hexagon:2611.01263v2

$\mathbb{Z}$ IS DIOPHANTINE IN EVERY REAL QUADRATIC FIELD

MANVIR JASWAL

Abstract. We prove that $\mathbb{Z}$ is Diophantine in every real quadratic field, so that Hilbert's tenth problem over each of them has a negative answer; for $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ this is due to Sun. We let the curve in Sun's construction vary with the field. For each odd squarefree $d > 1$ we build a curve $y^2 = x^3 - Ax$ over $\mathbb{Q}(\zeta_8)$ of $\mathbb{Z}[i]$-rank one whose twist by d has rank zero, from prime elements in a linear pattern found with Kai's estimates, so that the rank stays one over $\mathbb{Q}(\zeta_8, \sqrt{d})$. Run on such a curve, Sun's construction proves that $\mathbb{Z}$ is Diophantine in a totally real Galois field K with $\sqrt{3} \notin K$ and $K \cap \mathbb{Q}(\zeta_8) = \mathbb{Q}$ whenever the rank is one over $K(\zeta_8)$ as well, with conditions on torsion and quadratic characters; this gives $\mathbb{Q}(\sqrt{2d})$ and, for $d \neq 3$, $\mathbb{Q}(\sqrt{d})$. With two marked primes the same descents give $\mathbb{Q}(\sqrt{5a}, \sqrt{13b})$ for positive odd squarefree a and b prime to 65.

Contents

1. Introduction 1
2. The coefficient 5
3. The certificate 11
4. Soundness 18
5. Completeness 19
6. Proofs of Theorems 1.5 and 1.1 24
7. Proof of Theorem 1.2 25
Declarations 26
References 26

1. Introduction

A subset S of a commutative ring R is *Diophantine in* R if there are $k \geq 0$ and $f \in \mathbb{Z}[X, Y_1, \ldots, Y_k]$ such that, for every $a \in R$, $a \in S$ if and only if $f(a, y_1, \ldots, y_k) = 0$ for some $y_1, \ldots, y_k \in R$. Hilbert's tenth problem over R asks for an algorithm that decides whether a given polynomial with integer coefficients has a zero with coordinates in R. Over $\mathbb{Z}$ there is none, by Matiyasevich's theorem [9], which completed work of Davis, Putnam and Robinson. If $\mathbb{Z}$ is Diophantine in a field K with a real embedding, there is none over K either: replacing each integer unknown by an unknown in K subject to a Diophantine definition of $\mathbb{Z}$ turns a system of equations over $\mathbb{Z}$ into one over K, and over a real field a system is equivalent to one equation, a sum of squares.

Date: November 28, 2026.

2020 *Mathematics Subject Classification.* Primary 11U05; Secondary 03D35, 11G05, 11G15.

Key words and phrases. Hilbert's tenth problem, Diophantine sets, real quadratic fields, elliptic curves, complex multiplication, prime elements.

For rings of integers the problem is settled. Koymans and Pagano proved that $\mathbb{Z}$ is Diophantine in the ring of integers of every number field [8, Theorem 1.2], so that Hilbert's tenth problem over each of these rings has a negative answer, which Alpöge, Bhargava, Ho and Shnidman also proved [1, Corollary 1.2]. Both proofs construct curves, or abelian varieties, of positive rank whose rank does not grow in a quadratic extension. Poonen proved that an elliptic curve of rank one over a number field and over a finite extension of it makes the ring of integers of the smaller field Diophantine in that of the larger [13], and Shlapentokh that the same holds for a curve of equal positive rank over both fields [15].

Over a field, a Diophantine definition of $\mathbb{Z}$ must also exclude the elements whose denominators are divisible only by large primes. Over $\mathbb{Q}$, after OpenAI's proof that Hilbert's tenth problem has a negative answer [11], Glazer and collaborators turned that proof into a Diophantine definition of $\mathbb{Z}$ [18], and Bhargava and Burungale proved that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ [2, Theorem A]. Pasten and Vidaux proved that $\mathbb{Z}$ is Diophantine in every quadratic field over which the *abc* conjecture holds [12, Corollary 1.2]. Sun proved that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ [17, Theorems 1.2–1.4], by a construction that reads integers off as multiples of one point on an elliptic curve E over a real quadratic field $F \not\subseteq K$, of rank one over F and over KF. Our earlier paper [4] carries his construction to every totally real field K over which one of four curves of this kind has rank one over KF, with torsion killed by 2 and $2E(KF) \subseteq E(F)$.

Theorem 1.1. *For every squarefree integer $D > 1$, $\mathbb{Z}$ is a Diophantine subset of $K = \mathbb{Q}(\sqrt{D})$: there are an integer $k \geq 1$ and a polynomial $\mathbf{F} \in \mathbb{Z}[X, Y_1, \dots, Y_k]$ such that, for every $x \in K$,*

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

This is the case of real quadratic fields of Sun's conjecture that $\mathbb{Z}$ is Diophantine in every number field [17, Conjecture 1.5].

Why the curve changes with D. Sun's construction needs, for $K = \mathbb{Q}(\sqrt{D})$, a curve $E\colon y^2 = x^3 - Ax$ over a number field $F \not\subseteq K$, with complex multiplication by $\mathbb{Z}[i]$, rank one over F and over KF, and conditions on torsion. If F is real quadratic and E is fixed, the rank of $E(F(\sqrt{D}))$ is that of $E(F)$ plus that of the twist of E by D, and the twist has to be shown to have rank zero. A descent does this for the D it reaches, and in our earlier paper these are families of fields [4, Theorem 1.2]. For some curves no 2-descent can do it. For Sun's curve over $\mathbb{Q}(\sqrt{3})$ and every odd D, and for every curve $y^2 = x^3 - c^2x$ over a real quadratic field F with $c \in F^\times$ when $D \equiv \pm 1 \pmod 8$, provided $\sqrt{D} \notin F$, the 2^∞-Selmer rank over $F(\sqrt{D})$ is even [4, Remark 12.16], so a 2-descent cannot show that the rank there is one.

We therefore let the coefficient depend on D, and we take $F = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$. Throughout, $\zeta = e^{\pi i/4}$, $i = \zeta^2$, $F = \mathbb{Q}(\zeta)$, $\mathcal{O} = \mathbb{Z}[\zeta]$ and $\lambda = 1 - \zeta$, so that $\sqrt{2} = \zeta - \zeta^3$ lies in F. For $A \in \mathcal{O} \setminus \{0\}$ let

$$E_A\colon y^2 = x^3 - Ax \quad \text{over } F, \qquad T = (0, 0). \tag{1.1}$$

The automorphism $[i](x, y) = (-x, iy)$ of E_A is defined over F, so $E_A(M)$ is a $\mathbb{Z}[i]$-module for every field $M \supseteq F$; we speak of its $\mathbb{Z}[i]$-*rank*, and the integers the construction reads off become Gaussian integers. The twist of E_A by $d \in F^\times$ is E_{d^2A}, again a curve of the family.

The field F is chosen for four properties. As $[i]$ is defined over F, $1+i$ is an endomorphism of degree 2 whose Selmer group bounds the $\mathbb{Z}[i]$-rank, and, for the coefficients we construct, the descent of every twist E_{d^2A} by an odd integer d has the same local conditions at λ (Lemma 2.4(a)). As $\sqrt{2} \in F$, the fields $K = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}(\sqrt{2d})$ give the same field

$KF = F(\sqrt{d})$ and the same twist, and $F \cap \mathbb{Q}(\sqrt{D}) = \mathbb{Q}$ for every $D \neq 2$. The automorphism $\sigma\colon \zeta \mapsto -\zeta$ fixes i and exchanges the two complex places of F and the two primes of F above a Gaussian prime $\pi \equiv 9 \pmod{16}$; it takes the place of the Galois conjugation of Sun's real quadratic base, and as it commutes with $[i]$, the Gaussian labels survive it. Finally, $\mathcal{O}$ has class number one and one prime λ above 2, so a class in $F^\times/F^{\times 2}$ with even valuation outside finitely many primes is a product of the classes of units and of generators of these primes, and the dyadic conditions sit at one place, where they depend only on residues modulo 32.

The idea. For each odd squarefree $d > 1$ we construct a coefficient $A = A(d)$ such that E_A has $\mathbb{Z}[i]$-rank one over F, its twist by d has $\mathbb{Z}[i]$-rank zero over F, its torsion over $F(\sqrt{d})$ is $\{O, T\}$, and A is a square modulo exactly one of the two primes of F above each Gaussian prime that the construction selects (Theorem 1.4). We prove that Sun's construction runs with any coefficient that has these properties, over $K = \mathbb{Q}(\sqrt{2d})$ and, for $d \neq 3$, over $K = \mathbb{Q}(\sqrt{d})$; Theorem 1.5 states what it needs over every totally real Galois field K with $K \cap F = \mathbb{Q}$ and $\sqrt{3} \notin K$. We construct $A(d)$ by the method of Koymans and Pagano [8, §§1.3, 5.1–5.2]. A coefficient made of linear forms carries a point that can be written down, Kai's estimates for linear patterns of prime elements [6] make the forms take prime values in prescribed residue classes, and the Selmer groups are then decided by congruences alone. This is the strategy by which Koymans and Pagano, and Zywina with a twist of rank zero, obtain curves of rank exactly one [7, Theorem 1.3], [19, Theorem 1.5]. The nearest construction is Savoie's, of curves $y^2 = x^3 - Ax$ over $\mathbb{Q}(i)$ with j-invariant 1728 and rank 2 from Gaussian primes in a linear pattern [14, Theorem 1.2]. Our forms are u, v and $w = (u - v)/\lambda$, and

$$A = -4uv(u - v)^2, \qquad G = \big(2iu(u - v),\, (2 - 2i)u(u - v)^2\big) \in E_A(F); \tag{1.2}$$

the point lies on E_A because $x^2 - A = -4u(u - v)^3$ at $x = 2iu(u - v)$, and $-8i = (2 - 2i)^2$. When u, v and w are prime, the descents by $1 + i$ over F see only the primes above 2, uvw and d. At λ the local conditions depend only on u and v modulo 32, so we fix these residues; at a prime above d they depend on the residue of v/u; and at u, v and w the local images are generated by the classes of T and G, so no quadratic symbol between u, v and w enters. At one prime above d we make A a square and the abscissa of G a non-square, and Hilbert reciprocity then removes the class of G from the Selmer group of the twist by d, while E_A keeps it.

For the fields K of Theorem 1.2, KF is biquadratic over F, so three twists of E_A must have rank zero. We mark one prime above 5 and one above 13, the two smallest primes $\equiv 5 \pmod 8$, so that $2 + i$ and $3 - 2i$ stay prime in F and their product $8 - i$ is a square at λ; the same descents then give rank zero for the twists by $5a$ and $13b$, and, through $8 - i$, for their product.

Theorem 1.2. *Let a and b be positive odd squarefree integers prime to 65. Then $\mathbb{Z}$ is Diophantine in $\mathbb{Q}(\sqrt{5a}, \sqrt{13b})$.*

Corollary 1.3. *For every real quadratic field K, and for every field K of Theorem 1.2, there is no algorithm that decides, given a polynomial over K in any number of variables, whether it has a zero with coordinates in K.*

Proof. By Theorems 1.1 and 1.2 and the reduction recalled in the first paragraph, as K is real. □

The coefficient is given by the following theorem.

Theorem 1.4. *For every odd squarefree integer $d > 1$ there are prime elements u, v, w of $\mathcal{O}$ with $u - v = \lambda w$, whose absolute norms $\mathrm{N}\,u$, $\mathrm{N}\,v$, $\mathrm{N}\,w$ are distinct rational primes prime to $2d$, such that $A = -4uv(u-v)^2$ has the following properties.*

(a) *$E_A(F)$ has $\mathbb{Z}[i]$-rank one, and the point G of (1.2) has infinite order; $E_{d^2A}(F)$ has $\mathbb{Z}[i]$-rank zero. The Selmer groups of the endomorphism $1+i$ of E_A and of E_{d^2A} over F have dimensions 2 and 1 over $\mathbb{F}_2$.*

(b) *$E_A(F(\sqrt{d}))_{\mathrm{tors}} = \{O, T\}$.*

(c) *If π is a Gaussian prime with $\pi \equiv 9 \pmod{16}$, $\pi \equiv 1+i \pmod{\mathrm{N}\,u\,\mathrm{N}\,v}$ and $\mathrm{N}\,\pi \neq \mathrm{N}\,w$ (that is, w lies above neither π nor $\bar{\pi}$), then A is a unit at the two primes of F above π and a square modulo exactly one of them.*

The construction is Sun's [17, §§9, 10, 12, 13], and we write it out over F, for a totally real Galois field K of any degree and general A, in the form we use (Sections 3, 4, 5 and 6). It reads the coefficient in three places, and the hypotheses of the next theorem are what each of them needs. Its quantifiers run over the points of $2E_A(L)$, $L = KF$, which hypotheses (i) and (ii) below make a free $\mathbb{Z}[i]$-module of rank one generated by a point of $E_A(F)$. Its completeness proof selects Gaussian primes π and needs an index h divisible by the order of the reduction of E_A at one prime of F above each π and congruent to a fixed even integer modulo the order at the other. These orders are $\mathrm{N}(\pi \mp 1)$ where A is a square and $\mathrm{N}(\pi \mp i)$ where it is not (Lemma 5.1), and the prime pattern makes orders of the two kinds prime to each other at odd primes; hypothesis (iii) puts one prime of each kind above every selected π, so the congruences can be met together. And the primes dividing $\mathrm{N}_{F/\mathbb{Q}}(A)$ join a finite set of primes that the tests leave aside.

Theorem 1.5. *Let K be a totally real Galois number field of degree n with $K \cap F = \mathbb{Q}$ and $\sqrt{3} \notin K$, put $L = KF$, let $A \in \mathcal{O} \setminus \{0\}$, and let M_A be the product of the odd primes other than 5 and 7 that divide $\mathrm{N}_{F/\mathbb{Q}}(A)$. Suppose that*

(i) *E_A has $\mathbb{Z}[i]$-rank one over F and over L;*

(ii) *$E_A(L)_{\mathrm{tors}} = \{O, T\}$;*

(iii) *for every Gaussian prime π with $\pi \equiv 9 \pmod{16}$ and $\pi \equiv 1+i \pmod{M_A}$ whose norm is prime to $\mathrm{N}_{F/\mathbb{Q}}(A)$, A is a square modulo exactly one of the two primes of F above π.*

Then $\mathbb{Z}$ is Diophantine in K.

The hypothesis $\sqrt{3} \notin K$ is there because the height bound on the tube (Theorem 3.7) needs a prime $q \equiv 7 \pmod{12}$ with a prime of K of odd residue degree above it; such q are inert in $\mathbb{Q}(\sqrt{3})$, so if $\sqrt{3} \in K$ every prime of K above them has even residue degree. And M_A leaves out 5 and 7 because the prime pattern fixes π itself modulo 25 and modulo 7, as $\pi \equiv 6 \pmod{25}$ and $\pi \equiv 1 + 3i \pmod{7}$ (Theorem 5.2(i)), so hypothesis (iii) can ask $\pi \equiv 1 + i$ only modulo the other odd primes of $\mathrm{N}_{F/\mathbb{Q}}(A)$.

For $D \notin \{2, 3\}$, Theorem 1.1 follows from Theorems 1.4 and 1.5 with d the odd part of D, as $\sqrt{2} \in F$; we give the proof at the end of Section 6. The polynomial $\mathbf{F}$ exists, but the proof is ineffective, through the constants H and κ of the height bound of our earlier paper [4, Theorem 1.6], on which the integers m and M of the certificate (Section 3.5) depend. The prime pattern [4, Theorem 4.3] only supplies witnesses for each integer. For a given d a triple u, v, w can be found by a finite search, since the proof of Theorem 1.4 asks of it only primality and congruences. We do not count the unknowns.

The plan. Section 2 proves Theorem 1.4. Sections 3, 4, 5 and 6 prove Theorem 1.5 for any coefficient A, and the end of Section 6 deduces Theorem 1.1 from Theorems 1.4 and 1.5. Section 7 proves Theorem 1.2 from the lemmas of Section 2.4 and Theorem 1.5. From our earlier paper we take the height bound on the tube [4, Theorem 1.6], with lemmas on the tube, the pole predicate [4, Lemmas 5.1 and 5.3] and the four-unit prime pattern [4, Theorem 4.3].

Computations. The proofs of Theorems 1.4 and 1.2 use one computation at the prime above 2, of square classes and Hilbert symbols in the completion of F at λ (Lemma 2.3), which Lemma 2.4 carries to every pair of prime elements with the residues modulo 32 that we fix. We made it with the exact local routines of PARI/GP and checked it in Python by removing valuations and testing units modulo λ^9. The deposit [5] holds the programs and their outputs.

2. The coefficient

We prove Theorem 1.4, with $u \equiv u_0$ and $v \equiv v_0 \pmod{32}$, where

$$u_0 = \zeta^3 - 3\zeta^2 + 3\zeta - 2, \qquad v_0 = 3 - \zeta - \zeta^2.$$

The local conditions of the two descents are read off a finite computation at λ for u_0 and v_0, carried to every such u and v, and fixed at the primes above d by residues of u and v. In this section $\mathfrak{p}$ denotes a prime of F, $F_\mathfrak{p}$ the completion, $v_\mathfrak{p}$ its normalized valuation, so that $v_\lambda(2) = 4$, and $(a/\mathfrak{p})$ the quadratic residue symbol of a $\mathfrak{p}$-unit a at an odd $\mathfrak{p}$. For a field M and $b \in M^\times$, $[b]$ is the class of b in $M^\times/M^{\times 2}$. Since $-1 = i^2$, $2i = (1+i)^2$ and $-4 = (1+i)^4$ are squares in F, we use freely that $[-b] = [2ib] = [-4b] = [b]$. The field F has class number one, as its Minkowski bound $\frac{4!}{4^4}\left(\frac{4}{\pi}\right)^2\sqrt{256}$ is less than 3 and (λ) is the only prime of norm 2. Its unit group $\mathcal{O}^\times$ is generated by ζ and $1+\sqrt{2}$: for a unit c, $c/\bar{c}$ is a power of ζ that is $\equiv 1 \pmod{\lambda^2}$, as complex conjugation is trivial on $\mathcal{O}/\lambda^2\mathcal{O}$, so $c/\bar{c} = \zeta^{2k}$ and $\zeta^{-k}c = \pm(1+\sqrt{2})^n$.

For $a, b \in F_\mathfrak{p}^\times$, $(a,b)_\mathfrak{p}$ is the Hilbert symbol. If $F_\mathfrak{p}(\sqrt{a})/F_\mathfrak{p}$ is unramified and b is a unit, then $(a,b)_\mathfrak{p} = 1$; and at an odd $\mathfrak{p}$ at which a is a unit, $(a,b)_\mathfrak{p} = (a/\mathfrak{p})^{v_\mathfrak{p}(b)}$ [10, Chapter III, Theorem 4.4(d) and Proposition 1.2]. For $a, b \in F^\times$ Hilbert reciprocity reads $\prod_\mathfrak{p}(a,b)_\mathfrak{p} = 1$, as F has no real place.

2.1. Descent by $1+i$.

For $B \in F^\times$ let E_B and T be as in (1.1). The kernel of $[1+i]$ on E_B is $\{O, T\}$: $[1+i]V = O$ means $[i]V = -V$, that is $(-x, iy) = (x, -y)$.

Lemma 2.1. *Let $B \in F^\times$ and let $M \supseteq F$ be a field.*

(a) *There is an injective homomorphism $\delta_M \colon E_B(M)/(1+i)E_B(M) \to M^\times/M^{\times 2}$ with $\delta_M(O) = 1$, $\delta_M(T) = [B]$ and $\delta_M(V) = [x(V)]$ for $V \neq O, T$.*

(b) *If $B' = Bt^4$ with $t \in M^\times$, then $(x,y) \mapsto (t^2x, t^3y)$ is an isomorphism $E_B \to E_{B'}$ over M that commutes with $[i]$ and carries δ_M for E_B to δ_M for $E_{B'}$.*

Proof. (a) Let $\varphi \colon E_B \to E'$, $E' \colon Y^2 = X^3 + 4BX$, be the isogeny of degree two with kernel $\{O, T\}$ of [16, Proposition X.4.9] (with $a = 0$, $b = -B$). By that proposition and its proof, $E'(M)/\varphi(E_B(M)) \to M^\times/M^{\times 2}$, $(X,Y) \mapsto [X]$, $(0,0) \mapsto [4B]$, is an injective homomorphism. The map $\iota(X,Y) = (X/(2i), Y/(2i(1+i)))$ is an isomorphism $E' \to E_B$ over F, as $(1+i)^4 = -4$. So $\iota \circ \varphi$ is an endomorphism of E_B of degree two with kernel $E_B[1+i]$; it factors through $[1+i]$ [16, Corollary III.4.11], by an automorphism, which is some $[\eta]$ with $\eta^4 = 1$. Hence ι^{-1} carries $(1+i)E_B(M)$ onto $\varphi(E_B(M))$, and $\delta_M(V)$ is the

class of $x(\iota^{-1}V) = 2i\,x(V)$, which is $[x(V)]$; and $\delta_M(T) = [4B] = [B]$. (b) is direct, and $[t^2 x] = [x]$, $[B'] = [B]$. □

For a prime $\mathfrak{p}$ of F write $W_{\mathfrak{p}}(B)$ for the image of $\delta_{F_{\mathfrak{p}}}$. As F has no real place, the Selmer group of $1+i$ on E_B over F is

$$\mathrm{Sel}(B) = \{b \in F^\times/F^{\times 2} :\ b \in W_{\mathfrak{p}}(B) \text{ for every prime } \mathfrak{p} \text{ of } F\},$$

and it contains $\delta_F(E_B(F))$.

Lemma 2.2. *Let $B \in F^\times$ and $\mathfrak{p}$ a prime of F.*

(a) $\#W_{\mathfrak{p}}(B) = 2$ *if $\mathfrak{p}$ is odd, and* $\#W_\lambda(B) = 8$.

(b) *If $\mathfrak{p}$ is odd and $v_{\mathfrak{p}}(B) = 0$, then $W_{\mathfrak{p}}(B)$ is the group of unit classes. If $\mathfrak{p}$ is odd and $v_{\mathfrak{p}}(B)$ is odd, then $W_{\mathfrak{p}}(B) = \{1, [B]\}$.*

(c) *If r is the $\mathbb{Z}[i]$-rank of $E_B(F)$, then $r+1 \le \dim_{\mathbb{F}_2} \mathrm{Sel}(B)$.*

Proof. (a) By Lemma 2.1(b) we may assume B integral at $\mathfrak{p}$. Let R be the valuation ring of $F_{\mathfrak{p}}$, $\mathfrak{m}$ its maximal ideal, p the residue characteristic and $e = v_{\mathfrak{p}}(p)$. For the integral equation of E_B the parameter $\mathfrak{z} = -x/y$ identifies $E_1 = \{O\} \cup \{V : v_{\mathfrak{p}}(x(V)) < 0\}$ with the formal group on $\mathfrak{m}$ [16, Proposition VII.2.2], whose proof uses only that the equation is integral. Fix an integer $s > e/(p-1)$. The formal logarithm ℓ is an isomorphism of the subgroup U of E_1 consisting of the points with $v_{\mathfrak{p}}(\mathfrak{z}) \ge s$ onto $\mathfrak{m}^s$ [16, Theorem IV.6.4(b)], so U is open, of finite index in the compact group $G = E_B(F_{\mathfrak{p}})$. Since $\mathfrak{z}([i]V) = i\,\mathfrak{z}(V)$, the endomorphism $[i]$ of the formal group is $Z \mapsto iZ$, so $\ell(iZ) = i\,\ell(Z)$ [16, Corollary IV.4.3], and $[1+i]$ preserves U and acts on $U \cong \mathfrak{m}^s$ as multiplication by $1+i$. The snake lemma for $0 \to U \to G \to G/U \to 0$, with G/U finite, gives

$$\frac{\#G/(1+i)G}{\#\ker([1+i]|_G)} = \#\,\mathfrak{m}^s/(1+i)\mathfrak{m}^s = \#R/(1+i)R,$$

which is 1 if p is odd and 4 at λ, as $v_\lambda(1+i) = 2$ and the residue field is $\mathbb{F}_2$. The kernel is $\{O, T\}$, and $\delta_{F_{\mathfrak{p}}}$ is injective.

(b) The unit classes form a group of order two. If $v_{\mathfrak{p}}(B) = 0$ and $V = (x, y)$ with $x \ne 0$, then $2v_{\mathfrak{p}}(y) = 3v_{\mathfrak{p}}(x)$ if $v_{\mathfrak{p}}(x) < 0$ and $2v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(x)$ if $v_{\mathfrak{p}}(x) > 0$; so $W_{\mathfrak{p}}(B)$ consists of unit classes, and (a) gives equality. If $v_{\mathfrak{p}}(B)$ is odd, $[B] = \delta(T)$ is a nontrivial class in a group of order two.

(c) As $\mathbb{Z}[i]$ is a principal ideal domain, $E_B(F) \cong \mathbb{Z}[i]^r \oplus \mathcal{T}$ with $\mathcal{T}$ finite, and $\#\mathcal{T}/(1+i)\mathcal{T} = \#\mathcal{T}[1+i] = 2$. So $E_B(F)/(1+i)E_B(F)$ has dimension $r+1$, and δ_F embeds it in $\mathrm{Sel}(B)$. □

2.2. **The prime above 2.** Put $\varepsilon = 1 + \zeta + \zeta^2 = \zeta(1+\sqrt{2})$,

$$A_0 = -4u_0v_0(u_0 - v_0)^2, \qquad X_0 = 2iu_0(u_0 - v_0),$$

the coefficient and the abscissa of G for $(u, v) = (u_0, v_0)$. A unit of F_λ is a square if and only if it is a square modulo λ^9, since if r is a unit with $v_\lambda(r^2 - b) \ge 9 > 2v_\lambda(2r)$, Hensel's lemma gives a square root of b. The 256 elements $1 + c_1\lambda + \cdots + c_8\lambda^8$ with $c_j \in \{0, 1\}$ represent the units of $\mathcal{O}/\lambda^9\mathcal{O}$, and we find that exactly 8 of them are squares. This decides square classes in F_λ, and gives the following facts, with

$$x_1 = \lambda^4(1 + \lambda^3 + \lambda^6), \qquad x_2 = \lambda^5(1 + \lambda^4).$$

Lemma 2.3. (a) *For $k \in \{1, 5\}$ and $j \in \{1, 2\}$, $x_j^3 - k^2A_0x_j$ is a nonzero square in F_λ, and $[A_0]$, $[x_1]$, $[x_2]$ span a subgroup W_0 of order 8 of $F_\lambda^\times/F_\lambda^{\times 2}$. Hence $W_\lambda(A_0) = W_\lambda(25A_0) = W_0$.*

(b) $[X_0] = [\varepsilon\lambda] = [A_0x_1x_2]$ *in* $F_\lambda^\times/F_\lambda^{\times 2}$, *and the Hilbert symbol* $(X_0, b)_\lambda$ *is* 1 *for every* $b \in W_0$.

(c) *Of the sixteen classes* $[\zeta^{a_1}\varepsilon^{a_2}\lambda^{a_3}u_0^{a_4}]$, $a_k \in \{0,1\}$, *in* $F_\lambda^\times/F_\lambda^{\times 2}$, *exactly* [1] *and* $[\varepsilon\lambda]$ *lie in* W_0.

(d) $(\varepsilon\lambda/u_0) = ((1+i)/u_0) = -1$ *and* $((1+i)/v_0) = 1$.

Proof. In (a)–(c) we find the stated squares, that the eight products of A_0, x_1, x_2 are pairwise inequivalent, the classes in (b) and (c), and $(X_0, g)_\lambda = 1$ for $g = A_0, x_1, x_2$. In (a), $[k^2A_0] = [A_0]$ is $\delta(T)$, and $[x_j]$ is δ of a point of $E_{k^2A_0}(F_\lambda)$ with abscissa x_j; so these classes lie in $W_\lambda(k^2A_0)$, which has order 8 by Lemma 2.2(a), and therefore span it. The second assertion of (b) follows by bilinearity. (d) The prime (u_0) has norm 17, and $u_0 = (\zeta-1)^3 - 1$ vanishes at $\zeta = 2$ in $\mathbb{F}_{17}$, where $2^4 = -1$; so the residue field of (u_0) is $\mathbb{F}_{17}$ with $\zeta \mapsto 2$; there $\varepsilon\lambda = 1 - \zeta^3 \mapsto -7$ and $1 + i \mapsto 5$, and neither is a square modulo 17. The prime (v_0) has norm 113, and modulo 113, $18^4 \equiv -1$ and $3 - 18 - 18^2 = -3 \cdot 113$, so the residue field of (v_0) is $\mathbb{F}_{113}$ with $\zeta \mapsto 18$, and $1 + i \mapsto 325 \equiv 9 \cdot 11$; by quadratic reciprocity $(11/113) = (113/11) = (3/11) = 1$. □

Lemma 2.4. *Let* $u, v \in \mathcal{O}$ *be prime elements with* $u \equiv u_0$ *and* $v \equiv v_0 \pmod{32}$, *and put* $w = (u-v)/\lambda$, $A = -4uv(u-v)^2$ *and* $X = 2iu(u-v)$.

(a) A/A_0 *is a fourth power and* X/X_0, u/u_0 *are squares in* F_λ. *Hence* $W_\lambda(A) = W_\lambda(d^2A) = W_0$ *for every odd integer* d, $[X] = [X_0]$, $(X, b)_\lambda = 1$ *for* $b \in W_0$, *and Lemma 2.3(c) holds with* u *in place of* u_0.

(b) $(\varepsilon\lambda/u) = ((1+i)/u) = -1$ *and* $((1+i)/v) = 1$.

Proof. (a) As $(32) = (\lambda^{20})$ and $u_0, v_0, w_0 = (u_0 - v_0)/\lambda$ are units at λ (of norms 17, 113, 433), the ratios u/u_0, v/v_0 and w/w_0 are $\equiv 1 \pmod{\lambda^{19}}$. If $t \equiv 1 \pmod{\lambda^{19}}$, Hensel's lemma gives r with $r^2 = t$ and $v_\lambda(r-1) \geq 15$, and then s with $s^2 = r$; so t is a fourth power. Now $A/A_0 = (u/u_0)(v/v_0)(w/w_0)^2$ and $X/X_0 = (u/u_0)(w/w_0)$, as $u - v = \lambda w$. An odd integer is ± 1 or ± 5 times a square in $\mathbb{Q}_2$, so $d \in \{1,5\} \cdot F_\lambda^{\times 2}$, and $d^2A \in \{1, 25\} \cdot A_0 \cdot F_\lambda^{\times 4}$. Lemma 2.1(b) and Lemma 2.3(a), (b) give the rest.

(b) Let $h \in \{\varepsilon\lambda, 1+i\}$. If $(u) = (u_0)$ there is nothing to prove. Otherwise apply Hilbert reciprocity to $(h, u/u_0)$. At λ the factor is 1 by (a). As h is a unit at every odd prime, the factors at odd primes are $(h/\mathfrak{p})^{v_\mathfrak{p}(u/u_0)}$, and the formula reads $(h/u)(h/u_0) = 1$. The same argument gives $((1+i)/v) = ((1+i)/v_0)$, and Lemma 2.3(d) gives the values. □

2.3. **The prime elements.** Let $d > 1$ be an odd squarefree integer and $\mathcal{P}_d$ the set of primes of F above d. For $\mathfrak{p} \in \mathcal{P}_d$ the residue field $k_\mathfrak{p}$ contains the image of μ_8, so $Q_\mathfrak{p} = \#k_\mathfrak{p} \equiv 1 \pmod 8$ and $Q_\mathfrak{p} \geq 9$; let $\chi_\mathfrak{p}$ be its quadratic character. Fix one prime $\mathfrak{p}^* \in \mathcal{P}_d$.

Lemma 2.5. *There are* $t_\mathfrak{p} \in k_\mathfrak{p} \setminus \{0,1\}$, $\mathfrak{p} \in \mathcal{P}_d$, *with* $\chi_{\mathfrak{p}^*}(t_{\mathfrak{p}^*}) = 1$, $\chi_{\mathfrak{p}^*}(1 - t_{\mathfrak{p}^*}) = -1$, *and* $\chi_\mathfrak{p}(t_\mathfrak{p}) = -1$ *for* $\mathfrak{p} \neq \mathfrak{p}^*$.

Proof. For $\mathfrak{p} \neq \mathfrak{p}^*$ take any non-square. At $\mathfrak{p}^*$ write $\chi = \chi_{\mathfrak{p}^*}$, $Q = Q_{\mathfrak{p}^*}$; the number of admissible t is $\frac{1}{4}\sum_{t \neq 0,1}(1 + \chi(t))(1 - \chi(1-t))$. Here $\sum_{t\neq 0,1}\chi(t) = \sum_{t\neq 0,1}\chi(1-t) = -1$, and $\chi(t(1-t)) = \chi(t^{-1} - 1)$, where $t^{-1} - 1$ runs over $k_{\mathfrak{p}^*} \setminus \{0, -1\}$, so $\sum_{t\neq 0,1}\chi(t(1-t)) = -\chi(-1) = -1$. The number is $(Q-1)/4 > 0$. □

Lemma 2.6. *Let* $t_\mathfrak{p} \in k_\mathfrak{p} \setminus \{0,1\}$ *for* $\mathfrak{p} \in \mathcal{P}_d$. *There are prime elements* u, v, w *of* $\mathcal{O}$ *with* $u - v = \lambda w$, $u \equiv u_0$ *and* $v \equiv v_0 \pmod{32}$, $w \equiv 1$ *and* $v \equiv t_\mathfrak{p} u$ *modulo every* $\mathfrak{p} \in \mathcal{P}_d$, *whose absolute norms are three distinct rational primes prime to* $2d$.

Proof. By the Chinese remainder theorem choose $U, V \in \mathcal{O}$ with $U \equiv u_0$, $V \equiv v_0 \pmod{32}$, and $U \equiv \lambda/(1-t_{\mathfrak{p}})$, $V \equiv t_{\mathfrak{p}}\lambda/(1-t_{\mathfrak{p}})$ modulo each $\mathfrak{p} \in \mathcal{P}_d$. Then $U - V \equiv \lambda w_0 \pmod{32}$, so $(U-V)/\lambda \in \mathcal{O}$, and on $\mathcal{O}^2 \cong \mathbb{Z}^8$, in the coordinates of the basis $1, \zeta, \zeta^2, \zeta^3$, we have the affine maps

$$\psi_1(s,t) = U + 32ds, \qquad \psi_2(s,t) = V + 32dt, \qquad \psi_3(s,t) = \frac{U-V}{\lambda} + \frac{32d}{\lambda}(s-t)$$

to $\mathcal{O}$, with $\psi_1 - \psi_2 = \lambda\psi_3$.

Let H be a large integer and $\Omega = [-H, H]^8$, let ρ_F be the residue of $\zeta_F(s)$ at $s = 1$, and let $\Lambda(x) = \log \mathrm{N}\mathfrak{P}$ if $x\mathcal{O} = \mathfrak{P}^k$ with $\mathfrak{P}$ prime and $k \geq 1$, and $\Lambda(x) = 0$ otherwise. Let Λ_{Cr} be Kai's Cramér model of Λ on $\mathcal{O}$ at the level $Q = \exp((\log H)^{1/10})$ [6, §1.2.2 and Definition 5.1]. Fix a norm-length compatible basis of $\mathcal{O}$ [6, Proposition 3.1], and let $\mathcal{X}$ be the set of elements of $\mathcal{O}$ whose coordinates in it lie in $[-R, R]$, for an integer R with $H \leq R \ll_d H$ such that $\psi_j(\Omega \cap \mathbb{Z}^8) \subseteq \mathcal{X}$ for each j. For $N = H$ and $N = R$ we have $\exp((\log N)^{1/100}) < Q < \exp((\log N)^{1/3})$. Both weights are $O_d(\log H)$ on $\mathcal{X}$: there $|\mathrm{N}\, x| \ll R^4$, and the nonzero value of Λ_{Cr} is $\rho_F^{-1} \prod_{p<Q} \prod_{\mathfrak{P}|p} (1 - 1/\mathrm{N}\mathfrak{P})^{-1} \ll \log Q$ by [6, Proposition B.1], as $\mathrm{N}\mathfrak{P} < Q^4$ in this product.

Choose a rational prime p_0 with $4R < p_0 < 9R$ and $p_0 \nmid 2d$, put $\mathcal{G} = \mathcal{O}/p_0\mathcal{O}$, and write $\widetilde{f}$ for the extension by zero to $\mathcal{G}$ of a function f on $\mathcal{X}$. A congruence $z_1 + z_4 \equiv z_2 + z_3 \pmod{p_0}$ between elements of $\mathcal{X}$ is an equality, as their coordinates differ by at most $4R$. So

$$\|\widetilde{f}\|_{U^2(\mathcal{G})}^4 = \frac{\mathfrak{d}(\mathcal{X})}{|\mathcal{G}|^3} \|f\|_{U^2(\mathcal{X})}^4 \leq \|f\|_{U^2(\mathcal{X})}^4,$$

where $\mathfrak{d}(\mathcal{X})$, the number of ordered parallelograms in $\mathcal{X}$, is the denominator of the average that defines $\|f\|_{U^2(\mathcal{X})}$ [6, Definition 2.1, pp. 6–7]. Hence [6, Corollary 9.2] gives $\|\widetilde{\Lambda} - \widetilde{\Lambda}_{\mathrm{Cr}}\|_{U^2(\mathcal{G})} \ll_{d,c} (\log H)^{-c}$ for every $c > 1$.

Reduction modulo p_0 is injective on $\Omega \cap \mathbb{Z}^8$ and on $\mathcal{X}$, so the sum in (2.1) below is p_0^8 times a mean over $\mathcal{G}^2$, in which the indicators of the eight coordinate intervals of Ω are inserted. Each indicator has Fourier coefficients of absolute sum $O(\log p_0)$, since the normalized geometric sum at a frequency r with $0 < |r| \leq (p_0 - 1)/2$ is at most $1/(2|r|)$. We expand the indicators and change variables to $u = \psi_1(s,t)$, $v = \psi_2(s,t)$. As multiplication by $32d$ is invertible on $\mathcal{G}$, each character of (s,t) is a constant times a character of u times a character of v, and we absorb these into the first two factors. With $\widehat{f}(\chi) = \mathbb{E}_x f(x)\overline{\chi(x)}$ and $\chi_*(z) = \chi(z/\lambda)$, Fourier inversion gives

$$\mathbb{E}_{u,v} f(u) g(v) h((u-v)/\lambda) = \sum_{\chi} \widehat{f}(\overline{\chi_*})\, \widehat{g}(\chi_*)\, \widehat{h}(\chi),$$

and the three index maps permute the characters. In each term of the telescoping sum we bound the coefficients of the difference by $\|\widehat{f}\|_\infty \leq (\sum_\chi |\widehat{f}(\chi)|^4)^{1/4} = \|f\|_{U^2(\mathcal{G})}$, and use Cauchy–Schwarz and Parseval for the other two factors; multiplying by a character only permutes the coefficients. So replacing the three weights by Λ_{Cr} costs $O_{d,c}(p_0^8 (\log p_0)^8 (\log H)^{2-c})$, which is $o_d(H^8)$ for $c > 10$.

The linear parts of the ψ_j have images $32d\mathcal{O}$, $32d\mathcal{O}$ and $(32d/\lambda)\mathcal{O}$, of finite index, and kernels $s = 0$, $t = 0$ and $s = t$, no one of which contains another. Their coefficients do not depend on H, so they are eventually below $\exp((\log H)^{1/101})$, and the sixteen faces of Ω have parametrizations with Lipschitz constant $2H$ [6, Definition C.1]. By [6, Proposition 5.2] the sum with the weights Λ_{Cr} is $(2H)^8 \rho_F^{-3} \prod_{p<Q} \beta_p + o_d(H^8)$. At 2 the three values are units at λ, being $\equiv u_0, v_0 \pmod{32}$ and $\equiv w_0 \pmod{\lambda^{19}}$. At $p \mid d$ their residues $\lambda/(1-t_{\mathfrak{p}})$,

$t_\mathfrak{p}\lambda/(1-t_\mathfrak{p})$ and 1 are nonzero at every $\mathfrak{p} \mid p$. For $p \nmid 2d$, $u \equiv 1$ and $v \equiv -1 \pmod p$ give $w \equiv 2/\lambda$. Moreover, for $\mathfrak{p} \mid p \nmid 2d$ with $k = \#\mathcal{O}/\mathfrak{p}$, the residues of u and v at $\mathfrak{p}$ are uniform and independent, and all three values are nonzero at $\mathfrak{p}$ for $(k-1)(k-2)$ pairs, so the factor of $\mathfrak{p}$ in part (2) of that proposition is $k(k-2)/(k-1)^2$. Hence $\beta_p = 1 + O(p^{-2})$ for $p \nmid 2d$, $\prod_p \beta_p > 0$, and

$$\sum_{x \in \Omega \cap \mathbb{Z}^8} \Lambda(\psi_1(x))\Lambda(\psi_2(x))\Lambda(\psi_3(x)) = (2H)^8 \rho_F^{-3} \prod_p \beta_p + o_d(H^8) \gg_d H^8. \tag{2.1}$$

We remove the x at which some $\psi_j(x)$ does not generate a prime of degree one, or two of the norms agree; constants may depend on d. For $x \in \Omega$ every conjugate of $\psi_j(x)$ is $O(H)$, so $\mathrm{N}\,\psi_j(x) \ll H^4$ and each weight is $O(\log H)$. An ideal $\mathfrak{P}^k$ whose norm is not a prime has norm p^e with $e \geq 2$; there are $O(H^2)$ such ideals of norm $\ll H^4$. A nonzero ideal has $O(\log H)$ generators all of whose conjugates are $O(H)$: generators differ by units $\zeta^a(1+\sqrt{2})^n$, and $1+\sqrt{2}$ has absolute values $1+\sqrt{2}$ and $\sqrt{2}-1$ at the two complex places, while the absolute values of a generator lie in $[(cH)^{-1}, cH]$, as its norm is at least 1. A value of ψ_1, ψ_2 or ψ_3 determines s, t or $s-t$, leaving $O(H^4)$ points; so these x contribute $O(H^6 \log^4 H)$ to (2.1). For $j \neq j'$, $\mathrm{N}\,\psi_j(x) - \mathrm{N}\,\psi_{j'}(x)$ is a nonzero polynomial of degree at most 4 on $\mathbb{Z}^8$, since one of the two terms depends on a variable the other does not involve; so it vanishes at $O(H^7)$ points of Ω, which contribute $O(H^7 \log^3 H)$. For large H some x remains, and $(u,v,w) = (\psi_1,\psi_2,\psi_3)(x)$ will do; the three values are units at every prime above $2d$, so their norms are prime to $2d$. □

2.4. **The descents.** In this subsection u, v, w are prime elements of $\mathcal{O}$ with $u - v = \lambda w$, $u \equiv u_0$ and $v \equiv v_0 \pmod{32}$, whose absolute norms are distinct rational primes, and $A = -4uv(u-v)^2$ and $X = x(G) = 2iu(u-v)$ are as in (1.2). Then $A = -4\lambda^2 uvw^2$ and $X = 2i\lambda uw$, so

$$[A] = [uv], \qquad [X] = [\lambda uw], \tag{2.2}$$

$v_\lambda(A) = 10$, and A has valuation 1 at u and v and 2 at w. If $\mathfrak{p}$ is an odd prime of F with $w \equiv 1$ and $v \equiv tu \pmod{\mathfrak{p}}$ for some $t \in k_\mathfrak{p} \setminus \{0,1\}$, and $\chi_\mathfrak{p}$ is the quadratic character of $k_\mathfrak{p}$, then $u - v \equiv \lambda$ gives $u \equiv \lambda/(1-t)$, $A \equiv -4tu^2\lambda^2$ and $X \equiv 2iu\lambda$ modulo $\mathfrak{p}$, and hence

$$\chi_\mathfrak{p}(A) = \chi_\mathfrak{p}(t), \qquad \chi_\mathfrak{p}(X) = \chi_\mathfrak{p}(1-t). \tag{2.3}$$

Lemma 2.7. (a) $\mathrm{Sel}(A) = \{1, [A], [X], [AX]\}$, *of dimension two.*

(b) *If $M \supseteq F$ is a number field unramified over F at (u) and (v), then $E_A(M)_{\mathrm{tors}} = \{O, T\}$.*

(c) *$E_A(F)$ has $\mathbb{Z}[i]$-rank one, and G has infinite order.*

(d) *If π is a Gaussian prime with $\pi \equiv 9 \pmod{16}$, $\pi \equiv 1+i \pmod{\mathrm{N}\,u\,\mathrm{N}\,v}$ and $\mathrm{N}\,\pi \neq \mathrm{N}\,w$, then A is a unit at the two primes of F above π and a square modulo exactly one of them.*

Proof. (a) At odd $\mathfrak{p} \notin \{(u),(v),(w)\}$, $W_\mathfrak{p}(A)$ is the group of unit classes, and at u and v it is $\{1,[A]\}$ (Lemma 2.2(b)). At λ it is W_0 (Lemma 2.4(a)). At w it has order two and contains $\delta(G) = [X]$, of odd valuation; so $W_w(A) = \{1,[X]\}$. Let $b \in \mathrm{Sel}(A)$. Then b has even valuation at every prime other than λ, u, v, w, and as F has class number one and $\mathcal{O}^\times$ is generated by ζ and $\zeta^{-1}\varepsilon = 1+\sqrt{2}$, b is a product of the classes of ζ, ε, λ, u, v, w. By (2.2), $[A]$ has odd valuation at v and even at w, and $[X]$ the reverse. Multiplying b by a product of $[A]$ and $[X]$, which lie in $\mathrm{Sel}(A)$, we obtain $b' \in \mathrm{Sel}(A)$ in the span of $[\zeta]$, $[\varepsilon]$, $[\lambda]$, $[u]$. Its class at λ lies in W_0, so $b' \in \{1,[\varepsilon\lambda]\}$ by Lemma 2.4(a) and Lemma 2.3(c). At u, $\varepsilon\lambda$ is a non-square unit (Lemma 2.4(b)), while $W_u(A) = \{1,[A]\}$ with $[A]$ of odd valuation; so

$b' = 1$. Hence $\mathrm{Sel}(A) = \{1, [A], [X], [AX]\}$, of dimension two, as $[A]$ and $[X]$ are independent by their valuations at v and w.

(b) Let $\mathfrak{u}$ be (u) or (v), p its residue characteristic, $V \in E_A(M)$ a torsion point of order prime to p, and $\mathfrak{U}$ a prime of M above $\mathfrak{u}$; as $M_{\mathfrak{U}}/F_{\mathfrak{u}}$ is unramified, A has valuation 1 in $M_{\mathfrak{U}}$. Let $\alpha^4 = A$. The polynomial $Z^4 - A$ is Eisenstein, so $N = M_{\mathfrak{U}}(\alpha)$ is totally ramified of degree 4 over $M_{\mathfrak{U}}$, and Galois, as $i \in F$; let g be the automorphism with $g(\alpha) = i\alpha$. Over N, $(x, y) \mapsto (x/\alpha^2, y/\alpha^3)$ is an isomorphism of E_A onto E_1, which has good reduction since p is odd. Let Q be the image of V. Since g fixes the coordinates of V, $g(Q) = (-x/\alpha^2,\, iy/\alpha^3) = [i]Q$. As g acts trivially on the residue field, $g(Q)$ and Q have the same reduction, and reduction is injective on the torsion of $E_1(N)$ of order prime to p [16, Proposition VII.3.1(b)]; so $[i]Q = Q$ and $Q \in E_1[1 + i]$. So $V \in \{O, T\}$. As $\mathrm{N}\, u \neq \mathrm{N}\, v$, every torsion point of $E_A(M)$ is a sum of one of order prime to $\mathrm{N}\, u$ and one of order prime to $\mathrm{N}\, v$, and $E_A(M)_{\mathrm{tors}} = \{O, T\}$.

(c) By (b) with $M = F$, $E_A(F)_{\mathrm{tors}} = \{O, T\}$, whose image under δ_F is $\{1, [A]\}$; as $\delta_F(G) = [X]$, G has infinite order. By (a) and Lemma 2.2(c) the $\mathbb{Z}[i]$-rank of $E_A(F)$ is at most one, so it is one.

(d) As $\mathrm{N}\, \pi \equiv 1 \pmod{16}$, π has two primes $\mathfrak{Q}$, $\mathfrak{Q}'$ of F above it, and $\mathrm{N}\, \pi \notin \{\mathrm{N}\, u, \mathrm{N}\, v\}$, as π does not divide $1 + i$; so π is a unit at u, v, w, and A is a unit at $\mathfrak{Q}$, $\mathfrak{Q}'$. Apply Hilbert reciprocity to (A, π). The factor at λ is 1, as $v_\lambda(\pi/9 - 1) \geq 16$ makes π a square in F_λ. The factors at $\mathfrak{Q}$ and $\mathfrak{Q}'$ are $(A/\mathfrak{Q})$ and $(A/\mathfrak{Q}')$, and those at u and v are $(\pi/u) = ((1+i)/u) = -1$ and $(\pi/v) = ((1 + i)/v) = 1$, as $u \mid \mathrm{N}\, u$ and $v \mid \mathrm{N}\, v$ in $\mathcal{O}$ (Lemma 2.4(b)). At w the factor is $(\pi/w)^2 = 1$, and at every other prime both entries are units. So $(A/\mathfrak{Q})(A/\mathfrak{Q}') = -1$. □

Lemma 2.8. *Let $d > 1$ be an odd squarefree integer prime to $\mathrm{N}\, u\, \mathrm{N}\, v\, \mathrm{N}\, w$, with $w \equiv 1$ modulo every $\mathfrak{p} \in \mathcal{P}_d$.*

(a) *d is a square in F_w, and $W_{\mathfrak{p}}(d^2 A) = W_{\mathfrak{p}}(A)$ for every prime $\mathfrak{p} \notin \mathcal{P}_d$. For $\mathfrak{p} \in \mathcal{P}_d$, A is a unit at $\mathfrak{p}$; $W_{\mathfrak{p}}(d^2 A)$ is the group of unit classes if A is not a square in $F_{\mathfrak{p}}$, and $W_{\mathfrak{p}}(d^2 A) = \{1, [da]\}$ if $A = a^2$ with $a \in F_{\mathfrak{p}}$.*

(b) *For $z \in \mathrm{Sel}(d^2 A)$, the product of the symbols $(X, z)_{\mathfrak{p}}$ over the $\mathfrak{p} \in \mathcal{P}_d$ at which A is a square is 1.*

(c) *If A is a square at exactly one $\mathfrak{p}^* \in \mathcal{P}_d$, and X is a non-square unit at $\mathfrak{p}^*$, then $\mathrm{Sel}(d^2 A) = \{1, [A]\}$, and $E_{d^2 A}(F)$ has $\mathbb{Z}[i]$-rank zero.*

Proof. (a) Apply Hilbert reciprocity to (d, w). The factor at w is (d/w), and the factor at $\mathfrak{p} \in \mathcal{P}_d$ is $(w/\mathfrak{p}) = 1$, as $w \equiv 1 \pmod{\mathfrak{p}}$ and $v_{\mathfrak{p}}(d) = 1$. At λ, $d \in \{1, 5\} \cdot F_\lambda^{\times 2}$ (Lemma 2.4(a)), $F_\lambda(\sqrt{5})/F_\lambda$ is unramified, and w is a unit, so $(d, w)_\lambda = 1$. The other factors are 1, as both entries are units at odd primes. So $(d/w) = 1$, and d is a square in F_w.

At λ, $W_\lambda(d^2 A) = W_\lambda(A)$ by Lemma 2.4(a). At odd $\mathfrak{p} \notin \{(u), (v), (w)\} \cup \mathcal{P}_d$ both are the group of unit classes, and at u and v both are $\{1, [A]\}$ (Lemma 2.2(b)). At w, $W_w(d^2 A) = W_w(A)$ by Lemma 2.1(b) with $t = \sqrt{d} \in F_w$. Let $\mathfrak{p} \in \mathcal{P}_d$. As d is prime to $\mathrm{N}\, u\, \mathrm{N}\, v\, \mathrm{N}\, w$, $A = -4\lambda^2 uvw^2$ is a unit at $\mathfrak{p}$, and $W_{\mathfrak{p}}(d^2 A)$ has order two and contains $[d^2 A] = [A]$. If A is not a square, this is a non-square unit class, and $W_{\mathfrak{p}}(d^2 A)$ is the group of unit classes. If $A = a^2$, then $(da, 0) \in E_{d^2 A}(F_{\mathfrak{p}})$, and $[da]$, of odd valuation, generates $W_{\mathfrak{p}}(d^2 A)$.

(b) Apply Hilbert reciprocity to (X, z). At λ the factor is 1 by Lemma 2.4(a), as $z \in W_0$. At u and v, both $[X] = \delta(G)$ and z lie in $\{1, [A]\}$, and at w both lie in $\{1, [X]\}$, by (a) and the proof of Lemma 2.7(a); as $(c, c)_{\mathfrak{p}} = (c, -1)_{\mathfrak{p}} = 1$, these factors are 1. At the primes of $\mathcal{P}_d$

at which A is not a square and at the remaining odd primes, X is a unit and z a unit class, by (a), so the factor is 1.

(c) Let $z \in \mathrm{Sel}(d^2A)$. By (b), $(X,z)_{\mathfrak{p}^*} = 1$; as X is a non-square unit at $\mathfrak{p}^*$, $(X,z)_{\mathfrak{p}^*} = (-1)^{v_{\mathfrak{p}^*}(z)}$, so $v_{\mathfrak{p}^*}(z)$ is even, and as $z \in W_{\mathfrak{p}^*}(d^2A) = \{1,[da]\}$, z is a square at $\mathfrak{p}^*$. At the other primes of $\mathcal{P}_d$, z is a unit class by (a). So z has even valuation at every prime of $\mathcal{P}_d$, where $W_{\mathfrak{p}}(A)$ is the group of unit classes, and $W_{\mathfrak{p}}(d^2A) = W_{\mathfrak{p}}(A)$ at every other prime; so $z \in \mathrm{Sel}(A)$. Of $[A]$, $[X]$, $[AX]$, only $[A]$ is a square at $\mathfrak{p}^*$. So $\mathrm{Sel}(d^2A) \subseteq \{1,[A]\}$ by Lemma 2.7(a); as $[A] = [d^2A] = \delta(T)$, equality holds, and $E_{d^2A}(F)$ has $\mathbb{Z}[i]$-rank zero by Lemma 2.2(c). □

Lemma 2.9. *Let $B \in F^\times$, and let $D_1,\dots,D_r$ be integers such that $L' = F(\sqrt{D_1},\dots,\sqrt{D_r})$ has degree 2^r over F. For $S \subseteq \{1,\dots,r\}$ put $D_S = \prod_{j\in S} D_j$. Then the $\mathbb{Z}[i]$-rank of $E_B(L')$ is the sum over S of the $\mathbb{Z}[i]$-ranks of $E_{D_S^2B}(F)$.*

Proof. The group $\mathrm{Gal}(L'/F)$ is $(\mathbb{Z}/2\mathbb{Z})^r$, and its characters are the χ_S with $g(\sqrt{D_S}) = \chi_S(g)\sqrt{D_S}$. As $[i]$ is defined over F, the $\mathbb{Q}(i)$-vector space $E_B(L')\otimes\mathbb{Q}$ is the sum of the eigenspaces of the χ_S. The isomorphism $\psi_S(x,y) = (D_Sx, D_S\sqrt{D_S}\,y)$ of E_B onto $E_{D_S^2B}$ over L' commutes with $[i]$ and satisfies $g\psi_S(V) = [\chi_S(g)]\psi_S(gV)$ for $g \in \mathrm{Gal}(L'/F)$, so it carries the χ_S-eigenspace onto the invariants of $\mathrm{Gal}(L'/F)$ in $E_{D_S^2B}(L')\otimes\mathbb{Q}$, which are $E_{D_S^2B}(F)\otimes\mathbb{Q}$. □

Proof of Theorem 1.4. Let $d>1$ be odd and squarefree, and take $t_{\mathfrak{p}}$, $\mathfrak{p}^*$ and u,v,w as in Lemmas 2.5 and 2.6; the norms of u, v, w are prime to $2d$, and $w \equiv 1$ and $v \equiv t_{\mathfrak{p}}u$ modulo every $\mathfrak{p} \in \mathcal{P}_d$. By (2.3) with $t = t_{\mathfrak{p}}$ and Lemma 2.5, A is a square and X a non-square unit at $\mathfrak{p}^*$, and A is a non-square unit at the other primes of $\mathcal{P}_d$. So Lemma 2.7(a), (c) and Lemma 2.8(c) give (a). Lemma 2.7(b) with $M = F(\sqrt{d})$, which is unramified over F at (u) and (v), gives (b), and Lemma 2.7(d) gives (c). □

3. The certificate

Sections 3, 4, 5 and 6 prove Theorem 1.5. This section sets up the certificate, a statement about $X \in K$ that Sections 4 and 5 show holds exactly when $X \in \mathbb{Z}$ (Propositions 4.3 and 5.6).

We follow Sun [17, §§9, 10, 12, 13] and our earlier paper [4, §7], with four changes, all forced by the base field $F = \mathbb{Q}(\zeta_8)$, which has degree 4 and no real place. First, $L = KF$ has degree 4 over K, with basis $1,\zeta,\zeta^2,\zeta^3$ (Lemma 3.1(a)), so an abscissa $x(\mathsf{N}_i) \in L$ has four coordinates in K, while the height bound (Theorem 3.7) and the pole predicate Φ_K (Lemma 3.9) are statements about elements of K. The certificate (Section 3.5) therefore gives each of the sixteen coordinates a_j its own tube variable $s_j = y_j^2\eta + 1/q$, with $y_j = 1+\varpi a_j^2$, and its own detector B_j; it adds B_0, with $y_0 = 1$, for the height of η, and a scalar detector B_{sc} for the twelve tests that lie in K. Each detector is read at one prime at a time by Lemma 4.1, which is Sun's [17, Lemma 9.1] for L/K of degree 4, and the proof of Proposition 4.3 bounds the height of each a_j by the primes at which its own detector acts. Second, E_A has complex multiplication by $\mathbb{Z}[i]$ over F, so $2E_A(L) = \mathbb{Z}[i]P$ (Lemma 3.2), the indices that the certificate reads are Gaussian integers, and the count for $\beta - n_1$ in Proposition 4.3 runs over primes of $K(i)$. Third, completeness must make every test small at every archimedean place of L, and these lie over the two complex places of F; the closure of the multiples of P in the product of the two complex curves has a torus as identity component, on which suitable multiples are dense (Lemma 5.4), in place of Sun's real torus. Fourth, the conjugation is

$\sigma\colon \zeta \mapsto -\zeta$, the generator of $\mathrm{Gal}(F/\mathbb{Q}(i))$. It fixes i, so it commutes with $[i]$ and keeps the Gaussian labels, and it exchanges the two complex places of F (Lemma 3.1(d)) and the two primes of F above each Gaussian prime $\pi \equiv 9 \pmod{16}$, where hypothesis (iii) of Theorem 1.5 is read. As in [17, Lemma 9.3] and [4, §7], the tube variable carries $\eta = a_0^2 + b_0^2$, which keeps s_j totally positive with $v_{\mathfrak{q}}(s_j) \le -1$ (Lemma 3.8(b)) and lets completeness take $\eta = \mathrm{N}(\pi_0)/w_0^2$ for the Gaussian prime π_0 given by the prime pattern (Proposition 5.6).

Throughout this section and the next three, K, $n = [K:\mathbb{Q}]$, L and A are as in Theorem 1.5 and satisfy its hypotheses, d_K is the discriminant of K, $G = \mathrm{Gal}(L/F)$, $E = E_A$ and $T = (0,0)$. Let σ be the automorphism $\zeta \mapsto \zeta^5 = -\zeta$ of F; it fixes i and sends $\sqrt{2}$ to $-\sqrt{2}$. Let $E^\sigma\colon y^2 = x^3 - \sigma(A)x$ be the conjugate curve. For a point $V \ne O$ of E or E^σ put $\rho(V) = 1/x(V)$ and $\mathfrak{z}(V) = -x(V)/y(V)$ where these are finite, and $\rho(O) = \mathfrak{z}(O) = 0$. Both curves have the integral equations above at every prime of F, with discriminants $64A^3$ and $64\sigma(A)^3$, so they have good reduction at every prime of F not dividing $2\,\mathrm{N}_{F/\mathbb{Q}}(A)$.

3.1. **Fields and points.**

Lemma 3.1. (a) *$K \cap F = \mathbb{Q}$, so $[L:K] = 4$, $1, \zeta, \zeta^2, \zeta^3$ is a K-basis of L, and restriction $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/\mathbb{Q})$ is an isomorphism. For $c_0, \dots, c_3 \in K$, $\mathrm{Tr}_{L/K}(c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3) = 4c_0$, and the coordinates of an element of F in this basis are rational.*

(b) *L/K is unramified outside 2, and $L/\mathbb{Q}$ is unramified outside $2d_K$.*

(c) *A rational prime $p \equiv 1 \pmod 8$ splits completely in F.*

(d) *σ exchanges the two complex places of F.*

Proof. (a) $K \cap F = \mathbb{Q}$ is a hypothesis, and the rest follows, as $F/\mathbb{Q}$ is Galois and $\mathrm{Tr}_{F/\mathbb{Q}}(\zeta^k) = 0$ for $k = 1, 2, 3$. (b) $F/\mathbb{Q}$ is ramified only at 2, $K/\mathbb{Q}$ only at primes dividing d_K, and $L = K(\zeta)$. (c) is the decomposition law in $\mathbb{Q}(\zeta_8)$. (d) The places of F are $\{\zeta \mapsto e^{\pi i/4}, e^{-\pi i/4}\}$ and $\{\zeta \mapsto e^{3\pi i/4}, e^{-3\pi i/4}\}$, and σ multiplies the exponents by 5. □

Let $\tau \in \mathrm{Gal}(L/K)$ restrict to σ. For $V \in E(L)$ let $V^\tau \in E^\sigma(L)$ be the point with the τ-conjugate coordinates. As $\tau(i) = i$,

$$([u]V)^\tau = [u]V^\tau \qquad (u \in \mathbb{Z}[i],\ V \in E(L)), \tag{3.1}$$

and for $V \in E(F)$, $V^\tau = V^\sigma$ has the σ-conjugate coordinates.

Lemma 3.2. *$2E(L) \subseteq E(F)$, and $2E(L) = \mathbb{Z}[i]P$ for a point $P \in E(F)$ of infinite order.*

Proof. By (i), $E(F)$ and $E(L)$ have the same $\mathbb{Z}[i]$-rank, and $E(L)$ is finitely generated, so $E(L)/E(F)$ is finite: for $R \in E(L)$ there is $k \ge 1$ with $[k]R \in E(F)$. For $g \in G$, $[k](gR - R) = O$, so $gR - R \in \{O, T\}$ by (ii), and $g([2]R) = [2]R$; hence $[2]R \in E(F)$. If $[2]V$ is torsion, then V is, $V \in \{O, T\}$ and $[2]V = O$. So $2E(L)$ is a torsion-free $\mathbb{Z}[i]$-submodule of $E(F)$ of rank one, and it is free, $\mathbb{Z}[i]$ being a principal ideal domain. □

We fix P as in Lemma 3.2.

3.2. **Formal logarithms.**

Let $\omega = (1 + \sum_{t\ge1} b_t Z^t)\,dZ$ be the normalized invariant differential of the formal group $\hat{E}$ of the equation of E at the parameter $\mathfrak{z}$. Its coefficients lie in $\mathbb{Z}[A]$, as the group law does [16, Proposition IV.1.1 and Example IV.2.2.3] and ω is computed from it [16, Proposition IV.4.2]. With $b_0 = 1$, the formal logarithm is $\ell(Z) = \sum_{t\ge1}(b_{t-1}/t)Z^t$, and $\ell_m(Z) = \sum_{t\le m}(b_{t-1}/t)Z^t$. For E^σ we write ℓ^σ and ℓ_m^σ; their coefficients are the σ-conjugates. As $\mathfrak{z}([i]V) = i\,\mathfrak{z}(V)$, $[i]$ acts on $\hat{E}$ as $Z \mapsto iZ$, and $\ell(iZ) = i\,\ell(Z)$, as in the proof of Lemma 2.2(a); likewise for ℓ^σ.

Let k be the completion of L or of F at a prime above a rational prime p, with valuation ring R, maximal ideal $\mathfrak{m}$, normalized valuation v and $e = v(p)$. For the integral equation of E, $E_1(k) = \{O\} \cup \{V : v(x(V)) < 0\}$ is identified with $\hat{E}(\mathfrak{m})$ by $\mathfrak{z}$, with $v(x(V)) = -2v(\mathfrak{z}(V))$ for $V \neq O$, as in the proof of Lemma 2.2(a). So $E_1(k)$ is an open subgroup of the compact group $E(k)$, of finite index, and $V \in E_1(k)$ if and only if $\rho(V)$ is finite and $v(\rho(V)) \geq 1$. On $E_1(k)$, $\ell \circ \mathfrak{z}$ is a homomorphism [16, Theorem IV.6.4(a)], so for $V \in E_1(k)$ and $u = a + bi \in \mathbb{Z}[i]$,

$$\ell(\mathfrak{z}([u]V)) = a\,\ell(\mathfrak{z}(V)) + b\,\ell(i\,\mathfrak{z}(V)) = u\,\ell(\mathfrak{z}(V)). \tag{3.2}$$

The same holds for E^σ, and here and below a Gaussian integer is read in k through $\mathbb{Z}[i] \subset F \subseteq k$.

Lemma 3.3. *Let k be as above with $e = 1$ and $p \geq 5$, and let $Z \in \mathfrak{m}$ and $m \geq 1$.*

(a) $v(\ell(Z)) = v(\ell_m(Z)) = v(Z)$.

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

(c) *Let $Y \in E(k)$ and $\nu, \nu' \in \mathbb{Z}[i]$, $\nu' \neq 0$, with $[\nu]Y, [\nu']Y \in E_1(k)$ and $[\nu']Y \neq O$. Then $v(\mathfrak{z}([\nu]Y)) - v(\mathfrak{z}([\nu']Y)) = v(\nu) - v(\nu')$, the quotient $\Lambda = \ell_m(\mathfrak{z}([\nu]Y))/\ell_m(\mathfrak{z}([\nu']Y))$ is defined, and $v(\Lambda) = v(\nu) - v(\nu')$. If $p > m+1$ and $v(\nu) \geq v(\nu')$, then $v(\Lambda - \nu/\nu') \geq m$.*

The same holds for E^σ with ℓ^σ and ℓ^σ_m.

Proof. (a) At $Z = 0$ both logarithms vanish, giving (a) and (b). For $Z \neq 0$ and $t \geq 2$, $v((b_{t-1}/t)Z^t) \geq v(Z) + (t-1) - v_p(t) > v(Z)$, as $v_p(t) \leq \log_5 t < t - 1$. (b) For $t \geq m + 1$, $t - 1 - v_p(t) \geq m$: this is clear if $p \nmid t$, and if $v_p(t) = f \geq 1$ then $t - 1 - f \geq p^f - 1 - f \geq p - 2 \geq m$. (c) Put $Z = \mathfrak{z}([\nu]Y)$ and $Z' = \mathfrak{z}([\nu']Y) \neq 0$. By (3.2) applied to $[\nu]Y$ and to $[\nu']Y$, $\nu'\ell(Z) = \ell(\mathfrak{z}([\nu'][\nu]Y)) = \nu\ell(Z')$, and (a) gives the valuations. If $p > m+1$ and $v(\nu) \geq v(\nu')$, then $r = \nu/\nu'$ is integral and $\ell_m(Z) - r\ell_m(Z') = (\ell_m - \ell)(Z) - r(\ell_m - \ell)(Z')$ has valuation at least $v(Z') + m$ by (b); divide by $\ell_m(Z')$. □

Lemma 3.4. *Let $m \geq 1$ and $c_* \neq 0$ be integers, and $\mathfrak{Q}$ a prime of L above a prime $p > m+1$, $p \geq 5$, $p \nmid c_*$, with $e = 1$ at $\mathfrak{Q}$. Let $h, u_i, n_i \in \mathbb{Z}[i]$ $(1 \leq i \leq 4)$, and put $\mathsf{H} = [h]P$, $\mathsf{U}_i = [u_i]P$, $V_0 = \mathsf{H} - [c_*]P$ and $V_i = \mathsf{U}_i - [c_* n_i]P$. Suppose that $\mathsf{H} \neq O \neq V_0$, that $\mathsf{H}, \mathsf{U}_i \in E_1(L_\mathfrak{Q})$ and $V_0^\tau, V_i^\tau \in E_1^\sigma(L_\mathfrak{Q})$, and that*

$$L_i = \frac{\ell_m(\mathfrak{z}(\mathsf{U}_i))}{\ell_m(\mathfrak{z}(\mathsf{H}))}, \qquad L_i' = \frac{\ell^\sigma_m(\mathfrak{z}(V_i^\tau))}{\ell^\sigma_m(\mathfrak{z}(V_0^\tau))}$$

satisfy $v(L_i - L_i') \geq m$. Then $v(L_i - n_i) \geq m$ for $1 \leq i \leq 4$. Hence, if $f \in \mathbb{Z}[X_1, \ldots, X_4]$ and $v(f(L_1, \ldots, L_4)) \geq m$, then $\mathfrak{p}^m$ divides $f(n_1, \ldots, n_4)$ in $\mathbb{Z}[i]$, where $\mathfrak{p}$ is the prime of $\mathbb{Z}[i]$ below $\mathfrak{Q}$.

Proof. We follow the proof of [17, Lemma 9.2]. By (3.1), $V_0^\tau = [h - c_*]P^\tau$ and $V_i^\tau = [u_i - c_* n_i]P^\tau$, with the same Gaussian labels as on E, read through the same embedding of $\mathbb{Z}[i]$ in $L_\mathfrak{Q}$, since τ fixes i. As $p \nmid c_*$, one of h and $h - c_*$ is a unit at $\mathfrak{Q}$. If h is, Lemma 3.3(c) on E with $Y = P$ gives $v(L_i - u_i/h) \geq m$; so L_i and L_i' are integral, and Lemma 3.3(c) on E^σ with $Y = P^\tau$ gives $v(u_i - c_* n_i) \geq v(h - c_*)$ and then $v(L_i' - (u_i - c_* n_i)/(h - c_*)) \geq m$. If $h - c_*$ is a unit, 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 $\mathfrak{m}^m$, so

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

and c_* is a unit. Then $f(L_1, \ldots, L_4) \equiv f(n_1, \ldots, n_4)$, and $v = v_\mathfrak{p}$ on $\mathbb{Z}[i]$ as $e = 1$. □

Lemma 3.5. *Let $p \geq 5$ be a prime not dividing $\mathrm{N}_{F/\mathbb{Q}}(A)$, $m \geq 1$, and $h, s \in \mathbb{Z}[i]$ nonzero. Let $G_1, \dots, G_{12} \in \mathbb{Q}$ be the coordinates of $\rho([h]P)$, $\rho([s]P)$ and $\mathfrak{z}([s]P)/\mathfrak{z}([h]P)$, in this order. If $v_p(G_k) \geq 1$ for $k \leq 8$ and $v_p(G_k) \geq m$ for $9 \leq k \leq 12$, then p^m divides s in $\mathbb{Z}[i]$.*

Proof. We follow the proof of [17, Lemma 12.3]. Let $\mathfrak{Q}$ be a prime of F above p; then $e = 1$. As $\mathcal{O} = \mathbb{Z}[\zeta]$, the hypotheses give $v_{\mathfrak{Q}}(\rho([h]P)), v_{\mathfrak{Q}}(\rho([s]P)) \geq 1$ and $v_{\mathfrak{Q}}(\mathfrak{z}([s]P)/\mathfrak{z}([h]P)) \geq m$. So $[h]P, [s]P \in E_1(F_{\mathfrak{Q}})$, both $\neq O$, and Lemma 3.3(c) gives $v_{\mathfrak{Q}}(s) \geq m + v_{\mathfrak{Q}}(h) \geq m$. Every prime of $\mathbb{Z}[i]$ above p lies below a prime of F. □

3.3. **Integers and heights.** Put

$$\mathcal{L}(X_1, X_2, X_3, X_4) = X_3^2 - X_2(X_2 - 2)X_3X_4 + (X_2 - 2)^2X_4^2 - 1, \tag{3.3}$$

which does not involve X_1. For $\nu \in \mathbb{Z}[i]$, $|\nu|$ is the complex absolute value.

Lemma 3.6. (a) *If $n_2, n_3, n_4 \in \mathbb{Z}[i]$, $|n_2| \geq 9$, $n_4 \neq 0$ and $\mathcal{L}(X_1, n_2, n_3, n_4) = 0$, then $\log|n_4| \geq |n_2| - 4$.*

(b) *For every integer $n_2 \geq 3$ there are positive integers n_3, n_4 with $\mathcal{L}(X_1, n_2, n_3, n_4) = 0$.*

Proof. We follow the proof of [17, Lemma 12.4], over $\mathbb{Z}[i]$. Put $a = n_2$ and $w = (a-2)n_4$, so that $\mathcal{L} = 0$ reads $t^2 - atw + w^2 = 1$ with $t = n_3$. Let $U_0 = 0$, $U_1 = 1$, $U_{k+1} = aU_k - U_{k-1}$ and $U_{-k} = -U_k$. Each U_k is a polynomial in a with integer coefficients, equal to k at $a = 2$, so $U_k \equiv k \pmod{a-2}$; and $U_{k+1}^2 - aU_{k+1}U_k + U_k^2 = U_k^2 - U_{k+1}U_{k-1}$ does not depend on k, so it is 1.

(b) Take $k = 2(a-2)$, $n_3 = U_{k+1}$ and $n_4 = U_k/(a-2) \in \mathbb{Z}$. As $U_{j+1} - U_j = (a-2)U_j + (U_j - U_{j-1})$, the U_j with $j \geq 1$ increase, so $n_3, n_4 > 0$.

(a) Here $|a| \geq 9$, and $a^2 - 4$ is not a square in $\mathbb{Q}(i)$: otherwise $(a-b)(a+b) = 4$ with $b \in \mathbb{Z}[i]$, and $|2a| \leq |a-b| + |a+b| \leq 5$. Let $\varrho_\pm$ be the roots of $X^2 - aX + 1$, with $|\varrho_+| \geq 1$; then $\varrho_- = \varrho_+^{-1}$, $\varrho_\pm \notin \mathbb{Q}(i)$ and $|\varrho_+| \geq |a| - 1 \geq 8$. The numbers $\epsilon = t - w\varrho_+$ with $(t, w) \in \mathbb{Z}[i]^2$ and $t^2 - atw + w^2 = 1$ form a subgroup $\mathcal{U}$ of $\mathbb{C}^\times$, with $\epsilon^{-1} = t - w\varrho_-$, as $t^2 - atw + w^2 = (t - w\varrho_+)(t - w\varrho_-)$; and $|w|\,|\varrho_+ - \varrho_-| = |\epsilon - \epsilon^{-1}| \leq |\epsilon| + |\epsilon|^{-1}$, so only finitely many ϵ have $|\epsilon|$ in a given compact subset of $(0, \infty)$. If $1 \leq |\epsilon| < |\varrho_+|$, then $|w| \leq (|\varrho_+|+1)/(|\varrho_+| - |\varrho_+|^{-1}) = |\varrho_+|/(|\varrho_+|-1) < \sqrt{2}$, so $w \in \{0, \pm 1, \pm i\}$. Now $w = 0$ gives $\epsilon = \pm 1$; $w = \pm 1$ gives $t \in \{0, aw\}$ and $|\epsilon| = |\varrho_+|^{\pm 1}$; and $w = \pm i$ gives $(2t - aw)^2 = 8 - a^2$, so $(a + ib')(a - ib') = 8$ with $b' = 2t - aw$, and $|2a| \leq 9$. Hence $\mathcal{U} = \{\pm\varrho_+^k : k \in \mathbb{Z}\}$.

Now $w \neq 0$, and $\varrho_+^k = U_k\varrho_+ - U_{k-1}$ for all k, so comparing coefficients of ϱ_+ gives $w = \mp U_k$ with $k \neq 0$. As $a - 2$ divides w, hence U_k, hence k, we have $|k| \geq |a| - 2$. From $U_k = (\varrho_+^k - \varrho_-^k)/(\varrho_+ - \varrho_-)$ and $|\varrho_+ - \varrho_-| \leq 2|\varrho_+|$,

$$|w| \geq \frac{|\varrho_+|^{|k|} - 1}{2|\varrho_+|} \geq \frac{(|a| - 1)^{|a|-3}}{4},$$

so $\log|n_4| \geq (|a| - 3)\log(|a| - 1) - \log(4(|a| + 2))$. This exceeds $|a| - 4$ at $|a| = 9$, where the difference is $6\log 8 - \log 44 - 5 > 0$, and the difference increases with $|a|$. □

Let h be the absolute logarithmic Weil height, $\mathrm{h}_x(Y) = \mathrm{h}(x(Y))$ for $Y \in E(\overline{F}) \setminus \{O\}$, $\mathrm{h}_x(O) = 0$, and $\hat{\mathrm{h}}$ the canonical height of E. There is C_E with $|\mathrm{h}_x - 2\hat{\mathrm{h}}| \leq C_E$ on $E(\overline{F})$, $\hat{\mathrm{h}}(Y) > 0$ if Y has infinite order, and the pairing $\langle Y, Y' \rangle = \hat{\mathrm{h}}(Y + Y') - \hat{\mathrm{h}}(Y) - \hat{\mathrm{h}}(Y')$ is bilinear [16, Theorem VIII.9.3]. As $x([2^N][i]Y) = -x([2^N]Y)$, $\hat{\mathrm{h}} \circ [i] = \hat{\mathrm{h}}$, so the pairing is invariant under $[i]$; hence $\langle Y, [i]Y \rangle = \langle [i]Y, -Y \rangle = -\langle Y, [i]Y \rangle = 0$, and

$$\hat{\mathrm{h}}([a + bi]Y) = a^2\hat{\mathrm{h}}(Y) + b^2\hat{\mathrm{h}}([i]Y) + ab\langle Y, [i]Y \rangle = (a^2 + b^2)\hat{\mathrm{h}}(Y). \tag{3.4}$$

For a number field k and $\alpha \in k^\times$, let $\mathfrak{a}(\alpha)$ be its numerator ideal $\prod_{v_\mathfrak{P}(\alpha)>0} \mathfrak{P}^{v_\mathfrak{P}(\alpha)}$. For a finite place $v \mid p$ we normalize $|p|_v = p^{-1}$ and put $n_v = [k_v : \mathbb{Q}_p]$. Then

$$\log \mathrm{N}\,\mathfrak{a}(\alpha) = \sum_{v \text{ finite}} n_v \log \max(1, |\alpha^{-1}|_v) \le [k:\mathbb{Q}]\,\mathrm{h}(\alpha^{-1}) = [k:\mathbb{Q}]\,\mathrm{h}(\alpha). \tag{3.5}$$

We use $\mathrm{h}(\alpha\beta) \le \mathrm{h}(\alpha) + \mathrm{h}(\beta)$, $\mathrm{h}(\alpha_1 + \cdots + \alpha_k) \le \sum \mathrm{h}(\alpha_j) + \log k$, $\mathrm{h}(\zeta^k \alpha) = \mathrm{h}(\alpha)$, $\mathrm{h}(\nu) = \log\max(1,|\nu|)$ for $\nu \in \mathbb{Z}[i]$, and $\mathrm{h}(\phi(t)) = d\,\mathrm{h}(t) + O(1)$ for a rational function $\phi \in \mathbb{Q}(t)$ of degree d [16, Theorem VIII.5.6].

3.4. **The tube and the pole predicate.** For a prime $q \ge 7$ let $D_q = q^2+3$, $a_q = (q-3)(q+1)/D_q$, $b_q = (q-1)(q+3)/D_q^2$ and

$$g_q(z) = \frac{(a_q z + b_q - qz^2)(a_q z + b_q - 4qz^2)}{4q^2},$$

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

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

Sun's formulas [17, (1.3)–(1.7)] with q in place of 367. For a prime $\mathfrak{P}$ of K, $z \in K \setminus \mathcal{C}_q$ 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. Let Σ be a finite set of primes of K containing those above the rational primes $p \le 324$ and above q, and those at which a nonzero finite contact or the difference of two distinct finite contacts has nonzero valuation. For $z \in K \setminus \mathcal{C}_q$, $\mathfrak{N}_\Sigma(z)$ is the product of the norms of the primes $\mathfrak{P} \notin \Sigma$ at which z has positive odd contact with a point of $\mathcal{C}_q$. For a prime $\mathfrak{q}$ of K above q, the *positive tube* is $\mathcal{D} = \{z \in K : v_\mathfrak{q}(z-1) \ge 1 \text{ and } g_q(z) \text{ is totally positive}\}$.

Theorem 3.7 ([4, Theorem 1.6])**.** *Let $q \equiv 7 \pmod{12}$ be a prime, $\mathfrak{q}$ a prime of K above q, unramified over q, of odd residue degree, and Σ, $\mathfrak{N}_\Sigma$ and $\mathcal{D}$ as above. Then $\mathcal{D} \cap \mathcal{C}_q = \emptyset$, and there are $H > 0$ and $\kappa > 0$ with $\mathrm{h}(z) \le H\,\mathfrak{N}_\Sigma(z)^\kappa$ for every $z \in \mathcal{D}$.*

For $K = \mathbb{Q}(\sqrt{2})$ and $q = 367$ this is Sun's height bound [17, Theorem 1.7] on the positive tube, and for $K = \mathbb{Q}(\sqrt{6})$ and $q = 331$ it is [17, Lemma 15.4]; the proof in our earlier paper is Sun's [17, §§5–8], over K. Put $\theta_0 = 0$, $\theta_i = q/(\gamma_i - 1)$ for $1 \le i \le 6$, and $\mathcal{T} = \{\theta_0, \ldots, \theta_6\}$.

Lemma 3.8 ([4, Lemmas 3.2 and 6.6])**.** *Let q and $\mathfrak{q}$ be as in Theorem 3.7, and Σ as above.*

(a) *The finite contacts lie in $(-1,1)$, and $v_q(\gamma_i - 1) \le 0$.*

(b) *If $\eta = a_0^2 + b_0^2 \ne 0$ with $a_0, b_0 \in K$, and $y \in K^\times$, then $s = y^2\eta + 1/q$ is totally positive and $v_\mathfrak{q}(s) \le -1$.*

(c) *If $s \in K$ is totally positive and $v_\mathfrak{q}(s) \le 0$, then $1 + q/s \in \mathcal{D}$ and $|\mathrm{h}(1+q/s) - \mathrm{h}(s)| \le C_q$, with C_q depending only on q. If $\mathfrak{P} \notin \Sigma$ and every θ_i with $i \ge 1$ and every $1 - \gamma_i$ is a unit at $\mathfrak{P}$, then $1 + q/s$ 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 $\theta \in \mathcal{T}$.*

(d) *For $t \in K$, $\psi_q(t) = 10q + 1 + q^2 t/(1+q^2t^2)$ lies in $\mathcal{D}$. Let $f_0 = 1 + q^2t^2$, $f_i = (10q + 1 - \gamma_i) f_0 + q^2 t$ $(1 \le i \le 6)$, and $R_\psi = C_* \prod_{i=0}^6 f_i$, with C_* the least positive integer such that $R_\psi \in \mathbb{Z}[t]$. Then R_ψ has degree 14 and is positive on $\mathbb{R}$. If $\mathfrak{P} \notin \Sigma$ divides neither C_* nor the leading coefficients of the f_i nor their pairwise resultants,*

then $\psi_q(t)$ 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 $v_{\mathfrak{P}}(R_\psi(t)) = 14v_{\mathfrak{P}}(t)$ if $v_{\mathfrak{P}}(t) < 0$.

These are Sun's [17, Lemma 9.3 and (12.4)–(12.8)] for general q.

Let $\mathcal{M} = \{\mu_0, 17\mu_0 : \mu_0 \in \{1,2,3,5,6,7,10,14\}\}$. 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 $H_b = \mu b(\mu b - b^2)$, there are $e, w \in k$ with $\mu b\, e\, H_b\, w \neq 0$ such that

$$\mu b(\mu b - e)(\mu b + e) \qquad \text{and} \qquad \mu b(\mu b w^2 - eH_b)(\mu b w^2 + eH_b)$$

are squares in k. This is the predicate of [4, §5]: Sun's two-parameter pole relation [17, (12.9) and Lemma 12.2], with his curves $y^2 = x(x-e)(x+3e)$ replaced by $y^2 = x^3 - e^2x$.

Lemma 3.9 ([4, Lemmas 5.1 and 5.3])**.** (a) *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.*

(b) *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 $e, w \in \mathbb{Q}$, so $\Phi_k(B)$ holds for every field $k \supseteq \mathbb{Q}$.*

Pasten and Vidaux show that every number field has a Diophantine predicate that holds at every rational number with square reduced denominator and, outside a finite set of primes, only at elements without poles of odd order [12, Theorem 3.1].

3.5. **The certificate.** For $u \in L$ write $u = u^{(0)} + u^{(1)}\zeta + u^{(2)}\zeta^2 + u^{(3)}\zeta^3$ with $u^{(k)} \in K$. The following data are fixed once, in this order.

(F1) A prime $q \equiv 7 \pmod{12}$ that splits completely in K, with $q \nmid 2d_K \operatorname{N}_{F/\mathbb{Q}}(A)$, and a prime $\mathfrak{q}$ of K above q, so that $\mathfrak{q}$ is unramified of residue degree one. Such q exist by [4, Lemma 3.1], as $\sqrt{3} \notin K$ and $K/\mathbb{Q}$ is Galois. The contacts γ_i, the set $\mathcal{T}$, $f_0, \ldots, f_6$, C_* and R_ψ for this q; $\xi = 1$, $\mathcal{T}^+ = \mathcal{T} \cup \{-1\}$, $F_8(S) = \prod_{\theta \in \mathcal{T}^+}(S - \theta)$, and $d_j = (2q+2)j$ for $0 \leq j \leq 16$. The least set Σ_0 allowed for Σ in Theorem 3.7, and the constants H, κ that the theorem gives for Σ_0.

(F2) An integer $m > 8n\kappa + 100$; a positive even integer c_*; $\Gamma = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17$ and $C = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot q \cdot \Gamma^2$.

(F3) The set $\mathfrak{B}$ of primes of K above: the rational primes $p \leq \max(324, m+1)$; q; the primes dividing $d_K \operatorname{N}_{F/\mathbb{Q}}(A) c_* C C_*$; and the rational primes at which one of the following has nonzero valuation: the nonzero γ_i, the $1 - \gamma_i$, the nonzero θ_i, the differences of two distinct elements of $\{1/q\} \cup \bigcup_{j=0}^{16}((\mathcal{T}^+ \cup \{\xi\}) - d_j)$, the nonzero coefficients of $f_0, \ldots, f_6$, and their pairwise resultants.

(F4) An integer $M \geq 10$, large enough for Proposition 4.3.

Lemma 3.10. (a) *$\mathcal{T}^+ \cup \{\xi\}$ has nine elements, lies in $(-(q+1), 1]$, and $-1 \notin \mathcal{T}$. $1/q$ lies in none of the seventeen sets $(\mathcal{T}^+ \cup \{\xi\}) - d_j$.*

(b) *A prime $\mathfrak{P} \notin \mathfrak{B}$ of K lies above a prime $p > \max(324, m+1)$ with $p \nmid 2qd_K \operatorname{N}_{F/\mathbb{Q}}(A) c_* C$; L/K is unramified at $\mathfrak{P}$; at every prime of L above $\mathfrak{P}$, $e = 1$ and E, E^σ have good reduction; and $\mathfrak{P}$ satisfies the conditions on $\mathfrak{P}$ in Lemma 3.8(c), (d).*

(c) *$\Sigma_0 \subseteq \mathfrak{B}$, and $\mathrm{h}(z) \leq H_{\mathfrak{B}}\, \mathfrak{N}_{\mathfrak{B}}(z)^\kappa$ for $z \in \mathcal{D}$, where $H_{\mathfrak{B}} = H \prod_{\mathfrak{P} \in \mathfrak{B} \setminus \Sigma_0} \operatorname{N}\mathfrak{P}^\kappa$.*

Proof. (a) The first sentence is [4, Lemma 7.1(a)]. For $j \geq 1$ the j-th set lies in $(-\infty, 1 - d_j]$, below 0, and for $j = 0$ its elements are 1, 0, -1 and the $\theta_i < 0$ (Lemma 3.8(a)), while $0 < 1/q < 1$. (b) follows from Lemma 3.1(b) and (F3). (c) For $i, k \geq 1$, $\gamma_i - \gamma_k = q(\theta_k - \theta_i)/(\theta_i\theta_k)$,

so a prime at which a nonzero contact or a difference of two distinct finite contacts has nonzero valuation is in $\mathfrak{B}$; and $\mathfrak{N}_{\Sigma_0}(z) \le \mathfrak{N}_{\mathfrak{B}}(z) \prod_{\mathfrak{P}\in\mathfrak{B}\setminus\Sigma_0} \mathrm{N}\,\mathfrak{P}$. □

Let $X \in K$. The certificate at X is read off nine points $\mathsf{Q}, \mathsf{N}_1, \mathsf{N}_3, \mathsf{N}_4, \mathsf{H}, \mathsf{U}_1, \dots, \mathsf{U}_4$ of $2E(L)$, elements $a_0, b_0 \in K$, and an element β, one of $3+(X^3+X)$ and $3-(X^3+X)$, through the following quantities. Put $\mathsf{R} = [M]\mathsf{Q}$, $\mathsf{N}_2 = P + \mathsf{R}$, $V_0 = \mathsf{H} - [c_*]P$, $V_i = \mathsf{U}_i - [c_*]\mathsf{N}_i$, $\eta = a_0^2 + b_0^2$, and L_i, L_i' as in Lemma 3.4 ($1 \le i \le 4$). The sixteen *comparison tests* $D_1, \dots, D_{16} \in L$, with *precisions* k_i, are $\rho(\mathsf{H}), \rho(\mathsf{U}_1), \dots, \rho(\mathsf{U}_4)$ and $\rho(V_0^\tau), \rho(V_1^\tau), \dots, \rho(V_4^\tau)$, of precision 1, and $L_i - L_i'$ ($1 \le i \le 4$), $\mathcal{L}(L_1, \dots, L_4)$ and $L_1 - \beta$, of precision m. The twelve *scalar tests* $G_1, \dots, G_{12} \in K$ are the coordinates of $\rho(\mathsf{H})$, $\rho(\mathsf{R})$ and $\mathfrak{z}(\mathsf{R})/\mathfrak{z}(\mathsf{H})$, in this order, with precisions $m_k = 1$ for $k \le 8$ and $m_k = m$ for $k \ge 9$. The sixteen *abscissa coordinates* are $a_{4i-3+k} = x(\mathsf{N}_i)^{(k)}$ ($1 \le i \le 4,\ 0 \le k \le 3$). Then

$$r = R_\psi(\beta), \qquad \varpi = \frac{\Gamma^2 r}{(1+Cr)^2}, \qquad y_0 = 1, \qquad y_j = 1 + \varpi a_j^2 \ (1 \le j \le 16),$$

$$s_j = y_j^2\eta + \frac{1}{q}, \qquad t_j = s_j + d_j - \xi, \qquad R_j = \frac{F_8(s_j + d_j)}{t_j^8}, \qquad \alpha_j = \varpi R_j \qquad (0 \le j \le 16),$$

and, with $\Psi(v) = v/(1+v)$,

$$W_j = \prod_{i=1}^{16} \Big(1 + \alpha_j \Big(\frac{D_i}{t_j^{k_i+1}\alpha_j^{k_i}}\Big)^2\Big), \quad \Theta_j = \mathrm{Tr}_{L/K}(W_j^{-1}), \quad B_j = \frac{\alpha_j}{\Theta_j^2},$$

$$W_{\mathrm{sc}} = \prod_{k=1}^{12} \Big(1 + \varpi \Big(\frac{\Psi(G_k)}{\varpi^{m_k}}\Big)^2\Big), \quad \Theta_{\mathrm{sc}} = \frac{4}{W_{\mathrm{sc}}}, \quad B_{\mathrm{sc}} = \frac{\varpi}{\Theta_{\mathrm{sc}}^2}.$$

We call $B_0, \dots, B_{16}$ the *detectors* and B_{sc} the *scalar detector*. As $W_{\mathrm{sc}} \in K$, $\Theta_{\mathrm{sc}} = \mathrm{Tr}_{L/K}(W_{\mathrm{sc}}^{-1})$, so the scalar detector has the form of the others, with $R \equiv 1$.

The certificate works as follows. Its points are Gaussian multiples of P (Lemma 3.2), say $\mathsf{N}_i = [n_i]P$. At a prime outside $\mathfrak{B}$ at which $v(\varpi)$ is even and $v(s_j + d_j - \theta)$ is positive and odd for some $\theta \in \mathcal{T}$, the detector B_j and Φ_K force each comparison test to vanish to its precision at a prime above it (Lemma 4.1), and Lemma 3.4 turns this into $\mathfrak{p}^m \mid \mathcal{L}(n_1, \dots, n_4)$ and $\beta \equiv n_1$ to order m. The scalar detector does the same for $n_2 - 1$ at the primes where $v(\varpi)$ is odd (Lemma 4.2). The height bound bounds the labels by these primes; this forces $\mathcal{L}(n_1, \dots, n_4) = 0$, so that $|n_4|$ is exponentially large in $|n_2|$ (Lemma 3.6(a)), and then $\beta = n_1$ (Proposition 4.3). For $X \in \mathbb{Z}$, Section 5 chooses the labels and, through the prime pattern (Theorem 5.2), the primes at which every detector passes (Proposition 5.6).

Definition 3.11. Let $X \in K$. The *certificate* at X is the statement that there exist nine points $\mathsf{Q}, \mathsf{N}_1, \mathsf{N}_3, \mathsf{N}_4, \mathsf{H}, \mathsf{U}_1, \dots, \mathsf{U}_4$ of $2E(L)$, elements $a_0, b_0 \in K$, an element $\beta \in \{3 + (X^3 + X), 3 - (X^3 + X)\}$, and witnesses in K of $\Phi_K(B)$ for the eighteen elements $B = B_0, \dots, B_{16}, B_{\mathrm{sc}}$, such that every quantity above is defined (no displayed denominator vanishes, and x, ρ and $\mathfrak{z}$ are applied only where they are finite), and

(i) Q, R, N_1, N_2, N_3, N_4, H, $\mathsf{U}_1, \dots, \mathsf{U}_4$ and V_0 are not O, and

(ii) $\eta \ne 0$.

Lemma 3.12. *Suppose the certificate holds at $X \in K$. Then $\mathsf{N}_i = [n_i]P$, $\mathsf{H} = [h]P$, $\mathsf{U}_i = [u_i]P$ and $\mathsf{Q} = [k_{\mathsf{Q}}]P$ with Gaussian integers $n_i, h, u_i, k_{\mathsf{Q}}$; $n_2 - 1 = Mk_{\mathsf{Q}}$, and $n_1, \dots, n_4$, $n_2 - 1$, h and $h - c_*$ are nonzero. All these points, R and the V_i lie in $E(F)$; the G_k and the a_j are rational; and r, ϖ, η, the y_j, s_j and $s_j + d_j$ are totally positive.*

Proof. By Lemma 3.2, $2E(L) = \mathbb{Z}[i]P \subseteq E(F)$, which gives the labels, $\mathsf{N}_2 = [1+Mk_{\mathsf{Q}}]P$ and, with (i), the nonvanishing. The coordinates of elements of F are rational (Lemma 3.1(a)). As K is totally real and $R_\psi > 0$ on $\mathbb{R}$ (Lemma 3.8(d)), r, $1+Cr$ and ϖ are totally positive, hence so are the y_j; η is a nonzero sum of two squares, $1/q > 0$ and $d_j \geq 0$. □

4. Soundness

This section proves that the certificate holds only at integers (Proposition 4.3), by the argument outlined before Definition 3.11. The first lemma is the local form of the detectors.

Lemma 4.1. *Let $\mathfrak{P} \notin \mathfrak{B}$ be a prime of K, $\alpha \in K$ with $v_{\mathfrak{P}}(\alpha)$ odd, and $Y_1, \dots, Y_J \in L$ and integers $k_1, \dots, k_J \geq 1$ such that*

$$W = \prod_{i=1}^{J} \Big(1 + \alpha\Big(\frac{Y_i}{\alpha^{k_i}}\Big)^2\Big) \quad \text{and} \quad \Theta = \mathrm{Tr}_{L/K}(W^{-1})$$

are nonzero and $\Phi_K(\alpha/\Theta^2)$ holds. Then $v_{\mathfrak{P}}(\alpha) > 0$, and some prime $\mathfrak{Q}$ of L above $\mathfrak{P}$ has $v_{\mathfrak{Q}}(Y_i) \geq k_i$ for every i.

Proof. We follow the proof of [17, Lemma 9.1], for L/K of degree 4. Put $a = v_{\mathfrak{P}}(\alpha)$. As L/K is unramified at $\mathfrak{P}$ (Lemma 3.10(b)), $v_{\mathfrak{Q}} = v_{\mathfrak{P}}$ on K for every $\mathfrak{Q} \mid \mathfrak{P}$. If $Y_i \neq 0$, the summand y_i of the i-th factor has $v_{\mathfrak{Q}}(y_i) = a(1-2k_i) + 2v_{\mathfrak{Q}}(Y_i)$, which is odd, so $v_{\mathfrak{Q}}(1+y_i) = \min(0, v_{\mathfrak{Q}}(y_i))$, and $\mu_{\mathfrak{Q}} = v_{\mathfrak{Q}}(W) \leq 0$ is the sum of these numbers. Let $\mu = \max_{\mathfrak{Q}\mid\mathfrak{P}} \mu_{\mathfrak{Q}}$ and $\pi_{\mathfrak{P}}$ a uniformiser of K at $\mathfrak{P}$. Then $\pi_{\mathfrak{P}}^{\mu} W^{-1}$ is integral at every $\mathfrak{Q} \mid \mathfrak{P}$, so its trace $\pi_{\mathfrak{P}}^{\mu}\Theta$ is $\mathfrak{P}$-integral and $v_{\mathfrak{P}}(\Theta) \geq -\mu$. As $v_{\mathfrak{P}}(\alpha/\Theta^2) = a - 2v_{\mathfrak{P}}(\Theta)$ is odd, it is positive by Lemma 3.9(a). Hence $a \geq 1$ and $a + 2\mu \geq 1$. At a $\mathfrak{Q}$ with $\mu_{\mathfrak{Q}} = \mu$, every $v_{\mathfrak{Q}}(y_i)$ with $Y_i \neq 0$ is at least $\mu \geq (1-a)/2$, which gives $v_{\mathfrak{Q}}(Y_i) \geq k_i a - \frac{3a-1}{4} \geq k_i - \frac{1}{2}$, and so $v_{\mathfrak{Q}}(Y_i) \geq k_i$. □

Lemma 4.2. *Suppose the certificate holds at $X \in K$, with labels as in Lemma 3.12. Let $\mathfrak{P} \notin \mathfrak{B}$ be a prime of K above p with $v_{\mathfrak{P}}(\varpi)$ odd. Then $v_{\mathfrak{P}}(\varpi) = v_{\mathfrak{P}}(r) > 0$, $v_{\mathfrak{P}}(\beta) \geq 0$, and p^m divides $n_2 - 1$ in $\mathbb{Z}[i]$.*

Proof. Write $v = v_{\mathfrak{P}}$; Γ and C are $\mathfrak{P}$-units. If $v(\beta) < 0$, then $v(r) = 14v(\beta)$ by Lemma 3.8(d), so $v(1+Cr) = v(r)$ and $v(\varpi) = -v(r)$ is even. So r is integral, and $v(r) > 0$, as otherwise $v(\varpi) = -2v(1+Cr)$; hence $v(\varpi) = v(r)$. Lemma 4.1 with $\alpha = \varpi$ and $Y_k = \Psi(G_k) \in \mathbb{Q}$ gives $v_p(\Psi(G_k)) \geq m_k \geq 1$, as $\mathfrak{P}$ is unramified over p. If $v_p(G_k) \leq 0$, then $v_p(\Psi(G_k)) \leq 0$; so $v_p(G_k) > 0$, $1 + G_k$ is a p-unit and $v_p(G_k) \geq m_k$. As $\mathsf{R} = [n_2 - 1]P$ and $\mathsf{H} = [h]P$ with $n_2 - 1, h \neq 0$, Lemma 3.5 gives $p^m \mid n_2 - 1$. □

Proposition 4.3. *If M in (F4) is large enough, every $X \in K$ at which the certificate holds lies in $\mathbb{Z}$.*

Proof. We follow the proof of [17, Proposition 13.6]. Let the certificate hold at X, with labels as in Lemma 3.12, and put $N = \max(1, |n_1|, \dots, |n_4|)$ and $\Delta = \mathcal{L}(n_1, n_2, n_3, n_4) \in \mathbb{Z}[i]$. As $|n_2 - 1| = M|k_{\mathsf{Q}}| \geq M$, $N \geq |n_2| \geq M - 1 \geq 9$. The constants $c_1, c_2, \dots$ depend on E, P and (F1)–(F3), not on M or X.

Local alternatives. Let $\mathfrak{P} \notin \mathfrak{B}$ be a prime of K above p.

(i) Suppose $v_{\mathfrak{P}}(s_j + d_j - \theta)$ is positive and odd for some j and some $\theta \in \mathcal{T}$, and $v_{\mathfrak{P}}(\varpi)$ is even. The other factors $s_j + d_j - \theta'$, $\theta' \in \mathcal{T}^+$, and t_j are units at $\mathfrak{P}$, as $\theta - \theta'$ and $\theta - \xi$ are; so $v_{\mathfrak{P}}(R_j)$ is positive and odd and t_j is a unit. By Lemma 4.1 for B_j, with $\alpha = \alpha_j$ and $Y_i = D_i/t_j^{k_i+1}$, there is $\mathfrak{Q} \mid \mathfrak{P}$ with $v_{\mathfrak{Q}}(D_i) \geq k_i$ for all i: so

$\mathsf{H}, \mathsf{U}_i \in E_1(L_\mathfrak{Q})$, $V_0^\tau, V_i^\tau \in E_1^\sigma(L_\mathfrak{Q})$ and $v_\mathfrak{Q}(L_i - L_i') \geq m$. By Lemma 3.4, which applies by Lemma 3.10(b), and the tests $\mathcal{L}(L_1, \dots, L_4)$ and $L_1 - \beta$, $\mathfrak{p}^m$ divides Δ for the prime $\mathfrak{p}$ of $\mathbb{Z}[i]$ below $\mathfrak{Q}$, and $v_\mathfrak{Q}(\beta - n_1) \geq m$.

(ii) Suppose $v_\mathfrak{P}(\varpi)$ is odd. By Lemma 4.2, $v_\mathfrak{P}(\beta) \geq 0$ and $p^m \mid n_2 - 1$.

(iii) Suppose $v_\mathfrak{P}(r)$ is positive and odd. Then $1 + Cr$ is a unit, $v_\mathfrak{P}(\varpi) = v_\mathfrak{P}(r)$, and (ii) applies.

Counting. Let $\mathfrak{M}_j$ be the product of $\mathrm{N}\mathfrak{P}$ over the $\mathfrak{P} \notin \mathfrak{B}$ at which $v_\mathfrak{P}(s_j + d_j - \theta)$ is positive and odd for some $\theta \in \mathcal{T}$, and $\mathfrak{M}_{\mathrm{sc}}$ that over the $\mathfrak{P} \notin \mathfrak{B}$ at which $v_\mathfrak{P}(r)$ is positive and odd. For each p, $\prod_{\mathfrak{P}|p} \mathrm{N}\mathfrak{P} \leq p^n$. If $\Delta \neq 0$, then by (i) and (ii) p^m divides $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\Delta(n_2 - 1)) = |\Delta(n_2 - 1)|^2$ for every p below a prime counted in $\mathfrak{M}_j$, so $\mathfrak{M}_j^m \leq |\Delta(n_2 - 1)|^{2n}$. If $\beta \neq n_1$, then at every $\mathfrak{P}$ counted in $\mathfrak{M}_j$ there is a prime $\mathfrak{P}'$ of $K(i)$ above $\mathfrak{P}$ with $v_{\mathfrak{P}'}((\beta - n_1)(n_2 - 1)) \geq m$: in case (i) the prime below $\mathfrak{Q}$, over which $\mathfrak{Q}$ is unramified, and in case (ii) any $\mathfrak{P}'$. These $\mathfrak{P}'$ are distinct and $\mathrm{N}\mathfrak{P} \leq \mathrm{N}\mathfrak{P}'$, so (3.5) over $K(i)$, of degree $2n$, gives $\mathfrak{M}_j^m \leq \mathrm{N}\,\mathfrak{a}((\beta - n_1)(n_2 - 1)) \leq \exp(2n\,\mathrm{h}((\beta - n_1)(n_2 - 1)))$. By (iii) and (ii), p^m divides $n_2 - 1$ for every p below a prime counted in $\mathfrak{M}_{\mathrm{sc}}$, so $\mathfrak{M}_{\mathrm{sc}}^m \leq |n_2 - 1|^n$.

Heights. By Lemma 3.12 and Lemma 3.8(b), s_j and $s_j + d_j$ are totally positive with $v_\mathfrak{q} \leq -1$. By Lemma 3.8(c) and Lemma 3.10(b), $1 + q/(s_j + d_j) \in \mathcal{D}$, and its primes of positive odd contact outside $\mathfrak{B}$ are those counted in $\mathfrak{M}_j$; so Lemma 3.10(c) gives $\mathrm{h}(s_j) \leq c_1(1 + \mathfrak{M}_j^\kappa)$, as $d_j \in \mathbb{Z}$. By Lemma 3.8(d), $\psi_q(\beta) \in \mathcal{D}$, its primes of positive odd contact outside $\mathfrak{B}$ are those counted in $\mathfrak{M}_{\mathrm{sc}}$, and ψ_q has degree 2; so $\mathrm{h}(\beta) \leq c_2(1 + \mathfrak{M}_{\mathrm{sc}}^\kappa) \leq c_2(1 + |n_2 - 1|^{n\kappa/m})$. Finally, by (3.4), $2|n_i|^2 \hat{\mathrm{h}}(P) = 2\hat{\mathrm{h}}(\mathsf{N}_i) \leq \mathrm{h}_x(\mathsf{N}_i) + C_E \leq \sum_k \mathrm{h}(a_{4i-3+k}) + \log 4 + C_E$, with $\hat{\mathrm{h}}(P) > 0$; for $j \geq 1$, $a_j^2 = (y_j - 1)/\varpi$ gives $2\mathrm{h}(a_j) \leq \frac{1}{2}\mathrm{h}(y_j^2) + \mathrm{h}(\varpi) + \log 2$; $y_j^2 = (s_j - 1/q)/(s_0 - 1/q)$ gives $\mathrm{h}(y_j^2) \leq \mathrm{h}(s_j) + \mathrm{h}(s_0) + 2\log(2q)$; and $\mathrm{h}(\varpi) \leq 3\mathrm{h}(r) + O(1) \leq 42\mathrm{h}(\beta) + O(1)$. Hence

$$N^2 \leq c_3\Big(1 + \sum_{j=0}^{16} \mathfrak{M}_j^\kappa + |n_2 - 1|^{n\kappa/m}\Big). \tag{4.1}$$

$\Delta = 0$. Otherwise $|\Delta| \leq 14N^4$ and $|n_2 - 1| \leq 2N$, so $\mathfrak{M}_j \leq (28N^5)^{2n/m}$, and (4.1) gives $N^2 \leq c_4(1 + N^{10n\kappa/m})$, with $10n\kappa/m < \frac{5}{4}$ by (F2). This fails for $N > N_1$, with N_1 depending only on the constants; we take $M > N_1 + 1$. So $\Delta = 0$, and Lemma 3.6(a) gives $\log N \geq \log|n_4| \geq |n_2| - 4 \geq |n_2 - 1| - 5$.

$\beta = n_1$. Otherwise $\mathrm{h}((\beta - n_1)(n_2 - 1)) \leq \mathrm{h}(\beta) + 2\log(2N)$, and with $\epsilon = 2n\kappa/m < \frac{1}{4}$, (4.1), the bound on $\mathrm{h}(\beta)$ and $|n_2 - 1| \leq \log N + 5$ give

$$N^2 \leq c_5(1 + e^{\epsilon \mathrm{h}(\beta)}(2N)^{2\epsilon}), \qquad \mathrm{h}(\beta) \leq c_2(1 + (\log N + 5)^{\epsilon/2}).$$

The second bound gives $e^{\epsilon\mathrm{h}(\beta)} \leq N^{1/4}$ for $N > N_2$, and then the first fails for $N > N_3$. As $N \geq |n_4| \geq \exp(|n_2| - 4) \geq \exp(M - 5)$, we take M with $\exp(M - 5) > \max(N_2, N_3)$. So $\beta = n_1$. As $\beta \in K$, $n_1 \in \mathbb{Q}(i)$ and $K \cap \mathbb{Q}(i) = \mathbb{Q}$, $n_1 \in \mathbb{Z}$; so $X^3 + X = \pm(n_1 - 3) \in \mathbb{Z}$, and $X \in \mathbb{Z}$ by [17, Lemma 12.1], K being totally real. □

5. Completeness

This section proves that the certificate holds at every integer (Proposition 5.6). The detectors need primes at which the reductions of E have known orders: Lemma 5.1 gives these orders at Gaussian primes $\pi \equiv 9 \pmod{16}$ of rational prime norm prime to $\mathrm{N}_{F/\mathbb{Q}}(A)$, and the prime pattern of Theorem 5.2 supplies such primes with every congruence the construction asks for.

5.1. **The reductions at the pattern primes.**

Lemma 5.1. *Let $\pi \equiv 9 \pmod{16}$ be a Gaussian prime of rational prime norm $p = \mathrm{N}\,\pi$, and $\mathfrak{p}$ a prime of F above π at which A is a unit. Then $p \equiv 1 \pmod{16}$ splits completely in F, E has good reduction $\tilde{E}$ at $\mathfrak{p}$, and $\#\tilde{E}(\mathcal{O}/\mathfrak{p}) = \mathrm{N}(\pi - \upsilon)$ for some $\upsilon \in \{\pm 1, \pm i\}$, with $\upsilon \in \{\pm 1\}$ if and only if A is a square modulo $\mathfrak{p}$.*

Proof. Writing $\pi = a + bi$ with $a \equiv 9$, $b \equiv 0 \pmod{16}$ gives $p \equiv 1 \pmod{16}$, so $\mathcal{O}/\mathfrak{p} = \mathbb{F}_p$ by Lemma 3.1(c), and the discriminant $64A^3$ is a unit at $\mathfrak{p}$. Identify $\mathcal{O}/\mathfrak{p}$ and $\mathbb{Z}[i]/(\pi)$ with $\mathbb{F}_p$, take $D \in \mathbb{Z}$ with $D \equiv A \pmod{\mathfrak{p}}$, and let $\upsilon \in \{\pm 1, \pm i\}$ be the quartic residue symbol of D modulo π, so that $\upsilon \equiv D^{(p-1)/4} \pmod{\pi}$. As $\pi \equiv 1 \pmod{2+2i}$ is primary, the curve $y^2 = x^3 - Dx$, which is $\tilde{E}$, has $p + 1 - \bar{\upsilon}\pi - \upsilon\bar{\pi} = \mathrm{N}(\pi - \upsilon)$ points over $\mathbb{F}_p$ [3, Chapter 18, §4]. As $\upsilon^2 \equiv D^{(p-1)/2} \pmod{\pi}$, $\upsilon = \pm 1$ exactly when D, that is A, is a square modulo $\mathfrak{p}$. □

Theorem 5.2 ([4, v2, Theorem 4.3], with $(\ell, r) = (7, 1 + 3i)$)**.** *Let $k \geq 2$, let $c_1, \dots, c_k$ be distinct integers, D_0 and Y positive integers, $\Lambda_0 > 0$, N_0 an odd squarefree positive integer prime to 210, 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) *$\pi_j \equiv 9 \pmod{16}$, $\pi_j \equiv 1 + i \pmod{3}$, $\pi_j \equiv 6 \pmod{25}$, $\pi_j \equiv 1 + 3i \pmod{7}$ 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 $\mathrm{N}(\pi_j + 1)$, $\mathrm{N}(\pi_j \mp i)$, and each $\mathrm{N}(\pi_j - \alpha)$, $\alpha \in \{\pm 1, \pm i\}$, is prime to $21N_0$.*

It is the four-unit form of Sun's pattern [17, Proposition 10.3].

5.2. **Bounds at the complex places and at fixed primes.**

Lemma 5.3. *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. We follow the proof of [17, Lemma 13.7], where Γ and C are chosen large; here they are fixed by (F2), and $C > \Gamma^2$ gives the bound $\frac{1}{4}$. As $(1 + Cr)^2 \geq 4Cr$, $\varpi \leq \Gamma^2/(4C)$. If $p \mid C$, then $1 + Cr$ is a p-unit. In general $v_p(\varpi) \equiv v_p(r) \pmod{2}$, and if $v_p(r)$ is odd, then $p \mid r$, $1 + Cr$ is a p-unit and $v_p(\varpi) > 0$. □

Fix an embedding $\iota_1 \colon F \to \mathbb{C}$ and put $\iota_2 = \iota_1 \circ \sigma$; by Lemma 3.1(d) every embedding of F in $\mathbb{C}$ is ι_1, ι_2 or the complex conjugate of one of them. Let E^{ι_k} be the complex curve obtained from E by ι_k, $\mathbf{E} = E^{\iota_1}(\mathbb{C}) \times E^{\iota_2}(\mathbb{C})$, a compact abelian Lie group, and $V_{\mathbb{C}} = (\iota_1(V), \iota_2(V))$ for $V \in E(F)$. Then $\iota_1(V^\sigma) = \iota_2(V)$ and $\iota_2(V^\sigma) = \iota_1(V)$: the conjugate point has the two complex coordinates in the reverse order. Let $\mathbf{G}$ be the closure of $\{([k]P)_{\mathbb{C}} : k \in \mathbb{Z}\}$, $\mathbf{G}^0$ its identity component, and $e_{\mathbb{C}}$ the exponent of the finite group $\mathbf{G}/\mathbf{G}^0$.

Lemma 5.4. (a) *For finite sets $Z_k \subset E^{\iota_k}(\mathbb{C})$, the points of $\mathbf{G}^0$ with a coordinate in Z_1 or Z_2 form a closed set with empty interior.*

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

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

Proof. $\mathbf{G}$ is a compact abelian Lie group, so $\mathbf{G}^0$ is a torus of finite index. (a) The projection of $\mathbf{G}$ to $E^{\iota_k}(\mathbb{C})$ is infinite, as P has infinite order, so the projection of $\mathbf{G}^0$, of finite index in it, is a nontrivial homomorphism on a connected group. Its fibers are cosets of a proper closed subgroup, closed with empty interior, and so is a finite union of them. (b) In a compact group the closure of the positive multiples of an element is the closed subgroup it generates. That of $([N^*]P)_{\mathbb{C}}$ is $N^*\mathbf{G} \supseteq N^*\mathbf{G}^0 = \mathbf{G}^0$, and $([h^*]P)_{\mathbb{C}} \in e_{\mathbb{C}}\mathbf{G} \subseteq \mathbf{G}^0$; so the closure of the set is $\mathbf{G}^0$. (c) The closed subgroup $e\mathbf{G}$ contains the identity. □

Formal groups at a prime of F. Let $\mathfrak{Q}$ be a prime of F above p, with $v = v_{\mathfrak{Q}}$ and $e = v(p)$; so $e = 4$ if $p = 2$ and $e = 1$ otherwise. For $s \geq 1$ let $E^{(s)} = \{V \in E_1(F_{\mathfrak{Q}}) : V = O \text{ or } v(\mathfrak{z}(V)) \geq s\}$, the subgroup that corresponds to $\hat{E}(\mathfrak{m}^s)$; these subgroups form a basis of neighborhoods of O in $E(F_{\mathfrak{Q}})$.

- $[p]E^{(s)} \subseteq E^{(s+1)}$, as $[p]$ acts on $\hat{E}$ by pZ plus terms of degree at least 2 with integral coefficients.
- For $s \geq 5$, so that $s > e/(p-1)$, ℓ is an isometry of $\mathfrak{m}^s$ onto itself, inverse to the formal exponential, which is continuous there, as in the proof of Lemma 2.2(a); and $v(\ell_m(Z)) = v(Z)$ for $v(Z) \geq s$, since both sides are $+\infty$ at $Z = 0$ and for $Z \neq 0$ we have $v((b_{t-1}/t)Z^t) \geq tv(Z) - ev_p(t) > v(Z)$ for $t \geq 2$.
- (Depth) Let $J \geq 1$ with $[J]P \in E_1(F_{\mathfrak{Q}})$ for every $\mathfrak{Q} \mid p$, and $k \neq 0$ with $J \mid k$. Then $[k]P \in E^{(1+v_p(k)-v_p(J))}$ at every $\mathfrak{Q} \mid p$, by the first item. If moreover $Jp^4 \mid k$, then $[k]P = [k/(Jp^4)][Jp^4]P$ with $[Jp^4]P \in E^{(5)}$, so by (3.2) and the second item $v(\mathfrak{z}([k]P)) = e\,v_p(k/(Jp^4)) + v(\mathfrak{z}([Jp^4]P))$.
- (Coordinates) If $s \geq 0$ is an integer and $u \in F$ has $v_{\mathfrak{Q}}(u) \geq es$ at every $\mathfrak{Q} \mid p$, then the four coordinates of u have $v_p \geq s$, as $u/p^s \in \mathbb{Z}_{(p)}[\zeta]$.

The next lemma bounds the comparison tests at a fixed prime uniformly in the later choices.

Lemma 5.5. *Let p be a prime, $J \geq 1$ an integer with $[J]P \in E_1(F_{\mathfrak{Q}})$ for every prime $\mathfrak{Q}$ of F above p, $\nu \geq v_p(J) + 4$ an integer, and $n_1, \dots, n_4$ nonzero integers. For an integer h let $D_1(h), \dots, D_{16}(h)$ be the comparison tests of the certificate at $\mathsf{H} = [h]P$, $\mathsf{U}_i = [n_i h]P$, $\mathsf{N}_i = [n_i]P$ and $\beta = n_1$, so that $V_0 = [h - c_*]P$ and $V_i = [n_i]V_0$. There are integers h_p, $b \geq \nu + 1$ and $B_p \geq 0$, with $J \mid h_p$ and $h_p \equiv p^\nu \pmod{p^{\nu+1}}$, such that for every integer h with $J \mid h$ and $h \equiv h_p \pmod{p^b}$ the sixteen tests are defined and $v_{\mathcal{Q}}(D_i(h)) \geq -B_p$ at every prime $\mathcal{Q}$ of L above p.*

Proof. All the points lie in $E(F)$, so $V^\tau = V^\sigma$, $\rho(V_i^\sigma) = \sigma(\rho(V_i))$, and L_i' is the σ-conjugate of $\ell_m(\mathfrak{z}(V_i))/\ell_m(\mathfrak{z}(V_0))$. Let $\mathfrak{Q} \mid p$ be a prime of F, and let h satisfy $J \mid h$ and $v_p(h) = \nu$. By (Depth), H and $\mathsf{U}_i = [n_i]\mathsf{H}$ lie in $E^{(5)} \setminus \{O\}$, so $\rho(\mathsf{H})$ and $\rho(\mathsf{U}_i)$ are integral at $\mathfrak{Q}$; by (3.2) and the second item above, $\ell_m(\mathfrak{z}(\mathsf{H})) \neq 0$ and $v(L_i) = ev_p(n_i) \geq 0$, so $\mathcal{L}(L_1, \dots, L_4)$ and $L_1 - n_1$ are integral at $\mathfrak{Q}$.

Since the L_i are integral, it suffices to bound below the valuations of the σ-conjugates of the values at V_0 of the rational functions $\rho(Y)$, $\rho([n_i]Y)$ and $\ell_m(\mathfrak{z}([n_i]Y))/\ell_m(\mathfrak{z}(Y))$ on E. These are regular off a finite set $\mathcal{Z}$ of points over $\overline{F}$: the points of $E[2]$, those Y with $[n_i]Y \in E[2]$ for some i, and the zeros of $\ell_m \circ \mathfrak{z}$. As P has infinite order, only finitely many k have $[k]P \in [c_*]P + \mathcal{Z}$; choose h_p in the progression $J \mid h$, $h \equiv p^\nu \pmod{p^{\nu+1}}$ outside them, and put $Y_0 = [h_p - c_*]P$. At every prime $\mathfrak{Q} \mid p$ of F these functions are regular at Y_0, so there are $s \geq 1$ and $B' \geq 0$ with all their values on $Y_0 + E^{(s)} \subseteq E(F_{\mathfrak{Q}})$ defined and of valuation at least $-B'$, for every $\mathfrak{Q} \mid p$. Take $b \geq \nu + 1$ with $1 + b - v_p(J) \geq s$. If $J \mid h$

and $h \equiv h_p \pmod{p^b}$, then $v_p(h) = \nu$, and $[h - h_p]P \in E^{(s)}$ by (Depth); so $V_0 \in Y_0 + E^{(s)}$, and $V_0 \neq O$. Hence all sixteen tests are defined, and $v_{\mathfrak{Q}}(D_i(h)) \geq -B'$ at every $\mathfrak{Q} \mid p$, since $v_{\mathfrak{Q}}(\sigma(u)) = v_{\sigma\mathfrak{Q}}(u)$. A prime $\mathcal{Q}$ of L above $\mathfrak{Q}$ has $e(\mathcal{Q}/\mathfrak{Q}) \leq [L : F] = n$, so $B_p = nB'$ will do. □

5.3. **The construction.**

Proposition 5.6. *For every $X \in \mathbb{Z}$ the certificate holds at X.*

Proof. We follow the proof of [17, Proposition 13.9]. Steps 1–8 make the choices, in this order, each depending only on the earlier ones, and Steps 9–12 verify the eighteen predicates.

Step 1 (the input). Take $\beta = 3 + |X^3 + X|$, an odd integer ≥ 3, as $X^3 + X$ is even. Then $r = R_\psi(\beta)$ is a positive integer by Lemma 3.8(d), and ϖ is as in Lemma 5.3. Let $\mathcal{S}$ be the set of rational primes below $\mathfrak{B}$ together with the primes at which ϖ has nonzero valuation, and $g_p = 3 + 2m|v_p(\varpi)|$ for $p \in \mathcal{S}$.

Step 2 (the class of h). Let $J = J_0 e_{\mathbb{C}}$, where J_0 is the least common multiple of the orders of P in the finite groups $E(F_{\mathfrak{Q}})/E_1(F_{\mathfrak{Q}})$, $\mathfrak{Q} \mid p \in \mathcal{S}$. Choose integers $\nu_p \geq v_p(J) + 4 + 2g_p$, and let $\mathcal{C}$ be the set of h with $J \mid h$ and $h \equiv p^{\nu_p} \pmod{p^{\nu_p+1}}$ $(p \in \mathcal{S})$. For $h \in \mathcal{C}$ and $\mathfrak{Q} \mid p \in \mathcal{S}$, (Depth) gives $v_{\mathfrak{Q}}(\rho([h]P)) \geq 2(5+2g_p) \geq eg_p$, so by (Coordinates) the coordinates $G_1, \dots, G_4$ of $\rho([h]P)$ have $v_p \geq g_p$.

Step 3 (a complex neighborhood). Let $\varepsilon_0 = \varpi^m/100$, and $\mathcal{N}$ a neighborhood of the identity in $\mathbf{G}^0$ on which both coordinates avoid $E[2] \setminus \{O\}$ and have $|\rho| < \varepsilon_0$. By Lemma 5.4(a), $\mathcal{N}$ contains a nonempty open set $\mathcal{U}$ whose closure lies in $\mathcal{N}$ and has no point with a coordinate O; so $|\mathfrak{z}| \geq \delta_0$ at both coordinates on $\mathcal{U}$, for some $\delta_0 > 0$.

Step 4 (the index n_2). By Lemma 5.4(c) choose a positive multiple k_* of $MJ \prod_{p \in \mathcal{S}} p^{\nu_p + 2g_p + 4}$ such that both coordinates of $([k_*]P)_{\mathbb{C}}$ have $|\rho| \leq \varepsilon_0$ and $|\mathfrak{z}| \leq \varepsilon_0\delta_0$, and put $n_2 = k_* + 1$. At $\mathfrak{Q} \mid p \in \mathcal{S}$, (Depth) gives $v_{\mathfrak{Q}}(\rho([k_*]P)) \geq eg_p$ and, for $h \in \mathcal{C}$, $v_{\mathfrak{Q}}(\mathfrak{z}([k_*]P)/\mathfrak{z}([h]P)) = e(v_p(k_*) - \nu_p) \geq eg_p$; so by (Coordinates) $G_5, \dots, G_{12}$ have $v_p \geq g_p$. As $u^{(k)} = \frac{1}{4}\operatorname{Tr}_{F/\mathbb{Q}}(u\zeta^{-k})$ for $u \in F$, $|u^{(k)}| \leq \max(|\iota_1(u)|, |\iota_2(u)|)$, and all twelve $|G_k|$ are at most ε_0 when $([h]P)_{\mathbb{C}} \in \mathcal{U}$.

Step 5 (the other indices). Put $n_1 = \beta$, and take positive integers n_3, n_4 with $\mathcal{L}(n_1, n_2, n_3, n_4) = 0$ (Lemma 3.6(b)). The abscissa coordinates a_j and the $y_j = 1 + \varpi a_j^2 > 0$ are now fixed rationals. At ι_1 and ι_2 the sixteen comparison tests are rational functions of $([h]P)_{\mathbb{C}}$, regular off the points with a coordinate in a finite set; for example $\iota_1(\rho(V_0^\sigma)) = \rho(\iota_2([h]P) - \iota_2([c_*]P))$. By Lemma 5.4(a) there is a nonempty open set $\mathcal{U}_1$ with compact closure in $\mathcal{U}$ avoiding those points; on it the tests are defined and their absolute values at all four embeddings are at most some $B_{\mathbb{C}}$.

Step 6 (the classes at $\mathcal{S}$). For each $p \in \mathcal{S}$, Lemma 5.5 with J, $\nu = \nu_p$ and $n_1, \dots, n_4$ gives h_p, b_p and B_p.

Step 7 (the selected primes). For $0 \leq j \leq 16$ and $\theta \in \mathcal{T}^+ \cup \{\xi\}$ let $c_{j,\theta} = (1/q + d_j - \theta)/y_j^2$, a nonzero rational by Lemma 3.10(a); for fixed j the nine values are distinct. Take $D_* \geq 1$ with all $D_*^2 c_{j,\theta} \in \mathbb{Z}$, and apply Theorem 5.2 to the distinct integers among 0 and the $D_*^2 c_{j,\theta}$ $(\theta \in \mathcal{T}^+)$, with the following data. First, $D_0 = \prod_{p \in \mathcal{S}} p^{f_p}$, with f_p so large that, for $w_0 = D_* w$ and every w divisible by D_0,

$$\text{(w1)} \quad v_p(c_{j,\theta} w_0^2) \geq 1 \quad (0 \leq j \leq 16,\ \theta \in \mathcal{T}^+ \cup \{\xi\}),$$

$$\text{(w2)} \quad 4(k_i + 1)e(v_p(w_0) - v_p(y_j)) \geq 3e + 2B_p + (2k_i - 1)e|v_p(\varpi)|$$

for $0 \leq j \leq 16$, $1 \leq i \leq 16$ and every prime $\mathcal{Q}$ of L above p, with $e = v_{\mathcal{Q}}(p)$. Next, N_0 is the product of the odd primes other than 3, 5 and 7 that lie in $\mathcal{S}$ or divide J; $\mathcal{S}'$ is the set of primes dividing D_*, k_*, c_*, or a numerator or denominator of a y_j, a $c_{j,\theta}$

or a nonzero difference $c_{j,\theta}-c_{j,\theta'}$; Y exceeds $m+1$, the primes of $\mathcal{S}\cup\mathcal{S}'$ and the prime divisors of J; the finite set is $\mathcal{S}$; and Λ_0 is so large that $u/w^2>\Lambda_0$ implies, with $\eta=u/w_0^2$, $|R_j-1|\le\frac{1}{100}$, $t_j\ge1$ and $\varpi^{1-2m}2^{2m}B_{\mathbb{C}}^2t_j^{-4}\le\frac{1}{500}$ for every j, which is possible as $s_j\to\infty$ with η. We obtain u and w; let π_0 be the Gaussian prime of norm u that the theorem gives, $a_0=\mathrm{Re}(\pi_0)/w_0$ and $b_0=\mathrm{Im}(\pi_0)/w_0$, so that $\eta=a_0^2+b_0^2$ and (ii) holds. For $\theta\in\mathcal{T}^+\cup\{\xi\}$,

$$s_j+d_j-\theta=\frac{y_j^2}{w_0^2}(u+c_{j,\theta}w_0^2),\qquad R_j=\frac{\prod_{\theta\in\mathcal{T}^+}(u+c_{j,\theta}w_0^2)}{(u+c_{j,\xi}w_0^2)^8},\tag{5.1}$$

and the numerator factors are the *selected primes* $u+D_*^2c_{j,\theta}w^2$ of the j-th detector. A selected prime p' exceeds Y, and $p'\nmid w$, since otherwise $p'\mid u$ and $p'=u>w\ge p'$. So the other factors in (5.1) for the same j are units at p', as $u+c_{j,\theta'}w_0^2\equiv(c_{j,\theta'}-c_{j,\theta})w_0^2$, and $v_{p'}(R_j)=1$.

Step 8 (the index h). Let p' be a selected prime, with Gaussian prime π'. As the primes of M_A are 3 or divide N_0, $\pi'\equiv1+i\pmod{M_A}$, and $p'\nmid\mathrm{N}_{F/\mathbb{Q}}(A)$. The two primes of F above π' are exchanged by σ, the generator of $\mathrm{Gal}(F/\mathbb{Q}(i))$; by (iii), A is a square modulo exactly one of them, $\mathfrak{p}'_+$, and we put $\mathfrak{p}'_-=\sigma\mathfrak{p}'_+$ and $N_\pm(p')=\#\tilde{E}(\mathcal{O}/\mathfrak{p}'_\pm)$. By Lemma 5.1, $N_+(p')=\mathrm{N}(\pi'-\epsilon')$ and $N_-(p')=\mathrm{N}(\pi'-\eta'i)$ with $\epsilon',\eta'\in\{1,-1\}$. Let $\Pi_\pm$ be the least common multiple of the $N_\pm(p')$ over the selected primes, and consider the congruences $h\equiv0\pmod{\Pi_+}$, $h\equiv c_*\pmod{\Pi_-}$, $J\mid h$ and $h\equiv h_p\pmod{p^{b_p}}$ $(p\in\mathcal{S})$. They are compatible. By Theorem 5.2(ii), (iii), no odd prime divides both Π_+ and Π_-; $v_2(\Pi_+)\le6\le\nu_2=v_2(h_2)$, $v_2(\Pi_-)=1$ and $2\mid c_*$; $v_5(\Pi_+)\le2$, $5\nmid\Pi_-$ and $v_5(h_5)=\nu_5\ge\max(2,v_5(J))$; and $\Pi_+\Pi_-$ is prime to 3, 7 and the primes of N_0, so to every other odd prime of $\mathcal{S}$ or of J. So the solutions form a progression $h^*+N^*\mathbb{Z}$ with $N^*>0$, $J\mid h^*,N^*$ and, we may assume, $h^*>|c_*|$. As $e_{\mathbb{C}}\mid J$, Lemma 5.4(b) gives $h=h^*+kN^*$ with $k\ge1$ and $([h]P)_{\mathbb{C}}\in\mathcal{U}_1$; as $h\in\mathcal{C}$, Steps 2 and 4 apply to it. Put $\mathsf{H}=[h]P$, $\mathsf{U}_i=[n_ih]P$, $\mathsf{N}_i=[n_i]P$ $(i\ne2)$ and $\mathsf{Q}=[k_*/M]P$; then $\mathsf{R}=[k_*]P$ and $\mathsf{N}_2=[n_2]P$, and the nine points lie in $\mathbb{Z}P\subseteq2E(L)$. (i) holds, as the labels and $h-c_*$ are nonzero, and the tests are defined by Lemma 5.5. As all ingredients of W_j lie in F or $\mathbb{Q}$, $\Theta_j=\mathrm{Tr}_{F/\mathbb{Q}}(W_j^{-1})$ and B_j are rational (Lemma 3.1(a)), and so are W_{sc} and B_{sc}.

Step 9 (the complex size). At each embedding of F in $\mathbb{C}$, the summand $\alpha_j^{1-2k_i}D_i^2t_j^{-2k_i-2}$ of the i-th factor of W_j has absolute value at most $\varpi^{1-2m}2^{2m}B_{\mathbb{C}}^2t_j^{-4}\le\frac{1}{500}$, as $\varpi<1$, $R_j\ge\frac12$ and $t_j\ge1$. So each conjugate of W_j lies within $(1+\frac{1}{500})^{16}-1<0.04$ of 1, each conjugate of W_j^{-1} within 0.05 of 1, $\Theta_j\in(3.8,4.2)$, and $0<B_j=\varpi R_j/\Theta_j^2<\varpi<\frac14$. As $|G_k|\le\varepsilon_0<\frac12$, $|\Psi(G_k)|\le2|G_k|$, so each summand of W_{sc} lies in $[0,4\varpi^{1-2m}\varepsilon_0^2]\subseteq[0,\frac{1}{500}]$, $1\le W_{\mathrm{sc}}<1.03$ and $0<B_{\mathrm{sc}}=\varpi W_{\mathrm{sc}}^2/16<\varpi$. So no denominator vanishes.

Step 10 (the primes of $\mathcal{S}$). Let $p\in\mathcal{S}$, $\mathcal{Q}$ a prime of L above p and $e=v_{\mathcal{Q}}(p)$. As u is a p-unit, (w1) makes every factor in (5.1) congruent to u modulo p, so R_j is a p-unit, $v_{\mathcal{Q}}(\alpha_j)=ev_p(\varpi)$ and $v_p(t_j)=2v_p(y_j)-2v_p(w_0)$. With $v_{\mathcal{Q}}(D_i)\ge-B_p$ from Lemma 5.5, the summand of the i-th factor of W_j has valuation $(1-2k_i)ev_p(\varpi)+2v_{\mathcal{Q}}(D_i)+4(k_i+1)e(v_p(w_0)-v_p(y_j))\ge3e$ by (w2). So $W_j^{-1}\equiv1\pmod{p^3}$ at every prime above p, and $\Theta_j\equiv4\pmod{p^3}$: $v_2(\Theta_j)=2$ and $v_p(\Theta_j)=0$ for odd p. By Steps 2 and 4, $v_p(\Psi(G_k))=v_p(G_k)\ge g_p$, so each summand of W_{sc} has $v_p\ge2g_p-(2m-1)|v_p(\varpi)|\ge6$, and $v_p(\Theta_{\mathrm{sc}})=v_p(4)$. Hence $v_p(B)=v_p(\varpi)-2v_p(4)$ for each of $B=B_0,\dots,B_{16},B_{\mathrm{sc}}$. By Lemma 5.3, $v_2(B)=2v_2(\Gamma)+v_2(r)-4\ge4$, $v_p(B)=2+v_p(r)\ge2$ for $p\in\{3,5,7,17\}$, and an odd $v_p(B)$ is positive.

Step 11 (the selected primes). Let p' be a selected prime of the j-th detector, and $\mathfrak{p}_\pm=\mathfrak{p}'_\pm$; then $v_{p'}(\alpha_j)=1$ and t_j is a p'-unit. As $N_+(p')\mid h$, H and $\mathsf{U}_i=[n_i]\mathsf{H}$ lie in $E_1(F_{\mathfrak{p}_+})$; as

$N_-(p') \mid h - c_*$, V_0 and $V_i = [n_i]V_0$ lie in $E_1(F_{\mathfrak{p}_-})$. Since $\sigma\mathfrak{p}_+ = \mathfrak{p}_-$, all ten tests $\rho(\cdot)$ have positive valuation at $\mathfrak{p}_+$. By Lemma 3.3(c) over $F_{\mathfrak{p}_\pm} \cong \mathbb{Q}_{p'}$, applied at $\mathfrak{p}_+$ to $Y = P$ with the labels $n_i h$ and h, and at $\mathfrak{p}_-$ to $Y = V_0$ with the labels n_i and 1, $L_i \equiv n_i$ and $L_i' \equiv n_i$ modulo $\mathfrak{p}_+^m$. So $L_i - L_i'$, $\mathcal{L}(L_1, \dots, L_4) \equiv \mathcal{L}(n_1, \dots, n_4) = 0$ and $L_1 - \beta \equiv n_1 - \beta = 0$ have valuation at least m, every summand of W_j is 0 or has valuation $1 + 2v_{\mathfrak{p}_+}(D_i) - 2k_i \geq 1$, and $W_j^{-1} \equiv 1 \pmod{\mathfrak{p}_+}$. At the other three primes $\mathfrak{Q}$ of F above p', every nonzero summand has odd valuation, so each factor $1 + y$ has valuation $\min(0, v_{\mathfrak{Q}}(y))$ and $W_j^{-1} \equiv 0$ or $1 \pmod{\mathfrak{Q}}$. As $F \otimes \mathbb{Q}_{p'} \cong \mathbb{Q}_{p'}^4$, Θ_j is congruent to one of $1, 2, 3, 4$ modulo p', so it is a p'-unit and $v_{p'}(B_j) = 1$. And $v_{p'}(B_{\mathrm{sc}}) = 2v_{p'}(W_{\mathrm{sc}})$ is even.

Step 12 (the predicate). Let B be one of the eighteen elements and $p \notin \mathcal{S}$. Then $v_p(B_{\mathrm{sc}}) = 2v_p(W_{\mathrm{sc}})$, and if p is not a selected prime of the j-th detector, $v_p(B_j) = -8v_p(u + c_{j,\xi} w_0^2) - 2v_p(\Theta_j)$; both are even. With Steps 10 and 11, every negative valuation of B is even, so its reduced denominator is a square, and by Steps 9 and 10 Lemma 3.9(b) applies: $\Phi_K(B)$ holds with rational witnesses. □

6. Proofs of Theorems 1.5 and 1.1

Proof of Theorem 1.5. By Propositions 4.3 and 5.6, the certificate holds at $X \in K$ if and only if $X \in \mathbb{Z}$, and it is a finite system of equations and inequations over F, combined by conjunctions and disjunctions, in unknowns from L and K. A point of E over L is a triple (x, y, o) with $o \in \{0, 1\}$, where $o = 1$ stands for O and $x = y = 0$, and $o = 0$ for the affine point (x, y); the relation $W = U + V$ is a finite disjunction of conjunctions of equations and inequations given by the group law [16, Algorithm III.2.3]. The unknowns of the certificate are β, with $(\beta - 3)^2 = (X^3 + X)^2$, and a_0 and b_0. Each of the nine points is the double of an unknown point of $E(L)$, and the points built from these and from P and $[c_*]P$ in Section 3.5, through fixed addition chains for $[M]\mathsf{Q}$ and the $[c_*]\mathsf{N}_i$, and their conjugates V^τ are unknowns too. Each quotient has an unknown that times the denominator equals the numerator, and each predicate $\Phi_K(B)$ has its witnesses and two more unknowns for its two squares. On these charts x, ρ and $\mathfrak{z}$ are rational, with the values at O as above, and ℓ_m, ℓ_m^σ, F_8, R_ψ and $\mathcal{L}$ are polynomials over F; a condition $g \neq 0$ becomes $gw = 1$ with a new unknown w. Each unknown $y \in L$ is written $y = \sum_{j=0}^{3} c_j \zeta^j$ with four unknowns $c_j \in K$; then $y^{(j)} = c_j$, $\mathrm{Tr}_{L/K}(y) = 4c_0$ and $\tau(y) = \sum_j (-1)^j c_j \zeta^j$ (Lemma 3.1(a)), and an equation over L, reduced with $\zeta^4 = -1$, is four equations over K. As K is real, a conjunction of equations $f_1 = 0, \dots, f_k = 0$ over K is the equation $f_1^2 + \cdots + f_k^2 = 0$, and, with the new unknowns of two disjuncts taken disjoint, a disjunction is the product of their equations. This gives $\mathbf{F}_1 \in K[X, T_1, \dots, T_k]$ such that, for $x \in K$, $\mathbf{F}_1(x, t) = 0$ for some $t \in K^k$ if and only if $x \in \mathbb{Z}$. As in [17, Lemma 4.1], let $\mathbf{F}_2 = \prod_{g \in \mathrm{Gal}(K/\mathbb{Q})} \mathbf{F}_1^g$, where $\mathbf{F}_1^g$ has the coefficients of $\mathbf{F}_1$ transformed by g. Then $\mathbf{F}_2$ is fixed by $\mathrm{Gal}(K/\mathbb{Q})$, so it has rational coefficients. For $x \in K$ and $t \in K^k$, $\mathbf{F}_1^g(x, t) = g(\mathbf{F}_1(g^{-1}x, g^{-1}t))$. Hence $\mathbf{F}_2(x, t) = 0$ for some t if and only if $\mathbf{F}_1(g^{-1}x, t') = 0$ for some g and some t', that is, if and only if $g^{-1}x \in \mathbb{Z}$ for some g, that is, if and only if $x \in \mathbb{Z}$. A positive integer multiple $\mathbf{F}$ of $\mathbf{F}_2$ lies in $\mathbb{Z}[X, T_1, \dots, T_k]$, and $\mathbb{Z}$ is Diophantine in K. □

Proof of Theorem 1.1. For $D = 2$ and $D = 3$ see [17, Theorems 1.2 and 1.3] and [4, Corollary 12.6 and Theorem 1.2(d)]. Let $D \notin \{2, 3\}$. Then K is totally real and Galois, $K \cap F = \mathbb{Q}$ as the quadratic subfields of F are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{2})$ and $D \neq 2$, and $\sqrt{3} \notin K$ as $D \neq 3$. Let $d > 1$ be the odd part of D, and take u, v, w and A as in Theorem 1.4 for d; for $D = 6$ this is $d = 3$. Since $\sqrt{2} \in F$, $L = F(\sqrt{D}) = F(\sqrt{d})$, of degree 2 over F, and

by Lemma 2.9 with $D_1 = d$ the $\mathbb{Z}[i]$-rank of $E_A(L)$ is that of $E_A(F)$ plus that of $E_{d^2A}(F)$. So (a) of Theorem 1.4 gives (i) of Theorem 1.5, and (b) gives (ii). As $A = -4\lambda^2 uvw^2$ and $\mathrm{N}_{F/\mathbb{Q}}(\lambda) = 2$, we have $\mathrm{N}_{F/\mathbb{Q}}(A) = 2^{10}\,\mathrm{N}\,u\,\mathrm{N}\,v(\mathrm{N}\,w)^2$; the three norms are norms of primes of degree one prime to λ, so they are congruent to 1 modulo 8, and $M_A = \mathrm{N}\,u\,\mathrm{N}\,v\,\mathrm{N}\,w$. A Gaussian prime π as in (iii) is therefore $\equiv 1 + i$ modulo $\mathrm{N}\,u\,\mathrm{N}\,v$ and has $\mathrm{N}\,\pi \neq \mathrm{N}\,w$, and Theorem 1.4(c) gives (iii). Theorem 1.5 completes the proof. □

7. Proof of Theorem 1.2

Let a and b be positive odd squarefree integers prime to 65, $K = \mathbb{Q}(\sqrt{5a}, \sqrt{13b})$, $L = KF$, and c the squarefree integer with ab/c a square, so that $5a$, $13b$ and $65c$ represent the three nontrivial classes in $\langle 5a, 13b\rangle \subseteq \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. We check the hypotheses of Theorem 1.5, with $n = 4$, by the lemmas of Section 2.4.

The field. Each of $5a$, $13b$ and $65c$ has odd valuation at 5 or at 13, which are unramified in F, so none of them is a square in F. Hence K is totally real and Galois of degree 4, $[L : F] = 4$, and the quadratic subfields $\mathbb{Q}(\sqrt{5a})$, $\mathbb{Q}(\sqrt{13b})$, $\mathbb{Q}(\sqrt{65c})$ of K are neither $\mathbb{Q}(\sqrt{2})$ nor $\mathbb{Q}(\sqrt{3})$. As K is real and $\mathbb{Q}(\sqrt{2})$ is the largest real subfield of F, $K \cap F = \mathbb{Q}$; and $\sqrt{3} \notin K$.

The marked primes. The Gaussian primes $2 + i$ and $3 - 2i$ have norms 5 and 13, and $i \equiv 3 \pmod{2+i}$, $i \equiv 8 \pmod{3-2i}$ are non-squares modulo 5 and 13. So $\mathfrak{g} = (2+i)\mathcal{O}$ and $\mathfrak{h} = (3-2i)\mathcal{O}$ are primes of F, with residue fields $k_\mathfrak{g} = \mathbb{F}_5(\zeta)$ and $k_\mathfrak{h} = \mathbb{F}_{13}(\zeta)$ of orders 25 and 169, where $\zeta^2 = 3$, resp. 8. An element $x + y\zeta$ of such a field $\mathbb{F}_p(\zeta)$ is a square if and only if its norm $x^2 - \zeta^2 y^2$ is a square modulo p, and every element of $\mathbb{F}_p^\times$ is a square in it. Put $s_\mathfrak{g} = 1 + \zeta$, $s_\mathfrak{h} = 2 + \zeta$ and $t_\mathfrak{p} = s_\mathfrak{p}^2$ for $\mathfrak{p} \in \{\mathfrak{g}, \mathfrak{h}\}$. The norms of $s_\mathfrak{g}$ and $s_\mathfrak{h}$ are -2 and -4, and those of $1 - t_\mathfrak{p} = (1 - s_\mathfrak{p})(1 + s_\mathfrak{p})$ are $(-3)\cdot 1$ and $(-7)\cdot 1$; so $t_\mathfrak{p} \notin \{0, 1\}$ and

$$\chi_\mathfrak{g}(s_\mathfrak{g}) = -1, \qquad \chi_\mathfrak{h}(s_\mathfrak{h}) = 1, \qquad \chi_\mathfrak{g}(1 - t_\mathfrak{g}) = \chi_\mathfrak{h}(1 - t_\mathfrak{h}) = -1. \tag{7.1}$$

The coefficient. Let d_0 be the product of the primes dividing $65ab$. Take $t_\mathfrak{g}$, $t_\mathfrak{h}$ as above and a non-square $t_\mathfrak{p} \in k_\mathfrak{p}$ at every other $\mathfrak{p} \in \mathcal{P}_{d_0}$, and u, v, w as in Lemma 2.6 for d_0, whose norms are prime to $2d_0$. Let $A = -4uv(u - v)^2$ and $X = 2iu(u - v)$. Then (2.2) holds, and (2.3) holds for $\mathfrak{p} \in \mathcal{P}_{d_0}$ with $t = t_\mathfrak{p}$, so A is a non-square unit at $\mathfrak{p} \in \mathcal{P}_{d_0} \setminus \{\mathfrak{g}, \mathfrak{h}\}$, and X is a non-square unit at $\mathfrak{g}$ and $\mathfrak{h}$. For $\mathfrak{p} \in \{\mathfrak{g}, \mathfrak{h}\}$, modulo $\mathfrak{p}$ we have $A \equiv -4t_\mathfrak{p} u^2\lambda^2$ and $\lambda \equiv (1 - t_\mathfrak{p})u$, so $A \equiv (2is_\mathfrak{p} u^2(1 - t_\mathfrak{p}))^2$, and A has a square root $a_\mathfrak{p} \in F_\mathfrak{p}$ with this residue up to sign. As $2i = (1 + i)^2$ and -1 is a square in $k_\mathfrak{p}$, (7.1) gives

$$\chi_\mathfrak{g}(a_\mathfrak{g}) = 1, \qquad \chi_\mathfrak{h}(a_\mathfrak{h}) = -1.$$

E_A over F and the single twists. By Lemma 2.7, with $M = L$ in (b), which is unramified over F at u and v as $\mathrm{N}\,u$ and $\mathrm{N}\,v$ are prime to $2d_0$, $\mathrm{Sel}(A) = \{1, [A], [X], [AX]\}$, $E_A(L)_{\mathrm{tors}} = \{O, T\}$, and $E_A(F)$ has $\mathbb{Z}[i]$-rank one. Let $d = 5a$ and $\mathfrak{p}^* = \mathfrak{g}$, or $d = 13b$ and $\mathfrak{p}^* = \mathfrak{h}$. Then d is prime to $\mathrm{N}\,u\,\mathrm{N}\,v\,\mathrm{N}\,w$, and $w \equiv 1$ modulo every $\mathfrak{p} \in \mathcal{P}_d \subseteq \mathcal{P}_{d_0}$ by Lemma 2.6. Among the primes of $\mathcal{P}_d$, A is a square only at $\mathfrak{p}^*$, where X is a non-square unit. So $E_{d^2A}(F)$ has $\mathbb{Z}[i]$-rank zero by Lemma 2.8(c).

The product twist. Let $d = 65c$, so that $\mathfrak{g}, \mathfrak{h} \in \mathcal{P}_d$; again d is prime to $\mathrm{N}\,u\,\mathrm{N}\,v\,\mathrm{N}\,w$ and $w \equiv 1$ modulo every $\mathfrak{p} \in \mathcal{P}_d$. By Lemma 2.8(a), $W_\mathfrak{p}(d^2A) = W_\mathfrak{p}(A)$ at every prime $\mathfrak{p} \neq \mathfrak{g}, \mathfrak{h}$, as both are the group of unit classes at the other primes of $\mathcal{P}_d$, while $W_\mathfrak{p}(d^2A) = \{1, [da_\mathfrak{p}]\}$ at $\mathfrak{p} \in \{\mathfrak{g}, \mathfrak{h}\}$. Let $z \in \mathrm{Sel}(d^2A)$. Among the primes of $\mathcal{P}_d$, A is a square exactly at $\mathfrak{g}$ and $\mathfrak{h}$, where X is a non-square unit, so Lemma 2.8(b) gives $(-1)^{v_\mathfrak{g}(z)+v_\mathfrak{h}(z)} = 1$, and $v_\mathfrak{g}(z) \equiv v_\mathfrak{h}(z)$

(mod 2). If both are even, z is a square at $\mathfrak{g}$ and $\mathfrak{h}$, so $z \in \mathrm{Sel}(A)$, and $z \in \{1, [A]\}$, since $[X]$ and $[AX]$ are not squares at $\mathfrak{g}$.

Suppose both are odd, so that z is the class of $da_{\mathfrak{p}}$ at $\mathfrak{p} \in \{\mathfrak{g}, \mathfrak{h}\}$, and put $m_0 = (2+i)(3-2i) = 8-i$. Then $m_0 = -i(1+8i)$ is a square in F_λ, as $-i = \zeta^6$ and $1+8i \equiv 1 \pmod{\lambda^{12}}$ (Section 2.2). For $y \in \{u, v, w\}$, Hilbert reciprocity for (m_0, y) gives $(m_0/y) = (y/\mathfrak{g})(y/\mathfrak{h})$. This is 1 for $y = w$, as $w \equiv 1$ modulo $\mathfrak{g}$ and $\mathfrak{h}$. Hilbert reciprocity for (m_0, λ) gives $(\lambda/\mathfrak{g})(\lambda/\mathfrak{h}) = 1$; as $u \equiv \lambda/(1-t_{\mathfrak{p}})$ modulo $\mathfrak{p}$, (7.1) gives $(u/\mathfrak{g})(u/\mathfrak{h}) = 1$; and as $v \equiv t_{\mathfrak{p}} u$ with $t_{\mathfrak{p}}$ a square, $(v/\mathfrak{g})(v/\mathfrak{h}) = 1$. So m_0 is a square at λ, u, v and w and a unit at the other primes $\mathfrak{p} \neq \mathfrak{g}, \mathfrak{h}$, where A is a unit. So $m_0 \in W_{\mathfrak{p}}(A) = W_{\mathfrak{p}}(d^2 A)$ for $\mathfrak{p} \neq \mathfrak{g}, \mathfrak{h}$, and z/m_0 lies in $W_{\mathfrak{p}}(A)$ at every prime, at $\mathfrak{g}$ and $\mathfrak{h}$ because its valuation there is even. Hence $z/m_0 \in \mathrm{Sel}(A) = \{1, [A], [X], [AX]\}$. At $\mathfrak{p} \in \{\mathfrak{g}, \mathfrak{h}\}$, z/m_0 is the class of $da_{\mathfrak{p}}/m_0 = c\,\bar{m}_0 a_{\mathfrak{p}}$, as $65 = m_0 \bar{m}_0$ with $\bar{m}_0 = 8+i$. Here c and $\bar{m}_0$ are units at $\mathfrak{p}$ with residues in $\mathbb{F}_5$, resp. $\mathbb{F}_{13}$, so they are squares in $k_{\mathfrak{p}}$, and the quadratic characters of z/m_0 at $\mathfrak{g}$ and $\mathfrak{h}$ are 1 and -1. But $[A]$ is a square at $\mathfrak{g}$ and $\mathfrak{h}$ and $[X]$ is a non-square unit at both, so each of 1, $[A]$, $[X]$, $[AX]$ has the same character at $\mathfrak{g}$ and at $\mathfrak{h}$. So this case does not occur, $\mathrm{Sel}(d^2 A) = \{1, [A]\}$, and $E_{d^2 A}(F)$ has $\mathbb{Z}[i]$-rank zero by Lemma 2.2(c).

The rank over L. By Lemma 2.9 with $D_1 = 5a$ and $D_2 = 13b$, the $\mathbb{Z}[i]$-rank of $E_A(L)$ is the sum of those of $E_A(F)$, $E_{(5a)^2 A}(F)$, $E_{(13b)^2 A}(F)$ and $E_{(65ab)^2 A}(F)$, and $E_{(65ab)^2 A} \cong E_{(65c)^2 A}$ over F by Lemma 2.1(b), with $t^2 = ab/c$. So E_A has $\mathbb{Z}[i]$-rank $1+0+0+0 = 1$ over L, which with the above gives (i) and (ii) of Theorem 1.5.

The characters. As in the proof of Theorem 1.1, $M_A = \mathrm{N}\,u\,\mathrm{N}\,v\,\mathrm{N}\,w$, so a Gaussian prime π as in (iii) is $\equiv 1+i$ modulo $\mathrm{N}\,u\,\mathrm{N}\,v$ and has $\mathrm{N}\,\pi \neq \mathrm{N}\,w$, and Lemma 2.7(d) gives (iii). Theorem 1.5 completes the proof. □

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 accompanying data package [5] contains both programs, their saved outputs and instructions for running them.

References

1. 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.
2. Manjul Bhargava and Ashay Burungale, *A Diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$*, 2026, Preprint, arXiv:2611.16130v2.
3. 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.
4. Manvir Jaswal, *Diophantine definitions of $\mathbb{Z}$ in totally real fields from rank-one elliptic curves*, 2026, Preprint, Version 2, Zenodo, doi:10.5281/zenodo.24531540.
5. ———, *Programs and data for "$\mathbb{Z}$ is Diophantine in every real quadratic field"*, 2026, Zenodo, doi:10.5281/zenodo.24619048.

6. Wataru Kai, *Linear patterns of prime elements in number fields*, 2026, Preprint, arXiv:2306.16983v5.
7. Peter Koymans and Carlo Pagano, *Elliptic curves of rank one over number fields*, 2025, Preprint, arXiv:2505.16910v1.
8. ———, *Hilbert's tenth problem via additive combinatorics*, J. Amer. Math. Soc. **40** (2027), 195–234, doi:10.1090/jams/1081, arXiv:2412.01768v3.
9. Yuri Matiyasevich, *Diophantine representation of enumerable predicates*, Math. USSR-Izv. **5** (1971), no. 1, 1–28, doi:10.1070/IM1971v005n01ABEH001004.
10. James S. Milne, *Class field theory*, 2020, Course notes, version 4.03, https://www.jmilne.org/math/CourseNotes/CFT.html.
11. 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`.
12. Hector Pasten and Xavier Vidaux, *On Hilbert's tenth problem for number fields*, 2026, Preprint, arXiv:2611.24748v1.
13. 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.
14. Ben Savoie, *Infinitely many elliptic curves over $\mathbb{Q}(i)$ with rank 2 and j-invariant 1728*, 2025, Preprint, arXiv:2506.17605v2.
15. Alexandra Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3556, doi:10.1090/S0002-9947-08-04302-X.
16. 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.
17. Zhi-Wei Sun, *On Hilbert's tenth problem over quadratic fields*, 2026, Preprint, arXiv:2611.25002v3.
18. *$\mathbb{Z}$ is Diophantine in $\mathbb{Q}$: Version 13*, 2026, Research manuscript, November 7, 2026, https://github.com/elliotglazer/diophantine-z-q.
19. David Zywina, *Rank one elliptic curves and rank stability*, 2025, Preprint, arXiv:2505.16960v1.

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