hexagon:2611.01058v1

DIOPHANTINE DEFINITIONS OF $\mathbb{Z}$ IN TOTALLY REAL FIELDS FROM RANK-ONE ELLIPTIC CURVES

MANVIR JASWAL

Abstract. Let K be a totally real number field, let $E\colon y^2 = x^3 - Ax$ be one of four explicit elliptic curves over a real quadratic field $F \not\subseteq K$, and put $L = KF$. We prove that if $E(L)$ has rank one and torsion in $E[2]$, and $2E(L) \subseteq E(F)$, then $\mathbb{Z}$ is Diophantine in K, with 25 unknowns, so Hilbert's tenth problem over K has a negative answer. For a suitable curve these conditions hold for every layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, for infinitely many real quadratic fields and for some further fields of degree at most 8. The construction is Z.-W. Sun's, from his proofs for $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$, except that our predicate excluding poles of odd order uses the congruent-number twists of our earlier proof for $\mathbb{Q}$. Its main step is a height bound on a q-adic tube of a quaternionic Shimura curve. We prove it over every totally real field by Sun's method, with a scalar cochain over K, a comparison with Shimura curves over K in every degree and, when $\sqrt{3} \in K$, a second tube prime.

Contents

1. Introduction 2
2. The index curves 7
3. A height bound on a tube 16
4. Primes in a quadratic pattern 24
5. The pole predicate 27
6. Local lemmas 28
7. The certificate 31
8. Soundness 33
9. Completeness 35
10. Fields containing $\sqrt{3}$ 40
11. Proof of Theorem 1.1 43
12. The fields of Theorem 1.2 43
13. The cyclotomic $\mathbb{Z}_2$-extension 58
Appendix A. Proof of Proposition 3.5 64
Appendix B. The number of unknowns 67
Appendix C. Two steps at a composite modulus 71
Declarations 74
References 74

Date: November 25, 2026.

2020 *Mathematics Subject Classification.* Primary 11U05; Secondary 03D35, 11G05, 11G18, 11F80.

Key words and phrases. Hilbert's tenth problem, Diophantine sets, totally real fields, elliptic curves, Shimura curves, heights.

1. Introduction

A subset A of a commutative ring R is *Diophantine in* R if there is a polynomial $f \in \mathbb{Z}[X, Y_1, \dots, Y_k]$ such that, for every $a \in R$, $a \in A$ if and only if $f(a, y_1, \dots, y_k) = 0$ for some $y_1, \dots, y_k \in R$. Hilbert's tenth problem over R asks for an algorithm that decides, for every polynomial with integer coefficients, whether it has a zero with coordinates in R. Matiyasevich's theorem [38], completing work of Davis, Putnam and Robinson, makes every recursively enumerable subset of $\mathbb{Z}$ Diophantine in $\mathbb{Z}$, so no such algorithm exists over $\mathbb{Z}$. If $\mathbb{Z}$ is Diophantine in a field K that has a real embedding, then a system of equations over K is equivalent to one equation (a sum of squares), and solvability over $\mathbb{Z}$ reduces to solvability over K; so no algorithm exists over K either.

For rings of integers the question has a complete answer. Koymans and Pagano proved that $\mathbb{Z}$ is Diophantine in the ring of integers of every number field [35, Theorem 1.2], and so did Alpöge, Bhargava, Ho and Shnidman [2, Theorem 1.1 and Corollary 1.2]. For fields the question is different, because a Diophantine definition of $\mathbb{Z}$ in K has to separate integers from all other elements of K, including those whose denominators are divisible only by large primes. For $\mathbb{Q}$, Glazer and collaborators turned OpenAI's proof that Hilbert's tenth problem over $\mathbb{Q}$ has a negative answer [44] into a Diophantine definition of $\mathbb{Z}$ [68], and Bhargava and Burungale proved that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ [5, Theorem A]. Our earlier paper [31] gives a proof for $\mathbb{Q}$ whose outside inputs are published theorems; here its completeness argument is carried to totally real fields. Sun proved that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}(\sqrt{2})$ and in $\mathbb{Q}(\sqrt{6})$, with 25 unknowns, by a construction on an elliptic curve over $\mathbb{Q}(\sqrt{3})$ [60, Theorems 1.2 and 1.4], and in $\mathbb{Q}(\sqrt{3})$ [60, Theorem 1.3]. Version 3 of [60] (arXiv:2611.25002v3, §13) lowers the count for these three fields to 24; we follow version 2 and its numbering. We carry that construction to the totally real fields over which that curve, or one of three further curves over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$, has the arithmetic the construction needs.

The idea. The construction is Sun's [60, §§1–4, 9, 10, 12, 13]: the first index curve, the tube and its seven contacts, the certificate and the order in which its parameters are chosen. It uses the field in two ways. It reads integers off as multiples of one point, so the curve, defined over a real quadratic field F, must have rank one over $L = KF$, with the conditions (I2) and (I3) below on torsion and descent. And its soundness rests on a bound for the height of an element of K in a q-adic tube in terms of the primes at which it meets seven fixed points of $\mathbf{P}^1$ to odd order. The rest uses only that K is totally real. We run the construction on Sun's curve over $\mathbb{Q}(\sqrt{3})$ and on three further curves $y^2 = x^3 - Ax$, over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$, as he runs it for $\mathbb{Q}(\sqrt{3})$ on the curve [60, (14.1)] over $\mathbb{Q}(\sqrt{2})$. The curves differ only in the facts about the curve proved in Section 2 and in the prime pattern they need (Theorems 4.1 and 4.3).

Our main step is the height bound over every totally real field not containing $\sqrt{3}$ (Theorem 1.6), and, with a second tube prime, over the fields containing $\sqrt{3}$ (Theorem 10.2). For $\mathbb{Q}(\sqrt{3})$ Sun adds a second prime of another kind [60, (14.8)]. We follow Sun's proof over real quadratic fields [60, §§5–8], which carries the method of [44, §4] from $\mathbb{Q}$. A point z of the tube gives an abelian surface with quaternionic multiplication, whose 3-adic representation, once a sign cocycle is split by a scalar cochain, is shown to be modular and compared with the Jacobian of a Shimura curve of level bounded by a power of the odd-contact primes of z. As in his proof, the tube is what makes this work, here over every totally real field not containing $\sqrt{3}$. On it the residual representation is induced from a character of the CM extension $K\big(\sqrt{-g_q(z)}\big)$ [60, Lemmas 8.3 and 8.4], hence modular by automorphic induction,

so Gee's lifting theorem [21] applies over any totally real K. The tube prime also gives a supercuspidal local component, so the comparison can be made on a Shimura curve over K in every degree [9]. The arithmetic of K enters only through the scalar cochain, which we construct with at most $d_2(K)$ auxiliary primes, $d_2(K)$ being the Leopoldt defect of K at 2 (Proposition 3.5). The scalar cochain over K and the comparison in every degree are what the proof needs beyond Sun's.

Results. Let (F, A) be one of the four pairs

$$(\mathbb{Q}(\sqrt{3}), (4+\sqrt{3})^2), \quad (\mathbb{Q}(\sqrt{2}), (3+6\sqrt{2})^2), \quad (\mathbb{Q}(\sqrt{2}), 1+2\sqrt{2}), \quad (\mathbb{Q}(\sqrt{17}), \tfrac{1}{2}(11-7\sqrt{17})),$$

write $F = \mathbb{Q}(\sqrt{d})$, so that d is 3, 2, 2 and 17, and let E be the elliptic curve

$$E\colon y^2 = x^3 - Ax \tag{1.1}$$

over F. We call E the *first*, *second*, *third* or *fourth index curve*; the first is the curve of Sun's construction [60, (1.1)]. For the first two, $A = a^2$ with $a = 4+\sqrt{3}$, respectively $a = 3+6\sqrt{2}$, and $E[2] \subseteq E(F)$; for the last two, A is not a square in F, and $(0,0)$ is the only point of order two in $E(F)$. For a totally real number field K with $\sqrt{d} \notin K$ put $L = KF$. We consider three conditions:

(I1) $\operatorname{rank} E(L) = 1$;
(I2) $E(L)_{\mathrm{tors}} \subseteq E[2]$;
(I3) $2E(L) \subseteq E(F)$.

For the first two curves (I2) says that $E(L)_{\mathrm{tors}} = E[2]$. Condition (I3) follows from (I1) and (I2) when L/F is Galois, in particular when $K/\mathbb{Q}$ is Galois (Lemma 2.7).

Theorem 1.1. *Let E be one of the index curves, and let K be a totally real number field with $\sqrt{d} \notin K$, for which (I1), (I2) and (I3) hold. Then there is a polynomial $\mathbf{F} \in \mathbb{Z}[X, Y_1, \dots, Y_{25}]$ such that, for every $x \in K$,*

$$x \in \mathbb{Z} \iff \mathbf{F}(x, y_1, \dots, y_{25}) = 0 \text{ for some } y_1, \dots, y_{25} \in K.$$

In particular $\mathbb{Z}$ is Diophantine in K.

For each K and index curve the polynomial $\mathbf{F}$ exists, but the proof does not compute it. It depends on the integer M of (F4) (Section 7.1), which is chosen in terms of constants that are only shown to exist, among them the constant H of Theorem 1.6 (of Theorem 10.2 when $\sqrt{3} \in K$), which depends on a finite set of parameters with complex multiplication that the proof does not determine.

Theorem 1.2. (a) *For the first index curve, conditions (I1), (I2) and (I3) hold for $K = \mathbb{Q}(\sqrt{2m})$ and for $K = \mathbb{Q}(\sqrt{6m})$, where $m \geq 1$ is any squarefree integer such that every prime factor $p \neq 13$ of m satisfies $p \equiv \pm 5 \pmod{12}$ and $\left(\frac{p}{13}\right) = -1$.*

(b) *For the second index curve, they hold for $K = \mathbb{Q}(\sqrt{D})$ and for $K = \mathbb{Q}(\sqrt{2D})$, where $D \neq 3$ is any positive squarefree integer with $D \equiv \pm 3 \pmod 8$ whose prime factors other than 7 are all congruent to 3, 5, 13, 19, 27 or 45 modulo 56.*

(c) *For the third index curve, they hold for $K = \mathbb{Q}(\sqrt{D})$ and for $K = \mathbb{Q}(\sqrt{2D})$, where D is any positive squarefree integer with $7 \mid D$ and $D \equiv \pm 1 \pmod 8$, each of whose prime factors $p \neq 7$ is congruent to 3, 5, 13, 19, 27 or 45 modulo 56, or is congruent to 1 modulo 8 with $1 + 2\sqrt{2}$ a nonsquare modulo both primes of $\mathbb{Q}(\sqrt{2})$ above p.*

(d) *They hold for the fields K of Table 1, each for the index curve of its row.*
Hence $\mathbb{Z}$ is Diophantine in each of these fields, with 25 unknowns.

TABLE 1. The fields of Theorem 1.2(d)

K	$[K:\mathbb{Q}]$	Curve	$L = KF$	Proposition
the cyclic cubic fields of conductor 9, 13, 19 and 37	3	first	$K(\sqrt{3})$	12.7
$\mathbb{Q}(\zeta_{11})^+$	5	first	$K(\sqrt{3})$	12.7
$\mathbb{Q}(\zeta_{16})^+$	4	first	$\mathbb{Q}(\zeta_{48})^+$	12.7
$\mathbb{Q}(\sqrt{3(2+\sqrt{2})})$	4	first	$\mathbb{Q}(\zeta_{48})^+$	12.23(a)
$\mathbb{Q}(\zeta_{32})^+$	8	first	$\mathbb{Q}(\zeta_{96})^+$	12.7
$\mathbb{Q}(\sqrt{3(2+\sqrt{2+\sqrt{2}})})$	8	first	$\mathbb{Q}(\zeta_{96})^+$	12.23(a)
$\mathbb{Q}(\sqrt{3})$	2	second	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	12.14
$\mathbb{Q}(\sqrt{D})$, for 77 integers $D \le 10500$	2	third	$\mathbb{Q}(\sqrt{2},\sqrt{D})$	12.20
$\mathbb{Q}(\sqrt{2D})$, for the same D	2	third	$\mathbb{Q}(\sqrt{2},\sqrt{D})$	12.23(c)
$\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{51})$, $\mathbb{Q}(\sqrt{3},\sqrt{34})$, $\mathbb{Q}(\sqrt{6},\sqrt{34})$	4	fourth	$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{17})$	12.21

In (a), $m = 1$ gives $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{6})$, in which $\mathbb{Z}$ is Diophantine by [60, Theorems 1.2 and 1.4], and Corollary 12.6 records this case with explicit tube primes. For $m = 13$ the fields are $\mathbb{Q}(\sqrt{26})$ and $\mathbb{Q}(\sqrt{78})$. The primes $p \neq 13$ allowed in m are those inert in both $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{13})$, a set of primes of density $1/4$. The five least D of (b) are 5, 13, 19, 21 and 35, and the seven least of (c) are 7, 105, 273, 399, 455, 665 and $791 = 7 \cdot 113$. A prime $p \neq 3$ congruent to 3, 5, 13, 19, 27 or 45 modulo 56 is one of the D of (b), and $21p$ is one of those of (c), so both sets are infinite, by Dirichlet's theorem. Some fields $\mathbb{Q}(\sqrt{2D})$ of (b) are also in (a), such as $\mathbb{Q}(\sqrt{10})$ and $\mathbb{Q}(\sqrt{26})$. Infinitely many are not, the least being $\mathbb{Q}(\sqrt{118})$ (Section 12.8). Three fields of Table 1 contain $\sqrt{3}$: $\mathbb{Q}(\sqrt{3})$, in which $\mathbb{Z}$ is Diophantine by [60, Theorem 1.3], $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}(\sqrt{3},\sqrt{34})$. Theorem 1.1 covers them through Section 10.

Table 1 lists the single fields for which the descents of Section 12 close. The cyclic cubic fields of conductor below 50 have conductors 7, 9, 13, 19, 31, 37 and 43. For 9, 13, 19 and 37 the 2-Selmer group of E over L has dimension 3 and is spanned by the images of $E[2]$ and of Sun's point P_0 (Proposition 2.6), so $\operatorname{rank} E(L) = 1$. For 7, 31 and 43 it has dimension 5, and a 2-descent does not decide the rank. Deciding it would need a further step, such as a search for points or the Cassels–Tate pairing on the Selmer group. In (b) and (c) the conditions on D are ones under which the 2-isogeny descents of the twists show rank 0.

Theorem 1.3. *For $k \ge 2$ let $K_{2^k} = \mathbb{Q}(\zeta_{2^k})^+$, and for $k \ge 3$ let $K'_{2^k} = \mathbb{Q}(\sqrt{3}\,(\zeta_{2^k} + \zeta_{2^k}^{-1}))$. These fields are totally real and cyclic of degree 2^{k-2} over $\mathbb{Q}$, and $\sqrt{3}$ lies in none of them. For the first index curve, conditions (I1), (I2) and (I3) hold for $K = K_{2^k}$ for every $k \ge 2$ and for $K = K'_{2^k}$ for every $k \ge 3$. Hence $\mathbb{Z}$ is Diophantine in each of these fields, with 25 unknowns.*

The fields K_{2^k} are the layers of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, and the fields $L_{2^k} = K_{2^k}F = \mathbb{Q}(\zeta_{3\cdot 2^k})^+$ those of the cyclotomic $\mathbb{Z}_2$-extension of F; so E has rank one over every layer of the latter. For $k = 2$ and $k = 3$ the fields are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ and $K'_8 = \mathbb{Q}(\sqrt{6})$, in which $\mathbb{Z}$ is already known to be Diophantine (Remark 1.5 and Corollary 12.6); for $k = 4, 5$ they are $\mathbb{Q}(\zeta_{16})^+$, $\mathbb{Q}(\zeta_{32})^+$ and the two cyclic fields of degrees 4 and 8 of Table 1. Section 13 proves

that the rank does not grow from $L_{2^{k-1}}$ to L_{2^k} when $k \geq 5$, with the relative Selmer groups of Mazur and Rubin [40] and a computation at the prime above 2.

Corollary 1.4. *For each field K of Theorems 1.2 and 1.3, there is no algorithm that decides, for an arbitrary polynomial $f \in \mathbb{Z}[X_1, \ldots, X_k]$, whether f has a zero in K^k.*

Proof. By Theorems 1.2, 1.3 and 1.1, $\mathbb{Z}$ is Diophantine in K; as K has a real embedding, the reduction recalled at the start of this introduction gives the corollary. □

Remark 1.5. Theorem 1.1 also applies to $K = \mathbb{Q}$, where $L = F$ and the three conditions are Proposition 2.6 for the first curve, Proposition 2.13 for the second and Propositions 2.16 and 2.17 for the third and fourth; this case recovers the theorem that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$, and it is the case $k = 2$ of Theorem 1.3. For this case [31] gives a direct proof. Theorem 1.1 does not apply, with a given curve, to fields that contain its field F, for which $L = K$; so no index curve applies to a field that contains $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{17}$. For fields that contain $\sqrt{3}$ the tube of Section 3 needs a second prime, which Section 10 adds.

The height bound. The height bound behind Theorem 1.1 holds over every totally real field not containing $\sqrt{3}$, and we state it in that generality; over fields containing $\sqrt{3}$ it holds on a smaller tube (Theorem 10.2). Let K be a totally real number field of degree n_K, and let h be the absolute logarithmic Weil height. For a prime $q \geq 7$, Section 3.1 defines, following Sun [60, (1.3)–(1.7)], a polynomial $g_q \in \mathbb{Q}[z]$ of degree 4 and a set $\mathcal{C}_q \subset \mathbf{P}^1(\mathbb{Q})$ consisting of ∞ and six finite *contacts* $\gamma_1, \ldots, \gamma_6$.

For a prime $\mathfrak{P}$ of K and $z \in K \setminus \mathcal{C}_q$ we say that z has *positive odd contact* with γ_i at $\mathfrak{P}$ if $v_{\mathfrak{P}}(z - \gamma_i)$ is positive and odd, and with ∞ if $v_{\mathfrak{P}}(1/z)$ is positive and odd. Let Σ be a finite set of primes of K containing every prime above a rational prime $p \leq 324$ (as in [60, §1]), every prime above q, and every prime at which a nonzero finite contact, or the difference of two distinct finite contacts, has nonzero valuation. For $z \in K \setminus \mathcal{C}_q$ put

$$\mathfrak{N}_\Sigma(z) = \prod_{\mathfrak{P}} N\mathfrak{P},$$

the product over the primes $\mathfrak{P} \notin \Sigma$ at which z has positive odd contact with a point of $\mathcal{C}_q$ (an empty product is 1). For a prime $\mathfrak{q}$ of K above q, the *positive tube* is

$$\mathcal{D} = \{z \in K : \ v_{\mathfrak{q}}(z - 1) \geq 1 \text{ and } g_q(z) \text{ is totally positive}\}.$$

Theorem 1.6. *Let $q \equiv 7 \pmod{12}$ be a prime, let $\mathfrak{q}$ be a prime of K above q that is unramified over q and has odd residue degree, and let Σ, $\mathfrak{N}_\Sigma$ and $\mathcal{D}$ be as above. Then $\mathcal{D} \cap \mathcal{C}_q = \emptyset$, and there are constants $H > 0$ and $\kappa > 0$ such that*

$$h(z) \leq H\, \mathfrak{N}_\Sigma(z)^\kappa \qquad \text{for every } z \in \mathcal{D}.$$

For $K = \mathbb{Q}(\sqrt{2})$ and $q = 367$ this is the height bound of [60, Theorem 1.7] on the positive tube, and for $K = \mathbb{Q}(\sqrt{6})$ and $q = 331$ that of [60, Lemma 15.4]. Primes q and $\mathfrak{q}$ as in the theorem exist when $\sqrt{3} \notin K$, by Lemma 3.1, and only then: a prime $q \equiv 7 \pmod{12}$ is inert in $\mathbb{Q}(\sqrt{3})$, so if $\sqrt{3} \in K$ every prime of K above q has even residue degree. When $\sqrt{3} \in K$ we add a second prime to the tube (Section 10).

The proof in outline. Let K be as in Theorem 1.1, for one of the index curves. By (I1)–(I3), $2E(L)$ is infinite cyclic, generated by a point $P \in E(F)$ (Lemma 2.8), so the points of $2E(L)$ are the multiples $[n]P$ with $n \in \mathbb{Z}$; this is how the definition quantifies over integers. For $x \in K$ put $\beta = 3 + \delta(x^3 + x)$ with $\delta = \pm 1$; since K is totally real, $\beta \in \mathbb{Z}$ forces $x \in \mathbb{Z}$ (Lemma 6.1).

(1) *The certificate* (Section 7). The definition asks for nine points of $2E(L)$, each given by the coordinates of a point of $E(L)$ that doubles to it, and for two elements B_0, B_1 of K built from them and from β. It requires that neither B_0 nor B_1 has a pole of odd order outside a fixed finite set of primes, a condition enforced by a predicate on congruent-number twists (Section 5).

(2) *Local tests* (Section 6). At a prime where an auxiliary parameter has positive odd contact with a point of $\mathcal{C}_q$, the element B_j has a pole of odd order unless a list of local tests holds there. Through the formal logarithm of E, as in Poonen's reading of indices from coordinates [50], the tests say that β is congruent to an index n_1 to high order and that an integer built from the indices is divisible to high order.

(3) *Soundness* (Section 8). Theorem 1.6 (Theorem 10.2 when $\sqrt{3} \in K$) bounds the height of the parameter by a power of the product of its odd-contact primes, and a theorem of von Buhren bounds the indices by heights (Lemma 2.10). The two bounds are incompatible with a solution unless $\beta = n_1$, which is an integer.

(4) *Completeness* (Section 9). For $x \in \mathbb{Z}$ the indices are chosen by the Chinese remainder theorem, with primes in a quadratic pattern (Theorems 4.1 and 4.3). Then all the points lie in $E(F)$, B_0 and B_1 are rational, and the predicate holds by [31, Theorem 1.2] (Lemma 5.3).

Earlier work. Denef proved that $\mathbb{Z}$ is Diophantine in the ring of integers of every totally real number field [14], and Denef and Lipshitz extended this to quadratic extensions of totally real fields [15]. Denef suggested elliptic curves of rank one in place of Pell's equation [14]. Poonen proved that if $F \subseteq K$ are number fields and an elliptic curve over F has rank one over both F and K, then the ring of integers of F is Diophantine over that of K [50], and Cornelissen, Pheidas and Zahidi gave a related criterion [10]; see Shlapentokh's book [55] for the earlier theory. Mazur and Rubin deduced from this approach, assuming finiteness of Shafarevich–Tate groups, that Hilbert's tenth problem has a negative answer over the ring of integers of every number field [39]. Zywina proved that for every quadratic extension L/K of number fields there are infinitely many elliptic curves E/K with $\operatorname{rank} E(K) = \operatorname{rank} E(L) = 1$ [67, Theorem 1.2].

For fields, Robinson defined $\mathbb{Z}$ in $\mathbb{Q}$ by a first-order formula [53], Poonen by a $\forall\exists$-formula [51], and Koenigsmann by a universal one [34]; Park defined the ring of integers of every number field by a universal formula [46]. Over $\mathbb{Q}$ the approach through rank-one curves and local divisibility conditions goes back to Pheidas [49], whose work anticipates the predicate excluding poles of odd order [68, §1], [36, §1.2]; OpenAI's proof follows that strategy. Kozachinskiy, Pasten and Vidaux proved that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ if Shafarevich–Tate groups of elliptic curves over $\mathbb{Q}$ have finite 2-primary part and the *abc* conjecture and Dickson's conjecture hold [36, Theorem 1.1]. Over other fields, Pasten and Vidaux proved that $\mathbb{Z}$ is Diophantine in a number field K if the *abc* conjecture holds over K and some elliptic curve over $\mathbb{Q}$ has $0 < \operatorname{rank} E(\mathbb{Q}) = \operatorname{rank} E(K)$ [47, Theorem 1.1], and that this holds for every quadratic field if the *abc* conjecture holds over it [47, Corollary 1.2].

Plan. Section 2 proves what the construction needs about the four index curves, with the facts special to the second in Section 2.6 and to the third and fourth in Section 2.7. Sections 6–11 read the curve only through (E1)–(E3), Lemmas 2.9 and 2.10 and the prime patterns of Theorems 4.1 and 4.3. Section 3 proves Theorem 1.6 and does not use the index curves. The scalar cochain it needs is constructed in Appendix A. Section 4 proves the prime patterns, with two steps in Appendix C, and Section 5 the properties of the pole predicate.

Section 6 collects the local lemmas, Section 7 writes the certificate, and Sections 8 and 9 prove that it holds at $x \in K$ exactly when $x \in \mathbb{Z}$. Section 10 adds a second tube prime for fields containing $\sqrt{3}$, and Section 11 deduces Theorem 1.1, with the count of unknowns in Appendix B. Section 12 proves Theorem 1.2, from Section 2 and 2-isogeny descents over F for the quadratic and biquadratic fields, and by a complete 2-descent over L for the others. There Lemma 12.22 carries the conditions to the fields with the same L. Section 13 proves Theorem 1.3.

Computations. The proofs use exact computations, in PARI/GP [45] and in Python with SymPy: the 2-descents of Sections 2 and 12, the identities in q and q' of Sections 3 and 10, and a few point counts, discriminants and congruences. The programs are in the deposit [30], whose README matches each statement to its program.

2. The index curves

2.1. **What the proof uses.** Let σ be the nontrivial automorphism of F, $\bar{A} = \sigma(A)$, and $E^\sigma\colon y^2 = x^3 - \bar{A}x$ the conjugate curve; for the first two curves $\bar{a} = \sigma(a)$, so $\bar{A} = \bar{a}^2$. Let $\mathcal{P}$ be the set of rational primes dividing $2d\,\mathrm{N}_{F/\mathbb{Q}}(A)$. For the four curves $\mathrm{N}_{F/\mathbb{Q}}(A)$ is 13^2, 63^2, -7 and $-178 = -2 \cdot 89$, and $\mathcal{P}$ is $\{2,3,13\}$, $\{2,3,7\}$, $\{2,7\}$ and $\{2,17,89\}$; every prime of $\mathcal{P}$ is at most 89. The following properties of F, E and L are proved in this section for each curve; the facts special to the second curve are in Section 2.6, and those special to the third and fourth in Section 2.7.

(E1) F is a real quadratic field and $\sqrt{d} \notin K$, so $L = KF$ is totally real, $[L : K] = 2$ with basis $1, \sqrt{d}$, and the nontrivial element τ of $\mathrm{Gal}(L/K)$ restricts to σ on F; hence $\mathrm{Tr}_{L/K}(u) = \mathrm{Tr}_{F/\mathbb{Q}}(u)$ for $u \in F$.

(E2) $(0,0) \in E(F)$, and $E[2] \subseteq E(F)$ for the first two curves; the discriminant of (1.1) is $64A^3$, so E and E^σ have good reduction at every prime of F not above a prime of $\mathcal{P}$; and (1.1) is minimal at every prime of F (Section 2.2 for the first curve, Lemma 2.11 for the second, Lemma 2.14 for the third and fourth).

(E3) Under (I1)–(I3), $2E(L) = \mathbb{Z}P$ for a point $P \in E(F)$ of infinite order, and $x([n]P)$ is totally positive for $n \neq 0$ (Lemma 2.8).

2.2. **Descent over F.** For the first curve write $\mathcal{O}_F = \mathbb{Z}[\sqrt{3}]$, $\varepsilon = 2 + \sqrt{3}$ and $\lambda = 1 + \sqrt{3}$; then $\bar{a} = 4 - \sqrt{3}$, $\lambda^2 = 2\varepsilon$, $a\bar{a} = 13$ and $\varepsilon a = 11 + 6\sqrt{3}$. The ring $\mathcal{O}_F$ is a principal ideal domain (the Minkowski bound is $\sqrt{3} < 2$), and $\mathcal{O}_F^\times = \{\pm\varepsilon^k\}$, since $u^2 - 3v^2 = -1$ has no solution modulo 3 and $(2,1)$ is the least solution of $u^2 - 3v^2 = 1$. The prime 2 ramifies, $2\mathcal{O}_F = (\lambda)^2$, and $[2] = [\varepsilon]$ in $F^\times/F^{\times 2}$. The prime 13 splits; $\mathfrak{a} = (a)$ is a prime of norm 13, and $F_\mathfrak{a} = \mathbb{Q}_{13}$ with $\sqrt{3} \mapsto -4$, so that $\varepsilon \equiv -2 \equiv 11 \pmod{\mathfrak{a}}$. Modulo 13 we take $\iota \equiv 5$, a square root of -1; then $2\iota \equiv 10 \equiv 6^2$ is a square, and 2 and $\varepsilon \equiv 11$ are not. A prime $p \geq 5$ is inert in F exactly when $p \equiv \pm 5 \pmod{12}$. The equation (1.1) is minimal at every prime of F: it has good reduction outside 2 and 13; its discriminant $64a^6$ has valuation 6 at $\mathfrak{a}$ and 0 at $\sigma\mathfrak{a} = (\bar{a})$, the two primes above 13; and at the prime above 2, where it has valuation 12, no change of variables makes it more integral (a finite search modulo 8). For the second curve $\varepsilon = 1 + \sqrt{2}$ and $\lambda = \sqrt{2}$, and the corresponding facts are in Section 2.6. For the first two curves $\mathcal{O}_F$ is a principal ideal domain, $\mathcal{O}_F^\times = \{\pm\varepsilon^k\}$, and $2\mathcal{O}_F = (\lambda)^2$ with $v_\lambda(2) = 2$.

For $c \in F^\times$ and an extension M of F let

$$E_c\colon y^2 = x^3 - c^2x, \qquad E_c'\colon y^2 = x^3 + 4c^2x, \qquad \phi_c(x,y) = \Big(\frac{y^2}{x^2}, \frac{y(-c^2 - x^2)}{x^2}\Big),$$

so $E = E_a$ for the first two curves, and $\phi_c\colon E_c \to E_c'$ is the 2-isogeny with kernel $\{O, (0,0)\}$ [56, Example III.4.5]; let $\hat{\phi}_c$ be its dual. By [56, Proposition X.4.9] there are injective homomorphisms

$$\alpha_c'\colon E_c'(M)/\phi_c(E_c(M)) \to M^\times/M^{\times 2}, \qquad \alpha_c\colon E_c(M)/\hat{\phi}_c(E_c'(M)) \to M^\times/M^{\times 2},$$

given by $(x,y) \mapsto [x]$ for $x \neq 0$, with $\alpha_c'(0,0) = [4c^2] = 1$ and $\alpha_c(0,0) = [-c^2] = [-1]$ (the second map is the first one for E_c', composed with the isomorphism $(x,y) \mapsto (4x, 8y)$ of E_c onto $y^2 = x^3 - 16c^2x$). A class e lies in the image of α_c', respectively α_c, exactly when

$$W^2 = eU^4 + \frac{4c^2}{e}V^4, \qquad \text{respectively} \qquad W^2 = eU^4 - \frac{c^2}{e}V^4, \tag{2.1}$$

has a solution over M with $(U,V) \neq (0,0)$ [56, Proposition X.4.9]. We write $\operatorname{Im}\alpha_{c,v}$, $\operatorname{Im}\alpha_{c,v}'$ for the images over a completion $M = F_v$.

Lemma 2.1. *Let M be a field of characteristic zero containing F, and $c \in F^\times$. Then*

$$|E_c(M)/2E_c(M)| = |\operatorname{Im}\alpha_c| \cdot |\operatorname{Im}\alpha_c'|.$$

In particular, if M is a number field, $2^{\operatorname{rank} E_c(M)} = |\operatorname{Im}\alpha_c| \cdot |\operatorname{Im}\alpha_c'|/4$.

Proof. Since $\hat{\phi}_c \circ \phi_c = [2]$, the sequence

$$0 \to \frac{E_c'(M)[\hat{\phi}_c]}{\phi_c(E_c(M)[2])} \to \frac{E_c'(M)}{\phi_c(E_c(M))} \xrightarrow{\hat{\phi}_c} \frac{E_c(M)}{2E_c(M)} \to \frac{E_c(M)}{\hat{\phi}_c(E_c'(M))} \to 0$$

is exact: a point R maps to zero exactly when $\hat{\phi}_c(R) = \hat{\phi}_c(\phi_c(Q))$ for some Q, that is $R \in \phi_c(E_c(M)) + E_c'(M)[\hat{\phi}_c]$. The first term vanishes, because $\phi_c(c,0) = (0,0)$ and $E_c'[\hat{\phi}_c] = \phi_c(E_c[2]) = \{O, (0,0)\}$. The maps α_c, α_c' are injective, which gives the first formula. Over a number field $E_c(M)[2] = E_c[2]$ has order 4, so $|E_c(M)/2E_c(M)| = 2^{\operatorname{rank} E_c(M)+2}$. □

Lemma 2.2 (Support)**.** *Let $c \in F^\times$ and let v be a finite prime of F with either $v \nmid 2$ and $v(c)$ even, or $v = (\lambda)$ and $v_\lambda(c) \in \{0,2\}$. Then every class in $\operatorname{Im}\alpha_c$ and in $\operatorname{Im}\alpha_c'$, over F or over F_v, has even valuation at v.*

Proof. For a point (x,y) with $x \neq 0$ on $y^2 = x(x^2+b)$ with $b \in \{-c^2, 4c^2\}$, the valuation $v(b)$ is divisible by 4 ($2v(c)$ if $v \nmid 2$; 0, 4 or 8 at λ, as $v_\lambda(2) = 2$). If $v(x)$ were odd, then $2v(x) \neq v(b)$, so $v(x^2+b) = \min(2v(x), v(b))$ is even and $v(y^2) = v(x) + v(x^2+b)$ would be odd. The torsion classes 1 and $[-c^2]$ have even valuation. □

Since $\mathcal{O}_F$ is a principal ideal domain with units $\pm\varepsilon^{\mathbb{Z}}$, Lemma 2.2 places $\operatorname{Im}\alpha_c$ and $\operatorname{Im}\alpha_c'$ in the subgroup of $F^\times/F^{\times 2}$ generated by -1, ε and generators of the odd primes dividing c to an odd power, whenever $v_\lambda(c) \in \{0,2\}$.

Lemma 2.3 (Odd additive places)**.** *Let v be a prime of F not above 2 such that $v(c)$ is odd. If -1 is a square in F_v, say $\iota^2 = -1$, then $\operatorname{Im}\alpha_{c,v} = \langle [c] \rangle$ and $\operatorname{Im}\alpha_{c,v}' = \langle [2\iota c] \rangle$ in $F_v^\times/F_v^{\times 2}$. If -1 is not a square in F_v, then $\operatorname{Im}\alpha_{c,v} = F_v^\times/F_v^{\times 2}$ and $\operatorname{Im}\alpha_{c,v}' = \{1\}$.*

Proof. If $T = (e_1, 0)$ is a point of order two on $y^2 = (x-e_1)(x-e_2)(x-e_3)$ and $T = 2R$ with $R = (x_0, y_0)$ over a field of characteristic not 2, then $y_0 \neq 0$, the tangent line $y = \mu(x-x_0)+y_0$ at R meets the curve again at $-2R = T$, so $(x-e_1)(x-e_2)(x-e_3) - (\mu(x-x_0)+y_0)^2 = (x-x_0)^2(x-e_1)$, and evaluating at $x = e_2 \neq x_0$ shows that $e_1 - e_2 = \left((\mu(e_2-x_0)+y_0)/(e_2-x_0)\right)^2$ is a square; likewise $e_1 - e_3$. The roots are $0, \pm c$ for E_c and $0, \pm 2\iota c$ for E_c', all in F_v; the differences $e_1 - e_2$ for the three choices of e_1 are $\{-c, c\}$ (for $e_1 = 0$), $\{c, 2c\}$, $\{-c, -2c\}$ on

E_c and $\{\mp 2\iota c\}$, $\{2\iota c, 4\iota c\}$, $\{-2\iota c, -4\iota c\}$ on E'_c, all of odd valuation. So no point of order two lies in $2E_c(F_v)$ or $2E'_c(F_v)$, and $E_c(F_v)[2]$ injects into $E_c(F_v)/2E_c(F_v)$. For an abelian group G with $G/2G$ and $G[2]$ finite put $\chi(G) = |G/2G|/|G[2]|$; it is multiplicative in short exact sequences and equals 1 on finite groups. The group $E_c(F_v)$ has a subgroup of finite index isomorphic to the additive group of the ring of integers of F_v [56, Proposition VII.6.3], which is uniquely 2-divisible, so $\chi(E_c(F_v)) = 1$ and $|E_c(F_v)/2E_c(F_v)| = 4$. Hence $E_c(F_v)/2E_c(F_v)$ is the image of $E_c[2]$, and $\operatorname{Im}\alpha_{c,v} = \alpha_c(E_c[2]) = \{1, [-c^2], [c], [-c]\} = \langle [c]\rangle$ since -1 is a square. The same argument for E'_c gives $\operatorname{Im}\alpha'_{c,v} = \{1, [4c^2], [2\iota c], [-2\iota c]\} = \langle [2\iota c]\rangle$. If -1 is not a square in F_v, the computation of χ still gives $|E_c(F_v)/2E_c(F_v)| = 4$, so $|\operatorname{Im}\alpha_{c,v}|\cdot|\operatorname{Im}\alpha'_{c,v}| = 4$ by Lemma 2.1; and $\operatorname{Im}\alpha_{c,v}$ contains $\alpha_c(E_c[2]) = \{1, [-c^2], [c], [-c]\} = \langle [-1], [c]\rangle$, which is all of $F_v^\times/F_v^{\times 2}$, since $[-1]$ is the nontrivial unit class and $[c]$ has odd valuation. Hence $\operatorname{Im}\alpha'_{c,v} = \{1\}$. □

2.3. **The conditions over F.** Lemma 2.4 and Proposition 2.6 are about the first curve; the corresponding facts for the second are Lemma 2.12 and Proposition 2.13, and for the third and fourth Lemma 2.15 and Propositions 2.16 and 2.17.

Lemma 2.4. *Let E be the first index curve, and let $L \supseteq F$ be a totally real number field.*

(a) *If every element of $F \cap L^{\times 2}$ has its norm to $\mathbb{Q}$ in $\mathbb{Q}^{\times 2}$, then $E(L)$ has no point of order four and none of order three.*

(b) *Let $p \equiv 3 \pmod 4$ be a prime that splits in F, and let $\mathfrak{P}$ be a prime of L above p, with residue field $\mathbb{F}_{p^k}$. Then E has good reduction at $\mathfrak{P}$, the reduction has $N_k(p) = p^k + 1 - (i\sqrt{p})^k - (-i\sqrt{p})^k$ points over $\mathbb{F}_{p^k}$, and $E(L)[\ell]$ injects into it for every prime $\ell \neq p$.*

(c) *Suppose that L is as in (a) and has primes as in (b) above two primes $p_1 \neq p_2$, with residue fields $\mathbb{F}_{p_1^{k_1}}$ and $\mathbb{F}_{p_2^{k_2}}$, such that no prime $\ell \geq 5$ divides both $p_1 N_{k_1}(p_1)$ and $p_2 N_{k_2}(p_2)$. Then $E(L)_{\mathrm{tors}} = E[2]$.*

(d) *If L is as in (a) and $[L : F] \leq 2$, then $E(L)_{\mathrm{tors}} = E[2]$. In particular $E(F)_{\mathrm{tors}} = E[2]$.*

Proof. (a) By the first paragraph of the proof of Lemma 2.3, a point $T = (e_1, 0)$ of E is in $2E(L)$ only if $e_1 - e_2$ and $e_1 - e_3$ are squares in L. For $T = (0, 0)$ this needs $-a$ and a to be squares, so -1 would be a square in the real field L. For $T = (-a, 0)$ it needs $-a$ to be a square, but $-a < 0$ at every real place. For $T = (a, 0)$ it needs a to be a square in L, which the hypothesis excludes, as $\mathrm{N}_{F/\mathbb{Q}}(a) = 13$. As $E[2] \subseteq E(F)$, $E(L)$ has no point of order four. A point $R = (x, y)$ with $y \neq 0$ on E has order three exactly when $x(2R) = x(R)$, that is $3x^4 - 6a^2x^2 - a^4 = 0$. So $x^2 = a^2 r$ with $r = 1 \pm \frac{2}{3}\sqrt{3} \in F$. If $x \in L$, then $r = (x/a)^2 \in F \cap L^{\times 2}$, which the hypothesis excludes, as $\mathrm{N}_{F/\mathbb{Q}}(r) = -\frac{1}{3}$.

(b) As $p \equiv 3 \pmod 4$ and p splits in F, p is not 2, 3 or 13, so E has good reduction at $\mathfrak{P}$ by (E2). At the prime of F below $\mathfrak{P}$ the reduction is $y^2 = x^3 - s^2 x$ over $\mathbb{F}_p$ with $s \neq 0$, which has $p+1$ points, as -1 is not a square modulo p. So its Frobenius has trace 0 and eigenvalues $\pm i\sqrt{p}$, which gives the count over $\mathbb{F}_{p^k}$. The injection is [56, Proposition VII.3.1(b)], over the completion of L at $\mathfrak{P}$.

(c) By (a), the 2-primary part of $E(L)_{\mathrm{tors}}$ is $E[2]$, and $E(L)[3] = 0$. If $E(L)[\ell] \neq 0$ for a prime $\ell \geq 5$, then by (b) ℓ divides $N_{k_j}(p_j)$ when $\ell \neq p_j$, so it divides $p_j N_{k_j}(p_j)$ for $j = 1, 2$, which is excluded.

(d) The primes 11 and 23 are congruent to 3 modulo 4 and split in F, as $3 \equiv 5^2 \pmod{11}$ and $3 \equiv 7^2 \pmod{23}$. As $[L : F] \leq 2$, primes of L above them have residue degree 1 or 2,

and $N_1(p) = p+1$, $N_2(p) = (p+1)^2$. So the prime factors of $11N_{k_1}(11)$ are among 2, 3 and 11, those of $23N_{k_2}(23)$ among 2, 3 and 23, and (c) applies. □

Lemma 2.5. *Let E be one of the index curves, let $L \supseteq F$ be a totally real number field, and let ℓ be an odd prime. If $E(L)[\ell] \neq 0$, then $L(i)$ contains a root of unity of order ℓ.*

Proof. The curve E has complex multiplication by $\mathbb{Z}[i]$, with $[i](x,y) = (-x, iy)$ defined over $F(i)$. Let $P \in E(L)$ have order ℓ, and let c be complex conjugation, acting on $E(\overline{\mathbb{Q}}) \subseteq E(\mathbb{C})$; it fixes P, as L is totally real, and $c([\alpha]Q) = [\bar{\alpha}]c(Q)$ for $\alpha \in \mathbb{Z}[i]$. So the annihilator of P in $\mathbb{Z}[i]$ is a proper ideal containing ℓ and stable under conjugation. As ℓ is odd, the primes of $\mathbb{Z}[i]$ above ℓ are $\ell\mathbb{Z}[i]$ or two conjugate primes, so this annihilator is $\ell\mathbb{Z}[i]$, and $\mathbb{Z}[i]P$, of order ℓ^2, is $E[\ell]$. Every element of $\mathrm{Gal}(\overline{\mathbb{Q}}/L(i))$ fixes i and P, hence commutes with $[i]$ and fixes $\mathbb{Z}[i]P = E[\ell]$. By the Galois equivariance of the Weil pairing [56, §III.8], $L(i)$ contains a root of unity of order ℓ. □

Proposition 2.6 (Sun [60, Theorem 1.6 and Lemma 2.2])**.** $\operatorname{rank} E(F) = 1$ *and* $E(F)_{\mathrm{tors}} = E[2]$*; the point*

$$P_0 = (244 + 139\sqrt{3},\ 5334 + 3082\sqrt{3})$$

lies in $E(F)$ and has infinite order.

Proof. Direct expansion shows $P_0 \in E(F)$. The only odd prime dividing a is $\mathfrak{a}$, and $v_\lambda(a) = 0$, so by Lemma 2.2 both images for $c = a$ lie in $\langle -1, \varepsilon, a\rangle$. Lemma 2.3 at $\mathfrak{a}$ (where -1 and 2ι are squares) gives $\operatorname{Im}\alpha_{a,\mathfrak{a}} = \operatorname{Im}\alpha'_{a,\mathfrak{a}} = \langle [a]\rangle$. A class $(-1)^h\varepsilon^i a^j$ has coordinates (j,i) at $\mathfrak{a}$ and $[a]$ has $(1,0)$, so both images lie in $\langle -1, a\rangle$; the image of α'_a is totally positive, so it lies in $\{1, [a]\}$. By Lemma 2.1, $2^{\operatorname{rank} E(F)} \leq 4 \cdot 2/4 = 2$, so $\operatorname{rank} E(F) \leq 1$.

By Lemma 2.4(d), $E(F)_{\mathrm{tors}} = E[2]$. The point P_0 has $y(P_0) \neq 0$, so it is not 2-torsion and has infinite order; $\operatorname{rank} E(F) = 1$. □

Lemma 2.7. *Let K be totally real with $\sqrt{d} \notin K$ and $L = KF$, and suppose (I1) and (I2). If L/F is Galois, in particular if $K/\mathbb{Q}$ is Galois, then (I3) holds.*

Proof. By (I1), $E(L)/E(L)_{\mathrm{tors}} \cong \mathbb{Z}$, and $\mathrm{Gal}(L/F)$ acts on it through a character with values ± 1. A point of $E(F)$ of infinite order (Propositions 2.6, 2.13, 2.16 and 2.17 for the four curves) is fixed, so the character is trivial: $g(Q) - Q \in E(L)_{\mathrm{tors}}$ for every $g \in \mathrm{Gal}(L/F)$ and $Q \in E(L)$, and $E(L)_{\mathrm{tors}} \subseteq E[2]$ by (I2). Then $g(2Q) = 2Q$, so $2Q \in E(L)^{\mathrm{Gal}(L/F)} = E(F)$. If $K/\mathbb{Q}$ is Galois, so is KF/F. □

Lemma 2.8. *Assume (I1)–(I3). Then $2E(L) = \mathbb{Z}P$ for a point $P \in E(F)$ of infinite order, unique up to sign; and for every integer $n \neq 0$ the point $[n]P$ is $2R$ for some $R \in E(L)$, and $x([n]P) \in F$ is positive at both real embeddings of F.*

Proof. Compare [60, Lemma 2.6], where L is biquadratic. By (I2), $2E(L)$ is torsion-free, and by (I1) it has rank one; so it is infinite cyclic, generated by some P, which lies in $E(F)$ by (I3). Then $[n]P = 2[n]R_1$ where $2R_1 = P$. For $R = (x_R, y_R)$ with $2R \neq O$ the duplication formula gives $x(2R) = \left((x_R^2 + A)/(2y_R)\right)^2$, a nonzero square in the totally real field L (it is not 0, since $(0,0)$ is not in $2E(L)$ when $2E(L)$ is torsion-free). Every embedding of F into $\mathbb{R}$ extends to L, so $x([n]P)$ is positive at both real embeddings. □

2.4. **Orders of reductions.** For a Gaussian integer π write $\mathrm{N}(\pi) = \pi\bar{\pi}$. We call π *primary* if $\pi \equiv 1 \pmod{2+2i}$.

Lemma 2.9. *Let $p \equiv 1 \pmod 4$ be a prime, $p \notin \mathcal{P}$, that splits in F, let $\mathfrak{Q}$ be a prime of F above p, and let π be a primary Gaussian prime of norm p. Identify $\mathcal{O}_F/\mathfrak{Q}$ and $\mathbb{Z}[i]/(\pi)$ with $\mathbb{F}_p$, and let $u_\mathfrak{Q} \in \{\pm 1, \pm i\}$ be the unit with $u_\mathfrak{Q} \equiv A^{(p-1)/4} \pmod \pi$. Then E has good reduction at $\mathfrak{Q}$,*

$$\#\tilde{E}(\mathcal{O}_F/\mathfrak{Q}) = \mathrm{N}(\pi - u_\mathfrak{Q}),$$

and $u_\mathfrak{Q} = \pm 1$ exactly when A is a square modulo $\mathfrak{Q}$.

(a) *Let E be the first or second curve, with $(\frac{\mathrm{N}_{F/\mathbb{Q}}(a)}{p}) = -1$. Then the reductions of E at $\mathfrak{Q}$ and at $\sigma\mathfrak{Q}$ have orders $\mathrm{N}(\pi - 1)$ and $\mathrm{N}(\pi + 1)$ in some order. Every prime $p \equiv 1 \pmod{48}$ with $p \equiv 5 \pmod{13}$, for the first curve, or with $p \equiv 3 \pmod 7$, for the second, splits in F and satisfies $(\frac{\mathrm{N}_{F/\mathbb{Q}}(a)}{p}) = -1$.*

(b) *Let E be the third or fourth curve, with $(\frac{\mathrm{N}_{F/\mathbb{Q}}(A)}{p}) = -1$. Then A is a square modulo exactly one of $\mathfrak{Q}$ and $\sigma\mathfrak{Q}$, say $\mathfrak{p}_+$, and the reductions of E at $\mathfrak{p}_+$ and at $\sigma\mathfrak{p}_+$ have orders $\mathrm{N}(\pi - \epsilon)$ and $\mathrm{N}(\pi - \eta i)$ for some $\epsilon, \eta \in \{1, -1\}$.*

Proof. Compare [60, Lemma 10.2]. As p splits in F and $p \notin \mathcal{P}$, E has good reduction at $\mathfrak{Q}$ (E2), and the residue field is $\mathbb{F}_p$; let $D \in \mathbb{Z}$ be prime to p with $D \equiv A \pmod \mathfrak{Q}$. For $p \equiv 1 \pmod 4$ and primary π of norm p, the curve $y^2 = x^3 - Dx$ has $p + 1 - \bar{u}\pi - u\bar{\pi} = \mathrm{N}(\pi - u)$ points over $\mathbb{F}_p$, where u is the quartic residue symbol of D modulo π, so that $u \equiv D^{(p-1)/4} \pmod \pi$ [28, Chapter 18, §4, Theorem 5]; this is the first formula. As $u_\mathfrak{Q}^2 \equiv D^{(p-1)/2} \pmod \pi$, $u_\mathfrak{Q} = \pm 1$ exactly when D is a square modulo p. The residue of A modulo $\sigma\mathfrak{Q}$ is that of $\bar{A}$ modulo $\mathfrak{Q}$, so $u_\mathfrak{Q} u_{\sigma\mathfrak{Q}} \equiv \mathrm{N}_{F/\mathbb{Q}}(A)^{(p-1)/4} \pmod \pi$, whose square is $(\frac{\mathrm{N}_{F/\mathbb{Q}}(A)}{p})$.

(a) Here $A = a^2$, so $u_\mathfrak{Q} = (\frac{a}{\mathfrak{Q}})$, the quadratic residue symbol, and $u_\mathfrak{Q} u_{\sigma\mathfrak{Q}} = (\frac{\mathrm{N}_{F/\mathbb{Q}}(a)}{p}) = -1$; this gives the first statement. For the second, let $p \equiv 1 \pmod{48}$. For the first curve, $(\frac{3}{p}) = (\frac{p}{3}) = 1$, so p splits in $\mathbb{Q}(\sqrt{3})$, and $p \equiv 5 \pmod{13}$ gives $(\frac{13}{p}) = (\frac{p}{13}) = (\frac{5}{13}) = -1$. For the second, $p \equiv 1 \pmod 8$ gives $(\frac{2}{p}) = 1$, so p splits in $\mathbb{Q}(\sqrt{2})$, and as $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 7$, $(\frac{-63}{p}) = (\frac{7}{p}) = (\frac{p}{7}) = (\frac{3}{7}) = -1$, the squares modulo 7 being 1, 2, 4.

(b) Here $(u_\mathfrak{Q} u_{\sigma\mathfrak{Q}})^2 = -1$, so one of $u_\mathfrak{Q}$, $u_{\sigma\mathfrak{Q}}$ is ± 1 and the other is $\pm i$. □

2.5. **Heights of traces of abscissas.** For an elliptic curve over a number field, $\hat{h}$ is its canonical height, and h is the absolute logarithmic Weil height on $\overline{\mathbb{Q}}$.

Lemma 2.10. *Suppose that*

$$A \notin \bar{A}^k F(i)^{\times 4} \qquad (k = 0, 1, 2, 3), \tag{2.2}$$

and let $P \in E(F)$ be a point of infinite order. There are constants $C_1 > 0$ and $C_2 \geq 0$ such that for all nonzero integers $n_1, \dots, n_4$,

$$T = \frac{1}{2}\,\mathrm{Tr}_{F/\mathbb{Q}}\Big(\sum_{k=1}^{4} x([n_k]P)\Big) \quad \textit{satisfies} \quad \max_k n_k^2 \leq C_1 h(T) + C_2.$$

Each index curve satisfies (2.2). Let $\mathfrak{l}$ be $(4 + \sqrt{3})$, $(1 + 2\sqrt{2})$, $(1 + 2\sqrt{2})$, respectively the prime of F above 89 that divides A. It lies above 13, 7, 7, respectively 89, so it is unramified in $F(i)$; $v_\mathfrak{l}(A)$ is 2, 2, 1, respectively 1, and $v_\mathfrak{l}(\bar{A}) = 0$. At a prime of $F(i)$ above $\mathfrak{l}$ every element of $\bar{A}^k F(i)^{\times 4}$ has valuation divisible by 4, and A does not.

Proof. For the first curve this is [60, Lemma 10.1], and for the others it is his lemma with the hypothesis (2.2); the method is that of [69, §A38]. Let $E_0 \colon Y^2 = X^3 - X$, choose $s, \bar{s} \in \overline{\mathbb{Q}}$

with $s^4 = A$ and $\bar{s}^4 = \bar{A}$, and let $M = F(i, s, \bar{s})$. The maps $(x, y) \mapsto (x/s^2, y/s^3)$ and $(x, y) \mapsto (x/\bar{s}^2, y/\bar{s}^3)$ are isomorphisms $E \to E_0$ and $E^\sigma \to E_0$ over M; let $Q_1, Q_2 \in E_0(M)$ be the images of P and of $P^\sigma \in E^\sigma(F)$. Both have infinite order.

Q_1 and Q_2 are independent over $\mathrm{End}(E_0) = \mathbb{Z}[i]$ modulo torsion. As $F(i)$ contains the fourth roots of unity, Kummer theory and (2.2) give $s \notin F(i, \bar{s})$; so there is an automorphism g of $M/F(i, \bar{s})$ with $g(s) = i^j s$ for some $j \in \{1, 2, 3\}$. It fixes Q_2, and $g(Q_1) = [i^j]Q_1$, because $[i](X, Y) = (-X, iY)$ on E_0; and it commutes with $\mathbb{Z}[i]$, which is defined over $\mathbb{Q}(i)$. If $\mu Q_1 + \nu Q_2$ is torsion with $\mu, \nu \in \mathbb{Z}[i]$, applying g and subtracting shows that $(i^j - 1)\mu Q_1$ is torsion, so $\mu = 0$, and then $\nu = 0$.

The function. On $\mathcal{E} = E_0^8$ with coordinates $(U_1, \dots, U_4, V_1, \dots, V_4)$ let

$$\Phi = \frac{s^2}{2} \sum_{k=1}^{4} X(U_k) + \frac{\bar{s}^2}{2} \sum_{k=1}^{4} X(V_k),$$

a rational map $\mathcal{E} \to \mathbf{P}^1$, and $\mathbf{q} = ([n_1]Q_1, \dots, [n_4]Q_1, [n_1]Q_2, \dots, [n_4]Q_2)$. Then $\Phi(\mathbf{q}) = \frac{1}{2}\sum_k (x([n_k]P) + x([n_k]P)^\sigma) = T$, and $\mathbf{q}$ lies in the domain of Φ since no coordinate is O.

No positive-dimensional translate. Suppose that Φ is constant on $\mathbf{q} + B$ for an abelian subvariety $B \neq 0$ of $\mathcal{E}$. Since $\mathcal{E}$ is a power of E_0, B contains the image of a nonzero homomorphism $E_0 \to \mathcal{E}$, $U \mapsto (\mu_1 U, \dots, \mu_4 U, \nu_1 U, \dots, \nu_4 U)$ with $\mu_k, \nu_k \in \mathbb{Z}[i]$; so $U \mapsto \Phi(\mathbf{q} + (\mu_k U, \nu_k U)_k)$ is constant on E_0. Suppose some $\mu_k \neq 0$, and let U_0 satisfy $[n_k]Q_1 + \mu_k U_0 = O$. If also $[n_l]Q_1 + \mu_l U_0 = O$, then $n_k \mu_l Q_1 = n_l \mu_k Q_1$, so $\mu_l = (n_l/n_k)\mu_k$ as Q_1 has infinite order. Near U_0, with a local parameter ζ for which the invariant differential is $d\zeta$, the term $X([n_l]Q_1 + \mu_l U)$ has leading part $(\mu_l \zeta)^{-2}$, where μ_l acts on the tangent space as a complex number; the sum of the leading parts of the first block is $\mu_k^{-2}\zeta^{-2}\sum_l (n_k/n_l)^2 \neq 0$, the sum over the l with a pole at U_0. No term of the second block has a pole at U_0: if $[n_l]Q_2 + \nu_l U_0 = O$, then $n_k \nu_l Q_1 - n_l \mu_k Q_2 = \nu_l([n_k]Q_1 + \mu_k U_0) - \mu_k([n_l]Q_2 + \nu_l U_0) = O$ with $n_l \mu_k \neq 0$, contrary to independence. So the restriction has a pole at U_0, a contradiction. The same argument applies if some $\nu_k \neq 0$. Hence no translate of a nonzero abelian subvariety through $\mathbf{q}$ lies in a fibre of Φ.

Von Buhren's theorem. Let $V \subseteq \mathcal{E} \times \mathbf{P}^1$ be the closure of the graph of Φ, an integral closed subscheme, and V_t its fibre over $t \in \mathbf{P}^1$. A translate of a nonzero abelian subvariety through $\mathbf{q}$ inside V_T meets the domain of Φ in a dense open subset, on which $\Phi = T$; we have just excluded this, so $\mathbf{q} \in V_T \setminus Z_{V_T}$ in the notation of [65, p. 307]. Let $\Gamma \subseteq \mathcal{E}(\overline{\mathbb{Q}})$ be the subgroup generated by the eight points with one coordinate Q_1 or Q_2 and the others O; it has finite rank and contains $\mathbf{q}$, so $\mathbf{q} \in C(\Gamma, \epsilon)$ for every $\epsilon > 0$. Von Buhren's theorem [65, Théorème 1.1], applied to $V \subseteq \mathcal{E} \times \mathbf{P}^1$ with the hyperplane bundle on $\mathbf{P}^1$ and a symmetric very ample bundle on $\mathcal{E}$ satisfying the normality condition [65, (1.1)] (a sufficiently high power of the product of symmetric ample bundles on the factors), gives $\mu \geq 0$ and $\varepsilon > 0$ such that for every subgroup $\Gamma \subset \mathcal{E}(\overline{\mathbb{Q}})$ of finite rank there is $\nu \geq 0$ with $\hat{h}_{\mathcal{E}}(a) \leq \mu h(t) + \nu$ for all $t \in \mathbf{P}^1(\overline{\mathbb{Q}})$ and all $a \in (V_t \setminus Z_{V_t})(\overline{\mathbb{Q}}) \cap C(\Gamma, \varepsilon)$. With our Γ, $t = T$ and $a = \mathbf{q}$ it gives $\hat{h}_{\mathcal{E}}(\mathbf{q}) \leq \mu h(T) + \nu$, where $\hat{h}_{\mathcal{E}}(\mathbf{q})$ is a fixed positive multiple of $\sum_k (\hat{h}([n_k]Q_1) + \hat{h}([n_k]Q_2)) = 2\hat{h}_E(P)\sum_k n_k^2$, because canonical heights are invariant under isomorphisms of elliptic curves and under Galois conjugation. Since $\hat{h}_E(P) > 0$, the lemma follows. □

2.6. **The second curve.** In this subsection E is the second index curve: $F = \mathbb{Q}(\sqrt{2})$ and $a = 3{+}6\sqrt{2}$. Write $\mathcal{O}_F = \mathbb{Z}[\sqrt{2}]$, $\varepsilon = 1{+}\sqrt{2}$, $\lambda = \sqrt{2}$, $\pi_7 = 1{+}2\sqrt{2}$ and $\bar{\pi}_7 = \sigma(\pi_7) = 1{-}2\sqrt{2}$, so that $a = 3\pi_7$, $\bar{a} = 3\bar{\pi}_7$, $\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = -1$ and $\mathrm{N}_{F/\mathbb{Q}}(\pi_7) = -7$. The ring $\mathcal{O}_F$ is a principal

ideal domain (the Minkowski bound is $\sqrt{2} < 2$), and $\mathcal{O}_F^\times = \{\pm\varepsilon^k\}$, since a unit $u + v\sqrt{2} > 1$ has $u, v \geq 1$ (its conjugate $\pm 1/(u + v\sqrt{2})$ has absolute value less than 1). The prime 2 ramifies, $2\mathcal{O}_F = (\lambda)^2$, and $[2] = 1$ in $F^\times/F^{\times 2}$. A prime $p \equiv \pm 3 \pmod 8$, such as 3, 5 or 13, is inert in F, as $\left(\frac{2}{p}\right) = -1$. The prime 7 splits: $7 = -\pi_7\bar{\pi}_7$, and $(\pi_7) \neq (\bar{\pi}_7)$ because $\pi_7/\bar{\pi}_7 = -(9 + 4\sqrt{2})/7 \notin \mathcal{O}_F$. For $\mathfrak{p}_7 = (\pi_7)$ we have $F_{\mathfrak{p}_7} = \mathbb{Q}_7$ with $\sqrt{2} \mapsto 3$, as $\pi_7 \equiv 0$ gives $\sqrt{2} \equiv -\frac{1}{2} \equiv 3 \pmod{\mathfrak{p}_7}$, and $3^2 \equiv 2 \pmod 7$. The nonzero squares modulo 7 are 1, 2, 4; so at $\mathfrak{p}_7$ the unit $\varepsilon \mapsto 4$ is a square, and -1 and 3 are not.

Lemma 2.11. *The equation (1.1) is minimal at every prime of F, and so is its conjugate. Its discriminant is a unit outside (λ), (3) and (π_7), and that of the conjugate outside (λ), (3) and $(\bar{\pi}_7)$.*

Proof. The discriminant is $64a^6 = 2^6 3^6 \pi_7^6$. At (3) and (π_7) its valuation is $6 < 12$, so the equation is minimal there. At (λ) its valuation is 12, as a is a λ-unit ($\mathrm{N}_{F/\mathbb{Q}}(a) = -63$ is odd); so a more integral model would come from a change of variables with $v_\lambda(u) = 1$, say $u = \lambda$ times a unit, which we may take to be 1. Suppose that $x = \lambda^2 x' + r$, $y = \lambda^3 y' + \lambda^2 s x' + t$ gives an integral model. With $a_1 = a_2 = a_3 = a_6 = 0$ and $a_4 = -a^2$, its coefficients are [56, §III.1]

$$a_1' = \frac{2s}{\lambda}, \quad a_2' = \frac{3r - s^2}{\lambda^2}, \quad a_3' = \frac{2t}{\lambda^3}, \quad a_4' = \frac{3r^2 - a^2 - 2st}{\lambda^4}, \quad a_6' = \frac{r(r^2 - a^2) - t^2}{\lambda^6}.$$

Write $v = v_\lambda$. First r, s, t are integral: $b_8' = (3r^4 - 6a^2r^2 - a^4)/\lambda^8$ is integral and 3 is a unit, so r is integral over $\mathbb{Z}_2[\sqrt{2}]$, hence in it; then $s^2 = 3r - \lambda^2 a_2'$ and $t^2 = r(r^2 - a^2) - \lambda^6 a_6'$ are integral. Now a_3' gives $v(t) \geq 1$, and a_4' gives $v(3r^2 - a^2) \geq 3$, so r is a unit. Next a_2' gives $s^2 \equiv 3r \pmod{\lambda^2}$; the square of a unit $w_0 + w_1\sqrt{2}$ (w_0 odd) is $w_0^2 + 2w_1^2 + 2w_0w_1\sqrt{2} \equiv 1 \pmod{\lambda^2}$, so s is a unit and $r \equiv 1 \pmod{\lambda^2}$. From a_4', $r^2 - a^2 \equiv -2r^2 + 2st \pmod{\lambda^4}$, and $v(2r^2) = 2 < v(2st)$, so $v(r^2 - a^2) = 2$ and $v(r(r^2 - a^2)) = 2$. Then a_6' forces $v(t^2) = 2$, since otherwise $v(r(r^2 - a^2) - t^2) = 2 < 6$; so $t = \lambda t_1$ with t_1 a unit. Now a_6' gives $2t_1^2 = t^2 \equiv r(r^2 - a^2) \pmod{\lambda^6}$, and multiplying the congruence from a_4' by the unit r gives $r(r^2 - a^2) \equiv -2r^3 + 2\lambda r s t_1 \pmod{\lambda^4}$. So $2t_1^2 \equiv -2r^3 + 2\lambda r s t_1 \pmod{\lambda^4}$, and dividing by $2 = \lambda^2$, $t_1^2 \equiv -r^3 + \lambda r s t_1 \pmod{\lambda^2}$. Modulo $\lambda^2 = 2$ we have $t_1^2 \equiv 1$, $r^3 \equiv 1$ and $\lambda r s t_1 \equiv \lambda$, so $1 \equiv -1 + \lambda \equiv 1 + \lambda \pmod 2$, that is $\lambda \equiv 0 \pmod 2$, which is false. So no such model exists. For the conjugate apply σ. □

Lemma 2.12. *Let $D \geq 1$ be a squarefree integer. Then $E(F(\sqrt{D}))_{\mathrm{tors}} = E[2]$.*

Proof. The field $L' = F(\sqrt{D})$ is totally real. By the first paragraph of the proof of Lemma 2.3, a point $T = (e_1, 0)$ of E is in $2E(L')$ only if $e_1 - e_2$ and $e_1 - e_3$ are squares in L'. For $T = (0, 0)$ this needs $-a$ and a, hence -1, to be squares; for $T = (a, 0)$ it needs a to be a square (and $2a$, but $2 = \lambda^2$); for $T = (-a, 0)$ it needs $-a$ to be a square. But $a = 3 + 6\sqrt{2}$ is negative at the real places of L' above $\sqrt{2} \mapsto -\sqrt{2}$, and $-a$ at those above $\sqrt{2} \mapsto \sqrt{2}$. So $E(L')$ has no point of order four.

Let $q \in \{23, 31\}$. Then $q \equiv 7 \pmod 8$ splits in F, and $q \nmid 2 \cdot 3 \cdot 7$, so E has good reduction at both primes of F above q (E2). Each reduction is $y^2 = x^3 - s^2x$ over $\mathbb{F}_q$, with $s \neq 0$ the image of a; since $q \equiv 3 \pmod 4$, it has $q+1$ points ($x \mapsto -x$ changes the quadratic character of $x^3 - s^2x$, as -1 is a nonsquare), hence $(q+1)^2$ points over $\mathbb{F}_{q^2}$ (its Frobenius has trace 0, so its square is $-q$). A prime of L' above q has residue field $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$, as $[L' : F] \leq 2$ and q splits in F. By [56, Proposition VII.3.1(b)], $E(L')[\ell]$ injects into the reduction at such a prime for every prime $\ell \neq q$. With $q = 31$ the reduction has 32 or 1024 points, so

$E(L')[\ell] = 0$ for every odd prime $\ell \neq 31$; with $q = 23$ it has 24 or 576 points, prime to 31, so $E(L')[31] = 0$. Hence $E(L')_{\mathrm{tors}} = E[2]$. □

Proposition 2.13. $\operatorname{rank} E(F) = 1$ *and* $E(F)_{\mathrm{tors}} = E[2]$*; the point*

$$P_0' = (3 - 3\sqrt{2},\ 9\sqrt{2})$$

lies in $E(F)$ *and has infinite order.*

Proof. For $x = 3 - 3\sqrt{2}$ we have $x^3 = 27(7 - 5\sqrt{2})$ and $a^2x = 9(9 + 4\sqrt{2}) \cdot 3(1 - \sqrt{2}) = 27(1 - 5\sqrt{2})$, so $x^3 - a^2x = 162 = (9\sqrt{2})^2$ and $P_0' \in E(F)$. By Lemma 2.12 with $D = 1$, $E(F)_{\mathrm{tors}} = E[2]$; as $y(P_0') \neq 0$, P_0' has infinite order.

The prime (λ) does not divide a, and the odd primes dividing a are (3) and (π_7), each to the first power; so by Lemma 2.2 both images for $c = a$ lie in $V = \langle -1, \varepsilon, 3, \pi_7 \rangle$. Write a class of V as $(-1)^h \varepsilon^i 3^j \pi_7^k$ with exponents in $\{0, 1\}$. At the real place $\sqrt{2} \mapsto \sqrt{2}$ only -1 is negative; at $\sqrt{2} \mapsto -\sqrt{2}$ the elements -1, ε and π_7 are negative. At (3), in the coordinates (valuation modulo 2, class of the unit part in $\mathbb{F}_9^\times/\mathbb{F}_9^{\times 2}$), the elements -1, ε, 3, π_7 have coordinates $(0,0)$, $(0,1)$, $(1,0)$, $(0,1)$: a unit of $\mathbb{F}_9$ is a square exactly when its norm to $\mathbb{F}_3$ is, and $\mathrm{N}_{F/\mathbb{Q}}(\varepsilon) = -1$ and $\mathrm{N}_{F/\mathbb{Q}}(\pi_7) = -7$ are nonsquares modulo 3. At $\mathfrak{p}_7$, in the coordinates (valuation modulo 2, residue symbol of the unit part with respect to the uniformiser π_7), they have $(0,1)$, $(0,0)$, $(0,1)$, $(1,0)$.

The local images are these. At (3), F_v is unramified of degree two over $\mathbb{Q}_3$, -1 is a square, and so is 2ι, since its residue is (every element of $\mathbb{F}_3$ is a square in $\mathbb{F}_9$, and $\iota^4 = 1$ in the cyclic group $\mathbb{F}_9^\times$ of order 8); so by Lemma 2.3 both images are $\langle [a] \rangle$, with coordinates $\langle (1,1) \rangle$. At $\mathfrak{p}_7$, $F_v = \mathbb{Q}_7$ and -1 is not a square, so by Lemma 2.3 $\operatorname{Im} \alpha'_{a,v} = \{1\}$. At a real place a point of $E'_a\colon y^2 = x(x^2 + 4a^2)$ has $x \geq 0$, so the image of α'_a is totally positive.

For α'_a, total positivity gives $h = 0$ and $i + k = 0$; the place (3) gives $j = i + k$; and $\mathfrak{p}_7$ gives $k = 0$ and $h + j = 0$. So $\operatorname{Im} \alpha'_a = \{1\}$. For α_a the place (3) gives $j = i + k$, which leaves $\langle -1, 3\varepsilon, 3\pi_7 \rangle = \langle [-1], [-3\varepsilon], [a] \rangle$, of order 8. By Lemma 2.1, $2^{\operatorname{rank} E(F)} \leq 8 \cdot 1/4 = 2$, so $\operatorname{rank} E(F) \leq 1$, and $\operatorname{rank} E(F) = 1$. □

2.7. **The third and fourth curves.** In this subsection E is the third or the fourth index curve. For the third, $F = \mathbb{Q}(\sqrt{2})$, and we keep the notation of Section 2.6: $A = \pi_7 = 1 + 2\sqrt{2}$, $\bar{A} = \bar{\pi}_7$ and $\mathrm{N}_{F/\mathbb{Q}}(A) = -7$. For the fourth, $F = \mathbb{Q}(\sqrt{17})$, $A = \frac{1}{2}(11 - 7\sqrt{17})$ and $\mathrm{N}_{F/\mathbb{Q}}(A) = -178$. Its ring of integers $\mathcal{O}_F = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{17})]$ is a principal ideal domain: the Minkowski bound is $\sqrt{17}/2 < 3$, and $2 = \frac{1}{2}(5 + \sqrt{17}) \cdot \frac{1}{2}(5 - \sqrt{17})$ is the product of two distinct primes $\mathfrak{p}$, $\sigma\mathfrak{p}$ of norm 2. The prime 89 splits in F, as $(\frac{17}{89}) = (\frac{89}{17}) = (\frac{4}{17}) = 1$, and, choosing the labels, $(A) = \mathfrak{p}\mathfrak{l}$ with $\mathrm{N}\,\mathfrak{l} = 89$. For both curves $\mathrm{N}_{F/\mathbb{Q}}(A) < 0$, so A is not a square in F, and $(0,0)$ is the only point of order two in $E(F)$.

For $A \in F^\times$ and an extension M of F, the curve $y^2 = x^3 - Ax$ has the 2-isogeny $\phi(x,y) = (y^2/x^2,\ y(-A - x^2)/x^2)$ onto $y^2 = x^3 + 4Ax$, with kernel $\{O, (0,0)\}$, and, as in Section 2.2, injective homomorphisms α' and α into $M^\times/M^{\times 2}$, given by $(x,y) \mapsto [x]$ for $x \neq 0$, with $\alpha'(0,0) = [A]$ and $\alpha(0,0) = [-A]$; a class e lies in the image of α', respectively α, exactly when $W^2 = eU^4 + (4A/e)V^4$, respectively $W^2 = eU^4 - (A/e)V^4$, has a solution over M with $(U,V) \neq (0,0)$ [56, Proposition X.4.9]. If $A \notin M^{\times 2}$, the first term of the exact sequence in the proof of Lemma 2.1 has order 2, and so has $E(M)[2]$; so again $2^{\operatorname{rank} E(M)} = |\operatorname{Im} \alpha| \cdot |\operatorname{Im} \alpha'|/4$ when M is a number field.

Lemma 2.14. *For the third and the fourth curve,* (1.1) *and its conjugate are minimal at every prime of F. The discriminant of* (1.1) *is a unit outside* (λ) *and* (π_7) *for the third curve, and outside* $\mathfrak{p}$, $\sigma\mathfrak{p}$ *and* $\mathfrak{l}$ *for the fourth.*

Proof. The discriminant is $64A^3$. For the fourth curve 64 has valuation 6 at $\mathfrak{p}$ and at $\sigma\mathfrak{p}$, so $64A^3$ has valuations 9, 6 and 3 at $\mathfrak{p}$, $\sigma\mathfrak{p}$ and $\mathfrak{l}$, all less than 12. For the third, it has valuation 3 at (π_7), and 12 at (λ), as A is a λ-unit. At (λ) we argue as in the proof of Lemma 2.11, with $a_4 = -A$: a more integral model comes from $x = \lambda^2 x' + r$, $y = \lambda^3 y' + \lambda^2 s x' + t$, and $b_8' = (3r^4 - 6Ar^2 - A^2)/\lambda^8$ shows as there that r, s, t are integral. Then $a_3' = 2t/\lambda^3$ gives $v(t) \geq 1$; $a_4' = (3r^2 - A - 2st)/\lambda^4$ gives $v(3r^2 - A) \geq 3$, so r is a unit; and $a_2' = (3r - s^2)/\lambda^2$ gives $s^2 \equiv 3r \pmod{\lambda^2}$, so s is a unit and $r \equiv 1 \pmod{\lambda^2}$, hence $r^2 \equiv 1 \pmod{\lambda^4}$. Since $A = 1 + \lambda^3$, a_4' now gives $3 - A - 2st = \lambda^2(1 - \lambda - st) \equiv 0 \pmod{\lambda^4}$, that is $st \equiv 1 - \lambda \pmod{\lambda^2}$; but $v(st) \geq 1$ and $1 - \lambda$ is a unit. So no such model exists. For the conjugates apply σ. □

Lemma 2.15. *Let L be $F(\sqrt{D})$ for the third curve, where D is a positive squarefree integer divisible by 7, and $F(\sqrt{2}, \sqrt{3})$ for the fourth. Then $E(L)_{\mathrm{tors}} = \{O, (0,0)\}$; in particular $E(F)_{\mathrm{tors}} = \{O, (0,0)\}$.*

Proof. The field L is totally real. For the third curve $D \notin F^{\times 2}$, as $F^{\times 2} \cap \mathbb{Q} = \mathbb{Q}^{\times 2} \cup 2\mathbb{Q}^{\times 2}$. By Kummer theory, $F \cap L^{\times 2}$ is $F^{\times 2} \cup DF^{\times 2}$ for the third curve and the union of the $D'F^{\times 2}$, $D' \in \{1, 2, 3, 6\}$, for the fourth. The norms to $\mathbb{Q}$ of $\pm A$ and $\pm DA$ are -7 and $-7D^2$, and those of $\pm D'A$ are $-178D'^2$; all are negative, so A and $-A$ are not squares in L. Hence $(0,0)$ is the only point of order two in $E(L)$, and no point Q of $E(L)$ has $2Q = (0,0)$, since by the duplication formula of Lemma 2.8 this needs $x(Q)^2 = -A$. So the 2-primary part of $E(L)_{\mathrm{tors}}$ is $\{O, (0,0)\}$.

Let ℓ be an odd prime. By Lemma 2.5, if $E(L)[\ell] \neq 0$, then $L(i)$ contains a root of unity of order ℓ. The field $L(i)$ is multiquadratic, so this happens only if $\ell = 3$ and $\sqrt{-3} \in L(i)$. For the third curve the quadratic subfields of $L(i) = \mathbb{Q}(\sqrt{2}, \sqrt{D}, i)$ are the $\mathbb{Q}(\sqrt{n})$ with $n \in \{-1, \pm 2, \pm D, \pm 2D\}$, and -3 is not a square times any of these, as $7 \mid D$; so $\sqrt{-3} \notin L(i)$. For the fourth, $A - 2 = -7 \cdot \frac{1}{2}(\sqrt{17} - 1)$, so E has good reduction at the prime $7\mathcal{O}_F$, which is inert as $(\frac{17}{7}) = (\frac{3}{7}) = -1$, with reduction $y^2 = x^3 - 2x$, defined over $\mathbb{F}_7$. As $7 \equiv 3 \pmod 4$, this curve has 8 points over $\mathbb{F}_7$ and 64 over $\mathbb{F}_{49}$, as in the proof of Lemma 2.12. The primes of L above 7 have residue field $\mathbb{F}_{49}$, so $E(L)[3] = 0$ by [56, Proposition VII.3.1(b)]. □

Proposition 2.16. *For the third curve,* $\operatorname{rank} E(F) = 1$ *and* $E(F)_{\mathrm{tors}} = \{O, (0,0)\}$*; the point*

$$P_0'' = (-\tfrac{1}{2} - \sqrt{2},\ \tfrac{1}{2} - \tfrac{3}{4}\sqrt{2})$$

lies in $E(F)$ and has infinite order.

Proof. For $x = -\frac{1}{2} - \sqrt{2}$ we have $x^2 = \frac{9}{4} + \sqrt{2}$, $x^3 = -\frac{25}{8} - \frac{11}{4}\sqrt{2}$ and $Ax = -\frac{9}{2} - 2\sqrt{2}$, so $x^3 - Ax = \frac{11}{8} - \frac{3}{4}\sqrt{2} = (\frac{1}{2} - \frac{3}{4}\sqrt{2})^2$ and $P_0'' \in E(F)$. By Lemma 2.15, $E(F)_{\mathrm{tors}} = \{O, (0,0)\}$, so P_0'' has infinite order. For the rank, a 2-isogeny descent over F: we find that the Selmer group of ϕ, which contains $\operatorname{Im}\alpha'$, is $\{1, [\varepsilon], [A], [\varepsilon A]\}$, and that the Selmer group of its dual, which contains $\operatorname{Im}\alpha$, is $\{1, [-A]\}$. The first is $\operatorname{Im}\alpha'$: $\alpha'(0,0) = [A]$, and the point $Q' = (2 + 2\sqrt{2},\ 8 + 4\sqrt{2})$ of $y^2 = x^3 + 4Ax$ has $\alpha'(Q') = [2\varepsilon] = [\varepsilon]$, since $(2 + 2\sqrt{2})^3 + 4A(2 + 2\sqrt{2}) = (56 + 40\sqrt{2}) + (40 + 24\sqrt{2}) = 96 + 64\sqrt{2} = (8 + 4\sqrt{2})^2$. So $2^{\operatorname{rank} E(F)} \leq 4 \cdot 2/4 = 2$, and $\operatorname{rank} E(F) = 1$. □

Proposition 2.17. *For the fourth curve,* $\operatorname{rank} E(F) = 1$ *and* $E(F)_{\mathrm{tors}} = \{O, (0,0)\}$*; the point*

$$P_0''' = \left(\tfrac{1}{2}(5 - \sqrt{17}),\ 2\right)$$

lies in $E(F)$ *and has infinite order.*

Proof. For $x = \frac{1}{2}(5 - \sqrt{17})$ we have $x^2 = \frac{1}{2}(21 - 5\sqrt{17})$, $x^3 = \frac{1}{2}(95 - 23\sqrt{17})$ and $Ax = \frac{1}{2}(87 - 23\sqrt{17})$, so $x^3 - Ax = 4$ and $P_0''' \in E(F)$. By Lemma 2.15, $E(F)_{\mathrm{tors}} = \{O, (0,0)\}$, so P_0''' has infinite order. For the rank, a 2-isogeny descent over F: we find that the Selmer group of ϕ is $\{1, [A]\}$ and that of its dual is $\{1, [\frac{1}{2}(5 - \sqrt{17})], [8 + 3\sqrt{17}], [-A]\}$. So $2^{\operatorname{rank} E(F)} \leq 2 \cdot 4/4 = 2$, and $\operatorname{rank} E(F) = 1$. □

3. A height bound on a tube

Throughout this section K is a totally real number field of degree n_K, and h is the absolute logarithmic Weil height. We bound the height of an element z of K that lies in a q-adic tube by a power of the product of the primes at which z meets seven fixed points of $\mathbf{P}^1$ to odd order. The proof follows [60, §§5–8]. Facts about the Shimura curve of discriminant 6 and its covers are quoted from [60] with their numbers, and with the reason they hold over K and for every q (Section 3.2). The other steps that depend on K or on q are proved here: the behaviour at the tube prime (Lemmas 3.3 and 3.4), a scalar cochain over K (Proposition 3.5), the local behaviour at the primes above 3, and the comparison with a Shimura curve over K in every degree (Section 3.4).

3.1. **The data.** For a prime $q \geq 7$ put

$$D_q = q^2 + 3, \qquad a_q = \frac{(q-3)(q+1)}{D_q}, \qquad b_q = \frac{(q-1)(q+3)}{D_q^2},$$

$$x_q(z) = \frac{a_q z + b_q}{q z^2}, \qquad j(x) = \frac{16x^2}{(x-4)^3},$$

$$g_q(z) = \frac{(a_q z + b_q - q z^2)(a_q z + b_q - 4q z^2)}{4q^2} = \frac{z^4}{4}\big(x_q(z) - 1\big)\big(x_q(z) - 4\big), \tag{3.1}$$

and let $\mathcal{C}_q \subset \mathbf{P}^1(\mathbb{Q})$ consist of ∞ and the six finite *contacts*

$$\gamma_1 = 0, \quad \gamma_2 = -\frac{(q-1)(q+3)}{(q-3)(q+1)D_q}, \quad \gamma_3 = \frac{q-1}{D_q},$$
$$\gamma_4 = -\frac{q+3}{qD_q}, \quad \gamma_5 = \frac{(q-1)(q+3)}{4qD_q}, \quad \gamma_6 = -\frac{1}{D_q}.$$

These are Sun's formulas [60, (1.3)–(1.7)] with q in place of 367. The map x_q has a double pole at 0, $x_q(\gamma_2) = 0$, $x_q(\gamma_3) = x_q(\gamma_4) = 1$ and $x_q(\gamma_5) = x_q(\gamma_6) = 4$; the zeros of g_q are $\gamma_3, \ldots, \gamma_6$; and $z \mapsto j(x_q(z))$ is a rational function of degree 6. We also use the identities

$$a_q^2 + 4qb_q = 1, \qquad a_q + 1 = \frac{2q(q-1)}{D_q}, \qquad b_q + \frac{1}{3} = \frac{q(q^3 + 9q + 6)}{3D_q^2},$$
$$-\big(27j(x_q(z)) + 16\big) = -g_q(z)\Big(\frac{8(x_q(z) + 8)}{z^2(x_q(z) - 4)^2}\Big)^2, \tag{3.2}$$

the last of which is [60, (5.3)] for general q.

Positive odd contact, the set Σ, the function $\mathfrak{N}_\Sigma$ and the positive tube $\mathcal{D}$ are defined before Theorem 1.6.

Lemma 3.1. *If $\sqrt{3} \notin K$, there are infinitely many primes $q \equiv 7 \pmod{12}$ for which some prime of K above q is unramified over q and has residue degree one.*

Proof. Let M be the Galois closure of K over $\mathbb{Q}$ and $M' = M(\zeta_{12})$. The subfields of $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{3})$ are $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\zeta_{12})$; the totally real ones are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{3})$, so $K \cap \mathbb{Q}(\zeta_{12}) = \mathbb{Q}$ and restriction maps $\mathrm{Gal}(M'/K)$ onto $\mathrm{Gal}(K(\zeta_{12})/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times$. Choose $g \in \mathrm{Gal}(M'/K)$ acting on ζ_{12} by $\zeta_{12} \mapsto \zeta_{12}^7$. By Chebotarev's density theorem there are infinitely many primes q, unramified in M', with a prime $\mathfrak{Q}$ of M' above q whose Frobenius is g. Then $q \equiv 7 \pmod{12}$, and the decomposition group $\langle g \rangle$ of $\mathfrak{Q}$ over $\mathbb{Q}$ lies in $\mathrm{Gal}(M'/K)$, so the prime $\mathfrak{Q} \cap K$ has residue degree one over q; it is unramified because q is unramified in M'. □

Lemma 3.2. *Let q and $\mathfrak{q}$ be as in Theorem 1.6.*

(a) *Every finite contact lies in the open interval $(-1, 1)$. As rational functions of q, $\gamma_i - 1 = N_i(q)/E_i(q)$ with $N_i, E_i \in \mathbb{Z}[q]$ and $N_i(0) = -1, 12, -4, -3, -3, -4$ for $i = 1, \dots, 6$; hence $v_\mathfrak{q}(\gamma_i - 1) \le 0$, and $\mathcal{D} \cap \mathcal{C}_q = \emptyset$.*

(b) *Every $z \in K$ with $v_\mathfrak{q}(z - 1) \ge 1$ and $z - 1$ totally positive lies in $\mathcal{D}$.*

(c) *If $s \in K$ is totally positive and $v_\mathfrak{q}(s) \le 0$, then $1 + q/s \in \mathcal{D}$.*

(d) *For every $t \in K$, $\psi_q(t) = 10q + 1 + \dfrac{q^2 t}{1 + q^2 t^2}$ lies in $\mathcal{D}$.*

Proof. (a) The formulas for N_i are direct; $N_i(q) \equiv N_i(0) \pmod{q}$ is prime to $q \ge 7$, so $v_q(\gamma_i - 1) \le 0$, and $v_\mathfrak{q} = v_q$ on $\mathbb{Q}$ because $\mathfrak{q}$ is unramified. That each γ_i lies in $(-1, 1)$ for $q \ge 7$ is checked by writing $1 \pm \gamma_i$ as quotients of polynomials in q that are positive at $q = 7$ and have no real root ≥ 7. (b) Since $0 < a_q, b_q < 1$, for real $z > 1$ we have $0 < x_q(z) < (a_q + b_q)/q < 1$, so $g_q(z) > 0$ by (3.1). (c) $v_\mathfrak{q}(q/s) \ge 1$ because $v_\mathfrak{q}(q) = 1$, and $q/s > 0$ at every real place; apply (b). (d) Put $u = qt$; then $\psi_q(t) - 1 = q(10 + u/(1 + u^2))$. The residue field of $\mathfrak{q}$ has q^f elements with f odd and $q \equiv 3 \pmod{4}$, so -1 is not a square in it; hence $v_\mathfrak{q}(1 + u^2) = \min(0, 2v_\mathfrak{q}(u))$, and $u/(1 + u^2)$ is $\mathfrak{q}$-integral. So $v_\mathfrak{q}(\psi_q(t) - 1) \ge 1$. At every real place $|u/(1 + u^2)| \le \frac{1}{2}$, so $\psi_q(t) \ge 9.5q + 1 > 1$; apply (b). □

Lemma 3.3. *Let q and $\mathfrak{q}$ be as in Theorem 1.6 and let $z \in K$ with $v_\mathfrak{q}(z - 1) \ge 1$. Put $j_z = j(x_q(z))$ and $d_z = -(27 j_z + 16)$. Then $v_\mathfrak{q}(x_q(z)) = v_\mathfrak{q}(x_q(z) - 4) = -1$, $v_\mathfrak{q}(j_z) = 1$, d_z is a $\mathfrak{q}$-adic unit with $d_z \equiv -16 \pmod{\mathfrak{q}}$, and $g_q(z)$ is a square in the completion $K_\mathfrak{q}$.*

Proof. By (3.2), $a_q \equiv -1$ and $b_q \equiv -\frac{1}{3}$ modulo q (note $D_q \equiv 3 \pmod{q}$). Since $z \equiv 1$ and $v_\mathfrak{q}(qz^2) = 1$, both $a_q z + b_q$ and $a_q z + b_q - 4qz^2$ are congruent to $-\frac{4}{3}$ modulo $\mathfrak{q}$, a unit. Hence $v_\mathfrak{q}(x_q(z)) = v_\mathfrak{q}(x_q(z) - 4) = -1$ and $v_\mathfrak{q}(j_z) = 2(-1) - 3(-1) = 1$. Then $27 j_z + 16 \equiv 16$, so $d_z \equiv -16$. By the last identity of (3.2), $g_q(z) \cdot s^2 = -d_z \equiv 16$ with $s = 8(x_q(z) + 8)/(z^2(x_q(z) - 4)^2) \ne 0$, so $g_q(z) s^2$ is a unit congruent to a nonzero square modulo $\mathfrak{q}$, hence a square in $K_\mathfrak{q}$ by Hensel's lemma (q is odd). □

3.2. **The fibres, the sign cocycle and the representations.** Let $B = (2, -3)_\mathbb{Q}$ be the quaternion algebra over $\mathbb{Q}$ generated by $\mathbf{i}, \mathbf{j}$ with $\mathbf{i}^2 = 2$, $\mathbf{j}^2 = -3$, $\mathbf{ij} = -\mathbf{ji}$; it is ramified exactly at 2 and 3, and $O = \mathbb{Z}[\mathbf{i}, (1 + \mathbf{j})/2]$ is a maximal order. We use the following facts about the Shimura curve of O over $\mathbb{Q}$, proved in [60, §§5, 6, 8]. (S1) and (S2) involve neither K nor q; (S3)–(S5) are proved there over $\mathbb{Q}(\sqrt{2})$; the proofs of (S3) and (S4) are local at one prime and that of (S5) is formal in the base field, so they apply over K as stated.

(S1) [60, §5 and Lemma 5.1] The quotient of the Shimura curve of O by its full Atkin–Lehner group $W \cong (\mathbb{Z}/2\mathbb{Z})^2$ is the projective line, with a coordinate j whose elliptic points

have orders 4, 6 and 2 above $j = 0$, ∞ and $-16/27$; the normalisation of j is that of [37, Example 29], and the quotient and its intermediate covers are those of [4, Theorems 2.1, 3.10 and 3.17].

(S2) [60, Lemma 5.3, proof of Proposition 5.7, Lemma 8.1] There is a smooth proper fine moduli scheme $\mathcal{X}$ over $\mathbb{Z}[1/30]$ of principally polarised abelian surfaces with an action of O and a full level-three structure $\mathrm{Isom}_O(O/3O, A[3])$; it is built from Buzzard's model at an auxiliary level five [8, Theorem 2.1 and Corollary 2.3] and Deligne's canonical models [13, §4]. A group $\mathcal{G}$ of order 144 acts on its generic fibre over the j-line, the fibre above a point $j \notin \{0, \infty, -16/27\}$ is a $\mathcal{G}$-torsor, and $\mathcal{G}$ has a normal subgroup $U \cong (\mathbb{Z}/3\mathbb{Z})^2$ with $\mathcal{G}/U \cong D_8 \times \mathbb{Z}/2\mathbb{Z}$ [60, (8.1)].

(S3) [60, Proposition 1.8, proved in §5] Let $z \in K \setminus \mathcal{C}_q$ and let $\mathfrak{P} \notin \Sigma$ be a prime of K. The fibre of $\mathcal{X}$ above $j(x_q(z))$ is unramified at $\mathfrak{P}$ unless z has positive odd contact with a point of $\mathcal{C}_q$ at $\mathfrak{P}$, and then inertia at $\mathfrak{P}$ acts on it through a group of order 2. Sun states this for $q = 367$; the proof is local at $\mathfrak{P}$ and uses only that the seven points of $\mathcal{C}_q$ and the three elliptic points have distinct reductions modulo $\mathfrak{P}$ and that $|\mathcal{G}|$ is prime to the residue characteristic, so it applies to every prime $q \geq 7$ with Σ as in Section 1.

(S4) [60, Lemma 5.5 and Proposition 5.7] Let $\mathfrak{P}$ be a prime of K not dividing 30, and let $j_0 \in K$ with $v_{\mathfrak{P}}(j_0) = 1$. Then inertia at $\mathfrak{P}$ acts on the fibre of $\mathcal{X}$ above j_0 through the class in $\mathcal{G}$ of $\gamma = 1 + \mathbf{i} + \mathbf{j}$ (up to inverse). Here $\mathrm{Nrd}(\gamma) = 2$, the reduced characteristic polynomial of γ is $X^2 - 2X + 2$, γ has order 4 modulo the centre, and the ratio of the roots of $X^2 - 2X + 2$ has order 4 in $\mathbb{F}_9^\times$. Sun states this for primes of residue characteristic $p > 144$ and norm $\equiv -1 \pmod 4$ [60, Proposition 5.7]; the proof of the inertia statement uses of the prime only that p does not divide $30|\mathcal{G}|$, that is $p \nmid 30$, and that $v_{\mathfrak{P}}(j_0) = 1$.

(S5) [60, Remark 6.2] Let $z \in K \setminus \mathcal{C}_q$ be such that the abelian surfaces in the fibre above $j_z = j(x_q(z))$ have no complex multiplication, that is, $\mathrm{End}^0(A \otimes \overline{K}) = B$. Let K_z be the splitting field over K of this fibre, so that $[K_z : K] \leq 144$, and let A_z be the abelian surface over K_z given by a point of it. All homomorphisms between Galois conjugates of A_z over $\overline{K}$ are defined over K_z. For $g \in G_K$ choose a B-linear quasi-isogeny $\mu_g \colon {}^g A_z \to A_z$ (for the labels transported as in [60, Remark 6.2]), depending only on the image of g in $\mathrm{Gal}(K_z/K)$, with $\mu_1 = \mathrm{id}$ (this is possible because ${}^g A_z$ and its transported labels depend only on that image); and put $\nu_g = (\deg \mu_g)^{-1/4} \mu_g$. Then $\nu_g \circ {}^g\nu_h = \varsigma(g,h)\, \nu_{gh}$ with $\varsigma(g,h) \in \{\pm 1\}$ (Ribet's construction [52, §6]); ς is a normalised 2-cocycle inflated from $\mathrm{Gal}(K_z/K)$. If $\vartheta \colon G_K \to \mu_\infty$ is continuous with $\delta\vartheta = \varsigma$, where $\delta\vartheta(g,h) = \vartheta(g)\vartheta(h)\vartheta(gh)^{-1}$, then $R_\ell(g) = \vartheta(g)^{-1} \nu_g \circ g$ is a continuous representation of G_K on $V_\ell(A_z) \otimes_{\mathbb{Q}_\ell} E_\ell$ commuting with B, where $V_\ell(A_z) = T_\ell(A_z) \otimes \mathbb{Q}_\ell$ and E_ℓ is a finite extension of $\mathbb{Q}_\ell$ containing the values of ϑ and the numbers $(\deg \mu_g)^{1/4}$ (finitely many), embedded once and for all. Taking E_ℓ also to split B, $R_\ell \cong r_\ell^{\oplus 2}$ with r_ℓ of dimension two and $\det r_\ell = \chi_{\mathrm{cyc}} \chi^{-1}$, where $\chi = \vartheta^2$ and χ_{cyc} is the ℓ-adic cyclotomic character; and on $G_{K'_z}$, where K'_z is the fixed field of the kernel of $\vartheta|_{G_{K_z}}$, R_ℓ is the Galois action on $V_\ell(A_z)$.

The map ϑ is provided by Proposition 3.5 below, which needs ς to be normalised; with $\mu_1 = \mathrm{id}$ it is. We write $\bar{r}_3$ for the semisimplification of the reduction of r_3 and $\mathbb{P}\bar{r}_3$ for its image in $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$; the latter does not depend on ϑ, since another choice of ϑ twists r_3 by a character.

Lemma 3.4. *Let q and $\mathfrak{q}$ be as in Theorem 1.6, let $z \in \mathcal{D}$ be as in (S5), and let ϑ and r_3 be as there. Let $D_\mathfrak{q} \supset I_\mathfrak{q}$ be decomposition and inertia groups at $\mathfrak{q}$.*

(a) *The images of $I_\mathfrak{q}$ under $\mathbb{P}\bar{r}_3$ and in $\mathrm{PGL}_2(E_3)$ under r_3 are cyclic of order 4, and a Frobenius element at $\mathfrak{q}$ conjugates a generator τ of either to τ^{-1}.*

(b) *$\bar{r}_3|_{D_\mathfrak{q}}$ is absolutely irreducible, and the Weil–Deligne representation attached to $r_3|_{D_\mathfrak{q}}$ has irreducible Weil part and zero monodromy.*

(c) *$\mathbb{P}\bar{r}_3(G_K)$ is dihedral of order 8, and the fixed field of its cyclic subgroup of order 4 is $M_z = K(\sqrt{-g_q(z)})$, a totally imaginary quadratic extension of K.*

(d) *$\bar{r}_3|_{G_{K(\zeta_3)}}$ is absolutely irreducible.*

Proof. First, A_z has potentially good reduction at every prime of K_z: after a finite extension it has semistable reduction, the action of O extends to the Néron model and acts on the character group of its toric part, which has rank at most 2; a nonzero module over the division algebra B has $\mathbb{Q}$-dimension at least 4, so the toric part is trivial [60, proof of Lemma 8.5].

(a) By Lemma 3.3, $v_\mathfrak{q}(j_z) = 1$, and $\mathfrak{q} \nmid 30$. By (S4), inertia at $\mathfrak{q}$ acts through the class of γ, whose image under r_3 is projectively of order 4, also after reduction because the ratio of its eigenvalues has order 4 in $\mathbb{F}_9^\times$ [60, Proposition 5.7]. The image of $I_\mathfrak{q}$ has order prime to q, so it factors through tame inertia, on which a Frobenius acts by raising to the power $N\mathfrak{q} = q^f$. Since $q \equiv 3 \pmod 4$ and f is odd, $\tau^{N\mathfrak{q}} = \tau^{-1}$.

(b) The element τ has two fixed points P_1, P_2 on $\mathbf{P}^1(\overline{\mathbb{F}}_3)$, with multipliers λ and λ^{-1}, where λ has order 4. A Frobenius ϕ maps the fixed points of τ to those of $\phi\tau\phi^{-1} = \tau^{-1}$, which are again P_1, P_2, and the multiplier of τ^{-1} at $\phi(P_1)$ is the multiplier λ of τ at P_1; since the multiplier of τ^{-1} at P_1 is $\lambda^{-1} \neq \lambda$, $\phi(P_1) = P_2$. So no point of $\mathbf{P}^1$ is fixed by the image of $D_\mathfrak{q}$, and $\bar{r}_3|_{D_\mathfrak{q}}$ is absolutely irreducible. The same argument over E_3 shows that the Weil part is irreducible. On an open subgroup of $I_\mathfrak{q}$ that acts trivially on $V_3(A_z)$ (potentially good reduction) r_3 is a character of finite order, so the monodromy is zero.

(c) This is [60, Lemmas 8.3 and 8.4], whose proof uses of the tube prime only (a) and (b). By (S2) and [60, proof of Lemma 8.3], $\mathrm{Gal}(K_z/K)$ embeds in the opposite group of $\mathcal{G}$. On G_{K_z} the three-torsion of A_z is constant and $R_3(g) = \vartheta(g)^{-1}V_3(A_z)(g)$, so all eigenvalues of $\bar{r}_3(g)$ coincide and $\mathbb{P}\bar{r}_3(G_{K_z})$ is a 3-group, normal in $\mathbb{P}\bar{r}_3(G_K)$. A nontrivial 3-subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ has exactly one fixed point on $\mathbf{P}^1$, which the whole image would then fix, against (b); so $\mathbb{P}\bar{r}_3(G_{K_z}) = 1$. In the same way the image of U is trivial, so $\mathbb{P}\bar{r}_3(G_K)$ is a subquotient of $D_8 \times \mathbb{Z}/2\mathbb{Z}$: a 2-group of order at most 16 and exponent at most 4. Finite 2-subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ are cyclic or dihedral, and a cyclic or dihedral group of order 16 has an element of order 8; so the image has order at most 8, and by (a) and (b) it contains a cyclic group of order 4 and an element outside it inverting it. Hence it is dihedral of order 8. Sun identifies the rotation subgroup with the image of the kernel of the Atkin–Lehner parity at 3, which contains the class of γ [60, proof of Lemma 8.3], and Baba and Granath compute the corresponding quadratic cover as $\mathbb{Q}(j)(\sqrt{-(27j+16)})$ [4, Theorem 3.10, Corollary 3.11, Theorem 3.17], [60, Lemma 8.4]. By (3.2) its fibre above j_z gives $M_z = K(\sqrt{d_z}) = K(\sqrt{-g_q(z)})$. As $g_q(z)$ is totally positive, M_z is totally imaginary.

(d) The group $H = \mathbb{P}\bar{r}_3(G_{K(\zeta_3)})$ has index at most 2 in D_8 and order prime to 3, so $\bar{r}_3|_{G_{K(\zeta_3)}}$ is absolutely reducible exactly when H fixes a point of $\mathbf{P}^1$. The dihedral group of order 8 and its two Klein four-subgroups fix no point (commuting involutions of PGL_2 have disjoint fixed pairs), so reducibility forces H to be the cyclic subgroup of order 4, that is

$K(\zeta_3) = M_z$, that is $3g_q(z) \in K^{\times 2}$. But $g_q(z)$ is a square in $K_{\mathfrak{q}}$ (Lemma 3.3) and 3 is not a square in the residue field $\mathbb{F}_{q^f}$ of $\mathfrak{q}$: f is odd and $\left(\frac{3}{q}\right) = -1$ for $q \equiv 7 \pmod{12}$. □

3.3. **Scalar cochains over a totally real field.** Characters are continuous of finite order and are identified by class field theory with characters of $K_v^\times$ or of $\mathbf{A}_K^\times/K^\times$. A 2-cochain ς on G_K is *normalised* if $\varsigma(1,g) = \varsigma(g,1) = 1$. For a finite prime v of K, $U_v^{(0)} = \mathcal{O}_v^\times$, $U_v^{(i)} = 1 + \mathfrak{p}_v^i$, and e_v is the absolute ramification index. Let S_2 be the set of dyadic primes of K, $\hat{E} = \mathcal{O}_K^\times \otimes \mathbb{Z}_2$, $\hat{U}_2 = \prod_{v\in S_2} U_v^{(1)}$, and $\iota\colon \hat{E} \to \hat{U}_2$ the diagonal map. The *Leopoldt defect* $d_2(K)$ is the $\mathbb{Z}_2$-rank of the kernel of ι [43, (10.3.7)] (the real places, at which the 2-completion of the units is finite, do not change the rank); $d_2(K) = 0$ when Leopoldt's conjecture holds for K at 2, in particular when K is abelian over $\mathbb{Q}$ [43, (10.3.16)].

For $K = \mathbb{Q}$ compare [44, Lemma 4.5], and for $K = \mathbb{Q}(\sqrt{2})$ a statement of this kind is [60, Theorem 1.9]. Over a general totally real field the following proposition allows at most $d_2(K)$ auxiliary primes, and none when Leopoldt's conjecture holds for K at 2.

Proposition 3.5. *Let Z be a finite set of primes of K. There is a constant $C \geq 1$, depending only on K and Z, with the following property. Let T_0 be a finite set of finite primes of K containing S_2, let K_0/K be a finite Galois extension unramified at every finite prime outside T_0, and let ς be a normalised 2-cocycle on G_K with values in $\{\pm 1\}$, inflated from $\mathrm{Gal}(K_0/K)$, whose class in $\mathrm{Br}(K_v)$ is trivial at every finite prime $v \notin T_0$. Let T_- be the set of odd primes $v \in T_0$ at which this class has invariant $\frac{1}{2}$, and let $2^\nu = \max_{v\in T_-} 2^{v_2(Nv-1)}$ ($2^\nu = 2$ if $T_- = \emptyset$). Then there are*

- *a set Q of at most $d_2(K)$ odd primes of K, disjoint from Z, with $N\mathfrak{Q} \leq C \cdot 2^{1042\, n_K \nu}$ for $\mathfrak{Q} \in Q$, and $Q = \emptyset$ if $d_2(K) = 0$;*
- *a character χ of G_K of order $m \leq C \cdot 2^\nu$ and a continuous map $\vartheta\colon G_K \to \mu_{2m}$ with $\vartheta^2 = \chi$ and $\delta\vartheta = \varsigma$,*

such that χ and $\vartheta|_{G_{K_0}}$ (a homomorphism) are unramified at every finite prime outside $T_0 \cup Q$ and tamely ramified at every odd prime, the conductor exponent of χ at each $v \in S_2$ is at most $e_v(\nu + C)$, and the fixed field K' of the kernel of $\vartheta|_{G_{K_0}}$ satisfies $[K' : K] \leq 2m[K_0 : K]$.

Proposition 3.5 is proved in Appendix A.

3.4. **Proof of Theorem 1.6.** Fix K, q, $\mathfrak{q}$ and Σ. In this subsection $C, C', \ldots$ denote positive constants that depend only on these data and on the fixed choices made below, never on z. For $z \in \mathcal{D}$ write $\mathfrak{N} = \mathfrak{N}_\Sigma(z) \geq 1$.

Step 0. By Lemma 3.2(a), $\mathcal{D} \cap \mathcal{C}_q = \emptyset$, so $\mathfrak{N}_\Sigma$ is defined on $\mathcal{D}$. For $z \in \mathcal{D}$, $v_{\mathfrak{q}}(j_z) = 1$ (Lemma 3.3), so $j_z \notin \{0, \infty, -16/27\}$. The fibre of $\mathcal{X}$ above j_z consists of principally polarised abelian surfaces A with $O \subseteq \mathrm{End}(A \otimes \overline{K})$, and $\mathrm{End}^0(A \otimes \overline{K})$ is either B or $M_2(k)$ for an imaginary quadratic field k; in the second case we say that z has *complex multiplication*. Steps 1–8 treat the $z \in \mathcal{D}$ without complex multiplication, and Step 9 the others.

Step 1 (the cochain and r_3). Let K_z, A_z and ς be as in (S5), and let T_0 be the union of Σ and the primes $\mathfrak{P} \notin \Sigma$ at which z has positive odd contact with a point of $\mathcal{C}_q$. By (S3), K_z/K is unramified outside T_0. At a finite prime $v \notin T_0$ the restriction of ς to a decomposition group is inflated from the unramified quotient $\hat{\mathbb{Z}}$, whose second cohomology with coefficients $\{\pm 1\}$ vanishes, so the Brauer class of ς is trivial at v. Apply Proposition 3.5 with $Z = \Sigma$ and $K_0 = K_z$; it gives Q, χ of order m, ϑ and the field K_z'. The primes of T_- outside Σ divide $\mathfrak{N}$, so $2^\nu \leq C\mathfrak{N}$, and therefore

$$m \leq C\mathfrak{N}, \qquad [K_z' : \mathbb{Q}] \leq 2 \cdot 144\, n_K m \leq C\mathfrak{N}, \qquad N\mathfrak{Q} \leq C\mathfrak{N}^{1042 n_K} \quad (\mathfrak{Q} \in Q).$$

Let r_3 be the representation of (S5) for this ϑ. It is unramified at every finite prime $v \notin T_0 \cup Q$: such a v does not divide 3, the inertia group I_v lies in G_{K_z}, $\vartheta|_{I_v} = 1$, and A_z has good reduction over K_z at the primes above v, because it has potentially good reduction (proof of Lemma 3.4), so that inertia acts on $T_3(A_z)$ through a finite group, and it acts trivially on $A_z[3]$, while $1 + 3M_4(\mathbb{Z}_3)$ has no nontrivial element of finite order [54, Theorems 1 and 2].

Step 2 (the tube prime). Lemma 3.4 applies. Consequently, if Π is a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbf{A}_K)$ whose 3-adic Galois representation is r_3 up to duals and twists by characters, then $\Pi_{\mathfrak{q}}$ is supercuspidal. Indeed, Skinner's local–global compatibility at primes not above 3 [57, p. 242, (1)], valid for every totally real field, identifies the Frobenius-semisimplified Weil–Deligne representation of that Galois representation at $\mathfrak{q}$ with the Langlands parameter of $\Pi_{\mathfrak{q}} \otimes |\det|^{-1/2}$; it is irreducible by Lemma 3.4(b), as duals and twists preserve irreducibility; and an irreducible two-dimensional Weil–Deligne parameter corresponds to a supercuspidal representation [9, §§0.5 and 0.9].

Step 3 (the primes above 3). Let v be a prime of K above 3; K_v may be any finite extension of $\mathbb{Q}_3$. We show that $r_3|_{G_{K_v}}$ is potentially Barsotti–Tate and not potentially ordinary. Choose a finite extension F' of K_v that contains the completion of K'_z at a place above v and over which A_z has good reduction, and let $\mathcal{G}_3 = A_z[3^\infty]$ over the integers of F'. Then O acts on $\mathcal{G}_3$, and on $G_{F'}$, where $\vartheta = 1$, $V_3(\mathcal{G}_3) \otimes E_3 = V_3(A_z) \otimes E_3 \cong r_3^{\oplus 2}$. *$\mathcal{G}_3$ has no étale part*: $V_3(\mathcal{G}_3^{\mathrm{et}})$ is a module over $B \otimes \mathbb{Q}_3$, a division algebra of dimension 4 because 3 ramifies in B, so its dimension is 0 or at least 4; the principal polarisation identifies $\mathcal{G}_3$ with its Cartier dual, which exchanges the étale and multiplicative parts, so $2\,\mathrm{ht}(\mathcal{G}_3^{\mathrm{et}}) \le \mathrm{ht}(\mathcal{G}_3) = 4$; hence $\mathcal{G}_3^{\mathrm{et}} = 0$ [60, proof of Lemma 8.5], and the same holds after every finite extension of F'. *Potentially Barsotti–Tate*: $V_3(\mathcal{G}_3)$ is crystalline with Hodge–Tate weights 0 and 1, and $r_3|_{G_{F'}}$ is a direct summand of $V_3(\mathcal{G}_3) \otimes E_3$ with determinant the cyclotomic character, so it is crystalline with each of the weights $0, 1$ once at each embedding. *Not potentially ordinary*: suppose that for a finite extension F'' of F', $r_3|_{G_{F''}}$ had a stable line with unramified quotient. Then $V_3(\mathcal{G}_3)$ would have a nonzero unramified quotient $V_3(\mathcal{G}_3) \to W$ as a $\mathbb{Q}_3[G_{F''}]$-module; the scheme-theoretic closure of the kernel gives a 3-divisible subgroup $\mathcal{H} \subseteq \mathcal{G}_3$ over the integers of F'' with $V_3(\mathcal{G}_3/\mathcal{H}) = W$ [62, §4]. As W is unramified, it has only the Hodge–Tate weight 0, so $\mathcal{G}_3/\mathcal{H}$ has dimension 0 [62, §4], that is, it is étale and nonzero, and $\mathcal{G}_3 \to \mathcal{G}_3/\mathcal{H}$ factors through $\mathcal{G}_3^{\mathrm{et}} = 0$: a contradiction.

Step 4 (residual modularity). By Lemma 3.4(c), $\bar{r}_3|_{G_{M_z}}$ has cyclic projective image of order 4, prime to 3, so it is the sum of two distinct characters, which $G_K \setminus G_{M_z}$ exchanges; hence $\bar{r}_3 \cong \mathrm{Ind}_{G_{M_z}}^{G_K} \bar{\theta}$ for a character $\bar{\theta}$ of G_{M_z} with $\bar{\theta} \ne \bar{\theta}^c$, c the nontrivial automorphism of M_z/K. Choose a CM type Φ of the CM field M_z. On units of K the infinity type $u \mapsto \prod_{\phi\in\Phi} \phi(u)$ equals $\mathrm{N}_{K/\mathbb{Q}}(u) \in \{\pm 1\}$, and the units of K together with the roots of unity have finite index in the units of M_z; so there is an algebraic Hecke character ψ_0 of M_z of infinity type Φ. Let θ be the 3-adic character of ψ_0 multiplied by the Teichmüller lift of the finite-order character $\bar{\theta}\bar{\psi}_0^{-1}$ (of order prime to 3). Then $\theta \ne \theta^c$, the automorphic induction f of θ from M_z to K is cuspidal of parallel weight 2 [3, Chapter 3, §6, Theorem 6.2], and $\bar{\rho}_f \cong \bar{r}_3$; a change in the normalisation of ρ_f replaces $\mathrm{Ind}\,\bar{\theta}$ by its dual or by a twist by a power of the cyclotomic character, again induced from a character of M_z of the same kind, so θ can be chosen to match.

Step 5 (modularity). Gee's theorem [21, Theorem 4.1], with the erratum [22], says in the case $p = 3$ that a continuous representation $\rho\colon G_K \to \mathrm{GL}_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_3$, unramified outside a finite set of primes and with determinant a finite-order character times the 3-adic cyclotomic character, is modular if (1)

ρ is potentially Barsotti–Tate at each $v \mid 3$; (2) there is a Hilbert modular form f of parallel weight 2 over K with $\bar{\rho}_f \cong \bar{\rho}$ such that ρ_f is potentially ordinary at each $v \mid 3$ at which ρ is; and (3) $\bar{\rho}|_{G_{K(\zeta_3)}}$ is absolutely irreducible. We apply it to r_3 on a stable lattice. It is unramified outside $T_0 \cup Q$ (Step 1) with determinant $\chi_{\mathrm{cyc}}\chi^{-1}$; (1) holds by Step 3; (2) holds with the form of Step 4, the ordinarity condition being empty because r_3 is not potentially ordinary at any $v \mid 3$ (Step 3); and (3) holds by Lemma 3.4(d). So there is a cuspidal automorphic representation Π of $\mathrm{GL}_2(\mathbf{A}_K)$ of parallel weight 2, with central character of finite order, attached to r_3 in the normalisation of [33, (3.1.3) and (3.4.1)]: for almost all finite w the characteristic polynomial of r_3 at an arithmetic Frobenius is $X^2 - T_w X + N w\, S_w$, where T_w and S_w are the eigenvalues on the spherical vector of Π_w of the double cosets of $\mathrm{diag}(\varpi_w, 1)$ and $\mathrm{diag}(\varpi_w, \varpi_w)$.

Step 6 (the conductor). We show $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{n}(\Pi)) \leq C\mathfrak{N}^A$ with $A = A_0 + 2084\, n_K\, d_2(K)$, where A_0 depends only on the data. By Skinner's local–global compatibility, [57, p. 242, (1)] at $v \nmid 3$ and [57, Theorem 1] at $v \mid 3$, which apply to Π (in Skinner's notation $k_i = 2$ and $w = 0$), the conductor exponent of Π at each finite prime v is that of the Weil–Deligne representation of $r_3|_{G_{K_v}}$, defined through D_{pst} at $v \mid 3$; here r_3 is the dual of Skinner's ρ_Π (compare the Frobenius eigenvalues of Step 5), and conductors do not change under duals. The local exponents are bounded as in [60, proof of Lemma 7.6], using Proposition 3.5:

- at a dyadic v (all in Σ): r_3 restricted to G_{K_z} is the Tate action twisted by ϑ^{-1}, the Tate action is unramified at v over K_z (Step 1 with $\ell = 3$), K_z/K has degree at most 144, so its completions run through finitely many extensions of K_v, and the conductor exponent of χ at v is at most $e_v(\nu + C) \leq C'(1 + \log \mathfrak{N})$; squaring maps sufficiently deep principal units onto deeper ones, so the same bound holds for $\vartheta|_{G_{K_z}}$, and the exponent of r_3 at v is at most $C(1 + \log \mathfrak{N})$;
- at an odd $v \in \Sigma$: ϑ and χ are tame, K_z/K runs through finitely many local extensions, and at $v \mid 3$ the field $K_z(A_z[5])$ has degree bounded independently of z and A_z has good reduction at its primes w above v (Raynaud's criterion), so on the decomposition group at such a w the representation r_3 is crystalline twisted by the tame character ϑ^{-1}, and wild inertia acts on its Weil–Deligne representation through the Galois closure over K_v of the completion of $K_z(A_z[5])$ at w, one of finitely many fields; the exponent is at most C;
- at $v \in T_0 \setminus \Sigma$: the inertia of K_z/K has order at most 2 by (S3) and ϑ is tame, so r_3 is tamely ramified and its exponent is at most 2;
- at $\mathfrak{Q} \in Q \setminus T_0$: the exponent is at most 2 (tame scalar inertia); elsewhere r_3 is unramified (Step 1).

Multiplying, the primes of Σ contribute at most $C\mathfrak{N}^{C'}$, those of $T_0 \setminus \Sigma$ at most $\mathfrak{N}^2$, and those of Q at most $(C\mathfrak{N}^{1042 n_K})^{2d_2(K)}$.

Step 7 (a Shimura curve over K). Suppose first $n_K \geq 2$, and let $\tau_1, \dots, \tau_{n_K}$ be the real places of K. Let $\mathbf{B}_K$ be the quaternion algebra over K ramified exactly at $\tau_2, \dots, \tau_{n_K}$ and, when n_K is even, at $\mathfrak{q}$; the number of these places is even, so $\mathbf{B}_K$ exists [64, Main Theorem 14.6.1], and it is the algebra of [9, §0.10] with $v = \mathfrak{q}$. As [60, (7.1), Proposition 7.4 and Remark 7.5] does over $\mathbb{Q}(\sqrt{2})$, we make the comparison for the contragredient of Π. The contragredient $\Pi^\vee$ is cuspidal of parallel weight 2 with $w = 0$ in Carayol's notation [9, §0.2], and when n_K is even $\Pi^\vee_{\mathfrak{q}}$ is supercuspidal (Step 2), so $\Pi^\vee$ satisfies the hypotheses of [9, §0.3], the only one depending on the degree being the existence of an essentially square-integrable local component when n_K is even. By the Jacquet–Langlands correspondence as used in [9,

§0.10] ([29, §16]) there is an automorphic representation π' of $(\mathbf{B}_K \otimes \mathbf{A}_K)^\times$ with $\pi'_{\tau_1} \cong D_{2,0}$, $\pi'_{\tau_i} \cong D'_{2,0}$ for $i \geq 2$, and $\pi'_w \cong \Pi_w^\vee$ at every finite w at which $\mathbf{B}_K$ splits. For a sufficiently small compact open subgroup U with $(\pi'_f)^U \neq 0$, Carayol's representation $\sigma_\lambda(\pi')$ [9, §§2.2.3–2.2.4] is a two-dimensional constituent of $H^1_{\text{ét}}(M_U \otimes \overline{K}, E_\lambda)$, where M_U is Carayol's Shimura curve over K, proper because $\mathbf{B}_K$ is a division algebra, and the coefficient sheaf is constant because the weights are $k_i = 2$, $w = 0$ [9, §2.1.1]. At a finite $w \notin T_0 \cup Q$ at which Π is unramified write $\Pi_w = \mathrm{Ind}(\xi_1, \xi_2)$ (unitary induction) and $\alpha = \xi_1(\varpi_w)$, $\beta_w = \xi_2(\varpi_w)$. By Step 5, $T_w = Nw^{1/2}(\alpha + \beta_w)$ and $S_w = \alpha\beta_w$, so r_3 at an arithmetic Frobenius has eigenvalues $Nw^{1/2}\alpha$ and $Nw^{1/2}\beta_w$, and so does $r_3^\vee$ at a geometric Frobenius. On the other side [9, §0.5, p. 410] gives, for $\pi_\mathfrak{p} = \mathrm{Ind}(\xi_1, \xi_2)$,

$$\sigma(\pi_\mathfrak{p}) = \xi_1^{-1} \cdot \omega_\mathfrak{p}^{-1/2} \oplus \xi_2^{-1} \cdot \omega_\mathfrak{p}^{-1/2}, \qquad \omega_\mathfrak{p} = |\cdot|_\mathfrak{p},$$

with geometric Frobenius corresponding to uniformisers [9, §0.4]. For $\Pi_w^\vee = \mathrm{Ind}(\xi_1^{-1}, \xi_2^{-1})$ this is $\xi_1\omega_w^{-1/2} \oplus \xi_2\omega_w^{-1/2}$, with eigenvalues $Nw^{1/2}\alpha$ and $Nw^{1/2}\beta_w$ at a geometric Frobenius. By [9, Théorème (B′), p. 412] the restriction of $\sigma_\lambda(\pi')$ to a decomposition group at w is $\sigma(\pi'_w) = \sigma(\Pi_w^\vee)$, so these are its eigenvalues at a geometric Frobenius. Both representations are semisimple, and r_3 is irreducible because $\bar{r}_3$ is; by Chebotarev's theorem and the Brauer–Nesbitt theorem, $\sigma_\lambda(\pi') \cong r_3^\vee$. Dualising, with $V_\lambda(J_U) \cong H^1_{\text{ét}}(M_U \otimes \overline{K}, E_\lambda)^\vee$ for the Jacobian $J_U = \mathrm{Pic}^0_{M_U/K}$ (the product of the Jacobians of the geometric components when M_U is not geometrically connected) [41, I, Theorem 12.1(a), and III, Corollary 9.6], r_3 is isomorphic to a two-dimensional G_K-constituent of $V_3(J_U) \otimes E_3$. For n_K odd this comparison is made in the same way by Alpöge [1, §4]. If $n_K = 1$, take for M_U a modular curve and for H^1 the parabolic cohomology [9, §2.2.1], which for the constant sheaf is H^1 of the smooth compactification X_U, and $J_U = \mathrm{Pic}^0(X_U)$; the rest is unchanged.

Step 8 (heights). We follow von Känel's strategy [66]. (i) By Step 1, $V_3(A_z) \otimes E_3 \cong r_3^{\oplus 2}$ on $G_{K'_z}$, and by Step 7 and the semisimplicity of $V_3(J_U)$ [18], r_3 is a direct summand of $V_3(J_U) \otimes E_3$; so there is a nonzero $G_{K'_z}$-equivariant map $V_3(A_z) \to V_3(J_U)$, and Faltings's theorem [18] gives $\mathrm{Hom}_{K'_z}(A_z, J_U) \neq 0$ [60, Corollary 7.2]. As A_z is geometrically simple, the image B_z of a nonzero homomorphism is a two-dimensional abelian subvariety of $J_U \otimes K'_z$ isogenous to A_z over K'_z. (ii) Fix a neat compact open subgroup U_0 of $(\mathbf{B}_K \otimes \mathbf{A}_{K,f})^\times$ and a Belyi map on each geometric component of M_{U_0}; when $n_K = 1$, take $U_0 = \ker(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}))$ and on each component of X_{U_0} the Belyi map $j/1728$, under which the cusps lie over ∞. Choose $U \subseteq U_0$ with $(\pi'_f)^U \neq 0$: at a split finite w the principal congruence subgroup of level $w^{a_w(\Pi)}$ fixes the newvector and has index at most $Nw^{4a_w(\Pi)}$; at $\mathfrak{q}$, when n_K is even, $a_\mathfrak{q}(\Pi)$ is bounded (Step 6) and one fixed depth suffices. So $d_U = [U_0 : U] \leq C\ \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{n}(\Pi))^4 \leq C'\mathfrak{N}^{4A}$. (iii) The map $M_U \to M_{U_0}$ is finite étale on geometric components (when $n_K = 1$, the map $X_U \to X_{U_0}$ is étale outside the cusps, which lie over $\{0, 1, \infty\}$); composed with the fixed Belyi maps it gives each component $M_{U,i}$ (of X_U when $n_K = 1$) a Belyi map of degree $d_i \leq Cd_U$, so that its genus is at most $(d_i - 1)/2$ by the Riemann–Hurwitz formula, so Javanpeykar's bound [32, Theorem 1.1.1] gives $h_F(J_U) \leq C\sum_i d_i^6 \leq C'\mathfrak{N}^{24A}$, where h_F is the stable Faltings height, and $\dim J_U \leq C\mathfrak{N}^{4A}$. (iv) Over K'_z, with $[K'_z : \mathbb{Q}] \leq C\mathfrak{N}$, Gaudron and Rémond's bounds [20, Corollary 1.5 and Theorem 1.4] give $h_F(B_z) \leq h_F(J_U) + \frac{1}{2}\log\kappa_{\mathrm{GR}}(J_U) \leq C\mathfrak{N}^{24A}$ and an isogeny between B_z and A_z of degree at most $\kappa_{\mathrm{GR}}(B_z)$ with $\log\kappa_{\mathrm{GR}}(B_z) \leq C(1 + \log\mathfrak{N})$, so $h_F(A_z) \leq C\mathfrak{N}^{24A}$ (compare [60, proof of Proposition 7.7]). (v) On the fixed curve, Pazuki's comparison of the theta height with the Faltings height [48, Theorem 1.1 and Corollary 1.3(2)] gives $h(j_z) \leq C(1 + \max(0, h_F(A_z)))$ [60, proof of Proposition 7.7], and

$z \mapsto j(x_q(z))$ is a rational function of degree 6 over $\mathbb{Q}$, so $h(z) \le \frac{1}{6}h(j_z) + C$. Hence there is H_1 with $h(z) \le H_1\mathfrak{N}^{24A}$ for every $z \in \mathcal{D}$ without complex multiplication.

Step 9 (complex multiplication). Let $z \in \mathcal{D}$ have complex multiplication. Since $j_z \in K$, the moduli point P_z of the fibre on the Shimura curve X of O over $\mathbb{Q}$ lies above a point of X/W of degree at most n_K over $\mathbb{Q}$, so $[\mathbb{Q}(P_z) : \mathbb{Q}] \le 4n_K$. The point P_z is a CM point for an optimal embedding of an order S of an imaginary quadratic field k into O; it is defined over the ring class field H_S of S, and $\mathrm{Gal}(H_S/k) \cong \mathrm{Pic}(S)$ acts on such points with orbits of size at least $h(S)/4$ [64, §43.8.2, (43.8.3)–(43.8.4), Corollary 30.4.23] (the reduced norm maps $O^\times$ onto $\{\pm 1\}$, and an embedding and its conjugate fix the same point). So $h(S) \le 4[k(P_z) : k] \le 16n_K$. There are finitely many imaginary quadratic orders of class number at most $16n_K$ ([27], and the class number formula for orders [12, Theorem 7.24]), finitely many CM points for each, and $z \mapsto j_z$ has degree 6; so the $z \in \mathcal{D}$ with complex multiplication are finitely many (compare [60, Lemma 8.7]). Put $H = \max(H_1, \max h(z))$, the inner maximum over these z, and $\kappa = 24A$. Since $\mathfrak{N} \ge 1$, $h(z) \le H\mathfrak{N}^\kappa$ for every $z \in \mathcal{D}$. □

4. Primes in a quadratic pattern

For a Gaussian integer π put $d_+(\pi) = \mathrm{N}(\pi + 1)$ and $d_-(\pi) = \mathrm{N}(\pi - 1)$. The completeness proof (Section 9) needs primes $u + c_j w^2$ with prescribed Gaussian generators whose adjacent norms are coprime across the pattern. For $(\ell, r) = (13, 1 + 2i)$ and without the class modulo N_0 this is [60, Proposition 10.3]; we need the following form, which we derive from [58, Theorem 4.1] and the appendix of [68].

Theorem 4.1. *Let (ℓ, r) be $(13, 1 + 2i)$ or $(7, 1 + 3i)$. Let $k \ge 2$, let $c_1, \dots, c_k$ be pairwise distinct integers, let D_0 and Y be positive integers, $\Lambda_0 > 0$ a real number, N_0 an odd squarefree positive integer prime to 6ℓ, and $\mathcal{S}$ a finite set of primes. There are positive integers u, w with $D_0 \mid w$ and $u/w^2 > \Lambda_0$ such that the numbers $p_j = u + c_j w^2$ are distinct primes greater than Y and not in $\mathcal{S}$, and each p_j is the norm of a Gaussian prime π_j with*

(i) $\pi_j \equiv 9 \pmod{16}$, $\pi_j \equiv i \pmod 3$, $\pi_j \equiv r \pmod \ell$ *and* $\pi_j \equiv i \pmod{N_0}$;
(ii) $v_2(d_+(\pi_j)) = 2$, $v_2(d_-(\pi_j)) = 6$, *and* $\gcd(d_+(\pi_j), d_-(\pi_h)) = 4$ *for all* j, h;
(iii) $d_+(\pi_j)d_-(\pi_j)$ *is prime to* $3\ell N_0$.

The congruences (i) also give the following, which is how the theorem is used.

Lemma 4.2. *Let (ℓ, r) be $(13, 1 + 2i)$ for the first curve and $(7, 1 + 3i)$ for the second, let N_0 be an odd squarefree positive integer prime to 6ℓ, let π be a Gaussian prime with $\pi \equiv 9 \pmod{16}$, $\pi \equiv i \pmod 3$, $\pi \equiv r \pmod \ell$ and $\pi \equiv i \pmod{N_0}$, and $p = \mathrm{N}(\pi)$. Then $p \equiv 1 \pmod{48}$, $p \equiv \mathrm{N}(r) \pmod \ell$, π is primary, $v_2(d_+(\pi)) = 2$, $v_2(d_-(\pi)) = 6$, and $d_+(\pi)d_-(\pi)$ is prime to $3\ell N_0$. In particular, by Lemma 2.9(a), p splits in F and the reductions of E at the two primes of F above p have orders $d_-(\pi)$ and $d_+(\pi)$.*

Proof. Write $\pi = x + yi$ with $x = 9 + 16x'$, $y = 16y'$. Then $p \equiv 81 \equiv 1 \pmod{16}$, $p \equiv \mathrm{N}(i) = 1 \pmod 3$ and $p \equiv \mathrm{N}(r) \pmod \ell$, that is $p \equiv \mathrm{N}(1 + 2i) = 5 \pmod{13}$, respectively $p \equiv \mathrm{N}(1 + 3i) = 10 \equiv 3 \pmod 7$. Since $\pi - 1 \equiv 8 \pmod{16}$ and $8 = (2 + 2i)(2 - 2i)$, π is primary. Next $d_+(\pi) = (x + 1)^2 + y^2$ with $x + 1 = 2 \cdot \text{odd}$, so $d_+(\pi) \equiv 4 \pmod{32}$, and $d_-(\pi) = (x - 1)^2 + y^2 = 64\big((1 + 2x')^2 + 4y'^2\big)$ with an odd second factor. Finally $d_\pm(\pi) \equiv \mathrm{N}(i \pm 1) = 2$ modulo 3 and modulo every prime of N_0, and $d_\pm(\pi) \equiv \mathrm{N}(r \pm 1)$ modulo ℓ: these are $\mathrm{N}(2 + 2i) = 8$ and $\mathrm{N}(2i) = 4$ modulo 13 for $r = 1 + 2i$, and $\mathrm{N}(2 + 3i) = 13 \equiv 6$ and $\mathrm{N}(3i) = 9 \equiv 2$ modulo 7 for $r = 1 + 3i$, all units. □

Proof of Theorem 4.1. We use the appendix "Simultaneous primes with coprime adjacent norms" of [68], which follows the strategy of [44, §6] and [58]. Its main theorem, which is [58, Theorem 4.1], reads: for distinct integers $c_1, \dots, c_k$ ($k \geq 2$), $q \geq 1$, an odd squarefree M with $7 \nmid M$, and $H, Y > 0$, there are positive integers u, w with $q \mid w$, $u/w^2 > H$ and every $p_j = u + c_j w^2 > Y$ prime, such that each p_j has a Gaussian prime generator π_j with $\pi_j \equiv 9 \pmod{16}$, $\pi_j \equiv 1 + 3i \pmod 7$ and $\pi_j \equiv i \pmod M$; no odd prime divides both $d_-(\pi_j)$ and $d_+(\pi_j)$, nor, for $j \neq h$, both $d_\epsilon(\pi_j)$ and $d_\eta(\pi_h)$ for any signs ϵ, η; $v_2(d_-(\pi_j)) = 6$, $v_2(d_+(\pi_j)) = 2$ and $\gcd(d_-(\pi_j), d_+(\pi_h)) = 4$ for all j, h; and all these norms are prime to M. For $(\ell, r) = (7, 1 + 3i)$ we apply it with $M = 3N_0$, which is odd, squarefree and prime to 7, $q = D_0$, $H = \Lambda_0$, and Y larger than every element of $\mathcal{S}$. For $(\ell, r) = (13, 1 + 2i)$ we apply it in the same way with 13 and $1 + 2i$ in place of 7 and $1 + 3i$ (so with $13 \nmid M$). The class modulo 7 enters the proof in three places: the base residue, modulo a multiple of $16 \cdot 7M$, must be a unit residue that is $1 + 3i$ modulo 7; the two complex-conjugate ray classes it determines are distinct (an equality would make the base residue a Gaussian unit times its conjugate; modulo 16 the unit must be 1, and then $1 + 3i \equiv 1 - 3i \pmod 7$, which is false); and the adjacent norms of $1 + 3i$ are units modulo 7. All three hold for $1 + 2i$ modulo 13: $\mathrm{N}(1 + 2i) = 5$ is prime to 13; $1 - 2i \not\equiv 1 + 2i \pmod{13}$; and $\mathrm{N}(2 + 2i) = 8$ and $\mathrm{N}(2i) = 4$ are units modulo 13. In both cases $\pi_j \equiv i \pmod 3$ because $3 \mid M$; distinct c_j give distinct p_j; and (ii), (iii) are part of the conclusion and of Lemma 4.2.

The proof of the appendix's theorem, with these substitutions, rests on the following published results, each applied at a fixed ray class field of $\mathbb{Q}(i)$ and a fixed modulus: Mitsui's prime ideal theorem for Hecke characters of a fixed field [42, §1, Lemma 15, p. 12]; the quantitative equidistribution of polynomial orbits on nilmanifolds [24, Theorem 2.9 and Lemma 4.5], the orthogonality of the Möbius function to nilsequences [23, §§2–3] and the inverse theorem for the Gowers norms [25, Theorem 1.3]; the normal form of linear systems, the linear forms and correlation conditions, the pseudorandom majorant and the generalised von Neumann theorem of [26, Lemma 4.4, Definitions 6.1–6.3, Propositions 6.4 and 7.1, Appendix D]; the inverse theorem for interval norms of [16, Theorem 5.1]; the dense model and local uniformity theorems and the polynomial forms condition for polynomial patterns of [61, Theorems 9, 11, 13 and 15, Corollary 3, Proposition 6]; and the sieves for quadrics of [6, Theorem 4.1] and [7, Lemmas 2.1 and 4.1]. The appendix follows the ideal-norm method of Frei and Tinková [19, Theorem 1.4]. Two of these results are stated for the modulus $\prod_{p \leq w} p$: Tao and Ziegler's theorems, and Green and Tao's majorant. The appendix applies them at the moduli $\Delta \prod_{p \leq v,\, p \nmid \Delta} p$ and $V_z = \Delta \prod_{p \leq z,\, p \nmid \Delta} p$, where Δ is its fixed modulus, a multiple of the conductor of the maximal abelian subfield of its ray class field. Appendix C carries out these two steps (Lemmas C.1 and C.2). They hold for every fixed Δ, so for both choices of (ℓ, r). With them in place of the appendix's two steps, its argument gives the theorem; its conclusion is ineffective, through Siegel zeros in Mitsui's theorem and a qualitative error term. □

For the third and fourth curves the reductions at the two primes above a pattern prime have orders $\mathrm{N}(\pi - \epsilon)$ and $\mathrm{N}(\pi - \eta i)$ with unknown signs (Lemma 2.9(b)), so the pattern has to control all four norms $\mathrm{N}(\pi - \alpha)$, $\alpha \in \{\pm 1, \pm i\}$. We derive the following from the appendix of [68] in the same way.

Theorem 4.3. *Let (ℓ, r) be $(7, 1 + 3i)$ or $(89, 1 + 5i)$. Let $k \geq 2$, let $c_1, \dots, c_k$ be pairwise distinct integers, let D_0 and Y be positive integers, $\Lambda_0 > 0$ a real number, N_0 an odd squarefree positive integer prime to 30ℓ, and $\mathcal{S}$ a finite set of primes. There are positive*

integers u, w with $D_0 \mid w$ and $u/w^2 > \Lambda_0$ such that the numbers $p_j = u + c_j w^2$ are distinct primes greater than Y and not in $\mathcal{S}$, and each p_j is the norm of a Gaussian prime π_j with

(i) $\pi_j \equiv 9 \pmod{16}$, $\pi_j \equiv 1+i \pmod 3$, $\pi_j \equiv 6 \pmod{25}$, $\pi_j \equiv r \pmod \ell$ *and* $\pi_j \equiv 1+i \pmod{N_0}$;

(ii) *for all j, h, $j = h$ included, and all $\epsilon, \eta \in \{1, -1\}$, no odd prime divides both $\mathrm{N}(\pi_j - \epsilon)$ and $\mathrm{N}(\pi_h - \eta i)$; and $v_2(\mathrm{N}(\pi_j - 1)) = 6$, $v_2(\mathrm{N}(\pi_j + 1)) = 2$, $v_2(\mathrm{N}(\pi_j \mp i)) = 1$;*

(iii) $v_5(\mathrm{N}(\pi_j - 1)) = 2$, 5 *divides none of* $\mathrm{N}(\pi_j + 1)$, $\mathrm{N}(\pi_j - i)$, $\mathrm{N}(\pi_j + i)$, *and each* $\mathrm{N}(\pi_j - \alpha)$, $\alpha \in \{\pm 1, \pm i\}$, *is prime to $3\ell N_0$.*

Lemma 4.4. *Let (ℓ, r) be $(7, 1+3i)$ for the third curve and $(89, 1+5i)$ for the fourth, let N_0 be an odd squarefree positive integer prime to 30ℓ, divisible by 17 for the fourth curve, let π be a Gaussian prime with the congruences* (i) *of Theorem 4.3, and $p = \mathrm{N}(\pi)$. Then $p \equiv 1 \pmod{16}$, $p \equiv 2 \pmod 3$, $p \equiv \mathrm{N}(r) \pmod \ell$, π is primary, and the four norms $\mathrm{N}(\pi - \alpha)$ have the valuations at 2 and 5 stated in Theorem 4.3*(ii), (iii) *and are prime to $3\ell N_0$. Moreover p splits in F, $p \notin \mathcal{P}$ and $\left(\frac{\mathrm{N}_{F/\mathbb{Q}}(A)}{p}\right) = -1$; so, by Lemma 2.9*(b), *the reductions of E at the prime $\mathfrak{p}_+$ of F above p at which A is a square and at $\sigma\mathfrak{p}_+$ have orders $\mathrm{N}(\pi - \epsilon)$ and $\mathrm{N}(\pi - \eta i)$ for some $\epsilon, \eta \in \{1, -1\}$.*

Proof. Write $\pi = x + yi$. As in the proof of Lemma 4.2, $p \equiv 1 \pmod{16}$, π is primary, $v_2(\mathrm{N}(\pi - 1)) = 6$ and $v_2(\mathrm{N}(\pi + 1)) = 2$; and $\mathrm{N}(\pi \mp i) = x^2 + (y \mp 1)^2$ with x and $y \mp 1$ odd is 2 modulo 4. Since $\pi - 1 = 5(1 + 5t)$ with $t \in \mathbb{Z}[i]$, $\mathrm{N}(\pi - 1) = 25\,\mathrm{N}(1 + 5t)$ with $\mathrm{N}(1 + 5t) \equiv 1 \pmod 5$; and as $\pi \equiv 1 \pmod 5$, $\mathrm{N}(\pi + 1) \equiv 4$ and $\mathrm{N}(\pi \mp i) \equiv 2 \pmod 5$. Modulo 3 and modulo every prime of N_0, $p \equiv \mathrm{N}(1 + i) = 2$, and the norms $\mathrm{N}(1 + i - \alpha)$ are 1, 5, 1, 5 for $\alpha = 1, -1, i, -i$, units as $5 \nmid N_0$. Modulo ℓ, $p \equiv \mathrm{N}(r)$, which is $10 \equiv 3 \pmod 7$, respectively $26 \pmod{89}$, and the norms $\mathrm{N}(r - \alpha)$ are 9, 13, 5, 17, that is 2, 6, 5, 3 modulo 7, respectively 25, 29, 17, 37, units modulo 89. For the third curve, $\left(\frac{2}{p}\right) = 1$ as $p \equiv 1 \pmod 8$, so p splits in $\mathbb{Q}(\sqrt{2})$; $p \neq 7$; and $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right) = \left(\frac{3}{7}\right) = -1$. For the fourth, $17 \mid N_0$ gives $p \equiv 2 \pmod{17}$, so $\left(\frac{17}{p}\right) = \left(\frac{2}{17}\right) = 1$ and p splits in $\mathbb{Q}(\sqrt{17})$; $p \notin \{2, 17, 89\}$; and, as $p \equiv 1 \pmod 8$ and $89 \equiv 1 \pmod 4$, $\left(\frac{-178}{p}\right) = \left(\frac{p}{89}\right) = \left(\frac{26}{89}\right) = \left(\frac{13}{89}\right) = \left(\frac{11}{13}\right) = -1$. □

Proof of Theorem 4.3. We apply the appendix of [68] as in the proof of Theorem 4.1, with $M = 3N_0$, $q = D_0$, $H = \Lambda_0$, Y larger than every element of $\mathcal{S}$, and ℓ, r in place of 7, $1 + 3i$. The adjacent norms and the base class enter its proof at the following places, which change as stated; the rest of the proof is unchanged.

(1) The statement: the classes (i) and the conclusions (ii), (iii). The forbidden common divisors are those of (ii): the appendix's condition that no odd prime divide two of the norms $\mathrm{N}(\pi_j \pm 1)$ is dropped, as 5 divides every $\mathrm{N}(\pi_j - 1)$.

(2) The counts over finite fields and the sieve over medium primes, for two positions. A count in which $\mathrm{N}(z' - \eta i)$ vanishes for the second Gaussian integer z' becomes, after the substitution $z' \mapsto -iz'$, the count in which $\mathrm{N}(z' + \eta)$ vanishes: the substitution preserves the norm of z', the box and the region of the appendix, and $\mathrm{N}(-iz' + \eta) = \mathrm{N}(z' + \eta i)$. So the counts, and the bounds the appendix proves for them, are unchanged; the sieve of [6, Theorem 4.1] sees the residue sets only through their sizes.

(3) Large common divisors: the same substitution reduces each new pair of norms to a pair the appendix treats.

(4) One position: an odd prime dividing both $\mathrm{N}(z - \epsilon) = (a - \epsilon)^2 + b^2$ and $\mathrm{N}(z - \eta i) = a^2 + (b - \eta)^2$, $z = a + bi$, divides their difference $2(\eta b - \epsilon a)$; so $b \equiv \epsilon\eta a$ and it divides

$2a^2 - 2\epsilon a + 1$. The polynomials $b - \epsilon\eta a$ and $2a^2 - 2\epsilon a + 1$ have no common factor and no common prime content, so [7, Lemma 2.1] gives the bound of the appendix for this pair.

(5) The base residue is 9 modulo 16, r modulo ℓ, 6 modulo 25, and $1 + i$ modulo the other odd primes of the fixed modulus. It is a unit residue, and the two complex-conjugate ray classes it determines are distinct, as in the proof of Theorem 4.1, since $r \not\equiv \bar{r} \pmod{\ell}$.

(6) The abelian fibres: at a cutoff prime the condition is that none of the four norms $\mathrm{N}(z - \alpha)$ vanishes. In a fibre of the norm this excludes at most 8 residues, two for each α, and the set of allowed residues is stable under conjugation; so the lower bounds of the appendix hold with $1 - 8/(\ell' - 1)$ and $(\log L)^{-8k}$ in place of $1 - 4/(\ell' - 1)$ and $(\log L)^{-4k}$.

(7) The final choice of L, with $(\log L)^{8k}$ in place of $(\log L)^{4k}$. The ray conditions exclude every odd prime at most L from each of the four norms $\mathrm{N}(\pi_j - \alpha)$, except 5, which divides $\mathrm{N}(\pi_j - 1)$ only, exactly to the power 2; the valuations at 2 and 5 and the units at 3, ℓ and N_0 are those of Lemma 4.4.

The class prime ℓ divides the fixed modulus, so it is never a cutoff prime. The proof rests on the published results listed in the proof of Theorem 4.1, with the two steps of Appendix C, which hold for every fixed modulus; its conclusion is ineffective, as there. □

5. The pole predicate

Let $\mathcal{M} = \{\mu_0,\ 17\mu_0 :\ \mu_0 \in \{1, 2, 3, 5, 6, 7, 10, 14\}\}$, a set of sixteen positive integers whose prime factors are $2, 3, 5, 7$ and 17. For a field $k \supseteq \mathbb{Q}$ and $b \in k$, let $\Phi_k(b)$ be the statement: $b = 0$, or for some $\mu \in \mathcal{M}$, with

$$A = \mu b \quad \text{and} \quad H_b = A(A - b^2),$$

there are $e, w \in k$ with $A\,e\,H_b\,w \neq 0$ such that

$$A(A - e)(A + e) \qquad \text{and} \qquad A(Aw^2 - eH_b)(Aw^2 + eH_b) \tag{5.1}$$

are squares in k. This is the predicate of [44, (3.2)] in the two-parameter form of [58, Proposition 2.5], with the curves $y^2 = x(x - e)(x + 3e)$ replaced by the congruent-number twists $y^2 = x^3 - e^2x$ as in [31], and with the list $\mathcal{M}$.

Lemma 5.1. *Let k be a number field, $b \in k^\times$ with $\Phi_k(b)$, and $\mathfrak{P}$ a prime of k not above $2, 3, 5, 7$ or 17. If $v_\mathfrak{P}(b) < 0$, then $v_\mathfrak{P}(b)$ is even.*

Proof. Write $v = v_\mathfrak{P}$ and suppose $v(b) = r < 0$ is odd; let μ be the multiplier used, a $\mathfrak{P}$-unit. Then $v(A) = r$, $v(b^2) = 2r < r$, so $v(A - b^2) = 2r$ and $v(H_b) = 3r$ is odd. Hence $v(e)$ and $v(eH_b)$ have opposite parities. Let $\ell \in \{e, eH_b\}$ be the one of even valuation $2s$, ϖ a uniformiser at $\mathfrak{P}$, and $L = \ell/\varpi^{2s}$, a unit. If $\ell = e$, put $X = A/\varpi^{2s}$ and $Y = \sigma_1/\varpi^{3s}$ with $\sigma_1^2 = A(A - e)(A + e)$; if $\ell = eH_b$, put $X = Aw^2/\varpi^{2s}$ and $Y = w\sigma_2/\varpi^{3s}$ with $\sigma_2^2 = A(Aw^2 - eH_b)(Aw^2 + eH_b)$. In both cases $X(X - L)(X + L) = Y^2$ and $v(X)$ is odd, so $X \neq 0, \pm L$. If $v(X) > 0$ then $X \mp L$ are units and $v(X(X - L)(X + L)) = v(X)$; if $v(X) < 0$ then $v(X \mp L) = v(X)$ and the valuation is $3v(X)$. In both cases it is odd, while $v(Y^2)$ is even. □

The completeness proof rests on the following theorem.

Theorem 5.2 ([31, Theorem 1.2])**.** *Let $\beta > 1$ and $\theta \geq 1$ be coprime squarefree integers with $\beta \equiv \theta \equiv 1 \pmod 8$, such that θ is a square modulo every prime dividing β and β is a square modulo every prime dividing θ. Then there is a positive squarefree integer n such that the curves $y^2 = x^3 - n^2x$ and $y^2 = x^3 - (n\theta)^2x$ both have analytic rank one and Mordell–Weil rank one, and each has a rational point of infinite order with abscissa in $\beta\mathbb{Q}^{\times 2}$.*

Lemma 5.3. *Let $B \in \mathbb{Q}$ with $0 < B < 1$, with square reduced denominator, $v_2(B) \geq 4$, and $v_p(B) \geq 2$ for $p \in \{3, 5, 7, 17\}$. Then $\Phi_{\mathbb{Q}}(B)$ holds with $e, w \in \mathbb{Q}$; in particular $\Phi_k(B)$ holds for every field $k \supseteq \mathbb{Q}$.*

Proof. The multiplier. Write $B = 2^j u$ with $u \in \mathbb{Z}_2^\times$. Then $\mu_0 B \in \mathbb{Q}_2^{\times 2}$ exactly when $v_2(\mu_0) \equiv j \pmod 2$ and the odd part of μ_0 times u is 1 modulo 8; the odd parts of $1, 3, 5, 7$ and of $2, 6, 10, 14$ each run once through the odd classes modulo 8, so exactly one μ_0 has $\mu_0 B \in \mathbb{Q}_2^{\times 2}$. Put $\mu = 17\mu_0$ if $\mu_0 B$ is a rational square and $\mu = \mu_0$ otherwise. Then $\mu B \in \mathbb{Q}_2^{\times 2}$ and μB is not a rational square.

The pair. Let β, θ be the positive squarefree integers with $A = \mu B \in \beta\mathbb{Q}^{\times 2}$ and $H_B = \mu B^2(\mu - B) \in \theta\mathbb{Q}^{\times 2}$; so θ is the squarefree part of $\mu(\mu - B)$ and of $1 - B/\mu$. We check the hypotheses of Theorem 5.2. Both are positive as $\mu \geq 1 > B > 0$, and $\beta > 1$ as μB is not a square. At 2: β is odd and $\equiv 1 \pmod 8$ since $\mu B \in \mathbb{Q}_2^{\times 2}$; $v_2(B/\mu) \geq 3$, so $1 - B/\mu \in 1 + 8\mathbb{Z}_2$ and $\theta \equiv 1 \pmod 8$. At $p \in \{3, 5, 7, 17\}$: $v_p(\mu) \leq 1$, so $1 - B/\mu \in 1 + p\mathbb{Z}_p$, hence $p \nmid \theta$ and θ is a nonzero square modulo p. At an odd prime $p \notin \{3, 5, 7, 17\}$: if $v_p(B) > 0$, then $1 - B/\mu \in 1 + p\mathbb{Z}_p$, so $p \nmid \theta$ and θ is a square modulo p, and $p \mid \beta$ exactly when $v_p(B)$ is odd; if $v_p(B) < 0$, it is even, so $p \nmid \beta$, and $1 - B/\mu = -(B/\mu)(1 - \mu/B)$ has even valuation, so $p \nmid \theta$; if $v_p(B) = 0$, then $p \nmid \beta$, and if $p \mid \theta$ then $B \equiv \mu \pmod p$, so $\mu B \equiv \mu^2$ and β is a nonzero square modulo p. So every prime dividing β is prime to θ and θ is a square modulo it, and β is a square modulo every prime dividing θ.

The witnesses. Theorem 5.2 gives n and points P_1 on $y^2 = x^3 - n^2x$ and P_2 on $y^2 = x^3 - (n\theta)^2x$ with $x(P_1), x(P_2) \in \beta\mathbb{Q}^{\times 2} = A\mathbb{Q}^{\times 2}$. Write $x(P_1) = A\lambda^2$ and $H_B = \theta c^2$ with $\lambda, c \in \mathbb{Q}^\times$, and put $e = n/\lambda^2$. The map $(x, y) \mapsto (x/\lambda^2, y/\lambda^3)$ takes $y^2 = x^3 - n^2x$ to $y^2 = x^3 - e^2x$ and P_1 to a point with abscissa A, so $A(A - e)(A + e) = (y(P_1)/\lambda^3)^2$. With $\rho = c/\lambda$ we have $eH_B = n\theta\rho^2$, and $(x, y) \mapsto (\rho^2 x, \rho^3 y)$ takes $y^2 = x^3 - (n\theta)^2x$ to $y^2 = x^3 - (eH_B)^2x$ and P_2 to a point with abscissa $\rho^2 x(P_2) = Aw^2$, $w \in \mathbb{Q}^\times$; then $w^2 \cdot A(Aw^2 - eH_B)(Aw^2 + eH_B) = (\rho^3 y(P_2))^2$. Finally $A, e, H_B, w \neq 0$. □

6. Local lemmas

6.1. Integers, a Lucas relation and heights.

Lemma 6.1 ([60, Lemma 12.1])**.** *Let k be a totally real number field and $x \in k$. Then $x^3 + x \in \mathbb{Z}$ if and only if $x \in \mathbb{Z}$.*

Proof. If $x^3 + x = c \in \mathbb{Z}$, then x is a root of $T^3 + T - c$, so it is an algebraic integer, and every conjugate of x is a real root of this polynomial. As $t \mapsto t^3 + t$ is strictly increasing on $\mathbb{R}$, there is only one real root, so x equals all its conjugates and lies in $\mathbb{Q}$; being integral, $x \in \mathbb{Z}$. The converse is clear. □

Put

$$\mathcal{L}(X_1, X_2, X_3, X_4) = X_3^2 - X_2(X_2 - 2)X_3X_4 + (X_2 - 2)^2X_4^2 - 1, \tag{6.1}$$

a polynomial that does not involve X_1.

Lemma 6.2 ([60, Lemma 12.4], [69, Lemma 14.9])**.** (a) *If $n_2, n_3, n_4 \in \mathbb{Z}$, $|n_2| \geq 7$, $n_4 \neq 0$ and $\mathcal{L}(X_1, n_2, n_3, n_4) = 0$, then $|n_3| > \exp(|n_2| - 3)$.*

(b) *For every integer $n_2 \geq 7$ there are positive integers n_3, n_4 with $\mathcal{L}(X_1, n_2, n_3, n_4) = 0$.*

Proof. Put $a = |n_2|$, $w = \operatorname{sgn}(n_2)(n_2 - 2)n_4$, so that $\mathcal{L} = 0$ reads $n_3^2 - an_3w + w^2 = 1$. Let $U_0 = 0$, $U_1 = 1$, $U_{k+1} = aU_k - U_{k-1}$, and $\rho = (a + \sqrt{a^2 - 4})/2 > 1$, so that $\rho + \rho^{-1} = a$ and $U_k = (\rho^k - \rho^{-k})/(\rho - \rho^{-1})$. The integer solutions (t, w) of $t^2 - atw + w^2 = 1$ are the pairs with $t - w\rho^{-1}$, or equivalently $t - w\rho$, a unit of norm one of $\mathbb{Z}[\rho]$, and the units of norm one of $\mathbb{Z}[\rho]$ are $\pm\rho^k$, $k \in \mathbb{Z}$: a unit $\upsilon > 0$ of norm one can be moved into $[1, \rho)$ by a power of ρ, and then $\upsilon = c_0 + c_1\rho$ with $c_1 = (\upsilon - \upsilon^{-1})/(\rho - \rho^{-1}) \in [0, 1) \cap \mathbb{Z} = \{0\}$, so $\upsilon = 1$. For $k \geq 0$, induction gives $\rho^k = U_{k+1} - U_k\rho^{-1}$, hence $\rho^{-k} = U_{k+1} - U_k\rho$ and, with $\rho^{-1} = a - \rho$, $\rho^k = -U_{k-1} + U_k\rho$ for $k \geq 1$. So the solutions with $w \neq 0$ have $|w| = U_k$ and $|t| \in \{U_{k-1}, U_{k+1}\}$ for some $k \geq 1$.

(a) Here $w \neq 0$. Since $a \equiv 2 \pmod{a-2}$ and $a \equiv -2 \pmod{a+2}$, induction gives $U_k \equiv k \pmod{a-2}$ and $U_k \equiv (-1)^{k-1}k \pmod{a+2}$. The integer $|n_2 - 2|$, which is $a - 2$ if $n_2 > 0$ and $a + 2$ if $n_2 < 0$, divides w, hence U_k, hence k; so $k \geq a - 2$. Since $U_{j+1} \geq (a-1)U_j$ for $j \geq 1$, $|n_3| \geq U_{k-1} \geq (a-1)^{k-2} \geq (a-1)^{a-4}$, and $(a-1)^{a-4} > e^{a-3}$ for $a \geq 7$ (at $a = 7$, $216 > e^4$, and $(a-4)\log(a-1) - (a-3)$ increases with a).

(b) Take $a = n_2$, $k = 2(n_2 - 2)$, $n_3 = U_{k+1}$ and $n_4 = U_k/(n_2 - 2)$, an integer as $U_k \equiv k \equiv 0 \pmod{n_2 - 2}$. Then $\mathcal{L} = U_{k+1}^2 - aU_{k+1}U_k + U_k^2 - 1 = 0$, and both are positive. □

For $\alpha \in K^\times$ let $\mathfrak{a}(\alpha) = \prod_{v_\mathfrak{P}(\alpha) > 0} \mathfrak{P}^{v_\mathfrak{P}(\alpha)}$ be its numerator ideal. With $h(\alpha) = \frac{1}{n_K}\sum_v n_v \log\max(1, |\alpha|_v)$, the sum over the places of K with local degrees n_v, the product formula gives

$$\log \mathrm{N}\,\mathfrak{a}(\alpha) = \sum_{v_\mathfrak{P}(\alpha) > 0} v_\mathfrak{P}(\alpha) \log N\mathfrak{P} \leq \sum_{v \text{ finite}} n_v \log\max(1, |\alpha^{-1}|_v) \leq n_K h(\alpha^{-1}) = n_K h(\alpha). \tag{6.2}$$

We also use that a rational function φ of degree d over $\mathbb{Q}$, a morphism $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d, satisfies $h(\varphi(t)) = d\,h(t) + O(1)$ for $t \in \overline{\mathbb{Q}}$ ([56, Theorem VIII.5.6], after taking logarithms), and the elementary bounds $h(st) \leq h(s) + h(t)$ and $h(s + t) \leq h(s) + h(t) + \log 2$.

6.2. **The formal group of the index curve.** For a point $V \neq O$ of E put $\rho(V) = 1/x(V)$ and $\mathfrak{z}(V) = -x(V)/y(V)$ when these are defined, and $\rho(O) = \mathfrak{z}(O) = 0$. Let $\ell(T) = \sum_{t \geq 1}(c_t/t)T^t$ be the formal logarithm of E at the parameter $\mathfrak{z}$, normalised by $c_1 = 1$; its coefficients lie in F, and $\ell_m(T) = \sum_{t \leq m}(c_t/t)T^t$ is its truncation in degree m. For the conjugate curve E^σ the same objects are ℓ^σ, ℓ_m^σ, with conjugate coefficients.

Setting. Let $\mathcal{Q}$ be a prime of L, or of F, above a rational prime $p \geq 5$, $p \notin \mathcal{P}$, with $\mathcal{Q}$ unramified over $\mathbb{Q}$. Let R be the valuation ring of $L_\mathcal{Q}$, $\mathfrak{m}$ its maximal ideal and v its valuation, with $v(p) = 1$. By (E2) the equation (1.1) has good reduction at $\mathcal{Q}$ and is minimal there, and so does its conjugate. Let $E_1(L_\mathcal{Q}) = \{O\} \cup \{V : v(x(V)) < 0\}$ be the kernel of reduction. From [56]: the formal group of (1.1) is defined over R [56, Example IV.2.2.3]; its normalised invariant differential has coefficients in R [56, Proposition IV.4.2], so $c_t \in R$ [56, §IV.5]; $V \mapsto \mathfrak{z}(V)$ is an isomorphism of $E_1(L_\mathcal{Q})$ onto the formal group on $\mathfrak{m}$, with $v(x(V)) = -2v(\mathfrak{z}(V))$ for $V \neq O$ [56, Proposition VII.2.2 and Proposition IV.1.1]; and ℓ is a homomorphism from the formal group on $\mathfrak{m}$ to $L_\mathcal{Q}$ [56, §§IV.5–IV.6]. In particular $V \in E_1(L_\mathcal{Q})$ if and only if $v(\rho(V)) \geq 1$.

Lemma 6.3. *In the Setting, let $Z \in \mathfrak{m}$.*

(a) *$v(\ell(Z)) = v(\ell_m(Z)) = v(Z)$ for every $m \geq 1$.*

(b) *If $p > m + 1$, then $v(\ell(Z) - \ell_m(Z)) \geq v(Z) + m$.*

(c) *Let $Y \in E(L)$, and let n, n' be integers, $n' \neq 0$, with $[n]Y, [n']Y \in E_1(L_{\mathcal{Q}})$ and $[n']Y \neq O$. Then $v(\mathfrak{z}([n]Y)) - v(\mathfrak{z}([n']Y)) = v_p(n/n')$, the quotient $\Lambda = \ell_m(\mathfrak{z}([n]Y))/\ell_m(\mathfrak{z}([n']Y))$ is defined and $v(\Lambda) = v_p(n/n')$; and if $p > m+1$ and $v_p(n/n') \geq 0$, then $v(\Lambda - n/n') \geq m$.*

The same holds for E^σ with $\ell^\sigma, \ell^\sigma_m$. Part (c) is the analogue of [44, Proposition 2.2] *for E.*

Proof. (a) For $t \geq 2$, $v((c_t/t)Z^t) \geq v(Z) + (t-1) - v_p(t) > v(Z)$, because $v_p(t) \leq \log_3 t < t - 1$. (b) For $t \geq m+1$ we have $t - 1 - v_p(t) \geq m$: if $p \nmid t$ this is $t - 1 \geq m$, and if $v_p(t) = e \geq 1$ then $t \geq p^e$ and $p^e - 1 - e \geq p - 2 \geq m$. Hence every term of $\ell(Z) - \ell_m(Z)$ has valuation at least $v(Z) + m$. (c) Put $Z = \mathfrak{z}([n]Y)$, $Z' = \mathfrak{z}([n']Y) \neq 0$ and $r = n/n'$. Since $[n'][n]Y = [n][n']Y$ and $\ell \circ \mathfrak{z}$ is a homomorphism on $E_1(L_{\mathcal{Q}})$, $n'\ell(Z) = n\ell(Z')$, so by (a) $v(Z) - v(Z') = v(n) - v(n') = v_p(r)$, and $v(\ell_m(Z')) = v(Z') < \infty$, so Λ is defined, with $v(\Lambda) = v_p(r)$ by (a) (if $n = 0$, then $Z = 0$ and $\Lambda = 0$). If $p > m+1$ and $v_p(r) \geq 0$, then $\ell_m(Z) - r\ell_m(Z') = (\ell_m - \ell)(Z) - r(\ell_m - \ell)(Z')$ has valuation at least $v(Z') + m$ by (b), as $v(Z) \geq v(Z')$; dividing by $\ell_m(Z')$ gives $v(\Lambda - r) \geq m$. □

For $V \in E(L)$ let $V^\tau \in E^\sigma(L)$ be the point with τ-conjugate coordinates; τ is a group isomorphism $E(L) \to E^\sigma(L)$.

Lemma 6.4 ([60, Lemma 9.2])**.** *Let $m \geq 1$ and $c_* \neq 0$ be integers, and let $\mathcal{Q}$ be as in the Setting with $p > m+1$ and $p \nmid c_*$. Let h, u_i, n_i $(1 \leq i \leq 4)$ be integers with $h \neq 0$ and $h \neq c_*$, and put $H = [h]P$, $U_i = [u_i]P$, $P_i = [n_i]P$, $V_0 = H - [c_*]P$ and $V_i = U_i - [c_*]P_i$, where P is a point of infinite order of $E(L)$. Suppose that $H, U_i \in E_1(L_{\mathcal{Q}})$, that $V_0^\tau, V_i^\tau \in E_1^\sigma(L_{\mathcal{Q}})$, and that*

$$L_i = \frac{\ell_m(\mathfrak{z}(U_i))}{\ell_m(\mathfrak{z}(H))}, \qquad L_i' = \frac{\ell_m^\sigma(\mathfrak{z}(V_i^\tau))}{\ell_m^\sigma(\mathfrak{z}(V_0^\tau))}$$

satisfy $v(L_i - L_i') \geq m$ for $1 \leq i \leq 4$. Then $v(L_i - n_i) \geq m$ for $1 \leq i \leq 4$. Consequently $v(f(L_1, \ldots, L_4)) \geq m$ for $f \in \mathbb{Z}[X_1, \ldots, X_4]$ implies $p^m \mid f(n_1, \ldots, n_4)$.

Here $V_0^\tau = [h - c_*]P^\tau$ and $V_i^\tau = [u_i - c_* n_i]P^\tau$. The shifted anchor V_0 is the device of [44, Lemma 2.3 and Corollary 6.2], with c_* in place of 4.

Proof. Since $p \nmid c_*$, one of h, $h - c_*$ is prime to p. If $p \nmid h$, Lemma 6.3(c) on E with $Y = P$ gives $v(L_i - u_i/h) \geq m$; then $v(L_i') \geq 0$, so by Lemma 6.3(c) on E^σ with $Y = P^\tau$ the index quotient $(u_i - c_* n_i)/(h - c_*)$ has $v_p \geq 0$ and $v(L_i' - (u_i - c_* n_i)/(h - c_*)) \geq m$. If $p \nmid h - c_*$ the same argument runs in the other order. In both cases $hL_i \equiv u_i$ and $(h - c_*)L_i' \equiv u_i - c_* n_i$ modulo $\mathfrak{m}^m$, and therefore

$$c_* L_i = hL_i - (h - c_*)L_i' - (h - c_*)(L_i - L_i') \equiv c_* n_i \pmod{\mathfrak{m}^m}.$$

Divide by the unit c_*. The last assertion follows because v restricts to v_p on $\mathbb{Q}$. □

Lemma 6.5 ([60, Lemma 12.3])**.** *Let $p \geq 5$, $p \notin \mathcal{P}$, be a prime, $m \geq 1$, $P \in E(F)$ a point of infinite order, and h, c nonzero integers. Write $\rho([h]P) = G_1 + \sqrt{d}\, G_2$, $\rho([c]P) = G_3 + \sqrt{d}\, G_4$ and $\mathfrak{z}([c]P)/\mathfrak{z}([h]P) = G_5 + \sqrt{d}\, G_6$ with $G_k \in \mathbb{Q}$. If $v_p(G_k) \geq 1$ for $k \leq 4$ and $v_p(G_5), v_p(G_6) \geq m$, then $p^m \mid c$.*

Proof. Let $\mathfrak{Q}$ be a prime of F above p; it is unramified, $\sqrt{d}$ is a unit at it, as $p \nmid 2d$, and the Setting applies over $F_{\mathfrak{Q}}$. Then $v_{\mathfrak{Q}}(\rho([h]P)) \geq 1$ and $v_{\mathfrak{Q}}(\rho([c]P)) \geq 1$, so $[h]P, [c]P \in E_1(F_{\mathfrak{Q}})$, both $\neq O$; and $v_{\mathfrak{Q}}(\mathfrak{z}([c]P)/\mathfrak{z}([h]P)) \geq m$. By Lemma 6.3(c), $v_p(c) - v_p(h) \geq m$, so $v_p(c) \geq m$. □

6.3. **The tube in the certificate.** Fix q and $\mathfrak{q}$ as in Theorem 1.6, and put

$$\theta_0 = 0, \qquad \theta_i = \frac{q}{\gamma_i - 1}\ (1 \le i \le 6), \qquad \mathcal{T} = \{\theta_0, \dots, \theta_6\}.$$

By Lemma 3.2(a) the θ_i are seven distinct rationals whose denominators are prime to q, and they lie in $(-(q+1), 0]$, because $\gamma_i < 1/(q+1)$ for every i (Lemma 7.1(a)).

Lemma 6.6 ([60, Lemma 9.3 and (12.4)–(12.8)])**.** (a) *Let $\eta = a_0^2 + b_0^2 \neq 0$ with $a_0, b_0 \in K$, and let $A \in K^{\times 2}$ be totally positive. Then $s = A\eta + 1/q$ is totally positive and $v_{\mathfrak{q}}(s) \le -1$.*

(b) *Let $s \in K$ be totally positive with $v_{\mathfrak{q}}(s) \le 0$. Then $1 + q/s \in \mathcal{D}$. Let $\Sigma' \supseteq \Sigma$ contain the primes at which some θ_i $(i \ge 1)$ or $1 - \gamma_i$ has nonzero valuation. For $\mathfrak{P} \notin \Sigma'$, $1 + q/s$ has positive odd contact with a point of $\mathcal{C}_q$ at $\mathfrak{P}$ if and only if $v_{\mathfrak{P}}(s - \theta)$ is positive and odd for some $\theta \in \mathcal{T}$; and $|h(1 + q/s) - h(s)| \le C$ with C depending only on q.*

(c) *Let $R_\psi(t) = C_* D(t) \prod_{i=1}^{6} ((10q + 1 - \gamma_i) D(t) + q^2 t)$, where $D(t) = 1 + q^2 t^2$ and C_* is the least positive integer with $R_\psi \in \mathbb{Z}[t]$. Then R_ψ has degree 14 and is positive on $\mathbb{R}$. Let $\Sigma'' \supseteq \Sigma$ contain the primes dividing C_*, the leading coefficients of the seven quadratic factors, and their pairwise resultants. For $t \in K$ and $\mathfrak{P} \notin \Sigma''$, $\psi_q(t)$ has positive odd contact with a point of $\mathcal{C}_q$ at $\mathfrak{P}$ if and only if $v_{\mathfrak{P}}(R_\psi(t))$ is positive and odd; and if $v_{\mathfrak{P}}(t) < 0$ then $v_{\mathfrak{P}}(R_\psi(t)) = 14 v_{\mathfrak{P}}(t)$.*

Proof. (a) At every real place $\eta > 0$ (a nonzero sum of two real squares), $A > 0$ and $1/q > 0$. The residue field of $\mathfrak{q}$ has q^f elements with f odd and $q \equiv 3 \pmod 4$, so -1 is not a square in it; with $\mu = \min(v_{\mathfrak{q}}(a_0), v_{\mathfrak{q}}(b_0))$ the residues of $a_0 \varpi^{-\mu}$ and $b_0 \varpi^{-\mu}$ (ϖ a uniformiser) are not both zero, so their squares do not cancel and $v_{\mathfrak{q}}(\eta) = 2\mu$. Hence $v_{\mathfrak{q}}(A\eta)$ is even while $v_{\mathfrak{q}}(1/q) = -1$, so $v_{\mathfrak{q}}(s) = \min(v_{\mathfrak{q}}(A\eta), -1) \le -1$.

(b) The first assertion is Lemma 3.2(c). For $1 \le i \le 6$, $1 + q/s - \gamma_i = (1 - \gamma_i)(s - \theta_i)/s$, and $1/(1 + q/s) = s/(s + q)$. Let $\mathfrak{P} \notin \Sigma'$, so q, θ_i $(i \ge 1)$, $1 - \gamma_i$ and the differences of the θ's are $\mathfrak{P}$-units (the last as $\Sigma \subseteq \Sigma'$). If $v_{\mathfrak{P}}(s - \theta_i) > 0$ for some $i \ge 1$ then $v_{\mathfrak{P}}(s) = 0$ and the contact with γ_i is $v_{\mathfrak{P}}(s - \theta_i)$; if $v_{\mathfrak{P}}(s) > 0$, the contact with ∞ is $v_{\mathfrak{P}}(s) = v_{\mathfrak{P}}(s - \theta_0)$; and if no $s - \theta$ has positive valuation, then $v_{\mathfrak{P}}(s) \le 0$ and no contact is positive. The height bound holds because $s \mapsto 1 + q/s$ is a Möbius transformation over $\mathbb{Q}$.

(c) Since $10q + 1 - \gamma_i > 10q - 1 > q/2$, each factor $(10q + 1 - \gamma_i)(1 + u^2) + qu$, $u = qt$, has negative discriminant in u, so $R_\psi > 0$ on $\mathbb{R}$. Write $f_0 = D$ and $f_i = (10q + 1 - \gamma_i) D + q^2 t$, so that $\psi_q(t) - \gamma_i = f_i(t)/D(t)$ and $1/\psi_q(t) = D(t)/((10q + 1) D(t) + q^2 t)$. Let $\mathfrak{P} \notin \Sigma''$. If $v_{\mathfrak{P}}(t) < 0$, each $f_i(t)$ has valuation $2 v_{\mathfrak{P}}(t)$ (its leading coefficient is a unit), so $v_{\mathfrak{P}}(R_\psi(t)) = 14 v_{\mathfrak{P}}(t)$ and $\psi_q(t)$ has no positive contact. If $v_{\mathfrak{P}}(t) \ge 0$, the $f_i(t)$ are integral and at most one has positive valuation (resultants); if $v_{\mathfrak{P}}(f_i(t)) > 0$ with $i \ge 1$, the contact of $\psi_q(t)$ with γ_i is $v_{\mathfrak{P}}(f_i(t))$; if $v_{\mathfrak{P}}(D(t)) > 0$, then t is a unit, $(10q + 1) D(t) + q^2 t \equiv q^2 t$ is a unit, and the contact with ∞ is $v_{\mathfrak{P}}(D(t))$; in every case $v_{\mathfrak{P}}(R_\psi(t))$ is the one positive contact, or 0. □

7. The certificate

Throughout this section and the next two, K is a totally real number field with $\sqrt{3} \notin K$ and $\sqrt{d} \notin K$ satisfying (I1)–(I3) (for $\sqrt{3} \in K$ see Section 10), $n_K = [K : \mathbb{Q}]$, and $P \in E(F)$ is the generator of $2E(L)$ given by (E3) and Lemma 2.8.

7.1. **The fixed data.** The following are chosen once, in this order, before any input.

(F1) A prime $q \equiv 7 \pmod{12}$ and a prime $\mathfrak{q}$ of K above q, unramified with odd residue degree (Lemma 3.1); the contacts γ_i, the set $\mathcal{T}$ of Section 6.3, $\omega = -1$, $\xi = 1$, $\mathcal{T}^+ = \mathcal{T} \cup \{\omega\}$,

$F_8(S) = \prod_{\theta\in\mathcal{T}^+}(S-\theta)$, $d_0 = 0$, $d_1 = 2q+2$, and the polynomial R_ψ of Lemma 6.6(c). Let Σ_0 be the least set Σ allowed in Theorem 1.6, and κ the exponent that theorem gives for Σ_0.

(F2) An integer $m > 8n_K\kappa + 100$; a positive multiple c_* of 64; $\Gamma = 2^3\cdot 3\cdot 5\cdot 7\cdot 17$ and $C = 2\cdot 3\cdot 5\cdot 7\cdot 13\cdot 17\cdot q\cdot \Gamma^2$.

(F3) The finite set $\mathfrak{B}$ of primes of K lying above: every rational prime $p \le \max(324, m+1)$; q; the primes dividing c_*, C or C_*; the primes ramified in $K/\mathbb{Q}$; and every rational prime at which one of the following rationals has nonzero valuation: the $\gamma_i \ne 0$, the $1-\gamma_i$, the $\theta_i \ne 0$, the differences of two distinct elements of $(\mathcal{T}^+\cup\{\xi\})\cup((\mathcal{T}^+\cup\{\xi\})-d_1)\cup\{1/q\}$, and the leading coefficients and pairwise resultants of the seven quadratic factors of R_ψ.

(F4) A positive integer M, large enough for Proposition 8.3.

Lemma 7.1. (a) $\mathcal{T}^+\cup\{\xi\} \subset (-(q+1),1]$, $(\mathcal{T}^+\cup\{\xi\})-d_1 \subset (-(3q+3),-(2q+1)]$, *these two sets are disjoint,* $1/q$ *lies in neither,* $\omega\notin\mathcal{T}$, *and* $\mathcal{T}^+\cup\{\xi\}$ *has nine elements.*

(b) *Every prime* $\mathfrak{P}\notin\mathfrak{B}$ *lies above a rational prime* $p > \max(324, m+1)$ *with* $p\ne q$, $p\nmid c_*C$, *unramified in* L; *and every prime* $\mathcal{Q}$ *of* L *above it is as in the Setting of Section 6.2.*

(c) $\Sigma_0\subseteq\mathfrak{B}$, *and for* $z\in K\setminus\mathcal{C}_q$, $\mathfrak{N}_{\Sigma_0}(z) \le C_{\mathfrak{B}}\mathfrak{N}_{\mathfrak{B}}(z)$ *with* $C_{\mathfrak{B}} = \prod_{\mathfrak{P}\in\mathfrak{B}\setminus\Sigma_0} N\mathfrak{P}$. *Hence there is* $H_{\mathfrak{B}}$ *with* $h(z) \le H_{\mathfrak{B}}\mathfrak{N}_{\mathfrak{B}}(z)^\kappa$ *for every* $z\in\mathcal{D}$.

Proof. (a) For $i\ge 1$, $\theta_i = -q/(1-\gamma_i)$ with $1-\gamma_i\in(0,2)$, so $\theta_i < -q/2 < -1$; and $\theta_i > -(q+1)$ because $\gamma_i < 1/(q+1)$ (the positive contacts are $\gamma_3 = (q-1)/D_q$ and γ_5, both below $1/(q+1)$). With $\theta_0 = 0$, $\omega = -1$ and $\xi = 1$ this gives the first inclusion and $\omega\notin\mathcal{T}$; the second follows by subtracting $2q+2$; and $0 < 1/q < 1$. (b) The primes ramified in $L/\mathbb{Q}$ lie above a prime that is ramified in $F/\mathbb{Q}$, hence divides $2d$, or in $K/\mathbb{Q}$; and every prime of $\mathcal{P}$ is at most 89. (c) Σ_0 consists of primes above $p\le 324$, above q, and at which a nonzero finite contact or a difference of two distinct finite contacts has nonzero valuation; the differences $\gamma_i-\gamma_k$ are, up to the units q and $(1-\gamma_i)(1-\gamma_k)$, the differences $\theta_k-\theta_i$ times q^{-1}, so these primes are in $\mathfrak{B}$. Each prime of $\mathfrak{B}\setminus\Sigma_0$ removes at most the factor $N\mathfrak{P}$ from $\mathfrak{N}_{\Sigma_0}(z)$. Then $H_{\mathfrak{B}} = HC_{\mathfrak{B}}^\kappa$ works, by Theorem 1.6. □

7.2. **The conditions.** For $u\in L$ write $u = u^{(0)} + \sqrt{d}\,u^{(1)}$ with $u^{(0)}, u^{(1)}\in K$ (E1).

Definition 7.2. Let $X\in K$. The *certificate* at X is the statement that there exist

- a sign $\delta\in\{1,-1\}$;
- nine points $\mathsf{Q}, \mathsf{N}_1, \mathsf{N}_3, \mathsf{N}_4, \mathsf{H}, \mathsf{U}_1, \dots, \mathsf{U}_4$ of $2E(L)$;
- $a_0, b_0\in K$, and, for $j = 0, 1$, elements witnessing $\Phi_K(B_j)$ (Section 5),

such that all quantities defined below are defined (every displayed denominator is nonzero, every point to which ρ, $\mathfrak{z}$ or ℓ_m is applied has the needed coordinate nonzero, and $W_j\Theta_j\ne 0$), and the following hold:

(C1) Q, $\mathsf{R} = [M]\mathsf{Q}$, $\mathsf{N}_1, \mathsf{N}_2, \mathsf{N}_3, \mathsf{N}_4$, H, $\mathsf{U}_1, \dots, \mathsf{U}_4$ and V_0 are not O, where $\mathsf{N}_2 = P+\mathsf{R}$ and $V_0 = \mathsf{H} - [c_*]P$;

(C2) $\eta = a_0^2 + b_0^2 \ne 0$;

(C3) $\Phi_K(B_0)$ and $\Phi_K(B_1)$.

The quantities are as follows. Put $\beta = 3 + \delta(X^3+X)$, $V_i = \mathsf{U}_i - [c_*]\mathsf{N}_i$ $(1\le i\le 4)$, and

$$L_i = \frac{\ell_m(\mathfrak{z}(\mathsf{U}_i))}{\ell_m(\mathfrak{z}(\mathsf{H}))}, \qquad L_i' = \frac{\ell_m^\sigma(\mathfrak{z}(V_i^\tau))}{\ell_m^\sigma(\mathfrak{z}(V_0^\tau))} \qquad (1\le i\le 4).$$

The tests below, shared by the two parameters, follow [70]. The sixteen *comparison tests* $D_1,\dots,D_{16}\in L$, with their *precisions* k_i, are

tests	number	precision
$\rho(\mathsf{H}),\ \rho(\mathsf{U}_1),\dots,\rho(\mathsf{U}_4)$	5	1
$\rho(V_0^\tau),\ \rho(V_1^\tau),\dots,\rho(V_4^\tau)$	5	1
$L_i-L_i'\ (1\le i\le 4)$	4	m
$\mathcal{L}(L_1,L_2,L_3,L_4)$	1	m
$L_1-\beta$	1	m

with $\mathcal{L}$ as in (6.1). The six *scalar tests* $G_1,\dots,G_6\in K$ are the coordinates

$$\rho(\mathsf{H})=G_1+\sqrt{d}\,G_2,\qquad \rho(\mathsf{R})=G_3+\sqrt{d}\,G_4,\qquad \mathfrak{z}(\mathsf{R})/\mathfrak{z}(\mathsf{H})=G_5+\sqrt{d}\,G_6,$$

with precisions $(\ell_1,\dots,\ell_6)=(1,1,1,1,m,m)$. Further,

$$T_{\mathrm{ag}}=\tfrac12\operatorname{Tr}_{L/K}\bigl(x(\mathsf{N}_1)+x(\mathsf{N}_2)+x(\mathsf{N}_3)+x(\mathsf{N}_4)\bigr),\qquad r=R_\psi(\beta),\qquad \varpi=\frac{\Gamma^2 r}{(1+Cr)^2},$$

$$A_0=1,\quad A_1=(1+\varpi T_{\mathrm{ag}}^2)^2,\quad s_j=A_j\eta+\frac{1}{q},\quad t_j=s_j+d_j-\xi,$$

$$R_j=\frac{F_8(s_j+d_j)}{t_j^8},\quad \alpha_j=\varpi R_j,$$

$\Psi_R(v)=Rv/(1+Rv)$, and, for $j=0,1$,

$$W_j=\prod_{i=1}^{16}\Bigl(1+\alpha_j\Bigl(\frac{D_i}{t_j^{k_i+1}\alpha_j^{k_i}}\Bigr)^2\Bigr)\prod_{k=1}^{6}\Bigl(1+\alpha_j\Bigl(\frac{\Psi_{R_j}(G_k)}{\varpi^{\ell_k}}\Bigr)^2\Bigr),$$

$$\Theta_j=\operatorname{Tr}_{L/K}(W_j^{-1}),\qquad B_j=\frac{\alpha_j}{\Theta_j^2}.$$

The certificate follows that of [59, §3] over $\mathbb{Q}$, carried to $\mathbb{Q}(\sqrt{2})$ in [60, §§12.1–13.1].

Lemma 7.3. *Suppose the certificate holds at $X\in K$. Then there are integers $n_1,\dots,n_4$, h, $u_1,\dots,u_4$ and k_{Q} with $\mathsf{N}_i=[n_i]P$, $\mathsf{H}=[h]P$, $\mathsf{U}_i=[u_i]P$ and $\mathsf{Q}=[k_{\mathsf{Q}}]P$; $n_2-1=Mk_{\mathsf{Q}}\neq 0$; $n_1,\dots,n_4$, h and $h-c_*$ are nonzero; all nine points and V_0,V_i lie in $E(F)$; T_{ag} and the G_k are rational, and $T_{\mathrm{ag}}>0$; and r, ϖ, η, A_j, s_j and s_j+d_j are totally positive.*

Proof. By (E3) and Lemma 2.8, $2E(L)=\mathbb{Z}P$ with $P\in E(F)$; this gives the integers, and $\mathsf{N}_2=[1+Mk_{\mathsf{Q}}]P$. (C1) gives the nonvanishing. All points are multiples of P, so lie in $E(F)$, and τ acts on their coordinates as σ; so $\rho(\mathsf{H}),\rho(\mathsf{R}),\mathfrak{z}(\mathsf{R})/\mathfrak{z}(\mathsf{H})\in F$ have rational coordinates, and $\operatorname{Tr}_{L/K}=\operatorname{Tr}_{F/\mathbb{Q}}$ on F (E1), so $T_{\mathrm{ag}}\in\mathbb{Q}$, and $T_{\mathrm{ag}}>0$ because each $x([n_i]P)$ is totally positive by (E3) and Lemma 2.8. $R_\psi>0$ on $\mathbb{R}$ and K is totally real, so r is totally positive, hence so are $1+Cr$ and ϖ. $\eta\neq 0$ is a sum of two squares, hence totally positive; $A_0=1$, and A_1 is the square of $1+\varpi T_{\mathrm{ag}}^2$, which is totally positive; $1/q>0$ and $d_j\ge 0$. □

8. Soundness

Lemma 8.1 ([60, Lemma 13.1])**.** *Suppose the certificate holds at $X\in K$. Let $\mathfrak{P}\notin\mathfrak{B}$ be a prime of K above p, $j\in\{0,1\}$, $\mu=v_{\mathfrak{P}}(\varpi)$, $\nu=v_{\mathfrak{P}}(R_j)$, and suppose $\alpha=\mu+\nu$ is odd. Then $\alpha>0$, and there is a prime $\mathcal{Q}$ of L above $\mathfrak{P}$ with*

$$v_{\mathcal{Q}}(D_i/t_j^{k_i+1})\ge k_i\quad(1\le i\le 16),\qquad v_{\mathcal{Q}}(\Psi_{R_j}(G_k))>\ell_k\mu-\tfrac34\alpha\quad(1\le k\le 6).$$

If moreover t_j is a $\mathfrak{P}$-unit, then $v_{\mathcal{Q}}(D_i) \geq k_i$ for all i; if R_j is a $\mathfrak{P}$-unit and $\mu > 0$, then $v_p(G_k) \geq \ell_k$ for all k.

Proof. By Lemma 7.1(b), L/K is unramified at $\mathfrak{P}$, so $v_{\mathcal{Q}} = v_{\mathfrak{P}}$ on K for every $\mathcal{Q} \mid \mathfrak{P}$, and $v_{\mathfrak{P}}(\alpha_j) = \alpha$. A factor of W_j is $1+y$ with $y = \alpha_j(D_i/(t_j^{k_i+1}\alpha_j^{k_i}))^2$ or $y = \alpha_j(\Psi_{R_j}(G_k)/\varpi^{\ell_k})^2$; if $y \neq 0$, then $v_{\mathcal{Q}}(y)$ is α plus an even integer, hence odd, so $v_{\mathcal{Q}}(1+y) = \min(0, v_{\mathcal{Q}}(y))$; if $y = 0$ the factor is 1. So $\lambda_{\mathcal{Q}} = v_{\mathcal{Q}}(W_j) \leq 0$ is the sum of the nonpositive numbers $\min(0, v_{\mathcal{Q}}(y))$. Let $\lambda = \max_{\mathcal{Q}\mid\mathfrak{P}} \lambda_{\mathcal{Q}}$ and π a uniformiser of K at $\mathfrak{P}$. Then $\pi^{\lambda}W_j^{-1}$ is integral at every $\mathcal{Q} \mid \mathfrak{P}$, so its trace $\pi^{\lambda}\Theta_j$ is $\mathfrak{P}$-integral, and $v_{\mathfrak{P}}(\Theta_j) \geq -\lambda \geq 0$. Now $v_{\mathfrak{P}}(B_j) = \alpha - 2v_{\mathfrak{P}}(\Theta_j)$ is odd and $B_j \neq 0$, and $\mathfrak{P}$ is not above $2, 3, 5, 7, 17$, so Lemma 5.1 and $\Phi_K(B_j)$ give $v_{\mathfrak{P}}(B_j) \geq 1$. Hence $\alpha \geq 1 + 2v_{\mathfrak{P}}(\Theta_j) \geq 1$, and $1 \leq \alpha + 2\lambda$, that is $\lambda \geq (1-\alpha)/2$. Choose $\mathcal{Q}$ with $\lambda_{\mathcal{Q}} = \lambda$. Every term of the sum defining $\lambda_{\mathcal{Q}}$ is at least λ. For a comparison test with $D_i \neq 0$ this gives $\alpha(1-2k_i) + 2v_{\mathcal{Q}}(D_i/t_j^{k_i+1}) \geq (1-\alpha)/2$, so

$$v_{\mathcal{Q}}(D_i/t_j^{k_i+1}) \geq k_i\alpha - \tfrac{3\alpha-1}{4} = (k_i - \tfrac{3}{4})\alpha + \tfrac{1}{4} \geq k_i - \tfrac{1}{2},$$

and $v_{\mathcal{Q}}(D_i/t_j^{k_i+1}) \geq k_i$ as valuations are integers. For a scalar test, $\alpha + 2v_{\mathcal{Q}}(\Psi_{R_j}(G_k)) - 2\ell_k\mu \geq (1-\alpha)/2$ gives $v_{\mathcal{Q}}(\Psi_{R_j}(G_k)) \geq \ell_k\mu - \frac{3\alpha-1}{4}$. The third assertion is immediate. For the fourth, $\alpha = \mu \geq 1$, so $v_{\mathcal{Q}}(\Psi_{R_j}(G_k)) > (\ell_k - \frac{3}{4})\mu \geq \ell_k - \frac{3}{4}$, hence $\geq \ell_k \geq 1$; with R_j a unit, $\Psi_{R_j}(G_k) = R_jG_k/(1+R_jG_k)$ has positive valuation only if $v_{\mathfrak{P}}(G_k) > 0$, and then its valuation is $v_{\mathfrak{P}}(G_k)$. By Lemma 7.3, $G_k \in \mathbb{Q}$, and $v_{\mathfrak{P}} = v_p$ on $\mathbb{Q}$. □

Lemma 8.2 ([60, Lemma 13.2])**.** *Suppose the certificate holds at $X \in K$, and let $\mathfrak{P} \notin \mathfrak{B}$ with $v_{\mathfrak{P}}(\varpi)$ odd. Then $v_{\mathfrak{P}}(\varpi) = v_{\mathfrak{P}}(r) > 0$, $v_{\mathfrak{P}}(\beta) \geq 0$, and R_0 or R_1 is a $\mathfrak{P}$-unit.*

Proof. Write $v = v_{\mathfrak{P}}$; Γ and C are $\mathfrak{P}$-units. If $v(\beta) < 0$, then $v(r) = 14v(\beta)$ by Lemma 6.6(c), $v(1+Cr) = v(r)$, and $v(\varpi) = -v(r)$ is even. So $v(\beta) \geq 0$ and r is integral; if $v(r) = 0$ then $v(\varpi) = -2v(1+Cr)$ is even; so $v(r) > 0$, $1 + Cr$ is a unit, and $v(\varpi) = v(r)$. Now $v(\varpi T_{\mathrm{ag}}^2)$ is odd. If it is positive, $A_1 \equiv 1 \pmod{\mathfrak{P}}$. If $v(\eta) < 0$, then $v(s_j) = v(\eta) < 0$ for both j, each factor $s_j + d_j - \theta$ ($\theta \in \mathcal{T}^+ \cup \{\xi\}$) has valuation $v(\eta)$, and $R_j = \prod_{\theta\in\mathcal{T}^+}(1-\theta/S)/(1-\xi/S)^8$ with $S = s_j + d_j$ is $\equiv 1$, a unit. If $v(\eta) \geq 0$, then all s_j are integral and $s_1 \equiv s_0 \pmod{\mathfrak{P}}$; if neither R_j were a unit, then $s_0 \equiv \theta$ and $s_0 + d_1 \equiv \theta'$ for some $\theta, \theta' \in \mathcal{T}^+ \cup \{\xi\}$, so $\mathfrak{P}$ would divide the nonzero difference $\theta - (\theta' - d_1)$, which is a unit outside $\mathfrak{B}$ by Lemma 7.1(a) and (F3). If $v(\varpi T_{\mathrm{ag}}^2) < 0$, then $v(A_1) < 0$. If $v(\eta) \leq 0$, then $v(s_1) = v(A_1\eta) < 0$ and $R_1 \equiv 1$ as before. If $v(\eta) > 0$, then $s_0 \equiv 1/q$, and every $s_0 - \theta$, $\theta \in \mathcal{T}^+ \cup \{\xi\}$, is a unit because $1/q - \theta$ is; so R_0 is a unit. □

Proposition 8.3. *If M in (F4) is large enough, then every $X \in K$ at which the certificate holds lies in $\mathbb{Z}$.*

Proof. We follow the proof of [60, Proposition 13.3]. Let the certificate hold at X, with the integers of Lemma 7.3, and put $N = \max(1, |n_1|, \dots, |n_4|)$ and $\Delta = \mathcal{L}(n_1, n_2, n_3, n_4) \in \mathbb{Z}$. Then $|n_2 - 1| \geq M$, so $N \geq M - 1$. Constants $c_1, c_2, \dots$ below depend on K, E, P and the data (F1)–(F3), but not on M or X.

Step 1 (local alternatives). Let $\mathfrak{P} \notin \mathfrak{B}$ be a prime above p.

(i) Suppose $v_{\mathfrak{P}}(s_j + d_j - \theta)$ is positive and odd for some $\theta \in \mathcal{T}$, and $v_{\mathfrak{P}}(\varpi)$ is even. The other seven factors $s_j + d_j - \theta'$ ($\theta' \in \mathcal{T}^+$) and t_j are $\mathfrak{P}$-units, since $\theta - \theta'$ and $\theta - \xi$ are; so $v_{\mathfrak{P}}(R_j)$ is positive and odd and t_j is a unit. By Lemma 8.1 there is $\mathcal{Q} \mid \mathfrak{P}$ with $v_{\mathcal{Q}}(D_i) \geq k_i$ for all i. Thus $\mathsf{H}, \mathsf{U}_i \in E_1(L_{\mathcal{Q}})$ and $V_0^{\tau}, V_i^{\tau} \in E_1^{\sigma}(L_{\mathcal{Q}})$, and $v_{\mathcal{Q}}(L_i - L_i') \geq m$. By Lemma 7.1(b)

and Lemma 6.4 (with $h \neq 0$, $h \neq c_*$), $v_{\mathcal{Q}}(L_i - n_i) \geq m$; so $v_{\mathcal{Q}}(\mathcal{L}(n_1, \dots, n_4)) \geq m$, that is $p^m \mid \Delta$, and $v_{\mathfrak{P}}(\beta - n_1) = v_{\mathcal{Q}}(\beta - n_1) \geq m$, using $L_1 - \beta$.

(ii) Suppose $v_{\mathfrak{P}}(\varpi)$ is odd. By Lemma 8.2, $v_{\mathfrak{P}}(\varpi) > 0$, $v_{\mathfrak{P}}(\beta) \geq 0$, and some $R_{j'}$ is a unit. By Lemma 8.1 for j', $v_p(G_k) \geq \ell_k$ for all k, and by Lemma 6.5 (with h and $c = n_2 - 1$; $p \geq 5$, $p \notin \mathcal{P}$), $p^m \mid n_2 - 1$.

(iii) Suppose $v_{\mathfrak{P}}(r)$ is positive and odd. Then $1 + Cr$ is a unit and $v_{\mathfrak{P}}(\varpi) = v_{\mathfrak{P}}(r)$ is odd, so $p^m \mid n_2 - 1$ by (ii).

Step 2 (counting). Let $\mathfrak{M}_j$ be the product of $N\mathfrak{P}$ over the primes $\mathfrak{P} \notin \mathfrak{B}$ at which $v_{\mathfrak{P}}(s_j + d_j - \theta)$ is positive and odd for some $\theta \in \mathcal{T}$, and $\mathfrak{M}_{\mathrm{sc}}$ the product of $N\mathfrak{P}$ over the $\mathfrak{P} \notin \mathfrak{B}$ with $v_{\mathfrak{P}}(r)$ positive and odd. For a rational prime p, $\prod_{\mathfrak{P}\mid p} N\mathfrak{P} \leq p^{n_K}$. By (i) and (ii), if $\Delta \neq 0$, then $p^m \mid \Delta(n_2 - 1)$ for every p below a prime counted in $\mathfrak{M}_j$, so $\mathfrak{M}_j^m \leq |\Delta(n_2 - 1)|^{n_K}$. If $\beta \neq n_1$, then $v_{\mathfrak{P}}((\beta - n_1)(n_2 - 1)) \geq m$ at every prime counted in $\mathfrak{M}_j$ (in case (ii) because $v_{\mathfrak{P}}(\beta - n_1) \geq 0$ and $v_{\mathfrak{P}}(n_2 - 1) = v_p(n_2 - 1)$), so by (6.2)

$$\mathfrak{M}_j^m \leq \mathrm{N}\,\mathfrak{a}\big((\beta - n_1)(n_2 - 1)\big) \leq \exp\big(n_K h((\beta - n_1)(n_2 - 1))\big).$$

By (iii), $\mathfrak{M}_{\mathrm{sc}}^m \leq |n_2 - 1|^{n_K}$.

Step 3 (heights). By Lemma 6.6(a), s_j is totally positive with $v_{\mathfrak{q}}(s_j) \leq -1$, so the same holds for $s_j + d_j$. By Lemma 6.6(b), applied with $\Sigma' = \mathfrak{B}$, $1 + q/(s_j + d_j) \in \mathcal{D}$ and its odd-contact primes outside $\mathfrak{B}$ are those counted in $\mathfrak{M}_j$; by Lemma 7.1(c), $h(s_j) \leq c_1(1 + \mathfrak{M}_j^\kappa)$. By Lemma 3.2(d), $\psi_q(\beta) \in \mathcal{D}$, and by Lemma 6.6(c) its odd-contact primes outside $\mathfrak{B}$ are those counted in $\mathfrak{M}_{\mathrm{sc}}$; as ψ_q has degree 2, $h(\beta) \leq c_2(1 + \mathfrak{M}_{\mathrm{sc}}^\kappa) \leq c_2(1 + |n_2 - 1|^{n_K\kappa/m})$. By Lemma 2.10, $N^2 \leq c_3 h(T_{\mathrm{ag}}) + c_4$. Since $A_1 = (s_1 - 1/q)/(s_0 - 1/q)$ and $T_{\mathrm{ag}}^2 = (\sqrt{A_1} - 1)/\varpi$ with $\sqrt{A_1} = 1 + \varpi T_{\mathrm{ag}}^2$, and $h(\varpi) \leq c_5(1 + h(\beta))$,

$$N^2 \leq c_6(1 + h(s_0) + h(s_1) + h(\beta)).$$

Step 4 ($\Delta = 0$). Suppose $\Delta \neq 0$. Then $|\Delta| \leq 14N^4$ and $|n_2 - 1| \leq 2N$, so $\mathfrak{M}_j \leq (28N^5)^{n_K/m}$, and Step 3 gives $N^2 \leq c_7(1 + N^{5n_K\kappa/m})$ with $5n_K\kappa/m < 5/8$. This fails once N exceeds a bound N_1 depending only on the constants; choosing $M > N_1 + 1$ excludes it. So $\Delta = 0$. As $|n_2| \geq M - 1 \geq 7$ and $n_4 \neq 0$, Lemma 6.2(a) gives $|n_3| > \exp(|n_2| - 3)$, so $\log N > |n_2| - 3 \geq |n_2 - 1| - 4$.

Step 5 ($\beta = n_1$). Suppose $\beta \neq n_1$. Then $h((\beta - n_1)(n_2 - 1)) \leq h(\beta) + 3\log(2N)$, so by Steps 2 and 3, with $\epsilon = n_K\kappa/m < 1/8$,

$$N^2 \leq c_8(1 + e^{\epsilon h(\beta)}(2N)^{3\epsilon} + h(\beta)), \qquad h(\beta) \leq c_2(1 + (\log N + 4)^\epsilon).$$

The second bound gives $e^{\epsilon h(\beta)} \leq N^{1/4}$ and $h(\beta) \leq \log N$ once N exceeds a bound N_2 depending only on the constants, and then $N^2 \leq c_8(1 + 2N^{5/8} + \log N)$, which fails for N beyond a bound N_3. Since $N > \exp(|n_2| - 3) \geq \exp(M - 4)$, choosing M with $\exp(M - 4) > \max(N_2, N_3)$ excludes it. So $\beta = n_1 \in \mathbb{Z}$, hence $X^3 + X = \delta(n_1 - 3) \in \mathbb{Z}$, and $X \in \mathbb{Z}$ by Lemma 6.1. □

9. Completeness

9.1. Three lemmas.

Lemma 9.1 ([60, Lemma 13.4])**.** *For every positive integer r, the rational number $\varpi = \Gamma^2 r/(1 + Cr)^2$ satisfies $0 < \varpi \leq \Gamma^2/(4C) < \frac{1}{4}$; $v_p(\varpi) = 2v_p(\Gamma) + v_p(r)$ for every prime $p \mid C$; and every odd valuation of ϖ is positive.*

Proof. $(1+Cr)^2 \geq 4Cr$ gives the bound, and $C > 4\Gamma^2$. If $p \mid C$, $1+Cr$ is a p-unit. In general $v_p(\varpi) \equiv v_p(r) \pmod 2$; if $v_p(r)$ is odd then $p \mid r$, $1+Cr$ is a p-unit and $v_p(\varpi) = 2v_p(\Gamma) + v_p(r) > 0$. □

Fix a real embedding ι of F. For $V \in E(F)$ write $V_{\mathbf{R}} = (\iota(V), \iota(V^\sigma))$, a point of the compact abelian Lie group $\mathbf{E} = E^\iota(\mathbb{R}) \times E^{\iota\sigma}(\mathbb{R})$, where E^ι and $E^{\iota\sigma}$ are the real curves obtained from E by ι and $\iota \circ \sigma$. Let $G_{\mathbf{R}}$ be the closure of $\{([k]P)_{\mathbf{R}} : k \in \mathbb{Z}\}$, $G^0_{\mathbf{R}}$ its identity component, and $e_{\mathbf{R}}$ the exponent of the finite group $G_{\mathbf{R}}/G^0_{\mathbf{R}}$.

Lemma 9.2. (a) *Both projections of $G^0_{\mathbf{R}}$ to the factors of $\mathbf{E}$ are nontrivial, and for finite sets $Z_1 \subset E^\iota(\mathbb{R})$, $Z_2 \subset E^{\iota\sigma}(\mathbb{R})$ the set of $g \in G^0_{\mathbf{R}}$ with a coordinate in Z_1 or Z_2 is closed with empty interior in $G^0_{\mathbf{R}}$.*

(b) *If h^* and $N^* \neq 0$ are integers divisible by $e_{\mathbf{R}}$, then $\{([h^* + kN^*]P)_{\mathbf{R}} : k \geq 1\}$ is dense in $G^0_{\mathbf{R}}$.*

(c) *For every nonzero integer e and every neighbourhood $\mathcal{V}$ of the identity of $\mathbf{E}$ there is $k \geq 1$ with $([ke]P)_{\mathbf{R}} \in \mathcal{V}$.*

Proof. $G_{\mathbf{R}}$ is a closed subgroup of a compact abelian Lie group, so $G^0_{\mathbf{R}}$ is a torus of finite index. (a) The first projection of $G_{\mathbf{R}}$ is the closure of $\{\iota([k]P)\}$, which is infinite as P has infinite order; its image of $G^0_{\mathbf{R}}$ is connected and of finite index in it, hence not trivial. The same holds for the second projection, as P^σ has infinite order. A fibre of a nontrivial homomorphism from the connected group $G^0_{\mathbf{R}}$ is a coset of a proper closed subgroup, hence closed with empty interior, and a finite union of such sets has empty interior. (b) In a compact group the closure of the positive multiples of an element is the closure of the subgroup it generates. Let $g_0 = ([h^*]P)_{\mathbf{R}}$ and $g_1 = ([N^*]P)_{\mathbf{R}}$. The closure of $\langle g_1 \rangle$ is $N^*G_{\mathbf{R}} \supseteq N^*G^0_{\mathbf{R}} = G^0_{\mathbf{R}}$, multiplication by N^* being surjective on a torus, and $g_0 \in e_{\mathbf{R}}G_{\mathbf{R}} \subseteq G^0_{\mathbf{R}}$; so the closure of $\{g_0 + kg_1 : k \geq 1\}$ contains $g_0 + G^0_{\mathbf{R}} = G^0_{\mathbf{R}}$. (c) The closure of the positive multiples of $([e]P)_{\mathbf{R}}$ is the group $eG_{\mathbf{R}}$, which contains the identity. □

The following lemma bounds the comparison tests uniformly at the primes of a fixed finite set, a step in the proof of [60, Proposition 13.6]. For a prime $\mathfrak{Q}$ of F above p let $v = v_{\mathfrak{Q}}$ be normalised on $F_{\mathfrak{Q}}$, $e = v(p) \leq 2$, R the valuation ring and $\mathfrak{m}$ its maximal ideal. The equation (1.1) is minimal at every prime of F (E2). Hence [56, Proposition VII.2.2] identifies $E_1(F_{\mathfrak{Q}})$ with the formal group on $\mathfrak{m}$ through $\mathfrak{z}$; we write $E^{(s)} = \{O\} \cup \{V : v(\mathfrak{z}(V)) \geq s\}$ for $s \geq 1$, a subgroup. We use: $[p]E^{(s)} \subseteq E^{(s+1)}$ [56, §IV.3]; for an integer $r > e/(p-1)$, ℓ and the formal exponential are inverse isomorphisms between $E^{(s)}$ and $\mathfrak{m}^s$ for every $s \geq r$ [56, §IV.6], so $v(\ell(\mathfrak{z}(V))) = v(\mathfrak{z}(V))$ on $E^{(r)}$, and the exponential is continuous on $\mathfrak{m}^r$ (its n-th term has valuation at least $r + (n-1)(r - e/(p-1))$ there, by the estimates of [56, §IV.6]); and if $v(Z) > e/(p-1)$ then $v(\ell_m(Z)) = v(Z)$, since $v((c_t/t)Z^t) \geq tv(Z) - ev_p(t) > v(Z)$ for $t \geq 2$, as $v_p(t) \leq (t-1)/(p-1)$.

Lemma 9.3. *Let $m \geq 1$ and c_* be integers, $n_1, \dots, n_4$ nonzero integers, $\mathcal{S}$ a finite set of primes, J a positive integer and a_p $(p \in \mathcal{S})$ integers such that*

(J1) *$[J]P \in E_1(F_{\mathfrak{Q}})$ for every prime $\mathfrak{Q}$ of F above every $p \in \mathcal{S}$;*

(J2) *$a_p \geq v_p(J) + 2$ for every $p \in \mathcal{S}$.*

Let $\mathcal{C} = \{h \in \mathbb{Z} : J \mid h,\ h \equiv p^{a_p} \pmod{p^{a_p+1}}$ for $p \in \mathcal{S}\}$. For $h \in \mathcal{C}$ let $D_1(h), \dots, D_{16}(h)$ be the comparison tests of Definition 7.2 for $\mathsf{H} = [h]P$, $\mathsf{N}_i = [n_i]P$, $\mathsf{U}_i = [n_i]\mathsf{H}$ and $\beta = n_1$, so that $V_0 = [h - c_*]P$ and $V_i = [n_i]V_0$. Then for each $p \in \mathcal{S}$ there are an integer $b_p \geq a_p + 1$,

a residue class $\mathcal{C}'_p$ modulo p^{b_p} contained in $\{h : h \equiv p^{a_p} \pmod{p^{a_p+1}}\}$, and numbers $B_{\mathfrak{Q}} \geq 0$ for the primes $\mathfrak{Q} \mid p$ of F, such that for every $h \in \mathcal{C} \cap \mathcal{C}'_p$:

(a) *H, U_i, V_0, V_i have infinite order, and $\ell_m(\mathfrak{z}(\mathsf{H})) \neq 0$, $\ell_m(\mathfrak{z}(V_0)) \neq 0$; so all sixteen tests are defined;*

(b) *$v_{\mathfrak{Q}}(D_i(h)) \geq -B_{\mathfrak{Q}}$ for every $i \leq 16$ and every prime $\mathfrak{Q} \mid p$ of F.*

All points here lie in $E(F)$, so $V^\tau = V^\sigma$ and the tests lie in F.

Proof. Fix $p \in \mathcal{S}$. *Step 0 (the class and its depth).* Since $v_p(J) \leq a_p$, the condition $J \mid h$ asks for $h \in \mathcal{C}$ only that the prime-to-$\mathcal{S}$ part of J divide h, so $\mathcal{C}$ is one residue class $h_0 + \tilde{J}\mathbb{Z}$, $\tilde{J} = \operatorname{lcm}(J, \prod_{p' \in \mathcal{S}} p'^{a_{p'}+1})$, with $v_p(\tilde{J}) = a_p + 1$. Let $\mathfrak{Q} \mid p$ and $r = 1 + a_p - v_p(J) \geq 3$. If $k \neq 0$ and $J \mid k$, write $k/J = p^j u$ with $p \nmid u$; by (J1), $[p]E^{(s)} \subseteq E^{(s+1)}$ and the subgroup property, $[k]P \in E^{(1+j)}$. Hence $H_0 = [h_0]P$ and every $[h]P$, $h \in \mathcal{C}$, lie in $E^{(r)} \setminus \{O\}$, and $P' = [\tilde{J}]P \in E^{(r+1)} \setminus \{O\}$. As $e \leq 2$, $r \geq 3 > e/(p-1)$.

Step 1 (a p-adic interpolation). For $\mu \in \mathbb{Z}_p$ put $t(\mu) = \ell(\mathfrak{z}(H_0)) + \mu\, \ell(\mathfrak{z}(P')) \in \mathfrak{m}^r$ and let $\varphi_{\mathfrak{Q}}(\mu) \in E^{(r)}$ be the point whose parameter is the formal exponential of $t(\mu)$. For $\mu \in \mathbb{Z}$, $\varphi_{\mathfrak{Q}}(\mu) = [h_0 + \tilde{J}\mu]P$, since $\ell \circ \mathfrak{z}$ is a homomorphism on $E^{(r)}$ with inverse the exponential. The map $\varphi_{\mathfrak{Q}}$ is injective, as $\ell(\mathfrak{z}(P')) \neq 0$, and continuous, as t is affine, the exponential is continuous on $\mathfrak{m}^r$ and $Z \mapsto [Z : -1 : w(Z)]$ is continuous on $\mathfrak{m}$.

Step 2 (the tests at H and U_i). For $h \in \mathcal{C}$, H and $\mathsf{U}_i = [n_i]\mathsf{H}$ lie in $E^{(r)} \setminus \{O\}$, so $v(\rho(\mathsf{H})), v(\rho(\mathsf{U}_i)) \geq 2r > 0$; $v(\ell_m(\mathfrak{z}(V))) = v(\mathfrak{z}(V))$ for $V = \mathsf{H}, \mathsf{U}_i$, and $\ell(\mathfrak{z}(\mathsf{U}_i)) = n_i \ell(\mathfrak{z}(\mathsf{H}))$ gives $v(\mathfrak{z}(\mathsf{U}_i)) = e v_p(n_i) + v(\mathfrak{z}(\mathsf{H}))$; so $\ell_m(\mathfrak{z}(\mathsf{H})) \neq 0$ and $v(L_i) = e v_p(n_i) \geq 0$. Hence $\mathcal{L}(L_1, \ldots, L_4)$ and $L_1 - n_1$ are integral.

Step 3 (the conjugate side). For $Y \in E$ put $f_0(Y) = \rho(Y)$, $f_i(Y) = \rho([n_i]Y)$ and $g_i(Y) = \ell_m(\mathfrak{z}([n_i]Y))/\ell_m(\mathfrak{z}(Y))$, rational functions on E over F. Then $\rho(V_0^\sigma) = \sigma(f_0(V_0))$, $\rho(V_i^\sigma) = \sigma(f_i(V_0))$ and $L'_i = \sigma(g_i(V_0))$, and $v_{\mathfrak{Q}}(\sigma(u)) = v_{\sigma\mathfrak{Q}}(u)$ for $u \in F$. Let $\mathcal{Z}$ be the set of points Y of E over an algebraic closure of $F_{\mathfrak{Q}}$ with $Y \in E[2]$, or $[n_i]Y \in E[2]$ for some i, or $\ell_m(\mathfrak{z}(Y)) = 0$; it is finite, and off $\mathcal{Z}$ all of $f_0, \ldots, f_4, g_1, \ldots, g_4$ are regular, hence continuous on $E(F_{\mathfrak{Q}}) \setminus \mathcal{Z}$. With $G = [c_*]P$, the set $\Lambda = \bigcup_{\mathfrak{Q}|p} \{\mu \in \mathbb{Z}_p : \varphi_{\mathfrak{Q}}(\mu) - G \in \mathcal{Z}\}$ is finite, by injectivity of $\varphi_{\mathfrak{Q}}$.

Step 4 (the refined class). Choose $\mu_0 \in \mathbb{Z} \setminus \Lambda$ and $b \geq 0$ with $b > v_p(\mu_0 - \lambda)$ for all $\lambda \in \Lambda$; then the ball $\mathcal{V} = \mu_0 + p^b\mathbb{Z}_p$ misses Λ. Put $b_p = b + a_p + 1$ and $\mathcal{C}'_p = \{h : h \equiv h_0 + \tilde{J}\mu_0 \pmod{p^{b_p}}\}$. For $h = h_0 + \tilde{J}\mu \in \mathcal{C}$, $h \in \mathcal{C}'_p$ if and only if $\mu \in \mathcal{V}$, because $v_p(\tilde{J}) = a_p + 1$; and $\mathcal{C}'_p$ lies in the class of p^{a_p} modulo p^{a_p+1}. For each $\mathfrak{Q} \mid p$ the functions $\mu \mapsto f_i(\varphi_{\mathfrak{Q}}(\mu) - G)$, $g_i(\varphi_{\mathfrak{Q}}(\mu) - G)$ are continuous on the compact set $\mathcal{V}$, so there is $B'_{\mathfrak{Q}}$ with all their valuations at least $-B'_{\mathfrak{Q}}$ there. Let $h \in \mathcal{C} \cap \mathcal{C}'_p$. Then $V_0 = \varphi_{\mathfrak{Q}}(\mu) - G \notin \mathcal{Z}$ for every $\mathfrak{Q} \mid p$; so $V_0 \neq O$, hence V_0 and V_i have infinite order, and $\ell_m(\mathfrak{z}(V_0)) \neq 0$; with Step 2 this is (a). At $\mathfrak{Q}$, the conjugate-side tests have valuation at least $-B'_{\sigma\mathfrak{Q}}$, so $v_{\mathfrak{Q}}(L_i - L'_i) \geq -B'_{\sigma\mathfrak{Q}}$, and (b) holds with $B_{\mathfrak{Q}} = \max(B'_{\mathfrak{Q}}, B'_{\sigma\mathfrak{Q}})$. □

9.2. **The construction.** We use two elementary facts. (Coordinates) If $k \geq 0$, $u \in F$ and $v_{\mathfrak{Q}}(u) \geq k$ at every prime $\mathfrak{Q}$ of F above p, then $u^{(0)} = \frac{1}{2}\operatorname{Tr}_{F/\mathbb{Q}}(u)$ and $u^{(1)} = \frac{1}{2}\operatorname{Tr}_{F/\mathbb{Q}}(u/\sqrt{d})$ have $v_p \geq k/2 - 2$. (Depth) Under (J1), if $J \mid k$ then $[k]P \in E^{(1+v_p(k)-v_p(J))}$ at every prime above p, and if $Jp^2 \mid k$ then $v(\mathfrak{z}([k]P)) = e v_p(k/(Jp^2)) + v(\mathfrak{z}([Jp^2]P))$; the first is in Step 0 of the proof of Lemma 9.3, and the second follows from it by the isometry of ℓ on $E^{(3)}$.

Proposition 9.4. *For every $X \in \mathbb{Z}$ the certificate holds at X.*

Proof. We follow the proof of [60, Proposition 13.6]. The choices are made in the following order; each depends only on the earlier ones.

Step 1 (the input). Let δ be the sign with $\beta = 3 + |X^3 + X|$; since $X(X^2+1)$ is even, $\beta \geq 3$ is odd. Then $r = R_\psi(\beta)$ is a positive integer and $\varpi \in \mathbb{Q}_{>0}$ satisfies Lemma 9.1. Let $\mathcal{S}$ be the set of rational primes below $\mathfrak{B}$ together with the primes at which ϖ has nonzero valuation; it contains every prime $p \leq 324$, among them $2, 3, 5, 7, 13, 17$ and the primes of $\mathcal{P}$, and q. The prime q may lie in $\mathcal{P}$ ($q = 7$ for the second or third curve); no step uses the reduction of E at q. For $p \in \mathcal{S}$ put $g_p = 3 + 2m|v_p(\varpi)|$.

Step 2 (the class of h). For each prime $\mathfrak{Q}$ of F above each $p \in \mathcal{S}$, the group $E(F_\mathfrak{Q})/E_1(F_\mathfrak{Q})$ is finite; let J_0 be the least common multiple of the orders of P in these groups, and $J = J_0 e_\mathbf{R}$. Then (J1) holds. Choose $a_p \geq v_p(J) + 1 + g_p$ for $p \in \mathcal{S}$, with $a_2 \geq 6$; then (J2) holds. Let $\mathcal{C}$ be as in Lemma 9.3. For $h \in \mathcal{C}$, $[h]P \in E^{(1+a_p-v_p(J))}$ at every prime above $p \in \mathcal{S}$, so the coordinates G_1, G_2 of $\rho([h]P)$ have $v_p \geq g_p$ by (Coordinates).

Step 3 (a real neighbourhood). Let $\varepsilon_0 = \varpi^m/100$. The points $g \in G^0_\mathbf{R}$ near the identity whose coordinates g_1, g_2 satisfy $|\rho(g_1)|, |\rho(g_2)| < \varepsilon_0$ form a neighbourhood of the identity in $G^0_\mathbf{R}$; by Lemma 9.2(a) it contains a point with both coordinates $\neq O$, and hence a nonempty open set $\mathcal{U}$ whose closure lies in it and avoids the points with a coordinate O. By compactness there is $\delta_0 > 0$ with $|\mathfrak{z}(g_1)|, |\mathfrak{z}(g_2)| \geq \delta_0$ on $\mathcal{U}$.

Step 4 (the index n_2). By Lemma 9.2(c) choose a positive multiple c of $MJ \prod_{p\in\mathcal{S}} p^{a_p+2g_p+4}$ such that both coordinates of $([c]P)_\mathbf{R}$ have $|\rho| \leq \varepsilon_0$ and $|\mathfrak{z}| \leq \varepsilon_0\delta_0$. Put $n_2 = c + 1$; then $n_2 \geq 7$. By (Depth), at every prime above $p \in \mathcal{S}$ the coordinates G_3, G_4 of $\rho([c]P)$ have $v_p \geq g_p$, and for every $h \in \mathcal{C}$ we have $v(\mathfrak{z}([c]P)/\mathfrak{z}([h]P)) = e(v_p(c) - a_p)$, so the coordinates G_5, G_6 of $\mathfrak{z}([c]P)/\mathfrak{z}([h]P)$ have $v_p \geq g_p$. For every h with $([h]P)_\mathbf{R} \in \mathcal{U}$, all six G_k have absolute value at most ε_0, since $|u^{(0)}|, |u^{(1)}| \leq \max(|\iota(u)|, |\iota\sigma(u)|)$.

Step 5 (the other indices). Put $n_1 = \beta$, and choose positive n_3, n_4 with $\mathcal{L}(n_1, n_2, n_3, n_4) = 0$ by Lemma 6.2(b). Now $T_\mathrm{ag} = \frac{1}{2}\operatorname{Tr}_{F/\mathbb{Q}} \sum_k x([n_k]P) \in \mathbb{Q}_{>0}$ and $A_1 = (1 + \varpi T_\mathrm{ag}^2)^2 \in \mathbb{Q}$ are fixed. The sixteen comparison tests are, at the real embeddings, rational functions of $([h]P)_\mathbf{R}$ that are regular off the points with a coordinate in a finite set; by Lemma 9.2(a) there is a nonempty open $\mathcal{U}_1 \subseteq \mathcal{U}$ with compact closure on which all of them are defined and bounded in absolute value by some $B_\mathbf{R}$.

Step 6 (the classes at $\mathcal{S}$). Apply Lemma 9.3 with these m, c_*, $n_1, \dots, n_4$, $\mathcal{S}$, J, a_p; it gives b_p, $\mathcal{C}'_p$ and $B_\mathfrak{Q}$ for $p \in \mathcal{S}$.

Step 7 (the selected primes). For $j = 0, 1$ and $\theta \in \mathcal{T}^+ \cup \{\xi\}$ put $c_{j,\theta} = (1/q + d_j - \theta)/A_j$, a nonzero rational by Lemma 7.1(a); for fixed j the nine values are distinct. Let D be a positive integer with all $D^2 c_{j,\theta} \in \mathbb{Z}$. Apply Theorem 4.1, with $(\ell, r) = (13, 1 + 2i)$ for the first curve and $(7, 1 + 3i)$ for the second, or Theorem 4.3, with $(\ell, r) = (7, 1 + 3i)$ for the third and $(89, 1 + 5i)$ for the fourth, to the distinct integers among $D^2 c_{j,\theta}$ ($j = 0, 1$, $\theta \in \mathcal{T}^+$) and 0, with: $D_0 = \prod_{p\in\mathcal{S}} p^{f_p}$, where f_p is so large that, with $w_0 = Dw$ and any w divisible by D_0,

$$\begin{aligned}
&\text{(w1)} \quad v_p(c_{j,\theta} w_0^2) \geq 1 \quad (j = 0, 1,\ \theta \in \mathcal{T}^+ \cup \{\xi\}),\\
&\text{(w2)} \quad (2k_i + 2)e(2v_p(w_0) - v_p(A_j)) \geq 3e + 2B_\mathfrak{Q} + (2k_i - 1)e|v_p(\varpi)|\\
&\qquad\qquad (\mathfrak{Q} \mid p,\ e = v_\mathfrak{Q}(p),\ j = 0, 1,\ i \leq 16);
\end{aligned}$$

N_0 the product of the odd primes other than 3 and ℓ, and other than 5 for the third and fourth curves, that lie in $\mathcal{S}$ or divide J (so $17 \mid N_0$ for the fourth curve, as Lemma 4.4 asks); $\mathcal{S}'$ the set of primes dividing D, c, c_*, a numerator or denominator of A_1, of a $c_{j,\theta}$ or of a nonzero difference $c_{j,\theta} - c_{j',\theta'}$, or the norm of a nonzero element among $\rho(V)$, $\mathfrak{z}(V)$ and

their inverses for $V = [c]P, [c_*]P$; Y larger than $m+1$, than every prime of $\mathcal{S} \cup \mathcal{S}'$ and than every prime divisor of J; and Λ_0 so large that $u/w^2 > \Lambda_0$ implies: $u > 400$, every selected prime lies in $(\frac{3}{4}u, \frac{5}{4}u)$, and, with $\eta = u/w_0^2$, for $j = 0, 1$: $|R_j - 1| \le \frac{1}{100}$, $t_j \ge 1$, and $\varpi^{1-2m} 2^{2m} B_{\mathbf{R}}^2 t_j^{-4} \le \frac{1}{500}$ (possible because $s_j \to \infty$ as $\eta \to \infty$). We obtain u, w; write $w_0 = Dw$ and $\eta = u/w_0^2$, let π_0 be the Gaussian prime of u, and put $a_0 = \mathrm{Re}(\pi_0)/w_0$ and $b_0 = \mathrm{Im}(\pi_0)/w_0$, so (C2) holds. For $\theta \in \mathcal{T}^+ \cup \{\xi\}$,

$$s_j + d_j - \theta = \frac{A_j}{w_0^2}(u + c_{j,\theta} w_0^2), \qquad R_j = \frac{\prod_{\theta \in \mathcal{T}^+}(u + c_{j,\theta} w_0^2)}{(u + c_{j,\xi} w_0^2)^8}, \tag{9.1}$$

and the numerator factors are the selected primes $p_{j,\theta} = u + D^2 c_{j,\theta} w^2$. A selected prime does not divide w_0 (it would divide u), nor D, A_1, or a nonzero difference of shifts; so at $p_{j,\theta}$ the other factors of (9.1) for the same j and t_j are units, and $v_p(R_j) = 1$.

Step 8 (the index h). For each selected prime p' with Gaussian prime π', let $\mathfrak{p}'_+$ and $\mathfrak{p}'_- = \sigma\mathfrak{p}'_+$ be the primes of F above p', and $N_\pm(p') = \#\tilde{E}(\mathcal{O}_F/\mathfrak{p}'_\pm)$, with the signs assigned as follows. For the first two curves $\mathfrak{p}'_\pm$ is the prime at which E has $N_\pm(p') = d_\pm(\pi')$ points (Lemma 4.2). For the last two, $\mathfrak{p}'_+$ is the prime $\mathfrak{p}_+$ of Lemma 4.4, and $N_+(p') = \mathrm{N}(\pi' - \epsilon)$, $N_-(p') = \mathrm{N}(\pi' - \eta i)$ with $\epsilon, \eta \in \{1, -1\}$. Let $L_\pm = \operatorname{lcm} N_\pm(p')$ and $P_{\mathrm{sel}} = \prod p'$ over the selected primes. Consider the congruences

$$h \equiv 0 \pmod{L_+}, \quad h \equiv c_* \pmod{L_-}, \quad h \equiv 0 \pmod{P_{\mathrm{sel}}}, \quad h \in \mathcal{C}, \quad h \in \mathcal{C}'_p \ (p \in \mathcal{S}).$$

They are compatible. For the first two curves, by Theorem 4.1(ii), $\gcd(L_+, L_-) = 4$ and $64 \mid c_*$; at 2, $v_2(L_+) = 2$, $v_2(L_-) = 6$, and every $h \in \mathcal{C}'_2$ has $v_2(h) = a_2 \ge 6$, as $c_* \equiv 0 \pmod{64}$; by Theorem 4.1(iii) and the choice of N_0, L_+L_- is prime to every odd prime of $\mathcal{S}$ and of J. For the last two, by Theorem 4.3(ii), $\gcd(L_+, L_-) = 2$ and $2 \mid c_*$; at 2, $v_2(L_+) \le 6$ and $v_2(L_-) = 1$, and every $h \in \mathcal{C}'_2$ has $v_2(h) = a_2 \ge 6$; at 5, $v_5(L_+) \le 2$ and $5 \nmid L_-$, and every $h \in \mathcal{C}'_5$ has $v_5(h) = a_5 \ge 4$ (Step 2); by Theorem 4.3(iii) and the choice of N_0, L_+L_- is prime to every other odd prime of $\mathcal{S}$ and of J. In all cases the selected primes are not in $\mathcal{S}$, do not divide J, and do not divide L_+L_-: for selected primes p', p'', the number $N_\pm(p'')$ is even, as $(0,0)$ reduces to a point of order two, and $0 < N_\pm(p'') \le p'' + 1 + 2\sqrt{p''} < \frac{3}{2}u < 2p'$, as $u > 400$. So the solutions form a progression $h^* + N^*\mathbb{Z}$ with $J \mid h^*$ and $J \mid N^*$. Take $N^* > 0$ and k_0 with $h^* + k_0 N^* > |c_*|$; by Lemma 9.2(b), applied to $h^* + k_0 N^*$ and N^* (both divisible by $e_{\mathbf{R}}$), choose $h = h^* + k_0 N^* + kN^*$ with $k \ge 1$ and $([h]P)_{\mathbf{R}} \in \mathcal{U}_1$. Put $\mathsf{H} = [h]P$, $\mathsf{U}_i = [hn_i]P$, $\mathsf{N}_i = [n_i]P$ $(i \ne 2)$, $\mathsf{Q} = [c/M]P$; then $\mathsf{R} = [c]P$, $\mathsf{N}_2 = [n_2]P$, and all nine points lie in $2E(L) = \mathbb{Z}P$. (C1) holds as all indices and $h - c_*$ are nonzero. All tests are defined by Lemma 9.3(a); all ingredients of W_j lie in F or $\mathbb{Q}$, so $W_j \in F$ and $\Theta_j, B_j \in \mathbb{Q}$.

Step 9 (the real size). At both real embeddings every summand of every factor of W_j is nonnegative, as $\alpha_j = \varpi R_j > 0$. By Step 7, $R_j \in [\frac{99}{100}, \frac{101}{100}]$; for a comparison factor the summand is at most $\varpi^{1-2k_i} R_j^{1-2k_i} B_{\mathbf{R}}^2 t_j^{-2k_i-2} \le \frac{1}{500}$; for a scalar factor, $|G_k| \le \varepsilon_0$ gives $|\Psi_{R_j}(G_k)| \le 3|G_k|$ and the summand is at most $2\varpi^{1-2\ell_k} \cdot 9\varepsilon_0^2 \le \frac{1}{500}$. So $1 \le W_j \le (1 + \frac{1}{500})^{22} < 1.05$ at both embeddings, $\Theta_j \in [1.9, 2]$, and $0 < B_j = \varpi R_j/\Theta_j^2 < \varpi < 1$. In particular $1 + R_j G_k \ne 0$, $t_j \ne 0$ and $W_j \Theta_j \ne 0$.

Step 10 (the primes of $\mathcal{S}$). Let $p \in \mathcal{S}$ and $\mathfrak{Q} \mid p$, $e = v_{\mathfrak{Q}}(p)$. By (w1) and as u is a p-unit, every factor in (9.1) is $\equiv u \pmod{p}$, so R_j is a p-unit, $v_{\mathfrak{Q}}(\alpha_j) = e v_p(\varpi)$ and $v_p(t_j) = v_p(A_j) - 2v_p(w_0)$. By Lemma 9.3(b), $v_{\mathfrak{Q}}(D_i) \ge -B_{\mathfrak{Q}}$, so the summand of the i-th comparison factor has valuation

$$(1 - 2k_i) e v_p(\varpi) + 2v_{\mathfrak{Q}}(D_i) + (2k_i + 2) e (2v_p(w_0) - v_p(A_j)) \ge 3e$$

by (w2). By Steps 2 and 4, $v_p(G_k) \geq g_p > 0$, so $v_{\mathfrak{Q}}(\Psi_{R_j}(G_k)) = ev_p(G_k)$ and the summand of a scalar factor has valuation at least $e(2g_p - (2m-1)|v_p(\varpi)|) \geq 6e$. Hence $W_j \equiv 1 \pmod{p^3}$ in $F \otimes \mathbb{Z}_p$, $\Theta_j \equiv 2 \pmod{p^3}$, $v_2(\Theta_j) = 1$, and $v_p(\Theta_j) = 0$ for odd p. So $v_2(B_j) = v_2(\varpi) - 2 = 2v_2(\Gamma) + v_2(r) - 2 \geq 4$ and $v_p(B_j) = v_p(\varpi) = 2 + v_p(r) \geq 2$ for $p = 3, 5, 7, 17$ (Lemma 9.1); and for every $p \in \mathcal{S}$ an odd $v_p(B_j)$ is positive.

Step 11 (the selected primes). Let p' be a numerator prime of the j-th detector, π' its Gaussian prime, $\mathfrak{p}_\pm = \mathfrak{p}'_\pm$. Then $v_{p'}(\alpha_j) = 1$ and t_j is a unit. As $N_+(p') \mid h/p'$ (since $p' \mid h$ and $p' \nmid N_+(p')$), $[h/p']P \in E_1(F_{\mathfrak{p}_+})$ and $\mathsf{H} \in E^{(2)}$ at $\mathfrak{p}_+$; as $N_-(p') \mid h - c_*$, $V_0 \in E_1(F_{\mathfrak{p}_-})$. Since $\sigma\mathfrak{p}_+ = \mathfrak{p}_-$, at $\mathfrak{p}_+$: $\rho(\mathsf{H}), \rho(\mathsf{U}_i)$ have positive valuation; $\rho(V_0^\sigma), \rho(V_i^\sigma)$ have the valuations of $\rho(V_0), \rho(V_i)$ at $\mathfrak{p}_-$, which are positive; by Lemma 6.3(c), applied over $F_{\mathfrak{p}_\pm} = \mathbb{Q}_{p'}$ ($p' > m+1$), $L_i \equiv n_i$ at $\mathfrak{p}_+$ and $L'_i = \sigma(\ell_m(\mathfrak{z}(V_i))/\ell_m(\mathfrak{z}(V_0))) \equiv n_i$ at $\mathfrak{p}_+$, modulo the m-th power; so $L_i - L'_i$, $\mathcal{L}(L_1, \dots, L_4) \equiv \Delta = 0$ and $L_1 - \beta \equiv n_1 - \beta = 0$ have valuation at least m. So every comparison summand has valuation $1 + 2v(D_i) - 2k_i \geq 1$ at $\mathfrak{p}_+$. For the scalar tests: p' avoids the primes of $\rho([c]P)$, $\mathfrak{z}([c]P)$, $\rho([c_*]P)$, $\mathfrak{z}([c_*]P)$ and their inverses, so H, which reduces to the reduction of $[c_*]P$ at $\mathfrak{p}_-$, has $\rho(\mathsf{H})$ and $\mathfrak{z}(\mathsf{H})$ units there, $\rho(\mathsf{H})$ is integral at $\mathfrak{p}_+$, and $u_5 := \mathfrak{z}([c]P)/\mathfrak{z}(\mathsf{H})$ has valuation ≤ -2 at $\mathfrak{p}_+$ and 0 at $\mathfrak{p}_-$. As p' splits in F (Lemmas 4.2 and 4.4) and $2\sqrt{d}$ is a unit at p', $G_1, \dots, G_4$ are p'-integral and $v_{p'}(G_5), v_{p'}(G_6) \leq -2$. So $v_{p'}(R_jG_k) \neq 0$ and $\Psi_{R_j}(G_k)$ is integral, and every scalar summand has valuation ≥ 1 at $\mathfrak{p}_+$. At $\mathfrak{p}_-$ every summand has odd valuation. Hence $W_j^{-1} \equiv 1$ at $\mathfrak{p}_+$ and $W_j^{-1} \equiv 0$ or 1 at $\mathfrak{p}_-$, $\Theta_j \equiv 1$ or 2 $\pmod{p'}$, and $v_{p'}(B_j) = 1$.

Step 12 (the predicate). At a prime p that is neither in $\mathcal{S}$ nor a numerator prime of the j-th detector, $v_p(\varpi) = 0$ and $v_p(R_j) = -8v_p(u + c_{j,\xi}w_0^2)$, so $v_p(B_j)$ is even. With Steps 10 and 11, every negative valuation of B_j is even, so its reduced denominator is a square. By Steps 9 and 10, B_j satisfies the hypotheses of Lemma 5.3, which gives $\Phi_{\mathbb{Q}}(B_j)$ with rational witnesses, hence $\Phi_K(B_j)$: (C3) holds. □

10. Fields containing $\sqrt{3}$

For the first index curve $\sqrt{d} = \sqrt{3}$, so Theorem 1.1 asks $\sqrt{3} \notin K$ through $\sqrt{d} \notin K$. In this section E is the second, third or fourth index curve, and K is a totally real number field with $\sqrt{3} \in K$ and $\sqrt{d} \notin K$ satisfying (I1)–(I3), with $n_K = [K : \mathbb{Q}]$ and $P \in E(F)$ the generator of $2E(L)$ given by (E3) and Lemma 2.8. Then 3 is a square in every residue field of K of characteristic $p \geq 5$, so the tube of Theorem 1.6 is not available: no prime of K above a prime $q \equiv 7 \pmod{12}$ has odd residue degree, and the last step of the proof of Lemma 3.4(d) fails. We add a second prime to the tube, at which $3g_q(z)$ is not a square. Apart from the tube, Sections 2, 4, 5, 6, 7, 8 and 9 do not use $\sqrt{3} \notin K$.

10.1. The height bound at two primes.

Definition 10.1. Let K be a totally real number field. A *tube datum at two primes* for K is a quadruple $(q, \mathfrak{q}, q', \mathfrak{q}')$ such that

(T1) $q \geq 7$ is a prime with $q \equiv 3 \pmod 4$, and $\mathfrak{q}$ is a prime of K above q, unramified over q, of residue degree one;

(T2) q' is a prime not dividing $6qD_q$, and $\mathfrak{q}'$ is a prime of K above q', unramified over q', of residue degree one, such that $g_q(1)$ is a q'-adic unit and neither -1 nor $3g_q(1)$ is a square modulo $\mathfrak{q}'$.

We put $\hat{q} = qq'$ and call

$$\mathcal{D}' = \{z \in K : \ v_{\mathfrak{q}}(z-1) \geq 1, \ v_{\mathfrak{q}'}(z-1) \geq 1 \text{ and } g_q(z) \text{ is totally positive}\}$$

the *positive tube at two primes*.

By (T2), $q' \equiv 3 \pmod 4$ and $q' \neq q$. If $\sqrt{3} \in K$, then 3 is a square modulo $\mathfrak{q}$ and modulo $\mathfrak{q}'$, so $q \equiv q' \equiv 11 \pmod{12}$, and (T2) asks that $g_q(1)$ is not a square modulo $\mathfrak{q}'$. The polynomials $D_q^2(a_q z + b_q - q z^2)$ and $D_q^2(a_q z + b_q - 4q z^2)$ lie in $\mathbb{Z}[z]$, as $D_q^2 a_q = (q-3)(q+1)D_q$ and $D_q^2 b_q = (q-1)(q+3)$, and their product is $4q^2 D_q^4 g_q$ by (3.1); as $q' \nmid 2qD_q$, the coefficients of g_q are q'-integral. Both primes are taken unramified: at a ramified prime of residue degree one the conclusion of Lemma 3.3 fails (in $\mathbb{Q}(\sqrt{3}, \sqrt{11})$ the primes above 11 are such, and $v(j_z) = 2$ there for $z = 254$).

Theorem 10.2. *Suppose that $\sqrt{3} \in K$, let $(q, \mathfrak{q}, q', \mathfrak{q}')$ be a tube datum at two primes for K, and let Σ be a set as before Theorem 1.6 that also contains every prime above q'. Then $\mathcal{D}' \cap \mathcal{C}_q = \emptyset$, and there are constants $H > 0$ and $\kappa > 0$ such that*

$$h(z) \leq H\, \mathfrak{N}_\Sigma(z)^\kappa \qquad \text{for every } z \in \mathcal{D}'.$$

Proof. The proofs of Lemma 3.2(a) and Lemma 3.3 use of q and $\mathfrak{q}$ only that $q \geq 7$ is prime and $\mathfrak{q}$ is unramified over q; the proofs of Lemma 3.4(a)–(c) use in addition only that $N\mathfrak{q} \equiv 3 \pmod 4$ (so that $\tau^{N\mathfrak{q}} = \tau^{-1}$ in (a)) and that $g_q(z)$ is totally positive. By (T1) these lemmas hold for q, $\mathfrak{q}$ and every $z \in \mathcal{D}'$, as $\mathcal{D}' \subseteq \mathcal{D}$; in particular $\mathcal{D}' \cap \mathcal{C}_q = \emptyset$. Lemma 3.4(d) holds for $z \in \mathcal{D}'$ as in (S5): by its proof, if it failed then $3g_q(z) \in K^{\times 2}$; but g_q has q'-integral coefficients and $z \equiv 1 \pmod{\mathfrak{q}'}$, so $3g_q(z) \equiv 3g_q(1) \pmod{\mathfrak{q}'}$ is a $\mathfrak{q}'$-adic unit that is not a square modulo $\mathfrak{q}'$, hence not a square in $K_{\mathfrak{q}'}$. The proof of Theorem 1.6 in Section 3.4 reads the tube only through these lemmas (Steps 0, 2, 4 and 5), through $\mathfrak{q}$ in Steps 6–8, which use only that $\Pi_\mathfrak{q}$ is supercuspidal (Step 2) and that $\mathfrak{q}$ is an odd prime of Σ, and through Σ as a finite set of primes. So it proves Theorem 10.2 with $\mathcal{D}'$ in place of $\mathcal{D}$, with $\kappa = 24A$ as there. □

Lemma 10.3. *If $\sqrt{3} \in K$, then K has a tube datum at two primes, with $q \equiv q' \equiv 11 \pmod{12}$.*

Proof. Since $x_q(1) = (a_q + b_q)/q$, (3.1) gives $g_q(1) = G(q)/(4q^2 D_q^4)$ with

$$G(q) = (q^2+4)(q^2-q+4)(q^3+4q+3)(4q^3-q^2+10q+3),$$

and $g_q(1) > 0$, as $0 < x_q(1) < 1$. The resultants of q^2+4 with q^2-q+4, q^3+4q+3, $4q^3-q^2+10q+3$, q^2+3 and q are 4, 9, 193, 1 and 4 in absolute value. Choose a prime $\ell \equiv 1 \pmod 4$, unramified in K, with $\ell \nmid 2 \cdot 3 \cdot 193$, and $r \in \mathbb{Z}$ with $r^2 \equiv -4 \pmod \ell$ and $v_\ell(r^2+4) = 1$ (replace r by $r+\ell$ if needed, as $\ell \nmid 2r$). Every integer $q \equiv r \pmod{\ell^2}$ then has $v_\ell(q^2+4) = 1$, with the other three factors of $G(q)$, D_q and q prime to ℓ, so $v_\ell(g_q(1)) = 1$.

Let M be the Galois closure of K over $\mathbb{Q}$ and $\Phi = \mathbb{Q}(\zeta_{12\ell^2})$. The field $M \cap \Phi$ is abelian, totally real and unramified at ℓ, so it lies in the fixed field $\mathbb{Q}(\zeta_{12})$ of the inertia group at ℓ, hence in $\mathbb{Q}(\sqrt{3})$. The element of $\mathrm{Gal}(\Phi/\mathbb{Q}) = (\mathbb{Z}/12\ell^2\mathbb{Z})^\times$ that is 11 modulo 12 and r modulo ℓ^2 acts on $\mathbb{Q}(\zeta_{12})$ as complex conjugation, which fixes $\sqrt{3} = \zeta_{12} + \zeta_{12}^{-1}$, so it agrees on $M \cap \Phi$ with the identity of $\mathrm{Gal}(M/\mathbb{Q})$. By Chebotarev's theorem in $M\Phi$ there are infinitely many primes q, unramified in $M\Phi$, that split completely in M and satisfy $q \equiv 11 \pmod{12}$ and $q \equiv r \pmod{\ell^2}$. Take one with $q \geq 7$ and a prime $\mathfrak{q}$ of K above it: (T1) holds, and $g_q(1)$ has valuation 1 at every prime of K above ℓ, so $g_q(1) \notin K^{\times 2}$.

The extension $K(i)/K$ is totally imaginary and $K(\sqrt{g_q(1)})/K$ is quadratic and totally real, so $K(i, \sqrt{g_q(1)})/K$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^2$. By Chebotarev's theorem the primes $\mathfrak{q}'$

of K that are inert in both quadratic subextensions $K(i)$ and $K(\sqrt{g_q(1)})$ have density $1/4$; take one of residue degree one over a prime q' that is unramified in K and in $K(i,\sqrt{g_q(1)})$ and does not divide $6qD_qG(q)$. Then -1 and $g_q(1)$ are units and non-squares modulo $\mathfrak{q}'$, and 3 is a nonzero square there because $\sqrt{3}\in K$; so (T2) holds. □

10.2. **The certificate at two primes.** Fix a tube datum at two primes. In this subsection θ_i, $\mathcal{T}$ and $\hat{\psi}$ denote

$$\theta_0=0,\qquad \theta_i=\frac{\hat{q}}{\gamma_i-1}\ (1\le i\le 6),\qquad \mathcal{T}=\{\theta_0,\dots,\theta_6\},\qquad \hat{\psi}(t)=10\hat{q}+1+\frac{\hat{q}^2t}{1+\hat{q}^2t^2},$$

that is, the objects of Section 6.3 with $\hat{q}$ in place of q where q occurs outside the contacts; x_q, g_q, the γ_i and $\mathcal{C}_q$ keep q.

Lemma 10.4. (a) *The θ_i are seven distinct rationals, and $-q'(q+1)<\theta_i<-\hat{q}/2$ for $1\le i\le 6$.*

(b) *If $s\in K$ is totally positive with $v_{\mathfrak{q}}(s)\le 0$ and $v_{\mathfrak{q}'}(s)\le 0$, then $1+\hat{q}/s\in\mathcal{D}'$.*

(c) *For every $t\in K$, $\hat{\psi}(t)\in\mathcal{D}'$.*

Proof. (a) The γ_i are distinct, and $-1<\gamma_i<1/(q+1)$ by Lemma 3.2(a) and the proof of Lemma 7.1(a); so $1-\gamma_i\in(q/(q+1),2)$ and $\theta_i=-\hat{q}/(1-\gamma_i)\in(-q'(q+1),-\hat{q}/2)$. (b) Both primes are unramified and $q\ne q'$, so $v_{\mathfrak{q}}(\hat{q})=v_{\mathfrak{q}'}(\hat{q})=1$ and $v(\hat{q}/s)\ge 1$ at both; and $1+\hat{q}/s>1$ at every real place, so $g_q(1+\hat{q}/s)$ is totally positive by the proof of Lemma 3.2(b). (c) As in the proof of Lemma 3.2(d), with $u=\hat{q}t$, at $\mathfrak{q}$ and at $\mathfrak{q}'$: -1 is not a square in either residue field, as $q\equiv q'\equiv 3\pmod 4$. □

Lemma 10.5. *Let Σ be as in Theorem 10.2. Then Lemma 6.6 holds with $\hat{q}$ in place of q in $1/q$, $1+q/s$, $1+q^2t^2$, $10q+1$ and q^2t, with $\mathcal{T}$ as above and $\hat{\psi}$ in place of ψ_q, $\mathcal{D}'$ in place of $\mathcal{D}$, "$v_{\mathfrak{q}}(s)\le -1$ and $v_{\mathfrak{q}'}(s)\le -1$" in (a), and "$v_{\mathfrak{q}}(s)\le 0$ and $v_{\mathfrak{q}'}(s)\le 0$" in (b). We write $\hat{R}_\psi$ and $\hat{C}_*$ for the polynomial and the integer of (c). The leading coefficients and the pairwise resultants of the seven quadratic factors of $\hat{R}_\psi$ are nonzero.*

Proof. (a) The proof of Lemma 6.6(a) applies at $\mathfrak{q}$ and at $\mathfrak{q}'$: -1 is not a square in either residue field, and $v(1/\hat{q})=-1$ at both. (b) The first assertion is Lemma 10.4(b). In the rest of the proof of Lemma 6.6(b), $1+\hat{q}/s-\gamma_i=(1-\gamma_i)(s-\theta_i)/s$, and $\hat{q}$ is a unit at every prime outside Σ. (c) Since $10\hat{q}+1-\gamma_i>\hat{q}/2$, the proof of Lemma 6.6(c) applies with $\hat{q}$. Write $\hat{D}(t)=1+\hat{q}^2t^2$ and $f_i=(10\hat{q}+1-\gamma_i)\hat{D}+\hat{q}^2t$. The leading coefficients $\hat{q}^2$ and $(10\hat{q}+1-\gamma_i)\hat{q}^2$ are nonzero. A common root of $\hat{D}$ and f_i would satisfy $\hat{q}^2t=0$, but $\hat{D}(0)=1$; a common root of f_i and f_k with $i\ne k$ would satisfy $(\gamma_k-\gamma_i)\hat{D}(t)=f_i(t)-f_k(t)=0$, hence $\hat{D}(t)=0$, and then $\hat{q}^2t=f_i(t)=0$, again impossible. □

The fixed data are those of Section 7.1, with (F2) and (F4) unchanged and (F1), (F3) replaced by:

(F1′) a tube datum at two primes $(q,\mathfrak{q},q',\mathfrak{q}')$ for K (Lemma 10.3); the contacts γ_i, the set $\mathcal{T}$ of this subsection, $\omega=-1$, $\xi=1$, $\mathcal{T}^+=\mathcal{T}\cup\{\omega\}$, $F_8(S)=\prod_{\theta\in\mathcal{T}^+}(S-\theta)$, $d_0=0$, $d_1=2\hat{q}+2$, and $\hat{R}_\psi$. Let Σ_0 be the least set Σ allowed in Theorem 10.2, and κ the exponent that theorem gives for Σ_0;

(F3′) the set $\mathfrak{B}$ of (F3), with the primes above q' added, $\hat{C}_*$ and $\hat{R}_\psi$ in place of C_* and R_ψ, the θ_i, $\mathcal{T}^+$ and d_1 of (F1′), and $1/\hat{q}$ in place of $1/q$ in the list of differences.

Lemma 10.6. *Lemma 7.1 holds for these data, with* $(-q'(q+1), 1]$ *and* $(-q'(q+1) - 2\hat{q} - 2, -(2\hat{q}+1)]$ *as the two intervals of (a), with* $p \notin \{q, q'\}$ *in (b), and with* $\mathcal{D}'$ *in place of* $\mathcal{D}$ *in (c).*

Proof. (a) The inclusions follow from Lemma 10.4(a) with $\theta_0 = 0$, $\omega = -1$ and $\xi = 1$, and the two sets are disjoint because $-(2\hat{q}+1) < -\hat{q} - q' = -q'(q+1)$; also $0 < 1/\hat{q} < 1$. (b) As before, as $\mathfrak{B}$ contains the primes above q and q'. (c) Σ_0 consists of the primes above $p \le 324$, above q and q', and at which a nonzero finite contact or the difference of two distinct finite contacts has nonzero valuation, and $\gamma_i - \gamma_k = (\theta_k - \theta_i)(1-\gamma_i)(1-\gamma_k)/\hat{q}$; so $\Sigma_0 \subseteq \mathfrak{B}$, and the rest is the proof of Lemma 7.1(c) with Theorem 10.2 in place of Theorem 1.6. □

Proposition 10.7. *Define the certificate at* $X \in K$ *by Definition 7.2 with the data (F1′), (F2), (F3′), (F4), with* $s_j = A_j\eta + 1/\hat{q}$ *in place of* $A_j\eta + 1/q$ *and* $r = \hat{R}_\psi(\beta)$ *in place of* $R_\psi(\beta)$*. If* M *is large enough, the certificate holds at* $X \in K$ *if and only if* $X \in \mathbb{Z}$*.*

Proof. The proofs of Lemmas 7.3, 8.1 and 8.2 and Propositions 8.3 and 9.4 read K only through (E1)–(E3), and the tube only as follows; with these replacements they prove the proposition.

- Lemma 7.3: $1/\hat{q} > 0$, and $\hat{R}_\psi > 0$ on $\mathbb{R}$ (Lemma 10.5).
- Lemma 8.1 and Step 1 of Proposition 8.3: Lemma 10.6(b) for Lemma 7.1(b).
- Lemma 8.2: Lemma 10.5(c), Lemma 10.6(a) and (F3′) for Lemma 6.6(c), Lemma 7.1(a) and (F3); and if $v(\eta) > 0$ then $s_0 \equiv 1/\hat{q}$, and every $s_0 - \theta$ is a unit because $1/\hat{q} - \theta$ is.
- Step 3 of Proposition 8.3: by Lemma 10.5(a), s_j is totally positive with $v_{\mathfrak{q}}(s_j) \le -1$ and $v_{\mathfrak{q}'}(s_j) \le -1$, and so is $s_j + d_j$; by Lemma 10.5(b) with $\Sigma' = \mathfrak{B}$, $1 + \hat{q}/(s_j + d_j) \in \mathcal{D}'$ and its odd-contact primes outside $\mathfrak{B}$ are those counted in $\mathfrak{M}_j$, and Lemma 10.6(c) gives $h(s_j) \le c_1(1 + \mathfrak{M}_j^\kappa)$; by Lemma 10.4(c) and Lemma 10.5(c), $\hat{\psi}(\beta) \in \mathcal{D}'$ and its odd-contact primes outside $\mathfrak{B}$ are those counted in $\mathfrak{M}_{\mathrm{sc}}$; and $A_1 = (s_1 - 1/\hat{q})/(s_0 - 1/\hat{q})$. Steps 2, 4 and 5 read the data only through κ and (F2).
- Proposition 9.4: in Step 1, $r = \hat{R}_\psi(\beta)$ is a positive integer, and $\mathcal{S}$ contains q and q'; in Step 7, $c_{j,\theta} = (1/\hat{q} + d_j - \theta)/A_j$, a nonzero rational by Lemma 10.6(a). The other steps do not read the tube. □

11. Proof of Theorem 1.1

By Propositions 8.3 and 9.4 when $\sqrt{3} \notin K$, and by Proposition 10.7 when $\sqrt{3} \in K$ (then E is not the first curve, as $\sqrt{d} \notin K$), for $x \in K$ the certificate of Definition 7.2 holds at x if and only if $x \in \mathbb{Z}$. Appendix B writes the certificate as one polynomial equation with integer coefficients in x and 25 further unknowns, solvable in K exactly when $x \in \mathbb{Z}$ (Proposition B.5 and the end of Appendix B); this proves Theorem 1.1.

12. The fields of Theorem 1.2

For a totally real field K with $\sqrt{d} \notin K$, conditions (I1)–(I3) are statements about the index curve over $L = KF$. In Sections 12.1, 12.2, 12.3 and 12.4, E is the first index curve and $F = \mathbb{Q}(\sqrt{3})$. Section 12.5 treats the second, Section 12.6 the third and Section 12.7 the fourth, and Section 12.8 adds the fields with the same L as a field already treated.

Lemma 12.1. *Let* M *be a number field,* $B \in M^\times$ *and* $\delta \in M^\times \setminus M^{\times 2}$*. Let* $C\colon y^2 = x^3 - Bx$ *and* $C^\delta\colon y^2 = x^3 - \delta^2 Bx$*, over* M*, let* $M' = M(\sqrt{\delta})$*, and let* τ *be the nontrivial element of*

$\mathrm{Gal}(M'/M)$. *Then* $(X,Y)\mapsto(X/\delta,\,Y/(\delta\sqrt{\delta}))$ *with* $O\mapsto O$, *is a group isomorphism from* $C^\delta(M)$ *onto* $\{Q\in C(M'):\tau Q=-Q\}$, *and*

$$\operatorname{rank} C(M')=\operatorname{rank} C(M)+\operatorname{rank} C^\delta(M).$$

For $C=E_c$ *the twist* C^δ *is* $E_{\delta c}$.

Proof. If $(X,Y)\in C^\delta(M)$, then $(x,y)=(X/\delta,Y/(\delta\sqrt{\delta}))$ satisfies $y^2=(X^3-\delta^2BX)/\delta^3=x^3-Bx$, and $\tau(x,y)=(x,-y)=-(x,y)$. Conversely, a point $(x,y)\in C(M')$ with $\tau(x,y)=(x,-y)$ has $x\in M$ and $y/\sqrt{\delta}\in M$, so it comes from $(\delta x,\delta y\sqrt{\delta})\in C^\delta(M)$. The map is the restriction of the isomorphism $(X,Y)\mapsto(u^2X,u^3Y)$, $u=1/\sqrt{\delta}$, of C^δ onto C over M', so it is a homomorphism. For $Q\in C(M')$ we have $2Q=(Q+\tau Q)+(Q-\tau Q)$, where $Q+\tau Q\in C(M)$ and τ maps $Q-\tau Q$ to its negative. A point of $C(M)$ that τ maps to its negative has order at most two. So the map $(R,Q)\mapsto R+Q$ from $C(M)\oplus\{Q\in C(M'):\tau Q=-Q\}$ to $C(M')$ has finite kernel and a cokernel killed by 2, and the ranks add. □

12.1. **Real quadratic fields.** For $K=\mathbb{Q}(\sqrt{2m})$ or $\mathbb{Q}(\sqrt{6m})$ with m as in Theorem 1.2, the field L is $F(\sqrt{2m})$, and by Lemma 12.1 the rank of $E(L)$ is that of $E(F)$ plus that of the quadratic twist E_{2ma} over F. A 2-isogeny descent over F shows that this twist has rank 0.

Let $F_\lambda=\mathbb{Q}_2(\sqrt{3})$, with ring of integers $\mathbb{Z}_2[\sqrt{3}]$ and $v_\lambda(2)=2$. By Hensel's lemma a unit $u\equiv1\pmod{\lambda^5}$ is a square in F_λ, as $5>2v_\lambda(2)$. Since $v_\lambda(8)=6$, a unit is therefore a square exactly when it is congruent modulo 8 to one of the squares of units

$$1,\qquad 3,\qquad 5+4\sqrt{3},\qquad 7+4\sqrt{3},\tag{12.1}$$

the values of $(s+t\sqrt{3})^2$ with $s+t$ odd. So $-1\equiv7$ is not a square, while $-5\equiv3$ and $-7\equiv1$ are, and every odd rational integer is a square or minus a square in F_λ. Neither $\varepsilon a\equiv3+6\sqrt{3}$ nor $-\varepsilon a\equiv5+2\sqrt{3}$ is a square, and no product of a nonempty subset of $\{-1,\varepsilon,\varepsilon a\}$ is congruent to an element of (12.1), so -1, ε and εa are independent in $F_\lambda^\times/F_\lambda^{\times2}$.

Lemma 12.2 (The dyadic image)**.** *Let* $c\in F_\lambda^\times$ *with* $c\in\pm2aF_\lambda^{\times2}$. *Then over* F_λ, $\operatorname{Im}\alpha_c'=\{1,[-1]\}$ *and* $|\operatorname{Im}\alpha_c|=8$.

Proof. If $c=su^2 2a$ with $s=\pm1$, the maps $(x,y)\mapsto(u^2x,u^3y)$ are isomorphisms $E_{2a}\to E_c$ and $E_{2a}'\to E_c'$ (note $E_{-c}=E_c$); they commute with ϕ, multiply abscissas by a square and fix $(0,0)$, so they preserve both images. We may therefore take $c=2a$. The ring of integers of F_λ is isomorphic to $\mathbb{Z}_2^2$, so $\chi(E_c(F_\lambda))=|\mathbb{Z}_2^2/2\mathbb{Z}_2^2|=4$ in the notation of the proof of Lemma 2.3, and $|E_c(F_\lambda)/2E_c(F_\lambda)|=16$; by Lemma 2.1, $|\operatorname{Im}\alpha_c|\cdot|\operatorname{Im}\alpha_c'|=16$. On $E_{2a}'\colon y^2=x^3+16a^2x$ the abscissa $x=-2/\varepsilon=-4+2\sqrt{3}$ gives

$$x^3+16a^2x=-\Big(\frac{\lambda^3}{\varepsilon^3}\Big)^2(917+528\sqrt{3}),$$

and $-(917+528\sqrt{3})\equiv3\pmod8$ is a unit square by (12.1); so $[-2/\varepsilon]=[-1]$ lies in $\operatorname{Im}\alpha_c'$. On E_{2a} the abscissa $x=2$ gives $x^3-4a^2x=16\cdot(-(9+4\sqrt{3}))$ and $-(9+4\sqrt{3})\equiv7+4\sqrt{3}=\varepsilon^2\pmod8$, so $[2]=[\varepsilon]\in\operatorname{Im}\alpha_c$. With the torsion classes $\alpha_c(0,0)=[-1]$ and $\alpha_c(2a,0)=[2a]=[\varepsilon a]$, $\operatorname{Im}\alpha_c$ contains $\langle-1,\varepsilon,\varepsilon a\rangle$, of order 8, as -1, ε and εa are independent. Hence $|\operatorname{Im}\alpha_c'|\le2$, and since -1 is not a square in F_λ, $\operatorname{Im}\alpha_c'=\{1,[-1]\}$ and $|\operatorname{Im}\alpha_c|=8$. □

Proposition 12.3. *Let* $m\ge1$ *be a squarefree integer all of whose prime factors* p *satisfy* $p\equiv\pm5\pmod{12}$ *and* $\left(\frac{p}{13}\right)=-1$, *and let* $c=2ma$. *Then* $\operatorname{Im}\alpha_c'=\{1\}$ *and* $\operatorname{Im}\alpha_c=\langle[-1],[c]\rangle$ *over* F, *and* $\operatorname{rank}E_c(F)=0$.

Proof. Write $m = p_1 \cdots p_r$ ($r \geq 0$). Each p_k is inert in F, so the odd primes dividing c are $\mathfrak{a}$ and the (p_k), each to the first power, and $v_\lambda(c) = 2$. By Lemma 2.2 both images lie in $V = \langle -1, \varepsilon, a, p_1, \ldots, p_r \rangle$. Write $e \in V$ as $e = (-1)^h \varepsilon^i a^j \prod_k p_k^{l_k}$ with exponents in $\{0, 1\}$.

At $v = (p_k)$ the field F_v is unramified of degree two over $\mathbb{Q}_{p_k}$, with residue field $\mathbb{F}_{p_k^2}$. Every element of $\mathbb{F}_{p_k}$ is a square in $\mathbb{F}_{p_k^2}$, so -1, 2, p_j ($j \neq k$) and $\varepsilon = \lambda^2/2$ are squares in F_v; a unit of F_v is a square exactly when its norm to $\mathbb{Q}_{p_k}$ is a square modulo p_k, and $\mathrm{N}_{F/\mathbb{Q}}(a) = 13$ is a nonsquare modulo p_k because $(\frac{13}{p_k}) = (\frac{p_k}{13}) = -1$. Also $\iota = \sqrt{-1}$ and 2ι are squares in $\mathbb{F}_{p_k^2}$ (as $8 \mid p_k^2 - 1$). At $v = \mathfrak{a}$, $F_v = \mathbb{Q}_{13}$, -1 and 2ι are squares and 2, ε, p_k are not. So Lemma 2.3 gives $\operatorname{Im} \alpha_{c,v} = \operatorname{Im} \alpha'_{c,v} = \langle [c] \rangle$ at $\mathfrak{a}$ and at each (p_k).

In $F_v^\times / F_v^{\times 2} \cong (\mathbb{Z}/2)^2$ use the coordinates (valuation modulo 2, residue symbol of the unit part with respect to the uniformizer p_k, respectively a). At (p_k), $[c]$ has coordinates $(1, 1)$ (the unit part $2a \prod_{j \neq k} p_j$ is a nonsquare because of a) and e has coordinates (l_k, j); so $e \in \langle [c] \rangle$ forces $l_k = j$. At $\mathfrak{a}$, $[c]$ has coordinates $(1, 1 + r)$ (unit part $2m$) and e has $(j, i + \sum_k l_k)$; with $l_k = j$ the condition is $i + rj = j(1 + r)$, that is $i = j$. Hence both images lie in $\{e \in V : l_k = j \text{ for all } k,\ i = j\} = \langle [-1], [\varepsilon a m] \rangle = \langle [-1], [c] \rangle$, since $[c] = [2ma] = [\varepsilon m a]$. The torsion gives $\alpha_c(0, 0) = [-1]$ and $\alpha_c(c, 0) = [c]$, so $\operatorname{Im} \alpha_c = \langle [-1], [c] \rangle$.

A class e in $\operatorname{Im} \alpha'_c$ is totally positive: if $e < 0$ at a real place then the right-hand side of the first equation (2.1) is negative there for $(U, V) \neq (0, 0)$. So $\operatorname{Im} \alpha'_c \subseteq \{1, [c]\}$. At λ, m is an odd rational integer, hence a square or minus a square, so $c \in \pm 2a F_\lambda^{\times 2}$, and Lemma 12.2 gives $\operatorname{Im} \alpha'_{c,\lambda} = \{1, [-1]\}$; but $[c] = [\varepsilon a][m]$ with $[m] \in \{1, [-1]\}$, and neither εa nor $-\varepsilon a$ is a square in F_λ. So $[c] \notin \operatorname{Im} \alpha'_c$, and $\operatorname{Im} \alpha'_c = \{1\}$. By Lemma 2.1, $2^{\operatorname{rank} E_c(F)} = 4 \cdot 1/4 = 1$. □

Proposition 12.4 (Sun [60, Theorem 1.6])**.** *For $L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\operatorname{rank} E(L_1) = 1$, $E(L_1)_{\mathrm{tors}} = E[2]$ and $2E(L_1) \subseteq E(F)$.*

Proof. Here $L_1 = F(\sqrt{2})$. By Lemma 12.1 with $M = F$, $B = a^2$ and $\delta = 2$, $\operatorname{rank} E(L_1) = \operatorname{rank} E(F) + \operatorname{rank} E_{2a}(F) = 1 + 0$, by Proposition 2.6 and by Proposition 12.3 with $m = 1$. By Kummer theory $F \cap L_1^{\times 2} = F^{\times 2} \cup 2F^{\times 2}$, whose elements have square norms, so Lemma 2.4(d) gives $E(L_1)_{\mathrm{tors}} = E[2]$. Finally Lemma 2.7 gives $2E(L_1) \subseteq E(F)$. □

Proposition 12.5. *Let $m' \geq 1$ be a squarefree integer as in Proposition 12.3, prime to 13, and $m = 13m'$. Then $\operatorname{rank} E_{2ma}(F) = 0$.*

Proof. Since $13 = a\bar{a}$, $2ma = 2m'\bar{a} \cdot a^2$, and $(x, y) \mapsto (a^2 x, a^3 y)$ is an isomorphism $E_{2m'\bar{a}} \to E_{2ma}$ over F. The curve $E_{2m'\bar{a}}$ is the conjugate of $E_{2m'a}$ under σ, and σ maps $E_{2m'a}(F)$ bijectively onto $E_{2m'\bar{a}}(F)$. So $\operatorname{rank} E_{2ma}(F) = \operatorname{rank} E_{2m'a}(F) = 0$ by Proposition 12.3. □

Proof of Theorem 1.2. For (a), let m be as in Theorem 1.2 and $K = \mathbb{Q}(\sqrt{2m})$ or $\mathbb{Q}(\sqrt{6m})$. Then $\sqrt{3} \notin K$, since $6m$ and $18m$ are not squares, and $L = K(\sqrt{3}) = F(\sqrt{2m})$ in both cases (as $\sqrt{6m}/\sqrt{3} = \sqrt{2m}$). By Lemma 12.1 with $M = F$, $B = a^2$ and $\delta = 2m$, $\operatorname{rank} E(L) = \operatorname{rank} E(F) + \operatorname{rank} E_{2ma}(F)$, and $\operatorname{rank} E_{2ma}(F) = 0$ by Proposition 12.3 if $13 \nmid m$ and by Proposition 12.5 if $13 \mid m$. So (I1) holds by Proposition 2.6. By Kummer theory $F \cap L^{\times 2} = F^{\times 2} \cup 2mF^{\times 2}$, whose elements have square norms, so Lemma 2.4(d) gives (I2). Since $K/\mathbb{Q}$ is Galois, Lemma 2.7 gives (I3). Theorem 1.1 then gives a Diophantine definition of $\mathbb{Z}$ in K with 25 unknowns. For the seven cyclic fields of Proposition 12.7, that proposition gives $\sqrt{3} \notin K$ and (I1)–(I3), and Theorem 1.1 applies in the same way. For $K = \mathbb{Q}(\sqrt{D})$ in (b), Proposition 12.13 gives $\sqrt{2} \notin K$, $\sqrt{3} \notin K$ and (I1)–(I3) for the second curve, and Theorem 1.1 applies. For $K = \mathbb{Q}(\sqrt{3})$, Proposition 12.14 gives $\sqrt{2} \notin K$ and (I1)–(I3), and Theorem 1.1 applies. For $K = \mathbb{Q}(\sqrt{D})$ in (c) and for the 77 fields $\mathbb{Q}(\sqrt{D})$ of Table 1,

Propositions 12.19 and 12.20 give $\sqrt{2} \notin K$ and (I1)–(I3) for the third curve, and Theorem 1.1 applies. For the four biquadratic fields of Table 1, Proposition 12.21 gives $\sqrt{17} \notin K$ and (I1)–(I3) for the fourth curve, and Theorem 1.1 applies, through Section 10 for the two fields that contain $\sqrt{3}$. The fields of Proposition 12.23, among them $\mathbb{Q}(\sqrt{2D})$, are treated in Section 12.8. □

Corollary 12.6 (Sun [60, Theorems 1.2 and 1.4])**.** *$\mathbb{Z}$ is Diophantine in $\mathbb{Q}(\sqrt{6})$ and in $\mathbb{Q}(\sqrt{2})$, with 25 unknowns.*

Proof. This is the case $m = 1$ of Theorem 1.2. In the proof of Theorem 1.1 one may take the tube prime $q = 19$ and $\mathfrak{q} = (5 - \sqrt{6})$ for $\mathbb{Q}(\sqrt{6})$, where Sun takes $q = 331$ [60, (15.1)], and Sun's $q = 367$ [60, §1], with $\mathfrak{q} = (23 - 9\sqrt{2})$, for $\mathbb{Q}(\sqrt{2})$; see Lemma 3.1. □

12.2. **Cyclic fields of degrees 3, 4, 5 and 8.** Let K_f be the cyclic cubic field of conductor f for $f = 9$, 13, 19 and 37, and the maximal real subfield $\mathbb{Q}(\zeta_f)^+$ of $\mathbb{Q}(\zeta_f)$ for $f = 11$, 16 and 32. Put $L_f = K_f F$ and $L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and write D_M for the discriminant of a number field M. For odd f the degree $[L_f : F]$ is odd, and we bound $\operatorname{rank} E(L_f)$ by a complete 2-descent over L_f, as in Section 12.3. The field L_{16} is a quadratic extension of L_1, and L_{32} of L_{16}, so for them the descent is that of a twist, by Lemma 12.1. Torsion is excluded by Lemma 2.4.

Proposition 12.7. *Let $K = K_f$ be one of these seven fields, and $L = L_f$. Then $K = \mathbb{Q}(\theta)$ for a root θ of the polynomial g_f in the table, and q and $\mathfrak{q}$ are as there:*

K	$g_f(t)$	$\operatorname{disc}(g_f) = D_K$	q	$\mathfrak{q}$
K_9	$t^3 - 3t - 1$	3^4	19	$(19, \theta - 10)$
K_{13}	$t^3 - t^2 - 4t - 1$	13^2	31	$(31, \theta - 4)$
K_{19}	$t^3 - t^2 - 6t + 7$	19^2	7	$(7, \theta)$
K_{37}	$t^3 - t^2 - 12t - 11$	37^2	31	$(31, \theta - 2)$
K_{11}	$t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1$	11^4	43	$(43, \theta - 4)$
K_{16}	$t^4 - 4t^2 + 2$	2^{11}	31	$(31, \theta - 5)$
K_{32}	$t^8 - 8t^6 + 20t^4 - 16t^2 + 2$	2^{31}	31	$(31, \theta - 4)$

(a) *K is totally real and Galois over $\mathbb{Q}$, with cyclic Galois group, and $\sqrt{3} \notin K$; L is totally real and Galois over $\mathbb{Q}$, of degree $2[K : \mathbb{Q}]$.*

(b) *Conditions (I1), (I2) and (I3) hold for K.*

(c) *$q \equiv 7 \pmod{12}$, and $\mathfrak{q}$ is a prime of K above q, unramified over q, of residue degree one. For K_9, K_{13} and K_{37} the prime 7 is inert, so (7) is also a prime of K unramified over 7, of odd residue degree 3.*

By (a) and (b), Theorem 1.1 applies to these fields, and (c) gives primes q and $\mathfrak{q}$ as in Theorem 1.6, explicit tube primes for its proof, as Corollary 12.6 does for $\mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{2})$.

Lemma 12.8. *Parts (a) and (c) of Proposition 12.7 hold. Moreover:*

(i) *K_f is the subfield of $\mathbb{Q}(\zeta_f)$ fixed by H_f, where $H_f = \{\pm 1\}$ for $f = 9$, 11, 16, 32 and H_f is the group of cubes in $(\mathbb{Z}/f)^\times$ for $f = 13$, 19, 37. A prime $p \nmid f$ has residue degree in K_f the order of p in $(\mathbb{Z}/f)^\times / H_f$, and if p splits in F, so has every prime of L_f above p. The prime 11 is totally ramified in K_{11}.*

(ii) *$F \cap L_f^{\times 2}$ is $F^{\times 2}$ for odd f, and $F^{\times 2} \cup 2F^{\times 2}$ for $f = 16$ and 32.*

(iii) *For a root θ of g_{16} put $\sqrt{2}=\theta^2-2$. Then $L_{16}=L_1(\theta)$, of degree 2 over L_1, with $\theta^2=2+\sqrt{2}$. If ϑ is a root of g_{32}, then $\theta=\vartheta^2-2$ is a root of g_{16}, and $L_{32}=L_{16}(\vartheta)$, of degree 2 over L_{16}, with $\vartheta^2=\alpha=2+\theta$.*

Proof. The fields K. Each cubic g_f has no rational root, as ±1, ±7 and ±11 are not roots, so it is irreducible, and its discriminant is f^2. So $K=\mathbb{Q}(\theta)$ is cyclic of degree 3, and it is totally real, as a real root generates it. As D_K divides f^2 with square quotient and a cubic field has $|D_K|\geq 23$, $\mathcal{O}_K=\mathbb{Z}[\theta]$ and $D_K=f^2$, and $K=K_f$ by the conductor–discriminant formula. For $f=11$, 16 and 32, $\zeta_f+\zeta_f^{-1}$ is a root of g_f: for $f=11$ by $1+\sum_{k=1}^{5}(\zeta_{11}^k+\zeta_{11}^{-k})=0$, and for $f=16$ and 32 because $(\zeta_f+\zeta_f^{-1})^2-2=\zeta_f^2+\zeta_f^{-2}$, $\zeta_8+\zeta_8^{-1}=\sqrt{2}$ and $g_{32}(t)=g_{16}(t^2-2)$. The polynomials g_{16} and g_{32} are Eisenstein at 2, and $g_{11}(t+2)$ at 11, the only prime dividing $\operatorname{disc}(g_f)$. So g_f is irreducible, $\mathcal{O}_K=\mathbb{Z}[\theta]$, $D_K=\operatorname{disc}(g_f)$, and $K=\mathbb{Q}(\zeta_f)^+$ by degrees, with Galois group $(\mathbb{Z}/f)^\times/\{\pm1\}$, cyclic as $(\mathbb{Z}/2^j)^\times=\{\pm1\}\times\langle5\rangle$. In (i), K_f is the fixed field of $\{\pm1\}$ for $f=11$, 16 and 32. A cyclic cubic field of conductor f lies in $\mathbb{Q}(\zeta_f)$, and for $f=9$, 13, 19 and 37 the group $(\mathbb{Z}/f)^\times$ is cyclic, with H_f as its subgroup of index 3. The residue degree of $p\nmid f$ is the order of its Frobenius, and 11 is totally ramified in $\mathbb{Q}(\zeta_{11})$. For odd f, $[K:\mathbb{Q}]$ is odd. For $f=16$ and 32 the only quadratic subfield of the cyclic field K is $\mathbb{Q}(\sqrt{2})$, as $\theta^2-2=\pm\sqrt{2}$ lies in $K_{16}\subseteq K_{32}$. So $\sqrt{3}\notin K$.

The fields L. Since $\sqrt{3}\notin K$, $[L:K]=2$. As $K\cap F=\mathbb{Q}$, L is Galois over $\mathbb{Q}$ with $\operatorname{Gal}(L/\mathbb{Q})=\operatorname{Gal}(K/\mathbb{Q})\times\operatorname{Gal}(F/\mathbb{Q})$, and it is totally real. A prime $p\nmid f$ that splits in F has Frobenius $(\operatorname{Frob}_K,1)$ at a prime of L, which gives the last claim of (i). Restriction maps $\operatorname{Gal}(L/F)$ isomorphically onto $\operatorname{Gal}(K/\mathbb{Q})$. For odd f, if $x\in L$ and $x^2\in F$, then $[F(x):F]\leq2$ divides the odd degree $[L:F]$, so $x\in F$. For $f=16$ and 32, L/F is cyclic, its only quadratic subextension is $F(\sqrt{2})=L_1$, and Kummer theory gives (ii). For (iii), $L_{16}=\mathbb{Q}(\theta,\sqrt{3})$ contains $\sqrt{2}=\theta^2-2$, so $L_{16}=L_1(\theta)$, and $g_{16}(\vartheta^2-2)=g_{32}(\vartheta)=0$ and $L_{32}=\mathbb{Q}(\vartheta,\sqrt{3})=L_{16}(\vartheta)$; the degrees of L_1, L_{16} and L_{32} over $\mathbb{Q}$ are 4, 8 and 16.

Part (c). Each prime q of the table is congruent to 7 modulo 12 and does not divide $\operatorname{disc}(g_f)$, so it is unramified in K. The r of $\mathfrak{q}=(q,\theta-r)$ is a root of g_f modulo q, simple as $q\nmid\operatorname{disc}(g_f)$, and since $\mathcal{O}_K=\mathbb{Z}[\theta]$, Dedekind's criterion makes $\mathfrak{q}$ a prime of degree one. By (i), 7 is inert in K_9, K_{13} and K_{37}, as $7\not\equiv\pm1 \pmod 9$ and 7 is not a cube modulo 13 or 37. □

12.3. **A complete 2-descent.** Let M be a totally real number field containing F, of degree n_M, and let $c\in\mathcal{O}_M$ be nonzero. The curve $E_c\colon y^2=x^3-c^2x=x(x-c)(x+c)$ of Section 2.2, now over M, has its points of order two $(0,0)$, $(c,0)$, $(-c,0)$ defined over M, and we bound $\operatorname{rank}E_c(M)$ by a complete 2-descent. Dimensions are over $\mathbb{F}_2$. Let S be the set of finite primes of M dividing $2c$, and

$$M(S,2)=\{x\in M^\times/M^{\times2}:\ v(x)\text{ is even for every finite prime }v\notin S\}.$$

For a field $k\supseteq M$ let $\partial_k\colon E_c(k)\to(k^\times/k^{\times2})^2$ be the map

$$(x,y)\mapsto(x,\,x-c)\ \ (x\neq0,c),\qquad(0,0)\mapsto(-c^2,-c),\qquad(c,0)\mapsto(c,2c^2),\qquad O\mapsto(1,1),$$

and write $\partial=\partial_M$ and $\partial_v=\partial_{M_v}$ for a place v of M, with $\mathcal{O}_v$ the ring of integers of M_v when v is finite.

By [56, Proposition X.1.4], with $e_1=0$, $e_2=c$ and $e_3=-c$, the map ∂_k is a homomorphism with kernel $2E_c(k)$ for $k=M$; its values there at $(0,0)$ and $(c,0)$ are $(-1,-c)$ and $(c,2)$, equal modulo squares to those above. The same holds for $k=M_v$, as the proof uses only that k is perfect of characteristic not 2 with $E_c[2]\subseteq E_c(k)$. As E_c has discriminant $64c^6$, S

contains the primes of bad reduction, and the same proposition gives $\partial(E_c(M)) \subseteq M(S,2)^2$. So $E_c(M)/2E_c(M)$, of dimension rank $E_c(M)+2$, embeds in

$$\mathrm{Sel}(E_c/M) = \{\xi \in M(S,2)^2 : \ \xi_v \in \partial_v(E_c(M_v)) \text{ for every } v \in S \text{ and every real place } v\}, \tag{12.2}$$

where ξ_v is the image of ξ in $(M_v^\times/M_v^{\times 2})^2$. Hence $\operatorname{rank} E_c(M) \le \dim \mathrm{Sel}(E_c/M) - 2$.

Lemma 12.9. *Let v be a place of M.*

(i) *If v is finite, then $|E_c(M_v)/2E_c(M_v)|$ is $4\cdot 2^{[M_v:\mathbb{Q}_2]}$ if $v \mid 2$ and 4 if $v \nmid 2$. So $\partial_v(E_c(M_v))$ has dimension $2+[M_v:\mathbb{Q}_2]$, respectively 2, and any subspace of it of that dimension is all of it.*

(ii) *If v is real, then $\partial_v(E_c(M_v)) = \{(1,1),(-1,-c)\}$, of dimension 1.*

(iii) *If v is finite, with uniformiser π and ramification index e over p, then $\pi^k u \mapsto (k \bmod 2,\ u \bmod v^m)$ ($u \in \mathcal{O}_v^\times$) induces an isomorphism $M_v^\times/M_v^{\times 2} \to \mathbb{Z}/2 \times G/G^2$, where $G = (\mathcal{O}_v/v^m)^\times$ with $m = 2e+1$ if $p=2$ and $m=1$ if p is odd.*

Proof. (i) As in the proofs of Lemmas 2.3 and 12.2: $\chi(A) = |A/2A|/|A[2]|$ is multiplicative in short exact sequences and 1 on finite groups, $E_c(M_v)$ has a subgroup of finite index isomorphic to the additive group of $\mathcal{O}_v$ [56, Proposition VII.6.3], $\chi(\mathcal{O}_v) = |\mathcal{O}_v/2\mathcal{O}_v|$ is $2^{[M_v:\mathbb{Q}_2]}$ if $v \mid 2$ and 1 otherwise, and $E_c(M_v)[2] = E_c[2]$ has order 4. As ∂_v has kernel $2E_c(M_v)$, it is injective on $E_c(M_v)/2E_c(M_v)$.

(ii) On $E_c(\mathbb{R})$ the cubic $x(x-c)(x+c)$ is nonnegative exactly when $-|c| \le x \le 0$ or $x \ge |c|$. For $x \ge |c|$ we have $x > 0$ and $x - c \ge 0$, with $x - c = 0$ only at $(c,0)$ when $c > 0$, whose image $(c, 2c^2)$ is $(1,1)$; so these points map to $(1,1)$. For $-|c| \le x \le 0$ we have $x \le 0$, and $x - c$ has the sign of $-c$; it vanishes only at $(c,0)$ when $c < 0$, whose image is $(c, 2c^2) = (-1,1) = (-1,-c)$. So these points map to $(-1,-c) = \partial_v(0,0)$.

(iii) A unit u with $u \equiv w^2 \pmod{v^m}$ has $v(u/w^2 - 1) \ge m$. For $p=2$, $m = 2e+1 > 2v(2)$, so Hensel's lemma applied to $X^2 - u/w^2$ at $X = 1$ gives a root; for p odd, a unit that is a square modulo v is a square. So $\mathcal{O}_v^\times/\mathcal{O}_v^{\times 2} \cong G/G^2$. □

Proposition 12.10. *For the fields M and the curves E_c in the table, where $\alpha = 2+\theta$ for a root θ of g_{16}, every prime ideal of M of norm at most $B_M = (n_M!/n_M^{n_M})\sqrt{|D_M|}$ is principal, and $\mathrm{Sel}(E_c/M)$ has the dimension given there. The column S gives the ramification index and the residue degree of the prime of M above 2 and of the prime above $\mathfrak{a} = (a)$, and "rank" is the rank of the local conditions that define $\mathrm{Sel}(E_c/M)$ in $M(S,2)^2$.*

M	D_M	S	$\dim M(S,2)$	c	*rank*	$\dim \mathrm{Sel}(E_c/M)$
L_9	$2^6\cdot 3^9$	$(2,3);\ (1,3)$	8	a	13	3
L_{13}	$2^6\cdot 3^3\cdot 13^4$	$(2,3);\ (3,1)$	8	a	13	3
L_{19}	$2^6\cdot 3^3\cdot 19^4$	$(2,3);\ (1,3)$	8	a	13	3
L_{37}	$2^6\cdot 3^3\cdot 37^4$	$(2,3);\ (1,3)$	8	a	13	3
L_{11}	$2^{10}\cdot 3^5\cdot 11^8$	$(2,5);\ (1,5)$	12	a	21	3
L_1	$2^8\cdot 3^2$	$(4,1);\ (1,2)$	6	$(2+\sqrt{2})a$	10	2
L_{16}	$2^{24}\cdot 3^4$	$(8,1);\ (1,4)$	10	αa	18	2

Proof. For each prime ideal $\mathfrak{p}$ of norm at most B_M we find $\beta \in \mathfrak{p}$ with $|\mathrm{N}_{M/\mathbb{Q}}(\beta)| = N\mathfrak{p}$; then $\mathfrak{p} \mid (\beta)$ and the norms agree, so $\mathfrak{p} = (\beta)$. By Minkowski's bound M then has class number one. So $M(S,2)$ is the image of the group of S-units, and by Dirichlet's S-unit theorem it has dimension $n_M + \#S$, as M is totally real and an S-unit that is a square in

M is the square of an S-unit. We find a basis of $M(S,2)$ consisting of -1, n_M-1 units and generators of the primes of S. Their independence modulo squares is shown by quadratic characters: at a prime $\mathfrak{l}\notin S$ of degree one at which they are units, $x\mapsto (x \bmod \mathfrak{l})^{(N\mathfrak{l}-1)/2}$ kills squares, and the matrix of these characters at some such primes has full rank.

Local classes at a finite place are computed through Lemma 12.9(iii), by discrete logarithms in $(\mathcal{O}_v/v^m)^\times$, and at a real place they are signs. At the prime above 2 we find points of $E_c(M_v)$ whose images span a space of the dimension $2+[M_v:\mathbb{Q}_2]=2+n_M$ of Lemma 12.9(i), which is therefore the whole image. At the prime above $\mathfrak{a}$ the images of $E_c[2]$ span the image, of dimension 2, and at the real places it is given by Lemma 12.9(ii). So $\mathrm{Sel}(E_c/M)$ is the kernel of $2n_M+4=2\dim M(S,2)$ linear forms on $M(S,2)^2$: n_M+2 at the prime above 2, two at the prime above $\mathfrak{a}$ and one at each of the n_M real places. We find the ranks in the table.

The sets S come from the splitting of 2 and 13. For odd f, 2 is inert in K_f by Lemma 12.8(i), as $2\not\equiv\pm1$ modulo 9 and 11, and 2 is not a cube modulo 13, 19 or 37. As 2 ramifies in F, L_f has one prime above 2, with ramification index 2 and residue degree $[K_f:\mathbb{Q}]$. In L_{16} the prime 2 is totally ramified. Indeed an inertia group above 2 maps onto $\mathrm{Gal}(K_{16}/\mathbb{Q})$, as g_{16} is Eisenstein at 2, and if it had index 2 in $\mathrm{Gal}(L_{16}/\mathbb{Q})$, its fixed field would be a quadratic field unramified at 2; but the quadratic subfields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ of L_{16} all ramify at 2. The same argument applies to L_1, whose quadratic subfields are these three. The prime $\mathfrak{a}$ is totally ramified in L_{13}/F. It is inert in $L_1=F(\sqrt{2})$, as 2 is not a square modulo 13, and in the other L_f of the table, as 13 has order $[K_f:\mathbb{Q}]$ in $(\mathbb{Z}/f)^\times/H_f$. For $c=(2+\sqrt{2})a$ and $c=\alpha a$ the set S is the same as for $c=a$: $(2+\sqrt{2})=(\sqrt{2})$ is the prime of $\mathbb{Q}(\sqrt{2})$ above 2, and $\mathrm{N}_{K_{16}/\mathbb{Q}}(\alpha)=g_{16}(-2)=2$, so $\alpha\mathcal{O}_{L_{16}}$ is the square of the prime above 2.

For $M=L_{11}$ the image at the prime $\mathfrak{w}=\lambda\mathcal{O}_M$ above 2 comes from explicit points. Here $M_\mathfrak{w}$ is unramified of degree 5 over F_λ, with residue field $k\cong\mathbb{F}_{32}$, and $a=3+\lambda\equiv1 \pmod{\mathfrak{w}}$, so x^3-a^2x reduces to $x^3+x=x(x+1)^2$. For each of the 31 elements $r\neq1$ of k, let $y_r=\lambda$ if $r=0$, and otherwise let $y_r\in\mathcal{O}_M$ lift the square root of r^3+r in k. Then r is a simple root of $X^3-a^2X-y_r^2$ modulo $\mathfrak{w}$. Newton's method, run modulo 2^{40}, gives $\tilde{x}_r\in\mathcal{O}_M$ with $\tilde{x}_r\equiv r \pmod{\mathfrak{w}}$ such that $\tilde{x}_r^3-a^2\tilde{x}_r$ is a nonzero square in $M_\mathfrak{w}$, by Lemma 12.9(iii); so $\tilde{x}_r$ is the abscissa of a point of $E(M_\mathfrak{w})$. The images of these 31 points, with $\partial_\mathfrak{w}(0,0)$ and $\partial_\mathfrak{w}(a,0)$, span a space of dimension $12=2+[M_\mathfrak{w}:\mathbb{Q}_2]$, the whole image. □

12.4. **The conditions over L.**

Proof of Proposition 12.7. Parts (a) and (c) are Lemma 12.8. We prove (b).

Condition (I1). For odd f, $\dim\mathrm{Sel}(E/L_f)=3$ by Proposition 12.10, so $\mathrm{rank}\,E(L_f)\le1$ by (12.2). The point $P_0\in E(F)\subseteq E(L_f)$ has infinite order by Proposition 2.6, so $\mathrm{rank}\,E(L_f)=1$.

For $f=16$ put $s=2+\sqrt{2}$, so that $L_{16}=L_1(\theta)$ with $\theta^2=s$, by Lemma 12.8(iii). Lemma 12.1 with $M=L_1$, $B=a^2$ and $\delta=s$ gives $\mathrm{rank}\,E(L_{16})=\mathrm{rank}\,E(L_1)+\mathrm{rank}\,E_{sa}(L_1)$. Here $\mathrm{rank}\,E(L_1)=1$ by Proposition 12.4, and $\dim\mathrm{Sel}(E_{sa}/L_1)=2$ by Proposition 12.10, so $\mathrm{rank}\,E_{sa}(L_1)=0$ by (12.2). Hence $\mathrm{rank}\,E(L_{16})=1$. For $f=32$ the same argument, with $M=L_{16}$, $\delta=\alpha$ and $L_{32}=L_{16}(\vartheta)$, gives $\mathrm{rank}\,E(L_{32})=\mathrm{rank}\,E(L_{16})+\mathrm{rank}\,E_{\alpha a}(L_{16})=1+0$.

Condition (I2). By Lemma 12.8(ii), every element of $F\cap L^{\times2}$ has its norm in $\mathbb{Q}^{\times2}$. So Lemma 2.4(c) gives $E(L)_{\mathrm{tors}}=E[2]$, with the primes p_1, p_2 and the residue degrees k_1, k_2 of the primes of L above them in the following table, for which no prime $\ell\ge5$ divides both

$p_1 N_{k_1}(p_1)$ and $p_2 N_{k_2}(p_2)$:

f	9	13	19	37	11	16	32
p_1 (k_1)	11 (3)	11 (3)	11 (1)	11 (1)	11 (1)	11 (4)	11 (8)
p_2 (k_2)	23 (3)	23 (3)	23 (3)	23 (1)	23 (1)	23 (2)	47 (2)

The primes 11, 23 and 47 are congruent to 3 modulo 4 and split in F, as 3 is 5^2, 7^2 and 12^2 modulo them. The residue degrees come from Lemma 12.8(i), except at 11 in L_{11}, where they are one, as 11 splits in F and is totally ramified in K_{11}. For L_{32} the prime 47 replaces 23: the primes of L_{32} above 23 have residue degree 4, and $N_4(23) = (23^2-1)^2$ is divisible by 11.

Condition (I3). Since $K/\mathbb{Q}$ is Galois, (I3) follows from (I1) and (I2) by Lemma 2.7. □

12.5. **Real quadratic fields for the second curve.** In this subsection E is the second index curve, over $F = \mathbb{Q}(\sqrt{2})$, with the notation of Section 2.6. Let I^- be the set of primes q with $q \equiv \pm 3 \pmod 8$ and $(\frac{q}{7}) = -1$, that is, $q \equiv 3$, 5, 13, 19, 27 or 45 (mod 56). The integers D of Theorem 1.2(b) are the products $D = 7^k q_1 \cdots q_r \neq 3$ with $k \in \{0,1\}$, r odd and $q_1, \dots, q_r$ distinct primes of I^-: a product of r residues in $\{3,5\}$ modulo 8 lies in $\{3,5\}$ exactly when r is odd, and $7 \equiv -1$ exchanges 3 and 5.

Lemma 12.11 (The dyadic place)**.** *Let $F_\lambda = \mathbb{Q}_2(\sqrt{2})$, with ring of integers $\mathcal{O}_\lambda = \mathbb{Z}_2[\sqrt{2}]$ and $v_\lambda(2) = 2$.*

(a) *A unit $u = x + y\sqrt{2}$ of $\mathcal{O}_\lambda$ (x odd) is a square in F_λ if and only if $u \equiv 1$ or $3 + 2\sqrt{2}$ (mod $4\sqrt{2}$), that is, (x mod 8, y mod 4) is $(1,0)$ or $(3,2)$.*

(b) *In $F_\lambda^\times / F_\lambda^{\times 2}$ the subgroup $\langle [-1], [5] \rangle$ has order 4 and is the set of classes of units $x + y\sqrt{2}$ with y even. It contains the classes of π_7, of 3 and of every odd rational integer, and $[\pi_7] = [3] = [-5]$; it contains neither $[\varepsilon]$ nor $[\lambda]$.*

(c) *If $c \in \pm 5 F_\lambda^{\times 2}$, then over F_λ, $\operatorname{Im} \alpha_c = \operatorname{Im} \alpha'_c = \langle [-1], [5] \rangle$.*

Proof. (a) If $u \equiv w^2 \pmod{4\sqrt{2}}$ with w a unit, then $u/w^2 \equiv 1 \pmod{\lambda^5}$, and $X^2 - u/w^2$ has a root by Hensel's lemma, since $5 > 2v_\lambda(2) = 4$. The squares of units are $(x + y\sqrt{2})^2 = x^2 + 2y^2 + 2xy\sqrt{2}$, which is $\equiv 1$ (y even) or $3 + 2\sqrt{2}$ (y odd) modulo $(8, 4\sqrt{2})$; and the ideal $(4\sqrt{2})$ is $\{8n + 4n'\sqrt{2} : n, n' \in \mathbb{Z}_2\}$, so a residue modulo $4\sqrt{2}$ is the pair (x mod 8, y mod 4).

(b) The residues of $1, -1, 5, -5$ are $(1,0)$, $(7,0)$, $(5,0)$, $(3,0)$; multiplied by $3 + 2\sqrt{2}$ they give $(3,2)$, $(5,2)$, $(7,2)$, $(1,2)$. These eight residues are distinct, so the four classes are distinct, and together they are all units with x odd and y even. The residue of π_7 is $(1,2)$, that of $3(3 + 2\sqrt{2})$, so $[\pi_7] = [3] = [-5]$; an odd rational integer has $y = 0$; ε has $y = 1$; and λ has odd valuation.

(c) The isomorphisms $(x, y) \mapsto (u^2 x, u^3 y)$ of E_c onto E_{cu^2} and of E'_c onto E'_{cu^2} commute with ϕ and multiply abscissas by a square, and $E_{-c} = E_c$, $E'_{-c} = E'_c$; so the images depend only on the class of c in $F_\lambda^\times / \pm F_\lambda^{\times 2}$, and we may take $c = 5$. As $\mathcal{O}_\lambda \cong \mathbb{Z}_2^2$, $\chi(E_5(F_\lambda)) = 4$ in the notation of the proof of Lemma 2.3, so $|E_5(F_\lambda)/2E_5(F_\lambda)| = 16$ and $|\operatorname{Im} \alpha_5| \cdot |\operatorname{Im} \alpha'_5| = 16$ by Lemma 2.1. The image of α_5 contains $\{1, [-25], [5], [-5]\} = \langle [-1], [5] \rangle$, of order 4 by (b). On $E'_5 \colon y^2 = x^3 + 100x$ the point $(5, 25)$ gives $[5] \in \operatorname{Im} \alpha'_5$; and $X_1 = -6 - 4\sqrt{2} = -2\varepsilon^2$ gives $X_1^3 + 100X_1 = 16(-87 - 60\sqrt{2})$, where $-87 - 60\sqrt{2}$ has residue $(1,0)$ and is a square by (a); so there is a local point with abscissa X_1, and $[X_1] = [-2\varepsilon^2] = [-1] \in \operatorname{Im} \alpha'_5$, as $2 = \lambda^2$. So $|\operatorname{Im} \alpha'_5| \geq 4$, hence $|\operatorname{Im} \alpha_5| \leq 4$ and $\operatorname{Im} \alpha_5 = \langle [-1], [5] \rangle$; then $|\operatorname{Im} \alpha'_5| = 4$ and $\operatorname{Im} \alpha'_5 = \langle [-1], [5] \rangle$. □

Proposition 12.12. *Let $s \geq 0$ be even, let $q_1, \dots, q_s$ be distinct primes of I^-, and put $c_1 = \pi_7 q_1 \cdots q_s$. Then over F, $\operatorname{Im} \alpha'_{c_1} = \{1\}$, $\operatorname{Im} \alpha_{c_1} = \langle [-1], [c_1] \rangle$ and $\operatorname{rank} E_{c_1}(F) = 0$. The same holds for $\bar{c}_1 = \bar{\pi}_7 q_1 \cdots q_s$.*

Proof. Each (q_k) is a prime of F, as q_k is inert. The primes dividing $2c_1$ are (λ), (π_7) and the (q_k), the odd ones to the first power, and $v_\lambda(c_1) = 0$; so by Lemma 2.2 both images lie in $V = \langle -1, \varepsilon, \pi_7, q_1, \dots, q_s \rangle$.

At (λ), by Lemma 12.11(b), $[\pi_7] = [-5]$ and each $[q_k]$ is $[5]$ or $[-5]$ (as $q_k \equiv 5$ or $3 \pmod 8$), so $c_1 \in \pm 5^{s+1} F_\lambda^{\times 2} = \pm 5 F_\lambda^{\times 2}$, s being even. By Lemma 12.11(c) both local images at (λ) are $\langle [-1], [5] \rangle$, which on V says that the exponent of ε is 0, by Lemma 12.11(b). Write the remaining classes as $e = (-1)^h \pi_7^j \prod_k q_k^{l_k}$.

At $v = (q_k)$ the field F_v is unramified of degree two over $\mathbb{Q}_{q_k}$, with residue field $\mathbb{F}_{q_k^2}$. Every element of $\mathbb{F}_{q_k}$ is a square in $\mathbb{F}_{q_k^2}$, so -1 and every rational integer prime to q_k are squares in F_v; so is 2ι, as $8 \mid q_k^2 - 1$. The element π_7 is a unit at v, as $\mathrm{N}_{F/\mathbb{Q}}(\pi_7) = -7$, and it is not a square: a unit is a square exactly when its residue z satisfies $z^{(q_k^2-1)/2} = 1$, and $z^{(q_k^2-1)/2} = (z^{q_k+1})^{(q_k-1)/2} = \mathrm{N}(z)^{(q_k-1)/2}$, as the Frobenius of the inert prime acts as σ; so π_7 is a square exactly when $\left(\frac{-7}{q_k}\right) = 1$, and $\left(\frac{-7}{q_k}\right) = \left(\frac{q_k}{7}\right) = -1$ by quadratic reciprocity. Since $v(c_1) = 1$, Lemma 2.3 gives $\operatorname{Im} \alpha_{c_1,v} = \operatorname{Im} \alpha'_{c_1,v} = \langle [c_1] \rangle$; the unit part of c_1 at v is π_7 times a rational integer, a nonsquare.

For α_{c_1}: the unit part of e at (q_k) is $(-1)^h \pi_7^j$ times a rational number, a square exactly when $j = 0$. So $l_k = 0$ forces $j = 0$, and $l_k = 1$ forces e/c_1, whose unit part is $(-1)^h \pi_7^{j-1}$ times a rational number, to be a square, that is $j = 1$: the condition at (q_k) is $l_k = j$. (For $s = 0$ there is nothing to impose: the classes $(-1)^h \pi_7^j$ already form $\langle [-1], [c_1] \rangle$.) Hence $e = (-1)^h (\pi_7 q_1 \cdots q_s)^j = (-1)^h c_1^j$, and $\operatorname{Im} \alpha_{c_1} \subseteq \langle [-1], [c_1] \rangle$; equality holds since $\alpha_{c_1}(0,0) = [-1]$ and $\alpha_{c_1}(c_1, 0) = [c_1]$.

For α'_{c_1}: at a real place a point of $y^2 = x(x^2 + 4c_1^2)$ has $x \geq 0$, so e is totally positive. Now -1 is negative at both real places, π_7 is negative at $\sqrt{2} \mapsto -\sqrt{2}$ and positive at the other, and the q_k are positive; so $h = j = 0$ and $e = \prod_k q_k^{l_k}$. At (q_k) the unit part of e is rational, hence a square, so $l_k = 1$ would need e/c_1, whose unit part is π_7^{-1} times a rational number, to be a square, which it is not. So every $l_k = 0$, and $\operatorname{Im} \alpha'_{c_1} = \{1\}$. By Lemma 2.1, $2^{\operatorname{rank} E_{c_1}(F)} = 4 \cdot 1/4 = 1$.

For $\bar{c}_1$ apply σ, which carries E_{c_1} to $E_{\bar{c}_1}$ and $E_{c_1}(F)$ onto $E_{\bar{c}_1}(F)$. □

Proposition 12.13. *Let D be as in Theorem 1.2(b), $K = \mathbb{Q}(\sqrt{D})$ and $L = KF = F(\sqrt{D})$. Then $\operatorname{rank} E_{Da}(F) = 0$, $\sqrt{2} \notin K$ and $\sqrt{3} \notin K$, and (I1), (I2) and (I3) hold for K.*

Proof. Write $D = 7^k 3^j m$ with $k, j \in \{0, 1\}$ and m prime to 21, and put $c_1 = 3^{1-j} m \pi_7$. Since $a = 3\pi_7$ and $7\pi_7 = -\pi_7^2 \bar{\pi}_7$, we have $Da = (3^j)^2 c_1$ if $k = 0$, and $Da = -(3^j \pi_7)^2 \cdot 3^{1-j} m \bar{\pi}_7 = -(3^j \pi_7)^2 \bar{c}_1$ if $k = 1$. As $E_{cu^2} \cong E_c$ and $E_{-c} = E_c$, E_{Da} is isomorphic over F to E_{c_1} or to $E_{\bar{c}_1}$. The primes dividing c_1/π_7 are 3 (if $j = 0$) and those of m; they are distinct and lie in I^- ($3 \in I^-$), and with r the number of prime factors of D other than 7, there are $(1 - j) + (r - j) = r + 1 - 2j$ of them, an even number. So $\operatorname{rank} E_{Da}(F) = 0$ by Proposition 12.12.

As D is squarefree and odd and $D \neq 3$, K is a real quadratic field other than $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, and $D \notin F^{\times 2}$, as $F^{\times 2} \cap \mathbb{Q} = \mathbb{Q}^{\times 2} \cup 2\mathbb{Q}^{\times 2}$. So Lemma 12.1 with $M = F$, $B = a^2$ and $\delta = D$ gives $\operatorname{rank} E(L) = \operatorname{rank} E(F) + \operatorname{rank} E_{Da}(F) = 1 + 0$, by Proposition 2.13; this is (I1). Lemma 2.12 gives (I2), and Lemma 2.7 gives (I3), as L/F is Galois. □

For $D = 5$ and $D = 13$ one may take the tube prime $q = 19$, respectively $q = 43$, in the proof of Theorem 1.1: both are congruent to 7 modulo 12 and split in K, as $(\frac{5}{19}) = (\frac{19}{5}) = (\frac{4}{5}) = 1$ and $(\frac{13}{43}) = (\frac{43}{13}) = (\frac{4}{13}) = 1$, so a prime of K above q is unramified of residue degree one (Lemma 3.1).

Proposition 12.14. *Let $K = \mathbb{Q}(\sqrt{3})$ and $L = KF = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then* $\operatorname{rank} E_{3a}(F) = 0$, *$\sqrt{2} \notin K$, and (I1), (I2) and (I3) hold for K.*

Proof. The proof of Proposition 12.13 applies to $D = 3$, which is squarefree with $D \equiv 3 \pmod 8$ and $3 \in I^-$: there $k = 0$, $j = 1$, $m = 1$, $c_1 = \pi_7$ and $3a = 3^2 c_1$, and the number of primes dividing c_1/π_7 is $r + 1 - 2j = 0$, so Proposition 12.12 applies with $s = 0$. In its second paragraph, $K = \mathbb{Q}(\sqrt{3})$ is a real quadratic field other than $\mathbb{Q}(\sqrt{2})$, and $3 \notin F^{\times 2}$ as before; the rest applies as written. □

For $K = \mathbb{Q}(\sqrt{3})$ one may take the tube datum at two primes $q = 11$, $q' = 23$ (Definition 10.1), with any primes $\mathfrak{q} \mid 11$ and $\mathfrak{q}' \mid 23$ of K: both primes are 11 modulo 12 and split in K, as $3 \equiv 5^2 \pmod{11}$ and $3 \equiv 7^2 \pmod{23}$; $23 \nmid 6 \cdot 11 \cdot 124$; and $g_{11}(1) = 2^{-6} \cdot 3^2 \cdot 5^3 \cdot 11^{-2} \cdot 13 \cdot 19 \cdot 31^{-4} \cdot 53 \cdot 443$ is a 23-adic unit with $3g_{11}(1) \equiv 7 \pmod{23}$, which, like -1, is not a square modulo 23. Sun proves that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}(\sqrt{3})$, with 25 unknowns, using the curve $y^2 = x^3 - (15 + 6\sqrt{2})^2 x$ over $\mathbb{Q}(\sqrt{2})$ and a tube at the primes 347 and 359 built on another map, whose second prime acts through ramification [60, Theorem 1.3, (14.1), (14.5) and (14.8)]; Proposition 12.14 and Theorem 1.1 give another proof, with the second index curve and the tube of Definition 10.1 at the primes 11 and 23.

Remark 12.15. The second curve does not serve the fields K with $\sqrt{2} \notin K$ and $KF = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, namely $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{10})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ and $\mathbb{Q}(\sqrt{6}, \sqrt{10})$, nor those with $KF = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{13})$, namely $\mathbb{Q}(\sqrt{3}, \sqrt{13})$, $\mathbb{Q}(\sqrt{3}, \sqrt{26})$, $\mathbb{Q}(\sqrt{6}, \sqrt{13})$ and $\mathbb{Q}(\sqrt{6}, \sqrt{26})$: for them (I1) fails. Indeed $15a = 3^2 \cdot 5\pi_7$ and $39a = 3^2 \cdot 13\pi_7$, and the points

$$(23 - 17\sqrt{2},\ 168 - 105\sqrt{2}) \in E_{5\pi_7}(F),$$

$$\Big(\frac{4120503543 + 2435996511\sqrt{2}}{5183^2},\ -\frac{320982675468000 + 231018578548485\sqrt{2}}{5183^3}\Big) \in E_{13\pi_7}(F)$$

have infinite order: $(x, y) \mapsto (9x, 27y)$ followed by the map of Lemma 12.1 carries them to points Q of $E(F(\sqrt{15}))$, respectively $E(F(\sqrt{39}))$, with $y(Q) \neq 0$, and these groups have torsion $E[2]$ by Lemma 2.12. By Lemma 12.1, $\operatorname{rank} E(L) \geq \operatorname{rank} E(F(\sqrt{15})) = \operatorname{rank} E(F) + \operatorname{rank} E_{15a}(F) \geq 2$, respectively with $\sqrt{39}$ and $39a$.

Remark 12.16 (Odd D and the parity of the rank). In this paper the quadratic fields $\mathbb{Q}(\sqrt{D})$ with D odd come only from the second and third index curves, not from Sun's curve: from the second only with $D \equiv \pm 3 \pmod 8$, and from the third with $7 \mid D$ and $D \equiv \pm 1 \pmod 8$. Apart from the condition $D \equiv \pm 1 \pmod 8$ for the third curve, which the proof of Proposition 12.19 uses at (λ), the reason is the parity of the rank. Let F be a real quadratic field, $c \in F^\times$, D an odd integer with $\sqrt{D} \notin F$, and $L = F(\sqrt{D})$. The quadratic twist of E_c by D is E_{cD}, so the global root number of E_c over L is $w(E_c/F)\, w(E_{cD}/F)$ [11, Lemma 2.10]. Suppose that D is ± 1 times a square in F_v at every place v of F above 2. This holds when $D \equiv \pm 1 \pmod 8$, and for every odd D when $F = \mathbb{Q}(\sqrt{3})$, since every odd class of $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$ lies in $\pm \mathbb{Q}_2(\sqrt{3})^{\times 2}$. Then $w(E_{cD}/F) = w(E_c/F)$, by comparing local root numbers [11, Theorem 2.3]. Both are -1 at the real places. For $v \mid 2$, $E_{cD} \cong E_c$ over F_v, as $E_{-c} = E_c$ and $E_{ct^2} \cong E_c$. At an odd place v, E_c has good reduction if $v(c)$ is even, and type I_0^* with root number $(-1)^{(Nv-1)/2}$ if $v(c)$ is odd; so the two root numbers differ only

at the places where $v(D)$ is odd. These lie above the primes p with $v_p(D)$ odd, and above each such p the ratios multiply to $(\frac{-1}{p})^{n_p}$, where n_p is the number of places $v \mid p$ with odd ramification index and odd residue degree; n_p is even because $[F:\mathbb{Q}] = 2$. Hence E_c has root number $+1$ over L, and by the theorem of T. and V. Dokchitser [17, Corollary 1.6] its 2^∞-Selmer rank over L is even. So if $\operatorname{rank} E_c(L) = 1$, then the 2-primary part of the Tate–Shafarevich group of E_c over L is infinite, and no 2-descent can prove (I1): the bound it gives for $\operatorname{rank} E_c(L)$ also bounds the 2^∞-Selmer rank, so a bound 1 together with a point of infinite order would make that rank 1, which is odd. The second index curve lies over $\mathbb{Q}(\sqrt{2})$, where an odd D is ± 1 times a square at the prime above 2 only if $D \equiv \pm 1 \pmod 8$; for $D \equiv \pm 3 \pmod 8$ the parity is not forced.

The third and fourth index curves are not of the form E_c. Let E be one of them, over F, let D be an odd squarefree integer with $D \equiv \pm 1 \pmod 8$ and $\sqrt{D} \notin F$, and let $L = F(\sqrt{D})$; the twist of E by D is $E^{(D)}\colon y^2 = x^3 - D^2Ax$. The root number of E over L is $w(E/F)\, w(E^{(D)}/F)$ [11, Lemma 2.10], and we compare local root numbers [11, Theorem 2.3(i), (ii), (viii)]. At the real places both are -1. For $v \mid 2$, D^2 is a fourth power in F_v, as $\pm D \in \mathbb{Q}_2^{\times 2}$, so $E^{(D)} \cong E$ over F_v. At an odd place v, with residue field k and uniformiser ϖ, the curve $y^2 = x^3 - A'x$ is isomorphic to the one with $A'\varpi^4$ for A', and by Tate's algorithm it has type I_0, III, I_0^* or III*, with root number 1, $(\frac{-2}{k})$, $(\frac{-1}{k})$ or $(\frac{-2}{k})$, as $v(A')$ is congruent to 0, 1, 2 or 3 modulo 4. Since $v(D^2A) = v(A) + 2v(D)$, the root numbers of E and $E^{(D)}$ at v agree where $v(D)$ is 0 or 2, the latter above the odd primes ramified in F; where $v(D) = 1$ they agree if $v(A)$ is odd and differ by $(\frac{-1}{k})$ if $v(A)$ is even.

Above a prime $p \mid D$ inert in F, $k = \mathbb{F}_{p^2}$ and $(\frac{-1}{k}) = 1$; above a prime $p \mid D$ split in F there are two places, each with $k = \mathbb{F}_p$. Hence the root number of E over L is the product of $(\frac{-1}{p})$ over the primes $p \mid D$ split in F such that $v(A)$ is odd at exactly one of the two places above p. For the third curve the only odd place at which $v(A)$ is odd is (π_7), above the split prime 7, and $(\frac{-1}{7}) = -1$. So the root number of E over L is -1 if $7 \mid D$, and parity does not obstruct (I1); it is $+1$ if $7 \nmid D$. For the fourth the only such place is $\mathfrak{l}$, above the split prime $89 \equiv 1 \pmod 4$, so the root number is $+1$ for every such D.

When the root number of E over L is $+1$, the theorem of T. and V. Dokchitser on curves with a rational 2-isogeny [17, Theorem 1.8], applied to E over L and the isogeny with kernel $\{O, (0,0)\}$, makes the 2^∞-Selmer rank of E over L even, hence at least 2, as it is at least $\operatorname{rank} E(L) \geq \operatorname{rank} E(F) = 1$ (Propositions 2.16 and 2.17). The bound that a 2-isogeny descent or a 2^n-descent gives for $\operatorname{rank} E(L)$ also bounds that Selmer rank, so no such descent can prove (I1). Thus, among odd $D \equiv \pm 1 \pmod 8$ with $\sqrt{D} \notin F$, that is, $D \neq 1$, and $D \neq 17$ for the fourth curve, these descents can prove (I1) over $L = F(\sqrt{D})$ for the third curve only when $7 \mid D$, and for the fourth curve never.

12.6. **Real quadratic fields for the third curve.** In this subsection E is the third index curve, over $F = \mathbb{Q}(\sqrt{2})$, with the notation of Sections 2.6, 2.7 and 12.5: $A = \pi_7 = 1 + 2\sqrt{2}$, $\bar{A} = \bar{\pi}_7$, $\varepsilon = 1 + \sqrt{2}$, $\lambda = \sqrt{2}$, $\mathfrak{p}_7 = (\pi_7)$, $F_\lambda = \mathbb{Q}_2(\sqrt{2})$ and the set of primes I^-. Put $\bar{\mathfrak{p}}_7 = (\bar{\pi}_7)$, so that $F_{\bar{\mathfrak{p}}_7} = \mathbb{Q}_7$ with $\sqrt{2} \mapsto -3 \equiv 4$. For a positive squarefree integer D the quadratic twist of E by D is $E^{(D)}\colon y^2 = x^3 - D^2Ax$, and α', α are the maps of Section 2.7 for $E^{(D)}$, that is, with D^2A for A; so $\alpha'(0,0) = [D^2A] = [A]$ and $\alpha(0,0) = [-A]$.

The integers D of Theorem 1.2(c) are the products $D = 7q_1 \cdots q_r p_1 \cdots p_s$ with r even, $q_1, \ldots, q_r$ distinct primes of I^-, and $p_1, \ldots, p_s$ distinct primes $p \equiv 1 \pmod 8$ such that A is a nonsquare modulo both primes of F above p. The condition $D \equiv \pm 1 \pmod 8$ says that

r is even, as the primes of I^- are congruent to 3 or 5 modulo 8, so that $D \equiv -q_1 \cdots q_r \pmod 8$.

Lemma 12.17 (Odd places)**.** *Let v be a prime of F not above 2, let $b \in F_v^\times$, and let (X, Y) be a point of $y^2 = x^3 + bx$ over F_v with $X \neq 0$.*

(a) *If $v(b)$ is even, then $v(X)$ is even.*

(b) *If $v(b) = 3$, or if $v(b) = 2$ and $-b$ is not a square in F_v, then $[X] \in \{1, [b]\}$.*

Proof. Let $k = v(X)$. (a) If k were odd, then $2k \neq v(b)$, so $v(X^2 + b) = \min(2k, v(b))$ would be even and $v(Y^2) = k + v(X^2 + b)$ odd.

(b) As $v \nmid 2$, $1 + z$ is a square in F_v whenever $v(z) \geq 1$, by Hensel's lemma. If $2k < v(b)$, then $Y^2 = X^3(1+b/X^2)$ with $v(b/X^2) \geq 1$, so $[X] = 1$. If $2k > v(b)$, then $Y^2 = Xb(1+X^2/b)$ with $v(X^2/b) \geq 1$, so $[X] = [b]$. If $2k = v(b)$, then $v(b) = 2$ and $k = 1$; with π a uniformiser, $X = \pi u$ for a unit u, and $X^2+b = \pi^2(u^2+b/\pi^2)$, where u^2+b/π^2 is a unit, because $-b/\pi^2$ is a unit that is not a square, so its residue is not a square. Then $v(Y^2) = v(X)+v(X^2+b) = 3$, which is impossible. □

The image of α' over F_v consists of 1, the class $[4D^2A] = [A]$ of $(0, 0)$, and the classes $[X]$ of abscissas $X \neq 0$ of points of $y^2 = x^3 + bx$ with $b = 4D^2A$; the image of α likewise, with $b = -D^2A$ and $[-A]$.

Lemma 12.18 (Local images)**.** *Let D be a positive squarefree integer with $7 \mid D$, and consider α' and α over the completions F_v of F.*

(a) *At the real place with $\sqrt{2} \mapsto \sqrt{2}$, $\operatorname{Im}\alpha' = \{1\}$; at the real place with $\sqrt{2} \mapsto -\sqrt{2}$, $\operatorname{Im}\alpha = \{1\}$.*

(b) *At $\bar{\mathfrak{p}}_7$, $\operatorname{Im}\alpha' = \{1\}$; at $\mathfrak{p}_7$, $\operatorname{Im}\alpha' \subseteq \{1, [A]\}$.*

(c) *If $D \equiv \pm 1 \pmod 8$, then at (λ), $\operatorname{Im}\alpha = \{1, [5]\}$ and $\operatorname{Im}\alpha' = \langle [-1], [5], [\varepsilon]\rangle$, of order 8.*

(d) *Let $p \neq 7$ be a prime factor of D that lies in I^-, or satisfies $p \equiv 1 \pmod 8$ with A a nonsquare modulo both primes of F above p. At each prime v of F above p, $\operatorname{Im}\alpha \subseteq \{1, [-A]\}$ and $\operatorname{Im}\alpha' \subseteq \{1, [A]\}$, and $[A]$ and $[-A]$ are unit classes.*

(e) *At each prime v of F not dividing $14D$, every class in $\operatorname{Im}\alpha$ and in $\operatorname{Im}\alpha'$ has even valuation.*

Proof. Put $B = D^2A$.

(a) At the first real place $A = 1 + 2\sqrt{2} > 0$, so a point of $y^2 = x(x^2 + 4B)$ with $x \neq 0$ has $x > 0$, and $[A] = 1$. At the second $A = 1 - 2\sqrt{2} < 0$, so $-B > 0$, and the same holds for $y^2 = x(x^2 - B)$ and $[-A]$.

(b) At $\bar{\mathfrak{p}}_7$, $v(B) = 2$, as $v(D) = 1$ and $v(A) = 0$; the unit $A \equiv 1 + 2 \cdot 4 = 9 = 3^2 \pmod{\bar{\mathfrak{p}}_7}$ is a square in $\mathbb{Q}_7$, and -1 is not. So $-4B$ is not a square, and Lemma 12.17(b) with $b = 4B$ gives $\operatorname{Im}\alpha' \subseteq \{1, [4B]\} = \{1, [A]\} = \{1\}$. At $\mathfrak{p}_7$, $v(B) = 3$, and Lemma 12.17(b) gives $\operatorname{Im}\alpha' \subseteq \{1, [A]\}$.

(c) As D is odd and $D \equiv \pm 1 \pmod 8$, one of $\pm D$ is a square t^2 with $t \in \mathbb{Q}_2$, and $B = t^4A$. The maps $(x, y) \mapsto (t^2x, t^3y)$ of $y^2 = x^3 - Ax$ onto $y^2 = x^3 - Bx$ and of $y^2 = x^3 + 4Ax$ onto $y^2 = x^3 + 4Bx$ commute with the isogenies, multiply abscissas by a square and fix $(0, 0)$; so the images for $E^{(D)}$ are those for E. By Lemma 12.11(b), $[A] = [\pi_7] = [-5] \neq 1$ in $F_\lambda^\times/F_\lambda^{\times 2}$, so $(0, 0)$ is the only point of order two in $E(F_\lambda)$. As $\mathcal{O}_\lambda \cong \mathbb{Z}_2^2$, $\chi(E(F_\lambda)) = 4$ in the notation of the proof of Lemma 2.3, so $|E(F_\lambda)/2E(F_\lambda)| = 8$; and the exact sequence in the proof of Lemma 2.1, whose first term has order 2 here (Section 2.7), gives $|\operatorname{Im}\alpha| \cdot |\operatorname{Im}\alpha'| = 2 \cdot 8 = 16$. The image of α' contains $\alpha'(0, 0) = [-5]$; $\alpha'(Q') = [2\varepsilon] = [\varepsilon]$ for the point

$Q' = (2+2\sqrt{2},\, 8+4\sqrt{2})$ of $y^2 = x^3 + 4Ax$ over F (Proposition 2.16); and $[-4] = [-1]$, since $X = -4$ gives $X^3+4AX = -16(4+A) = 16(-5-2\sqrt{2})$, and $-5-2\sqrt{2}$ has residue $(3,2)$ and is a square by Lemma 12.11(a). These three classes are independent by Lemma 12.11(b), so $|\operatorname{Im}\alpha'| \geq 8$ and $|\operatorname{Im}\alpha| \leq 2$. As $\operatorname{Im}\alpha$ contains $\alpha(0,0) = [-A] = [5] \neq 1$, we get $\operatorname{Im}\alpha = \{1,[5]\}$ and $\operatorname{Im}\alpha' = \langle[-1],[5],[\varepsilon]\rangle$.

(d) The prime p is odd, unramified in F and different from 7, so $v(D) = 1$, $v(A) = 0$, as $\mathrm{N}_{F/\mathbb{Q}}(A) = -7$, and $v(B) = 2$. In F_v, -1 is a square and A is not. If $p \in I^-$, then p is inert, and the residue field of F_v is $\mathbb{F}_{p^2}$, in which every element of $\mathbb{F}_p$ is a square; a unit u of F_v is a square exactly when $\mathrm{N}_{F_v/\mathbb{Q}_p}(u)$ is a square modulo p, since its residue z satisfies $z^{(p^2-1)/2} = (z^{p+1})^{(p-1)/2}$, and z^{p+1} is the residue of that norm; and $\mathrm{N}_{F_v/\mathbb{Q}_p}(A) = \mathrm{N}_{F/\mathbb{Q}}(A) = -7$, with $(\frac{-7}{p}) = (\frac{p}{7}) = -1$. If $p \equiv 1 \pmod 8$, then $F_v = \mathbb{Q}_p$, -1 is a square as $p \equiv 1 \pmod 4$, and A is not, by hypothesis. Hence neither B nor $-4B$ is a square in F_v, and Lemma 12.17(b), with $b = -B$ and with $b = 4B$, gives $\operatorname{Im}\alpha \subseteq \{1,[-B]\} = \{1,[-A]\}$ and $\operatorname{Im}\alpha' \subseteq \{1,[4B]\} = \{1,[A]\}$; these are unit classes, as $v(A) = 0$.

(e) Here $v(B) = 0$, so Lemma 12.17(a) applies with $b = 4B$ and with $b = -B$, and the classes $[A]$, $[-A]$ of $(0,0)$ are units at v. □

Proposition 12.19. *Let D be a positive squarefree integer with $7 \mid D$ and $D \equiv \pm 1 \pmod 8$, each of whose prime factors $p \neq 7$ lies in I^-, or satisfies $p \equiv 1 \pmod 8$ with A a nonsquare modulo both primes of F above p. Let $K = \mathbb{Q}(\sqrt{D})$ and $L = KF = F(\sqrt{D})$. Then over F, $\operatorname{Im}\alpha' = \{1,[A]\}$ and $\operatorname{Im}\alpha = \{1,[-A]\}$, and $\operatorname{rank} E^{(D)}(F) = 0$; $\sqrt{2} \notin K$, and (I1), (I2) and (I3) hold for K.*

Proof. By Lemma 12.18(d),(e), every class in $\operatorname{Im}\alpha$ and in $\operatorname{Im}\alpha'$ has even valuation at every prime of F not dividing 14. As $\mathcal{O}_F$ is a principal ideal domain with units $\pm\varepsilon^{\mathbb{Z}}$, both images lie in $V = \langle -1, \varepsilon, \lambda, \pi_7, \bar{\pi}_7\rangle$. Write $e \in V$ as $e = (-1)^h\varepsilon^i\lambda^l\pi_7^j\bar{\pi}_7^k$ with exponents in $\{0,1\}$. At the real place with $\sqrt{2} \mapsto \sqrt{2}$, -1 and $\bar{\pi}_7$ are negative and ε, λ, π_7 are positive; at the other, $\bar{\pi}_7$ is positive and the other four are negative. At $\bar{\mathfrak{p}}_7$ the residues of -1, ε, λ, π_7 are 6, 5, 4, 2, and at $\mathfrak{p}_7$ those of -1, ε, λ, $\bar{\pi}_7$ are 6, 4, 3, 2; the nonzero squares modulo 7 are 1, 2, 4. At (λ), λ has odd valuation, and $[\pi_7] = [\bar{\pi}_7] = [-5]$ by Lemma 12.11(b), as $\pi_7\bar{\pi}_7 = -7$ is a square in $\mathbb{Q}_2$.

For α': by Lemma 12.18(a), e is positive at the place $\sqrt{2} \mapsto \sqrt{2}$, so $h + k = 0$; by Lemma 12.18(b), e is a square at $\bar{\mathfrak{p}}_7$, so $k = 0$ and $h + i = 0$, and $e \in \{1,[\pi_7]\}$ at $\mathfrak{p}_7$, so e/π_7^j is a square there and $h + l = 0$. Hence $h = i = l = k = 0$, and $\operatorname{Im}\alpha' \subseteq \{1,[A]\}$.

For α: by Lemma 12.18(c), e lies in $\{1,[5]\}$ at (λ), so $l = 0$ and $[(-1)^{h+j+k}5^{j+k}\varepsilon^i] \in \{1,[5]\}$, which gives $i = 0$ and $h + j + k = 0$, as $[-1]$, $[5]$, $[\varepsilon]$ are independent (Lemma 12.11(b)); and by Lemma 12.18(a), e is positive at the place $\sqrt{2} \mapsto -\sqrt{2}$, so $h + i + l + j = 0$. Hence $h = j$ and $k = 0$, and $\operatorname{Im}\alpha \subseteq \{1,[-A]\}$.

Equality holds in both, since $\alpha'(0,0) = [A]$ and $\alpha(0,0) = [-A]$ are nontrivial, as $\mathrm{N}_{F/\mathbb{Q}}(\pm A) = -7$. As $D^2A \notin F^{\times 2}$, Section 2.7 gives $2^{\operatorname{rank} E^{(D)}(F)} = 2 \cdot 2/4 = 1$.

As D is odd and squarefree, K is a real quadratic field other than $\mathbb{Q}(\sqrt{2})$, and $D \notin F^{\times 2}$. So Lemma 12.1 with $M = F$, $B = A$ and $\delta = D$ gives $\operatorname{rank} E(L) = \operatorname{rank} E(F) + \operatorname{rank} E^{(D)}(F) = 1$, by Proposition 2.16. This is (I1). Lemma 2.15 gives (I2), and Lemma 2.7 gives (I3), as L/F is Galois. □

Proposition 12.20. *Let D be one of the following 77 integers, each squarefree, divisible by 7 and congruent to ± 1 modulo 8, and none as in Proposition 12.19:* 119, 217, 287, 329, 609,

623, 721, 777, 959, 1015, 1169, 1295, 1393, 1407, 1785, 1799, 2191, 2247, 2289, 2345, 2639, 2681, 3031, 3143, 3255, 3353, 3367, 3689, 3745, 3759, 3815, 3857, 4151, 4207, 4431, 4529, 4711, 4921, 4935, 5033, 5089, 5327, 5593, 5873, 6097, 6209, 6265, 6503, 6671, 6839, 6881, 7161, 7273, 7343, 7385, 7511, 7665, 7903, 8057, 8169, 8351, 8463, 8617, 8687, 8897, 8911, 8953, 9247, 9303, 9737, 9919, 10031, 10185, 10199, 10311, 10423, 10479. *Let* $K = \mathbb{Q}(\sqrt{D})$ *and* $L = KF$. *Then* $\operatorname{rank} E^{(D)}(F) = 0$; $\sqrt{2} \notin K$, *and* (I1), (I2) *and* (I3) *hold for* K.

Proof. For each D, a 2-isogeny descent over F as in Section 2.7, with D^2A for A: we find that the Selmer groups are $\{1, [A]\}$ and $\{1, [-A]\}$, the images of $(0, 0)$; so $\operatorname{rank} E^{(D)}(F) = 0$. The last paragraph of the proof of Proposition 12.19 then applies as written, since it uses only that D is odd, squarefree and divisible by 7. □

12.7. **Biquadratic fields.** In this subsection E is the fourth index curve, $F = \mathbb{Q}(\sqrt{17})$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{17})$.

Proposition 12.21. *The quadratic twists* $E^{(D)} \colon y^2 = x^3 - D^2Ax$, $D = 2, 3, 6$, *have rank* 0 *over* F. *Each of* $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{51})$, $\mathbb{Q}(\sqrt{3}, \sqrt{34})$ *and* $\mathbb{Q}(\sqrt{6}, \sqrt{34})$ *has* $\sqrt{17} \notin K$ *and* $KF = L$, *and* (I1), (I2) *and* (I3) *hold for it.*

Proof. For each D, a 2-isogeny descent over F as in Section 2.7, with D^2A for A: we find that the Selmer groups are $\{1, [A]\}$ and $\{1, [-A]\}$, the images of $(0, 0)$; so $\operatorname{rank} E^{(D)}(F) = 0$. Lemma 12.1, applied to $L/F(\sqrt{2})$ with $\delta = 3$ and then to $F(\sqrt{2})/F$ with $\delta = 2$, for E and for $E^{(3)}$, whose twist by 2 is $E^{(6)}$, gives $\operatorname{rank} E(L) = \operatorname{rank} E(F) + \sum_D \operatorname{rank} E^{(D)}(F) = 1$, by Proposition 2.17. This is (I1). Lemma 2.15 gives (I2), and Lemma 2.7 gives (I3), as L/F is Galois. These conditions concern $E(L)$ and $E(F)$ only, so they hold for each of the four fields. Each K is generated by square roots of two integers whose classes, with 17, span the classes of 2, 3 and 17 in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, so $KF = L$; and 17 is not in the span of the two, so $\sqrt{17} \notin K$ by Kummer theory. □

12.8. **Fields with the same L.** In this subsection E is the first index curve and $F = \mathbb{Q}(\sqrt{3})$, except in Lemma 12.22, which concerns any index curve, and in Proposition 12.23(b) and (c), which concern the second and the third. Let ζ be a primitive 32nd root of unity. By the proof of Lemma 12.8, $\vartheta = \zeta + \zeta^{-1}$ is a root of g_{32}, with $K_{32} = \mathbb{Q}(\vartheta)$, and $\theta = \vartheta^2 - 2 = \zeta^2 + \zeta^{-2}$ is a root of $g = g_{16}$, with $K_{16} = \mathbb{Q}(\theta)$. As in Lemma 12.8(iii), $\sqrt{2} = \theta^2 - 2$, $\alpha = 2 + \theta = \vartheta^2$, $L_{16} = L_1(\theta)$ and $L_{32} = L_{16}(\vartheta)$. We take these roots in Proposition 12.7, which is allowed, since Proposition 12.7 and its proof hold for every root of g_{16} and of g_{32}.

Lemma 12.22. *Let* E *be an index curve, over* $F = \mathbb{Q}(\sqrt{d})$, *and let* K *and* K' *be totally real number fields with* $\sqrt{d} \notin K$, $\sqrt{d} \notin K'$ *and* $K'F = KF$. *Then* (I1), (I2) *and* (I3) *hold for* K' *if and only if they hold for* K. *In particular, if they hold for* K, *then Theorem 1.1 applies to* K'.

Proof. With $L = KF = K'F$, each of the three conditions is a statement about the groups $E(L)$ and $E(F)$ only, so it is the same statement for K and for K'. The hypotheses of Theorem 1.1 on K' are that it is totally real, that $\sqrt{d} \notin K'$, and (I1)–(I3). □

If $K/\mathbb{Q}$ is Galois with cyclic Galois group, and K' is as in Lemma 12.22, then K' is a subfield of the abelian field $L = KF$ with $[L : K'] = 2$ and $F \not\subseteq K'$, so it is the fixed field of a subgroup of order 2 of $\operatorname{Gal}(L/\mathbb{Q}) = \operatorname{Gal}(K/\mathbb{Q}) \times \operatorname{Gal}(F/\mathbb{Q})$ not contained in $\operatorname{Gal}(K/\mathbb{Q}) \times 1$. These subgroups are generated by $(1, \rho)$, which gives K, and, when $[K : \mathbb{Q}]$ is even, by (γ_0, ρ), where ρ generates $\operatorname{Gal}(F/\mathbb{Q})$ and γ_0 is the element of order two of $\operatorname{Gal}(K/\mathbb{Q})$. For

the fields of Theorem 1.2 this pairs $\mathbb{Q}(\sqrt{2m})$ with $\mathbb{Q}(\sqrt{6m})$ and leaves the cyclic cubic fields and $\mathbb{Q}(\zeta_{11})^+$ alone; it pairs K_{16} and K_{32} with the fields K'_{16} and K'_{32} below, and $\mathbb{Q}(\sqrt{D})$ with $\mathbb{Q}(\sqrt{2D})$, and $\mathbb{Q}(\sqrt{3})$ with $\mathbb{Q}(\sqrt{6})$, a field of (a), for the second curve; and $\mathbb{Q}(\sqrt{D})$ with $\mathbb{Q}(\sqrt{2D})$ for the third, where $D = 7$ gives $\mathbb{Q}(\sqrt{7})$ and $\mathbb{Q}(\sqrt{14})$, the second also a field of (a), with $m = 7$.

Proposition 12.23. (a) *Let $v = \sqrt{3}\,\theta \in L_{16}$ and $w = \sqrt{3}\,\vartheta \in L_{32}$, so that $v^2 = 3(2+\sqrt{2})$ and $w^2 = 3(2+\theta)$, and let $K'_{16} = \mathbb{Q}(v)$ and $K'_{32} = \mathbb{Q}(w)$. Then v and w are roots of*

$$h_{16} = t^4 - 12t^2 + 18, \qquad h_{32} = t^8 - 24t^6 + 180t^4 - 432t^2 + 162.$$

The fields K'_{16} and K'_{32} are totally real and Galois over $\mathbb{Q}$, with cyclic Galois groups of orders 4 and 8; their only quadratic subfield is $\mathbb{Q}(\sqrt{2})$, so $\sqrt{3}$ lies in neither; and $K'_{16}F = L_{16}$, $K'_{32}F = L_{32}$. For the first index curve, conditions (I1), (I2) and (I3) hold for K'_{16} and for K'_{32}. The prime $q = 7$ splits completely in K'_{16} and the prime $q = 79$ in K'_{32}; both are congruent to 7 modulo 12, and $\mathfrak{q} = (7, v-1)$, respectively $\mathfrak{q} = (79, w-9)$, is a prime above q of residue degree one.

(b) *For the second index curve, let D be as in Theorem 1.2(b) and $K' = \mathbb{Q}(\sqrt{2D})$. Then $\sqrt{2} \notin K'$, $\sqrt{3} \notin K'$, and (I1), (I2) and (I3) hold for K'.*

(c) *For the third index curve, let D be as in Theorem 1.2(c) or one of the 77 integers of Proposition 12.20, and $K' = \mathbb{Q}(\sqrt{2D})$. Then $\sqrt{2} \notin K'$, and (I1), (I2) and (I3) hold for K'.*

Proof. (a) Since $v^2 = 3\theta^2 = 3(2+\sqrt{2})$, we have $(v^2-6)^2 = 18$, that is $h_{16}(v) = 0$. Since $w^2/3 - 2 = \vartheta^2 - 2 = \theta$ and $h_{32}(t) = 81\,g(t^2/3-2)$, we have $h_{32}(w) = 81\,g(\theta) = 0$. Both polynomials are Eisenstein at 2, so $[K'_{16} : \mathbb{Q}] = 4$ and $[K'_{32} : \mathbb{Q}] = 8$. The fields contain $\sqrt{2} = v^2/3 - 2$, respectively $\sqrt{2} = (w^2/3-2)^2 - 2$. As subfields of the totally real abelian fields L_{16} and L_{32}, they are totally real and Galois over $\mathbb{Q}$. The field $K'_{16}(\sqrt{3})$ contains $\theta = v/\sqrt{3}$, so $K'_{16}F \supseteq \mathbb{Q}(\theta, \sqrt{3}) = L_{16}$, with equality by degrees; then $[L_{16} : K'_{16}] = 2$, and $\sqrt{3} \notin K'_{16}$. Likewise $K'_{32}F$ contains $\vartheta = w/\sqrt{3}$, so $K'_{32}F = L_{32}$ and $\sqrt{3} \notin K'_{32}$.

Write $\mathrm{Gal}(L_{32}/\mathbb{Q}) = \langle\gamma\rangle \times \langle\rho\rangle$, where γ fixes $\sqrt{3}$ and has order 8, and ρ fixes K_{32} and maps $\sqrt{3}$ to $-\sqrt{3}$ (proof of Lemma 12.8). The restriction of γ^4 to K_{32} is the element of order two of $\mathrm{Gal}(K_{32}/\mathbb{Q})$, which fixes the subfield K_{16} of degree 4 and not ϑ; as $\vartheta^2 = \alpha \in K_{16}$, $\gamma^4(\vartheta) = -\vartheta$. Hence $\gamma^4\rho$ fixes w, K'_{32} is the fixed field of $\langle\gamma^4\rho\rangle$, and $\mathrm{Gal}(K'_{32}/\mathbb{Q})$ is generated by the image of γ, of order 8 because no γ^k with $0 < k < 8$ lies in $\langle\gamma^4\rho\rangle$. On L_{16} the same argument, with γ^2 and $\theta^2 = 2+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, shows that K'_{16} is the fixed field of the restriction of $\gamma^2\rho$, with cyclic Galois group of order 4. A cyclic group of order 4 or 8 has one subgroup of index 2, so $\mathbb{Q}(\sqrt{2})$ is the only quadratic subfield. Conditions (I1)–(I3) hold for K_{16} and K_{32} by Proposition 12.7, hence for K'_{16} and K'_{32} by Lemma 12.22.

The prime $79 \equiv 7 \pmod{12}$ is inert in F, and $79 \equiv 15 \pmod{32}$ has order 2 in $(\mathbb{Z}/32)^\times/\{\pm1\}$, so its Frobenius in $\mathrm{Gal}(L_{32}/\mathbb{Q})$ is $\gamma^4\rho$, which fixes K'_{32}; so 79 splits completely in K'_{32}. Likewise 7 is inert in F and has order 2 in $(\mathbb{Z}/16)^\times/\{\pm1\}$, so its Frobenius in $\mathrm{Gal}(L_{16}/\mathbb{Q})$ is the restriction of $\gamma^2\rho$, and 7 splits completely in K'_{16}. Concretely, $h_{16} \equiv (t^2-1)(t^2-4) \pmod 7$, and h_{32} has the roots 9, 19, 21, 22, 57, 58, 60, 70 modulo 79; as $\mathrm{disc}(h_{16}) = 2^{11}\cdot 3^6$ and $\mathrm{disc}(h_{32}) = 2^{31}\cdot 3^{28}$ are prime to 7 and 79, Dedekind's criterion makes $(7, v-1)$ and $(79, w-9)$ primes of degree one.

(b) The integer D is odd, squarefree and at least 5, so $2D$ is squarefree and different from 1, 2 and 3; as $\sqrt{n} \in K'$ for a squarefree integer n only if $n \in \{1, 2D\}$, neither $\sqrt{2}$ nor $\sqrt{3}$

lies in K'. Since $K'F = \mathbb{Q}(\sqrt{2}, \sqrt{D}) = \mathbb{Q}(\sqrt{D})F$, Proposition 12.13 and Lemma 12.22 give (I1)–(I3).

(c) The proof of (b) applies, with $D \geq 7$, and with Propositions 12.19 and 12.20 for Proposition 12.13. □

For the second curve and $D = 59$, 61 one may take the tube prime $q = 19$, respectively $q = 43$, for $\mathbb{Q}(\sqrt{2D})$: both are congruent to 7 modulo 12, and $118 \equiv 2^2 \pmod{19}$ and $122 \equiv 6^2 \pmod{43}$, so q splits in $\mathbb{Q}(\sqrt{2D})$. Some of the fields of Proposition 12.23(b) are already in Theorem 1.2(a). As $2D$ is squarefree, $\mathbb{Q}(\sqrt{2D}) = \mathbb{Q}(\sqrt{2m})$ only for $m = D$, and $\mathbb{Q}(\sqrt{2D}) = \mathbb{Q}(\sqrt{6m})$ only for $m = D/3$; so $\mathbb{Q}(\sqrt{2D})$ is one of the fields of Theorem 1.2(a) exactly when every prime factor $p \notin \{3, 13\}$ of D satisfies $p \equiv \pm 5 \pmod{12}$ and $\left(\frac{p}{13}\right) = -1$. This happens for the five least D, namely $D = 5$, 13, 19, 21 and 35, which give $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{26})$, $\mathbb{Q}(\sqrt{38})$, $\mathbb{Q}(\sqrt{42})$ and $\mathbb{Q}(\sqrt{70})$; of the 27 integers $D < 400$ of Theorem 1.2(b), 11 give a field of Theorem 1.2(a) and 16 do not, the three least of these being 59, 61 and 83. Infinitely many do not: a prime $D \equiv 59 \pmod{168}$ satisfies $D \equiv 3 \pmod{8}$ and $D \equiv 3 \pmod{56}$, so it is one of the integers of Theorem 1.2(b), and $D \equiv 11 \pmod{12}$, so $\mathbb{Q}(\sqrt{2D})$ is not one of the fields of Theorem 1.2(a); there are infinitely many such primes by Dirichlet's theorem.

Proof of Theorem 1.2 for the fields of Proposition 12.23. The fields K'_{16}, K'_{32} and $\mathbb{Q}(\sqrt{2D})$ are totally real, $\sqrt{3}$ does not lie in them, nor $\sqrt{2}$ in $\mathbb{Q}(\sqrt{2D})$, and (I1)–(I3) hold for the first index curve, respectively the second or the third; Theorem 1.1 then gives a Diophantine definition of $\mathbb{Z}$ in each of them with 25 unknowns. □

13. The cyclotomic $\mathbb{Z}_2$-extension

In this section E is the first index curve and $F = \mathbb{Q}(\sqrt{3})$, with the notation of Sections 2.2, 12.1 and 12.3: $\lambda = 1+\sqrt{3}$, $\varepsilon = 2+\sqrt{3}$, $a = 4+\sqrt{3}$, $\mathfrak{a} = (a)$, $F_\lambda = \mathbb{Q}_2(\sqrt{3})$, and the map ∂_k of Section 12.3 for $c = a$. We prove Theorem 1.3. For $k \leq 5$ it is contained in Propositions 2.6, 12.4, 12.7 and 12.23; the proof below uses these only for $k \leq 4$. For $k \geq 5$ we show that $\operatorname{rank} E(L_{2^k}) = \operatorname{rank} E(L_{2^{k-1}})$. Following Mazur and Rubin [40, §§6–8], the points of $E(L_{2^k})$ on which $\operatorname{Gal}(L_{2^k}/L_{2^{k-1}})$ acts by -1 are the F-points of an abelian variety over F with multiplication by $\mathbb{Z}[\zeta_{2^{k-2}}]$, and they are bounded by a Selmer group inside $H^1(F, E[2])$, cut out by local conditions at the places of F (Section 13.2). At the prime above 2 the local condition is controlled by norms of abscissas of points over a 2-adic field, which we compute by an elementary argument in the 2-adic tower (Section 13.3).

13.1. **The tower.** Fix roots of unity ξ_j ($j \geq 2$) with ξ_2 of order 12, $\xi_2 + \xi_2^{-1} = \sqrt{3}$ and $\xi_j^2 = \xi_{j-1}$, so that ξ_j has order $3 \cdot 2^j$, and put $\zeta_{2^j} = \xi_j^3$, of order 2^j, and

$$t_j = \xi_j + \xi_j^{-1}, \qquad \eta_j = \zeta_{2^j} + \zeta_{2^j}^{-1} = t_j^3 - 3t_j, \qquad \alpha_j = 2 + \eta_j.$$

Then $t_2 = \sqrt{3}$, $\eta_2 = 0$, $\eta_3^2 = 2$, $t_j^2 = t_{j-1} + 2$ and $\eta_j^2 = \eta_{j-1} + 2 = \alpha_{j-1}$ for $j \geq 3$. For $k \geq 2$ let $K_{2^k} = \mathbb{Q}(\eta_k) = \mathbb{Q}(\zeta_{2^k})^+$ and $L_{2^k} = K_{2^k}F$. Thus $K_4 = \mathbb{Q}$, $K_8 = \mathbb{Q}(\sqrt{2})$, $L_4 = F$, $L_8 = L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and K_{16}, L_{16}, K_{32}, L_{32} are the fields of Section 12.2.

Lemma 13.1. *Let $k \geq 3$.*

(a) *K_{2^k} is totally real and cyclic of degree 2^{k-2} over $\mathbb{Q}$, its only quadratic subfield is $\mathbb{Q}(\sqrt{2})$, and $\sqrt{3} \notin K_{2^k}$. The field L_{2^k} is $\mathbb{Q}(t_k) = \mathbb{Q}(\xi_k)^+$, of degree 2^{k-1}; restriction maps $\operatorname{Gal}(L_{2^k}/F)$ isomorphically onto $\operatorname{Gal}(K_{2^k}/\mathbb{Q})$, so L_{2^k}/F is cyclic and its only quadratic*

subextension is $L_1 = F(\sqrt{2})$*; and* $F \cap L_{2^k}^{\times 2} = F^{\times 2} \cup 2F^{\times 2}$*. Moreover* $L_{2^k} = L_{2^{k-1}}(\eta_k)$*, and the nontrivial element of* $\mathrm{Gal}(L_{2^k}/L_{2^{k-1}})$ *maps* η_k *to* $-\eta_k$*.*

(b) *The extension* L_{2^k}/F *is unramified at every finite prime not above* 2*, the prime* 2 *is totally ramified in* L_{2^k}*, and* $\mathfrak{a}$ *and* $\sigma\mathfrak{a}$ *are inert in* L_{2^k}/F*.*

(c) $E(L_{2^k})_{\mathrm{tors}} = E[2]$*.*

Proof. (a) The group $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) = (\mathbb{Z}/2^k)^\times$ is $\{\pm 1\} \times \langle 5\rangle$, with $\langle 5\rangle$ cyclic of order 2^{k-2}, so K_{2^k}, the fixed field of $\{\pm 1\}$, is totally real and cyclic of degree 2^{k-2}. So it has exactly one quadratic subfield; as $\eta_3 = \zeta_8 + \zeta_8^{-1}$ with $\zeta_8 = \zeta_{2^k}^{2^{k-3}}$ lies in K_{2^k} and $\eta_3^2 = 2$, that subfield is $\mathbb{Q}(\sqrt{2})$. Hence $\sqrt{3} \notin K_{2^k}$ and $[L_{2^k} : \mathbb{Q}] = 2^{k-1}$. As $\zeta_{2^k} = \xi_k^3$ and $\sqrt{3} = t_2 = \xi_k^{2^{k-2}} + \xi_k^{-2^{k-2}}$, the totally real field L_{2^k} lies in $\mathbb{Q}(\xi_k)^+ = \mathbb{Q}(t_k)$, of degree $\varphi(3 \cdot 2^k)/2 = 2^{k-1}$; so the two are equal. Since $K_{2^k} \cap F = \mathbb{Q}$, restriction maps $\mathrm{Gal}(L_{2^k}/F)$ isomorphically onto $\mathrm{Gal}(K_{2^k}/\mathbb{Q})$, so L_{2^k}/F is cyclic, with the single quadratic subextension $F(\eta_3) = L_1$, and by Kummer theory $F \cap L_{2^k}^{\times 2} = F^{\times 2} \cup 2F^{\times 2}$. Finally $L_{2^{k-1}}(\eta_k)$ contains K_{2^k} and F, so it is L_{2^k}; since $[L_{2^k} : L_{2^{k-1}}] = 2$ and $\eta_k^2 = \alpha_{k-1} \in L_{2^{k-1}}$, the conjugate of η_k is $-\eta_k$.

(b) We have $L_{2^k} \subseteq \mathbb{Q}(\xi_k)$, and $\mathrm{Gal}(\mathbb{Q}(\xi_k)/\mathbb{Q}) = (\mathbb{Z}/3)^\times \times (\mathbb{Z}/2^k)^\times$, in which the inertia groups are $1 \times (\mathbb{Z}/2^k)^\times$ above 2, $(\mathbb{Z}/3)^\times \times 1$ above 3, and trivial above every other prime. So the ramification index of L_{2^k} over $\mathbb{Q}$ is at most 2 above 3, where F is already ramified, and L_{2^k}/F is unramified at the finite primes not above 2. The inertia group above 2 does not contain complex conjugation $(-1,-1)$, so it maps injectively to $\mathrm{Gal}(L_{2^k}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\xi_k)/\mathbb{Q})/\langle(-1,-1)\rangle$, onto a subgroup of order $2^{k-1} = [L_{2^k} : \mathbb{Q}]$; so 2 is totally ramified. The prime 13 splits in F, so the Frobenius of $\mathfrak{a}$, and that of $\sigma\mathfrak{a}$, in $\mathrm{Gal}(L_{2^k}/F) \cong \mathrm{Gal}(K_{2^k}/\mathbb{Q}) = (\mathbb{Z}/2^k)^\times/\{\pm 1\}$ is the class of 13; as $13 \equiv 5 \pmod 8$, it has order 2^{k-2}, and $\mathfrak{a}$ and $\sigma\mathfrak{a}$ are inert.

(c) Let $L = L_{2^k}$. By (a), $F \cap L^{\times 2} = F^{\times 2} \cup 2F^{\times 2}$, whose elements have square norms, so $E(L)$ has no point of order four and none of order three by Lemma 2.4(a). If $E(L)[\ell] \neq 0$ for a prime $\ell \geq 5$, then by Lemma 2.5 the field $L(i)$, which lies in $\mathbb{Q}(\xi_k)$, contains a root of unity of order ℓ. This is false, since the roots of unity in $\mathbb{Q}(\xi_k)$ have order dividing $3 \cdot 2^k$. Hence $E(L)_{\mathrm{tors}} = E[2]$. □

13.2. **A Selmer group over F.** For a field $k \supseteq F$ of characteristic 0 let $\delta_k \colon E(k)/2E(k) \to H^1(k, E[2])$ be the Kummer map, let e_2 be the Weil pairing on $E[2]$ [56, §III.8], and let $\iota \colon E[2] \to \mu_2 \times \mu_2$ be $T \mapsto (e_2(T,(0,0)), e_2(T,(a,0)))$. It is an isomorphism of Galois modules, as e_2 is nondegenerate and $(0,0)$ and $(a,0)$ lie in $E(F)$ and generate $E[2]$. With Kummer theory it identifies $H^1(k, E[2])$ with $(k^\times/k^{\times 2})^2$, compatibly with restriction to extensions of k; we use this identification from now on.

Lemma 13.2. *For every field* $k \supseteq F$ *of characteristic* 0*, the Kummer map* δ_k *is the map* ∂_k *of Section 12.3 for* $c = a$*, that is* $(x,y) \mapsto (x, x-a)$ *for* $x \neq 0, a$*.*

Proof. For $T = (0,0)$ and $T = (a,0)$ let $f_T = x$, respectively $x - a$, so that $\mathrm{div}(f_T) = 2(T) - 2(O)$, and let

$$g_{(0,0)} = \frac{x^2 + a^2}{2y}, \qquad g_{(a,0)} = \frac{x^2 - 2ax - a^2}{2y};$$

the duplication formula gives $g_T^2 = f_T \circ [2]$, and $g_T \in F(E)$. By the definition of the Weil pairing [56, §III.8], $e_2(S,T) = g_T(X+S)/g_T(X)$ for $S \in E[2]$ and any X at which both values are defined and nonzero. Let $P \in E(k)$ with $P \notin \{O, T\}$, and $Q \in E(\bar{k})$ with $2Q = P$;

then g_T is defined and nonzero at Q and at σQ for $\sigma \in \mathrm{Gal}(\bar{k}/k)$, as its zeros and poles lie in $[2]^{-1}\{O, T\}$, and

$$e_2(\sigma Q - Q, T) = \frac{g_T(\sigma Q)}{g_T(Q)} = \frac{\sigma(g_T(Q))}{g_T(Q)}, \qquad g_T(Q)^2 = f_T(P).$$

So the coordinate of $\iota_* \delta_k(P)$ belonging to T is the class of $f_T(P)$. This gives $\delta_k = \partial_k$ at every point except at $(0,0)$ in the first coordinate and at $(a,0)$ in the second. There we use that δ_k is a homomorphism: $(0,0) = (a,0) + (-a,0)$ and $(a,0) = (0,0) + (-a,0)$ give the values $a \cdot (-a) = -a^2$ and $(-a)(-2a) = 2a^2$, which are those of ∂_k. In particular ∂_k is a homomorphism with kernel $2E(k)$. □

This is the computation behind [56, Proposition X.1.4]. Now let $k \geq 4$, $L = L_{2^k}$ and $L' = L_{2^{k-1}}$. Let $G = \mathrm{Gal}(L/F)$, cyclic of order $N = 2^{k-2} \geq 4$ (Lemma 13.1); fix a generator γ, and let $\tau = \gamma^{N/2}$, which generates $\mathrm{Gal}(L/L')$. Let χ be the quadratic character of G, which cuts out $L_1 = F(\sqrt{2})$; its class in $F^\times/F^{\times 2}$ is [2].

We use the twist of E by L/F of Mazur and Rubin [40, §§6–8], with their $A = E$, $K = F$ and $\ell = 2$; their λ is the prime $2\mathbb{Z}$ of $\mathbb{Q}$, so their $A[\lambda]$ is $E[2]$. Their standing assumptions [40, §5] hold: E is simple, and the centre of $\mathrm{End}_F(E)$ is $\mathbb{Z}$, as the endomorphisms of E over $\overline{F}$ form $\mathbb{Z}[i]$ and $[i]$ is not defined over F; so 2 does not divide its discriminant. Following [40, Definitions 6.1 and 6.2], let

$$I = \ker(\mathbb{Z}[G] \to \mathbb{Z}[G/\langle\tau\rangle]) = (1-\tau)\mathbb{Z}[G], \qquad \mathcal{O} = \mathbb{Z}[G]/(1+\tau),$$

so that $1+\tau$ is the element denoted $N_{L/L'}$ there. Then $\mathcal{O} \cong \mathbb{Z}[\zeta_N]$ by $\gamma \mapsto \zeta_N$; with $\bar{\gamma}$ the image of γ and $\varpi = 1 - \bar{\gamma}$, the ideal $\varpi\mathcal{O}$ is the prime of $\mathcal{O}$ above 2 and $2\mathcal{O} = \varpi^{N/2}\mathcal{O}$. The group I is free over $\mathbb{Z}$ with basis $\gamma^j(1-\tau)$, $0 \leq j < N/2$, and it is an $\mathcal{O}$-module, isomorphic to $\mathcal{O}$ by $s(1-\tau) \mapsto \bar{s}$. Let $u = (2/\varpi)(1-\tau) \in I$, so $\varpi u = 2(1-\tau)$; its image $\bar{u}$ in $I/2I \cong \mathcal{O}/\varpi^{N/2}$ spans the line $(I/2I)[\varpi]$, and $\gamma\bar{u} = \bar{u}$, as $(\gamma - 1)u = -2(1-\tau) \in 2I$.

The twist is $A = \ker(\mathrm{Res}^L_F E \to \mathrm{Res}^{L'}_F E)$, their A_L [40, Definition 6.1], an abelian variety over F on which $\mathcal{O}$ acts [40, Proposition 6.3(i)]. For an F-algebra D, $A(D)$ is the kernel of the trace $E(D \otimes_F L) \to E(D \otimes_F L')$, $R \mapsto R + \tau R$; in particular $A(F) = \{R \in E(L) : \tau R = -R\}$. By [40, Corollary 6.4] the isomorphism $A[2] \cong I \otimes E[2] = (I/2I) \otimes E[2]$ of [40, Proposition 6.3(iii)] induces an isomorphism of Galois modules $A[\varpi] \cong E[2]$. It maps $\bar{u} \otimes T$ to T: by its proof, it sends an element of $((I/2I) \otimes E[2])[\bar{\gamma} - 1]$ to its image $\sum_{g \in G} g \otimes T'$ in $\mathbb{F}_2[G] \otimes E[2]$, and then to T'; and the image of $\bar{u}$ in $\mathbb{F}_2[G]$ is nonzero (the cokernel $\mathbb{Z}[G/\langle\tau\rangle]$ of $I \to \mathbb{Z}[G]$ is free over $\mathbb{Z}$) and fixed by G, so it is $\sum_{g \in G} g$. Let $\mathrm{Sel}(L/F, E[2]) \subseteq H^1(F, E[2])$ be the Selmer group of [40, Definition 8.1], defined by the local conditions $\mathcal{H}_v \subseteq H^1(F_v, E[2])$ at all places v of F, where L_v is the completion of L at a place above v and $\mathcal{H}_v$ is the group $H_\lambda(L_v/F_v)$ of [40, Definition 7.1]: the image of the Kummer map of the twist of E by L_v/F_v, followed by the isomorphism of [40, Corollary 6.4].

Lemma 13.3. *Let r be the rank of the finitely generated $\mathcal{O}$-module $A(F)$. Then*

$$\mathrm{rank}\, E(L) = \mathrm{rank}\, E(L') + \tfrac{N}{2} r, \qquad r \leq \dim_{\mathbb{F}_2} \mathrm{Sel}(L/F, E[2]) - 2.$$

Proof. For $Q \in E(L)$, $2Q = (Q + \tau Q) + (Q - \tau Q)$ with $Q + \tau Q \in E(L')$ and $Q - \tau Q \in A(F)$, and $E(L') \cap A(F) \subseteq E[2]$; so $\mathrm{rank}\, E(L) = \mathrm{rank}\, E(L') + \mathrm{rank}_{\mathbb{Z}} A(F)$. Over the Dedekind domain $\mathcal{O}$, $A(F)$ is the direct sum of a projective module of rank r, of $\mathbb{Z}$-rank $r \cdot \mathrm{rank}_{\mathbb{Z}} \mathcal{O} = rN/2$, and the finite module $A(F)_{\mathrm{tors}}$. Then $\dim_{\mathbb{F}_2} A(F)/\varpi A(F) = r + \dim A(F)_{\mathrm{tors}}/\varpi A(F)_{\mathrm{tors}}$, and $\dim A(F)_{\mathrm{tors}}/\varpi A(F)_{\mathrm{tors}} = \dim A(F)_{\mathrm{tors}}[\varpi]$, as both count the cyclic summands of the ϖ-primary part of $A(F)_{\mathrm{tors}}$. Here $A(F)_{\mathrm{tors}}[\varpi] = A[\varpi](F)$, the

ϖ-torsion of the twist, which is $E[2]$ ([40, Corollary 6.4]) and has dimension 2. The Kummer map of the isogeny ϖ embeds $A(F)/\varpi A(F)$ in $H^1(F, A[\varpi]) = H^1(F, E[2])$, with image in the classical ϖ-Selmer group of A, which is $\mathrm{Sel}(L/F, E[2])$ by [40, Lemma 8.4], as in the proof of [40, Proposition 8.8]. So $r + 2 \le \dim \mathrm{Sel}(L/F, E[2])$. □

Lemma 13.4. *Let $\mathfrak{w}$ be the prime of L above 2, $L_\mathfrak{w}$ the completion, and $L'_\mathfrak{w} \subseteq L_\mathfrak{w}$ the closure of L'.*

(i) *If v is a finite prime of F other than (λ) and $\mathfrak{a}$, then $\mathcal{H}_v$ consists of the pairs of classes of even valuation.*

(ii) *If v is real, then $\mathcal{H}_v = \{(1,1), (-1,-1)\}$.*

(iii) *$\mathcal{H}_\mathfrak{a} = \langle [2] \rangle^2$, the pairs of classes of units of $F_\mathfrak{a}$.*

(iv) *The restriction to $H^1(L_\mathfrak{w}, E[2]) = (L_\mathfrak{w}^\times / L_\mathfrak{w}^{\times 2})^2$ of every element of $\mathcal{H}_{(\lambda)}$ is $(1,1)$ or $(\mathrm{N}(x(R)), \mathrm{N}(x(R) - a))$ for a point $R \in E(L_\mathfrak{w}) \setminus E[2]$ with $\tau R = -R$, where $x(R) \in L'_\mathfrak{w}$ and $\mathrm{N} = \mathrm{N}_{L'_\mathfrak{w}/F_\lambda}$.*

Proof. (i) The model (1.1) has discriminant $64a^6$, and a is a unit at $\sigma\mathfrak{a}$ (as $a + \bar{a} = 8$), so E has good reduction at v, and L_v/F_v is unramified by Lemma 13.1(b). By [40, Lemma 7.3(ii)], $\mathcal{H}_v$ is the unramified subgroup of $H^1(F_v, E[2]) = (F_v^\times / F_v^{\times 2})^2$, which consists of the pairs of classes of even valuation.

(ii) As L is totally real, $L_v = F_v = \mathbb{R}$, and $\mathcal{H}_v$ is the image of $E(\mathbb{R})/2E(\mathbb{R})$ under $\delta_\mathbb{R} = \partial_\mathbb{R}$ [40, Definition 7.1], Lemma 13.2. By Lemma 12.9(ii) it is $\{(1,1), (-1,-a)\}$, and $a > 0$ at both real places.

For (iii) and (iv) let $v = \mathfrak{a}$ or $v = (\lambda)$. By Lemma 13.1(b) the decomposition group of v is all of G, so L_v/F_v is cyclic with group G, and the objects I, $\mathcal{O}$, ϖ, u of the local twist A_v of [40, §§6–7] for L_v/F_v are those above. Let Ω be an algebraic closure of F_v. By [40, Proposition 6.3(ii)], with Ω as the Galois extension (as in the proof of [40, Proposition 6.3(iii)]), $A_v(\Omega) \cong I \otimes E(\Omega)$, where $\mathcal{O}$ acts on I and $\sigma \in \mathrm{Gal}(\Omega/F_v)$ acts as $\bar{\sigma}^{-1} \otimes \sigma$, $\bar{\sigma}$ being the image of σ in G. Let $T \in E[2]$; then $\bar{u} \otimes T \in A_v[\varpi](F_v)$. Put $\tilde{u} = (2/\varpi^2)(1 - \tau) \in I$ (here $N \ge 4$ is used), so $\varpi\tilde{u} = u$, and $S = \tilde{u} \otimes T$, so $\varpi S = \bar{u} \otimes T$. If $\bar{\sigma} = \gamma^j$, then $\bar{\gamma}^{-j} - 1 \equiv j\varpi \pmod{\varpi^2}$ in $\mathcal{O}$, so $\sigma S - S = (\gamma^{-j} - 1)\tilde{u} \otimes T = j\,\bar{u} \otimes T$, as $\varpi^2 \tilde{u} = 2(1 - \tau) \in 2I$. Hence the Kummer class of $\bar{u} \otimes T$ is $\sigma \mapsto \chi(\sigma)T$, that is, $([2]^{t_1}, [2]^{t_2})$ with (t_1, t_2) the exponents of $\iota(T)$. So $\mathcal{H}_v$ contains $\langle [2] \rangle^2$.

(iii) At $\mathfrak{a}$ the residue characteristic is 13, so $\dim \mathcal{H}_\mathfrak{a} = \dim E(F_\mathfrak{a})[2] = 2$ by [40, Lemma 7.2(i)]. Since 2 is not a square modulo 13, $\langle [2] \rangle^2$ has dimension 2, so it is $\mathcal{H}_\mathfrak{a}$; and $[2]$ is the nontrivial class of units of $F_\mathfrak{a} = \mathbb{Q}_{13}$.

(iv) Here $L_v = L_\mathfrak{w}$. As $\mathrm{Gal}(\Omega/L_\mathfrak{w})$ acts trivially on I, which is free over $\mathbb{Z}$, $A_v(L_\mathfrak{w}) = I \otimes E(L_\mathfrak{w})$ and $A_v(F_\lambda) = (I \otimes E(L_\mathfrak{w}))^G$, with γ acting as $\gamma^{-1} \otimes \gamma$. Write an element of $I \otimes E(L_\mathfrak{w})$ as $\sum_{j < N/2} \gamma^j (1 - \tau) \otimes R_j$. Since $\gamma^{-1}(1 - \tau) = -\gamma^{N/2-1}(1 - \tau)$, it is invariant exactly when $R_j = \gamma R_{j+1}$ for $j < N/2 - 1$ and $R_{N/2-1} = -\gamma R_0$, that is, when $R_j = \gamma^{-j} R_0$ and $\tau R_0 = -R_0$. Next, for $s \in \mathbb{Z}[G]$ and $P \in E(L_\mathfrak{w})$ choose $Q \in E(\Omega)$ with $2Q = P$. Then $s(1 - \tau) \otimes P = \varpi(su \otimes Q)$, and for $\sigma \in \mathrm{Gal}(\Omega/L_\mathfrak{w})$, $\sigma(su \otimes Q) - su \otimes Q = su \otimes (\sigma Q - Q) = \mathrm{aug}(s)\,\bar{u} \otimes (\sigma Q - Q)$, where $\mathrm{aug}(s)$ is the sum of the coefficients of s, because $\gamma\bar{u} = \bar{u}$. So the Kummer class over $L_\mathfrak{w}$ of $s(1 - \tau) \otimes P$ is $\mathrm{aug}(s)\,\delta_{L_\mathfrak{w}}(P)$, and the restriction to $L_\mathfrak{w}$ of the Kummer class of the invariant element above is

$$\sum_{j < N/2} \delta_{L_\mathfrak{w}}(\gamma^{-j} R_0) = \delta_{L_\mathfrak{w}}\Big(\sum_{j < N/2} \gamma^{-j} R_0 \Big).$$

If $R_0 \in E[2]$ this is $\delta_{L_\mathfrak{w}}((N/2)R_0) = 0$. Otherwise $x(R_0)$ is fixed by τ, so lies in $L'_\mathfrak{w}$, no $\gamma^{-j}R_0$ lies in $E[2]$, and by Lemma 13.2 the class is $\prod_{j<N/2}(\gamma^{-j}x(R_0), \gamma^{-j}x(R_0) - a) = (\mathrm{N}(x(R_0)), \mathrm{N}(x(R_0) - a))$, since the γ^{-j} with $0 \le j < N/2$ restrict to the elements of $\mathrm{Gal}(L'_\mathfrak{w}/F_\lambda)$. □

Proposition 13.5. *Let $k \ge 4$, with L, L', $\mathfrak{w}$, $L_\mathfrak{w}$ and $L'_\mathfrak{w}$ as above, and suppose that $\mathrm{N}_{L'_\mathfrak{w}/F_\lambda}(x(R)) \in F_\lambda^{\times 2} \cup 2F_\lambda^{\times 2}$ for every $R \in E(L_\mathfrak{w}) \setminus E[2]$ with $\tau R = -R$. Then $\mathrm{Sel}(L/F, E[2]) \subseteq \langle[\varepsilon]\rangle^2$ and $\operatorname{rank} E(L) = \operatorname{rank} E(L')$.*

Proof. Let $(d_1, d_2) \in \mathrm{Sel}(L/F, E[2])$. By Lemma 13.4(i),(iii), d_1 and d_2 have even valuation at every finite prime other than (λ), so they lie in $\langle -1, \varepsilon, \lambda\rangle$, as $\mathcal{O}_F$ is a principal ideal domain with units $\pm\varepsilon^{\mathbb{Z}}$ (Section 2.2). The signs of -1, ε, λ at the two real places are $(-,-)$, $(+,+)$, $(+,-)$, so Lemma 13.4(ii) gives $d_1 d_2 \in \langle\varepsilon\rangle$. By Lemma 13.4(iv) and the hypothesis, d_1 is a square in $L_\mathfrak{w}$, because 2 is (as $\sqrt{2} \in L_1 \subseteq L$). The extension $L_\mathfrak{w}/F_\lambda$ is cyclic with group G, so its only quadratic subextension is $F_\lambda(\sqrt{2})$, and by Kummer theory $d_1 \in F_\lambda^{\times 2} \cup 2F_\lambda^{\times 2}$. The classes of -1, ε, λ are independent in $F_\lambda^\times/F_\lambda^{\times 2}$ (see after (12.1), and λ has odd valuation), and $[2] = [\varepsilon]$; so $d_1 \in \langle\varepsilon\rangle$, and then $d_2 \in \langle\varepsilon\rangle$. Hence $\mathrm{Sel}(L/F, E[2]) \subseteq \langle[\varepsilon]\rangle^2$, and Lemma 13.3 gives $r = 0$ and $\operatorname{rank} E(L) = \operatorname{rank} E(L')$. □

13.3. **The prime above 2.** Fix an embedding of the union of the fields L_{2^j} in an algebraic closure of F_λ that extends $F \subseteq F_\lambda$. For $j \ge 2$ let Λ_j be the closure of L_{2^j}, so $\Lambda_2 = F_\lambda$, and Λ_j is the completion of L_{2^j} at its prime above 2 (Lemma 13.1(b)); let v_j be its normalised valuation, $\mathfrak{m}_j$ its maximal ideal, $U_n(\Lambda_j) = 1 + \mathfrak{m}_j^n$, and $\pi_j = t_j - 1$.

Lemma 13.6. *Let $j \ge 2$.*

(a) *$\Lambda_j = F_\lambda(t_j)$, π_j is a uniformiser of Λ_j, the residue field is $\mathbb{F}_2$, and $v_j(2) = 2^{j-1}$. If $j \ge 3$, then Λ_j/Λ_{j-1} is totally ramified of degree 2, its nontrivial automorphism maps t_j to $-t_j$ and η_j to $-\eta_j$, and $\mathcal{O}_{\Lambda_j} = \mathcal{O}_{\Lambda_{j-1}} + \mathcal{O}_{\Lambda_{j-1}}\pi_j$.*

(b) *$\alpha_j = \pi_j^2(\pi_j + 3)$.*

(c) *$\mathrm{N}_{\Lambda_j/F_\lambda}(\alpha_j) = 2$ if $j \ge 3$.*

(d) *Every unit b of F_λ satisfies $v_j(b-1) \ge 2^{j-2}$.*

Proof. (a) For $j = 2$, $\pi_2 = \sqrt{3} - 1$ is a root of the Eisenstein polynomial $X^2 + 2X - 2$. Let $j \ge 3$ and assume the statement for $j-1$. The element $(t_j - 1)(t_j + 1) = t_j^2 - 1 = \pi_{j-1} + 2$ of Λ_{j-1} has valuation 1, as $v_{j-1}(2) \ge 2$. If t_j, which is integral, lay in Λ_{j-1}, its two factors, which differ by 2, would both be units or both lie in $\mathfrak{m}_{j-1}$, and their valuations could not add up to 1. So $\Lambda_j = \Lambda_{j-1}(t_j)$ has degree 2, with conjugation $t_j \mapsto -t_j$, under which $\eta_j = t_j(t_j^2 - 3) \mapsto -\eta_j$. The norm of π_j to Λ_{j-1} is $1 - t_j^2 = -(\pi_{j-1} + 2)$, of valuation 1; so the extension is totally ramified, π_j is a uniformiser, $v_j(2) = 2v_{j-1}(2)$, and $\mathcal{O}_{\Lambda_j} = \mathcal{O}_{\Lambda_{j-1}}[\pi_j]$.

(b) $t^3 - 3t + 2 = (t-1)^2(t+2)$.

(c) Put $\beta_i = 2 - \eta_i$. For $i \ge 3$ the conjugation of Λ_i/Λ_{i-1} maps η_i to $-\eta_i$, so the norms of α_i and of β_i to Λ_{i-1} are both $4 - \eta_i^2 = 2 - \eta_{i-1} = \beta_{i-1}$. Hence $\mathrm{N}_{\Lambda_j/F_\lambda}(\alpha_j) = \beta_2 = 2 - \eta_2 = 2$.

(d) The residue field of F_λ is $\mathbb{F}_2$, so $v_2(b-1) \ge 1$, and $v_j = 2^{j-2}v_2$ on F_λ by (a). □

For $b = 4 \pm \sqrt{3}$, $b - 1 = \sqrt{3}(\sqrt{3} \pm 1)$ has valuation exactly 1 in F_λ; Proposition 13.8 below needs only (d).

Lemma 13.7. *For every $j \ge 3$, $\mathrm{N}_{\Lambda_j/F_\lambda}(U_6(\Lambda_j)) \subseteq F_\lambda^{\times 2}$.*

Proof. Let $i \geq 3$, $n \geq 1$ and $z \in \Lambda_i$ with $v_i(z) \geq n$. Write $z = z_0 + z_1\pi_i$ with $z_0, z_1 \in \Lambda_{i-1}$ (Lemma 13.6(a)). The two terms have valuations of different parity, so $v_{i-1}(z_0) \geq n/2$ and $v_{i-1}(z_1) \geq (n-1)/2$. As the trace of π_i is -2, $\mathrm{Tr}(z) = 2(z_0 - z_1)$ has valuation at least $2^{i-2} + \lceil (n-1)/2 \rceil$, and $\mathrm{N}(z)$ has valuation $v_i(z) \geq n$. Since $\mathrm{N}(1+z) = 1 + \mathrm{Tr}(z) + \mathrm{N}(z)$,

$$\mathrm{N}_{\Lambda_i/\Lambda_{i-1}}(U_n(\Lambda_i)) \subseteq U_s(\Lambda_{i-1}), \qquad s = \min(n,\, 2^{i-2} + \lceil (n-1)/2 \rceil).$$

For $n = 6$ this is $s = 6$ if $i \geq 4$ and $s = 5$ if $i = 3$. So $\mathrm{N}_{\Lambda_j/F_\lambda}(U_6(\Lambda_j)) \subseteq U_5(F_\lambda)$, and a unit $\equiv 1$ modulo λ^5 is a square in F_λ by Hensel's lemma, as in Section 12.1. □

Proposition 13.8. *Let $k \geq 5$, let b be a unit of F_λ, and put $\Lambda = \Lambda_{k-1}$, $\alpha = \alpha_{k-1}$ and $\mathrm{N} = \mathrm{N}_{\Lambda/F_\lambda}$. If $x, y \in \Lambda$, $y \neq 0$, and $\alpha y^2 = x(x-b)(x+b)$, then $\mathrm{N}(x) \in F_\lambda^{\times 2} \cup 2F_\lambda^{\times 2}$. More precisely, $\mathrm{N}(x) \in 2F_\lambda^{\times 2}$ if $v(x) \neq 0$ or $v(x/b - 1) = 1$, and $\mathrm{N}(x) \in F_\lambda^{\times 2}$ otherwise, where $v = v_{k-1}$.*

Proof. Let $e = v(2) = 2^{k-2} \geq 8$, $\pi = \pi_{k-1}$, and $U_n = U_n(\Lambda)$. The set $F_\lambda^{\times 2} \cup 2F_\lambda^{\times 2}$ is a group, and it contains $\mathrm{N}(\alpha) = 2$ (Lemma 13.6(c)), $\mathrm{N}(-1) = 1$, $\mathrm{N}(\pm b) = b^{2^{k-3}}$, $\mathrm{N}(\Lambda^{\times 2})$ and $\mathrm{N}(U_6)$ (Lemma 13.7). We show that x is a product of such elements. Here $x \neq 0, \pm b$, since $y \neq 0$.

Case $v(x) < 0$. Put $\nu = b/x$, so $v(\nu) = -v(x) \geq 1$ and $\alpha y^2 = x^3(1-\nu)(1+\nu)$. Then $x = \alpha s^2 u$ with $s = y/(x(1+\nu))$ and $u = (1+\nu)/(1-\nu) = 1 + 2\nu/(1-\nu) \in U_{e+1} \subseteq U_6$; so $\mathrm{N}(x) \in 2F_\lambda^{\times 2}$.

Case $v(x) > 0$. Put $\nu = x/b$, so $v(\nu) \geq 1$ and $\alpha y^2 = -b^2 x(1-\nu)(1+\nu)$. Then $x = -\alpha s^2 u$ with $s = y/(b(1+\nu))$ and $u = (1+\nu)/(1-\nu) \in U_{e+1} \subseteq U_6$; so $\mathrm{N}(x) \in 2F_\lambda^{\times 2}$.

Case $v(x) = 0$. As the residue field is $\mathbb{F}_2$, $x/b = 1 + \delta$ with $h = v(\delta) \geq 1$, and $\alpha y^2 = b^3(1+\delta)\,\delta\,(\delta+2)$.

If $h < e$, then $\delta + 2 = \delta u_1$ with $u_1 = 1 + 2/\delta \in U_{e-h}$, and $x = \alpha\big(y/(b\delta u_1)\big)^2 u_1$. We claim that $h = 1$ or $h = e-1$. Suppose $2 \leq h \leq e-2$. By Lemma 13.6(b), $\pi + 3 = b^3(1+\delta)u_1 s^2$ with $s = \delta/(\pi y)$. Here b, $1+\delta$ and u_1 lie in U_2 (Lemma 13.6(d), as $k - 1 \geq 3$), so s is a unit; then $s = 1 + s_1\pi$ with s_1 integral, and $s^2 = 1 + 2s_1\pi + s_1^2\pi^2 \in U_2$. So $\pi + 3 \in U_2$; but $\pi + 3 = 1 + \pi + 2$ with $v(\pi + 2) = 1$, a contradiction. If $h = 1$, then $u_1 \in U_{e-1} \subseteq U_6$ and $\mathrm{N}(x) \in 2F_\lambda^{\times 2}$. If $h = e-1$, then $x = b(1+\delta)$ with $1 + \delta \in U_{e-1} \subseteq U_6$, and $\mathrm{N}(x) \in F_\lambda^{\times 2}$.

If $h > e$, then $x = b(1+\delta)$ with $1 + \delta \in U_{e+1} \subseteq U_6$, and $\mathrm{N}(x) \in F_\lambda^{\times 2}$.

If $h = e$, then $\delta = 2r$ with $r \equiv 1$ modulo $\mathfrak{m}_{k-1}$, so $v(\delta + 2) \geq e + 1$, and $x = -b\big(1 - (\delta+2)\big)$ with $1 - (\delta + 2) \in U_6$; so $\mathrm{N}(x) \in F_\lambda^{\times 2}$. □

Remark 13.9. The proof needs $k \geq 5$, that is $e \geq 8$, only in the cases $h = 1$ and $h = e - 1$, where the unit lies only in U_{e-1} and Lemma 13.7 needs U_6. For $k = 4$ ($e = 4$) the other cases still go through: as $v(\alpha) = 2$, the equation forces the valuations of x, of δ when $h > e$, and of $\delta + 2$ when $h = e$, to be even, which puts the units of the proof in $U_{e+2} = U_6$; and $h = 2$ is excluded as above. The cases $v(x) = 0$, $h \in \{1, 3\}$ are left open, and the case $k = 4$ of Theorem 1.3 is Proposition 12.7. Proposition 13.8 is a statement at the prime above 2 for every unit b of F_λ; what is special to E is global, the local conditions of Lemma 13.4 away from 2 and the space $\langle -1, \varepsilon, \lambda \rangle$ in the proof of Proposition 13.5.

Proof of Theorem 1.3. Condition (I2). For $k = 2$ this is Proposition 2.6, and for $k \geq 3$ Lemma 13.1(c).

Condition (I1). For $k = 2, 3, 4$ this is Propositions 2.6, 12.4 and 12.7. Let $k \geq 5$, $L = L_{2^k}$ and $L' = L_{2^{k-1}}$, and let $R \in E(L_\mathfrak{w}) \setminus E[2]$ with $\tau R = -R$. By Lemma 13.1(a) and Lemma 13.6(a), $L_\mathfrak{w} = \Lambda_k = \Lambda_{k-1}(\eta_k)$ and $L'_\mathfrak{w} = \Lambda_{k-1}$, with $\tau(\eta_k) = -\eta_k$ and $\eta_k^2 = \alpha_{k-1}$. Write $R = (x, z)$; then $\tau x = x$ and $\tau z = -z$, so $x \in \Lambda_{k-1}$ and $z = y\eta_k$ with $y \in \Lambda_{k-1}$, $y \neq 0$,

and $\alpha_{k-1}y^2 = x(x-a)(x+a)$. By Proposition 13.8 with $b = a$, $\mathrm{N}_{L'_{\mathfrak{w}}/F_\lambda}(x) \in F_\lambda^{\times 2} \cup 2F_\lambda^{\times 2}$. So Proposition 13.5 gives $\operatorname{rank} E(L_{2^k}) = \operatorname{rank} E(L_{2^{k-1}})$, and by induction $\operatorname{rank} E(L_{2^k}) = 1$.

Condition (I3). $K_{2^k}/\mathbb{Q}$ is Galois, so Lemma 2.7 applies.

The fields. K_{2^k} is totally real, and $\sqrt{3} \notin K_{2^k}$ (Lemma 13.1(a); $K_4 = \mathbb{Q}$), so Theorem 1.1 applies. Let $k \geq 3$. Write $\mathrm{Gal}(L_{2^k}/\mathbb{Q}) = \langle\gamma\rangle \times \langle\rho\rangle$, where γ fixes $\sqrt{3}$ and restricts to a generator of $\mathrm{Gal}(K_{2^k}/\mathbb{Q})$, and ρ fixes K_{2^k} and maps $\sqrt{3}$ to $-\sqrt{3}$; and let $\tau = \gamma^{2^{k-3}}$, the element of order two of $\langle\gamma\rangle$. By Lemma 13.1(a), $\tau\rho$ fixes $\sqrt{3}\,\eta_k$. The fixed field of $\tau\rho$ is totally real as a subfield of L_{2^k}, of degree 2^{k-2}. It contains $\mathbb{Q}(\sqrt{3}\,\eta_k)$, and $\mathbb{Q}(\sqrt{3}\,\eta_k)F$ contains η_k, hence L_{2^k}; so the fixed field of $\tau\rho$ is $\mathbb{Q}(\sqrt{3}\,\eta_k) = K'_{2^k}$, the field of Theorem 1.3, and $K'_{2^k}F = L_{2^k}$. As $\tau\rho(\sqrt{3}) = -\sqrt{3}$, $\sqrt{3} \notin K'_{2^k}$. No power $\gamma^m \neq 1$ lies in $\langle\tau\rho\rangle$, so the image of γ generates $\mathrm{Gal}(K'_{2^k}/\mathbb{Q})$, which is cyclic. By Lemma 12.22, (I1)–(I3) hold for K'_{2^k}, and Theorem 1.1 applies. For $k = 3$, $\sqrt{3}\,\eta_3 = \pm\sqrt{6}$; for $k = 4, 5$, with $\zeta = \zeta_{32}$ in Section 12.8, $\eta_4 = \theta$ and $\eta_5 = \vartheta$, so $\sqrt{3}\,\eta_4$ and $\sqrt{3}\,\eta_5$ are the elements v and w of Proposition 12.23. □

Appendix A. Proof of Proposition 3.5

We keep the notation of Section 3.3. For $v \in S_2$ let $(-1)_v \in \hat{U}_2$ be -1 at v and 1 at the other dyadic primes.

Lemma A.1. *Let F_v be a finite extension of $\mathbb{Q}_p$ or $F_v = \mathbb{R}$, and λ a character of $F_v^\times$. Then λ is the square of a character if and only if $\lambda(-1) = 1$. Consequently the image of λ under the boundary map $H^1(G_{F_v}, \mu_\infty) \to H^2(G_{F_v}, \mu_2) = \mathrm{Br}(F_v)[2]$ of $1 \to \mu_2 \to \mu_\infty \xrightarrow{2} \mu_\infty \to 1$ has invariant $\frac{1}{2}$ if and only if $\lambda(-1) = -1$.*

Proof. If $\lambda = \psi^2$ then $\lambda(-1) = \psi(1) = 1$. Conversely, for F_v non-archimedean write $F_v^\times = \varpi^{\mathbb{Z}} \times \mu(F_v) \times V$ with $V \cong \mathbb{Z}_p^{[F_v:\mathbb{Q}_p]}$; take any square root of $\lambda(\varpi)$; on V the group of finite-order characters is divisible; on the cyclic group $\mu(F_v)$ of even order the squares of characters are the characters trivial on its element of order 2, which is -1. For $F_v = \mathbb{R}$, a finite-order character is trivial or the sign, and the sign is not a square. The image of λ vanishes exactly when λ is a square, and $\mathrm{Br}(F_v)[2]$ has order 2. □

Lemma A.2. *Let ς be a normalised 2-cocycle on G_K with values in $\{\pm 1\}$, $s_v = (-1)^{2\,\mathrm{inv}_v[\varsigma]}$, and λ a character of G_K of order m with $\lambda_v(-1) = s_v$ at every place v. Then there is a continuous $\vartheta\colon G_K \to \mu_{2m}$ with $\vartheta^2 = \lambda$, $\delta\vartheta = \varsigma$ and $\vartheta(1) = 1$.*

Proof. By Lemma A.1 the boundary of λ and $[\varsigma]$ have the same local invariants, so they are equal, $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$ being injective [43, (8.1.17)]. Choose b with $b^2 = \lambda$, constant on the cosets of $\ker\lambda$, with $b(1) = 1$; then δb takes values in μ_2 and represents the boundary of λ, so $\delta b = \varsigma \cdot \delta c$ for a continuous $c\colon G_K \to \mu_2$, and $\vartheta = bc^{-1}$ works; $\vartheta(1) = \delta\vartheta(1,1) = \varsigma(1,1) = 1$. □

Lemma A.3. *Let ς be normalised and inflated from $\mathrm{Gal}(K_0/K)$, and $\delta\vartheta = \varsigma$. For $g \in G_K$ and $h \in G_{K_0}$, $\vartheta(gh) = \vartheta(g)\vartheta(h) = \vartheta(hg)$. Hence $\vartheta|_{G_{K_0}}$ is a homomorphism invariant under conjugation by G_K, and the fixed field of its kernel is Galois over K.*

Proof. $\varsigma(g,h) = \varsigma(\bar{g},1) = 1$ and $\varsigma(h,g) = \varsigma(1,\bar{g}) = 1$ in $\mathrm{Gal}(K_0/K)$, which gives the two equalities; then $\vartheta(ghg^{-1}) = \vartheta(h)$ from $gh = (ghg^{-1})g$. □

Lemma A.4. *In Lemma A.3, let $v \notin T_0$ be a finite prime at which $\lambda = \vartheta^2$ is unramified, and $I_v \subset D_v$ inertia and decomposition groups at v. Then $I_v \subset G_{K_0}$, $\vartheta|_{I_v}$ is a homomorphism of order at most 2, and it is the restriction of a character of D_v; if v is odd and $\vartheta|_{I_v} \neq 1$, this character corresponds on $\mathcal{O}_v^\times$ to the Legendre symbol.*

Proof. K_0 is unramified at v. The restriction of ς to D_v is inflated from $D_v/I_v \cong \hat{\mathbb{Z}}$, and $H^2(\hat{\mathbb{Z}}, \mu_2) = 0$, so $\varsigma|_{D_v} = \delta c_v$ with c_v inflated from D_v/I_v and normalised; ϑc_v^{-1} is a character of D_v that agrees with ϑ on I_v. On $\mathcal{O}_v^\times$ (v odd) the only nontrivial quadratic character is the Legendre symbol, since $U_v^{(1)}$ is pro-p with p odd. □

Lemma A.5. *Let $H \subseteq \hat{U}_2$ be a closed subgroup such that the torsion subgroup of $\hat{U}_2/H$ has exponent dividing 2^t. Every character of H with values in μ_{2^r} extends to a character θ of $\hat{U}_2$ with values in $\mu_{2^{r+t}}$, and θ is trivial on $U_v^{(e_v(r+t+1)+1)}$ for every $v \in S_2$.*

Proof. Let θ' be any extension (Pontryagin duality). Then θ'^{2^r} is a character of $\hat{U}_2/H \cong \mathbb{Z}_2^\rho \times F$ with F finite of exponent dividing 2^t; write $\theta'^{2^r} = \lambda_1\lambda_2$ with λ_1 trivial on F and λ_2 trivial on $\mathbb{Z}_2^\rho$, and $\lambda_1 = \mu^{2^r}$ (the characters of $\mathbb{Z}_2^\rho$ form a divisible group). Then $\theta = \theta'\mu^{-1}$ extends the given character and $\theta^{2^{r+t}} = \lambda_2^{2^t} = 1$. For $i > e_v$, squaring maps $U_v^{(i)}$ onto $U_v^{(i+e_v)}$ (if $v(x) = i > e_v$ then $(1+x)^2 = 1 + 2x(1+x/2)$, and successive approximation), so the 2^{r+t}-th powers of $U_v^{(e_v+1)}$ are $U_v^{(e_v(r+t+1)+1)}$, on which θ is trivial. □

Lemma A.6. *Let k be a field of characteristic 0 with $i \notin k$, $k_\infty = k(\mu_{2^\infty})$, and $u \in k^\times$. If $u \in k_\infty^{\times 4}$ then $u \in \pm k^{\times 2}$.*

Proof. $\mathrm{Gal}(k_\infty/k)$ is abelian; let ω be its action on μ_4 and c an element with $\omega(c) = -1$. Write $u = y^4$ and $\sigma(y) = \zeta(\sigma)y$ with $\zeta(\sigma) \in \mu_4$, so $\zeta(\sigma\tau) = \zeta(\sigma)\sigma(\zeta(\tau))$. From $\sigma c = c\sigma$, $\zeta(\sigma)\sigma(\zeta(c)) = \zeta(c)c(\zeta(\sigma)) = \zeta(c)\zeta(\sigma)^{-1}$, so $\zeta(\sigma)^2 = \zeta(c)^{1-\omega(\sigma)}$. Put $s = y^2$; then $\sigma(s) = \zeta(\sigma)^2 s$, so s is fixed by every σ with $\omega(\sigma) = 1$, that is $s \in k(i)$, and $c(s) = \pm s$. If $c(s) = s$ then $s \in k$ and $u = s^2$; otherwise $s = it$ with $t \in k$ and $u = -t^2$. □

Proof of Proposition 3.5. Write $d_2 = d_2(K)$ and $s_v = (-1)^{2\,\mathrm{inv}_v[\varsigma]}$ for every place v; $s_v = 1$ at finite $v \notin T_- \cup S_2$ by hypothesis and by the definition of T_-, and $\prod_v s_v = 1$ [43, (8.1.17)].

Data depending only on K and Z. Let $\Lambda = \{x \in \hat{E} : \iota(x) \in \langle (-1)_v : v \in S_2\rangle\}$ and, for $x \in \Lambda$, write $\iota(x) = \prod_v (-1)_v^{a_v(x)}$. Since Λ contains $\ker\iota$ with finite index and $\hat{E}$ has torsion $\{\pm1\} \subset \Lambda$, $\Lambda/\{\pm1\}$ is a free $\mathbb{Z}_2$-module of rank d_2. Choose a basis $e_1, \dots, e_{n_K-1}$ of $\hat{E}/\{\pm1\}$ and integers $0 \le c_1 \le \cdots \le c_{d_2}$ with $\Lambda/\{\pm1\} = \bigoplus_{i \le d_2} 2^{c_i}\mathbb{Z}_2 e_i$, lifts $z_i \in \hat{E}$ of e_i, and put $\lambda_i = z_i^{2^{c_i}} \in \Lambda$, so that $\Lambda = \{\pm1\} \times \langle \lambda_1, \dots, \lambda_{d_2}\rangle$; let $c = c_{d_2}$ ($c = 0$ if $d_2 = 0$). Let $H = \iota(\hat{E}) \cdot \langle (-1)_v \rangle$ and let 2^t be the exponent of the torsion of $\hat{U}_2/H$. Fix $M_Z \ge 0$ with $2^{M_Z} > N\mathfrak{Q}$ for every $\mathfrak{Q} \in Z$.

Step 1 (local data). For $v \in T_-$ let χ_v be the character of $K_v^\times$ that is trivial on a fixed uniformiser and on $U_v^{(1)}$ and has exact order $2^{v_2(Nv-1)}$ on $\mathcal{O}_v^\times$; then $\chi_v(-1) = -1 = s_v$. At a real place v let χ_v be the sign if $s_v = -1$ and trivial otherwise. Let $\Phi_0 \colon \hat{E} \to \mu_{2^\nu}$ extend $u \mapsto \prod_{v \in T_- \cup S_\infty} \chi_v(u)$, and let $\sigma_0 \colon \Lambda \to \{\pm1\}$, $\sigma_0(x) = \prod_{v \in S_2} s_v^{a_v(x)}$. Then $\Phi_0(-1) = \prod_{v \in T_- \cup S_\infty} s_v = \prod_{v \in S_2} s_v = \sigma_0(-1)$. Put $\omega_i = \sigma_0(\lambda_i)\Phi_0(\lambda_i)^{-1} \in \mu_{2^\nu}$.

Step 2 (auxiliary primes; only if $d_2 > 0$). Put $M = \nu + c + d_2 + 2 + M_Z + \lceil \log_2 n_K \rceil$ and $k = K(\mu_{2^M})$. Choose units $u_i \in \mathcal{O}_K^\times$ with $u_i \equiv z_i$ in $\hat{E}/\hat{E}^4$ and let $\Gamma = \langle -1, u_1, \dots, u_{d_2}\rangle$. The u_i are independent in $\mathcal{O}_K^\times/\pm\mathcal{O}_K^{\times 2}$, so $\Gamma \cap \pm\mathcal{O}_K^{\times 2} = \pm\Gamma^2$. Let $W \subseteq \Gamma/\pm\Gamma^2$ be the classes of elements that are squares in k, and change the basis of $\Gamma/\{\pm1\}$ by a matrix in $\mathrm{GL}_{d_2}(\mathbb{Z})$

to $u_1', \dots, u_a', w_1, \dots, w_b$ with the w_l spanning W. Then $\Gamma \cap k^{\times 4} = \langle -1, w_1^2, \dots, w_b^2, \Gamma^4 \rangle$: the inclusion $\supseteq$ holds as $-1 = \zeta_{16}^8$; conversely, if $x \in \Gamma \cap k^{\times 4}$, Lemma A.6 (with $i \notin K$) gives $x \in \pm K^{\times 2} \cap \Gamma = \pm\Gamma^2$, $x = \pm g^2$, and $g^2 \in k^{\times 4}$ forces $g \in \pm k^{\times 2}$, so the class of g lies in W. By Kummer theory over k, $\mathrm{Gal}(k(\Gamma^{1/4})/k) \cong \mathrm{Hom}(\Gamma/(\Gamma \cap k^{\times 4}), \mu_4)$ with $\Gamma/(\Gamma \cap k^{\times 4}) \cong (\mathbb{Z}/4)^a \times (\mathbb{Z}/2)^b$ on the basis u', w. Let h_j ($j \le d_2$) be the Kummer character with $h_j(u_i') = \zeta_4^{[i=j]}$ and $h_j(w_l) = 1$ for $j \le a$, and $h_j(u_i') = 1$, $h_j(w_l) = (-1)^{[l=j-a]}$ for $j > a$; let $\sigma_j \in \mathrm{Gal}(k(\Gamma^{1/4})/K)$ be trivial on k with Kummer character h_j. Its conjugacy class consists of elements trivial on k with Kummer character $h_j^{\pm 1}$, and it meets the abelian subgroup $\mathrm{Gal}(k(\Gamma^{1/4})/K(i))$. The conductor of $k(\Gamma^{1/4})/K(i)$ divides $2^M \prod_{\mathfrak{P}|2} \mathfrak{P}^{3e(\mathfrak{P})+1}$ (a character of order dividing 4 of a dyadic field with ramification index e is trivial on $U^{(3e+1)} = (U^{(e+1)})^4$), so every character of that group has conductor of norm at most $2^{2n_K(M+4)}$. Thorner and Zaman's bound for the least prime in a Chebotarev class [63, Theorem 1.1] gives a prime $\mathfrak{Q}_j$ of K, unramified in $k(\Gamma^{1/4})$, with Frobenius class that of σ_j, and with

$$N\mathfrak{Q}_j \ll D_{K(i)}^{694}\, 2^{2n_K(M+4)\cdot 521} + D_{K(i)}^{232}\, 2^{2n_K(M+4)\cdot 367} (2n_K)^{580 n_K} \le C \cdot 2^{1042 n_K \nu}.$$

The $\mathfrak{Q}_j$ are pairwise distinct; they are odd, because $2^{M-1} > n_K \ge e_v$ for $v \in S_2$, so every dyadic prime ramifies in k (its completions contain $\mathbb{Q}_2(\mu_{2^M})$, of ramification index 2^{M-1}); $N\mathfrak{Q}_j \equiv 1 \pmod{2^M}$, so $N\mathfrak{Q}_j > 2^{Mz}$ and $\mathfrak{Q}_j \notin Z$; and the quartic residue symbol $(x/\mathfrak{Q}_j)_4$ equals $h_j^{\pm 1}(x)$ for $x \in \Gamma$. Put $Q = \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_{d_2}\}$.

Step 3 (solving on Λ). Let g_j generate the 2-Sylow subgroup of $(\mathcal{O}_K/\mathfrak{Q}_j)^\times$, cyclic of order 2^{k_j} with $k_j \ge M$, and let $\log_j \colon \hat{E} \to \mathbb{Z}/2^{k_j}$ be the induced map. Then $\log_j(x) \bmod 4$ is determined by $(x/\mathfrak{Q}_j)_4$, so the matrix $(\log_j(y))$, y running through u', w, is congruent modulo 4 to $D_0 U$ with $D_0 = \mathrm{diag}(1^a, 2^b)$ and U diagonal with odd entries. The matrix $R = (\log_j(z_i))_{i,j}$, lifted to $\mathbb{Z}_2$, satisfies $R \equiv P D_0 U \pmod 4$ for some $P \in \mathrm{GL}_{d_2}(\mathbb{Z})$ (as $z_i \equiv u_i$ modulo fourth powers and $\log_j(-1) \equiv 0 \pmod 4$), so $R = P(D_0 U + 4X)$ and $v_2(\det R) = b$. Let ζ be a primitive 2^{M-1}-th root of unity and write $\omega_i = \zeta^{y_i}$ with $y_i \in 2^{M-1-\nu}\mathbb{Z}$. Then $y_i' = y_i/2^{c_i} \in 2^{M-1-\nu-c}\mathbb{Z} \subseteq 2^b\mathbb{Z}$, since $M - 1 - \nu - c > d_2 \ge b$, so $x = R^{-1} y' \in \mathbb{Z}_2^{d_2}$ and $\sum_j 2^{c_i} R_{ij} x_j = y_i$. Let ξ_j be the character of $(\mathcal{O}_K/\mathfrak{Q}_j)^\times$ that is trivial on the odd part and maps g_j to ζ^{x_j}; then $\xi_j(-1) = 1$ and $\prod_j \xi_j(\lambda_i) = \omega_i$. So $\Psi = \Phi_0 \prod_j \xi_j$ (on $\hat{E}$, through reduction modulo $\mathfrak{Q}_j$) satisfies $\Psi|_\Lambda = \sigma_0$ and takes values in $\mu_{2^{M-1}}$. If $d_2 = 0$, put $Q = \emptyset$, $M = \nu + 1$ and $\Psi = \Phi_0$; again $\Psi|_\Lambda = \sigma_0$, as $\Lambda = \{\pm 1\}$.

Step 4 (the character). The rule $\iota(x) \prod_v (-1)_v^{b_v} \mapsto \Psi(x)^{-1} \prod_v s_v^{b_v}$ is a well-defined character of H (its only relations come from $x \in \Lambda$, where $\Psi = \sigma_0$), with values in $\mu_{2^{M-1}}$. By Lemma A.5 it extends to a character θ of $\hat{U}_2$ with values in $\mu_{2^{M-1+t}}$, trivial on $U_v^{(e_v(M+t)+1)}$ for $v \in S_2$. Consider the character of $\prod_v U_v$ ($U_v = \mathcal{O}_v^\times$ at finite v, $U_v = \mathbb{R}^\times$ at real v) equal to θ composed with the projection $\mathcal{O}_v^\times \to U_v^{(1)}$ at $v \in S_2$, to χ_v at $v \in T_- \setminus Q$, to $\chi_v \xi_j$ at $v = \mathfrak{Q}_j \in T_-$, to ξ_j at $v = \mathfrak{Q}_j \notin T_-$, to χ_v at the real places, and trivial elsewhere. On $\mathcal{O}_K^\times$ it equals $\theta(\iota(u))\Psi(u) = 1$, so it is a character of an open subgroup of finite index of $\mathbf{A}_K^\times / K^\times$; any extension χ_1 to $\mathbf{A}_K^\times / K^\times$ has order dividing $2^{M-1+t} \exp \mathrm{Cl}(K)$, is unramified outside $T_0 \cup Q$, is tame at every odd prime, and has $\chi_{1,v}(-1) = s_v$ at every v. Lemma A.2 gives ϑ_1 with $\vartheta_1^2 = \chi_1$ and $\delta\vartheta_1 = \varsigma$.

Step 5 (removing ramification outside $T_0 \cup Q$). By Lemma A.3, $\vartheta_1|_{G_{K_0}}$ is a homomorphism of finite order, so the set Σ' of finite primes $v \notin T_0 \cup Q$ with $\vartheta_1|_{I_v} \ne 1$ is finite, and by Lemma A.4 $\vartheta_1|_{I_v}$ comes from the Legendre symbol for $v \in \Sigma'$. Let $\varphi(x) = \prod_{v \in \Sigma'} (x/v)$ on

$\hat{E}$, choose signs τ_v ($v \in S_2$) with $\prod_v \tau_v = \varphi(-1)$, and let $\sigma'(x) = \prod_v \tau_v^{a_v(x)}$ on Λ. If $d_2 > 0$, solve as in Step 3, with the same primes, for characters ξ'_j of $(\mathcal{O}_K/\mathfrak{Q}_j)^\times$ with values in $\mu_{2^{M-1}}$ and $\prod_j \xi'_j(\lambda_i) = \sigma'(\lambda_i)\varphi(\lambda_i)^{-1}$; then $\Psi' = \varphi \prod_j \xi'_j$ satisfies $\Psi'|_\Lambda = \sigma'$. As in Step 4, $\iota(x)\prod(-1)_v^{b_v} \mapsto \Psi'(x)^{-1}\prod \tau_v^{b_v}$ extends to a character θ' of $\hat{U}_2$ trivial on $U_v^{(e_v(M+t)+1)}$, and the character of $\prod_v U_v$ equal to the Legendre symbol at $v \in \Sigma'$, to ξ'_j at $\mathfrak{Q}_j$, to θ' at S_2 and trivial elsewhere is trivial on $\mathcal{O}_K^\times$; it extends to a character ψ of G_K of order dividing $2^{M-1+t}\exp \mathrm{Cl}(K)$, with $\psi|_{I_v} = \vartheta_1|_{I_v}$ for $v \in \Sigma'$ and ψ unramified outside $T_0 \cup Q \cup \Sigma'$. Put $\vartheta = \vartheta_1\psi^{-1}$ and $\chi = \chi_1\psi^{-2}$. Then $\delta\vartheta = \varsigma$, $\vartheta^2 = \chi$, $\vartheta|_{G_{K_0}}$ and χ are unramified outside $T_0 \cup Q$ (ψ^2 is trivial on $\mathcal{O}_v^\times$ for $v \in \Sigma'$), χ is tame at every odd prime, and so is $\vartheta|_{G_{K_0}}$ (its square is tame, and wild inertia at an odd prime is pro-odd). The order m of χ divides $2^{M-1+t}\exp \mathrm{Cl}(K) \le C \cdot 2^\nu$; the dyadic conductor exponents of χ_1 and ψ^2 are at most $e_v(M+t)+1 \le e_v(\nu + C)$; and $[K' : K] \le [K' : K_0][K_0 : K] \le 2m[K_0 : K]$, because $\vartheta|_{G_{K_0}}$ takes values in μ_{2m}. □

Appendix B. The number of unknowns

We write the certificate of Definition 7.2 as one polynomial equation in x and 25 further unknowns, solvable in K exactly when $x \in \mathbb{Z}$ (Proposition B.5).

The construction follows [60, Lemmas 10.4 and 13.7] and [58, §§10.3–10.6] (a separating element, a gcd filter and one polynomial that absorbs the inequations). The finite choices here satisfy a triangular system whose fibres need not be reduced; instead of stratifying to reduced fibres, as in [60, proof of Lemma 10.4], we recover each choice together with its multiplicity (Lemma B.2).

B.1. **Coordinates and finite choices.** Each of the nine points of Definition 7.2 is $V_\iota = [2]V'_\iota$ for a point $V'_\iota \in E(L)$, $1 \le \iota \le 9$; by (C1), $V'_\iota \notin E[2]$, so V'_ι has a finite abscissa $x(V'_\iota) = \xi_{2\iota-1} + \sqrt{d}\,\xi_{2\iota}$ with $\xi_{2\iota-1}, \xi_{2\iota} \in K$. The *structural coordinates* are the 24 elements

$$\mathbf{x} = (\xi_1, \dots, \xi_{18}, a_0, b_0, e^{(0)}, w^{(0)}, e^{(1)}, w^{(1)}) \in K^{24},$$

where $e^{(j)}, w^{(j)}$ are the witnesses of $\Phi_K(B_j)$; put $\bar{x} = (X, \mathbf{x}) \in K^{25}$. Everything in the certificate is obtained from $\bar{x}$ by rational operations with coefficients in F, together with the following finite choices:

(c1) the ordinates $y(V'_\iota) \in L$, roots of $y^2 - f(x(V'_\iota))$, where $f(t) = t^3 - At$;
(c2) the square roots in K of the two expressions (5.1) for B_0 and for B_1.

The finitely many discrete alternatives (the sign δ; for B_0 and for B_1, the alternative $B_j = 0$ or a multiplier $\mu \in \mathcal{M}$; the cases of coincident or opposite points in each use of the group law) are called *outer branches*. On an outer branch, all conditions of Definition 7.2 (the definitions of the points by duplication and the group law, (C1)–(C3), and every guard) become polynomial equations and inequations in $\bar{x}$ and the choices, after multiplying by guarded denominators. An element $u = u^{(0)} + \sqrt{d}\,u^{(1)}$ of L is 0 if and only if $u^{(0)} = u^{(1)} = 0$, and nonzero if and only if $(u^{(0)})^2 - d(u^{(1)})^2 \ne 0$, as $\sqrt{d} \notin K$ (E1); and $\mathrm{Tr}_{L/K}(u) = 2u^{(0)}$.

Scaling. If T is a root of $a_d T^d + \cdots + a_0$ with $a_d \ne 0$ (a guard), then $a_d T$ is a root of the monic polynomial $T'^d + \sum_{i<d} a_i a_d^{d-1-i} T'^i$. Clearing denominators in this way makes each choice in (c1)–(c2) a root of a monic polynomial whose coefficients are polynomials in $\bar{x}$ and the earlier choices.

Lemma B.1 (Restriction of scalars)**.** *Let $\mathcal{K}$ be a polynomial ring over $\mathbb{Q}$ or over K, $p \in \mathcal{K}[\sqrt{d}][T]$ monic of degree n, p^τ its conjugate, and*

$$q_0(Y) = 2^{-n^2}\operatorname{Res}_\eta(p(\eta), p^\tau(2Y-\eta)), \qquad q_1(y_0;Y) = (-d)^{-n}p(y_0+\sqrt{d}\,Y)\,p^\tau(y_0-\sqrt{d}\,Y).$$

(i) *$q_0 \in \mathcal{K}[Y]$ is monic of degree n^2, and $q_1 \in \mathcal{K}[y_0][Y]$ is monic of degree $2n$ in Y.*

(ii) *At any specialisation of $\mathcal{K}$ to K, if $y = y_0 + \sqrt{d}\,y_1$ $(y_0, y_1 \in K)$ is a root of p, then $q_0(y_0) = 0$ and $q_1(y_0; y_1) = 0$.*

(iii) *Writing $p(y_0 + \sqrt{d}\,y_1) = P_0 + \sqrt{d}\,P_1$ with $P_0, P_1 \in \mathcal{K}[y_0, y_1]$, any $y_0, y_1 \in K$ with $P_0 = P_1 = 0$ give the root $y_0 + \sqrt{d}\,y_1 \in L$ of p.*

Proof. (i) For monic p, $\operatorname{Res}_\eta(p(\eta), g(\eta)) = \prod_{p(\eta)=0} g(\eta)$ over an algebraic closure; with $g(\eta) = p^\tau(2Y-\eta) = \prod_{\eta'}(2Y-\eta-\eta')$, the product over the roots η' of p^τ, this is $2^{n^2}\prod_{\eta,\eta'}(Y - \frac{\eta+\eta'}{2})$. Conjugating the coefficients exchanges p and p^τ and leaves the product unchanged, so the coefficients lie in $\mathcal{K}$. The leading coefficient of $p(y_0+\sqrt{d}\,Y)p^\tau(y_0-\sqrt{d}\,Y)$ in Y is $(\sqrt{d})^n(-\sqrt{d})^n = (-d)^n$, and conjugation fixes the product. (ii) Conjugating $p(y) = 0$ gives $p^\tau(y_0 - \sqrt{d}\,y_1) = 0$; so y_0 is one of the $(\eta+\eta')/2$, and $q_1(y_0; y_1) = (-d)^{-n}p(y)p^\tau(y^\tau) = 0$. (iii) is clear. □

Replacing each L-valued choice by its two coordinates, which are roots of q_0 and of $q_1(y_0;\cdot)$ (Lemma B.1), and adding the equations $P_0 = P_1 = 0$, each outer branch $\mathfrak{b}$ of the certificate at $\bar{x}$ reads: *there is $t = (t_1, \dots, t_N) \in K^N$ with $p_i(\bar{x}, t_1, \dots, t_i) = 0$ $(1 \le i \le N)$, $E_l(\bar{x}, t) = 0$ $(1 \le l \le r)$ and $G(\bar{x}, t) \neq 0$*, where p_i is monic in t_i of degree $d_i \ge 1$ with coefficients in $K[\bar{x}, t_1, \dots, t_{i-1}]$, the E_l and G are polynomials over K, and G is the product of all guards.

B.2. **Recovering the choices from one element.** Let $\mathcal{A} = K[\bar{x}][t_1, \dots, t_N]/(p_1, \dots, p_N)$. Division by $p_N, p_{N-1}, \dots, p_1$ in turn shows that $\mathcal{A}$ is a free $K[\bar{x}]$-module with basis the monomials t^α, $0 \le \alpha_i < d_i$, of rank $D = \prod d_i$, and that this basis specialises to a K-basis of $\mathcal{A}_{\bar{x}_0} = K[t]/(p(\bar{x}_0, t))$ at every $\bar{x}_0 \in K^{25}$. For $h \in K[\bar{x}][t]$ let M_h be the matrix of multiplication by h. For $b \in \mathbb{Z}$ put $z_b = \sum_{i=1}^N b^{i-1}t_i$, $\chi_b(Z) = \det(Z - M_{z_b})$ and $\Phi_{b,h}(Z) = \operatorname{Tr}\big(M_h \operatorname{adj}(Z - M_{z_b})\big)$, polynomials in $K[\bar{x}][Z]$, the first monic of degree D.

Lemma B.2. *Let $\bar{x}_0 \in K^{25}$ and $t \in K^N$ with $p_i(\bar{x}_0, t_1, \dots, t_i) = 0$ for all i. Call the solutions t' over an algebraic closure $\overline{K}$ of the system $p_1 = \cdots = p_N = 0$ at $\bar{x}_0$ its points; there are at most D of them.*

(i) *There is $b \in \{1, \dots, 1 + (N-1)(D-1)\}$ with $z_b(t') \neq z_b(t)$ for every point $t' \neq t$.*

(ii) *For such b, $\zeta = z_b(t) \in K$ is a root of $\chi_b(\bar{x}_0; Z)$ of some multiplicity m, $1 \le \mathsf{m} \le D$, and for every $h \in K[\bar{x}][t]$*

$$h(\bar{x}_0, t) = \frac{\Phi_{b,h}^{(\mathsf{m}-1)}(\bar{x}_0; \zeta)}{\chi_b^{(\mathsf{m})}(\bar{x}_0; \zeta)},$$

derivatives in Z, with nonzero denominator.

Proof. (i) For each point $t' \neq t$, $z_b(t') - z_b(t)$ is a nonzero polynomial in b of degree at most $N-1$. (ii) Let $V = \mathcal{A}_{\bar{x}_0} \otimes_K \overline{K}$, of dimension D, with the commuting operators $T_i = M_{t_i}$. Then V is the direct sum of the joint generalised eigenspaces $V_\lambda = \{v : (T_i - \lambda_i)^D v = 0\ \forall i\}$, $\lambda \in \overline{K}^N$. On $V_\lambda \neq 0$, $M_h - h(\lambda)$ is nilpotent for every polynomial h; with $h = p_i$, which is 0 in $\mathcal{A}$, this gives $p_i(\lambda) = 0$, so every such λ is a point. Evaluation at t is a nonzero linear form ϵ on V with $\epsilon(t_i a) = t_i \epsilon(a)$, a common eigenvector of the transposes of the T_i, and the transposes

have the dual decomposition; so $V_t \neq 0$. Put $\mathsf{m}_\lambda = \dim V_\lambda$ and $\mathsf{m} = \mathsf{m}_t$. As $M_{z_b} - z_b(\lambda)$ is nilpotent on V_λ, $\chi_b(Z) = \prod_\lambda (Z - z_b(\lambda))^{\mathsf{m}_\lambda} = (Z-\zeta)^{\mathsf{m}} g(Z)$ with $g(\zeta) \neq 0$ by (i). As rational functions, $\operatorname{adj}(Z - M_{z_b}) = \chi_b(Z)(Z - M_{z_b})^{-1}$, and $(Z - M_{z_b})^{-1}$ preserves each V_λ; so $\Phi_{b,h}(Z) = \chi_b(Z) \sum_\lambda \operatorname{Tr}\big(M_h (Z - M_{z_b})^{-1}|_{V_\lambda}\big)$, where the summand for $\lambda \neq t$ is regular at ζ. On V_t write $M_{z_b} = \zeta + \mathfrak{n}$ with $\mathfrak{n}^{\mathsf{m}} = 0$; then $(Z - M_{z_b})^{-1} = \sum_{k<\mathsf{m}} \mathfrak{n}^k (Z-\zeta)^{-k-1}$, $\operatorname{Tr}(M_h \mathfrak{n}^k|_{V_t}) = 0$ for $k \geq 1$ (a nilpotent operator), and $\operatorname{Tr}(M_h|_{V_t}) = \mathsf{m}\, h(t)$. So $\Phi_{b,h}(Z) = (Z-\zeta)^{\mathsf{m}-1} u(Z)$ with u regular at ζ and $u(\zeta) = \mathsf{m}\, h(t) g(\zeta)$; hence $\Phi_{b,h}^{(\mathsf{m}-1)}(\zeta) = (\mathsf{m}-1)!\, \mathsf{m}\, h(t) g(\zeta)$, while $\chi_b^{(\mathsf{m})}(\zeta) = \mathsf{m}!\, g(\zeta) \neq 0$. □

Lemma B.3. *Let k be a field, $f \in k[Z]$ monic of degree $d \geq 1$, $g \in k[Z]$, M_g the matrix of multiplication by g on $k[Z]/(f)$ in the basis $1, Z, \dots, Z^{d-1}$, and $\varrho = \operatorname{rank} M_g$. Then $\deg \gcd(f,g) = d - \varrho$. If $\varrho = 0$, then $\gcd(f,g) = f$. If $\varrho \geq 1$, some set C' of ϱ columns has nonzero minor μ' on the rows of $Z^{d-\varrho}, \dots, Z^{d-1}$, and for any such C' the combination of the columns C' whose coordinates on those rows are $(1, 0, \dots, 0)$ is the monic $\gcd(f,g)$.*

Proof. The image of M_g is $(g,f)/(f) = (\gamma)/(f)$ with $\gamma = \gcd(f,g)$, of dimension $d - \deg\gamma$. If $\varrho = 0$, then $\deg\gamma = d$, so $\gamma = f$. Let $\varrho \geq 1$. An element of the image whose coordinates at $Z^{d-\varrho}, \dots, Z^{d-1}$ vanish has degree $< \deg\gamma$ and is divisible by γ, so is 0; hence projection to those rows is bijective on the image, and a column basis of the image has a nonzero minor there. For any C' with $\mu' \neq 0$ the columns C' form a basis of the image, and the element with top coordinates $(1, 0, \dots, 0)$ is monic of degree $d - \varrho$ and divisible by γ, so it is γ. □

If f, g have coefficients in $K(\bar{x})$ with guarded denominators, a *gcd branch* is a choice of ϱ and, if $\varrho \geq 1$, of C'; its conditions are that every $(\varrho+1)$-minor of M_g vanishes and, if $\varrho \geq 1$, that $\mu' \neq 0$. Every $\bar{x}_0$ at which the denominators of f and g are nonzero lies on some gcd branch, and on a gcd branch the monic gcd is f if $\varrho = 0$, and otherwise has coefficients in $K[\bar{x}][1/\mu', \text{denominators}]$.

B.3. **The polynomial.** Fix an outer branch $\mathfrak{b}$, $b \in \{1, \dots, 1 + (N-1)(D-1)\}$ and $\mathsf{m} \in \{1, \dots, D\}$. Put $t_i^{\mathrm{rec}}(Z) = \Phi_{b,t_i}^{(\mathsf{m}-1)}(Z) / \chi_b^{(\mathsf{m})}(Z)$; let $\hat{E} \in K[\bar{x}][Z]$ be the sum of the squares of the numerators of $p_i(\bar{x}, t^{\mathrm{rec}}(Z))$ and $E_l(\bar{x}, t^{\mathrm{rec}}(Z))$ written over powers of $\chi_b^{(\mathsf{m})}(Z)$, and $\hat{H} = \chi_b^{(\mathsf{m})}(Z)$ times the numerator of $G(\bar{x}, t^{\mathrm{rec}}(Z))$. Let $\mathcal{R}_0 = \gcd(\chi_b, \hat{E})$ and $\mathcal{R}_1 = \mathcal{R}_0 / \gcd(\mathcal{R}_0, \hat{H}^{\deg \mathcal{R}_0})$, computed by Lemma B.3 on gcd branches and by exact division of monic polynomials; on a branch where $\deg \mathcal{R}_0 = 0$, $\mathcal{R}_0 = \mathcal{R}_1 = 1$. At $\bar{x}_0$ on these branches the roots of $\mathcal{R}_1(\bar{x}_0; \cdot)$ are exactly the common roots ζ of χ_b and $\hat{E}$ with $\hat{H}(\zeta) \neq 0$: a common root with $\hat{H}(\zeta) = 0$ has multiplicity at least $\deg \mathcal{R}_0$ in $\hat{H}^{\deg \mathcal{R}_0}$ and is removed entirely.

Lemma B.4. *In this situation: if $\zeta \in K$ is a root of $\mathcal{R}_1(\bar{x}_0; \cdot)$, then $t^{\mathrm{rec}}(\zeta) \in K^N$ satisfies the branch $\mathfrak{b}$ at $\bar{x}_0$; and if $\mathfrak{b}$ holds at $\bar{x}_0$ with some $t \in K^N$, then for b, m as in Lemma B.2, $\zeta = z_b(t) \in K$ is a root of $\mathcal{R}_1(\bar{x}_0; \cdot)$ on the gcd branches through $\bar{x}_0$.*

Proof. If $\mathcal{R}_1(\bar{x}_0; \zeta) = 0$ with $\zeta \in K$, then $\hat{H}(\zeta) \neq 0$, so $\chi_b^{(\mathsf{m})}(\zeta) \neq 0$, and $\hat{E}(\zeta) = 0$; as K is real, each p_i and E_l vanishes at $t^{\mathrm{rec}}(\zeta)$, and $G \neq 0$ there. Conversely Lemma B.2 gives $t^{\mathrm{rec}}(\zeta) = t$ and $\chi_b^{(\mathsf{m})}(\zeta) \neq 0$, so $\chi_b(\zeta) = 0$, $\hat{E}(\zeta) = 0$ and $\hat{H}(\zeta) \neq 0$. □

A *final branch* γ is a choice of $(\mathfrak{b}, b, \mathsf{m})$, of a gcd branch for $\mathcal{R}_0$ and, if $\deg \mathcal{R}_0 \geq 1$, of one for $\gcd(\mathcal{R}_0, \hat{H}^{\deg \mathcal{R}_0})$, and of $c_0 \in \{0, 1\}$. On it let $d_1 = \deg \mathcal{R}_1$ and write $\mathcal{R}_1(T - c_0) = T^{d_1} + \sum_{k=1}^{d_1} (\mathcal{N}_k / \mathcal{B}) T^{d_1 - k}$ with $\mathcal{N}_k, \mathcal{B} \in K[\bar{x}]$, where $\mathcal{B}$ is the product of the denominators (guarded factors of the branch); let $\mathcal{H}_\gamma \in K[\bar{x}]$ be the product of the numerators of all

inequations of the branch (the minors μ' and the denominators), and $E_{\gamma,1},\dots,E_{\gamma,s}\in K[\bar{x}]$ its equations (the vanishing minors). As in [58, (10.8)], put

$$\Psi_\gamma(\bar{x},U)=1+\sum_{k=1}^{d_1}\mathcal{N}_k\mathcal{B}^{2k-1}\mathcal{H}_\gamma^kU^k.$$

If $\mathcal{B}\mathcal{H}_\gamma=0$ at $\bar{x}$, then $\Psi_\gamma(\bar{x},U)=1$. If $\mathcal{B}\mathcal{H}_\gamma\neq0$ and $\mathcal{S}_\gamma=\mathcal{B}^2\mathcal{H}_\gamma$, then for $U\neq0$, $\Psi_\gamma(\bar{x},U)=(\mathcal{S}_\gamma U)^{d_1}\,\mathcal{R}_1(1/(\mathcal{S}_\gamma U)-c_0)$, because $\mathcal{S}_\gamma^k/\mathcal{B}=\mathcal{B}^{2k-1}\mathcal{H}_\gamma^k$. Hence $\Psi_\gamma(\bar{x},U)=0$ for some $U\in K$ if and only if $\mathcal{B}\mathcal{H}_\gamma\neq0$ and $\mathcal{R}_1$ has a root $\zeta\in K$ with $\zeta\neq-c_0$; every root is $\neq-c_0$ for $c_0=0$ or for $c_0=1$. Let

$$F_1(\bar{x},U)=\prod_\gamma\Big(\Psi_\gamma(\bar{x},U)^2+\sum_l E_{\gamma,l}(\bar{x})^2\Big)\in K[X,\mathbf{x},U],$$

the product over the finitely many final branches.

Proposition B.5. *For $x\in K$: there are $\mathbf{x}\in K^{24}$ and $U\in K$ with $F_1(x,\mathbf{x},U)=0$ if and only if $x\in\mathbb{Z}$.*

Proof. If $x\in\mathbb{Z}$, the certificate holds at x (Proposition 9.4); it holds on some outer branch with some $\mathbf{x}$ and t; take b,m,ζ from Lemma B.2, the gcd branches through $\bar{x}$, and c_0 with $\zeta\neq-c_0$; then the equations $E_{\gamma,l}$ vanish, $\mathcal{B}\mathcal{H}_\gamma\neq0$, and $U=1/(\mathcal{S}_\gamma(\zeta+c_0))$ makes $\Psi_\gamma=0$ by Lemma B.4. Conversely, if $F_1(\bar{x},U)=0$, some factor vanishes; K being real, $E_{\gamma,l}(\bar{x})=0$ for all l and $\Psi_\gamma(\bar{x},U)=0$, so $\bar{x}$ lies on the branch γ and $\mathcal{R}_1$ has a root $\zeta\in K$; by Lemma B.4 the certificate holds at x, and $x\in\mathbb{Z}$ by Proposition 8.3. □

B.4. **Coefficients in $\mathbb{Z}$.** Let F_1 be the polynomial of Proposition B.5, with $(Y_1,\dots,Y_{25})=(\mathbf{x},U)$. We show that its coefficients are rational.

In the coordinates $u=u^{(0)}+\sqrt{d}\,u^{(1)}$, the product of $u,v\in L$ is $(u^{(0)}v^{(0)}+d\,u^{(1)}v^{(1)})+\sqrt{d}\,(u^{(0)}v^{(1)}+u^{(1)}v^{(0)})$, the inverse of $u\neq0$ is $(u^{(0)}-\sqrt{d}\,u^{(1)})/((u^{(0)})^2-d(u^{(1)})^2)$, τ changes the sign of $u^{(1)}$, $\mathrm{Tr}_{L/K}(u)=2u^{(0)}$, and an element of F has rational coordinates. So a rational expression whose constants lie in F becomes, in coordinates, a pair of rational expressions with coefficients in $\mathbb{Q}$. Every constant in the conditions of Definition 7.2 and in the choices (c1)–(c2) lies in F: the coefficients of E and of E^σ; the coordinates of P and of $[c_*]P$, since $P\in E(F)$ (E3); the coefficients of ℓ_m and of ℓ_m^σ (Section 6.2); the coefficients of the group law, of the duplication formula and of f, which lie in $\mathbb{Z}[A]$; and the rational numbers q (and q' when $\sqrt{3}\in K$), γ_i, θ_i, ω, ξ, d_j, m, c_*, Γ, C, M, the precisions, the elements of $\mathcal{M}$, and the coefficients of F_8, R_ψ (or $\hat{R}_\psi$) and $\mathcal{L}$. The primes $\mathfrak{q}$ and $\mathfrak{q}'$, the sets Σ_0 and $\mathfrak{B}$ and the exponent κ do not occur in the conditions; they enter only the proofs of Propositions 8.3, 9.4 and 10.7.

Hence, on every outer branch, the conditions written in coordinates are polynomial equations and inequations with rational coefficients in $\bar{x}$ and the coordinates of the choices, and after scaling each choice is a root of a monic polynomial with coefficients in $\mathcal{K}[\sqrt{d}]$, where $\mathcal{K}$ is the polynomial ring over $\mathbb{Q}$ in $\bar{x}$ and the coordinates of the earlier choices. By Lemma B.1, applied to this $\mathcal{K}$, q_0 and q_1 have coefficients in $\mathcal{K}$, and the p_i, E_l and G lie in $\mathbb{Q}[\bar{x},t]$. Each later object is given by a formula with rational coefficients in the objects before it: the matrices M_h, the polynomials χ_b and $\Phi_{b,h}$ (with $b\in\mathbb{Z}$) and their derivatives, t^{rec}, $\hat{E}$ and $\hat{H}$; the minors, μ' and the gcd of Lemma B.3 (Cramer's rule), and the exact division of monic polynomials; the substitution $T\mapsto T-c_0$ with $c_0\in\{0,1\}$; and $\mathcal{N}_k$, $\mathcal{B}$, $\mathcal{H}_\gamma$, $E_{\gamma,l}$ and Ψ_γ. Therefore $F_1\in\mathbb{Q}[X,Y_1,\dots,Y_{25}]$.

Let c be a positive integer with $\mathbf{F} = cF_1 \in \mathbb{Z}[X, Y_1, \dots, Y_{25}]$. By Proposition B.5, an element x of K lies in $\mathbb{Z}$ if and only if $\mathbf{F}(x, y) = 0$ for some $y \in K^{25}$. So $\mathbb{Z}$ is Diophantine in K with 25 unknowns: the eighteen coordinates of the abscissas of nine points of $E(L)$, the two coordinates a_0, b_0, the four witnesses of the two pole predicates, and the parameter U. □

Appendix C. Two steps at a composite modulus

We give the two steps used in the proofs of Theorems 4.1 and 4.3. Throughout, *the appendix* is the appendix "Simultaneous primes with coprime adjacent norms" of [68], and we keep its notation. Let Δ be a positive integer (in the appendix, its fixed modulus) and $\Delta' = \Delta/\prod_{p|\Delta} p$. For v at least the largest prime factor of Δ put $W_v = \prod_{p\le v} p$; then $\Delta \prod_{p\le v,\, p\nmid\Delta} p = \Delta' W_v$, so $\Delta \mid \Delta' W_v$, and Δ' does not depend on v. Let $\Lambda'(n) = \log n$ if n is prime and $\Lambda'(n) = 0$ otherwise, and for a unit b modulo a positive integer V put $\lambda_{V,b}(n) = \frac{\varphi(V)}{V}\Lambda'(Vn + b)$, Green and Tao's $\Lambda'_{b,V}$.

(A) Tao and Ziegler's theorems with their own modulus. We keep the notation of the appendix's fixed-field polynomial count, which evaluates $\sum_{u\le N}\sum_{w\le T}\prod_{j=1}^{k}\Lambda'_j(u + c_j w^2)$: $\Lambda'_j(p) = \log p$ at the unramified primes p whose Frobenius in the fixed ray class field lies in the jth prescribed set, $\Lambda'_j = 0$ elsewhere, and μ_j is the corresponding density, a function on residues modulo Δ with values in $[0, 1]$ that vanishes at non-units. Fix a small $\rho > 0$ and, to begin with, v; put $A = W_v^{1/\rho}$, $n = \lfloor N/W_v \rfloor$ and $R = n^\rho$, and for a unit b modulo W_v, $1 \le b \le W_v$, put

$$f_{j,b}(x) = \tfrac{\varphi(W_v)}{W_v}\Lambda'_j(W_v x + b)\mathbf{1}_{R\le x\le n}, \qquad \theta_{j,b}(x) = \mu_j(W_v x + b), \qquad g_{j,b} = f_{j,b} - \theta_{j,b},$$

as functions on $\mathbb{Z}/n\mathbb{Z}$ with representatives $1, \dots, n$. As $\Delta' W_v \equiv 0 \pmod{\Delta}$, $\theta_{j,b}$ is Δ'-periodic on $\mathbb{Z}$, with values in $[0, 1]$. The appendix uses the modulus $\Delta' W_v$ and centres $f_{j,b}$ by a constant; with Tao and Ziegler's modulus W_v the density at $W_v x + b$ depends on x modulo Δ', and we centre by $\theta_{j,b}$. The norms are the appendix's: $\|\cdot\|_{U^a_{s[J]}}$ is the Gowers norm of order a on $\mathbb{Z}/n\mathbb{Z}$ with differences from the multiset $s(h - h')$, $h, h' \in [J]$.

Lemma C.1. *Let $a \ge 2$ and $C_1 < C_2 < C_3$ be fixed. Uniformly in j, in the units b modulo W_v, in $s \le A^{C_1}$ and in $nA^{-C_3} \le J \le nA^{-C_2}$,*

$$\|g_{j,b}\|^{2^a}_{U^a_{s[J]}} \ll \frac{1}{\log v} + o_v(1),$$

where the implied constant depends on a, C_1, C_2, C_3, ρ and the fixed data.

Proof. We follow the appendix's proof of its bound for these norms, with the centring $\theta_{j,b}$ in place of a constant, and evaluate the ordinary cube as Tao and Ziegler do in the proof of [61, Proposition 6]. Removing the values $x < R$ costs $o_v(1)$. Expand the centred cube and split its domain by the wrap-around integers m_ω, $\omega \in \{0, 1\}^a$: on each of the $O_a(1)$ convex regions the vertices are the integers $y_\omega = x + s\sum_r \omega_r(h_r - h'_r) - m_\omega n \in [1, n]$, and the $\psi_\omega = W_v y_\omega + b$ are affine-linear forms in $(x, h, h') \in \mathbb{Z}^{1+2a}$ with pairwise nonproportional linear parts. Split each region further by the class of (x, h, h') modulo Δ', into at most Δ'^{1+2a} cells. On a cell each y_ω is constant modulo Δ', so $\theta_{j,b}(y_\omega) = \mu_j(\psi_\omega)$ is a constant $c_\omega \in [0, 1]$; writing $(x, h, h') = \Delta'(x_1, h_1, h'_1)$ plus fixed residues makes the cell a convex region and multiplies every linear part by Δ', so they stay pairwise nonproportional. Expand $\prod_\omega (f_{j,b}(y_\omega) - c_\omega)$

over the sets $\Omega \subseteq \{0,1\}^a$ of factors $f_{j,b}$. The appendix's fixed-system linear replacement lemma, whose main term reads the density $\mu_j(\psi_\omega)$ at each output, gives on the cell

$$\sum \prod_{\omega\in\Omega} \Lambda'_j(\psi_\omega) = \prod_{\omega\in\Omega} c_\omega \cdot \sum \prod_{\omega\in\Omega} \Lambda'(\psi_\omega) + o_v(nJ^{2a}).$$

Summing over Ω, the centred cube on the cell is $\prod_\omega c_\omega$ times the centred cube $\sum \prod_\omega (\lambda_{W_v,b}(y_\omega) - 1)$ on the cell, up to $o_v(nJ^{2a})$. This ordinary cube is evaluated as in the proof of [61, Proposition 6], by Green and Tao's linear correlation estimate for primes [26, §1, Main Theorem] on the cell, which holds unconditionally by [23, Theorem 1.1] and [25, Theorem 1.3]. At $p \mid W_v$ every ψ_ω is prime to p, so the local factor cancels the normalisation, whatever the cell, since every prime factor of Δ' divides W_v. At $p \nmid W_v$ one has $p \nmid \Delta'$, so the condition modulo Δ' does not change the local density at p, and the local factors are those of the appendix: $1 + O_a(p^{-2})$ for $p \nmid sW_v$, and $1 + O_a(p^{-1})$ for the $O(v/\log v)$ primes $p > v$ dividing s, with product $1 + O(1/\log v)$. Centring cancels the common main term, so the ordinary cube on each cell is $(O(1/\log v) + o_v(1))nJ^{2a}$. As $0 \le c_\omega \le 1$ and the number of cells is bounded, summing over the cells gives the bound. □

The transfer. Theorem 11 and Corollary 3 of [61] apply to $f_{j,b}$: their modulus $\prod_{p\le w} p$ is W_v with $w = v$, their length is n, b is a unit modulo W_v, and $0 \le f_{j,b} \le \lambda_{W_v,b}$ since $\Lambda'_j \le \Lambda'$. With W_v in place of the appendix's modulus, the appendix's choice of their parameters is unchanged. They give a model $f'_{j,b}$, with $0 \le f'_{j,b} \le B_* - 1$ for a constant $B_* \ge 2$ of the fixed data, accurate in the local box norms and in the norms of Lemma C.1. Put $F_{j,b} = (f'_{j,b} - \theta_{j,b})/B_*$, so $|F_{j,b}| \le 1$. By the triangle inequality for these norms, the global part of Corollary 3 and Lemma C.1, the global norms of $F_{j,b}$ tend to 0 in the appendix's diagonal limit. Their Theorem 9, applied to the bounded $F_{j,b}$, gives small local norms for $F_{j,b}$, hence, multiplying by B_* and using the local part of Corollary 3, for $g_{j,b}$. Their Theorem 13 applies to products of factors f_{j,b_j}, θ_{j,b_j} and g_{j,b_j}, each bounded in absolute value by $\lambda_{W_v,b_j} + 1$, as it requires; so every polynomial average with a factor g_{j,b_j} is $o(1)$.

The main term. Write $u = W_v x + b$ and $w = W_v m + c$ with b, c modulo W_v. Then $u + c_j w^2 = W_v(x + P_j(m)) + b_j$, where $1 \le b_j \le W_v$, $b_j \equiv b + c_j c^2 \pmod{W_v}$ and $P_j(m) = c_j W_v m^2 + 2c_j cm + (b + c_j c^2 - b_j)/W_v$, with coefficients $O(W_v)$; only the (b, c) with every b_j a unit contribute. Write $\prod_j f_{j,b_j}(x+P_j(m)) = \prod_j (\theta_{j,b_j}+g_{j,b_j})(x+P_j(m))$ and expand. The terms with a factor g_{j,b_j} are $o(1)$ by the transfer, and the end intervals and wrap-around are treated as in the appendix. The remaining term is the average of $\prod_j \theta_{j,b_j}(x + P_j(m))$ over $x \le n$ and $m \le M_0$, where $M_0 = \lfloor T/W_v \rfloor$. Its summand depends only on x and m modulo Δ', as $P_j \in \mathbb{Z}[m]$, so this average is the average of $\prod_j \mu_j(W_v(x + P_j(m)) + b_j)$ over x, m modulo Δ', up to $O(\Delta'/M_0 + \Delta'/n)$. Here $W_v(x + P_j(m)) + b_j = u + c_j w^2$, and as (b, c) runs over $(\mathbb{Z}/W_v\mathbb{Z})^2$ and (x, m) over $(\mathbb{Z}/\Delta'\mathbb{Z})^2$, (u, w) runs once over $(\mathbb{Z}/\Delta' W_v\mathbb{Z})^2$. So the total main term, divided by NT, is

$$\Big(\frac{W_v}{\varphi(W_v)}\Big)^k \mathbb{E}_{u,w \bmod \Delta' W_v} \prod_{j=1}^{k} \mathbf{1}_{\gcd(u+c_j w^2,\, W_v)=1}\, \mu_j(u + c_j w^2).$$

As $\Delta' W_v = \Delta \prod_{p\le v,\, p\nmid\Delta} p$, the Chinese remainder theorem splits this average into a factor modulo Δ, where μ_j vanishes at non-units, and one factor at each $p \le v$ with $p \nmid \Delta$. With

$W_v/\varphi(W_v) = (\Delta/\varphi(\Delta))\prod_{p\le v,\,p\nmid\Delta} p/(p-1)$ it equals

$$\Big(\frac{\Delta}{\varphi(\Delta)}\Big)^k \mathbb{E}_{u,w \bmod \Delta} \prod_{j=1}^{k} \mu_j(u+c_jw^2) \prod_{p\le v,\,p\nmid\Delta} \beta_p, \qquad \beta_p = \mathbb{E}_{u,w \bmod p} \prod_{j=1}^{k} \frac{p}{p-1}\mathbf{1}_{p\nmid u+c_jw^2},$$

which tends to the appendix's main term $\mathfrak{S}$ as $v\to\infty$, since $\beta_p = 1+O_k(p^{-2})$ for all but finitely many p. The admissible residues have total mass $O(1)$, as in the appendix, so summing over them does not amplify the $o(1)$ errors. Hence the appendix's fixed-field polynomial count holds as stated, with its main term $\mathfrak{S}$.

(B) Green and Tao's majorant at the modulus V_z. For z at least the largest prime factor of Δ, $V_z = \Delta' W_z$. If $\Delta' = 1$, then $V_z = W_z$ and [26, Proposition 6.4] applies; so let $\Delta' \ge 2$. For an integer $\kappa \ge 1$, a κ-pseudorandom measure is one in the sense of [26, Definitions 6.1–6.3], where it is called D-pseudorandom, and $C_0(\kappa)$ is the constant of [26, Proposition 6.4] at level κ. The following lemma follows Green and Tao's construction, averaged over the classes modulo Δ'.

Lemma C.2. *Let $\kappa \ge 1$, let $b_1,\dots,b_t$ be units modulo V_z, and write $b_i = b_i' + W_z e_i$ with $0 \le b_i' < W_z$ and $0 \le e_i < \Delta'$. Let $X \ge 2$, $N = \Delta'(X+1)$ and $C \ge C_0(\kappa\Delta')$, let $N' \in [CN, 2CN]$ be prime, and let ν be the $\kappa\Delta'$-pseudorandom measure on $\mathbb{Z}/N'\mathbb{Z}$ that* [26, Proposition 6.4] *gives for $W = W_z$, with $w = z$, and the residues $b_1',\dots,b_t'$, where $z = z(X) \to \infty$ and $z \le \frac12 \log\log N$, as in Green and Tao's convention for w* [26, §5]. *Put $\nu'(n) = \Delta'^{-1}\sum_{s=0}^{\Delta'-1} \nu(\Delta' n + s)$, with arguments modulo N'. Then*

(i) *ν' is a κ-pseudorandom measure on $\mathbb{Z}/N'\mathbb{Z}$;*

(ii) $1 + \sum_{i=1}^{t} \lambda_{V_z,b_i}(n) \ll_{\kappa,C,\Delta',t} \nu'(n)$ *for all $n \in [X^{3/5}, X]$.*

Proof. Each b_i' is a unit modulo W_z, $V_z n + b_i = W_z(\Delta' n + e_i) + b_i'$, and $\varphi(V_z)/V_z = \varphi(W_z)/W_z$, as V_z and W_z have the same prime factors; so $\lambda_{V_z,b_i}(n) = \lambda_{W_z,b_i'}(\Delta' n + e_i)$. As $N' > \Delta'$ is prime, $y \mapsto \Delta' y + s$ is a bijection of $\mathbb{Z}/N'\mathbb{Z}$.

(i) The mean of ν' is that of ν, $1+o(1)$. For the linear forms condition at level κ [26, Definition 6.2], let $1 \le d \le \kappa$ and $1 \le m \le \kappa$, and let $(\psi_1,\dots,\psi_m)$ be a finite complexity system of affine-linear forms on $\mathbb{Z}^d$ with linear coefficients at most κ in absolute value. Then

$$\mathbb{E}_{n\in(\mathbb{Z}/N'\mathbb{Z})^d} \prod_{i=1}^{m} \nu'(\psi_i(n)) = \Delta'^{-m} \sum_{s_1,\dots,s_m=0}^{\Delta'-1} \mathbb{E}_{n\in(\mathbb{Z}/N'\mathbb{Z})^d} \prod_{i=1}^{m} \nu(\Delta'\psi_i(n) + s_i),$$

and each system $(\Delta'\psi_i + s_i)_i$ has finite complexity and linear coefficients at most $\kappa\Delta'$ in absolute value, so each average is $1+o(1)$ by the linear forms condition for ν at level $\kappa\Delta'$. For the correlation condition at level κ [26, Definition 6.3], let $1 < m \le \kappa$ and $h_1,\dots,h_m \in \mathbb{Z}/N'\mathbb{Z}$, and let τ be the weight of ν for m. Putting $y = \Delta' n$,

$$\mathbb{E}_n \prod_{i=1}^{m} \nu'(n+h_i) = \Delta'^{-m} \sum_{s_1,\dots,s_m=0}^{\Delta'-1} \mathbb{E}_y \prod_{i=1}^{m} \nu(y + \Delta' h_i + s_i) \le \sum_{1\le i<j\le m} \tau'(h_i - h_j),$$

with $\tau'(h) = \sum_{|\sigma|<\Delta'} \tau(\Delta' h + \sigma)$, and $\mathbb{E}\,\tau'^q \le (2\Delta'-1)^q\,\mathbb{E}\,\tau^q \ll_{m,q,\Delta'} 1$ for $1 \le q < \infty$.

(ii) For $n \in [X^{3/5}, X]$, $\Delta' n + e_i \in [\Delta' X^{3/5}, \Delta' X + \Delta' - 1] \subseteq [N^{3/5}, N]$, as $\Delta' \ge 2$ and $X \ge 2$. So [26, Proposition 6.4] gives $\nu(\Delta' n + e_i) \gg 1 + \lambda_{W_z,b_i'}(\Delta' n + e_i) = 1 + \lambda_{V_z,b_i}(n)$, and $\nu'(n) \ge \Delta'^{-1}\nu(\Delta' n + e_i)$. Summing over i gives (ii). □

Use of Lemma C.2. At the appendix's scale, which we write X, take $C \ge \max(20, C_0(\kappa\Delta'))$, with $C\Delta'$ at least the constant C_1 of [26, Proposition 7.1], and N' prime in $[C\Delta'(X+$

$1), 2C\Delta' X]$, as is possible for large X. Then $N' \in [C'X, 2C'X]$ with $C' = C\Delta' \geq 20$, the size that [16, Theorem 5.1] and [26, Proposition 7.1] ask for at scale X. With ν' in place of the appendix's ordinary prime majorant at modulus V_z, the appendix's bound for the interval norms at modulus V_z and its proof of the linear replacement lemma run as written: the Gowers norms of $\nu' - 1$ on $\mathbb{Z}/N'\mathbb{Z}$ of the orders it needs are $o(1)$, by (i) and the expansion of the cube, and (ii) gives the domination with the appendix's fixed factor α. Green and Tao's Proposition 7.1 applies with $C' = C\Delta'$ in place of their C: its error terms already depend on their C, which enters their proof only through $N' = O(N)$ [26, Appendix C], and their condition $C \leq O_{s,t,d,L}(1)$ asks only that C not grow with N, while Δ' is fixed by the field data.

Declarations

Use of AI. This paper and its results were produced by an AI research system that the author designed, built and directs, running on Anthropic's Claude Opus 5.5 in Claude Code and OpenAI's GPT-6.2 Astra in Codex. The author chooses the problems and prioritizes the work. Separate AI agents checked each result, and a second program confirmed the computations the proofs use, with any exceptions listed in the public deposit. The system also searched the literature and checked the citations against reliable sources. The author read the paper, reran the computations from the deposit and takes full responsibility for all of the paper's contents.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [30].

References

1. Levent Alpöge, *Modularity and effective Mordell I*, 2021, Preprint, arXiv:2109.07917v2.
2. Levent Alpöge, Manjul Bhargava, Wei Ho, and Ari Shnidman, *Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field*, Invent. Math. **243** (2026), no. 3, 1129–1139, doi:10.1007/s00222-025-01392-3.
3. James Arthur and Laurent Clozel, *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies, vol. 120, Princeton University Press, Princeton, NJ, 1989.
4. Srinath Baba and Håkan Granath, *Genus 2 curves with quaternionic multiplication*, Canad. J. Math. **60** (2008), no. 4, 734–757, doi:10.4153/CJM-2008-033-7.
5. Manjul Bhargava and Ashay Burungale, *A Diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$*, 2026, Preprint, arXiv:2611.16130v2.
6. Tim Browning and Daniel Loughran, *Sieving rational points on varieties*, Trans. Amer. Math. Soc. **371** (2019), no. 8, 5757–5785, doi:10.1090/tran/7514.
7. Tim D. Browning and D. Roger Heath-Brown, *The geometric sieve for quadrics*, Forum Math. **33** (2021), no. 1, 147–165, doi:10.1515/forum-2020-0074.
8. Kevin Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), no. 3, 591–612, doi:10.1215/S0012-7094-97-08719-6.
9. Henri Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468, doi:10.24033/asens.1512.
10. Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735, doi:10.5802/jtnb.516.
11. Lilybelle Cowland Kellock and Vladimir Dokchitser, *Root numbers and parity phenomena*, 2023, Preprint, arXiv:2303.07883v1.
12. David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., John Wiley & Sons, Hoboken, NJ, 2013.
13. Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389, Lecture Notes in Math., vol. 244, Springer, Berlin, 1971, pp. 123–165.
14. Jan Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236, doi:10.1090/S0002-9947-1980-0549163-X.

15. Jan Denef and Leonard Lipshitz, *Diophantine sets over some rings of algebraic integers. II*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391, doi:10.1112/jlms/s2-18.3.385.
16. Pandelis Dodos and Vassilis Kanellopoulos, *Uniformity norms, their weaker versions, and applications*, Acta Arith. **203** (2022), 251–270, cited from arXiv:1610.00487v4.
17. Tim Dokchitser and Vladimir Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64, doi:10.1515/crelle.2011.060.
18. Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, doi:10.1007/BF01388432; erratum, Invent. Math. **75** (1984), 381.
19. Christopher Frei and Magdaléna Tinková, *Linear constellations in primes with arithmetic restrictions*, 2025, Preprint, with an appendix by C. Frei, J. König and M. Tinková, arXiv:2408.17441v3.
20. Éric Gaudron and Gaël Rémond, *Polarisations et isogénies*, Duke Math. J. **163** (2014), no. 11, 2057–2108, doi:10.1215/00127094-2782528.
21. Toby Gee, *A modularity lifting theorem for weight two Hilbert modular forms*, Math. Res. Lett. **13** (2006), no. 5, 805–811, doi:10.4310/MRL.2006.v13.n5.a10; cited from arXiv:math/0601515v2, which includes the erratum.
22. ———, *Errata to "A modularity lifting theorem for weight two Hilbert modular forms"*, Math. Res. Lett. **16** (2009), no. 1, 57–58, doi:10.4310/MRL.2009.v16.n1.a6.
23. Ben Green and Terence Tao, *The Möbius function is strongly orthogonal to nilsequences*, Ann. of Math. (2) **175** (2012), no. 2, 541–566, doi:10.4007/annals.2012.175.2.3.
24. ———, *The quantitative behaviour of polynomial orbits on nilmanifolds*, Ann. of Math. (2) **175** (2012), no. 2, 465–540, doi:10.4007/annals.2012.175.2.2.
25. Ben Green, Terence Tao, and Tamar Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*, Ann. of Math. (2) **176** (2012), no. 2, 1231–1372, doi:10.4007/annals.2012.176.2.11.
26. Benjamin Green and Terence Tao, *Linear equations in primes*, Ann. of Math. (2) **171** (2010), no. 3, 1753–1850, doi:10.4007/annals.2010.171.1753.
27. Hans Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. **5** (1934), 150–160.
28. Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer, New York, 1990, doi:10.1007/978-1-4757-2103-4.
29. Hervé Jacquet and Robert P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Mathematics, vol. 114, Springer, Berlin, 1970.
30. Manvir Jaswal, *Programs and data for "Diophantine definitions of $\mathbb{Z}$ in totally real fields from rank-one elliptic curves"*, 2026, Zenodo, doi:10.5281/zenodo.24520749.
31. ———, *A proof that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ through congruent-number twists*, 2026, Preprint, Zenodo, doi:10.5281/zenodo.24135589.
32. Ariyan Javanpeykar, *Polynomial bounds for Arakelov invariants of Belyi curves*, Algebra Number Theory **8** (2014), no. 1, 89–140, doi:10.2140/ant.2014.8.89.
33. Mark Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180, doi:10.4007/annals.2009.170.1085.
34. Jochen Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. (2) **183** (2016), no. 1, 73–93, doi:10.4007/annals.2016.183.1.2.
35. Peter Koymans and Carlo Pagano, *Hilbert's tenth problem via additive combinatorics*, J. Amer. Math. Soc. **40** (2027), 195–234, doi:10.1090/jams/1081; cited from arXiv:2412.01768v3.
36. Alexander Kozachinskiy, Hector Pasten, and Xavier Vidaux, *Why should $\mathbb{Z}$ be Diophantine in $\mathbb{Q}$?*, 2026, Preprint, arXiv:2611.17124v1.
37. Yi-Hsuan Lin and Yifan Yang, *Quaternionic loci in Siegel's modular threefold*, Math. Z. **295** (2020), 775–819, doi:10.1007/s00209-019-02372-z.
38. Yuri Matiyasevich, *Diophantine representation of enumerable predicates*, Math. USSR-Izv. **5** (1971), no. 1, 1–28, doi:10.1070/IM1971v005n01ABEH001004.
39. Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575, doi:10.1007/s00222-010-0252-0.
40. ———, *Diophantine stability*, Amer. J. Math. **140** (2018), no. 3, 571–616, with an appendix by Michael Larsen; doi:10.1353/ajm.2018.0014; cited from arXiv:1503.04642v3.
41. James S. Milne, *Abelian varieties*, 2008, Course notes, v2.00, https://www.jmilne.org/math/CourseNotes/av.html.
42. Takayoshi Mitsui, *Generalized prime number theorem*, Japan. J. Math. **26** (1956), 1–42.

43. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, Berlin, 2008, cited from the electronic edition, version 2.3 (2020).
44. OpenAI, *Hilbert's tenth problem over the rational numbers*, 2026, Preprint, October 6, 2026, https://github.com/openai/math, commit 3014888, folder `preprints/Hilberts-tenth-problem-over-the-rational-numbers-October-6-2026`.
45. *PARI/GP, version 2.17.3*, 2026, The PARI Group, Université de Bordeaux, https://pari.math.u-bordeaux.fr.
46. Jennifer Park, *A universal first-order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), no. 5, 961–980, doi:10.4310/MRL.2013.v20.n5.a12.
47. Hector Pasten and Xavier Vidaux, *On Hilbert's tenth problem for number fields*, 2026, Preprint, arXiv:2611.24748v1.
48. Fabien Pazuki, *Theta height and Faltings height*, Bull. Soc. Math. France **140** (2012), no. 1, 19–49, doi:10.24033/bsmf.2623.
49. Thanases Pheidas, *An effort to prove that the existential theory of* $\mathbb{Q}$ *is undecidable*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 237–252, doi:10.1090/conm/270/04376.
50. Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42, doi:10.1007/3-540-45455-1_4.
51. ———, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682, doi:10.1353/ajm.0.0057.
52. Kenneth A. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, Algebra and Topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79.
53. Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114, doi:10.2307/2266510.
54. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
55. Alexandra Shlapentokh, *Hilbert's tenth problem: Diophantine classes and extensions to global fields*, New Mathematical Monographs, vol. 7, Cambridge University Press, Cambridge, 2007, doi:10.1017/CBO9780511542954.
56. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, doi:10.1007/978-0-387-09494-6.
57. Christopher Skinner, *A note on the p-adic Galois representations attached to Hilbert modular forms*, Doc. Math. **14** (2009), 241–258.
58. Zhi-Wei Sun, *48 unknowns for Hilbert's tenth problem over the rationals*, 2026, Preprint, arXiv:2610.20691v3.
59. ———, $\mathbb{Z}$ *is diophantine over* $\mathbb{Q}$ *with 26 unknowns*, 2026, Preprint, arXiv:2611.14605v2.
60. ———, *On Hilbert's tenth problem over quadratic fields*, 2026, Preprint, arXiv:2611.25002v2.
61. Terence Tao and Tamar Ziegler, *Polynomial patterns in the primes*, Forum Math. Pi **6** (2018), e1, doi:10.1017/fmp.2017.3.
62. John Tate, *p-divisible groups*, Proceedings of a Conference on Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183.
63. Jesse Thorner and Asif Zaman, *An explicit bound for the least prime ideal in the Chebotarev density theorem*, Algebra Number Theory **11** (2017), no. 5, 1135–1197, doi:10.2140/ant.2017.11.1135.
64. John Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, 2021, cited from the open revised edition, version 1.0.7u.
65. Jérôme von Buhren, *Borne de hauteur semi-effective pour le problème de Mordell–Lang dans une variété abélienne*, J. Théor. Nombres Bordeaux **29** (2017), no. 1, 307–320, doi:10.5802/jtnb.981.
66. Rafael von Känel, *The effective Shafarevich conjecture for abelian varieties of* GL_2*-type*, Forum Math. Sigma **9** (2021), Paper No. e39, 29 pp., doi:10.1017/fms.2021.29.
67. David Zywina, *Rank one elliptic curves and rank stability*, 2025, Preprint, arXiv:2505.16960v1.
68. ℤℚ Diophantine Project contributors, $\mathbb{Z}$ *is Diophantine in* $\mathbb{Q}$*, Version 13*, 2026, Manuscript, November 7, 2026, https://github.com/elliotglazer/diophantine-z-q, commit 9c0b3ab.
69. ———, $\mathbb{Z}$ *is Diophantine in* $\mathbb{Q}$*, Version 15*, 2026, Manuscript, November 10, 2026, https://github.com/elliotglazer/diophantine-z-q/releases/tag/quartic-222-version-15.

70. ———, $\mathbb{Z}$ *is Diophantine in* $\mathbb{Q}$*, Version 19*, 2026, Manuscript, November 16, 2026, https://github.com/elliotglazer/diophantine-z-q, commit 86b8326.

Toronto, Canada
Email address: manvirjaswal@icloud.com
URL: https://manvirjaswal.github.io