THE GENERALIZED FERMAT EQUATION $x^2 + y^5 = z^9$

MANVIR JASWAL

Abstract. We show that the equation $x^2 + y^5 = z^9$ has no solution in coprime nonzero integers. Equivalently, none of the equations $x^2+y^5 = z^9$, $x^2+y^9 = z^5$ and $x^5+y^9 = z^2$ has such a solution. By Edwards' parametrization of the coprime solutions of $a^2 + b^3 + c^5 = 0$, a solution gives coprime integers u, v at which one of 27 binary forms g_i of degree 20 takes the value $-z^3$. A 2-adic argument and a descent modulo cubes over number fields of degree at most 10 exclude 22 of the 27 forms and, for each of the other five, determine the values of the factors of g_i up to cubes. These five forms lead to rational points on an elliptic curve over $\mathbb{Q}$, on a curve of genus 2 over $\mathbb{Q}$, and on elliptic curves over $\mathbb{Q}(\sqrt[3]{5})$ and over $\mathbb{Q}(\sqrt{-5})$. We determine the relevant points by a 2-descent over $\mathbb{Q}$, by elliptic Chabauty over a cubic field together with a Mordell–Weil sieve, by a descent via 3-isogeny over $\mathbb{Q}(\sqrt[3]{5})$, and by elliptic Chabauty over $\mathbb{Q}(\sqrt{-5})$. No step assumes the generalized Riemann hypothesis.

Contents

1. Introduction 1
2. Edwards' parametrization 5
3. Descent modulo cubes 7
4. Eighteen forms without Edwards triples 9
5. The nine remaining forms 11
6. Form 3 14
7. Forms 1 and 20 15
8. Form 2 21
9. Form 4 23
10. Proof of Theorem 1.1 26
Appendix A. Class groups 26
Appendix B. Computations 27
Declarations 29
References 29

1. Introduction

1.1. **The equation.** For integers $p, q, r \geq 2$ the *generalized Fermat equation* of signature (p, q, r) is

$$x^p + y^q = z^r, \qquad \gcd(x, y, z) = 1.$$

A solution is *trivial* if $xyz = 0$. When $1/p+1/q+1/r < 1$, Darmon and Granville [12] proved that there are only finitely many solutions, and the Fermat–Catalan conjecture predicts that,

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

Key words and phrases. Generalized Fermat equation, Fermat–Catalan conjecture, Edwards' parametrization, descent, elliptic Chabauty, Mordell–Weil sieve.

taken over all such signatures together, there are only finitely many nontrivial solutions in positive integers (counting $1 + 2^3 = 3^2$ once); see [2] and the survey [27]. This paper concerns the signature $(2, 5, 9)$, for which $1/2 + 1/5 + 1/9 = 73/90 < 1$.

Ratcliffe and Grechuk [27, §1.1] list $(2, 5, 9)$ and $(2, 3, 25)$ as the only signatures whose exponents are not all prime that remained to be considered. A composite exponent can often be replaced by one of its prime factors: if $r = st$, a solution of $x^p + y^q = z^r$ gives the solution (x, y, z^s) of $x^p + y^q = z^t$. For these two signatures this does not help, since replacing 9 by 3, or 25 by 5, gives the spherical signature $(2, 5, 3)$ or $(2, 3, 5)$, whose equation has infinitely many coprime solutions. By the computer search of Ratcliffe and Grechuk [27, Proposition 1.3], none of the equations $x^2 + y^5 = z^9$, $x^2 + y^9 = z^5$ and $x^5 + y^9 = z^2$ has a solution in coprime positive integers whose right-hand side is at most 2^{100}. Some special cases follow from signatures that have been solved. By a result of Bennett, Chen, Dahmen and Yazdani [1, Proposition 19], $a^2 + b^{2n} = c^9$ has no solution in nonzero coprime integers for $n \geq 2$, so with $n = 5$ there is no nontrivial solution of $x^2 + y^5 = z^9$ in which y is a positive square. By [1, Proposition 13], $a^2 + b^5 = c^6$ has no solution in nonzero coprime integers, so there is none in which z is a square, since $z = w^2$ gives $z^9 = (w^3)^6$.

Theorem 1.1. *The solutions of*

$$x^2 + y^5 = z^9, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x, y, z) = 1, \tag{1.1}$$

are exactly $(\pm 1, -1, 0)$, $(\pm 1, 0, 1)$, $(0, 1, 1)$ *and* $(0, -1, -1)$. *In particular* (1.1) *has no solution with* $xyz \neq 0$.

Since 5 and 9 are odd, a solution of any one of

$$x^2 + y^5 = z^9, \qquad x^2 + y^9 = z^5, \qquad x^5 + y^9 = z^2$$

gives a solution of the others after changing signs and moving a term across the equation. For instance $x^2 + y^9 = z^5$ is $x^2 + (-z)^5 = (-y)^9$. So Theorem 1.1 says equally that none of these three equations has a solution in coprime nonzero integers.

The six solutions listed in Theorem 1.1 are the trivial ones. Indeed, if $x = 0$ then $y^5 = z^9$ with $\gcd(y, z) = 1$ forces $y = t^9$, $z = t^5$ and $t = \pm 1$. If $y = 0$ then $x^2 = z^9$ forces $z = t^2$, $x = \pm t^9$ and $t = \pm 1$. If $z = 0$ then $x^2 = -y^5$ forces $y = -t^2$, $x = \pm t^5$ and $t = \pm 1$. In a solution, a prime dividing two of x, y, z divides the third, so x, y, z are pairwise coprime.

With Theorem 1.1, the signature $(2, 3, 25)$ is the only one on the list of Ratcliffe and Grechuk whose exponents are not all prime. Freitas and Stoll [19] treat it with the same parametrization as we do (Section 1.2) and reduce it to five equations $H(u, v) = w^5$, with H a binary form of degree 10 over a sextic number field. They describe these equations as beyond the reach of current methods. Among signatures whose exponents are three distinct primes, the author treats $(2, 5, 7)$ in [20], assuming a classification from Putz's thesis [26].

1.2. **The idea of the proof.** Since $z^9 = (z^3)^3$, a solution of (1.1) gives the coprime solution $(a, b, c) = (x, -z^3, y)$ of $a^2 + b^3 + c^5 = 0$. This equation has signature $(2, 3, 5)$, with $1/2 + 1/3 + 1/5 > 1$, and such spherical equations have infinitely many coprime solutions, which fall into finitely many polynomial families. By a theorem of Beukers [3] these families are given by binary forms, and Edwards [13] found them: there are 27 triples (f_i, g_i, h_i) of binary forms with integer coefficients, of degrees 30, 20 and 12, such that every coprime solution is $(a, b, c) = (\pm f_i(u, v), g_i(u, v), h_i(u, v))$ for some i and coprime integers u, v (Theorem 2.1). So for some i the form g_i of degree 20 takes the value $-z^3$, a cube, at a pair of coprime integers (u, v). The extra condition falls on g_i because z enters through $z^9 = (z^3)^3$, while x and y appear with the exponents 2 and 5 of the spherical equation. We

call such a triple (i, u, v) an *Edwards triple* of the solution. The proof shows that every Edwards triple of a solution with $z \neq 0$ is an Edwards triple of one of the trivial solutions $(\pm 1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$. It has three stages.

(1) *Descent modulo cubes* (Sections 3, 4 and 5). Over a number field K over which g_i factors, the value of each factor at (u, v) is, modulo cubes, one of finitely many classes: those whose valuations are divisible by 3 at every prime not above 2, 3 or 5. Local conditions at the primes above 2, 3 and 5 cut this finite set down. Seven forms are excluded because $g_i(u, v)$ is never a 2-adic cube when u, v are coprime and $f_i(u, v)$, $g_i(u, v)$, $h_i(u, v)$ are not all even (Lemma 4.1). For eleven of the remaining forms, g_i is irreducible even over $\mathbb{Q}(\sqrt{5})$. Over the subfield of degree 10 of the field generated by a root of $g_i(t, 1)$, it has a quadratic factor, and already the values of this factor have no class compatible with the local conditions at 2 and 3 (Theorem 4.2). The other nine forms factor over $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{5})$, which allows descents over fields in which they split into more factors. Descents over $\mathbb{Q}(\sqrt[3]{5})$ and over octic fields exclude forms 10, 17, 18 and 26 (Proposition 5.1). For each of the forms 1, 2, 3, 4 and 20 exactly one tuple of classes survives, and Proposition 5.2 identifies it: for forms 1, 3 and 4 it is the tuple of classes of the factors at $(u, v) = (0, 1)$, for form 20 at $(2, 0)$, and for form 2 at $(0, 1)$, except that the class at the factor u is that of 2.

(2) *Curves* (Sections 6, 7, 8 and 9). For each of the five remaining forms, the condition that some factors take values in known classes modulo cubes defines a curve on which the Edwards triple gives a rational point. Form 3 leads to an elliptic curve over $\mathbb{Q}$ of rank 0 (Proposition 6.1). For forms 1 and 20, $g_i(u, v)$ is a quartic form in u^5 and v^5, and over $\mathbb{Q}(\sqrt{5})$ it is a constant times the norm of a quadratic form $A_i + B_i\sqrt{5}$. The descent shows that $(A_i + B_i\sqrt{5})(u^5, v^5)$ is an explicit constant times $(m + n\sqrt{5})^3$ with $m, n \in \mathbb{Q}$. Two members of the pencil of quadratic forms $A_i + \nu B_i$ are squares of linear forms, and multiplying the two identities they give eliminates u and v. What remains says that $(m : n)$ is the x-coordinate of a rational point on the curve of genus 2

$$C : \ y^2 = \Psi(x) = 25x^6 - 342x^5 + 1920x^4 - 5700x^3 + 9525x^2 - 8550x + 3250,$$

the same curve for both forms (Proposition 7.1). Its Jacobian has analytic rank 2 according to a numerical computation, so Chabauty's method over $\mathbb{Q}$ is not expected to apply. Form 2 leads to the elliptic curve $Y^2 = X^3 + 36\sqrt[3]{5}$ over $\mathbb{Q}(\sqrt[3]{5})$. For form 4, two factors of g_4 over $\mathbb{Q}(\sqrt{-5})$ take cube values, and this gives a point on the elliptic curve $Y^2 = X^3 - 108 - 432\sqrt{-5}$ over $\mathbb{Q}(\sqrt{-5})$ at which a certain function takes the value $\overline{L_1}/L_1$, where L_1 is a linear form in u^2 and v^2 with coefficients in $\mathbb{Q}(\sqrt{-5})$. As u^2 and v^2 are rational, this value has norm 1 from $\mathbb{Q}(\sqrt{-5})$ to $\mathbb{Q}$ (Lemma 9.1).

(3) *Points on the curves.* Over the cubic field $\mathbb{Q}(\xi)$, where $\xi^3 - 18\xi - 12 = 0$, the sextic Ψ factors as $25\Psi_2\Psi_4$ with Ψ_2 quadratic. For a rational point of C with $x \neq \infty$, local conditions force $\Psi_2(x)$ to be a square in $\mathbb{Q}(\xi)$ (Lemma 7.4). So the point gives a point of the elliptic curve $w^2 = \Psi_4(x)$ over $\mathbb{Q}(\xi)$, whose Mordell–Weil group has rank 2, less than the degree 3 of the field. A Mordell–Weil sieve and elliptic Chabauty at the prime 59 then give $C(\mathbb{Q}) = \{\infty_+, \infty_-, (3, \pm 8)\}$, where $\infty_\pm$ are the two points at infinity (Theorem 7.10). The curve of form 2 has only the point at infinity over $\mathbb{Q}(\sqrt[3]{5})$, by a descent via 3-isogeny (Proposition 8.2), and the curve of form 4 has rank $1 < 2$ over $\mathbb{Q}(\sqrt{-5})$, so that elliptic Chabauty at the prime 23 applies (Proposition 9.4).

Table 1 summarizes what happens to each form.

Forms i	How they are treated	Where
5, 12, 15, 16, 23, 25, 27	$v_2(g_i(u,v)) \in \{1,2\}$ whenever u, v are coprime and f_i, g_i, h_i are not all even at (u,v)	Lemma 4.1
6, 7, 8, 9, 11, 13, 14, 19, 21, 22, 24	descent over a field of degree 10; conditions at 2 and 3	Theorem 4.2
10, 26	descent over $\mathbb{Q}(\sqrt[3]{5})$	Proposition 5.1
17, 18	descent over an octic field	Proposition 5.1
3	descent over $\mathbb{Q}(\sqrt{-5})$; an elliptic curve of rank 0 over $\mathbb{Q}$	Proposition 6.1
1, 20	descent over fields of degree 10; the genus-2 curve C; elliptic Chabauty over a cubic field	Proposition 7.2
2	descent over $\mathbb{Q}(\sqrt[3]{5})$; an elliptic curve with trivial Mordell–Weil group	Proposition 8.4
4	descent over $\mathbb{Q}(\sqrt{-5})$; elliptic Chabauty over $\mathbb{Q}(\sqrt{-5})$	Proposition 9.6

TABLE 1. The fate of Edwards' 27 forms.

1.3. **Relation to earlier work.** The modular method, which has resolved many infinite families of signatures (see the survey [27]), has not been made to work for $(2,5,9)$, whose exponents have no prime factor larger than 5. Our method combines published techniques: Edwards' parametrization [13], and descents on parametrizations of the kind used by Bruin [6], by Siksek and Stoll [31] and by Freitas and Stoll [19]. Bruin [4, 6] used such descents to solve several generalized Fermat equations of hyperbolic signature. In particular Bruin [6] solves $x^3 + y^9 = z^2$ by requiring a binary form in the (tetrahedral) parametrization of $a^3 + b^3 = c^2$ to be a cube, running a descent modulo cubes over number fields, and finishing with elliptic Chabauty. Our argument has the same shape for the icosahedral case. For Edwards' parametrization, Siksek and Stoll [31] require the forms f_i to be squares ($x^3 + y^4 + z^5 = 0$), and Freitas and Stoll [19] require the forms h_i to be fifth powers ($x^2 + y^3 = z^{25}$), in both cases with descents over the number fields over which the forms factor. Siksek and Stoll [32] describe the route through h_i being a cube for $x^2 + y^3 = z^{15}$, and solve that equation by another route. Here the condition falls on the forms g_i of degree 20.

For the curves, we use elliptic Chabauty over number fields, due to Bruin [5] and to Flynn and Wetherell [17, 18], with covering collections in the sense of Coombes and Grant [11], Wetherell [35] and Bruin and Flynn [7, 8]. We also use the Mordell–Weil sieve of Bruin and Stoll [9], which goes back to Scharaschkin [29] and Flynn [16]. Chabauty's method and a Mordell–Weil sieve were combined by Poonen, Schaefer and Stoll [25] to resolve $x^2 + y^3 = z^7$. The Chabauty step for forms 1 and 20 (Lemma 7.8) is a rank condition on a matrix modulo p, of the same type as in Siksek's explicit Chabauty over number fields [30]. The descents on elliptic curves are 2-descents [33, Chapter X] and descents via 3-isogeny [10, 28, 34].

What is specific to this equation is the treatment of the five forms that survive the descent. Forms 1 and 20 lead, through an identity in a pencil of quadratic forms, to the same curve of genus 2. Form 2 is finished by combining two factors of g_2, since each of its quadratic factors alone leads to a curve whose Jacobian has rank 3 over $\mathbb{Q}(\sqrt[3]{5})$ (Section 8). Form 4 becomes a norm condition on a function on an elliptic curve of rank 1.

1.4. **What is assumed, and what is computed.** The proof rests on the following.

(i) Edwards' theorem [13] (Theorem 2.1), with the forms as printed by Siksek and Stoll [31, Table 1], which agree with those of Freitas and Stoll [19, Table 3].

(ii) Explicit computations with PARI/GP 2.17.3 [24] and Python. Each is stated in the text where it is used, most of them within numbered lemmas, propositions and theorems. Table 6 in Appendix B lists them all, and each was repeated by a separately written program. The programs and their outputs are deposited at [21].

No step assumes the generalized Riemann hypothesis. Class groups are bounded using Minkowski's bound and explicit relations between ideals (Appendix A). For the fields of degree 10 in Section 4 this involves up to about 10^4 prime ideals per field. The units and S-units proposed by PARI are checked by power residue characters at auxiliary primes (Lemma 3.3).

1.5. **Plan of the paper.** Section 2 recalls Edwards' parametrization and reduces Theorem 1.1 to a statement about Edwards triples. Section 3 sets up the descent modulo cubes, Section 4 removes 18 forms, and Section 5 removes four more and restricts the last five. Sections 6, 7, 8 and 9 treat form 3, forms 1 and 20, form 2 and form 4, and Section 10 proves Theorem 1.1. Appendix A bounds the class groups, and Appendix B describes the computations.

Throughout, for a number field K and $\alpha \in K^\times$ we write $[\alpha]$ for the class of α in $K^\times/K^{\times 3}$, and we write this group additively. For a prime $\mathfrak{p}$ of K, $v_\mathfrak{p}$ is its normalized valuation, and Σ is the set of primes of K above 2, 3 and 5. Table 2 lists the main notation.

Symbol	Meaning
(x, y, z)	a solution of (1.1)
$f_i,\ g_i,\ h_i$	Edwards' forms of degrees 30, 20, 12 ($1 \le i \le 27$; Section 2)
(i, u, v)	an Edwards triple (Definition 2.3); condition (2.2) is primitivity at p
$\mathcal{I}_2,\ \mathcal{I}_{10},\ \mathcal{I}_\mathrm{r}$	the forms removed at 2, the eleven forms treated over fields of degree 10, and the nine others (Section 4)
$\Sigma,\ K(\Sigma, 3),\ [\alpha]$	the primes above $2, 3, 5$; the classes modulo cubes with valuations divisible by 3 outside Σ; the class of α modulo cubes (Section 3)
$\mathcal{L}_p$	the local image at $p \in \{2, 3, 5\}$ (Section 3.2)
$M_i;\ K_1, K_{20}, K'_{17}, K'_{18}, K''$	the fields of the descents (Tables 3 and 4)
reference pair	$(0, 1)$ for forms 1, 2, 3, 4, and $(2, 0)$ for form 20 (Proposition 5.2)
$C,\ \Psi$	the genus-2 curve $y^2 = \Psi(x)$ of forms 1 and 20 (Section 7)
$\xi;\ \Psi_2, \Psi_4;\ H,\ E,\ \iota$	the cubic field $\mathbb{Q}(\xi)$ of Section 7; the factors of Ψ over it; the genus-1 curve $w^2 = \Psi_4(x)$, its Jacobian and the isomorphism $\iota : H \to E$
$\theta,\ E_D$	$\sqrt[3]{5}$ and the curve $Y^2 = X^3 + D$ over $\mathbb{Q}(\theta)$ (Section 8)
$E_A;\ t,\ G,\ P_0$	the curve $Y^2 = X^3 + A$ over $\mathbb{Q}(\sqrt{-5})$; the function and points on it (Section 9)

TABLE 2. Main notation. The letter K denotes a general number field in Sections 3, 4 and 5, and in each of Sections 6, 7, 8 and 9 the field fixed at its start. The symbols P_0 and n_0 have different meanings in Sections 7 and 9.

2. EDWARDS' PARAMETRIZATION

We recall Edwards' parametrization and turn Theorem 1.1 into a statement about the forms g_i of degree 20 (Proposition 2.4).

For $\alpha = (\alpha_0, \dots, \alpha_{12}) \in \mathbb{Q}^{13}$ let h_α be the binary form

$$h_\alpha(u, v) = \sum_{k=0}^{12} \binom{12}{k} \alpha_k \, u^k v^{12-k}.$$

Siksek and Stoll [31, Table 1] list vectors $\alpha^{(1)}, \dots, \alpha^{(27)}$, and we put $h_i = h_{\alpha^{(i)}}$. Freitas and Stoll [19, Table 3] list the same vectors in the same order. For $1 \le i \le 27$ let

$$g_i = \frac{1}{132^2} \left(\frac{\partial^2 h_i}{\partial u^2} \frac{\partial^2 h_i}{\partial v^2} - \Big(\frac{\partial^2 h_i}{\partial u \, \partial v} \Big)^2 \right), \qquad f_i = \frac{1}{240} \left(\frac{\partial h_i}{\partial u} \frac{\partial g_i}{\partial v} - \frac{\partial h_i}{\partial v} \frac{\partial g_i}{\partial u} \right). \tag{2.1}$$

Thus, up to the constant factors, where $132 = 12 \cdot 11$ and $240 = 12 \cdot 20$, the form g_i is the Hessian of h_i, and f_i is the Jacobian of h_i and g_i. The forms f_i, g_i, h_i have degrees 30, 20, 12 and integer coefficients, and $f_i^2 + g_i^3 + h_i^5 = 0$ (Lemma 2.2). The later sections work with explicit formulas only for $i = 1, 2, 3, 4, 20$, where

$$\begin{aligned}
\alpha^{(1)} &= (0, 1, 0, 0, 0, 0, -\tfrac{144}{7}, 0, 0, 0, 0, -20736, 0), \\
\alpha^{(2)} &= (-1, 0, 0, -2, 0, 0, \tfrac{80}{7}, 0, 0, 640, 0, 0, -102400), \\
\alpha^{(3)} &= (-1, 0, -1, 0, 3, 0, \tfrac{45}{7}, 0, 135, 0, -2025, 0, -91125), \\
\alpha^{(4)} &= (1, 0, -1, 0, -3, 0, \tfrac{45}{7}, 0, -135, 0, -2025, 0, 91125), \\
\alpha^{(20)} &= (0, 81, 0, 0, 0, 0, -\tfrac{144}{7}, 0, 0, 0, 0, -256, 0).
\end{aligned}$$

Theorem 2.1 (Edwards [13, pp. 235–236]; see [19, Theorem 2.1] and [31, Theorem 4.1])**.** *Suppose that a, b, c are coprime integers with $a^2 + b^3 + c^5 = 0$. Then for some $i \in \{1, \dots, 27\}$ there are coprime integers u, v and a sign $\pm$ such that*

$$a = \pm f_i(u, v), \qquad b = g_i(u, v), \qquad c = h_i(u, v).$$

In [31, Theorem 4.1] the theorem is stated without the sign, for 49 triples: the 27 triples (f_i, g_i, h_i) and 22 of the triples $(-f_i, g_i, h_i)$. The statement above follows from it.

Lemma 2.2. *For every i, the forms f_i, g_i, h_i have integer coefficients and satisfy $f_i^2 + g_i^3 + h_i^5 = 0$. The discriminant of g_i and the resultant of g_i and h_i, taken as binary forms of degrees 20 and 12, are nonzero and divisible by no prime other than 2, 3 and 5.*

Proof. This is a computation with polynomials over $\mathbb{Q}$ (Appendix B). □

Definition 2.3. Let (x, y, z) be a solution of (1.1). An *Edwards triple* of (x, y, z) is a triple (i, u, v) with $i \in \{1, \dots, 27\}$ and coprime integers u, v such that $x = \pm f_i(u, v)$, $g_i(u, v) = -z^3$ and $h_i(u, v) = y$ for a choice of sign.

Proposition 2.4. *Every solution (x, y, z) of (1.1) has an Edwards triple (i, u, v). For every Edwards triple, $g_i(u, v)$ is a cube, and no prime divides all three of $f_i(u, v)$, $g_i(u, v)$, $h_i(u, v)$.*

Proof. Put $(a, b, c) = (x, -z^3, y)$. Then $a^2 + b^3 + c^5 = x^2 - z^9 + y^5 = 0$, and $\gcd(a, b, c) = 1$ because a prime dividing x, z^3 and y divides x, y and z. Theorem 2.1 gives an Edwards triple. For an Edwards triple, $g_i(u, v) = (-z)^3$, and $(f_i, g_i, h_i)(u, v) = (\pm x, -z^3, y)$ has no common prime factor. □

We will use primitivity only at the primes 2, 3 and 5, through the following condition on a pair of coprime integers u, v and a prime p:

$$f_i(u, v),\ g_i(u, v) \text{ and } h_i(u, v) \text{ are not all divisible by } p. \tag{2.2}$$

By Proposition 2.4, an Edwards triple satisfies (2.2) for every prime p. Conversely, by Lemma 2.2, if u, v are coprime and a prime $p \notin \{2, 3, 5\}$ divides $g_i(u, v)$ and $h_i(u, v)$, then p divides the resultant of g_i and h_i, which is impossible. (Here we use that for binary forms A, B of degrees m, n with integer coefficients there are forms U_1, V_1, U_2, V_2 with integer coefficients such that $U_1A + V_1B = \mathrm{Res}(A, B)\, u^{m+n-1}$ and $U_2A + V_2B = \mathrm{Res}(A, B)\, v^{m+n-1}$, where $\mathrm{Res}(A, B)$ is the Sylvester determinant of A and B taken as forms of degrees m and n.) So (2.2) holds automatically for $p \notin \{2, 3, 5\}$. Hence, for coprime integers u, v with $g_i(u, v) = -z^3$, the triple $(\pm f_i(u, v), h_i(u, v), z)$ is a solution of (1.1) with Edwards triple (i, u, v) exactly when (2.2) holds for $p = 2, 3, 5$.

Since f_i, g_i, h_i have even degree, (i, u, v) and $(i, -u, -v)$ are Edwards triples of the same solutions. The values

$$(f_1, g_1, h_1)(0, 1) = (-1, -1, 0), \qquad (f_2, g_2, h_2)(0, 1) = (1, 0, -1),$$
$$(f_3, g_3, h_3)(0, 1) = (0, 1, -1), \qquad (f_4, g_4, h_4)(0, 1) = (0, -1, 1)$$

(Appendix B) show that $(1, 0, \pm 1)$ is an Edwards triple of $(\pm 1, 0, 1)$, $(2, 0, \pm 1)$ of $(\pm 1, -1, 0)$, $(3, 0, \pm 1)$ of $(0, -1, -1)$ and $(4, 0, \pm 1)$ of $(0, 1, 1)$. The rest of the paper shows that every Edwards triple of a solution with $z \neq 0$ is one of $(1, 0, \pm 1)$, $(3, 0, \pm 1)$ and $(4, 0, \pm 1)$. Solutions with $z = 0$ need no further work: they are $(\pm 1, -1, 0)$ by Section 1.1.

3. Descent modulo cubes

This section describes the descent that Sections 4 and 5 apply to the forms g_i. Over a number field K over which g_i factors, the value of each factor at an Edwards triple lies, modulo cubes, in a finite group (Lemmas 3.1 and 3.3), and its images in the completions at the primes above 2, 3 and 5 lie in finite sets that can be computed (Lemma 3.4).

3.1. **The descent lemma.** Let K be a number field with ring of integers $\mathcal{O}_K$, let Σ be the set of primes of K above 2, 3 and 5, and let

$$K(\Sigma, 3) = \{[\alpha] \in K^\times/K^{\times 3} \ : \ v_\mathfrak{p}(\alpha) \equiv 0 \pmod 3 \text{ for every prime } \mathfrak{p} \notin \Sigma\}.$$

For a binary form $F \in K[u, v]$, the *content ideal* of F is the fractional ideal generated by its coefficients.

Lemma 3.1. *Let $g \in \mathbb{Z}[u, v]$ be a binary form, and suppose that $g = c\, F_1 \cdots F_k$ with $c \in K^\times$ and binary forms $F_1, \ldots, F_k \in \mathcal{O}_K[u, v]$ such that*

(a) *c is a Σ-unit, and the content ideal of each F_j is a product of powers of primes in Σ;*
(b) *for $j \neq l$, the resultant $\mathrm{Res}(F_j, F_l)$ is divisible only by primes in Σ.*

Let u, v be coprime integers and z a nonzero integer with $g(u, v) = -z^3$. Then $[F_j(u, v)] \in K(\Sigma, 3)$ for every j, and $\sum_j [F_j(u, v)] = -[c]$.

Proof. Let $\mathfrak{p} \notin \Sigma$ be a prime of K. The resultant identities recalled in Section 2 hold for binary forms over $\mathcal{O}_K$, with U_1, V_1, U_2, V_2 over $\mathcal{O}_K$. The values $F_j(u, v)$ are $\mathfrak{p}$-integral, and nonzero because $z \neq 0$. Since u and v are coprime, (b) shows that $\mathfrak{p}$ divides at most one of the values $F_j(u, v)$. By (a), $\sum_j v_\mathfrak{p}(F_j(u, v)) = v_\mathfrak{p}(-z^3/c) = 3v_\mathfrak{p}(z)$, so each $v_\mathfrak{p}(F_j(u, v))$ is 0 or $3v_\mathfrak{p}(z)$. Finally $\prod_j F_j(u, v) = -z^3/c$ and $-1 = (-1)^3$. □

Remark 3.2. Condition (b) follows from (a) and Lemma 2.2 when $g = g_i$. Indeed, for $\mathfrak{p} \notin \Sigma$ the forms F_j are $\mathfrak{p}$-integral with $\mathfrak{p}$-unit content, and the discriminant of g, a $\mathfrak{p}$-unit, is $c^{2 \deg g - 2}$ times the product of the discriminants of the F_j and of the squares of the resultants $\mathrm{Res}(F_j, F_l)$, $j < l$. In the computations both (a) and (b) are also checked directly.

Lemma 3.3. *Suppose that 3 does not divide the class number of K and that K contains no primitive cube root of unity. Let $\mathcal{O}_\Sigma$ be the ring of Σ-integers of K, and r_1, r_2 the numbers of real and complex places of K. Then $K(\Sigma,3) = \mathcal{O}_\Sigma^\times/\mathcal{O}_\Sigma^{\times 3}$, and it is a vector space over $\mathbb{F}_3$ of dimension $n = r_1 + r_2 - 1 + \#\Sigma$. Moreover, if $B_1, \dots, B_n \in \mathcal{O}_\Sigma^\times$ and there are primes $\mathfrak{q}_1, \dots, \mathfrak{q}_m \notin \Sigma$ of norm $\equiv 1 \pmod 3$ such that the matrix $(\chi_{\mathfrak{q}_l}(B_j))$ of cubic residue characters has rank n over $\mathbb{F}_3$, then the classes of $B_1, \dots, B_n$ form a basis of $K(\Sigma,3)$.*

Here, for a prime $\mathfrak{q} \notin \Sigma$ of norm $N\mathfrak{q} \equiv 1 \pmod 3$ and a $\mathfrak{q}$-unit α, $\chi_\mathfrak{q}(\alpha) \in \mathbb{F}_3$ is defined by $\alpha^{(N\mathfrak{q}-1)/3} \equiv \zeta_\mathfrak{q}^{\chi_\mathfrak{q}(\alpha)} \pmod{\mathfrak{q}}$ for a fixed cube root of unity $\zeta_\mathfrak{q} \neq 1$ in $\mathcal{O}_K/\mathfrak{q}$. It is a homomorphism that vanishes on cubes.

Proof. If $[\alpha] \in K(\Sigma,3)$, then $\alpha\mathcal{O}_\Sigma = \mathfrak{a}^3$ for a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_\Sigma$. This gives an exact sequence $0 \to \mathcal{O}_\Sigma^\times/\mathcal{O}_\Sigma^{\times 3} \to K(\Sigma,3) \to \mathrm{Cl}(\mathcal{O}_\Sigma)[3] \to 0$. The group $\mathrm{Cl}(\mathcal{O}_\Sigma)$ is a quotient of the class group of K, so $\mathrm{Cl}(\mathcal{O}_\Sigma)[3] = 0$. By Dirichlet's S-unit theorem, $\mathcal{O}_\Sigma^\times \simeq \mu(K) \times \mathbb{Z}^n$, and $\mu(K)$ has order prime to 3. So $\mathcal{O}_\Sigma^\times/\mathcal{O}_\Sigma^{\times 3} \simeq \mathbb{F}_3^n$. If $\prod_j B_j^{b_j} = \gamma^3$ with $b_j \in \mathbb{Z}$ and $\gamma \in K^\times$, then $\gamma \in \mathcal{O}_\Sigma^\times$, and applying $\chi_{\mathfrak{q}_l}$ gives $\sum_j b_j \chi_{\mathfrak{q}_l}(B_j) = 0$ for all l, so every b_j is divisible by 3. Hence the n classes are independent, and they form a basis. □

For every field over which a descent modulo cubes or a descent via 3-isogeny is run below, Appendix A shows that 3 does not divide the class number and that the field contains no primitive cube root of unity. The elements $B_1, \dots, B_n$ were proposed by PARI's `bnfunits` and checked as in Lemma 3.3. Each is a Σ-unit, by its norm and its ideal factorization, and their cubic residue characters at the primes of K above small rational primes $q \geq 7$ (all $q \leq 400$ for the fields M_i of Section 4) have rank n.

3.2. **Local conditions.** Let $p \in \{2,3,5\}$, and for a prime $\mathfrak{p} \mid p$ of K let $K_\mathfrak{p}$ be the completion. Let $g = g_i = cF_1 \cdots F_k$ over K as in Lemma 3.1. Let P_p be the set of pairs $(u,v) \in \mathbb{Z}_p^2$ such that

(i) u and v are not both divisible by p,
(ii) $g(u,v) \neq 0$ is a cube in $\mathbb{Q}_p$, and
(iii) $f_i(u,v)$, $g_i(u,v)$, $h_i(u,v)$ are not all divisible by p.

The *local image* at p is the set $\mathcal{L}_p$ of tuples $\left([F_j(u,v)]_\mathfrak{p}\right)_{j,\ \mathfrak{p}\mid p}$ for $(u,v) \in P_p$, where $[\cdot]_\mathfrak{p}$ is the class in $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 3}$.

Lemma 3.4. *Let (i,u,v) be an Edwards triple of a solution with $z \neq 0$, and let $p \in \{2,3,5\}$. Then $(u,v) \in P_p$, and the images of $[F_1(u,v)], \dots, [F_k(u,v)]$ in $\prod_{\mathfrak{p}\mid p} K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 3}$ form an element of $\mathcal{L}_p$.*

Proof. By Definition 2.3, u and v are coprime and $g_i(u,v) = -z^3 \neq 0$, which gives (i) and (ii), and (iii) is Proposition 2.4. □

A class in $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 3}$ is determined by the valuation modulo 3 and by the class modulo cubes of the unit part in $(\mathcal{O}_K/\mathfrak{p}^{m_\mathfrak{p}})^\times$, where $m_\mathfrak{p} = 1$ if $p \neq 3$ and $m_\mathfrak{p} = \lfloor 3e_\mathfrak{p}/2 \rfloor + 1$ if $p = 3$, with $e_\mathfrak{p}$ the ramification index. This is because $1 + \mathfrak{p}^{m_\mathfrak{p}}$ consists of cubes: for $p \neq 3$ it is a pro-p group, and for $p = 3$ the map $x \mapsto x^3$ sends $1 + \mathfrak{p}^k$ onto $1 + \mathfrak{p}^{k+e_\mathfrak{p}}$ when $k > e_\mathfrak{p}/2$.

Every $(u,v) \in \mathbb{Z}_p^2$ with (i) is $\lambda(t,1)$ or $\lambda(1,pt)$ with $\lambda \in \mathbb{Z}_p^\times$ and $t \in \mathbb{Z}_p$. We call $t \mapsto (t,1)$ and $t \mapsto (1,pt)$ the two *charts*. Since $F_j(\lambda u, \lambda v) = \lambda^{\deg F_j} F_j(u,v)$, the effect of λ can be treated separately. For $p = 2$ and $p = 5$ every element of $\mathbb{Z}_p^\times$ is a cube, so λ changes no class, and condition (ii) says that $v_p(g(u,v)) \equiv 0 \pmod 3$. For $p = 3$, suppose that $v_3(g(t,1)) = 3a$

is divisible by 3, and write $g(t,1) = 3^{3a}w$ (or $g(1,3t) = 3^{3a}w$) with $w \in \mathbb{Z}_3^\times$. Then (ii) holds for $\lambda(t,1)$ exactly when $\lambda^{20}w$ is a cube, that is, when $\lambda \equiv w$ modulo $\mathbb{Z}_3^{\times 3}$, and then $[F_j(\lambda u, \lambda v)] = [F_j(u,v)] + \deg F_j \cdot [w]$.

We compute a finite set that contains $\mathcal{L}_p$ as follows. In each chart we cover $\mathbb{Z}_p$ by the residue classes $t_0 + p\mathbb{Z}_p$, and we replace a residue class $t_0 + p^s\mathbb{Z}_p$ by the p residue classes $t_0 + ap^s + p^{s+1}\mathbb{Z}_p$, $0 \le a < p$, until the Taylor expansion at t_0 shows that the following data are constant on it: the valuation $v_p(g)$; for $p = 3$, the value of w modulo 9, which determines $[w]$; and, for each j and each $\mathfrak{p} \mid p$, the residue of F_j modulo $\mathfrak{p}^{v_\mathfrak{p}(F_j)+m_\mathfrak{p}}$, which determines $[F_j]_\mathfrak{p}$. Explicitly, let $G(t)$ be the value of g, or of F_j, at the point of the chart with parameter t, and write $G(t_0 + p^s y) = \sum_{l \ge 0} c_l y^l$. The data are constant on $t_0 + p^s\mathbb{Z}_p$ when $c_0 \ne 0$ and $v(c_l) \ge v(c_0) + m$ for every $l \ge 1$, where v is the valuation of $\mathbb{Q}_p$ or of $K_\mathfrak{p}$, and $m = 1$ for g if $p \ne 3$, $m = 2$ for g if $p = 3$ (this fixes w modulo 9 as well), and $m = m_\mathfrak{p}$ for F_j at $\mathfrak{p}$. A residue class is discarded if f_i, g_i, h_i are all divisible by p on it, or if the test above succeeds for g on it and $v_p(g)$ is not divisible by 3. Every other residue class on which the data are constant contributes the tuple of local classes of its points, shifted for $p = 3$ by $\deg F_j \cdot [w]$ as above.

The refinement stops at depth $s = 18$. A residue class that is still undecided then is kept, with each undecided entry left free. If the class of F_j at $\mathfrak{p}$ is not constant on it, every class in $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 3}$ is allowed at that entry, or every class with the given valuation modulo 3 when that valuation is constant. For $p = 3$, if $[w]$ is not constant on it, all three values of $[w]$ are allowed in the shift. Undecided residue classes lie around the roots of g_i in the charts: for instance, at $p = 3$, around $t = 0$ when the factor u or v divides g_i (forms 2 and 10), around $t = \pm 1$ in the first chart for form 26, whose linear factors are $u - v$ and $u + v$, and around the 3-adic roots of g_i for $i \in \{7, 8, 9, 13, 14\}$ in Theorem 4.2. Undecided residue classes can only enlarge the computed set, which therefore contains $\mathcal{L}_p$.

3.3. **Admissible tuples.** Fix a basis of $K(\Sigma, 3)$ as in Lemma 3.3, and let $\mathrm{loc}_p : K(\Sigma,3) \to \prod_{\mathfrak{p} \mid p} K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 3}$ be the localization map. A tuple $(e_1, \dots, e_k) \in K(\Sigma,3)^k$ is *admissible* if $\sum_j e_j = -[c]$ and $(\mathrm{loc}_p(e_j))_j$ lies in the computed set containing $\mathcal{L}_p$ for $p = 2, 3, 5$. By Lemmas 3.1 and 3.4, for an Edwards triple with $z \ne 0$ the tuple $([F_j(u,v)])_j$ is admissible. We find the admissible tuples by linear algebra over $\mathbb{F}_3$. For each j we first find the classes $e \in K(\Sigma,3)$ whose localizations lie in the projections of the computed sets to the factor F_j, and then the tuples of such classes that are admissible.

Remark 3.5. Condition (iii) at $p = 3$ cannot be omitted. The form g_7 takes the cube value $g_7(1,1) = -576^3$, but f_7, g_7, h_7 are all divisible by $2^{10}3^4$ at $(1,1)$. Similarly $g_{19}(0,1) = -9^3$, where f_{19}, g_{19}, h_{19} are all divisible by 3^4, and this point gives the solution $(3^9 \cdot 17, -2 \cdot 3^4, 3^2)$ of $x^2 + y^5 = z^9$ with $\gcd(x,y,z) = 9$. Without condition (iii) at $p = 3$, the descent of Theorem 4.2 keeps exactly the classes of these two points and one class for form 24. With it, the descent keeps nothing.

4. Eighteen forms without Edwards triples

This section shows that 18 of the 27 forms have no Edwards triple: seven by a 2-adic valuation argument (Lemma 4.1), and eleven of the remaining forms, which are irreducible

over $\mathbb{Q}(\sqrt{5})$, by the descent of Section 3 (Theorem 4.2). Let

$$\begin{aligned}\mathcal{I}_2 &= \{5, 12, 15, 16, 23, 25, 27\},\\ \mathcal{I}_{10} &= \{6, 7, 8, 9, 11, 13, 14, 19, 21, 22, 24\},\\ \mathcal{I}_{\mathrm{r}} &= \{1, 2, 3, 4, 10, 17, 18, 20, 26\}.\end{aligned}$$

Lemma 4.1. *Let $i \in \mathcal{I}_2$ and let u, v be coprime integers. If $u \equiv v \equiv 1 \pmod 2$ for $i \in \{5, 15, 16, 25, 27\}$, or $u \equiv 0 \pmod 2$ for $i \in \{12, 23\}$, then $f_i(u, v)$, $g_i(u, v)$, $h_i(u, v)$ are all even. Otherwise $v_2(g_i(u, v)) = 1$, or $v_2(g_i(u, v)) = 2$ when $i = 25$. In particular no Edwards triple has $i \in \mathcal{I}_2$.*

Proof. The values of f_i, g_i, h_i modulo 2 and of g_i modulo 8 depend only on (u, v) modulo 8, so it suffices to check the pairs modulo 8 with u or v odd (Appendix B). An Edwards triple has $g_i(u, v) = -z^3$, so $v_2(g_i(u, v))$ is divisible by 3 or $g_i(u, v) = 0$, and (2.2) holds at 2. □

For $i \in \mathcal{I}_{10}$ the form g_i is irreducible over $\mathbb{Q}(\sqrt{5})$. Let L_i be the field generated by a root of $g_i(t, 1)$, of degree 20. A computation of its subfields shows that L_i has exactly one subfield other than $\mathbb{Q}$ and L_i: a field M_i of degree 10 and signature $(2, 4)$, over which g_i factors into irreducible forms of degrees 2, 6 and 12 (Appendix B). Table 3 gives data on M_i. Forms 8 and 14 have the same field, as do 9 and 13, and 21 and 24.

The fields are $M_i = \mathbb{Q}(\eta)$, where η is a root of

$$\begin{aligned}
i = 6: &\quad \eta^{10} - 10\eta^8 + 25\eta^6 - 54\eta^5 - 35\eta^4 + 180\eta^3 + 50\eta^2 - 150\eta - 71,\\
i = 7: &\quad \eta^{10} - 30\eta^6 - 78\eta^5 - 30\eta^4 - 360\eta^3 - 120\eta^2 - 160\eta - 24,\\
i = 8, 14: &\quad \eta^{10} - 10\eta^7 - 15\eta^6 - 36\eta^5 + 5\eta^4 + 30\eta^3 + 60\eta^2 + 40\eta + 9,\\
i = 9, 13: &\quad \eta^{10} - 20\eta^7 + 15\eta^6 - 18\eta^5 + 135\eta^4 - 60\eta^3 - 90\eta^2 - 30\eta - 9,\\
i = 11: &\quad \eta^{10} + 5\eta^8 - 5\eta^6 - 18\eta^5 - 35\eta^4 - 60\eta^3 - 40\eta^2 - 30\eta - 14,\\
i = 19: &\quad \eta^{10} - 15\eta^8 - 10\eta^7 + 105\eta^6 + 102\eta^5 - 175\eta^4 - 90\eta^3 + 120\eta^2 + 40\eta - 24,\\
i = 21, 24: &\quad \eta^{10} - 40\eta^7 - 45\eta^6 - 66\eta^5 - 25\eta^4 - 30\eta^2 + 10\eta + 39,\\
i = 22: &\quad \eta^{10} - 10\eta^7 + 60\eta^6 - 54\eta^5 - 40\eta^4 + 240\eta^3 - 240\eta^2 + 220\eta - 36.
\end{aligned}$$

i	disc M_i	primes above 2; 3; 5 (e, f)	n	after 2
6	$2^{12}3^85^{11}$	$(2,1)(4,1)(2,2)$; $(5,2)$; $(10,1)$	10	729
7	$2^{10}3^{10}5^{11}$	$(4,1)(6,1)$; $(1,1)(6,1)(3,1)$; $(10,1)$	11	19683
8, 14	$2^{12}3^{10}5^{11}$	$(4,1)(2,1)(2,2)$; $(6,1)(3,1)(1,1)$; $(10,1)$	12	6561
9, 13	$2^{12}3^{10}5^{11}$	$(2,1)(4,1)(2,2)$; $(1,1)(3,1)(6,1)$; $(10,1)$	12	6561
11	$2^{10}3^85^{11}$	$(6,1)(4,1)$; $(5,2)$; $(10,1)$	9	2187
19	$2^{10}3^{10}5^{11}$	$(4,1)(6,1)$; $(1,1)(3,1)(6,1)$; $(10,1)$	11	19683
21, 24	$2^{12}3^{10}5^{11}$	$(4,1)(2,1)(2,2)$; $(6,1)(1,1)(3,1)$; $(10,1)$	12	6561
22	$2^83^{10}5^{11}$	$(5,2)$; $(6,1)(3,1)(1,1)$; $(10,1)$	10	6561

TABLE 3. The fields M_i for $i \in \mathcal{I}_{10}$. The primes of M_i above 2, 3 and 5 are given by their ramification indices and residue degrees (e, f), and $n = \dim_{\mathbb{F}_3} M_i(\Sigma, 3)$. The last column is the number of classes in $M_i(\Sigma, 3)$ whose image under loc_2 lies in the local image at 2 of the quadratic factor. After the condition at 3 none is left.

Theorem 4.2. *Let $i \in \mathcal{I}_{10}$. There are no coprime integers u, v such that $g_i(u, v)$ is a nonzero cube and (2.2) holds for $p = 2$ and $p = 3$. In particular no Edwards triple has $i \in \mathcal{I}_{10}$.*

Proof. Write $g_i = c\,Q\,S\,T$ over $M = M_i$, with $Q, S, T \in \mathcal{O}_M[u, v]$ irreducible of degrees 2, 6, 12 satisfying (a) and (b) of Lemma 3.1 (checked directly). To obtain (a), each monic factor is multiplied by an element of M that turns its content ideal into (1) if that ideal is principal, and into an integral ideal supported on Σ otherwise. The class number of M divides 2 (Appendix A), and M has a real place, so it contains no primitive cube root of unity. By Lemma 3.3, $M(\Sigma, 3) \simeq \mathbb{F}_3^n$ with $n = 5 + \#\Sigma$, with an explicit basis. Suppose u, v are as in the statement, with $g_i(u, v) = -z^3$. By Lemma 3.1, $e = [Q(u, v)] \in M(\Sigma, 3)$. For $p = 2, 3$ the pair (u, v) satisfies (i)–(iii) of Section 3.2, so $(u, v) \in P_p$ and $\mathrm{loc}_p(e)$ lies in the projection to the factor Q of the local image $\mathcal{L}_p$. At $p = 2$ the computed projection is a single vector, and the number of classes $e \in M(\Sigma, 3)$ with $\mathrm{loc}_2(e)$ equal to it is the last column of Table 3. At $p = 3$ the computed projection is a finite set of vectors in which undecided entries (Section 3.2) are left free, that is, a finite union of cosets of coordinate subspaces. Entries are left free only for $i \in \{7, 8, 9, 13, 14\}$, where six residue classes at 3, three around each of the two roots of g_i in $\mathbb{P}^1(\mathbb{Q}_3)$, remain undecided at depth 18. The linear algebra over $\mathbb{F}_3$ finds no $e \in M(\Sigma, 3)$ compatible with the conditions at 2 and 3, for each of the eleven forms (Appendix B). Finally, an Edwards triple (i, u, v) with $i \in \mathcal{I}_{10}$ would satisfy (2.2) at 2 and 3, and $g_i(u, v) \neq 0$ because g_i is irreducible over $\mathbb{Q}$ of degree 20. □

Remark 4.3. The descent with all three factors Q, S, T, local conditions at 2, 3, 5 and a condition at the auxiliary primes $q \leq 400$ also leaves nothing (Appendix B). The auxiliary condition uses that, at a prime $\mathfrak{q} \mid q$ not dividing $Q(u, v)$, the cubic residue character of the class of $Q(u, v)$ is that of $Q(u, v)$ itself, which depends only on (u, v) modulo q, and similarly for S and T. So, at the primes not dividing the values, the characters of the three classes must be those of the values at some nonzero pair $(u_0, v_0) \in \mathbb{F}_q^2$. The proof above needs only the factor Q and the conditions at 2 and 3. Using only the valuations at 2, 3 and 5, and not the unit parts of the local classes, removes ten of the eleven forms: form 14 then keeps the class of the pair $(0, 15)$, where $g_{14}(0, 15) = 15^{20} g_{14}(0, 1) = -3^{21} 5^{24}$ is a cube but $(0, 15)$ is not coprime.

Corollary 4.4. *Every Edwards triple (i, u, v) of a solution with $z \neq 0$ has $i \in \mathcal{I}_{\mathrm{r}}$.*

Proof. Lemma 4.1 excludes $i \in \mathcal{I}_2$, and Theorem 4.2 excludes $i \in \mathcal{I}_{10}$. □

5. The nine remaining forms

For $i \in \mathcal{I}_{\mathrm{r}}$ the form g_i factors over $\mathbb{Q}$ or over $\mathbb{Q}(\sqrt{5})$, and it factors further over fields of small degree. This section runs the descent of Section 3 over the fields of Table 4. It excludes forms 10, 17, 18 and 26 (Proposition 5.1). For forms 1, 3, 4 and 20 it shows that the classes of all factors are those at an explicit reference pair, and for form 2 that this holds for every factor other than u, while u is twice a cube in $\mathbb{Q}(\sqrt[3]{5})$ (Proposition 5.2). Sections 6, 7, 8 and 9 use only Proposition 5.2.

The fields are $\mathbb{Q}(\sqrt[3]{5})$, $\mathbb{Q}(\sqrt{-5})$ and

$$\begin{aligned}
K_1 &= \mathbb{Q}(\eta), \quad \eta^{10} - 5\eta^9 + 5\eta^8 - 20\eta^7 + 15\eta^6 - 17\eta^5 + 15\eta^4 - 80\eta^3 + 115\eta^2 - 95\eta + 11 = 0,\\
K_{20} &= \mathbb{Q}(\eta), \quad \eta^{10} - 3\eta^9 + 5\eta^8 - 12\eta^7 + 25\eta^6 - 33\eta^5 + 25\eta^4 - 12\eta^3 + 5\eta^2 - 3\eta + 1 = 0,\\
K'_{17} &= \mathbb{Q}(\eta), \quad \eta^8 - 2\eta^7 - 14\eta^6 - 26\eta^5 - 21\eta^4 + 2\eta^3 + 4\eta^2 - 4\eta + 1 = 0,\\
K'_{18} &= \mathbb{Q}(\eta), \quad \eta^8 - 4\eta^7 + 4\eta^6 + 2\eta^5 - 21\eta^4 - 26\eta^3 - 14\eta^2 - 2\eta + 1 = 0,\\
K'' &= \mathbb{Q}(\eta), \quad \eta^8 - 4\eta^7 + 4\eta^6 + 2\eta^5 - \eta^4 - 6\eta^3 + 16\eta^2 - 12\eta + 6 = 0.
\end{aligned}$$

The fields K_1 and K_{20} have degree 10 and signature $(2,4)$ and contain $\mathbb{Q}(\sqrt{5})$. Over K_1 and K_{20}, respectively, g_1 and g_{20} split into factors of degrees 2, 2, 4, 4, 4, 4, and the two fields were chosen for this splitting. The octic fields K'_{17}, K'_{18} and K'' are generated by roots of factors of degree 8 of g_{17} and g_{18}. The first two have signature $(4,2)$ and are isomorphic, since their defining polynomials are reciprocal to each other, and K'' has signature $(0,4)$. Over each of them g_{17} and g_{18} acquire linear factors.

i	K	degrees of the factors of g_i over K	n	tuples	admissible tuples
10, 26	$\mathbb{Q}(\sqrt[3]{5})$	1, 1, 2, 2, 2, 4, 4, 4	5	0	none
17	K'_{17}	1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2	9	0	none
18	K'_{18}	1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2	9	0	none
17, 18	K''	1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2	9	0	none
1	K_1	2, 2, 4, 4, 4, 4	8	1	one: the classes at $(0,1)$
2	$\mathbb{Q}(\sqrt[3]{5})$	1, 1, 2, 2, 2, 4, 4, 4	5	46656	one (Proposition 5.2)
3, 4	$\mathbb{Q}(\sqrt{-5})$	2, 2, 4, 4, 8	4	9, 1	one: the classes at $(0,1)$
20	K_{20}	2, 2, 4, 4, 4, 4	10	1	one: the classes at $(2,0)$

TABLE 4. The descents for $i \in \mathcal{I}_{\mathrm{r}}$; $n = \dim_{\mathbb{F}_3} K(\Sigma,3)$. The column "tuples" is the number of tuples $(e_1,\dots,e_k) \in K(\Sigma,3)^k$ in which, for each j separately, the localizations of e_j lie in the projections of the computed sets containing $\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_5$ (Section 3.2) to the factor F_j. The admissible tuples (Section 3.3) are those among them that also satisfy the conditions on the whole tuple.

Proposition 5.1. *Let $i \in \{10,17,18,26\}$. There are no coprime integers u,v such that $g_i(u,v)$ is a nonzero cube and (2.2) holds for each $p \in \{2,3,5\}$. In particular no Edwards triple of a solution with $z \neq 0$ has $i \in \{10,17,18,26\}$.*

Proof. Over the field K of Table 4, write $g_i = cF_1 \cdots F_k$ as in Lemma 3.1, with the linear factors u and v included when they divide g_i (as for $i = 10$). In each case some factor F_j has no class $e \in K(\Sigma,3)$ whose localizations lie in the projections of the sets $\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_5$ to that factor (Appendix B). By Lemma 3.1 and Lemma 3.4, whose proof uses only conditions (i)–(iii) of Section 3.2 at p, there is no pair as in the statement. For $i = 17$ and $i = 18$ each of the two octic fields used suffices. □

We call $(0,1)$ the *reference pair* of forms 1, 2, 3 and 4, and $(2,0)$ that of form 20.

Proposition 5.2. *Let (i,u,v) be an Edwards triple of a solution with $z \neq 0$, with $i \in \{1,2,3,4,20\}$, and let K be the field of Table 4 for i. Let $F \in K[u,v]$ be an irreducible factor of g_i over K.*

(i) *If $i \in \{1,3,4\}$, then $F(u,v) \in F(0,1)\,K^{\times 3}$.*

(ii) *If $i = 20$, then $F(u, v) \in F(2, 0)\, K^{\times 3}$.*

(iii) *If $i = 2$, then $u \in 2\, K^{\times 3}$, and $F(u, v) \in F(0, 1)\, K^{\times 3}$ unless F is a constant multiple of u.*

These statements do not depend on how the factors are normalized: multiplying F by a constant $\kappa \in K^\times$ multiplies both sides by κ. In (i)–(iii) the right-hand sides are nonzero: $g_1(0, 1) = -1$, $g_3(0, 1) = 1$, $g_4(0, 1) = -1$ and $g_{20}(2, 0) = -2^{36}$, and the factors of g_2 other than u do not vanish at $(0, 1)$. The pair $(2, 0)$, which is not coprime, is a point at which g_{20} takes a cube value.

Proof. Over K, write $g_i = cF_1 \cdots F_k$ as in Lemma 3.1, with the factors u and v included for $i = 2$. Since $z \neq 0$, no $F_j(u, v)$ vanishes. For each of the five forms exactly one tuple $(e_1, \ldots, e_k)$ is admissible (Appendix B), so it is the tuple $([F_j(u, v)])_j$. For $i \in \{1, 3, 4\}$ it equals $([F_j(0, 1)])_j$, as it must, since $(i, 0, 1)$ is itself an Edwards triple of a solution with $z \neq 0$ (Section 2). For $i = 20$ it equals $([F_j(2, 0)])_j$. For $i = 2$ it equals $[F_j(0, 1)]$ at every factor other than u, and $[2]$ at the factor u. These identifications are computations in $K(\Sigma, 3)$ (Appendix B). □

Remark 5.3. Over the smaller fields $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-5}, \sqrt{2})$, forms 17 and 18 keep the class of the pair $(0, 25)$, at which g_{17} and g_{18} take cube values but which is not coprime. The octic fields remove it. The class of $(2, 0)$ for form 20 also survives over the quartic and quintic fields generated by roots of $y^4 - 10y^2 - 15y - 5$ and $y^5 - y^4 - 8y^3 + 16y^2 - 7y + 1$, over which g_{20} factors, and over the field of degree 20 generated by a root of g_{20}. At 2, the only prime at which $(2, 0)$ fails (2.2), its local classes coincide with those of pairs that satisfy (2.2), so local conditions are unlikely to remove it. Form 20 is therefore treated with the curve of Section 7. Descents over $\mathbb{Q}$ itself give a weaker form of Proposition 5.2: for $i = 2$, $u = 50a^3$ and $v = b^3$ with $a, b \in \mathbb{Z}$, and each of the three sextic factors of g_2 over $\mathbb{Q}$ takes a cube value.

Example 5.4. We describe the descent for form 3 over $K = \mathbb{Q}(\sqrt{-5})$ in detail. The primes of K above 2, 3 and 5 are $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$ and $\mathfrak{p}_5$, with $2 = \mathfrak{p}_2^2$, $3 = \mathfrak{p}_3\mathfrak{p}_3'$, $5 = \mathfrak{p}_5^2$ and $1 + \sqrt{-5} \in \mathfrak{p}_3$. The class number of K is 2, and $\mathfrak{p}_2$ is not principal. The Σ-units 2, $\sqrt{-5}$, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ generate the ideals $\mathfrak{p}_2^2$, $\mathfrak{p}_5$, $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3'$, which span a sublattice of index 2 in the group of ideals supported on Σ. The principal ideals form a sublattice of the same index, so these four elements generate $\mathcal{O}_\Sigma^\times$ modulo ± 1, and their classes form a basis of $K(\Sigma, 3) \simeq \mathbb{F}_3^4$. Over K, $g_3 = F_1F_2F_3F_4F_5$ with

$$F_1 = Q_3 = v^2 + (-5 + 2\sqrt{-5})u^2, \qquad F_2 = \overline{Q_3},$$
$$F_3 = v^4 + 12\sqrt{-5}\, u^2v^2 - 45u^4, \qquad F_4 = \overline{F_3},$$
$$F_5 = v^8 - 180u^2v^6 - 3330u^4v^4 - 8100u^6v^2 + 2025u^8,$$

where Q_3 is the form of Section 6, the bar denotes complex conjugation, and F_5 is irreducible over K. Each F_j has content ideal (1) and $F_j(0, 1) = 1$, so $c = 1$. The local conditions are those of the computed sets of Section 3.2, which contain $\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_5$. For each factor, the conditions at 2 leave 27 of the 81 classes in $K(\Sigma, 3)$. The conditions at 3 then leave 9, 9, 1, 1, 3 of them, and those at 5 leave 3, 3, 1, 1, 1. Of the 9 tuples formed from these classes, only the zero tuple is admissible. It is the tuple of classes at $(0, 1)$, and so $F_j(u, v)$ is a cube in K for every j. Section 6 uses this for $F_1 = Q_3$.

6. Form 3

Form 3 gives only the trivial solution $(0,-1,-1)$ (Proposition 6.1). The cube condition of Proposition 5.2 on one quadratic factor of g_3 over $\mathbb{Q}(\sqrt{-5})$ leads to a genus-2 curve, and an unramified double covering of it leads to an elliptic curve over $\mathbb{Q}$ whose only rational point is the point at infinity.

Let $K=\mathbb{Q}(\sqrt{-5})$, with ring of integers $\mathbb{Z}[\sqrt{-5}]$. Over $\mathbb{Q}$ the form g_3 has the factor

$$45u^4-10u^2v^2+v^4=Q_3(u,v)\,\overline{Q_3}(u,v),\qquad Q_3=v^2+(-5+2\sqrt{-5})\,u^2,$$

where the bar denotes complex conjugation. The form Q_3 is irreducible over K: it factors only if $5-2\sqrt{-5}$ is a square in K, and its norm 45 is not a square. So Q_3 is a constant multiple of one of the two irreducible quadratic factors of g_3 over K (Appendix B). Let

$$\Phi(m,n)=2m^3+15m^2n-30mn^2-25n^3.$$

Proposition 6.1. *Let $(3,u,v)$ be an Edwards triple of a solution with $z\neq 0$. Then $(u,v)=\pm(0,1)$, and the solution is $(0,-1,-1)$.*

Proof. The cube. By Proposition 5.2(i), $Q_3(u,v)\in Q_3(0,1)K^{\times 3}=K^{\times 3}$. So $Q_3(u,v)=\gamma^3$ with $\gamma\in K$, and γ is integral because $Q_3(u,v)\in\mathbb{Z}[\sqrt{-5}]$. Write $\gamma=m+n\sqrt{-5}$ with $m,n\in\mathbb{Z}$. Since $\gamma^3=(m^3-15mn^2)+(3m^2n-5n^3)\sqrt{-5}$,

$$v^2-5u^2=m^3-15mn^2,\qquad 2u^2=n(3m^2-5n^2),\qquad\text{hence}\qquad 2v^2=\Phi(m,n).$$

Coprimality. If a prime p divides m and n, then p^3 divides v^2-5u^2 and $2u^2$. This gives $p\mid u$ and then $p\mid v$, contradicting $\gcd(u,v)=1$. So $\gcd(m,n)=1$.

Reduction to finitely many curves. If $u=0$ then $(u,v)=\pm(0,1)$. Suppose $u\neq 0$. Then $n\neq 0$, and $\gcd(n,3m^2-5n^2)=\gcd(n,3m^2)$ divides 3. Since $n(3m^2-5n^2)=2u^2$, every prime $p\geq 5$ divides at most one of the two factors, to an even power. Hence $n=da^2$ with $a\in\mathbb{Z}$ and d a squarefree divisor of 6 (with sign), and $3m^2-5n^2=2db^2$ with $b=u/(da)\in\mathbb{Q}$. Put $x=m/n$, $t=b/n$ and $s=v/(d^2a^3)$. Then $3x^2-5=2dt^2$ and, since $2v^2=n^3\Phi(x,1)=d^3a^6\Phi(x,1)$, also $\Phi(x,1)=2ds^2$. So (x,t,s) is a rational point of the curve

$$D_d:\quad 3x^2-5=2dt^2,\qquad 2x^3+15x^2-30x-25=2ds^2.$$

Local conditions. For $d\neq 6$ the curve D_d has no affine point $(x,t,s)\in\mathbb{Q}_p^3$ for the following p (Appendix B): $d=1$: $p=2,3$; $d=-1$: $p=2$; $d=2$: $p=2,5$; $d=-2$: $p=3,5$; $d=3$: $p=2,3,5$; $d=-3$: $p=2,5$; $d=-6$: $p=2,3$. So $d=6$.

The elliptic curve. For $d=6$ the second equation reads $12s^2=\Phi(x,1)$. With $X=24x$ and $Y=288s$ it becomes

$$E_6:\quad Y^2=X^3+180X^2-8640X-172800.$$

The cubic on the right is irreducible over $\mathbb{Q}$ (it is $6912\,\Phi(X/24,1)$), so $E_6(\mathbb{Q})[2]=0$. The 2-Selmer group of E_6 over $\mathbb{Q}$ is trivial (Appendix B), so $E_6(\mathbb{Q})$ has rank 0. Its torsion is trivial, since the $\#E_6(\mathbb{F}_p)$ for the primes $7\leq p\leq 43$ of good reduction have greatest common divisor 1. So $E_6(\mathbb{Q})=\{O\}$, which contradicts the existence of the affine point (X,Y). Hence $u=0$. Finally $(f_3,g_3,h_3)(0,\pm 1)=(0,1,-1)$ gives the solution $(0,-1,-1)$. □

Remark 6.2. The curve D_d is an unramified double covering of the genus-2 curve $Y^2=n(3m^2-5n^2)\Phi(m,n)$, on which $(m:n:2uv)$ is a rational point. The Jacobian of the genus-2 curve has rank at most 1 by a 2-descent, but the covering argument above avoids Chabauty's method altogether. The elliptic curve E_6 has conductor 24300, and numerically $L(E_6,1)=2.1066\ldots\neq 0$, in agreement with rank 0. The proof does not use this.

7. Forms 1 and 20

This section shows that forms 1 and 20 give only the trivial solution $(\pm 1, 0, 1)$ (Proposition 7.2). Both lead to rational points on the genus-2 curve

$$C:\ y^2 = \Psi(x), \qquad \Psi(x) = 25x^6 - 342x^5 + 1920x^4 - 5700x^3 + 9525x^2 - 8550x + 3250$$

(Proposition 7.1), and we determine $C(\mathbb{Q})$ by elliptic Chabauty over a cubic field together with a Mordell–Weil sieve (Theorem 7.10). The polynomial Ψ has no real root. Its leading coefficient is a square, so C has two rational points $\infty_\pm$ at infinity, at which $y/x^3 = \pm 5$.

7.1. **From the forms to the curve.** For $i \in \{1, 20\}$ the form g_i involves only u^5 and v^5: $g_i(u, v) = \widehat{g}_i(u^5, v^5)$ with

$$\widehat{g}_1(X, Y) = -429981696X^4 + 680804352X^3Y - 10243584X^2Y^2 - 32832XY^3 - Y^4,$$
$$\widehat{g}_{20}(X, Y) = -65536X^4 + 8404992X^3Y - 10243584X^2Y^2 - 2659392XY^3 - 6561Y^4.$$

Over $\mathbb{Q}(\sqrt{5})$, $\widehat{g}_1 = -429981696\, R_1\overline{R_1}$ and $\widehat{g}_{20} = -65536\, R_{20}\overline{R_{20}}$, where the bar denotes the nontrivial automorphism of $\mathbb{Q}(\sqrt{5})$ and $R_i = A_i + B_i\sqrt{5}$ with

$$A_1 = X^2 - \tfrac{19}{24}XY - \tfrac{1}{20736}Y^2, \qquad B_1 = -\tfrac{25}{72}XY,$$
$$A_{20} = X^2 - \tfrac{513}{8}XY - \tfrac{81}{256}Y^2, \qquad B_{20} = -\tfrac{225}{8}XY.$$

Put $\delta_1 = R_1(0, 1) = -1/20736$ and $\delta_{20} = R_{20}(2^5, 0) = 1024$. These are the values of R_i at (u^5, v^5) for the reference pairs $(u, v) = (0, 1)$ and $(2, 0)$ of Proposition 5.2. Let

$$\begin{aligned}\widetilde{\Psi}(m, n) &= n^6\Psi(m/n)\\ &= 25m^6 - 342m^5n + 1920m^4n^2 - 5700m^3n^3 + 9525m^2n^4 - 8550mn^5 + 3250n^6.\end{aligned}$$

Proposition 7.1. *Let (i, u, v) be an Edwards triple of a solution with $z \neq 0$, with $i \in \{1, 20\}$, and put $(X, Y) = (u^5, v^5)$. Then $R_i(X, Y) = \delta_i\gamma^3$ for some $\gamma = m + n\sqrt{5}$ with $m, n \in \mathbb{Q}$ not both zero, and*

$$\Big(\frac{5\,(X^2 + \epsilon_i Y^2)}{\delta_i}\Big)^2 = \widetilde{\Psi}(m, n), \qquad \epsilon_1 = \frac{1}{20736}, \quad \epsilon_{20} = \frac{81}{256}.$$

In particular $(m : n)$ is the x-coordinate of a rational point of C (with $n = 0$ for the points at infinity).

Proof. The cube. The field K_i of Table 4 contains $\mathbb{Q}(\sqrt{5})$, and over K_i the form $R_i(u^5, v^5)$ factors into irreducible factors of degrees 2, 4, 4, each of which is a factor of g_i (Appendix B). By Proposition 5.2, each of them takes at (u, v) a value in the class of its value at the reference pair, so $R_i(X, Y) \in \delta_i K_i^{\times 3}$. Let $\alpha = R_i(X, Y)/\delta_i \in \mathbb{Q}(\sqrt{5})$, so that $\alpha = \beta^3$ with $\beta \in K_i$. Here $\alpha \neq 0$: if $R_i(X, Y) = 0$ with $X, Y \in \mathbb{Q}$, then $B_i(X, Y) = 0$ gives $XY = 0$, and then $A_i(X, Y) \neq 0$ unless $X = Y = 0$. Since $[K_i : \mathbb{Q}(\sqrt{5})] = 5$, taking norms from K_i to $\mathbb{Q}(\sqrt{5})$ gives $\alpha^5 = N(\beta)^3$, so $\alpha = (\alpha^2/N(\beta))^3$ is a cube in $\mathbb{Q}(\sqrt{5})$. Write $\alpha = \gamma^3$ with $\gamma = m + n\sqrt{5}$.

The curve. Since $X, Y \in \mathbb{Q}$, comparing the coefficients of 1 and $\sqrt{5}$ in $R_i(X, Y) = \delta_i(m + n\sqrt{5})^3$ gives

$$A_i(X, Y) = C_0 \coloneqq \delta_i(m^3 + 15mn^2), \qquad B_i(X, Y) = C_1 \coloneqq \delta_i(3m^2n + 5n^3).$$

Consider the pencil of quadratic forms $A_i + \nu B_i$. For the roots $\nu_\pm = (-57 \pm \sqrt{-1})/25$ of $25\nu^2 + 114\nu + 130$ the form $A_i + \nu_\pm B_i$ is a square:

$$A_1 + \nu_\pm B_1 = \Big(X \mp \frac{\sqrt{-1}}{144} Y\Big)^2, \qquad A_{20} + \nu_\pm B_{20} = \Big(X \mp \frac{9\sqrt{-1}}{16} Y\Big)^2,$$

because $57 + 25\nu_\pm = \pm\sqrt{-1}$ and $513 + 225\nu_\pm = \pm 9\sqrt{-1}$. Multiplying the two identities for ν_+ and ν_- gives

$$(X^2 + \epsilon_i Y^2)^2 = (C_0 + \nu_+ C_1)(C_0 + \nu_- C_1) = C_0^2 - \tfrac{114}{25} C_0 C_1 + \tfrac{130}{25} C_1^2 = \tfrac{\delta_i^2}{25}\, \widetilde{\Psi}(m, n),$$

where the last equality is a direct expansion. □

Proposition 7.2. *If (i, u, v) is an Edwards triple of a solution with $z \neq 0$ and $i \in \{1, 20\}$, then $i = 1$, $(u, v) = \pm(0, 1)$, and the solution is $(\pm 1, 0, 1)$. In particular form 20 has no Edwards triple of a solution with $z \neq 0$.*

The proof, given at the end of this section, uses Theorem 7.10, which determines $C(\mathbb{Q})$.

Remark 7.3. Numerically, the L-function of the Jacobian J of C vanishes to order 2 at $s = 1$. This suggests that $J(\mathbb{Q})$ has rank 2, the genus of C, in which case Chabauty's method on C over $\mathbb{Q}$ does not apply. The proof does not use this. Besides $\infty_\pm$, the only rational points of C with $x = m/n$ in lowest terms and $\max(|m|, |n|) \leq 10^5$ are $(3, \pm 8)$.

7.2. **The cubic field and the elliptic curve.** Let $K = \mathbb{Q}(\xi)$ with $\xi^3 - 18\xi - 12 = 0$. It is totally real, of discriminant $4860 = 2^2 \cdot 3^5 \cdot 5$, its class number is 1 (Appendix A), and its roots of unity are ± 1. Let $\sigma_1, \sigma_2, \sigma_3$ be its real embeddings, and Σ the set of primes of K above 2, 3 and 5: $2 = \mathfrak{p}_2 \mathfrak{p}_2'^2$, $3 = \mathfrak{p}_3^3$ and $5 = \mathfrak{p}_5 \mathfrak{p}_5'^2$, so $\#\Sigma = 5$. Over K, $\Psi = 25\, \Psi_2\, \Psi_4$ with Ψ_2, Ψ_4 monic and irreducible:

$$\Psi_2 = x^2 + \tfrac{-3\xi^2+14\xi-78}{25}\, x + \tfrac{3\xi^2-14\xi+28}{10},$$
$$\Psi_4 = x^4 + b_1 x^3 + b_2 x^2 + b_3 x + b_4, \qquad b_1 = \tfrac{3\xi^2-14\xi-264}{25}, \quad b_2 = \tfrac{-31\xi^2+166\xi+1972}{50},$$
$$b_3 = \tfrac{5\xi^2-34\xi-312}{5}, \quad b_4 = \tfrac{-\xi^2+10\xi+74}{2}.$$

Let $H : w^2 = \Psi_4(x)$, a curve of genus 1 over K, and put $b_2' = b_2 - b_1^2/4 = (-81\xi^2 + 578\xi + 7478)/625$. Let

$$E : \; V^2 = U^3 + a_2 U^2 + a_4 U + a_6,$$
$$a_2 = 4b_2, \qquad a_4 = 16 b_1 b_3 - 64 b_4, \qquad a_6 = 64(b_3^2 - 4 b_2 b_4 + b_1^2 b_4),$$

so that $a_2 = (-62\xi^2 + 332\xi + 3944)/25$, $a_4 = (-20160\xi^2 + 126848\xi + 988864)/125$ and $a_6 = (-1624448\xi^2 + 12660480\xi + 80522752)/625$. The norm of the discriminant of E is $2^{76} 3^{10} 5^{-12}$, so E has good reduction at every prime of K outside Σ. The map $\iota : H \to E$,

$$U = 8(w + x^2 + \tfrac{b_1}{2} x), \qquad V = 8\big(2(U/4 + b_2')\, x + \tfrac{b_1}{8} U + b_3\big),$$

is an isomorphism, which sends the point at infinity of H with $w/x^2 \to 1$ to the origin O of E. The function x on H becomes the function

$$x = \frac{V - b_1 U - 8 b_3}{4(U + 4 b_2')}$$

of degree 2 on E, and the involution $w \mapsto -w$ of H becomes $P \mapsto P_1 - P$, where

$$P_1 = \Big(\tfrac{324\xi^2-2312\xi-29912}{625}, \; \tfrac{408\xi^2+15696\xi+40896}{15625}\Big)$$

is the image of the other point at infinity of H. Let

$$P_2 = \iota(3, w_3) = \Big(\tfrac{36\xi^2-248\xi-1208}{25},\ \tfrac{840\xi^2-3888\xi-2304}{125}\Big), \qquad w_3 = \tfrac{4-2\xi}{5},$$

so that $P_1 - P_2 = \iota(3, -w_3)$. The 2-torsion of E is $T = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}$ with

$$e_1 = \tfrac{8\xi^2-88\xi-1096}{25}, \qquad e_2 = \tfrac{24\xi^2-104\xi-1208}{25}, \qquad e_3 = \tfrac{6\xi^2-28\xi-328}{5},$$

and we put $T_3 = (e_3, 0)$. Translation by T_3 acts on x by $x \mapsto (5x - 10)/(2x - 5)$, a Möbius map defined over $\mathbb{Q}$. The eight points

$$O,\ P_1\ (x = \infty); \quad P_2,\ P_1{-}P_2\ (x = 3); \quad P_2{+}T_3,\ P_1{-}P_2{+}T_3\ (x = 5); \quad T_3,\ P_1{+}T_3\ (x = 5/2)$$

are the points of $E(K)$ with $x \in \mathbb{P}^1(\mathbb{Q})$ that we know. Only $x = \infty$ and $x = 3$ come from points of C: $\Psi(3) = 8^2$, while $\Psi(5) = 2^6 \cdot 5^3$ and $\Psi(5/2) = 5^5/2^6$ are not squares. All these formulas are identities in K (Appendix B).

Lemma 7.4. *If $(x_0, y_0) \in C(\mathbb{Q})$ and $x_0 \neq \infty$, then $\Psi_2(x_0)$ and $\Psi_4(x_0)$ are nonzero squares in K.*

Proof. Write $x_0 = m/n$ in lowest terms and put $\widetilde{\Psi}_2(m, n) = n^2\Psi_2(m/n)$ and $\widetilde{\Psi}_4(m, n) = n^4\Psi_4(m/n)$, so that $\widetilde{\Psi}_2\widetilde{\Psi}_4 = (n^3 y_0/5)^2$. Both are nonzero because Ψ has no real root. The coefficients of Ψ_2 and Ψ_4 are integral away from the primes above 5 (the denominators 2 in these coefficients are harmless: the coefficients of 1 and ξ in their numerators are even, and $\xi^2/2$, a root of $y^3 - 18y^2 + 81y - 18$, is integral), and the norm of $\mathrm{Res}(\Psi_2, \Psi_4)$ is $2^{16}3^{10}5^{-8}$. So at a prime $\mathfrak{p} \notin \Sigma$ the values $\widetilde{\Psi}_2(m, n)$, $\widetilde{\Psi}_4(m, n)$ are $\mathfrak{p}$-integral and not both divisible by $\mathfrak{p}$, and $v_\mathfrak{p}(\widetilde{\Psi}_2(m, n))$ is even. Hence the class δ of $\Psi_2(x_0)$ in $K^\times/K^{\times 2}$ lies in the group $K(\Sigma, 2)$ of classes with even valuation outside Σ. As the class number of K is 1, $K(\Sigma, 2) = \mathcal{O}_\Sigma^\times/\mathcal{O}_\Sigma^{\times 2}$, of dimension $1 + 2 + 5 = 8$, and eight explicit Σ-units whose quadratic characters at eight auxiliary primes have rank 8 form a basis. Since Ψ is irreducible over $\mathbb{Q}$, $\mathrm{N}_{K/\mathbb{Q}}(\Psi_2(x_0)) = \Psi(x_0)/25 = (y_0/5)^2$, so δ has square norm. The norm map from $K(\Sigma, 2)$ to the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by -1, 2, 3, 5 is surjective, so 16 of the 256 classes have square norm. At the real places, $\Psi_2^{\sigma_j}$ has no real root and $\Psi_2^{\sigma_j}(0) > 0$, so δ is totally positive. On the classes with square norm the signs at the three real places have rank 2 (their product is positive), so four classes remain.

For $p \in \{2, 3, 5\}$ we computed the set of classes of $\Psi_2(x)$ in $\prod_{\mathfrak{p}|p} K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ over the $x \in \mathbb{P}^1(\mathbb{Q}_p)$ with $\Psi(x)$ a square in $\mathbb{Q}_p$, by covering $\mathbb{P}^1(\mathbb{Q}_p)$ with discs $a + p^k\mathbb{Z}_p$ and $1/x \in p\mathbb{Z}_p$. On a disc the class of a polynomial f in $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ is constant when every term of its Taylor expansion at a satisfies $v(f^{(l)}(a)/l!) + e\,k\,l \geq v(f(a)) + 2v(2) + 1$ for $l \geq 1$, where v is the normalized valuation of $K_\mathfrak{p}$ and e its ramification index, since $1 + 4\pi\mathcal{O}_\mathfrak{p}$ consists of squares for a uniformizer π. Discs are split until Ψ and Ψ_2 pass this test. At $p = 5$ the test does not succeed on two discs of radius 5^{-40} around the two roots of Ψ in $\mathbb{Q}_5$ (for the root of valuation -2, the disc is taken in the coordinate $1/x$). Each of these roots is a root of Ψ_2 in the completion at the unramified prime $\mathfrak{p}_5$ and a root of Ψ_4 in the completion at the ramified prime $\mathfrak{p}_5'$. On these two discs we use Ψ_4 at $\mathfrak{p}_5$ and Ψ_2 at $\mathfrak{p}_5'$, which pass the test there. This is allowed because, when $\Psi(x)$ is a square, the classes of $\Psi_2(x)$ and $\Psi_4(x)$ coincide, as their product $\Psi(x)/25$ is a square. After $p = 2$, two classes remain, $p = 3$ removes none, and after $p = 5$ only $\delta = 1$ remains (Appendix B). So $\Psi_2(x_0)$ is a square, and so is $\Psi_4(x_0) = (y_0/5)^2/\Psi_2(x_0)$. □

7.3. **The Mordell–Weil group.**

Lemma 7.5. *Let $\Gamma' \subseteq \Gamma$ be abelian groups with Γ/Γ' finite, ℓ a prime with $\Gamma[\ell] \subseteq \Gamma'$, and $\psi : \Gamma \to A$ a homomorphism to an abelian group A with $\ell A = 0$ whose restriction to Γ' induces an injection $\Gamma'/\ell\Gamma' \to A$. Then ℓ does not divide $[\Gamma : \Gamma']$.*

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

Proposition 7.6. *$E(K) \simeq \mathbb{Z}^2 \times (\mathbb{Z}/2)^2$ with torsion subgroup T, and the index n_0 of $\Gamma' = \mathbb{Z}P_1 + \mathbb{Z}P_2 + T$ in $E(K)$ is finite and prime to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 59$.*

The primes 2, 3, 5, 7 are those dividing the modulus $N_1 = 2^7 \cdot 3^2 \cdot 5 \cdot 7^2$ of the Mordell–Weil sieve in the proof of Proposition 7.7, and 59 is the prime at which Proposition 7.9 applies Chabauty's method.

Proof. Rank at most 2. The set Σ contains the primes above 2 and those dividing the differences $e_j - e_l$. The map $\kappa_2(P) = (U - e_1, U - e_2)$ (with the usual values at the points of T) embeds $E(K)/2E(K)$ into $K(\Sigma, 2)^2$, with image in the 2-Selmer group, which consists of the pairs that lie in the image of $E(K_v)$ at every $v \in \Sigma$ and at the three real places. For $v \in \Sigma$ the local image has dimension $2 + [K_v : \mathbb{Q}_2]$ if $v \mid 2$ and 2 otherwise, since $E(K_v)[2]$ has order 4. It was computed as the span of the images of local points, which reaches this dimension in every case. At a real place the image has dimension 1. The 2-Selmer group has dimension 4 (Appendix B), so $\operatorname{rank} E(K) \leq 4 - 2 = 2$.

Rank 2*, torsion, and the index at* 2. The quadratic characters of $\kappa_2(P_1)$, $\kappa_2(P_2)$, $\kappa_2((e_1, 0))$, $\kappa_2((e_2, 0))$ at auxiliary primes have rank 4. As $\dim_{\mathbb{F}_2} E(K)/2E(K) = \operatorname{rank} E(K) + 2 \leq 4$, these four images form a basis of $\kappa_2(E(K))$. Hence $\operatorname{rank} E(K) = 2$ and $E(K) = \Gamma' + 2E(K)$. As $E(K)$ is finitely generated, the quotient $E(K)/\Gamma'$ is then finite of odd order, so n_0 is finite and odd, and P_1, P_2 are independent points of infinite order. Moreover no point of $T \smallsetminus \{O\}$ lies in $2E(K)$, so $E(K)$ has no point of order 4. At a prime above 59 and at the prime of degree 1 above 37 the reductions have 64 and 32 points, so $E(K)$ has no torsion of odd order, and $E(K)_{\mathrm{tors}} = T$.

The index at $\ell = 3, 5, 7, 59$. For each ℓ, two primes $\mathfrak{q}$ of good reduction with cyclic ℓ-part of $E(\mathbb{F}_\mathfrak{q})$ give a homomorphism $E(K) \to \prod_\mathfrak{q} E(\mathbb{F}_\mathfrak{q})/\ell E(\mathbb{F}_\mathfrak{q})$, and the images of P_1, P_2 are independent. Each of the rational primes 13, 19, 23, 337, 457 has one prime of degree 1 and one of degree 2 above it, and we use the primes of degree 2 above 13 and of degree 1 above 23 for $\ell = 3$, of degree 1 above 13 and 19 for $\ell = 5$, of degree 2 above 19 and 23 for $\ell = 7$, and of degree 2 above 337 and 457 for $\ell = 59$. Since $E(K)[\ell] = 0$ and $T \subseteq \ell\Gamma'$ for odd ℓ, Lemma 7.5 gives $\ell \nmid n_0$. □

7.4. **The Mordell–Weil sieve.** For a point $P \in E(K)$ we write $x(P) \in \mathbb{P}^1(K)$ for the value of the function x. The modulus 224 in the next proposition is the least common multiple of the exponents 32, 28, 32 of the groups $E(\mathbb{F}_\mathfrak{q})$ at the three primes $\mathfrak{q}$ above 59, the prime used in Proposition 7.9.

Proposition 7.7. *Let $P \in E(K)$ with $x(P) \in \mathbb{P}^1(\mathbb{Q})$, and, if $x(P) \neq \infty$, with $\Psi(x(P))$ a square in $\mathbb{Q}$. Then $P \in P_0 + 224\,E(K)$ for some $P_0 \in \{O, P_1, P_2, P_1 - P_2\}$.*

Proof. Let $N_1 = 282240 = 2^7 \cdot 3^2 \cdot 5 \cdot 7^2$ and $\mathcal{Q} = \{59, 37, 23, 47, 79, 31\}$. For every prime $\mathfrak{q}$ of K above some $q \in \mathcal{Q}$, E has good reduction and the exponent of $E(\mathbb{F}_\mathfrak{q})$ divides N_1, and the six primes were chosen for this property. The groups are $\mathbb{Z}/32 \times \mathbb{Z}/2$, $\mathbb{Z}/28 \times \mathbb{Z}/2$, $\mathbb{Z}/32 \times \mathbb{Z}/2$ above 59; $\mathbb{Z}/8 \times \mathbb{Z}/4$ and $\mathbb{Z}/36 \times \mathbb{Z}/36$ above 37; $\mathbb{Z}/12 \times \mathbb{Z}/2$ and $\mathbb{Z}/252 \times \mathbb{Z}/2$

above 23; $\mathbb{Z}/24 \times \mathbb{Z}/2$ and $\mathbb{Z}/280 \times \mathbb{Z}/8$ above 47; $\mathbb{Z}/48 \times \mathbb{Z}/2$ and $\mathbb{Z}/384 \times \mathbb{Z}/16$ above 79; and $\mathbb{Z}/20 \times \mathbb{Z}/2$ and $\mathbb{Z}/490 \times \mathbb{Z}/2$ above 31. For $\mathfrak{q} \nmid 30$ the quartic Ψ_4 has $\mathfrak{q}$-integral coefficients and discriminant prime to $\mathfrak{q}$ (the norm of its discriminant is $2^{28}3^{10}5^{-12}$), so H has good reduction at $\mathfrak{q}$ and ι reduces to an isomorphism of the reductions.

Since n_0 is prime to N_1 (Proposition 7.6), $E(K) = \Gamma' + N_1 E(K)$. Write $P = k_1 P_1 + k_2 P_2 + \tau + N_1 R$ with $k_1, k_2 \in \mathbb{Z}$, $\tau \in T$ and $R \in E(K)$. Then $(k_1 \bmod N_1, k_2 \bmod N_1, \tau)$ is determined by P. Since N_1 kills $E(\mathbb{F}_\mathfrak{q})$, P and $P' = k_1 P_1 + k_2 P_2 + \tau$ have the same reduction at every $\mathfrak{q}$. Let $r = x(P) \in \mathbb{P}^1(\mathbb{Q})$. Since ι reduces to an isomorphism, the reduction of x takes the value $r \bmod q$ at the reduction of P for every $\mathfrak{q} \mid q$, and if $r \not\equiv \infty \pmod q$ then $\Psi(r) \bmod q$ is a square in $\mathbb{F}_q$. So (k_1, k_2, τ) must satisfy the following condition for each $q \in \mathcal{Q}$: there is $\varrho \in \mathbb{P}^1(\mathbb{F}_q)$ with $\varrho = \infty$, $\Psi(\varrho) = 0$ or $\Psi(\varrho)$ a nonzero square, such that x takes the value ϱ at the reduction of P' at every $\mathfrak{q} \mid q$. At q this condition depends on (k_1, k_2) modulo the least common multiple L_q of the orders of the reductions of P_1 and P_2 at the primes above q. Here $L_{59}, L_{37}, L_{23}, L_{47}, L_{79}, L_{31}$ are 224, 24, 252, 840, 384, 980, whose least common multiple is N_1. Enumerating the classes at each q and lifting compatible classes to the least common multiple of the moduli leaves 336 classes modulo N_1 (Appendix B). Reduced modulo 224, they give exactly four classes, $(0, 0, O)$, $(1, 0, O)$, $(0, 1, O)$ and $(1, -1, O)$, those of O, P_1, P_2 and $P_1 - P_2$. Since $P - P' \in N_1 E(K) \subseteq 224\, E(K)$, the proposition follows. □

The classes of the four translates by T_3 are removed at $q = 37$, where $\Psi(5)$ and $\Psi(5/2)$ are not squares in $\mathbb{F}_{37}$. The number of surviving classes stays roughly constant as primes are added (336, 112, 72, 240, 240, 336 classes modulo 224, 672, 2016, 10080, 40320, 282240), as one expects when the rank is one less than the degree of K. So the sieve alone does not finish, and Proposition 7.9 completes the argument.

7.5. **Chabauty's method.**

Lemma 7.8. *Let K be a number field of degree d and $p \geq 3$ a prime that splits completely in K, with embeddings $\sigma_1, \ldots, \sigma_d : K \to \mathbb{Q}_p$. Let E/K be given by $V^2 = U^3 + a_2 U^2 + a_4 U + a_6$ such that each conjugate E^{σ_j} has coefficients in $\mathbb{Z}_p$ and good reduction. Suppose that $E(K)$ has rank $r \leq d - 1$, and let $Q_1, \ldots, Q_r \in E(K)$ with $p \nmid [E(K) : \langle Q_1, \ldots, Q_r \rangle + E(K)_{\mathrm{tors}}]$. 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 $D = 2V\,\partial/\partial U + (3U^2 + 2a_2 U + a_4)\,\partial/\partial V$, the derivation dual to the invariant differential $\omega = dU/2V$. Let $P_0 \in E(K)$ 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 $c_j = \sigma_j((D\rho)(P_0))$; 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 $\lambda_{ij} = \log_j(N \cdot Q_i^{\sigma_j})$, 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 $P \in P_0 + N \cdot E(K)$ with $\rho(P) \in \mathbb{Q}$.

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 [33, VII.2.2, IV.6.4]. For $R \in E(K)$, $N \cdot R^{\sigma_j} \in E_1^{(j)}$ because N kills $E^{\sigma_j}(\mathbb{F}_p)$. Let $m = [E(K) : \langle Q_i \rangle + E(K)_{\mathrm{tors}}]$, so that $p \nmid m$ and $mR = \sum_i b_i Q_i + \tau$ with $b_i \in \mathbb{Z}$ and τ torsion. Torsion injects into $E^{\sigma_j}(\mathbb{F}_p)$ [33, VII.3.1, IV.6.4],

so $N\tau = 0$. Hence $\log_j(N \cdot R^{\sigma_j}) = \sum_i \beta_i \lambda_{ij}$ with $\beta_i = b_i/m \in \mathbb{Z}_p$, the same β for every j. So every $P \in P_0 + N \cdot E(K)$ 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.

(b) *Integrality.* Write $\exp_j(T) = \sum_k \epsilon_k T^k$ with $k!\,\epsilon_k \in \mathbb{Z}_p$ [33, 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 $\Delta(\beta) = \big(f_1(z_1(\beta)) - f_j(z_j(\beta))\big)_{2 \leq j \leq d}$. By (b), $\Delta(\beta) = p\,(\mathcal{J}'\beta + p\,\Omega(\beta))$ 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 $\Delta(\beta) = \Delta(\beta') = 0$ 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. □

Proposition 7.9. *Let $P_0 \in \{O, P_1, P_2, P_1 - P_2\}$. Then P_0 is the only point $P \in P_0 + 224\,E(K)$ with $x(P) \in \mathbb{P}^1(\mathbb{Q})$.*

Proof. Apply Lemma 7.8 with $d = 3$, $r = 2$, $p = 59$, $N = 224$, $Q_1 = P_1$ and $Q_2 = P_2$. The prime 59 is the smallest prime that splits completely in K, as Lemma 7.8 requires, and we order the embeddings $\sigma_j : K \to \mathbb{Q}_{59}$ by $\sigma_j(\xi) \equiv 11, 23, 25 \pmod{59}$. The points P_1, P_2 and $P_1 - P_2$ have 59-integral coordinates, so no conjugate of them reduces to the origin. Each E^{σ_j} has 59-integral coefficients and good reduction, the groups $E(\mathbb{F}_\mathfrak{q})$ for $\mathfrak{q} \mid 59$ have exponents 32, 28, 32, which divide 224, and $59 \nmid n_0$ by Proposition 7.6. For $P_0 \in \{O, P_1\}$ take $\rho = 1/x = 4(U + 4b_2')/(V - b_1U - 8b_3)$. At O (case (ii)), write $U = t/s(t)$ and $V = -1/s(t)$, where $s(t) \in t^3\mathbb{Z}_{59}[[t]]$ is the power series of the formal group [33, IV.1]. Then $\rho = 4(t + 4b_2's)/(-1 - b_1t - 8b_3s) \in \mathbb{Z}_{59}[[t]]$, and $c_j = -4$. At P_1 (case (i)), $V - b_1U - 8b_3$ is a 59-adic unit at every σ_j. For $P_0 \in \{P_2, P_1 - P_2\}$ take $\rho = x$, whose denominator $4(U + 4b_2')$ is a 59-adic unit at every $P_0^{\sigma_j}$. In each case ρ is 59-adically integral on the whole coset, by (b) of the proof of Lemma 7.8, so for P in the coset, $\rho(P) \in \mathbb{Q}$ exactly when $x(P) \in \mathbb{P}^1(\mathbb{Q})$. The logarithms λ_{ij} are computed modulo 59^2 as the formal parameters of $224 \cdot P_i^{\sigma_j}$, which is allowed because these parameters lie in $59\mathbb{Z}_{59}$, the formal logarithm has the form $\sum_k a_k t^k/k$ with $a_k \in \mathbb{Z}_{59}$ [33, IV.5.5], and $v(t^k/k) \geq 2$ for $k \geq 2$. The matrices $\mathcal{J}/59$ modulo 59 are

$$\begin{pmatrix} 46 & 24 \\ 41 & 36 \end{pmatrix}, \quad \begin{pmatrix} 13 & 35 \\ 18 & 23 \end{pmatrix}, \quad \begin{pmatrix} 15 & 5 \\ 56 & 33 \end{pmatrix}, \quad \begin{pmatrix} 44 & 54 \\ 3 & 26 \end{pmatrix}$$

at O, P_1, P_2 and $P_1 - P_2$, all of rank 2 (Appendix B). □

Theorem 7.10. $C(\mathbb{Q}) = \{\infty_+, \infty_-, (3, 8), (3, -8)\}$.

Proof. Let $(x_0, y_0) \in C(\mathbb{Q})$ with $x_0 \neq \infty$. By Lemma 7.4, $\Psi_4(x_0) = w_0^2$ with $w_0 \in K$, so $P = \iota(x_0, w_0) \in E(K)$ has $x(P) = x_0 \in \mathbb{Q}$, and $\Psi(x_0) = y_0^2$. By Propositions 7.7 and 7.9, $P \in \{O, P_1, P_2, P_1 - P_2\}$. Since $x(O) = x(P_1) = \infty$, we get $x_0 = 3$ and $y_0 = \pm 8$. □

Proof of Proposition 7.2. By Proposition 7.1 and Theorem 7.10, $(m : n)$ is $(1 : 0)$ or $(3 : 1)$. If $(m : n) = (1 : 0)$, then $C_1 = 0$, so $B_i(X, Y) = 0$ and $XY = 0$. If $(m : n) = (3 : 1)$,

then $(C_0 : C_1) = (72 : 32)$, and the equation $32A_i(X,Y) = 72B_i(X,Y)$, which with $Y = 0$ forces $X = 0$, gives $X/Y \in \{-1/288, 1/72\}$ for $i = 1$ and $X/Y \in \{-9/32, 9/8\}$ for $i = 20$. None of these four numbers is the fifth power of a rational number, while $X/Y = (u/v)^5$. Hence $uv = 0$, and as u, v are coprime, (u, v) is $\pm(1, 0)$ or $\pm(0, 1)$. Now $g_1(1, 0) = -2^{16}3^8$, $g_{20}(1, 0) = -2^{16}$ and $g_{20}(0, 1) = -3^8$ are not cubes, so $i = 1$ and $(u, v) = \pm(0, 1)$, which gives the solution $(\pm 1, 0, 1)$ (Section 2). □

8. Form 2

This section shows that form 2 has no Edwards triple of a solution with $z \neq 0$ (Proposition 8.4). The classes of Proposition 5.2(iii) over $K = \mathbb{Q}(\sqrt[3]{5})$ give a K-point on a plane cubic curve, which maps to the elliptic curve $Y^2 = X^3 + 36\sqrt[3]{5}$, and a descent via 3-isogeny shows that this curve has no K-point other than its origin.

Let $\theta = \sqrt[3]{5}$ be the real cube root and $K = \mathbb{Q}(\theta)$. We have

$$g_2(u, v) = -20\, u\, v\, \mathcal{S}_1\mathcal{S}_2\mathcal{S}_3, \qquad \begin{aligned} \mathcal{S}_1 &= 40u^6 - 5u^3v^3 + v^6, \\ \mathcal{S}_2 &= 320u^6 + 320u^3v^3 - v^6, \\ \mathcal{S}_3 &= 2560u^6 + 40u^3v^3 + v^6, \end{aligned}$$

and over K, $\mathcal{S}_k(x, 1) = c_k A_k(x) B_k(x)$ with $c_k = 40, 320, 2560$, B_k monic of degree 4, and

$$A_1 = x^2 + \tfrac{\theta}{2}x + \tfrac{\theta^2}{10}, \qquad A_2 = x^2 + \tfrac{\theta}{2}x - \tfrac{\theta^2}{20}, \qquad A_3 = x^2 - \tfrac{\theta}{4}x + \tfrac{\theta^2}{40}.$$

For $D \in K^\times$ let E_D be the elliptic curve $Y^2 = X^3 + D$ over K.

Lemma 8.1. *Let $x_0 \in K^\times$ and $w \in K$ with $x_0A_2(x_0) = 2A_2(0)\, w^3 = -\frac{\theta^2}{10}w^3$. Then $(X, Y) = (2w/x_0,\ 2\theta^2 - 2/x_0)$ lies on $E_{36\theta}$. Similarly, if $x_0A_1(x_0) = 2A_1(0)\, w^3 = \frac{\theta^2}{5}w^3$, then $(2w/x_0,\ \theta^2 + 2/x_0)$ lies on $E_{-3\theta}$.*

Proof. From $x_0A_2(x_0) = -(\theta^2/10)w^3$ we get $8w^3/x_0^3 = -80A_2(x_0)/(\theta^2x_0^2)$. Expanding with $\theta^3 = 5$, $1/\theta^2 = \theta/5$ and $1/\theta = \theta^2/5$ gives $X^3 = -16\theta - 8\theta^2/x_0 + 4/x_0^2$, so $X^3 + 36\theta = 20\theta - 8\theta^2/x_0 + 4/x_0^2$. This equals $Y^2 = 4\theta^4 - 8\theta^2/x_0 + 4/x_0^2$, since $4\theta^4 = 20\theta$. For the second statement, $w^3 = \theta x_0A_1(x_0)$, so $X^3 = 8\theta + 4\theta^2/x_0 + 4/x_0^2$ and $X^3 - 3\theta = 5\theta + 4\theta^2/x_0 + 4/x_0^2 = (\theta^2 + 2/x_0)^2$. □

The map was found as follows. With $s = 1/x$ and $W = w/x$, the curve $xA(x) = 2A(0)w^3$, for $A = x^2 + a_1x + a_0$, becomes $a_0s^2 + a_1s + 1 = 2a_0W^3$. Completing the square gives a Mordell curve $Y^2 = X^3 + 64a_0^4(a_1^2 - 4a_0)$, and for A_2 the constant is $36\theta \cdot (\theta^2/10)^6$.

Proposition 8.2. *$E_{36\theta}(K) = \{O\}$ and $E_{-3\theta}(K) = \{O\}$.*

Proof. Let $D \in \{36\theta, -3\theta\}$, $E = E_D$ and $E' = E_{-27D}$. Let $\phi : E \to E'$ be the 3-isogeny $(X, Y) \mapsto ((X^3 + 4D)/X^2,\ Y(X^3 - 8D)/X^3)$, with kernel $\{O, (0, \pm\sqrt{D})\}$, and $\hat{\phi}$ its dual, so that $\hat{\phi} \circ \phi = [3]$.

Torsion. The discriminant of E is $-432D^2$, so E has good reduction at every prime of K not above 2, 3, 5. Reduction at a prime $\mathfrak{q}$ of good reduction is injective on the torsion of order prime to the characteristic of $\mathfrak{q}$ [33, VII.3.1]. At the prime of degree 1 above 11 (where $\theta \equiv 3$) the reduction has 12 points, and at the prime of degree 1 above 13 with $\theta \equiv 11$ it has 7 points, for both values of D. So a point of prime order ℓ in $E(K)$ would have $\ell = 11$ or $\ell \mid 12$, and $\ell = 13$ or $\ell \mid 7$, which is impossible. Hence $E(K)_{\mathrm{tors}} = 0$.

The rank formula. Neither D nor $-3D$ is a square in K: the norm of D is 2^63^65 or -3^35, $-3 \cdot 36\theta < 0$ at the real place, and $-3 \cdot (-3\theta) = 9\theta$ with θ not a square, as its norm is 5.

So $E(K)[\phi] = 0$ and $E'(K)[\hat{\phi}] = 0$. Put $L = K(\sqrt{D})$ and $L' = K(\sqrt{-27D})$. The function $Y - \sqrt{D}$ has divisor $3(0, \sqrt{D}) - 3\,O$, so $\alpha : E(K) \to L^\times/L^{\times 3}$, $P \mapsto Y(P) - \sqrt{D}$ (with $\alpha(O) = 1$), is a homomorphism with kernel $\hat{\phi}(E'(K))$ (as for $K = \mathbb{Q}$ in [10, Proposition 1.4]). Its image lies in the kernel of the norm to $K^\times/K^{\times 3}$ because $(Y - \sqrt{D})(Y + \sqrt{D}) = X^3$. In the same way $\alpha' : E'(K) \to L'^\times/L'^{\times 3}$, $P \mapsto Y(P) - \sqrt{-27D}$, has kernel $\phi(E(K))$. Since $E(K)[3] = 0$ and $E'(K)[\hat{\phi}] = 0$, the sequence

$$0 \to E'(K)/\phi E(K) \xrightarrow{\hat{\phi}} E(K)/3E(K) \to E(K)/\hat{\phi}E'(K) \to 0$$

is exact, and $\operatorname{rank} E(K) = \dim_{\mathbb{F}_3} \alpha(E(K)) + \dim_{\mathbb{F}_3} \alpha'(E'(K))$.

Selmer groups. Let Σ be the set of primes of K above 2, 3 and 5: $2 = \mathfrak{p}_2\mathfrak{p}_2'$ with residue degrees 1 and 2, $3 = \mathfrak{p}_3^3$ and $5 = \mathfrak{p}_5^3$. The image of α lies in the Selmer group of classes $a \in L(\Sigma, 3)$ with norm a cube in K and with a in the image $\operatorname{Im}\alpha_v$ of the local Kummer map on $E(K_v)$ for every $v \in \Sigma$. Here $L(\Sigma, 3)$ is the group of classes in $L^\times/L^{\times 3}$ with valuation divisible by 3 at every prime of L not above Σ. Outside Σ the local condition is the unramified one, which $L(\Sigma, 3)$ already encodes, and at the real place there is no condition, as $E[\phi]$ has odd order. The same holds for α' and L'. The two fields are $K(\sqrt{\theta}) = \mathbb{Q}(\sqrt[6]{5})$ and $K(\sqrt{-3\theta})$, the latter generated by a root of $t^6 - 3t^5 - 5t^3 + 15t^2 + 12t + 4$. For $D = 36\theta$, $L = K(\sqrt{\theta})$ and $L' = K(\sqrt{-3\theta})$, and for $D = -3\theta$ the roles are exchanged. The class number of $\mathbb{Q}(\sqrt[6]{5})$ is 1 and that of $K(\sqrt{-3\theta})$ divides 2 (Appendix A), and neither field contains a primitive cube root of unity. So $L(\Sigma, 3) = \mathcal{O}_{L,\Sigma}^\times/\mathcal{O}_{L,\Sigma}^{\times 3}$, of dimension 8 in both fields, with a basis of Σ-units checked by cubic residue characters at 68 auxiliary primes (Lemma 3.3). The subgroup of classes whose norm to K is a cube has dimension 3.

Local images. For $v \in \Sigma$, sampled points of $E(K_v)$ and $E'(K_v)$ span subspaces of $\operatorname{Im}\alpha_v$ and $\operatorname{Im}\alpha_v'$. The Weil pairing $E[\phi] \times E'[\hat{\phi}] \to \mu_3$ and local Tate duality [22, I.2.3] make $H^1(K_v, E[\phi])$ and $H^1(K_v, E'[\hat{\phi}])$ dual to each other, and under this duality the images of the Kummer maps of ϕ and $\hat{\phi}$ are exact annihilators of each other. This form of local Tate duality for an isogeny of elliptic curves is stated in [14, §2]. Hence

$$\dim \operatorname{Im}\alpha_v + \dim \operatorname{Im}\alpha_v' = \dim_{\mathbb{F}_3} H^1(K_v, E[\phi]).$$

By the local Euler characteristic formula [22, I.2.8] and local duality for H^2 [22, I.2.3], this dimension is $\varepsilon_v(D) + \varepsilon_v(-27D) + [K_v : \mathbb{Q}_3]$ if $v \mid 3$ and $\varepsilon_v(D) + \varepsilon_v(-27D)$ otherwise, where $\varepsilon_v(a) = 1$ if a is a square in K_v and 0 otherwise. Sampling continues until the dimensions of the two spans add up to this number, and then both spans are the full local images. For $D = 36\theta$ the dimensions of $\operatorname{Im}\alpha_v$ at $\mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3, \mathfrak{p}_5$ are $0, 1, 2, 0$, and those of $\operatorname{Im}\alpha_v'$ are $1, 1, 1, 0$. For $D = -3\theta$ the two lists are exchanged.

Result. For both values of D both Selmer groups are 0 (Appendix B). So $E(K)$ has rank 0, and $E(K) = E(K)_{\text{tors}} = \{O\}$. □

Remark 8.3. A 2-descent over K gives a second proof of $\operatorname{rank} E_D(K) = 0$. As $-D$ is not a cube in K, $X^3 + D$ is irreducible and $E_D(K)[2] = 0$. The descent runs over the field $K[T]/(T^3 + D)$ of degree 9 over $\mathbb{Q}$, whose class number divides 3 for $D = 36\theta$ and is 1 for $D = -3\theta$ (Minkowski's bound, as in Appendix A), and gives a trivial 2-Selmer group for both curves.

Proposition 8.4. *Form* 2 *has no Edwards triple* $(2, u, v)$ *of a solution with* $z \neq 0$.

Proof. Suppose $(2, u, v)$ is one. As $z \neq 0$, u and v are nonzero. By Proposition 5.2(iii), applied to the factor v (with $v(0, 1) = 1$) and to the factor of g_2 that is a constant multiple of

$v^2A_2(u/v)$, we have $u \in 2K^{\times 3}$, $v \in K^{\times 3}$ and $v^2A_2(u/v) \in A_2(0)K^{\times 3}$. Put $x_0 = u/v \in \mathbb{Q}^\times$. Then $x_0 \in 2K^{\times 3}$ and, as v^2 is a cube, $A_2(x_0) \in A_2(0)K^{\times 3}$. Moreover $A_2(x_0) \neq 0$: the discriminant of A_2 is $9\theta^2/20$, which is not a square in K because 5 is not, so A_2 has no root in K. Hence $x_0A_2(x_0) = 2A_2(0)w^3$ with $w \in K^\times$, and by Lemma 8.1 the point $(2w/x_0, 2\theta^2 - 2/x_0)$ lies in $E_{36\theta}(K) \smallsetminus \{O\}$. This contradicts Proposition 8.2. □

The same argument with A_1, the curve $E_{-3\theta}$ and the second half of Lemma 8.1 gives a second proof.

Remark 8.5. The curves $A_k(x) = A_k(0)W^3$ given by a single factor have Jacobians isomorphic over K to E_{-15} ($k = 1, 3$) or E_{720} ($k = 2$), which come from $\mathbb{Q}$ and have rank $3 = [K : \mathbb{Q}]$ over K. So elliptic Chabauty on them over K is not available. The factor x_0, whose class is fixed by the condition $u \in 2K^{\times 3}$, is what makes the argument above work.

9. Form 4

We show that form 4 gives only the trivial solution $(0, 1, 1)$ (Proposition 9.6). Over $K = \mathbb{Q}(\sqrt{-5})$ two factors of g_4 take cube values, and in the variables $U = u^2$, $V = v^2$ their product defines a curve of genus 1 over K itself, isomorphic to an elliptic curve E_A of rank 1. The condition that U and V are rational becomes the condition that a function on E_A has norm 1, and elliptic Chabauty at the prime 23 shows that only the point given by $(u, v) = \pm(0, 1)$ satisfies it.

9.1. **The curve.** Let $K = \mathbb{Q}(\sqrt{-5})$, with complex conjugation $\alpha \mapsto \bar\alpha$. For $U, V \in \mathbb{Q}$ put

$$L_1 = V + (5+2\sqrt{-5})U, \qquad L_2 = V + (5-2\sqrt{-5})U = \overline{L_1}, \qquad R = 45U^2 + 12\sqrt{-5}\,UV - V^2.$$

Over K, g_4 is the product of $-Q_4\overline{Q_4}$, $R(u^2, v^2)\overline{R}(u^2, v^2)$ and a form of degree 8, where $Q_4(u, v) = L_1(u^2, v^2)$, and these five factors are irreducible over K (Appendix B). Let

$$r_{11} = 1 + \tfrac{\sqrt{-5}}{2}, \quad r_{12} = -\tfrac{3\sqrt{-5}}{2}, \quad r_{22} = \sqrt{-5} - 2, \quad \beta = 2 - \sqrt{-5},$$

so that $R = r_{11}L_1^2 + r_{12}L_1L_2 + r_{22}L_2^2$ identically. Put $A = 108\beta^2 = -108 - 432\sqrt{-5}$. As $\beta = -r_{22}$, also $A = 16r_{22}^2(r_{12}^2 - 4r_{11}r_{22})$, which is how A arises in the proof of Lemma 9.1. Let

$$E_A : \; Y^2 = X^3 + A, \qquad t = \frac{Y - 30 - 12\sqrt{-5}}{-8 - 32\sqrt{-5}},$$

and let $G = (-6 - 6\sqrt{-5},\, 54) \in E_A(K)$ and $P_0 = 2G = (8 - 4\sqrt{-5},\, 22 - 20\sqrt{-5})$, at which $t(P_0) = 1$.

Lemma 9.1. *Let $(U : V) \in \mathbb{P}^1(\mathbb{Q})$ and suppose that $R(U, V)L_1(U, V)$ is a cube in $K^\times$. Then there is a point $P \in E_A(K)$ with $t(P) = L_2/L_1$. In particular $\mathrm{N}_{K/\mathbb{Q}}(t(P)) = 1$.*

Proof. For $U, V \in \mathbb{Q}$ not both 0, $L_1 = (V + 5U) + 2U\sqrt{-5} \neq 0$, and the hypothesis and the ratio L_2/L_1 depend only on $(U : V)$, since RL_1 is homogeneous of degree 3. Write $RL_1 = w^3$ and put $s = L_2/L_1$ and $W = w/L_1$. Then $W^3 = R/L_1^2 = r_{11} + r_{12}s + r_{22}s^2$. Put $X = 4r_{22}W$ and $Y = 8r_{22}(r_{22}s + r_{12}/2)$. The identity

$$Y^2 - X^3 - A = 64r_{22}^3(r_{22}s^2 + r_{12}s + r_{11} - W^3)$$

shows that $P = (X, Y) \in E_A(K)$. Since $4r_{22}r_{12} = 30 + 12\sqrt{-5}$ and $8r_{22}^2 = -8 - 32\sqrt{-5}$, the function t takes the value $s = L_2/L_1$ at P. Since $U, V \in \mathbb{Q}$, $L_2 = \overline{L_1}$, so $\mathrm{N}_{K/\mathbb{Q}}(t(P)) = 1$. □

9.2. **The Mordell–Weil group.**

Proposition 9.2. *$E_A(K)$ is infinite cyclic, and $G = mG'$ for a generator G' and an integer m prime to 2, 3, 5, 7, 23, 29, 83 and 89.*

Proposition 9.4 uses that m is prime to 2 and 3, the primes dividing $\#E_A(\mathbb{F}_\mathfrak{q}) = 24$ at the primes $\mathfrak{q}$ above 23, and to 23 itself. Remark 9.5 repeats the argument at 29, 83 and 89, and uses the remaining primes: 5 and 7 divide $\#E_A(\mathbb{F}_\mathfrak{q}) = 30$, 84 and 90 at the primes $\mathfrak{q}$ above 29, 83 and 89.

Proof. Torsion. At the two primes of K above 7, which have degree 1, the reductions of E_A have 13 and 7 points. Reduction at a prime of good reduction above $\ell \geq 3$ with ramification index 1 is injective on torsion [33, VII.3.1, IV.6.4], so $E_A(K)_{\mathrm{tors}} = 0$.

A 2-descent. The cubic $X^3 + A$ is irreducible over K, so $E_A(K)[2] = 0$. Let $F = K(\vartheta)$ with $\vartheta^3 = -A$, a sextic field generated by a root of $\eta^6 - 216\eta^3 + 944784$, of signature $(0, 3)$ and with $|\operatorname{disc} F| = 2^8 3^6 5^3$. The map $(X, Y) \mapsto X - \vartheta$ embeds $E_A(K)/2E_A(K)$ into $F^\times/F^{\times 2}$, with image in the Selmer group of classes $a \in F(S, 2)$ with $\mathrm{N}_{F/K}(a)$ a square in K and with a in the image of $E_A(K_v)$ for every $v \in S_K$. Here S_K is the set of the three primes of K above 2 and 3, outside which E_A has good reduction (its discriminant is $-432A^2$, and $\mathrm{N}_{K/\mathbb{Q}}(\beta) = 9$), S is the set of the four primes of F above them, and $F(S, 2)$ is the group of classes with even valuation outside S. As K has no real place, there is no condition at infinity. The class group of F has order at most 2 and is generated by the class of the prime above 2 (Appendix A), so the S-class group of F is trivial and $F(S, 2) = \mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^{\times 2}$, of dimension $1 + (0 + 3 - 1 + 4) = 7$. Seven S-units proposed by PARI, -1 among them, have quadratic characters of rank 7 at auxiliary primes, so they form a basis. The norm condition is read off in the S_K-units $-1, 2, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ of K, which generate $\mathcal{O}_{K,S_K}^\times$: the valuations of 2, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ at the three primes of S_K form a matrix of determinant ± 2, and 2 is also the index of the principal ideals in the group of ideals supported on S_K, because the class number of K is 2 and the primes above 2 and 3 are not principal. The image of $E_A(K_v)$ has dimension $\dim E_A(K_v)[2] + [K_v : \mathbb{Q}_2]$ if $v \mid 2$ and $\dim E_A(K_v)[2]$ otherwise, that is, 2 at the prime above 2 and 1 and 0 at the two primes above 3, and the images of sampled local points reach these dimensions. The 2-Selmer group has dimension 1 and is spanned by the image of G (Appendix B). So $\operatorname{rank} E_A(K) \leq 1$, and as $G \neq O$ and the torsion is trivial, $E_A(K) = \mathbb{Z}G'$ is infinite cyclic, with $G = mG'$. As the image of G is nonzero, $G \notin 2E_A(K)$ and m is odd.

The index at $\ell = 3, 5, 7, 23, 29, 83, 89$. For each such ℓ there is a prime $\mathfrak{q}$ of K of good reduction with $\ell \,\|\, \#E_A(\mathbb{F}_\mathfrak{q})$ and $(\#E_A(\mathbb{F}_\mathfrak{q})/\ell) \cdot G \neq O$ in $E_A(\mathbb{F}_\mathfrak{q})$. The primes lie above 5, 29, 37, 827, 347, 4481 and 1601, respectively; for $\ell = 5$ it is the prime above 29 that contains $\sqrt{-5} - 13$. As $\ell \,\|\, \#E_A(\mathbb{F}_\mathfrak{q})$, the subgroup $\ell E_A(\mathbb{F}_\mathfrak{q})$ is the kernel of multiplication by $\#E_A(\mathbb{F}_\mathfrak{q})/\ell$. If ℓ divided m, then $G = \ell(m/\ell)G'$ and the reduction of G would lie in $\ell E_A(\mathbb{F}_\mathfrak{q})$, a contradiction. □

Remark 9.3. A descent via 3-isogeny over K gives a second proof of $\operatorname{rank} E_A(K) \leq 1$, with the auxiliary fields $K(\sqrt{3})$ and $K(\sqrt{-1})$, whose class numbers divide 2 and are equal to 1, respectively (Minkowski's bound). For $\phi : E_A \to E'_A$ with kernel $\{O, (0, \pm\sqrt{A})\}$ the rank formula $\operatorname{rank} E_A(K) = \dim \operatorname{Im} \alpha + \dim \operatorname{Im} \alpha'$ of the proof of Proposition 8.2 holds because $E_A(K)[3] = 0$ and $E'_A(K)[\hat{\phi}] = 0$, and the two Selmer groups have dimensions 1 and 0.

9.3. **Chabauty's method at 23.**

Proposition 9.4. *The only point $P \in E_A(K)$ with $\mathrm{N}_{K/\mathbb{Q}}(t(P)) = 1$ is P_0.*

Proof. Set-up. The argument needs a prime that splits in K and at which E_A has good reduction. We use 23, at which the filter below leaves a single family, with Strassmann bound 1 (Remark 9.5 gives three more such primes). The prime 23 splits in K, as $-5 \equiv 8^2 \pmod{23}$. Let $\iota_1, \iota_2 : K \to \mathbb{Q}_{23}$ be the two embeddings, with $\iota_1(\sqrt{-5}) \equiv 8 \pmod{23}$, so that $\iota_2(\alpha) = \iota_1(\bar{\alpha})$, and let $E^{(j)} = \iota_j(E_A) : Y^2 = X^3 + k_j$ with $k_j = \iota_j(-108 - 432\sqrt{-5})$. Both curves have good reduction (k_j is a 23-adic unit), and both $\iota_j(-8 - 32\sqrt{-5})$ are units, so t is a regular function on the smooth model away from the origin. Both reductions have 24 points, and the reductions of $\iota_1 G$ and $\iota_2 G$ have orders 4 and 8. For $P \in E_A(K)$ put $t_j = \iota_j(t(P))$, so that $\mathrm{N}_{K/\mathbb{Q}}(t(P)) = 1$ means $t_1 t_2 = 1$.

Families. Let $P = nG' \in E_A(K)$ (Proposition 9.2). Choose $n_0 \in \{0, \dots, 7\}$ with $n_0 m \equiv n \pmod 8$. Then $P - n_0 G = 8kG'$ for some $k \in \mathbb{Z}$. As m is prime to 24, the reduction of G' at each prime above 23 lies in the cyclic group generated by that of G and has the same order, so $8G'$ reduces to the origin at both primes. The kernel of reduction $E_1^{(j)}(\mathbb{Q}_{23})$ is a $\mathbb{Z}_{23}$-module, isomorphic to $23\mathbb{Z}_{23}$ through the formal logarithm $\log_j$ [33, VII.2.2, IV.6.4], and in it $\iota_j(8kG') = \mu \cdot \iota_j(8G)$ with $\mu = k/m \in \mathbb{Z}_{23}$. So

$$\iota_j(P) = \iota_j(n_0 G) + \mu \cdot \iota_j(8G) \qquad (j = 1, 2)$$

with a single $\mu \in \mathbb{Z}_{23}$, and μ determines P within the family of n_0.

The filter modulo 23. If $\iota_j(P)$ does not reduce to the origin, then t_j is 23-integral, and t_j modulo 23 is the value of t at the reduction of $\iota_j(n_0 G)$. If it does, then $v(Y(\iota_j P)) \le -3$ and so $v(t_j) \le -3$. So $t_1 t_2 = 1$ forces the following: if neither reduction is the origin, then $t_1 t_2 \equiv 1 \pmod{23}$; if exactly one is, then the other t_j reduces to 0; and they cannot both be the origin. A computation in $\mathbb{F}_{23}$ shows that among $n_0 \in \{0, \dots, 7\}$ only $n_0 = 2$ satisfies these conditions (Appendix B).

The family $n_0 = 2$. Here $n_0 G = P_0$, and $\iota_j(P_0)$ does not reduce to the origin. Translation by $\iota_j(P_0)$ is an automorphism of the smooth model over $\mathbb{Z}_{23}$, so $\tau_j(z) = \iota_j(t)(\iota_j(P_0) + Z_j(z))$ is a power series in $\mathbb{Z}_{23}[[z]]$, where $Z_j(z)$ is the point of the kernel of reduction with formal parameter z, and $\tau_j(0) = 1$. Let $\lambda_j = \log_j(\iota_j(8G)) \in 23\mathbb{Z}_{23}$. The point $\mu \cdot \iota_j(8G)$ has formal parameter $z_j(\mu) = \exp_j(\mu\lambda_j)$, and as in (b) of the proof of Lemma 7.8, $z_j(\mu) \equiv \mu\lambda_j$ modulo $23^2\mathbb{Z}_{23}[[\mu]]$, with all coefficients in $23\mathbb{Z}_{23}$ and tending to 0. Hence

$$\Lambda(\mu) = \tau_1(z_1(\mu))\,\tau_2(z_2(\mu)) - 1 = \sum_{i \ge 0} a_i \mu^i$$

with $a_i \in \mathbb{Z}_{23}$, $a_i \to 0$, $a_0 = 0$ and $v(a_i) \ge 2$ for $i \ge 2$, and $a_1 = \sum_j \tau_j'(0)\lambda_j$ with $\tau_j'(0) = \iota_j(3X(P_0)^2/(-8 - 32\sqrt{-5}))$, since the derivation dual to $dX/2Y$ sends Y to $3X^2$. The computation gives $v(a_1) = 1$ (Appendix B). By Strassmann's theorem, Λ has at most one zero in $\mathbb{Z}_{23}$, and $\mu = 0$ is one. So $P = P_0$. □

Remark 9.5. The same argument at the primes 29, 83 and 89, which also split in K, again leaves only the family of P_0, with Strassmann bound 1. The coefficient a_1 can also be computed without formal logarithms, from the values $\Lambda(\mu)$ at small integers μ, computed in $E_A(K)$ and reduced modulo 23^2. Both computations give $a_1/23 \equiv 12 \pmod{23}$.

9.4. **Edwards triples of form 4.**

Proposition 9.6. *Let $(4, u, v)$ be an Edwards triple of a solution with $z \neq 0$. Then $(u, v) = \pm(0, 1)$, and the solution is $(0, 1, 1)$.*

Proof. By Proposition 5.2(i), $Q_4(u, v) \in Q_4(0, 1)K^{\times 3} = K^{\times 3}$ and $R(u^2, v^2) \in R(0, 1)K^{\times 3} = -K^{\times 3} = K^{\times 3}$. Both are nonzero as $g_4(u, v) \neq 0$. With $U = u^2$ and $V = v^2$,

$R(U,V)L_1(U,V) = R(u^2,v^2)Q_4(u,v)$ is a nonzero cube in K. By Lemma 9.1 and Proposition 9.4, $L_2/L_1 = t(P_0) = 1$. Since $L_2 - L_1 = -4\sqrt{-5}\,U$, this gives $u = 0$, and then $v = \pm 1$. Finally $(f_4, g_4, h_4)(0, \pm 1) = (0, -1, 1)$ gives $(x, y, z) = (0, 1, 1)$. □

10. Proof of Theorem 1.1

Let (x, y, z) be a solution of (1.1). If $z = 0$, then $(x, y, z) = (\pm 1, -1, 0)$ (Section 1.1). Suppose $z \neq 0$, and let (i, u, v) be an Edwards triple (Proposition 2.4). By Corollary 4.4, $i \in \mathcal{I}_{\mathrm{r}} = \{1, 2, 3, 4, 10, 17, 18, 20, 26\}$. By Proposition 5.1, $i \notin \{10, 17, 18, 26\}$, and by Proposition 8.4, $i \neq 2$. If $i \in \{1, 20\}$ then $(x, y, z) = (\pm 1, 0, 1)$ (Proposition 7.2, with Theorem 7.10). If $i = 3$ then $(x, y, z) = (0, -1, -1)$ (Proposition 6.1), and if $i = 4$ then $(x, y, z) = (0, 1, 1)$ (Proposition 9.6). Conversely the six triples of Theorem 1.1 are solutions. □

Appendix A. Class groups

The descents use, for each field K, only an upper bound on the class group: that 3 does not divide the class number (the cube descents of Sections 4 and 5 and the descent via 3-isogeny of Section 8), or that the class group is trivial or generated by classes of primes in the set S of the descent (the 2-descents of Sections 6, 7 and 9). This appendix explains how these bounds are proved without the generalized Riemann hypothesis.

Method. Let K be a number field of degree n with r_2 complex places and discriminant d_K, and let $M_K = (4/\pi)^{r_2}\, n!\, n^{-n} \sqrt{|d_K|}$ be its Minkowski bound. By Minkowski's theorem every ideal class of K contains an integral ideal of norm at most M_K (see [23, Theorem 4.3]), so the classes of the prime ideals of norm at most M_K generate the class group. PARI's `bnfinit`, whose output is guaranteed only under the generalized Riemann hypothesis, is used only to propose ideals $\mathfrak{g}_1, \dots, \mathfrak{g}_k$ with orders $c_1, \dots, c_k$, and for each prime ideal $\mathfrak{P}$ of norm at most M_K an element $a_{\mathfrak{P}}$ and exponents $e_{\mathfrak{P},l}$. We then check by ideal arithmetic that

$$\begin{aligned} \mathfrak{g}_l^{c_l} &= (a_l) && \text{for explicit } a_l \in K^\times, \\ \mathfrak{P} &= (a_{\mathfrak{P}}) \prod_l \mathfrak{g}_l^{e_{\mathfrak{P},l}} && \text{for every prime ideal } \mathfrak{P} \text{ with } N\mathfrak{P} \leq M_K. \end{aligned}$$

Then the class group is generated by the classes of the $\mathfrak{g}_l$, and its order divides $\prod_l c_l$. The maximal orders were checked by the Pohst–Zassenhaus criterion at every prime whose square divides their discriminant; this suffices, since a prime dividing the index of an order in $\mathcal{O}_K$ divides the discriminant of that order to at least the second power. Whether K contains a primitive cube root of unity is decided by factoring $x^2 + x + 1$ over K. None of the fields does.

Table 5 lists the results. The field generated by a root of $2x^3 + 15x^2 - 30x - 25$, over which the 2-descent on the curve E_6 of Section 6 runs, is isomorphic to $\mathbb{Q}(\xi)$. For the fields M_i, the class number is exactly 2: a quadratic extension of M_i of relative discriminant (1) in which both real places of M_i stay real was found and checked, so 2 divides the class number by class field theory. The proof uses only that this class number is prime to 3. For F in the last row, the prime above 2 is not principal and generates the class group, so the S-class group used in Proposition 9.2 is trivial. For $\mathbb{Q}(\xi)$ each of the six prime ideals of norm at most 15 (two above 2, one above 3, two above 5 and one above 13) was shown to be principal by an explicit generator. The fields used only in remarks were treated in the same way. Among them are the two fields $K[T]/(T^3 + 36\theta)$ and $K[T]/(T^3 - 3\theta)$ of degree 9

Field	Used in	Signature	$\lceil M_K \rceil$	Primes	Order of Cl(K)
$\mathbb{Q}(\sqrt{-5})$	Proposition 5.2, Sections 6 and 9	$(0,1)$	3	1	divides 2
$\mathbb{Q}(\sqrt[3]{5})$	Propositions 5.1 and 5.2, Section 8	$(1,1)$	8	4	1
K'_{17}, K'_{18}	Proposition 5.1	$(4,2)$	281	58	divides 2
K''	Proposition 5.1	$(0,4)$	455	82	divides 4
K_1	Proposition 5.2	$(2,4)$	8637	1076	1
K_{20}	Proposition 5.2	$(2,4)$	346	54	1
M_6	Theorem 4.2	$(2,4)$	34547	3698	2
M_7	Theorem 4.2	$(2,4)$	51820	5203	2
$M_8 = M_{14}$	Theorem 4.2	$(2,4)$	103640	9920	2
$M_9 = M_{13}$	Theorem 4.2	$(2,4)$	103640	9896	2
M_{11}	Theorem 4.2	$(2,4)$	17274	1935	2
M_{19}	Theorem 4.2	$(2,4)$	51820	5194	2
$M_{21} = M_{24}$	Theorem 4.2	$(2,4)$	103640	9970	2
M_{22}	Theorem 4.2	$(2,4)$	25910	2920	2
$\mathbb{Q}(\xi)$	Sections 6 and 7	$(3,0)$	16	6	1
$\mathbb{Q}(\sqrt[6]{5})$	Proposition 8.2	$(2,2)$	38	9	1
$K(\sqrt{-3\theta})$	Proposition 8.2	$(0,3)$	84	16	divides 2
$F = K(\sqrt[3]{-A})$	Proposition 9.2	$(0,3)$	154	39	divides 2

TABLE 5. The class groups used in the proof. "Primes" is the number of prime ideals of norm at most M_K. In the last two rows K and θ (or A) are those of Section 8 (or Section 9).

in the remark after Proposition 8.2 (class numbers dividing 3 and equal to 1, respectively), and the fields $K(\sqrt{3})$ and $K(\sqrt{-1})$ over $K = \mathbb{Q}(\sqrt{-5})$ in the remark after Proposition 9.2 (class numbers dividing 2 and equal to 1, respectively).

APPENDIX B. COMPUTATIONS

B.1. **List of computational statements.** Table 6 lists the statements used in the proof that rest on machine computation; the README of the code package [21] also covers the computations behind the remarks and Example 5.4. In the computations of Table 6 the arithmetic is exact (integers, rationals, number fields given by explicit polynomials, finite fields, and p-adic numbers whose precision is tracked and checked), with two exceptions: the Minkowski bounds of Appendix A and the signs of elements at real places are computed in floating point, with at least 38 significant digits. Each Minkowski bound is at least 0.01 from an integer, and each value whose sign is used in Lemma 7.4 and Proposition 7.6 exceeds $6 \cdot 10^{-4}$ in absolute value. The computations used PARI/GP 2.17.3 [24] and Python 3.12 with SymPy, NumPy and python-flint 0.8 (FLINT 3.3 [15]). PARI's `bnfinit` and `bnfunits` are used only to propose ideal generators, units and S-units, which are then checked as described in Section 3 and Appendix A.

The README of the code package [21] gives, for each row of Table 6, the programs, the commands that run them and their output files. On one core of an Apple M5 laptop, each computation on which the proof relies runs in under two minutes; the longest is the Mordell–Weil sieve of Proposition 7.7, which takes one to two minutes. Running every program of the code package, including computations that the proof does not use, takes about 70 minutes.

Statement	What is computed
Lemma 2.2, Section 2	the forms f_i, g_i, h_i from the vectors $\alpha^{(i)}$; their integrality; the identity $f_i^2 + g_i^3 + h_i^5 = 0$; the resultants and discriminants; the values at $(0, 1)$ and $(1, 0)$
Lemma 4.1	f_i, g_i, h_i modulo 2 and g_i modulo 8 at the pairs modulo 8 with u or v odd
Theorem 4.2, Table 3	the fields L_i and M_i; the factorization of g_i over M_i and conditions (a), (b) of Lemma 3.1; the Σ-unit bases and their cubic characters; the local images at 2 and 3; the linear algebra over $\mathbb{F}_3$
Propositions 5.1 and 5.2, Table 4	the same for the fields of Table 4, with local images at 2, 3, 5; the admissible tuples; the classes at the reference pairs
Proposition 6.1	the factorization of g_3 over $\mathbb{Q}(\sqrt{-5})$; the local solubility of the curves D_d at 2, 3, 5; the 2-Selmer group and the torsion of E_6
Propositions 7.1 and 7.2	the forms $\widehat{g}_1$, $\widehat{g}_{20}$, R_i and the values δ_i; the factors of $R_i(u^5, v^5)$ over K_1, K_{20}; the identities for the pencil $A_i + \nu B_i$; the values of X/Y at $(m : n) = (3 : 1)$
Section 7: the curve E, Lemma 7.4, Propositions 7.6, 7.7 and 7.9	the formulas for $\Psi_2, \Psi_4, E, \iota, P_1, P_2, T$; the Σ-units of $\mathbb{Q}(\xi)$ and the local images of Lemma 7.4; the 2-Selmer group of E, the torsion and the index; the sieve; the 59-adic matrices
Lemma 8.1, Propositions 8.2 and 8.4	the identities of Lemma 8.1; the descents via 3-isogeny, with the local images determined by the duality identity; the torsion; the factors A_k
Lemma 9.1, Propositions 9.2, 9.4 and 9.6	the identities of Lemma 9.1; the factorization of g_4; the 2-descent over $\mathbb{Q}(\sqrt{-5})$; the torsion and the index; the filter modulo 23 and the coefficient a_1
Appendix A	the maximal orders, the Minkowski bounds, the prime ideals of small norm and their relations

TABLE 6. The computational statements used in the proof.

B.2. **Second computations.** Every computation on which the proof depends was repeated by a second program, written separately from the first. The two share the definitions in the text, including the defining polynomials of the fields printed there, and the vectors $\alpha^{(i)}$ of Edwards' forms. The second programs for Sections 2, 4 and 7 take these vectors from a new transcription of [19, Table 3]. The others use the first transcription, also of [19, Table 3], which agrees with the new one entry by entry, and three of them (for Proposition 6.1, Section 8 and Appendix A) also use the first programs' lines that compute h_i, g_i and f_i from it. The second programs use other precisions for the local images in Sections 4 and 5, other charts in Section 5, other models of some of the fields in Section 8, and, where possible, other algorithms. For example, the Mordell–Weil sieve of Proposition 7.7 was rewritten without PARI, and the matrices of Proposition 7.9 were recomputed by evaluating the function ρ at the points $P_0 + 224P_i$ in $E(K)$, without logarithms. All second computations agree with the first. As a further test, the descent programs of Sections 4 and 5 were run on 17 equations $g_i(u, v) = -dz^3$ that have a known solution (u_0, v_0), with d a product of powers of 2, 3 and 5 ($d = 1$ in two of them); forms 17, 18 and 20 were run over several fields, 27 runs in all. Since these solutions do not satisfy condition (iii) of Section 3.2, that condition was omitted. In every case the class tuple of (u_0, v_0) survives.

B.3. **Data availability.** The programs, their inputs and their outputs, with the commands that run them, 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. Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani, *Generalized Fermat equations: a miscellany*, Int. J. Number Theory **11** (2015), no. 1, 1–28, https://doi.org/10.1142/S179304211530001X.
2. Michael A. Bennett, Preda Mihăilescu, and Samir Siksek, *The generalized Fermat equation*, Open problems in mathematics (John Forbes Nash, Jr. and Michael Th. Rassias, eds.), Springer, Cham, 2016, pp. 173–205, https://doi.org/10.1007/978-3-319-32162-2_3.
3. Frits Beukers, *The Diophantine equation $Ax^p + By^q = Cz^r$*, Duke Math. J. **91** (1998), no. 1, 61–88, https://doi.org/10.1215/S0012-7094-98-09105-0.
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. ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49, https://doi.org/10.1515/crll.2003.076.
6. ———, *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.
7. Nils Bruin and E. Victor Flynn, *N-covers of hyperelliptic curves*, Math. Proc. Cambridge Philos. Soc. **134** (2003), no. 3, 397–405, https://doi.org/10.1017/S0305004102006448.
8. ———, *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, *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.
10. Henri Cohen and Fabien Pazuki, *Elementary 3-descent with a 3-isogeny*, Acta Arith. **140** (2009), no. 4, 369–404, https://doi.org/10.4064/aa140-4-6.
11. Kevin R. Coombes and David R. Grant, *On heterogeneous spaces*, J. London Math. Soc. (2) **40** (1989), no. 3, 385–397, https://doi.org/10.1112/jlms/s2-40.3.385.
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. Johnny Edwards, *A complete solution to $X^2 + Y^3 + Z^5 = 0$*, J. Reine Angew. Math. **571** (2004), 213–236, https://doi.org/10.1515/crll.2004.043.
14. Tom Fisher, *The Cassels–Tate pairing and the Platonic solids*, J. Number Theory **98** (2003), no. 1, 105–155, https://doi.org/10.1016/S0022-314X(02)00038-0.
15. The FLINT team, *FLINT: Fast Library for Number Theory*, 2025, Version 3.3.0, https://flintlib.org.
16. 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.
17. 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.

18. ———, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205, https://doi.org/10.4064/aa98-2-9.
19. Nuno Freitas and Michael Stoll, *The generalized Fermat equation* $x^2 + y^3 = z^{25}$, 2025, Preprint, arXiv:2506.10667.
20. Manvir Jaswal, *The generalized Fermat equation* $x^2+y^5 = z^7$, 2026, Preprint, https://doi.org/10.5281/zenodo.22983879.
21. ———, *Programs and data for "The generalized Fermat equation* $x^2+y^5 = z^9$ *"*, 2026, Zenodo, https://doi.org/10.5281/zenodo.23004600.
22. James S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.
23. ———, *Algebraic number theory (v3.08)*, 2020, Available at https://www.jmilne.org/math/.
24. The PARI Group, *PARI/GP version 2.17.3*, Univ. Bordeaux, 2025, https://pari.math.u-bordeaux.fr/.
25. Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2+y^3 = z^7$, Duke Math. J. **137** (2007), no. 1, 103–158, https://doi.org/10.1215/S0012-7094-07-13714-1.
26. Piet Hein Casper Putz, *Enumeration of local and global étale algebras applied to generalized Fermat equations*, Ph.D. thesis, Vrije Universiteit Amsterdam, 2024, https://doi.org/10.5463/thesis.832.
27. 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.
28. Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231, https://doi.org/10.1090/S0002-9947-03-03366-X.
29. Victor Scharaschkin, *Local-global problems and the Brauer–Manin obstruction*, Ph.D. thesis, University of Michigan, 1999.
30. 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.
31. Samir Siksek and Michael Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation* $x^3+y^4+z^5 = 0$, Bull. London Math. Soc. **44** (2012), no. 1, 151–166, https://doi.org/10.1112/blms/bdr086.
32. ———, *The generalised Fermat equation* $x^2+y^3 = z^{15}$, Arch. Math. (Basel) **102** (2014), no. 5, 411–421, https://doi.org/10.1007/s00013-014-0639-z.
33. 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.
34. Jaap Top, *Descent by 3-isogeny and 3-rank of quadratic fields*, Advances in number theory (Kingston, ON, 1991), Oxford Univ. Press, New York, 1993, pp. 303–317.
35. Joseph L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California, Berkeley, 1997.

Toronto, Canada
Email address: manvirjaswal@icloud.com