THE PRIMITIVE SOLUTIONS OF SEVEN SMALL GENERALIZED FERMAT EQUATIONS

MANVIR JASWAL

Abstract. Version 9 of Grechuk's list of open Diophantine equations contains seven equations $ax^p + by^q + cz^r = 0$ with $1/p + 1/q + 1/r < 1$ and $|a|2^p + |b|2^q + |c|2^r \leq 60$ for which the complete list of primitive solutions was not known. We determine the primitive solutions of all seven:

$$x^5 + y^4 - 2z^2 = 0, \qquad x^5 + y^4 - 3z^2 = 0, \qquad x^5 + y^4 + 3z^2 = 0,$$
$$2x^4 - y^4 + z^3 = 0, \qquad x^4 + 3y^3 + 2z^3 = 0, \qquad x^4 + 4y^3 + z^3 = 0,$$
$$x^4 + 3y^3 + z^3 = 0.$$

Besides solutions with entries 0 and ± 1, the only ones are $(11, \pm 29, \pm 538)$ of $x^5 + y^4 = 3z^2$ and $(\pm 895, -6202, 4199)$ of $x^4 + 3y^3 + z^3 = 0$. For the last equation this answers a question of Grechuk; J. Agbanwa has announced a proof in an unpublished manuscript, and ours is by a different method. The proofs combine descent over number fields of small degree with elliptic Chabauty and the Mordell–Weil sieve. For $x^4 + 3y^3 + z^3 = 0$ we also use a covering by a curve of genus one over a number field of degree 12, whose Jacobian has unknown rank, and Stoll's form of Chabauty's method at the prime 2, which uses a Selmer group of a 2-isogeny in place of the Mordell–Weil group. No step assumes the generalized Riemann hypothesis.

Contents

1. Introduction 2
2. Tools 5
3. The equations $x^5 + y^4 = Dz^2$: descent 9
4. The case $k = 0$ 11
5. The cases $k \neq 0$ 15
6. The equation $2x^4 - y^4 + z^3 = 0$ 19
7. The equations $x^4 + 4y^3 + z^3 = 0$ and $x^4 + 3y^3 + 2z^3 = 0$ 21
8. Five curves of genus one over cubic fields 23
9. The equation $x^4 + 3y^3 + z^3 = 0$: descent and the class $j = 0$ 26
10. A covering over a field of degree 12 29
11. Stoll's method at the prime 2 32
Appendix A. Class groups and units 39
Appendix B. Data for equation (g) 41
Appendix C. Computations 45
Declarations 48
References 48

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G05, 11G30, 11Y50.

Key words and phrases. Generalized Fermat equation, primitive solutions, descent, elliptic Chabauty, Mordell–Weil sieve, Selmer groups.

1. Introduction

1.1. **Grechuk's list.** An integer solution (x, y, z) of an equation

$$ax^p + by^q + cz^r = 0 \qquad (a, b, c \in \mathbb{Z} \smallsetminus \{0\},\ p, q, r \geq 2) \tag{1.1}$$

is *primitive* if $\gcd(x, y, z) = 1$. When $1/p + 1/q + 1/r < 1$, the theorem of Darmon and Granville [12] shows that (1.1) has only finitely many primitive solutions, and the problem is to list them. See the survey of Ratcliffe and Grechuk [25] for the cases solved so far.

Grechuk orders polynomial Diophantine equations by a size H, which for (1.1) is $H = |a|2^p + |b|2^q + |c|2^r$ [18], and keeps a list of the smallest equations of various kinds whose solution is not known to him [19]. Its Table 4 lists the equations (1.1) with $H \leq 60$ and $1/p + 1/q + 1/r < 1$ "for which a complete list of primitive solutions is not known to the author". In version 9 of the list this table has seven entries:

$$x^4 + 3y^3 + z^3 = 0\ (H = 48), \quad x^4 + 3y^3 + 2z^3 = 0\ (56), \quad x^4 + 4y^3 + z^3 = 0\ (56),$$
$$2x^4 - y^4 + z^3 = 0\ (56), \quad x^5 + y^4 - 2z^2 = 0\ (56), \quad x^5 + y^4 + 3z^2 = 0\ (60),$$
$$x^5 + y^4 - 3z^2 = 0\ (60).$$

The same seven, together with two since solved, appear in Table 2.2 of the survey [25] ("uninvestigated equations"), where the authors write that they could not find a reference solving any of them and invite the reader to investigate them [25, §2.5]. The two solved since are $x^4 + 2y^3 + z^3 = 0$ and $x^5 + 2y^3 + z^3 = 0$: as Grechuk's list records, the identity $(2y^3 - z^3)^2 + (2yz)^3 = (2y^3 + z^3)^2$ reduces them to the equations $A^2 + B^3 = C^8$ and $A^2 + B^3 = C^{10}$, which are solved ([6, Theorem 1.3] and [3, 29]). We solve all seven.

1.2. **The result.**

Theorem 1.1. *The primitive solutions $(x, y, z) \in \mathbb{Z}^3$ of the following equations are exactly those listed.*

(a) $x^5 + y^4 - 2z^2 = 0$: $(-1, \pm 1, 0)$ *and* $(1, \pm 1, \pm 1)$.
(b) $x^5 + y^4 - 3z^2 = 0$: $(-1, \pm 1, 0)$ *and* $(11, \pm 29, \pm 538)$.
(c) $x^5 + y^4 + 3z^2 = 0$: $(-1, \pm 1, 0)$.
(d) $2x^4 - y^4 + z^3 = 0$: $(0, \pm 1, 1)$ *and* $(\pm 1, \pm 1, -1)$.
(e) $x^4 + 3y^3 + 2z^3 = 0$: $(\pm 1, -1, 1)$.
(f) $x^4 + 4y^3 + z^3 = 0$: $(\pm 1, 0, -1)$.
(g) $x^4 + 3y^3 + z^3 = 0$: $(\pm 1, 0, -1)$ *and* $(\pm 895, -6202, 4199)$.

All choices of the signs $\pm$ are allowed, independently.

The solution $(11, \pm 29, \pm 538)$ of (b) comes from

$$11^5 + 29^4 = 161\,051 + 707\,281 = 868\,332 = 3 \cdot 538^2,$$

and the solution $(\pm 895, -6202, 4199)$ of (g) from $3 \cdot 6202^3 - 4199^3 = 641\,641\,050\,625 = 895^4$. They are the only primitive solutions of the seven equations with an entry other than 0 and ± 1. The solutions with $xyz \neq 0$ are $(1, \pm 1, \pm 1)$ for (a), $(11, \pm 29, \pm 538)$ for (b), $(\pm 1, \pm 1, -1)$ for (d), $(\pm 1, -1, 1)$ for (e) and $(\pm 895, -6202, 4199)$ for (g). Equations (c) and (f) have none.

1.3. **Equation (g).** Equation (g), with $H = 48$, is the smallest of the seven. Grechuk asked on MathOverflow [20] whether the primitive solutions of Theorem 1.1(g) are the only ones, for the equation written as $3y^3 + z^3 = x^4$. An answer there by S. Y. Xiao proposes a reduction to rational points on plane quartic curves of genus 3 and does not determine them.

J. Agbanwa [1] announced a proof that the list is complete, in an unpublished manuscript, by a descent over $\mathbb{Q}(\sqrt[3]{3})$ and a computer determination of the rational points on three curves of genus 2. The equation is still listed as open in version 9 of [19]. Sections 9, 10 and 11 prove the list by a different method from that of [1]. Both proofs begin with a descent over $\mathbb{Q}(\sqrt[3]{3})$ and meet curves of genus 2. This descent leaves two classes of units, and for one of them (the class $j = 1$ of Section 9) our proof also leads to a curve $Y^2 = g(t)$ of genus 2. We do not determine its rational points: a computation gives two independent divisor classes on its Jacobian, so its rank is at least its genus and Chabauty's method does not apply directly (Remark 9.5). We pass instead to a covering by a curve of genus one over a field of degree 12 (Sections 10 and 11). We have not checked the arguments of [1].

1.4. **The method.** Methods based on Frey curves and modularity treat families of equations with a large prime exponent. For a single small signature one proceeds instead by descent: a factorization over a number field of small degree turns a primitive solution into a point on one of finitely many curves, and one determines the points on each curve that come from solutions. The difficulty is to reach curves on which this can be done. Elliptic Chabauty needs an elliptic curve whose rank is smaller than the degree of its field, and the descents need class groups and unit groups, which we determine without assuming the generalized Riemann hypothesis (GRH).

Equations (a)–(c) (Sections 3, 4 and 5). Write them as $x^5 + y^4 = Dz^2$ with $D \in \{2, 3, -3\}$. In $\mathbb{Q}(\sqrt{D})$, which has class number 1, the element $y^2 + z\sqrt{D}$ is a unit times a fifth power, and comparing rational parts gives $y^2 = F(a, b)$ for one of finitely many binary quintic forms F. When F is irreducible, a 2-descent over the quintic field that it defines leaves no solution, except in one case, where it leaves a curve of genus one over that field. Its Jacobian has rank 2, and elliptic Chabauty over the quintic field with a Mordell–Weil sieve finishes the proof. When F has a linear factor, a further descent leads to elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ of ranks 0 and 1 and to a curve of genus 2 over $\mathbb{Q}$ whose Jacobian has rank 0. Elliptic Chabauty at the prime 11 on the curve of rank 1 finds the solution $(11, \pm 29, \pm 538)$ and no other.

Equations (d)–(f) (Sections 6, 7 and 8). For (d), a descent over $\mathbb{Q}(\sqrt{2})$ leads to elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ with finitely many points and, after a further descent over a cubic field, to a curve of genus one over that field. For (e) and (f), a descent over the pure cubic fields $\mathbb{Q}(\sqrt[3]{12})$ and $\mathbb{Q}(\sqrt[3]{2})$ and the parametrization of a conic put a solution on a curve of genus one over the cubic field, at a point with a rational coordinate. The five curves over cubic fields that arise have Jacobians of rank 1 or 2, less than the degree 3, and elliptic Chabauty with a Mordell–Weil sieve determines their points with a rational coordinate.

Equation (g) (Sections 9, 10 and 11). In $K_g = \mathbb{Q}(\sqrt[3]{3})$ the element $-(z + y\sqrt[3]{3})$ is a unit of norm 1 times a fourth power. Conditions at 2 leave two classes of such units modulo fourth powers, $j = 0$ and $j = 1$, and as for (e) and (f) a conic puts the solution on a curve of genus one over K_g, at a point with a rational coordinate t. For $j = 0$ the Jacobian has rank 2 and elliptic Chabauty gives only $(\pm 1, 0, -1)$. For $j = 1$ three independent points show that the Jacobian has rank at least $3 = [K_g : \mathbb{Q}]$ (Remark 9.5), so elliptic Chabauty over K_g cannot be used, and we argue differently. Here t is the first coordinate of a rational point on the curve $Y^2 = g(t)$ of genus 2, and t lies in the 2-adic disk $2 + 8\mathbb{Z}_2$ (Lemma 9.4). The six roots of g fall into three pairs, the roots of three quadratic factors of g that are conjugate over $\mathbb{Q}$, and the sum of two roots from different pairs generates a field Ξ of degree 12. A 2-covering, in the sense of the covering collections of Bruin and Flynn [8] and Flynn and Wetherell [16], puts t on a curve C_g of genus one over Ξ. Its Jacobian E_g has rank between

2 and 6, where 6 is the bound given by the Selmer groups of a 2-isogeny (Section 10). These Selmer groups are computable without GRH because Ξ has class number 1, while a full 2-descent would need the class group of the field $\Xi(\sqrt{-1})$, of degree 24, generated by the 2-torsion of E_g, which we know only under GRH. As we do not know the rank, we use Stoll's form of Chabauty's method [34], which needs only a Selmer group that injects into the corresponding local group at one prime, and we apply it at the prime 2 through the 2-isogeny.

Stoll's method needs a condition at every 2-adic point P of C_g with $t(P) \in 2 + 8\mathbb{Z}_2$. Let $A = [P - B] \in E_g$ for a base point B. Then, for every $m \geq 0$, the local classes of the points Q with $2^m Q = A$ that come from the Selmer group must be those of the two rational torsion points, and similarly on the isogenous curve (Definition 11.1 and Theorem 11.2). We verify this by covering these 2-adic points with 128 disks, with explicit 2-adic estimates on each disk. Near the four points of C_g with $t = 2$ and $t = -\frac{10}{3}$, which come from the non-primitive solution $(\pm 3, 6, -9)$ and from $(\pm 895, -6202, 4199)$, we use an explicit form of Stoll's Lemmas 3.4 and 3.7 [34] (Section 11).

1.5. **Relation to earlier work.** *Neighboring equations.* The case $D = -2$ of $x^5 + y^4 = Dz^2$ is the equation $A^4 + 2B^2 = C^5$, solved by Bennett, Ellenberg and Ng [2, §9, Proposition 16]. In our coordinates (x, y, z) its primitive solutions are $(-1, \pm 1, 0)$ and $(-3, \pm 1, \pm 11)$. Their reduction leads to $y^2 = a(a^4 - 20a^2b^2 + 20b^4)$, which has the shape of our case $k = 0$, and they also finish with elliptic Chabauty over a number field. The cases $D = \pm 1$ belong to the signature $(2, 4, 5)$, solved by Bruin [6, Theorems 1.1 and 1.2]. For $D = 1$ there are, for instance, the solutions $(3, \pm 11, \pm 122)$ and $(-2, \pm 3, \pm 7)$. Equation (c) is $3z^2 + y^4 = (-x)^5$, the exponent-5 member of the family $3x^2 + y^4 = z^r$, which Dieulefait and Urroz solved for primes $r > 131$ [13] (see also Pacetti and Villagra Torcomian [23]). The exponent 5 lies outside that range. Among the neighbors of (e) and (f), $x^4 + 2y^3 + 2z^3 = 0$ is solved by Wilcox [35, Appendix A, Proposition A.4], and the equations $x^3 + y^3 = z^4$ and $x^3 + y^3 = z^5$ with coefficients one by Bruin [5]. The identity used above for $x^4 + 2y^3 + z^3 = 0$ has analogues for (e) and (f), which lead to $X^2 + 3Y^3 = x^8$ and $X^2 + 2Y^3 = x^8$. We have not found these equations solved, so they give no shortcut. A neighbor of (d), $y^4 + 2x^4 = z^3$, was solved by Söderlund [32].

Methods. Descents of this kind for generalized Fermat equations, with elliptic Chabauty over number fields to finish, go back to Bruin [4, 6, 7]. Elliptic Chabauty is due to Bruin [6] and to Flynn and Wetherell [15, 16]. Our criterion (Lemma 2.3) is a linear-algebra test modulo p of the type used in Siksek's explicit Chabauty over number fields [29]. The Mordell–Weil sieve goes back to Scharaschkin [28] and Flynn [14]. See Bruin and Stoll [10] and, for its use together with other methods, Bugeaud, Mignotte, Siksek, Stoll and Tengely [11]. The descent for $y^2 = F(a, b)$ with a binary form F of odd degree is a two-cover descent in the sense of Bruin and Stoll [9]. For the 2-descents on elliptic curves over number fields see [30, Chapter X] and [31], and for Jacobians of curves of genus 2, Schaefer [26] and Stoll [33]. For (g), the descent, the conics, elliptic Chabauty and the sieve are those used for (e) and (f), and the descent via 2-isogeny is classical [30, §X.4]. Stoll's theorem [34, Theorem 2.1] and his local lemmas [34, §3] are the basis of Section 11. Freitas, Naskręcki and Stoll used his method in an elliptic-Chabauty setting for $x^2 + y^3 = z^{11}$ [17].

What is new is the complete list of solutions of equations (a)–(f), and, for (g), a proof of the list asked about in [20], by a different method from that of Agbanwa [1]: a covering over a field of degree 12 and Stoll's form of Chabauty's method at 2, where his proof uses three curves of genus 2. One technical point may be of use elsewhere: the Chabauty criterion is

stated and proved in the form in which it is applied (Lemma 2.3). For (g), the covering over a field of degree 12 is new. The closest precedent for the 2-adic part is Stoll's elliptic-Chabauty example [34, §9]: it applies his method at the prime 2 to an elliptic curve over a field of degree 10, restricted to the points with rational x-coordinate, and uses [34, Lemma 3.7] over completions of ramification index 2 without writing out the estimates. Another close precedent is [17, §7.2]: Freitas, Naskręcki and Stoll apply his method at 2 to the points of $X_0(11)$ over fields of degree 12 with rational j-coordinate and write out their 2-adic estimates [17, Lemmas 7.9 and 7.10], but $X_0(11)$ is defined over $\mathbb{Q}$ and has good reduction at 2. In Section 11 the 2-adic estimates for a curve of genus one parametrized by a rational coordinate are written out in full, over completions of ramification index up to 4 at which the Jacobian has additive reduction. In Stoll's application at the prime 2 to Fermat's Last Theorem [34, §7] the curves are defined over $\mathbb{Q}$ with good reduction at 2, and ramification occurs only in the algebra $\mathbb{Q}_2(2^{1/l})$ generated by the 2-torsion. Here the curve is defined over the ramified completions themselves, its Jacobian has additive reduction there, and the formal logarithm is an isometry only from the level $e+1$ of the filtration on, where e is the ramification index. So the estimates of Lemmas 11.3 and 11.6 replace [34, (3.1)], and Lemma 11.8 is an explicit version of [34, Lemmas 3.4 and 3.7] for this setting.

1.6. **What is assumed, and what is computed.** Besides standard theory, the proofs rest on explicit computations with PARI/GP 2.17.3 [24], stated in the text as numbered lemmas and propositions. All arithmetic is exact: integers, rationals, number fields given by explicit polynomials, finite fields, and p-adic numbers with tracked precision, a local square class or valuation being read off only when the precision suffices to determine it. No step assumes the generalized Riemann hypothesis. PARI's `bnfinit` and `bnfunits`, which are correct under that hypothesis, are used only to propose ideal generators, units and S-units, which are then checked without assuming GRH, and every class group the proofs use is bounded by Minkowski's bound with explicit generators of the prime ideals below the bound (Appendix A). Local conditions at the real places are proved by sign arguments stated in the text. Every computation on which the proofs depend was carried out by two separately written programs, which Appendix C describes, and the programs and their outputs are deposited at [21].

1.7. **Plan and notation.** Section 2 collects the tools: square classes and local images, a model change from quartics to Weierstrass form, saturation, the sieve and a Chabauty criterion. Sections 3, 4 and 5 prove (a)–(c), Sections 6 and 7 reduce (d), (e) and (f) to five curves of genus one over cubic fields, which Section 8 treats, and Sections 9, 10 and 11 prove (g). Appendix A proves the class numbers used, Appendix B gives the data for (g), and Appendix C describes the computations.

For a number field K, $\mathcal{O}_K$ is its ring of integers, Nm the norm to $\mathbb{Q}$, and $v_{\mathfrak{p}}$ the normalized valuation at a prime ideal $\mathfrak{p}$. For a finite set S of primes of K, $K(S,2)$ is the subgroup of $K^\times/K^{\times 2}$ of classes δ with $v_{\mathfrak{p}}(\delta)$ even for every $\mathfrak{p}\notin S$. When $\mathrm{Cl}(K)=1$, it equals $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ and has dimension $r_1+r_2+\#S$ over $\mathbb{F}_2$, where (r_1,r_2) is the signature of K. We write $\mathbb{P}^1(\mathbb{Q})=\mathbb{Q}\cup\{\infty\}$, and "$X\in\mathbb{P}^1(\mathbb{Q})$" for a function X on a curve means that its value is rational or infinite.

2. Tools

2.1. **Square classes and local images.** Let $\mathfrak{p}$ be a prime of a number field K above p, with completion $K_{\mathfrak{p}}$ and normalized valuation $v=v_{\mathfrak{p}}$. If $\alpha,\alpha'\in K_{\mathfrak{p}}^\times$ and $v(\alpha'-\alpha)>v(\alpha)+2v(2)$,

then α'/α is a square in $K_\mathfrak{p}$, since $1+\xi$ is a square when $v(\xi) > 2v(2)$ (Hensel's lemma). So the class of α in $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ is determined by α modulo $\mathfrak{p}^{v(\alpha)+2v(2)+1}$. Similarly, its class modulo fourth powers is determined modulo $\mathfrak{p}^{v(\alpha)+3v(2)+1}$.

Several steps below need the *local image* of a map from the p-adic points of a variety to a group of square classes: for instance, for a root ϑ of a binary form F with leading coefficient c (as in Lemma 5.1), the set of classes of $ca-\vartheta b$ in $\prod_{\mathfrak{p}\mid p} K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ as (a,b) runs over the primitive pairs in $\mathbb{Z}_p^2$ satisfying some conditions. We compute such images by covering the p-adic points by residue classes modulo p^n and refining a class until every quantity involved has constant square class on it, using the criterion above with explicit valuations. The refinement stops at a fixed exponent n, the *depth* of the computation. A residue class on which some quantity still does not have constant class at that depth is either kept with all classes it could contribute (so the computed set contains the true image), or treated by a separate argument that is stated where it occurs. A set computed this way contains the local image, and this suffices for an argument showing that no class survives. Where the text asserts that the computed set *equals* the image, the programs also exhibit a point for every class. Classes are compared through Hilbert symbols or through discrete logarithms in $(\mathcal{O}_K/\mathfrak{p}^{2e+1})^\times$ with $e=v(2)$.

2.2. **Class groups and units.** Every class number used below is bounded by Minkowski's bound: every ideal class contains an integral ideal of norm at most $M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$, where $n=[K:\mathbb{Q}]$ and d_K is the discriminant, so if every prime ideal of norm at most M_K is principal then $\mathrm{Cl}(K)=1$. Appendix A lists, for each field, the prime ideals below the bound and explicit generators. A set of units, or of S-units, is shown to be independent modulo squares by its quadratic residue characters at auxiliary primes. When the set has $r_1+r_2+\#S$ elements and $\mathrm{Cl}(K)=1$, it is a basis of $K(S,2)$.

2.3. **Quartic curves and Weierstrass models.**

Lemma 2.1. *Let k be a field of characteristic 0 and $H(u)=u^4+bu^3+cu^2+du+e\in k[u]$ a monic quartic with nonzero discriminant. Put $\kappa_H = c-b^2/4$ and*

$$E:\ V^2 = U^3+4cU^2+(16bd-64e)U+64(d^2-4ce+b^2e).$$

The maps

$$(u,w)\mapsto(U,V) = \big(8w+8u^2+4bu,\ 4Uu+16\kappa_H u+bU+8d\big),$$
$$(U,V)\mapsto(u,w) = \Big(\frac{V-bU-8d}{4(U+4\kappa_H)},\ \frac{U}{8}-u^2-\frac{b}{2}u\Big),$$

are mutually inverse birational maps between the curve $w^2=H(u)$ and E, so they extend to an isomorphism of the smooth projective model of $w^2=H(u)$ with E. The point at infinity with $w/u^2\to 1$ goes to the origin O of E, and the one with $w/u^2\to -1$ goes to a point with $U=-4\kappa_H$.

Proof. Put $X=U/8=w+u^2+\frac{b}{2}u$. Squaring $w=X-u^2-\frac{b}{2}u$ and using $w^2=H(u)$ gives $X^2-e=(2X+\kappa_H)u^2+(bX+d)u$. Hence $Y':=2(2X+\kappa_H)u+bX+d$ satisfies $Y'^2=(bX+d)^2+4(2X+\kappa_H)(X^2-e)=8X^3+4cX^2+(2bd-8e)X+d^2-4\kappa_H e$, which is the equation of E in $U=8X$, $V=8Y'$. Solving the definitions of X and Y' for w and u gives the inverse. Along the branch $w=u^2+\frac{b}{2}u+\frac{\kappa_H}{2}+O(1/u)$ we have $U\to\infty$, and along $w=-(u^2+\frac{b}{2}u+\frac{\kappa_H}{2})+O(1/u)$ we have $U\to -4\kappa_H$. □

All coefficients of these maps lie in $\mathbb{Z}[\frac{1}{2}][b,c,d,e]$, and the discriminant of the model E is $2^{16}\operatorname{disc} H$. Hence, if $\mathfrak{q}$ is a prime of a number field not dividing 2, the coefficients of H are $\mathfrak{q}$-integral and $\operatorname{disc} H$ is a $\mathfrak{q}$-unit, then both curves have good reduction at $\mathfrak{q}$, the maps reduce to mutually inverse isomorphisms of the reductions, and for a point P the reduction of $u(P)\in\mathbb{P}^1$ is the value of the reduced function at the reduction of P.

A curve $C: Y^2=Q(x)$ with Q of degree 4 and a point (x_0,Y_0) with $Y_0\neq 0$ is brought to this form by $u=1/(x-x_0)$ and $w=Yu^2/Y_0$, which give $w^2=H(u):=u^4Q(x_0+1/u)/Y_0^2$, a monic quartic. The point (x_0,Y_0) goes to the point at infinity with $w/u^2\to 1$ and so to O, and on E the function x is x_0+1/u.

2.4. **Mordell–Weil groups.** Let E be an elliptic curve over a number field K and $G=E(K)$. An upper bound for $\operatorname{rank} G$ comes from a 2-descent: $\operatorname{rank} G\le \dim_{\mathbb{F}_2}\operatorname{Sel}^2(E/K)-\dim_{\mathbb{F}_2}E(K)[2]$, where the 2-Selmer group is computed inside $M(S,2)$ for the étale algebra M of 2-torsion (or inside $K(S,2)$ for a descent by 2-isogeny) [30, Chapter X], [31]. The local images are computed as spans of images of local points, and each is checked to reach the dimension it must have: $\dim E(K_v)[2]+[K_v:\mathbb{Q}_2]$ for $v\mid 2$, $\dim E(K_v)[2]$ for other finite v, and $\dim E(\mathbb{R})[2]-1$ at a real place. For a descent by a 2-isogeny $\phi\colon E\to E'$ with dual $\hat\phi$, whose kernels are generated by K-rational points, the two local images satisfy

$$\dim_{\mathbb{F}_2}E'(K_v)/\phi(E(K_v))+\dim_{\mathbb{F}_2}E(K_v)/\hat\phi(E'(K_v))=\begin{cases}2+[K_v:\mathbb{Q}_2] & (v\mid 2),\\ 2 & (v\nmid 2\text{ finite}),\\ 1 & (v\text{ real}).\end{cases}$$

Indeed, the exact sequence of groups of K_v-points

$$0\to E'[\hat\phi]/\phi(E[2])\to E'/\phi E\to E/2E\to E/\hat\phi E'\to 0$$

shows that the left side is $\dim E(K_v)/2E(K_v)+\dim E'(K_v)[\hat\phi]/\phi(E(K_v)[2])$. Here $\#E(K_v)/2E(K_v)$ is $\#E(K_v)[2]\cdot 2^{[K_v:\mathbb{Q}_2]}$ if $v\mid 2$ and $\#E(K_v)[2]$ at the other finite places [27, Proposition 3.9], and $\#E(\mathbb{R})[2]/2$ at a real place, where $E(\mathbb{R})$ is a circle or a circle times $\mathbb{Z}/2$. The second term is 0 if $E(K_v)[2]$ has order 4 and 1 if it has order 2. We call this the *local dimension formula*, and each pair of local images is checked to reach it. A lower bound comes from explicit points. When their images, together with those of a basis of $E(K)[2]$, are independent under quadratic characters at auxiliary primes of the Kummer map $P\mapsto(U(P)-e_i)_i$, where e_1,e_2,e_3 are the roots of the cubic in U defining E, the points are independent of infinite order and no point of $E(K)[2]\smallsetminus\{O\}$ lies in $2G$, so G has no point of order 4.

Torsion of odd order is excluded by counting points: if $\mathfrak{q}$ is a prime of good reduction above an odd prime q with ramification index $e(\mathfrak{q}/q)<q-1$, then $E(K)_{\mathrm{tors}}$ injects into $E(\mathbb{F}_{\mathfrak{q}})$ [30, Theorem IV.6.4 and Proposition VII.3.1]. For Jacobians of curves of genus 2 over $\mathbb{Q}$ we use the same fact at odd primes of good reduction: if an abelian variety A over $\mathbb{Q}$ has good reduction at an odd prime p, then $A(\mathbb{Q})_{\mathrm{tors}}$ injects into $A(\mathbb{F}_p)$. This is the case $K=\mathbb{Q}$ of [22, Appendix, Lemma]: for an abelian variety A over a number field K and a prime $\mathfrak{p}$ of K above p with absolute ramification index less than $p-1$, the torsion of $A(K)$ injects into the special fiber at $\mathfrak{p}$ of the Néron model of A, which is the reduction of A when A has good reduction at $\mathfrak{p}$.

Lemma 2.2. *Let $G'\subseteq G$ be abelian groups with G/G' finite, ℓ a prime with $G[\ell]\subseteq G'$, and $\psi: G\to A$ a homomorphism to an abelian group A with $\ell A=0$ whose restriction to G' induces an injection $G'/\ell G'\to A$. Then ℓ does not divide $[G:G']$.*

Proof. Otherwise some $Q \in G \smallsetminus G'$ has $\ell Q \in G'$. Then $\psi(\ell Q) = \ell\psi(Q) = 0$, so $\ell Q \in \ell G'$, say $\ell Q = \ell P'$ with $P' \in G'$. Then $Q - P' \in G[\ell] \subseteq G'$, so $Q \in G'$, a contradiction. □

We apply Lemma 2.2 with $G' = \langle g_1, \dots, g_r \rangle + E(K)_{\mathrm{tors}}$ for explicit points g_i. For $\ell = 2$, ψ is the Kummer map above. For odd ℓ, ψ is reduction at one or two primes $\mathfrak{q}$ of good reduction at which the ℓ-part of $E(\mathbb{F}_\mathfrak{q})$ is cyclic, followed by the projection to $E(\mathbb{F}_\mathfrak{q})/\ell E(\mathbb{F}_\mathfrak{q})$, computed by discrete logarithms. As $E(K)[\ell] = 0$ in all our cases, the hypothesis $G[\ell] \subseteq G'$ holds.

2.5. **The Mordell–Weil sieve.** Let $G' = \langle g_1, \dots, g_r \rangle + T$ with $T = E(K)_{\mathrm{tors}}$ have index n_0 in $G = E(K)$. Let $M \geq 1$ be an integer prime to n_0 with $MT = 0$. If $n_0 n_0' \equiv 1 \pmod{M}$, then every $P \in G$ satisfies $P = n_0'(n_0 P) + (1 - n_0 n_0')P \in G' + MG$, so

$$P = \textstyle\sum_i a_i g_i + t + MQ \qquad (a \in \mathbb{Z}^r,\ t \in T,\ Q \in G), \tag{2.1}$$

and the class of $(a \bmod M, t)$ is determined by P, because $G'/MG' \to G/MG$ is an isomorphism. If $\mathfrak{q}$ is a prime of good reduction and M is a multiple of the exponent of $E(\mathbb{F}_\mathfrak{q})$, then P and $\sum_i a_i g_i + t$ have the same reduction at $\mathfrak{q}$. Suppose that a function X on E reduces well at every prime $\mathfrak{q}$ above a rational prime q, in the sense of the paragraph after Lemma 2.1: the reduction of $X(P)$ at $\mathfrak{q}$ is the value of the reduced function at the reduction of P. If $X(P) \in \mathbb{P}^1(\mathbb{Q})$, then the reductions of $X(P)$ at the primes $\mathfrak{q} \mid q$ are one and the same element of $\mathbb{P}^1(\mathbb{F}_q)$. Further conditions ("$f(X)$ is a square") may be imposed in the same way. Each such condition at q depends only on $(a \bmod L_q, t)$, where L_q is the exponent of $\prod_{\mathfrak{q}|q} E(\mathbb{F}_\mathfrak{q})$. To collect the conditions at several primes q in a fixed modulus N, take $M = \mathrm{lcm}(N, L_q : q)$, and say that a class $(a' \bmod L_q, t)$ *passes* at q if it satisfies the conditions imposed at q. A class $(a \bmod N, t)$ survives at q if some class $(a' \bmod L_q, t)$ that passes at q has $a' \equiv a \pmod{\gcd(N, L_q)}$. The decomposition (2.1) with this M requires n_0 to be prime to N and to every L_q. We verify this below by Lemma 2.2 at every prime ℓ dividing N or an L_q of a prime q that removes classes, that is, at which some class surviving the earlier primes does not survive. A prime that removes no class can be left out of the sieve, and its L_q out of M, without changing the set of surviving classes.

2.6. **Elliptic Chabauty.**

Lemma 2.3. *Let K be a number field of degree d and $p \geq 3$ a prime that splits completely in K, with embeddings $\sigma_1, \dots, \sigma_d : K \to \mathbb{Q}_p$. Let E/K be given by $V^2 = U^3 + a_2U^2 + a_4U + a_6$ such that each conjugate E^{σ_j} has coefficients in $\mathbb{Z}_p$ and good reduction. Let $G = E(K)$, of rank $r \leq d - 1$, and let $g_1, \dots, g_r \in G$ with $p \nmid m := [G : \langle g_1, \dots, g_r \rangle + G_{\mathrm{tors}}]$. Let $N \geq 1$ kill $E^{\sigma_j}(\mathbb{F}_p)$ for every j. Let $\rho = A/B$ with $A, B \in K[U, V]$ whose coefficients are p-integral at every σ_j, and let $\mathcal{D} = 2V\,\partial/\partial U + (3U^2 + 2a_2U + a_4)\,\partial/\partial V$, the derivation dual to the invariant differential $\omega = dU/2V$. Let $P_0 \in G$ with $\rho(P_0) \in \mathbb{Q}$, and suppose that either*

(i) *no $P_0^{\sigma_j}$ reduces to the origin and every $B(P_0)^{\sigma_j}$ lies in $\mathbb{Z}_p^\times$; put $c_j = \sigma_j((\mathcal{D}\rho)(P_0))$; or*

(ii) *$P_0 = O$, and $\rho^{\sigma_j}(Z_j(t)) \in \mathbb{Z}_p[[t]]$ for every j, where $Z_j(t)$ is the point of E^{σ_j} with formal parameter $t = -U/V$; let c_j be the coefficient of t.*

Let $\lambda_{ij} = \log_j(N \cdot g_i^{\sigma_j})$, where $\log_j$ is the formal logarithm of E^{σ_j}, normalized by $\log_j(t) = t + O(t^2)$, and let $\mathcal{J}$ be the $(d-1) \times r$ matrix with entries $\mathcal{J}_{j-1,i} = c_1\lambda_{i1} - c_j\lambda_{ij}$ $(2 \leq j \leq d)$. Then $\mathcal{J}$ has entries in $p\mathbb{Z}_p$, and if $\mathcal{J}/p$ has rank r modulo p, then P_0 is the only point $P \in P_0 + N \cdot G$ with $\rho(P) \in \mathbb{Q}$. If moreover $p \nmid N$, then P_0 is the only point $P \in P_0 + G^0$ with $\rho(P) \in \mathbb{Q}$, where $G^0 \supseteq N \cdot G$ is the subgroup of $Q \in G$ such that every Q^{σ_j} reduces to the origin.

Proof. (a) *Parametrization.* Let $E_1^{(j)}$ be the kernel of reduction in $E^{\sigma_j}(\mathbb{Q}_p)$. Since $p \geq 3$, $\log_j : E_1^{(j)} \to p\mathbb{Z}_p$ is an isomorphism of groups [30, Theorem IV.6.4]. For $g \in G$, $N \cdot g^{\sigma_j} \in E_1^{(j)}$ because N kills $E^{\sigma_j}(\mathbb{F}_p)$. Write $mg = \sum_i b_i g_i + \tau$ with $b_i \in \mathbb{Z}$ and τ torsion. Torsion injects into $E^{\sigma_j}(\mathbb{F}_p)$ [30, Proposition VII.3.1 and Theorem IV.6.4], so $N\tau = 0$. Hence $\log_j(Ng^{\sigma_j}) = \sum_i \beta_i \lambda_{ij}$ with $\beta_i = b_i/m \in \mathbb{Z}_p$, the same β for every j. So every $P \in P_0 + N \cdot G$ has $P^{\sigma_j} = P_0^{\sigma_j} + Z_j(z_j(\beta))$, where $z_j(\beta) = \exp_j(\sum_i \beta_i \lambda_{ij})$ and $\beta \in \mathbb{Z}_p^r$. Here $\beta = 0$ gives P_0, and different P give different β because $E_1^{(j)}$ is torsion-free. If $p \nmid N$ and $Q \in G^0$, then $mNQ = \sum_i b_i N g_i$ as before, so $\log_j(Q^{\sigma_j}) = \sum_i \beta_i \lambda_{ij}$ with $\beta_i = b_i/(mN) \in \mathbb{Z}_p$, and the same parametrization covers $P_0 + G^0$.

(b) *Integrality.* Write $\exp_j(T) = \sum_k \epsilon_k T^k$ with $k!\,\epsilon_k \in \mathbb{Z}_p$ [30, Proposition IV.5.5]. Since $\lambda_{ij} \in p\mathbb{Z}_p$ and $v_p(p^k/k!) \geq 2$ for $k \geq 2$ (as $p \geq 3$), $z_j(\beta) \equiv \sum_i \beta_i \lambda_{ij}$ modulo $p^2\mathbb{Z}_p[[\beta]]$, and all coefficients of z_j lie in $p\mathbb{Z}_p$. In case (i), translation by $P_0^{\sigma_j}$ is an automorphism of the smooth model over $\mathbb{Z}_p$, so U and V at $P_0^{\sigma_j} + Z_j(t)$ are power series in $\mathbb{Z}_p[[t]]$. As $B(P_0)^{\sigma_j}$ is a unit, $f_j(t) \coloneqq \rho^{\sigma_j}(P_0^{\sigma_j} + Z_j(t)) \in \mathbb{Z}_p[[t]]$, and its coefficient of t is c_j because $\omega = (1 + O(t))\,dt$ and ω is invariant under translation. In case (ii) this is the hypothesis. Hence $f_j(z_j(\beta)) \equiv \rho(P_0) + c_j \sum_i \beta_i \lambda_{ij}$ modulo $p^2\mathbb{Z}_p[[\beta]]$, and the series converge on $\mathbb{Z}_p^r$.

(c) *Uniqueness.* $\rho(P) \in \mathbb{Q}$ exactly when $\sigma_1(\rho(P)) = \cdots = \sigma_d(\rho(P))$, since the σ_j are the d distinct embeddings of K. Put $\Phi(\beta) = \big(f_1(z_1(\beta)) - f_j(z_j(\beta))\big)_{2 \leq j \leq d}$. By (b), $\Phi(\beta) = p\,(\mathcal{J}'\beta + p\,\Omega(\beta))$ with $\mathcal{J}' = \mathcal{J}/p$ a matrix over $\mathbb{Z}_p$ and Ω a vector of power series over $\mathbb{Z}_p$ converging on $\mathbb{Z}_p^r$. If $\Phi(\beta) = \Phi(\beta') = 0$ then $\mathcal{J}'(\beta - \beta') = -p(\Omega(\beta) - \Omega(\beta'))$, and $\|\Omega(\beta) - \Omega(\beta')\| \leq \|\beta - \beta'\|$, since each monomial is 1-Lipschitz on $\mathbb{Z}_p^r$. If $\mathcal{J}'$ has rank r modulo p, then $\|\mathcal{J}'(\beta - \beta')\| = \|\beta - \beta'\|$, so $\|\beta - \beta'\| \leq p^{-1}\|\beta - \beta'\|$ and $\beta = \beta'$. Since $\beta = 0$ is a zero, it is the only one. □

In the applications the entries λ_{ij} are needed only modulo p^2: if $t_{ij} \in p\mathbb{Z}_p$ is the formal parameter of $N \cdot g_i^{\sigma_j}$, then $\lambda_{ij} \equiv t_{ij} \pmod{p^2}$, because the formal logarithm is $t + \sum_{k \geq 2} (\alpha_k/k) t^k$ with $\alpha_k \in \mathbb{Z}_p$ and $v_p(t^k/k) \geq 2$ for $k \geq 2$.

3. The equations $x^5 + y^4 = Dz^2$: descent

For $D \in \{2, 3, -3\}$ let $\mathcal{E}_D$ denote the equation

$$x^5 + y^4 = Dz^2, \tag{3.1}$$

so that equations (a), (b), (c) of Theorem 1.1 are $\mathcal{E}_2$, $\mathcal{E}_3$ and $\mathcal{E}_{-3}$. A descent over $\mathbb{Q}(\sqrt{D})$ reduces $\mathcal{E}_D$ to the equations $y^2 = F_{D,k}(a, b)$ with binary quintic forms $F_{D,k}$, one for each case (D, k). Section 4 treats $k = 0$ and Section 5 the cases with $k \neq 0$.

Let $\mathcal{O}_D$ be the ring of integers of $\mathbb{Q}(\sqrt{D})$: $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\zeta]$ with $\zeta = (-1 + \sqrt{-3})/2$. Each has class number 1 (Minkowski's bound is below 2). Let $\varepsilon = \varepsilon_D$ be the fundamental unit $1 + \sqrt{2}$ (of norm -1) for $D = 2$ and $2 + \sqrt{3}$ (of norm 1) for $D = 3$. The units of $\mathbb{Z}[\zeta]$ are the six roots of unity.

Lemma 3.1. *Let (x, y, z) be a primitive solution of $\mathcal{E}_D$.*

(a) *x, y, z are pairwise coprime.*
(b) *If $z = 0$ then $(x, y) = (-1, \pm 1)$. There is no primitive solution with $x = 0$ or $y = 0$.*
(c) *If $D = 2$, then x and y are odd. If $D = \pm 3$, then exactly one of y, z is even, x is odd, and $3 \nmid xy$.*

Proof. (a) If a prime ℓ divides x and y, then $\ell^4 \mid Dz^2$, so $\ell \mid z$ because D is squarefree. A prime dividing z and one of x, y divides the other. (b) If $z = 0$ then $x^5 = -y^4$ with $\gcd(x, y) = 1$, so $(x, y) = (-1, \pm 1)$. If $x = 0$ then $y^4 = Dz^2$, impossible with $y \neq 0$ since D is not a square. If $y = 0$ then $x^5 = Dz^2$, so $|D|$ divides x. Then $|D|^5 \mid Dz^2$, so $|D| \mid z$, against (a). (c) If $D = 2$, then y is odd by (a), since $x^5 = 2z^2 - y^4$, and hence x is odd. Let $D = \pm 3$. If y and z are both odd, then $y^4 \equiv 1$ and $z^2 \equiv 1$ or $9 \pmod{16}$, so $x^5 = Dz^2 - y^4 \equiv 2$ or 10 (if $D = 3$), 4 or 12 (if $D = -3$) modulo 16: x is even but $32 \nmid x^5$, a contradiction. They are not both even, by (a). So exactly one is even and x is odd. Modulo 3 the equation reads $x^5 \equiv -y^4$, so 3 divides both x and y or neither, and by (a) it divides neither. □

Lemma 3.2. *Let (x, y, z) be a primitive solution of $\mathcal{E}_D$ with $z \neq 0$. Then*

$$y^2 + z\sqrt{D} = \varepsilon^k (a + b\sqrt{D})^5, \qquad x = -\operatorname{Nm}(\varepsilon)^k (a^2 - Db^2), \tag{3.2}$$

with coprime integers a, b and $k \in \{0, 1, 2, 3, 4\}$, where $k = 0$ if $D = -3$.

Proof. The norm of $y^2 + z\sqrt{D}$ is $y^4 - Dz^2 = (-x)^5$. A prime π of $\mathcal{O}_D$ dividing $y^2 + z\sqrt{D}$ and $y^2 - z\sqrt{D}$ divides $2y^2$ and $2z\sqrt{D}$. It does not divide 2, since the norm $(-x)^5$ is odd, and it does not divide $\sqrt{D}$ when $D = \pm 3$, since $3 \nmid y$ (Lemma 3.1(c)). So it divides y and z, against Lemma 3.1(a). As $\mathcal{O}_D$ is a principal ideal domain, $y^2 + z\sqrt{D} = u\,\alpha^5$ with u a unit and $\alpha \in \mathcal{O}_D$. Since $-1 = (-1)^5$, and for $D = -3$ every unit is a fifth power, we may take $u = \varepsilon^k$ with $0 \leq k \leq 4$, and $u = 1$ if $D = -3$. For $D = 2, 3$, $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Z}$. For $D = -3$ we show that $\alpha \in \mathbb{Z}[\sqrt{-3}]$. Modulo 2, $\mathbb{Z}[\zeta]$ becomes $\mathbb{F}_4$ and $\mathbb{Z}[\sqrt{-3}]$ becomes $\mathbb{F}_2$. The element $y^2 + z\sqrt{-3}$ has odd norm, so its image is 1, and α^5 has image $\bar{\alpha}^2$, which is 1 only if $\bar{\alpha} = 1$, that is, $\alpha \in \mathbb{Z}[\sqrt{-3}]$. A common prime factor of a and b would divide y^2 and z. Taking norms gives $(-x)^5 = \operatorname{Nm}(\varepsilon)^k (a^2 - Db^2)^5$. □

Expanding (3.2) gives $y^2 = F_{D,k}(a, b)$ and $z = G_{D,k}(a, b)$ with integral binary quintic forms. The forms used below are

$$\begin{aligned}
F_{2,0} &= a(a^4 + 20a^2b^2 + 20b^4), & F_{3,0} &= a(a^4 + 30a^2b^2 + 45b^4),\\
F_{-3,0} &= a(a^4 - 30a^2b^2 + 45b^4), & G_{3,0} &= b(5a^4 + 30a^2b^2 + 9b^4),\\
F_{2,1} &= a^5 + 10a^4b + 20a^3b^2 + 40a^2b^3 + 20ab^4 + 8b^5,\\
F_{2,2} &= 3a^5 + 20a^4b + 60a^3b^2 + 80a^2b^3 + 60ab^4 + 16b^5,\\
F_{3,1} &= 2a^5 + 15a^4b + 60a^3b^2 + 90a^2b^3 + 90ab^4 + 27b^5,\\
F_{3,2} &= 7a^5 + 60a^4b + 210a^3b^2 + 360a^2b^3 + 315ab^4 + 108b^5,
\end{aligned}$$

and $G_{2,0}(a, 0) = 0$, $G_{2,1}(1, 0) = 1$. For $k = 1, 2$ the polynomials $F_{D,k}(X, 1)$ are irreducible over $\mathbb{Q}$ with Galois group the Frobenius group F_{20} of order 20.

Lemma 3.3. *Let (x, y, z) be a primitive solution of $\mathcal{E}_D$.*

(a) *If (x, y, z) lies in the case k, that is, satisfies (3.2) with this k, then $(x, y, -z)$ lies in the case $-k \bmod 5$. So for $D = 2, 3$ it suffices to treat $k \in \{0, 1, 2\}$.*

(b) *If $D = 2$ then a is odd. If $D = \pm 3$ then $a + b$ is odd and $F_{D,k}(a, b) = y^2 \equiv 1 \pmod 3$.*

Proof. (a) Conjugating (3.2) gives $y^2 - z\sqrt{D} = \bar{\varepsilon}^k \bar{\alpha}^5$, and $\bar{\varepsilon} = \pm\varepsilon^{-1}$. The unit ε^{-k} is ε^{5-k} times a fifth power. (b) x is odd by Lemma 3.1(c), and $x = \pm(a^2 - Db^2) \equiv \pm(a + Db) \pmod 2$. Also $3 \nmid y$ by Lemma 3.1(c), so $y^2 \equiv 1 \pmod 3$. □

4. The case $k = 0$

The case $k = 0$ of equations (a)–(c) contains only the solutions of Theorem 1.1. We prove this for $D = 2$ in Proposition 4.1, for $D = -3$ in Proposition 4.5, and for $D = 3$ in Proposition 4.7.

For $k = 0$, (3.2) gives $y^2 = a\,Q(a,b)$ with $Q = a^4 + c_2a^2b^2 + c_4b^4$ and $(c_2, c_4) = (20, 20)$, $(30, 45)$, $(-30, 45)$ for $D = 2, 3, -3$. Since $\gcd(a, b) = 1$, $\gcd(a, Q(a, b))$ divides c_4. For $D = 2$, a is odd (Lemma 3.3(b)). For $D = \pm3$, $Q \equiv a^4 \pmod 3$, so $a \equiv a^5 \equiv y^2 \equiv 1 \pmod 3$. In both cases $\gcd(a, Q(a, b))$ divides 5, and as $y \neq 0$ (Lemma 3.1(b)),

$$a = d\,s^2, \qquad Q(a,b) = d\,t^2, \qquad d \in \{1, -1, 5, -5\},\ s, t \in \mathbb{Z}. \tag{4.1}$$

Proposition 4.1. *For $D = 2$, the case $k = 0$ contains only the solutions $(-1, \pm1, 0)$.*

Proof. Since $y^2 = aQ(a, b)$ and $Q(a, b) > 0$, we have $a > 0$ and $d \in \{1, 5\}$. The curve $dt^2 = a^4 + 20a^2b^2 + 20b^4$ in weighted projective coordinates $(a : b : t)$ has the rational points $(1 : 0 : \pm1)$ if $d = 1$ and $(0 : 1 : \pm2)$ if $d = 5$, so it is isomorphic to its Jacobian, which is

$$E_{(1)}:\ y^2 = x(x^2 - 10x + 20) \quad (d = 1), \qquad E_{(5)}:\ y^2 = x(x^2 - 50x + 500) \quad (d = 5),$$

both of conductor 1600. For both values of d, a descent via 2-isogeny gives the Selmer group $\{1, 5\}$ for $E_{(d)}$ and for its 2-isogenous curve, so $\operatorname{rank} E_{(d)}(\mathbb{Q}) = 0$. The numbers $\#E_{(d)}(\mathbb{F}_p)$ for the primes $7 \leq p < 200$ have greatest common divisor 2, so $E_{(d)}(\mathbb{Q}) = \{O, (0, 0)\}$. Hence each of the two quartic curves has exactly the two rational points listed, and $(a : b) = (1 : 0)$ or $(0 : 1)$. The second has $a = 0$ even, against Lemma 3.3(b). The first gives $a = 1$, $b = 0$, $y^2 = 1$, $z = G_{2,0}(1, 0) = 0$ and $x = -1$. □

For $D = \pm3$ put $\gamma = -c_2/2$, so that $\gamma = -15$ if $D = 3$ and $\gamma = 15$ if $D = -3$.

Lemma 4.2. *Let $D = \pm3$ and let (x, y, z) be a primitive solution of $\mathcal{E}_D$ in the case $k = 0$. Then $d = 1$, $a = s^2$ with s odd, and b is even. If $b = 0$ the solution is $(-1, \pm1, 0)$. If $b \neq 0$, then there are coprime integers u, h, exactly one of them even, with $|b| = |uh|$ and*

$$s^4 = u^4 + \gamma u^2h^2 + 45h^4. \tag{4.2}$$

Proof. From $a \equiv 1 \pmod 3$ we get $d \equiv 1 \pmod 3$, so $d \in \{1, -5\}$. If $D = 3$ then $Q(a, b) > 0$ forces $d > 0$, so $d = 1$. Let $D = -3$ and suppose $d = -5$. If a is odd then b is even and $Q \equiv 1 + 8(b/2)^2 \equiv 1$ or $9 \pmod{16}$, while t is odd and $-5t^2 \equiv 11$ or $3 \pmod{16}$. If a is even then $4 \mid a$, b is odd and $Q \equiv 45b^4 \equiv 13 \pmod{16}$, while $-5t^2 \equiv 11$ or 3. Both are impossible, so $d = 1$.

With $d = 1$: if $a = s^2$ were even, then b would be odd and $t^2 = Q \equiv 45 \equiv 13 \pmod{16}$, which is not a square. So a and s are odd and b is even. If $b = 0$ then $a = 1$, $y^2 = 1$, $z = 0$, $x = -1$. Let $b \neq 0$ and put $V = s^4 + \frac{c_2}{2}b^2$, which is odd. Then $t^2 - V^2 = (c_4 - c_2^2/4)b^4 = -180b^4$, and $P' = (t + V)/2$, $M' = (t - V)/2$ are integers with $P'M' = -45b^4$ and $P' - M' = V$. If a prime ℓ divides P' and M', then $\ell \mid V$ and $\ell^2 \mid 45b^4$. If $\ell \mid b$, then $\ell \mid V - \frac{c_2}{2}b^2 = s^4$, against $\gcd(a, b) = 1$. Otherwise $\ell^2 \mid 45$, so $\ell = 3$ and $3 \mid V \equiv s^4 \pmod 3$, against $a \equiv 1 \pmod 3$. So $\gcd(P', M') = 1$, and $P' = \sigma g_1u^4$, $M' = -\sigma g_2h^4$ with $\sigma = \pm1$, $g_1g_2 = 45$, $g_1 \in \{1, 5, 9, 45\}$, $\gcd(u, h) = 1$ and $|b| = |uh|$. Then $V = \sigma(g_1u^4 + g_2h^4)$, that is,

$$s^4 = \sigma(g_1u^4 + g_2h^4) + \gamma u^2h^2,$$

and exactly one of u, h is even because b is even. We exclude all cases but $(\sigma, g_1) \in \{(1, 1), (1, 45)\}$:

- $\sigma = -1$, $\gamma = -15$: the right side is negative, while $s^4 > 0$;

- $\sigma = -1$, $\gamma = 15$: if u is even, then modulo 16 we get $1 \equiv -g_2 - u^2$ with $u^2 \equiv 0$ or 4, so $g_2 \equiv 15$ or 11 (mod 16), while $g_2 \in \{45, 9, 5, 1\}$ is 13, 9, 5 or 1; if h is even, the same with g_1;
- $\sigma = 1$, $g_1 \in \{5, 9\}$: modulo 5 the equation reads $s^4 \equiv -h^4$ (if $g_1 = 5$) or $s^4 \equiv -u^4$ (if $g_1 = 9$); as fourth powers are 0 or 1 modulo 5, 5 divides s and h (resp. s and u), and then modulo 25 it divides u (resp. h) too, against $\gcd(u, h) = 1$.

Finally $(\sigma, g_1) = (1, 45)$ is $(1, 1)$ with u and h exchanged. □

Lemma 4.3. *Let u, h, s be as in Lemma 4.2. The point $(\xi_1 : \xi_2 : \xi_3) = (u^2 : h^2 : s^2)$ lies on the conic $\xi_3^2 = \xi_1^2 + \gamma\xi_1\xi_2 + 45\xi_2^2$, which is parametrized by*

$$(\xi_1 : \xi_2 : \xi_3) = (f_1 : f_2 : f_3)(m, n),$$
$$f_1 = 45m^2 - n^2, \qquad f_2 = m(2n - \gamma m), \qquad f_3 = n^2 - \gamma mn + 45m^2,$$

with inverse $(m : n) = (\xi_2 : \xi_3 - \xi_1)$. For the coprime integers m, n with $(m : n) = (h^2 : s^2 - u^2)$ there are $\mu \in \mathbb{Z}$ and $\lambda \in \{\pm 1, \pm 3, \pm 5, \pm 15\}$ such that

$$f_1(m, n) = \mu u^2, \quad f_2(m, n) = \mu h^2, \quad f_3(m, n) = \mu s^2, \qquad \mu \in \lambda\,\mathbb{Q}^{\times 2}, \tag{4.3}$$

and μ is odd, $v_2(f_3) = \min(v_2(f_1), v_2(f_2)) < \max(v_2(f_1), v_2(f_2))$.

Proof. The identity $f_3^2 = f_1^2 + \gamma f_1 f_2 + 45 f_2^2$ and the inverse are direct computations, as for instance $f_3 - f_1 = n(2n - \gamma m)$. Since $\gcd(u^2, h^2, s^2) = 1$, we have $f_i(m, n) = \mu\xi_i$ with $\mu = \pm \gcd(f_1, f_2, f_3)(m, n)$. A prime dividing μ divides the resultants of the pairs f_i, f_j, which are ± 45 and -2025. So $\mu = \pm 3^\alpha 5^\beta$, which is odd and lies in $\lambda\mathbb{Q}^{\times 2}$ for one of the eight values of λ. The last assertion holds because s is odd and exactly one of u, h is even. □

Write $Z^{(\lambda)}$ for the curve over $\mathbb{Q}$ defined by the conditions that $f_1(m, n)/\lambda$, $f_2(m, n)/\lambda$ and $f_3(m, n)/\lambda$ are squares. It is a $(\mathbb{Z}/2)^3$-covering of the line with coordinate $(m : n)$, of genus 5.

Lemma 4.4. *Pairs (m, n) satisfying (4.3) and the 2-adic condition of Lemma 4.3 exist over $\mathbb{R}$, $\mathbb{Q}_2$, $\mathbb{Q}_3$ and $\mathbb{Q}_5$ only for $\lambda \in \{1, -5\}$ if $\gamma = -15$, and only for $\lambda = -5$ if $\gamma = 15$.*

Proof. At the real place, for $\gamma = 15$ and $\lambda > 0$, we would need $f_1, f_2, f_3 \geq 0$. With $X = n/m$, $f_1 \geq 0$ gives $|X| \leq 3\sqrt{5} < 15/2$ and $f_2 \geq 0$ gives $X \geq 15/2$ (and $m = 0$ gives $f_1 = -n^2 < 0$), which is impossible. At $p \in \{2, 3, 5\}$ we refine residue classes (m_0, n_0) modulo p^j of primitive pairs until each f_i has constant square class on the residue class, which holds once $j \geq v_p(f_i(m_0, n_0)) + 3$ for $p = 2$ and $j \geq v_p(f_i(m_0, n_0)) + 1$ for odd p (Section 2.1). A class is discarded if some f_i has constant class different from that of λ, or, at $p = 2$, if all valuations are constant and violate the 2-adic condition. Classes not resolved at depth 14, 9, 7 (for $p = 2, 3, 5$) are kept. The kept set contains every local solution. For the three pairs (γ, λ) that remain, $(-15, 1)$, $(-15, -5)$ and $(15, -5)$, the kept sets are large, and Appendix C.1 gives their sizes. For the other values of λ there is no local point at the places listed in Table 1: at ∞ by the argument above, and at each prime listed because every residue class is resolved, and discarded, before the depth given above is reached. □

4.1. The case $D = -3$.

Proposition 4.5. *For $D = -3$ the case $k = 0$ contains only the solutions $(-1, \pm 1, 0)$.*

γ	λ	no point at	γ	λ	no point at
-15	-1	$2,3$	15	1	$\infty,2$
-15	3	$3,5$	15	-1	$2,3$
-15	-3	$2,3,5$	15	3	$\infty,3,5$
-15	5	$2,3$	15	-3	$2,3,5$
-15	15	$2,3,5$	15	5	$\infty,2,3$
-15	-15	$3,5$	15	15	$\infty,2,3,5$
			15	-15	$2,3,5$

TABLE 1. The places at which no pair (m,n) satisfies (4.3) and the 2-adic condition of Lemma 4.3, for the values of λ excluded in Lemma 4.4; ∞ is the real place.

Proof. By Lemma 4.2 we may assume $b \neq 0$, and then $\lambda = -5$ by Lemma 4.4. Write $\mu = \lambda g^2$. If $m \neq 0$, then $X = n/m$ and $W = \lambda^2 g^3 uhs/m^3$ give a rational point on the curve of genus 2

$$\begin{aligned} C:\ W^2 &= -5\,(45 - X^2)(2X - 15)(X^2 - 15X + 45) \\ &= 10X^5 - 225X^4 + 1125X^3 + 6750X^2 - 70875X + 151875, \end{aligned}$$

and $m = 0$ corresponds to the point ∞ of C. Let J be the Jacobian of C. The quintic factors over $\mathbb{Q}$ into irreducible factors of degrees 2, 1, 2, so $J(\mathbb{Q})[2] \simeq (\mathbb{Z}/2)^2$. A 2-descent on J over $\mathbb{Q}$, with local images at ∞, 2, 3, 5 of dimensions 2, 4, 2, 2, gives $\dim \mathrm{Sel}^2(J/\mathbb{Q}) = 2$, so $\operatorname{rank} J(\mathbb{Q}) = 0$. The numbers $\#J(\mathbb{F}_p)$ for the primes $7 \leq p \leq 300$ (all of good reduction, as the leading coefficient 10 and the discriminant of the quintic are divisible only by 2, 3, 5) have greatest common divisor 4, so $J(\mathbb{Q}) = J(\mathbb{Q})[2]$. If $P \in C(\mathbb{Q})$, then $[P - \infty] \in J(\mathbb{Q})[2]$, so $2P \sim 2\infty$ and P is ∞ or a Weierstrass point. The only rational root of the quintic is $15/2$. Hence $(m : n) \in \{(0 : 1), (2 : 15)\}$, where $f_2 = 0$, so $h = 0$, against $b \neq 0$. □

4.2. **The case $D = 3$.** For $D = 3$ we use elliptic curves over $\mathbb{Q}(\sqrt{5})$, which we now construct. Let $K = \mathbb{Q}(\sqrt{5})$ and $\tau = (1 + \sqrt{5})/2$. The ring $\mathcal{O}_K = \mathbb{Z}[\tau]$ has class number 1 and unit group $\pm\tau^{\mathbb{Z}}$. Let S be the set of primes of K above 2, 3, 5 (they are $2\mathcal{O}_K$, $3\mathcal{O}_K$ and $\sqrt{5}\mathcal{O}_K$), so that $K(S,2)$ has basis $-1, \tau, 2, 3, \sqrt{5}$. Let $r_\pm$ be the roots of $X^2 - \gamma X + 45$: for $\gamma = -15$, $r_\pm = (-15 \pm 3\sqrt{5})/2$; for $\gamma = 15$, $r_\pm = (15 \pm 3\sqrt{5})/2$. Then, with $X = n/m$,

$$f_1 = -m^2(X - 3\sqrt{5})(X + 3\sqrt{5}), \qquad f_2 = m^2(2X - \gamma), \qquad f_3 = m^2(X - r_+)(X - r_-).$$

Lemma 4.6. *Let (m,n) satisfy (4.3) with $m \neq 0$, and let $r \in \{r_+, r_-\}$. Then there is $\delta \in K(S,2)$ such that $X = n/m$ is the first coordinate of a point of the curve*

$$\Gamma_\delta:\ \delta W^2 = (2X - \gamma)(X - 3\sqrt{5})(X - r)$$

over K. The class δ is that of $\lambda(n - 3\sqrt{5}m)(n - rm)$, it lies in $\tau\langle -1, 2, 3\rangle$, and at the primes above 2, 3, 5 and at the two real places it lies in the image of the local points of $Z^{(\lambda)}$ under $(m,n) \mapsto \lambda(n - 3\sqrt{5}m)(n - rm)$.

Proof. For coprime m, n, a common prime factor of $n - 3\sqrt{5}m$ and its conjugate divides $6\sqrt{5}m$ and $2n$, so lies in S. Let $\mathfrak{p} \notin S$ lie above ℓ. If ℓ is inert, $\mathfrak{p}$ cannot divide $n - 3\sqrt{5}m$ (it would divide the conjugate too). If ℓ splits, then $v_\mathfrak{p}(n - 3\sqrt{5}m) \in \{0, v_\ell(f_1)\}$, and $v_\ell(f_1) = v_\ell(\mu u^2)$ is even because ℓ does not divide $\mu = \pm 3^\alpha 5^\beta$. The same holds for $n - r_\pm m$ and f_3. Hence the classes of $n - 3\sqrt{5}m$ and $n - rm$ lie in $K(S,2)$. As $f_2 = m(2n - \gamma m) = \mu h^2 \in \lambda\mathbb{Q}^{\times 2}$, the product $m(2n - \gamma m)(n - 3\sqrt{5}m)(n - rm) = m^4(2X - \gamma)(X - 3\sqrt{5})(X - r)$ lies in the

class δ of $\lambda(n-3\sqrt{5}m)(n-rm)$, which gives the point. The norm of $\lambda(n-3\sqrt{5}m)(n-rm)$ is $\lambda^2\,(n^2-45m^2)\,f_3(m,n) = -\lambda^2 f_1 f_3 = -(\lambda\mu us)^2$, and the elements of $K(S,2)$ of norm in $-\mathbb{Q}^{\times 2}$ are those of $\tau\langle -1,2,3\rangle$. □

With $c = 2\delta$, $x = cX$ and $y = c^2W/2$, the curve Γ_δ becomes the elliptic curve $y^2 = (x-ce_1)(x-ce_2)(x-ce_3)$ with $e_1 = \gamma/2$, $e_2 = 3\sqrt{5}$, $e_3 = r$, all of whose 2-torsion is K-rational. We denote this model by Γ_δ too. Let σ_1, σ_2 be the real places of K, with $\sigma_1(\sqrt{5}) > 0$ and $\sigma_2(\sqrt{5}) < 0$. By Lemma 4.4 and its proof, the real points of $Z^{(\lambda)}$ have X in the intervals

$$[r_+, 3\sqrt{5}] \ \ (\gamma = -15,\ \lambda = 1), \qquad [r_-, -15/2] \ \ (\gamma = -15,\ \lambda = -5),$$

where $\sqrt{5} > 0$ (for $\lambda = 1$: $f_1 \geq 0$, $f_2 \geq 0$, $f_3 \geq 0$; and similarly for $\lambda = -5$). At a real point with $m \neq 0$ the sign of $\sigma_j(\delta)$ is that of $\lambda\,(X - \sigma_j(3\sqrt{5}))(X - \sigma_j(r))$. With the choices of r made below, this expression has constant sign on the interval at each σ_j, because its zeros in the interval are irrational endpoints, so the sign of δ at both real places is fixed. In the two cases used below it is negative at σ_1 and positive at σ_2. For instance, for $\gamma = -15$, $\lambda = 1$, $r = r_-$ and $X \in [r_+, 3\sqrt{5}]$, at σ_1 the factors are $X - 3\sqrt{5} \leq 0$ and $X - r_- > 0$, and at σ_2 they are $X + 3\sqrt{5} > 0$ and $X - r_+ \geq 0$.

Table 2 lists, in the two cases used below, the classes $\delta \in \tau\langle -1,2,3\rangle$ that satisfy the condition at 2 of Lemma 4.6, and those that also satisfy the conditions at 3, 5 and the real places.

used in	γ	λ	r	after 2	after 3, 5 and ∞
Proposition 4.7(i)	-15	-5	r_+	3τ, $-\tau$	$-\tau$
Proposition 4.7(ii)	-15	1	r_-	6τ, -2τ	-2τ

TABLE 2. The classes δ of Lemma 4.6 left by the local conditions ($\tau = (1+\sqrt{5})/2$; the eight candidates are $\pm\tau, \pm 2\tau, \pm 3\tau, \pm 6\tau$).

Proposition 4.7. *For $D = 3$ the case $k = 0$ contains only the solutions $(-1, \pm 1, 0)$ and $(11, \pm 29, \pm 538)$.*

Proof. By Lemma 4.2 we may assume $b \neq 0$. Then $\gamma = -15$ and $\lambda \in \{1, -5\}$ (Lemma 4.4). If $m = 0$ then $f_2 = 0$ and $h = 0$, so let $m \neq 0$.

(i) $\lambda = -5$. Take $r = r_+ = (-15 + 3\sqrt{5})/2$. The local conditions leave only $\delta = -\tau$ (Table 2), and $\Gamma^{(-5)} := \Gamma_{-\tau}$ is

$$\Gamma^{(-5)}: \ y^2 = x^3 + \tfrac{15-21\sqrt{5}}{2}x^2 - (90 + 180\sqrt{5})x + 4050 + 1350\sqrt{5}.$$

A 2-descent over K gives $\dim \mathrm{Sel}^2(\Gamma^{(-5)}/K) = 2$, so $\operatorname{rank}\Gamma^{(-5)}(K) = 0$. Here the 2-torsion is K-rational and the local images have dimensions 4, 2 and 2 at the primes above 2, 3 and 5, and 1 at each real place. The same holds for $\Gamma^{(1)}$ in (ii). The numbers $\#\Gamma^{(-5)}(\mathbb{F}_\mathfrak{q})$ at the primes of good reduction of norm at most 400 have greatest common divisor 4, so $\Gamma^{(-5)}(K) = \Gamma^{(-5)}[2]$, whose points have $X \in \{\infty, -15/2, 3\sqrt{5}, r_+\}$. The rational values are $X = \infty$, excluded, and $X = -15/2$, where $f_2 = 0$. So there is no solution with $b \neq 0$.

(ii) $\lambda = 1$. Take $r = r_- = (-15 - 3\sqrt{5})/2$. The local conditions leave only $\delta = -2\tau$ (Table 2), and $\Gamma^{(1)} := \Gamma_{-2\tau}$ is

$$\Gamma^{(1)}: \ y^2 = x^3 - (15 + 27\sqrt{5})x^2 - (540 + 540\sqrt{5})x + 75600 + 32400\sqrt{5}.$$

A 2-descent gives $\dim \mathrm{Sel}^2(\Gamma^{(1)}/K) = 3$, so $\operatorname{rank}\Gamma^{(1)}(K) \le 1$, and $\Gamma^{(1)}(K)_{\mathrm{tors}} = \Gamma^{(1)}[2]$ as in (i). The point

$$P_3 = (6 + 6\sqrt{5},\ 144 + 72\sqrt{5}) \qquad (X = -3)$$

has infinite order, so $\Gamma^{(1)}(K)$ has rank 1. Let $G' = \langle P_3\rangle + \Gamma^{(1)}[2]$. By Lemma 2.2, $[\Gamma^{(1)}(K) : G']$ is prime to $2 \cdot 3 \cdot 5 \cdot 11$: for $\ell = 2$ the Kummer images of P_3, $T_1 = (ce_1, 0)$ and $T_2 = (ce_2, 0)$ are independent at primes above 7 and 11, and for $\ell = 3, 5, 11$, P_3 is not an ℓ-th multiple modulo a prime above 11, 31, 7, respectively, where the ℓ-part is cyclic.

Sieve. Let $P \in \Gamma^{(1)}(K)$ come from a pair (m, n). At $q = 11, 31, 61, 71, 89$ the groups $\prod_{\mathfrak{q}|q} \Gamma^{(1)}(\mathbb{F}_{\mathfrak{q}})$ have exponents 12, 20, 96, 360, 120, with least common multiple 1440, which is prime to $[\Gamma^{(1)}(K) : G']$. Imposing, as above, that the reductions of $X(P)$ agree and that $f_i(m, n)/\lambda$ are squares modulo q leaves only the classes aP_3 with $a \equiv \pm 1 \pmod{1440}$. Since 12 kills both groups above 11, P has the same reduction as P_3 or as $-P_3$ at both primes above 11.

Chabauty. Apply Lemma 2.3 (the version with G^0, as $11 \nmid 12$) with $d = 2$, $r = 1$, $p = 11$ (split in K, good reduction), $N = 12$, $g_1 = P_3$, $\rho = X = x/c$ (here $c = 2\delta = -2 - 2\sqrt{5}$ has norm -16, a unit at 11) and $P_0 = \pm P_3$, case (i): the coordinates of P_3 lie in $\mathbb{Z}[\sqrt{5}]$, so no conjugate of $\pm P_3$ reduces to the origin at the primes above 11. The 1×1 matrices $\mathcal{J}/11$ are 8 and 3 modulo 11 for $P_0 = P_3$ and $-P_3$, with $\sigma_1(\sqrt{5}) \equiv 4 \pmod{11}$. So $P = \pm P_3$ and $X = -3$.

Finally $X = -3$ gives $(m : n) = (1 : -3)$ and $(f_1 : f_2 : f_3) = (36 : 9 : 9)$, so $(u^2 : h^2 : s^2) = (4 : 1 : 1)$, $|b| = |uh| = 2$ and $a = s^2 = 1$. Then $y^2 = F_{3,0}(1, \pm 2) = 841 = 29^2$, $z = G_{3,0}(1, \pm 2) = \pm 538$ and $x = -(a^2 - 3b^2) = 11$. □

5. The cases $k \neq 0$

By Lemmas 3.2 and 3.3, it remains to treat the cases $(D, k) = (2, 1), (2, 2), (3, 1), (3, 2)$. A two-cover descent over a quintic field excludes the last three (Proposition 5.3). In the case $(2, 1)$ it leaves one class, which we treat by elliptic Chabauty over the quintic field (Proposition 5.5).

5.1. **A descent for binary quintic forms.**

Lemma 5.1. *Let $F \in \mathbb{Z}[a, b]$ be a binary quintic form, irreducible over $\mathbb{Q}$, with $c = F(1, 0) \neq 0$, and let $\Phi(X) = c^4 F(X/c, 1) \in \mathbb{Z}[X]$, which is monic. Let $K = \mathbb{Q}(\vartheta)$ with $\Phi(\vartheta) = 0$ and let S be the set of primes of K dividing $2c \operatorname{disc}(\Phi)$. If a, b are coprime integers with $F(a, b) = y^2 \neq 0$, then $\alpha = ca - \vartheta b \in \mathcal{O}_K$ satisfies $\mathrm{Nm}(\alpha) = c^4 y^2$ and $v_{\mathfrak{p}}(\alpha)$ is even for every prime $\mathfrak{p} \notin S$. If moreover $\mathrm{Cl}(K) = 1$, then $\alpha \in \delta K^{\times 2}$ for some $\delta \in K(S, 2)$ with $\mathrm{Nm}(\delta) \in \mathbb{Q}^{\times 2}$.*

Proof. $\mathrm{Nm}(ca - \vartheta b) = \widetilde{\Phi}(ca, b) = c^4 F(a, b)$, where $\widetilde{\Phi}$ is the homogenization of Φ. Let $\mathfrak{p} \notin S$ divide α and let p be the prime below $\mathfrak{p}$. If $p \mid b$ then $p \mid ca$, so $p \mid a$ (as $p \nmid c$), which is impossible. So $\vartheta \equiv ca/b \pmod{\mathfrak{p}}$, $\mathfrak{p}$ has degree 1, and $ca/b \bmod p$ is a root of $\Phi \bmod p$. As $p \nmid \operatorname{disc}(\Phi)$, $\Phi \bmod p$ is separable and p does not divide the index of $\mathbb{Z}[\vartheta]$, so by Dedekind's criterion the primes above p correspond bijectively to the irreducible factors of $\Phi \bmod p$. A second prime above p dividing α would correspond to the same factor $X - ca/b$. So $\mathfrak{p}$ is the only prime above p dividing α, and $v_{\mathfrak{p}}(\alpha) = v_p(\mathrm{Nm}\,\alpha) = 2v_p(y)$. If $\mathrm{Cl}(K) = 1$, write the ideal (α) as $\mathfrak{a}^2\mathfrak{b}$ with $\mathfrak{b}$ supported on S. Then $\mathfrak{a} = (\gamma)$ for some $\gamma \in K$, and $\delta = \alpha/\gamma^2$ is an S-unit, with $\mathrm{Nm}(\delta) = c^4 y^2 / \mathrm{Nm}(\gamma)^2$. □

We use two quintic fields,

$$K_2 = \mathbb{Q}(\nu), \quad \nu^5 + 5\nu^3 + 5\nu - 2 = 0, \quad d_{K_2} = 2^6 \cdot 5^5;$$
$$K_3 = \mathbb{Q}(u), \quad u^5 - 5u^3 + 5u - 4 = 0, \quad d_{K_3} = 2^4 \cdot 3^2 \cdot 5^5.$$

Both have signature $(1,2)$ and class number 1 (Appendix A). In both, the polynomial discriminant equals d_K, so $\mathcal{O}_{K_2} = \mathbb{Z}[\nu]$ and $\mathcal{O}_{K_3} = \mathbb{Z}[u]$. For $(D,k) = (2,1), (2,2)$ the field of Lemma 5.1 is isomorphic to K_2, and for $(3,1), (3,2)$ to K_3.

Lemma 5.2. *Let F, c, ϑ and K be as in Lemma 5.1, let p be a prime, and let $\mathfrak{p}_0$ be a prime of K above p with ramification index and residue degree 1, so that $K_{\mathfrak{p}_0} = \mathbb{Q}_p$. Let U be a set of pairs $(a,b) \in \mathbb{Z}_p^2$ with $F(a,b) \neq 0$ on which, for every prime $\mathfrak{p} \neq \mathfrak{p}_0$ above p, the class of $\alpha = ca - \vartheta b$ in $K_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^{\times 2}$ is constant. Put $\alpha' = \prod_{\mathfrak{p}\mid p,\ \mathfrak{p}\neq\mathfrak{p}_0} \mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha)$. Then the class of α' in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ is constant on U, and for $(a,b) \in U$, $F(a,b)$ is a square in $\mathbb{Q}_p$ if and only if α and α' have the same class in $K_{\mathfrak{p}_0}^\times / K_{\mathfrak{p}_0}^{\times 2} = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.*

Proof. We have $c^4 F(a,b) = \mathrm{Nm}(\alpha) = \alpha \cdot \alpha'$, with α taken in $K_{\mathfrak{p}_0} = \mathbb{Q}_p$, and c^4 is a square. The local norms map squares to squares, so the class of α' depends only on the classes of α at the primes $\mathfrak{p} \neq \mathfrak{p}_0$. □

Proposition 5.3. *Let $(D,k) \in \{(2,2),(3,1),(3,2)\}$. There are no coprime integers a,b such that $F_{D,k}(a,b)$ is a square and (a,b) satisfies the conditions of Lemma 3.3(b). Hence the cases $k = 2,3$ of $\mathcal{E}_2$ and $k = 1,2,3,4$ of $\mathcal{E}_3$ contain no primitive solution.*

Proof. Apply Lemma 5.1 with $c = 3, 2, 7$ respectively. Here $F_{D,k}(a,b) \neq 0$ since $F_{D,k}$ is irreducible. The monic polynomials are

$$\Phi_{2,2} = X^5 + 20X^4 + 180X^3 + 720X^2 + 1620X + 1296,$$
$$\Phi_{3,1} = X^5 + 15X^4 + 120X^3 + 360X^2 + 720X + 432,$$
$$\Phi_{3,2} = X^5 + 60X^4 + 1470X^3 + 17640X^2 + 108045X + 259308,$$

and S consists of the primes above $2,3,5$ for $(2,2)$ and $(3,1)$ and above $2,3,5,7$ for $(3,2)$, with $\#S = 5, 5, 7$. For each, $3 + \#S$ explicit S-units are independent modulo squares by quadratic characters at auxiliary primes, so they form a basis of $K(S,2)$, of dimension 8, 8, 10. The class δ of Lemma 5.1 must satisfy: (1) $\mathrm{Nm}(\delta) \in \mathbb{Q}^{\times 2}$; (2) $\delta > 0$ at the real place, because $\mathrm{Nm}(\alpha) = c^4 y^2 > 0$ and the two complex places contribute positive factors; (3) for every prime p below S, the image of δ in $\prod_{\mathfrak{p}\mid p} K_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^{\times 2}$ lies in the local image

$$I_p = \{\text{class of } ca - \vartheta b : \ (a,b) \in \mathbb{Z}_p^2 \text{ primitive, satisfying Lemma 3.3(b), } \ F(a,b) \in \mathbb{Q}_p^{\times 2}\},$$

where Lemma 3.3(b) is imposed only through its conditions at p. We compute a set containing I_p as in Section 2.1: residue classes (a_0, b_0) modulo p^n are refined until the class of $F(a,b)$ in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ (constant once $n \geq v_p(F(a_0,b_0)) + 3$ for $p = 2$, $+1$ for odd p) and the classes of α at the primes $\mathfrak{p} \mid p$ (constant once $ne_{\mathfrak{p}} \geq v_{\mathfrak{p}}(\alpha_0) + 2v_{\mathfrak{p}}(2) + 1$) are constant. Near a root of F in $\mathbb{P}^1(\mathbb{Q}_p)$ the class of $F(a,b)$ is not constant on any residue class containing the root, and the root corresponds to a prime $\mathfrak{p}_0 \mid p$ of degree 1, at which the class of α is not constant either. On such a residue class, if the classes of α at the other primes above p are constant, Lemma 5.2 shows that the condition $F(a,b) \in \mathbb{Q}_p^{\times 2}$ holds exactly when the class of α at $\mathfrak{p}_0$ is that of α', and only this class at $\mathfrak{p}_0$ is recorded. The computed sets equal the local images: for every class in them, a search over pairs of coprime integers (a,b) satisfying the conditions at p found one with $F(a,b)$ a nonzero square in $\mathbb{Q}_p$ and $ca - \vartheta b$ in that class.

With the conditions of Lemma 3.3(b), the images have sizes $4, 2, 1$ (at $2, 3, 5$) for $(2, 2)$; $4, 1, 1$ for $(3, 1)$; and $4, 1, 1, 2$ (at $2, 3, 5, 7$) for $(3, 2)$. No δ satisfies (1)–(3): Table 3 gives the number of classes δ left after conditions (1) and (2) and after the condition at each prime. The classes left by the condition at 2 are, with ϑ the root of $\Phi_{D,k}$,

$$(2,2)\colon 1;\ (3,1)\colon \tfrac{1}{144}(31\vartheta^4+753\vartheta^3+7068\vartheta^2+31716\vartheta+23184);$$
$$(3,2)\colon 1,\ \tfrac{1}{1764}(-5\vartheta^4-258\vartheta^3-4389\vartheta^2-32634\vartheta-86436),\ \tfrac{1}{1764}(4\vartheta^4+219\vartheta^3+4620\vartheta^2+43659\vartheta+172872).$$

For $(3, 2)$ the class 1 survives the conditions at 3 and 5 and is excluded at 7. So no (a, b) exists. The cases $k = 3$ of $\mathcal{E}_2$ and $k = 3, 4$ of $\mathcal{E}_3$ follow by Lemma 3.3(a). □

(D, k)	$\dim K(S, 2)$	(1), (2)	after 2	after 3	after 5	after 7
$(2, 2)$	8	16	1	0	0	–
$(3, 1)$	8	16	1	0	0	–
$(3, 2)$	10	32	3	1	1	0
$(2, 1)$	6	8	1	–	1	–

TABLE 3. The number of classes $\delta \in K(S, 2)$ left by the conditions of Proposition 5.3: (1) and (2) together, then the local conditions at 2, 3, 5 and 7 in turn. The last row is the descent in the proof of Proposition 5.5; there S lies above 2 and 5 only.

Remark 5.4. Without the conditions of Lemma 3.3(b) the same computation leaves 1, 2 and 2 classes δ for $(2, 2)$, $(3, 1)$ and $(3, 2)$. The class for $(2, 2)$ is that of the pair $(a, b) = (0, 1)$, the two classes for $(3, 1)$ are those of $(3, -1)$ and $(29, -21)$, and one of the two classes for $(3, 2)$ is that of $(1, -1)$. These pairs are coprime but violate Lemma 3.3(b), and they give the non-primitive solutions $(2, 4, \pm 12)$ of $\mathcal{E}_2$ and $(-6, 18, \pm 180)$, $(482, 12646, \pm 92377564)$, $(2, 2, \pm 4)$ of $\mathcal{E}_3$. No coprime pair with $|a|, |b| \le 3000$ lies in the second class for $(3, 2)$. With the conditions of Lemma 3.3(b), the images at 2 and 3 already leave no class for $(2, 2)$ and $(3, 1)$, and for $(3, 2)$ it takes the images at 2, 3 and 7.

5.2. **The case $(D, k) = (2, 1)$.** Here $F_{2,1}(a, b)$ has leading coefficient $c = 1$ and $f(X) = F_{2,1}(X, 1) = X^5 + 10X^4 + 20X^3 + 40X^2 + 20X + 8$. In K_2 its root is

$$\vartheta = -\nu^4 - \nu^3 - 5\nu^2 - 4\nu - 6,$$

and S is the set of the three primes of K_2 above 2 and 5.

Proposition 5.5. *For $D = 2$ the case $k = 1$ contains only the solutions $(1, \pm 1, 1)$, and the case $k = 4$ only $(1, \pm 1, -1)$.*

Proof. The descent. As in Proposition 5.3, $K_2(S, 2)$ has dimension 6, and the conditions (1)–(3) leave only $\delta = 1$ (local images of sizes 4 at 2 and 1 at 5 with the conditions of Lemma 3.3(b), and again only $\delta = 1$ without them, when the set computed at 2 has 6 classes). So $a - \vartheta b = \gamma^2$ with $\gamma \in K_2$, and with $q_1(X) = f(X)/(X - \vartheta)$,

$$q_1(X) = X^4 + (4 - 4\nu - 5\nu^2 - \nu^3 - \nu^4)X^3 + (12 - 20\nu - 6\nu^3)X^2 + (8 - 16\nu + 2\nu^2 - 6\nu^3 + 2\nu^4)X + (4 - 8\nu - 4\nu^3),$$

we get $q_1(a/b) = \big(y/(b^2\gamma)\big)^2$ if $b \neq 0$. So $X = a/b$ is the first coordinate of a point of the curve $C_{2,1}\colon w^2 = q_1(X)$ over K_2, and $b = 0$ corresponds to a point at infinity of $C_{2,1}$.

The elliptic curve. Apply Lemma 2.1 to q_1, with coefficients b_1, c_1, d_1, e_1 and $\kappa_{q_1} = c_1 - b_1^2/4$. The cubic of the resulting model has exactly one root $U_0 = 8\nu^3 - 16$ in K_2, and $U = 16x + U_0$, $V = 64y$ give

$$E_{2,1}: \ y^2 = x^3 - 5\nu\, x^2 + 5\nu^2\, x,$$

the quadratic twist by ν of $y^2 = x^3 - 5x^2 + 5x$, which has conductor 200. On $E_{2,1}$,

$$X = \frac{64y - 16b_1 x - b_1 U_0 - 8d_1}{4\,(16x + U_0 + 4\kappa_{q_1})}. \tag{5.1}$$

The point of $C_{2,1}$ at infinity with $w/X^2 \to 1$ goes to O, and the other goes to

$$P_1 = (\,-\tfrac{5}{8}\nu^4 - \tfrac{25}{8}\nu^2 + \tfrac{5}{4}\nu,\ \tfrac{35}{32}\nu^4 - \tfrac{5}{32}\nu^3 + \tfrac{195}{32}\nu^2 - \tfrac{5}{8}).$$

The involution $w \mapsto -w$ of $C_{2,1}$ is $P \mapsto P_1 - P$ on $E_{2,1}$, so $X(P_1 - P) = X(P)$. At the one point $-P_1$ where (5.1) reads $0/0$ we evaluate it at $P_1 - P$ instead.

The Mordell–Weil group. A descent via the 2-isogeny with kernel $\langle T\rangle$, $T = (0,0)$, gives Selmer groups of dimension 2 for $E_{2,1}$ and for the isogenous curve (for the two curves, the local images have dimensions 2 and 1 at the prime above 2 with $(e,f) = (1,1)$, 3 and 3 at the prime above 2 with $(e,f) = (2,2)$, 1 and 1 at the prime above 5, and 0 and 1 at the real place, as the local dimension formula of Section 2.4 requires). As $E_{2,1}(K_2)[2] = \langle T\rangle$, this gives $\operatorname{rank} E_{2,1}(K_2) \le 2$. With

$$R = (2\nu^4 + 3\nu^3 + 4\nu^2 + 4\nu,\ 3\nu^4 + 21\nu^3 + 7\nu^2 + 24\nu - 12),$$

the points P_1, R, T are independent in $E_{2,1}(K_2)/2E_{2,1}(K_2)$ (their Kummer images at primes above 3 and 11 with split 2-torsion have rank 3). So $\operatorname{rank} E_{2,1}(K_2) = 2$. The numbers $\#E_{2,1}(\mathbb{F}_\mathfrak{q})$ at the degree-one primes of norm at most 200 (odd, of good reduction) have greatest common divisor 2, so $E_{2,1}(K_2)_{\mathrm{tors}} = \langle T\rangle$. By Lemma 2.2, $G' = \langle P_1, R\rangle + \langle T\rangle$ has index prime to 2, 3 and 751 in $E_{2,1}(K_2)$: for $\ell = 3$ we use primes above 3 and 7, and for $\ell = 751$ the primes of degree 5 above 1669 and 7561, where the 751-parts are cyclic.

The sieve at 751. The prime 751 splits completely in K_2, and it is the first such prime at which the five groups $E_{2,1}(\mathbb{F}_\mathfrak{q})$ have one and the same exponent (the smaller primes that split completely are 179, 229, 379, 389 and 601). At each of the five primes above 751, $E_{2,1}$ and $C_{2,1}$ have good reduction (the discriminants of $E_{2,1}$ and q_1 are supported above 2 and 5), the constants b_1, d_1, U_0, κ_{q_1} are integral, and 64 is a unit, so X reduces well. The five groups $E_{2,1}(\mathbb{F}_\mathfrak{q})$ are all isomorphic to $\mathbb{Z}/384 \times \mathbb{Z}/2$. The sieve and the Chabauty step below use the same modulus $N = 384$, and since $384 = 2^7 \cdot 3$, it suffices that the index of G' is prime to 2, 3 and 751. By Section 2.5 with $N = M = 384$, a point P with $X(P) \in \mathbb{P}^1(\mathbb{Q})$ reduces like $a_1P_1 + a_2R + a_3T$ for one of the $2 \cdot 384^2$ classes (a_1, a_2, a_3). Exactly 16 classes give values of X in $\mathbb{P}^1(\mathbb{F}_{751})$ that agree at the five primes, and each of them reduces to O at all five primes (eight classes) or to P_1 at all five primes (eight classes). So $P - O$ or $P - P_1$ lies in the subgroup G^0 of points reducing to the origin at all five primes above 751.

Chabauty at 751. Apply Lemma 2.3 (the version with G^0; $751 \nmid 384$) with $d = 5$, $r = 2$, $p = 751$, $N = 384$, $g_1 = P_1$, $g_2 = R$ and $\rho = 1/X$. At $P_0 = O$ (case (ii)), in the formal parameter the numerator and denominator of (5.1) are $-64t^{-3}(1 + O(t))$ and $64t^{-2}(1 + O(t))$ with 751-integral coefficients, so $\rho = -t(1 + O(t)) \in \mathbb{Z}_{751}[[t]]$ and $c_j = -1$. At $P_0 = P_1$ (case (i)) the numerator of (5.1) is a 751-adic unit at every embedding. The matrices $\mathcal{J}/751$

modulo 751 are

$$\begin{pmatrix} 8 & 238 \\ 651 & 608 \\ 16 & 366 \\ 505 & 165 \end{pmatrix} \ (P_0 = O), \qquad \begin{pmatrix} 743 & 513 \\ 100 & 143 \\ 735 & 385 \\ 246 & 586 \end{pmatrix} \ (P_0 = P_1),$$

both of rank 2. So $P \in \{O, P_1\}$, and $X(P) = \infty$, that is $b = 0$. Then $a = \pm 1$ and $a = a - \vartheta b$ is a square in K_2, so $a = 1$ (as $-1 < 0$ at the real place). So $y^2 + z\sqrt{2} = 1 + \sqrt{2}$, which gives $y = \pm 1$, $z = 1$ and $x = -\operatorname{Nm}(1 + \sqrt{2}) = 1$. The case $k = 4$ follows by Lemma 3.3(a). □

5.3. **Proof of Theorem 1.1(a)–(c).** Let (x, y, z) be a primitive solution of $\mathcal{E}_D$ with $D \in \{2, 3, -3\}$. If $z = 0$, then $(x, y, z) = (-1, \pm 1, 0)$ by Lemma 3.1(b). Otherwise Lemma 3.2 puts the solution in a case (D, k) with $0 \le k \le 4$, and $k = 0$ if $D = -3$. By Lemma 3.3(a), the cases $k = 3$ and $k = 4$ are the images of the cases $k = 2$ and $k = 1$ under $z \mapsto -z$. By Propositions 4.1, 4.5 and 4.7, the case $k = 0$ contains no solution with $z \ne 0$ for $D = 2$ and $D = -3$, and only $(11, \pm 29, \pm 538)$ for $D = 3$. The cases $(2, 2)$, $(3, 1)$, $(3, 2)$ and their images under $z \mapsto -z$ contain no solution (Proposition 5.3), and the cases $(2, 1)$ and $(2, 4)$ contain only $(1, \pm 1, 1)$ and $(1, \pm 1, -1)$ (Proposition 5.5). This gives the lists of Theorem 1.1(a)–(c).

6. The equation $2x^4 - y^4 + z^3 = 0$

We prove Theorem 1.1(d), taking from Proposition 8.1 the points of one curve of genus one over a cubic field.

Let (x, y, z) be a primitive solution, so that $y^4 - 2x^4 = z^3$. Then $\gcd(x, y) = 1$, since a common prime factor would divide z. If y were even, x would be odd and $z^3 \equiv -2 \pmod{16}$, which is impossible. So y and z are odd.

Let $K = \mathbb{Q}(\sqrt{2})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ (class number 1) and $\varepsilon = 1 + \sqrt{2}$. A prime dividing $y^2 - x^2\sqrt{2}$ and $y^2 + x^2\sqrt{2}$ divides $2y^2$ and $2\sqrt{2}x^2$, hence $\sqrt{2}$, but the norm z^3 is odd. Since -1 is a cube,

$$y^2 - x^2\sqrt{2} = \varepsilon^k (a + b\sqrt{2})^3, \qquad k \in \{0, 1, 2\}, \tag{6.1}$$

with coprime integers a, b (a common prime factor would divide y^2 and x^2). Writing the right side as $F_k(a, b) + G_k(a, b)\sqrt{2}$, we have $y^2 = F_k(a, b)$, $-x^2 = G_k(a, b)$ and $z = (-1)^k(a^2 - 2b^2)$, where

$$\begin{aligned} F_0 &= a(a^2 + 6b^2), & G_0 &= b(3a^2 + 2b^2), \\ F_1 &= a^3 + 6a^2b + 6ab^2 + 4b^3, & G_1 &= a^3 + 3a^2b + 6ab^2 + 2b^3, \\ F_2 &= 3a^3 + 12a^2b + 18ab^2 + 8b^3, & G_2 &= 2a^3 + 9a^2b + 12ab^2 + 6b^3. \end{aligned}$$

Since $\sqrt{2}(a + b\sqrt{2}) = 2b + a\sqrt{2}$, we have $F_k(2b, a) = 4G_k(a, b)$ and $G_k(2b, a) = 2F_k(a, b)$.

Proposition 6.1. *The case $k = 0$ gives only the solutions $(0, \pm 1, 1)$.*

Proof. From $y^2 = a(a^2 + 6b^2)$ with y odd: $a > 0$, a is odd, and $\gcd(a, a^2 + 6b^2)$ divides 3. Suppose $x \ne 0$. Then $b < 0$ and $x^2 = (-b)(3a^2 + 2b^2)$ with $\gcd(b, 3a^2 + 2b^2) \mid 3$. If $3 \nmid b$, then $3a^2 + 2b^2$ is a square n^2, and $2b^2 \equiv n^2 \pmod 3$ is impossible. So $3 \mid b$, $3 \nmid a$, and $a = s^2$. Since $v_3(3a^2 + 2b^2) = 1$, we get $-b = 3m^2$ and $3a^2 + 2b^2 = 3n^2$ with $m \ne 0$, that is, $n^2 = s^4 + 6m^4$. The map $(s, n) \mapsto (X, Y) = (2(n + s^2), 4s(n + s^2))$ (in the affine chart $m = 1$) sends the curve $n^2 = s^4 + 6m^4$ to $E : Y^2 = X^3 - 24X$, and no affine point goes to O or to $(0, 0)$ ($X = 0$ would force $6 = 0$). A descent via 2-isogeny gives the Selmer groups $\{1, -6\}$ for

E and $\{1,6\}$ for $Y^2 = X^3 + 96X$, so $\operatorname{rank} E(\mathbb{Q}) = 0$, and $E(\mathbb{Q}) = \{O, (0,0)\}$ ($\#E(\mathbb{F}_5) = 4$, and a point P with $2P = (0,0)$ would have $x(P)^2 = -24$). So the quartic has only its two points with $m = 0$, a contradiction. Hence $x = 0$, $b = 0$, $a = 1$, and $(x, y, z) = (0, \pm 1, 1)$. □

Proposition 6.2. *The case $k = 1$ gives no solution.*

Proof. If $b = 0$ then $a = \pm 1$ and $y^2 = \pm 1$, $-x^2 = \pm 1$ with the same sign, which is impossible. If $a = 0$ then $y^2 = F_1(0, \pm 1) = \pm 4$, against y odd. So $t = a/b \in \mathbb{Q}^\times$, and $(t, xy/b^3)$ is a point of the curve of genus 2

$$C' : \ w^2 = f_1(t) \coloneqq -F_1(t,1)G_1(t,1).$$

The symmetry above gives $t^6 f_1(2/t) = 8 f_1(t)$, and indeed $f_1(t) = t^3 h_1(T)$ with $T = t + 2/t$ and $h_1(T) = -T^3 - 9T^2 - 24T - 24$. The map $(t, w) \mapsto (T, Y) = \big(t + 2/t,\ w(t + \sqrt{2})/t^2\big)$ sends C' to the curve

$$Q' : \ Y^2 = (T + 2\sqrt{2})\, h_1(T)$$

over K, since $(t + \sqrt{2})^2/t = T + 2\sqrt{2}$, and it sends our point to a point with $T \in \mathbb{Q}$. The curve Q' has the K-point $(-2\sqrt{2}, 0)$, so it is isomorphic to its Jacobian, which is

$$E' : \ y^2 = x^3 + 8 - 6\sqrt{2}$$

(its invariants are $I = 0$ and $-27J = 6^6(8 - 6\sqrt{2})$). The cubic extension of K generated by a point of order 2 of E' (the algebra $K[x]/(x^3 + 8 - 6\sqrt{2})$ of the 2-descent) is $K(\sqrt[3]{1 + \sqrt{2}}) = \mathbb{Q}[y]/(y^6 - 2y^3 - 1)$, of class number 1 (Appendix A), and a 2-descent over K gives $\mathrm{Sel}^2(E'/K) = 0$. So $E'(K)$ is finite with trivial 2-torsion. As $\#E'(\mathbb{F}_\mathfrak{q}) = 3$ and 7 at the two primes above 7, $E'(K) = \{O\}$. So $Q'(K) = \{(-2\sqrt{2}, 0)\}$ (the leading coefficient -1 of Q' is not a square in the real field K, so there is no point with $T = \infty$), and $T = -2\sqrt{2} \notin \mathbb{Q}$. □

For the case $k = 2$ we descend once more, over the cubic field

$$L = \mathbb{Q}(\omega), \qquad \omega^3 + 3\omega - 2 = 0, \qquad d_L = -216 = -2^3 \cdot 3^3,$$

with $\mathcal{O}_L = \mathbb{Z}[\omega]$, class number 1 (Appendix A) and signature $(1,1)$. The unit $\eta_L = -\omega^2 - \omega + 1$ has norm 1, and neither η_L nor $-\eta_L$ is a square (both are non-residues modulo the prime $(13, \omega + 4)$ of degree 1). So ± 1, $\pm\eta_L$ represent $\mathcal{O}_L^\times/\mathcal{O}_L^{\times 2}$. In L, $3 = \mathfrak{p}_3^3$ and $2 = \mathfrak{p}\mathfrak{p}'^2$. The element $\varrho = (\omega^2 - \omega - 2)/3$ is a root of $F_2(t,1)$, and $-(\omega^2 + 5)/2 = 2/\varrho$ is a root of $G_2(t,1)$.

Proposition 6.3. *The case $k = 2$ gives only the solutions $(\pm 1, \pm 1, -1)$.*

Proof. If $b = 0$ then $y^2 = F_2(\pm 1, 0) = \pm 3$, which is impossible, so $b \neq 0$. Put

$$\beta = 3a - (\omega^2 - \omega - 2)b = 3(a - \varrho b) \in \mathcal{O}_L, \qquad \mathrm{Nm}(\beta) = 9F_2(a,b) = 9y^2.$$

Let β' be another conjugate of β in the Galois closure. From $\beta - \beta' = (3\varrho' - 3\varrho)b$ and $3\varrho'\beta - 3\varrho\beta' = 3(3\varrho' - 3\varrho)a$ with $\gcd(a,b) = 1$, a common prime factor of β and β' divides $3(3\varrho - 3\varrho')$, so lies above 2 or 3 (the minimal polynomial $X^3 + 12X^2 + 54X + 72$ of 3ϱ has discriminant $-2^5 \cdot 3^5$). As in the proof of Lemma 5.1, every prime $\mathfrak{p} \nmid 6$ dividing β (so that $3\varrho \equiv 3a/b \pmod{\mathfrak{p}}$) is the only prime above its p dividing β, has degree 1, and $v_\mathfrak{p}(\beta) = v_p(9y^2)$ is even. The element β is a unit above 2, since $\mathrm{Nm}(\beta)$ is odd, and $v_{\mathfrak{p}_3}(\beta) = v_3(9y^2)$ is even. So (β) is the square of an ideal, $\beta = u\gamma^2$ with $\gamma \in \mathcal{O}_L$ and u a unit, and $\mathrm{Nm}(u) > 0$ gives $u \in \{1, \eta_L\}$ modulo squares.

The case $u = 1$ is impossible 2-adically: the class of β in $\prod_{\mathfrak{p}|2} L_\mathfrak{p}^\times/L_\mathfrak{p}^{\times 2}$ depends only on (a,b) mod 16, and over all $(a,b) \in \mathbb{Z}_2^2$, not both even, with $F_2(a,b) \equiv 1 \pmod 8$ and

$-G_2(a,b)$ a square in $\mathbb{Q}_2$, it is never trivial. (Explicitly, β is a square in $L\otimes\mathbb{Q}_2$ only when $a\equiv 3$ or $11 \pmod{16}$ and $b\equiv 0 \pmod 4$, and then $v_2(G_2(a,b))=1$.)

So $\beta=\eta_L\gamma^2$, and $(t,Y)=(a/b,\ \eta_L\gamma x/b^2)$ is a point of

$$C_L:\ Y^2=Q_L(t)\coloneqq -\eta_L\left(3t-(\omega^2-\omega-2)\right)G_2(t,1)$$

over L with $t\in\mathbb{Q}$. By Proposition 8.1 (case C_1), the only points of $C_L(L)$ with $t\in\mathbb{P}^1(\mathbb{Q})$ have $t=-1$. So $(a,b)=\pm(1,-1)$. As $F_2(-1,1)=-1$ is not a square, $(a,b)=(1,-1)$, and $F_2(1,-1)=1$, $G_2(1,-1)=-1$ give $x^2=y^2=1$ and $z=a^2-2b^2=-1$. □

Proof of Theorem 1.1(d). Every primitive solution lies in a case $k\in\{0,1,2\}$, and Propositions 6.1, 6.2 and 6.3 leave $(0,\pm1,1)$ and $(\pm1,\pm1,-1)$. □

7. The equations $x^4+4y^3+z^3=0$ and $x^4+3y^3+2z^3=0$

Equations (e) and (f) lead to four curves of genus one over pure cubic fields, on which a primitive solution gives a point with a rational coordinate. Section 8 determines these points.

7.1. **The fields.** Let $K_f=\mathbb{Q}(\theta)$ with $\theta=\sqrt[3]{2}$. Then $\mathcal{O}_{K_f}=\mathbb{Z}[\theta]$ (x^3-2 is Eisenstein at 2, and $(x+2)^3-2$ at 3) and $d_{K_f}=-108$. Let $K_e=\mathbb{Q}(\phi)$ with $\phi=\sqrt[3]{12}$ and $\psi=\phi^2/2=\sqrt[3]{18}$. Then $\mathcal{O}_{K_e}=\mathbb{Z}[\phi,\psi]$ with basis $1,\phi,\psi$ and $d_{K_e}=-972$. Both fields have signature $(1,1)$ and class number 1 (Appendix A). The units

$$\eta_f=\theta-1\in K_f,\qquad \eta_e=1+3\phi-3\psi\in K_e$$

have norm 1. For $\eta=\eta_f$ and for $\eta=\eta_e$, neither η nor $-\eta$ is a square: $-\eta<0$ at the real place, and η is a non-residue modulo the prime $(5,\theta-3)$, respectively $(13,\phi-10)$. As the unit groups have rank 1 and torsion $\{\pm1\}$, it follows that η_f^j, $0\le j\le 3$, represent the units of norm 1 of K_f modulo fourth powers, and η_e^j those of K_e. In K_e the prime 2 is totally ramified, $2\mathcal{O}=\mathfrak{p}_2^3$ with $\mathfrak{p}_2=(\pi_2)$, $\pi_2=\psi+\phi+2$ of norm 2.

7.2. **The descent.** *Equation (f).* Replacing (y,z) by $(-y,-z)$, the primitive solutions of $x^4+4y^3+z^3=0$ correspond to those of $z^3+4y^3=x^4$. Then $\gcd(y,z)=1$ (a common prime p gives $p^3\mid x^4$, so $p\mid x$). Also, z is odd (if z is even, y is odd and $x^4\equiv 4 \pmod 8$), so x is odd and $x\neq 0$. Put $\alpha=z+y\theta^2\in\mathcal{O}_{K_f}$, so that $\mathrm{Nm}(\alpha)=z^3+4y^3=x^4$, and $\beta=z^2-zy\theta^2+y^2\theta^4$, so that $\alpha\beta=\mathrm{Nm}(\alpha)$ and $\alpha^2-\beta=3zy\theta^2$. A prime $\mathfrak{q}\nmid 6$ dividing α and β divides yz, hence y and z, which is impossible. So for such $\mathfrak{q}$, $v_\mathfrak{q}(\alpha)$ is 0 or $v_\mathfrak{q}(x^4)$, a multiple of 4. The prime above 2 does not divide α ($\mathrm{Nm}(\alpha)$ is odd), and at the prime above 3 (totally ramified) $v(\alpha)=v_3(x^4)$. So $(\alpha)=(\gamma)^4$ with $\gamma\in\mathcal{O}_{K_f}$, and as the unit α/γ^4 has positive norm,

$$z+y\theta^2=\eta_f^j\gamma^4,\qquad \gamma\in\mathcal{O}_{K_f},\ j\in\{0,1,2,3\}. \tag{7.1}$$

Equation (e). A primitive solution of $x^4+3y^3+2z^3=0$ has $\gcd(y,z)=1$. Moreover $x\equiv y \pmod 2$, and both even would force z even, so x and y are odd, and $3\nmid x$ (else $3\mid z$ and then $3\mid y$). Put $\alpha=2z+y\phi$, with $\mathrm{Nm}(\alpha)=8z^3+12y^3=-4x^4$. Then $v_{\mathfrak{p}_2}(\alpha)=v_2(4x^4)=2$, α is prime to 3, and as before, with $\beta=4z^2-2zy\phi+y^2\phi^2=\mathrm{Nm}(\alpha)/\alpha$ and $\alpha^2-\beta=6zy\phi$, every other prime $\mathfrak{q}$ has $4\mid v_\mathfrak{q}(\alpha)$. So $(\alpha)=\mathfrak{p}_2^2(\gamma)^4$ with $\gamma\in\mathcal{O}_{K_e}$, and as $\mathrm{Nm}(\pi_2^2)=4$, the unit $\alpha/(\pi_2^2\gamma^4)$ has norm -1,

$$2z+y\phi=-\eta_e^j\pi_2^2\gamma^4,\qquad \gamma\in\mathcal{O}_{K_e},\ j\in\{0,1,2,3\}. \tag{7.2}$$

Lemma 7.1. *In* (7.1), $j\in\{0,2\}$; *in* (7.2), $j\in\{1,2\}$.

Proof. In both fields 2 is totally ramified, $K_{\mathfrak{p}} \simeq \mathbb{Q}_2(\sqrt[3]{2})$ with $e = 3$, and $1 + \mathfrak{p}^k$ consists of fourth powers for $k \geq 3e + 1 = 10$: a fourth root of $1 + \xi$ is obtained by taking square roots twice, and $1 + \mathfrak{p}^k$ consists of squares when $k > 2e$, with one of the square roots of an element of $1 + \mathfrak{p}^k$ lying in $1 + \mathfrak{p}^{k-e}$. So $(\mathcal{O}_K/16)^\times/(\text{fourth powers}) = \mathcal{O}_{\mathfrak{p}}^\times/\mathcal{O}_{\mathfrak{p}}^{\times 4}$, a group of order 128. The unit α/η_f^j, respectively $\alpha/(-\eta_e^j\pi_2^2)$, must be a fourth power at $\mathfrak{p}$, and modulo 16 it depends only on (y, z) mod 16. Running over all (y, z) modulo 16 with z odd (equation (f)), respectively y odd (equation (e)), gives the stated classes. □

Conics. Write $j = j_0 + 2j_1$ with $j_0, j_1 \in \{0, 1\}$, let η be η_f for (f) and η_e for (e), and put $\delta = \eta^{j_1}\gamma^2$. Then $\alpha = \varepsilon_0\delta^2$ with $\varepsilon_0 = \eta_f^{j_0}$ for (f) and $\varepsilon_0 = -\eta_e^{j_0}\pi_2^2$ for (e). One computes $-\pi_2^2 = -16 - 7\phi - 6\psi$ and $-\eta_e\pi_2^2 = 2 - \phi$. In (f) the coordinate of α at θ vanishes, and in (e) the coordinate at ψ. In the coordinates of δ this says that a ternary quadratic form over $\mathbb{Z}$ vanishes, so δ lies on a conic. Each conic is smooth and has a rational point, and it is parametrized by an isomorphism $\mathbb{P}^1 \to$ conic, $(m : n) \mapsto \delta(m, n)$, whose coordinates are binary quadratic forms:

case	basis	coordinates of $\delta(m, n)$
(f), $j_0 = 0$	$1, \theta, \theta^2$	$m^2,\ -n^2,\ -mn$
(e), $j_0 = 1$	$1, \phi, \psi$	$-3m^2 + 2n^2,\ -2mn + 2n^2,\ -2m^2 + 2mn$
(e), $j_0 = 0$	$1, \phi, \psi$	$42m^2 - 36mn + 8n^2,\ -21m^2 + 16mn - 3n^2,\ 4m^2 - 2mn$

So $\delta = \lambda\,\delta(m, n)$ with $\lambda \in \mathbb{Q}^\times$ and coprime integers m, n. Let $q(X) = \mathrm{Nm}(\delta(X, 1))/\delta(X, 1) \in K[X]$, a quartic, and $c = \eta^{j_1}$. From $\lambda\delta(m, n) = c\gamma^2$ we get $\lambda^3\,\mathrm{Nm}(\delta(m, n)) = \mathrm{Nm}(\gamma)^2$, and

$$c\,n^4 q(m/n) = c\,\frac{\mathrm{Nm}(\delta(m, n))}{\delta(m, n)} = \Big(\frac{\mathrm{Nm}(\gamma)}{\lambda\gamma}\Big)^2.$$

So $X = m/n \in \mathbb{P}^1(\mathbb{Q})$ is the first coordinate of a K-point of the curve of genus one

$$Y^2 = c\,q(X)$$

($n = 0$ gives the points with $X = \infty$). Conversely, from (m, n) one reads off $\alpha = \lambda^2\varepsilon_0\delta(m, n)^2$ and then (z, y):

$$\begin{aligned}
&\text{(f), } j_0 = 0: && z = \lambda^2(m^4 + 4mn^3), \qquad y = \lambda^2(n^4 - 2m^3n);\\
&\text{(e), } j_0 = 1: && 2z = \lambda^2(-54m^4 + 168m^3n - 216m^2n^2 + 144mn^3 - 40n^4),\\
& && y = \lambda^2(15m^4 - 72m^3n + 108m^2n^2 - 64mn^3 + 12n^4);\\
&\text{(e), } j_0 = 0: && 2z = \lambda^2(-1476m^4 + 2544m^3n - 1656m^2n^2 + 480mn^3 - 52n^4),\\
& && y = \lambda^2(240m^4 - 264m^3n + 72m^2n^2 + 8mn^3 - 4n^4).
\end{aligned}$$

(For (f) these are the coordinates of $\varepsilon_0\delta(m, n)^2 = (m^4 + 4mn^3) + (n^4 - 2m^3n)\theta^2$ at 1 and θ^2; for (e), those at 1 and ϕ.)

7.3. **The curves and the solutions.** The four curves $Y^2 = c\,q(X)$ that arise, for the unit classes of Lemma 7.1, are the curves $C_2, \ldots, C_5$ of Section 8. The curve C_1 there is the curve C_L of Section 6. Proposition 8.1 determines their points with $X \in \mathbb{P}^1(\mathbb{Q})$, and the table gives the solutions.

equation	j	curve	$X \in \mathbb{P}^1(\mathbb{Q})$	solutions
(f)	0	C_4	$\infty, 0, 2$	$X=\infty$: $(z,y)=(1,0)$, the solutions $(\pm1,0,-1)$; $X=0$: $(z,y)=(0,1)$, and $z^3+4y^3=4$ is not a fourth power; $X=2$: $(z,y)=(24,-15)\lambda^2$, not coprime for any λ
(f)	2	C_5	-1	$(z,y)=(-3,3)\lambda^2$, not coprime for any λ
(e)	1	C_2	1	$(z,y)=(1,-1)$, the solutions $(\pm1,-1,1)$
(e)	2	C_3	$1/2,\ 1/3$	$X=1/2$: $(z,y)=(-2,0)\lambda^2$; $X=1/3$: $(z,y)=(0,-12)\lambda^2$; neither is coprime for any λ

Proof of Theorem 1.1(e), (f). By Lemma 7.1 and the reduction above, every primitive solution gives a point of one of the curves C_2, C_3 (equation (e)) or C_4, C_5 (equation (f)) with $X \in \mathbb{P}^1(\mathbb{Q})$. By Proposition 8.1 these are the points listed in the table, and the table shows that they give only $(\pm1,0,-1)$ for (f) and $(\pm1,-1,1)$ for (e). □

8. Five curves of genus one over cubic fields

We now determine the points with a rational coordinate on the five curves of genus one met in Sections 6 and 7. This completes the proofs of Theorem 1.1(d)–(f).

In this section K is one of the cubic fields $L=\mathbb{Q}(\omega)$ $(\omega^3+3\omega-2=0)$, $K_e=\mathbb{Q}(\phi)$ $(\phi^3=12)$ and $K_f=\mathbb{Q}(\theta)$ $(\theta^3=2)$ of Sections 6 and 7, each of signature $(1,1)$ and class number 1. For $i=1,\dots,5$ let $C_i: Y^2=Q_i(X)$ be the following curves over K, each with a point (X_0,Y_0):

- $C_1=C_L$ of Proposition 6.3, over L, with $(X_0,Y_0)=(-1,\,1-2\omega)$:

$$Q_1=(6\omega^2+6\omega-6)X^4+(41\omega^2+25\omega-31)X^3+(99\omega^2+27\omega-54)X^2 \\ +(102\omega^2+6\omega-42)X+42\omega^2-6\omega-12;$$

- C_2, from equation (e) with $j=1$, over K_e, with $(X_0,Y_0)=(1,-1)$:

$$Q_2=(-3\phi^2+12\phi+9)X^4+(3\phi^2-30\phi-24)X^3+(6\phi^2+18\phi+36)X^2 \\ +(-10\phi^2+4\phi-24)X+4\phi^2-4\phi+4;$$

- C_3, from equation (e) with $j=2$, over K_e, with $(X_0,Y_0)=(\frac12,\,\frac12-\frac{\phi}{4})$:

$$Q_3=(-255\phi^2+1308\phi-1620)X^4+(504\phi^2-2412\phi+2820)X^3 \\ +(-372\phi^2+1638\phi-1764)X^2+(122\phi^2-488\phi+468)X-15\phi^2+54\phi-44;$$

- C_4, from equation (f) with $j=0$, over K_f, with $(X_0,Y_0)=(0,-\theta)$:

$$Q_4=X^4+\theta^2X^3+3\theta X^2-2X+\theta^2;$$

- C_5, from equation (f) with $j=2$, over K_f, with $(X_0,Y_0)=(-1,\,-\theta^2+\theta-1)$:

$$Q_5=(\theta-1)X^4+(2-\theta^2)X^3+(3\theta^2-3\theta)X^2+(2-2\theta)X+2-\theta^2.$$

Here $Q_1=-\eta_L(3X-(\omega^2-\omega-2))G_2(X,1)$ as in Proposition 6.3, and $Q_2,\dots,Q_5$ are the quartics of the four curves of Section 7. Let E_i be the elliptic curve attached to

$(C_i, (X_0, Y_0))$ by Lemma 2.1, so that $(X_0, Y_0) \mapsto O$ and, with $H(u) = u^4 Q_i(X_0 + 1/u)/Y_0^2 = u^4 + bu^3 + cu^2 + du + e$ and $\kappa_H = c - b^2/4$,

$$X = X_0 + \frac{4(U + 4\kappa_H)}{V - bU - 8d} = X_0 + \frac{4(V + bU + 8d)}{U^2 - 64e}. \tag{8.1}$$

The models are

$$\begin{aligned}
E_1 :\ & V^2 = U^3 + 12U^2 + (288\omega^2 + 192\omega + 912)U + 1152\omega^2 + 768\omega + 3520,\\
E_2 :\ & V^2 = U^3 + (72 - 12\phi^2)U^2 + (-2304\phi^2 + 4032\phi + 1728)U\\
& \qquad - 48384\phi^2 + 179712\phi - 161280,\\
E_3 :\ & V^2 = U^3 + (96\phi^2 + 288\phi + 864)U^2 + (82944\phi^2 + 92160\phi + 470016)U\\
& \qquad + 8847360\phi^2 + 13271040\phi + 60456960,\\
E_4 :\ & V^2 = U^3 + 6\theta^2 U^2 - 48\theta U - 256,\\
E_5 :\ & V^2 = U^3 + (8 - 4\theta)U^2 + \tfrac{32\theta^2 - 96\theta + 64}{3} U + \tfrac{384\theta^2 - 512\theta}{9}.
\end{aligned}$$

All five have j-invariant 1728.

Proposition 8.1. *For $i = 1, \dots, 5$, the points of $C_i(K)$ with $X \in \mathbb{P}^1(\mathbb{Q})$ are exactly the two points above each of the following values of X:*

$$C_1 :\ X = -1; \quad C_2 :\ X = 1; \quad C_3 :\ X = \tfrac{1}{2},\ \tfrac{1}{3}; \quad C_4 :\ X = \infty,\ 0,\ 2; \quad C_5 :\ X = -1.$$

The proof follows the same six steps for each curve, with the data in Table 4 and in the list after it.

Step 1: torsion. The group $E_i(K)[2]$ is given by the roots in K of the cubic. The Kummer images of a basis of $E_i(K)[2]$ are independent, so no point of order 2 is divisible by 2, there is no 4-torsion, and the 2-primary torsion is $E_i(K)[2]$. The greatest common divisor of $\#E_i(\mathbb{F}_\mathfrak{q})$ over the degree-one primes $\mathfrak{q}$ of good reduction above the rational primes q with $5 \le q < 300$, all unramified in K, equals $\#E_i(K)[2]$, so the torsion of odd order, which injects into these groups (Section 2.4), is trivial.

Step 2: rank. A 2-descent over K bounds the rank by the number in Table 4. For E_1 and E_2 the 2-torsion is $\mathbb{Z}/2$ and the descent runs over $K \times M$ with M the sextic field $\mathbb{Q}[y]/(y^6 - 3y^2 + 6)$, respectively $\mathbb{Q}[y]/(y^6 + 6y^4 + 12y^2 - 4)$. The class group of the first field has order dividing 2 and is generated by the class of a prime above 2, so its S-class group is trivial. The second has class number 1 (Appendix A). For E_3, E_4, E_5 the 2-torsion is $(\mathbb{Z}/2)^2$ and the descent runs over $K \times K \times K$ (E_3 is isomorphic over K to $y^2 = x^3 - 36x$, and we use that model for the descent). In every case the local images reach the dimensions required in Section 2.4. For E_1 they are 2 and 4 at the two primes above 2, 1 at the prime above 3 and 0 at the real place. In K_e and in K_f there is only one prime above 2 and one above 3, and at the prime above 2, the prime above 3 and the real place the dimensions are 4, 2 and 1 for E_2, and 5, 2 and 1 for E_3, E_4, E_5. Descents via 2-isogeny give the same bounds, except for E_2, for which they give only $\operatorname{rank} E_2(K) \le 3$, so for E_2 the full 2-descent is needed.

Step 3: generators. The points g_i of Table 4, together with a basis of $E_i(K)[2]$, have independent Kummer images, computed with quadratic characters at degree-one primes above 13 and 29 (E_1), 5 (E_2), 5 and 11 (E_3, E_5), and 5, 11 and 17 (E_4). So the rank equals the bound of Step 2, and $G' = \langle g_i \rangle + E_i(K)_{\mathrm{tors}}$ has odd index in $E_i(K)$ (Lemma 2.2).

Step 4: odd saturation. Let ℓ be an odd prime in the column "saturation" of Table 4. We use one prime $\mathfrak{q}$ of good reduction (for the curves of rank 1) or two (for rank 2) at which

the ℓ-part of $E_i(\mathbb{F}_\mathfrak{q})$ is cyclic and the images of the g_i in $\bigoplus_\mathfrak{q} E_i(\mathbb{F}_\mathfrak{q})/\ell E_i(\mathbb{F}_\mathfrak{q})$ are independent. Then $\ell \nmid [E_i(K) : G']$ by Lemma 2.2. For the curves E_3 and E_4 of rank 2 two primes are needed, since $E_i(\mathbb{F}_\mathfrak{q})/\ell E_i(\mathbb{F}_\mathfrak{q})$ has dimension 1 when the ℓ-part is cyclic. The table gives, for each ℓ, the rational primes below the primes $\mathfrak{q}$ used. The primes ℓ treated in this way are p and the odd primes dividing N or the exponent L_q of a sieve prime q that removes classes.

Step 5: sieve. For each sieve prime q and every $\mathfrak{q} \mid q$, the data of Lemma 2.1 are $\mathfrak{q}$-integral and Y_0 and $\operatorname{disc} H$ are $\mathfrak{q}$-units, so X reduces well. The sieve of Section 2.5 with modulus N and the condition that the reductions of $X(P)$ at the primes above q are one and the same element of $\mathbb{P}^1(\mathbb{F}_q)$ leaves the classes listed, each of which contains a known point P_0.

Step 6: Chabauty. For each surviving class, with its known point P_0, we apply Lemma 2.3 with the prime p and the modulus N of the table. Here p splits completely in K, and N kills $E_i^{\sigma_j}(\mathbb{F}_p)$ for the three embeddings σ_j. We take $\rho = X$, written as one of the expressions in (8.1), or $\rho = 1/X$ at points with $X = \infty$. The lemma shows that P_0 is the only point of $P_0 + N\,E_i(K)$ with $\rho \in \mathbb{Q}$. At $P_0 = O$ we use case (ii): $\rho - X_0 = -4t(1 + O(t))$ in the formal parameter, with p-integral coefficients. At the other points we use case (i). The matrices $\mathcal{J}/p$ modulo p are listed below, and all have full rank. Hence every point with $X \in \mathbb{P}^1(\mathbb{Q})$ is one of the known points.

	$E_i(K)$	Sel. bound	generators g_i	p, N	sieve q (L_q)	saturation
E_1	$\mathbb{Z} \times \mathbb{Z}/2$	1	$(12\omega^2 + 8,\ -24\omega^2 + 48\omega - 168)$	29, 20	29 (20)	5 (13), 29 (109)
E_2	$\mathbb{Z} \times \mathbb{Z}/2$	1	$(-8\phi^2 - 36\phi + 120,$ $216\phi^2 + 432\phi - 2160)$	19, 20	19 (20), 79 (80)	5 (13), 19 (683)
E_3	$\mathbb{Z}^2 \times (\mathbb{Z}/2)^2$	2	$(-80\phi^2 - 96\phi - 288,\ 6912);$ $(64\phi^2 + 1056\phi - 2592,$ $-36864\phi^2 + 27648\phi + 110592)$	19, 10	19 (10), 13 (10), 79 (40)	5 (13, 13), 19 (227, 683)
E_4	$\mathbb{Z}^2 \times (\mathbb{Z}/2)^2$	2	$(-5\theta^2,\ -18);$ $(2\theta^2 + 2\theta + 4,\ 12\theta^2 + 12)$	31, 16	31 (16), 43 (22), 109 (58), 127 (64)	11 (43, 43), 29 (109, 109), 31 (743, 1487)
E_5	$\mathbb{Z} \times (\mathbb{Z}/2)^2$	1	$(-\frac{4}{3}\theta^2 + \frac{2}{3}\theta,\ -\frac{4}{3}\theta^2 - \frac{8}{3}\theta + \frac{20}{3})$	31, 16	31 (16)	31 (743)

TABLE 4. Data for Proposition 8.1. The sieve primes listed are those that remove classes. In the column "saturation", each odd prime ℓ is followed by the rational primes below the primes used for it in Step 4.

The surviving classes and the Chabauty matrices. We write a class as $\sum a_i g_i + t$ modulo N, with $t \in E_i(K)_{\mathrm{tors}}$. For E_1, E_2 and E_5 the classes listed have $t = O$.

- E_1: $a \equiv 0$ ($P_0 = O$, $X = -1$) and $a \equiv 2$ ($P_0 = 2g_1 = (4\omega^2 + 2\omega + 1,\ 27\omega^2 + 21\omega + 71)$, the image of $(-1, -Y_0)$, $X = -1$); $\mathcal{J}/29 = (2, 9)^\mathsf{T}$ and $(27, 20)^\mathsf{T}$.
- E_2: $a \equiv 0$ (O, $X = 1$) and $a \equiv 1$ (g_1, the image of $(1, -Y_0)$, $X = 1$); $\mathcal{J}/19 = (7, 7)^\mathsf{T}$ and $(12, 12)^\mathsf{T}$.
- E_3, with $T = (64\phi^2 - 96\phi - 288, 0)$ ($X = 1/3$): the classes of O ($X = \frac{1}{2}$), T ($X = \frac{1}{3}$), g_1 ($X = \frac{1}{2}$) and $g_1 + T = (-64\phi^2 - 96\phi - 288,\ -6144)$ ($X = \frac{1}{3}$); $\mathcal{J}/19 = \left(\begin{smallmatrix} 5 & 8 \\ 3 & 7 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 16 & 10 \\ 14 & 6 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 14 & 11 \\ 16 & 12 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 3 & 9 \\ 5 & 13 \end{smallmatrix}\right)$.
- E_4, with $T = (4\theta^2, 0)$ ($X = \infty$): the classes of O ($X = 0$), T ($X = \infty$), g_2 ($X = 2$), g_1 ($X = 0$), $g_1 + T = (-4\theta^2, 16)$ ($X = \infty$) and $g_1 - g_2 = (-2\theta^2 - 6\theta,\ 12\theta^2 - 12\theta + 12)$

$(X=2)$; $\mathcal{J}/31 = \left(\begin{smallmatrix}22 & 19\\ 8 & 25\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}29 & 24\\ 10 & 14\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}26 & 28\\ 19 & 27\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}9 & 12\\ 23 & 6\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}2 & 7\\ 21 & 17\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}5 & 3\\ 12 & 4\end{smallmatrix}\right)$, with $\rho = 1/X$ at the two points with $X=\infty$ and the second expression in (8.1) at g_2.

- E_5: $a \equiv 0$ (O, $X=-1$) and $a \equiv 1$ (g_1, the image of $(-1,-Y_0)$, $X=-1$); $\mathcal{J}/31 = (8,25)^{\mathsf{T}}$ and $(23,6)^{\mathsf{T}}$.

9. The equation $x^4+3y^3+z^3=0$: descent and the class $j=0$

The remaining three sections prove Theorem 1.1(g), for the equation

$$x^4+3y^3+z^3=0. \tag{9.1}$$

A descent over $\mathbb{Q}(\sqrt[3]{3})$ leaves two classes of units, $j=0$ and $j=1$. The class $j=0$ gives only the solutions $(\pm1,0,-1)$ (Proposition 9.3). The class $j=1$ leads to rational points on a curve of genus 2 with a condition at 2 (Lemma 9.4), which Sections 10 and 11 treat.

9.1. **The field.** Let $K_g=\mathbb{Q}(\chi)$ with $\chi^3=3$. Then $\mathcal{O}_{K_g}=\mathbb{Z}[\chi]$ (the polynomial discriminant -243 equals d_{K_g}), K_g has signature $(1,1)$ and class number 1 (Appendix A), $3\mathcal{O}_{K_g}=(\chi)^3$, and $2\mathcal{O}_{K_g}=\mathfrak{q}_1\mathfrak{q}_2$ with $\mathfrak{q}_1=(\chi-1)$ of degree 1 and $\mathfrak{q}_2=(\chi^2+\chi+1)$ of degree 2. The unit $\eta_g=\chi^2-2$ has norm 1, and it is a quadratic non-residue modulo the prime $(5,\chi-2)$, at which -1 is a residue, so neither η_g nor $-\eta_g$ is a square. As the unit group of K_g has rank 1 and torsion $\{\pm1\}$, it follows that η_g^j, $0\le j\le 3$, represent the units of norm 1 modulo fourth powers (see Appendix A).

9.2. **Unit classes.**

Lemma 9.1. *Let (x,y,z) be a primitive solution of (9.1) and $\alpha=-(z+y\chi)\in\mathcal{O}_{K_g}$. Then $\gcd(y,z)=1$, x is odd, $3\nmid xz$, $\mathrm{Nm}(\alpha)=x^4$, and*

$$\alpha=\eta_g^j\gamma^4 \qquad \text{with } \gamma\in\mathcal{O}_{K_g} \text{ and } j\in\{0,1\}. \tag{9.2}$$

Moreover $(y,z)\equiv(0,15)$ or $(13,0)$ (mod 16) if $j=0$, and $(y,z)\equiv(6,7)$ (mod 16) if $j=1$.

Proof. A prime dividing y and z divides x^4, so $\gcd(y,z)=1$. If $3\mid x$ then $3\mid z$, so $27\mid x^4+z^3=-3y^3$ and $3\mid y$, contradicting primitivity. So $3\nmid x$, and then $3\nmid z$. We have $\mathrm{Nm}(z+y\chi)=z^3+3y^3$, so $\mathrm{Nm}(\alpha)=-(z^3+3y^3)=x^4$. Put $\beta=z^2-zy\chi+y^2\chi^2$. Then $(z+y\chi)\beta=z^3+3y^3$, so $\alpha\beta=x^4$, and $(z+y\chi)^2-\beta=3yz\chi$. A prime $\mathfrak{q}\nmid 3$ of K_g dividing α and β divides yz, and together with $\mathfrak{q}\mid z+y\chi$ this makes $\mathfrak{q}$ divide both y and z, which is impossible. So $v_{\mathfrak{q}}(\alpha)$ is 0 or $v_{\mathfrak{q}}(x^4)$ for $\mathfrak{q}\nmid 3$, and $v_{(\chi)}(\alpha)=v_3(\mathrm{Nm}\,\alpha)=0$. Hence (α) is the fourth power of an ideal, which is principal, and $\alpha=\varepsilon\gamma^4$ with a unit ε of norm $x^4/\mathrm{Nm}(\gamma)^4>0$, that is, of norm 1. So we may take $\varepsilon=\eta_g^j$ with $0\le j\le 3$.

For the conditions at 2, let $\chi_1\in\mathbb{Z}_2$ and $\chi_2\in\mathbb{Z}_2[\zeta_3]$ be the images of χ in $K_{g,\mathfrak{q}_1}=\mathbb{Q}_2$ and in $K_{g,\mathfrak{q}_2}=\mathbb{Q}_2(\zeta_3)$, an unramified extension. In both rings of integers the units congruent to 1 modulo 16 are fourth powers, since $1+2^k\mathcal{O}$ consists of squares of elements of $1+2^{k-1}\mathcal{O}$ for $k\ge 3$. The residue of χ_2 modulo 2 is a primitive cube root of unity, so α is a unit at $\mathfrak{q}_2$ (otherwise y and z would be even), and $v_{\mathfrak{q}_1}(\alpha)=v_2(\mathrm{Nm}\,\alpha)=4v_2(x)$. By (9.2), $\alpha\eta_g^{-j}$ is a fourth power in $K_{g,\mathfrak{q}_1}$ and in $K_{g,\mathfrak{q}_2}$. If x is odd, α is a unit at both primes and this condition depends only on (y,z) mod 16. Modulo 16 we have $\chi_1\equiv 11$ and, for one of the two embeddings of K_g into $\mathbb{Q}_2(\zeta_3)$, $\chi_2\equiv 11\zeta_3$ (the other embedding gives the same conditions). Hence $\eta_g\equiv 7$ at $\mathfrak{q}_1$ and $\eta_g\equiv 5+7\zeta_3$ at $\mathfrak{q}_2$. The fourth powers of units are $\equiv 1$ (mod 16) in $\mathbb{Z}_2$, and modulo 16 in $\mathbb{Z}_2[\zeta_3]$ they form the subgroup $\{1,9\}\times\{1,\zeta_3,\zeta_3^2\}$ of order 6 of $(\mathbb{Z}_2[\zeta_3]/16)^\times$. At $\mathfrak{q}_1$ the condition reads $z+11y\equiv -7^j$ (mod 16), which leaves 16 pairs (y,z) for each j. At $\mathfrak{q}_2$ it asks that $-(z+11y\zeta_3)(5+7\zeta_3)^{-j}$ lie in that subgroup modulo 16, and

among the 16 pairs this leaves exactly $(0,15)$ and $(13,0)$ for $j=0$, $(6,7)$ for $j=1$, and none for $j=2,3$. If x were even, then $z+y\chi_1\equiv 0 \pmod{16}$, so $\alpha\equiv y(\chi_1-\chi_2) \pmod{16\mathcal{O}_{\mathfrak{q}_2}}$ with y odd, and one checks for each odd y modulo 16 and each j that $y(\chi_1-\chi_2)\eta_g^{-j}$ is not a fourth power in $(\mathcal{O}_{\mathfrak{q}_2}/16)^\times$. So x is odd. □

9.3. **Conics.**

Lemma 9.2. *In the situation of Lemma 9.1 there are coprime integers m,n and $\mu\in\mathbb{Q}^\times$ with $\gamma^2=\mu\,\delta_j(m,n)$, where*

$$\delta_0(m,n)=n^2-2mn\,\chi-2m^2\,\chi^2,$$
$$\delta_1(m,n)=(2m^2-2mn-4n^2)+(m^2-4n^2)\,\chi+(m^2-2n^2)\,\chi^2.$$

Then

$$\begin{aligned} j=0:&\quad z=-\mu^2(n^4+24m^3n),\qquad y=-\mu^2(12m^4-4mn^3);\\ j=1:&\quad z=-\mu^2(m^4+4m^3n-12m^2n^2+16mn^3+4n^4),\\ &\quad y=-\mu^2(m^4-4m^3n-8mn^3+8n^4).\end{aligned}$$

Proof. Put $\delta=\gamma^2=d_0+d_1\chi+d_2\chi^2$ with $d_i\in\mathbb{Z}$. The χ^2-coordinate of $\alpha=\eta_g^j\delta^2$ vanishes, and it equals $d_1^2+2d_0d_2$ for $j=0$ and $d_0^2-4d_0d_2-2d_1^2+6d_1d_2$ for $j=1$. Both ternary forms are nondegenerate, and the maps $(m:n)\mapsto\delta_j(m,n)$, whose coordinates are three linearly independent binary quadratic forms without common zero, are isomorphisms from $\mathbb{P}^1$ onto these conics. So $(d_0:d_1:d_2)$ is the image of some $(m:n)$ with m,n coprime integers, and $\delta=\mu\,\delta_j(m,n)$. The formulas for z and y follow by comparing the coefficients of 1 and χ in $-(z+y\chi)=\alpha=\mu^2\eta_g^j\delta_j(m,n)^2$. □

The element $\delta=\gamma^2$ is primitive, that is, not divisible in $\mathcal{O}_{K_g}$ by a rational prime p: otherwise $p^2\mid\alpha$ and p would divide y and z. So $\mu=\pm1/c$, where c is the gcd of the coordinates of $\delta_j(m,n)$.

9.4. **The class $j=0$.**

Proposition 9.3. *The only primitive solutions of (9.1) with $j=0$ in (9.2) are $(\pm1,0,-1)$.*

Proof. Let $f_0(t)=\mathrm{Nm}(\delta_0(t,1))/\delta_0(t,1)=12\chi t^4-12t^3+6\chi^2t^2+2\chi t+1\in K_g[t]$. From $\gamma^2=\mu\delta_0(m,n)$ we get $\mu^3\,\mathrm{Nm}(\delta_0(m,n))=\mathrm{Nm}(\gamma)^2$ and

$$n^4 f_0(m/n)=\frac{\mathrm{Nm}(\delta_0(m,n))}{\delta_0(m,n)}=\Big(\frac{\mathrm{Nm}(\gamma)}{\mu\gamma}\Big)^2,$$

so $t=m/n\in\mathbb{P}^1(\mathbb{Q})$ is the first coordinate of a K_g-point of $C_0: Y^2=f_0(t)$ ($n=0$ gives the points at infinity, which are K_g-rational because $12\chi=(2\chi^2)^2$). We show below that the points of $C_0(K_g)$ with $t\in\mathbb{P}^1(\mathbb{Q})$ are those with $t\in\{0,\infty\}$. For $t=0$, $(m,n)=\pm(0,1)$, $\delta_0=1$, $\mu=\pm1$, and $(y,z)=(0,-1)$: the solutions $(\pm1,0,-1)$. For $t=\infty$, $(m,n)=\pm(1,0)$, $\delta_0=-2\chi^2$, $\mu=\pm\frac12$, and $(y,z)=(-3,0)$, $x=\pm3$: not primitive.

The curve C_0 has the point $(0,1)$, and Lemma 2.1 with this base point gives the model

$$E_0:\ V^2=U^3+24\chi^2U^2-1152\chi U-36864,$$

isomorphic over K_g to $Y^2=X^3-36X$. On E_0, t is given by (8.1) with $X_0=0$, and the four points of C_0 with $t\in\{0,\infty\}$ go to known points of $E_0(K_g)$. We follow the steps of Section 8. The torsion subgroup is $E_0(K_g)[2]\cong(\mathbb{Z}/2)^2$ (no point of order 2 is twice a point, by the Kummer images below, and the orders of $E_0(\mathbb{F}_{\mathfrak{q}})$ over the degree-one primes $\mathfrak{q}$ of

good reduction above the rational primes q with $5 \le q < 300$ (all unramified in K_g) have greatest common divisor 4). A 2-descent over K_g (on the model $Y^2 = X^3 - 36X$, whose 2-torsion is rational) gives a Selmer group of dimension 4, so $\operatorname{rank} E_0(K_g) \le 2$. The points

$$g_1 = (-20\chi^2,\, 216), \qquad g_2 = (-80\chi^2 + 120\chi - 72,\, -288\chi^2 - 1728\chi + 3168)$$

and a basis of $E_0(K_g)[2]$ have independent Kummer images. Hence $E_0(K_g) \cong \mathbb{Z}^2 \times (\mathbb{Z}/2)^2$, and the index of $\langle g_1, g_2\rangle + E_0(K_g)_{\mathrm{tors}}$ is odd and, by Lemma 2.2, prime to 13 and 61. The Mordell–Weil sieve with modulus $N = 26$ and the primes 61 and 103, where $L_{61} = 26$ and $L_{103} = 52$ (the primes 67 and 73 remove no class), leaves four classes modulo $26E_0(K_g)$, each containing one of the four known points. The prime 61 splits completely in K_g, and Lemma 2.3 with $p = 61$, $N = 26$, and $\rho = t$, or $\rho = 1/t$ at the two points with $t = \infty$, shows that each known point is the only point of its class with $t \in \mathbb{P}^1(\mathbb{Q})$: the matrices $\mathcal{J}/61$ modulo 61 are

$$\begin{pmatrix} 7 & 21 \\ 37 & 38 \end{pmatrix}, \quad \begin{pmatrix} 36 & 8 \\ 20 & 55 \end{pmatrix}, \quad \begin{pmatrix} 54 & 40 \\ 24 & 23 \end{pmatrix}, \quad \begin{pmatrix} 25 & 53 \\ 41 & 6 \end{pmatrix},$$

all of rank 2. □

9.5. **The class $j = 1$.** Let

$$g(m,n) = \tfrac{1}{2}\operatorname{Nm}(\delta_1(m,n)) = m^6 - 3m^5n + 15m^4n^2 - 10m^3n^3 - 30m^2n^4 + 24mn^5 - 20n^6,$$

and $g(t) = g(t,1)$, an irreducible polynomial of discriminant $2^8 \cdot 3^{25}$.

Lemma 9.4. *Let (x,y,z) be a primitive solution with $j = 1$ in (9.2), and m, n, μ as in Lemma 9.2. Then m is even, $\mu = \frac{1}{2}$, $g(m,n) = 4x^2$, and $t = m/n \in 2 + 8\mathbb{Z}_2$.*

Proof. If m is odd, then $\delta_1(m,n)$ is primitive: its coordinate $m^2 - 4n^2$ is odd, and an odd prime dividing all three coordinates divides $(m^2 - 4n^2) - (m^2 - 2n^2) = -2n^2$, hence n and then m. Then $\mu = \pm 1$ and $y = -(m^4 - 4m^3n - 8mn^3 + 8n^4)$ is odd, contradicting $y \equiv 6 \pmod{16}$ (Lemma 9.1). So m is even and n odd. Then the coordinates of $\delta_1(m,n)$ are even and the third divided by 2, $m^2/2 - n^2$, is odd, so $\mu = \pm\frac{1}{2}$.

Since $\mu\delta_1(m,n) = \gamma^2$, the element $\mu\delta_1(t,1) = \mu\delta_1(m,n)/n^2$ is a square in $K_{g,\mathfrak{q}_1}$ and in $K_{g,\mathfrak{q}_2}$, with $t \in 2\mathbb{Z}_2$. A finite computation shows that this happens only for $\mu = +\frac{1}{2}$ and $t \in 2 + 8\mathbb{Z}_2$. We cover $2\mathbb{Z}_2$ by disks $t_0 + 2^k\mathbb{Z}_2$ on each of which the square classes of $\delta_1(t,1)$ in $K_{g,\mathfrak{q}_1}$ and $K_{g,\mathfrak{q}_2}$ are constant, and test the condition on each disk. By Section 2.1, the class is constant on such a disk when $\min_{i \ge 1} v(\delta_1^{(i)}(t_0,1)2^{ki}/i!) > v(\delta_1(t_0,1)) + 2v(2)$, where $\delta_1^{(i)}$ is the i-th derivative in t and v is the valuation at $\mathfrak{q}_1$ or $\mathfrak{q}_2$. Finally $\operatorname{Nm}(\gamma)^4 = \operatorname{Nm}(\alpha)/\operatorname{Nm}(\eta_g) = x^4$ and $\operatorname{Nm}(\gamma)^2 = \mu^3 \operatorname{Nm}(\delta_1(m,n)) = 2\mu^3 g(m,n) = g(m,n)/4$, so $g(m,n) = 4x^2$. □

Remark 9.5. In the class $j = 1$ one could proceed as for $j = 0$, with $f_1(t) = \operatorname{Nm}(\delta_1(t,1))/\delta_1(t,1)$ and the curve $Y^2 = f_1(t)$ over K_g. Its Jacobian is isomorphic over K_g to $E_{\eta_g} : Y^2 = X^3 - 36\eta_g X$. The points of $E_{\eta_g}(K_g)$ with

$$X = 24\chi^2 - 18\chi - 24, \qquad X = 12\chi^2 - 9\chi - 12, \qquad X = 9\chi - 9,$$

together with $(0,0)$, have independent Kummer images (quadratic characters at primes above 5, 11 and 17), so $\operatorname{rank} E_{\eta_g}(K_g) \ge 3 = [K_g : \mathbb{Q}]$, and elliptic Chabauty over K_g does not apply. A 2-descent gives $\dim \mathrm{Sel}^2(E_{\eta_g}/K_g) = 4$ with $E_{\eta_g}(K_g)[2]$ of order 2, hence $\operatorname{rank} E_{\eta_g}(K_g) \le 3$. This descent uses the class group of $K_g(\sqrt{\eta_g})$ as computed by PARI's `bnfinit`, which we have not certified, so the computation shows that the rank equals 3 only under GRH. The Jacobian J_g of the curve $Y^2 = g(t)$ of genus 2, on which Lemma 9.4 puts the point $(t, 2x/n^3)$, has rank at least 2 over $\mathbb{Q}$. Indeed, let $\infty_\pm$ be its two points at

infinity. The classes of $\infty_- - \infty_+$ and $(2,6) - \infty_+$ are independent modulo 11, as their images under the homomorphisms $J_g(\mathbb{Q}) \to \mathbb{Z}/11$ given by reduction at $p = 83$, 179 and 227 (where the 11-part of $J_g(\mathbb{F}_p)$ is cyclic) span a space of dimension 2. Since $J_g(\mathbb{Q})$ has no torsion ($\#J_g(\mathbb{F}_7) = 57$ and $\#J_g(\mathbb{F}_{11}) = 82$ are coprime, Section 2.4), and in particular no 11-torsion, the two classes are independent in $J_g(\mathbb{Q})$. So Chabauty's method does not apply to this curve directly either. The programs for this remark in the deposit [21] carry out these computations. The proof of Theorem 1.1(g) does not use them, and they explain the route taken in Sections 10 and 11.

10. A covering over a field of degree 12

Let t be the parameter of a solution in the class $j = 1$ (Lemma 9.4). It gives a rational point on the curve $Y^2 = g(t)$ of genus 2, whose Jacobian has rank at least 2, so Chabauty's method does not apply to this curve directly (Remark 9.5). We pass to a covering instead: we show that t is the first coordinate of a point on a curve C_g of genus one over a field Ξ of degree 12 (Lemma 10.1), and we prove the facts about the Jacobian of C_g that Section 11 uses (Proposition 10.3).

10.1. **The field Ξ.** Over K_g, $g(t)$ has the quadratic factor $\delta_1(t,1)/(2+\chi+\chi^2)$, since $2g = \mathrm{Nm}(\delta_1(\cdot,1))$. So the six roots of g fall into three pairs, the roots of $\delta_1(t,1)$ and of its two conjugates over $\mathbb{Q}$. Call a pair of roots of g *mixed* if its two roots lie in different ones of these three pairs. There are twelve mixed pairs. The sums of the roots of the twelve mixed pairs are the roots of an irreducible polynomial of degree 12, so the Galois group of g permutes the mixed pairs transitively. Let Ξ be the field generated by the sum of the roots of one mixed pair. The choice of the mixed pair does not matter, since the twelve choices give conjugate fields and conjugate data. We take for Ξ the field $\mathbb{Q}[\xi]/(f_{12}(\xi))$ with

$$f_{12} = \xi^{12} - 6\xi^{11} + 18\xi^{10} - 32\xi^9 + 45\xi^8 - 78\xi^7 + 146\xi^6 - 180\xi^5 + 99\xi^4 + 30\xi^3 - 72\xi^2 + 36\xi - 6,$$

a defining polynomial with small coefficients. It is not the minimal polynomial of the sum of a mixed pair, and in Ξ the chosen mixed pair has the sum s given in (B.1). The field Ξ has degree 12, signature $(2,5)$ and discriminant $-2^{14}3^{21}$. Its subfields are $\mathbb{Q}$, K_g, $K_g(\sqrt{\eta_g})$ of degree 6, and Ξ. Its class number is 1 (Appendix A). The prime 2 factors as $2\mathcal{O}_\Xi = \mathfrak{p}_1^4\mathfrak{p}_2^2\mathfrak{p}_3^2$ with residue degrees $1,2,2$, and $3\mathcal{O}_\Xi$ has two prime factors. Let S be the set of the five primes of Ξ above 2 and 3. As the class number is 1, $\Xi(S,2)$ has dimension $r_1 + r_2 + \#S = 2+5+5 = 12$. Appendix B gives a basis $\pi_1, \dots, \pi_5, u_1, \dots, u_6, -1$ of $\Xi(S,2)$, where π_i generates $\mathfrak{p}_i$ for $i = 1,2,3$, π_4, π_5 generate the two primes above 3, and the u_i are units. We write $v_i = v_{\mathfrak{p}_i}$, $\Xi_i = \Xi_{\mathfrak{p}_i}$, and $e_i = 4,2,2$ for the ramification indices. The labels $\mathfrak{p}_2$, $\mathfrak{p}_3$ are fixed by π_2, π_3, and Section 11.3 characterizes them by a property of the points P_3, P_4 defined below.

Over Ξ we write $g = g_2 g_4$, where $g_2 \in \mathcal{O}_\Xi[t]$ is the monic quadratic polynomial whose roots are the chosen mixed pair and $g_4 = g/g_2 \in \mathcal{O}_\Xi[t]$ (the coefficients are integral because g is monic with integer coefficients). Explicitly, $g_2 = t^2 - st + p$ with $s, p \in \Xi$ given in (B.1). All the data below are computed from f_{12} and g_2. The resultant of g_2 and g_4 is divisible only by primes in S. Put

$$q(t) = \frac{g_4(t)}{g_4(2)} \in \Xi[t], \qquad C_g : \ w^2 = q(t),$$

a curve of genus one over Ξ (q has four distinct roots). It has the points

$$P_1 = (2,1), \quad P_2 = (2,-1), \quad P_3 = (-\tfrac{10}{3}, w_0), \quad P_4 = (-\tfrac{10}{3}, -w_0),$$

where $w_0 \in \Xi$ is the square root of $q(-\frac{10}{3})$ given in (B.2) (Section 11.3 explains this choice of sign). We call $P_1, \dots, P_4$ the *known points*.

10.2. **The reduction.**

Lemma 10.1. *Let (x, y, z) be a primitive solution of (9.1) with $j = 1$ in (9.2), and $t = m/n$ as in Lemma 9.4. Then $t \in \mathbb{Q} \cap (2 + 8\mathbb{Z}_2)$ and $q(t)$ is a square in Ξ; that is, $(t, w) \in C_g(\Xi)$ for some $w \in \Xi$.*

Proof. By Lemma 9.4, $t \in 2 + 8\mathbb{Z}_2$ and $g(t) = 4x^2/n^6$ is a nonzero square in $\mathbb{Q}$. Let $G_2(m,n) = n^2 g_2(m/n)$ and $G_4(m,n) = n^4 g_4(m/n)$. They lie in $\mathcal{O}_\Xi$ and $G_2(m,n)G_4(m,n) = g(m,n) = 4x^2$. A prime $\mathfrak{p} \notin S$ dividing both $G_2(m,n)$ and $G_4(m,n)$ would divide the resultant of the binary forms G_2, G_4 (as m, n are coprime), which is not the case. So $v_\mathfrak{p}(G_2(m,n))$ is 0 or $v_\mathfrak{p}(4x^2)$, an even number. Hence the class of $g_2(t) = G_2(m,n)/n^2$ in $\Xi^\times/\Xi^{\times 2}$ lies in $\Xi(S, 2)$.

On the disk $2 + 8\mathbb{Z}_2$ the square class of $g_2(t)$ in $\Xi_i^\times/\Xi_i^{\times 2}$ is constant for $i = 1, 2, 3$: with $v = v_i$ and $e = e_i$, $\min_{l \geq 1} v(g_2^{(l)}(2)\, 8^l/l!) > v(g_2(2)) + 2e$ (the left side is 14, 6, 6 and the right side 12, 5, 5 for $i = 1, 2, 3$). So $g_2(t)/g_2(2)$ is a square in each Ξ_i. The map $\Xi(S, 2) \to \prod_{i=1}^3 \Xi_i^\times/\Xi_i^{\times 2}$ is injective: the images of the basis $\pi_1, \dots, \pi_5, u_1, \dots, u_6, -1$ are twelve independent local classes (their coordinates in the local bases of Appendix B form a matrix of rank 12). Since $g_2(t)/g_2(2) \in \Xi(S, 2)$ is locally trivial at 2, it is a square in Ξ. Finally $g_2(2)g_4(2) = g(2) = 36$, so

$$q(t) = \frac{g_4(t)}{g_4(2)} = \frac{g(t)}{36} \cdot \frac{g_2(2)}{g_2(t)} \in \Xi^{\times 2}. \qquad \square$$

The values $t = 2$ and $t = -\frac{10}{3}$ of the known points come from solutions: by Lemma 9.2 with $\mu = \frac{1}{2}$, $t = 2$ gives $(m, n) = \pm(2, 1)$ and $(x, y, z) = (\pm 3, 6, -9)$, which is not primitive, and $t = -\frac{10}{3}$ gives $(m, n) = \pm(-10, 3)$ and the solutions $(\pm 895, -6202, 4199)$.

Remark 10.2. The six roots of g form a regular octahedron on $\mathbb{P}^1$ up to a Möbius transformation, with the three pairs of roots of the conjugates of $\delta_1(t, 1)$ as antipodal pairs: the curves of genus one $Y^2 =$ (product of two antipodal pairs) have j-invariant 1728, and those $Y^2 =$ (a mixed pair times an antipodal pair), which include C_g, have j-invariant 128. This explains the j-invariants below.

10.3. **The Jacobian of C_g.** Let E_g be the Jacobian of C_g, an elliptic curve over Ξ, and $\iota : C_g \to E_g$, $P \mapsto [P - P_1]$, which is an isomorphism over Ξ. For $B \in C_g(\Xi)$ write $\iota_B(P) = \iota(P) - \iota(B)$.

Proposition 10.3(a) below gives a model of E_g of the form $Y^2 = X(X^2 + aX + b)$ with $a, b \in \Xi$, and we use it throughout: Lemma 2.1 applied to $w^2 = q(t)$ with the base point P_1 (that is, to $W^2 = u^4 q(2 + 1/u)$, which is monic as $q(2) = 1$, where $t = 2 + 1/u$ and $w = W/u^2$) gives a model $V^2 = U^3 + A_2U^2 + A_4U + A_6$ whose 2-division cubic has exactly one root $U_0 \in \Xi$, and $X = U - U_0$, $Y = V$. We identify E_g with this model so that ι is the map of Lemma 2.1 followed by this translation. Let

$$E_g :\ Y^2 = X(X^2 + aX + b), \qquad E_g' :\ Y^2 = X(X^2 - 2aX + a^2 - 4b),$$

$T = (0, 0) \in E_g$, $T' = (0, 0) \in E_g'$, let $\mathcal{K}$ be Ξ or one of its completions, and let $\varphi : E_g \to E_g'$ be the 2-isogeny with kernel $\{O, T\}$ and $\hat{\varphi} : E_g' \to E_g$ its dual, so that $\hat{\varphi}\varphi = [2]$, $\varphi\hat{\varphi} = [2]$

and $\ker\hat{\varphi} = \{O, T'\}$. The maps

$$\kappa : E_g(\mathcal{K}) \to \mathcal{K}^\times/\mathcal{K}^{\times 2}, \quad (X,Y) \mapsto X, \quad T \mapsto b,$$
$$\kappa' : E'_g(\mathcal{K}) \to \mathcal{K}^\times/\mathcal{K}^{\times 2}, \quad (X,Y) \mapsto X, \quad T' \mapsto a^2 - 4b,$$

are homomorphisms with kernels $\hat{\varphi}(E'_g(\mathcal{K}))$ and $\varphi(E_g(\mathcal{K}))$ [30, §X.4]. For $\mathcal{K} = \Xi$ their Selmer groups $\mathrm{Sel}(\kappa)$ and $\mathrm{Sel}(\kappa')$ are the subgroups of $\Xi^\times/\Xi^{\times 2}$ of classes that lie in the image of the local map at every place. They contain $\kappa(E_g(\Xi))$ and $\kappa'(E'_g(\Xi))$, and

$$\operatorname{rank} E_g(\Xi) = \dim \kappa(E_g(\Xi)) + \dim \kappa'(E'_g(\Xi)) - 2 \tag{10.1}$$

when $E_g(\Xi)[2] = \{O, T\}$ and $E'_g(\Xi)[2] = \{O, T'\}$ (from the exact sequence $0 \to E'_g(\Xi)[\hat{\varphi}]/\varphi(E_g(\Xi)[2]) \to E'_g(\Xi)/\varphi E_g(\Xi) \to E_g(\Xi)/2E_g(\Xi) \to E_g(\Xi)/\hat{\varphi}E'_g(\Xi) \to 0$). We write κ_i, κ'_i for the maps over Ξ_i, and $\mathrm{loc} : \mathrm{Sel}(\kappa) \to \prod_{i=1}^3 \Xi_i^\times/\Xi_i^{\times 2}$, $\mathrm{loc}' : \mathrm{Sel}(\kappa') \to \prod_{i=1}^3 \Xi_i^\times/\Xi_i^{\times 2}$ for the localizations at the primes above 2.

Proposition 10.3. (a) *E_g has j-invariant 128 and a model $Y^2 = X(X^2 + aX + b)$ with $a \in \Xi^\times$ and $b = a^2/2$, where a is given in (B.2) and has norm $-2^{18}3^4$. So $\kappa(T) = b \equiv 2$ and $\kappa'(T') = a^2 - 4b = -a^2 \equiv -1$ modulo squares. The point T is the only point of order 2 of $E_g(\Xi)$, $E'_g(\Xi)[2] = \{O, T'\}$, and $E_g(\Xi)_{\mathrm{tors}} = \{O, T\}$.*

(b) $\mathrm{Sel}(\kappa)$ *and* $\mathrm{Sel}(\kappa')$ *lie in $\Xi(S, 2)$ and have dimensions 5 and 3. Hence* $\operatorname{rank} E_g(\Xi) \le 6$.

(c) $\iota(P_2) = \iota(P_3) + \iota(P_4)$, *and* $\operatorname{rank} E_g(\Xi) \ge 2$.

(d) loc *and* loc' *are injective.*

(e) *At each $\mathfrak{p}_i$: 2 is not a square in Ξ_i, and -1 is a square in Ξ_1 but not in Ξ_2, Ξ_3. The group $E_g(\Xi_i)[2]$ has order $4, 2, 2$ for $i = 1, 2, 3$, $E'_g(\Xi_i)[2] = \{O, T'\}$, and neither $E_g(\Xi_i)$ nor $E'_g(\Xi_i)$ has a point of order 4. A tuple $(\kappa_i(t_i))_i$ with $t_i \in E_g(\Xi_i)[2]$ lies in $\mathrm{loc}(\mathrm{Sel}(\kappa))$ only if it is $(\kappa_i(O))_i$ or $(\kappa_i(T))_i$; a tuple $(\kappa'_i(t'_i))_i$ with $t'_i \in \{O, T'\}$ lies in $\mathrm{loc}'(\mathrm{Sel}(\kappa'))$ only if it is $(\kappa'_i(O))_i$ or $(\kappa'_i(T'))_i$.*

(f) *For $B \in C_g(\Xi)$ let $B^T \in C_g(\Xi)$ be the point with $\iota(B^T) = \iota(B) + T$. For $B = P_1, \dots, P_4$ the coordinate $t(B^T)$ has degree 6 over $\mathbb{Q}$; for $B = P_1, P_2$ its minimal polynomial is $t^6 + 6t^4 + 24t^3 + 12t^2 + 8$.*

Proof. (a) On the model obtained from Lemma 2.1 as described above, with a as in (B.2), one checks that $b = a^2/2$ in Ξ. Then $j(E_g) = 256(a^2 - 3b)^3/(b^2(a^2 - 4b)) = 128$. The polynomial $X^2 + aX + a^2/2$ has discriminant $-a^2$, which is not a square in Ξ as Ξ has real places, so T is the only point of order 2. Similarly $X^2 - 2aX - a^2$ has discriminant $8a^2$, and 2 is not a square in Ξ by (e), so $E'_g(\Xi)[2] = \{O, T'\}$. The point T is not in $2E_g(\Xi) \subseteq \hat{\varphi}(E'_g(\Xi))$, since $\kappa(T) \equiv 2$ is not a square, so $E_g(\Xi)$ has no point of order 4. The orders $\#E_g(\mathbb{F}_\mathfrak{p})$ at the primes $\mathfrak{p}$ of good reduction above $5, 7, \dots, 23$ have greatest common divisor 4, so $E_g(\Xi)$ has no torsion of odd order.

(b) The element a is an S-unit (its ideal factorization involves only primes in S), so the model has discriminant $-4a^6$, a unit outside S. Hence E_g and E'_g have good reduction outside S, and both Selmer groups lie in $\Xi(S, 2)$ [30, §X.4]. The local images at the primes of S and at the two real places are spanned by images of explicit local points. At each place the two images together reach the order $\#E_g(\Xi_v)/2E_g(\Xi_v) \cdot \#E'_g(\Xi_v)[\hat{\varphi}]/\varphi(E_g(\Xi_v)[2])$ forced by the exact sequence above, which is $4 \cdot 2^{[\Xi_v:\mathbb{Q}_2]}$, 4 and 2 for v above 2, above 3 and real, so they are the full images (as in Section 2.4). Intersecting with $\Xi(S, 2)$ gives the dimensions 5 and 3, and (10.1) gives the bound. Bases of the two Selmer groups, as products of the basis elements of $\Xi(S, 2)$, are listed in (B.5).

(c) The relation holds because the divisors $P_3 + P_4$ and $P_1 + P_2$ are fibers of t, hence linearly equivalent, and $\iota(P_1) = O$. For the bound, the point $R \in E_g(\Xi)$ of (B.3) satisfies $2R = \iota(P_2) + \iota(P_3)$, which is checked by a direct computation in $E_g(\Xi)$. The subgroup $\Omega = \langle T, R, \iota(P_3)\rangle$ has $\dim \kappa(\Omega) = 2$, and the subgroup of $E'_g(\Xi)$ generated by T' and by $\hat{\varphi}$-preimages of the elements of $\Omega \cap \ker \kappa$ has an image of dimension 2 under κ' (both shown by quadratic characters at auxiliary primes). So $\dim \kappa(E_g(\Xi)) \geq 2$ and $\dim \kappa'(E'_g(\Xi)) \geq 2$, and (10.1) gives $\operatorname{rank} E_g(\Xi) \geq 2$.

(d) By (b), $\mathrm{Sel}(\kappa)$ and $\mathrm{Sel}(\kappa')$ are subgroups of $\Xi(S,2)$, and $\Xi(S,2) \to \prod_{i=1}^{3} \Xi_i^\times/\Xi_i^{\times 2}$ is injective (proof of Lemma 10.1).

(e) The local square classes of 2 and -1 are read off from their images in the local bases of Appendix B: 2 is nontrivial at each $\mathfrak{p}_i$, and -1 is trivial at $\mathfrak{p}_1$ and nontrivial at $\mathfrak{p}_2$, $\mathfrak{p}_3$. The roots of $X^2 + aX + a^2/2$ are $a(-1 \pm \sqrt{-1})/2$, so $E_g(\Xi_i)[2]$ has order $4, 2, 2$. The roots of $X^2 - 2aX - a^2$ are $a(1 \pm \sqrt{2})$, so $E'_g(\Xi_i)[2] = \{O, T'\}$. A point Q with $2Q$ of order 2 would be found by taking a preimage under $\hat{\varphi}$ and then under φ, which requires two square roots in Ξ_i. Carrying this out for every point of order 2 of $E_g(\Xi_i)$ and of $E'_g(\Xi_i)$ gives no such Q, so there is no point of order 4. Let $T_1 = (a(-1 + \sqrt{-1})/2, 0) \in E_g(\Xi_1)$. The tuples $(\kappa_i(t_i))_i$ with $t_i \in E_g(\Xi_i)[2]$ form the subgroup of $\prod_i \Xi_i^\times/\Xi_i^{\times 2}$ spanned by the classes of T at each $\mathfrak{p}_i$ and of T_1 at $\mathfrak{p}_1$. This subgroup has dimension 4, and its intersection with $\mathrm{loc}(\mathrm{Sel}(\kappa))$ has dimension 1, so the intersection is $\{(\kappa_i(O))_i, (\kappa_i(T))_i\}$. Likewise the tuples $(\kappa'_i(t'_i))_i$ with $t'_i \in \{O, T'\}$ form a subgroup of dimension 2 (as $\kappa'_1(T') \equiv -1$ is trivial), whose intersection with $\mathrm{loc}'(\mathrm{Sel}(\kappa'))$ has dimension 1. These dimensions are ranks of matrices over $\mathbb{F}_2$ formed from the vectors in Appendix B.

(f) For each of the four points B, the point $\iota(B) + T$ is computed in $E_g(\Xi)$ and mapped back to C_g by the inverse map of Lemma 2.1, and the coordinate t of the image has a minimal polynomial over $\mathbb{Q}$ of degree 6. □

By (b) and (c), $2 \leq \operatorname{rank} E_g(\Xi) \leq 6$. The upper bound is less than $[\Xi : \mathbb{Q}] = 12$, so a Chabauty argument for the points of $C_g(\Xi)$ with $t \in \mathbb{Q}$ is possible in principle, but we do not know generators of a subgroup of finite index in $E_g(\Xi)$. Stoll's method, in the form of the next section, uses (a), (b), (d), (e) and (f), but neither the rank nor (c).

11. Stoll's method at the prime 2

The points of $C_g(\Xi)$ whose coordinate t lies in $\mathbb{Q} \cap (2 + 8\mathbb{Z}_2)$ are the four known points (Theorem 11.11). We prove this by Stoll's form of Chabauty's method at the prime 2 through a 2-isogeny, and then complete the proof of Theorem 1.1(g).

11.1. **Local class sets.** In this section v runs over the three primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ of Ξ above 2. We write v also for the normalized valuation of Ξ_v and $e = e_v = v(2)$. Let $k_2 = \Xi \otimes \mathbb{Q}_2 = \prod_v \Xi_v$, $E_g(k_2) = \prod_v E_g(\Xi_v)$, $E'_g(k_2) = \prod_v E'_g(\Xi_v)$, and $G = \prod_v \Xi_v^\times/\Xi_v^{\times 2}$. Let $\kappa_2 = (\kappa_v)_v : E_g(k_2) \to G$ and $\kappa'_2 = (\kappa'_v)_v : E'_g(k_2) \to G$ (Section 10.3). Put

$$\Sigma = \mathrm{loc}(\mathrm{Sel}(\kappa)), \quad \Sigma' = \mathrm{loc}'(\mathrm{Sel}(\kappa')), \quad b_2 = \kappa_2(T), \quad b'_2 = \kappa'_2(T'),$$

and let $\mathbf{1}$ be the unit element of G. By Proposition 10.3(e), $E_g(\Xi_v)$ and $E'_g(\Xi_v)$ have no point of order 4, so their 2-power torsion is their 2-torsion. Let $\mathcal{T} \subseteq G$ be the set of tuples $(\kappa_v(Q_v))_v$ with $Q_v \in E_g(\Xi_v)[2]$, and $\mathcal{T}'$ the set of tuples $(\kappa'_v(Q'_v))_v$ with $Q'_v \in \{O, T'\}$. In this notation Proposition 10.3(e) states that

$$\Sigma \cap \mathcal{T} = \{\mathbf{1}, b_2\}, \qquad \Sigma' \cap \mathcal{T}' = \{\mathbf{1}, b'_2\}. \tag{11.1}$$

For $A = (A_v)_v \in E_g(k_2)$ let $\nu(A) = \sup\{m \geq 0 : A \in 2^m E_g(k_2)\} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$, and for $m \geq 0$

$$R_m(A) = \prod_v \kappa_v(\{Q \in E_g(\Xi_v) : 2^m Q = A_v\}),$$
$$R'_m(A) = \prod_v \kappa'_v(\{Q' \in E'_g(\Xi_v) : 2^m \hat{\varphi}(Q') = A_v\}),$$

subsets of G (empty if one factor is empty, in particular $R_m(A) = \emptyset$ for $m > \nu(A)$). Put $\mathcal{S}(A) = \bigcup_{m\geq 0} R_m(A)$ and $\mathcal{S}'(A) = \bigcup_{m\geq 0} R'_m(A)$.

Definition 11.1. $A \in E_g(k_2)$ is *admissible* if $\kappa_2(A) = \mathbf{1}$, $\mathcal{S}(A) \cap \Sigma \subseteq \{\mathbf{1}, b_2\}$ and $\mathcal{S}'(A) \cap \Sigma' \subseteq \{\mathbf{1}, b'_2\}$.

For $B \in C_g(\Xi)$ and $P \in C_g(k_2) = \prod_v C_g(\Xi_v)$ we write $\iota_B(P) = \iota(P) - \iota(B) \in E_g(k_2)$.

Theorem 11.2 (Stoll [34, Theorem 2.1])**.** *Let $\mathcal{U} \subseteq C_g(k_2)$ and $B \in C_g(\Xi)$ be such that $\iota_B(P)$ is admissible for every $P \in \mathcal{U}$. If $P \in C_g(\Xi)$ and the image of P in $C_g(k_2)$ lies in $\mathcal{U}$, then $\iota_B(P) \in \{O, T\}$, that is, $P \in \{B, B^T\}$.*

This is [34, Theorem 2.1] for the endomorphism $\psi(Q, Q') = (\hat{\varphi}(Q'), \varphi(Q))$ of $E_g \times E'_g$, whose square is multiplication by 2, as in [34, Remark 2.2], with the set of classes that must be avoided made explicit. In Stoll's terms, we take for his subgroup Γ the kernel $\{O, T\} \times \{O, T'\}$ of ψ, which is the torsion subgroup of $(E_g \times E'_g)(\Xi)$. Indeed $E_g(\Xi)_{\mathrm{tors}} = \{O, T\}$ (Proposition 10.3(a)), and $E'_g(\Xi)$ has no odd torsion, being 2-isogenous to E_g, and no point Q' with $2Q' = T'$: for such a point $\hat{\varphi}(Q')$ would lie in $\{O, T\}$, but $\hat{\varphi}(Q') = O$ would give $Q' \in \{O, T'\}$, and $T \notin \hat{\varphi}E'_g(\Xi)$ because $\kappa(T) \equiv 2$ is not a square. Admissibility of $\iota_B(P)$ for every $P \in \mathcal{U}$, together with (11.1), gives his condition (2). His condition (1) holds because $\mathrm{loc} \times \mathrm{loc}'$ is injective (Proposition 10.3(d)), so that the localization map on the Selmer group has trivial kernel. Stoll states his results for curves of genus at least 2. His argument does not use the genus, and we give it here for C_g, which has genus one.

Proof. Let $\Gamma = \{O, T\} \times \{O, T'\} = \ker \psi$. The map $\tilde{\kappa} = (\kappa, \kappa')$ is injective on $(E_g \times E'_g)(\Xi)/\psi(E_g \times E'_g)(\Xi) = E_g(\Xi)/\hat{\varphi}E'_g(\Xi) \times E'_g(\Xi)/\varphi E_g(\Xi)$, with image in $\mathrm{Sel}(\kappa) \times \mathrm{Sel}(\kappa')$, and $\mathrm{loc} \times \mathrm{loc}'$ is injective (Proposition 10.3(d)).

Local step. Let $P \in \mathcal{U}$, $A = \iota_B(P)$, and let $(Q, Q') \in E_g(k_2) \times E'_g(k_2)$, $n \geq 0$ and $(T_0, T'_0) \in \Gamma$ satisfy $\psi^n(Q, Q') = (A + T_0, T'_0)$. We show: if $\kappa_2(Q) \in \Sigma$ then $\kappa_2(Q) \in \{\mathbf{1}, b_2\}$, and if $\kappa'_2(Q') \in \Sigma'$ then $\kappa'_2(Q') \in \{\mathbf{1}, b'_2\}$. Since $\kappa_2(A) = \mathbf{1}$, $\kappa_v(A_v + T)$ is the class of 2, a non-square in Ξ_v, so $A_v + T \notin \hat{\varphi}E'_g(\Xi_v) \supseteq 2E_g(\Xi_v)$ for every v. If $n = 2m$, then $2^m Q = A + T_0$ and $2^m Q' = T'_0$. So Q' is a 2-power torsion point at every v, and $\kappa'_2(Q') \in \mathcal{T}'$. If $T_0 = O$ then $\kappa_2(Q) \in R_m(A) \subseteq \mathcal{S}(A)$, and if $T_0 = T$ then $m = 0$ and $\kappa_2(Q) = \kappa_2(A + T) = b_2$. If $n = 2m + 1$, then $2^m \hat{\varphi}(Q') = A + T_0$ and $\varphi(2^m Q) = T'_0 \in \ker \hat{\varphi}$, so $2^{m+1} Q = \hat{\varphi}\varphi(2^m Q) = O$ and $\kappa_2(Q) \in \mathcal{T}$. The case $T_0 = T$ is impossible, as $A + T \notin \hat{\varphi}E'_g(k_2)$, and for $T_0 = O$, $\kappa'_2(Q') \in R'_m(A) \subseteq \mathcal{S}'(A)$. The claim follows from admissibility and (11.1).

Global step. Let $P \in C_g(\Xi)$ with image in $\mathcal{U}$, and $\tilde{A} = (\iota_B(P), O) \in (E_g \times E'_g)(\Xi)$. We show by induction that $\tilde{A} \in \Gamma + \psi^n(E_g \times E'_g)(\Xi)$ for all $n \geq 0$. If $\tilde{A} = \gamma_n + \psi^n \tilde{Q}_n$ with $\gamma_n \in \Gamma$ and $\tilde{Q}_n \in (E_g \times E'_g)(\Xi)$, then $\psi^n \tilde{Q}_n = \tilde{A} - \gamma_n$, and the local step applies to the image of $\tilde{Q}_n$ in $E_g(k_2) \times E'_g(k_2)$, whose classes $(\mathrm{loc} \times \mathrm{loc}')(\tilde{\kappa}(\tilde{Q}_n))$ lie in $\Sigma \times \Sigma'$. So they lie in $\{\mathbf{1}, b_2\} \times \{\mathbf{1}, b'_2\} = (\mathrm{loc} \times \mathrm{loc}')(\tilde{\kappa}(\Gamma))$, and by the two injectivities $\tilde{Q}_n = \gamma' + \psi \tilde{Q}_{n+1}$ for some $\gamma' \in \Gamma$ and $\tilde{Q}_{n+1} \in (E_g \times E'_g)(\Xi)$. Then $\tilde{A} = (\gamma_n + \psi^n \gamma') + \psi^{n+1} \tilde{Q}_{n+1}$ with $\gamma_n + \psi^n \gamma' \in \Gamma$ (as $\psi\Gamma = 0$). Since $\psi^2 = [2]$, $\tilde{A}$ lies in the torsion subgroup plus $2^m(E_g \times E'_g)(\Xi)$ for every m.

As $(E_g \times E_g')(\Xi)$ is finitely generated, $\tilde{A}$ is a torsion point. So $\iota_B(P) \in E_g(\Xi)_{\mathrm{tors}} = \{O, T\}$ (Proposition 10.3(a)), and $P = B$ or $P = B^T$ because ι is injective. □

11.2. **Formal groups at the primes above 2.** The model of Proposition 10.3(a) is integral but not minimal at the primes above 2, and the estimates below use a minimal one. Let $E_g^\circ : V^2 = U^3 + a_2U^2 + a_4U + a_6$ be the model of E_g over Ξ obtained from that of Proposition 10.3(a) by the change of coordinates $X = \Theta^2U + \Theta'$, $Y = \Theta^3V$, with $\Theta, \Theta' \in \Xi$ and a_2, a_4, a_6 given in (B.2). Its coefficients are integral at the three primes above 2, and

$$(v(a_2), v(a_4), v(a_6)) = (0, 2, 5),\ (0, 1, 1),\ (0, 0, 0) \quad \text{at } v = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3. \tag{11.2}$$

(It is a global minimal model, with Kodaira types I_0^*, II, II at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, but only (11.2) is used. That a_6 is not a square in $\Xi_{\mathfrak{p}_3}$ is shown in the proof of Lemma 11.3.) We identify $E_g(\Xi_v)$ with $E_g^\circ(\Xi_v)$. Let $\varpi = -U/V$, $\omega = dU/2V$, and for $n \geq 1$ let $E_{g,n}^\circ(\Xi_v)$ be the set consisting of O and the points P with $v(U(P)) < 0$ and $v(\varpi(P)) \geq n$. So $E_{g,1}^\circ(\Xi_v)$ is the kernel of reduction of E_g°, the points of the formal group, and $\log_v : E_{g,1}^\circ(\Xi_v) \to \Xi_v$ denotes the formal logarithm ($d \log_v = \omega$). Let $d_v = 1, 1, 2$ at $v = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$.

Lemma 11.3. (a) *If $P \in E_g(\Xi_v)$, $V(P) \neq 0$ and $v(\varpi(P)) \geq d_v$, then $P \in E_{g,1}^\circ(\Xi_v)$.*

(b) *For $n \geq e + 1$, $\log_v$ is a bijective isometry $E_{g,n}^\circ(\Xi_v) \to \pi_v^n \mathcal{O}_v$; hence $E_{g,n+ke}^\circ(\Xi_v) = 2^k E_{g,n}^\circ(\Xi_v)$ for $k \geq 0$, and $E_{g,(M+2)e+1}^\circ(\Xi_v) \subseteq 2^{M+1} E_g(\Xi_v)$ for $M \geq 0$. The map $\log_v$ is injective on $E_{g,1}^\circ(\Xi_v)$, and $v(\varpi(Q_1 - Q_2)) = v(\varpi(Q_1) - \varpi(Q_2))$ for $Q_1, Q_2 \in E_{g,1}^\circ(\Xi_v)$.*

Proof. (a) Let $P = (U, V) \notin E_{g,1}^\circ(\Xi_v)$, so $v(U) \geq 0$ and then $v(V) \geq 0$. If $U = 0$ then $a_6 = V^2$ is a square in Ξ_v, which is false (below). Otherwise let $\ell = v(U)$. Then $v(\varpi(P)) = \ell - v(V)$, so if $v(\varpi(P)) \geq 1$ then $\ell \geq 1$. Now $2v(V) = v(U^3 + a_2U^2 + a_4U + a_6)$ is at least $\min(3\ell, v(a_2) + 2\ell, v(a_4) + \ell, v(a_6))$, with equality if the minimum is attained once. At $\mathfrak{p}_1$: for $\ell = 1$ the minimum 2 is attained once, so $v(V) = 1 = \ell$; for $\ell = 2, 3$ the minimum is 4, respectively 5, so $v(V) \geq \ell$; for $\ell \geq 4$ the minimum 5 is attained once and is odd, which is impossible. So $v(\varpi(P)) \leq 0$. At $\mathfrak{p}_2$ the minimum $v(a_6) = 1$ is attained once for every $\ell \geq 1$ and is odd: impossible. At $\mathfrak{p}_3$ the minimum 0 is attained once, so $v(V) = 0$ and $v(\varpi(P)) = \ell = v(U(U^2 + a_2U + a_4)) = v(V^2 - a_6)$, as $v(a_4) = 0$. The residue field is $\mathbb{F}_4$, where squaring is bijective. Let $r_0 \in \mathcal{O}_v$ lift the square root of a_6 modulo π_v. Every V with $v(V^2 - a_6) \geq 1$ is $r_0 + \pi_v y_0$ with $y_0 \in \mathcal{O}_v$, and $V^2 \equiv r_0^2 \pmod{\pi_v^2}$ since $v(2) = 2$. One computes $v(r_0^2 - a_6) = 1$, so $v(V^2 - a_6) = 1$ and $v(\varpi(P)) = 1 < d_v$. The same computation shows that a_6 is not a square in Ξ_v at $\mathfrak{p}_3$, and at $\mathfrak{p}_1, \mathfrak{p}_2$ its valuation is odd.

(b) The model is integral at v, so its formal group is defined over $\mathcal{O}_v$ and $\log_v$ has the stated properties for $n > v(2)/(2-1) = e$ [30, Theorem IV.6.4]. The identity $\log_v(2^k Q) = 2^k \log_v(Q)$ gives the second statement, and $E_{g,(M+2)e+1}^\circ(\Xi_v) = 2^{M+1} E_{g,e+1}^\circ(\Xi_v)$. The kernel of $\log_v$ on $E_{g,1}^\circ(\Xi_v)$ is the torsion of the formal group, a 2-group [30, Proposition IV.3.2]. A nonzero point of it would give a point of order 2 in $E_{g,1}^\circ(\Xi_v)$, but points of order 2 have $V = 0$ and U a root of a monic cubic over $\mathcal{O}_v$, hence $v(U) \geq 0$. Finally, the formal group law gives $\varpi(Q_1 - Q_2) = (\varpi(Q_1) - \varpi(Q_2)) \cdot u(\varpi(Q_1), \varpi(Q_2))$, where u is a power series in two variables over $\mathcal{O}_v$ with constant term 1. □

Lemma 11.4 ([34, Lemma 3.1])**.** *Let $A, A' \in E_g(k_2)$ and $M \geq \nu(A)$ an integer with $A' - A \in 2^{M+1} E_g(k_2)$. Then $\nu(A') = \nu(A)$, and $R_m(A') = R_m(A)$ and $R_m'(A') = R_m'(A)$ for all $m \geq 0$; in particular $\kappa_2(A') = \kappa_2(A)$, $\mathcal{S}(A') = \mathcal{S}(A)$ and $\mathcal{S}'(A') = \mathcal{S}'(A)$.*

Proof. Write $A' = A + 2^{M+1}Z$. For $m \leq M$, $Q \mapsto Q + 2^{M+1-m}Z$ is a bijection from the 2^m-th roots of A_v to those of A_v' that preserves κ_v, as $2^{M+1-m}Z \in 2E_g \subseteq \hat{\varphi} E_g'$. Similarly

$Q' \mapsto Q' + \varphi(2^{M-m}Z)$ is a bijection from $\{Q' : 2^m\hat{\varphi}(Q') = A_v\}$ to $\{Q' : 2^m\hat{\varphi}(Q') = A'_v\}$ that preserves κ'_v, which vanishes on φE_g. For $m \geq M+1$, some A_v is not in $2^{M+1}E_g(\Xi_v)$, and then neither is A'_v. So R_m and R'_m are empty for both. The same bijections give $\nu(A') = \nu(A)$. □

Lemma 11.5 ([34, Lemma 3.3])**.** *If $A \in E_g(k_2)$ and $\nu(A) \geq 2$, then $\nu(2A) = \nu(A)+1$, $\mathcal{S}(2A) \subseteq \mathcal{S}(A) \cup \mathcal{T}$ and $\mathcal{S}'(2A) \subseteq \mathcal{S}'(A) \cup \mathcal{T}'$.*

Proof. Write $A = 4A_0$. Fix v. If $2^nQ = 2A_v$ with $n \geq 2$, then $T_0 = 2^{n-1}Q - A_v$ is a 2-torsion point and $T_0 = 2(2^{n-2}Q - 2A_{0,v})$. A nonzero point of order 2 that is twice a point would be twice a point of order 4, so $T_0 = O$ and Q is a 2^{n-1}-th root of A_v. If $n = 1$, then $Q = A_v + T_0$ with $T_0 \in E_g(\Xi_v)[2]$ and $\kappa_v(Q) = \kappa_v(T_0)$, as $\kappa_v(A_v) = 1$. If $n = 0$, $\kappa_v(2A_v) = 1 = \kappa_v(A_v)$. So $R_n(2A) \subseteq R_{n-1}(A)$ for $n \geq 2$, $R_1(2A) \subseteq \mathcal{T}$ and $R_0(2A) = R_0(A)$. On the other side, if $2^n\hat{\varphi}(Q') = 2A_v$ with $n \geq 2$ the same argument shows $2^{n-1}\hat{\varphi}(Q') = A_v$. If $n = 1$, put $Z' = Q' - \varphi(2A_{0,v})$. Then $\hat{\varphi}(Z') = \hat{\varphi}(Q') - A_v$ has order dividing 2, so $\hat{\varphi}(2Z') = O$, $2Z' \in \{O, T'\}$, $4Z' = O$, and $Z' \in E'_g(\Xi_v)[4] = \{O, T'\}$. Hence $Q' \in \varphi(2A_{0,v}) + \{O, T'\}$ and $\kappa'_v(Q') \in \{\kappa'_v(O), \kappa'_v(T')\}$. If $n = 0$, $\hat{\varphi}(Q') = 2A_v = \hat{\varphi}(\varphi(A_v))$ gives $Q' \in \varphi(A_v) + \{O, T'\}$, with the same classes. So $R'_n(2A) \subseteq R'_{n-1}(A)$ for $n \geq 2$ and $R'_1(2A), R'_0(2A) \subseteq \mathcal{T}'$. Finally, if $2A = 2^{\nu(A)+2}Z$ then, as above, $A = 2^{\nu(A)+1}Z$ at every v, which is false. So $\nu(2A) = \nu(A)+1$. □

11.3. **Sheets and charts.** For $t \in 2 + 8\mathbb{Z}_2$ and each v, $v(q(t) - 1) > 2e$: the coefficients of $q(2 + 8s) - 1 \in \Xi[s]$ have valuations at least $10, 5, 5$ at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$. So $q(t)$ has exactly one square root $W_v(t) \in \Xi_v$ with $v(W_v(t)-1) > e$. For $\sigma = (\sigma_v)_v \in \{\pm 1\}^3$ the *sheet* $\mathcal{X}_\sigma \subseteq C_g(k_2)$ is the set of the points

$$P_\sigma(t) = (t, (\sigma_v W_v(t))_v), \qquad t \in 2 + 8\mathbb{Z}_2.$$

A point of $C_g(\Xi)$ with $t \in \mathbb{Q} \cap (2 + 8\mathbb{Z}_2)$ lies on exactly one sheet, and it is enough to treat each of the eight sheets separately. The points P_1 and P_2 lie on $\mathcal{X}_{+++}$ and $\mathcal{X}_{---}$, respectively. The element w_0 of (B.2) satisfies $v(w_0 + 1) > e$ at $\mathfrak{p}_1$ and $\mathfrak{p}_3$ and $v(w_0 - 1) > e$ at $\mathfrak{p}_2$ (the valuations are 10, 5 and 5), so $P_3 \in \mathcal{X}_{-+-}$ and $P_4 \in \mathcal{X}_{+-+}$. Thus the two points with $t = -\frac{10}{3}$ lie on opposite sheets whose signs at $\mathfrak{p}_1$ agree with the sign at exactly one of the other two primes, and with our labels this prime is $\mathfrak{p}_3$.

Charts. To estimate $\iota(P)$ for P on a sheet we express the formal parameter ϖ of $\iota(P) - \iota(B)$, for a known point B, as a rational function of (t, w). For $B = (t_B, w_B) \in C_g(\Xi)$ with $w_B \neq 0$ let $\iota_B^\circ : C_g \to E_g^\circ$ be the isomorphism $P \mapsto \iota(P) - \iota(B)$ followed by the change of model to E_g°. It is obtained from Lemma 2.1 with base point B and an isomorphism onto E_g°, as follows. Let $H_B(u) = u^4 q(t_B + 1/u)/w_B^2 = u^4 + b_B u^3 + c_B u^2 + d_B u + H_B(0)$ and $\mu_B = c_B - b_B^2/4$. Lemma 2.1 maps (t, w), with $u = 1/h$ and $h = t - t_B$, to the point (U_B, V_B) of a model E_B with

$$h^2 U_B = 8Z, \qquad h^3 V_B = 32Z + 8b_B hZ + 16\mu_B h^2 + 8d_B h^3, \qquad Z = \frac{w}{w_B} + 1 + \frac{b_B}{2}h,$$

and $E_B \to E_g^\circ$ is $U_B = \Theta_B^2 U + r_B$, $V_B = \Theta_B^3 V$ with $(\Theta_B, r_B) = (\Theta, \Theta' + U_0)$ for $B = P_1$, $(-\Theta, \Theta' + U_0)$ for $B = P_2$, and $(\pm\Theta_{P_3}, r_{P_3})$ for $B = P_3, P_4$, with Θ_{P_3}, r_{P_3} given in (B.4) (as $\mathrm{Aut}(E_g^\circ, O) = \{\pm 1\}$, the sign of Θ_B decides between $P \mapsto \iota(P) - \iota(B)$ and its negative). Hence

$$\varpi(\iota_B^\circ(t, w)) = -\Theta_B \frac{U_B - r_B}{V_B} = \frac{N_B(t, w)}{M_B(t, w)}, \qquad N_B = n_0 + n_1 w, \quad M_B = d_0 + d_1 w, \quad (11.3)$$

at every point where $M_B \neq 0$, with

$$n_0 = -\Theta_B h(8 + 4b_B h - r_B h^2), \qquad n_1 = -8\Theta_B h/w_B,$$
$$d_0 = 32 + 24b_B h + (16\mu_B + 4b_B^2)h^2 + 8d_B h^3, \qquad d_1 = 8(4 + b_B h)/w_B,$$

polynomials in t of degrees $3, 1, 3, 1$. The differential ω satisfies $(\iota_B^\circ)^*\omega = c\,dt/w$ with $c \in \Xi^\times$ independent of B, as ω is translation invariant and dt/w spans the regular differentials of C_g. On the model of Lemma 2.1 one has $dU/2V = du/4w'$ on $w'^2 = H(u)$ (a direct computation), and with $u = 1/(t-2)$, $w' = wu^2$ for the base point P_1 this gives $c = -\Theta/4$. So $v(c) = v(\Theta) - 2e = -6, -3, -3$ at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, since $v(\Theta) = 2, 1, 1$.

11.4. **Constancy on disks.** The next lemma bounds how far the point $\iota(P_\sigma(t))$ moves as t runs over a disk $t_c + 2^r\mathbb{Z}_2$: Δ bounds the change of $q(t)/q(t_c)$, Δ' that of the square root w, h_f that of a polynomial $f \in \Xi[t]$, and β_N, β_M those of the numerator and the denominator of (11.3). The number b bounds from below the valuation of the change of ϖ, and Lemma 11.3(b) turns it into a statement about divisibility by powers of 2, which Lemma 11.7 uses.

Lemma 11.6. *Let v be a prime above 2, $\sigma \in \{\pm 1\}^3$, $B \in C_g(\Xi)$ with $w_B \neq 0$, and $D = t_c + 2^r\mathbb{Z}_2 \subseteq 2 + 8\mathbb{Z}_2$ with $t_c \in \mathbb{Q}$. Write $w_c = \sigma_v W_v(t_c)$, $N = N_B$, $M = M_B$, $N_c = N(t_c, w_c)$, $M_c = M(t_c, w_c)$, and $\epsilon_i = q^{(i)}(t_c)/(i!\,q(t_c))$ for $1 \leq i \leq 4$. Put*

$$\Delta = \min_i \big(v(\epsilon_i) + i\,e\,r\big), \qquad \Delta' = v(w_c) + \Delta - e, \qquad h_f = \min_{i \geq 1} \big(v(f^{(i)}(t_c)/i!) + i\,e\,r\big)\ (f \in \Xi[t]),$$

$$\beta_N = \min\big(h_{n_0},\, h_{n_1} + v(w_c),\, \min(v(n_1(t_c)), h_{n_1}) + \Delta'\big),$$

and β_M in the same way with d_0, d_1. Assume $\Delta > 2e$, $\beta_M > v(M_c)$, and either $N_c = 0$ or $v(N_c) - v(M_c) \geq d_v$. Let $b = \beta_N - v(M_c)$ if $N_c = 0$ and $b = \min(\beta_N + v(M_c), v(N_c) + \beta_M) - 2v(M_c)$ otherwise, and assume $b \geq d_v$. Then for every $t \in D$ the point $\iota_B^\circ(P_\sigma(t))$ lies in $E^\circ_{g,1}(\Xi_v)$, and $\iota(P_\sigma(t)) - \iota(P_\sigma(t_c)) \in E^\circ_{g,b}(\Xi_v)$.

Proof. Let $t = t_c + h$, so $v(h) \geq er$. Then $q(t)/q(t_c) = 1 + \epsilon(h)$ with $\epsilon(h) = \sum_i \epsilon_i h^i$ and $v(\epsilon(h)) \geq \Delta > 2e$. The quotient $W_v(t)/W_v(t_c)$ is the square root of $1 + \epsilon(h)$ that is congruent to 1 modulo π_v^{e+1}, and for it $v(W_v(t)/W_v(t_c) - 1) = v(\epsilon(h)) - e$. Hence $v(w(t) - w_c) \geq \Delta'$, where $w(t) = \sigma_v W_v(t)$. Writing

$$\begin{aligned} N(t, w(t)) - N_c = {} & \big(n_0(t) - n_0(t_c)\big) + \big(n_1(t) - n_1(t_c)\big)w_c \\ & + \big(n_1(t) - n_1(t_c)\big)(w(t) - w_c) + n_1(t_c)(w(t) - w_c) \end{aligned}$$

and expanding the polynomials at t_c gives $v(N(t, w(t)) - N_c) \geq \beta_N$, and likewise $v(M(t, w(t)) - M_c) \geq \beta_M > v(M_c)$, so $M(t, w(t)) \neq 0$ has valuation $v(M_c)$. Hence

$$\varpi(\iota_B^\circ(P_\sigma(t))) - \varpi(\iota_B^\circ(P_\sigma(t_c))) = \frac{(N - N_c)M_c - N_c(M - M_c)}{M\,M_c}$$

has valuation at least b. As $v(\varpi(\iota_B^\circ(P_\sigma(t_c)))) \geq d_v$ (or $N_c = 0$) and $b \geq d_v$, $v(\varpi(\iota_B^\circ(P_\sigma(t)))) \geq d_v$, and $\iota_B^\circ(P_\sigma(t)) \in E^\circ_{g,1}(\Xi_v)$ by Lemma 11.3(a) (ϖ is finite there, so $V \neq 0$). By Lemma 11.3(b) the difference $\iota_B^\circ(P_\sigma(t)) - \iota_B^\circ(P_\sigma(t_c)) = \iota(P_\sigma(t)) - \iota(P_\sigma(t_c))$ lies in $E^\circ_{g,b}(\Xi_v)$. □

All the estimates in this proof hold coefficientwise for the power series in h involved, that is, they bound Gauss norms on the disk $2^r\mathbb{Z}_2$. In particular $w(t_c + h)$, $N(t_c + h, w(t_c + h))$ and $1/M(t_c + h, w(t_c + h)) = M_c^{-1}\sum_{l \geq 0}(1 - M/M_c)^l$ are power series in h converging on $2^r\mathbb{Z}_2$, and so is $\varpi(\iota_B^\circ(P_\sigma(t_c + h)))$, whose difference with its value at $h = 0$ has Gauss valuation at least b. This is used in the proof of Lemma 11.8.

Lemma 11.7 ([34, Corollary 3.2]). *Let $\sigma \in \{\pm 1\}^3$, $B_0 \in C_g(\Xi)$, $D = t_c + 2^r\mathbb{Z}_2 \subseteq 2 + 8\mathbb{Z}_2$ with $t_c \in \mathbb{Q}$, and $A_c = \iota_{B_0}(P_\sigma(t_c))$ with $\nu(A_c) < \infty$. Suppose that for each v Lemma 11.6 applies to D, σ and some B, with $b = b_v \geq (\nu(A_c)+2)e_v + 1$. Then for every $t \in D$ the point $A = \iota_{B_0}(P_\sigma(t))$ satisfies $\nu(A) = \nu(A_c)$, $\kappa_2(A) = \kappa_2(A_c)$, $\mathcal{S}(A) = \mathcal{S}(A_c)$ and $\mathcal{S}'(A) = \mathcal{S}'(A_c)$. In particular A is admissible if A_c is.*

Proof. $A - A_c = \iota(P_\sigma(t)) - \iota(P_\sigma(t_c))$ lies in $E^\circ_{g,b_v}(\Xi_v) \subseteq 2^{\nu(A_c)+1}E_g(\Xi_v)$ for each v (Lemmas 11.6 and 11.3(b)), and Lemma 11.4 with $M = \nu(A_c)$ gives the claim. □

11.5. **Near a known point.** As P tends to a known point B of its sheet, $\iota_B(P)$ tends to O and $\nu(\iota_B(P))$ grows without bound, so finitely many disks as in Lemma 11.7 cannot cover a neighborhood of B. Near B we use the formal logarithm along the sheet instead, as in [34, Lemmas 3.4 and 3.7].

Lemma 11.8 ([34, Lemmas 3.4 and 3.7]). *Let $B = (t_B, w_B) \in C_g(\Xi)$ with $t_B \in \mathbb{Q} \cap (2+8\mathbb{Z}_2)$ lie on the sheet $\mathcal{X}_\sigma$, let $k_0 \geq 3$, and for $h \in 2^{k_0}\mathbb{Z}_2$ put $A(h) = \iota_B(P_\sigma(t_B + h))$. Write $q(t_B + h)/q(t_B) = 1 + \epsilon(h)$ with $\epsilon(h) = \sum_{i=1}^4 \epsilon_i h^i$, and let $\beta = \min_i v(\epsilon_i)/i$ and $N_0 = \max\{\nu(A(h)) : v_2(h) = k_0\}$. Assume that for each v:*

- (L1) *Lemma 11.6 applies to the disk $t_B + 2^{k_0}\mathbb{Z}_2$ with center t_B, the sign vector σ and some $B' \in C_g(\Xi)$;*
- (L2) *$e\,k_0 + \beta \geq 3e$;*
- (L3) *$v(c/w_B) + e\,k_0 \geq 3e + 1$;*
- (L4) *$v(c/w_B) + 2e\,k_0 + \beta - e \geq (N_0 + 3)e + 1$.*

Then for every $h \in 2^{k_0+1}\mathbb{Z}_2$ (including $h = 0$), $\kappa_2(A(h)) = \mathbf{1}$, $\mathcal{S}(A(h)) \subseteq \mathcal{S}_{k_0} \cup \mathcal{T}$ and $\mathcal{S}'(A(h)) \subseteq \mathcal{S}'_{k_0} \cup \mathcal{T}'$, where $\mathcal{S}_{k_0}$ and $\mathcal{S}'_{k_0}$ are the unions of the sets $\mathcal{S}(A(h'))$, respectively $\mathcal{S}'(A(h'))$, over $v_2(h') = k_0$.

Proof. Fix v. Let $(1+\epsilon(h))^{-1/2} = \sum_{n\geq 0}\rho_n h^n$. Since $\rho_n = \sum_{l=1}^n \binom{-1/2}{l}[h^n]\epsilon(h)^l$ for $n \geq 1$, $v_2\binom{-1/2}{l} = s_2(l) - 2l \geq 1 - 2l$ (s_2 the binary digit sum), and each coefficient of $\epsilon(h)^l$ at h^n has valuation at least $n\beta$, we have $v(\rho_n) \geq e(1-2n) + n\beta$ for $n \geq 1$. With $v_2(n) \leq n-1$ and (L2) this gives, for $n \geq 2$ and $k \geq k_0$,

$$v(\rho_{n-1}) - e\,v_2(n) + (n-1)e\,k \geq e + (n-1)(e\,k + \beta - 3e) > 0, \tag{11.4}$$

$$\Lambda_k := \min_{n\geq 2}\left(v(c/w_B) + v(\rho_{n-1}) + e - e\,v_2(n) + n\,e\,k\right) \geq v(c/w_B) + 2e\,k + \beta - e. \tag{11.5}$$

The logarithm along the sheet. By (L1) and Lemma 11.6, for $h \in 2^{k_0}\mathbb{Z}_2$ both $\iota^\circ_{B'}(P_\sigma(t_B+h))$ and $A(h) = \iota^\circ_{B'}(P_\sigma(t_B+h)) - \iota^\circ_{B'}(P_\sigma(t_B))$ lie in $E^\circ_{g,1}(\Xi_v)$. The function $w(t_B+h) = \sigma_v W_v(t_B+h) = w_B(1+\epsilon(h))^{1/2}$ is a power series in h convergent on $2^{k_0}\mathbb{Z}_2$ (the Gauss valuation of $\epsilon(h)$ there exceeds $2e$), and by the remark after Lemma 11.6 so is $\Phi(h) = \varpi(\iota^\circ_{B'}(P_\sigma(t_B+h)))$, with Gauss valuation at least $d_v \geq 1$. Hence $\Psi(h) = \log_v(\iota^\circ_{B'}(P_\sigma(t_B+h)))$ is a power series convergent on $2^{k_0}\mathbb{Z}_2$ (the coefficient of ϖ^n in the formal logarithm lies in $n^{-1}\mathcal{O}_v$, as ω has coefficients in $\mathcal{O}_v$). Indeed, the n-th term of the formal logarithm, evaluated at $\Phi(h)$, has Gauss valuation at least $n\,d_v - v(n) \geq n - e\,v_2(n)$, which tends to infinity with n, so these terms converge to a power series in h that converges on the disk. As a composition of the formal logarithm with the convergent power series Φ, Ψ may be differentiated termwise, and by the chain rule $\Psi'(h)\,dh$ is the pull-back of $\omega = d\log_v$ along $h \mapsto \iota^\circ_{B'}(P_\sigma(t_B+h))$, that is, of $(\iota^\circ_{B'})^*\omega = c\,dt/w$. Along the sheet $dt = dh$ and $1/w = w_B^{-1}(1+\epsilon(h))^{-1/2}$, so

$\Psi'(h) = (c/w_B)\sum_n \rho_n h^n$ at every point of the disk. The difference of these two power series converges on the disk and has infinitely many zeros, so it is zero by Strassmann's theorem. Hence $\Psi' = (c/w_B)\sum_n \rho_n h^n$ coefficientwise, and since $\log_v$ is a homomorphism on $E^\circ_{g,1}(\Xi_v)$,

$$\log_v(A(h)) = \Psi(h) - \Psi(0) = \frac{c}{w_B}\sum_{n\geq 1}\rho_{n-1}\frac{h^n}{n}.$$

Annuli. Let $v_2(h) = k \geq k_0$. By (11.4) the term $n = 1$ dominates, so $v(\log_v(A(h))) = v(c/w_B) + ek \geq 3e+1$ by (L3). By Lemma 11.3(b), $A(h) \in E^\circ_{g,3e+1}(\Xi_v) = 4\,E^\circ_{g,e+1}(\Xi_v)$, so $\nu(A(h)) \geq 2$ and $\kappa_2(A(h)) = \mathbf{1}$. Next,

$$\log_v(2A(h)) - \log_v(A(2h)) = \frac{c}{w_B}\sum_{n\geq 2}\rho_{n-1}(2-2^n)\frac{h^n}{n}$$

has valuation at least Λ_k, as $v(2-2^n) = e$. Let $N_k = \max\{\nu(A(h)) : v_2(h) = k\}$, so that $N_{k_0} = N_0$. If $\Lambda_k \geq (N_k+3)e+1$ at every v, then $2A(h) - A(2h) \in E^\circ_{g,(N_k+3)e+1}(\Xi_v) \subseteq 2^{N_k+2}E_g(\Xi_v)$ at every v (Lemma 11.3(b); both points lie in $E^\circ_{g,e+1}(\Xi_v)$), so $2A(h) - A(2h) \in 2^{\nu(A(h))+2}E_g(k_2)$, and Lemma 11.5 and Lemma 11.4 (with $M = \nu(2A(h)) = \nu(A(h))+1$) give $\nu(A(2h)) = \nu(A(h))+1$, $\mathcal{S}(A(2h)) = \mathcal{S}(2A(h)) \subseteq \mathcal{S}(A(h))\cup\mathcal{T}$ and $\mathcal{S}'(A(2h)) \subseteq \mathcal{S}'(A(h))\cup\mathcal{T}'$. As $h \mapsto 2h$ maps the annulus $v_2(h) = k$ onto $v_2(h) = k+1$, $N_{k+1} = N_k + 1$, while the bound (11.5) grows by $2e$. So, starting from (L4) at $k = k_0$, induction on k gives $\Lambda_k \geq (N_k+3)e+1$ for all $k \geq k_0$ and the inclusions for all h with $v_2(h) > k_0$. For $h = 0$, $A(0) = O$, and $\mathcal{S}(O) \subseteq \mathcal{T}$, $\mathcal{S}'(O) \subseteq \mathcal{T}'$, because the points Q with $2^mQ = O$ and Q' with $2^m\hat{\varphi}(Q') = O$ are 2-power torsion points. □

11.6. **The computation, and the proof of Theorem 1.1(g).** For each of the eight sheets $\mathcal{X}_\sigma$ we fix a base point $B(\sigma) \in \{P_1,\dots,P_4\}$: on the four sheets that contain a known point, $B(\sigma)$ is that point (P_1, P_2, P_3, P_4 on $\mathcal{X}_{+++}, \mathcal{X}_{---}, \mathcal{X}_{-+-}, \mathcal{X}_{+-+}$, respectively); on the other four, $B(\sigma) = P_1$ if $\sigma_{\mathfrak{p}_1} = +1$ (the sheets $\mathcal{X}_{++-}$, $\mathcal{X}_{+--}$) and $B(\sigma) = P_2$ if $\sigma_{\mathfrak{p}_1} = -1$ (the sheets $\mathcal{X}_{-++}$, $\mathcal{X}_{--+}$). In Lemma 11.6 we always use, at the prime v, the chart $\iota^\circ_{P_1}$ if $\sigma_v = +1$ and $\iota^\circ_{P_2}$ if $\sigma_v = -1$.

Proposition 11.9. (a) *Let $\mathcal{X}_\sigma$ contain the known point $B = B(\sigma)$. For $3 \leq k \leq 8$ the annulus $\{t \in 2+8\mathbb{Z}_2 : v_2(t-t_B) = k\}$ is the union of four disks $t_c + 2^{k+3}\mathbb{Z}_2$ with $t_c \in \mathbb{Q}$. For each of these 24 disks, $A_c = \iota_B(P_\sigma(t_c))$ is admissible, $\nu(A_c) = k-2$, and Lemma 11.6 applies with $b = (b_{\mathfrak{p}_1}, b_{\mathfrak{p}_2}, b_{\mathfrak{p}_3}) = (4k+2,\ 2k+1,\ 2k+1)$, which is at least $\big((\nu(A_c)+2)e_v+1\big)_v = (4k+1,\ 2k+1,\ 2k+1)$.*

(b) *Let $\mathcal{X}_\sigma$ contain no known point. For each of the eight disks $2+8u+2^6\mathbb{Z}_2$ $(0 \leq u \leq 7)$, $A_c = \iota_{B(\sigma)}(P_\sigma(t_c))$ with $t_c = 2+8u$ is admissible, $\nu(A_c) = 1$, and Lemma 11.6 applies with $b = (14,7,7) \geq (13,7,7)$.*

(c) *At each of the four known points B, with its sheet and $k_0 = 8$, the hypotheses of Lemma 11.8 hold: $N_0 = 6$ by (a) and Lemma 11.7; $v(c/w_B) = -6,-3,-3$ and $\beta = -2,-1,-1$ at $\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3$; Lemma 11.6 applies to $t_B + 2^8\mathbb{Z}_2$ with $b = 22,11,11$, the center being mapped to O or to a point with $v(\varpi) = 10,5,5$; and*

$$ek_0 + \beta - 3e = 18,9,9 \geq 0, \qquad v(c/w_B) + ek_0 = 26,13,13 \geq 3e+1 = 13,7,7,$$
$$v(c/w_B) + 2ek_0 + \beta - e = 52,26,26 \geq (N_0+3)e+1 = 37,19,19.$$

The admissibility statements in (a) and (b) are finite computations. For each center t_c and each prime v we compute the point $A_{c,v} \in E_g(\Xi_v)$. Then, for $m = 1,2,\dots$, we compute

the points Q with $2^m Q = A_{c,v}$, obtained from those for $m-1$ by taking all preimages under $\hat{\varphi}$ and then under φ (each preimage needs a square root in Ξ_v), and the preimages under $\hat{\varphi}$ of these points. We stop at the first m for which some prime has no such Q, and this m is $\nu(A_c)+1$. The classes κ_v and κ'_v of these points give the sets $R_m(A_c)$ and $R'_m(A_c)$, which we compare with Σ and Σ' by linear algebra over $\mathbb{F}_2$ in the coordinates of Appendix B. Local points are computed with explicit 2-adic precision, and square classes are read off from global approximations as in Appendix C.2. The outcome has the same shape at all 128 centers (Table 6): $R_0(A_c) = \{\mathbf{1}\}$, and $R'_0(A_c)$ has 4 elements and meets Σ' in $\{\mathbf{1}, b'_2\}$. For $1 \le m < \nu(A_c)$, $R_m(A_c)$ has 16 elements and meets Σ in $\{\mathbf{1}, b_2\}$, and $R'_m(A_c)$ has 4 elements and meets Σ' in $\{\mathbf{1}, b'_2\}$. For $m = \nu(A_c)$, $R_m(A_c)$ has 16 elements, none of them in Σ, and $R'_m(A_c)$ is empty. Appendix B gives these sets for one disk in full.

Remark 11.10. The admissibility test detects global points: if $\iota_B(Q)$ were admissible for every Q on a sheet $\mathcal{X}_\sigma$ that contains a known point $B' \neq B$, Theorem 11.2 would give $B' \in \{B, B^T\}$, which is false by Proposition 10.3(f). So, with B as base point, the test must fail somewhere on $\mathcal{X}_\sigma$. On each of the four sheets that contain a known point, the test with each of the other three known points as base point indeed fails. In all twelve cases it fails at $t = 78/7$, among other values.

Theorem 11.11. *The points $P \in C_g(\Xi)$ with $t(P) \in \mathbb{Q} \cap (2+8\mathbb{Z}_2)$ are exactly P_1, P_2, P_3, P_4.*

Proof. Let P be such a point, $\mathcal{X}_\sigma$ the sheet containing its image in $C_g(k_2)$, and $B = B(\sigma)$. We show that $\iota_B(Q)$ is admissible for every $Q \in \mathcal{X}_\sigma$. If $\mathcal{X}_\sigma$ contains no known point, the eight disks of Proposition 11.9(b) cover $2+8\mathbb{Z}_2$, and Lemma 11.7 carries admissibility from each center to its disk. If $\mathcal{X}_\sigma$ contains B, then $t_B \in 2+8\mathbb{Z}_2$, so every $t \in 2+8\mathbb{Z}_2$ has $v_2(t-t_B) \ge 3$. The 24 disks of Proposition 11.9(a) cover the points with $3 \le v_2(t-t_B) \le 8$, and Lemma 11.7 applies to them. For $v_2(t-t_B) \ge 9$, Lemma 11.8 with $k_0 = 8$ (Proposition 11.9(c)) gives $\kappa_2(\iota_B(Q)) = \mathbf{1}$ and $\mathcal{S}(\iota_B(Q)) \subseteq \mathcal{S}_8 \cup \mathcal{T}$, $\mathcal{S}'(\iota_B(Q)) \subseteq \mathcal{S}'_8 \cup \mathcal{T}'$, where $\mathcal{S}_8$, $\mathcal{S}'_8$ are the unions of the sets of the four disks with $k = 8$. By Proposition 11.9(a) and Lemma 11.7 these meet Σ, Σ' only in $\{\mathbf{1}, b_2\}$, $\{\mathbf{1}, b'_2\}$, and so do $\mathcal{T}$, $\mathcal{T}'$ by (11.1). So $\iota_B(Q)$ is admissible.

Theorem 11.2, applied with $\mathcal{U} = \mathcal{X}_\sigma$, gives $P \in \{B, B^T\}$. The coordinate $t(B^T)$ is irrational (Proposition 10.3(f)), so $P = B$. In particular $\mathcal{X}_\sigma$ is one of the four sheets that contain a known point. □

Proof of Theorem 1.1(g). Let (x, y, z) be a primitive solution of (9.1). By Lemma 9.1, $j \in \{0, 1\}$ in (9.2). If $j = 0$, Proposition 9.3 gives $(x, y, z) = (\pm 1, 0, -1)$. If $j = 1$, Lemmas 9.4 and 10.1 give a point $(t, w) \in C_g(\Xi)$ with $t = m/n \in \mathbb{Q} \cap (2+8\mathbb{Z}_2)$, where m, n are the coprime integers of Lemma 9.2, with $\mu = \frac{1}{2}$. By Theorem 11.11, $t \in \{2, -\frac{10}{3}\}$. For $t = 2$, Lemma 9.2 gives $(y, z) = (6, -9)$, which gives no primitive solution as $\gcd(y, z) = 3$, and for $t = -\frac{10}{3}$ it gives $(y, z) = (-6202, 4199)$, and then $x^4 = -3y^3 - z^3 = 3 \cdot 6202^3 - 4199^3 = 895^4$, so $x = \pm 895$. Conversely, $(\pm 1, 0, -1)$ and $(\pm 895, -6202, 4199)$ are primitive solutions. □

Appendix A. Class groups and units

For each field $K = \mathbb{Q}[x]/(P)$ below, the ring of integers is the one computed by PARI's `nfinit`, and PARI's `nfcertify` reports no unproved step. For all but two of the polynomials in the table the polynomial discriminant equals d_K, so $\mathcal{O}_K = \mathbb{Z}[x]$. (The two exceptions are $x^3 - 12$, of index 2, and $y^6 + 6y^4 + 12y^2 - 4$, of index 8. For $x^3 - 12$ the ring $\mathbb{Z}[\phi, \psi]$, with $\phi = \sqrt[3]{12}$ and $\psi = \phi^2/2$, contains $\mathbb{Z}[\phi]$ and $\mathbb{Z}[\psi]$, which are maximal at 3 and at 2 by Eisenstein's criterion.) Every prime ideal of norm at most the Minkowski bound M_K is

principal, with the generator listed. Each generator was checked by comparing Hermite normal forms of ideals. So $\mathrm{Cl}(K) = 1$ in each case.

field	d_K	M_K	prime ideals of norm $\le M_K$: norm, generator
$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$	8, 12, -3, 5	< 2	none
L: $\omega^3 + 3\omega - 2$	$-2^3 3^3$	4.16	2: ω; 2: $1-\omega$; 3: $\omega^2+\omega+3$
$\mathbb{Q}(\sqrt[3]{2})$: $\theta^3 - 2$	$-2^2 3^3$	2.94	2: θ
$\mathbb{Q}(\sqrt[3]{12})$: $\phi^3 - 12$	$-2^2 3^5$	8.82	2: $\psi+\phi+2$; 3: $\psi+\phi+3$; 5: $2\psi+2\phi+5$
$\mathbb{Q}(\sqrt[3]{3})$: $\chi^3 - 3$	-243	4.41	2: $\chi-1$; 3: χ; 4: $\chi^2+\chi+1$
K_2: $\nu^5 + 5\nu^3 + 5\nu - 2$	$2^6 5^5$	27.84	2: ν; 4: $\nu^3+2\nu-1$; 3: $-\nu^4-5\nu^2-\nu-5$; 5: ν^2+1; 7: $-\nu^2-3$; 11: $-\nu^4-3\nu^2-\nu+1$; 13: $\nu+1$; 17: $\nu^4+\nu^3+5\nu^2+4\nu+5$; 23: $\nu^3-\nu^2+2\nu-1$
K_3: $u^5 - 5u^3 + 5u - 4$	$2^4 3^2 5^5$	41.76	2: $u-2$; 4: $-u^2-u+1$; 3: $u-1$; 9: $u^4-u^3-3u^2+2u-1$; 5: $u+1$; 7: u^4-4u^2-2u+3; 13: $-u^2+3$; 17: $-u^3-u^2+u-1$; 23: u^3-u^2-3u+1; 31: $u^4-u^3-3u^2+u+1$; 37: $u^4-u^3-4u^2+4u-1$; 41: u^3-u^2-2u+1
$y^6 - 2y^3 - 1$	$2^9 3^6$	15.28	2: $y-1$; 4: y^2+y+1; 9: y^4+y^3-2y-1
$y^6 + 6y^4 + 12y^2 - 4$	$2^{10} 3^{10}$	194.5	36 prime ideals, all principal (Table 5)

For the sextic field $M = \mathbb{Q}[y]/(y^6 - 3y^2 + 6)$ ($d_M = -2^9 3^7$, signature $(0,3)$, $M_M = 33.7$), let $\mathfrak{p}_0 = (2, -\frac{1}{4}y^5 + \frac{1}{2}y^4 - \frac{1}{4}y^3 - \frac{1}{2}y - 1)$, a prime above 2. Then $\mathfrak{p}_0^2 = (\frac{1}{4}y^4 - \frac{1}{2}y^3 + \frac{1}{4}y^2 - \frac{1}{2})$ is principal, and each of the 10 prime ideals of norm at most M_M (three above 2, one above 3 and six above 29) is $\mathfrak{p}_0$ times a principal ideal. Explicitly, the ideals $(\gamma)\mathfrak{p}_0^{-1}$ for the following elements γ, grouped by the norm of $(\gamma)\mathfrak{p}_0^{-1}$ (the norm of γ is twice that),

norm 2: $\frac{1}{4}(y^4 - 2y^3 + y^2 - 2)$; $\frac{1}{2}(-y^4 - y^2 + 4)$; $\frac{1}{4}(-y^5 - y^3 + 2y^2 + 2y + 4)$
norm 3: $\frac{1}{4}(-y^5 - y^3 - 2y^2 + 2y)$
norm 29: $\frac{1}{4}(-2y^5 - y^4 - 4y^3 - y^2 + 4y + 2)$; $\frac{1}{4}(y^5 + y^3 + 2y^2 - 2y - 8)$; $\frac{1}{4}(-y^5 + 2y^4 - y^3 + 6y - 4)$; $\frac{1}{4}(y^5 + 2y^4 + y^3 + 4y^2 + 2y - 4)$; $\frac{1}{4}(y^4 + 2y^3 - 3y^2 - 2)$; $\frac{1}{4}(-y^5 - y^3 - 2y^2 + 2y - 8)$

are these ten prime ideals, each once, and $(\gamma)\mathfrak{p}_0^{-1} = \mathfrak{p}_0 \cdot (\gamma)\mathfrak{p}_0^{-2}$ with $\mathfrak{p}_0^2$ principal. Hence $\mathrm{Cl}(M)$ is generated by the class of $\mathfrak{p}_0$ and has order dividing 2, and the S-class group for S containing the primes above 2 is trivial, which is what the descent for E_1 in Section 8 needs.

For the field $\Xi = \mathbb{Q}[\xi]/(f_{12})$ of Section 10, of degree 12, the ring of integers is the one computed by PARI's `nfinit`, and `nfcertify` reports no unproved step. Its discriminant is $d_\Xi = -2^{14} 3^{21}$, while $\mathrm{disc}(f_{12}) = -2^{38} 3^{21} 17^2$. Minkowski's bound is

$$M_\Xi = \frac{12!}{12^{12}} \Big(\frac{4}{\pi}\Big)^5 \sqrt{|d_\Xi|} = 2353.399\ldots$$

Each of the 348 prime ideals of norm at most 2353 is principal: for each, an element of Ξ was found whose principal ideal has the same Hermite normal form as the prime ideal. So $\mathrm{Cl}(\Xi) = 1$. The 348 generators are too many to print, and they are listed in the deposit [21], where a short program checks them.

Units. The units used are $1+\sqrt{2}$ and $2+\sqrt{3}$ (fundamental units), $\tau = (1+\sqrt{5})/2$, $\eta_L = -\omega^2 - \omega + 1 \in L$, $\eta_f = \theta - 1 \in \mathbb{Q}(\sqrt[3]{2})$, $\eta_e = 1 + 3\phi - 3\psi \in \mathbb{Q}(\sqrt[3]{12})$ and $\eta_g = \chi^2 - 2 \in \mathbb{Q}(\sqrt[3]{3})$. For each of the four cubic units $\eta \in \{\eta_L, \eta_f, \eta_e, \eta_g\}$ we use only that neither η nor $-\eta$ is a square, shown by quadratic non-residues modulo small primes or by the sign at the real

place (Sections 6, 7 and 9). Since each of these fields has unit rank 1 and roots of unity ±1, it follows that $\eta = \pm\eta_0^k$ with k odd for a fundamental unit η_0, so that $\pm1, \pm\eta$ represent the units modulo squares and η^j $(0 \le j \le 3)$ represent the units of norm 1 modulo fourth powers. For K_2 and K_3, and for $\mathbb{Q}(\sqrt{5})$, the bases of $K(S,2)$ consist of -1, the units and the generators of the primes in S proposed by PARI. They are checked to be S-units by factorization and to be independent modulo squares by quadratic characters at auxiliary primes, and their number is $r_1 + r_2 + \#S$.

norm	generator	norm	generator
2	$-y^5 - 2y^4 - \frac{9}{2}y^3 - 3y^2 + y + 1$	53	$-\frac{1}{2}y^5 - 3y^3 - 7y - 1$
3	$\frac{1}{2}y^5 + \frac{1}{2}y^4 + \frac{7}{2}y^3 + 2y^2 + 9y + 4$	53	$-\frac{1}{2}y^5 - 3y^3 - 7y + 1$
3	$\frac{1}{2}y^5 + y^3 - 2y^2 - y + 1$	79	$-\frac{1}{2}y^5 + \frac{1}{2}y^4 - 3y^3 + 3y^2 - 7y + 5$
5	$\frac{3}{2}y^4 + \frac{3}{2}y^3 + 5y^2 - y - 2$	79	$-\frac{1}{2}y^5 - \frac{1}{2}y^4 - 3y^3 - 3y^2 - 7y - 5$
5	$-\frac{3}{2}y^5 - y^4 - 9y^3 - 6y^2 - 20y - 11$	83	$\frac{3}{2}y^5 + 2y^4 + \frac{11}{2}y^3 + y^2 - 2y$
25	$-\frac{1}{2}y^5 - \frac{1}{2}y^4 - \frac{7}{2}y^3 - 3y^2 - 8y - 8$	83	$-\frac{1}{2}y^5 - y^4 - 3y^3 - 3y^2 - 10y - 1$
25	$\frac{1}{2}y^4 + y^3 + 2y^2 + y - 1$	97	$y^5 - \frac{1}{2}y^4 + 6y^3 - 4y^2 + 14y - 11$
121	$y^2 + 1$	97	$-\frac{1}{2}y^5 - y^4 - \frac{5}{2}y^3 - 2y^2 - y$
13	$-\frac{1}{2}y^5 + \frac{3}{2}y^4 + \frac{1}{2}y^3 + 7y^2 - 2$	107	$-\frac{1}{2}y^3 + y^2 - 3y + 2$
13	$\frac{1}{2}y^5 + 2y^3 + y^2 + 3y - 1$	107	$\frac{1}{2}y^3 + y^2 + 3y + 2$
169	$-\frac{1}{2}y^4 - 3y^2 - 5$	131	$\frac{1}{2}y^5 + \frac{1}{2}y^4 + 2y^3 + y^2 + 2y + 1$
169	$-\frac{1}{2}y^4 - y^2 + 1$	131	$-\frac{1}{2}y^5 + \frac{1}{2}y^4 - 2y^3 + y^2 - 2y + 1$
17	$3y^5 + y^4 + 19y^3 + 7y^2 + 41y + 17$	137	$\frac{1}{2}y^5 + 3y^3 + y^2 + 7y + 3$
17	$\frac{1}{2}y^5 + \frac{1}{2}y^4 + \frac{5}{2}y^3 + 2y - 2$	137	$-\frac{1}{2}y^5 - 3y^3 + y^2 - 7y + 3$
19	$\frac{1}{2}y^3 + y + 2$	179	$-y^3 - 2y - 1$
19	$\frac{1}{2}y^3 + y - 2$	179	$-y^3 - 2y + 1$
47	$\frac{1}{2}y^3 + y^2 + 2y + 2$	191	$-\frac{1}{2}y^5 + \frac{1}{2}y^4 - 3y^3 + y^2 - 4y - 1$
47	$-\frac{1}{2}y^3 + y^2 - 2y + 2$	191	$\frac{1}{2}y^5 + \frac{1}{2}y^4 + 3y^3 + y^2 + 4y - 1$

TABLE 5. Generators of the 36 prime ideals of norm at most 194 of $\mathbb{Q}[y]/(y^6 + 6y^4 + 12y^2 - 4)$.

APPENDIX B. DATA FOR EQUATION (G)

We print here the data of Sections 10 and 11 from which the statements there can be checked. Elements of $\Xi = \mathbb{Q}[\xi]/(f_{12})$ are written in the power basis of ξ.

B.1. **The covering and the model of E_g.** The chosen mixed pair consists of the roots of $g_2 = t^2 - st + p$, where

$$\begin{aligned} s = \tfrac{1}{136}\big(&457\xi^{11} - 2304\xi^{10} + 5947\xi^9 - 8595\xi^8 \\ &+ 11535\xi^7 - 23575\xi^6 + 42726\xi^5 - 38169\xi^4 \\ &+ 3160\xi^3 + 20506\xi^2 - 12360\xi + 2170\big) \\ p = \tfrac{1}{136}\big(&694\xi^{11} - 3609\xi^{10} + 9575\xi^9 - 14346\xi^8 \\ &+ 19181\xi^7 - 37836\xi^6 + 69869\xi^5 - 66629\xi^4 \\ &+ 10724\xi^3 + 34448\xi^2 - 24150\xi + 4666\big) \end{aligned} \tag{B.1}$$

The minimal polynomial of s is $x^{12} - 12x^{11} + 102x^{10} - 556x^9 + \cdots + 63436$, not f_{12}. Then $g_4 = g/g_2$ and $q = g_4/g_4(2)$. The element a of Proposition 10.3(a), the change of coordinates

$X = \Theta^2 U + \Theta'$, $Y = \Theta^3 V$ to the model E_g° of Section 11.2, the coefficients of E_g°, and the square root w_0 of $q(-\frac{10}{3})$ that defines P_3 are

$$\begin{aligned}
a &= \tfrac{1}{68}\big(-113\xi^{11} + 792\xi^{10} - 2507\xi^9 + 4603\xi^8 \\
&\quad - 6079\xi^7 + 10239\xi^6 - 20534\xi^5 + 26345\xi^4 \\
&\quad - 12880\xi^3 - 7594\xi^2 + 10968\xi - 3450\big) \\
\Theta &= \tfrac{1}{136}\big(-542\xi^{11} + 2899\xi^{10} - 7851\xi^9 + 12148\xi^8 \\
&\quad - 16261\xi^7 + 31378\xi^6 - 58281\xi^5 + 58773\xi^4 \\
&\quad - 13836\xi^3 - 26660\xi^2 + 21574\xi - 4482\big) \\
\Theta' &= \tfrac{1}{17}\big(-338\xi^{11} + 1726\xi^{10} - 4485\xi^9 + 6555\xi^8 \\
&\quad - 8764\xi^7 + 17795\xi^6 - 32407\xi^5 + 29482\xi^4 \\
&\quad - 3194\xi^3 - 15542\xi^2 + 9708\xi - 1626\big) \\
a_2 &= \tfrac{1}{136}\big(281\xi^{11} - 1617\xi^{10} + 4612\xi^9 - 7571\xi^8 \\
&\quad + 10134\xi^7 - 18565\xi^6 + 35567\xi^5 - 39116\xi^4 \\
&\quad + 13796\xi^3 + 14534\xi^2 - 14998\xi + 4600\big) \\
a_4 &= \tfrac{1}{136}\big(268713\xi^{11} - 1501365\xi^{10} + 4216994\xi^9 - 6856181\xi^8 \\
&\quad + 9252872\xi^7 - 17116727\xi^6 + 32127941\xi^5 - 35048062\xi^4 \\
&\quad + 12024876\xi^3 + 13214826\xi^2 - 14097066\xi + 3970332\big) \\
a_6 &= \tfrac{1}{136}\big(24178892\xi^{11} - 135274441\xi^{10} + 380450015\xi^9 \\
&\quad - 619868164\xi^8 + 837882197\xi^7 - 1548437818\xi^6 \\
&\quad + 2905797855\xi^5 - 3180113559\xi^4 + 1114967096\xi^3 \\
&\quad + 1163494356\xi^2 - 1257547122\xi + 355214614\big) \\
w_0 &= \tfrac{1}{918}\big(2352\xi^{11} - 14253\xi^{10} + 41982\xi^9 - 71710\xi^8 \\
&\quad + 95190\xi^7 - 168856\xi^6 + 327864\xi^5 - 384579\xi^4 \\
&\quad + 152530\xi^3 + 143128\xi^2 - 161004\xi + 43980\big)
\end{aligned} \tag{B.2}$$

Here Θ is the constant of the chart of P_1 in Section 11.3, and replacing Θ by $-\Theta$ gives the same model E_g°. The point R of the proof of Proposition 10.3(c), with $2R = \iota(P_2) + \iota(P_3)$, is

$$\begin{aligned}
X(R) &= \tfrac{1}{68}\big(-583\xi^{11} + 2740\xi^{10} - 6153\xi^9 + 7251\xi^8 \\
&\quad - 9217\xi^7 + 25119\xi^6 - 41442\xi^5 + 22549\xi^4 \\
&\quad + 18508\xi^3 - 13250\xi^2 - 8256\xi + 6054\big) \\
Y(R) &= \tfrac{1}{68}\big(693\xi^{11} + 5796\xi^{10} - 25387\xi^9 + 61095\xi^8 \\
&\quad - 61335\xi^7 + 109811\xi^6 - 263388\xi^5 + 416373\xi^4 \\
&\quad - 215360\xi^3 - 9954\xi^2 + 12204\xi + 11718\big)
\end{aligned} \tag{B.3}$$

The charts of Section 11.3 for $B = P_3$ and $B = P_4$ use the constants $\pm\Theta_{P_3}$ and r_{P_3}, where

$$\begin{aligned}
\Theta_{P_3} &= \tfrac{1}{121720}\big(142488\xi^{11} - 815211\xi^{10} + 2308761\xi^9 \\
&\quad - 3783006\xi^8 + 5039235\xi^7 - 9300348\xi^6 \\
&\quad + 17647749\xi^5 - 19469619\xi^4 + 6521364\xi^3 \\
&\quad + 7612272\xi^2 - 7784694\xi + 1845774\big) \\
r_{P_3} &= \tfrac{1}{27234850}\big(-68637402\xi^{11} + 409814154\xi^{10} - 1194330042\xi^9 \\
&\quad + 2023358697\xi^8 - 2690941338\xi^7 + 4829697441\xi^6 \\
&\quad - 9281987478\xi^5 + 10765657431\xi^4 - 4145102694\xi^3 \\
&\quad - 3900207618\xi^2 + 4479011316\xi - 1119258558\big)
\end{aligned} \tag{B.4}$$

and those for P_1 and P_2 use $\pm\Theta$ and $\Theta' + U_0$, with U_0 the root in Ξ of the 2-division cubic of the model given by Lemma 2.1 (Section 10.3).

B.2. **The S-unit basis and the Selmer groups.** Together with -1, the following elements form a basis of $\Xi(S,2)$: π_1, π_2, π_3 generate the primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ above 2 (with $(e,f) = (4,1),(2,2),(2,2)$), π_4, π_5 the primes above 3 (with $(e,f) = (6,1),(3,2)$), and $u_1, \dots, u_6$ are units.

$$\begin{aligned}
\pi_1 &= \tfrac{1}{136}\big(247\xi^{11} - 1362\xi^{10} + 3813\xi^9 - 6177\xi^8 + 8417\xi^7 - 15573\xi^6 \\
&\quad + 29090\xi^5 - 31585\xi^4 + 11212\xi^3 + 11270\xi^2 - 12312\xi + 3682\big) \\
\pi_2 &= \tfrac{1}{136}\big(-192\xi^{11} + 1023\xi^{10} - 2719\xi^9 + 4106\xi^8 - 5409\xi^7 + 10788\xi^6 \\
&\quad - 19971\xi^5 + 19183\xi^4 - 3048\xi^3 - 9544\xi^2 + 6602\xi - 1222\big) \\
\pi_3 &= \tfrac{1}{136}\big(-199\xi^{11} + 1085\xi^{10} - 2976\xi^9 + 4683\xi^8 - 6270\xi^7 + 11941\xi^6 \\
&\quad - 22325\xi^5 + 23096\xi^4 - 6268\xi^3 - 9870\xi^2 + 8698\xi - 2008\big) \\
\pi_4 &= \tfrac{1}{136}\big(-218\xi^{11} + 1297\xi^{10} - 3795\xi^9 + 6492\xi^8 - 8777\xi^7 + 15634\xi^6 \\
&\quad - 29749\xi^5 + 34907\xi^4 - 15008\xi^3 - 10852\xi^2 + 14630\xi - 4734\big) \\
\pi_5 &= \tfrac{1}{8}\big(-\xi^{11} + 6\xi^{10} - 17\xi^9 + 27\xi^8 - 33\xi^7 + 63\xi^6 \\
&\quad - 128\xi^5 + 135\xi^4 - 16\xi^3 - 82\xi^2 + 36\xi + 2\big) \\
u_1 &= \xi - 1 \\
u_2 &= \tfrac{1}{136}\big(-120\xi^{11} + 633\xi^{10} - 1727\xi^9 + 2698\xi^8 - 3693\xi^7 + 6972\xi^6 \\
&\quad - 12875\xi^5 + 13241\xi^4 - 3860\xi^3 - 5472\xi^2 + 5210\xi - 1346\big) \\
u_3 &= \tfrac{1}{136}\big(-163\xi^{11} + 839\xi^{10} - 2242\xi^9 + 3435\xi^8 - 4732\xi^7 + 9149\xi^6 \\
&\quad - 16567\xi^5 + 16538\xi^4 - 4396\xi^3 - 6678\xi^2 + 6166\xi - 1628\big) \\
u_4 &= \tfrac{1}{136}\big(-56\xi^{11} + 343\xi^{10} - 951\xi^9 + 1522\xi^8 - 1873\xi^7 + 3716\xi^6 \\
&\quad - 7187\xi^5 + 7487\xi^4 - 1280\xi^3 - 3696\xi^2 + 2522\xi - 406\big) \\
u_5 &= \tfrac{1}{136}\big(253\xi^{11} - 1335\xi^{10} + 3618\xi^9 - 5603\xi^8 + 7608\xi^7 - 14565\xi^6 \\
&\quad + 26933\xi^5 - 27306\xi^4 + 7172\xi^3 + 11598\xi^2 - 9810\xi + 2068\big) \\
u_6 &= \tfrac{1}{136}\big(-231\xi^{11} + 1281\xi^{10} - 3568\xi^9 + 5713\xi^8 - 7622\xi^7 + 14283\xi^6 \\
&\quad - 26937\xi^5 + 28778\xi^4 - 8408\xi^3 - 12050\xi^2 + 10994\xi - 2444\big)
\end{aligned}$$

In terms of this basis,

$$\mathrm{Sel}(\kappa) = \langle \pi_5,\ -u_1,\ u_2u_5,\ u_3u_4u_5,\ u_6\rangle, \qquad \mathrm{Sel}(\kappa') = \langle \pi_5u_2u_5,\ u_3u_4u_5,\ -1\rangle, \tag{B.5}$$

and modulo squares $b \equiv 2 \equiv u_2u_3u_4$ and $a^2 - 4b \equiv -1$, which lie in $\mathrm{Sel}(\kappa)$ and $\mathrm{Sel}(\kappa')$, respectively.

For $v = \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ the classes of the following elements form a basis of $\Xi_v^\times/\Xi_v^{\times 2}$, which has dimension $2 + [\Xi_v : \mathbb{Q}_2] = 6$:

$$\begin{aligned}
\mathfrak{p}_1:&\ \ \pi_1,\ 3,\ \xi,\ \xi+1,\ \xi-1,\ \xi-2\\
\mathfrak{p}_2:&\ \ \pi_2,\ -1,\ \xi,\ \xi+1,\ \xi^2+\xi-1,\ \xi^2-\xi+1\\
\mathfrak{p}_3:&\ \ \pi_3,\ -1,\ \xi,\ \xi+1,\ \xi^2+\xi-1,\ \xi^2-\xi+1
\end{aligned}$$

We write an element of $G = \prod_v \Xi_v^\times/\Xi_v^{\times 2}$ as three blocks of six exponents on these bases, in the order $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$. The images of the basis of $\Xi(S, 2)$ are

π_1	100000 011111 000010	π_5	000000 010011 010011	u_4	100011 011011 000010
π_2	100101 100000 000111	u_1	000010 010100 011100	u_5	000000 011010 000110
π_3	100101 011011 100000	u_2	010000 011001 000101	u_6	001101 010011 010000
π_4	010110 000110 011101	u_3	001101 001101 011100	-1	000000 010000 010000

a matrix of rank 12. So the map from $\Xi(S, 2)$ to G is injective, as used in the proof of Lemma 10.1. The groups $\Sigma = \mathrm{loc}(\mathrm{Sel}(\kappa))$ and $\Sigma' = \mathrm{loc}'(\mathrm{Sel}(\kappa'))$ are spanned by the images of the bases in (B.5):

π_5	000000 010011 010011	$\pi_5u_2u_5$	010000 010000 010000
$-u_1$	000010 000100 001100	$u_3u_4u_5$	101110 001100 011000
u_2u_5	010000 000011 000011	-1	000000 010000 010000
$u_3u_4u_5$	101110 001100 011000		
u_6	001101 010011 010000		

The classes $b_2 = \kappa_2(T)$ and $b_2' = \kappa_2'(T')$, and the classes at $\mathfrak{p}_1$ of the other two points of order 2, $T_1 = (a(-1+\sqrt{-1})/2, 0)$, for a fixed choice of $\sqrt{-1}$ in Ξ_1, and $T_1 + T$, are

$$b_2 = 111110\,001111\,011011, \qquad b_2' = 000000\,010000\,010000,$$
$$\kappa_{\mathfrak{p}_1}(T_1) = 100011, \qquad \kappa_{\mathfrak{p}_1}(T_1 + T) = 011101.$$

The classes of T at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are the three blocks of b_2. With these vectors, the statements of Proposition 10.3(e) about Σ and Σ' are ranks of matrices over $\mathbb{F}_2$.

B.3. **The covering of the sheets.** Table 6 lists the 128 disks $t_c + 2^r\mathbb{Z}_2$ of Proposition 11.9: for the four sheets that contain a known point, the four disks of each annulus $v_2(t - t_B) = k$ ($3 \le k \le 8$), and for the other four sheets the eight disks $2 + 8u + 2^6\mathbb{Z}_2$. At every center the sets $R_m(A_c)$ and $R_m'(A_c)$ have the shape described after Proposition 11.9.

One disk in full. Take the sheet $\mathcal{X}_{+++}$, its base point P_1, and the disk $18 + 2^7\mathbb{Z}_2$ in the annulus $v_2(t - 2) = 4$. The table below gives, for $m = 0, 1, 2$ and each prime v, the classes $\kappa_v(Q)$ of the points $Q \in E_g(\Xi_v)$ with $2^mQ = A_{c,v}$ and the classes $\kappa_v'(Q')$ of the points $Q' \in E_g'(\Xi_v)$ with $2^m\hat{\varphi}(Q') = A_{c,v}$, as exponent vectors on the local bases of $\Xi_v^\times/\Xi_v^{\times 2}$ given in Appendix B.2. The columns are the primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, in this order, and each entry is a vector of six exponents on the basis at that prime. Here $A_c = \iota_{P_1}(P_{+++}(18))$, with the center $t_c = 18$.

sheets (base points)	k	centers t_c	r	$\nu(A_c)$	b
$\mathcal{X}_{+++}$ (P_1), $\mathcal{X}_{---}$ (P_2), $\mathcal{X}_{-+-}$ (P_3), $\mathcal{X}_{+-+}$ (P_4)	3	10, 26, 42, 58	6	1	$(14,7,7)$
$\mathcal{X}_{+++}$ (P_1), $\mathcal{X}_{---}$ (P_2)	4	18, 50, 82, 114	7	2	$(18,9,9)$
$\mathcal{X}_{-+-}$ (P_3), $\mathcal{X}_{+-+}$ (P_4)	4	2, 34, 66, 98	7	2	$(18,9,9)$
$\mathcal{X}_{+++}$ (P_1), $\mathcal{X}_{---}$ (P_2)	5	34, 98, 162, 226	8	3	$(22,11,11)$
$\mathcal{X}_{-+-}$ (P_3), $\mathcal{X}_{+-+}$ (P_4)	5	50, 114, 178, 242	8	3	$(22,11,11)$
$\mathcal{X}_{+++}$ (P_1), $\mathcal{X}_{---}$ (P_2)	6	66, 194, 322, 450	9	4	$(26,13,13)$
$\mathcal{X}_{-+-}$ (P_3), $\mathcal{X}_{+-+}$ (P_4)	6	18, 146, 274, 402	9	4	$(26,13,13)$
$\mathcal{X}_{+++}$ (P_1), $\mathcal{X}_{---}$ (P_2)	7	130, 386, 642, 898	10	5	$(30,15,15)$
$\mathcal{X}_{-+-}$ (P_3), $\mathcal{X}_{+-+}$ (P_4)	7	210, 466, 722, 978	10	5	$(30,15,15)$
$\mathcal{X}_{+++}$ (P_1), $\mathcal{X}_{---}$ (P_2)	8	258, 770, 1282, 1794	11	6	$(34,17,17)$
$\mathcal{X}_{-+-}$ (P_3), $\mathcal{X}_{+-+}$ (P_4)	8	$\frac{758}{3}$, $\frac{2294}{3}$, $\frac{3830}{3}$, $\frac{5366}{3}$	11	6	$(34,17,17)$
$\mathcal{X}_{++-}$ (P_1), $\mathcal{X}_{+--}$ (P_1), $\mathcal{X}_{-++}$ (P_2), $\mathcal{X}_{--+}$ (P_2)	–	2, 10, 18, 26, 34, 42, 50, 58	6	1	$(14,7,7)$

TABLE 6. The disks of Proposition 11.9: the sheets and their base points $B(\sigma)$, the index k of the annulus (for the sheets with a known point), the centers t_c, the radius exponent r, the number $\nu(A_c)$ of Section 11.1, and the bound $b = (b_{\mathfrak{p}_1}, b_{\mathfrak{p}_2}, b_{\mathfrak{p}_3})$ of Lemma 11.6.

m		$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$
0	$\kappa_v(Q)$	000000	000000	000000
	$\kappa'_v(Q')$	000000	000000, 010000	000000, 010000
1	$\kappa_v(Q)$	000000, 011101, 100011, 111110	000000, 001111	000000, 011011
	$\kappa'_v(Q')$	000000	000000, 010000	000000, 010000
2	$\kappa_v(Q)$	000010, 011111, 100001, 111100	010011, 011100	001011, 010000
	$\kappa'_v(Q')$	(none)	(none)	(none)

For $m = 3$ some prime has no point Q with $8Q = A_{c,v}$, so $\nu(A_c) = 2$. By the table, $R_0(A_c) = \{\mathbf{1}\}$, and $R'_0(A_c)$ consists of the four tuples $(\mathbf{1}, \epsilon_2, \epsilon_3)$ with $\epsilon_2, \epsilon_3 \in \{000000, 010000\}$. Of these, only $\mathbf{1}$ and b'_2 lie in Σ'. The set $R_1(A_c)$ has 16 elements, of which $\mathbf{1}$ and b_2 lie in Σ, and $R'_1(A_c) = R'_0(A_c)$. The set $R_2(A_c)$ has 16 elements, none in Σ, and $R'_2(A_c)$ is empty. So A_c is admissible, and as Lemma 11.6 gives $b = (18,9,9) \geq \big((\nu(A_c)+2)e_v + 1\big)_v = (17,9,9)$, Lemma 11.7 extends this to the whole disk.

APPENDIX C. COMPUTATIONS

Every computation on which the proofs depend was carried out twice, by two sets of programs. The *first programs* give the results stated in the text, and the *second programs*, described in Appendix C.3, repeat them with separately written code.

C.1. **List of computational statements.** Table 7 lists the statements that rest on machine computation. The computations used PARI/GP 2.17.3 [24] and Python 3.12 with SymPy, NumPy and python-flint. Each takes at most a few minutes on one core of a laptop, and the whole of Proposition 11.9 about six minutes. The deposit [21] contains the programs and their outputs, with the commands that run them statement by statement. It also contains the computations behind Remark 9.5.

Exactness and precision. All arithmetic on which the proofs rest is exact: integers, rationals, number fields given by explicit polynomials, finite fields, and p-adic numbers with

statement	what is computed
Section 3	the forms $F_{D,k}$, $G_{D,k}$, irreducibility and Galois groups
Proposition 4.1	the two elliptic curves over $\mathbb{Q}$, descents via 2-isogeny, torsion
Lemmas 4.2, 4.3 and 4.4	congruences (as a check of the hand arguments), the conic and the resultants, the local sets at 2, 3, 5
Proposition 4.5	$\mathrm{Sel}^2(J/\mathbb{Q})$, the numbers $\#J(\mathbb{F}_p)$
Lemma 4.6, the classes δ	the local images at 2, 3, 5 and at the real places
Proposition 4.7	ranks and torsion of $\Gamma^{(-5)}$, $\Gamma^{(1)}$, saturation, sieve, $\mathcal{J}/11$
Proposition 5.3, Remark 5.4	the fields, the S-unit bases, the local images, the sets of classes δ
Proposition 5.5	the class for $(2,1)$, $E_{2,1}$, X, P_1, R, the isogeny descent, saturation, the sieve and $\mathcal{J}/751$
Propositions 6.1, 6.2 and 6.3	$Y^2 = X^3 - 24X$ over $\mathbb{Q}$, the quotient Q' and E', the descent over $\mathbb{Q}(\sqrt{2})$, the field L, the 2-adic elimination
Section 7	the units, the 2-adic classes, the conics, the quartics $c\,q(X)$
Proposition 8.1	models, torsion, 2-descents, generators, saturation, sieves, $\mathcal{J}/p$
Section 9, the field K_g	$\mathcal{O}_{K_g}$, the primes above 2 and 3, η_g modulo $(5, \chi - 2)$
Lemma 9.1	fourth-power classes modulo 16 at $\mathfrak{q}_1$ and $\mathfrak{q}_2$
Lemma 9.2	the conics, their parametrizations, the quartic forms
Proposition 9.3	E_0, torsion, the 2-descent, the generators, saturation, the sieve, the matrices $\mathcal{J}/61$
Lemma 9.4	the disks of $2\mathbb{Z}_2$ and the square classes of $\pm\frac{1}{2}\delta_1(t,1)$ at $\mathfrak{q}_1, \mathfrak{q}_2$
Section 10, Lemma 10.1	Ξ, its subfields and primes, $g = g_2 g_4$, the resultant, the class of $g_2(t)$ on $2 + 8\mathbb{Z}_2$, the injectivity of $\Xi(S,2)$ at 2
Proposition 10.3	the model and $b = a^2/2$, torsion, the local images and the Selmer groups, rank $E_g(\Xi) \geq 2$, the local square classes and the local torsion, $t(B^T)$
Sections 11.2 and 11.3	(11.2), $v(r_0^2 - a_6) = 1$, the sheets and the signs of the known points, the charts (11.3), $v(c)$
Proposition 11.9	the points Q with $2^m Q = A_{c,v}$ and their classes at the 128 centers, the bounds of Lemma 11.6, the hypotheses of Lemma 11.8, the test with other base points
Proof of Theorem 1.1(g)	the solutions from $t = 0, \infty, 2, -\frac{10}{3}$
Appendix A	maximal orders, Minkowski bounds, generators
Appendix B	the data printed there, the class sets of the 128 disks in the coordinates used there

TABLE 7. The computational statements.

tracked precision. Local square classes are determined exactly from residues modulo p^n, with the bounds of Section 2.1. In the Chabauty steps, g_i is embedded in $\mathbb{Q}_p$ and $N \cdot g_i$ is computed there with tracked p-adic precision, enough that each entry of $\mathcal{J}$ is known modulo p^2, which suffices for the remark after Lemma 2.3. Signs at the real places are evaluated numerically in the first programs. The proofs use the sign arguments in the text instead.

The kept sets of Lemma 4.4. For the three pairs (γ, λ) that remain in Lemma 4.4, $(-15, 1)$, $(-15, -5)$ and $(15, -5)$, the kept sets of the proof have the following sizes. At $p = 2$ they consist of 32 classes on which the conditions hold for $(-15, 1)$, and of 10880 such classes and 65536 unresolved ones for $\lambda = -5$. At $p = 3$ they consist of 14760 classes on which the conditions hold and 13122 unresolved ones, in all three cases. At $p = 5$ they consist

of 130208 such classes and 62500 unresolved ones for $(-15, 1)$, and of 26040 and 62500 for $\lambda = -5$.

C.2. **The 2-adic computations for equation (g).** The completions Ξ_v are represented as $\mathbb{Q}_2[\xi]/(f_{12,v})$, where $f_{12,v}$ is the factor of f_{12} over $\mathbb{Q}_2$ that belongs to v. Here e is the ramification index of Ξ_v, and a digit is a power of a uniformizer of Ξ_v. Every local quantity is carried with the precision that PARI attaches to it. For a square root computed by Newton's method this precision leaves out the truncation error of the iteration, which is at most $5e+8$ digits. The second programs (Appendix C.3) track this error, and in every square class the precision they reach exceeds the required one by at least 518 digits. A square class of a local element α is read off only when α is known modulo $\mathfrak{p}^{v(\alpha)+2e+2}$, one digit more than Section 2.1 requires. Then any element of Ξ that approximates it to that precision has the same square class (Section 2.1), and the class of that global element is computed exactly, by discrete logarithms in $(\mathcal{O}_\Xi/\mathfrak{p}^{2e+1})^\times$. A local element is taken to be zero only when all its computed digits vanish (at least 200 of them are known). In the computation of Proposition 11.9 this happens only at the center $t_c = 2$, which is the center of one of the disks on each of the six sheets other than $\mathcal{X}_{+++}$ and $\mathcal{X}_{---}$ (on those two, $t = 2$ is the base point). There the point $P_\sigma(2)$ is, at each prime v, exactly the global point P_1 or P_2, and each element taken to be zero is exactly zero: it is a coordinate of a sum $Q + (-Q)$ that arises in computing A_c (for instance $\iota^\circ_{P_3}(P_1) + \iota(P_3) = \iota(P_1) = O$), or the coordinate $X = 0$ of T or T' among the points Q with $2^m Q = A_{c,v}$ at a prime where $A_{c,v} = O$ (all these points have order dividing 2), or the value N_c in Lemma 11.6 of the numerator of (11.3), which is exactly 0 because the chart used at v has base point $P_\sigma(2)$. At every other center no element is zero to the working precision, so every decision there is made from known digits.

The number fields K_g and Ξ, the points and the coefficients of the charts are exact. The quantities $v(c)$, $v(w_B)$, β and the bounds of Lemma 11.6 are computed from exact elements of Ξ, except w_c, N_c and M_c, which are local and are used only with a precision exceeding their valuations by at least 50 digits.

C.3. **The second programs.** The second programs share with the first only the definitions in the text, and their results agree with those of the first in every case. They were written in the same research process as the first (see the Declarations) and in the same systems, PARI/GP and Python, and none of the computations has been repeated in another computer algebra system. The second programs compute the local images through other parametrizations of the primitive pairs and through Hilbert symbols, and the images at the real places exactly by interval analysis. They contain their own descents: a full 2-descent over $\mathbb{Q}(\sqrt{5})$ for each of the 32 curves Γ_δ with $\gamma = \pm 15$, $r = r_\pm$ and $\delta \in \tau\langle -1, 2, 3\rangle$ (Lemma 4.6); a 2-descent on the Jacobian J of Proposition 4.5 that computes no class group, using the basis $-1, \tau, 2, 3, \sqrt{5}$ of $\mathbb{Q}(\sqrt{5})(S, 2)$; and, for the curves of Section 8, descents via 2-isogeny and, for E_2, a full 2-descent. They compute saturation, sieves and the matrices $\mathcal{J}/p$ with their own group law, point counts and evaluation of X on the reductions.

For equation (g) the second programs compute the unit classes of Lemma 9.1 by explicit arithmetic in $\mathbb{Z}_2$ and $\mathbb{Z}_2[\zeta_3]$ modulo 16 and the disks of Lemma 9.4 by their own recursion. They treat the class $j = 0$ with their own 2-descent over K_g, their own sieve modulo 120 and a Chabauty criterion at the prime 11, and they recover the solutions. They find generators of all 348 prime ideals of Ξ of norm at most 2353 by lattice reduction in the ideal lattices, without `bnfinit`, and check them by their norms and membership. They recompute the invariants of Ξ; Lemma 10.1, with square classes computed by Hilbert symbols; both Selmer

groups of Proposition 10.3, by Hilbert symbols, and their equality with the groups used in Proposition 11.9; the torsion of $E_g(\Xi)$, $\operatorname{rank} E_g(\Xi) \geq 2$ and the images of the known points; and the local 2-torsion facts and the injectivity of loc and loc$'$, with their own square test. For Section 11 they check (11.2) and Lemma 11.3(a) by a Newton-polygon argument, and the quartic-to-Weierstrass maps and the charts as symbolic identities. They recompute all 128 disks, the points Q with $2^m Q = A_{c,v}$ and the bounds with their own local arithmetic: square classes by discrete logarithms modulo $\mathfrak{p}^{2e+2}$, local minimal models by Tate's algorithm at each prime, without `bnfinit`, and the precision of every local quantity tracked rigorously, including the error of square roots obtained by Newton's method. They also check the hypotheses of Lemma 11.8, the logarithm identity in its proof numerically at sample points, and the covering of the sheets by the disks, by exact measure.

The deposit also contains a second proof of Proposition 4.5 by elliptic Chabauty over $\mathbb{Q}(\sqrt{5})$ at the prime 19, the sieve and the Chabauty step of Proposition 5.5 repeated at the prime 1151, and those of Proposition 8.1 repeated at a second prime for each curve.

C.4. **Data availability.** The programs, their inputs and their outputs, with the commands that run them, and a check of every explicit formula printed in this paper, are deposited at [21].

Declarations

Research methodology. The author designed and operated the multi-agent research system used in this work, built on Anthropic Claude Opus 5.5. The system carried out literature analysis, mathematical development and computation, with checks assigned to agents separate from those developing the arguments.

Funding. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interests. The author declares no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process. Anthropic Claude Opus 5.5 was used to draft and revise the manuscript. The author reviewed the material and takes full responsibility for the article.

References

1. Jamal Agbanwa, *Primitive integer solutions of* $3Y^3 + Z^3 = X^4$, 2026, Manuscript (source dated 10 July 2026, uploaded 17 July 2026), GitHub repository `JAgbanwa/PolynomialDiophantineEquations`, commit `8962594` (18 July 2026), https://github.com/JAgbanwa/PolynomialDiophantineEquations/tree/8962594f9c6154ab34b250883ba92a021862f959/primitive_solutions_3y3_plus_z3_equals_x4, accessed 29 September 2026.
2. Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng, *The Diophantine equation* $A^4 + 2^\delta B^2 = C^n$, Int. J. Number Theory **6** (2010), no. 2, 311–338, https://doi.org/10.1142/S1793042110002971.
3. David Brown, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, Int. Math. Res. Not. IMRN (2012), no. 2, 423–436, https://doi.org/10.1093/imrn/rnr022.
4. Nils Bruin, *The Diophantine equations* $x^2 \pm y^4 = \pm z^6$ *and* $x^2 + y^8 = z^3$, Compositio Math. **118** (1999), no. 3, 305–321, https://doi.org/10.1023/A:1001529706709.
5. ———, *On powers as sums of two cubes*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 169–184, https://doi.org/10.1007/10722028_9.

6. ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49, https://doi.org/10.1515/crll.2003.076.
7. ———, *The primitive solutions to* $x^3 + y^9 = z^2$, J. Number Theory **111** (2005), no. 1, 179–189, https://doi.org/10.1016/j.jnt.2004.11.008.
8. Nils Bruin and E. Victor Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347, https://doi.org/10.1090/S0002-9947-05-03954-1.
9. Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, https://doi.org/10.1090/S0025-5718-09-02255-8.
10. ———, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, https://doi.org/10.1112/S1461157009000187.
11. Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885, https://doi.org/10.2140/ant.2008.2.859.
12. Henri Darmon and Andrew Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543, https://doi.org/10.1112/blms/27.6.513.
13. Luis Dieulefait and Jorge Jiménez Urroz, *Solving Fermat-type equations via modular* $\mathbb{Q}$*-curves over polyquadratic fields*, J. Reine Angew. Math. **633** (2009), 183–195, https://doi.org/10.1515/CRELLE.2009.064.
14. E. Victor Flynn, *The Hasse principle and the Brauer–Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466, https://doi.org/10.1007/s00229-004-0502-9.
15. E. Victor Flynn and Joseph L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533, https://doi.org/10.1007/s002290050215.
16. ———, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205, https://doi.org/10.4064/aa98-2-9.
17. Nuno Freitas, Bartosz Naskręcki, and Michael Stoll, *The generalized Fermat equation with exponents 2, 3,* n, Compos. Math. **156** (2020), no. 1, 77–113, https://doi.org/10.1112/S0010437X19007693.
18. Bogdan Grechuk, *Polynomial Diophantine equations: a systematic approach*, Springer, Cham, 2024, https://doi.org/10.1007/978-3-031-62949-5.
19. ———, *A systematic approach to Diophantine equations: open problems*, 2026, arXiv:2404.08518v9, 30 August 2026.
20. ———, *What are the primitive solutions to* $3y^3 + z^3 = x^4$*?*, 2026, MathOverflow question 513113, 10 July 2026, https://mathoverflow.net/q/513113, with an answer by S. Y. Xiao.
21. Manvir Jaswal, *Programs and data for "The primitive solutions of seven small generalized Fermat equations"*, 2026, Zenodo, https://doi.org/10.5281/zenodo.23055562.
22. Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502, https://doi.org/10.1007/BF01394256.
23. Ariel Pacetti and Lucas Villagra Torcomian, $\mathbb{Q}$*-curves, Hecke characters and some Diophantine equations*, Math. Comp. **91** (2022), no. 338, 2817–2865, https://doi.org/10.1090/mcom/3759.
24. The PARI Group, *PARI/GP version 2.17.3*, Univ. Bordeaux, 2025, https://pari.math.u-bordeaux.fr/.
25. Ashleigh Ratcliffe and Bogdan Grechuk, *Generalized Fermat equation: a survey of solved cases*, Expo. Math. **43** (2025), no. 4, Paper No. 125688, https://doi.org/10.1016/j.exmath.2025.125688; arXiv:2412.11933v2.
26. Edward F. Schaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232, https://doi.org/10.1006/jnth.1995.1044.
27. ———, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114, https://doi.org/10.1006/jnth.1996.0006.
28. Victor Scharaschkin, *Local-global problems and the Brauer–Manin obstruction*, Ph.D. thesis, University of Michigan, 1999.
29. Samir Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793, https://doi.org/10.2140/ant.2013.7.765.
30. Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Grad. Texts in Math., vol. 106, Springer, New York, 2009, https://doi.org/10.1007/978-0-387-09494-6.
31. Denis Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7–17, https://doi.org/10.1112/S1461157000000668.
32. Gustaf Söderlund, *The primitive solutions to the Diophantine equation* $2X^4 + Y^4 = Z^3$, Notes Number Theory Discrete Math. **23** (2017), no. 2, 36–44.

33. Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, https://doi.org/10.4064/aa98-3-4.
34. ———, *Chabauty without the Mordell–Weil group*, Algorithmic and experimental methods in algebra, geometry, and number theory (Gebhard Böckle, Wolfram Decker, and Gunter Malle, eds.), Springer, Cham, 2017, pp. 623–663, https://doi.org/10.1007/978-3-319-70566-8_28; arXiv:1506.04286v2, whose numbering we use.
35. Ashleigh Wilcox, *A systematic approach to Diophantine equations: two thousand solved examples*, 2024, arXiv:2404.08719v2.

Toronto, Canada
Email address: manvirjaswal@icloud.com