t^4 + At^3 + Bt^2 + Ct + D, \quad q(t) = \frac{N(t - \eta)}{t - \eta}$$

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

$$U = 2v + 2t^2 + At, \quad V = 2(U + B - \frac{A^2}{4})t + \frac{A}{2}U + C, \quad R_\theta = 2\theta^3 - 4, \quad \xi = \frac{U - R_\theta}{4}, \quad \zeta = \frac{V}{8}.$$

Then (ξ, ζ) is a point of

$$E: \zeta^2 = \xi^3 - 5\theta\zeta^2 + 5\theta^2\zeta$$

and for $\omega = d\zeta/(2\zeta)$ we have $\phi^*\omega = dt/v$ ($dU/dt = V/v$). The two points at infinity with $v/t^2 \rightarrow +1$, -1 map to O and to

$$P = \left(\frac{-5\theta^4 - 25\theta^2 + 10\theta}{8}, \frac{35\theta^4 - 5\theta^3 + 195\theta^2 - 20}{32} \right)$$

respectively (certificate 1.2.4d).

Step 5: the rank. The partner curve is $E' : \zeta^2 = \zeta^3 + 10\theta\zeta^2 + 5\theta^2\zeta$. We use the 2-isogeny descent of [Sim02, Sil09]. For $E_{a,b} : y^2 = x^3 + ax^2 + bx$, the map α sends a point to the square class of x , and a class μ 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

$$2^{\text{rank } E(L)} = \frac{|\alpha(E(L))| |\alpha'(E'(L))|}{4}.$$

Lemma 4.3.6. $\text{rank } E(L) = 2$ and $E(L)_{\text{tors}} = \{O, T_0\}$ ($T_0 = (0, 0)$). 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 μ 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, $1, u_1 u_2, \ell, u_1 u_2 \ell$. 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 ($5\theta^2/\ell, \zeta(Q)/(u_1 u_2 \ell), \zeta(S)/(u_1 u_2 \ell)$ are squares in L). Hence both images have exactly four elements, and $\text{rank } E(L) = 2$ (certificate 1.2.4e).

For the dual isogeny $\hat{\phi}(x', y') = ((x' + 10\theta + 5\theta^2/x')/4, y'(5\theta^2 - x'^2)/(8x'^2))$ 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 $\{O, T'_0\}$. $\square$

Step 6: a sieve at 751.

Lemma 4.3.7. 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

$$|H| = 36864 = 2^{12} 3^2, \quad [\prod_i E_i(\mathbb{F}_p) : H] = 2^{28} 3$$

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 ∞) 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. $\square$

Step 7: 751-adic logarithms.

Lemma 4.3.8. *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 ,

$$\begin{aligned} \frac{1}{p} \log P &\equiv (423722, 191178, 352807, 294331, 252200), \\ \frac{1}{p} \log Q &\equiv (330447, 456587, 117975, 48293, 396869) \end{aligned}$$

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

$$c \equiv (626, 131, 473, 0, 0) \pmod{p}, \quad \sum_i c_i \equiv 479 \pmod{p}$$

(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 4.1.2, the disks contain only the center $u = 0$, and this is not a finite point. $\square$

Proof of Theorem 4.3.1. By Lemmas 4.3.5 and 4.3.8, 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 4.3.5 there is nothing for $j = \pm 2$, and by Lemma 4.3.3, $j = 0$ gives only $(-1, \pm 1, 0)$. Substituting gives $-1 + 1 = 0$ and $1 + 1 = 2$. $\square$

4.4 $x^5 + y^4 = 3z^2$ ($H = 60$)

Theorem 4.4.1. *The only primitive integer solutions ($\gcd(x, y, z) = 1$) of $x^5 + y^4 = 3z^2$ are*

$$(x, y, z) = (-1, \pm 1, 0), \quad (11, \pm 29, \pm 538)$$

(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

$$\mathcal{C} : u^4 = r^4 - 15r^2s^2 + 45s^4$$

(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

$$\mathcal{H} : Y^2 = f(X) := X(X^2 + 30X + 45)(X^2 - 45)$$

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

$$\rho = -15 + 6d = -21 + 12e, \quad \tau = 3d = -3 + 6e,$$

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 4.4.2. *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 $x = -1, y = \pm 1$. $\square$

Lemma 4.4.3. *For every primitive solution there exist $j \in \{-2, -1, 0, 1, 2\}$ and integers a, b such that*

$$y^2 + z\sqrt{3} = (2 + \sqrt{3})^j(a + b\sqrt{3})^5, \quad \gcd(a, b) = 1, \quad a + b \text{ odd}, \quad 3 \nmid a, \quad x = 3b^2 - a^2.$$

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 γ^5 , we get $j \in \{-2, \dots, 2\}$. 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 $3 \nmid x$, $3 \nmid a$. $\square$

Step 2: elimination of $j \neq 0$. Writing $(a + b\sqrt{3})^5 = F + G\sqrt{3}$, we have

$$F = a(a^4 + 30a^2b^2 + 45b^4), \quad G = b(5a^4 + 30a^2b^2 + 9b^4).$$

Multiplying by $(2 + \sqrt{3})^1$ and $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, we get, for $j = 1, 2$,

$$y^2 = F_1(a, b) := 2F + 3G, \quad y^2 = F_2(a, b) := 7F + 12G.$$

Taking conjugates changes (j, b, z) into $(-j, -b, -z)$, so it suffices to eliminate $j = 1, 2$.

We use the quintic field $L = \mathbb{Q}(\theta)$, $g(\theta) = 0$, $g(T) = T^5 - 5T^3 + 5T - 4$. The following facts are checked by certificate 1.2.6a.

- $\text{disc}(g) = 2^4 \cdot 3^2 \cdot 5^5$ 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 $\mathcal{O}_L^\times / \mathcal{O}_L^{\times 2}$.
- $\omega = \vartheta - 2$ and $\kappa = \vartheta^2 + \vartheta - 1$ have norms 2 and 4, and $(2) = (\omega)(\kappa)^2$. 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 $\mu_2 = -\vartheta^4 - \vartheta^3 + 3\vartheta^2 + 2\vartheta$,

$$N(2a - \mu_1 b) = 16F_1(a, b), \quad N(2a - \mu_2(a + b)) = 8F_2(a, b).$$

The discriminants of the minimal polynomials of μ_1 and μ_2 are $2^{24}3^{10}5^5$ and $2^{16}3^{10}5^5$.

Lemma 4.4.4. In Lemma 4.4.3, $j = 0$.

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 γ . The coefficient of μ_1 or μ_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 μ_1 (or μ_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 γ , 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, $v_2(N\gamma) = v_{\omega}(\gamma) + 2v_{\kappa}(\gamma)$, so $v_{\omega}(\gamma) \equiv v_2(N\gamma) \equiv j - 1 \pmod{2}$. Since $h_L = 1$,

$$\gamma = \omega^{j-1} e_1^i e_2^k \kappa^\ell w^2, \quad i, k, \ell \in \{0, 1\}, \quad w \in \mathcal{O}_L.$$

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 $a, b \pmod{8}$ with $a + b$ odd, the left side $\gamma \pmod{8}$ takes 16 values for each of $j = 1, 2$. The right side is, for each of the eight (i, k, ℓ) , the set of elements $\omega^{j-1} e_1^i e_2^k \kappa^\ell \cdot (\text{square})$. The intersection of the two sets is empty for $j = 1, 2$ and all eight (i, k, ℓ) (certificate 1.2.6a). This is a contradiction. $\square$

Step 3: the quartic curve $\mathcal{C}$.

Lemma 4.4.5. 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

$$x = 3r^2s^2 - u^4, \quad y = \pm u(r^4 - 45s^4), \quad z = \pm rs(5u^8 + 30u^4r^2s^2 + 9r^4s^4).$$

The solutions with $z = 0$ come from $(u, r, s) = (1, 1, 0)$.

Proof. By Lemma 4.4.4, $y^2 = aP$ 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 $a = u^2$, $b = \pm rs$. $\square$

Lemma 4.4.6. *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. $\square$

Step 4: descent over $\mathbb{Q}(\sqrt{5})$.

Lemma 4.4.7. *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 α have the same sign. Call this sign σ . A common prime factor of (α) 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 (α) 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 ± 1 , and $e^2 \notin \mathbb{F}_3$; hence $j = 0$. Writing $\beta^2 = A + Bd$, we get

$$\sigma(A^2 + 5B^2) = r^2 - \frac{15}{2}s^2, \quad 4AB = 3\sigma s^2, \quad A^2 - 5B^2 = u^2.$$

Then $B \neq 0$, and putting $t = s/(2B)$ we get $A = 3\sigma Bt^2$ and

$$(r/B)^2 = \sigma(9t^4 + 5) + 30t^2, \quad (u/B)^2 = 9t^4 - 5.$$

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 $(u, r, s) = (\pm 1, \pm 2, \pm 1)$. $\square$

Proposition 4.4.8. *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 4.4.9. *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 $\text{disc}(f) = 2^{14}3^{20}5^{10}$, 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 $q \bmod 3$ 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). $\square$

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 4.4.9 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 4.4.10. *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 ξ : $-1 - e, -4 + 4e$ 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 $\delta(T_0) = (r_1r_2, -r_1) = ((-e)(3d/e)^2, 3d(e - 1)^2) \equiv (-e, 3d)$. The kernel of δ is $2E_i(K)$, so the last claim follows. $\square$

The case $\sigma = 1$ does not occur, because $E_0(K) = E_0[2]$ and none of the ξ -coordinates $0, \rho, -\tau$ of the torsion points lies in $\mathbb{Q}^\times$.

Step 7: coset sieve.

Lemma 4.4.11. *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 4.4.10 are $P_1 + 2H_1$ (60 elements) and $T_0 + 2H_2$ (12 elements).

The ξ -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 η 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 λ_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. $\square$

Step 8: elliptic Chabauty.

Lemma 4.4.12. *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 $\log : E_i(K) \rightarrow \mathbb{Q}_p^2$, 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

$$\begin{aligned} \ell_1 &\equiv (2490, 2948) \pmod{89^2}, & c_1 &\equiv (11, 2) \pmod{89}, \\ \ell_2 &\equiv (117, 76) \pmod{11^2}, & c_2 &\equiv (10, 4) \pmod{11} \end{aligned}$$

(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 ω 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 ± 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 $X \neq 0$. $\square$

Proof of Proposition 4.4.8. If there is a rational point with $X = \sigma q^2 \neq 0$, then by Lemma 4.4.9 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 4.4.12. What remains is $X = -9$ on E_1 , and $f(-9) = 46656 = 216^2$. $\square$

Proof of Theorem 4.4.1. If $z = 0$, then the solution is $(-1, \pm 1, 0)$ by Lemma 4.4.2. If $z \neq 0$, then the point (u, r, s) of Lemma 4.4.5 has $s \neq 0$, and it is primitive since $\gcd(r, s) = 1$. By Lemma 4.4.7 and Proposition 4.4.8, $X = -9$ 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. $\square$

4.5 $x^5 + y^4 + 3z^2 = 0$ ($H = 60$)

Theorem 4.5.1. *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

$$\mathcal{H}: Y^2 = f(X) := X(X^2 - 30X + 45)(X^2 - 45)$$

(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 4.5.2. *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 $n = 1, y = \pm 1$. $\square$

Let $d_0 = \sqrt{-3}$, $\omega = (-1 + d_0)/2$, and put

$$F(a, b) = a^4 - 30a^2b^2 + 45b^4.$$

Lemma 4.5.3. *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*

$$n = a^2 + 3b^2, \quad y^2 = aF(a, b), \quad z = b(5a^4 - 30a^2b^2 + 9b^4).$$

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 ω -coefficient of γ 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 $(a + bd_0)^5$. $\square$

Lemma 4.5.4. *In Lemma 4.5.3, $a = u^2$ 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:

$$a = -5u^2, \quad F = -5c^2.$$

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 $F \pmod{16} \in \{1, 9, 13\}$. On the other hand, $c^2 \pmod{16} \in \{0, 1, 4, 9\}$, so $-5c^2 \pmod{16} \in \{0, 3, 11, 12\}$. 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. $\square$

Lemma 4.5.5. *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*

$$C : \quad u^4 = r^4 + 15r^2s^2 + 45s^4.$$

Proof. If $z \neq 0$, then $b \neq 0$. For u, b, c as in Lemma 4.5.4,

$$m = \frac{u^4 - 15b^2 + c}{2}, \quad k = \frac{u^4 - 15b^2 - c}{2}$$

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 C . $\square$

Lemma 4.5.6. *Every primitive integral point ($\gcd(u, r, s) = 1$) of 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. $\square$

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 ρ 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 4.5.7. *If a primitive integral point of 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 α is totally positive. A common prime factor of (α) 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 4.5.6; and a prime ideal above a prime factor of s would also divide r^2 , contradicting $\gcd(r, s) = 1$. Hence all valuations of (α) are multiples of 4. Since $h_K = 1$ and α 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 β 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

$$A^2 + 5B^2 = r^2 + \frac{15}{2}s^2, \quad 4AB = 3s^2, \quad A^2 - 5B^2 = u^2.$$

Since $s \neq 0$, $AB \neq 0$. Putting $t = s/(2B)$, we get $A = 3Bt^2$ and

$$(r/B)^2 = 9t^4 - 30t^2 + 5, \quad (u/B)^2 = 9t^4 - 5.$$

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). $\square$

Step 3: a Jacobian of rank 0.

Proposition 4.5.8. $J(\mathbb{Q}) \cong (\mathbb{Z}/2)^2$ and $\mathcal{H}(\mathbb{Q}) = \{\infty, (0, 0)\}$.

Proof. We have $\text{disc}(f) = 2^{14}3^{20}5^{10}$. 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],

$$J(\mathbb{Q})/2J(\mathbb{Q}) \hookrightarrow \ker(N : \mathbb{Q}^\times / \mathbb{Q}^{\times 2} \times (K^\times / K^{\times 2})^2 \rightarrow \mathbb{Q}^\times / \mathbb{Q}^{\times 2}).$$

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 $\dim J(\mathbb{Q})/2J(\mathbb{Q}) \leq 2 = \dim J(\mathbb{Q})[2]$, and $\text{rank } J(\mathbb{Q}) = 0$.

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 ∞ , X has a pole of order 2 and Y a pole of order 5, so $L(2\infty) = \langle 1, X \rangle$. Hence $2P - 2\infty = \text{div}(X - X(P))$, 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 $P = (0, 0)$. $\square$

Proof of Theorem 4.5.1. Suppose there is a primitive solution with $z \neq 0$. By Lemma 4.5.5, there is a point of $\mathcal{C}$ with $\text{urs} \neq 0$; dividing by the common divisor gives a primitive integral point, still with $s \neq 0$. By Lemma 4.5.7, this gives a rational point of $\mathcal{H}$ with $X \neq 0$, contradicting Proposition 4.5.8. Hence $z = 0$, and by Lemma 4.5.2, $n = 1$ and $y = \pm 1$, that is, $(x, y, z) = (-1, \pm 1, 0)$. These two points are indeed primitive solutions. $\square$

5 Rational points on eight 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 cases use elliptic or bitangent descent.

5.1 $x^4 + x^3y + xy^3 = z^4$ ($H = 64$)

Theorem 5.1.1. *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

$$A = 3\alpha^2 + 1, \quad g(t) = t^2 + \alpha t + \alpha^2 + 1, \quad G(x, y) = y^2 + \alpha xy + (\alpha^2 + 1)x^2 = x^2 g(y/x).$$

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 5.1.2. *The following hold (certificate 1.3.1a).*

- (i) $\text{disc}(T^3 + T + 1) = -31$ 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 $\pm \alpha^k$ ($0 \leq k \leq 3$) 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) $(t - \alpha)g(t) = t^3 + t + 1$, $N(y - \alpha x) = y^3 + x^2 y + x^3 = (y - \alpha x)G(x, y)$, 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 5.1.3. *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 $s = \pm 1$, $0 \leq k \leq 3$ and $\beta \in \mathcal{O}_F$ such that*

$$y - \alpha x = \delta \beta^4, \quad \delta = s \alpha^k, \quad \varepsilon = N(\delta) = s(-1)^k.$$

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 $z^4 = x(x^3 + x^2 y + y^3) = x N(y - \alpha x)$, 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 $\delta/\varepsilon = \alpha^k(-1)^k$. $\square$

Step 2: local elimination of $k = 2, 3$. The two lemmas below treat the system

$$x = \varepsilon a^4, \quad y - \alpha x = \delta \beta^4, \quad \gcd(x, y) = 1, \quad \varepsilon = N(\delta) \quad (*)$$

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 5.1.4. *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 α 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. $\square$

Lemma 5.1.5. *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 α 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 $\{1, 3, 9\}$. $\square$

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

$$G_0 : Y^4 = g(t) \quad (k = 0) \quad \text{or} \quad G_1 : Y^4 = -\alpha g(t) \quad (k = 1).$$

Step 3: two elliptic curves.

Lemma 5.1.6. *Smooth models of G_0 and G_1 are isomorphic over F to*

$$E_0 : y^2 = x^3 + (3\alpha^2 + 4)x, \quad E_1 : y^2 = x^3 + k_1x, \\ k_1 = \frac{39936\alpha^2 - 205568\alpha + 169216}{29791} = (3\alpha^2 + \alpha + 1) \left(\frac{40\alpha^2 - 4\alpha + 28}{31} \right)^4,$$

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

$$R_1 = \left(\frac{264\alpha^2 - 324\alpha - 212}{961}, \frac{23104\alpha^2 + 33848\alpha + 49008}{29791} \right).$$

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 $t = -(\alpha^2 + 2m)/(m^2 + \alpha)$, $U = (\alpha - \alpha^2 m - m^2)/(m^2 + \alpha)$. Then $Y^2 = U$ becomes $V^2 = (\alpha - \alpha^2 m - m^2)(m^2 + \alpha)$ ($V = Y(m^2 + \alpha)$), 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 $E_k \rightarrow G_k$ 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 . $\square$

Step 4: Mordell–Weil groups.

Lemma 5.1.7. *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 $2^{\text{rank}} = |\text{Im } \alpha_A| |\text{Im } \alpha'_A|/4$, 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 $\text{Sel}(\alpha)$.

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 ℓ : if there is a place v of degree 1 such that $\ell \mid N = \#E(\mathbb{F}_v)$, N/ℓ is even and $(N/\ell)\bar{P} \neq O$, then ℓ 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). $\square$

Step 5: Mordell–Weil sieve at 47.

Lemma 5.1.8. *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 $\bar{R} = n\bar{P} + e\bar{T}$ ($n \bmod 24, e \in \{0, 1\}$). 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]). $\square$

Step 6: Strassmann argument at 47.

Lemma 5.1.9. *In Lemma 5.1.8, $R = R_0$.*

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 5.1.7, $[K_1 : \langle Q \rangle]$ is prime to 47. Therefore $R - R_0 = sQ$ with $s \in \mathbb{Z}_{(47)}$, and for the three embeddings $\sigma_j : F \rightarrow \mathbb{Q}_{47}$ 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

$$h(s) = f(\sigma_1(R_0) + [s]\sigma_1 Q) - f(\sigma_2(R_0) + [s]\sigma_2 Q) = \sum_{n \geq 0} a_n s^n.$$

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). $\square$

Proof of Theorem 5.1.1. 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 $xN(y - \alpha x) = 0$, 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 5.1.3, 5.1.4, 5.1.5 we get a point of G_0 or G_1 , and by Lemma 5.1.6 there is $R \in E_k(F)$ with $t(R) = y/x$. By Lemmas 5.1.8 and 5.1.9, 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 $(x, 0, \pm x)$. $\square$

5.2 $x^4 - y^4 + x^2yz + yz^3 = 0$ ($H = 64$)

Theorem 5.2.1. *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

$$F_x = 2x(2x^2 + yz), \quad F_y = -4y^3 + x^2z + z^3, \quad F_z = y(x^2 + 3z^2).$$

$F_z = 0$ 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

$$r = y/x, \quad t = z/x, \quad F(r, t) := 1 + rt + rt^3 - r^4 = 0, \quad rt \neq 0.$$

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

$$V(r, t) = (r(t - r) : 1 : r^2 + rt + t^2 : r : t).$$

Indeed, $Q_1(V) = Q_2(V) = -F$ and $Q_3(V) = 2F$. Let M_i be the 5×5 symmetric matrix of Q_i , and M'_i its upper left 3×3 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 $C \rightarrow C/\iota$ is isogenous to the Jacobian of the genus 2 curve

$$H : \eta^2 = h(s), \quad J = \text{Jac}(H).$$

Let D_∞ be the sum of the two points at infinity of H (a rational divisor), and let $\kappa : J \rightarrow \mathcal{K} \subset \mathbb{P}^3$ 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 $C \rightarrow J$ is obtained directly in Lemma 5.2.2 by a computation over the function field.

Step 1: the map $\phi : C \rightarrow J$. At a point P of C ($rt \neq 0$) we take the tangent direction

$$w = \frac{1}{2\Delta} (-N_1, 4r^3 - t^3 - t, -N_3, 2\Delta, 0), \quad \Delta = r^4 - rt^3 + 1,$$

$$N_1 = 2r^4t - 3r^2t^3 + r^2t + rt^4 - rt^2 + 4r - 2t,$$

$$N_3 = 2r^4t + 4r^3t^2 + 3r^2t^3 - r^2t + rt^4 - rt^2 - 4r - t^5 - t^3 - 2t.$$

The following hold (certificate 1.3.2c).

- (i) $V^\top M_i w = 0$ ($i = 1, 2, 3$), and the left 3×3 minor of the tangent matrix $(V^\top M_i)_i$ 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

$$q_i = w^\top M_i w \quad (i = 1, 2, 3), \quad A_P(s) = q_1(P) - 2s q_2(P) + s^2 q_3(P).$$

The q_i are rational functions on C whose denominators are powers of Δ . If we replace the tangent direction by $aw + bV$ ($a \neq 0$), then, since $V^\top M_i V = 0$ and $V^\top M_i w = 0$, A_P is only multiplied by a^2 .

Lemma 5.2.2. *There is a map $\phi : C \rightarrow J$ 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 ∞).
- (b) For the two quartics Φ_1, Φ_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, $A(s) = q_1 - 2sq_2 + s^2q_3 \in K[s]$ 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 Φ_1, Φ_2 and the equation of the Kummer surface.

We choose one ϕ_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 $\phi : C \rightarrow J$. For the same reason, an effective divisor of degree 2 over K representing ϕ_K gives a morphism $\psi : C \rightarrow \text{Sym}^2 H$, and $\phi(P) = [\psi(P) - D_\infty]$. The composition of ψ with the s -projection $\text{Sym}^2 H \rightarrow \text{Sym}^2 \mathbb{P}^1 = \mathbb{P}^2$ 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

$$(r-1)^2(r+1)^2(r^2+1)^2, \quad t - r^7 + r^3 \in (F, \text{num } q_2, \text{num } q_3) \subset \mathbb{Q}[r, t]$$

(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. $\square$

Step 2: $J(\mathbb{Q})$.

Lemma 5.2.3. $J(\mathbb{Q}) = \langle T \rangle \oplus \langle G \rangle \cong \mathbb{Z}/2 \oplus \mathbb{Z}$, where, in Mumford representation,

$$T = (s^2 + s - \frac{1}{2}, 0), \quad G = (s^2 + 2s - 1, 2s - 1).$$

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, $\text{Sha}(J)[2] \neq 0$, and by [Sto01, PS97, PS99], $\text{rank } J(\mathbb{Q}) \leq 3 - 1 - 1 = 1$. 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. $\square$

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 5.2.2(b), $\Phi_i(\kappa(nG + eT)) = 0$. Kummer coordinates are normalized to primitive integer vectors. H has good reduction at 5, 29, 113.

Lemma 5.2.4. $e = 0$ 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.) $\square$

Lemma 5.2.5. $n \not\equiv \pm 14 \pmod{31}$.

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 $n' = 14 + 31d$ ($0 \leq d \leq 28$) only 231 satisfies this condition. Similarly, from 17 only 668 remains. $k = 2$: among $231 + 899d$ ($0 \leq d \leq 28$) 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 $n \bmod 6728$ with $n \bmod 841 \in \{291, 550\}$, none of the points $\kappa(n\bar{G})$ lies in $\Gamma(\mathbb{F}_{113})$ (certificate 1.3.2a). This is a contradiction. $\square$

Step 4: 29-adic isolation of the three remaining disks.

Lemma 5.2.6. $n \in \{0, 2, -2\}$.

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

$$(\kappa_1, \kappa_2, \kappa_3)([m]Q) = 29^{2+2e}(u^2 B(\zeta) + O(29)).$$

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 :

$$L_1 = -336k_1k_2 + 540k_1k_3 - 135k_2^2 + 672k_3^2, \quad L_2 = -192k_1k_2 + 388k_1k_3 - 97k_2^2 + 384k_3^2.$$

Hence $\Phi_1(\kappa([m]Q)) = 29^{4+4e}(u^4 c^2 L_1(9, 10, 6) + O(29))$. 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 $\kappa(2G + Y) = \kappa(2G) + \Lambda z(Y) + O(|z(Y)|^2)$ (Λ 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 $\kappa(2G + [m]Q) = \kappa(2G) + 29^{1+e}(u d + O(29))$. Since $\Phi_i(\kappa(2G)) = 0$,

$$\Phi_i(\kappa(2G + [m]Q)) = 29^{1+e}(u D_d \Phi_i(b) + O(29)),$$

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). $\square$

Step 5: fibers over the three classes.

Lemma 5.2.7. 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 5.2.2(a) is that divisor. Then A_P is a constant multiple of $s^2 + 4s - \frac{13}{8}$, and at P

$$2q_2 + 4q_3 = 0, \quad 8q_1 + 13q_3 = 0.$$

The lexicographic Gröbner basis of the ideal of $\mathbb{Q}[r, t]$ generated by these two equations (with denominators cleared) and F is

$$r^4 - rt - 1, \quad (r^2 - 1)t^2, \quad t^3$$

(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_∞ is the unique g_2^1 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

$$\frac{1}{64} r^4 (r - 1)^4 (r + 1)^4 (r^2 + 1)^4 A_8(r) B_8(r) C_{24}(r),$$

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. $\square$

Proof of Theorem 5.2.1. Suppose there is $P \in C(\mathbb{Q})$ with $xyz \neq 0$. Then $rt \neq 0$. By Lemma 5.2.3 we can write $\phi(P) = nG + eT$. By Lemmas 5.2.4, 5.2.5, 5.2.6, $\phi(P) \in \{0, \pm 2G\}$, which contradicts Lemma 5.2.7. 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. $\square$

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.

5.3 $x^4 + x^2 y^2 + y^3 z - y z^3 = 0$ ($H = 64$)

Theorem 5.3.1. The only integer solutions of $x^4 + x^2 y^2 + y^3 z - y z^3 = 0$ 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 $J_C = \text{Jac}(C)$. 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 $(2X + y^2)^2 = y^4 - 4y^3 z + 4y z^3$, so the quotient curve $E = C/\langle \iota \rangle$ is $W^2 = y^4 - 4y^3 z + 4y z^3$. 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 ι . 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 δ_P is a rational point of the Prym variety $\text{Prym}(C/E) = (1 - \iota_*)J_C$.

In the form of Ritzenthaler–Romagny,

$$C : x^4 - h_0x^2 + f_0g_0 = 0, \quad f_0 = yz, \quad h_0 = -y^2, \quad g_0 = y^2 - z^2.$$

The matrix of coefficients of (f_0, h_0, g_0) with respect to (y^2, yz, z^2) and its inverse are

$$A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 1 & 0 & -1 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix}.$$

Let (a_i, b_i, c_i) be the rows of A^{-1} , and put $a(s) = a_1 + 2a_2s + a_3s^2$, and $b(s), c(s)$ in the same way. Then $a = 2s, b = -(s^2 + 1), c = -s^2$. By [Bru08, RR18], $\text{Prym}(C/E)$ 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 $3 \leq p \leq 79$ (certificate 1.3.3b).

Step 1: the rank of the Prym.

Lemma 5.3.2. *rank $J_H(\mathbb{Q}) = 0$. Hence $\text{Prym}(C/E)(\mathbb{Q})$ is finite, and for every $P \in C(\mathbb{Q})$, δ_P is a torsion point of $J_C(\mathbb{Q})$.*

Proof. The 2-descent of [Sto01, PS97, PS99] gives the upper bound 0 for 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 $\text{Prym}(C/E)(\mathbb{Q})$ is a finite group, and its element δ_P is torsion. $\square$

Step 2: the order of δ_P .

Lemma 5.3.3. *For every $P \in C(\mathbb{Q})$, $2\delta_P = 0$.*

Proof. C has good reduction at 3 and 5, and

$$J_C(\mathbb{F}_3) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/14, \quad J_C(\mathbb{F}_5) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/176$$

(certificate 1.3.3a). The orders are $L_3(1) = 28$ and $L_5(1) = 352$, respectively, where

$$L_3(T) = 1 + 27T^6, \quad L_5(T) = 1 + 4T + 15T^2 + 32T^3 + 75T^4 + 100T^5 + 125T^6.$$

Let ℓ be a prime dividing the order of δ_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 δ_P is a power of 2, and by [Kat81, Appendix] the group generated by δ_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 $2\delta_P = 0$. $\square$

Step 3: fixed points.

Proof of Theorem 5.3.1. Let $P \in C(\mathbb{Q})$ with $P \neq \iota(P)$. By Lemma 5.3.3, $2[P - \iota(P)] = 0$. 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 ι 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. $\square$

$$5.4 \quad x^4 + y^4 + x^2yz - yz^3 = 0 \quad (H = 64)$$

Theorem 5.4.1. *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

$$C : X^4 + Y^4 + X^2YZ - YZ^3 = 0.$$

C is smooth (certificate 1.3.4a). Hence it has genus 3 and, by [Har77, Section IV.5], it is not hyperelliptic. Theorem 5.4.1 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 5.4.2. $C(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 1)\}$.

The involution $\iota(X : Y : Z) = (-X : Y : Z)$ preserves C . The fixed points of ι 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 $P_C = \text{im}(1 - \iota_*) \subset J_C$ be the Prym variety of the cover $C \rightarrow E$. 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

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix}.$$

Forming $\alpha_1 + 2\alpha_2s + \alpha_3s^2$ from each column $(\alpha_1, \alpha_2, \alpha_3)^T$ 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

$$H : y^2 = f_H(s), \quad \begin{aligned} f_H &= b(b^2 - ac) = 10s^6 - 26s^5 + 9s^4 + 18s^3 - 5s^2 - 6s - 1 \\ &= (2s^2 - 2s - 1)(5s^4 - 8s^3 - s^2 + 4s + 1). \end{aligned}$$

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 $\text{rank } J_H(\mathbb{Q}) = 0$ (Lemma 5.4.3), show that the torsion of $J_C(\mathbb{Q})$ has order at most 2 (Lemma 5.4.4), and use these two facts to show that every rational point is a fixed point of ι (Lemma 5.4.5).

Step 1: the rank of J_H .

Lemma 5.4.3. $\text{rank } J_H(\mathbb{Q}) = 0$. Hence $P_C(\mathbb{Q})$ is a finite group.

Proof. Let D_∞ 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, $\dim_{\mathbb{F}_2} \text{Sel}^2(\mathbb{Q}, J_H) = 2$ (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 ∞ 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 $\text{Sha}(J_H)[2] \neq 0$ and

$$\dim \text{Sel}^2 \geq \text{rank } J_H(\mathbb{Q}) + \dim J_H(\mathbb{Q})[2] + 1 \geq \text{rank } J_H(\mathbb{Q}) + 2.$$

Therefore $\text{rank } J_H(\mathbb{Q}) = 0$. Magma’s RankBounds gives the same upper bound 0 (certificate 1.3.4a). The rank does not change under isogeny, so $\text{rank } P_C(\mathbb{Q}) = 0$, and $P_C(\mathbb{Q})$ is a finite group. $\square$

Step 2: torsion of $J_C(\mathbb{Q})$.

Lemma 5.4.4. $J_C(\mathbb{Q})_{\text{tors}}$ 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

$$J_C(\mathbb{F}_5) \simeq \mathbb{Z}/110, \quad J_C(\mathbb{F}_7) \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/140, \quad J_C(\mathbb{F}_{11}) \simeq \mathbb{Z}/17 \oplus \mathbb{Z}/68$$

(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 ℓ divides $\#J_C(\mathbb{Q})_{\text{tors}}$. 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 $J_C(\mathbb{Q})_{\text{tors}}$ is a 2-group, and by [Kat81, Appendix] it injects into the 2-part $\mathbb{Z}/2$ of $J_C(\mathbb{F}_5)$. $\square$

Step 3: rational points are fixed points of ι .

Lemma 5.4.5. 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 ι . For $P \in C(\mathbb{Q})$,

$$\delta_P = [P - \iota(P)] = (1 - \iota_*)[P - Q_0] \in P_C(\mathbb{Q}).$$

By Lemma 5.4.3, δ_P is a torsion element, and by Lemma 5.4.4, $2\delta_P = 0$, that is, $2P \sim 2\iota(P)$. If $P \neq \iota(P)$, this contradicts [Har77, Section IV.5]. Hence $P = \iota(P)$. $\square$

Proof of Proposition 5.4.2. By Lemma 5.4.5, rational points are fixed points of ι , 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 . $\square$

5.5 $x^4 - x^2y^2 + y^3z + yz^3 = 0$ ($H = 64$)

Theorem 5.5.1. 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

$$C : F(X, Y, Z) = X^4 - X^2Y^2 + Y^3Z + YZ^3 = 0$$

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 5.5.1 is equivalent to the following proposition.

Proposition 5.5.2. $C(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0), (1 : 1 : 0), (-1 : 1 : 0)\}$.

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 $P_C = \text{im}(1 - \iota_*) \subset J_C$ be the Prym variety of the cover $C \rightarrow E$. 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)

$$q_1 = b^2 + ac, \quad q_2 = ab, \quad q_3 = -b^2 - ac + bc$$

and the curve $D : q_1 = u^2, q_2 = uv, q_3 = v^2$ in $\mathbf{P}^4$. The map

$$\pi : C \rightarrow D, \quad (X : Y : Z) \mapsto (a : b : c : u : v) = (YZ : X^2 : Y^2 + Z^2 : XY : XZ)$$

satisfies $q_1 - u^2 = F$, $q_2 - uv = 0$, $q_3 - v^2 = -F$, so it indeed maps to D . On $X \neq 0$, π 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 3×3 symmetric matrix of q_i , and let M_i be the 5×5 symmetric matrices of the three equations $q_1 - u^2, q_2 - uv, q_3 - v^2$ of D . The genus 2 curve is

$$\begin{aligned} H : \quad y^2 &= -4 \det(N_1 - 2sN_2 + s^2N_3) \\ &= -s^6 - 2s^5 + 3s^4 + 2s^3 - 3s^2 + 1 \\ &= -(s^2 - 1)(s^4 + 2s^3 - 2s^2 + 1). \end{aligned}$$

(certificate 1.3.5b), and the prime factors of its discriminant are 2, 7, 13. D_∞ 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 $\mathbf{v}^\top M_i$ 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

$$\tau_{\mathbf{v}}(s) = \mathbf{w}^\top (M_1 - 2sM_2 + s^2M_3) \mathbf{w}$$

the *tangent quadratic* at $\mathbf{v}$. Since $\mathbf{v}^\top M_i \mathbf{v} = \mathbf{v}^\top M_i \mathbf{w} = 0$, replacing $\mathbf{w}$ by $\alpha \mathbf{w} + \beta \mathbf{v}$ only multiplies $\tau_{\mathbf{v}}$ by α^2 . In the chart $Y = 1$, at the image $\mathbf{v}_{\text{gen}} = (t : R : 1 + t^2 : r : rt)$ of the generic point of C , the tangent quadratic is proportional to $A_2 s^2 + Bs + A_0$, formed from

$$\begin{aligned} A_2 &= -R^4 + 4R^3t - 2R^3 - R^2 + 12Rt^2 - 4Rt - 4R - 4t^2, \\ B &= 2(3R^2t^2 + 7R^2 + 3Rt^2 - 5R + 4t), \\ A_0 &= -4R^3t + 13R^2t - 12Rt^2 - Rt + 4R + 3t^2 - 1 \end{aligned}$$

(certificate 1.3.5b).

Kummer surface. Let $\kappa : J_H \rightarrow K_H \subset \mathbf{P}^3$ 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, $\kappa([P_1 + P_2 - D_\infty]) = (1 : x_1 + x_2 : x_1x_2 : *)$. $\Phi_1, \Phi_2 \in \mathbb{Z}[k_1, \dots, k_4]$ are the two quartic forms given in certificate 1.3.5b (28 terms each). In the chart $k_4 = 1$, Φ_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 $\varphi : C \rightarrow J_H$ over $\mathbb{Q}$ from the tangent quadratic (Lemma 5.5.3), determine $J_H(\mathbb{Q})$ (Lemma 5.5.4), and show $\varphi(C(\mathbb{Q})) \subset \{0, \pm 4G\}$ by a sieve modulo 3 and 3-adic analysis (Lemma 5.5.10). Finally, we determine the two fibers (Lemmas 5.5.11, 5.5.12).

Step 1: the map φ .

Lemma 5.5.3. *There is a map $\varphi : C \rightarrow J_H$ 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 $\mathbf{v}_{\text{gen}} = (t : R : 1 + t^2 : r : rt)$ lies on D , and $\dim W_{\mathbf{v}_{\text{gen}}} = 2$. The tangent quadratic has degree 2, is irreducible over $\mathbb{Q}(C)$, and is proportional to $A_2s^2 + Bs + A_0$. There are exactly two points $\pm\varphi_{\text{gen}}$ 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 $k_2A_2 + k_1B = 0$, $k_3A_2 - k_1A_0 = 0$.

$\varphi_{\text{gen}} \in J_H(\mathbb{Q}(C))$ 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 $\varphi : C \rightarrow J_H$. Likewise, the effective divisor of degree 2 determined by the Mumford representation of φ_{gen} is a $\mathbb{Q}(C)$ -point of $\text{Sym}^2 H$, and it extends to a morphism $\psi : C \rightarrow \text{Sym}^2 H$. The two maps φ 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 ψ with $\text{Sym}^2 H \rightarrow \text{Sym}^2 \mathbf{P}^1 \simeq \mathbf{P}^2$ (the coefficients of the quadratic form of the x -image) is a morphism $C \rightarrow \mathbf{P}^2$, 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 $\text{Pic}^0 D$), and $\lambda : P' \rightarrow J_H$ 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 $\pm\varphi_{\text{gen}}$. Hence $\varphi = \pm\lambda \circ d \circ \pi$ on $\pi^{-1}(U) \supset \{X \neq 0\}$. Moreover, the pullback $\nu : P' \rightarrow P_C \subset J_C$ under the normalization $C \rightarrow D$ 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 $2[P - \iota(P)] = 0$. $\square$

Step 2: $J_H(\mathbb{Q})$.

Lemma 5.5.4. $J_H(\mathbb{Q}) = \langle T \rangle \oplus \langle G \rangle \simeq \mathbb{Z}/2 \oplus \mathbb{Z}$, where, in Mumford representation,

$$T = (s^2 - 1, 0) = [(1, 0) + (-1, 0) - D_\infty], \quad G = (s^2 + s, -s - 1) = [(0, -1) + (-1, 0) - D_\infty],$$

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 $\kappa(4G)$. $\square$

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 5.5.5. 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 5.5.3(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 $\kappa(-x) = \kappa(x)$. $\square$

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 $\partial^\alpha \text{Ex}(0) \in \mathbb{Z}_3^2$ for every multi-index α . 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 $z = (z_1, \dots, z_g)$, J_1 , $\hat{F}$, L , Ex .

Lemma 5.5.6 (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 ($[p^k]S \rightarrow 0$), so they agree on all of $\mathbb{Z}_p$. $\square$

Lemma 5.5.7 (Logarithmic coordinates). *Suppose $\kappa \in \mathbb{Z}_p[[z]]$ satisfies $\kappa(0) = 0$ and $\kappa \circ [-1] = \kappa$. Then $\kappa(\text{Ex}(\ell)) = \sum_{n \geq 2, n \text{ even}} \kappa_n(\ell)$, where κ_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*

$$\kappa([m]Q) = m^2 \kappa_2(\ell_Q) + \varepsilon, \quad v_p(\varepsilon) \geq 4(e+1) - \frac{3}{p-1}.$$

Proof. Since $L \circ [-1] = -L$, we have $\text{Ex}(-\ell) = [-1]\text{Ex}(\ell)$, so $\kappa \circ \text{Ex}$ is an even function. Since $\kappa(0) = 0$, it has no constant term. By the chain rule and $\partial^\alpha \text{Ex}(0) \in \mathbb{Z}_p^g$, we have $\partial^\alpha (\kappa \circ \text{Ex})(0) \in \mathbb{Z}_p$. Therefore the coefficient of ℓ^α 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 $z([m]Q) = \text{Ex}(m\ell_Q)$. 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 $4(e+1) - 3/(p-1)$. $\square$

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 5.5.8. *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 Φ_1 has integer coefficients, Lemma 5.5.6 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 5.5.7 with $p = 3$ to the κ_i , and write $\kappa_{i,2}$ for the quadratic part of $\kappa_i \circ \text{Ex}$. 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 Φ_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 $f(m) \neq 0$. $\square$

Lemma 5.5.9. *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 5.5.6 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

$$a_0 = 0, \quad 3^{-2}a_1 \equiv 2, \quad 3^{-2}a_2 \equiv 2, \quad 3^{-3}a_3 \equiv 1 \pmod{3},$$

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 $h(m) \neq 0$. $\square$

Lemma 5.5.10. *For every $P \in C(\mathbb{Q})$, $\varphi(P) \in \{0, 4G, -4G\}$.*

Proof. Applying Lemma 5.5.3(i) and Lemmas 5.5.8, 5.5.9 to the two cases of Lemma 5.5.5 gives $m = 0$. Hence $\kappa(\varphi(P))$ is $\kappa(0)$ or $\kappa(4G)$, and $\varphi(P) = 0$ or $\pm 4G$. $\square$

Step 5: the two fibers.

Lemma 5.5.11. *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 5.5.3(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 $x_1 + x_2 = \frac{1}{2}$, $x_1x_2 = -\frac{3}{8}$. 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,

$$2B + A_2 = 0, \quad 8A_0 + 3A_2 = 0$$

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 $P = (\pm 1 : 1 : 0)$. $\square$

Lemma 5.5.12. *If $P \in C(\mathbb{Q})$ and $\varphi(P) = 0$, then $X(P) = 0$.*

Proof. Suppose $X(P) \neq 0$. By Lemma 5.5.3(iii), $2P \sim 2\iota(P)$. On the other hand, $P \neq \iota(P)$, because the only fixed points of ι are the line $X = 0$ and $(1 : 0 : 0) \notin C$. This contradicts [Har77, Section IV.5]. $\square$

Proof of Proposition 5.5.2. Let $P \in C(\mathbb{Q})$. If $X(P) \neq 0$, then $Y(P) \neq 0$, and by Lemma 5.5.12, $\varphi(P) \neq 0$. By Lemma 5.5.10, $\varphi(P) = \pm 4G$, and by Lemma 5.5.11, $P = (\pm 1 : 1 : 0)$. 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 . $\square$

$$5.6 \quad x^4 + x^2y^2 + y^3z + z^4 = 0 \quad (H = 64)$$

Theorem 5.6.1. *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

$$C : F(X, Y, Z) = X^4 + X^2Y^2 + Y^3Z + Z^4 = 0$$

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 5.6.1 is equivalent to the following proposition.

Proposition 5.6.2. $C(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 1 : -1)\}$.

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 $P_C = \text{im}(1 - \iota_*) \subset J_C$ be the Prym variety of the cover $C \rightarrow E$. 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)

$$q_1 = -(b^2 + ac), \quad q_2 = \frac{1}{2}(ab - b^2 - ac - bc), \quad q_3 = \frac{1}{2}(ab + b^2 + ac + bc)$$

and the curve $D : q_1 = u^2, q_2 = uv, q_3 = v^2 (\subset \mathbf{P}^4)$. The map

$$\pi : C \rightarrow D, \quad (X : Y : Z) \mapsto (a : b : c : u : v) = (Z(Y + Z) : X^2 : Y^2 - YZ + Z^2 : XY : XZ)$$

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 $X \neq 0$, π 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 3×3 symmetric matrix of q_i , the genus 2 curve is

$$\begin{aligned} H : y^2 &= -16 \det(N_1 - 2sN_2 + s^2N_3) \\ &= 2s^5 + 6s^4 - 4s^3 - 10s^2 + 12s - 4 \\ &= 2(s^2 + 2s - 2)(s^3 + s^2 - 2s + 1). \end{aligned}$$

(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 ∞ , 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 5.5, using the 5×5 symmetric matrices M_i of the three equations of D .

Kummer surface. $\kappa : J_H \rightarrow K_H \subset \mathbf{P}^3$ 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

$$Q_1 = 48k_1^2 - 4k_1k_3 + k_2^2 + 24k_2k_3, \quad Q_2 = -48k_1^2 + 240k_1k_3 - 60k_2^2 - 24k_2k_3$$

(certificate 1.3.6a).

The proof goes as in Section 5.5. We construct a map $\varphi : C \rightarrow J_H$, 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 φ .

Lemma 5.6.3. *There is a map $\varphi : C \rightarrow J_H$ 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 $\pm \varphi_{\text{gen}}$ 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 5.5.3. φ_{gen} extends to a morphism $\varphi : C \rightarrow J_H$, 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 $\lambda : P' \rightarrow J_H$ is an isomorphism. Therefore $\varphi = \pm \lambda \circ d \circ \pi$ on $\{X \neq 0\}$. The isogeny $\nu : P' \rightarrow P_C$ given by the normalization sends $d(\pi(P))$ to $2[\iota(P) - P]$. $\square$

Step 2: $J_H(\mathbb{Q})$.

Lemma 5.6.4. $J_H(\mathbb{Q}) = \langle T \rangle \oplus \langle G \rangle \simeq \mathbb{Z}/2 \oplus \mathbb{Z}$, where, in Mumford representation,

$$T = (s^2 + 2s - 2, 0) = [(\alpha, 0) + (\bar{\alpha}, 0) - 2\infty], \quad G = (s + \frac{5}{2}, -\frac{9}{4}) = [(-\frac{5}{2}, -\frac{9}{4}) - \infty],$$

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. $\square$

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 5.6.5. *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 5.6.3(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 $e\bar{T} + n\bar{G}$ ($e \in \{0, 1\}$, $0 \leq n < 28$) 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 $28 \mid n$. $\square$

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

$$\kappa_i(R)/47^2 \equiv (24, 7, 1)_i \pmod{47}, \quad Q_1(24, 7, 1) \equiv 39, \quad Q_2(24, 7, 1) \equiv 8 \pmod{47}.$$

Lemma 5.6.6. *If $m \in \mathbb{Z}$ and $m \neq 0$, then $\Phi_1(\kappa([m]R)) \neq 0$. More precisely, $v_{47}(\Phi_1(\kappa_1, \kappa_2, \kappa_3, 1)([m]R)) = 4v_{47}(m) + 4$.*

Proof. We apply Lemma 5.5.7 with $p = 47$ to the κ_i , and let $\kappa_{i,2}$ be the quadratic part of $\kappa_i \circ \text{Ex}$. 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 ,

$$\kappa_i([m]R) = m^2 \kappa_{i,2}(\ell_R) + O(47^{4e+4}) = 47^{2e+2}(u^2 d_i + O(47)).$$

Since Φ_1 has integer coefficients,

$$\Phi_1(\kappa_1, \kappa_2, \kappa_3, 1)([m]R) = 47^{4e+4}(u^4 Q_1(d) + O(47)) + O(47^{6e+6}).$$

Since $Q_1(d) \equiv 39 \not\equiv 0 \pmod{47}$ and $6e + 6 > 4e + 4$, the valuation is exactly $4e + 4$. $\square$

Step 5: the zero fiber.

Lemma 5.6.7. *For every $P \in C(\mathbb{Q})$, $X(P) = 0$.*

Proof. By Lemma 5.6.5, $\varphi(P) = [m]R$, and by Lemma 5.6.3(i) and Lemma 5.6.6, $m = 0$, that is, $\varphi(P) = 0$. Suppose $X(P) \neq 0$. By Lemma 5.6.3(ii), $2P \sim 2\iota(P)$. The only fixed points of ι are the line $X = 0$ and $(1 : 0 : 0) \notin C$, so $P \neq \iota(P)$, and this contradicts [Har77, Section IV.5]. $\square$

Proof of Proposition 5.6.2. By Lemma 5.6.7, $X = 0$. 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 . $\square$

5.7 $x^3z + y^3x + y^2z^2 - z^3y = 0$ ($H = 64$)

Theorem 5.7.1. *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 $J = \text{Jac}(C)$. 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 $\text{Sp}_6(\mathbb{F}_2)$ (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 $\text{rank } J(\mathbb{Q}) = 1$ (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 5.7.2. *C is smooth over $\mathbb{Q}$, so it has genus 3. The plane model $\mathcal{C} = \{F = 0\} \subset \mathbb{P}_{\mathbb{Z}}^2$ 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 $\mathbb{F}_p$; 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. $\square$

Lemma 5.7.3. (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) $\text{div}(z) = 3P_1 + P_2$, $\text{div}(y) = P_1 + 3P_3$, $\text{div}(x) = 2P_2 + P_3 + P_4$. 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) $\text{div}(z/y) = 2P_1 + P_2 - 3P_3$ and $\text{div}(x/y) = 2P_2 + P_4 - P_1 - 2P_3$. (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. $\square$

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 5.7.4. 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)

$$\begin{aligned}
2 : & (4, 1), (2, 3), (2, 3), (4, 3); & 11 : & (1, 1), (1, 3), (1, 6), (1, 6), (2, 6); \\
41269 : & (2, 2), (2, 4), (1, 8), (1, 8).
\end{aligned}$$

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. $\square$

Lemma 5.7.5. *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 Γ 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 Γ 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. $\square$

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 5.7.6. *Let $V = \mathbb{F}_2^6$ with the standard symplectic form, Θ 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, ι is injective, $V^\Gamma = 0$ and $(M/\iota V)^\Gamma = 0$ (certificate 1.3.7c). Hence $J(Q)[2] = 0$ and $\delta = \delta_Q$ is injective.*

Proof. The 63 transvections generate a permutation group of order $1451520 = \#\mathrm{Sp}_6(\mathbb{F}_2)$ on Θ , 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 γ has dimension $7 = \dim(\mathbb{F}_2\mathbf{1} + \iota V)$. The conclusion follows from Proposition I(1), (2) and Lemma 5.7.5. $\square$

Since $J(Q)[2] = 0$, injectivity gives $\mathrm{rank} J(Q) \leq \dim_{\mathbb{F}_2} \Sigma$ for every subgroup Σ containing $\delta(J(Q)/2J(Q))$.

Lemma 5.7.7. *Every class in $\delta(J(Q)/2J(Q))$ has a representative in*

$$K(2, S) = \{\kappa \in K^\times/K^{\times 2} : v_p(\kappa) \equiv 0 \pmod{2} \text{ for all prime ideals } p \notin S\},$$

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, $(v_p(\kappa) \bmod 2)_{p|11} \in \{0, (1, 1, 1, 1, 0)\}$ and $(v_p(\kappa) \bmod 2)_{p|41269} \in \{0, (0, 0, 1, 1)\}$.

Proof. At $p \notin \{2, 11, 41269\}$, $K/\mathbb{Q}$ is unramified and $c_p = 1$, so by Proposition I(3) all $v_p(\kappa)$, $p \mid p$, have the same parity; multiplying κ by suitable powers of these finitely many p gives a representative in $K(2, S)$. At $p = 11, 41269$, $c_p = 1$ (Lemma 5.7.2), and Proposition I(3) gives the two conditions, with $(e_p \bmod 2)$ read off from Lemma 5.7.4(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 $\mathbb{Q}(2, S) \rightarrow K^\times/K^{\times 2}$ is injective because K has no quadratic subfield. $\square$

Step 4: the class group of K .

Lemma 5.7.8. *Every prime ideal of $\mathcal{O}_K$ of norm $< e^{13}$ (that is, of norm ≤ 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. $\square$

Lemma 5.7.9. *The class number of K is odd; in particular $\text{Cl}(K)[2] = 0$.*

Proof. Apply Proposition B with $n = 28$, $r_1 = 4$, $D = 2^{42}11^641269^6$, $T = 13$, v the indicator function of $[0, T]$ (so $f(x) = (1 - |x|/T)_+$), and $k(q) = a(q)$ for all $q < e^{13}$ (Lemma 5.7.8). Since $1 - f(x) \leq x/T$ for $x \geq 0$, $\int_0^\infty (1 - f)W \leq \frac{1}{T} \int_0^\infty xW(x) dx = \frac{\pi^2}{4T} + \frac{2\alpha \log 2}{T}$. Hence $B^-(f) \geq B_0(13)$, where

$$B_0(T) = C_\infty - \frac{\pi^2}{4T} - \frac{2r_1 \log 2}{nT} + \frac{4}{n} \sum_{\mathfrak{p}, m \geq 1: N\mathfrak{p}^m < e^T} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^m + 1} \left(1 - \frac{m \log N\mathfrak{p}}{T}\right).$$

The sum involves 25,333 distinct pairs $(N\mathfrak{p}, m)$, that is, 37,333 pairs $(\mathfrak{p}, m)$. In ball arithmetic (256 bits),

$$C_\infty - \frac{\pi^2}{52} - \frac{2 \cdot 4 \log 2}{28 \cdot 13} = -0.78489255426850599306 \dots,$$

$$B_0(13) = 0.0303690492767119765536576158681 \pm 1.4 \cdot 10^{-32} > 0$$

(certificate 1.3.7d; the GP script of certificate 1.3.7d gives the same value in floating point). $\square$

Step 5: S -units.

Lemma 5.7.10. *Let $u_1, \dots, u_{15}$ and $\pi_1, \dots, \pi_{13}$ be the elements recorded in `data/paper_C2.json` of certificate 1.3.7e. Then $-1, u_1, \dots, u_{15}, \pi_1, \dots, \pi_{13}$ is an $\mathbb{F}_2$ -basis of $K(2, S)$, which has dimension 29.*

Proof. Each u_i is integral with norm ± 1 , so it is a unit. Each π_j is integral, and the ideals $(\pi_1), \dots, (\pi_{13})$ are the 13 prime ideals of S , in the order of Lemma 5.7.4(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 ± 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 29×29 matrix over $\mathbb{F}_2$. So they form a basis of $\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2}$. Finally $0 \rightarrow \mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2} \rightarrow K(2, S) \rightarrow \text{Cl}(\mathcal{O}_{K,S})[2] \rightarrow 0$ is exact, and $\text{Cl}(\mathcal{O}_{K,S})$ is a quotient of $\text{Cl}(K)$, which has odd order (Lemma 5.7.9). $\square$

Step 6: local images and the rank.

Lemma 5.7.11. $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) \leq 4$.

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 Δ of $\text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2)$ on Θ correspond to the prime ideals above 2, so they have sizes 4, 6, 6, 12. By Proposition I(1) and Lemma 5.7.6, a nonzero $T \in J[2]$ is fixed by Δ if and only if the 12-element set $\{\theta : q_\theta(T) = 0\}$ is Δ -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 $\dim J(\mathbb{Q}_2)[2] \leq 1$. $\square$

To compute in $(K \otimes \mathbb{Q}_2)^\times / (K \otimes \mathbb{Q}_2)^{\times 2} = \prod_{p|2} K_p^\times / K_p^{\times 2}$ we use, for each $p \mid 2$ with ramification index e , a uniformizer π_p and record $v_p(x)$ modulo 2, together with the discrete-logarithm coordinates modulo 2 of the unit $x\pi_p^{-v_p(x)}$ in $(\mathcal{O}_K/p^{2e+1})^\times$. This is an isomorphism $K_p^\times / K_p^{\times 2} \rightarrow \mathbb{F}_2^{2+ef}$, because a unit that is a square modulo p^{2e+1} is a square (Hensel's lemma). Together they give an isomorphism $\text{loc}_2 : (K \otimes \mathbb{Q}_2)^\times / (\text{squares}) \rightarrow \mathbb{F}_2^{36}$, under which the images of $-1, 2, 5$ are independent.

Lemma 5.7.12. *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 $\text{loc}_2(\ell(Q_i)a)$ ($i = 1, \dots, 4$) and of $\text{loc}_2(-1), \text{loc}_2(2), \text{loc}_2(5)$. 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 $Ne_p \geq v_p((Y - ax_0 - n)a) + 2e_p + 1$ for every $p \mid 2$, 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 $\text{loc}_2(\mathbb{Q}_2^\times)$. 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 5.7.11. All 82 points of $C(\mathbb{Q}_2)$ with $x_0 \in [-40, 40]$, and the four displayed points, give the same space. $\square$

Let $\Sigma \subseteq K(2, S)/\mathbb{Q}(2, S)$ consist of the classes κ satisfying only

$$(v_p(\kappa) \bmod 2)_{p|11} \in \{0, (1, 1, 1, 1, 0)\}, \quad \text{loc}_2(\kappa) \in W_2^+.$$

These conditions are independent of the representative modulo $\mathbb{Q}(2, S)$. By Lemmas 5.7.7 and 5.7.12, this space contains $\delta(J(\mathbb{Q})/2J(\mathbb{Q}))$.

Lemma 5.7.13. *$\dim_{\mathbb{F}_2} \Sigma = 1$, and Σ is spanned by $\delta(G) = [a]$. Hence $\text{rank } J(\mathbb{Q}) = 1$ and $J(\mathbb{Q}) \cong \mathbb{Z}$.*

Proof. In the 29-element basis of Lemma 5.7.10, 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. $\square$

Step 7: Chabauty–Coleman at $p = 3$. By Lemma 5.7.2, 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 η 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 ± 1 , so the remaining affine coordinate is a power series in t with integer coefficients ($z = -t^3 + \dots$ at P_1 , $x = -t^2 + \dots$ at P_2 , $y = t^3 + \dots$ at P_3 , $y = 1 - t + \dots$ at P_4), and $\Omega = w_\Omega(t) dt$ with w_Ω 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 5.7.14. 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

$$80621568x^3 + 19551871x^2 - 576258756x + 551007360, \quad V(x) = \frac{27648}{10517}x^2 + \frac{154341055}{30667572}x - \frac{31989800}{2555631}.$$

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 Γ be a generator. The resultant $\text{Res}_y(F(x, y, 1), \Gamma(x, y, 1))$ 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 $\deg \text{div } \Gamma = 48 = 44 + 1 + 3$, $\text{div } \Gamma = 44P_1 + P_3 + E$, and $\text{div}(\Gamma/(y^{11}z)) = E + 30P_1 - 32P_3 - P_2$, 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 . $\square$

Lemma 5.7.15. With $L_\bullet = \int_{31G} \omega_\bullet$, which is a sum of three tiny integrals by Lemma 5.7.14,

$$L_x \equiv 642322739790, \quad L_y \equiv 657631671201, \quad L_z \equiv 233976154908 \pmod{3^{25}},$$

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 5.7.16. (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 $c_1, \dots, c_8$ (∞ means that the coefficient is 0) are:

disk	differential	$v_3(c_1), \dots, v_3(c_8)$	bound
P_1	η_1	$2, \infty, \infty, 6, \infty, 6, \infty, 10$	1
P_2	η_2	$2, 6, \infty, \infty, \infty, 7, 9, 10$	1
P_3	η_1	$3, 3, \infty, 6, 6, \infty, 10, 10$	2
P_3	η_2	$5, \infty, \infty, 5, \infty, \infty, 9, 13$	4
P_4	η_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 $I_1 = I_2 = 0$. $\square$

Proof of Theorem 5.7.1. Every point of $C(\mathbb{Q})$ lies in one of the four residue disks of $C(\mathbb{F}_3)$, and by Lemma 5.7.16 (which uses Lemma 5.7.13) 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 5.7.13. $\square$

5.8 $x^4 - y^3z + xyz^2 + xz^3 = 0$ ($H = 64$)

Theorem 5.8.1. 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 $J = \text{Jac}(C)$. Write

$$\infty = (0 : 1 : 0), \quad P_0 = (0 : 0 : 1), \quad P_1 = (-1 : 0 : 1).$$

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 ∞ , with multiplicity 4, so ∞ 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, $J(\mathbb{Q})_{\text{tors}} = \langle T \rangle \cong \mathbb{Z}/3$, 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 $\text{rank } J(\mathbb{Q}) = 1$ (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 5.8.2. *The points of C with $x = 0$ are ∞ 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 ∞ . So ∞, P_0, P_1 are the only rational points of C with a zero coordinate.*

Proof. $F(0, y, z) = -y^3z$, $F(x, 0, z) = x(x + z)(x^2 - xz + z^2)$, $F(x, y, 0) = x^4$. □

Lemma 5.8.3. (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 $\{F = 0\} \subset \mathbb{P}_{\mathbb{Z}_p}^2$ 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 ∞ , and $F_z(0, 1, 0) = -1$, so ∞ 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 5.8.4. *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 $C(\mathbb{F}_3) = \{\infty, \bar{P}_0, \bar{P}_1\}$.

Lemma 5.8.5. $J(\mathbb{Q})_{\text{tors}} = \langle T \rangle \cong \mathbb{Z}/3$, and G_1 has infinite order.

Proof. By [Kat81, Appendix], the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ 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 $\#J(\mathbb{Q})_{\text{tors}}$ divides 3. The line $x = 0$ meets C in $3P_0 + \infty$ and $z = 0$ in 4∞ , so $\text{div}(x/z) = 3P_0 - 3\infty$ and $3T = 0$; $T \neq 0$ since the genus is positive. The function x/z has a pole of order exactly 3 at ∞ , 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 . $\square$

Lemma 5.8.6. $C(\mathbb{R})$ 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 $x^2(4x - 27(x^3 + 1)^2)$. 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]. $\square$

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 θ be a root, and $K = \mathbb{Q}(\theta)$.

Lemma 5.8.7. (1) B is irreducible, and

$$\text{disc}(B) = 2^{318} \cdot 11^6 \cdot 41^2 \cdot 198839^2 \cdot 652081^6 \cdot 17743299257028546229859^2$$

(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 $\ell_\theta : y = \theta x + k(\theta)z$, θ running over the roots of B (certificate 1.3.8b).

Proof. (3) A line through ∞ other than $z = 0$ is $x = cz$; it meets C at ∞ 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. $\square$

Lemma 5.8.8. 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 θ of B put $h_\theta = (y - \theta x - k(\theta)z)/z$. At ∞ 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_θ 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 5.8.9. For a root θ of B let D_θ be the contact divisor of ℓ_θ (so $\text{div } h_\theta = 2D_\theta - 4\infty$) and $w_\theta = [D_\theta - 2\infty] \in J[2]$. Then $\iota : J[2] \rightarrow \mathbb{F}_2^{27}$, $\varepsilon \mapsto (e_2(\varepsilon, w_\theta))_\theta$, 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_θ ; 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 $q(a) = a_1a_2 + a_3a_4 + a_5^2 + a_6a_6 + a_6^2$. $\square$

This is the computation behind Proposition A(1), (2).

Lemma 5.8.10. $J(\mathbb{Q})[2] = 0$, and $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \rightarrow K^\times/K^{\times 2}$ is injective. Every element of $\delta(J(\mathbb{Q}))$ lies in

$$K(2, S) = \{a \in K^\times/K^{\times 2} : v_p(a) \text{ even for all } p \notin S\}, \quad S = \{p_1, p_2, p_3, p_4\},$$

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 5.8.3), 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 5.8.6) and is compatible with restriction (Proposition A(3)). $\square$

Step 4: the class group of K .

Lemma 5.8.11. 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 $\text{disc } B$ 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 θ 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. $\square$

Lemma 5.8.12. 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 $p \mid \text{disc } B$ 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 $p \nmid \text{disc } B$ 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. $\square$

Lemma 5.8.13. $\text{Cl}(K)$ has odd order. Consequently $\text{Cl}(\mathcal{O}_{K,S})[2] = 0$.

Proof. Apply Proposition B with $n = 27$, $(r_1, r_2) = (3, 12)$, $D = 2^{34}11^6652081^6$, $T = \log(5 \cdot 10^8) = 20.0301\dots$, $k(q) = a(q)$ for $q \leq 10^6$ (Lemma 5.8.11) and $k(q) = 0$ for $10^6 < q < 5 \cdot 10^8$ (Lemma 5.8.12), 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),

$$\begin{aligned} C_\infty &= -1.16146083530\dots, \\ C_\infty - \int_0^\infty (1-f)W &= -1.215796113312597138688\dots, \\ \frac{4}{n} \sum c_m(q) \frac{\log q}{q^m + 1} f(m \log q) &= 1.268980762763662101585\dots, \\ B^-(f) &\in [0.0531846494510649628970266145944 \pm 4.6 \cdot 10^{-32}]; \end{aligned}$$

the prime sum has positive part 1.3389143385... and negative part $-0.0699335757\dots$. Therefore $B^-(f) > 0$ and $\text{Cl}(K)[2] = 0$. $\text{Cl}(\mathcal{O}_{K,S})$ is a quotient of $\text{Cl}(K)$. $\square$

The window was chosen as the top eigenvector of the symmetric Toeplitz matrix Λ with $B^-(f) = \mathbf{h}^\top \Lambda \mathbf{h} / \mathbf{h}^\top \mathbf{h}$ 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

$$A(a) = C_\infty - \frac{\pi^2}{4a} - \frac{2\alpha \log 2}{a} + \frac{2}{a} \left(\text{Li}_2(e^{-a}) - \frac{\text{Li}_2(e^{-2a})}{4} \right) + \frac{2\alpha}{a} \log(1 + e^{-a}).$$

Step 5: S -units, the local image at 2, and the rank.

Lemma 5.8.14. *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 ε_i is integral with $N(\varepsilon_i) = \pm 1$, and each π_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 $q \leq 2791$, $q \nmid \text{disc } B$, 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 $0 \rightarrow \mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2} \rightarrow K(2, S) \rightarrow \text{Cl}(\mathcal{O}_{K,S})[2] \rightarrow 0$ and Lemma 5.8.13 give $K(2, S) = \mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 2}$. $\square$

Lemma 5.8.15. $\dim_{\mathbb{F}_2} J(\mathbb{Q}_2)[2] \leq 1$, so $\dim_{\mathbb{F}_2} \delta_{\mathbb{Q}_2}(J(\mathbb{Q}_2)) \leq 4$. 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 $W_2 \subset \prod_{\mathfrak{p}|2} K_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^{\times 2}$ 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 5.8.9), where D is the image of $\text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2)$; its orbits on the 27 coordinates have sizes 2, 5, 10, 10 (Lemma 5.8.8). 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 5.8.9 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 $\dim V^D \leq 1$, and by Proposition A(5) $\dim J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 3 + \dim J(\mathbb{Q}_2)[2] \leq 4$.

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 $v_{\mathfrak{p}}(Y - y) - v_{\mathfrak{p}}(Y - \theta x - k) \geq 2e + 1$ 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 .) $\square$

Let $\Sigma = \{a \in K(2, S) : a \text{ is totally positive and } (a)_{\mathfrak{p}|2} \in W_2\}$. By Lemmas 5.8.10 and 5.8.15, $\text{rank } J(\mathbb{Q}) = \dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \Sigma$.

Lemma 5.8.16. $\dim_{\mathbb{F}_2} \Sigma = 1$, and Σ is generated by $\theta - k(\theta) = \delta(G_1)$. Hence $\text{rank } J(\mathbb{Q}) = 1$, and $J(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3$.

Proof. In the basis of Lemma 5.8.14, Σ 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 $\text{rank } J(\mathbb{Q}) \leq 1$, and by Lemma 5.8.5 $\text{rank } J(\mathbb{Q}) \geq 1$ and $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/3$. (Consistently, $\theta - k(\theta)$ is totally positive with local class in W_2 , and $\delta(T) = -k(\theta)$ is a square in K .) $\square$

The condition at 2 alone already gives the bound: in the coordinates of Lemma 5.8.14 and on the basis of W_2 given by the four points of Lemma 5.8.15, 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 5.8.16 holds without the sign condition, and without the norm condition of Proposition A(4).

Step 6: Chabauty–Coleman at $p = 3$. By Lemma 5.8.3, C has good reduction at 3, and by Lemma 5.8.4, $C(\mathbb{Q}_3)$ 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 $\phi_L \in \mathbb{Z}[[X]]$:

$$\phi_z = X^4 + \cdots, \quad \phi_x = X + 2X^6 + \cdots, \quad \phi_y = 1 + 2X^5 + \cdots.$$

Lemma 5.8.17. 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 $x^i y^j$ ($j \leq 2$, $3i + 4j \leq 14$; x, y have poles of orders 3 and 4 at ∞) 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 $\text{ord}_{P_1} \geq 9$ 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 $\text{ord}_{P_1} g = 9$ exactly and pole order 13 at ∞ ; its reduction modulo 3 is nonzero with pole order exactly 9 at ∞ . So $\text{div } g = 9P_1 + \mathcal{E} - 13\infty$ with $\mathcal{E}$ effective of degree 4, and $\text{div } \bar{g} = 9\bar{P}_1 - 9\infty$; since divisors specialize on the smooth model, $\mathcal{E}$ reduces to 4∞ . Thus $[\mathcal{E} - 4\infty] = -9G_1$. The X -coordinates of the points of $\mathcal{E}$ are the roots of the irreducible polynomial $\text{Res}_Z(F(X, 1, Z), Z^4 g(X/Z, 1/Z))/X^3$,

$$\begin{aligned} \mathcal{E}(X) = & 268895426627707157987116133388416X^4 + 320337638116517237204091843045891X^3 \\ & + 219672860573908519668631358279748X^2 + 157894577001790646570719666475904X \\ & + 85988850899990436755428562963712, \end{aligned}$$

whose four roots all have 3-adic valuation $3/4$ (the coefficients of $X^0, \dots, X^4$ 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]

$$\lambda_L = \sum_{Q \in \mathcal{E}} \int_{\infty}^Q w_L = \text{Tr}_{M/\mathbb{Q}_3} \int_{\infty}^{Q_1} w_L = \sum_{k \geq 0} \frac{\phi_{L,k}}{k+1} p_{k+1}, \quad p_j = \sum_{Q \in \mathcal{E}} X(Q)^j,$$

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 $v_3(p_j) \geq 3j/4$, the terms with $k \geq 159$ have valuation greater than 115. As a check, the same computation with $\text{ord}_{P_1} \geq 18$ 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} . $\square$

Lemma 5.8.18. *Each residue disk $U_\infty, U_{P_0}, U_{P_1}$ contains exactly one rational point (certificate 1.3.8j).*

Proof. Since $\text{rank } J(\mathbb{Q}) = 1$ and G_1 has infinite order (Lemma 5.8.16), 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 5.8.17, $\lambda/9$ 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 $U_R \rightarrow 3\mathbb{Z}_3$, and every regular differential is $(a_0 + a_1 t + \dots) dt$ 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 $(z, x, y)(R) \pmod{3}$ 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 $Q = R$. $\square$

Proof of Theorem 5.8.1. $C(\mathbb{Q}) \subseteq U_\infty \cup U_{P_0} \cup U_{P_1}$, and by Lemma 5.8.18 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 5.8.16. $\square$

6 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.

$$\mathbf{6.1} \quad x^3 + 2x^2y + y^3 + y^2z + xz^2 + z^3 + t^2x - t^2y - t^2z + tyz + t^3 = 0 \quad (H = 96)$$

Theorem 6.1.1. *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 $S(\mathbb{Q}) = \emptyset$ by a Brauer–Manin obstruction of order 3 (Proposition J). Let

$$K = \mathbb{Q}(s), \quad s^2 = -23, \quad h(T) = T^3 - T + 1, \quad L = K(a), \quad h(a) = 0,$$

let $\tau(a) = -(23a + s(6a^2 + 9a - 4))/46 \in L$ (by Lemma 6.1.2(i), $a \mapsto \tau(a)$ defines a generator τ of $\text{Gal}(L/K)$), 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 inv_w and Frobenius elements $\text{Frob}_w \in \text{Gal}(L/K)$ are those of [Neu99, Chapters V–VI].

The proof goes as follows. We construct a twisted cubic $C \subset S_L$ with $\text{div}_S(G) = C + \tau C + \tau^2 C$ (Step 2), so that the cyclic algebra $\mathcal{B} = (L/K, \tau, G/(288x^3))$ lies in $\text{Br}(S_K)$ (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 6.1.2. (i) h is irreducible over K . Put $\tau^2(a) := -(23a - s(6a^2 + 9a - 4))/46$ (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 τ 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 $\text{Gal}(L/K) = \langle \tau \rangle$.

(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 $K_w = \mathbb{Q}_p$, $\text{Frob}_w = \tau^e$ and $\text{Frob}_{\bar{w}} = \tau^{-e}$ 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 $\text{Frob}_{w_+} = \tau$ and $\text{Frob}_{w_-} = \tau^2$.

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 $\text{disc } h = -23$. 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 $\mathbb{F}_p$. Then $\delta^2 = -23 \neq 0$, and the Frobenius $u \mapsto u^p$ maps δ to $\pm\delta$ according to the parity of the permutation it induces on the roots. Hence $h \bmod p$ has exactly one root if $(\frac{-23}{p}) = -1$, and three roots or none if $(\frac{-23}{p}) = 1$. If p is inert, Hensel's lemma gives $h = (T - r)g(T)$ over $\mathbb{Z}_p$, and $\text{disc } g \cdot g(r)^2 = \text{disc } h = -23$ 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 τ acts on it as the automorphism $\alpha_w: T \mapsto P(T, \sigma_w)$, $P(T, s) = -(23T + s(6T^2 + 9T - 4))/46$; $\alpha_w \neq 1$ 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 φ of $\mathbb{Q}_p[T]/(h)$, then $\text{Frob}_w = \tau^e$ with $e \equiv k^{-1}$ and $\text{Frob}_{\bar{w}} = \tau^{e'}$ 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 $h \bmod 2$ has no root, so it is irreducible. Finally, $L \otimes_K K_w$ is unramified over K_w for $p \neq 23$ because $h \bmod p$ 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 $\alpha_{w_-} = \varphi^2$. $\square$

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

$$q_k(\lambda w, \mu w, z, t) = w (A_k w + B_k z + C_k t) \quad (k = 0, 1),$$

with binary forms A_k of degree 2 and B_k, C_k of degree 1 in (λ, μ) . Put

$$\begin{aligned} W &= B_0 C_1 - C_0 B_1, & Z &= C_0 A_1 - A_0 C_1, & T &= A_0 B_1 - B_0 A_1, \\ \phi: \mathbb{P}_L^1 &\rightarrow \mathbb{P}_L^3, & (\lambda : \mu) &\mapsto (\lambda W : \mu W : Z : T), \end{aligned}$$

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 τ^j to the coefficients of ϕ , so that $(\tau^j \phi)(\mathbb{P}^1) = \tau^j(\phi(\mathbb{P}^1))$.

Lemma 6.1.3. (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 $C := \phi(\mathbb{P}_L^1)$ 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 τC 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) $\text{div}_S(G) = C + \tau C + \tau^2 C$.

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 ϕ 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 τ . The points: $\text{Res}(W, Z - aT) = \text{Res}(W, Z - \tau(a)T) = 0$, $\text{Res}(W, Z - \tau^2(a)T) \neq 0$ and $\text{Res}(W, T) \neq 0$ (**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], $\text{div}_S(G)$ (the divisor of G/ℓ^3 plus three times the plane section $\ell = 0$, for any linear form ℓ) 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. $\square$

Step 3: the Brauer class. For a linear form ℓ over K let H_ℓ be the plane section $\ell = 0$ of S . Put $\psi = G/(288x^3) \in K(S)^\times$. By Lemma 6.1.3(iv),

$$\text{div}_S(\psi) = C + \tau C + \tau^2 C - 3H_x = N_{L/K}(C - H_x),$$

so by Proposition J(1) the cyclic algebra $\mathcal{B} = (L/K, \tau, \psi)$ lies in $\text{Br}(S_K)$. Since $G/(288\ell^3) = \psi \cdot (x/\ell)^3$, Proposition J(1) also gives: for every field $K' \supseteq K$, every linear form ℓ over K and every $P \in S(K')$ with $G(P)\ell(P) \neq 0$ (so that P is not on $C \cup \tau C \cup \tau^2 C \cup H_\ell$),

$$\mathcal{B}(P) = (L \otimes_K K'/K', \tau, G(P)/(288\ell(P)^3)). \quad (16)$$

Step 4: reduction modulo primes.

Lemma 6.1.4. (i) S is smooth. For every prime $p \notin \{2, 3, 23, 31, 59, 9013\}$ the surface $\bar{S}_p: F \equiv 0 \pmod{p}$ 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 $\xi \in \mathbb{F}_p^4 \setminus \{0\}$ 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 $\mathbb{F}_p$ is singular along a curve (all partial derivatives of $F_1 F_2$ 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 $(g_0, g_1, \dots, g_4) \mapsto g_0 F + \sum_i g_i \partial F / \partial v_i$ 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 $\mathbb{F}_p$ gives the nonzero linear form "evaluation at ξ " on the forms of degree 5, which vanishes on the image, and two distinct points of $\mathbb{P}^3(\mathbb{F}_p)$ 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). $\square$

Step 5: the places not above 3.

Lemma 6.1.5. *Let $p \neq 3$ be a prime and $P \in S(\mathbb{Q}_p)$. Then $\sum_{w|p} \text{inv}_w \mathcal{B}(P) = 0$, and for $p \neq 2$ each term is 0. At the complex place w_∞ of K , $\text{inv}_{w_\infty} \mathcal{B}(P) = 0$ for every $P \in S(\mathbb{C})$.*

Proof. $\text{Br}(\mathbb{C}) = 0$. If $L \otimes_K K_w \cong K_w^3$, which by Lemma 6.1.2(ii) is the case when p is inert in K , when $p = 23$, and when p splits and $h \bmod p$ 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 $h \bmod p$ irreducible. Then $L_w/\mathbb{Q}_p$ is the unramified cubic extension, $\text{Frob}_w = \tau^e$ and $\text{Frob}_{\bar{w}} = \tau^{-e}$.

$p = 2$. 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 (16) 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], $\text{inv}_w \mathcal{B}(P) + \text{inv}_{\bar{w}} \mathcal{B}(P) = (2e + 2(-e))/3 = 0$.

$p \geq 5$ (this covers $p = 29, p = 31$ and all primes of good reduction with $h \bmod p$ irreducible). By Lemma 6.1.4, $\bar{S}_p$ 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 $F \bmod p$, 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 $\psi = G/(288\ell^3)$, ℓ a coordinate with $\ell(\bar{P}) \neq 0$, and $v_p(288) = 0$) gives $\text{inv}_w \mathcal{B}(P) = 0$. If $p = 31$ and $\bar{P} = P_{31}$, then $x(P)$ is a unit and $G^{(w)}(P) \equiv G^{(w)}(P_{31}) \equiv 6 \text{ or } 16 \pmod{31}$ is a unit (Lemma 6.1.4(ii)), so by (16) with $\ell = x$ and [Neu99, Chapters V–VI], $\text{inv}_w \mathcal{B}(P) = e \cdot 0/3 = 0$. $\square$

Step 6: the places above 3.

Lemma 6.1.6. *For every $P \in S(\mathbb{Q}_3)$ we have $v_3(G^{(w_+)}(P)) = 0$, $v_3(G^{(w_-)}(P)) = 1$, and*

$$\text{inv}_{w_+} \mathcal{B}(P) + \text{inv}_{w_-} \mathcal{B}(P) = \frac{2}{3}.$$

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 (16), Lemma 6.1.2(iii) and [Neu99, Chapters V–VI],

$$\text{inv}_{w_+} \mathcal{B}(P) = \frac{1 \cdot (-2)}{3} \equiv \frac{1}{3}, \quad \text{inv}_{w_-} \mathcal{B}(P) = \frac{2 \cdot (-1)}{3} \equiv \frac{1}{3} \pmod{1}.$$

(With the opposite sign convention for the invariants the sum is $1/3$; it is nonzero in either case.) $\square$

Step 7: conclusion.

Proof of Theorem 6.1.1. Suppose $P \in S(\mathbb{Q})$. Then $P \in S(K)$, and by Proposition J(4), $\sum_w \text{inv}_w \mathcal{B}(P) = 0$, the sum over all places of K . Grouping the places by the primes below them, Lemmas 6.1.5 and 6.1.6 give $\sum_w \text{inv}_w \mathcal{B}(P) = 2/3$, a contradiction. Hence $S(\mathbb{Q}) = \emptyset$. A nonzero integer solution would give a rational point of S . $\square$

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 $\mathcal{A} = \text{Cor}_{K/\mathbb{Q}} \mathcal{B} \in \text{Br}(S)$, whose local invariant at $P \in S(\mathbb{Q}_p)$ is $\sum_{w|p} \text{inv}_w \mathcal{B}(P)$, Steps 5 and 6 say that $\sum_p \text{inv}_p \mathcal{A}(P_p) = 2/3$ for every adelic point (P_p) ; so $S(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$, and the class of $\mathcal{A}$ in $\text{Br}(S)/\text{Br}(\mathbb{Q})$ has order 3.

6.2 $2x^3 + x^2y + xy^2 + y^3 + y^2z - 2xz^2 - z^3 + t^2y + tz^2 - t^3 = 0$ ($H = 96$)

Theorem 6.2.1. *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

$$\ell_{\pm} = (-1 \pm s)x + 4y, \quad \rho = -\frac{(s-1)q^2 + 8}{4(3q^2 - 1)}.$$

The plane $\ell_+ = 0$ meets S in three lines that are defined over L and permuted cyclically by $\text{Gal}(L/K)$ (Step 2). For a rational point P of S we put $\psi = \ell_+(P)/\ell_-(P) \in K^\times$ and compute the local invariants $\text{inv}_w(\psi)$ 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 6.2.2.** (i) h is irreducible over $\mathbb{Q}$ and $\text{disc}(h) = -23$. $L = K(q) \cong K[T]/(h)$, $[L : K] = 3$, and $\text{Gal}(L/K)$ is cyclic, generated by the automorphism τ with $\tau(q) = (-q + s/h'(q))/2$. Every element of $\text{Gal}(L/\mathbb{Q})$ outside $\text{Gal}(L/K)$ conjugates τ to τ^{-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 $\text{Gal}(L/K)$. This is the case for $p = 2$ and $p = 3$.
- (iv) Every prime p falls under (ii) or (iii).

Proof. (i) ± 1 are not roots of h , so h is irreducible, and $\text{disc}(h) = -4(-1)^3 - 27 = -23$. 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 $\text{Gal}(L/\mathbb{Q})$ acts faithfully and transitively on the roots, and the elements that fix δ are the even permutations; since $\delta \notin \mathbb{Q}$, $\text{Gal}(L/\mathbb{Q}) \cong S_3$ and $\text{Gal}(L/K) \cong A_3$ 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 τ 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 $\text{Gal}(L/K)$, 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. $\square$

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 $(1, 1, 6)$, $(2, \pm 1, 3)$), L is the Hilbert class field of K . We do not use this.

Step 2: the plane section.

- Lemma 6.2.3.** (i) As polynomials in x, z, t with coefficients in L ,

$$F\left(x, \frac{(1-s)x}{4}, z, t\right) = -\prod_{i=0}^2 (t - \tau^i(\rho)x - \tau^i(q)z).$$

- (ii) The determinant of the matrix with rows $(-\tau^i(\rho), -\tau^i(q), 1)$ ($i = 0, 1, 2$) is $(s - 1)/2$, and $N_{K/\mathbb{Q}}((s - 1)/2) = 6$.
- (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 τ : the product over the three roots θ 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) $N(3q^2 - 1) = N(h'(q)) = -\text{disc}(h) = 23$. $\square$

Lemma 6.2.4. *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 ± 1 are not roots (**certificate 1.4.2b**). $\square$

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 6.2.4**).

Lemma 6.2.5. *$\text{inv}_w(\psi) = 0$ 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 6.2.2**, L/K is split, so $\text{inv}_w(\psi) = 0$ by [**Neu99**, Chapters V–VI]. By **Lemma 6.2.2(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 6.2.2(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 6.2.3(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 6.2.3(ii)**, then $M(x, z, t)^T = (m_0, m_1, m_2)^T$, 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 $\text{inv}_w(\psi) = 0$ by [**Neu99**, Chapters V–VI]. $\square$

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 6.2.6. *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 $v_{w_2}(\psi) = v_2(\ell_+(P)) - v_2(\ell_-(P))$. $\square$

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 6.2.7. *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

$$\frac{1}{3}F = 1 + 2Y - 3T + 3Y^2 - 6TY + 9(-T^3 + T^2Y + T^2 + TZ^2 + Y^3 + Y^2Z - Z^3 - Z^2).$$

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. $\square$

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 6.2.1. Suppose that S has a rational point P , and let ψ be as in Step 3. By [Neu99, Chapter VI, Section 5], $\sum_w \text{inv}_w(\psi) = 0$, and by Lemma 6.2.5 only the places $w_2, c(w_2), w_3, c(w_3)$ can contribute. They are unramified in L with Frobenius elements generating $\text{Gal}(L/K)$ (Lemma 6.2.2(iii)). Write $\text{Frob}_{w_2} = \tau^m$ with $m \in \{1, 2\}$. By Lemma 6.2.2(i), the hypothesis of [Neu99, Chapters V–VI] holds (with $k = \mathbb{Q}$), and $c(\psi) = \psi^{-1}$; so $\text{inv}_{c(w)}(\psi) = \text{inv}_w(\psi)$ for $w = w_2, w_3$. By [Neu99, Chapters V–VI] and Lemma 6.2.7, $\text{inv}_{w_3}(\psi) = 0$, since $v_{w_3}(\psi) \equiv 0 \pmod{3}$. By [Neu99, Chapters V–VI] and Lemma 6.2.6, $\text{inv}_{w_2}(\psi) = m v_{w_2}(\psi)/3 \equiv m/3 \pmod{1}$. Hence

$$\sum_w \text{inv}_w(\psi) = 2 \text{inv}_{w_2}(\psi) = \frac{2m}{3} \not\equiv 0 \pmod{1},$$

a contradiction. Therefore $S(\mathbb{Q}) = \emptyset$. A nonzero integer solution would give a rational point of S , so the only integer solution is $(0, 0, 0, 0)$. $\square$

$$\mathbf{6.3} \quad 2x^3 + 2x^2y + 2y^3 + y^2z - 2xz^2 - z^3 + tz^2 - t^3 = 0 \quad (H = 96)$$

Theorem 6.3.1. *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 6.2, 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

$$\ell_{\pm} = (2 \pm s)y + 3t, \quad \rho = \frac{s + 2 - 6q^2}{6(3q^2 - 1)}.$$

The plane $\ell_+ = 0$ meets S in three lines permuted cyclically by $\text{Gal}(L/K)$ (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 6.2; again $c(\psi) = \psi^{-1}$.

Step 1: the fields.

Lemma 6.3.2. (i) g is irreducible over $\mathbb{Q}$ and $\text{disc}(g) = -176 = -11 \cdot 4^2$. $L = K(u) \cong K[U]/(g)$, $[L : K] = 3$, and $\text{Gal}(L/K)$ is cyclic, generated by the automorphism τ with $\tau(u) = (-u + 4s/g'(u))/2$. Every element of $\text{Gal}(L/\mathbb{Q})$ outside $\text{Gal}(L/K)$ conjugates τ to τ^{-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 $\text{Gal}(L/K)$. 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 6.2.2. The rational roots of g would divide 4, and $\pm 1, \pm 2, \pm 4$ are not roots. $\text{disc}(g) = -4(-4)^3 - 27 \cdot 16 = -176$, 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 τ 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 $\delta^2 = -176$ 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. $\square$

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 6.3.6 works for any cubic extension.

Step 2: the plane section.

Lemma 6.3.3. (i) As polynomials in x, y, z with coefficients in L ,

$$F\left(x, y, z, -\frac{(2+s)y}{3}\right) = 2 \prod_{i=0}^2 (x - \tau^i(\rho)y - \tau^i(q)z).$$

(ii) The determinant of the matrix with rows $(1, -\tau^i(\rho), -\tau^i(q))$ ($i = 0, 1, 2$) is 2.

(iii) u is an algebraic integer, $3q^2 - 1 = (3u^2 - 4)/4$, and $N_{\mathbb{Q}(u)/\mathbb{Q}}(3u^2 - 4) = -\text{disc}(g) = 176$. 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) $\rho = 4(s + 2 - \frac{3}{2}u^2)/(6(3u^2 - 4))$. $\square$

Lemma 6.3.4. 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 $\pm 1, \pm 2$ are not roots (certificate 1.4.3b). $\square$

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 6.3.5. $\text{inv}_w(\psi) = 0$ 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 6.3.2, 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 6.3.3(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 6.3.3(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 $\text{inv}_w(\psi) = 0$ by [Neu99, Chapters V–VI]. $\square$

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 6.3.6. 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 $\text{inv}_{w_2}(\psi) = 0$.

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 6.3.2(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 ψ is a local norm and $\text{inv}_{w_2}(\psi) = 0$ by [Neu99, Chapters V–VI]. (Equivalently, by [Neu99, Chapters V–VI]: the residue of ψ is 1, a cube in $\mathbb{F}_4^\times$.) $\square$

Lemma 6.3.7. 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

$$\frac{1}{3}F = 18X^3 + 18X^2Y - 18X^2 - 12XY - 18XZ^2 + 6X + 18Y^3 + 9Y^2Z + 2Y - 9Z^3 + 9Z^2 - 1.$$

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 $\ell_+ = 3((2+s_3)Y + 1) \equiv 3(33Y + 1)$ has valuation 1, and $\ell_- = 3((2-s_3)Y + 1) \equiv 3(1 - 29Y) \pmod{3^4}$, where $1 - 29Y \equiv 18$ or $9 \pmod{27}$ has valuation 2. So the pair is $(1, 3)$. $\square$

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 6.3.1. Suppose that S has a rational point P , and let ψ be as in Step 3. By Lemmas 6.3.5 and 6.3.6, only w_3 and $c(w_3)$ can contribute to $\sum_w \text{inv}_w(\psi)$, which is 0 by [Neu99, Chapter VI, Section 5]. These places are unramified in L , and $\text{Frob}_{w_3} = \tau^m$ with $m \in \{1, 2\}$ (Lemma 6.3.2(iii)). By [Neu99, Chapters V–VI] and $c(\psi) = \psi^{-1}$, $\text{inv}_{c(w_3)}(\psi) = \text{inv}_{w_3}(\psi)$, and by [Neu99, Chapters V–VI] and Lemma 6.3.7, $\text{inv}_{w_3}(\psi) = m v_{w_3}(\psi)/3 \equiv m/3 \pmod{1}$. Hence $\sum_w \text{inv}_w(\psi) = 2m/3 \not\equiv 0 \pmod{1}$, a contradiction. Therefore $S(\mathbb{Q}) = \emptyset$, and the only integer solution is $(0, 0, 0, 0)$. $\square$

6.4 $8x^4 + 7y^4 + 2z^4 - t^4 = 0$ ($H = 288$)

Theorem 6.4.1. *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

$$f = 7y^2 + 2z^2 - 3t^2, \quad g = 7y^2 + 2z^2 + 3t^2, \quad A_{\pm} = 2x^2 \pm 2xz + z^2.$$

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 6.4.2. (i) $-fg = 72x^4 + 14(y^2 - z^2)^2 = 2(36x^4 + 7(y^2 - z^2)^2)$, 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), $f \leq 0$, and $f = 0$ forces $x = 0$ and $y^2 = z^2$, so $t^4 = 9y^4$, $t^2 = 3y^2$, $y = t = 0$. $\square$

Step 2: odd primes other than 3 and 7.

Lemma 6.4.3. *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 6.4.2(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 $v_p(f) = v_p(-fg) = v_p(N(6x^2 + (y^2 - z^2)\sqrt{-7}))$ 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 $v_p(A_+) = v_p(t^4 - 7y^4) = v_p(N(t^2 + y^2\sqrt{7}))$ is even, because p is inert in $\mathbb{Q}(\sqrt{7})$. $\square$

Step 3: the prime 3.

Lemma 6.4.4. $v_3(f) \in \{0, 2\}$.

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. $\square$

Step 4: the prime 2.

Lemma 6.4.5. 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). $\square$

Step 5: the prime 7.

Lemma 6.4.6. 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	± 2	1	4
2	± 3	6	3
-2	± 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). $\square$

Step 6: Hilbert symbols.

Proof of Theorem 6.4.1. By Lemma 6.4.2(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 6.4.3, both are 1.

$p = 3$: $(-7, f)_3 = (-7/3)^{v_3(f)} = (-1)^{v_3(f)} = 1$ by Lemma 6.4.4, 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 6.4.5), $(7, A_+)_2 = (-1)^{\varepsilon(7)\varepsilon(A_+)} = 1$.

$p = 7$: f and A_+ are 7-adic units (Lemma 6.4.6) 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 6.4.6.

$v = \infty$: $-7 < 0$ 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. $\square$

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 $\mathbb{F}_5[G_Q]$ -module of dimension 2, $G_Q = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) 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_ℓ for the ℓ -adic valuation, $\Delta_{\min}$ for the minimal discriminant, $f_\ell(E)$ for the exponent of ℓ in the conductor N_E , $a_\ell(E) = \ell + 1 - \#\tilde{E}(\mathbb{F}_\ell)$ for a prime ℓ of good reduction, and χ_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 6.4.7. *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. $\square$

In the situation of Lemma 6.4.7(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

$$(u, v, w) = \varepsilon (t_i, t_j, t_k), \quad \varepsilon \in \{\pm 1\} \text{ such that } u \equiv -1 \pmod{4}.$$

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

$$E = E_{u,v} : Y^2 = X(X - u)(X + v), \quad c_4 = 16(u^2 + uv + v^2), \quad \Delta = 16u^2v^2w^2.$$

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 6.4.8(3); nothing below depends on this choice.

Lemma 6.4.8. *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 ℓ , $E_{u,v}$ 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	≥ 5
type	III	I ₁ [*]	III [*]	I ₀	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 Δ 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 . $\square$

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 6.4.9. *In the situation of Lemma 6.4.7(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 [Sil12, Theorem 3 and Proposition 5.1] for $p = 5$,*

$$N_5 = N_E / \prod_{\ell \parallel N_E, 5 \nmid v_\ell(\Delta_{\min})} \ell,$$

is $N_5 = 2^\alpha \prod_{\ell \mid ABC, \ell \text{ odd}} \ell$, where $\alpha = f_2(E)$ from Lemma 6.4.8(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 ℓ be odd. By Lemma 6.4.8(1), E is good at ℓ 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 ℓ . If $\ell \mid ABC$, then $1 \leq v_\ell(c) \leq 4$, so $5 \nmid v_\ell(\Delta_{\min})$ and ℓ divides N_5 exactly once. If $\ell \nmid ABC$, then $5 \mid v_\ell(\Delta_{\min})$, so $\ell \nmid N_5$. At 2, Lemma 6.4.8(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. $\square$

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 6.9). The resulting levels for each equation are printed by certificate 1.4.5a–certificate 1.4.10a.

Lemma 6.4.10. *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 $\psi: G_{\mathbb{Q}} \rightarrow \mathbb{F}_5^\times$; 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 ψ is unramified at ℓ . At 5, the image of inertia under ψ has order prime to 5, so ψ 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 $0 \rightarrow L \rightarrow E[5] \rightarrow E[5]/L \rightarrow 0$, 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 δ 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 ϵ is at least the codimension of the inertia invariants of $E[5]$ (in the multiplicative case because inertia fixes the line coming from μ_5 , [Sil94, Chapter V]). Since χ_5 is unramified at 2, $a_2(\psi') = a_2(\psi)$, so $a_2(\psi) \leq 2$. By the Kronecker–Weber theorem, ψ 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 Frob_q on $E[5]$ is $\psi(q) + q\psi(q)^{-1} \equiv 2\psi(q) \pmod{5}$. It equals $a_q(E) \pmod{5}$. $\square$

Lemma 6.4.11. *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 6.4.10. As there, ψ and ψ' 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 ψ and ψ' 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 χ_5 . Since $\psi\psi' = \chi_5$ is ramified at 5, one of ψ, ψ' 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 $\phi: E \rightarrow E' = E/L$ 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, ϕ maps $E[2]$ isomorphically onto $E'[2]$, so $E'(\mathbb{Q})$ contains $\mathbb{Z}/2 \times \mathbb{Z}/10$. Both cases contradict [Maz77]. $\square$

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

$$a_q(E_{u,v}) = - \sum_{X \in \mathbb{F}_q} \left(\frac{X(X-u)(X+v)}{q} \right) \quad (u, v, u+v \in \mathbb{F}_q^\times),$$

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 6.5–6.10 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 6.4.12. *In the situation of Lemma 6.4.7(2), let E be the Frey curve and N_5 its level from Lemma 6.4.9, and let $q \nmid 10ABC$ be a prime.*

- (1) *If $q \nmid xyz$, then E has good reduction at q and $a_q(E) \pmod{5} \in T_q$. If $q \mid xyz$, then $q \parallel N_E$, $q \nmid N_5$, and $\pm(q+1) \pmod{5} \in T_q$.*
- (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 $a_q(f) \pmod{\lambda} \in T_q$ 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 6.4.8(1)); its reduction is, by Lemma 6.4.8(3), isomorphic to E_{Ax^5, By^5} or its twist by -1 , and $E_{Ax^5, By^5} \equiv E_{\mu^5 Ax^5, \mu^5 By^5}$ is the twist of E_{Aa^5, Bb^5} by μ^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 6.4.7(2)), $(a : b : c)$ has a zero coordinate, and by the proof of Lemma 6.4.9, $q \parallel N_E$ 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 6.4.9, E is semistable at every odd prime, and Lemma 6.4.10 applies.

(3) By [Sik12, Theorem 3 and Proposition 5.1] with $p = 5$ there are f and λ with $a_q(f) \equiv a_q(E) \pmod{\lambda}$ if $q \nmid 5N_5$, and $a_q(f) \equiv \pm(q+1) \pmod{\lambda}$ if $q \nmid 5N_5$ and $q \parallel N_5$. Since N_5 divides $2^5 ABC$, every prime $q \nmid 10ABC$ is in one of these two cases, and (1) gives the claim. $\square$

The newforms of the levels N_5 are computed with PARI/GP (`mfininit`, `mfeigenbasis`). For each Galois orbit with coefficient field $K_f = \mathbb{Q}[y]/(P)$ the codes compute the maximal order of K_f (`nfininit`, certified by `nfcertify`) and test every prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ separately: the pair (orbit, λ) 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 6.4.13. *Let p be an odd prime and ℓ 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 $\phi: E_1[p] \rightarrow E_2[p]$ 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 ℓ_1, ℓ_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 ϕ^*e_2 is again a nondegenerate alternating pairing with values in μ_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 ε_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 $0 \rightarrow \mu_p \rightarrow E_{q_i}[p] \rightarrow \mathbb{Z}/p \rightarrow 0$ does not split, and $\varepsilon_i\mu_p$ is the only $G_{\mathbb{Q}_\ell}$ -stable line of $E_i[p]$. Hence ϕ maps $\varepsilon_1\mu_p$ to $\varepsilon_2\mu_p$, so $\varepsilon_1 = \varepsilon_2(-1 \neq 1 \text{ in } \mathbb{F}_p)$, and twisting both curves by ε_1 changes neither ϕ nor the Weil pairings. So we may assume $E_i = E_{q_i}$. In the bases (ζ, 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 ζ^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 $\phi: E[p] \rightarrow G[p]$; 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 ℓ_1 and at ℓ_2 . $\square$

$$6.5 \quad 14x^5 + 5y^5 + 3z^5 = 0 \quad (H = 704)$$

Theorem 6.5.1. *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 6 (Lemmas 6.4.7–6.4.13). 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

$$G_+ : Y^2 = X^3 + X^2 - 890X - 10200, \quad G_- : Y^2 = X^3 - X^2 - 890X + 10200$$

(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 6.5.2. *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

$$v_3(\Delta_{\min}) = 2 + 10v_3(z), \quad v_5(\Delta_{\min}) = 2 + 10v_5(y), \quad v_7(\Delta_{\min}) = 2 + 10v_7(x),$$

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 6.4.9 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 ± 1 . By Lemma 6.4.7, $xyz \neq 0$ 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 6.4.8(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 6.4.9: 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). $\square$

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 ± 4 .

Lemma 6.5.3. $E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(N_5))$, with N_5 as in Lemma 6.5.2, and a prime ideal $\lambda \mid 5$ of $\mathcal{O}_{K_f}$ such that $a_q(f) \pmod{\lambda} \in T_q$ 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 6.4.12(2). Since no q in the table divides $10 \cdot 14 \cdot 5 \cdot 3$, Lemma 6.4.12(3) gives f and λ . $\square$

Step 3: the sieve.

Lemma 6.5.4. (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 6.5.3 (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 6.5.3; 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). $\square$

Step 4: the two remaining newforms.

Lemma 6.5.5. The newform f of Lemma 6.5.3 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 $\mathbb{F}_5[G_Q]$ -modules. Both E and $G_{\pm}$ have multiplicative reduction at 3 and at 5, with discriminant valuations prime to 5: by Lemma 6.5.2, $v_3(\Delta_{\min}(E)) \equiv v_5(\Delta_{\min}(E)) \equiv 2 \pmod{5}$. The ratios are

$$\frac{v_3(\Delta_{\min}(G_{\pm}))}{v_3(\Delta_{\min}(E))} \equiv \frac{6}{2} \equiv 3, \quad \frac{v_5(\Delta_{\min}(G_{\pm}))}{v_5(\Delta_{\min}(E))} \equiv \frac{2}{2} = 1 \pmod{5},$$

and 3 is not a square modulo 5, while 1 is. This contradicts Lemma 6.4.13 with $p = 5$, $\ell_1 = 3$, $\ell_2 = 5$. $\square$

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 6.5.1. 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 6.5.2 and 6.5.3 there is a newform f of level 210 or 3360 with the conditions of Lemma 6.5.3. By Lemma 6.5.4, f is f_+ or f_- , which contradicts Lemma 6.5.5. $\square$

6.6 $21x^5 + 5y^5 + 4z^5 = 0$ ($H = 960$)

Theorem 6.6.1. *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 6 (Lemmas 6.4.7–6.4.12). 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 6.6.2. *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 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 ± 1 . By Lemma 6.4.7, $xyz \neq 0$, 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 6.4.8(2) gives type 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 6.4.9 gives N_5 (certificate 1.4.6a; the 2-adic data are also checked with PARI on all residue classes of εx and z modulo 2^6 in certificate 1.4.6c). $\square$

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 6.6.3. $E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(N_5))$, with $N_5 \in \{210, 840\}$ as in Lemma 6.6.2, 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 $f_2(E) \leq 5$, Lemma 6.4.12(2) applies; then Lemma 6.4.12(3) gives f and λ , since no q of the table divides $10 \cdot 21 \cdot 5 \cdot 4$. $\square$

Step 3: the sieve.

Lemma 6.6.4. No newform of level 210 or 840 satisfies the conditions of Lemma 6.6.3. 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, λ), 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. $\square$

Proof of Theorem 6.6.1. A solution other than $(0, 0, 0)$ gives a primitive one, and then, by Lemmas 6.6.2 and 6.6.3, a newform of level 210 or 840 that Lemma 6.6.4 excludes. $\square$

$$6.7 \quad 17x^5 + 6y^5 + 3z^5 = 0 \quad (H = 832)$$

Theorem 6.7.1. 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

$$1377X^5 + 2y^5 + z^5 = 0, \quad 1377 = 3^4 \cdot 17.$$

We apply the common framework of Section 6 (Lemmas 6.4.7–6.4.12) 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 6.7.2. 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 $17 \cdot 3^5 X^5 + 6y^5 + 3z^5 = 0$ 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 ± 1 . By Lemma 6.4.7, $XYZ \neq 0$, 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 6.4.8(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 6.4.9 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). $\square$

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 ± 10 .

Lemma 6.7.3. $E[5]$ is irreducible. There are a newform $f \in S_2(\Gamma_0(N_5))$, with $N_5 \in \{102, 1632\}$ as in Lemma 6.7.2, 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 $f_2(E) \leq 5$, Lemma 6.4.12(2) applies (so does $q = 41$); Lemma 6.4.12(3) gives f and λ , since no q of the table divides $10 \cdot 1377 \cdot 2$. $\square$

Step 3: the sieve.

Lemma 6.7.4. No newform of level 102 or 1632 satisfies the conditions of Lemma 6.7.3. 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, λ). 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. $\square$

Proof of Theorem 6.7.1. A solution other than $(0, 0, 0)$ gives a primitive one, and then, by Lemmas 6.7.2 and 6.7.3, a newform of level 102 or 1632 that Lemma 6.7.4 excludes. $\square$

$$6.8 \quad 17x^5 + 9y^5 + 5z^5 = 0 \quad (H = 992)$$

Theorem 6.8.1. 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 6 (Lemmas 6.4.7–6.4.12). 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 6.8.2. 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,

$$\begin{aligned} v_2(\Delta_{\min}) &= 10e - 8 \quad (e = v_2(xyz) \geq 1), \\ v_3(\Delta_{\min}) &= 4 + 10v_3(y), \quad v_5(\Delta_{\min}) = 2 + 10v_5(z), \quad v_{17}(\Delta_{\min}) = 2 + 10v_{17}(x), \end{aligned}$$

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 ± 1 . By Lemma 6.4.7, $xyz \neq 0$, the terms are pairwise coprime and exactly one is even; as the coefficients are odd, exactly one variable is even, and $r = 5e$ with $e = v_2(xyz) \geq 1$. By Lemma 6.4.8(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 6.4.9 (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). $\square$

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 ± 10 .

Lemma 6.8.3. $E[5]$ 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 6.4.12(2) applies; Lemma 6.4.12(3) gives f and λ . $\square$

Step 3: the sieve.

Lemma 6.8.4. No newform of level 510 satisfies the conditions of Lemma 6.8.3. 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, λ). 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. $\square$

Proof of Theorem 6.8.1. A solution other than $(0, 0, 0)$ gives a primitive one, and then, by Lemmas 6.8.2 and 6.8.3, a newform of level 510 that Lemma 6.8.4 excludes. $\square$

6.9 $14x^5 + 13y^5 + 2z^5 = 0$ ($H = 928$)

Theorem 6.9.1. 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

$$7x^5 + 208Y^5 + z^5 = 0, \quad 208 = 2^4 \cdot 13.$$

We apply the common framework of Section 6 (Lemmas 6.4.7–6.4.12) 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 6.9.2. 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 ± 1 . By Lemma 6.4.7, $xYz \neq 0$, 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 6.4.8(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 6.4.9). The rest is Lemma 6.4.9, with $5 \nmid 7 \cdot 208$ (certificate 1.4.9a; the 2-adic data are also checked with PARI in certificate 1.4.9b). $\square$

Step 2: irreducibility and level lowering.

Lemma 6.9.3. $E[5]$ 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 6.9.2, E has full rational 2-torsion, is semistable at every odd prime, has $f_2(E) \leq 1$, and has good reduction at 5 or multiplicative reduction with $5 \mid v_5(\Delta_{\min})$. Lemma 6.4.11 gives irreducibility, and Lemma 6.4.12(3) gives f and λ ($11 \nmid 10 \cdot 7 \cdot 208$). $\square$

Lemma 6.9.4. 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 ± 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). $\square$

Step 3: the newforms of level 91.

Lemma 6.9.5. $S_2(\Gamma_0(91))^{\text{new}}$ has dimension 7 and four Galois orbits, of dimensions 1, 1, 2, 3. The minimal polynomials of their eigenvalues a_{11} are

$$T, \quad T + 6, \quad T^2 - 18, \quad T^3 - 2T^2 - 6T + 8.$$

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. $\square$

Proof of Theorem 6.9.1. Suppose that there is a solution other than $(0, 0, 0)$, and take a primitive one. By Lemmas 6.9.3 and 6.9.4, 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 6.9.5. $\square$

6.10 $4x^5 + 4y^5 + 11z^5 = 0$ ($H = 608$)

Theorem 6.10.1. 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

$$x^5 + y^5 + 88w^5 = 0, \quad 88 = 2^3 \cdot 11.$$

The solutions with a zero coordinate are elementary (Step 1). For the others we apply the common framework of Section 6 (Lemmas 6.4.7–6.4.12): 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 6.10.2. *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 6.4.7(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 . $\square$

Lemma 6.10.3. *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 $\varepsilon = \pm 1$ 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 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 6.4.7(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 6.4.8(2) gives type 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 6.4.9, with $5 \nmid 88$ (certificate 1.4.10a; the 2-adic data are also checked with PARI in certificate 1.4.10b). $\square$

Step 2: irreducibility, level lowering and the prime 3.

Lemma 6.10.4. *$E[5]$ is irreducible, and there are a newform $f \in S_2(\Gamma_0(N_5))$, $N_5 \in \{22, 88\}$ as in Lemma 6.10.3, 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 6.10.3). Lemma 6.4.11 gives irreducibility, and Lemma 6.4.12(3) gives f and λ ($3 \nmid 10 \cdot 88$). $\square$

Lemma 6.10.5. $T_3(1, 1, 88) = \{0, 1, 4\}$.

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). $\square$

Step 3: the newforms of levels 22 and 88.

Lemma 6.10.6. $S_2(\Gamma_0(22))^{\text{new}} = 0$. $S_2(\Gamma_0(88))^{\text{new}}$ 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. $\square$

Proof of Theorem 6.10.1. By Lemma 6.10.2, it suffices to show that there is no primitive solution with $xyz \neq 0$. For such a solution, Lemma 6.10.4 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 6.10.5, so the reduction modulo 5 of the minimal polynomial of $a_3(f)$ would have a root in $\{0, 1, 4\}$, contrary to Lemma 6.10.6. $\square$

Reproducibility

The separate reproducibility archive contains the computational material for the thirty-eight proofs in this paper and its shared dependencies, together with the LaTeX source and BibTeX database. Its top-level README gives the build instructions, software requirements and current certificate map, and distinguishes historical computational outputs from the editorial and packaging checks performed for this edition. Generated large witness files are not needed to typeset the paper and can be reconstructed using the documented commands.

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 $\mathbf{Q}$: 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>.
- [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>.

- [BYY04] 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>.
- [Do12] 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>.
- [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*, 2026, arXiv:2607.06627, <https://arxiv.org/abs/2607.06627>.
- [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>.
- [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*, The American Mathematical Monthly (2026), To appear.
- [Gre26c] ———, *A systematic approach to Diophantine equations: open problems*, 2026, Available at <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.
- [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>.
- [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 Mihailescu, *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>.
- [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.

- [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>.
- [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.
- [Ser87] ———, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$* , 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>.
- [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. Sémin. 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/2404.08719v2>, 2024, Version 2, 17 December 2024; Appendix A was added in this revision.
- [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>.