hexagon:2611.00331v3

A PROOF THAT $\mathbb{Z}$ IS DIOPHANTINE IN $\mathbb{Q}$ THROUGH CONGRUENT-NUMBER TWISTS

MANVIR JASWAL

Abstract. We give a proof of Glazer and collaborators' theorem that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$, which builds on OpenAI's proof that Hilbert's tenth problem over $\mathbb{Q}$ has a negative answer. Integers are represented by multiples of a point on an elliptic curve of rank one over $\mathbb{Q}(\sqrt{2})$. An existential condition on two congruent-number twists forbids poles of odd order at odd primes. A height bound at six rational points, from a quaternionic Shimura curve and Serre's conjecture (a theorem of Khare–Wintenberger and Kisin), and a prime pattern from the Green–Tao–Ziegler theorem turn congruences at chosen primes into identities between multiples, and the growth of a Lucas sequence forces integrality. Our contribution is the existence of the rational points that the condition on twists requires: for coprime squarefree integers $\beta > 1$ and $\theta \geq 1$ with $\beta \equiv \theta \equiv 1 \pmod 8$, each a square modulo the primes of the other, there is an integer e such that $y^2 = x^3 - e^2x$ and $y^2 = x^3 - e^2\theta^2 x$ both have rank one and a rational point with abscissa in $\beta\mathbb{Q}^{\times 2}$. Where Glazer and collaborators use a restricted 2-converse theorem, this rests on published theorems: the genus criterion of Tian, Yuan and Zhang, with Gross–Zagier.

Contents

1. Introduction 1
2. The curve and the order of choices 5
3. The pole predicate 6
4. Reading an index at a prime 8
5. The formula 9
6. Two twists with a prescribed point 12
7. Heights at six contacts 18
8. The prime pattern 24
Appendix A. Computations 28
Declarations 28
References 28

1. Introduction

The theorem is Glazer and collaborators' [15],[1] and its proof builds on OpenAI's proof [38].

Date: November 13, 2026.

2020 *Mathematics Subject Classification.* Primary 11U05; Secondary 11G05, 11G18, 11F80, 11B30.

Key words and phrases. Hilbert's tenth problem, Diophantine sets, elliptic curves, congruent numbers, Shimura curves, Serre's conjecture.

[1]The manuscript [15] names no author. Its repository states that it was produced by Elliot Glazer with AI models, and that the project "uses the collective agentic notes from" Stefan Baranczuk, Jose Brox, Gabe Conant, Sohail Farhangi, James Freitag, Elliot Glazer, Jennifer Park and Caroline Terry.

Theorem 1.1. *There are an integer $N \geq 1$ and a polynomial $D \in \mathbb{Z}[X, Y_1, \ldots, Y_N]$ such that, for every $x \in \mathbb{Q}$,*

$$x \in \mathbb{Z} \quad \Longleftrightarrow \quad \text{there is } y \in \mathbb{Q}^N \text{ with } D(x, y) = 0.$$

Robinson defined $\mathbb{Z}$ in $\mathbb{Q}$ by a first-order formula [50], Poonen by a $\forall\exists$-formula [45], and Koenigsmann by a universal one [29]. An existential definition contradicts Mazur's conjecture that the closure of the rational points of a variety over $\mathbb{Q}$ in its real points has finitely many connected components [32], [33, Conjecture 3 and p. 166], so Theorem 1.1 shows that this conjecture is false, as recorded in [15, Corollary 13.1]. Koenigsmann states, in the arXiv versions of his paper, that a strong variant of the Bombieri–Lang conjecture, for varieties over $\mathbb{Q}$ with Zariski-dense rational points, would imply that no infinite subset of $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ [28, §4, Corollary 23]; granting that implication, Theorem 1.1 shows that the variant is false. Denef suggested elliptic curves of rank one in place of Pell's equation [9]; they were used for rings of integers by Poonen [44] and by Cornelissen, Pheidas and Zahidi [6], and over $\mathbb{Q}$ an approach through rank-one curves and local divisibility conditions is due to Pheidas [43]. On that strategy OpenAI proved that Hilbert's tenth problem over $\mathbb{Q}$ has a negative answer [38, Theorem 1.1], by compactness from finite tests that do not define $\mathbb{Z}$, and Glazer and collaborators turned that proof into a definition. With Matiyasevich's theorem [31], Theorem 1.1 recovers the negative answer to Hilbert's tenth problem over $\mathbb{Q}$.

How the formula works. Let $F = \mathbb{Q}(\sqrt{2})$ and $E : y^2 = x^3 - c_0^2 x$ with $c_0 = 3 - \sqrt{2}$. The group $E(F)$ has rank one; fix a torsion-free subgroup $G = \mathbb{Z}P$ of finite index, and call n the *index* of nP. Points of $E(F)$ are tuples of rational numbers, so addition of indices is a polynomial condition over $\mathbb{Q}$; multiplication is not. The formula therefore attaches to each point a rational number, which we call its *proxy*, and writes ring equations between proxies. The work is to make such an equation pass to the indices, and to force a given rational number to be an index. This takes five ideas.

(1) *A test for odd denominators.* An existential condition $\Phi(b)$ on two congruent-number twists forbids odd poles of b at odd primes and holds at $b = qz^2$ for primes $q \equiv 1 \pmod 8$ with $v_q(z) \geq 0$. Asking for Φ at r and at w^2/r^{2L-1} then forces $v_q(w) \geq L$ at every odd prime where r has odd valuation, so the formula never names a prime.

(2) *Reading an index at a prime.* If λP and γP reduce to O above q, the formal logarithm recovers λ/γ modulo a power of q from their coordinates, but not λ itself; reading an index from coordinates through the formal group follows Poonen [44, Lemmas 9 and 11]. A second reduction at the same place, on the conjugate E^σ of E under the nontrivial automorphism σ of F, ties γ to 1 and λ to the index modulo q^{24}. Imposed through (1), this makes a proxy agree with its index modulo q^{24}; the field F is there so that a split prime gives two reductions at one place, whose orders can be made coprime up to 4.

(3) *A height bound.* For six fixed rational numbers c, the height of $t \in \mathbb{Q}$ is at most a constant times the 24th power of the product of the primes where some $t - c$ has positive odd valuation. The exponent 24 comes out of the proof of this bound, and the same number is then the precision in (2). Write the coordinates of a point as sums of three fractions and apply (2) at these primes. If a polynomial equation holds between proxies but not indices, its value at the indices is divisible by q^{24} at each such prime, so it bounds the height of the point, which grows like the square of the index. Once P is replaced by a large enough multiple, quadratic equations therefore pass from proxies to indices.

(4) *Primes to test at.* For the formula to hold when proxies equal indices, every integer must be a sum of three fractions u_j/v with each $u_j - cv$ a bounded multiple of a prime $q \equiv 1 \pmod 8$ at which the reductions of E and its conjugate have orders with greatest common divisor 4. These come from Green–Tao–Ziegler and a sieve.

(5) *Integrality.* Let X be the rational number tested. Exact quadratic equations between indices, among them s and t, encode a Pell equation whose solutions have $\log|t| \gg |s|\log|s|$, while a separate test bounds the height of X^2+2 linearly in $|s|$. By (3) this forces X^2+2 to be an index, so $X \in \mathbb{Z}$.

What this paper adds. The proof of Theorem 1.1 given here uses only published theorems as outside input, with the authors' erratum [18] to one of them. One result here is ours: Theorem 1.2 below, with its use in (1). Glazer and collaborators obtain the corresponding step, their pole completeness theorem [15, Theorem 5.2], from a restricted 2-converse for $y^2 = x(x-\ell)(x+3\ell)$, proved along the lines of OpenAI's [39] with Kato's Euler system at 2; on congruent-number twists the genus criterion of Tian, Yuan and Zhang [59] replaces that converse. The same change of curves, from $y^2 = x(x-\ell)(x+3\ell)$ to $y^2 = x(x-\ell)(x+\ell)$, is made in J. McCarthy's Lean development and accompanying notes [34], with a different Selmer class and genus sum (Remark 6.3).

After the first version of this paper was posted, A. Burungale told us of his paper [3], written independently, which gives a proof that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ by a different deduction. His Theorem B is the counterpart of Theorem 1.2 for $\beta \equiv 7 \pmod 8$, from the genus sum used here, and neither is a case of the other; his Appendix A proves the last assertion of Theorem 6.12, also by an expansion over forests; his Theorem E is a bound of the form of Theorem 1.3, with the same exponent, at five contacts from another Shimura curve.

The rest is Glazer and collaborators' development of OpenAI's proof (its local comparison, the contact framework of its height bound, its curve and its prime-pattern strategy [38, §§2, 4–6]), and is reproved here. The deduction of Theorem 1.1 from Theorems 1.2, 1.3 and 1.4 follows a note in their repository [37], which has no named author and defines $\mathbb{Z}$ without compactness. The note takes a geometric hypothesis, at five contacts with one at infinity, and derives its height bound from it by a preprint of von Känel and Kret [61, (7.19) and Theorem 7.1(ii)]; Theorem 1.3, at six finite contacts, stands in place of both. Theorems 1.4 and 1.2 stand in place of its hypotheses on prime patterns and on rational points, and two further differences are named in Section 5.

The predicate Φ is a simplification of [38, (3.2)]: the curves are congruent-number twists, and the multiplier lists are dropped, since, as in [37], completeness is needed only at qz^2 with $q \equiv 1 \pmod 8$. Theorem 1.3 is [15, Theorem 4.1] in existence form, with modularity from Serre's conjecture at large primes of good reduction [25, 26, 27] in place of their route through Pan's theorem [40]. Theorem 1.4 follows [15, Proposition 6.2] and its proof, restricted to the eighteen forms the formula uses. The polynomial D is not explicit: P is not computed, and the constant of Theorem 1.3 is only shown to exist; explicit polynomials of degree four, the least possible [15, Theorem 18.1], are constructed there.

The three theorems. The proof rests on three theorems, which supply the points for (1), the bound of (3) and the primes of (4). Write $E_\ell : y^2 = x^3 - \ell^2 x$ for $\ell \in \mathbb{Q}^\times$, and let h be the absolute logarithmic height.

The pole predicate. For $b \in \mathbb{Q}^\times$ and $t \in \mathbb{Q}$ with $1 + bt^2 \neq 0$ put

$$U = b\,\frac{1-bt^2}{1+bt^2}, \qquad \Theta = b(b-U^2). \tag{1.1}$$

The *pole predicate* $\Phi(b)$ is the condition that either $b = 0$, or there are $t, e \in \mathbb{Q}$ with $1+bt^2 \neq 0$ and $e\Theta \neq 0$ such that each of E_e and $E_{e\Theta}$ has a rational point with abscissa in $b\mathbb{Q}^{\times 2}$. If $\Phi(b)$ holds and p is an odd prime, a count of valuations shows that $v_p(b)$ is not both negative and odd, since at such a pole $(1 - bt^2)/(1 + bt^2)$ is a p-adic unit, so $v_p(U) = v_p(b)$ and $v_p(\Theta) = 3v_p(b)$. For the converse at $b = qz^2$, with $q \equiv 1 \pmod 8$ prime and $v_q(z) \geq 0$, take t close to a root of $bt^2 = 1$ in $\mathbb{R}$ and in $\mathbb{Q}_2$; then every prime of odd valuation in Θ has b locally a square, so q and the squarefree part θ of Θ satisfy the hypotheses of the next theorem, and the integer e it provides is a witness.

Theorem 1.2. *Let $\beta > 1$ and $\theta \geq 1$ be coprime squarefree integers with $\beta \equiv \theta \equiv 1 \pmod 8$, such that θ is a square modulo every prime dividing β and β is a square modulo every prime dividing θ (we call such a pair* admissible*). Then there is a positive squarefree integer e such that E_e and $E_{e\theta}$ both have analytic rank one and Mordell–Weil rank one, and each has a rational point of infinite order with abscissa in $\beta\mathbb{Q}^{\times 2}$.*

The integer e is built by prescribing quadratic symbols, so that both twists have a 2-Selmer group of dimension three containing a prescribed class. Since the prescribed class makes a bordered Monsky determinant equal to 1 (Lemma 6.6), Smith's identity [57, Theorem 2.2, Table 2, row 5(a)], reproved here from Rédei's theorem [48], makes the first genus sum of [59, Theorem 1.4] odd, which gives analytic rank one, and Gross–Zagier [20] with Bump–Friedberg–Hoffstein [2] gives the point.

Six contacts. Let $\mathcal{C} = \{0, -15, -20, -24, -30, -60\}$; these six numbers are the branch points of the cover used in Section 7, an orbit of a dihedral group of order 12 acting on $\mathbf{P}^1$, and their differences have only the prime factors 2, 3 and 5. For a finite set S of primes and $t \in \mathbb{Q} \setminus \mathcal{C}$, the *contact primes* of t are the primes $p \notin S$ with $v_p(t - c)$ positive and odd for some $c \in \mathcal{C}$, and $M_S(t)$ is their product.

Theorem 1.3. *There is a finite set S_0 of primes such that for every finite set $S \supseteq S_0$ there is a constant $H(S) \geq 1$ with*

$$h(t) \leq H(S)\, M_S(t)^{24} \qquad \text{for every } t \in \mathbb{Q} \setminus \mathcal{C}.$$

If $S \supseteq \{2, 3, 5\}$ and $t \in \mathbb{Q} \setminus \mathcal{C}$, then $M_S(t)$ is the product of the primes outside S dividing the squarefree integer d with $t(t + 15)(t + 20)(t + 24)(t + 30)(t + 60) \in d\,\mathbb{Q}^{\times 2}$; so, with $S = S_0 \cup \{2, 3, 5\}$, every rational point (t, y) with $y \neq 0$ on $dy^2 = t(t+15)(t+20)(t+24)(t+30)(t+60)$, for a squarefree integer d, has $h(t) \leq H(S)\,|d|^{24}$.

A cover of $\mathbf{P}^1$ branched with index two exactly above $\mathcal{C}$ carries a family of abelian surfaces with multiplication by the quaternion algebra of discriminant 6. The fiber over t is defined over a field of bounded degree unramified outside S and the contact primes of t, and it has good reduction at places not above S; $M_S(t)$ enters through the ramification of that field. Fibers with complex multiplication have bounded Faltings height. For any other fiber, a twist descends the two-dimensional piece of its ℓ-adic Tate module to an odd representation of $G_{\mathbb{Q}}$ with prime-to-ℓ conductor $O_S(M_S(t)^2)$, uniformly in ℓ. At each large good ℓ its reduction has weight 2 and comes from a newform of that level by Serre's conjecture [25, 26, 27]. There are finitely many such newforms, so one serves infinitely many ℓ, and Faltings's theorem then makes the fiber an isogeny factor of $J_1(N)$ with N of that size. The bounds of Javanpeykar [24] and of Gaudron and Rémond [14] give $O_S(M_S(t)^{24})$ for its Faltings height, and Pazuki's comparison [42] turns this into the bound on $h(t)$. Bounding the Faltings height in this way is von Känel's method for abelian schemes of GL_2-type [60, Theorem A].

The prime pattern. As in Koymans and Pagano's work on rings of integers [30], additive combinatorics supplies the primes.

Theorem 1.4. *There is a finite set $\mathcal{K}$ of positive integers with the following property. For every $A \in \mathbb{Z}$ and every real B_0 there are integers u_1, u_2, u_3, v with $v \neq 0$ and $u_1+u_2+u_3 = Av$ such that each of the eighteen numbers $u_j - cv$ $(1 \le j \le 3,\ c \in \mathcal{C})$ equals $\varepsilon\kappa q$ with $\varepsilon = \pm 1$, $\kappa \in \mathcal{K}$ and $q > B_0$ a prime such that $q \equiv 1 \pmod 8$, E and E^σ have good reduction above q, and their reductions at a place above q have orders d_1, d_2 with $\gcd(d_1, d_2) = 4$ and $q \nmid d_1 d_2$.*

The lower bound for such patterns is Green and Tao's theorem on linear equations in primes [19], with [16, 17], and a Selberg sieve removes the primes with a larger common factor.

Plan. Sections 2, 3, 4 and 5 prove Theorem 1.1 from Theorems 1.2, 1.3 and 1.4. Sections 6, 7 and 8 prove those three theorems and depend on each other only through the notation of Section 2. What was computed, and with which software, is in Appendix A.

2. The curve and the order of choices

2.1. **Notation.** Throughout, $F = \mathbb{Q}(\sqrt{2})$ and σ is its nontrivial automorphism. We write $c_0 = 3 - \sqrt{2}$, $E : y^2 = x^3 - c_0^2 x$, and $E^\sigma : y^2 = x^3 - (c_0^\sigma)^2 x$; a point Q of $E(F)$ has a conjugate $Q^\sigma \in E^\sigma(F)$. The discriminant of E is $64c_0^6$ and c_0 has norm 7, so E and E^σ have good reduction at every place of F above a prime other than 2 and 7. For a point $Q \neq O$ with $xy \neq 0$ on E or E^σ put

$$\varpi(Q) = \frac{1}{x(Q)}, \qquad z(Q) = -\frac{x(Q)}{y(Q)}, \qquad \text{and} \quad \varpi(O) = z(O) = 0.$$

Then $\varpi(Q^\sigma) = \varpi(Q)^\sigma$ and $z(Q^\sigma) = z(Q)^\sigma$. Let $\log_{24} \in F[Z]$ be the truncation to degree at most 24 of the formal logarithm of E in the parameter z; its coefficients are b_{j-1}/j with $b_{j-1} \in \mathbb{Z}[\sqrt{2}]$ [56, IV.5.5].

The height h is the absolute logarithmic height. We use $h(ab) \le h(a) + h(b)$, $h(a + b) \le h(a) + h(b) + \log 2$, $h(a + b + c) \le h(a) + h(b) + h(c) + \log 3$, $h(\sqrt{2}) = \frac{1}{2}\log 2$, and $h(u/v) = \log\max(|u|, |v|)$ for coprime integers u, v. Let $\hat{h}$ be the canonical height of E [56, VIII.9.3]: $\hat{h}(nQ) = n^2\hat{h}(Q)$, $\hat{h}(Q) > 0$ for Q of infinite order, and there is a constant $C_E \ge 0$ with $|h(x(Q)) - 2\hat{h}(Q)| \le C_E$ for all $Q \neq O$ in $E(\overline{F})$.

2.2. **Rank one.**

Proposition 2.1. *The group $E(F)$ has rank one.*

Proof. The ring $\mathbb{Z}[\sqrt{2}]$ is principal, its units are $\pm(1+\sqrt{2})^{\mathbb{Z}}$, and the units -1 and $1+\sqrt{2}$ have real signs $(-,-)$ and $(+,-)$, so a totally positive unit is a square. The element c_0 is totally positive of norm 7, so it generates a prime with residue field $\mathbb{F}_7$. Let $E' : y^2 = x^3 + 4c_0^2 x$, and let $\alpha : E(F) \to F^\times/F^{\times 2}$ and $\alpha' : E'(F) \to F^\times/F^{\times 2}$ be the descent maps of the 2-isogeny, given by the abscissa away from O and $(0,0)$, with $\alpha(0,0) = -c_0^2$, $\alpha'(0,0) = 4c_0^2$ [56, X.4.8, X.4.9]. Since $E[2] \subset E(F)$, the isogeny carries $E[2]$ onto the kernel of its dual, and the exact sequence of [56, X.4.7] gives $2^{\operatorname{rank} E(F)+2} = |\operatorname{im}\alpha| \cdot |\operatorname{im}\alpha'|$.

On E, a prime $\mathfrak{p} \neq (c_0)$ cannot have $v_\mathfrak{p}(x)$ odd: the right side of the equation would have valuation $3v_\mathfrak{p}(x)$ if $v_\mathfrak{p}(x) < 0$ and $v_\mathfrak{p}(x)$ if $v_\mathfrak{p}(x) > 0$. So $\operatorname{im}\alpha$ lies in the group of order 8 generated by -1, $1 + \sqrt{2}$ and c_0. It contains the classes $1, -1, c_0, -c_0$ of the 2-torsion,

which have equal signs at the two real places. Since $(1+\sqrt{2})^3 - c_0^2(1+\sqrt{2}) = 8$, the point $(1+\sqrt{2}, 2\sqrt{2})$ lies on E, and its abscissa has signs $(+,-)$. So $|\operatorname{im}\alpha| = 8$.

On E', write the equation as $y^2 = x(x^2+4c_0^2)$. A nonzero abscissa is totally positive, since $x^2+4c_0^2 > 0$ at each real place. Suppose $v_{\mathfrak{p}}(x)$ is odd. If $\mathfrak{p} \nmid 2c_0$ the valuation of the right side is odd as before. If $\mathfrak{p} = (\sqrt{2})$, where $v_{\mathfrak{p}}(4c_0^2) = 4$, it is $3v_{\mathfrak{p}}(x)$ or $4 + v_{\mathfrak{p}}(x)$, again odd. If $\mathfrak{p} = (c_0)$, where $v_{\mathfrak{p}}(4c_0^2) = 2$, it is odd unless $v_{\mathfrak{p}}(x) = 1$; in that case $x = c_0 w$ with w a unit at $\mathfrak{p}$, and $y^2 = c_0^3 w(w^2+4)$ forces $w^2 \equiv -4 \pmod{c_0}$, which is impossible because $-4 \equiv 3$ is not a square in $\mathbb{F}_7$. So x is a totally positive unit times a square, hence a square, and $\operatorname{im}\alpha'$ is trivial. Therefore $2^{\operatorname{rank} E(F)+2} = 8$. □

2.3. **The order of choices.** The following objects are fixed once, in this order. None depends on a variable of the formula.

(1) The set S_0 of Theorem 1.3 and the set $\mathcal{K}$ of Theorem 1.4. Then $S = S_0 \cup \{p \le 31\} \cup \{p : p \mid \kappa \text{ for some } \kappa \in \mathcal{K}\}$, a finite set of primes. Every prime $q \notin S$ is at least 37; for such q and a place $\mathfrak{q} \mid q$ of F, the place is unramified and E, E^σ have good reduction at $\mathfrak{q}$.

(2) The constant $H = H(S) \ge 1$ of Theorem 1.3.

(3) An even integer $m_0 \ge 1$ killing the torsion of $E(F)$, and a generator P_0 of the infinite cyclic group $m_0E(F)$ (Proposition 2.1, and the Mordell–Weil theorem [56, VIII.6.7]).

(4) An integer $m_1 \ge 1$ such that

$$C := \frac{C_E + 9H + 3\log 3 + \frac{3}{2}\log 2}{2m_1^2\hat{h}(P_0)} < \frac{1}{4}. \tag{2.1}$$

Then $P = m_1P_0$, $m = m_0m_1$, and $G = mE(F) = \mathbb{Z}P$. The group G is torsion-free, every point of $G \setminus \{O\}$ has $xy \ne 0$, and $P \in 2E(F)$ because m_0 is even. Moreover $\hat{h}(P) = m_1^2\hat{h}(P_0)$.

(5) An integer $m_2 \ge 9$ with $\log(m_2 - 1) > 8H$.

Only P, m, m_2, $\mathcal{K}$ and $\mathcal{C}$ occur in the formula; S and H enter only through the sizes of m_1 and m_2, and no coordinate of P needs to be known.

Since finite conjunctions and disjunctions, inequations and graphs of rational functions over $\mathbb{Q}$ reduce to one polynomial equation in more variables, the formula may quantify over points of $E(F)$, given by their coordinates in the basis $1, \sqrt{2}$ of F, and use the group law; in particular $Q \in G$ is $\exists R \in E(F)\ [m]R = Q$, and $Q \in [m_2]G$ is $\exists R \in E(F)\ [mm_2]R = Q$.

3. The pole predicate

We prove the two properties of the predicate Φ of (1.1) and combine them into a test at a place of F.

Lemma 3.1. *Let p be an odd prime, $b \in \mathbb{Q}^\times$ with $v_p(b)$ odd, and $t \in \mathbb{Q}$ with $1 + bt^2 \ne 0$. Then $v_p(U) = v_p(b)$.*

Proof. If $t \ne 0$ then $v_p(bt^2)$ is odd, hence nonzero, so $(1-bt^2)/(1+bt^2)$ is a p-adic unit. If $t = 0$ then $U = b$. □

Lemma 3.2. (a) *If $\Phi(b)$ holds and p is an odd prime with $v_p(b) < 0$, then $v_p(b)$ is even.*
(b) *If $q \equiv 1 \pmod 8$ is prime and $z \in \mathbb{Q}^\times$ has $v_q(z) \geq 0$, then $\Phi(qz^2)$ holds.*

Proof. (a) Suppose $k = v_p(b) < 0$ is odd, and let t, e be witnesses. By Lemma 3.1, $v_p(U^2) = 2k < k$, so $v_p(\Theta) = 3k$ is odd. Hence exactly one of e and $e\Theta$ has even valuation. Scaling that parameter by a power of p^2, which keeps the square class of the abscissa, we get a point (X, Y) on $E_{e'}$ with e' a p-adic unit and $X \in b\mathbb{Q}^{\times 2}$, so $v_p(X)$ is odd. Then $Y^2 = X(X-e')(X+e')$ has valuation $3v_p(X)$ if $v_p(X) < 0$ and $v_p(X)$ if $v_p(X) > 0$, which is odd. This is a contradiction.

(b) Put $b = qz^2$, so $b > 0$, $k = v_q(b) \geq 1$ is odd, and b is a square in $\mathbb{Q}_2$. By weak approximation choose $t \in \mathbb{Q}$ close to a root of $bt^2 = 1$ in $\mathbb{R}$ and in $\mathbb{Q}_2$. Then U is close to 0 at both places, so $\Theta = b^2(1 - U^2/b)$ is positive and lies in $\mathbb{Q}_2^{\times 2}$. Write $\Theta = \theta c_1^2$ with $\theta \geq 1$ a squarefree integer and $c_1 \in \mathbb{Q}^\times$. We check that (q, θ) is admissible.

Since θ is a square in $\mathbb{Q}_2$, it is odd and $\theta \equiv 1 \pmod 8$. By Lemma 3.1, $v_q(U) = k$, so $v_q(U^2/b) = k > 0$ and $\Theta \in \mathbb{Q}_q^{\times 2}$; thus $q \nmid \theta$ and θ is a square modulo q. Let $p \mid \theta$, so that p is odd and $p \neq q$. Then $v_p(b) = 2v_p(z)$ is even and $v_p(\Theta)$ is odd, so $v_p(b - U^2)$ is odd. This forces $U \neq 0$, $v_p(b) = v_p(U^2)$, and $b/U^2 \in 1 + p\mathbb{Z}_p$. So b, and hence $q = b/z^2$, is a square in $\mathbb{Q}_p$, and q is a square modulo p.

Theorem 1.2 gives a positive squarefree integer e and rational points with abscissa in $q\mathbb{Q}^{\times 2} = b\mathbb{Q}^{\times 2}$ on E_e and on $E_{e\theta}$. The map $(x, y) \mapsto (c_1^2 x, c_1^3 y)$ carries $E_{e\theta}$ to $E_{e\Theta}$ and keeps the square class of the abscissa. Since $1 + bt^2 > 0$ and $e\Theta \neq 0$, the pair t, e is a witness for $\Phi(b)$. □

For $L \geq 1$, $r \in \mathbb{Q}^\times$ and $w \in \mathbb{Q}$, write $\Phi_L(r, w)$ for $\Phi(r) \wedge \Phi(w^2/r^{2L-1})$.

Lemma 3.3. *If $\Phi_L(r, w)$ holds and q is an odd prime with $v_q(r)$ odd, then $v_q(r) > 0$ and $v_q(w) \geq L$. Conversely, if $q \equiv 1 \pmod 8$ is prime and $v_q(w) \geq L$, then $\Phi_L(q, w)$ holds.*

Proof. Lemma 3.2(a) applied to r gives $v_q(r) > 0$. If $w \neq 0$, the number $2v_q(w) - (2L-1)v_q(r)$ is odd, so it is positive by the same lemma, and $v_q(w) \geq L$ because $v_q(r) \geq 1$. Conversely, $\Phi(q)$ is Lemma 3.2(b) with $z = 1$, and if $w \neq 0$ then $w^2/q^{2L-1} = q(w/q^L)^2$ with $v_q(w/q^L) \geq 0$. □

The next device makes all tests at a prime q happen at one place above it. For $D = A + B\sqrt{2} \in F$ with $A, B \in \mathbb{Q}$, and $\rho \in \mathbb{Q}$, write

$$\Phi_L^\rho(r; D) \ : \ \Phi_L(r, (\rho^2 - 2)B) \wedge \Phi_L(r, A + B\rho).$$

Lemma 3.4. *Let $D_1, \ldots, D_l \in F$ and $L_1, \ldots, L_l \geq 1$.*

(a) *If $\Phi_1(r, \rho^2 - 2)$ and all $\Phi_{L_i}^\rho(r; D_i)$ hold and q is an odd prime with $v_q(r)$ odd, then q splits in F and, at the place $\mathfrak{q} \mid q$ with $\sqrt{2} \equiv \rho$, one has $v_\mathfrak{q}(D_i) \geq L_i$ for all i.*
(b) *If $q \equiv 1 \pmod 8$ is prime and $\mathfrak{q} \mid q$ is a place with $v_\mathfrak{q}(D_i) \geq L_i$ for all i, then there is $\rho \in \mathbb{Q}$ such that $\Phi_1(q, \rho^2 - 2)$ and all $\Phi_{L_i}^\rho(q; D_i)$ hold.*

Proof. (a) By Lemma 3.3, $v_q(\rho^2 - 2) \geq 1$. So 2 is a square modulo q, and ρ is a q-adic unit. Let $\eta \in \mathbb{Z}_q$ be the root of $\eta^2 = 2$ with $\eta \equiv \rho \pmod q$. Since $\eta + \rho$ is a unit, $v_q(\eta - \rho) = v_q(\rho^2 - 2)$. At the place $\sqrt{2} \mapsto \eta$, write $D_i = A_i + B_i\sqrt{2}$; then $A_i + B_i\eta = (A_i + B_i\rho) + B_i(\eta - \rho)$, and both summands have valuation at least L_i by Lemma 3.3.

(b) Let $\eta \in \mathbb{Z}_q$ be the image of $\sqrt{2}$ at $\mathfrak{q}$, and choose $\rho \in \mathbb{Q}$ with $v_q(\rho - \eta) \geq \max(\{1\} \cup \{L_i - v_q(B_i) : B_i \neq 0\})$. Then $v_q(\rho^2 - 2) = v_q(\rho - \eta) \geq 1$, the numbers $(\rho^2 - 2)B_i$ have valuation at least L_i, and so does $A_i + B_i\rho = D_i(\mathfrak{q}) + B_i(\rho - \eta)$. Lemma 3.3 gives the assertions. □

4. Reading an index at a prime

This section defines the local condition and proves its two properties (Proposition 4.4). Throughout, $q \notin S$ is a prime, $\mathfrak{q} \mid q$ a place of F, and $v = v_{\mathfrak{q}}$ with $v(q) = 1$. By Section 2.3, $q \geq 37$, the place is unramified, and E, E^σ have good reduction at $\mathfrak{q}$.

Lemma 4.1. *Let $(\mathcal{E}, W)$ be (E, P) or (E^σ, P^σ). Let $U = uW$ and $V = u_0 W$ with $u, u_0 \in \mathbb{Z}$, $u_0 \neq 0$, reduce to the origin at $\mathfrak{q}$. Then:*

(a) $v(z(U)/z(V)) = v_q(u/u_0)$.

(b) *If $\mathcal{E} = E$ and $v_q(u/u_0) \geq 0$, then $\log_{24}(z(V)) \neq 0$ and*

$$v\big(\log_{24}(z(U))/\log_{24}(z(V)) - u/u_0\big) \geq 24.$$

Proof. Let log be the formal logarithm of $\mathcal{E}$ at $\mathfrak{q}$. Its coefficient of Z^j has valuation at least $-v_q(j)$ [56, IV.5.5], and it is a homomorphism on the kernel of reduction, which z identifies with the formal group [56, IV.6.3, IV.6.4, VII.2.2]. Since q is odd, $j - 1 > v_q(j)$ for $j \geq 2$, so $v(\log Z) = v(Z)$ when $v(Z) \geq 1$. From $u_0 U = uV$ we get $u_0 \log z(U) = u \log z(V)$, which proves (a) when $u \neq 0$; if $u = 0$ then $U = O$ and both sides are infinite. For (b), a prime $q \geq 37$ has $j - 1 - v_q(j) \geq 24$ for every $j > 24$. So the tail $\mathcal{R}_{24} = \log - \log_{24}$ satisfies $v(\mathcal{R}_{24}(Z)) \geq v(Z) + 24$ when $v(Z) \geq 1$, while $v(\log_{24}(Z)) = v(Z)$. With $a = u/u_0$,

$$\log_{24} z(U) - a \log_{24} z(V) = a\mathcal{R}_{24}(z(V)) - \mathcal{R}_{24}(z(U)).$$

The right side has valuation at least $v(z(V)) + 24$: the first term because $v(a) \geq 0$, the second because $v(z(U)) \geq v(z(V))$. Divide by $\log_{24} z(V)$, which has valuation exactly $v(z(V))$. □

Lemma 4.2. *Let $q \equiv 1 \pmod 8$ be a prime outside S, with a place $\mathfrak{q} \mid q$ at which the reductions of E and E^σ have orders d_1, d_2 with $\gcd(d_1, d_2) = 4$ and $q \nmid d_1 d_2$. There are integers $\gamma > 1$ and $j \neq 0$ such that γP reduces to the origin on E at $\mathfrak{q}$, jP^σ and $(\gamma - 1)P^\sigma$ reduce to the origin on E^σ at $\mathfrak{q}$, $q^{24} \mid \gamma - 1$, and $q \nmid j$.*

Proof. The residue field is $\mathbb{F}_q$. Each reduced curve has full rational 2-torsion, so doubling has image of index 4 in its group of points. Since $P \in 2E(F)$, the orders e_1, e_2 of the reductions of P and P^σ divide $d_1/4$ and $d_2/4$. So $\gcd(e_1, e_2) = 1$ and $q \nmid e_1 e_2$. Take $\gamma > 1$ with $\gamma \equiv 0 \pmod{e_1}$ and $\gamma \equiv 1 \pmod{e_2 q^{24}}$, and $j = e_2$. □

Definition 4.3. Let $k \geq 1$, $Q = (Q_1, \ldots, Q_k)$ with $Q_i \in G \setminus \{O\}$, $a \in \mathbb{Q}^k$ and $r \in \mathbb{Q}^\times$. Put $Q_0 = P$. The *local condition* $\mathsf{Loc}(r; Q; a)$ is the existence of $V_0, J \in G \setminus \{O\}$, $V_1, \ldots, V_k \in G$ and $\rho \in \mathbb{Q}$ such that, with $Y_i = V_i - Q_i$ $(0 \leq i \leq k)$, the number $\log_{24}(z(V_0))$ is nonzero, $\Phi_1(r, \rho^2 - 2)$ holds, and the following hold:

$$\Phi_1^\rho(r; \varpi(V_i)), \quad \Phi_1^\rho(r; \varpi(Y_i)^\sigma), \quad \Phi_{24}^\rho(r; z(Y_i)^\sigma / z(J)^\sigma) \quad (0 \leq i \leq k),$$
$$\Phi_1^\rho(r; \varpi(J)^\sigma), \quad \Phi_{24}^\rho(r; \log_{24}(z(V_i))/\log_{24}(z(V_0)) - a_i) \quad (1 \leq i \leq k).$$

Here V_0 and V_i are multiples γP and $\lambda_i P$ of P. The tests on $\varpi(V_i)$ make them reduce to the origin on E at one place above each prime q with $v_q(r)$ odd, and the last test compares a_i with λ_i/γ through the logarithm. The tests on Y_i^σ and J^σ, on E^σ at the same place, give $\lambda_i \equiv n_i$ and $\gamma \equiv 1$ modulo q^{24}, where $Q_i = n_i P$.

Proposition 4.4. *Write $Q_i = n_i P$.*

(a) *If $\mathsf{Loc}(r; Q; a)$ holds and $q \notin S$ is a prime with $v_q(r)$ odd, then for every i the number a_i is q-integral and $v_q(a_i - n_i) \geq 24$.*

(b) *If $q \notin S$ is a prime as in Lemma 4.2 and $a \in \mathbb{Q}^k$ has $v_q(a_i - n_i) \geq 24$ for all i, then $\mathsf{Loc}(q; Q; a)$ holds.*

Proof. A point $V \neq O$ reduces to the origin at $\mathfrak{q}$ exactly when $v(\varpi(V)) \geq 1$.

(a) By Lemma 3.4(a), q splits in F and there is one place $\mathfrak{q} \mid q$ at which all the quantities in Definition 4.3 have the prescribed valuations. Write $V_0 = \gamma P$, $J = jP$, $V_i = \lambda_i P$, with $\lambda_0 = \gamma$ and $n_0 = 1$. The points J^σ and Y_i^σ reduce to the origin on E^σ, so Lemma 4.1(a) gives $v_q((\lambda_i - n_i)/j) \geq 24$, and since j is an integer, $v_q(\lambda_i - n_i) \geq 24$ for $0 \leq i \leq k$. In particular $\gamma \equiv 1 \pmod{q^{24}}$, so γ is a unit and

$$\frac{\lambda_i}{\gamma} - n_i = \frac{(\lambda_i - n_i) - n_i(\gamma - 1)}{\gamma}$$

has valuation at least 24. The points V_i and V_0 reduce to the origin on E, so Lemma 4.1(b) applies with $U = V_i$, $V = V_0$. With the last test of Definition 4.3 this gives $v_q(a_i - \lambda_i/\gamma) \geq 24$, hence $v_q(a_i - n_i) \geq 24$. As $n_i \in \mathbb{Z}$, the number a_i is q-integral.

(b) Choose $\mathfrak{q}$ and γ, j as in Lemma 4.2, and put $V_0 = \gamma P$, $J = jP$, $V_i = \gamma n_i P$. Then $Y_0 = (\gamma - 1)P$ and $Y_i = (\gamma - 1)n_i P$. Every V_i reduces to the origin on E, and J^σ and every Y_i^σ on E^σ, at $\mathfrak{q}$. By Lemma 4.1, $\log_{24}(z(V_0)) \neq 0$, $v(\log_{24}(z(V_i))/\log_{24}(z(V_0)) - n_i) \geq 24$, and $v(z(Y_i^\sigma)/z(J^\sigma)) = v_q((\gamma - 1)n_i/j) \geq 24$. Since $v(a_i - n_i) \geq 24$, the ultrametric inequality gives $v(\log_{24}(z(V_i))/\log_{24}(z(V_0)) - a_i) \geq 24$. Lemma 3.4(b) produces ρ. □

5. The formula

We define the height and scalar conditions, prove their properties, and show that the formula (5.1) holds exactly at the integers. The set $\mathcal{C}$, the contact primes and $M_S(t)$ are those of the Introduction.

Lemma 5.1. *Let $u, v \in \mathbb{Q}$ with $v \neq 0$ and $t = u/v \notin \mathcal{C}$. If a prime $q \notin S$ divides $M_S(t)$, then $v_q(u - c'v)$ is odd for some $c' \in \mathcal{C}$.*

Proof. Let $c \in \mathcal{C}$ with $a = v_q(t - c) > 0$ odd, so $v_q(u - cv) = a + v_q(v)$. If $v_q(v)$ is even, take $c' = c$. If $v_q(v)$ is odd, take any $c' \in \mathcal{C} \setminus \{c\}$: the difference $c - c'$ has only the prime factors $2, 3, 5$, so it is a q-adic unit, $v_q(t - c') = 0$, and $v_q(u - c'v) = v_q(v)$. □

Definition 5.2. Let $k \geq 1$, $Q \in (G \setminus \{O\})^k$, $a \in \mathbb{Q}^k$. The *height condition* $\mathsf{Ht}(Q; a)$ is the existence of $\delta \in \mathbb{Q}^\times$ and $b_i, b_i' \in \mathbb{Q}$ with $\delta\, x(Q_i) = b_i + b_i'\sqrt{2}$ $(1 \leq i \leq k)$ such that the following holds. Let $(A_\iota)_{0 \leq \iota \leq 2k}$ be the list $\delta, b_1, \ldots, b_k, b_1', \ldots, b_k'$. For each ι there are $u_{\iota 1}, u_{\iota 2}, u_{\iota 3}, v_\iota \in \mathbb{Q}$ with $v_\iota \neq 0$ and $u_{\iota 1} + u_{\iota 2} + u_{\iota 3} = A_\iota v_\iota$, and for each ι, $j \in \{1, 2, 3\}$ and $c \in \mathcal{C}$ there are $r_{\iota jc} \in \mathbb{Q}^\times$, $\varepsilon \in \{\pm 1\}$ and $\kappa \in \mathcal{K}$ with $u_{\iota j} - cv_\iota = \varepsilon\kappa r_{\iota jc}$ and $\mathsf{Loc}(r_{\iota jc}; Q; a)$, with its own witnesses for each (ι, j, c).

The choice of ε, κ is a finite disjunction. The numbers $u_{\iota j} - cv_\iota$ are nonzero, so each slope $u_{\iota j}/v_\iota$ lies outside $\mathcal{C}$. Three fractions are used, and not two, so that $\mathcal{K}$ does not depend on the number written (Remark 8.1).

Proposition 5.3. *Let $Q_i = n_i P$, $B = \max|n_i|$, and let C be as in (2.1).*

(a) *If $\mathsf{Ht}(Q;a)$ holds with witnesses $u_{\iota j}, v_\iota$, and D_0 is a nonzero integer divisible by q^{24} for every prime $q \notin S$ at which some $u_{\iota j} - cv_\iota$ has odd valuation, then $B^2 \le C|D_0|$.*

(b) *If $\mathsf{Ht}(Q;a)$ holds and $R \in \mathbb{Z}[T_1,\dots,T_k]$ has $R(a) = 0 \ne R(n)$, then $B^2 \le C|R(n)|$. If $a_i \ne n_i$, then $B^2 \le C|D_0|$ for the reduced numerator D_0 of $a_i - n_i$.*

(c) *If $a_i = n_i$ for all i, then $\mathsf{Ht}(Q;a)$ holds.*

Proof. (a) Fix a slope $t = u_{\iota j}/v_\iota$. If $q \notin S$ divides $M_S(t)$, then by Lemma 5.1 some $u_{\iota j} - c'v_\iota$ has odd valuation at q, so $q^{24} \mid D_0$. As $M_S(t)$ is squarefree, $M_S(t)^{24}$ divides D_0, and Theorem 1.3 gives $h(t) \le H|D_0|$. Each A_ι is a sum of three slopes, so $h(A_\iota) \le 3H|D_0| + \log 3$. Since $x(Q_i) = (b_i + b_i'\sqrt{2})/\delta$,

$$h(x(Q_i)) \le h(b_i) + h(b_i') + h(\delta) + h(\sqrt{2}) + \log 2 \le 9H|D_0| + 3\log 3 + \tfrac{3}{2}\log 2.$$

Using $2\hat{h}(Q_i) \le h(x(Q_i)) + C_E$ and $|D_0| \ge 1$, we get $2n_i^2\hat{h}(P) \le |D_0|(C_E + 9H + 3\log 3 + \frac{3}{2}\log 2)$, which is $n_i^2 \le C|D_0|$ by (2.1).

(b) Let $q \notin S$ be a prime where a number $u_{\iota j} - cv_\iota = \varepsilon\kappa r_{\iota jc}$ has odd valuation. Since κ is a q-adic unit, $v_q(r_{\iota jc})$ is odd, and Proposition 4.4(a) makes every a_i q-integral with $a_i \equiv n_i \pmod{q^{24}}$. Hence $R(n) \equiv R(a) = 0 \pmod{q^{24}}$, and q^{24} divides the reduced numerator of $a_i - n_i$. Apply (a).

(c) Take δ a positive integer clearing the denominators of the coefficients of every $x(Q_i)$, so that all A_ι are integers. Apply Theorem 1.4 to each A_ι with $B_0 > \max S$. For a number $\varepsilon\kappa q$ of the pattern put $r = q$; then $q \notin S$, and $\mathsf{Loc}(q;Q;a)$ holds by Proposition 4.4(b). □

Definition 5.4. For $\beta \in \mathbb{Q}$ and $Q_s \in G \setminus \{O\}$, the *scalar condition* $\mathsf{Sc}(\beta, Q_s)$ is the existence of $u_1, u_2, u_3, v \in \mathbb{Q}$ with $v \ne 0$, $u_1 + u_2 + u_3 = \beta v$, and, for each $j \in \{1,2,3\}$ and $c \in \mathcal{C}$, of $r_{jc} \in \mathbb{Q}^\times$, $\varepsilon \in \{\pm 1\}$ and $\kappa \in \mathcal{K}$ with $u_j - cv = \varepsilon\kappa r_{jc}$ and $\mathsf{Loc}(r_{jc};(Q_s);0)$.

Lemma 5.5. *If $\mathsf{Sc}(\beta, sP)$ holds then $h(\beta) \le 3H|s| + \log 3$. For every $\beta \in \mathbb{Z}$ and every integer $m' \ge 1$, $\mathsf{Sc}(\beta, sP)$ holds for infinitely many positive multiples s of m'.*

Proof. Let $q \notin S$ with $v_q(r_{jc})$ odd. Proposition 4.4(a) with $Q = (sP)$ and $a = (0)$ gives $q^{24} \mid s$. By Lemma 5.1 and the fact that κ is a q-adic unit, every prime of $M_S(u_j/v)$ is such a prime. So $M_S(u_j/v)^{24} \le |s|$, $h(u_j/v) \le H|s|$ by Theorem 1.3, and $h(\beta) \le 3H|s| + \log 3$.

For the second assertion, apply Theorem 1.4 with $A = \beta$ and $B_0 > \max S$, with $r_{jc} = q_{jc}$ the primes obtained; they depend on β only. Let s be any positive common multiple of m' and all q_{jc}^{24}. Each q_{jc} is a prime outside S as in Lemma 4.2, so Proposition 4.4(b) with $Q = (sP)$ and $a = (0)$ gives $\mathsf{Loc}(q_{jc};(sP);0)$. □

The equation in (a) below is Matiyasevich's form of the Pell equation [31, Lemma 18], and reading a divisibility of j from the congruence $f_j \equiv j \pmod{\alpha - 2}$ is his device [31, Lemma 22].

Lemma 5.6. *Let $\alpha \ge 7$ be an integer and define $f_0 = 0$, $f_1 = 1$, $f_{j+1} = \alpha f_j - f_{j-1}$. Then:*

(a) *Every integer solution (t,y) of $t^2 - \alpha ty + y^2 = 1$ with $y \ne 0$ has $|y| = f_k$ and $|t| \in \{f_{k-1}, f_{k+1}\}$ for some $k \ge 1$.*

(b) *If s,t,w are integers with $|s| = \alpha$, $w \ne 0$, and $t^2 - s(s-2)tw + (s-2)^2w^2 = 1$, then $|t| \ge (\alpha-1)^{\alpha-4}$.*

(c) *For $s = \alpha$ there are positive integers t,w satisfying the equation of* (b).

Proof. By induction, $f_{j+1} \geq (\alpha-1)f_j$, so $f_j \geq (\alpha-1)^{j-1}$ for $j \geq 1$. Modulo $\alpha-2$ the recurrence gives $f_j \equiv j$, and modulo $\alpha+2$ it gives $f_j \equiv (-1)^{j-1}j$. Also $f_{j+1}^2 - \alpha f_{j+1}f_j + f_j^2 = f_j^2 - f_{j-1}f_{j+1}$ for $j \geq 1$, and this equals the same expression with $j-1$ in place of j, so its value is 1.

(a) If $t = 0$ then $y^2 = 1$ and $k = 1$. Otherwise $\alpha t y = t^2 + y^2 - 1 > 0$, so we may take $t, y > 0$; and $t \neq y$ since $t^2(2-\alpha) \neq 1$. By symmetry it suffices to show that a solution with $t > y > 0$ is (f_{k+1}, f_k) for some $k \geq 1$. Argue by induction on y. If $y = 1$ then $t = \alpha = f_2$. If $y \geq 2$, then $t' = \alpha y - t = (y^2-1)/t$ satisfies $0 < t' < y$, so by induction $(y, t') = (f_{k+1}, f_k)$ and $t = \alpha f_{k+1} - f_k = f_{k+2}$.

(b) Let $y = \operatorname{sgn}(s)(s-2)w \neq 0$. Then $\alpha y = s(s-2)w$, and the equation is that of (a), so $|y| = f_k$ and $|t| \geq f_{k-1}$. If $s > 0$ then $(\alpha-2) \mid f_k$, so $(\alpha-2) \mid k$; if $s < 0$ then $(\alpha+2) \mid f_k$, so $(\alpha+2) \mid k$. Either way $k \geq \alpha-2$ and $|t| \geq f_{k-1} \geq (\alpha-1)^{\alpha-4}$.

(c) Take $k = \alpha-2$, $w = f_k/(\alpha-2)$, and $t = f_{k+1}$. □

With m_2 as in Section 2.3, let $\mathsf{Int}(X)$ be the condition that, with $\beta = X^2+2$, there are points $Q_n, Q_s, Q_t, Q_w, Q_g, Q_{g'} \in G \setminus \{O\}$ with $Q_s \in [m_2]G$ and $\xi, \tau, \omega, \nu, \mu \in \mathbb{Q}$ such that

$$\begin{gathered} \nu = (\xi-2)\omega, \qquad \mu = \xi\nu, \qquad \tau^2 - \mu\tau + \nu^2 = 1, \\ \mathsf{Ht}((Q_n, Q_s, Q_t, Q_w, Q_g, Q_{g'}); (\beta, \xi, \tau, \omega, \nu, \mu)), \qquad \mathsf{Sc}(\beta, Q_s). \end{gathered} \tag{5.1}$$

Two further points differ from [37]: Sc uses the local condition with proxy 0 in place of a separate test on auxiliary points, and the guard $Q_s \in [m_2]G$ replaces a finite list of excluded multiples of P.

Theorem 5.7. *For $X \in \mathbb{Q}$, $\mathsf{Int}(X)$ holds if and only if $X \in \mathbb{Z}$.*

Proof. Suppose $\mathsf{Int}(X)$. Write the six points as $nP, sP, tP, wP, gP, g'P$ and let $B \geq 1$ be the largest absolute value of the six indices. Since $Q_s \in [m_2]G \setminus \{O\}$, we have $\alpha := |s| \geq m_2 \geq 9$. The polynomials

$$R_1 = T_5 - (T_2-2)T_4, \qquad R_2 = T_6 - T_2T_5, \qquad R_3 = T_3^2 - T_6T_3 + T_5^2 - 1$$

vanish at the proxies and are at most $4B^2$ in absolute value at the indices. If one of them were nonzero at the indices, Proposition 5.3(b) would give $B^2 \leq 4CB^2 < B^2$. Hence $g = (s-2)w$, $g' = sg$ and $t^2 - g't + g^2 = 1$, so t, s, w satisfy the equation of Lemma 5.6(b), with $w \neq 0$. Therefore, using $\alpha - 4 \geq \alpha/2$ and the choice of m_2,

$$\log B \geq (\alpha-4)\log(\alpha-1) > 4H\alpha. \tag{5.2}$$

Suppose $\beta \neq n$, and let D_0 be the reduced numerator of $\beta - n$. Writing β in lowest terms gives $|D_0| \leq (1+B)e^{h(\beta)} \leq 2Be^{h(\beta)}$. By Proposition 5.3(b), $B^2 \leq 2CBe^{h(\beta)}$. With Lemma 5.5 and $C < \frac{1}{4}$ this gives

$$\log B \leq \log(2C) + h(\beta) < 3H\alpha + \log\tfrac{3}{2}. \tag{5.3}$$

Since $H\alpha \geq 9$, the inequalities (5.2) and (5.3) contradict each other. So $X^2 + 2 = n \in \mathbb{Z}$, and $X \in \mathbb{Z}$ because X is rational.

Conversely let $X \in \mathbb{Z}$ and $n = X^2 + 2$. By Lemma 5.5, choose a positive multiple s of m_2 with $\mathsf{Sc}(n, sP)$; then $s \geq 9$. Choose positive t, w by Lemma 5.6(c), and put $g = (s-2)w$, $g' = sg$. These six integers are positive, the proxies $(\beta, \xi, \tau, \omega, \nu, \mu) = (n, s, t, w, g, g')$ satisfy the three equations of (5.1), and Ht holds by Proposition 5.3(c). □

Proof of Theorem 1.1. By Section 2.3, $\mathsf{Int}(X)$ is a finite positive existential formula over $\mathbb{Q}$ in the single free variable X, so it is equivalent to $\exists y \in \mathbb{Q}^N\ D(X, y) = 0$ for a polynomial D over $\mathbb{Z}$. Apply Theorem 5.7. □

6. Two twists with a prescribed point

By Proposition 6.2, Theorem 1.2 follows once each of $\ell = e$ and $\ell = e\theta$, both $\equiv 5 \pmod 8$, satisfies three conditions: a class (β, d) with $d \equiv 5 \pmod 8$ lies in the 2-Selmer group of E_ℓ, that group has dimension three, and the first genus sum is odd. The Selmer group is the solution space of a linear system over $\mathbb{F}_2$ whose coefficients are quadratic symbols at the primes of ℓ (Lemma 6.4), so the first condition is met by prescribing symbols. The class then gives a vector k in the kernel of a symmetric matrix M whose corank is the dimension of the Selmer group less two (Lemmas 6.5 and 6.6). So the second condition says that k spans the kernel, and this holds exactly when the matrix $M^{(c)}$, which is M with the row and column of a coordinate c with $k_c = 1$ deleted, is invertible (Lemma 6.13). The third condition then follows from the first two: the genus sum is, modulo 2, the determinant of M bordered by a fixed vector b (Theorem 6.12), and $b \cdot k = 1$ for this class, so that determinant is 1 when k spans the kernel (Lemma 6.6). It remains to make $M^{(c)}$ invertible for e and for $e\theta$ at once. For e, auxiliary primes merge the primes of β into one index (Lemma 6.14), which leaves a configuration on five indices where the system is solved by hand (Lemma 6.15). For $e\theta$, the symbols between one prime of e and the primes of θ are not constrained by the class, and $\det M^{(c)}$ is a multilinear function of them whose top coefficient is the determinant for e; so some choice of these symbols keeps it nonzero (Lemma 6.16). Section 6.1 sets up the system and M, Section 6.2 proves the identity with the genus sum, and Section 6.3 builds e.

For a positive squarefree integer ℓ the curve $\ell y^2 = x^3 - x$ of [59] is isomorphic over $\mathbb{Q}$ to E_ℓ, by $(x, y) \mapsto (\ell x, \ell^2 y)$. The 2-torsion of E_ℓ is rational, and 2-descent is the injection [56, X.1.4]

$$\partial : E_\ell(\mathbb{Q})/2E_\ell(\mathbb{Q}) \hookrightarrow (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2, \qquad \partial(x, y) = (x, x - \ell) \quad (x \neq 0, \ell),$$

with $\partial(0, 0) = (-1, -\ell)$, $\partial(\ell, 0) = (\ell, 2)$, $\partial(-\ell, 0) = (-\ell, -2\ell)$ and $\partial(O)$ trivial. We write $\mathrm{Sel}(\ell)$ for the 2-Selmer group of E_ℓ in these coordinates. For a positive squarefree d let $g(d) = \#2\,\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$, as in [59, p. 722]. For $\ell \equiv 5 \pmod 8$ the first genus sum of [59, Theorem 1.4] is

$$\Sigma_1(\ell) = \sum_{\ell = d_0 d_1 \cdots d_k} \prod_{i=0}^{k} g(d_i),$$

over unordered factorizations with all $d_i > 1$ and $d_i \equiv 1 \pmod 8$ for $i > 0$, with $k = 0$ allowed. Theorem 1.2 follows from the next two statements, applied to $\ell = e$ and $\ell = e\theta$.

Theorem 6.1. *Let (β, θ) be admissible. There are a positive squarefree integer $e = \beta m$ with m prime to $2\beta\theta$, and a divisor $d \equiv 5 \pmod 8$ of m, such that for $\ell = e$ and for $\ell = e\theta$: $\ell \equiv 5 \pmod 8$, $\dim_{\mathbb{F}_2} \mathrm{Sel}(\ell) = 3$, $(\beta, d) \in \mathrm{Sel}(\ell)$, and $\Sigma_1(\ell)$ is odd.*

Proposition 6.2. *Let ℓ be positive and squarefree with $\ell \equiv 5 \pmod 8$ and $\Sigma_1(\ell)$ odd. Suppose that $\dim_{\mathbb{F}_2} \mathrm{Sel}(\ell) = 3$ and that $\mathrm{Sel}(\ell)$ contains a class (β, d). Then E_ℓ has analytic rank one and Mordell–Weil rank one, and the class is $\partial(Q)$ for a point Q of infinite order. In particular $x(Q) \in \beta\mathbb{Q}^{\times 2}$.*

Proof. Tian, Yuan and Zhang attach to $\ell y^2 = x^3 - x$ a number $L(\ell)$, defined up to sign, which vanishes if the order of vanishing at $s = 1$ exceeds one [59, p. 722]. Their Theorem 1.4 [59, pp. 723–724] states that $L(\ell)$ is an integer and, for $\ell \equiv 5 \pmod 8$, that $\Sigma_1(\ell)$ is even whenever $2^{-\rho(\ell)} L(\ell)$ is, where $\rho(\ell) \geq 0$ is the integer defined in [59, p. 723]: for such ℓ the first of the two sums printed there is $\Sigma_1(\ell)$. So $\Sigma_1(\ell)$ odd gives $L(\ell) \neq 0$ and order at most one, and the root number is -1 [59, p. 722], so the order is exactly one.

The curve E_ℓ has complex multiplication by $\mathbb{Z}[i]$, so it is modular [54, p. 200], and Gross and Zagier's theorem [20, Ch. I, (7.3)(1), p. 231], that a modular elliptic curve E over $\mathbb{Q}$ with $L(E,1)=0$ and $L'(E,1)\neq 0$ has a rational point of infinite order, gives $r=\operatorname{rank} E_\ell(\mathbb{Q})\geq 1$; the imaginary quadratic field that its proof takes from Waldspurger's theorem [20, Ch. V, §2, p. 312] is also supplied by [2, Theorem (ii), p. 544].

Since $E_\ell[2]$ is rational, $\dim E_\ell(\mathbb{Q})/2E_\ell(\mathbb{Q})=2+r$, and ∂ embeds this group in $\mathrm{Sel}(\ell)$, of dimension 3. Hence $r=1$ and ∂ is onto. So the class is $\partial(Q)$ for some Q; if Q has finite order, replace it by $Q+2Q'$ with Q' of infinite order. Then $x(Q)\notin\{0,\pm\ell\}$, so the first coordinate of $\partial(Q)$ is the class of $x(Q)$. □

Remark 6.3. In McCarthy's notes [34] the 2-Selmer class has first coordinate of absolute value $\equiv 7 \pmod 8$ and the criterion is the part of Tian–Yuan–Zhang's second genus sum with factors $d_0\equiv 7$, $d_1\equiv 3 \pmod 8$, which is L_{5b} in [57, Table 2], whereas here the class is (β,d) with $\beta\equiv 1$, $d\equiv 5 \pmod 8$ and the criterion is their first sum Σ_1.

6.1. **The Selmer group as a linear system.** Let $\ell=p_1\cdots p_r$ be odd and squarefree. For an odd prime p and a p-adic unit a, let $\left[\frac{a}{p}\right]\in\mathbb{F}_2$ be 0 exactly when a is a square modulo p. Put $y_i=\left[\frac{-1}{p_i}\right]$, $z_i=\left[\frac{2}{p_i}\right]$, and $a_{ij}=\left[\frac{p_j}{p_i}\right]$ for $i\neq j$. Thus $p_i\equiv 1,3,5,7 \pmod 8$ according as $(y_i,z_i)=(0,0),(1,1),(0,1),(1,0)$, and reciprocity reads $a_{ij}+a_{ji}=y_iy_j$. The *Rédei matrix* A has entries $A_{ij}=a_{ij}$ for $i\neq j$ and $A_{ii}=\sum_{j\neq i}a_{ij}$, so $A\mathbf{1}=0$. We write D_v for the diagonal matrix of a vector v. Any data $(y,z,(a_{ij}))$ on a finite index set I with $a_{ij}+a_{ji}=y_iy_j$ will be called a configuration on I; apart from Lemma 6.4 and Proposition 6.7, everything below is linear algebra over $\mathbb{F}_2$ valid for all configurations. For $T\subseteq I$ put $Y_T=\sum_T y_i$, $Z_T=\sum_T z_i$, and say that T has *type* $1,5,3,7$ when $(Y_T,Z_T)=(0,0),(0,1),(1,1),(1,0)$, which for primes is $\prod_T p_i$ modulo 8. The j-th column sum of A is $y_j(Y_I+1)$, so if $Y_I=0$,

$$A+A^{\top}=yy^{\top}+D_y,\qquad A\mathbf{1}=0,\qquad A^{\top}\mathbf{1}=y. \tag{6.1}$$

Lemma 6.4. *Let $\ell\equiv 5 \pmod 8$. Then $\mathrm{Sel}(\ell)$ consists of the classes*

$$\Big((-1)^{\varepsilon}\prod_i p_i^{u_i},\ (-1)^{\varepsilon}2^{z\cdot u}\prod_i p_i^{w_i}\Big)$$

for the solutions $(\varepsilon,u,w)\in\mathbb{F}_2\times\mathbb{F}_2^r\times\mathbb{F}_2^r$ of the system

$$\text{(S1) } Au+D_yw=\varepsilon y,\qquad \text{(S2) } (A+D_y)w+D_zu+(z\cdot u)z=\varepsilon y,\qquad \text{(S3) } y\cdot w=y\cdot u.$$

Proof. We compute the local images, using $|E_\ell(\mathbb{Q}_p)/2E_\ell(\mathbb{Q}_p)|=4|2|_p^{-1}$. At ∞, the image is generated by $\partial(0,0)$: the two coordinates have the same sign. At odd $p\nmid\ell$ it is the group of unramified classes. At p_i, the classes $\partial(0,0)$ and $\partial(\ell,0)$ have valuation vectors $(0,1)$ and $(1,0)$, so they span the image. At 2, since $\ell/5\in\mathbb{Q}_2^{\times 2}$ we may take $\ell=5$; the classes $\partial(0,0)=(-1,-5)$, $\partial(5,0)=(5,2)$ and $\partial(-4,6)=(-1,-9)$ are independent, so they span the image, of order 8. Writing $a=2^va'\in\mathbb{Q}_2^{\times}$ with a' a unit, $s(a)=[a'\equiv 3 \bmod 4]$ and $t(a)=[a'\equiv\pm 3 \bmod 8]$, this image is $\{v(d_1)=0,\ v(d_2)=t(d_1),\ s(d_2)=s(d_1)\}$.

A Selmer class is supported on $-1,2,p_1,\dots,p_r$. The real condition equates the signs, and the condition at 2 gives no 2 in the first coordinate, the exponent $z\cdot u$ in the second, and (S3). At p_i the valuations (u_i,w_i) force the local class to be $\partial(0,0)^{w_i}\partial(\ell,0)^{u_i}$, and comparing unit parts of the two coordinates modulo squares gives row i of (S1) and of (S2). □

Let M be the $2r\times 2r$ symmetric matrix on coordinates $(U,W)\in\mathbb{F}_2^r\times\mathbb{F}_2^r$,

$$M=\begin{pmatrix}A+A^{\top} & A^{\top}\\ A & D_z\end{pmatrix},\qquad M_5=\begin{pmatrix}M & b\\ b^{\top} & 0\end{pmatrix},\quad b=\begin{pmatrix}y+z\\ 0\end{pmatrix}.$$

For $\ell \equiv 5 \pmod 8$, M and M_5 appear in [57, Table 2], whose notation y, z, A, D_v we use, and the next lemma is Monsky's matrix description [21, pp. 366–367] in these coordinates. Smith notes that M has corank one exactly when some bordered determinant of this shape is nonzero [57, p. 3]; Lemma 6.6 proves the direction used here for the border b and the class (β, d).

Lemma 6.5. *For a configuration of type* 5*, the map* $\Xi(u, w) = (u+w+(1+y\cdot u)\mathbf{1},\ u+\mathbf{1})$ *is a bijection from the solutions of* (S1)–(S3) *with* $\varepsilon = 0$ *and* $z\cdot u = 1$ *onto* $\ker M$*. The space of all solutions of* (S1)–(S3) *has dimension* $2+\operatorname{corank} M$*; in particular* $\dim \mathrm{Sel}(\ell) = 2+\operatorname{corank} M$ *for* $\ell \equiv 5 \pmod 8$.

Proof. Put $c = 1 + y\cdot u$, $U = u + w + c\mathbf{1}$, $W = u + \mathbf{1}$. Using (6.1), (S1) and (S2) with $\varepsilon = 0$ and $z\cdot u = 1$,

$$AU + D_z W = Au + Aw + D_z u + z = D_y w + (D_y w + D_z u + z) + D_z u + z = 0,$$

and, with $A^\top w = y(y\cdot w) + D_y w + Aw$,

$$(A + A^\top)U + A^\top W = y(y\cdot w + c + 1) = y(y\cdot(u+w)) = 0$$

by (S3). Conversely, for $(U, W) \in \ker M$, summing the two block equations gives $y\cdot U = 0$ and $z\cdot W = 0$; then $u = W + \mathbf{1}$, $w = U + u + (1 + y\cdot W)\mathbf{1}$ solves (S1)–(S3) with $z\cdot u = 1$, and the two maps are inverse. The solutions with $\varepsilon = 0$ have index two, since $(1, 0, \mathbf{1})$, the class $\partial(0, 0)$, has $\varepsilon = 1$. The condition $z\cdot u = 1$ cuts out the nontrivial coset of an index-two subgroup, since $(0, \mathbf{1}, 0)$, the class $\partial(\ell, 0)$, has $z\cdot\mathbf{1} = 1$. So the number of solutions is $4|\ker M|$. □

Lemma 6.6. *Let* $\ell \equiv 5 \pmod 8$, $\beta \mid \ell$ *with* $\beta \equiv 1 \pmod 8$ *and prime set* B*, and* $d \mid \ell$ *with* $d \equiv 5 \pmod 8$ *and indicator vector* w*. If* $(\beta, d) \in \mathrm{Sel}(\ell)$*, then* $k = (\mathbf{1}_B + w, \mathbf{1}_B) \in \ker M$ *and* $b\cdot k = 1$*. If moreover* $\dim \mathrm{Sel}(\ell) = 3$*, then* $\det M_5 = 1$.

Proof. The class is the solution $(0, \mathbf{1}_B, w)$; adding $(0, \mathbf{1}, 0)$ gives $u = \mathbf{1}_B + \mathbf{1}$ with $z\cdot u = 1$ and $y\cdot u = 0$, and Ξ of it is k. Then $b\cdot k = (y+z)\cdot\mathbf{1}_B + (y+z)\cdot w = 1$, as $Y_B = Z_B = 0$, $y\cdot w = y\cdot\mathbf{1}_B = 0$ by (S3), and $z\cdot w = 1$. If $\operatorname{corank} M = 1$ then $\ker M = \langle k\rangle$; if $Mx + tb = 0$ and $b\cdot x = 0$, then $0 = k^\top(Mx + tb) = t$, so $x \in \langle k\rangle$ and $b\cdot x = 0$ force $x = 0$. □

6.2. **The genus sum as a determinant.** Smith [57, Theorem 2.2, Table 2] proves that the sums of Tian, Yuan and Zhang are determinants of such matrices. We prove the case we need following his recursion, so that this section depends only on Rédei's theorem; the spanning forests of Lemma 6.9 and the parity lemma, Lemma 6.11, replace his induction on monomials. McCarthy's note on row 5*b* [34, file `docs/research/tyz-5b.md`, §3] proves the first identity of Theorem 6.12, and Smith's identity for L_{5b}, by the same forest expansion.

For $T \subseteq I$ let A_T be the Rédei matrix of the restricted configuration, and

$$\mathsf{G}(T) = \det(A_T \text{ with one column replaced by } z_T),$$

which does not depend on the column because $A_T\mathbf{1} = 0$. Put

$$\mathsf{L}(T) = \sum_{\pi} \prod_{T'\in\pi} \mathsf{G}(T'), \qquad \Sigma_1(I) = \sum_{\pi'} \prod_{T'\in\pi'} \mathsf{G}(T'),$$

where π runs over the partitions of T into blocks of type 1 ($\mathsf{L}(\emptyset) = 1$), and π' over the partitions of I with exactly one block of type 5 and all others of type 1.

Proposition 6.7. *Let $d > 1$ be squarefree with $d \equiv 1 \pmod 4$ and prime set T. Then $g(d)$ is odd if and only if $\mathsf{G}(T) = 1$. Consequently, for $\ell \equiv 5 \pmod 8$ with prime set I, $\Sigma_1(\ell) \equiv \Sigma_1(I) \pmod 2$.*

Proof. This is Rédei's criterion [48]; here is the form we need. Let $k = \mathbb{Q}(\sqrt{-d})$ with conjugation τ; its discriminant is $-4d$. The number $g(d)$ is odd if and only if $\mathrm{Cl}(k)[2] \cap 2\,\mathrm{Cl}(k) = 1$. Since τ acts on $\mathrm{Cl}(k)$ by inversion, $\mathrm{Cl}(k)[2]$ is the group of τ-invariant classes. If $\mathfrak{a}^\tau = \alpha\mathfrak{a}$ then $N(\alpha) = 1$, so $\alpha = \delta/\delta^\tau$ by Hilbert's Theorem 90, and $\mathfrak{a}\delta$ is a τ-stable ideal in the class of $\mathfrak{a}$. So $\mathrm{Cl}(k)[2]$ consists of the classes of the ideals $\mathfrak{a}_m$, products of ramified primes of norm $m \mid 2d$, and, since k has only the units ± 1, such an ideal is principal only for $m \in \{1, d\}$.

A class $[\mathfrak{a}]$ is a square if and only if $N\mathfrak{a}$ is the norm of an element of k: if $\mathfrak{a} = \mathfrak{b}^2(\gamma)$ then $\mathfrak{b}^2 = (N\mathfrak{b})\mathfrak{b}/\mathfrak{b}^\tau$ gives $N\mathfrak{a} = N(\gamma N\mathfrak{b})$; conversely if $N\mathfrak{a} = N(\alpha)$, then $\mathfrak{a}\alpha^{-1}$ has norm (1), so it equals $\mathfrak{c}/\mathfrak{c}^\tau = \mathfrak{c}^2/(N\mathfrak{c})$. By Hasse–Minkowski [51, Ch. IV, §3.2], $m > 0$ is a norm if and only if $(m, -d)_v = 1$ at every place. This is automatic at ∞ and at odd $p \nmid d$, and at 2 it follows from the others by the product formula [51, Ch. III, §2.1]. At $p_i \in T$, with $m = 2^{e'} \prod_{j \in T} p_j^{x_j}$, the formula for the Hilbert symbol [51, Ch. III, §1.2, Theorem 1] gives, additively, $(A_T x)_i + e' z_i$.

So $m \mapsto [\mathfrak{a}_m]$ identifies $\mathrm{Cl}(k)[2] \cap 2\,\mathrm{Cl}(k)$ with $\ker[A_T \mid z_T]/\langle(\mathbf{1}, 0)\rangle$. This is trivial if and only if $[A_T \mid z_T]$ has rank $|T|$, which, as $A_T\mathbf{1} = 0$, is $\mathsf{G}(T) = 1$. For the consequence: every d_i in $\Sigma_1(\ell)$ is $\equiv 1 \pmod 4$, and a factorization is a partition of I with one block of type 5. □

Lemma 6.8. *For a symmetric matrix N over $\mathbb{F}_2$, $\det N = \sum_\iota \prod_{\iota(x)=x} N_{xx} \prod_{\{x,x'\}} N_{xx'}$, the sum over the involutions ι of the index set and the second product over the 2-cycles of ι.*

Proof. In the permutation expansion pair each ς with ς^{-1} when $\varsigma^2 \neq 1$; the two products agree by symmetry. □

The next lemma is the case of $\mathbb{F}_2$ of the all-minors matrix-tree theorem of Chaiken [5].

Lemma 6.9. *Let A be the Rédei matrix of a configuration on I, and $R, P \subseteq I$ with $|R| = |P|$. Then $\det A[I \setminus R, I \setminus P]$ (rows $I \setminus R$, columns $I \setminus P$) is the sum, weighted by $\prod_{i \notin R} a_{i\varphi(i)}$, over the maps $\varphi : I \setminus R \to I$ with $\varphi(i) \neq i$ whose functional graph is a forest with root set R in which each tree contains exactly one element of P.*

Proof. Expand over bijections $\varsigma : I \setminus R \to I \setminus P$, and expand each diagonal entry $A_{ii} = \sum_{j \neq i} a_{ij}$. The terms correspond to pairs (φ, Z) with $Z = \{i : \varsigma(i) \neq i\}$, $\varphi = \varsigma$ on Z, for which ς_Z (equal to φ on Z and the identity off Z) is a bijection onto $I \setminus P$. Fix φ. If φ has a cycle, a valid Z contains all of it or none of it; adding or removing the cycle through the least vertex lying on a cycle is then an involution on the valid Z without fixed points, so these terms cancel in pairs. If φ is a forest with root set R, then ς_Z maps each tree T into itself, so it maps T minus its root bijectively onto $T \setminus P$, which forces $|T \cap P| = 1$; and if $T \cap P = \{p\}$, the only valid choice of $Z \cap T$ is the path from p up to, but excluding, the root. □

Two consequences. Expanding along the replaced column, $\mathsf{G}(T) = \sum_{k \in T} z_k c_k(T)$, where $c_k(T)$ is the weighted number of spanning trees of T oriented to the root k. And if $Y_T = 1$, then also $\mathbf{1}^\top A_T = 0$, so all cofactors of A_T are equal, $c_k(T) = c(T)$ for all k, and $\mathsf{G}(T) = c(T) Z_T$; in particular $\mathsf{G}(T) = 0$ for T of type 7.

Lemma 6.10. *Let I be a configuration and $1 \in I$. Let $M^{(U_1)}$ denote M with the row and column of U_1 deleted. Let $\mathsf{E}(V)$ be the sum, over partitions of V into blocks of type 3, of $\prod \mathsf{G}(T)$. Then:*

(1) $\det M(I) = \mathsf{E}(I)$ *if* $Y_I = 0$, *and* $\det M(I) = 0$ *if* $Y_I = 1$. *In particular* $\det M(I) = 0$ *if I has type 5.*
(2) *If* $Y_I = Z_I = 0$, *then* $\det M^{(U_1)}(I) = \sum_{1 \in T \subseteq I,\ T \text{ of type } 1} \mathsf{G}(T) \det M(I \setminus T)$.
(3) *If I has type 5, then* $\det M_5(I) = \sum_{T \subseteq I,\ T \text{ of type } 5} \mathsf{G}(T) \det M(I \setminus T)$.

Proof. The entries of M are $M_{U_iU_j} = y_iy_j$ $(i \neq j)$, $M_{U_iU_i} = 0$, $M_{U_iW_j} = A_{ji}$, $M_{W_iW_j} = 0$ $(i \neq j)$, $M_{W_iW_i} = z_i$. In Lemma 6.8, an involution pairs each U_i with some U_j or W_j, and fixes or pairs each W_j. Let P be the set of i with U_i paired to a U, and R the set of j with W_j fixed. The U–W pairs form a bijection $I \setminus R \to I \setminus P$ contributing $\det A[I \setminus R, I \setminus P]$, and the perfect matchings of P are odd in number, each of weight $\prod_P y_i$. So

$$\det M = \sum_{|P|=|R| \text{ even}} y^P z^R \det A[I \setminus R, I \setminus P].$$

Similarly $\det M^{(U_1)} = \sum_{1 \in P,\ |P|=|R| \text{ odd}} y^{P \setminus 1} z^R \det A[\dots]$, and, the border vertex pairing with some U_i, $i \in P$, with weight $b_i = y_i + z_i$, $\det M_5 = \sum_{|P|=|R| \text{ odd}} \bigl(\sum_{i \in P} b_i y^{P \setminus i}\bigr) z^R \det A[\dots]$. By Lemma 6.9, each is a sum over spanning forests in which every tree carries the weight $z_{\mathrm{root}} \prod a_e$ and one marked vertex. Summing over the marks, an ordinary tree contributes Y_T, the tree marked by the border contributes $Y_T + Z_T$, and the tree containing 1 in $M^{(U_1)}$ contributes 1; the number of trees is even for M and odd for the other two. Group the forests by their vertex partitions and use the two consequences above. In (1) every tree has $Y_T = 1$, hence type 3, and the number of trees is $\equiv Y_I$. In (2) and (3) the other trees have type 3 and are even in number, so the special tree has $Y_T = Y_I = 0$, and $\mathsf{E}(I \setminus T) = \det M(I \setminus T)$ by (1). In (2), T of type 5 would leave $I \setminus T$ of type 5, where $\mathsf{E} = 0$. In (3) the weight $Y_T + Z_T = Z_T$ forces type 5. □

Lemma 6.11. *If* $Y_I = Z_I = 0$, *then* $\operatorname{corank} M(I)$ *is even, and* $\det M^{(U_i)}(I) = \det M(I)$ *for every i.*

Proof. Let $N = M(I)$ and let $\delta = (0, z)$ be its diagonal. With $c = (\mathbf{1}, \mathbf{1})$, (6.1) gives $Nc = \delta$. For the form $\mathsf{b}(x, x') = x^\top N x'$ we have $\mathsf{b}(x, x) = \delta \cdot x = \mathsf{b}(c, x)$ and $\mathsf{b}(c, c) = Z_I = 0$. If $\delta = 0$ then b is alternating and has even rank. Otherwise $H = \{x : \mathsf{b}(c, x) = 0\}$ is a hyperplane containing c and $\ker N$, b is alternating on H, and its radical there is $\ker N + \langle c \rangle$; so $\dim \ker N$ is even. Now $\det N^{(x)} = \operatorname{adj}(N)_{xx}$. If $\operatorname{corank} N \geq 2$ the adjugate vanishes. If N is invertible then $\operatorname{diag}(N^{-1}) = N^{-1}\delta = c$, so $\operatorname{adj}(N)_{U_iU_i} = 1 = \det N$. □

Theorem 6.12 (Smith)**.** *If T has type 1 then* $\det M(T) = \mathsf{L}(T)$. *If I has type 5 then* $\det M_5(I) = \Sigma_1(I)$. *Hence* $\Sigma_1(\ell) \equiv \det M_5(\ell) \pmod 2$ *for* $\ell \equiv 5 \pmod 8$.

Proof. For type 1 use induction on $|T|$: by Lemmas 6.11 and 6.10(2), $\det M(T) = \det M^{(U_1)}(T) = \sum_{1 \in T'} \mathsf{G}(T')\mathsf{L}(T \setminus T') = \mathsf{L}(T)$, sorting partitions by the block containing 1. The second assertion is Lemma 6.10(3) with the first; the last is Proposition 6.7. □

6.3. **The construction.** By Lemmas 6.5 and 6.6 and Theorem 6.12, Theorem 6.1 asks for e such that on both supports the class (β, d) satisfies (S1)–(S3) and $\operatorname{corank} M = 1$. The primes of Π in Lemma 6.14 and the free bits of Lemma 6.16 adapt devices in [15, §5] and [38, Lemma 3.6].

Lemma 6.13. *Let N be symmetric over $\mathbb{F}_2$ with $Nk = 0$ and $k_c = 1$. Then* $\operatorname{corank} N = 1$ *if and only if $N^{(c)}$ (row and column c deleted) is invertible.*

Proof. If $N^{(c)}$ is invertible and $Nx = 0$, then $x - x_c k \in \ker N$ vanishes at c, so $x \in \langle k \rangle$. Conversely, if $N^{(c)}x' = 0$, extend x' by $x_c = 0$; then $(Nx)_i = 0$ for $i \neq c$, and $(Nx)_c = \sum_{i \neq c} k_i (Nx)_i = 0$ as $k^\top N = 0$. So $x \in \langle k \rangle$ with $x_c = 0$, that is, $x = 0$. □

For β prime the set Π below is empty and the next lemma is trivial; the formula uses only primes.

Lemma 6.14. *Let a configuration on $I = B \sqcup \Pi \sqcup R$ satisfy $Y_B = Z_B = 0$, $|\Pi| = |B| - 1$, and for $\pi \in \Pi$: $y_\pi = z_\pi = 0$; $a_{b\pi} = a_{\pi b} = C_{b\pi}$ for $b \in B$, where the columns of C form a basis of the even-weight vectors in $\mathbb{F}_2^B$; and $a_{\pi x} = a_{x\pi} = 0$ for every other x. Let I' be the configuration on $\{\hat\beta\} \sqcup R$ with $y_{\hat\beta} = z_{\hat\beta} = 0$, $a_{x\hat\beta} = a_{\hat\beta x} = \varsigma_x := \sum_{b \in B} a_{bx}$ for $x \in R$, and the same data on R. Then* $\det M(I)^{(c)} = \det M(I')^{(c)}$ *for every coordinate c of R.*

Proof. Use the basis consisting of $L = (\mathbf{1}_B, 0)$, $L' = (0, \mathbf{1}_B)$, the vectors $(h, 0), (0, h)$ for h in a basis of a complement H of $\langle \mathbf{1}_B \rangle$ in $\mathbb{F}_2^B$, and the coordinate vectors of Π and of R. The row of U_π in M is $\sum_b C_{b\pi} \mathbf{e}_{W_b}$ and that of W_π is $\sum_b C_{b\pi} \mathbf{e}_{U_b}$. So Π pairs only with the H-part, through $C^\top|_{\mathsf{H}}$, which is invertible because $\ker C^\top = \langle \mathbf{1}_B \rangle$. The Gram matrix has the shape

$$\begin{pmatrix} G_{11} & G_{12} & 0 \\ G_{21} & G_{22} & \mathsf{Y} \\ 0 & \mathsf{Y}^\top & 0 \end{pmatrix}$$

with Y invertible, so its determinant is $\det(\mathsf{Y})^2 \det G_{11}$, also after deleting a coordinate of R. Finally G_{11} is $M(I')$: $\mathsf{b}(L, L) = Y_B^2 + Y_B = 0$, $\mathsf{b}(L', L') = Z_B = 0$, $\mathsf{b}(L, L') = \sum_{b,b' \in B} A_{b'b} = \sum_{x \in R} \varsigma_x$, $\mathsf{b}(L, U_x) = y_x Y_B = 0$, $\mathsf{b}(L, W_x) = \sum_b a_{xb} = \varsigma_x$, $\mathsf{b}(L', U_x) = \varsigma_x$, $\mathsf{b}(L', W_x) = 0$, and the diagonal entry A_{xx} for $x \in R$ receives ς_x from B and 0 from Π. □

Lemma 6.15. *Let $I' = \{\hat\beta, r_1, r_2, r_3, r_4\}$ with $(y, z) = (0, 0)$ at $\hat\beta$, $(1, 1)$ at r_1, r_2, r_3, and $(1, 0)$ at r_4; $a_{r_i r_j} = 0$ for $i < j$, so $a_{r_j r_i} = 1$; and $a_{\hat\beta r} = a_{r\hat\beta} = 0, 0, 1, 1$ for $r = r_1, \dots, r_4$. Then the solutions of* (S1)–(S3) *on I' are $u = (u_0, \mathsf{a}, \mathsf{a}, \mathsf{a}, \mathsf{a})$, $w = (\varepsilon, \varepsilon, \varepsilon, \varepsilon + u_0 + \mathsf{a}, \varepsilon + u_0 + \mathsf{a})$ with $\varepsilon, u_0, \mathsf{a} \in \mathbb{F}_2$. So* $\operatorname{corank} M(I') = 1$, *and $(u, w) = (\mathbf{e}_{\hat\beta}, \mathbf{e}_{r_3} + \mathbf{e}_{r_4})$ is a solution.*

Proof. The Rédei matrix has rows $(0,0,0,1,1)$, $(0,0,0,0,0)$, $(0,1,1,0,0)$, $(1,1,1,1,0)$, $(1,1,1,1,0)$ in the order $\hat\beta, r_1, \dots, r_4$. Number the coordinates $0, \dots, 4$ in this order. Row by row, (S1) gives $u_3 = u_4$, $w_1 = \varepsilon$, $w_2 = \varepsilon + u_1 + u_2$, $w_3 = w_4 = \varepsilon + u_0 + u_1 + u_2 + u_3$; (S2) gives $w_3 = w_4$, $u_2 = u_3$, $u_1 = u_3$, $w_0 = \varepsilon$; and (S3) then holds. The count and Lemma 6.5 give the corank. □

Lemma 6.16. *Let I_0 be a configuration of type 5, $q_0 \in I_0$, and J a set of new indices with $Y_J = Z_J = 0$ such that $\sum_{j \in J} a_{xj} = \sum_{j \in J} a_{jx} = 0$ for every $x \in I_0 \setminus \{q_0\}$. Let the bits $t_j = a_{jq_0}$ $(j \in J)$ be free, all other data fixed. Let c be a coordinate of $I_0 \setminus \{q_0\}$. If $M(I_0)^{(c)}$ is invertible, then $M(I_0 \cup J)^{(c)}$ is invertible for some $t \in \mathbb{F}_2^J$.*

Proof. Changing t_j changes a_{jq_0} and $a_{q_0 j}$, so it adds $b_j b_j^\top$ to A with $b_j = \mathbf{e}_{q_0} + \mathbf{e}_j$, and adds the corresponding off-diagonal block to M. Let T be the change of basis $\mathbf{e}_{q_0} \mapsto \mathbf{e}_{q_0} + \mathbf{1}_J$ on both blocks. Then $\mathsf{T}^\top b_j = \mathbf{e}_j$, so in $M' = \mathsf{T}^\top M(I_0 \cup J)\mathsf{T}$ the bit t_j enters only the two entries (U_j, W_j) and (W_j, U_j), additively. With $f = \mathbf{e}_{q_0} + \mathbf{1}_J$, the entries of M' between f and the coordinates of I_0 are those of $M(I_0)$ plus the sums $\sum_J y$, $\sum_J z$, $\sum_J a_{xj}$, $\sum_J a_{jx}$, which vanish by hypothesis; the diagonal entry at f equals $A_{q_0 q_0}(I_0)$, up to $y_{q_0} Y_J = 0$; and the

other entries on I_0 are unchanged. So M' restricted to I_0 is $M(I_0)$. By Lemma 6.8, $\det M'^{(c)}$ is, as a function on $\mathbb{F}_2^J$, multilinear in t, and the coefficient of $\prod_j t_j$ is $\det M(I_0)^{(c)} = 1$. A nonzero multilinear polynomial over $\mathbb{F}_2$ has a nonzero value. Since T fixes the hyperplane $x_c = 0$, $\det M'^{(c)} = \det M(I_0 \cup J)^{(c)}$. □

Proof of Theorem 6.1. Let B be the set of primes of β and b_1 the least; let J be the primes of θ; and let $C_{b,i} = [b \in \{b_1, b_{i+1}\}]$ for $1 \le i \le |B| - 1$, $c_b = \sum_i C_{b,i}$, $z_b = \left[\frac{2}{b}\right]$. For $t \in \mathbb{F}_2^J$, chosen below, we ask for primes, in this order, all different from the primes of $\beta\theta$:

- $\pi_1, \dots, \pi_{|B|-1} \equiv 1 \pmod 8$ with $\left[\frac{\pi_i}{b}\right] = C_{b,i}$ $(b \in B)$, $\left[\frac{\pi_i}{q}\right] = 0$ $(q \in J)$, $\left[\frac{\pi_i}{\pi_h}\right] = 0$ $(h < i)$;
- $r_1, r_2, r_3 \equiv 3$ and $r_4 \equiv 7 \pmod 8$ with $\left[\frac{r}{b}\right] = X_r(b)$, where $X_{r_1}(b) = c_b + z_b$, $X_{r_2}(b) = 0$, $X_{r_3}(b) = [b = b_1]$, $X_{r_4}(b) = z_b + [b = b_1]$; $\left[\frac{r}{\pi_i}\right] = 0$; $\left[\frac{r_j}{r_i}\right] = 0$ for $i < j$; $\left[\frac{r}{q}\right] = 0$ for $r \in \{r_2, r_3, r_4\}$ and $q \in J$; and $\left[\frac{r_1}{q}\right] = t_q$ for $q \in J$.

Each condition is a residue class modulo 8 together with prescribed quadratic characters modulo earlier primes, so the Chinese remainder theorem and Dirichlet's theorem give such primes. Put $e = \beta\pi_1 \cdots \pi_{|B|-1} r_1 r_2 r_3 r_4$ and $d = r_3 r_4 \equiv 5 \pmod 8$. These conditions fix every symbol between primes of $e\theta$, so the configuration of $e\theta$ is determined by $t \in \mathbb{F}_2^J$; we choose t below from the configuration alone, and then choose the primes.

The sets B, J and each $\{\pi_i\}$ have type 1, and $\{r_1, \dots, r_4\}$ has type 5, so $e \equiv e\theta \equiv 5 \pmod 8$.

The class. It is $\varepsilon = 0$, $u = \mathbf{1}_B$, $w = \mathbf{e}_{r_3} + \mathbf{e}_{r_4}$, with $z \cdot u = Z_B = 0$. By reciprocity $\sum_b \left[\frac{b}{r}\right] = \sum_b X_r(b) = 0, 0, 1, 1$ for $r = r_1, \dots, r_4$. Row x of (S1) reads $(A\mathbf{1}_B)_x + y_x w_x = 0$: for $x \in B$, $(A\mathbf{1}_B)_x = \sum_{q \notin B} \left[\frac{q}{x}\right] = c_x + (c_x + z_x) + 0 + [x = b_1] + (z_x + [x = b_1]) = 0$, plus $\left[\frac{\theta}{x}\right] = 0$ on the support of $e\theta$; for $x = \pi_i$ it is a column sum of C; for $x = r$ it is $\left[\frac{\beta}{r}\right] = 0, 0, 1, 1 = y_r w_r$; for $x \in J$ it is $\left[\frac{\beta}{x}\right] = 0$. Row x of (S2) reads $(Aw)_x + y_x w_x + z_x[x \in B] = 0$: for $x \notin \{r_3, r_4\}$, $(Aw)_x = \left[\frac{d}{x}\right]$, which is $X_{r_3}(b) + X_{r_4}(b) = z_b$ at $b \in B$ and 0 elsewhere; for $x = r_3$, $(Aw)_{r_3} = \left[\frac{\beta}{r_3}\right] + \left[\frac{r_1}{r_3}\right] + \left[\frac{r_2}{r_3}\right] + \sum_i \left[\frac{\pi_i}{r_3}\right] = 1 + 1 + 1 + 0 = y_{r_3}$ (on the support of $e\theta$ add $\sum_{q \in J} \left[\frac{q}{r_3}\right] = Y_J = 0$), and likewise at r_4. Finally (S3) is $y_{r_3} + y_{r_4} = 0 = Y_B$. None of this involves t.

The dimension. Let $k = (\mathbf{1}_B + w, \mathbf{1}_B)$, in $\ker M$ on both supports for every t by Lemma 6.6, and let $c = U_{r_3}$, where $k_c = 1$. By Lemmas 6.5 and 6.13, on either support $\dim \mathrm{Sel} = 3$ if and only if $M^{(c)}$ is invertible. For e: by Lemma 6.14 with $R = \{r_1, \dots, r_4\}$ and $\varsigma_r = 0, 0, 1, 1$, $\det M(e)^{(c)} = \det M(I')^{(c)}$ for the configuration I' of Lemma 6.15. There $\operatorname{corank} M(I') = 1$, and the solution $(\mathbf{e}_{\hat{\beta}}, \mathbf{e}_{r_3} + \mathbf{e}_{r_4})$ gives, as in Lemma 6.6, the kernel vector $(\mathbf{e}_{\hat{\beta}} + \mathbf{e}_{r_3} + \mathbf{e}_{r_4}, \mathbf{e}_{\hat{\beta}})$ of $M(I')$, whose U_{r_3}-entry is 1; so $\det M(I')^{(c)} = 1$ by Lemma 6.13. For $e\theta$: apply Lemma 6.16 with I_0 the support of e, $q_0 = r_1$ and the same c. Its hypotheses hold: $Y_J = Z_J = 0$ as $\theta \equiv 1 \pmod 8$; for $b \in B$, $\sum_{q \in J} \left[\frac{q}{b}\right] = \left[\frac{\theta}{b}\right] = 0$ and $\sum_{q \in J} \left[\frac{b}{q}\right] = \left[\frac{\theta}{b}\right] + y_b Y_J = 0$; for π_i all symbols with J vanish; for $r \in \{r_2, r_3, r_4\}$, $\sum_q \left[\frac{r}{q}\right] = 0$ and $\sum_q \left[\frac{q}{r}\right] = y_r Y_J = 0$. So some t makes $M(e\theta)^{(c)}$ invertible.

The genus sum. By Lemma 6.6, $\det M_5 = 1$ on both supports, and by Theorem 6.12, $\Sigma_1(e)$ and $\Sigma_1(e\theta)$ are odd. □

7. Heights at six contacts

Theorem 1.3 is [15, Theorem 4.1] in existence form, in the contact and odd-support framework of [38, §4]. The geometry of the family, the two-dimensional representations and

the conductor bound follow the proof of Glazer and collaborators. Bounding a Faltings height through $J_1(N)$, Serre's conjecture, isogeny estimates and Javanpeykar's bound is von Känel's method for abelian schemes of GL_2-type [60, Theorem A and §1.2], and Pasten bounds the height of elliptic curves through Shimura curves [41]. For the fibers without complex multiplication the bound on the Faltings height also follows from a preprint of von Känel and Kret [61, Proposition 7.13], as explained in Remark 7.5. Throughout, u is the variable t of Theorem 1.3, h_F is the stable Faltings height, and $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Constants written $C(S)$ depend only on S and may change from line to line.

7.1. **A family over a Shimura curve.** Let $\mathbf{B} = (2,-3)_{\mathbb{Q}}$, with basis $1, \mathrm{i}, \mathrm{j}, \mathrm{ij}$, $\mathrm{i}^2 = 2$, $\mathrm{j}^2 = -3$; it is ramified exactly at 2 and 3. The ring $\mathcal{O} = \mathbb{Z}[\mathrm{i}, (1+\mathrm{j})/2]$ is a maximal order, of reduced discriminant 6, and $\mathrm{t} = 2\mathrm{j} + \mathrm{ij} \in \mathcal{O}$ has $\mathrm{t}^2 = -6$.

A *false elliptic curve* over a $\mathbb{Z}[1/6]$-scheme is an abelian surface A with an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(A)$; it carries a unique principal polarization whose Rosati involution is $x \mapsto \mathrm{t}^{-1}\bar{x}\mathrm{t}$ [4, §1]. Let $V_1(5) \subset (\mathcal{O} \otimes \widehat{\mathbb{Z}})^\times$ be the preimage of the matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ modulo 5. By [4, Theorem 2.1, Lemma 2.2, Corollary 2.3, Proposition 2.4] the moduli problem of false elliptic curves with level $V_1(5)$ has a fine moduli scheme whose generic fiber Y is a smooth projective geometrically connected curve over $\mathbb{Q}$, with a universal family $\mathcal{A} \to Y$ and $\mathcal{O}$ acting on it. Let X be the coarse curve of level one, and $\mathcal{W} \cong (\mathbb{Z}/2)^2$ the Atkin–Lehner group acting on X over $\mathbb{Q}$, sending (A, i) to $(A/A[\mathfrak{a}], i')$ for a two-sided ideal $\mathfrak{a}$ of $\mathcal{O}$. Put $X^* = X/\mathcal{W}$.

Over $\mathbb{C}$, $Y = \Gamma_U \backslash \mathfrak{H}$ and $X = \mathcal{O}^1 \backslash \mathfrak{H}$, with $\Gamma_U \subset \mathcal{O}^1$ torsion-free [4, Lemma 2.2]. The curve X^* is the quotient of $\mathfrak{H}$ by the triangle group of signature $(2,4,6)$ [12, §3.1, (32)], so it has genus 0 and three branch points, of indices $2, 4, 6$. Each is rational, being the only one of its index; so $X^* \cong \mathbf{P}^1_{\mathbb{Q}}$, and we choose the coordinate j on it with values $0, \infty, -16/27$ at the points of indices $4, 6, 2$.

Let $\pi_{\mathrm{j}} : Y \to \mathbf{P}^1_{\mathrm{j}}$ be the composite. As Γ_U acts freely, every point of Y above a branch point of index e has ramification index exactly e, and π_{j} is unramified elsewhere. Two points of Y with the same image in X^* have geometrically isogenous fibers, by an isogeny compatible with $\mathbf{B}$ up to an automorphism of $\mathbf{B}$. The moduli map from Y to the moduli space of principally polarized abelian surfaces is nonconstant.

The map π_{j} is now pulled back along a map $\lambda : \mathbf{P}^1_u \to \mathbf{P}^1_{\mathrm{j}}$ that has index 2, 6, 2 at every point above 0, ∞, $-16/27$: this removes the ramification above ∞ and $-16/27$ and leaves index 2 above 0. For λ we take the quotient of $\mathbf{P}^1_u$ by the dihedral group of order 12 generated by $u \mapsto -60(u+60)/(7u+240)$, of order 6, and the involution $u \mapsto -12u/(u+12)$. Its orbits with fewer than twelve points are the orbit of 0 (the set $\mathcal{C}$ of six rational points), the two fixed points of the first map, and one more orbit of six points; the coordinate on the quotient is chosen so that they lie above 0, ∞ and $-16/27$. Explicitly, let

$$\begin{aligned} \Pi(u) &= u(u+15)(u+20)(u+24)(u+30)(u+60), \\ \Delta(u) &= 7u^2 + 300u + 3600, \\ \Psi(u) &= (u^2 - 60u - 1800)(13u^2 + 480u + 3600)(11u^2 + 600u + 7200), \end{aligned}$$

and $\lambda = -57600\,\Pi^2/\Delta^6$. An exact computation shows $\Delta^6 - 97200\,\Pi^2 = \Psi^2$ and that Π, Δ, Ψ are squarefree and pairwise coprime. So λ has degree 12, $\lambda + 16/27 = 16\Psi^2/(27\Delta^6)$, and λ has index 2 at the six zeros of Π above 0, index 6 at the two zeros of Δ above ∞, and index 2 at the six zeros of Ψ above $-16/27$. By Riemann–Hurwitz ($22 = 6 + 10 + 6$) it is unramified elsewhere. Also $\lambda(\infty) = -57600/7^6$ differs from 0 and $-16/27$. The zeros of Π are $\mathcal{C}$.

Let Y' be the normalization of $Y \times_{\mathbf{P}^1_{\mathrm{j}}} \mathbf{P}^1_u$, a smooth projective curve over $\mathbb{Q}$, possibly geometrically disconnected, and $\pi : Y' \to \mathbf{P}^1_u$ the projection, with $\mathcal{A}$ pulled back.

Lemma 7.1. *The map π is ramified exactly at the points above $\mathcal{C}$, with index 2.*

Proof. By Abhyankar's lemma, the index of π at a point is $e/\gcd(e,a)$, with e, a the indices of π_{j} and of λ. It equals $4/2 = 2$ above $\mathcal{C}$, and $6/6 = 1$ and $2/2 = 1$ above the zeros of Δ and Ψ. □

Every fiber of $\mathcal{A}$ has $\mathbf{B}$ in its endomorphism algebra, and fibers above the same point of $\mathbf{P}^1_u$ are geometrically isogenous.

Let D be the degree bound of Lemma 7.2; it depends only on $\deg \pi$. Choose a finite set S_0 of primes containing $2, 3, 5$ and all primes up to D, such that over $\mathbb{Z}[1/S_0]$: Y' has a smooth proper model, $\mathcal{A}$ extends to an abelian scheme, π extends to a finite map, the six sections $u = c$ ($c \in \mathcal{C}$) and the section $u = \infty$ are pairwise disjoint, π is étale away from the six sections, and $\pi^*(c) = 2D_c$ with D_c étale.

7.2. **Fibers and their fields.** Let $S \supseteq S_0$, $u \in \mathbb{Q} \setminus \mathcal{C}$, $M = M_S(u)$, $T = S \cup \{p : p \mid M\}$, y' a point of Y' above u, and $A = \mathcal{A}_{y'}$. Let $\mathbb{K}$ be the splitting field of the fiber $\pi^{-1}(u)$, let Res be the restriction of scalars of A from $\mathbb{K}$ to $\mathbb{Q}$, and let L be $\mathbb{K}$ together with the field cut out by the action of $G_{\mathbb{Q}}$ on the lattice $\mathrm{End}(\mathrm{Res}_{\overline{\mathbb{Q}}})$.

Lemma 7.2. (a) *The field $\mathbb{K}$ is normal over $\mathbb{Q}$, of degree at most $(\deg \pi)!$, and unramified outside T, and A has good reduction at every place of $\mathbb{K}$ not above S.*

(b) *The field L is normal over $\mathbb{Q}$, of degree at most D with D depending only on $\deg \pi$, and unramified outside T; every conjugate of A is geometrically isogenous to A, and all homomorphisms between conjugates of A are defined over L.*

Proof. (a) At $p \notin T$: if u meets a section c at p, then $v_p(u - c) = 2k$ is even, and near D_c we have $\pi^*(u - c) = z^2 w$ with z a local equation of D_c and w a unit, so a point above u has $z = p^k y$ with $y^2 w = (u - c)/p^{2k}$, a p-adic unit; as p is odd, y lies in an unramified extension by Hensel's lemma, and so does the point; otherwise the fiber is étale at p, including when $v_p(u) < 0$, since ∞ is off the six sections. By properness, A has good reduction at every place of $\mathbb{K}$ not above S.

(b) Every Galois conjugate of A is a fiber above u, so it is geometrically isogenous to A. The group $G_{\mathbb{Q}}$ acts on the lattice $\mathrm{End}(\mathrm{Res}_{\overline{\mathbb{Q}}})$ through a finite group whose order is bounded in terms of the rank of the lattice, and inertia at $p \notin T$ acts trivially on the Tate module of Res for $\ell \neq p$. □

The first homology of a fiber is free of rank one over $\mathbf{B}$, and the complex structure is right multiplication by an element $\mathrm{J} \in \mathbf{B} \otimes \mathbb{R}$ with $\mathrm{J}^2 = -1$. So the centralizer of $\mathbf{B}$ in $\mathrm{End}^0(A_{\overline{\mathbb{Q}}})$ consists of the right multiplications by elements of $\mathbf{B}$ commuting with J, which is $\mathbb{Q}$ or an imaginary quadratic field k. Thus

$$\mathrm{End}^0(A_{\overline{\mathbb{Q}}}) = \mathbf{B} \quad \text{or} \quad \mathrm{End}^0(A_{\overline{\mathbb{Q}}}) = \mathbf{B} \otimes k \cong M_2(k).$$

Proposition 7.3. *If* $\mathrm{End}^0(A_{\overline{\mathbb{Q}}}) = M_2(k)$*, then* $h_F(A)$ *is bounded in terms of* D*. If* $\mathrm{End}^0(A_{\overline{\mathbb{Q}}}) = \mathbf{B}$*, then* $h_F(A) \le C(S)M^{24}$*.*

Proof in the case $M_2(k)$*.* Matrix units give an elliptic curve E_0/L with complex multiplication by an order of discriminant Δ_0, and an L-isogeny $E_0^2 \to A$. The class number of Δ_0 is $[\mathbb{Q}(j(E_0)) : \mathbb{Q}] \le D$. By Heilbronn [22] and the formula $h(f^2 d_0) \ge h(d_0)\varphi(f)/3$ there are finitely many such Δ_0, so finitely many E_0 over $\overline{\mathbb{Q}}$, and $h_F(E_0)$ is bounded in terms of D. By [14, Theorem 1.4] over L there is an isogeny $E_0^2 \to A$ of degree bounded in terms of D, so $h_F(A)$ is bounded in terms of D by the variation of the Faltings height under isogeny [13, Lemma 5]. □

7.3. **The two-dimensional representations.** Suppose $\mathrm{End}^0(A_{\overline{\mathbb{Q}}}) = \mathbf{B}$. We follow Ribet's descent for elliptic curves isogenous to their conjugates [49, §6], extended by Pyle to building blocks [46], and make explicit Tate's vanishing of $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)$ for the trivial action [49, (6.3)], to bound the conductor of the splitting character. For each $\varsigma \in \mathrm{Gal}(L/\mathbb{Q})$ choose an isogeny $\mu_\varsigma : {}^\varsigma A \to A$ over L commuting with $\mathbf{B}$, by composing an isogeny from the previous subsection with an element of $\mathbf{B}^\times$ (Skolem–Noether), with $\mu_1 = 1$. Then $c(\varsigma,\tau) = \mu_\varsigma\, {}^\varsigma\mu_\tau\, \mu_{\varsigma\tau}^{-1}$ lies in $\mathrm{End}^0(A)$ and commutes with $\mathbf{B}$, so it is in $\mathbb{Q}^\times$. Put $b_\varsigma = (\deg \mu_\varsigma)^{-1/4} > 0$. Taking degrees shows that $\epsilon(\varsigma,\tau) = c(\varsigma,\tau) b_\varsigma b_\tau / b_{\varsigma\tau}$ is ± 1, a 2-cocycle inflated from $\mathrm{Gal}(L/\mathbb{Q})$.

The class of ϵ lies in $\mathrm{Br}(\mathbb{Q})[2]$, and its invariant at $p \notin T$ vanishes, because it is inflated from the unramified quotient, of cohomological dimension one. For a Dirichlet character χ let $\delta\chi \in \mathrm{Br}(\mathbb{Q})[2]$ be the image under the connecting map of $1 \to \pm 1 \to \mu_{2m} \to \mu_m \to 1$. A character of $\mathbb{Q}_v^\times$ is a square if and only if it is trivial on ± 1, so $\delta\chi$ has invariant $\frac{1}{2}$ at v exactly when $\chi_v(-1) = -1$. Choose χ with $\chi_p(-1) = -1$ exactly at the finite primes p where $[\epsilon]$ is nonzero, using a character modulo p at odd p and modulo 4 at $p = 2$. Then $\chi_\infty(-1)$ is also correct, by the product formula, and $\delta\chi = [\epsilon]$ by the local-global principle for $\mathrm{Br}(\mathbb{Q})$ [36, Theorem (8.1.17)]. The order m of χ divides $2\prod_{p\in T,\, p\ne 2}(p-1)$, so $m \le C(S)M$.

Hence there is a continuous $\eta : G_{\mathbb{Q}} \to \mu_{2m}$ with $\eta^2 = \chi$ and $\eta(\varsigma)\eta(\tau)/\eta(\varsigma\tau) = \epsilon(\varsigma,\tau)$. At $p \notin T$, $\eta|_{I_p}$ is a quadratic character. Multiplying η by the quadratic Dirichlet character that removes these finitely many ramifications (at odd p, the group I_p has a unique nontrivial quadratic character, and $2 \in T$), we may assume $\eta|_{I_p} = 1$ for $p \notin T$. On G_L the map η is a homomorphism, normalized by $G_{\mathbb{Q}}$. Let L' be its kernel field. Then $L'/\mathbb{Q}$ is normal, $[L' : \mathbb{Q}] \le C(S)M$, and $L'/\mathbb{Q}$ is unramified outside T.

Fix a prime ℓ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. On $V_\ell(A) \otimes \overline{\mathbb{Q}}_\ell$ put

$$\rho_\ell(\varsigma) = \eta(\varsigma)^{-1} b_\varsigma\, \mu_\varsigma \circ \varsigma.$$

The cocycle relation makes this a representation of $G_{\mathbb{Q}}$. It commutes with $\mathbf{B} \otimes \overline{\mathbb{Q}}_\ell \cong M_2(\overline{\mathbb{Q}}_\ell)$, so $\rho_\ell \cong r_\ell \oplus r_\ell$ with $\dim r_\ell = 2$, and on $G_{L'}$ it is the Tate action.

Proposition 7.4. *Suppose* $\mathrm{End}^0(A_{\overline{\mathbb{Q}}}) = \mathbf{B}$*, and let* η*,* L' *and* r_ℓ *be as above, so that* $L'/\mathbb{Q}$ *is normal, of degree at most* $C(S)M$*, and unramified outside* T*.*

(a) *For every* ℓ*, the restriction* $r_\ell|_{G_{L'}}$ *is irreducible.*
(b) *For every* ℓ*,* r_ℓ *is odd: for a complex conjugation* c*,* $r_\ell(\mathsf{c})$ *has eigenvalues* $1, -1$*.*
(c) *For every prime* $p \notin T$ *there is an algebraic number* a_p *such that* $\operatorname{tr} r_\ell(\mathrm{Frob}_p) = a_p$ *for every* $\ell \ne p$*, under the chosen embedding.*
(d) *For* $\ell \notin T$*, the prime-to-*ℓ *Artin conductor of* r_ℓ *is divisible only by primes of* T *and is at most* $C(S)M^2$*, with* $C(S)$ *independent of* ℓ*.*

Proof. Irreducibility. By Faltings [13, Satz 3 and Satz 4] the commutant of $V_\ell(A)$ on $G_{L'}$ is $\mathbf{B} \otimes \overline{\mathbb{Q}}_\ell = M_2(\overline{\mathbb{Q}}_\ell)$ and $V_\ell(A)$ is semisimple, so $r_\ell|_{G_{L'}}$ is irreducible.

Oddness. Fix a complex embedding of L' and let c be complex conjugation. Then $\rho_\ell(\mathsf{c})$ comes from an operator R on $H_1(A(\mathbb{C}), \overline{\mathbb{Q}})$ of square 1, commuting with $\mathbf{B}$, which is a scalar multiple of the composite of an antiholomorphic map and a holomorphic isogeny. So on $H_1(A(\mathbb{C}), \mathbb{C})$ the operator R exchanges the two Hodge summands. Each summand is $\mathbf{B}$-stable of dimension two, so each corresponds to a line in the two-dimensional space on which R acts through r. An involution exchanging two complementary lines has eigenvalues $1, -1$.

Traces. Let $p \notin T$, $\ell \neq p$, and let ς be a Frobenius at a place of L' above p at which A reduces to $\bar{A}$. Then $\mu_\varsigma \circ \varsigma$ acts on $V_\ell(A) = V_\ell(\bar{A})$ as the endomorphism $\bar{\mu}_\varsigma \circ \mathrm{Frob}$ of $\bar{A}$, with $\mathrm{Frob} : \bar{A} \to \bar{A}^{(p)}$ the p-power Frobenius onto the reduction of ${}^\varsigma A$, so its trace is a rational number independent of ℓ. Hence $a_p := \frac{1}{2}\eta(\varsigma)^{-1} b_\varsigma \operatorname{Tr}(\bar{\mu}_\varsigma \mathrm{Frob})$ is an algebraic number independent of ℓ, with $\operatorname{tr} r_\ell(\mathrm{Frob}_p) = a_p$ under the chosen embedding.

Conductor. Let $\ell \notin T$. For $p \neq \ell$ let n_p be the exponent at p of the Artin conductor of r_ℓ.

- If $p \notin T$ then $n_p = 0$, since $I_p \subset G_{L'}$ and A has good reduction above p.
- If $p \mid M$, $p \notin S$, then A has good reduction above p, the ramification of $L/\mathbb{Q}$ at p is tame because $p > D$, and η is tame at p because $\eta^2 = \chi$ is tame and p is odd. So wild inertia acts trivially and $n_p \leq 2$.
- Let $p \in S$. Fix a prime $\ell_0 \notin S$. Over $\mathbb{F} = L_v(A[\ell_0])$, of degree over $\mathbb{Q}_p$ bounded in terms of S, A has semistable reduction by Raynaud's criterion [55, Theorem 3.5], so the wild inertia of $\mathbb{F}$ acts trivially on $V_\ell(A)$. Since $\chi|_{I_p}$ has conductor dividing p or 4, the character η is tame on $I_\mathbb{F}$ at odd p and has order at most 4 on $I_\mathbb{F}$ at $p = 2$. So there is a finite Galois extension $\mathbb{F}'$ of $\mathbb{Q}_p^{\mathrm{nr}}$, of degree e' bounded in terms of S, whose wild inertia acts trivially on r_ℓ. By the different formula, $\sum_{i \geq 0}(|\mathrm{G}_i| - 1) \leq e' - 1 + e' v_p(e')$ for the lower ramification groups G_i of $\mathbb{F}'$, so the Swan conductor of r_ℓ is at most $4(1 + v_p(e'))$ [52, Ch. III, §6; Ch. IV, §1; Ch. VI, §2]. Hence $n_p \leq 6 + 4v_p(e')$, which is bounded in terms of S.

Therefore the prime-to-ℓ Artin conductor of r_ℓ is at most $C(S)M^2$, with $C(S)$ independent of ℓ. □

7.4. **Modularity at large primes.**

Proof of Proposition 7.3 in the case $\mathbf{B}$. Let $\mathcal{L}$ be the set of primes $\ell \geq 5$ with $\ell \notin T$, $\ell \nmid 6 \deg \mu_\varsigma$ for every ς, and $\ell \geq \ell_1$, the constant of the paragraph on irreducibility below. The set $\mathcal{L}$ is infinite. It depends on the fiber, which is fixed.

The reduction. The ring $\mathcal{O}_A := \mathrm{End}_{L'}(A)$ is an order of $\mathbf{B}$ containing $\mathcal{O}$, which acts on $\mathcal{A}$, so $\mathcal{O}_A = \mathcal{O}$, and $\mathcal{O}_A \otimes \mathbb{Z}_\ell \cong M_2(\mathbb{Z}_\ell)$ for $\ell \in \mathcal{L}$, as $\ell \nmid 6$. Let e_ℓ be an idempotent of rank one, and $\mathcal{O}_\ell$ the ring of integers of a finite extension of $\mathbb{Q}_\ell$ containing the b_ς and the values of η. Each μ_ς is an isomorphism on T_ℓ and b_ς is an ℓ-adic unit, so ρ_ℓ preserves $T_\ell(A) \otimes \mathcal{O}_\ell$, and $\Lambda = e_\ell(T_\ell(A) \otimes \mathcal{O}_\ell)$ is a lattice for r_ℓ. Let $\bar{r}_\ell$ be its reduction. On $G_{L'}$ it is $e_\ell A[\ell]$ with coefficients extended.

Irreducibility. By Faltings and Zarhin, as stated in [1, Theorem 3.2] for the finitely generated field L': there is ℓ_1 such that for $\ell \geq \ell_1$ the $\mathbb{F}_\ell[G_{L'}]$-module $A[\ell]$ is semisimple with endomorphism ring $\mathrm{End}_{L'}(A) \otimes \mathbb{F}_\ell$. Here this ring is $M_2(\mathbb{F}_\ell)$, so $A[\ell] \cong W \oplus W$ with W simple of dimension two and $\mathrm{End}(W) = \mathbb{F}_\ell$. Hence W is absolutely irreducible, and $\bar{r}_\ell|_{G_{L'}}$ is absolutely irreducible. Since $r_\ell(\mathsf{c})$ has eigenvalues $1, -1$ and ℓ is odd, $\bar{r}_\ell$ is odd.

The weight. Let $v \mid \ell$ be the place of L' induced by the embedding, $K_v = L'_v$ and R_v its ring of integers. As $\ell \notin T$, $K_v/\mathbb{Q}_\ell$ is unramified, so $I_\ell \subset G_{L'}$ and $\bar{r}_\ell|_{I_\ell}$ is $W|_{I_\ell}$ with coefficients extended; and A has good reduction at v, with $\mathcal{O}_A$ acting on the Néron model $\mathcal{N}$. Thus $\mathcal{F} = e_\ell \mathcal{N}[\ell]$ is a finite flat R_v-group scheme of order ℓ^2 with generic fiber W. Let ϕ, ϕ' be the two characters of tame inertia on the semisimplification of $\bar{r}_\ell|_{G_{\mathbb{Q}_\ell}}$ [53, §2.1]. By [47, Corollaire 3.4.4], each is a product of distinct fundamental characters, so $\phi, \phi' \in \{1, \chi_\ell, \psi, \psi'\}$, with ψ, ψ' the fundamental characters of level 2 and χ_ℓ the cyclotomic character modulo ℓ. If one has level 2 then $\{\phi, \phi'\} = \{\psi, \psi'\}$ [53, §2.1, Proposition 1]. The Weil pairing gives $\det A[\ell] = \chi_\ell^2$ on $G_{L'}$, and $A[\ell] = W^2$, so $(\phi\phi')^2 = \chi_\ell^2$ on inertia. Since $\ell \geq 5$ this excludes $\{1, 1\}$ and $\{\chi_\ell, \chi_\ell\}$, so $\{\phi, \phi'\}$ is $\{\psi, \psi'\}$ or $\{1, \chi_\ell\}$.

If $\{\phi, \phi'\} = \{\psi, \psi'\}$, then $\bar{r}_\ell|_{I_\ell}$ has type (2.8.1) of [53], and $k(\bar{r}_\ell) = 2$ by [53, Proposition 3]. Suppose $\{\phi, \phi'\} = \{1, \chi_\ell\}$. The two characters are distinct and Frobenius-invariant, so by Clifford theory $W|_{G_{K_v}}$ is reducible, and the closure of a stable line gives an exact sequence of finite flat R_v-group schemes of order ℓ. A finite flat prolongation over R_v is unique, as the absolute ramification is $1 < \ell - 1$ [47, Proposition 3.3.2], so the factor with trivial inertia action is étale and the other is of multiplicative type. Over a finite étale extension R' of R_v the sequence is $0 \to \mathbb{Z}/\ell \to \mathcal{F} \to \mu_\ell \to 0$ or $0 \to \mu_\ell \to \mathcal{F} \to \mathbb{Z}/\ell \to 0$. In the first case the connected component splits the sequence, so wild inertia acts trivially. In the second the class of the extension is a unit of R' modulo ℓ-th powers, so the wild extension is peu ramifié in the sense of [53, §2.4]. Either way $\bar{r}_\ell|_{I_\ell}$ has type (2.8.2), and again $k(\bar{r}_\ell) = 2$ [53, Proposition 3]. The argument is that of the proof of [53, Proposition 4], given there over $\mathbb{Z}_\ell$.

The level. Let $N(\bar{r}_\ell)$ be the prime-to-ℓ Artin conductor of $\bar{r}_\ell$. For $p \neq \ell$ its exponent at p is at most that of the conductor of r_ℓ: the wild image is a finite p-group, on which reduction is injective and semisimple, so the Swan conductors agree, and the invariants of inertia can only grow under reduction, since Λ^{I_p} is saturated. Hence, by Proposition 7.4(d), $N(\bar{r}_\ell) \leq C(S)M^2$, and $N(\bar{r}_\ell)$ is divisible only by primes of T.

Serre's conjecture. The representation $\bar{r}_\ell$ is continuous, absolutely irreducible, two-dimensional and odd, so by [25, Theorem 9.1], whose lifting theorems are proved in [26] and whose hypothesis (H) is proved in [27], it arises from a newform of some weight and level. If that weight is one, multiplying by the Eisenstein series $E_{\ell-1}$, a lift of the Hasse invariant, gives a form of weight ℓ with the same reduction, and the lifting lemma [8, Lemme 6.11] gives an eigenform in characteristic zero. So $\bar{r}_\ell$ arises from a form of weight at least 2. By the refinement of Edixhoven [11, Theorem 4.5] for the weight and Diamond [10, Theorems 1.1, 5.1] for the level, recorded in [63, Theorem 2.1] and in weight two in [7, Theorem 3.15], $\bar{r}_\ell$ arises from a newform g_ℓ of weight $k(\bar{r}_\ell) = 2$ and level $N(\bar{r}_\ell)$ on $\Gamma_1(N(\bar{r}_\ell))$, with respect to the chosen embedding. For $\bar{r}_\ell$ of dihedral projective image this is [25, Lemma 6.2(i)]. The normalization is that of [53, (3.1.7)–(3.1.9)]: arithmetic Frobenius has trace the Hecke eigenvalue.

Finiteness. There are finitely many newforms of weight 2 and level at most $C(S)M^2$, so one newform f equals g_ℓ for infinitely many $\ell \in \mathcal{L}$. Let $N_f \leq C(S)M^2$ be its level. For $p \notin T$ and such $\ell \neq p$, the reductions of a_p and of the Hecke eigenvalue $a_p(f)$ at ℓ agree, so $a_p - a_p(f)$ lies in a prime above ℓ for infinitely many ℓ, whence $a_p = a_p(f)$. This is the argument of the proof of [25, Theorem 10.1], using only the traces outside T.

The transfer. Let $J = J_1(N_f)$, of dimension $\mathsf{g} \leq N_f^2$. There is a quotient A_f of J over $\mathbb{Q}$ on whose Tate module the representation $\rho_{f,\ell}$ of f occurs, with arithmetic Frobenius of trace $a_p(f)$ [7, Definition 1.44, Lemma 1.48, Theorem 3.1(a)]. So $\rho_{f,\ell}$ is a constituent of $V_\ell(J)$. Fix $\ell \in \mathcal{L}$ with $g_\ell = f$. By Chebotarev and Brauer–Nesbitt, $r_\ell \cong \rho_{f,\ell}$. So $V_\ell(A)$ and

$V_\ell(J)$ have a common constituent over L', and by Faltings [13, Satz 3 and Satz 4] there is a nonzero L'-homomorphism $A \to J$. As A is absolutely simple, Poincaré reducibility gives an L'-isogeny $A \times Z \to J$ with Z/L' an abelian variety.

The height. The curve $X_1(N_f)$ has a Belyi map of degree at most N_f^2, so [24, Theorem 1.1.1] gives, as in [60, Lemma 4.1], $h_F(J) \le 13 \cdot 10^6\, \mathsf{g}\, N_f^{10} \le 13 \cdot 10^6\, N_f^{12} \le C(S)M^{24}$. By [14, Theorem 1.4] over L' there is an isogeny $J \to A \times Z$ of degree at most

$$\kappa_J = \left((14\mathsf{g})^{64\mathsf{g}^2}\,[L' : \mathbb{Q}]\max(h_F(J), \log[L' : \mathbb{Q}], 1)^2\right)^{1024\mathsf{g}^3}.$$

With the variation under isogeny [13, Lemma 5], additivity, and Bost's lower bound $h_F(Z) \ge -\frac{3}{2}\dim Z$ [14, §9],

$$h_F(A) \le h_F(J) + \tfrac{1}{2}\log\kappa_J + \tfrac{3}{2}\dim Z \le C(S)M^{24},$$

because $\mathsf{g} \ll_S M^4$, $[L' : \mathbb{Q}] \ll_S M$, and so $\log\kappa_J \ll_S M^{20}\log(2M)$. □

Remark 7.5. The bound of Proposition 7.3 in the case **B** also follows from [61, Proposition 7.13], applied to A over the ring of S-integers of L, with $g = 2$, $\mathbb{Q}(\mathrm{i}) \subset \mathbf{B}$ as its quadratic field and the isogenies μ_ς: since $L/\mathbb{Q}$ is normal of degree at most D and unramified outside T, and all homomorphisms between conjugates of A are defined over L, it gives $h_F(A) \le (8D)^{288D}\big(M\prod_{p\in S} p\big)^{24}$.

7.5. **From the Faltings height to the height of the base point.** There is a constant C' with $h(u) \le C'(1 + \max(0, h_F(\mathcal{A}_{y'})))$ for every $u \in \mathbb{Q}\setminus\mathcal{C}$ and $y' \in Y'(\overline{\mathbb{Q}})$ above u. Indeed, over a finite cover Y'' of Y' choose a symmetric theta structure of level $r^2 = 4$ ($r = 2$ in Pazuki's notation) on each component, giving the map $\vartheta : Y'' \to \mathbf{P}^{15}$ of theta constants. It is nonconstant on each component, since the moduli map is nonconstant and theta constants determine the principally polarized surface up to finite ambiguity [42, §2.3.3]. So $\vartheta^*\mathcal{O}(1)$ is ample, and $h(\pi''(z)) \le a\,h(\vartheta(z)) + O(1)$ for the composite $\pi'' : Y'' \to \mathbf{P}^1_u$, by the height machine on a curve. On a nonempty open subset, $h(\vartheta(z))$ agrees up to a bounded term with the theta height h_Θ of the fiber [42, Definition 2.6]; on the finite complement $h \circ \pi''$ takes finitely many values. Finally [42, Corollary 1.3(2)] bounds $\max(h_\Theta, 1)$ by a constant times $\max(h_F, 1)$.

Proof of Theorem 1.3. Let $S \supseteq S_0$, $u \in \mathbb{Q}\setminus\mathcal{C}$, and A a fiber above u. By Proposition 7.3, $h_F(A)$ is bounded in terms of D or $h_F(A) \le C(S)M_S(u)^{24}$. The last subsection gives $h(u) \le H(S)M_S(u)^{24}$. □

8. The prime pattern

Theorem 1.4 is [15, Proposition 6.2] on the eighteen forms the formula uses, with $q \equiv 1 \pmod 8$ from its proof; their curve $y^2 = x^3 - (75 - 53\sqrt{2})^2 x$ is isomorphic to E over F, since $75 - 53\sqrt{2} = c_0(1 - \sqrt{2})^4$. The strategy is OpenAI's, on thirteen linear forms [38, §6]: the congruences $p \equiv 1 \pmod 8$, $p \equiv 3 \pmod 7$ giving the orders $p + 1 \mp 2\mathsf{a}$ for $p = \mathsf{a}^2 + \mathsf{b}^2$ [38, §6.1], and the comparison at a fixed cutoff L of a lower bound with a sieve bound for common factors above L [38, §§6.3–6.7]. Sun runs the same comparison on the quadratic patterns $u + c_j w^2$ [58, §§4 and 6.1]. An odd prime dividing both orders divides $p+1$, and the congruences imposed below exclude $p \equiv -1$ modulo the odd primes up to L; so a common odd factor exceeds L, and the patterns with one are the bad ones. Here the lower bound loses $(\log L)^{36}$ and the bad patterns save L, so for a large fixed L some pattern is not bad.

Let $P_s = \prod_{p \le 31} p$ and $W = 4P_s$; let $\mathcal{G}$ be the set of the first eighteen primes above 31 in each unit residue class modulo W (Dirichlet's theorem), and

$$\mathcal{K} = \{mg : \ m \mid P_s^4, \ m > 0, \ g \in \mathcal{G}\}.$$

Fix $A \in \mathbb{Z}$ and $B_0 \in \mathbb{R}$. Constants with subscript A may depend on A and on the choices made below before the parameter L, but not on L, X, or a varying prime.

8.1. **The forms and the fixed progression.** Write $T = (u_1, u_2, v)$ and let Λ_ν $(1 \le \nu \le 18)$ be the forms $u_1 - cv$, $u_2 - cv$, $-u_1 - u_2 + (A - c)v$ for $c \in \mathcal{C}$, so that the third is $u_3 - cv$ when $u_3 = Av - u_1 - u_2$. Each has a coefficient ± 1. Two forms from the same family have a 2×2 minor equal to a difference of contacts, and two from different families have a minor ± 1 in the first two coordinates. So every pair is linearly independent over $\mathbb{Q}$ and over $\mathbb{F}_q$ for every prime $q > 5$, and the relevant minors do not involve A.

Remark 8.1. Three slopes are what makes $\mathcal{K}$ independent of A. With two slopes u_1/v and $(Av - u_1)/v$, the forms $u_1 - cv$ and $-u_1 + (A - c')v$ have only the minor $A - c - c'$, which vanishes modulo a given prime for some A, and the choice of g_ν below then fails.

Fix a bounded open box $\Omega \subset \mathbb{R}^3$ whose closure avoids the eighteen zero planes and lies in $\{v > 0\}$, and signs ε_ν with $\varepsilon_\nu \Lambda_\nu > 0$ on $\overline{\Omega}$. There are $0 < \alpha_A < \alpha'_A$ with $\alpha_A X \le \varepsilon_\nu \Lambda_\nu(T) \le \alpha'_A X$ for $T \in X\Omega$.

At each prime $q \le 31$, the proportion of T modulo q^5 with $\Lambda_\nu(T) \equiv 0 \pmod{q^5}$ for some ν is at most $18/q^5 < 1$. Choose a residue outside this set and lift it modulo q^8. On this residue each Λ_ν has a fixed valuation $e_{\nu,q} \le 4$; put $m_\nu = \prod_{q \le 31} q^{e_{\nu,q}}$. The unit $\varepsilon_\nu \Lambda_\nu / m_\nu$ is then fixed modulo 8 and modulo each odd $q \le 31$. Choose $g_\nu \in \mathcal{G}$, pairwise distinct, such that $\varepsilon_\nu \Lambda_\nu / (m_\nu g_\nu)$ is $\equiv 1 \pmod 8$, $\equiv 3 \pmod 7$, and $\equiv 1 \pmod q$ for the other $q \le 31$; there are at most eighteen demands in any class. Put $\kappa_\nu = m_\nu g_\nu \in \mathcal{K}$.

At $g = g_\nu$ impose $\Lambda_\nu(T) \equiv 0 \pmod g$. This plane has g^2 points. For $\mu \ne \nu$ the restriction of Λ_μ is nonconstant, so excluding $\Lambda_\mu \equiv 0$ and $\varepsilon_\mu \Lambda_\mu \equiv -\kappa_\mu$ removes at most $34g < g^2$ points, as $g \ge 37$. Choose a remaining point. Among its lifts modulo g^2, the residue $\varepsilon_\nu \Lambda_\nu / (m_\nu g)$ modulo g takes every value; choose one different from 0 and -1.

The Chinese remainder theorem gives a residue r_0 modulo $W_0 = \prod_{q \le 31} q^8 \prod_\nu g_\nu^2$. On $r_0 + W_0 \mathbb{Z}^3$ the functions $\Psi_\nu = \varepsilon_\nu \Lambda_\nu / \kappa_\nu$ are integer-valued; at every prime dividing W_0 they are nonzero, and at every odd such prime they differ from -1. In the coordinates on this progression every variable coefficient is divisible by every prime dividing W_0. Put $Q_* = \max(31, \max \mathcal{G})$. Every value p of Ψ_ν on the progression has $p \equiv 1 \pmod 8$ and $p \equiv 3 \pmod 7$.

8.2. **The lower bound.** Take $L > \max(Q_*, B_0, 3)$. At each prime $q \le L$ with $q \nmid W_0$, exclude the 36 planes $\Lambda_\nu \equiv 0$ and $\varepsilon_\nu \Lambda_\nu \equiv -\kappa_\nu$; such q are at least 37. Let $W_L = W_0 \prod_{q \le L, \, q \nmid W_0} q$, and let $\mathcal{R}_L$ be the resulting set of residues modulo W_L reducing to r_0. Then

$$\frac{|\mathcal{R}_L|}{W_L^3} \ge W_0^{-3} \prod_{\substack{q \le L \\ q \nmid W_0}} \Big(1 - \frac{36}{q}\Big) \ge c_A (\log L)^{-36}, \qquad c_A > 0, \tag{8.1}$$

by $\log(1 - 36/q) = -36/q + O(q^{-2})$ and Mertens' second theorem [35].

Fix L. For $r \in \mathcal{R}_L$ apply [19, Main Theorem] to the forms $n \mapsto \varepsilon_\nu \Lambda_\nu(r + W_L n)/\kappa_\nu$ on the convex set $\{n : r + W_L n \in X\Omega\}$. These are integral affine forms with pairwise independent linear parts. Taking singleton classes in [19, Definition 1.5] gives complexity at most 16, and the inputs GI(16) and MN(16) of that theorem are [17, Theorem 1.3], with its

erratum [18], and [16, Theorem 1.1]. Coefficients and moduli are fixed before $X \to \infty$. The Archimedean factor is $\mathrm{vol}(\Omega)X^3/W_L^3$. At a prime $q \mid W_L$ the local factor is $(1-1/q)^{-18} \geq 1$. At $q \nmid W_L$ the substitution $n \mapsto r + W_L n$ is a bijection modulo q, so the local factor is $\beta_q = (1-1/q)^{-18}\mathbb{P}(\Lambda_\nu \neq 0 \text{ for all } \nu)$, and this probability is at least $1 - 18/q$. For $q \geq 37$ and $x = 1/q$,

$$\log \beta_q \geq \log(1-18x) - 18\log(1-x) \geq 9x^2 - \frac{162x^2}{1-18x} \geq -324x^2.$$

So the singular product is at least a positive absolute constant. There are finitely many r, so one threshold on X makes each error at most half its main term. Sum over r with (8.1). Proper prime powers contribute $O_A(X^{5/2}(\log X)^{19})$: a value of one form is fixed in $O_A(X^{1/2}\log X)$ ways, each with $O_A(X^2)$ solutions, each of weight $O_A((\log X)^{18})$. Hence, for X large in terms of A and L,

$$\#\{T \in X\Omega \cap \mathbb{Z}^3 : \ T \bmod W_L \in \mathcal{R}_L, \ \Psi_\nu(T) \text{ all prime}\} \geq a_A \frac{X^3}{(\log L)^{36}(\log X)^{18}}, \quad a_A > 0. \tag{8.2}$$

8.3. **A Selberg sieve.** Let $\mathcal{P}$ be a set of primes $q > Q_*$, and for $q \in \mathcal{P}$ let $\Omega_q \subset \mathbb{F}_q^2$ have $\rho(q) \leq 17q$ elements, $\rho(q) > 0$. Put $\delta(q) = \rho(q)/q^2$, $\delta^*(q) = \delta(q)/(1-\delta(q))$, extended multiplicatively to squarefree integers supported on $\mathcal{P}$, and $\mathfrak{G}(Z) = \sum_{d \leq Z} \delta^*(d)$. Note $(1-\delta(q))^{-1} \leq q$, as $17/q \leq 1 - 1/q$.

Lemma 8.2. *The number of integer points in an axis-parallel square of side $N \geq 1$ that avoid Ω_q for all $q \in \mathcal{P}$, $q \leq Z$, is $\ll N^2/\mathfrak{G}(Z) + NZ^6 + Z^8$, with an absolute implied constant.*

Proof. For squarefree d supported on $\mathcal{P}$, the Chinese remainder theorem gives

$$\#\{\text{points in the square lying in } \Omega_q \text{ for all } q \mid d\} = N^2\delta(d) + R_d, \qquad |R_d| \ll Nd + d^2.$$

For $d \leq Z$ define Selberg's weights

$$\lambda_d = \frac{\mu(d)}{\mathfrak{G}(Z)\prod_{q\mid d}(1-\delta(q))} \sum_{\substack{m \leq Z/d \\ (m,d)=1}} \delta^*(m),$$

so $\lambda_1 = 1$ and $|\lambda_d| \leq d$. Squaring $\sum \lambda_d$ majorizes the indicator of the sifted set. With $y_r = \sum_{r\mid d} \lambda_d \delta(d)$ and $1/\delta(m) = \sum_{r\mid m} 1/\delta^*(r)$, one has

$$\sum_{e,f} \lambda_e \lambda_f \delta([e,f]) = \sum_r y_r^2/\delta^*(r), \qquad y_r = \mu(r)\delta^*(r)/\mathfrak{G}(Z),$$

and the sum equals $\mathfrak{G}(Z)^{-1}$. There are at most Z^2 pairs (e,f), each with $|\lambda_e\lambda_f| \leq Z^2$ and $[e,f] \leq Z^2$, which gives the remainder. □

To bound $\mathfrak{G}(Z)$ from below, let $z = Z^{1/100}$ and $\mathfrak{H}(z) = \prod_{q \leq z,\, q \in \mathcal{P}}(1+\delta^*(q))$. Give each squarefree divisor d of $\prod_{q\leq z,\, q\in\mathcal{P}} q$ the probability $\delta^*(d)/\mathfrak{H}(z)$. The events $q \mid d$ are independent with probability $\delta(q)$, so $\mathbb{E}\log d = \sum \delta(q)\log q \leq 17\sum_{q\leq z}(\log q)/q \leq 34\log z$ for large z; here $\sum_{q\leq z}(\log q)/q = \log z + O(1)$ by Mertens' first theorem [35]. Markov's inequality gives $\mathbb{P}(d \leq Z) \geq \frac{1}{2}$, so

$$\mathfrak{G}(Z) \geq \tfrac{1}{2}\mathfrak{H}(Z^{1/100}). \tag{8.3}$$

We use two cases. If $\mathcal{P}$ consists of the primes $q > Q_*$ with $q \equiv 1 \pmod 4$, with at most one prime omitted, and $\delta(q) = 2/q - 1/q^2$, then Mertens in the progression 1 mod 4

[62, Theorem 1] gives $\log\mathfrak{H}(z) = \log\log z + O_{Q_*}(1)$, uniformly in the omitted prime, so $\mathfrak{G}(Z) \gg_{Q_*} \log Z$. If $\mathcal{P}$ is the set of all primes $q > Q_*$ and $17/q - 136/q^2 \le \delta(q) \le 17/q$, then $\log\mathfrak{H}(z) = 17\log\log z + O_{Q_*}(1)$, independently of the sets Ω_q, so $\mathfrak{G}(Z) \gg_{Q_*} (\log Z)^{17}$.

8.4. **The two reduced curves.** Let p be a prime value counted in (8.2), so $p \equiv 1 \pmod 8$, $p \equiv 3 \pmod 7$ and p is large. Then p splits in F, and $(7/p) = (p/7) = -1$. The two reductions of c_0 have product 7, so they have opposite quadratic characters. The curves E and E^σ have good reduction at the place $\mathfrak{p} \mid p$, where they are the quadratic twists of $y^2 = x^3 - x$ by these two classes. So their Frobenius traces are opposite.

As $p \equiv 1 \pmod 4$, the automorphism $(x, y) \mapsto (-x, \mathrm{i}y)$ of the reduced curve $\bar{E}$ is defined over $\mathbb{F}_p$, so the Frobenius of $\bar{E}$ lies in $\mathbb{Z}[\mathrm{i}]$ and is $\mathsf{a} + \mathsf{b}\mathrm{i}$ with $\mathsf{a}, \mathsf{b} \in \mathbb{Z}$. By [56, III.8.6],

$$\mathsf{a}^2 + \mathsf{b}^2 = p, \qquad d_1 = p + 1 - 2\mathsf{a}, \qquad d_2 = p + 1 + 2\mathsf{a},$$

for the orders of the two reduced groups, and $\mathsf{a} \ne 0$ since p is not a square. Both orders are divisible by 4, and $d_1 + d_2 = 2(p+1)$ has 2-adic valuation 2, so the 2-part of $\gcd(d_1, d_2)$ is 4. By Hasse's bound [56, V.1.1], $0 < d_i < 2p$, and $d_i \ne p$ since $4 \mid d_i$; so $p \nmid d_1 d_2$. If an odd prime ℓ divides both orders, it divides a and $p+1$, and $\mathsf{b}^2 \equiv -1 \pmod \ell$. The conditions on the progression give $p \not\equiv -1 \pmod \ell$ for every odd $\ell \le L$. So $\ell > L$; call such a p *bad*.

8.5. **Counting bad values.** Fix ν. A bad prime value p of Ψ_ν lies in $[\alpha_A X, \alpha'_A X]$, with κ_ν absorbed into the constants, and gives (a, b) in a square of side $O_A(\sqrt{X})$. If $L < \ell \le X^{1/8}$, write $\mathsf{a} = \ell U$ and $\mathsf{b} = b_0 + \ell V$ for one of the at most two roots b_0 of $b_0^2 \equiv -1 \pmod \ell$. The pair (U, V) lies in a square of side $N \asymp_A \sqrt{X}/\ell$. For $q > Q_*$, $q \equiv 1 \pmod 4$, $q \ne \ell$, the condition $\mathsf{a}^2 + \mathsf{b}^2 \equiv 0 \pmod q$ is a union of two lines of $2q - 1$ points, and the substitution is bijective modulo q. Since $p > Z = X^{1/100}$, every pair avoids these points, so Lemma 8.2 and the first case of (8.3) give $\ll_A X/(\ell^2 \log X)$ pairs. Summing over ℓ gives $O_A(X/(L\log X))$. If $\ell > X^{1/8}$, then $\ell \mid \mathsf{a} \ne 0$ leaves $O_A(\sqrt{X}/\ell)$ values of a and $O_A(\sqrt{X}/\ell + 1)$ values of b in each class, and $\ell \ll_A \sqrt{X}$; summing gives $O_A(X^{7/8} + \sqrt{X}\log X)$. Therefore, uniformly in L,

$$\#\{\text{bad prime values of } \Psi_\nu\} \ll_A \frac{X}{L\log X} + X^{7/8} + \sqrt{X}\log X. \tag{8.4}$$

For a prime p in this range, with $c_p = \varepsilon_\nu \kappa_\nu p$, consider the integer points of $X\Omega$ on $\Lambda_\nu = c_p$. Solving for a coordinate with coefficient ± 1 parametrizes them by a square of side $O_A(X)$, also modulo every prime. For $Q_* < q \le Z = X^{1/100}$ we have $c_p \not\equiv 0 \pmod q$, and each of the other seventeen forms restricts to a nonconstant affine form. Their zero lines are distinct: if two of them coincided, then $\Lambda_j - \lambda\Lambda_k = \mu_0(\Lambda_\nu - c_p)$ over $\mathbb{F}_q$ with $\lambda \ne 0$, and comparing constant terms gives $\mu_0 = 0$, contradicting independence. So the union has between $17q - 136$ and $17q$ points. Every pattern on this plane with all other Ψ_μ prime avoids it, so Lemma 8.2 and the second case of (8.3) give

$$\#\{\text{patterns with } \Psi_\nu = p\} \ll_A \frac{X^2}{(\log X)^{17}}, \tag{8.5}$$

uniformly in p and independent of L.

Proof of Theorem 1.4. Multiply (8.4) by (8.5) and sum over ν: the patterns in (8.2) with some bad value number at most

$$b_A \frac{X^3}{L(\log X)^{18}} + O_A\Big(\frac{X^{23/8}}{(\log X)^{17}} + \frac{X^{5/2}}{(\log X)^{16}}\Big),$$

with b_A independent of L. Choose L so large that $b_A/L < a_A/(2(\log L)^{36})$, and then X large. A pattern survives. It gives integers u_1, u_2, v with $v > 0$, and with $u_3 = Av - u_1 - u_2$ each of the eighteen numbers $u_j - cv$ is $\varepsilon_\nu \kappa_\nu p$ with $p > B_0$ prime and $\kappa_\nu \in \mathcal{K}$, and p is not bad. Since $\mathcal{K}$ was fixed before A, the theorem follows. □

Appendix A. Computations

One computation in the proofs is not done by hand: the identity $\Delta^6 - 97200\,\Pi^2 = \Psi^2$ of Section 7, with the squarefreeness and pairwise coprimality of Π, Δ, Ψ. It is exact, in Python 3.12 with integer and rational arithmetic. The programs deposited at [23], with their outputs, also recompute the elementary identities the text states: $(1+\sqrt{2})^3 - c_0^2(1+\sqrt{2}) = 8$ and the signs in the descent (Section 2); the system of Lemma 6.15; the discriminant of $\mathcal{O}$, from the form $\mathrm{Trd}(x\bar{y})$ on the basis $1, \mathrm{i}, (1+\mathrm{j})/2, (\mathrm{i}+\mathrm{ij})/2$, of determinant 36, and the Hilbert symbols of $(2, -3)$ (Section 7); and the 2×2 minors of the eighteen forms that do not involve A, whose prime factors are $2, 3, 5$ (Section 8).

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. The author chooses the problems and prioritizes the work. Separate AI agents checked each result, and a second program confirmed the computations the proofs use, with any exceptions listed in the public deposit. The system also searched the literature and checked the citations against reliable sources. The author read the paper, reran the computations from the deposit and takes full responsibility for all of the paper's contents.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [23].

References

1. Sara Arias-de Reyna, Wojciech Gajda, and Sebastian Petersen, *Big monodromy theorem for abelian varieties over finitely generated fields*, J. Pure Appl. Algebra **217** (2013), no. 2, 218–229, doi:10.1016/j.jpaa.2012.06.010; numbering of results as in the authors' copy of June 19, 2012.
2. Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618, doi:10.1007/BF01233440.
3. Ashay Burungale, *A Diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$*, 2026, Preprint, arXiv:2611.16130v1.
4. Kevin Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), no. 3, 591–612, doi:10.1215/S0012-7094-97-08719-6.
5. Seth Chaiken, *A combinatorial proof of the all minors matrix tree theorem*, SIAM J. Algebraic Discrete Methods **3** (1982), no. 3, 319–329, doi:10.1137/0603033.
6. Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735, doi:10.5802/jtnb.516.
7. Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Elliptic Curves, Modular Forms & Fermat's Last Theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2–140; the numbering is that of the authors' file of September 9, 2007.
8. Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530, doi:10.24033/asens.1277.
9. Jan Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236, doi:10.1090/S0002-9947-1980-0549163-X.
10. Fred Diamond, *The refined conjecture of Serre*, Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Hong Kong, 1993) (John Coates and S.-T. Yau, eds.), Int. Press, Cambridge, MA, 1995, pp. 22–37.
11. Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594, doi:10.1007/BF01232041.

12. Noam D. Elkies, *Shimura curve computations*, Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 1–47, doi:10.1007/BFb0054850; numbering as in arXiv:math/0005160v1.
13. Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, doi:10.1007/BF01388432; erratum, Invent. Math. **75** (1984), 381.
14. Éric Gaudron and Gaël Rémond, *Polarisations et isogénies*, Duke Math. J. **163** (2014), no. 11, 2057–2108, doi:10.1215/00127094-2782528.
15. *$\mathbb{Z}$ is Diophantine in $\mathbb{Q}$, Version 13*, 2026, Manuscript with no named author, November 7, 2026, public repository of Elliot Glazer, https://github.com/elliotglazer/diophantine-z-q, commit 9c0b3ab.
16. Ben Green and Terence Tao, *The Möbius function is strongly orthogonal to nilsequences*, Ann. of Math. (2) **175** (2012), no. 2, 541–566, doi:10.4007/annals.2012.175.2.3.
17. Ben Green, Terence Tao, and Tamar Ziegler, *An inverse theorem for the Gowers $U^{s+1}[N]$-norm*, Ann. of Math. (2) **176** (2012), no. 2, 1231–1372, doi:10.4007/annals.2012.176.2.11.
18. ———, *Erratum for "An inverse theorem for the Gowers $U^{s+1}[N]$-norm"*, 2024, Authors' erratum to Ann. of Math. (2) **176** (2012), 1231–1372, https://people.maths.ox.ac.uk/greenbj/papers/GI(s)-erratum.pdf.
19. Benjamin Green and Terence Tao, *Linear equations in primes*, Ann. of Math. (2) **171** (2010), no. 3, 1753–1850, doi:10.4007/annals.2010.171.1753.
20. Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, doi:10.1007/BF01388809.
21. David Rodney Heath-Brown, *The size of Selmer groups for the congruent number problem, II*, Invent. Math. **118** (1994), no. 2, 331–370, With an appendix by P. Monsky, doi:10.1007/BF01231536.
22. Hans Heilbronn, *On the class-number in imaginary quadratic fields*, Quart. J. Math. **5** (1934), 150–160, doi:10.1093/qmath/os-5.1.150.
23. Manvir Jaswal, *Programs and data for "A proof that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$ through congruent-number twists"*, 2026, Zenodo, doi:10.5281/zenodo.24135695.
24. Ariyan Javanpeykar, *Polynomial bounds for Arakelov invariants of Belyi curves*, Algebra Number Theory **8** (2014), no. 1, 89–140, doi:10.2140/ant.2014.8.89.
25. Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504, doi:10.1007/s00222-009-0205-7.
26. ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586, doi:10.1007/s00222-009-0206-6.
27. Mark Kisin, *Modularity of 2-adic Barsotti–Tate representations*, Invent. Math. **178** (2009), no. 3, 587–634, doi:10.1007/s00222-009-0207-5.
28. Jochen Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, 2013, Preprint, arXiv:1011.3424v2.
29. ———, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. (2) **183** (2016), no. 1, 73–93, doi:10.4007/annals.2016.183.1.2.
30. Peter Koymans and Carlo Pagano, *Hilbert's tenth problem via additive combinatorics*, J. Amer. Math. Soc. **40** (2027), 195–234, doi:10.1090/jams/1081.
31. Yuri Matiyasevich, *Diophantine representation of enumerable predicates*, Math. USSR-Izv. **5** (1971), no. 1, 1–28, doi:10.1070/IM1971v005n01ABEH001004.
32. Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45, doi:10.1080/10586458.1992.10504244.
33. ———, *Speculations about the topology of rational points: an up-date*, Astérisque **228** (1995), 165–181.
34. Jack McCarthy, *Lean: the frozen target's statement from two hypotheses (conditional; vendored Green–Tao proof and Selberg sieve)*, 2026, Lean development and notes, pull request 24 to the public repository https://github.com/elliotglazer/diophantine-z-q, November 9–10, 2026, commit 0c65382.
35. Franz Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. Reine Angew. Math. **78** (1874), 46–62, doi:10.1515/crll.1874.78.46.
36. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, Berlin, 2008.
37. *An existential definition of the integers in the rationals from reduced arithmetic inputs, third version*, 2026, Note with no named author, dated October 14, 2026, posted November 6, 2026, in the public repository https://github.com/elliotglazer/diophantine-z-q, commit 9c0b3ab, file `research/2026-11-06-collaborator-notes/supplied/two-proofs-reduced-inputs-v3.tex`.
38. 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`.

39. ———, *A pointwise* 2*-converse for elliptic curves with rational two-torsion*, 2026, Preprint, October 7, 2026, https://github.com/openai/math, commit 3014888, folder `preprints/A-pointwise-2-converse-for-elliptic-curves-with-rational-two-torsion-October-7-2026`.
40. Lue Pan, *The Fontaine–Mazur conjecture in the residually reducible case*, J. Amer. Math. Soc. **35** (2022), no. 4, 1031–1169, doi:10.1090/jams/991.
41. Hector Pasten, *Shimura curves and the abc conjecture*, J. Number Theory **254** (2024), 214–335, doi:10.1016/j.jnt.2023.07.002.
42. Fabien Pazuki, *Theta height and Faltings height*, Bull. Soc. Math. France **140** (2012), no. 1, 19–49, doi:10.24033/bsmf.2623.
43. Thanases Pheidas, *An effort to prove that the existential theory of* $\mathbb{Q}$ *is undecidable*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 237–252, doi:10.1090/conm/270/04376.
44. 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.
45. ———, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682, doi:10.1353/ajm.0.0057.
46. Elisabeth E. Pyle, *Abelian varieties over* $\mathbb{Q}$ *with large endomorphism algebras and their simple components over* $\overline{\mathbb{Q}}$, Modular Curves and Abelian Varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, doi:10.1007/978-3-0348-7919-4_14, pp. 189–239.
47. Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280, doi:10.24033/bsmf.1779.
48. László Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **171** (1934), 55–60, doi:10.1515/crll.1934.171.55.
49. Kenneth A. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, Algebra and Topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79.
50. Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114, doi:10.2307/2266510.
51. Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, New York-Heidelberg, 1973.
52. ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.
53. ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230, doi:10.1215/S0012-7094-87-05413-5.
54. Goro Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208, doi:10.1017/S0027763000014471.
55. Alice Silverberg and Yuri G. Zarhin, *Semistable reduction and torsion subgroups of abelian varieties*, Ann. Inst. Fourier (Grenoble) **45** (1995), no. 2, 403–420, doi:10.5802/aif.1459.
56. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, doi:10.1007/978-0-387-09494-6.
57. Alexander Smith, *The congruent numbers have positive natural density*, 2016, Preprint, arXiv:1603.08479v2.
58. Zhi-Wei Sun, *86 unknowns for Hilbert's tenth problem over the rationals*, 2026, Preprint, arXiv:2610.20691v2.
59. Ye Tian, Xinyi Yuan, and Shou-Wu Zhang, *Genus periods, genus points and congruent number problem*, Asian J. Math. **21** (2017), no. 4, 721–774, doi:10.4310/AJM.2017.v21.n4.a5; Theorem 1.4 is Theorem 1.2 of arXiv:1411.4728v1.
60. Rafael von Känel, *The effective Shafarevich conjecture for abelian varieties of* GL_2*-type*, Forum Math. Sigma **9** (2021), Paper No. e39, 29 pp., doi:10.1017/fms.2021.29.
61. Rafael von Känel and Arno Kret, *Integral points on coarse Hilbert moduli schemes*, 2023, Preprint, arXiv:2307.06944v1.
62. Kenneth S. Williams, *Mertens' theorem for arithmetic progressions*, J. Number Theory **6** (1974), 353–359, doi:10.1016/0022-314X(74)90032-8.
63. Jean-Pierre Wintenberger, *On Serre's modularity conjecture*, 2009, Lecture notes, https://math.sbg.ac.at/fuchsc/A&G/Wintenberger-2009.pdf.

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