NEW EXPONENTS FOR THE GENERALIZED FERMAT EQUATION $x^2 + y^3 = z^n$

MANVIR JASWAL

ABSTRACT. We determine the primitive solutions of $x^2 + y^3 = z^n$ for $n = 11$, 17 and 19 unconditionally; for $n = 11$ Freitas, Naskręcki and Stoll did so under the generalized Riemann hypothesis (GRH). For $n = 25$ we do not assume GRH but use a reduction of Freitas and Stoll that is available as a preprint, and for $n = 13$, 23, 26 and 29 we assume GRH. GRH enters only through the class numbers of eight fields of degree 24 and 30 and four of degree 56. The solutions are the trivial ones, with $xyz = 0$, and those coming from $3^2 - 2^3 = 1$. With earlier work this settles every exponent $6 \le n \le 36$ except 31, under the same conditions. Following Freitas, Naskręcki and Stoll, and Freitas and Stoll for $n = 25$, we reduce to points over number fields on modular curves or on curves $Y^2 = X^5 + \beta$. The new step is to find these points by descents that need only the class groups of their fields of definition or of small extensions, mostly along isogenies with kernel μ_ℓ, along $1 - \sigma$ for a diamond automorphism σ, and along $1 - \zeta_5$.

CONTENTS

1. Introduction 2

Part I. Points of $X_0(p)$ over the fields K_E 9
2. From solutions to points of $X_0(p)$ over number fields 9
3. Descents inside K_E 19
4. Local analysis and the disc test 30
5. Discs that contain a known point 38

Part II. The prime exponents 47
6. The exponent 11 47
7. The exponent 17 51
8. The exponent 19 56
9. The exponent 23 65
10. The exponent 29 74

Part III. The exponent 25 76
11. The reduction of Freitas and Stoll 76
12. Genus-2 curves and the descent by $1 - \zeta$ 84
13. The 5-adic argument 89
14. The forms decided by the first descent 94
15. The forms decided by a second descent, and the proof of Theorem C 95

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G05, 11G18, 11G30, 11R29, 11Y40.

Key words and phrases. Generalized Fermat equation, modular curves, Eisenstein ideal, Selmer groups, Chabauty's method, class groups.

Part IV. The exponents 13 and 26, and those that remain 98
16. The exponent 13: the descent 98
17. The exponent 13: the 3-adic analysis 102
18. The exponents that remain 107
Appendix A. Class groups and units without GRH 108
Appendix B. Computations 116
Appendix C. Data 124
Declarations 126
References 126

1. Introduction

1.1. The equation.

For an integer $n \geq 2$ consider

$$x^2 + y^3 = z^n, \qquad x, y, z \in \mathbb{Z}, \qquad \gcd(x, y, z) = 1. \tag{1.1}$$

The solutions of (1.1) are called *primitive*, and a solution is *trivial* if $xyz = 0$. The trivial solutions are $(\pm 1, -1, 0)$, $(\pm 1, 0, 1)$ and $(0, 1, 1)$, together with $(0, -1, -1)$ when n is odd, and $(\pm 1, 0, -1)$ and $(0, 1, -1)$ when n is even. For every n there are also the *Catalan solutions* $(\pm 3, -2, 1)$, which come from $3^2 - 2^3 = 1$, and for even n also $(\pm 3, -2, -1)$.

Equation (1.1) is the case $(2, 3, n)$ of the generalized Fermat equation $x^p + y^q = z^r$. For $n \leq 5$ it has infinitely many primitive solutions, which come in finitely many families [27, §1]. For $n \geq 7$, where $1/2 + 1/3 + 1/n < 1$, Darmon and Granville proved that there are only finitely many [19]. The equation has been solved for $n = 6$, where it reduces to an elliptic curve of rank 0 [5, Proposition 6], for $n = 7$ [46], 8 [11], 9 [12], 10 [10, 55] and 15 [57], and for $n = 11$ assuming the generalized Riemann hypothesis (GRH), by Freitas, Naskręcki and Stoll [27]; see the survey of Ratcliffe and Grechuk [47].

A solution for $n = mk$ gives the solution (x, y, z^m) for k, and every $n \geq 6$ is divisible by 6, 8, 9, 10, 15, 25 or a prime $p \geq 7$ [27, §1]. So the open cases were the exponent 25 and the primes $p \geq 11$. For $p = 13$, Freitas, Naskręcki and Stoll explain why their method does not reach the exponent: the descent they would need requires the class group of a number field of degree 84 [27, §9]. Freitas and Stoll reduced the exponent 25 to five equations $H(u, v) = w^5$ over number fields of degree 6 [28], and Ratcliffe and Grechuk list $(2, 3, 25)$ among the signatures that remain to be considered [47, §1.1]. Apart from the multiples of exponents already solved, the only infinite set of exponents known before this work is the set of $3p$ for primes $p \equiv 1 \pmod 8$, due to Bennett, Chen, Dahmen and Yazdani (Section 18). Zhou claims, in a preprint that applies inter-universal Teichmüller theory, that for $n \geq 110$ with $n \neq 113, 121$ the only non-trivial primitive solutions are those coming from $3^2 - 2^3 = 1$ [66]. We have not checked the arguments of this preprint, and these exponents include none of those treated here.

1.2. Results.

Theorem A. *Let $p \in \{11, 17, 19\}$. The primitive solutions of $x^2 + y^3 = z^p$ are $(\pm 1, -1, 0)$, $(\pm 1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ and $(\pm 3, -2, 1)$.*

For $p = 17$ and $p = 19$ this is new. For $p = 11$ Freitas, Naskręcki and Stoll proved it assuming GRH, which they needed to determine the class groups of five number fields of degree 36 [27, Theorem 1.4 and §7]. Our proof of Theorem A uses neither GRH nor

any unpublished result, and we have repeated in PARI/GP the Magma computations with which Freitas, Naskręcki and Stoll treat the CM twists at $p = 11$ [27, §7.1] (Proposition 2.3, Appendix B.2).

For an elliptic curve E over $\mathbb{Q}$ and a prime p, let K_E be the field of definition of a subgroup of order p of $E[p]$ (Definition 2.7); for the curves E that occur below it has degree $p + 1$. Elliptic curves over $\mathbb{Q}$ are named by their labels in Cremona's tables [17].

Theorem B. (a) *Suppose that the class numbers of the three fields K_E of degree 24 attached to $E =$ 864a1, 864b1, 864c1 are prime to 11. Then the primitive solutions of $x^2+y^3 = z^{23}$ are $(\pm1, -1, 0)$, $(\pm1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ and $(\pm3, -2, 1)$.*

(b) *Suppose that the class numbers of the five fields K_E of degree 30 attached to $E =$ 54a1, 96a1, 864a1, 864b1, 864c1 are prime to 7. Then the primitive solutions of $x^2 + y^3 = z^{29}$ are $(\pm1, -1, 0)$, $(\pm1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ and $(\pm3, -2, 1)$.*

Both hypotheses hold under GRH.

Under GRH, PARI/GP gives the three class numbers in (a) as 2 and the five in (b) as 1 (Tables 7 and 8). Two further fields at $p = 23$ and one at $p = 29$ enter the proof, those attached to the curves 27a1 and 288a1 with complex multiplication (only 27a1 at $p = 29$). For them we prove the needed statement without GRH (Proposition A.12).

Theorem C. *The primitive solutions of $x^2 + y^3 = z^{25}$ are $(\pm1, -1, 0)$, $(\pm1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ and $(\pm3, -2, 1)$. The proof uses the reduction of Freitas and Stoll [28], an arXiv preprint, with a supplement to one step of it (Lemma 11.3).*

Freitas and Stoll used GRH once in their reduction, for Stoll's determination of the rational points of a curve of genus 4. Our proof of Theorem C uses no GRH: we prove that result and determine the Selmer groups of the descent without it (Propositions 11.4 and 12.6). We also recompute without Magma the two results of [28] obtained with Magma's Mordell–Weil and rank-bound routines (Theorem 11.6).

For the exponent 13, let K_E be the field of degree 14 of Definition 2.7 attached to E and $p = 13$, and $L_E = K_E(\omega, \sqrt{d_E(3\omega - 1)})$, of degree 56. Here ω is a primitive cube root of unity, and $d_E \in K_E$ is given in Section 16.2.

Theorem D. *Suppose that the class numbers of the four fields L_E of degree 56 attached to $E =$ 96a1, 864a1, 864b1, 864c1 are prime to 3. Then the primitive solutions of $x^2 + y^3 = z^{13}$ are $(\pm1, -1, 0)$, $(\pm1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ and $(\pm3, -2, 1)$, and those of $x^2 + y^3 = z^{26}$ are $(\pm1, -1, 0)$, $(\pm1, 0, \pm1)$, $(0, 1, \pm1)$ and $(\pm3, -2, \pm1)$. The hypothesis holds under GRH.*

Under GRH the class group of L_E is generated by the prime ideals of norm below a bound of Belabas, Diaz y Diaz and Friedman [3, Corollary 2.2], and an explicit relation for each of these prime ideals, checked by exact arithmetic, shows that the class numbers of the four fields L_E divide 2, 32, 2 and 2 (Proposition 16.5). GRH enters the proof of Theorem D only through this bound.

Corollary E. *Let $n \geq 2$, and let k be a divisor of n such that $k \in \{6, 10, 11, 15, 17, 19, 25\}$, or $k \in \{7, 8, 9\}$ and $k < n$. Then the primitive solutions of $x^2 + y^3 = z^n$ are the trivial solutions and the Catalan solutions of Section 1.1. The same holds for $k \in \{23, 29\}$ under the hypothesis of Theorem B(a), respectively (b), and for $k = 13$ under the hypothesis of Theorem D. For $k \in \{11, 17, 19\}$ this rests on Theorem A, for $k = 25$ on Theorem C, for $k = 13$ on Theorem D, and for the other k on the results cited in Table 1.*

Proof. Let $n = mk$ with $m \geq 1$, and let (x, y, z) be a primitive solution for n. Then (x, y, z^m) is a primitive solution for k, since $\gcd(x, y, z^m) = \gcd(x, y, z)$, and conversely every primitive

solution for n arises in this way from a primitive solution for k whose last entry is an m-th power. Suppose that the solutions for k are the trivial and the Catalan ones. A trivial or Catalan solution for k with last entry w gives a solution for n exactly when $w = z^m$. As $w \in \{0, \pm 1\}$, this holds exactly when $z = w$, with m odd if $w = -1$, or when $w = 1$, $z = -1$ and m is even. So the solutions for n are the trivial and the Catalan ones, with the signs of z as stated in Section 1.1. For $k = 7$, 8, 9 the solutions other than these have last entry $w \in \{2, 17, 65, 113\}$, ± 43 and 2 respectively, none of which is a perfect power, so a proper multiple of 7, 8 or 9 has only the trivial and the Catalan solutions. □

Corollary F. *Let $6 \le n \le 36$ with $n \ne 31$. The primitive solutions of $x^2 + y^3 = z^n$ are those listed in Table 1. For $n \ne 7, 8, 9$ they are the trivial solutions and the Catalan solutions. For $n = 23$ and $n = 29$ this holds under the hypotheses of Theorem B, for $n = 13$ and $n = 26$ under the hypothesis of Theorem D, and so under GRH for these four exponents, and for $n = 25$ it rests on the reduction of Freitas and Stoll (Theorem C).*

Proof. For $n \in \{7, 8, 9\}$ the solutions are those of the results cited in Table 1. Every other n in the range has a divisor k as in Corollary E, which is n itself or is named in the last column of Table 1, and Corollary E applies. □

n	Primitive solutions with $xyz \ne 0$	Source
$6, 12, 18, 24, 30, 36$	$(\pm 3, -2, \pm 1)$	$n = 6$: [5, Proposition 6], [27, §1]
7	$(\pm 3, -2, 1)$, $(\pm 71, -17, 2)$, $(\pm 2213459, 1414, 65)$, $(\pm 15312283, 9262, 113)$, $(\pm 21063928, -76271, 17)$	[46, Theorem 1.1]
$14, 21, 28, 35$	$(\pm 3, -2, 1)$, and $(\pm 3, -2, -1)$ for even n	$n = 7$
8	$(\pm 3, -2, \pm 1)$, $(\pm 30042907, -96222, \pm 43)$	[11, Theorem 1.3]
$16, 32$	$(\pm 3, -2, \pm 1)$	$n = 8$
9	$(\pm 3, -2, 1)$, $(\pm 13, 7, 2)$	[12, Theorem 1.1]
27	$(\pm 3, -2, 1)$	$n = 9$
$10, 20$	$(\pm 3, -2, \pm 1)$	$n = 10$: [10, Theorem 1.1], [55, Theorem 1]
15	$(\pm 3, -2, 1)$	[57, Theorem 1.1]
$11, 22, 33$	$(\pm 3, -2, 1)$, and $(\pm 3, -2, -1)$ for even n	Theorem A ($n = 11$)
$17, 34$	$(\pm 3, -2, 1)$, and $(\pm 3, -2, -1)$ for even n	Theorem A ($n = 17$)
19	$(\pm 3, -2, 1)$	Theorem A
23, 29	$(\pm 3, -2, 1)$	Theorem B (class numbers prime to 11, 7)
25	$(\pm 3, -2, 1)$	Theorem C (with [28])
$13, 26$	$(\pm 3, -2, 1)$, and $(\pm 3, -2, -1)$ for even n	Theorem D ($n = 13$; class numbers prime to 3)
31	open	Section 18

TABLE 1. The exponents $6 \le n \le 36$. The trivial solutions are those of Section 1.1. Where the last column names an exponent k, the other exponents of the row follow from the case $n = k$ by Corollary E. The lists for $n = 8$ and $n = 9$ are those of [11, 12] after the change of variables that turns $x^8 + y^3 = z^2$ and $x^3 + y^9 = z^2$ into (1.1).

1.3. **The idea and the strategy.** The modular method does not settle these exponents by itself. For a prime exponent p, a primitive solution (a, b, c) with $abc \neq 0$ has a Frey curve with j-invariant $j_0 = 1728b^3/c^p$. By modularity, level lowering and the symplectic criteria of Freitas, Naskręcki and Stoll, some quadratic twist of it has the same mod p representation as one of a few curves E of conductor dividing 864, which depend on p modulo 24 [27, Theorem 5.1]. Some of these curves come from the trivial and the Catalan solutions, which exist for every exponent, so they cannot be removed by comparing traces of Frobenius. Published results remove some of the others (Theorem 2.1). Through twists of the modular curve $X(p)$, Freitas, Naskręcki and Stoll [27] reduce the problem to points of $X_0(p)$ with rational j-invariant over number fields K_E of degree $p + 1$, of which 26 occur for our exponents (Tables 6, 7 and 8). A solution gives a point P of $X_0(p)$ over K_E with $j(P) = j_0$ (Proposition 2.12). Freitas, Naskręcki and Stoll determine these points for $p = 11$ by a 2-descent on the elliptic curve $X_0(11)$. Its Kummer map needs the field generated over K_E by a point of order 2, of degree 36, and they determine the class group of this field under GRH. For $p = 17$ and 19 they expected fields of degree 36 or 40 [27, §9]. For $n = 25$ the reduction of Freitas and Stoll leads to curves $Y^2 = X^5 + \beta$ of genus 2 over fields L of degree 12, and a 2-descent on them needs the class groups of the fields $L(\beta^{1/5})$, of degree 60, which they describe as out of reach [28, §9].

Except for $p = 17$, we descend instead by an isogeny whose kernel is μ_ℓ as a Galois module, for a prime ℓ adapted to the curve. Its Kummer map takes values in $K^\times/K^{\times\ell}$ for the field K over which the points live, so its Selmer group is a group of S-units of K modulo ℓ-th powers, and every question about class groups stays in K itself. For $p = 11$, the curve $X_0(11)$ has a rational point T of order 5, the isogeny dual to the quotient by $\langle T\rangle$ has kernel μ_5, and S is the set of primes above 11 (Proposition 3.7). The class groups of the fields K_E of degree 12 can be determined without GRH (Appendix A). The same idea gives a μ_3-descent for $p = 19$. For $p = 23$ and 29, where $X_0(p)$ has genus 2, the kernel is the image of the Shimura subgroup of $J_0(p)$ in the quotient of $J_0(p)$ by its cuspidal subgroup, and is isomorphic to μ_ℓ for ℓ the numerator of $(p - 1)/12$ by Mazur's work on the Eisenstein ideal [39]. The Kummer map is evaluation of a modular unit. For $n = 25$ the isogeny is $1 - \zeta_5$, whose kernel is rational over $L(\zeta_5)$, of degree 48 instead of 60. At $p = 17$, where the rational point T of $X_0(17)$ has order 4, the isogenies with kernel μ_4 and μ_2 that the same idea gives cannot distinguish a point P from $P + T$ at the places above 2 (Remark 3.12). We therefore use a 2-descent over $K_E(i)$, whose class group is controlled from K_E by Chevalley's ambiguous class number formula.

The descent of Section 3 maps P to a class in the Selmer group. The reduction of the Frey curve at ℓ confines j_0 to finitely many ℓ-adic discs, and on each disc the local Kummer classes at the places above ℓ are among finitely many tuples computed at one point (Section 4). A disc is excluded when none of its tuples lies in the image of the Selmer group. A few Selmer classes that survive are removed by a sieve at primes of good reduction, which uses that j_0 is rational (Lemma 5.11). Table 2 lists the ingredients for each exponent, and Table 4 lists the twists that remain.

The real difficulty lies in the discs that contain the j-invariant of an explicitly known point, for example the point over $j(E)$ or a point coming from a trivial or Catalan solution, since such a disc passes every local test. For these discs we show that the known point P_0 is the only point over the disc with rational j-invariant. If P were another one, then $[P - P_0]$ would be divisible locally by a high power of the isogeny. The injectivity of the map from the Selmer group to the local groups turns local divisibility into global divisibility, and after

the last division the local class is determined by the tangent direction of the curve at P_0, and lies outside the image of the Selmer group. This is Stoll's method of Chabauty without the Mordell–Weil group [64] (Proposition 5.1), which Freitas, Naskręcki and Stoll used at $\ell = 2$ for $p = 11$ [27, Lemma 7.8].

We adapt it in three ways. At $p = 17$ and 19 the groups $J(K_v)$ at the places above ℓ contain torsion, so division by ℓ is not unique there. We therefore work modulo all local torsion, and measure divisibility by the ℓ-adic logarithm, which kills the torsion (Sections 5.2 and 5.3). At $p = 23$ and 29 the division is by the Eisenstein prime λ above ℓ. The Hecke algebra $\mathcal{O}$ of $J_0(p)$ is the ring of integers of a real quadratic field in which $\ell = \lambda\mu$ splits, with $\lambda \neq \mu$, so that $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda \times \mathcal{O}_\mu$ (Section 3.5). This splitting fails at $p = 31$ (Section 18). The tangent space of $J_0(p)$ at the origin splits accordingly into two lines on which $\mathcal{O}$ acts through $\mathcal{O}_\lambda$ and $\mathcal{O}_\mu$, so that λ has valuation one on the first line and is a unit on the second. We call the first line the λ-direction (Section 5.5), and we read divisibility by λ from the component of the formal logarithm along it. Finally, where the known point is a ramification point of the j-map (over 1728 at $p = 19$, over 0 and 1728 at $p = 23$, over 0 at $p = 29$), the points near it are described by branches through the ramification point rather than by a single power series in j (Lemma 4.5 and Section 8.7). Where the local information is too weak, we first make a second descent (Section 3.7).

For $n = 25$ the Frey curve is replaced by Edwards' parametrization of $x^2 + y^3 + z^5 = 0$, and the reduction of Freitas and Stoll leads to points of five genus-2 curves $Y^2 = X^5 + \beta$ over fields L of degree 12 (Section 11). The descent by $1 - \zeta_5$ over $F = L(\zeta_5)$ and a sieve leave, for each curve, the class of one known point and one 5-adic disc around it (Section 12). Stoll's criterion at a prime above 5 with ramification index 20 settles three of the five curves (Sections 13 and 14). For the other two it fails on a smaller 5-adic disc around the known point, although for one of them it still succeeds on the surrounding annulus. For the other, the first coefficient of the expansion of the logarithm along the disc has a local class that lies in the image of the Selmer group, but not in the span of the classes of the known point and of a torsion point. So the local information cannot exclude a global point that we have not found or an element of the Tate–Shafarevich group. We therefore lift the points to a $(1 - \zeta_5)$-covering of the curve and pass to a quotient of genus 2 on which all the lifts have the same descent class. There a Galois symmetry puts the relevant local classes outside the image of the Selmer group (Section 15).

For $n = 13$ the curve $X_0(13)$ has genus 0, and a solution gives instead a point on a twist X_ψ of $X_1(13)$, of genus 2, over a field K_E of degree 14 [27, §§8.1, 9]. The diamond automorphism σ of order 3 is defined over K_E, and we descend by $1 - \sigma$. The twist acts through the diamond operators, a cyclic group of order 6, and those of order 3 act trivially on the kernel of $1 - \sigma$. So the cubic part of the twist, its component of order 3, drops out, and the Kummer map takes values in the cube classes of a field L_E of degree 56 (Proposition 16.3). A 2-descent would need one of degree 84. The Selmer groups have dimensions 4, 2, 4, 2, in each case larger than the span of the known points, and a 3-adic analysis as above, with the logarithm on $J(K_\mathfrak{p})$ measured in powers of $1 - \sigma$, finishes the proof (Section 17). For 96a1 the known point is a cusp, and we divide $2[Q - \iota Q_0] - [Q_0 - \iota Q_0]$, where Q is the point given by a solution, Q_0 the point given by E and ι the hyperelliptic involution. With a cusp in place of Q this class is torsion (Lemma 17.8).

1.4. **Comparison with earlier work.** Compared with [27] and [28], what is new is the use of these descents inside the fields K_E, the forms of Stoll's criterion just described, and the sieve at good primes. Our location of the points over an ℓ-adic disc also covers the case

n	genus	descent	fields	known points and sieves
11	1	kernel μ_5, over K_E	5, degree 12	the ten known points of Table 9; sieves at 31 and 191
17	1	2-descent over $K_E(i)$	4, degree 18	2-adic logarithm modulo local torsion; sieve at 13
19	1	kernel μ_3, over K_E	6, degree 20	3-adic logarithm; ramification points over 1728; sieves at 13, 23, 43, 67
23	2	Eisenstein, kernel μ_{11}, over K_E	5, degree 24	λ-direction; second descent for the CM curves; sieves at 89 and 43
29	2	Eisenstein, kernel μ_7, over K_E	6, degree 30	λ-direction; second descent for 27a1
25	2	$1-\zeta_5$, over $L(\zeta_5)$	5, degree 12	Stoll's criterion at $e = 20$; a second descent for two curves
13	2	$1-\sigma$, through L_E of degree 56	4, degree 14	3-adic logarithm; the cusps for 96a1

TABLE 2. The ingredients for each exponent. The genus is that of $X_0(p)$, for $n = 25$ that of the curves $Y^2 = X^5 + \beta$, and for $n = 13$ that of the twists of $X_1(13)$. The known points are the points whose j-invariant is 0, 1728 or that of a curve isogenous to E by an isogeny of degree prime to p (Section 2.6). The λ-direction is explained in Section 1.3, and the second descent in Section 3.7.

in which ℓ divides the ramification index of the j-map, where [27, Lemma 7.5] as stated does not hold (Remark 4.3). For $n = 13$, which Freitas, Naskręcki and Stoll left open, what is new is the descent by $1-\sigma$ through fields of degree 56 instead of 84, and the 3-adic analysis of Section 17.

The most recent work on the equation is that of Freitas, Mocanu and Sánchez-Rodríguez [26], on the anti-symplectic twists $X_E^-(p)$ left by the reduction of [27], for all primes p. A criterion of Freitas and Mocanu decides whether $X_E^-(p)$ has a point over $\mathbb{Q}_\ell$, for primes $p \geq 7$ and $\ell \neq p$ at which E has good reduction [25, Theorem 5.3]; an earlier form of it is quoted in [26, Theorem 1.1]. Such local obstructions can occur only for $p \equiv 19 \pmod{24}$ and the three curves of conductor 864 [26, §2, (2.6)]. A search over the primes $p < 1000$ finds them, for instance, for $X_{864a1}^-(p)$ with $p = 19$, 43 and $X_{864b1}^-(p)$ with $p = 19$, 43, 67 [26, Theorem 1.2]. For the other pairs (E, p), if $X_E^-(p)$ has $\mathbb{Q}_\ell$-points for a prime $\ell > 3$ different from p, then it has $\mathbb{Q}_\ell$-points that come from ℓ-adic solutions of the equation, so these twists cannot be removed by local conditions at such primes [26, Theorem 3.1]. For $X_{864a1}^-(19)$ and $X_{864b1}^-(19)$ we use the result of Freitas and Kraus, which the local result of [26] recovers (Theorem 2.1). The twists that we treat (Table 4) are the ones their method cannot reach: the symplectic twists $X_E(p)$, which always have the rational point given by E, and anti-symplectic twists without such local obstructions.

Besides standard results, cited where they are used, the main published inputs are the reduction of Freitas, Naskręcki and Stoll [27], with the covering argument of their treatment of the CM twists at $p = 11$ [27, §7.1] (Proposition 2.3); for $p = 17$, the theorem of Balakrishnan, Dogra, Müller, Tuitman and Vonk on the non-split Cartan modular curve of level 17 [2, Theorem 1.2]; and the criterion of Belabas, Diaz y Diaz and Friedman [3]. The proof of Theorem C also uses the reduction of Freitas and Stoll [28], an arXiv preprint without a refereed version: Theorem 11.6 states what we use from it, and the list after its proof gives the statements of [28] that we use without a new proof.

Symbol	Meaning
$(a, b, c),\ j_0$	a primitive solution with $abc \neq 0$; the j-invariant $1728b^3/c^p$ of its Frey curve
$E,\ K_E$	a curve of Theorem 2.1; the field of a subgroup of order p of $E[p]$ (Definition 2.7)
$X_0(p),\ J,\ T$	the modular curve with the models of Table 5; its Jacobian $J_0(p)$ $(= X_0(p)$ with origin the cusp ∞ in genus 1); the rational torsion point of Table 5
$j,\ \mathcal{A}_p,\ \mathcal{B}_p,\ G_p$	the j-map and the polynomials $\mathcal{A}_p$, $\mathcal{B}_p$ that define it (Lemma 2.5); its fibre polynomial (2.4)
$\ell,\ \delta,\ \delta_v,\ \Sigma$	the prime of the descent; the global and local Kummer maps; the image of the Selmer group at the places above ℓ
$\lambda,\ \mu$	for genus 2, the Eisenstein prime above ℓ and its cofactor, $\ell = \lambda\mu$ (Section 3.5)
$P,\ P_0,\ Q$	the point of a solution (Proposition 2.12); a known point (Section 2.6); a point with rational j-invariant
$\Theta,\ \Lambda$	the classes of local torsion; the image of the logarithm (Section 5)

Terms defined in the paper

admissible configuration: one local point over j_1 at each place above ℓ, from distinct Galois orbits, of size n_v at v (Section 2.5)
family, *branch*: a set $\{j_c + \kappa t^e\}$ of j-values; a power series for the roots near a point of the fibre (Section 4.1)
class tuple, *disc test*: the local classes of a configuration; their test against Σ (Section 4.4)
level: the exponent of divisibility of a local point or of its logarithm (Section 5.1)
centre, *fixed term*, *branch term*, *branch datum*: the terms of the enumeration of Section 5.4
λ-*direction*: for genus 2, the line of the tangent space of J on which the Hecke algebra acts through its completion at λ; the component of the logarithm along it measures divisibility by λ (Sections 3.6 and 5.5)

TABLE 3. Main notation and terms of Parts I and II.

The computations use PARI/GP [43], Python with python-flint [23, 33] and SageMath [49]. Appendix B gives the software versions, explains how the precision is controlled and says, in a table, which computations were repeated and how; Table S31 lists the computations. The programs and their outputs are available at [32].

1.5. **Plan of the paper.** Part I (Sections 2, 3, 4 and 5) develops the method for the prime exponents 11, 17, 19, 23 and 29, Part II applies it to each of them, Part III treats the exponent 25, and Part IV the exponents 13 and 26, ending with the exponents that remain open (Section 18). Tables numbered S1, S2, ... are in the Supplement, which prints the data of the individual cases that the proofs use (bases of Selmer groups and local images, class tuples and levels), the defining polynomials of the fields, the forms of Part III, and a list of the computations.

For a finite extension M of $\mathbb{Q}_\ell$ we write v_ℓ for the valuation on M with $v_\ell(\ell) = 1$, and v_M for the normalized valuation. For a number field K and a place v of K above a prime ℓ we write K_v for the completion, $\mathcal{O}_v$ for its ring of integers, k_v for its residue field, $n_v = [K_v : \mathbb{Q}_\ell]$, and e_v, f_v for the ramification index and residue degree. Table 3 lists the notation of Parts I and II. Part III has its own short list (Section 11.7).

Part I. Points of $X_0(p)$ over the fields K_E

2. From solutions to points of $X_0(p)$ over number fields

A primitive solution (a, b, c) with $abc \neq 0$ of $x^2 + y^3 = z^p$, for $p \in \{11, 17, 19, 23, 29\}$, gives a point P of the modular curve $X_0(p)$ with rational j-invariant, defined over one of 26 explicit number fields K_E of degree $p + 1$ (Proposition 2.12).

2.1. **The Frey curve.** Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^p$ with $abc \neq 0$. Its *Frey curve* is

$$E_{a,b,c}\colon\ Y^2 = X^3 + 3bX - 2a, \tag{2.1}$$

with invariants

$$c_4 = -12^2 b, \qquad c_6 = 12^3 a, \qquad \Delta = -12^3 c^p, \qquad j(E_{a,b,c}) = j_0 := \frac{1728\, b^3}{c^p}$$

[27, §2, (2.2)]. Since a, b, c are nonzero, $j_0 \notin \{0, 1728, \infty\}$. A common prime factor of b and c would divide a, so $\gcd(b, c) = 1$. For $d \in \mathbb{Q}^\times$ we write $E^{(d)}$ for the quadratic twist of an elliptic curve E by d. Twisting does not change the j-invariant.

Let E be an elliptic curve over $\mathbb{Q}$ and p a prime. An isomorphism $\varphi\colon E'[p] \to E[p]$ of Galois modules multiplies the Weil pairing by a constant $r(\varphi) \in \mathbb{F}_p^\times$, and it is *symplectic* if $r(\varphi)$ is a square and *anti-symplectic* otherwise [27, §4]. The twists $X_E(p)$ and $X_E^-(p)$ of $X(p)$ are the curves over $\mathbb{Q}$ whose non-cuspidal points over a field F of characteristic 0 correspond to the pairs (E', φ) of an elliptic curve E' over F and an isomorphism $\varphi\colon E'[p] \to E[p]$ of $\mathrm{Gal}(\bar{F}/F)$-modules with $r(\varphi) = 1$, respectively $r(\varphi)$ a fixed non-square in $\mathbb{F}_p^\times$, up to isomorphism [27, §§1,4], [46]. A primitive solution *gives a point* on $X_E^\pm(p)$ if some twist $E' = E_{a,b,c}^{(d)}$ admits such an isomorphism over $\mathbb{Q}$.

2.2. **The reduction of Freitas, Naskręcki and Stoll.**

Theorem 2.1 (Freitas, Naskręcki and Stoll)**.** *Let $p \in \{11, 17, 19, 23, 29\}$ and let (a, b, c) be a primitive solution of $x^2 + y^3 = z^p$ with $abc \neq 0$. Then there is $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ such that $E' = E_{a,b,c}^{(d)}$ gives a rational point on one of the twists $X_E^\pm(p)$ of Table 4. In particular $E'[p] \simeq E[p]$ as $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules for a curve E in that table. Moreover $3 \nmid c$ when $p = 17$, and $3 \mid c$ if and only if $E = 96\mathrm{a}1$ when $p = 19$.*

p	p mod 24	twists of Theorem 2.1	CM twists
11	11	27a1, 54a1, 96a1, 288a1, 288a2, 864a1, 864b1, 864c1	Proposition 2.3
17	17	27a1, 54a1, 864a1, 864b1, 864c1	Proposition 2.2
19	19	54a1, $96\mathrm{a}1^-$, $288\mathrm{a}1^\pm$, 864a1, 864b1, $864\mathrm{c}1^\pm$	Proposition 8.11
23	23	27a1, 288a1, 864a1, 864b1, 864c1	Propositions 9.9 and 9.13
29	5	27a1, 54a2, 96a1, $864\mathrm{a}1^\pm$, $864\mathrm{b}1^\pm$, $864\mathrm{c}1^\pm$	Proposition 10.2

Table 4. The twists of $X(p)$ that can carry the point of a primitive solution with $abc \neq 0$. An entry E stands for $X_E(p)$, E^- for $X_E^-(p)$, and $E^\pm$ for both. The last column points to the treatment of the twists of the CM curves 27a1, 288a1, 288a2. At $p = 29$ the curve 54a2 is 3-isogenous to 54a1, so $54\mathrm{a}2[29] \simeq 54\mathrm{a}1[29]$ as Galois modules, and we work with $E = 54\mathrm{a}1$.

Proof. By [27, Proposition 2.4] the mod p representation of $E_{a,b,c}$ is irreducible, so by [27, Lemma 2.3] some twist $E' = E^{(d)}_{a,b,c}$ with $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ has $E'[p] \simeq E[p]$ for one of the seven curves 27a1, 54a1, 96a1, 288a1, 864a1, 864b1, 864c1. Theorem 5.1 of [27] lists the twists that can carry the resulting point, by p modulo 24: for $p = 11$ and $p = 23$ they are those of Table 4. For $p = 17$ the list also contains $X_{288\mathrm{a}1}(17)$. For $p = 19$ it is $X_{27\mathrm{a}1}$, $X_{54\mathrm{a}1}$, $X_{96\mathrm{a}2}$, $X_{288\mathrm{a}1}$, $X_{288\mathrm{a}2}$, $X^{\pm}_{864\mathrm{a}1}$, $X^{\pm}_{864\mathrm{b}1}$, $X^{\pm}_{864\mathrm{c}1}$. For $p = 29$ the list also contains $X_{288\mathrm{a}1}(29)$ and $X_{288\mathrm{a}2}(29)$.

For $p = 11$, $X_{288\mathrm{a}2}(11) \simeq X^{-}_{288\mathrm{a}1}(11)$ because $(2/11) = -1$. For $p = 19$, $X_{96\mathrm{a}2}(19) \simeq X^{-}_{96\mathrm{a}1}(19)$ and $X_{288\mathrm{a}2}(19) \simeq X^{-}_{288\mathrm{a}1}(19)$ because $(2/19) = -1$, as in the proof of [27, Theorem 5.1]. For $p = 17$ and $p = 29$, the twists attached to 288a1 and to the 2-isogenous curve 288a2 give only trivial solutions by [27, Lemma 6.1(2)], since $17 \equiv 29 \equiv 1 \pmod 4$. For $p = 19$, $X_{27\mathrm{a}1}(19)$ gives only trivial solutions by [27, Lemma 6.1(1)], since $19 \equiv 1 \pmod 3$. Also for $p = 19$, $X^{-}_{864\mathrm{a}1}(19)$ and $X^{-}_{864\mathrm{b}1}(19)$ carry no point coming from a primitive solution, by Freitas and Kraus [24, §32, Theorem 23], working at the primes 5 and 7 respectively (see [27, §5, before Proposition 5.4]). This leaves the twists of Table 4.

The proof of [27, Theorem 5.1] shows that $3 \mid c$ if and only if a twist of the Frey curve has multiplicative reduction at 3, and that the curve E is then 96a1, the only one of the seven curves with multiplicative reduction at 3. Conversely, the curve $E = 96\mathrm{a}1$ occurs only in line 1 of [27, Table 2], where $3 \mid c$. This gives the statement for $p = 19$. For $p = 17$, suppose that $3 \mid c$. Then $E = 96\mathrm{a}1$, and the isomorphism $E'[17] \simeq 96\mathrm{a}1[17]$ is symplectic if and only if $(-6/17) = 1$ ([27, Theorem 4.1] and the proof of [27, Theorem 5.1]), and $(-6/17) = -1$. On the other hand c is odd, since $6 \nmid c$ [27, Corollary 3.2]. So E' has potentially good reduction at 2 with the same inertial field as 96a1, whose inertia group at 2 is the quaternion group. As $(2/17) = 1$, [27, Theorem 4.6(1)] shows that the isomorphism is symplectic. This contradiction shows $3 \nmid c$. □

From now on only the isomorphism $E'[p] \simeq E[p]$ is used, so $X_E(p)$ and $X^{-}_E(p)$ are treated together. The curve 27a1 has complex multiplication by $\mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$, and the curves 288a1, 288a2 by $\mathbb{Z}[i]$. At $p = 11$ and $p = 17$ their twists are removed as follows.

Proposition 2.2. *No primitive solution of $x^2 + y^3 = z^{17}$ with $abc \neq 0$ gives a rational point on $X_{27\mathrm{a}1}(17)$.*

Proof. As $17 \equiv 2 \pmod 3$, the prime 17 is inert in $\mathbb{Q}(\sqrt{-3})$, whose maximal order $\mathbb{Z}[\omega]$ is the endomorphism ring of 27a1. So the image of the mod 17 representation of 27a1 lies in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_{17})$. If $E'[17] \simeq 27\mathrm{a}1[17]$, the same holds for E'. Since the determinant is surjective, E' then defines a non-cuspidal rational point of $X^{+}_{\mathrm{ns}}(17)$ with j-invariant j_0. By [2, Theorem 1.2], $X^{+}_{\mathrm{ns}}(17)(\mathbb{Q})$ consists of seven CM points, of discriminants -3, -7, -11, -12, -27, -28, -163. So j_0 is one of the integers 0, -3375, -32768, 54000, -12288000, 16581375, -262537412640768000. By Lemma 2.15(a), (a, b, c) is then a Catalan solution, with $j_0 = -13824$, which is not in the list. □

Proposition 2.3 ([27, §7.1])**.** *Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{11}$ with $abc \neq 0$, and let E' be an elliptic curve over $\mathbb{Q}$ with $j(E') = j_0$, that is, a twist $E^{(d)}_{a,b,c}$ for some $d \in \mathbb{Q}^{\times}$. Then there is no isomorphism $E'[11] \simeq E[11]$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules, symplectic or not, with $E \in \{27\mathrm{a}1, 288\mathrm{a}1, 288\mathrm{a}2\}$. In particular no primitive solution with $abc \neq 0$ gives a rational point on $X_E(11)$ or $X^{-}_E(11)$ for these E.*

The proof in [27, §7.1 and the remark after Theorem 7.1] uses a covering collection of the twists of the non-split Cartan curve of level 11 and elliptic Chabauty over a cubic field,

carried out in Magma by Stoll's script [62]. It does not use GRH: the script assumes GRH only when it recomputes the Selmer groups of [27, §7.2], and the published script does not recompute them. The argument of [27, §7.1] uses only the isomorphism class of the Galois module $E'[11]$, not the symplectic type. So the reduction at $p = 11$ to the five curves of Section 6 needs from [27] only Lemma 2.3, Proposition 2.4 and §7.1, and not Theorem 5.1, which at $p = 11$ removes none of the seven curves (Table 4). We have recomputed the Mordell–Weil groups over the cubic field and the elliptic Chabauty step without Magma and without GRH (Appendix B.2).

2.3. **The curve $X_0(p)$ and its j-map.** For $p \in \{11, 17, 19\}$ the curve $X_0(p)$ has genus one, and $J = X_0(p)$ is the elliptic curve of Table 5, with origin O the cusp ∞. For $p \in \{23, 29\}$ it has genus two, and $J = J_0(p)$ is its Jacobian. In both cases the rational cuspidal subgroup of J is cyclic of order the numerator of $(p-1)/12$, namely 5, 4, 3, 11, 7 [39]. The prime ℓ dividing this order is the prime of the descents of Section 3, and the table gives $T \in J(\mathbb{Q})$.

p	model of $X_0(p)$	ℓ	T	cusps ∞ and 0
11	11a1: $y^2 + y = x^3 - x^2 - 10x - 20$	5	$(5, 5)$, of order 5	O; $3T = (16, 60)$
17	17a1: $y^2 + xy + y = x^3 - x^2 - x - 14$	2	$(7, 13)$, of order 4	O; $-T = (7, -21)$
19	19a1: $y^2 + y = x^3 + x^2 - 9x - 15$	3	$(5, 9)$, of order 3	O; $-T = (5, -10)$
23	$y^2 = x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$	11	$[(0) - (\infty)]$, of order 11	at infinity, with $y/x^3 \to -1$, resp. 1
29	$y^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$	7	$[(0) - (\infty)]$, of order 7	the same

TABLE 5. The curves $X_0(p)$. For $p \le 19$ the model is the minimal model of the elliptic curve with the given Cremona label, $J(\mathbb{Q})$ is cyclic of order 5, 4, 3, generated by T, and the x-coordinate x_p^0 of the cusp 0 is 16, 7, 5. The non-cuspidal rational points are $\{T, 2T, 4T\}$ for $p = 11$, $\{T, 2T\}$ for $p = 17$ and $\{T\}$ for $p = 19$. For $p = 17$, $2T = (11/4, -15/8)$, $j(T) = -17 \cdot 373^3/2^{17}$ and $j(2T) = -17^2 \cdot 101^3/2$. For $p = 19$, $j(T) = -2^{15} \cdot 3^3$.

For $p \in \{11, 17, 19\}$, $J(\mathbb{Q})$ consists of cusps and of the points attached to the rational p-isogenies [39, 40]. We write the models of Table 5 as $y^2 + H(x)y = F(x)$, with $H = 1$, $x + 1$, 1 for $p = 11$, 17, 19, and $H = 0$ for $p = 23$, 29.

For $p \in \{23, 29\}$ the model comes from cusp forms. Let $g_1 = q + O(q^3)$ and $g_2 = q^2 + O(q^3)$ be the basis of $S_2(\Gamma_0(p))$ in echelon form, with integral q-expansions, and put

$$x = g_1/g_2, \qquad y = q\,\frac{dx}{dq}\Big/ g_2,$$

and let w_p be the Atkin–Lehner involution. The Hecke algebra of $S_2(\Gamma_0(p))$ is $\mathbb{Z}[T_2]$, with $T_2^2 + T_2 - 1 = 0$ for $p = 23$ and $T_2^2 + 2T_2 - 1 = 0$ for $p = 29$. Both Atkin–Lehner eigenvalues are -1, so $a_p = +1$ for both newforms.

Proposition 2.4. *Let $p \in \{23, 29\}$. Then $X_0(p)$ is the smooth projective curve of genus two with the affine model $y^2 = F(x)$ of Table 5. For $p = 23$, $F = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$. We have* $\operatorname{disc} F = 2^{12} \cdot 23^6$, *resp.* $2^{12} \cdot 29^5$. *The involution w_p is $(x, y) \mapsto (x, -y)$, the hyperelliptic involution. The two points at infinity are the cusps: ∞, where $y/x^3 \to -1$, and 0, where $y/x^3 \to 1$.*

Proof. The space $S_2(\Gamma_0(p))$ has dimension 2, and w_p acts on it as -1, so x is w_p-invariant. The differentials $g\,dq/q$ ($g \in S_2$) are the holomorphic differentials of $X_0(p)$, so the canonical map is $(g_1 : g_2) = x\colon X_0(p) \to \mathbb{P}^1$, of degree 2. So $X_0(p)$ is hyperelliptic and x is the quotient by the hyperelliptic involution. It has simple poles at the cusp ∞ (where $x = q^{-1} + 2 + O(q)$ for $p = 23$) and at $0 = w_p(\infty)$. Hence w_p is the hyperelliptic involution, $dx/y = g_2\,dq/q$ is holomorphic, y has poles of order 3 at the two cusps and nowhere else, and $y \circ w_p = -y$. The function $y^2 - F(x)$ has poles only at the two cusps, of order at most 6 at each, so at most 12 poles in all. Its q-expansion at ∞ is $O(q^{13})$ (Appendix B), so it has a zero of order at least 13 there, and it is 0. The discriminant of F is as stated, and $y/x^3 = \mp 1 + O(q)$ at the two cusps is read off from the expansions. □

The next lemma gives the j-map and, for $p \in \{23, 29\}$, the modular unit that computes the Kummer map of Section 3.5, with $r_p = 12$, resp. 6, chosen so that $r_p(p-1)/24 = \ell$.

Lemma 2.5. (a) *Let $p \in \{11, 17, 19\}$. The j-map $j\colon J \to \mathbb{P}^1$ has degree $p+1$, with a simple pole at O and a pole of order p at the cusp 0, and*

$$j = \frac{\mathcal{A}_p(x) + \mathcal{B}_p(x)\,y}{(x - x_p^0)^p} \tag{2.2}$$

with $\mathcal{A}_p, \mathcal{B}_p \in \mathbb{Z}[x]$ of degrees p and $p-1$.

(b) *Let $p \in \{23, 29\}$. The j-map on $X_0(p)$ is*

$$j = \mathcal{A}_p(x) + \mathcal{B}_p(x)\,y \tag{2.3}$$

with $\mathcal{A}_p, \mathcal{B}_p \in \frac{1}{2}\mathbb{Z}[x]$ of degrees p and $p-3$ such that $2\mathcal{A}_p$ and $2\mathcal{B}_p$ are monic.

(c) *Let $p \in \{23, 29\}$. The function $f = (\eta(\tau)/\eta(p\tau))^{r_p}$ on $X_0(p)$ equals $f_0(x) + f_1(x)\,y$ with $f_0, f_1 \in \frac{1}{2}\mathbb{Z}[x]$ of degrees 11 and 8 for $p = 23$, and 7 and 4 for $p = 29$. Moreover $f_0^2 - f_1^2 F = p^{r_p/2}$ ($= 23^6$, resp. 29^3), $f \circ w_p = p^{r_p/2}/f$, $\operatorname{div} f = \ell(0) - \ell(\infty)$, $f/x^\ell \to 1$ at the cusp ∞ and $f\,x^\ell \to p^{r_p/2}$ at the cusp 0.*

The polynomials $\mathcal{A}_p$ and $\mathcal{B}_p$ determine the fibre polynomials G_p and the fields K_E below. For $p = 11$ they are those of [27, §7.2]. *For $p = 17$, 19, 23, 29 their coefficients have up to 21 digits, and they are not printed here but given in* [32] *(Appendix C.1); f_0 and f_1 are printed in Appendix C.1.*

Proof. The coefficients were found by linear algebra on q-expansions, and the q-expansions below are those of Appendix B.

(a) The function $g = j\,(x - x_p^0)^p - \mathcal{A}_p(x) - \mathcal{B}_p(x)y$ on J has poles at most at O, of order at most $2p+1$, and at the cusp 0, of order at most p. The coefficients of its expansion in q at the cusp ∞ vanish from q^{-2p-1} to q^p and beyond. So g has a zero of order greater than p at O and at most p poles, hence $g = 0$. The q-expansions of x and y are those of the modular parametrization computed by PARI for $p = 17, 19$, and of its composite with -1 for $p = 11$. The later sections use only that (2.2) is the j-map for some isomorphism $X_0(p) \to J$ that takes the cusp ∞ to O.

(b) The function $j - (\mathcal{A}_p(x) + \mathcal{B}_p(x)y)$ has poles only at the cusps, of order at most p at each, since j has a simple pole at ∞ and a pole of order p at 0. Its q-expansion at ∞ is $O(q^{2p+1})$, so it has more zeros than poles and is 0.

(c) Likewise $f - (f_0 + f_1 y)$ has poles of order at most ℓ at each cusp, and its q-expansion is $O(q^{2\ell+1})$. The η-quotient f has order $r_p(1-p)/24 = -\ell$ at ∞ and $+\ell$ at 0. The identity $\eta(-1/\tau) = \sqrt{\tau/i}\,\eta(\tau)$ gives $f(-1/(p\tau)) = p^{r_p/2}/f(\tau)$, that is $f \circ w_p = p^{r_p/2}/f$.

Since $f\circ w_p = f_0 - f_1 y$, this is $f_0^2 - f_1^2 F = p^{r_p/2}$. The limits at the cusps follow from $f = q^{-\ell} + O(q^{1-\ell})$, $x = q^{-1} + O(1)$ and $f\circ w_p = p^{r_p/2}/f$. □

For $p \in \{23, 29\}$ the model $y^2 = F(x)$ is smooth over $\mathbb{Z}[1/(2p)]$, in particular over $\mathbb{Z}_\ell$, and j and f have ℓ-integral coefficients. The cuspidal divisor class

$$T := [(0) - (\infty)] \in J(\mathbb{Q})$$

has order ℓ, since $\ell((0)-(\infty)) = \operatorname{div} f$ (Lemma 2.5(c)) and $T \neq 0$, as $X_0(p)$ has positive genus. For $p \in \{11, 17, 19\}$ the class $[(0)-(\infty)]$ is the cusp 0, which is $3T$, $-T$, $-T$ (Table 5). For these p we work with the generator T of $J(\mathbb{Q})$ given in the table.

The points of $X_0(p)$ over a value of j are described by the *fibre polynomial*. For $p \in \{23, 29\}$ put $G_p(x, J) := \big(\mathcal{A}_p(x) - J\big)^2 - \mathcal{B}_p(x)^2 F(x)$, and for $p \in \{11, 17, 19\}$ put

$$G_p(x, J) := -\frac{\big(J(x-x_p^0)^p - \mathcal{A}_p\big)^2 + H(x)\,\mathcal{B}_p\,\big(J(x-x_p^0)^p - \mathcal{A}_p\big) - \mathcal{B}_p^2\,F(x)}{(x-x_p^0)^p}, \tag{2.4}$$

where J is an indeterminate. For $p \le 19$ this comes from eliminating y between (2.2) and the equation $y^2 + H(x)y = F(x)$ of J. For $p = 11$ it is the polynomial F of [27, (7.4)].

Lemma 2.6. *Let $p \in \{11, 17, 19, 23, 29\}$. Then $G_p(x, J)$ is monic of degree $p+1$ in x. For $p \le 19$ the division in (2.4) is exact, $G_p \in \mathbb{Z}[x, J]$, and G_p has degree 2 in J. For $p \ge 23$ the coefficients of G_p lie in $\mathbb{Z}[J]$. For $J_1 \in \bar{\mathbb{Q}}$ the roots of $G_p(x, J_1)$, with multiplicity, are the x-coordinates of the $p+1$ points of $X_0(p)$ over $j = J_1$, each counted with its ramification index.*

Proof. For $p \le 19$, the function $\varphi = (x - x_p^0)^p(j - J_1)$ vanishes at the points over J_1, and to order p at the point with $x = x_p^0$ other than the cusp 0, and it has no other zeros. Its only pole is O, of order $2p+1$. By (2.2), $\varphi = \mathcal{B}_p y - U$ with $U = J_1(x - x_p^0)^p - \mathcal{A}_p$, and since $y \mapsto -H - y$ is the nontrivial automorphism of the function field over $\bar{\mathbb{Q}}(x)$, the norm of φ to $\bar{\mathbb{Q}}(x)$ is $(\mathcal{B}_p y - U)(\mathcal{B}_p(-H-y) - U) = U^2 + H\mathcal{B}_p U - \mathcal{B}_p^2 F = -(x - x_p^0)^p G_p(x, J_1)$. The divisor of the norm is the image under x of the divisor of φ, so the norm is a constant times $(x - x_p^0)^p \prod_Q (x - x(Q))$, the product over the points over J_1 counted with ramification index. The norm has degree $2p+1$ and leading coefficient -1, since F is monic of degree 3 and $\mathcal{B}_p$ has degree $p-1$ and leading coefficient ± 1. That $\mathcal{B}_p$ has leading coefficient ± 1 follows from (2.2) at O, the cusp ∞, where j, x and y have leading terms q^{-1}, q^{-2} and $\pm q^{-3}$. Hence $G_p(x, J_1) = \prod_Q (x - x(Q))$, which is monic of degree $p+1$. As this holds for every J_1, $(x - x_p^0)^p$ divides the numerator of (2.4) in $\mathbb{Q}[x, J]$, hence in $\mathbb{Z}[x, J]$ by Gauss's lemma, and G_p has degree 2 in J. For $p \ge 23$, the product $(j - J)(j\circ w_p - J) = (\mathcal{A}_p - J)^2 - \mathcal{B}_p^2 F$ is w_p-invariant, with poles of order $p+1$ at each cusp, hence a polynomial of degree $p+1$ in x. Its coefficients were computed exactly. Its divisor on $X_0(p)$ is $j^*(J) + w_p^* j^*(J) - (p+1)\big((\infty) + (0)\big)$, which is also the divisor of $\prod_Q (x - x(Q))$, the product over the fibre $j^*(J)$ with multiplicities. □

2.4. The fields K_E.

Definition 2.7. For an elliptic curve E over $\mathbb{Q}$ and a prime p, K_E is the field of definition of one subgroup of order p of $E[p]$. It is well defined up to isomorphism when the Galois group permutes these subgroups transitively.

We use K_E for the 26 pairs (p, E) of Table 4 other than those removed by Propositions 2.2 and 2.3, with 54a1 in place of 54a2 at $p = 29$. They are listed in Tables 6, 7 and 8, and for $p = 11$ they are those of [27, §7.2 and Table 5]. For E other than 288a1 put $j_E := j(E)$

if E has no complex multiplication, and $j_E := j(27a2) = -12288000$ if $E = 27a1$, where 27a2: $y^2 + y = x^3 - 270x - 1708$ is 3-isogenous to 27a1. The j-invariants 0 and 1728 of 27a1 and 288a1 are branch values of j, so their fibres do not give the fields. The field K_{288a1} is described in Proposition 2.9.

Proposition 2.8. *Let (p, E) be one of the 26 pairs above.*

(a) *If $E \neq 288a1$, the polynomial $G_p(x, j_E)$ is irreducible of degree $p+1$, and $K_E \simeq \mathbb{Q}[x]/(G_p(x, j_E))$.*
(b) *The field K_E has degree $p+1$ and the invariants listed in Table 6 ($p \leq 19$) and Tables 7 and 8 ($p = 23, 29$).*
(c) *If $p \leq 19$ and $E \neq 288a1$, then K_E has no subfields other than $\mathbb{Q}$ and K_E.*
(d) *For $p = 17$ the mod 17 representation of E is surjective.*

Proof. (a) Let E_1 be E, or 27a2 if $E = 27a1$. An isogeny of degree prime to p identifies the Galois sets of subgroups of order p, so we may use E_1. As $j(E_1) \notin \{0, 1728\}$, $\mathrm{Aut}(E_{1,\bar{\mathbb{Q}}}) = \{\pm 1\}$ fixes every subgroup of order p, and the fibre of $X_0(p) \to X(1)$ over $j(E_1)$ is, as a Galois set, the set of subgroups of order p of $E_1[p]$. By Lemma 2.6 the x-coordinates of its points are the roots of $G_p(x, j_E)$. A computation (Appendix B) shows that this polynomial is irreducible. So the Galois action is transitive, x separates the points of the fibre, and the field of definition of a subgroup is $\mathbb{Q}(x(Q)) \simeq \mathbb{Q}[x]/(G_p(x, j_E))$ for the corresponding point Q.

(b) and (c) are computations (Appendix B), with the rings of integers, hence the discriminants, determined unconditionally. The captions say what is proved about the class groups.

(d) Let $H \subseteq \mathrm{GL}_2(\mathbb{F}_{17})$ be the image of the mod 17 representation. By (a), H acts transitively on the 18 lines of $E[17]$. By Dickson's classification, a subgroup of $\mathrm{PGL}_2(\mathbb{F}_{17})$ not containing $\mathrm{PSL}_2(\mathbb{F}_{17})$ is contained in a Borel subgroup (which fixes a line), in the normalizer of a split Cartan subgroup (which has an orbit of size 2), in the normalizer of a non-split Cartan subgroup, or is isomorphic to A_4 or S_4 (whose orders are not divisible by 18). The group A_5 does not occur, since $5 \nmid \#\,\mathrm{PGL}_2(\mathbb{F}_{17}) = 4896$. The non-split case is excluded by a prime q of good reduction with $a_q \not\equiv 0$ and $a_q^2 - 4q$ a nonzero square modulo 17. Then Frob_q has distinct eigenvalues in $\mathbb{F}_{17}$ and nonzero trace, which no element of the normalizer of a non-split Cartan subgroup has. One can take $(q, a_q) = (11, -3)$ for 54a1 and $(5, -1)$, $(5, 2)$, $(5, -2)$ for 864a1, 864b1, 864c1. So $H \supseteq \mathrm{SL}_2(\mathbb{F}_{17})$, and $H = \mathrm{GL}_2(\mathbb{F}_{17})$ since the determinant is the cyclotomic character. This also gives (c) for $p = 17$, since $\mathrm{PGL}_2(\mathbb{F}_{17})$ acts 2-transitively on the lines, so the stabilizer of a line is a maximal subgroup. □

Defining polynomials follow from (a) and the j-maps of Appendix C.1, and for 288a1 from Proposition 2.9. For $p \in \{23, 29\}$, ℓ is unramified in every K_E, so K_E contains no nontrivial ℓ-th root of unity, as $\mathbb{Q}(\zeta_\ell)$ is ramified at ℓ. When $\#\,\mathrm{Aut}(K_E) = 2$ we write ι_K for the nontrivial automorphism. For the fields of (c), $\mathrm{Aut}(K_E)$ is trivial: if $\sigma \neq 1$ were an automorphism, its fixed field would be $\mathbb{Q}$ by (c), so $K_E/\mathbb{Q}$ would be Galois of degree $p+1$, and a subgroup of prime order of its Galois group would fix a subfield other than $\mathbb{Q}$ and K_E.

The curve 288a1 has j-invariant 1728, so its field is found from the p-division polynomial. For a subgroup C of order p of $E[p]$, where $E = 288a1$: $y^2 = x^3 + 3x$, put $s(C) = \sum_{R \in C \setminus \{O\}} x(R)$. Let $m_{288}^{(19)}$ and $m_{288}^{(23)}$ be the polynomials of degrees 20 and 24 printed in Appendix C.2.

p	E	signature	$\lvert\operatorname{disc} K_E\rvert$	(e, f) of the places above ℓ	class number
11	54a1	$(2, 5)$	$2^{10}3^{14}11^{9}$	$\ell = 5$: $(1, 1), (1, 11)$	1
	96a1	$(2, 5)$	$2^{18}3^{10}11^{11}$	$(1, 6), (1, 6)$	1
	864a1	$(2, 5)$	$2^{18}3^{14}11^{11}$	$(1, 1), (1, 1), (1, 5), (1, 5)$	divides 2 (2 under GRH)
	864b1, 864c1	$(2, 5)$	$2^{18}3^{14}11^{11}$	$(1, 6), (1, 6)$	divides 2 (2 under GRH)
17	54a1	$(2, 8)$	$2^{16}3^{20}17^{17}$	$\ell = 2$: $(1, 1), (17, 1)$	generated by 5 prime classes (16 under GRH)
	864a1, 864b1, 864c1	$(2, 8)$	$2^{24}3^{20}17^{17}$	$(4, 1), (2, 1), (4, 2), (2, 2)$	1
19	54a1	$(2, 9)$	$2^{18}3^{22}19^{19}$	$\ell = 3$: $(2, 1), (6, 1), (6, 2)$; above 19: $(1, 1), (19, 1)$	1
	96a1	$(2, 9)$	$2^{30}3^{18}19^{19}$	$(1, 1), (19, 1)$; above 19: $(1, 1), (19, 1)$	1
	864a1, 864b1, 864c1	$(2, 9)$	$2^{30}3^{22}19^{19}$	$(2, 1), (6, 1), (6, 2)$; above 19: $(1, 1), (19, 1)$	divides 2 (2 under GRH)
	288a1	$(2, 9)$	$2^{30}3^{10}19^{19}$	$(2, 1), (2, 1), (2, 2)^4$; above 19: $(20, 1)$	$(\mathbb{Z}/2)^k$, $k \le 4$ ($k = 4$ under GRH)

TABLE 6. The fields K_E for $p \in \{11, 17, 19\}$. The discriminant of K_E is positive for $p = 17$ and negative for $p = 11, 19$. The discriminants and the decompositions of primes are computed in rings of integers proved maximal (Appendix A). All class number statements are proved without GRH (Appendix A), and values under GRH are given in parentheses. For 54a1 at $p = 17$ the class group is proved to be generated by the classes of the three primes above 2 and 17 and of two further primes (Proposition A.6). The field $K_{288\text{a}1}$ has subfields of degrees 2, 4, 5 and 10 (Section 8).

Proposition 2.9. *Let $E = 288\text{a}1$ and let C_0 be a subgroup of order p of $E[p]$.*

(a) *For $p = 19$, the minimal polynomial of $s(C_0)$ is $m_{288}^{(19)}$, and $K_E = \mathbb{Q}(s(C_0))$.*

(b) *For $p = 23$, $K_E \simeq \mathbb{Q}[X]/(m_{288}^{(23)})$.*

In both cases $[K_E : \mathbb{Q}] = p + 1$, and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the $p + 1$ subgroups of order p of $E[p]$.

Proof. Let F' be a number field and $\psi_C \in F'[x]$ a monic polynomial of degree $(p-1)/2$ that divides the p-division polynomial ψ_p of E and whose set of roots is mapped into itself by the duplication map $x \mapsto (x^2 - 3)^2/(4x(x^2 + 3))$, which sends $x(R)$ to $x(2R)$. Let $R \in E$ with $x(R)$ a root of ψ_C. Then R has order p, the denominator $4x(x^2 + 3)$ does not vanish at the roots (points of odd order), and every $x(2^k R)$ is a root. The elements -1 and 2 generate $(\mathbb{Z}/p)^\times$, since 2 is a primitive root modulo 19 and has odd order 11 modulo 23. So the $(p-1)/2$ roots of ψ_C are the x-coordinates of the nonzero points of $\langle R\rangle$, each of them for two points $\pm kR$. As $\mathrm{Gal}(\bar{\mathbb{Q}}/F')$ permutes the roots of ψ_C, it maps R into $\langle R\rangle$, so $\langle R\rangle$ is defined over F'. Moreover $s(\langle R\rangle)$ is -2 times the coefficient of $x^{(p-3)/2}$ in ψ_C.

(a) The polynomial $\prod_C (X - s(C))$, over the 20 subgroups C of order 19, has rational coefficients, and $m_{288}^{(19)}$ was found as its numerical value. An exact computation proves

E	j_E	$\operatorname{disc} K_E$	degrees above 11	(e,f) above 23	$\mathrm{Cl}(K_E)$	$\#\operatorname{Aut}$
864a1	-216	$-2^{36}3^{28}23^{21}$	24	$(1,1),(1,1),$ $(22,1)$	$\mathbb{Z}/2$ (GRH)	1
864b1	-13824	$-2^{36}3^{28}23^{23}$	$8,8,8$	$(1,1),(23,1)$	$\mathbb{Z}/2$ (GRH)	1
864c1	1536	$-2^{36}3^{28}23^{21}$	$1,1,22$	$(1,1),(1,1),$ $(22,1)$	$\mathbb{Z}/2$ (GRH)	1
27a1	-12288000	$-3^{28}23^{23}$	$1,1,2^{11}$	$(24,1)$	$\mathbb{Z}/3$ (GRH); $h\in\{1,3\}$	2
288a1	—	$-2^{36}3^{12}23^{23}$	$1,1,2^{11}$	$(24,1)$	$\mathbb{Z}/4\times(\mathbb{Z}/2)^4$ (GRH); $h\mid 2^7$	2

TABLE 7. The fields K_E of degree 24 for $p=23$, all of signature $(2,11)$. The exponent 2^{11} means eleven places of degree 2. The discriminants and the decompositions of primes are computed in rings of integers proved maximal (Appendix A). Groups marked (GRH) are PARI's values, correct under GRH. The statements on the class number h after the semicolons are proved without GRH (Proposition A.12).

E	j_E	$\operatorname{disc} K_E$	degrees above 7	(e,f) above 29	$\mathrm{Cl}(K_E)$	$\#\operatorname{Aut}$
864a1	-216	$2^{42}3^{34}29^{29}$	$15,15$	$(1,1),(29,1)$	1 (GRH)	1
864b1	-13824	$2^{42}3^{34}29^{29}$	$15,15$	$(1,1),(29,1)$	1 (GRH)	1
864c1	1536	$2^{42}3^{34}29^{29}$	5^6	$(1,1),(29,1)$	1 (GRH)	1
54a1	9261/8	$2^{28}3^{34}29^{29}$	5^6	$(1,1),(29,1)$	1 (GRH)	1
96a1	21952/9	$2^{42}3^{28}29^{29}$	$15,15$	$(1,1),(29,1)$	1 (GRH)	1
27a1	-12288000	$3^{34}29^{29}$	5^6	$(30,1)$	$\mathbb{Z}/3$ (GRH); $h\in\{1,3\}$	2

TABLE 8. The fields K_E of degree 30 for $p=29$, all of signature $(2,14)$. The exponent 5^6 means six places of degree 5. The discriminants and the decompositions of primes are computed in rings of integers proved maximal (Appendix A). Groups marked (GRH) are PARI's values, correct under GRH. The statement $h\in\{1,3\}$ on the class number is proved without GRH (Proposition A.12).

equality. The polynomial $m_{288}^{(19)}$ is irreducible. Let s_0 be a root and $F'=\mathbb{Q}(s_0)$. Over F', ψ_{19} has a monic factor ψ_C of degree 9 whose coefficient of x^8 is $-s_0/2$, and ψ_C divides the numerator of $\psi_C((x^2-3)^2/(4x(x^2+3)))$, so the duplication map preserves its roots. By the first paragraph of the proof, $\langle R\rangle$ is defined over F' and $s(\langle R\rangle)=s_0$, so its field of definition is F', of degree 20. So the Galois orbit of $\langle R\rangle$ consists of all 20 subgroups of order 19, C_0 is conjugate to $\langle R\rangle$, $K_E\simeq F'$, and the minimal polynomial of $s(C_0)$ is $m_{288}^{(19)}$.

(b) Let $F'=\mathbb{Q}[X]/(m_{288}^{(23)})$. A computation gives a polynomial $\psi_C\in F'[x]$ of degree 11 that divides ψ_{23} and whose roots are permuted by the duplication map. By the first paragraph of the proof, its roots are the x-coordinates of the nonzero points of a subgroup C of order 23 that is stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/F')$, so the field of definition $\mathbb{Q}(C)$ is contained in F'. The element $s(C)=-2\cdot(\text{coefficient of } x^{10} \text{ in } \psi_C)$ lies in $\mathbb{Q}(C)$ and generates F', since its characteristic polynomial is irreducible of degree 24. Hence $F'=\mathbb{Q}(s(C))\subseteq\mathbb{Q}(C)\subseteq F'$. As $[\mathbb{Q}(C):\mathbb{Q}]=24$, the Galois orbit of C consists of all 24 subgroups of order 23, and $K_E\simeq F'$. □

2.5. **The point attached to a solution.** A solution gives a point P with $j(P) = j_0$ whose x-coordinate generates K_E (Proposition 2.12 below). So $G_p(x, j_0)$ is the minimal polynomial of $x(P)$, and Section 4 uses this to find the images of P at the places above ℓ.

Lemma 2.10. *Let $p \in \{11, 17, 19\}$, let $K = K_E$ for one of the pairs (p, E) of Section 2.4 with $E \neq$ 288a1, and let $Q \in J(K) \setminus J(\mathbb{Q})$. Then $x(Q)$ generates K. If moreover $j(Q) \in \mathbb{Q}$, then $G_p(x, j(Q))$ is the minimal polynomial of $x(Q)$, so it is separable, and Q induces an isomorphism* $\operatorname{Spec} K \to j^{-1}(j(Q))$.

Proof. If $x(Q) \in \mathbb{Q}$, then Q is defined over a field of degree at most 2 inside K. By Proposition 2.8(c) this field is $\mathbb{Q}$, so $Q \in J(\mathbb{Q})$. Hence $\mathbb{Q}(x(Q))$, a subfield of K other than $\mathbb{Q}$, is K. If $j(Q) \in \mathbb{Q}$, then $x(Q)$ is a root of $G_p(x, j(Q)) \in \mathbb{Q}[x]$, which is monic of degree $p + 1 = [K : \mathbb{Q}]$ (Lemma 2.6), so it is the minimal polynomial of $x(Q)$. The $p + 1$ conjugates of Q lie over $j(Q)$ and have distinct x-coordinates, so they are all the points over $j(Q)$. □

At $p = 19$ the field K_{288a1} has the quadratic subfield $\mathbb{Q}(\sqrt{19})$, and the following lemma replaces Lemma 2.10.

Lemma 2.11. *Let $p = 19$, $K = K_{288a1}$, and let $Q \in J(K)$ with $j(Q) \in \mathbb{Q}$ and $\mathbb{Q}(x(Q), y(Q)) = K$. Then $x(Q)$ generates K.*

Proof. Suppose that $F' = \mathbb{Q}(x(Q))$ is not K. As $K = F'(y(Q))$, the extension K/F' is quadratic, and its nontrivial automorphism maps $Q = (x, y)$ to $(x, -1 - y) = -Q$. So $-Q$ lies over $j(Q)$ as well, and $-Q \neq Q$ because $y(Q) \notin F'$. At Q we then have $0 = j(Q) - j(-Q) = \mathcal{B}_{19}(x)(2y + 1)/(x - 5)^{19}$, and $2y + 1 \neq 0$, so $\mathcal{B}_{19}(x(Q)) = 0$. This is impossible, because $\mathcal{B}_{19}$ is irreducible of degree 18 (Appendix B) and $[F' : \mathbb{Q}] = 10$. □

Proposition 2.12. *Let (p, E) be one of the 26 pairs of Section 2.4, $K = K_E$, and let (a, b, c) be a primitive solution of $x^2 + y^3 = z^p$ with $abc \neq 0$ such that some twist $E' = E^{(d)}_{a,b,c}$ has $E'[p] \simeq E[p]$, symplectically or not.*

(a) *There is a point $P \in X_0(p)(K)$ with $j(P) = j_0$ that induces an isomorphism of $\mathbb{Q}$-schemes* $\operatorname{Spec} K \to j^{-1}(j_0)$. *In particular $P \notin X_0(p)(\mathbb{Q})$.*

(b) *The coordinate $x(P)$ generates K, and $G_p(x, j_0)$ is its minimal polynomial. In particular $G_p(x, j_0)$ is separable.*

(c) *For every prime q, the map $v \mapsto$ (the $\operatorname{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$-orbit of P_v) is a bijection from the places $v \mid q$ of K to the orbits of $\operatorname{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ on $j^{-1}(j_0)(\bar{\mathbb{Q}}_q)$, and the orbit of P_v has $n_v = [K_v : \mathbb{Q}_q]$ elements. Here $P_v \in X_0(p)(K_v)$ is the image of P.*

Proof. (a) Since $j_0 \notin \{0, 1728, \infty\}$, the fibre $j^{-1}(j_0)$ is étale over $\mathbb{Q}$, $\operatorname{Aut}(E'_{\bar{\mathbb{Q}}}) = \{\pm 1\}$, and the Galois set of geometric points of the fibre is the set of subgroups of order p of $E'[p]$. An isomorphism $E'[p] \to E[p]$ of Galois modules, symplectic or not, maps these subgroups bijectively and Galois-equivariantly onto those of $E[p]$. These form the Galois set $\operatorname{Hom}(K, \bar{\mathbb{Q}})$, by Proposition 2.8(a) (for 27a1 through the 3-isogeny to 27a2) and by Proposition 2.9 for 288a1. So $j^{-1}(j_0) \simeq \operatorname{Spec} K$. The point P corresponding to the identity embedding (the subgroup with stabilizer $\operatorname{Gal}(\bar{\mathbb{Q}}/K)$) is a K-point. Both schemes are spectra of fields of degree $p + 1$, so P induces the isomorphism. Its residue field is $K \neq \mathbb{Q}$, so $P \notin X_0(p)(\mathbb{Q})$.

(b) For $p \leq 19$ and $E \neq$ 288a1 this is Lemma 2.10. For $(p, E) = (19,$ 288a1$)$, (a) gives $\mathbb{Q}(x(P), y(P)) = K$, and $x(P)$ generates K by Lemma 2.11. Then $G_p(x, j_0)$ is its minimal polynomial, as in Lemma 2.10. For $p \in \{23, 29\}$, two distinct points of $X_0(p)$ with the same x-coordinate have the form Q and $w_p(Q)$. Suppose that both lay over j_0. Since $j(w_p(Q))$ is

the j-invariant of the quotient of E' by the subgroup of order p attached to Q, the curve E' would have an endomorphism of degree p over $\bar{\mathbb{Q}}$, hence complex multiplication. Then j_0 would be the j-invariant of a curve with complex multiplication, which Lemma 2.15(a) excludes. Since $j_0 \notin \{0, 1728\}$ the fibre is also unramified. So by Lemma 2.6 the roots of $G_p(x, j_0)$ are simple, and they are the x-coordinates of the $p+1$ conjugates of P. Hence $x(P)$ has $p+1$ conjugates, generates K, and has minimal polynomial $G_p(x, j_0)$.

(c) Base change of (a) to $\mathbb{Q}_q$ gives $K \otimes \mathbb{Q}_q = \prod_{v|q} K_v \simeq j^{-1}(j_0) \times \mathbb{Q}_q$, compatibly with P. □

The local tests of Section 4 use only the following families of local points.

Definition 2.13. Let K be one of the fields K_E, ℓ the prime of Table 5, and $j_1 \in \mathbb{Q}_\ell$ with $G_p(x, j_1)$ separable. An *admissible configuration over* j_1 is a family $(Q_v)_{v|\ell}$ of points $Q_v \in X_0(p)(K_v)$ over j_1 such that the $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-orbit of Q_v has n_v elements and the orbits for different v are different. Equivalently, the $x(Q_v)$ are roots of pairwise distinct irreducible factors of $G_p(x, j_1)$ over $\mathbb{Q}_\ell$, and the factor at v has degree n_v.

By Proposition 2.12(b) and (c), for every prime q the $x(P_v)$, $v \mid q$, are roots of pairwise distinct $\mathbb{Q}_q$-irreducible factors of $G_p(x, j_0)$, and the factor at v has degree n_v and defines K_v. So the local points $(P_v)_{v|\ell}$ of the point attached to a solution form an admissible configuration over j_0.

2.6. **Known points.** Let (p, E) be one of the 26 pairs of Section 2.4. A *known point* of $X_0(p)(K_E)$ is a point whose j-invariant is 0, 1728, or the j-invariant of an elliptic curve over $\mathbb{Q}$ that is isogenous to E by an isogeny of degree prime to p. Known points include the point over $j(E)$ given by E, and the points of the trivial solutions $(\pm 1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ and of the Catalan solutions $(\pm 3, -2, 1)$, whose Frey curves have j-invariants 0, 1728 and $-13824 = j(864\mathrm{b}1)$.

The ℓ-adic disc of j-values that contains the j-invariant of a known point survives every local test of Section 4, and Section 5 treats these discs. Except for the Catalan solutions, no solution has the j-invariant of a known point (Lemma 2.15).

The curves isogenous to the curves E of Table 4 by isogenies of degree prime to p (of degrees 1, 2, 3, 9) are as follows. The curve 27a1 is isogenous to curves with $j = 0$ and $j = -12288000$. The curve 54a1 ($j = 9261/8$) is isogenous to 54a2 and 54a3, with $j = -1167051/512$ and $j = -132651/2$. The curve 96a1 ($j = 21952/9$) is isogenous to three curves with $j = 7301384/3$, $97336/81$ and $140608/3$. The curves 288a1 and 288a2 have $j = 1728$. The curves 864a1, 864b1, 864c1 ($j = -216$, -13824, 1536) are alone in their isogeny classes. So the known j-invariants are

$$0,\ 1728,\ -216,\ -13824,\ 1536,\ \tfrac{9261}{8},\ -\tfrac{132651}{2},\ -\tfrac{1167051}{512},\ \tfrac{21952}{9},\ \tfrac{7301384}{3},\ \tfrac{97336}{81},\ \tfrac{140608}{3},\ -12288000. \quad (2.5)$$

Lemma 2.14. *Let (p, E) be one of the 26 pairs of Section 2.4 with $E \neq 288\mathrm{a}1$, let $K = K_E$, and let E'' be an elliptic curve over $\mathbb{Q}$ isogenous to E by an isogeny of degree prime to p, with $j(E'') \notin \{0, 1728\}$. Then $G_p(x, j(E''))$ is separable, $j^{-1}(j(E'')) \simeq \operatorname{Spec} K$, and there are exactly $\#\operatorname{Aut}(K)$ points of $X_0(p)(K)$ over $j(E'')$.*

Proof. The isogeny gives $E''[p] \simeq E[p]$, and the proof of Proposition 2.12(a) applies to E'' in place of E'. So $j^{-1}(j(E'')) \simeq \operatorname{Spec} K$. The K-points of $\operatorname{Spec} K$ are the $\mathbb{Q}$-embeddings $K \to K$, that is, the automorphisms of K. For $p \leq 19$, $G_p(x, j(E''))$ is separable by Lemma 2.10, applied to the point given by the identity embedding. For $p \geq 23$ and

$j(E'') = -12288000$ the polynomial $G_p(x, -12288000)$ is irreducible (Appendix B). For the other j-invariants with $p \geq 23$ the curve E'' has no complex multiplication, so the argument of Proposition 2.12(b) shows that $G_p(x, j(E''))$ is separable. □

So for the fields with $\mathrm{Aut}(K_E) = 1$ there is one point of $X_0(p)(K_E)$ over each such $j(E'')$. For the curves with complex multiplication the known j-invariants are 0, 1728 and -12288000 for 27a1, and 0 and 1728 for 288a1 and 288a2; which of them carry points over K_E is stated where these curves are treated (Section 8.5, Sections 9.6 and 9.7 and Section 10). For $p = 11$ the known points used in Section 6 are listed in Table 9.

Lemma 2.15. *Let $p \in \{11, 17, 19, 23, 29\}$ and let (a, b, c) be a primitive solution of $x^2 + y^3 = z^p$ with $abc \neq 0$.*

(a) *If $j_0 \in \mathbb{Z}$, then $(a, b, c) = (\pm 3, -2, 1)$ and $j_0 = -13824$. In particular j_0 is not the j-invariant of an elliptic curve with complex multiplication.*

(b) *If j_0 is one of the known j-invariants (2.5), then $j_0 = -13824$ and $(a, b, c) = (\pm 3, -2, 1)$.*

Proof. (a) If a prime q divided c, then $q \nmid b$ by primitivity, and $v_q(j_0) \leq v_q(1728) - p < 0$, since $v_q(1728) \leq 6$. So $c = \pm 1$ and $a^2 + b^3 = \pm 1$. The elliptic curves $y^2 = x^3 + 1$ and $y^2 = x^3 - 1$ have Mordell–Weil groups $\mathbb{Z}/6$ and $\mathbb{Z}/2$, with points $(-1, 0), (0, \pm 1), (2, \pm 3)$ and $(1, 0)$. As $ab \neq 0$, the solution is $(\pm 3, -2, 1)$, with $j_0 = 1728 \cdot (-8) = -13824$. The rational CM j-invariants are integers, and $-13824 = j(864\mathrm{b}1)$ is not one of them, since 864b1 has no complex multiplication.

(b) As $j_0 \notin \{0, 1728\}$, we may exclude these two values. Write $j_0/1728 = b^3/c^p$ with $\gcd(b, c) = 1$. Let q be a prime with $t = v_q(j_0/1728) \neq 0$. If $q \nmid c$ then $t = 3v_q(b)$, so $t \in 3\mathbb{Z}_{>0}$. If $q \mid c$ then $q \nmid b$ and $t = -p\, v_q(c)$, so $t \in p\mathbb{Z}_{<0}$. The values of $j/1728$ for the other known j-invariants are $-1/8$, -8, $8/9$, $7^3/2^9$, $-73^3/(2^{15}3^2)$, $-17^3/2^7$, $7^3/3^5$, $97^3/(2^3 3^4)$, $23^3/(2^3 3^7)$, $13^3/3^4$ and $-2^9\, 5^3/3^2$. In each case except -8 some prime $q \in \{2, 3\}$ has $t \in \{-2, -3, -4, -5, -7, -9\}$, which is neither a positive multiple of 3 nor a multiple of p. Let $j_0/1728 = -8$. Every odd prime of c would divide b. If $v_2(c) > 0$, then $v_2(b) = 0$ and $3v_2(b) = 3 + p\, v_2(c)$, which is impossible. So $c = \pm 1$ and $b = \mp 2$, and $a^2 = c^p - b^3$ is 9 for $c = 1$ and -9 for $c = -1$. So $(a, b, c) = (\pm 3, -2, 1)$. □

3. Descents inside K_E

Let K be one of the fields K_E of Section 2.4, and let $P \in X_0(p)(K)$ be the point attached to a solution (Proposition 2.12). We attach to P a class $\delta(P)$ in a finite group of S-units of K modulo ℓ-th powers, where ℓ is the prime of Table 5. The class comes from an isogeny onto J with kernel μ_ℓ, whose Kummer map is the evaluation of a function (Lemma 3.4). For $p = 17$ we use instead a 2-descent over $K(i)$, whose class group is controlled from that of K (Appendix A.4).

3.1. **General facts.** Let $\phi\colon B \to B'$ be an isogeny of abelian varieties over a number field K. Its Kummer map $\delta_\phi\colon B'(K)/\phi(B(K)) \to H^1(K, B[\phi])$ and the local Kummer maps $\delta_{\phi,v}$ at the places v of K are injective homomorphisms. The Selmer group $\mathrm{Sel}^\phi(B/K) \subseteq H^1(K, B[\phi])$ consists of the classes whose restriction to every place v lies in the image of $\delta_{\phi,v}$ ([59, Chapter X] for elliptic curves, with the same arguments for abelian varieties). For a finite set S of primes of K and a prime ℓ put

$$K(S, \ell) \coloneqq \{\alpha \in K^\times/K^{\times\ell} :\ v(\alpha) \equiv 0 \pmod{\ell} \text{ for every finite place } v \notin S\}.$$

Lemma 3.1 ([50, Lemma 3.8])**.** *Let $\phi\colon B \to B'$ be an isogeny of elliptic curves over K. Let v be a finite place of K, $|\cdot|_v$ the normalized absolute value of K_v, $\omega_B, \omega_{B'}$ Néron differentials, $\phi^*\omega_{B'} = \alpha\,\omega_B$, and $c_v(\cdot)$ the Tamagawa numbers at v. Then*

$$\#B'(K_v)/\phi(B(K_v)) = \#B(K_v)[\phi] \cdot |\alpha|_v^{-1} \cdot c_v(B')/c_v(B).$$

Lemma 3.2 ([18, Theorem 2.19], stated there over an arbitrary number field)**.** *Let $\phi\colon B \to B'$ be an isogeny of elliptic curves over K of prime degree ℓ, with dual $\hat{\phi}\colon B' \to B$. With $\mathbb{F}_\ell$-dimensions,*

$$\begin{aligned}\dim \mathrm{Sel}^{\phi}(B/K) - \dim \mathrm{Sel}^{\hat{\phi}}(B'/K)\\ = \dim B(K)[\phi] - \dim B'(K)[\hat{\phi}] + \sum_v \big(\dim B'(K_v)/\phi(B(K_v)) - \dim B(K_v)[\phi]\big),\end{aligned}$$

the sum running over all places v of K (almost all terms are 0).

The lemma applies because $\mathrm{Sel}^{\hat{\phi}}(B'/K)$ is the dual Selmer group of $\mathrm{Sel}^{\phi}(B/K)$ in the sense of [18, Theorem 2.19]: under the local Tate pairing $H^1(K_v, B[\phi]) \times H^1(K_v, B'[\hat{\phi}]) \to \mathbb{Q}/\mathbb{Z}$ induced by the Weil pairing, the images of the local Kummer maps of ϕ and $\hat{\phi}$ are orthogonal complements of each other [14, Proposition B.1].

Lemma 3.3. *Let $\phi\colon B \to B'$ be an isogeny of abelian varieties over K, and let v be a finite place of K at which B has good reduction. Then ϕ extends to an isogeny of abelian schemes over the ring of integers $\mathcal{O}_v$ of K_v, whose kernel $\mathcal{G}$ is a finite flat group scheme over $\mathcal{O}_v$.*

(a) *If $\mathcal{G} \simeq \mu_\ell$, then the image of $\delta_{\phi,v}$ in $H^1(K_v, \mu_\ell) = K_v^\times/K_v^{\times\ell}$ is contained in the group $\mathcal{O}_v^\times K_v^{\times\ell}/K_v^{\times\ell}$ of unit classes.*

(b) *If $\mathcal{G} \simeq \mathbb{Z}/\ell$, then the image of $\delta_{\phi,v}$ in $H^1(K_v, \mathbb{Z}/\ell)$ is contained in the group of unramified classes.*

In particular, if $B[\phi] \simeq \mu_\ell$ and (a) *applies at every finite place $v \notin S$, then $\mathrm{Sel}^{\phi}(B/K) \subseteq K(S, \ell)$.*

Proof. The Néron models $\mathcal{B}$, $\mathcal{B}'$ of B, B' over $\mathcal{O}_v$ are abelian schemes, and by the Néron mapping property ϕ extends to an isogeny $\mathcal{B} \to \mathcal{B}'$, faithfully flat with kernel $\mathcal{G}$. So $0 \to \mathcal{G} \to \mathcal{B} \to \mathcal{B}' \to 0$ is exact in the fppf topology. Since $\mathcal{B}'(\mathcal{O}_v) = B'(K_v)$, comparing the long exact sequences over $\mathcal{O}_v$ and over K_v shows that $\delta_{\phi,v}$ factors through $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{G}) \to H^1(K_v, B[\phi])$. If $\mathcal{G} = \mu_\ell$, the Kummer sequence and $\mathrm{Pic}(\mathcal{O}_v) = 0$ give $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mu_\ell) = \mathcal{O}_v^\times/\mathcal{O}_v^{\times\ell}$, which gives (a). If $\mathcal{G} = \mathbb{Z}/\ell$, which is étale, $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathbb{Z}/\ell) = H^1(\mathcal{O}_v, \mathbb{Z}/\ell)$, whose image in $H^1(K_v, \mathbb{Z}/\ell)$ is the group of unramified classes, which gives (b). The last statement follows from (a). □

The Kummer maps of the isogenies with kernel μ_ℓ below are computed as follows. Let X be a smooth projective geometrically connected curve over a field K of characteristic 0, with Jacobian J_X, and let $T \in J_X(K)$ have prime order ℓ. Suppose that T is the class of a divisor D_T of degree 0 supported on K-rational points, and let $f \in K(X)^\times$ with $\operatorname{div} f = \ell D_T$. At each point Q of the support of D_T fix a uniformizer $t_Q \in K(X)$ and put $f(Q) \coloneqq (f\,t_Q^{-\operatorname{ord}_Q f})(Q) \in K^\times$, and at every other point let $f(Q)$ be the value of f. For a divisor $D = \sum n_Q Q$ of degree 0 defined over K put $f(D) \coloneqq \prod_Q f(Q)^{n_Q} \in K^\times$. Let $\delta_{[\ell]}\colon J_X(K) \to H^1(K, J_X[\ell])$ be the Kummer map of multiplication by ℓ, and e_ℓ the Weil pairing on $J_X[\ell]$.

Lemma 3.4. *In this situation the following hold.*

(a) *The class of $f(D)$ in $K^\times/K^{\times\ell}$ depends only on the class of D in $J_X(K)$, and not on the choice of the uniformizers t_Q. So $D \mapsto f(D)$ defines a homomorphism $\delta_f\colon J_X(K) \to K^\times/K^{\times\ell}$.*

(b) *Up to a factor in $\mathbb{F}_\ell^\times$, which depends only on the normalization of e_ℓ, $\delta_f = \big(e_\ell(T,\cdot)\big)_* \circ \delta_{[\ell]}$, where $(e_\ell(T,\cdot))_*\colon H^1(K, J_X[\ell]) \to H^1(K,\mu_\ell) = K^\times/K^{\times\ell}$.*

(c) *Let $\psi\colon J_X \to J'_X$ be an isogeny with kernel $\langle T\rangle$, let $\phi\colon J'_X \to J_X$ be an isogeny, and let θ be an endomorphism of J_X over K with $\phi\circ\psi\circ\theta = \ell$. Suppose that $z \mapsto e_\ell(T,z)$ on $J_X[\ell]$ factors as $\iota\circ\psi\circ\theta$ with an isomorphism of Galois modules $\iota\colon \ker\phi \to \mu_\ell$. Then $\delta_f = \iota_*\circ\delta_\phi$ up to a factor in $\mathbb{F}_\ell^\times$. In particular the kernel of δ_f is $\phi(J'_X(K))$.*

Proof. (a) Another uniformizer ut_Q changes $f(Q)$ by $u(Q)^{-\operatorname{ord}_Q f}$, an ℓ-th power since $\operatorname{ord}_Q f \in \ell\mathbb{Z}$. Let $h \in K(X)^\times$. Weil reciprocity for the tame symbols [53, Chapter III, §1, no. 4, Propositions 6 and 7] gives $\prod_Q (-1)^{m_Q n_Q}(f_Q^{n_Q}/h_Q^{m_Q})(Q) = 1$, where $m_Q = \operatorname{ord}_Q f$, $n_Q = \operatorname{ord}_Q h$, and $f = t_Q^{m_Q} f_Q$, $h = t_Q^{n_Q} h_Q$ for a uniformizer t_Q at Q, the fixed one on the support of D_T. There $m_Q \in \ell\mathbb{Z}$, and elsewhere $m_Q = 0$. Hence $f(\operatorname{div} h) = \prod_Q (-1)^{m_Q n_Q} h_Q(Q)^{m_Q}$, the product over the support of D_T, an ℓ-th power in $K^\times$ (for $\ell = 2$ the sign is 1 as m_Q is even).

(b) Let $D \in J_X(K)$ be represented by a K-rational divisor D_P of degree 0 prime to the support of D_T. Choose $D' \in J_X(\bar K)$ with $\ell D' = D$, a divisor D_Q prime to the support of D_T representing D', and a function h with $\ell D_Q = D_P + \operatorname{div} h$. The Weil pairing is given by functions: $e_\ell(R,R') = g_R(D_{R'})/g_{R'}(D_R)$ when $\ell D_R = \operatorname{div} g_R$ and $\ell D_{R'} = \operatorname{div} g_{R'}$. Apply this to $R = T$, with D_T and $g_T = f$, and to $R' = \sigma D' - D'$ for $\sigma \in \operatorname{Gal}(\bar K/K)$, with $D_{R'} = \sigma D_Q - D_Q$ and $g_{R'} = \sigma h/h$. One finds $e_\ell(T, \sigma D' - D') = \sigma(\alpha)/\alpha$ with $\alpha = f(D_Q)/h(D_T)$, and $\alpha^\ell = f(D_P)\, f(\operatorname{div} h)/h(\operatorname{div} f) = f(D_P)$ by Weil reciprocity. So the class of $f(D_P)$ corresponds under Kummer theory to $\sigma \mapsto e_\ell(T, \delta_{[\ell]}(D)(\sigma))$, up to the normalization of e_ℓ.

(c) If $\ell D' = D$, then $\phi(\psi\theta(D')) = D$, so $\delta_\phi(D)$ is represented by $\sigma \mapsto \psi\theta(\sigma D' - D')$. Applying ι gives $e_\ell(T, \sigma D' - D')$, and (b) gives $\delta_f = \iota_*\circ\delta_\phi$. Since ι is an isomorphism and $K^\times/K^{\times\ell} = H^1(K,\mu_\ell)$, the maps δ_f and δ_ϕ have the same kernel, $\phi(J'_X(K))$. □

For an elliptic curve J over K with origin O and a point $T \in J(K)$ of prime order ℓ, take $D_T = (T) - (O)$, so that $\operatorname{div} f = \ell(T) - \ell(O)$. Let $\psi\colon J \to J' = J/\langle T\rangle$ be the quotient map, $\phi = \hat\psi$ its dual and $\theta = 1$, so that $\hat\psi\psi = \ell$. The functional $e_\ell(T,\cdot)$ on $J[\ell]$ vanishes exactly on $\langle T\rangle = \ker\psi$, since e_ℓ is alternating and non-degenerate. So it factors through an isomorphism $\iota\colon \psi(J[\ell]) = \ker\hat\psi \to \mu_\ell$, and Lemma 3.4(c) applies. If f and the uniformizer at O are defined over $\mathbb{Q}$, it gives $\delta_f(P) = c_0 f(P)$ for $P \neq O, T$, with the constant $c_0 = f(O)^{-1} \in \mathbb{Q}^\times$. This is the case of Lemma 3.6 and of Section 3.3. The same argument applies verbatim with the integer 4 in place of ℓ (Remark 3.12). In genus two the function f is the modular unit of Proposition 3.13.

The last general fact determines $K(S,\ell)$ from S-units. Let $\mathcal{O}_S^\times$ be the group of S-units of K, (r_1, r_2) the signature of K, and $\operatorname{Cl}_S(K)$ the quotient of the class group of K by the classes of the primes in S.

Lemma 3.5. *Suppose that ℓ does not divide $\#\operatorname{Cl}_S(K)$, for instance that $\ell \nmid h_K$. Then $K(S,\ell) = \mathcal{O}_S^\times K^{\times\ell}/K^{\times\ell} \simeq \mathcal{O}_S^\times/\mathcal{O}_S^{\times\ell}$, an $\mathbb{F}_\ell$-vector space of dimension*

$$n = r_1 + r_2 - 1 + \#S + \dim_{\mathbb{F}_\ell} \mu_\ell(K),$$

which is $r_1 + r_2 - 1 + \#S$ *when* $\mu_\ell \not\subset K$. *Moreover, let* $u_1, \dots, u_n \in \mathcal{O}_S^\times$, *and let* $\chi_1, \dots, \chi_m \colon \mathcal{O}_S^\times \to \mathbb{F}_\ell$ *be homomorphisms such that the matrix* $(\chi_i(u_k))$ *has rank* n. *Then the classes of* $u_1, \dots, u_n$ *form a basis of* $K(S, \ell)$.

Proof. If $\alpha \in K^\times$ has $v(\alpha) \equiv 0 \pmod{\ell}$ for all finite $v \notin S$, then $(\alpha) = \mathfrak{a}^\ell \mathfrak{s}$ with $\mathfrak{s}$ supported on S. Sending the class of α to the class of $\mathfrak{a}$ gives an exact sequence

$$0 \longrightarrow \mathcal{O}_S^\times / \mathcal{O}_S^{\times \ell} \longrightarrow K(S, \ell) \longrightarrow \mathrm{Cl}_S(K)[\ell] \longrightarrow 0.$$

The first map is injective because an S-unit that is an ℓ-th power in K is the ℓ-th power of an S-unit, and the right-hand term is 0 by hypothesis. By Dirichlet's S-unit theorem $\mathcal{O}_S^\times \simeq \mu(K) \times \mathbb{Z}^{r_1 + r_2 - 1 + \#S}$, and $\mu(K)/\mu(K)^\ell \simeq \mu_\ell(K)$ because $\mu(K)$ is cyclic, which gives the dimension. Each χ_i vanishes on $\mathcal{O}_S^{\times \ell}$, so the rank condition says that the classes of $u_1, \dots, u_n$ are linearly independent in $\mathcal{O}_S^\times / \mathcal{O}_S^{\times \ell}$, a space of dimension n. □

Two kinds of χ_i are used. For a prime $\mathfrak{q} \notin S$ of K with $\mathrm{N}\,\mathfrak{q} \equiv 1 \pmod{\ell}$, the ℓ-th power residue character $\chi_\mathfrak{q}$ is defined on $\mathfrak{q}$-units by $\alpha^{(\mathrm{N}\,\mathfrak{q} - 1)/\ell} \equiv \zeta_\mathfrak{q}^{\chi_\mathfrak{q}(\alpha)} \pmod{\mathfrak{q}}$, for a fixed primitive ℓ-th root of unity $\zeta_\mathfrak{q}$ in $\mathcal{O}_K/\mathfrak{q}$. For ℓ odd and a place $v \mid \ell$ of K with $v \notin S$ and K_v unramified over $\mathbb{Q}_\ell$, let k_v be the residue field and $q_v = \#k_v$. The map

$$\mathcal{O}_v^\times \longrightarrow k_v, \qquad u \longmapsto \frac{u^{q_v - 1} - 1}{\ell} \bmod \ell, \tag{3.1}$$

is a homomorphism with kernel $\mathcal{O}_v^{\times \ell}$, so it identifies $\mathcal{O}_v^\times / \mathcal{O}_v^{\times \ell}$ with k_v, and its coordinates on an $\mathbb{F}_\ell$-basis of k_v are homomorphisms $\mathcal{O}_S^\times \to \mathbb{F}_\ell$. Residue characters prove the bases for $p = 11$, 19 and 17 (Propositions A.4, A.10 and A.8), and the map (3.1) at the places above ℓ proves them for $p = 23$ and 29 (Remark 3.15).

3.2. **The exponent 11: descent by an isogeny with kernel $\boldsymbol{\mu_5}$.** For $p = 11$ the descent embeds $J(K)/5J(K)$ into $K(S, 5)$, with S the set of primes above 11 (Proposition 3.7). The curve J of Table 5 has two rational 5-isogenies, so $J[5] = C \oplus M$ with $C = \langle T \rangle \simeq \mathbb{Z}/5$ and $M \simeq \mu_5$ as Galois modules. Let $\psi \colon J \to J' = J/C$ (the curve 11a2) be the quotient map. As after Lemma 3.4, the Weil pairing identifies $\ker \hat{\psi} = \psi(J[5])$ with μ_5, and the Kummer map of $\hat{\psi}$ is a homomorphism

$$\delta \colon J(K)/\hat{\psi}(J'(K)) \longrightarrow H^1(K, \mu_5) = K^\times / K^{\times 5}.$$

Let $f_T = xy - 4x^2 + 30x - 4y - 55$. It has divisor $5(T) - 5(O)$, as its norm to $\mathbb{Q}(x)$ is $-(x - 5)^5$ and $f_T(-T) = -11 \neq 0$.

Lemma 3.6. *For* $P \in J(K) \setminus \{O, T\}$, $\delta(P)$ *is the class of* $f_T(P)$, *and* $\delta(T)$ *is the class of* $1/11$.

Proof. By Lemma 3.4 and the paragraph after it, with the uniformizer $t = -x/y$ at O, $\delta(P) = c_0 f_T(P)$ for $P \neq O, T$, with a constant $c_0 \in \mathbb{Q}^\times$. The values $f_T(2T) = -11^3$, $f_T(3T) = 11^2$, $f_T(4T) = -11$ and the relation $\delta(3T) = 2\,\delta(4T)$ (written additively) give $c_0 \in \mathbb{Q}^{\times 5}$, and $\delta(T) = -\delta(4T)$ is the class of $1/11$. □

Proposition 3.7. *Let* K *be one of the five fields* K_E *of degree* 12, *and* S *the set of primes of* K *above* 11.

(a) *The Selmer group* $\mathrm{Sel}^{\hat{\psi}}(J'/K)$ *equals* $K(S, 5)$.
(b) $K(S, 5) = \mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 5}$ *has dimension* $6 + \#S$, *which is* 9 *for* 54a1 *and* 8 *for the other four curves, and its restriction to* $\prod_{v \mid 5} K_v^\times / K_v^{\times 5}$ *is injective.*

(c) $\mathrm{Sel}^{\psi}(J/K)=0$. *Hence* $\hat\psi(J'(K))=5J(K)$, *and* δ *induces an injective homomorphism* $J(K)/5J(K)\to K(S,5)$.

Proof. (a) We compute the local images with Lemma 3.1 for $\phi=\hat\psi$. Let $v\mid 5$. The places above 5 are unramified (Table 6), and J, J' have good ordinary reduction at 5 ($a_5=1$). As T reduces to a nonzero point, C is étale, ψ is an isomorphism on formal groups, $\hat\psi^*\omega_J=5u\,\omega_{J'}$ with u a unit, and $J'(K_v)[\hat\psi]=\mu_5(K_v)=1$. So the image of δ_v has order 5^{n_v}. Since $\hat\psi$ extends over $\mathcal{O}_v$ with kernel μ_5, the image lies in the group $\mathcal{O}_v^\times/\mathcal{O}_v^{\times 5}$ of unit classes by Lemma 3.3(a), which also has order 5^{n_v}, so it is that group. Let $v\mid 11$. Every place above 11 has residue field $\mathbb{F}_{11}$, which contains μ_5. The curves J and J' are split multiplicative at 11, of types I_5 and I_1 over $\mathbb{Q}_{11}$, hence I_{5e_v} and I_{e_v} over K_v. So $c_v(J)/c_v(J')=5$, α is a unit and $J'(K_v)[\hat\psi]=\mu_5$, and the image has order $25=\#K_v^\times/K_v^{\times 5}$: there is no condition at v. At the other finite places J has good reduction and $v\nmid 5$, so the image consists of the unramified classes, and at the infinite places $H^1(K_v,\mu_5)=0$. Hence the Selmer group consists of the classes unramified outside S that are unit classes above 5. A class unramified outside S has valuation divisible by 5 above 5, so $\mathrm{Sel}^{\hat\psi}(J'/K)=K(S,5)$.

(b) The fields K have class number 1 or 2 (Proposition A.3), so 5 does not divide the class number, and $\mu_5\not\subset K$. By Lemma 3.5, $K(S,5)=\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 5}$, which has dimension $r_1+r_2-1+\#S=6+\#S$ (signature $(2,5)$). Generators are given by Proposition A.4. The injectivity is a computation: the $6+\#S$ generators have images of full rank in $\prod_{v\mid 5}\mathcal{O}_v^\times/\mathcal{O}_v^{\times 5}\simeq\mathbb{F}_5^{12}$.

(c) Apply Lemma 3.2 to $\phi=\hat\psi\colon J'\to J$. The global term is $\dim J'(K)[\hat\psi]-\dim J(K)[\psi]=0-1$. At the two real places the terms vanish, as $\hat\psi$ has odd degree. At each of the five complex places the term is $0-1$. At a place $v\mid 5$ it is n_v-0, and these add up to 12. At a place above 11 it is $2-1$, and all other terms vanish. So $\dim\mathrm{Sel}^{\hat\psi}(J'/K)-\dim\mathrm{Sel}^{\psi}(J/K)=6+\#S$, and (a), (b) give $\mathrm{Sel}^{\psi}(J/K)=0$. Then $J'(K)/\psi(J(K))$, which injects into $\mathrm{Sel}^{\psi}(J/K)$, is trivial, so $\hat\psi(J'(K))=\hat\psi\psi(J(K))=5J(K)$. □

3.3. **The exponent 19: descent by an isogeny with kernel $\boldsymbol{\mu_3}$.** For $p=19$ the descent embeds $J(K)/3J(K)$ into a subgroup of $K(S,3)$, with S the set of primes above 3 and 19, and describes that subgroup at the places above 3 (Proposition 3.8). The 3-division polynomial is $(x-5)(3x+4)(x^2+5x+7)$, and $J[3]=\langle T\rangle\oplus C$ with $C\simeq\mu_3$, the points with $x=-4/3$. Let $\phi\colon J\to J'=J/\langle T\rangle$ (the curve 19a2) be the quotient map and $\hat\phi\colon J'\to J$ its dual, whose kernel $\phi(J[3])$ is μ_3 by the Weil pairing. The tangent line to J at T is $y=4x-11$, and $x^3+x^2-9x-15-(y^2+y)$ restricted to it is $(x-5)^3$, so $f_T=y-4x+11$ has divisor $3(T)-3(O)$. As for $p=11$, the Kummer map of $\hat\phi$ is $P\mapsto c_0 f_T(P)$ with $c_0\in\mathbb{Q}^\times$ (Lemma 3.4), and here c_0 is a cube. Near O, $f_T=-t^{-3}(1+O(t))$ in the parameter $t=-x/y$, so $f_T(P)$ is a cube in every completion for P close to O, where the Kummer map is trivial. So c_0 is a cube in every completion of $\mathbb{Q}$, hence in $\mathbb{Q}$. We obtain

$$\delta\colon J(K)/\hat\phi(J'(K))\longrightarrow K^\times/K^{\times 3},\qquad P\longmapsto\text{class of } f_T(P)\quad(P\neq O,T),$$

with $\delta(-T)$ the class of $f_T(5,-10)=-19$, so $\delta(T)$ is the class of $-1/19$. We write $\mathrm{Sel}(K)=\mathrm{Sel}^{\hat\phi}(J'/K)\subseteq K^\times/K^{\times 3}$.

Proposition 3.8. *Let* $K=K_E$ *for one of the six curves* E *at* $p=19$ *of Table 6.*

(a) $\mathrm{Sel}(K)$ *is the subgroup of* $K(S,3)$ *of classes whose image at each* $v\mid 3$ *lies in the image of* δ_v, *a subgroup of dimension* $n_v+\dim\mu_3(K_v)$ *of* $K_v^\times/K_v^{\times 3}$.

(b) $\dim \mathrm{Sel}(K) = 10 + \#\{v \mid 19\}$, *which is* 12 *for the five curves without complex multiplication and* 11 *for* 288a1. *Hence* $\mathrm{Sel}^{\phi}(J/K) = 0$, $\hat{\phi}(J'(K)) = 3J(K)$, *and* δ *induces an injective homomorphism* $J(K)/3J(K) \to \mathrm{Sel}(K)$.

(c) *The restriction of* $\mathrm{Sel}(K)$ *to* $\prod_{v|3} K_v^\times/K_v^{\times 3}$ *has rank* $\dim \mathrm{Sel}(K) - 1$. *Its kernel is spanned by* $\delta(T)$, *the class of* $-1/19$.

Proof. (a) We argue as in the proof of Proposition 3.7(a). At $v \mid 3$, J has good ordinary reduction ($a_3 = -2$) and T reduces to $(2,0) \neq O$, so $\langle T \rangle$ is étale and $\hat{\phi}^*\omega_J = 3u\,\omega_{J'}$ with u a unit. By Lemma 3.1 the image has dimension $n_v + \dim \mu_3(K_v)$, one less than $\dim K_v^\times/K_v^{\times 3}$. The isogeny $\hat{\phi}$ extends over $\mathcal{O}_v$ with kernel μ_3 (the image under ϕ of the connected part C of $J[3]$, which is the connected part of $J'[3]$, as the reduction is ordinary). So by Lemma 3.3(a) the image of δ_v is the group $\mathcal{O}_v^\times/\mathcal{O}_v^{\times 3}$ of unit classes, which has the same dimension. At $v \mid 19$, $\mu_3 \subset \mathbb{Q}_{19}$, and J, J' are split multiplicative of types I_3 and I_1 over $\mathbb{Q}_{19}$, so $c_v(J)/c_v(J') = 3$ and the image is everything. At the other places the image is unramified or $H^1(K_v, \mu_3) = 0$, so $\mathrm{Sel}(K) \subseteq K(S,3)$ is cut out by the conditions at the places above 3.

(b) By (a), a class of $K(S,3)$ lies in $\mathrm{Sel}(K)$ if and only if its valuation is divisible by 3 at every $v \mid 3$. So $\mathrm{Sel}(K) = K(S_{19}, 3)$, where S_{19} is the set of primes above 19, and this equals $\mathcal{O}_{K,S_{19}}^\times/\mathcal{O}_{K,S_{19}}^{\times 3}$ because $3 \nmid h_K$ (Proposition A.9 and Lemma 3.5). Since $\mu_3 \not\subset K$, it has dimension $r_1 + r_2 - 1 + \#\{v \mid 19\} = 10 + \#\{v \mid 19\}$ by Dirichlet's theorem, which is 12 and 11 as stated, since the five fields of the curves without complex multiplication have two places above 19 and $K_{288\mathrm{a}1}$ has one (Table 6). Lemma 3.2 applied to $\phi\colon J \to J'$ gives $\dim \mathrm{Sel}^{\phi}(J/K) - \dim \mathrm{Sel}(K) = 1 - 2 - 9 - \#\{v \mid 19\}$. The global term is $\dim J(K)[\phi] - \dim J'(K)[\hat{\phi}] = 1 - 0$. Each of the two real and nine complex places contributes $0 - 1$, since $J(K_v)[\phi] = \langle T \rangle$ and ϕ is surjective on points over $\mathbb{R}$ and $\mathbb{C}$. The places above 3 contribute 0, since ϕ is étale there and J has good reduction. Each place above 19 contributes $0 - 1$, since $c_v(J')/c_v(J) = 1/3$. So $\mathrm{Sel}^{\phi}(J/K) = 0$, and as for $p = 11$ we obtain $\hat{\phi}(J'(K)) = 3J(K)$ and the injectivity.

(c) The rank is a computation with the basis of $K(S,3)$ of Proposition A.10. The class of $-1/19$ is nonzero, since 19 has valuation 1 at the place of degree one above 19 of the five fields without complex multiplication, and valuation 20 at the place above 19 of $K_{288\mathrm{a}1}$, neither divisible by 3. It is a cube at every place above 3, since $19 \equiv 1 \pmod 9$. □

3.4. **The exponent 17: a 2-descent through $K(i)$.** For $p = 17$ the descent is by multiplication by 2, with values in the square classes of $L = K(i)$ (Proposition 3.11), and Remark 3.12 explains this choice. Let K be one of the four fields K_E. The field K does not contain i, since it has no quadratic subfield. Put $L = K(i)$, of degree 36. Completing the square in the model of Table 5 gives

$$(2y + x + 1)^2 = 4x^3 - 3x^2 - 2x - 55 = (4x - 11)(x^2 + 2x + 5),$$

so $J[2]$ consists of O, the rational point $2T = (11/4, -15/8)$ and the two points with $x = \theta, \bar{\theta}$, where $\theta = -1 + 2i$. For a field $F \supseteq K$, such as K or a completion K_v, put $F_L = F \otimes_K L$, which is a quadratic field extension of F or $F \times F$. For a point $P \in J(F)$ let $\delta(P)$ be the class of $x(P) - \theta$ in $F_L^\times/F_L^{\times 2}$, and $\delta(O) = 1$. At a point of order 2 where a component of $x(P) - \theta$ vanishes, that component is replaced, as usual, by the product of the differences of $x(P)$ with the other two roots of the 2-division polynomial, as in [59, Proposition X.1.4].

Lemma 3.9. *The map* δ *is an injective homomorphism* $J(F)/2J(F) \to F_L^\times/F_L^{\times 2}$, *and* $\delta(2T) = 1$.

Proof. The Kummer map of multiplication by 2 sends $P \neq O, 2T$ to the class of $(x(P) - 11/4,\ x(P) - \theta)$ in $F^\times/F^{\times 2} \times F_L^\times/F_L^{\times 2}$ and is an injective homomorphism on $J(F)/2J(F)$. For $i \in F$ this is [59, Proposition X.1.4]. In general, with $A = F \times F_L$, $J[2]$ is the kernel of the norm $\mathrm{Res}_{A/F}\,\mu_2 \to \mu_2$, and $\mu_2(A) \to \mu_2(F)$ is onto. So $H^1(F, J[2]) \to A^\times/A^{\times 2}$ is injective, and its composite with the Kummer map is $P \mapsto (x(P) - 11/4,\ x(P) - \theta)$. Since $(x - 11/4)\ \mathrm{N}_{F_L/F}(x - \theta) = (2y + x + 1)^2/4$ is a square, the first component is determined by the second, so δ alone is injective. Finally $11/4 - \theta = (15 - 8i)/4 = \big((4 - i)/2\big)^2$, so the component of $2T$ in $F_L^\times/F_L^{\times 2}$ is trivial. □

We write δ_v for the map over the completion K_v, with values in $\prod_{w|v} L_w^\times/L_w^{\times 2}$. We define the 2-Selmer group $\mathrm{Sel}^2(J/K)$ as the set of classes $\sigma \in L^\times/L^{\times 2}$ whose image in $\prod_{w|v} L_w^\times/L_w^{\times 2}$ lies in $\delta_v(J(K_v))$ for every place v of K. It contains $\delta(J(K))$ (Lemma 3.9).

Lemma 3.10. (i) *If $v \nmid 2 \cdot 17$ is finite, the image of δ_v consists of the classes of even valuation at every place of L above v.*

(ii) *The image of δ_v has $\mathbb{F}_2$-dimension $\dim J(K_v)[2] + [K_v : \mathbb{Q}_2]$ if $v \mid 2$, and $\dim J(K_v)[2]$ if $v \mid 17$.*

(iii) *At a real place the condition is empty: $L_w = \mathbb{C}$, and $J(\mathbb{R})$ is connected since $4x^3 - 3x^2 - 2x - 55$ has one real root.*

Proof. For finite v, $\#J(K_v)/2J(K_v) = \#J(K_v)[2] \cdot |2|_v^{-1}$ (Lemma 3.1 for $\phi = [2]$), which gives (ii). If $v \nmid 2 \cdot 17$, then J has good reduction and L/K is unramified at v, so the image is the unramified subgroup, which gives (i). □

Let S be the set of primes of L above 2 and 17, and $L(S, 2)$ the group of classes in $L^\times/L^{\times 2}$ with even valuation at every prime of L outside S. So $\mathrm{Sel}^2(J/K)$ is the subgroup of $L(S, 2)$ cut out by the local conditions at the places above 2 and 17.

Proposition 3.11. (a) *For $K = K_E$ with $E \in \{864\mathrm{a}1, 864\mathrm{b}1, 864\mathrm{c}1\}$: $\dim L(S, 2) = 28$, $\dim \mathrm{Sel}^2(J/K) = 11$, and the restriction map from $\mathrm{Sel}^2(J/K)$ to $\prod_{v|2} \prod_{w|v} L_w^\times/L_w^{\times 2}$ is injective.*

(b) *For $K = K_{54\mathrm{a}1}$: $\dim L(S, 2) = 23$, $\dim \mathrm{Sel}^2(J/K) = 12$, and the image of $\mathrm{Sel}^2(J/K)$ at the two places above 2 has dimension 11.*

In both cases the classes $\delta(T)$ and $\delta(P_E)$ lie in $\mathrm{Sel}^2(J/K)$, and they are nonzero and distinct. Here $P_E \in J(K)$ is the unique point over $j(E)$ (Lemma 2.14 with $E'' = E$, as $\mathrm{Aut}(K) = 1$).

Proof. By Proposition A.8 in Appendix A, $L(S, 2)$ is spanned by explicit S-units of L (with auxiliary primes for 54a1), which are proved to be a basis without GRH. The local images at the places above 2 and 17 are spanned by the classes of explicit points of $J(K_v)$: the point $2T$, points of the formal group, lifts of points of the reduction, and further points found by search. In every case the span reaches the dimension of Lemma 3.10(ii), so it is the image. The Selmer group is then the kernel of the $\mathbb{F}_2$-linear map from $L(S, 2)$ to the product over $v \mid 2 \cdot 17$ of the quotients of $\prod_{w|v} L_w^\times/L_w^{\times 2}$ by $\delta_v(J(K_v))$ (Appendix B). □

Remark 3.12. The duals of the quotient maps $J \to J/\langle T\rangle$ and $J \to J/\langle 2T\rangle$ have kernels $J[4]/\langle T\rangle \simeq \mu_4$ and $J[2]/\langle 2T\rangle \simeq \mu_2$ by the Weil pairing, and give descents inside K as in Sections 3.2 and 3.3. Let $f = x^2 + 14x - 43 - 8y$, which has divisor $4(T) - 4(O)$. As in the proof of Lemma 3.6, the Kummer maps of these two descents send $P \neq O, T$ to the class of $c_0 f(P)$ in $K^\times/K^{\times 4}$ for a constant c_0, and $P \neq O, 2T$ to the class of $x(P) - 11/4$ in

$K^\times/K^{\times 2}$. Both give T the class of $1/17$, as $f(3T)/f(2T) = 2^8/17$ modulo fourth powers and $x(T) - 11/4 = 17/4$ modulo squares. Since $17 \equiv 1 \pmod{16}$ is a fourth power in $\mathbb{Q}_2$, these descents give P and $P+T$ the same class at every place above 2. The 2-descent separates them: $\delta(T)$ is the class of $x(T) - \theta = 8 - 2i$, which is 5 times a square in $\mathbb{Q}_2(i)$. It is nontrivial at the place with $(e, f) = (2, 1)$ for 864a1 and 864b1, at the place with $(e, f) = (4, 1)$ for 864c1, and at both places for 54a1. For $p = 19$ the class of T is likewise trivial at the places above 3 (Proposition 3.8(c)), but there a 3-descent would need the field $K(\sqrt{-3})$, of degree 40.

3.5. **Genus two: the Eisenstein descent.** For $p = 23$ and 29 the descent runs on $J = J_0(p)$ along the Eisenstein prime λ of its Hecke algebra, above $\ell = 11$ and $\ell = 7$ respectively, and embeds $J(K)/\lambda J(K)$ into $K(S, \ell)$, with S the set of primes above p, when $\ell \nmid h_K$ (Proposition 3.14). Throughout, $r = r_p$ and $f = (\eta(\tau)/\eta(p\tau))^r$ is the modular unit of Lemma 2.5(c), with $\operatorname{div} f = \ell(0) - \ell(\infty)$.

The Eisenstein kernel. The Hecke operator T_2 acts on J, and $\mathcal{O} \coloneqq \mathbb{Z}[T_2] \subset \operatorname{End}_{\mathbb{Q}}(J)$ is the ring of integers of $\mathbb{Q}(\sqrt{5})$ for $p = 23$ and of $\mathbb{Q}(\sqrt{2})$ for $p = 29$ (Section 2.3). It contains all Hecke operators. Let $\lambda \subset \mathcal{O}$ be the *Eisenstein prime* above ℓ, the kernel of the ring homomorphism $\mathcal{O} \to \mathbb{F}_\ell$ that sends T_q to $1 + q$ for every prime $q \neq p$. Explicitly,

$$\begin{aligned} p = 23: &\quad \lambda = (T_2 - 3), \quad \mu \coloneqq -(T_2 + 4), \quad \lambda\mu = 11; \\ p = 29: &\quad \lambda = (T_2 + 4), \quad \mu \coloneqq 2 - T_2, \quad \lambda\mu = 7, \end{aligned}$$

using $T_2^2 + T_2 = 1$, respectively $T_2^2 + 2T_2 = 1$. We write λ also for the generator given here. The ideals λ and $\mu\mathcal{O}$ are distinct primes of norm ℓ, so $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda \times \mathcal{O}_\mu$ with $\mathcal{O}_\lambda = \mathcal{O}_\mu = \mathbb{Z}_\ell$. The element μ maps to a unit of $\mathcal{O}_\lambda$ whose residue is

$$\varepsilon \coloneqq \mu \bmod \lambda = 4 \in \mathbb{F}_{11}^\times \quad (p = 23), \qquad \varepsilon = -1 \in \mathbb{F}_7^\times \quad (p = 29). \tag{3.2}$$

We use the following results of Mazur [39], for the prime level p and the prime ℓ dividing the numerator of $(p-1)/12$.

(M1) The point T has order ℓ and is killed by λ [39, Chapter II, Proposition (11.1)]. We put $C \coloneqq \langle T \rangle$.

(M2) The Shimura subgroup Sh, the kernel of the map $J \to J_2(p)$ induced by the maximal étale subcovering $X_2(p) \to X_0(p)$ of $X_1(p) \to X_0(p)$, is cyclic of order ℓ and of multiplicative type, hence isomorphic to μ_ℓ as a Galois module, and it is killed by λ [39, Chapter II, Corollary (2.3), and §11: (11.5), the Definition following it, Propositions (11.6) and (11.7)].

(M3) $J[\lambda] = C \oplus \mathrm{Sh}$ [39, Chapter II, Corollary (16.3)].

(M4) J has split toric reduction at p, and the component group of its Néron model at p is cyclic of order ℓ, generated by the image of T [39, Chapter II, (11.3) and the proof of Proposition (11.1), with Appendix A.1].

The toric reduction in (M4) is split as $a_p = +1$. Over $\mathbb{Z}[1/p]$ the schematic closures of C and Sh in the Néron model are the constant group $\mathbb{Z}/\ell$ and μ_ℓ. Over $\mathbb{Z}[1/(\ell p)]$ this follows from (M1), (M2), and at ℓ from Raynaud's theorem [48, Théorème 3.3.3], since the absolute ramification index 1 is less than $\ell - 1$.

The λ-pairing. The Tate module $T_\ell J$ is free of rank two over $\mathcal{O} \otimes \mathbb{Z}_\ell$, so $J[\ell] \simeq (\mathcal{O}/\ell)^2$, $J[\mu] = \lambda J[\ell]$ and $\mu J[\ell] = J[\lambda]$. The Hecke operators are self-adjoint for the Weil pairing e_ℓ on $J[\ell]$, since the Rosati involution of the canonical polarization sends T_n to $w_p T_n w_p = T_n$, as $w_p = -1$ on J. For $u, u' \in J[\lambda]$ put $\langle u, u' \rangle_\lambda \coloneqq e_\ell(u, z)$, where $z \in J[\ell]$ and $\mu z = u'$.

This is well defined because $e_\ell(u, \lambda J[\ell]) = e_\ell(\lambda u, J[\ell]) = 1$. It is non-degenerate because $\mu\colon J[\ell] \to J[\lambda]$ is onto and e_ℓ is perfect. It is alternating because $\langle u, u\rangle_\lambda = e_\ell(\mu z, z) = e_\ell(z, \mu z) = e_\ell(\mu z, z)^{-1}$ with ℓ odd, and it is Galois-equivariant. So $J[\lambda]$ is a symplectic plane in which C is a Lagrangian line, and

$$\iota\colon J[\lambda]/C \longrightarrow \mu_\ell, \qquad u \longmapsto \langle T, u\rangle_\lambda, \tag{3.3}$$

is an isomorphism of Galois modules.

The isogenies. Let $\psi\colon J \to J' := J/C$ be the quotient map and $\phi\colon J' \to J$ the isogeny with $\phi \circ \psi = \lambda$. Then $\ker\phi = \psi(J[\lambda]) \simeq J[\lambda]/C \simeq \mu_\ell$ by (3.3), and over $\mathbb{Z}[1/p]$ the finite flat group scheme $\ker\phi$ is μ_ℓ (at ℓ again by Raynaud's theorem). Similarly let $\psi'\colon J \to J/\mathrm{Sh}$ and $\phi'\colon J/\mathrm{Sh} \to J$ with $\phi' \circ \psi' = \lambda$. Then $\ker\phi' = \psi'(C) \simeq \mathbb{Z}/\ell$, constant over $\mathbb{Z}[1/p]$.

The Kummer map. For a field K of characteristic 0 and a divisor D of degree 0 on $X_0(p)$ defined over K, let $f(D)$ be as in Section 3.1, with $D_T = (0) - (\infty)$ and the uniformizer $t = 1/x$ at both cusps, so that $f(\infty) = 1$ and $f(0) = p^{r/2}$ (Lemma 2.5(c)). Let $\delta_\phi\colon J(K) \to H^1(K, \ker\phi)$ be the Kummer map of ϕ.

Proposition 3.13. *$D \mapsto f(D) \bmod K^{\times\ell}$ is well defined on divisor classes and defines a homomorphism $\delta\colon J(K) \to K^\times/K^{\times\ell}$. Up to a factor in $\mathbb{F}_\ell^\times$, $\delta = \iota_* \circ \delta_\phi$, where $\iota_*\colon H^1(K, \ker\phi) \to H^1(K, \mu_\ell) = K^\times/K^{\times\ell}$ is induced by (3.3). In particular δ vanishes exactly on $\phi(J'(K))$, $\delta([Q - \infty]) = f(Q)$ for $Q \neq 0, \infty$, and $\delta(T) = p^{r/2}$.*

Proof. The function $t = 1/x$ is a uniformizer at both cusps, since x has simple poles there, so Lemma 3.4(a) gives the first statement. The hypotheses of Lemma 3.4(c) hold with $\theta = \mu$, since $\phi\psi\mu = \lambda\mu = \ell$, $\psi\mu(J[\ell]) = \psi(J[\lambda]) = \ker\phi$, and for $z \in J[\ell]$ the definition of the λ-pairing gives $\iota(\psi\mu z) = \langle T, \mu z\rangle_\lambda = e_\ell(T, z)$. So Lemma 3.4(c) gives $\delta = \iota_* \circ \delta_\phi$ and the kernel. The last two formulas follow from $f(\infty) = 1$ and $f(0) = p^{r/2}$. □

The descent. For a number field K let S be the set of places of K above p, and $K(S, \ell)$ as in Section 3.1.

Proposition 3.14. *Let K be a number field unramified at ℓ whose class number h_K is prime to ℓ.*

(a) *If $Q \in X_0(p)(K)$ and $j(Q)$ is integral at a place $v \mid \ell$, then Q does not reduce to a cusp at v, $x(Q)$ is integral at v, and $f(Q)$ is a unit at v.*

(b) *$\delta(J(K)) \subseteq K(S, \ell)$, and δ induces an injection $J(K)/\lambda J(K) \hookrightarrow K(S, \ell)$.*

(c) *$K(S, \ell) = \mathcal{O}_S^\times K^{\times\ell}/K^{\times\ell} \simeq \mathcal{O}_S^\times/\mathcal{O}_S^{\times\ell}$, an $\mathbb{F}_\ell$-vector space of dimension $r_1 + r_2 - 1 + \#S$, where $\mathcal{O}_S^\times$ is the group of S-units and (r_1, r_2) the signature of K.*

Proof. (a) On the smooth model of $X_0(p)$ over $\mathbb{Z}_\ell$ the reduction of $j = \mathcal{A}_p + \mathcal{B}_p\, y$ has poles only at the reductions of the two cusps (the points at infinity), of total order $p+1$, its degree. So if $j(Q)$ is v-integral, Q does not reduce to a point at infinity, and $x(Q)$ is integral. Then $f(Q) = f_0 + f_1 y$ and $f(w_p Q) = f_0 - f_1 y$, evaluated at Q, are integral with product $p^{r/2}$, a unit.

(b) *Local conditions for ψ*, whose kernel C is the constant group $\mathbb{Z}/\ell$ over $\mathbb{Z}[1/p]$. At the archimedean places $H^1(K_v, \mathbb{Z}/\ell) = 0$, as ℓ is odd. At a finite place $v \nmid p$ the image of $J'(K_v)$ in $H^1(K_v, C)$ consists of unramified classes by Lemma 3.3(b). At $v \mid p$ the image is trivial. By (M4), J has split toric reduction over $\mathbb{Q}_p$, so by rigid analytic uniformization (Mumford and Raynaud; see [6] and [29, Chapter 6]) $J = \mathbb{T}/\Lambda$ for a split torus $\mathbb{T}$ over $\mathbb{Q}_p$ and a lattice $\Lambda \subset \mathbb{T}(\mathbb{Q}_p)$ of rank two. It is compatible with base change, so it stays

valid over K_v, which may be ramified over $\mathbb{Q}_p$. As $\Lambda \simeq \mathbb{Z}^2$ with trivial Galois action, $H^1(K_v, \Lambda) = \mathrm{Hom}(\mathrm{Gal}(\bar{K}_v/K_v), \mathbb{Z}^2) = 0$, and so $J(K_v) = \mathbb{T}(K_v)/\Lambda$. Let $\tilde{c} \in \mathbb{T}(\mathbb{Q}_p)$ lift T. Then $\Lambda'' = \Lambda + \mathbb{Z}\tilde{c}$ is again a lattice, containing Λ with index ℓ, since $\ell T = 0$ and $T \neq 0$, and $J' = \mathbb{T}/\Lambda''$. Again $H^1(K_v, \Lambda'') = 0$, so $J'(K_v) = \mathbb{T}(K_v)/\Lambda''$, and $\psi\colon J(K_v) \to J'(K_v)$ is surjective. Hence every class in $\mathrm{Sel}^{\psi}(J/K) \subseteq \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), \mathbb{Z}/\ell)$ is unramified everywhere and trivial at the places above p, so it factors through the class group, and $\mathrm{Sel}^{\psi}(J/K) = 0$ as $\ell \nmid h_K$. Therefore $J'(K) = \psi J(K)$, $\phi(J'(K)) = \lambda J(K)$, and by Proposition 3.13 δ is injective on $J(K)/\lambda J(K)$.

Local conditions for ϕ, whose kernel is μ_ℓ over $\mathbb{Z}[1/p]$. By Lemma 3.3(a), at every finite place $v \nmid p$, including the places above ℓ, the local image consists of classes with $v(\alpha) \equiv 0 \pmod{\ell}$. So $\delta(J(K)) \subseteq K(S, \ell)$.

(c) This is Lemma 3.5, since $\ell \nmid h_K$ and $\mu_\ell \not\subset K$, as K is unramified at ℓ. □

Remark 3.15. For the fields K_E at $p = 23$ and 29, we use $r_1 + r_2 - 1 + \#S$ explicit elements u_i of K, which are S-units since the ideals they generate are products of primes above p. Their images under the map (3.1) in $\bigoplus_{v|\ell} k_v$ are linearly independent (Sections 9 and 10), so by Lemma 3.5 they form a basis of $K(S, \ell)$ as soon as $\ell \nmid h_K$. So GRH enters the use of Proposition 3.14 only through the hypothesis $\ell \nmid h_K$. Proposition A.12 proves this hypothesis without GRH for $K_{27\mathrm{a}1}$ at $p = 23$ and 29 and for $K_{288\mathrm{a}1}$ at $p = 23$.

3.6. **Local classes in the λ-direction.** For Stoll's criterion at $p = 23$ and 29 (Lemma 5.9) we describe the local classes δ_v at the places above ℓ through the formal logarithm in the λ-direction (Lemma 3.16) and, under a hypothesis on $\tilde{J}(k_v)$, through a splitting of $J(K_v)$ (Lemma 3.17).

Let $v \mid \ell$ be a place of a number field K unramified at ℓ, so that K_v is unramified over $\mathbb{Q}_\ell$. The map (3.1) identifies $\mathcal{O}_v^\times/\mathcal{O}_v^{\times\ell}$ with k_v. For $R \in J(K_v)$ we write $\delta_v(R) \in k_v$ for the image of $\delta(R)$, which is a unit class up to ℓ-th powers by the proof of Proposition 3.14(b). For $Q \in X_0(p)(K_v)$ not reducing to a cusp we put $\delta_v(Q) \coloneqq \delta_v([Q - \infty])$, the class of $f(Q)$. For a number field K as in Proposition 3.14 let

$$\Sigma \coloneqq \text{the image of } K(S, \ell) \text{ in } \textstyle\bigoplus_{v|\ell} k_v, \qquad \Theta_T \coloneqq \bigoplus_{v|\ell} \mathbb{F}_\ell\, \delta_v(T),$$

and $\delta(R)|_\ell \coloneqq (\delta_v(R))_{v|\ell}$.

Let $\widehat{J}$ be the formal group of the Néron model of J over $\mathbb{Z}_\ell$, an abelian scheme, so that $\widehat{J}(\ell\mathcal{O}_v)$ is the kernel of reduction $J(K_v) \to \tilde{J}(k_v)$. Let $\mathfrak{t}_v$ be the tangent space of the Néron model over $\mathcal{O}_v$. Let $a_\lambda, a_\mu \in \mathbb{Z}_\ell$ be the roots of $t^2 + t - 1$ ($p = 23$), respectively $t^2 + 2t - 1$ ($p = 29$), with $a_\lambda \equiv 3 \pmod{\ell}$. They are the images of T_2 in $\mathcal{O}_\lambda$ and $\mathcal{O}_\mu$. The newforms of level p are $g_1 + ag_2$ with $a \in \{a_\lambda, a_\mu\}$, where g_1, g_2 is the basis of cusp forms of Section 2.3. So the differentials $\omega_\lambda \coloneqq (x + a_\lambda)\,dx/y = (g_1 + a_\lambda g_2)\,dq/q$ and $\omega_\mu \coloneqq (x + a_\mu)\,dx/y$ are regular on $X_0(p)_{\mathbb{Z}_\ell}$, and $\mathcal{O}$ acts on them through $\mathcal{O}_\lambda$ and $\mathcal{O}_\mu$. They form a $\mathbb{Z}_\ell$-basis of the regular differentials, since $a_\lambda - a_\mu$ is an ℓ-adic unit ($\equiv 7$, respectively 1, modulo ℓ). Dually, $\mathfrak{t}_v$ is the direct sum of two free $\mathcal{O}_v$-modules of rank one on which $\mathcal{O}$ acts through $\mathcal{O}_\lambda$ and through $\mathcal{O}_\mu$. Let $\log_\lambda\colon \widehat{J}(\ell\mathcal{O}_v) \to \ell\mathcal{O}_v$ be the formal logarithm in the direction ω_λ. Let $\lambda_\lambda \in \ell\mathbb{Z}_\ell^\times$ and $\mu_\lambda \in \mathbb{Z}_\ell^\times$ be the images of λ, μ in $\mathcal{O}_\lambda$, so that $\mu_\lambda \equiv \varepsilon \pmod{\ell}$.

Lemma 3.16. (F1) *The formal logarithm is an $\mathcal{O}$-equivariant isomorphism $\widehat{J}(\ell^m\mathcal{O}_v) \to \ell^m\mathfrak{t}_v$ for $m \geq 1$. Hence $\widehat{J}(\ell^2\mathcal{O}_v) \subseteq \lambda\widehat{J}(\ell\mathcal{O}_v)$, and a point $R \in \widehat{J}(\ell\mathcal{O}_v)$ lies in $\lambda^d\widehat{J}(\ell\mathcal{O}_v)$ if and only if $\log_\lambda R \in \ell^{d+1}\mathcal{O}_v$.*

(F2) *The λ-torsion of $\tilde{J}(k_v)$ is $\langle \tilde{T} \rangle$, of order ℓ.*

(F3) *δ_v vanishes on $\lambda J(K_v)$, and its restriction to $\widehat{J}(\ell\mathcal{O}_v)$ has kernel $\lambda\widehat{J}(\ell\mathcal{O}_v)$. So there is an $\mathbb{F}_\ell$-linear bijection $N_v\colon k_v \to k_v$ with $\delta_v(R) = N_v(\log_\lambda(R)/\ell \bmod \ell)$ for $R \in \widehat{J}(\ell\mathcal{O}_v)$. If $\log_\lambda R \in \ell^{d+1}\mathcal{O}_v$, the unique formal point R' with $\lambda^d R' = R$ has $\delta_v(R') = \varepsilon^d\, N_v(\log_\lambda(R)/\ell^{d+1} \bmod \ell)$.*

Proof. (F1) The formal logarithm is an isomorphism on $\widehat{J}(\ell^m\mathcal{O}_v)$ for $m > 1/(\ell-1)$, since K_v is unramified over $\mathbb{Q}_\ell$. On the two summands of $\mathfrak{t}_v$, λ acts by λ_λ, of valuation one, and by a unit. So $\lambda(\ell\mathfrak{t}_v)$ consists of the vectors whose λ-coordinate lies in $\ell^2\mathcal{O}_v$, which gives both statements for $d = 1$. Induct on d.

(F2) By (M3) and the paragraph after (M4), $J[\lambda]$ extends over $\mathbb{Z}_\ell$ to $\mathbb{Z}/\ell \oplus \mu_\ell$, whose special fibre has k_v-points $\mathbb{Z}/\ell$, the reduction of C.

(F3) $\lambda J(K_v) = \phi\psi J(K_v) \subseteq \phi(J'(K_v))$, on which the local Kummer map of ϕ vanishes. Since $\ker\psi = C$ is étale over $\mathcal{O}_v$, ψ induces an isomorphism of formal groups, so $\lambda\widehat{J}(\ell\mathcal{O}_v) = \phi\big(\widehat{J'}(\ell\mathcal{O}_v)\big)$. If $Y \in J'(K_v)$ and $\phi(Y) \in \widehat{J}(\ell\mathcal{O}_v)$, then the reduction of Y lies in $(\ker\phi)(k_v) = \mu_\ell(k_v) = 1$, so $Y \in \widehat{J'}(\ell\mathcal{O}_v)$. Hence $\widehat{J}(\ell\mathcal{O}_v) \cap \phi(J'(K_v)) = \lambda\widehat{J}(\ell\mathcal{O}_v)$, which is the kernel of δ_v on $\widehat{J}(\ell\mathcal{O}_v)$ by Proposition 3.13. By (F1), $R \mapsto \log_\lambda(R)/\ell \bmod \ell$ identifies $\widehat{J}(\ell\mathcal{O}_v)/\lambda\widehat{J}(\ell\mathcal{O}_v)$ with k_v, which gives N_v. For the last formula, $\log_\lambda R' = \lambda^{-d}\log_\lambda R = \mu_\lambda^d \log_\lambda(R)/\ell^d$. □

We also use the following hypothesis on a place $v \mid \ell$:

$$\text{the } \ell\text{-primary part of } \widetilde{J}(k_v) \text{ is } \langle\tilde{T}\rangle, \text{ cyclic of order } \ell. \tag{H_v}$$

It holds for $p = 23$ when $n_v \in \{1, 2\}$, since $\#\widetilde{J}(\mathbb{F}_{11}) = 220 = 2^2\cdot 5\cdot 11$ and $\#\widetilde{J}(\mathbb{F}_{121}) = 16720 = 2^4\cdot 5\cdot 11\cdot 19$. It holds for $p = 29$ when $n_v = 5$, since $\#\widetilde{J}(\mathbb{F}_{7^5}) = 282502136 = 2^3\cdot 7\cdot 41^2\cdot 3001$. These orders come from the characteristic polynomials $t^4 + 6t^3 + 26t^2 + 66t + 121$ and $t^4 + 6t^2 + 49$ of Frobenius on $\widetilde{J}$ over $\mathbb{F}_{11}$ and $\mathbb{F}_7$ (Appendix B). The hypothesis enters only through Lemma 3.17 and Proposition 3.18, that is, through case (ii) of Lemma 5.9, which is applied to $K_{27\mathrm{a}1}$ and $K_{288\mathrm{a}1}$ at $p = 23$ and $K_{27\mathrm{a}1}$ at $p = 29$.

Lemma 3.17. *Assume (H_v). Then $J(K_v) = J(K_v)' \oplus \langle T\rangle \oplus \widehat{J}(\ell\mathcal{O}_v)$ as $\mathcal{O}$-modules, where $J(K_v)'$ is the torsion subgroup of order prime to ℓ. Moreover $\lambda J(K_v) = J(K_v)' \oplus \lambda\widehat{J}(\ell\mathcal{O}_v)$, $J(K_v)[\lambda^\infty] = \langle T\rangle$, and $\widetilde{J}(k_v)/\lambda\widetilde{J}(k_v)$ is generated by $\tilde{T}$. Let $\pi_v\colon J(K_v) \to \widetilde{J}(k_v)/\lambda\widetilde{J}(k_v) \simeq \mathbb{Z}/\ell$ be reduction followed by the quotient map, normalized by $\pi_v(T) = 1$, and*

$$\delta_v^0 \coloneqq \delta_v - \pi_v\cdot\delta_v(T)\colon J(K_v) \longrightarrow k_v.$$

Then δ_v^0 is a homomorphism that vanishes on $\lambda J(K_v)$ and on T, and the map (δ_v, π_v) is injective on $J(K_v)/\lambda J(K_v)$.

Proof. The formal group $\widehat{J}(\ell\mathcal{O}_v)$ is torsion-free, as K_v is unramified over $\mathbb{Q}_\ell$ and $1 < \ell - 1$. So torsion injects into $\widetilde{J}(k_v)$, the torsion of order prime to ℓ of $\widetilde{J}(k_v)$ lifts, and by (H_v) the ℓ-primary torsion of $J(K_v)$ is $\langle T\rangle$. This gives the decomposition, and each summand is $\mathcal{O}$-stable, since $\mathcal{O}$ acts on $J[\lambda] \ni T$ through $\mathcal{O}/\lambda = \mathbb{F}_\ell$. As λ divides ℓ, it is invertible on groups of order prime to ℓ, and $\lambda T = 0$. This gives $\lambda J(K_v)$ and the statement on $\widetilde{J}(k_v)/\lambda\widetilde{J}(k_v)$. So $J(K_v)/\lambda J(K_v) = \widehat{J}(\ell\mathcal{O}_v)/\lambda\widehat{J}(\ell\mathcal{O}_v) \oplus \mathbb{F}_\ell T$. On the first summand δ_v is injective by (F3) and π_v vanishes, while $\pi_v(T) = 1$. □

3.7. **The second descent and chains of λ-divisions.** With the descent of Section 3.5 alone, case (i) of Lemma 5.9 tests the class of a known point against $\Sigma + \Theta_T$. A second descent, by the isogeny ϕ' with kernel $\mathbb{Z}/\ell$, shows that the reduction modulo λ of a global point is the same at all places above ℓ (Proposition 3.18). With it the test is against Σ

alone (case (ii) of Lemma 5.9), and Lemma 3.20 extends it to repeated division by λ, for the curves with complex multiplication in Sections 9 and 10.

Proposition 3.18. *Let K be a number field unramified at ℓ with $\ell \nmid h_K$, such that (H_v) holds for every place $v \mid \ell$ and the ray class group of K modulo $\mathfrak{m} := \prod_{v|p} v$ has ℓ-rank at most one. Then for every $R \in J(K)$ the value $\pi_v(R)$ is the same for all places $v \mid \ell$.*

Proof. Let $\delta_{\phi'} \colon J(K) \to H^1(K, \mathbb{Z}/\ell) = \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), \mathbb{Z}/\ell)$ be the Kummer map of $\phi' \colon J/\mathrm{Sh} \to J$, whose kernel is the constant group $\mathbb{Z}/\ell$ over $\mathbb{Z}[1/p]$. At $v \mid \ell$, ϕ' is étale, so it induces an isomorphism of formal groups and $\widehat{J}(\ell\mathcal{O}_v) \subseteq \phi'((J/\mathrm{Sh})(K_v))$. Hence the local Kummer map $\delta_{\phi',v}$ factors through $\widetilde{J}(k_v)$ and takes values in the unramified classes $H^1(k_v, \mathbb{Z}/\ell) \simeq \mathbb{Z}/\ell$ (Lemma 3.3(b)). On $\widetilde{J}(k_v)$ it is the connecting map of

$$0 \to \mathbb{Z}/\ell \to \widetilde{(J/\mathrm{Sh})}(k_v) \to \widetilde{J}(k_v) \to H^1(k_v, \mathbb{Z}/\ell) \to H^1(k_v, \widetilde{J/\mathrm{Sh}}) = 0$$

(Lang's theorem). So it is surjective, with kernel $\tilde{\phi}'(\widetilde{(J/\mathrm{Sh})}(k_v))$ of index ℓ. This kernel contains $\lambda\widetilde{J}(k_v) = \tilde{\phi}'\tilde{\psi}'(\widetilde{J}(k_v))$, which has index $\#\widetilde{J}(k_v)[\lambda] = \ell$ by (F2). So $\delta_{\phi',v} = \alpha_v \pi_v$ for some $\alpha_v \in \mathbb{F}_\ell^\times$. Globally, $\delta_{\phi'}(R)$ is unramified at every finite place not above p (at $v \mid \ell$ by what was just said) and tamely ramified at the places above p, since its order is prime to p. At the real places it is trivial, since ℓ is odd. So $\delta_{\phi'}(R)$ factors through the ray class group modulo $\mathfrak{m}$, whose ℓ-rank is at most one. Since $\delta_{\phi'}(T)$ restricts at $v \mid \ell$ to $\alpha_v \neq 0$, it spans the group of homomorphisms from this ray class group to $\mathbb{Z}/\ell$, and $\delta_{\phi'}(R) = c\,\delta_{\phi'}(T)$ for some $c \in \mathbb{F}_\ell$. Restricting to $v \mid \ell$ gives $\alpha_v \pi_v(R) = c\,\alpha_v$, so $\pi_v(R) = c$ for all $v \mid \ell$. □

Remark 3.19. Suppose that $\ell \nmid h_K$ and that K has a single place $\mathfrak{p}$ above p, with residue field $\mathbb{F}_p$. Then the ℓ-part of the ray class group modulo $\mathfrak{p}$ is a quotient of the ℓ-part of $(\mathcal{O}_K/\mathfrak{p})^\times = \mathbb{F}_p^\times$, which is cyclic of order ℓ since $\ell \,\|\, p-1$. So the last hypothesis of Proposition 3.18 follows from $\ell \nmid h_K$ for the fields $K_{27\mathrm{a}1}$ and $K_{288\mathrm{a}1}$ at $p = 23$ and $K_{27\mathrm{a}1}$ at $p = 29$, in which p is totally ramified (Tables 7 and 8).

Lemma 3.20 (chains of λ-divisions)**.** *Let K be as in Proposition 3.18, and assume that the localization $K(S,\ell) \to \bigoplus_{v|\ell} k_v$ is injective, with image Σ. Let $D \in J(K)$ and $m \geq 1$ be such that $D_v \in \lambda^m J(K_v) + \langle T \rangle$ for every $v \mid \ell$. If $W_v \in J(K_v)$ are points with $\lambda^m W_v \in D_v + \langle T \rangle$ for every $v \mid \ell$, then $(\delta_v^0(W_v))_{v|\ell} \in \Sigma$.*

Proof. We show by induction on $i = 0, \ldots, m$ that $D = \lambda^i R_i + c_i T$ with $R_i \in J(K)$ and $c_i \in \mathbb{Z}/\ell$. For $i = 0$ take $R_0 = D$. Let $i < m$ and $v \mid \ell$, and write $D_v = \lambda^m Y_v + a_v T$. If $i \geq 1$, then $(c_i - a_v)T = \lambda^m Y_v - \lambda^i R_{i,v} \in \lambda J(K_v)$, so $a_v = c_i$ by Lemma 3.17, and $R_{i,v} - \lambda^{m-i} Y_v \in J(K_v)[\lambda^i] \subseteq \langle T \rangle$. In all cases $R_{i,v} \in \lambda J(K_v) + \langle T \rangle$, so $R_{i,v} - \pi_v(R_i)T \in \lambda J(K_v)$. By Proposition 3.18, $\pi_v(R_i) = c$ is the same for all v. Then $\delta_v(R_i - cT) = 0$ for all $v \mid \ell$, so $\delta(R_i - cT)$, an element of $K(S,\ell)$ with trivial localization, is trivial, and $R_i - cT = \lambda R_{i+1}$ with $R_{i+1} \in J(K)$ by Proposition 3.14(b). Then $D = \lambda^{i+1} R_{i+1} + c_{i+1} T$ with $c_{i+1} = c_i$ if $i \geq 1$ and $c_1 = c$ if $i = 0$. For $i = m$ we have $\lambda^m(W_v - R_{m,v}) \in \langle T \rangle$, so $W_v - R_{m,v} \in J(K_v)[\lambda^\infty] = \langle T \rangle$ and $\delta_v^0(W_v) = \delta_v^0(R_{m,v})$. By Proposition 3.18, $\pi_v(R_m) = c'$ for all v, so $\delta_v^0(R_{m,v}) = \delta_v(R_m - c'T)$, and the tuple is the localization of $\delta(R_m - c'T) \in K(S,\ell)$. □

4. Local analysis and the disc test

Sections 6, 7, 8, 9 and 10 use the disc test proved here (Proposition 4.9) to confine j_0 to the sets that contain the j-invariant of a known point.

Throughout, $K=K_E$ is one of the fields of Section 2.4, and $\ell=5$, 2, 3, 11, 7 for $p=11$, 17, 19, 23, 29 is the prime of the descent of Section 3. For $v\mid\ell$ the local Kummer map δ_v takes values in H_v, which is $\prod_{w\mid v}L_w^\times/L_w^{\times 2}$ with $L=K(i)$ for $p=17$ (Section 3.4), $K_v^\times/K_v^{\times\ell}$ for $p=11,19$, and $k_v\simeq\mathcal{O}_v^\times/\mathcal{O}_v^{\times\ell}$ (Section 3.6) for $p=23,29$. Let $\Sigma\subseteq\prod_{v\mid\ell}H_v$ be the image of the Selmer group of Section 3 (of $K(S,\ell)$ for $p=23,29$). It contains the tuple $(\delta_v(Q_v))_{v\mid\ell}$ of every $Q\in J(K)$, and of every $Q\in X_0(p)(K)$ in genus 2, where $\delta_v(Q)\coloneqq\delta_v([Q-\infty])$. We identify $X_0(p)$ with its smooth model over $\mathbb{Z}_\ell$ (the minimal model of Table 5 in genus 1, the model of Section 2.3 in genus 2). The *residue disc* of $Q\in X_0(p)(K_v)$ is the set of points of $X_0(p)(\bar{\mathbb{Q}}_\ell)$ with the same reduction.

4.1. **Roots near a point of a fibre.** The next two lemmas locate the roots of the fibre polynomial $G_p(x,j)$ of (2.4) near a root of $G_p(x,j_c)$, for j near j_c, under the hypotheses of [27, Lemma 7.5], in the notation there. Let M be a finite extension of $\mathbb{Q}_\ell$, and extend its absolute value $|\cdot|$ to an algebraic closure $\bar{M}$. Let $F=\sum_{i,k\geq 0}f_{ik}X^iY^k\in M[X,Y]$, let $e\geq 1$ be an integer, and assume that $f_{0k}=0$ for $0\leq k<e$ and $f_{0e}=1$. Write $F=\sum_k F_k(X)Y^k$, and assume that $F_0(X)=-cX+$(terms of higher degree) with $c\neq 0$. For $r>0$ and a polynomial $h=\sum a_it^i$ put $|h|_r=\max_i r^i|a_i|$, the Gauss norm on the closed disc of radius r. The hypotheses are: (i) $|F_m(t^e)|_r<|F_0(t^e)|_r^{(e-m)/e}$ for $0<m<e$; (ii) $|F_e(t^e)-1|_r<1$; (iii) $|F_0(t^e)|_r^{(m-e)/e}\,|F_m(t^e)|_r<1$ for $m>e$; (iv) $|F_0(t^e)+ct^e|_r<|F_0(t^e)|_r$. Under (iv), $|F_0(t^e)|_r=|c|r^e$, and we put $\rho_0=|c|^{1/e}r$. There are exactly e formal power series $\varphi_0,\dots,\varphi_{e-1}$ with coefficients in the splitting field of X^e-c over M such that $\varphi_k(0)=0$ and $F(t^e,\varphi_k(t))=0$, and $\varphi_k(t)=\varphi_0(\zeta^kt)$ for a primitive e-th root of unity ζ [27, Lemma 7.5].

Lemma 4.1 (roots near a point)**.** *Assume* (i)–(iv)*, and let $\tau\in\bar{M}$ with $|\tau|\leq r$. Then the polynomial $F(\tau^e,Y)$ has exactly e roots, counted with multiplicity, in the closed disc $|Y|\leq\rho_0$, and each of them has absolute value $|c|^{1/e}|\tau|$.*

Proof. For $\tau=0$ the roots in the disc are 0, with multiplicity e, since $F(0,Y)=Y^e+\sum_{m>e}f_{0m}Y^m$ and $|f_{0m}|<\rho_0^{e-m}$ for $m>e$ by (iii). Let $\tau\neq 0$, $a_m=F_m(\tau^e)$ and $\sigma=|c|^{1/e}|\tau|\leq\rho_0$. For a polynomial h, $|h(\tau^e)|\leq|h(t^e)|_r$, and $|h(\tau^e)|\leq(|\tau|/r)^e|h(t^e)|_r$ if $h(0)=0$. As F_0+cX has no term of degree below 2, (iv) gives $|a_0+c\tau^e|\leq(|\tau|/r)^{2e}|F_0(t^e)+ct^e|_r<(|\tau|/r)^{2e}\rho_0^e\leq\sigma^e$, so $|a_0|=\sigma^e$. By (ii), $|a_e|=1$. For $0<m<e$, $F_m(0)=f_{0m}=0$ and (i) give $|a_m|<(|\tau|/r)^e\rho_0^{e-m}\leq\sigma^{e-m}$. For $m>e$, (iii) gives $|a_m|<\rho_0^{e-m}$. So $\max_m|a_m|\rho_0^m=\rho_0^e$ with e the largest index attaining it, and $\max_m|a_m|\sigma^m=\sigma^e$, attained at $m=0$ and $m=e$ only. By the Newton polygon [42, Chapter II, (6.3)], the number of roots of $\sum_m a_mY^m$, with multiplicity, in $|Y|\leq s$ is the largest index at which $\max_m|a_m|s^m$ is attained, and in $|Y|<s$ the smallest. So $F(\tau^e,Y)$ has e roots with $|Y|\leq\rho_0$, none with $|Y|<\sigma$, and e with $|Y|\leq\sigma$, so all of them have absolute value σ. □

Lemma 4.2 (branches)**.** *Assume* (i)–(iv) *and that $\ell\nmid e$. Then the power series $\varphi_0,\dots,\varphi_{e-1}$ converge on the closed disc of radius r in $\bar{M}$. Each has Gauss norm ρ_0 on this disc, attained at its linear term $\zeta^k\gamma t$, where $\gamma^e=c$, and at no other term. For every τ with $|\tau|\leq r$ the values $\varphi_k(\tau)$ are the roots of Lemma 4.1. They have absolute value $|c|^{1/e}|\tau|$ and are pairwise distinct if $\tau\neq 0$.*

Proof. Let L' be the splitting field of X^e-c over M, $\gamma\in L'$ with $\gamma^e=c$, $\mathcal{T}$ the ring of power series over L' converging on the closed disc of radius r, with the multiplicative Gauss norm, and $\mathcal{T}^\circ$ its closed unit ball, which is complete. Put $H(w)=(ct^e)^{-1}F(t^e,\gamma tw)=\sum_m h_mw^m$ with $h_m=c^{-1}\gamma^mt^{m-e}F_m(t^e)$. Each h_m lies in $\mathcal{T}$, since t^e divides $F_m(t^e)$ for $m<e$. By

(iv), $h_0 = -1 + (\text{norm} < 1)$, and by (ii), $h_e = 1 + (\text{norm} < 1)$. Since $|t^{m-e}F_m(t^e)|_r = r^{m-e}|F_m(t^e)|_r$, conditions (i) and (iii) say that $|h_m|_r < 1$ for $m \neq 0, e$. So $H \in \mathcal{T}^\circ[w]$ reduces to $w^e - 1$ modulo the elements of norm less than 1. As $\ell \nmid e$, $H'(\zeta^k) = e\zeta^{k(e-1)} + (\text{norm} < 1)$ is a unit of $\mathcal{T}^\circ$, and Newton's method gives $w_k \in \mathcal{T}^\circ$ with $H(w_k) = 0$ and $|w_k - \zeta^k|_r < 1$, with $w_k(0) = \zeta^k$ since $H = w^e - 1$ at $t = 0$. The series $\gamma t w_k$ vanish at 0 and satisfy $F(t^e, \gamma t w_k) = 0$, so they are the φ_k after renumbering, they converge on the disc, and $\varphi_k = \zeta^k\gamma t + \gamma t(w_k - \zeta^k)$ has Gauss norm $|\gamma|r = \rho_0$, attained only at the linear term. For $|\tau| \leq r$ we have $|w_k(\tau) - \zeta^k| < 1$, so $|\varphi_k(\tau)| = |\gamma||\tau|$ and $|\varphi_k(\tau) - \varphi_l(\tau)| = |\gamma||\tau|$ for $k \neq l$. If $\tau \neq 0$, these are e distinct roots of $F(\tau^e, Y)$ in $|Y| \leq \rho_0$, hence all the roots there by Lemma 4.1. □

Remark 4.3. Lemma 7.5 of [27] asserts that the φ_k converge on the closed disc of radius r, with $|\varphi_k(\tau)| = |c|^{1/e}|\tau|$ there, assuming only that the characteristic of M does not divide e. When $\ell \mid e$ this can fail: for $M = \mathbb{Q}_2$, $e = 2$, $r = 1$ and $F = Y^2 - aXY - X$ with $a \in \{2, 4\}$, conditions (i)–(iv) hold, but the root $\varphi_0 = at^2/2 + t(1 + a^2t^2/4)^{1/2}$ does not converge at $t = 1$, and $F(1, Y) = Y^2 - aY - 1$ has no root in $\mathbb{Q}_2$. Freitas, Naskręcki and Stoll apply their lemma with $e = 2$ at $\ell = 2$ in the proof of [27, Lemma 7.6], to the four families $\{12^3 + a\,2^{10}t^2 : t \in \mathbb{Z}_2\}$, $a \in \{\pm 1, \pm 3\}$, of [27, (7.2)]. For these families the conclusion of the lemma does hold. At a root ξ of $G_{11}(x, 12^3)$ (a double root) let $F(X, Y)$ be $G_{11}(\xi + Y, 12^3 + a\,2^{10}X)$ divided by its coefficient of X^0Y^2, so that $F(X, 0) = -cX + \dots$ as above, and let $\gamma^2 = c$ and $\Phi(w) = (ct^2)^{-1}F(t^2, \gamma t w)$, a polynomial in t and w. A computation shows that every coefficient of the polynomial $\Phi - (w^2 - 1)$ in t and w has absolute value at most $|4|$, with equality only for the monomials tw^3 and t^2w^4, and that if ρ is the residue of the coefficient of tw^3 divided by 4, then the residue of the coefficient of t^2w^4 divided by 4 is ρ^2. Hence $\Phi(1 + 2u)/4 \equiv u^2 + u + \rho t + \rho^2t^2$ modulo the maximal ideal, and the root $u = \rho t$ of the reduction lifts by Hensel's lemma to a power series converging on $|t| \leq 1$, which gives the convergence of the φ_k. The lift has $u(0) = 0$, as $\Phi = w^2 - 1$ at $t = 0$, so $\gamma t(1 + 2u) = \varphi_0$ and $\varphi_1(t) = \varphi_0(-t)$; and $|1 + 2u| = 1$ gives $|\varphi_k(\tau)| = |c|^{1/2}|\tau|$. This is the only use of the lemma with $\ell \mid e$ in their proof for $p = 11$, so that proof is not affected by the failure of the lemma when $\ell \mid e$. Outside their §7, which treats $p = 11$, a version of the lemma is used only in their §3, for Tables 1 and 2, and there, as their script shows [62, `section3.magma`, line 160], only at simple roots, $e = 1$. Their result for $p = 11$ is also recovered, unconditionally, by Theorem A. In the lines of Tables 1 and 2 of [27] that we use, lines 2, 3, 5 and 6 of Table 1 and lines 2 to 8 of Table 2, for $p = 19$, and for $p = 13$ lines 3, 4, 5 and 7, the description of j is confirmed by a computation over all residue classes of (a, b) (Appendix B.2). The assignment of these lines to the curves E, through the inertial fields, is used as published. Line 1 of Table 2, used only for 96a1, is derived directly in Sections 8.1 and 16.1. Where the ramification index is divisible by ℓ, at $p = 19$ and at $p = 13$, we use only Lemma 4.1, which rests on the Newton polygon and holds for every e (Proposition 8.1, Lemma 17.3(b)).

A *family* is a set $\{j_c + \kappa t^e : t \in \mathbb{Z}_\ell\}$ with $j_c, \kappa \in \mathbb{Q}$, $\kappa \neq 0$ and $e \in \{1, 2, 3\}$. Let ξ be a root of $G_p(x, j_c)$ of multiplicity e_ξ. We apply Lemma 4.1 over $M = \mathbb{Q}_\ell(\xi)$ with $r = 1$ to $F(X, Y) = G_p(\xi + Y, j_c + \kappa X)$, divided by its coefficient of $X^0Y^{e_\xi}$, with e_ξ in place of e. In all the families used below $e_\xi \in \{1, e\}$. When $e_\xi = 1 < e$ the lemma is applied in the variable $\tau_\xi = t^e$, otherwise in $\tau_\xi = t$. Put $\nu_\xi = v_\ell(c)/e_\xi$, so that the disc $|Y| \leq \rho_0$ of Lemma 4.1 is the disc of radius $\ell^{-\nu_\xi}$ about ξ. We also require the separation condition

$$\nu_\xi > v_\ell(\xi - \xi') \quad \text{for every other root } \xi' \text{ of } G_p(x, j_c). \tag{4.1}$$

Conditions (i)–(iv) and (4.1) are checked in $\mathbb{Q}(\xi)$ at every prime above ℓ, which covers every ℓ-adic root by conjugation. When $\ell \nmid e_\xi$, the series $x = \xi + \varphi(\tau_\xi)$ of Lemma 4.2 are the *branches* through ξ.

Lemma 4.4. *Suppose that* (i)–(iv) *and* (4.1) *hold at every root ξ of $G_p(x, j_c)$. Let $t \in \mathbb{Z}_\ell$ and $j = j_c + \kappa t^e$.*

(a) *For every root ξ, the closed disc of radius $\ell^{-\nu_\xi}$ about ξ contains exactly e_ξ roots x of $G_p(x, j)$, counted with multiplicity, and each satisfies $v_\ell(x - \xi) = \nu_\xi + v_\ell(\tau_\xi)$. These discs are pairwise disjoint and contain all the roots of $G_p(x, j)$.*

(b) *If $\ell \nmid e_\xi$, the roots in the disc about ξ are the values at τ_ξ of the branches through ξ. Every coefficient of a branch φ through ξ has valuation at least ν_ξ, so $v_\ell(\varphi(\tau) - \varphi(\tau')) \geq \nu_\xi + v_\ell(\tau - \tau')$ for $\tau, \tau' \in \mathbb{Z}_\ell$.*

(c) *Let K_v be a finite extension of $\mathbb{Q}_\ell$ and $x_1 \in K_v$ a root of $G_p(x, j)$. Then x_1 lies in the disc about a root $\xi \in K_v$. If moreover $e_\xi = 1$, the branch through ξ has coefficients in K_v, so its value at every $\tau' \in \mathbb{Z}_\ell$ lies in K_v.*

Proof. (a) The first statement is Lemma 4.1 at ξ with $\tau = \tau_\xi$. If the discs about two roots $\xi \neq \xi'$ met, then $v_\ell(\xi - \xi') \geq \min(\nu_\xi, \nu_{\xi'})$, contrary to (4.1). As G_p is monic in x of degree $p + 1 = \sum_\xi e_\xi$, the discs contain all the roots. (b) is Lemma 4.2: the Gauss norm on the unit disc is $\ell^{-\nu_\xi}$, and $\tau - \tau'$ divides $\tau^n - \tau'^n$ in $\mathbb{Z}_\ell$. (c) An automorphism σ of $\bar{\mathbb{Q}}_\ell$ over K_v permutes the roots of $G_p(x, j_c)$ and of $G_p(x, j)$, preserves distances, and carries the polynomial F at ξ to the one at $\sigma(\xi)$, so $e_{\sigma(\xi)} = e_\xi$ and $\nu_{\sigma(\xi)} = \nu_\xi$. So the disc about $\sigma(\xi)$ contains $\sigma(x_1) = x_1$, and $\sigma(\xi) = \xi$ by the disjointness in (a). If $e_\xi = 1$ there is only one branch through ξ, and its coefficients lie in $\mathbb{Q}_\ell(\xi) \subseteq K_v$. □

4.2. **The ramified regions.** For $p = 23, 29$ the points over a j-value close to 0 or 1728 cluster around the ramification points of j, and the disc test describes them by labels (Lemma 4.5) instead of roots. Let $\ell \geq 5$ and $w \in \mathbb{Z}_\ell^\times$. The two *ramified regions* are

$$\text{region A: } j_0 = \ell^{3k} w, \qquad \text{region B: } 1728 - j_0 = \ell^{2k} w, \qquad k \geq 1, \tag{4.2}$$

and k is the *depth* of j_0. In region A put $e = 3$, $j_c = 0$, $\varsigma = 1$, and in region B put $e = 2$, $j_c = 1728$, $\varsigma = -1$. So e is the ramification index of j over j_c. By Lemma 9.1(iii), the point of a solution with $\ell \mid b$ lies in region A at depth $v_\ell(b)$, and one with $\ell \mid a$ in region B at depth $v_\ell(a)$. Region A is used for $p \in \{23, 29\}$ ($p \equiv 2 \pmod 3$), region B for $p = 23$ ($p \equiv 3 \pmod 4$). For $p = 11$ and $\ell = 5$ the sets $\{1728 - 25ws^2 : s \in \mathbb{Z}_5\}$, $w \in \{1, 2\}$, of Lemma 4.6(c) make up region B at $\ell = 5$ together with 1728. The depth of $1728 - 25ws^2$ is $1 + v_5(s)$. Let $\rho_1, \ldots, \rho_{(p+1)/e}$ be the points of $X_0(p)$ over j_c. As $j^*(j_c) = e \sum_i (\rho_i)$ (proof of Lemma 4.5(a)), $G_p(x, j_c) = h(x)^e$ with h of degree $(p + 1)/e$, that is 8, 12, 10 for region A at 23, region B at 23, region A at 29.

Lemma 4.5. *Let $p \in \{23, 29\}$, and let e, j_c, ς be those of a region used for p. Here $\ell \in \{7, 11\}$ and $e \in \{2, 3\}$, so $\ell \nmid e$.*

(a) *The points ρ_i are defined over the maximal unramified extension of $\mathbb{Q}_\ell$, their reductions $\tilde{\rho}_i$ are pairwise distinct, and $\tilde{\jmath} - \bar{\jmath}_c$ has a zero of order exactly e at each $\tilde{\rho}_i$. Let z_i be $x - x(\rho_i)$, or $y - y(\rho_i)$ if $\tilde{\rho}_i$ is a Weierstrass point. It is a parameter at $\tilde{\rho}_i$, $z_{\sigma(i)} = \sigma(z_i)$ for $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, and on the residue disc of $\tilde{\rho}_i$*

$$j - j_c = z_i^e \, u_i(z_i), \qquad u_i \in \mathcal{O}_{L_i}[[z]], \quad u_i(0) \in \mathcal{O}_{L_i}^\times, \qquad L_i := \mathbb{Q}_\ell(\rho_i).$$

(b) *Let $j_0 = j_c + \varsigma\ell^{ek}w$ with $k \geq 1$ and $w \in \mathbb{Z}_\ell^\times$. Every point of $X_0(p)$ over j_0 lies in the residue disc of some $\tilde{\rho}_i$, and the points over j_0 in that disc are the e points with $z_i = \ell^k s$, $s^e u_i(\ell^k s) = \varsigma w$. Their residues $\bar{s}$ are the e distinct roots of $\bar{s}^e = \varsigma\bar{w}/\bar{u}_i(0)$. So the points over j_0 correspond to the* labels *$(i, \bar{s})$ with $\bar{s}^e = \varsigma\bar{w}/\bar{u}_i(0)$, and they are defined over an unramified extension of $\mathbb{Q}_\ell$.*

(c) *The Frobenius σ acts on the labels by $(i, \bar{s}) \mapsto (\sigma(i), \bar{s}^\ell)$. So the Frobenius orbits on the fibre over j_0 depend only on $\bar{w}$ and not on k. If moreover $G_p(x, j_0)$ is separable, as it is at the j-invariant of a solution (Proposition 2.12(b)) and, by computation, at the representatives j_D of the disc test (Section 4.4), then the $\mathbb{Q}_\ell$-factorization of $G_p(x, j_0)$ and the set of admissible configurations (Definition 2.13), described by labels, depend only on $\bar{w}$ and not on k.*

(d) *If $Q, Q' \in X_0(p)(K_v)$ lie in the residue disc of $\tilde{\rho}_i$ and $z_i(Q) \equiv z_i(Q') \pmod{\ell^2}$, then $\delta_v(Q) = \delta_v(Q')$. In particular, the class of a K_v-point over a j_0 of depth 1 depends only on its label, and a K_v-point over a j_0 of depth $k \geq 2$ in the disc of $\tilde{\rho}_i$ has the class $\delta_v(\rho_i)$ (and then $\rho_i \in X_0(p)(K_v)$).*

(e) *Let $k \geq 2$, let $Q \in X_0(p)(K_v)$ be a point over a j_0 of depth k in the disc of $\tilde{\rho}_i$, and let $Q^{(1)} \in X_0(p)(K_v)$ be the point of the same disc with $z_i(Q^{(1)}) = z_i(Q)/\ell^{k-1}$. Then, with $\log_\lambda$ the formal logarithm in the λ-direction (Section 3.6), $\log_\lambda[Q - \rho_i] \equiv \ell^{k-1}\log_\lambda[Q^{(1)} - \rho_i] \pmod{\ell^{k+1}}$.*

Proof. (a) In characteristic $\ell \geq 5$ the points of $X_0(p)_{\bar{\mathbb{F}}_\ell}$ over $\bar{j}_c$ are the pairs (E_c, D), with E_c the curve of j-invariant $\bar{j}_c$ and $D \subset E_c[p]$ of order p, up to $\mathrm{Aut}(E_c)$, which is μ_6 for $j_c = 0$ and μ_4 for $j_c = 1728$. An automorphism of order 3, respectively 4, acts on $E_c[p] \simeq \mathbb{F}_p^2$ with eigenvalues that are primitive cube, respectively fourth, roots of unity, which do not lie in $\mathbb{F}_p$ because $p \equiv 2 \pmod 3$, respectively $p \equiv 3 \pmod 4$. So it fixes no line, and the fibre has exactly $(p+1)/e$ distinct points. The same argument in characteristic 0 gives $j^*(j_c) = e\sum_i(\rho_i)$. As $X_0(p) \to \mathbb{P}^1$ is finite and flat over $\mathbb{Z}_\ell$, this divisor specializes to $\tilde{j}^*(\bar{j}_c)$, whose support has $(p+1)/e$ points, so the $\tilde{\rho}_i$ are pairwise distinct, each of multiplicity e. Inertia permutes the ρ_i and fixes their reductions, so it fixes each ρ_i. On the residue disc of $\tilde{\rho}_i$, $j - j_c$ is a power series in z_i over $\mathcal{O}_{L_i}$ with a zero of order e at ρ_i, so $j - j_c = z_i^e u_i(z_i)$, and $u_i(0)$ is a unit because $\tilde{j} - \bar{j}_c$ also has order e at $\tilde{\rho}_i$. (b) A point over j_0 reduces into the fibre over $\bar{j}_0 = \bar{j}_c$. In the disc of $\tilde{\rho}_i$, $z_i^e u_i(z_i) = \varsigma\ell^{ek}w$ forces $v_\ell(z_i) = k$, and with $z_i = \ell^k s$ it becomes $s^e u_i(\ell^k s) = \varsigma w$. As $\ell \nmid e$ and $u_i(0)$ is a unit, the e roots of $\bar{s}^e = \varsigma\bar{w}/\bar{u}_i(0)$ are distinct, and each lifts by Hensel's lemma to one solution, in an unramified extension. This gives e points in each of the $(p+1)/e$ discs, so all $p+1$ points. (c) Frobenius permutes the parameters and the power series, $z_{\sigma(i)} = \sigma(z_i)$ and $u_{\sigma(i)} = \sigma(u_i)$, and fixes ℓ^k and w, so it maps the label $(i, \bar{s})$ to $(\sigma(i), \bar{s}^\ell)$. If $G_p(x, j_0)$ is separable, its $p+1$ roots are the x-coordinates of the $p+1$ points over j_0 (Lemma 2.6), so x is injective on the fibre, and the $\mathbb{Q}_\ell$-irreducible factors of $G_p(x, j_0)$ correspond to the Frobenius orbits on labels. The degree of a factor is the length of its orbit. (d) This is the proof of Lemma 4.6(b) below, with z_i in place of $j - j_1$. If $Q \in X_0(p)(K_v)$ lies in the disc of $\tilde{\rho}_i$, then $\tilde{\rho}_i$ is k_v-rational, and ρ_i, the only point over j_c in the disc, is fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_v)$. (e) Write the differential ω_λ of Section 3.6 as $\omega_\lambda = \sum_{m\geq 0} b_m z^m\,dz$ with $z = z_i$ and $b_m \in \mathcal{O}_v$, so that $\log_\lambda[Q - \rho_i] = \sum_{m\geq 0} b_m z(Q)^{m+1}/(m+1)$. With $z(Q) = \ell^k s'$ and $z(Q^{(1)}) = \ell s'$, the terms with $m \geq 1$ have valuation at least $(m+1)k - v_\ell(m+1) \geq k+1$ on the left, and at least $k - 1 + (m+1) - v_\ell(m+1) \geq k+1$ in $\ell^{k-1}\log_\lambda[Q^{(1)} - \rho_i]$. The terms with $m = 0$ agree. □

The point $Q^{(1)}$ of (e) lies over $j_c+\varsigma\ell^e w'$ with $\bar{w}'=\bar{w}$ and has the label of Q, so by (d) its class is that of every K_v-point at depth 1 with this label.

4.3. **Constancy of the local classes.** The next three lemmas give explicit radii of constancy of the local Kummer classes: Lemma 4.6 where ℓ is odd and unramified in K, Lemmas 4.7 and 4.8 for $\ell=2$ and $\ell=3$.

Lemma 4.6. *Let $p\in\{11,23,29\}$, so that $\ell\in\{5,11,7\}$ is unramified in K, and let $v\mid\ell$.*

(a) *Let $j_1\in\mathbb{Z}_\ell$ with $j_1\not\equiv 0,1728 \pmod{\ell}$ and $G_p(x,j_1)$ separable modulo ℓ. The fibre of the reduction $\tilde{\jmath}$ of j over $\bar{\jmath}_1$ consists of $p+1$ distinct points, at which $\tilde{\jmath}$ is étale. For $j_0\in j_1+\ell\mathbb{Z}_\ell$, the fibre of j over j_0 has exactly one point in the residue disc of each of them, and this point lies in $X_0(p)(K_v)$ when its residue point is defined over k_v. The $\mathbb{Q}_\ell$-irreducible factors of $G_p(x,j_0)$ reduce to the $\mathbb{F}_\ell$-irreducible factors of $G_p(x,j_1) \bmod \ell$. In particular the admissible configurations over j_0 and over j_1 correspond bijectively, residue disc by residue disc.*

(b) *If $Q,Q'\in X_0(p)(K_v)$ lie in the same residue disc of a point over $\bar{\jmath}_1$ and $j(Q)\equiv j(Q') \pmod{\ell^2\mathcal{O}_v}$, then $[Q-Q']\in\widehat{J}(\ell^2\mathcal{O}_v)$ and $\delta_v(Q)=\delta_v(Q')$.*

(c) *Let $p=11$. For $j=1728-25ws^2$ with $w\in\{1,2\}$ and $s\in\mathbb{Z}_5$, the points of $J(\bar{\mathbb{Q}}_5)$ over j lie on the twelve analytic branches $s\mapsto P(s)$ through the six points over 1728, and along a branch that is defined over K_v the class $\delta_v(P(s))$ depends only on $s \bmod 5$. Near each point x_R over 1728 a branch has the form $x=x_R+5sZ(5s)$, with Z a power series with integral coefficients.*

Proof. (a) The reduction $\tilde{\jmath}$ is a finite morphism of degree $p+1$ whose poles are the reductions of the two cusps, and the roots of $G_p(x,j_1) \bmod \ell$ are the x-coordinates of the points of its fibre over $\bar{\jmath}_1$. For $p=11$ the fibre therefore has 12 distinct points, since $G_{11}(x,j_1)$ is squarefree modulo 5 and $\bar{\jmath}_1\notin\{0,1728,\infty\}$. For $p=23,29$, a root $\bar{x}$ with $\mathcal{B}_p(\bar{x})\equiv 0$ would have $\mathcal{A}_p(\bar{x})\equiv j_1$ and be a double root of $G_p(x,j_1)=(\mathcal{A}_p-j_1)^2-\mathcal{B}_p^2F$, so every root gives exactly one point $(\bar{x},(\bar{\jmath}_1-\mathcal{A}_p(\bar{x}))/\mathcal{B}_p(\bar{x}))$, and the fibre consists of $p+1$ distinct points. So $\tilde{\jmath}$ is étale there, and $z:=j-j_1$ is a uniformizer at each of these points on the smooth model. On the residue disc U of such a point, j maps $U(K_v)$ bijectively onto $j_1+\ell\mathcal{O}_v\supseteq j_1+\ell\mathbb{Z}_\ell$, and $U(\bar{\mathbb{Q}}_\ell)$ onto the open unit disc about j_1. The unique point of U over j_0 is fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K_v)$ when the residue point is defined over k_v. The statement on factors is Hensel's lemma, as $G_p(x,j_0)\equiv G_p(x,j_1)$ is separable modulo ℓ. (b) The map $U\times U\to J$, $(Q,Q')\mapsto[Q-Q']$, extends to the smooth models over $\mathcal{O}_v$ and sends the diagonal to 0, so the coordinates of $[Q-Q']$ in the formal group are divisible by $z(Q)-z(Q')=j(Q)-j(Q')$, and $[Q-Q']\in\widehat{J}(\ell^2\mathcal{O}_v)$. For $p=11$, $\widehat{J}(25\mathcal{O}_v)=5\widehat{J}(5\mathcal{O}_v)\subseteq 5J(K_v)$, on which δ_v vanishes (Proposition 3.7). For $p=23,29$, $\widehat{J}(\ell^2\mathcal{O}_v)\subseteq\lambda\widehat{J}(\ell\mathcal{O}_v)$ by (F1) of Lemma 3.16, on which δ_v vanishes by (F3). (c) The polynomial $G_{11}(x,1728)$ is the square of a sextic H_6 whose reduction modulo 5 is squarefree (a product of two distinct irreducible cubics), the reduced j-map has ramification index 2 at each root x_R of H_6, and ∂_jG_{11}, $\mathcal{B}_{11}$ and $2y+1$ are units at x_R. Writing $x=x_R+5sz$ and $j-1728=-25ws^2$, the equation $G_{11}=0$ divided by $25s^2$ reduces modulo 5 to $H_6'(x_R)^2z^2-w\,\partial_jG_{11}(x_R,1728)$, whose roots z_0 are simple since both coefficients are units. Hensel's lemma gives $z=Z(5s)$ with Z integral, so $x=x_R+5sZ(5s)$, and y is integral along the branch since $2y_R+1$ is a unit. The formal parameter $-x/y$ of $P(s)-P(s')$ has valuation $1+v_5(s-s')$, so for $s\equiv s' \pmod 5$ the difference lies in $\widehat{J}(25\mathcal{O}_v)\subseteq 5J(K_v)$. Galois permutes the twelve branches through its action

on their coefficients, independently of s, so a branch is defined over K_v for one $s \neq 0$ if and only if it is defined over K_v for all $s \neq 0$. □

Lemma 4.7. *Let $p = 17$, let $\theta = -1 + 2i$ be as in Section 3.4, let $v \mid 2$ and let $x, x' \in K_v$ with $x' \neq \theta$ in every L_w, $w \mid v$. Put*

$$r(x') = \max_{w|v} \Big(v_2(x' - \theta)_w + 2 + \frac{1}{e_w} \Big),$$

where $v_2(\cdot)_w$ is computed in L_w and e_w is the ramification index of $L_w/\mathbb{Q}_2$. If $v_2(x - x') \geq r(x')$, then $x - \theta$ and $x' - \theta$ have the same class in $\prod_{w|v} L_w^\times / L_w^{\times 2}$.

Proof. The quotient $(x-\theta)/(x'-\theta)$ is $1+z$ with $z = (x-x')/(x'-\theta)$ and $v_2(z) \geq 2 + 1/e_w$ in L_w. Every element of $1 + \pi_w^{2e_w+1}\mathcal{O}_{L_w}$ is a square in L_w, because the binomial series for $(1 + 4\pi_w u)^{1/2}$ converges. □

Lemma 4.8. *Let $p = 19$ and $v \mid 3$, and let $\widehat{J}(v^m)$ be the group of points of $J(K_v)$ in the formal group with parameter $t = -x/y$ of normalized valuation at least m. Then $\widehat{J}(v^N) \subseteq \hat{\phi}(J'(K_v)) = \ker \delta_v$ for $N = \lfloor 3e_v/2 \rfloor + 1$. Consequently, if $P_\xi = (\xi, y_\xi) \in J(K_v)$ has ξ, y_ξ integral and $2y_\xi + 1$ a unit, and $Q \in J(K_v)$ reduces to the same point as P_ξ and satisfies $v_v(x(Q) - \xi) \geq N$, then $\delta_v(Q) = \delta_v(P_\xi)$.*

Proof. For $k > e_v/2$ the formal logarithm is an isometry from $\widehat{J}(v^k)$ onto v^k [59, Theorem IV.6.4], so $[3]\widehat{J}(v^k) = \widehat{J}(v^{k+e_v})$. With $k = N - e_v = \lfloor e_v/2 \rfloor + 1$ this gives $\widehat{J}(v^N) = [3]\widehat{J}(v^k) = \hat{\phi}\phi\widehat{J}(v^k) \subseteq \hat{\phi}(J'(K_v))$. As $2y_\xi + 1$ is a unit, $x - \xi$ is a uniformizer of the smooth model at the reduction of P_ξ, and translation by $-P_\xi$ maps the residue disc of P_ξ to that of O, so $v_v(t(Q - P_\xi)) = v_v(x(Q) - \xi) \geq N$ and $Q - P_\xi \in \widehat{J}(v^N)$. □

4.4. **The disc test.** The disc test combines the location of the points with the radii of constancy, and is applied to sets $D \subseteq \mathbb{Q}_\ell$ of j-values of the following kinds, each with a representative $j_D \in D$: (1) for $p = 11$, a disc $j_1 + 25\mathbb{Z}_5$ as in Lemma 4.6(a), with $j_D = j_1$, or a set $\{1728 - 25ws^2 : s \in s_1 + 5\mathbb{Z}_5\}$ as in Lemma 4.6(c), with j_D the value at $s = s_1$; (2) for $p = 17$, a family with $e = 1$, with $j_D = j_c$, or a *half-family*, the values $j_c + \kappa t^e$ of a family with t even, or with t odd, with j_D the value at $t = 0$ or $t = 1$; (3) for $p = 19$, a family, with $j_D = j_c$; (4) for $p = 23, 29$, a disc $j_1 + \ell^2\mathbb{Z}_\ell$ with $j_1 = r + \ell t$, $r \in \mathcal{J}(E) \setminus \{0, 1728\}$ and $0 \leq t < \ell$ (Lemma 9.1), with $j_D = j_1$, or a set in a ramified region. For each $w_1 \in \{1, \dots, \ell - 1\}$, the j-values $j_c + \varsigma\ell^{ek}w$ with $w \equiv w_1 \pmod{\ell}$ and depth $k = 1$ form one such set, and those with depth $k \geq 2$ another, with $j_D = j_c + \varsigma\ell^{ek_1}w_1$ and $k_1 = 1$, respectively $k_1 = 2$. For $v \mid \ell$ let $C_{D,v} \subseteq H_v$ be the set of classes $\delta_v(R)$ of the points $R \in X_0(p)(K_v)$ over j_D (for $p = 17$, the classes of $x' - \theta$ for the roots $x' \in K_v$ of $G_{17}(x, j_D)$). A tuple in $\prod_{v|\ell} C_{D,v}$ is a *class tuple* of D. The class tuple of an admissible configuration $(R_v)_{v|\ell}$ over j_D (Definition 2.13) is $(\delta_v(R_v))_{v|\ell}$.

Proposition 4.9. *Let D be a set of j-values as above. For $p \in \{11, 17, 19\}$ let $Q \in J(K) \setminus J(\mathbb{Q})$ with $j(Q) \in D \cap \mathbb{Q}$. For $p \in \{23, 29\}$ assume that $\ell \nmid h_K$, and let $Q = P \in X_0(p)(K)$ be the point of Proposition 2.12 attached to a solution with $j_0 \in D$. Assume:*

- *for $p = 11$: the hypotheses of Lemma 4.6(a) or (c);*
- *for $p = 17$: (i)–(iv) and (4.1) hold at every root of $G_{17}(x, j_c)$. If $j_D \neq j_c$, then $e_\xi = 1$ at every root ξ. There is an integer $k \geq 0$ such that $v_2(\tau_\xi - \tau_\xi^D) \geq k$ for every t giving a value in D, where τ_ξ^D is the value of τ_ξ at the representative, and $\nu_\xi + k \geq r(x')$ for every root ξ and every root $x' \in K_v$ of $G_{17}(x, j_D)$ in the disc about ξ;*

- *for $p = 19$:* (i)–(iv) *and* (4.1) *hold at every root ξ of $G_{19}(x, j_c)$, with $\nu_\xi \geq 2$, and ξ and y_ξ are integral, $2y_\xi + 1$ is a unit and $v_3(\mathcal{B}_{19}(\xi)) < \min(\nu_\xi, v_3(\kappa))$ at every K_v-rational root;*
- *for $p = 23, 29$: if D is a disc $j_1 + \ell^2\mathbb{Z}_\ell$, then $G_p(x, j_1)$ is separable modulo ℓ.*

Then $(\delta_v(Q_v))_{v|\ell}$ lies in Σ and is a class tuple of D. For $p \in \{11, 23, 29\}$ it is the class tuple of an admissible configuration over j_D that corresponds to $(Q_v)_{v|\ell}$ residue disc by residue disc, or, in a ramified region, that has the labels of $(Q_v)_{v|\ell}$. In particular, if no such class tuple of D lies in Σ, no such Q exists.

Proof. For $p \in \{11, 17, 19\}$ the tuple lies in Σ by Section 3. For $p \in \{23, 29\}$, j_0 is ℓ-integral by Lemma 9.1, so $\delta([P - \infty]) = f(P) \in K(S, \ell)$ by Proposition 3.14(a),(b), and $(P_v)_{v|\ell}$ is an admissible configuration over j_0 by Proposition 2.12. Let $v \mid \ell$.

For $p = 17, 19$, $x(Q_v)$ is a root of $G_p(x, j(Q))$, and Lemma 4.4(c) puts it in the disc about a root $\xi \in K_v$ of $G_p(x, j_c)$. For $p = 17$, let x' be the root of $G_{17}(x, j_D)$ in the same disc given by the representative. If $j_D = j_c$, then $x' = \xi$ and $v_2(x(Q_v) - \xi) = \nu_\xi + v_2(\tau_\xi) \geq \nu_\xi + k$ by Lemma 4.4(a). Otherwise $e_\xi = 1$, x' is the value of the branch through ξ at the representative. This value lies in K_v by Lemma 4.4(c), and $v_2(x(Q_v) - x') \geq \nu_\xi + k$ by Lemma 4.4(b). In both cases $x' \in K_v$ and $v_2(x(Q_v) - x') \geq r(x')$, so $\delta_v(Q_v) \in C_{D,v}$ by Lemma 4.7. For $p = 19$, $v_3(x(Q_v) - \xi) \geq \nu_\xi \geq 2 \geq N/e_v$ by Lemma 4.4(a). The y-coordinate $(j(Q)(x - 5)^{19} - \mathcal{A}_{19}(x))/\mathcal{B}_{19}(x)$ of Q_v differs from y_ξ by an element of positive valuation, since its numerator and denominator differ from those at ξ by elements of valuation at least $\min(\nu_\xi, v_3(\kappa))$. So Q_v is in the residue disc of the point $P_\xi = (\xi, y_\xi)$ over $j_D = j_c$, and $\delta_v(Q_v) = \delta_v(P_\xi)$ by Lemma 4.8.

For $p \in \{11, 23, 29\}$ and D a disc, Lemma 4.6(a) puts one point over $j(Q)$ and one over j_D in every residue disc, with the same factorization of the fibre over $\mathbb{Q}_\ell$, and by Lemma 4.6(b) the two points of a residue disc have the same class, as $j(Q) \equiv j_D \pmod{\ell^2}$. By Lemma 2.10 for $p = 11$ and Proposition 2.12 for $p = 23, 29$, $K \otimes \mathbb{Q}_\ell = \prod_{v|\ell} K_v$ is $\mathbb{Q}_\ell[x]/(G_p(x, j(Q)))$. So the $x(Q_v)$ are roots of distinct irreducible factors of $G_p(x, j(Q))$ over $\mathbb{Q}_\ell$, and the factor at v defines K_v. The corresponding points over j_D form an admissible configuration with the same class tuple. For the sets of Lemma 4.6(c) the same argument runs along the branches, whose classes depend only on $s \bmod 5$. In a ramified region, the admissible configurations, described by labels, are the same over j_0 and over j_D by Lemma 4.5(c). By Lemma 4.5(d), the class of a K_v-point depends only on its label at depth 1, and is $\delta_v(\rho_i)$ at depth $k \geq 2$. □

The *disc test* lists the class tuples of D (for $p \in \{11, 23, 29\}$, those of admissible configurations over j_D) that lie in Σ. This is the test of Freitas, Naskręcki and Stoll [27, Lemma 7.7], made explicit for every e by Lemma 4.1 and extended to the ramified regions by Lemma 4.5. For $p = 23, 29$ the sets tested are the ℓ discs of (4) for each $r \in \mathcal{J}(E) \setminus \{0, 1728\}$ and, for each ramified region that occurs, the $2(\ell - 1)$ sets given by a residue $\bar{w}$ and depth 1 or depth ≥ 2. The points over j_D are located in each K_v by Hensel's lemma, to a precision far above the radius of constancy, and their classes are computed exactly (Appendix B.1).

When ℓ has two places of degree 1 and eleven of degree 2 in K (the fields K_{27a1} and K_{288a1} at $p = 23$), the fibre over each representative in the ramified regions has two Frobenius orbits of size 1 and eleven of size 2. An admissible configuration puts the orbits of size 1 at the places of degree 1 and those of size 2 at the places of degree 2, and chooses one of the two K_v-points of the orbit at each place of degree 2, so there are

$$2 \cdot 11! \cdot 2^{11} = 163\,499\,212\,800 \approx 1.6 \cdot 10^{11}$$

admissible configurations per set, searched by meeting in the middle. The localization is injective, so Σ has dimension 13 in $\bigoplus_{v\mid 11} k_v \simeq \mathbb{F}_{11}^{24}$ (Proposition 3.14(c)). Let W_v be the columns at v of an 11×24 matrix over $\mathbb{F}_{11}$ with kernel Σ, and split the thirteen places into sets V_1, V_2. An admissible configuration is, in exactly one way, a pair of choices of points on V_1 and on V_2 with disjoint sets of orbits, and its class tuple lies in Σ exactly when the two partial sums $\sum_{v\in V_i} W_v\,\delta_v(R_v)$ add up to 0. So the choices on V_2 are sorted by set of orbits and partial sum, and each choice on V_1 is matched against them. When D contains the j-invariant of a known point P_0, the class tuple of P_0 lies in Σ, and Section 5 treats D.

5. Discs that contain a known point

We show that, under conditions checked by computation, a known point P_0 is the only point with rational j-invariant in the set of the disc test that contains $j(P_0)$, and we give a sieve at primes of good reduction for the Selmer classes that remain (Section 5.6).

5.1. **Stoll's criterion and global divisibility.** We state Stoll's theorem [64, Theorem 2.1] with an endomorphism in place of multiplication by ℓ, as [64, Remark 2.2] allows, with any nonempty set of places above ℓ.

Proposition 5.1 (Stoll)**.** *Let A be an abelian variety over a number field F, let ℓ be a prime, and let ϖ be an endomorphism of A over F such that ϖ^{n_0} is ℓ times an automorphism of A for some $n_0 \geq 1$. Let $\mathcal{P}$ be a nonempty finite set of primes of F above ℓ, put $A(F_\mathcal{P}) \coloneqq \prod_{\mathfrak{p}\in\mathcal{P}} A(F_\mathfrak{p})$, and let*

$$\delta\colon A(F)/\varpi A(F) \hookrightarrow \mathcal{H}, \qquad \delta_\mathcal{P}\colon A(F_\mathcal{P})/\varpi A(F_\mathcal{P}) \to \mathcal{H}_\mathcal{P}, \qquad \mathrm{loc}_\mathcal{P}\colon \mathcal{H} \to \mathcal{H}_\mathcal{P}$$

be homomorphisms of abelian groups with δ injective and $\mathrm{loc}_\mathcal{P}\circ\delta = \delta_\mathcal{P}\circ$ (restriction). Let $\mathrm{Sel} \subseteq \mathcal{H}$ be a subgroup containing $\delta(A(F))$, and $\Gamma \subseteq A(F)$ a finite subgroup with $\varpi(\Gamma) \subseteq \Gamma$. For $D \in A(F_\mathcal{P})$ put

$$\mathcal{Q}(D) \coloneqq \{\delta_\mathcal{P}(R)\colon R \in A(F_\mathcal{P}),\ \varpi^n R = D \text{ for some } n \geq 0\}.$$

Let $\mathcal{X}$ be a curve over F, $\iota\colon \mathcal{X} \to A$ a morphism, and $\mathcal{U} \subseteq \mathcal{X}(F_\mathcal{P})$ a subset. Assume

(1) *$\mathrm{loc}_\mathcal{P}$ is injective on Sel;*
(2) *for every $Q \in \mathcal{U}$ and $\mathfrak{s} \in \Gamma$, $\mathcal{Q}(\iota(Q)+\mathfrak{s}) \cap \mathrm{loc}_\mathcal{P}(\mathrm{Sel}) \subseteq \delta_\mathcal{P}(\Gamma)$.*

Then $\iota(Q) \in A(F)_{\mathrm{tors}}$ for every $Q \in \mathcal{X}(F)$ whose image in $\mathcal{X}(F_\mathcal{P})$ lies in $\mathcal{U}$.

Proof. We follow [64, proof of Theorem 2.1]. Let $Q \in \mathcal{X}(F)$ with image in $\mathcal{U}$. We show by induction that for every $n \geq 0$ there are $\mathfrak{s}_n \in \Gamma$ and $R_n \in A(F)$ with $\iota(Q) = \mathfrak{s}_n + \varpi^n R_n$. For $n = 0$ take $\mathfrak{s}_0 = 0$ and $R_0 = \iota(Q)$. Given $\mathfrak{s}_n$ and R_n, we have $\varpi^n R_n = \iota(Q) - \mathfrak{s}_n$, so $\delta_\mathcal{P}(R_n) \in \mathcal{Q}(\iota(Q) - \mathfrak{s}_n)$. Also $\delta_\mathcal{P}(R_n) = \mathrm{loc}_\mathcal{P}(\delta(R_n)) \in \mathrm{loc}_\mathcal{P}(\mathrm{Sel})$. By (2), $\delta_\mathcal{P}(R_n) = \delta_\mathcal{P}(\mathfrak{s}')$ for some $\mathfrak{s}' \in \Gamma$, so $\mathrm{loc}_\mathcal{P}(\delta(R_n - \mathfrak{s}')) = 0$, and by (1) and the injectivity of δ, $R_n - \mathfrak{s}' = \varpi R_{n+1}$ for some $R_{n+1} \in A(F)$. Then $\iota(Q) = \mathfrak{s}_{n+1} + \varpi^{n+1} R_{n+1}$ with $\mathfrak{s}_{n+1} = \mathfrak{s}_n + \varpi^n \mathfrak{s}' \in \Gamma$. The group $A(F)/A(F)_{\mathrm{tors}}$ is free of finite rank, Γ is torsion, and $\varpi^{mn_0} A(F) = \ell^m A(F)$. So the image of $\iota(Q)$ in $A(F)/A(F)_{\mathrm{tors}}$ lies in ℓ^m times this group for every m, and hence is 0. □

In Part III, A is the Jacobian of $Y^2 = X^5 + \beta$, $\ell = 5$ and $\varpi = \pi = 1 - \zeta$, ζ a primitive fifth root of unity, and π^4 is 5 times a unit of $\mathbb{Z}[\zeta]$ because $5 = \prod_{a=1}^{4}(1-\zeta^a)$. With $\varpi = [\ell]$ and $n_0 = 1$, Proposition 5.1 is [64, Theorem 2.1]. The Eisenstein prime λ of Section 3.5 does not satisfy the hypothesis on ϖ ($\ell = \lambda\mu$ with λ and $\mu\mathcal{O}$ distinct primes), and in Part II the division stops after finitely many steps, at which a computed class is excluded (Lemma 5.2).

Let V be an abelian group with an endomorphism ϖ and a subgroup W. The *level* of $D \in V$ modulo W is

$$\operatorname{lev}(D) := \sup\{n \geq 0 \colon D \in \varpi^n V + W\} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

When $W = 0$ we speak of the level of D. In Part III, $V = J_{\mathcal{C}}(F_{\mathfrak{P}})$, $\varpi = \pi$ and $W = 0$. In Part II, $V = J(K_v)$, $\varpi = [\ell]$ or λ, and W is the torsion subgroup of $J(K_v)$ or $\langle T \rangle$. Suppose that

$$Y \in V \text{ and } \varpi Y \in W \implies Y \in W. \tag{5.1}$$

If D has level at least m modulo W and $Y, Y' \in V$ satisfy $\varpi^m Y, \varpi^m Y' \in D + W$, then $\varpi^m(Y - Y') \in W$, so $Y - Y' \in W$ by (5.1) applied m times. So for a homomorphism δ_v on V that vanishes on ϖV, the class of $\delta_v(Y)$ modulo $\delta_v(W)$ depends only on D and m. We call it the *class of D at level m*, and write $\mathrm{cl}_m(D)$.

Lemma 5.2 (global divisibility)**.** *Let A be an abelian variety over a number field K, ϖ an endomorphism of A over K, and $\mathcal{P}$ a finite set of places of K. For $v \in \mathcal{P}$ write $V_v = A(K_v)$ and R_v for the image of $R \in A(K)$ in V_v. Let $\delta \colon A(K) \to \mathcal{H}$ and $\delta_v \colon V_v \to \mathcal{H}_v$ be homomorphisms that vanish on $\varpi A(K)$ and on ϖV_v, and $\mathrm{loc} \colon \mathcal{H} \to \bigoplus_{v \in \mathcal{P}} \mathcal{H}_v$ a homomorphism with $\mathrm{loc}(\delta(R)) = (\delta_v(R_v))_{v \in \mathcal{P}}$. Let $\Gamma \subseteq A(K)$ be a subgroup with $\varpi\Gamma \subseteq \Gamma$, and for $v \in \mathcal{P}$ let $W_v \subseteq V_v$ be a subgroup that contains the image of Γ. Put $\Theta = \bigoplus_{v \in \mathcal{P}} \delta_v(W_v)$. Assume:*

(G) *every $R \in A(K)$ with $R_v \in \varpi V_v + W_v$ for all $v \in \mathcal{P}$ lies in $\varpi A(K) + \Gamma$;*
(L) *for every $v \in \mathcal{P}$, W_v satisfies (5.1) in V_v.*

Let $D \in A(K)$ and $m \geq 0$, and suppose that D_v has level at least m modulo W_v for every $v \in \mathcal{P}$. Then $D = \varpi^m R + \mathfrak{s}$ with $R \in A(K)$ and $\mathfrak{s} \in \Gamma$. If $Y_v \in V_v$ are points with $\varpi^m Y_v \in D_v + W_v$ for every $v \in \mathcal{P}$, then $Y_v - R_v \in W_v$, so

$$(\delta_v(Y_v))_{v \in \mathcal{P}} \in \mathrm{loc}(\delta(R)) + \Theta.$$

In particular $(\mathrm{cl}_m(D_v))_{v \in \mathcal{P}}$ is the class of $\mathrm{loc}(\delta(R))$ modulo Θ, and it lies in $(\Sigma + \Theta)/\Theta$ for every subgroup Σ of $\bigoplus_v \mathcal{H}_v$ that contains $\mathrm{loc}(\delta(A(K)))$.

Proof. We show by induction on $i = 0, \ldots, m$ that $D = \varpi^i R_i + \mathfrak{s}_i$ with $R_i \in A(K)$ and $\mathfrak{s}_i \in \Gamma$. For $i = 0$ take $R_0 = D$ and $\mathfrak{s}_0 = 0$. Let $i < m$ and $v \in \mathcal{P}$, and write $D_v = \varpi^m Y + w$ with $Y \in V_v$ and $w \in W_v$. Then $\varpi^i(R_{i,v} - \varpi^{m-i} Y) = w - \mathfrak{s}_{i,v} \in W_v$, so $R_{i,v} - \varpi^{m-i} Y \in W_v$ by (L) applied i times, and $R_{i,v} \in \varpi V_v + W_v$ because $m - i \geq 1$. By (G), $R_i = \varpi R_{i+1} + \mathfrak{s}'$ with $R_{i+1} \in A(K)$ and $\mathfrak{s}' \in \Gamma$, and $D = \varpi^{i+1} R_{i+1} + \mathfrak{s}_i + \varpi^i \mathfrak{s}'$ with $\mathfrak{s}_i + \varpi^i \mathfrak{s}' \in \Gamma$. Put $R = R_m$ and $\mathfrak{s} = \mathfrak{s}_m$. If $\varpi^m Y_v \in D_v + W_v$, then $\varpi^m(Y_v - R_v) \in \mathfrak{s}_v + W_v = W_v$, so $Y_v - R_v \in W_v$ by (L), and $\delta_v(Y_v) \in \delta_v(R_v) + \delta_v(W_v)$. □

Lemma 5.2 is applied in Lemmas 5.3 and 5.7 ($\varpi = [\ell]$, W_v the local torsion), in case (i) of Lemmas 5.9 and 5.10 ($\varpi = \lambda$, $W_v = \langle T \rangle$), and in Step 2 of the proof of Proposition 6.4 ($\varpi = [5]$, $W_v = \langle T \rangle$). Case (ii) of Lemmas 5.9 and 5.10 uses Lemma 3.20, proved by the same induction with Proposition 3.18 in place of (G).

5.2. **The logarithm modulo local torsion.** At $p = 17$ the division by 2 is not unique: unlike $X_0(11)(K_v)$ in [27, Lemma 7.8], $J(K_v)$ has 2-power torsion, for instance the point $2T \in J(\mathbb{Q})$ of order 2. So we work modulo all local torsion, through the logarithm, here and at $\ell = 3$ for $p = 19$ (Section 5.3).

Let $p = 17$, $K = K_E$ with $E \in \{864\mathrm{b}1, 864\mathrm{c}1\}$, and $V_v = J(K_v)$ for $v \mid 2$. The residue fields of K above 2 are $\mathbb{F}_2$ and $\mathbb{F}_4$ (Table 6), and the reduction of J at 2 has 4 points

over $\mathbb{F}_2$ and 8 over $\mathbb{F}_4$, so V_v is a pro-2 group, $V_v \simeq \mathbb{Z}_2^{n_v} \times V_{v,\mathrm{tors}}$ with $V_{v,\mathrm{tors}}$ finite. Put $\bar{V}_v = V_v/V_{v,\mathrm{tors}}$ and $\bar{V} = \bigoplus_{v|2} \bar{V}_v$, and let $\overline{J(K)}$ be the image of $J(K)$ in $\bar{V}$.

Let $\mathcal{F}_v \subseteq V_v$ be the group of points of the formal group with $v_2(t) > 1$, where $t = -x/y$. The formal logarithm is an isometric isomorphism from $\mathcal{F}_v$ onto $\{z \in K_v : v_2(z) > 1\}$ [59, Theorem IV.6.4]. For $Y \in V_v$ put $\mathrm{Log}_v(Y) = 2^{-a}\log(2^a Y)$ with a large enough that $2^a Y \in \mathcal{F}_v$. This homomorphism has kernel $V_{v,\mathrm{tors}}$ and image a $\mathbb{Z}_2$-lattice Λ_v of rank n_v containing $\{z : v_2(z) > 1\}$. So Log_v identifies $\bar{V}_v$ with Λ_v, and the level of $Y \in V_v$ modulo $V_{v,\mathrm{tors}}$ (with $\varpi = [2]$) is the largest d with $\mathrm{Log}_v(Y) \in 2^d\Lambda_v$.

Let δ_v be the local Kummer map of Lemma 3.9, injective on $V_v/2V_v$, and $\Theta_v = \delta_v(V_{v,\mathrm{tors}})$. As $V_{v,\mathrm{tors}} \cap 2V_v = 2V_{v,\mathrm{tors}}$,

$$\Lambda_v/2\Lambda_v \simeq \bar{V}_v/2\bar{V}_v \simeq \delta_v(V_v)/\Theta_v.$$

Put $\Theta = \bigoplus_{v|2}\Theta_v$, and let $\Sigma \subseteq \bigoplus_{v|2}\delta_v(V_v)$ be the image of $\mathrm{Sel}^2(J/K)$, on which the restriction is injective (Proposition 3.11). For $S \in J(K)$ whose image $\bar{S}$ lies in $2^m\bar{V}$, the tuple $\mathrm{cl}_m(S) \coloneqq (\mathrm{cl}_m(S_v))_{v|2}$ of Section 5.1 is the class in $\bar{V}/2\bar{V} = \bigoplus_v \delta_v(V_v)/\Theta_v$ of any $R' \in \bar{V}$ with $2^m R' = \bar{S}$.

Lemma 5.3 (global divisibility at 2)**.** *Assume that $\Sigma \cap \Theta = \{0, \delta(T)|_2\}$. Let $S \in J(K)$ with image $\bar{S} \in 2^m\bar{V}$. Then $S = 2^m R + \mathfrak{s}$ with $R \in J(K)$ and $\mathfrak{s} \in \langle T\rangle$, so $\bar{S} \in 2^m\overline{J(K)}$, and $\mathrm{cl}_m(S) \in (\Sigma + \Theta)/\Theta$.*

Proof. Apply Lemma 5.2 with $\varpi = [2]$, $\mathcal{P}$ the places above 2, $W_v = V_{v,\mathrm{tors}}$ and $\Gamma = \langle T\rangle$. (L) holds because $2Y$ torsion implies Y torsion. For (G), let $R \in J(K)$ with $R_v \in 2V_v + V_{v,\mathrm{tors}}$ for every $v \mid 2$. Then $\delta_v(R) \in \Theta_v$, so $\delta(R)|_2 \in \Sigma \cap \Theta = \{0, \delta(T)|_2\}$. Since $\mathrm{Sel}^2(J/K) \to \bigoplus_{v|2}\delta_v(V_v)$ and $J(K)/2J(K) \to \mathrm{Sel}^2(J/K)$ are injective, $R \in 2J(K)$ or $R - T \in 2J(K)$. The hypothesis $\bar{S} \in 2^m\bar{V}$ says that S_v has level at least m modulo $V_{v,\mathrm{tors}}$ at every $v \mid 2$. So $S = 2^m R + \mathfrak{s}$, $\bar{S} = 2^m\bar{R}$, and $\mathrm{cl}_m(S)$ is the class of $\delta(R)|_2 \in \Sigma$. □

For the two fields, $J(K)_{\mathrm{tors}} = \langle T\rangle \simeq \mathbb{Z}/4$, over which the point $\mathfrak{s}$ of Lemma 5.3 runs. Here $J(K)[2] = \{O, 2T\}$ since $i \notin K$. The points $Y \neq \pm T$ with $2Y = 2T$ are defined over $K(i)$ only. A point Y with $2Y = \pm T$ would be defined over a subfield of K of degree at most 4, hence over $\mathbb{Q}$ by Proposition 2.8(c), which is impossible as $J(\mathbb{Q}) = \mathbb{Z}/4$. There is no odd torsion, as $J(K_v)$ is pro-2 for $v \mid 2$. Let $j_c, \kappa \in \mathbb{Q}$, and consider the family $\{j_c + \kappa\tau : \tau \in \mathbb{Z}_2\}$ with $e = 1$. For $\xi \in J(K_v)$ over j_c at which Lemma 4.2 applies with $e = 1$, let $x(\xi) + X_\xi$ be the branch through $x(\xi)$, and for $\tau \in \mathbb{Z}_2$ let $\xi(\tau)$ be the point of J over $j_c + \kappa\tau$ with x-coordinate $x(\xi) + X_\xi(\tau)$ (well defined by the next lemma).

Lemma 5.4 (branches through a known point)**.** *Let $\xi \in J(K_v)$ lie over j_c, with $x(\xi)$ integral. Suppose that* (i)–(iv) *and* (4.1) *hold, with $e = 1$, at every point over j_c, let c_ξ be the linear coefficient of X_ξ, and let $\nu = v_2(c_\xi)$. Suppose that $\nu > 0$, that $2y + x + 1$ is a unit at ξ, that $x(\xi) \not\equiv x_{17}^0 = 7$ modulo the maximal ideal, and that $j(-\xi) \neq j_c$. Then $\xi(\tau) - \xi$ lies in the formal group, and $t_\xi(\tau) = t(\xi(\tau) - \xi)$ is a power series converging on $|\tau| \leq 1$ whose Gauss norm $2^{-\nu}$ is attained at its linear coefficient. If $\nu > 1$, then*

$$\mathcal{L}_\xi(\tau) \coloneqq \mathrm{Log}_v(\xi(\tau)) - \mathrm{Log}_v(\xi) = \log t_\xi(\tau) = \sum_{k\geq 1}\gamma_k\tau^k, \qquad v_2(\gamma_1) = \nu, \quad v_2(\gamma_k) \geq \nu \ (k \geq 2).$$

Proof. In the residue disc of ξ the function $z = x - x(\xi)$ is a coordinate, since the partial derivative $2y + x + 1$ of the equation of J with respect to y is a unit at ξ, and $y = y(\xi) + w(z)$ with $w \in z\mathcal{O}_v[[z]]$. The chord formula gives $t(R - \xi) = \mathcal{T}(z)$ with $\mathcal{T} \in z\mathcal{O}_v[[z]]$ and

$\mathcal{T}'(0) = 1/(2y(\xi)+x(\xi)+1)$, a unit. Let $R^*(\tau)$ be the point of the residue disc of ξ with $z = X_\xi(\tau)$. The residue discs of $\pm\xi$ contain no cusp, as $x(\pm\xi)$ is integral and $\not\equiv 7$, so $\tau \mapsto j(\pm R^*(\tau))$ are power series converging on $|\tau| \le 1$. As $\pm R^*(\tau)$ have the same x-coordinate, one of them lies over $j_c + \kappa\tau$, so $(j(R^*(\tau)) - j_c - \kappa\tau)(j(-R^*(\tau)) - j_c - \kappa\tau)$ vanishes on $\mathbb{Z}_2$, hence identically by Strassmann's theorem. The ring of power series converging on the closed unit disc is a domain, and the second factor is $j(-\xi) - j_c \neq 0$ at $\tau = 0$, so $j(R^*(\tau)) = j_c + \kappa\tau$. The 18 points over $j_c + \kappa\tau$ have x-coordinates in disjoint discs (Lemma 4.4(a)), so $\xi(\tau) = R^*(\tau)$ and $t_\xi = \mathcal{T} \circ X_\xi$. By Lemma 4.2, X_ξ has Gauss norm $|c_\xi| < 1$ on the closed unit disc, attained at its linear term $c_\xi\tau$, hence so has t_ξ. Finally $\log t = \sum_{k\ge1} a_k t^k/k$ with $a_k \in \mathbb{Z}$, and for $k \ge 2$, $2^{v_2(k)}|c_\xi|^k < |c_\xi|$ when $\nu > 1$. So $\mathcal{L}_\xi = \log \circ t_\xi$ has Gauss norm $|c_\xi|$, attained at $\gamma_1 = \mathcal{T}'(0)c_\xi$. □

Lemma 5.5 (comparison)**.** *In the situation of Lemma 5.4, let $a \ge 1$, and let $\tau = 2^n u$ and $\tau_0 = 2^{n_0}u_0$ with $u, u_0 \in \mathbb{Z}_2^\times$, $u \equiv u_0 \pmod{2^a}$, and either $n = n_0$ or $n, n_0 \ge a$. Then $v_2(2^{-n}\mathcal{L}_\xi(\tau) - 2^{-n_0}\mathcal{L}_\xi(\tau_0)) \ge \nu + a$. In particular, if $n = n_0$ then $\mathcal{L}_\xi(\tau) - \mathcal{L}_\xi(\tau_0) \in 2^k\Lambda_v$ for every integer $k \le \nu + a + n_0 - 2$.*

Proof. The statement is symmetric in (n, u) and (n_0, u_0), so we may assume $n \ge n_0$. The difference is $\gamma_1(u - u_0) + \sum_{k\ge2} \gamma_k 2^{(k-1)n_0}(2^{(k-1)(n-n_0)}u^k - u_0^k)$. The first term has valuation at least $\nu + a$. For $k \ge 2$, the bracket is divisible by $u - u_0$ if $n = n_0$, and $2^{(k-1)n_0}$ has valuation at least a if $n, n_0 \ge a$. For the last statement, an element of valuation at least $\nu + a + n_0$ lies in $2^k\{z : v_2(z) \ge 2\} \subseteq 2^k\Lambda_v$. □

5.3. **The logarithm at the prime 3.** For $p = 19$ the argument of Section 5.2 runs at $\ell = 3$ with the descent of Section 3.3. Let $K = K_E$ be one of the six fields of degree 20, and for $v \mid 3$ let $V_v = J(K_v)$ and M_v the exponent of $\widetilde{J}(k_v)$. The formal logarithm is an isometric isomorphism from $\widehat{J}(v^k)$ onto v^k for $k > e_v/2$, and we put $\mathrm{Log}_v(Y) = (3^a M_v)^{-1}\log(3^a M_v Y)$ for a large. Its image Λ_v is a $\mathbb{Z}_3$-lattice of rank n_v containing $\{z : v_v(z) \ge \lfloor e_v/2\rfloor + 1\}$, so an element of v_3-valuation at least c lies in $3^k\Lambda_v$ for $k = \lfloor c - (\lfloor e_v/2\rfloor + 1)/e_v\rfloor$. Here δ_v is the Kummer map of $\hat\phi$, $\Theta_v = \delta_v(V_{v,\mathrm{tors}})$, Σ is the image of $\mathrm{Sel}(K)$ at 3, and Θ, $\bar V_v$, $\bar V$ and $\overline{J(K)}$ are defined as at $\ell = 2$.

Lemma 5.6. *If $T \notin 3V_v$, then $\hat\phi(J'(K_v)) = 3V_v + \langle T\rangle$. Consequently, if $Y_1, \dots, Y_r \in V_v$ have classes spanning $\delta_v(V_v)$, then $\mathrm{Log}_v Y_1, \dots, \mathrm{Log}_v Y_r$ span Λ_v over $\mathbb{Z}_3$, and Θ_v consists of the combinations $\sum c_i\delta_v(Y_i)$ with $\sum c_i \mathrm{Log}_v Y_i \in 3\Lambda_v$.*

Proof. Both groups contain $3V_v + \langle T\rangle$, since $\delta_v(T)$, the class of $-1/19$, is trivial ($19 \equiv 1 \pmod 9$). Both have index $3^{n_v + \dim \mu_3(K_v)}$ in V_v: the first by Proposition 3.8(a), the second because $\#V_v/3V_v = 3^{n_v}\#V_v[3]$ and $V_v[3] = \langle T\rangle \oplus C(K_v)$ with $C(K_v) \simeq \mu_3(K_v)$. The rest follows by Nakayama's lemma, since $Y_1, \dots, Y_r, T$ span V_v modulo $3V_v$ and the prime-to-3 torsion. □

The hypothesis $T \notin 3V_v$ always holds: every residue field of K at a place above 3 is $\mathbb{F}_3$ or $\mathbb{F}_9$ (Table 6), and $a_3(19a1) = -2$, so $\#\widetilde{J}(\mathbb{F}_3) = 6$ and $\#\widetilde{J}(\mathbb{F}_9) = 12$, and a point Y with $3Y = T$ would reduce to a point of order 9, since T reduces to a point of order 3.

Lemma 5.7 (global divisibility at 3)**.** *Assume that $\Sigma \cap \Theta = \{0\}$. If $S \in J(K)$ and $\bar S \in 3^m\bar V$, then $\bar S \in 3^m\overline{J(K)}$, and the class $\mathrm{cl}_m(S)$ of $3^{-m}\bar S$ in $\bigoplus_v \delta_v(V_v)/\Theta_v$ lies in $(\Sigma + \Theta)/\Theta$.*

Proof. Apply Lemma 5.2 with $\varpi = [3]$, $W_v = V_{v,\mathrm{tors}}$ and $\Gamma = \langle T\rangle$. (L) holds as in Lemma 5.3. For (G), let $R \in J(K)$ with $R_v \in 3V_v + V_{v,\mathrm{tors}}$ for every $v \mid 3$. Then

$\delta_v(R) \in \Theta_v$ for every v, so $\delta(R)|_3 \in \Sigma \cap \Theta = \{0\}$. By Proposition 3.8(c), $\delta(R) \in \langle \delta(T) \rangle$, so $R \in \langle T \rangle + \hat{\phi}(J'(K)) = \langle T \rangle + 3J(K)$ by Proposition 3.8(b). □

Lemma 5.8 (branches and comparison at 3)**.** *Let $j_c, \kappa \in \mathbb{Q}$ and $\xi \in J(K_v)$ over j_c with $x(\xi)$, $y(\xi)$ integral and $2y(\xi)+1$, $\mathcal{B}_{19}(x(\xi))$ units. Suppose that* (i)–(iv) *and* (4.1) *hold, with $e = 1$, at every point over j_c, let c_ξ be the linear coefficient of X_ξ, and suppose $\nu = v_3(c_\xi) > 1/2$. Define $\xi(\tau)$ for $\tau \in \mathbb{Z}_3$ as before Lemma 5.4. Then $\mathcal{L}_\xi(\tau) = \operatorname{Log}_v \xi(\tau) - \operatorname{Log}_v \xi = \sum_k \gamma_k \tau^k$ with $v_3(\gamma_1) = \nu$ and $v_3(\gamma_k) > \nu$ for $k \geq 2$, so $v_3(\mathcal{L}_\xi(\tau)) = \nu + v_3(\tau)$. If $a \geq 1$, $\tau = 3^n u$, $\tau_0 = 3^{n_0} u_0$ with $u, u_0 \in \mathbb{Z}_3^\times$, $u \equiv u_0 \pmod{3^a}$, and either $n = n_0$ or $n, n_0 \geq a$, then $v_3(3^{-n}\mathcal{L}_\xi(\tau) - 3^{-n_0}\mathcal{L}_\xi(\tau_0)) \geq \nu + a$.*

Proof. We follow the proof of Lemma 5.4 with the unit $2y+1$, the partial derivative of $y^2+y = x^3+x^2-9x-15$ with respect to y, in place of $2y+x+1$: $z = x - x(\xi)$ is a coordinate on the residue disc of ξ, $y = y(\xi) + w(z)$, $t(R-\xi) = \mathcal{T}(z)$ with $\mathcal{T}'(0) = 1/(2y(\xi)+1)$, and X_ξ has Gauss norm $|c_\xi| < 1$ on the closed unit disc, attained only at its linear coefficient (Lemma 4.2). The main change is the identification of $\xi(\tau)$ with the point $R^*(\tau)$ of the residue disc of ξ with $z = X_\xi(\tau)$. Put $y^*(\tau) = y(\xi) + w(X_\xi(\tau))$. The point $\xi(\tau)$ has x-coordinate $x(\tau) = x(\xi) + X_\xi(\tau)$ and y-coordinate

$$y(\tau) = \frac{(j_c + \kappa\tau)(x(\tau) - 5)^{19} - \mathcal{A}_{19}(x(\tau))}{\mathcal{B}_{19}(x(\tau))},$$

a power series converging on $|\tau| \leq 1$, since $\mathcal{B}_{19}$ is a unit near $x(\xi)$, with $y(0) = y(\xi) = y^*(0)$. Both $y(\tau)$ and $y^*(\tau)$ are roots of $Y^2+Y = x(\tau)^3+x(\tau)^2-9x(\tau)-15$, so $(y(\tau)-y^*(\tau))(y(\tau)+y^*(\tau)+1)$ vanishes on $\mathbb{Z}_3$, hence identically by Strassmann's theorem, and the second factor is $2y(\xi)+1 \neq 0$ at $\tau = 0$. So $y = y^*$ and $\xi(\tau) = R^*(\tau)$. Hence $\xi(\tau) - \xi$ lies in the formal group, where Log_v is the formal logarithm, and $t_\xi = \mathcal{T} \circ X_\xi$ has Gauss norm $|c_\xi|$, attained only at $\mathcal{T}'(0)c_\xi$. With $\log t = \sum_{k \geq 1} a_k t^k/k$, $a_k \in \mathbb{Z}$, the term $a_k t_\xi^k/k$ for $k \geq 2$ has Gauss norm at most $3^{v_3(k)}|c_\xi|^k < |c_\xi|$, because $v_3(k) \leq (k-1)/2 < (k-1)\nu$. So $\gamma_1 = \mathcal{T}'(0)c_\xi$, $v_3(\gamma_1) = \nu$, $v_3(\gamma_k) > \nu$ for $k \geq 2$, and $v_3(\mathcal{L}_\xi(\tau)) = \nu + v_3(\tau)$ as $|\tau| \leq 1$. The comparison is the computation in the proof of Lemma 5.5, with 3 in place of 2. □

5.4. **The enumeration by branch data.** Together, Lemmas 5.3, 5.4 and 5.5 at $\ell = 2$ and Lemmas 5.7 and 5.8 at $\ell = 3$ reduce the question to a finite computation over the branch data, which is carried out for each curve in Section 7.5 and Propositions 7.6 and 8.3. The example after the proof of Proposition 7.7 follows one branch datum through it.

Let $\ell \in \{2, 3\}$, let $P_0 \in J(K)$ be a known point with $j(P_0) = j_c$, and let $Q \in J(K) \setminus J(\mathbb{Q})$ with $j(Q) = j_c + \kappa\tau \in \mathbb{Q}$, $\tau \in \mathbb{Z}_\ell$. By Lemma 2.10 the fibre over $j(Q)$ is $\operatorname{Spec} K$ via Q, so $\mathbb{Q}_\ell(x(Q_v)) = K_v$. By Lemma 4.4(c) and Lemma 5.4 (Lemma 5.8 at $\ell = 3$), $Q_v = \xi_v(\tau)$ for a point $\xi_v \in J(K_v)$ over j_c, the *centre* of the branch through Q_v. Moreover $\mathbb{Q}_\ell(x(\xi_v)) = K_v$, as the branch has coefficients in $\mathbb{Q}_\ell(x(\xi_v))$ and its value $x(Q_v)$ generates K_v. The points of $J(K_v)$ over j_c whose x-coordinate generates K_v are the images of P_0 under the $\mathbb{Q}_\ell$-embeddings $K \to K_v$ whose associated place v' has $K_{v'} \simeq K_v$. For the fields to which the enumeration is applied, the completions of K above ℓ are pairwise non-isomorphic (their (e, f) differ), so $\xi_v = g_v P_{0,v}$ for some $g_v \in \operatorname{Aut}(K_v/\mathbb{Q}_\ell)$, with the same τ at every place. Since Log_v commutes with $\operatorname{Aut}(K_v/\mathbb{Q}_\ell)$,

$$\operatorname{Log}_v(Q - P_0) = (g_v - 1)\operatorname{Log}_v(P_{0,v}) + \mathcal{L}_{g_v P_{0,v}}(\tau). \tag{5.2}$$

The first term of (5.2), the *fixed term*, is independent of τ, and the second, the *branch term*, is controlled by Lemmas 5.4 and 5.5 (Lemma 5.8 at $\ell = 3$). If $\tau = 0$ then $Q = P_0$, since

$j^{-1}(j_c) \simeq \operatorname{Spec} K$ via P_0 and $\operatorname{Aut}(K)=1$. More generally, for a reference point $P_1 \in J(K)$ and $S = Q - P_1$,

$$\operatorname{Log}_v(S) = \operatorname{Log}_v(\xi_v - P_{1,v}) + \mathcal{L}_{\xi_v}(\tau).$$

This is used with $P_1 = \varsigma P_0$ for a sign ς, and with a point $P_1 = R_0$ not over j_c, whose possible centres ξ_v are all the K_v-rational points over j_c whose x-coordinate generates K_v.

A choice of the centres $(\xi_v)_{v|\ell}$ (for $P_1 = P_0$, of $(g_v)_{v|\ell}$) and of a class of $\tau = \ell^n u$, given by $n = v_\ell(\tau)$ and by u modulo ℓ^a, is a *branch datum*. It is allowed by the disc test if the classes $\delta_v(\xi_v(\tau_0))$ at a representative τ_0 of the class form a class tuple in Σ (at $\ell = 2$ these classes are constant on the class of τ by Lemma 4.7). For each allowed branch datum, the level d_v of $\operatorname{Log}_v(S)$ in Λ_v and its class modulo $\ell\Lambda_v$ are computed from the formula above at the representative. Let $c_v = 2$ if $\ell = 2$ and $c_v = (\lfloor e_v/2 \rfloor + 1)/e_v$ if $\ell = 3$, so that an element of valuation at least c lies in $\ell^k \Lambda_v$ for every integer $k \le c - c_v$. Each application fixes an integer $n_{\max}$ such that the second case below applies to every $n > n_{\max}$.

- For $n \le n_{\max}$ we take $\tau_0 = \ell^n u_0$ and compute $\operatorname{Log}_v(\xi_v(\tau_0) - P_{1,v})$ directly. By Lemma 5.5 (Lemma 5.8), the level and the class are the same for every τ in the class provided $d_v < \lfloor \nu + a + n - c_v \rfloor$, which holds in all the applications.
- For $n > n_{\max}$: at places with $\xi_v = P_{1,v}$, the branch term $\mathcal{L}_{\xi_v}(\tau)$ is ℓ^{n-n_0} times a value with the same level and class as $\mathcal{L}_{\xi_v}(\tau_0)$, where $\tau_0 = \ell^{n_0} u_0$ and $n_0 = n_{\max}$ (Lemma 5.5 with $n, n_0 \ge a$). At the other places the fixed term $\operatorname{Log}_v(\xi_v - P_{1,v})$ has level smaller than $\lfloor \nu + n - c_v \rfloor$, a lower bound for the level of the branch term, so it alone determines d_v and the class.

Then $m = \min_v d_v$, and $\operatorname{cl}_m(S)$ is read off where $d_v = m$. If this class is not in $(\Sigma + \Theta)/\Theta$ for any allowed branch datum, then Lemma 5.3 (Lemma 5.7 at $\ell = 3$) shows that no such Q with $\tau \neq 0$ exists, and for $P_1 = P_0$ that P_0 is the only point of $J(K)$ with rational j-invariant in the family. In the applications at $\ell = 2$ all the ν are integers, so the bound $\lfloor \nu + a + n - 2 \rfloor$ is $\nu + a + n - 2$. For $K_{288\mathrm{a}1}$ at $p = 19$, where the known points lie at ramification points of j and some of the completions above 3 are isomorphic, see Propositions 8.9 and 8.10.

5.5. **The λ-direction on $J_0(p)$.** For $p = 23, 29$ the division is by the Eisenstein prime λ of Section 3.5, and the local classes are read through the formal logarithm $\log_\lambda$ in the λ-direction (Lemma 3.16). Throughout, $K = K_E$ is a field of Proposition 2.8 for $p \in \{23, 29\}$ with $\ell \nmid h_K$, and the localization $K(S, \ell) \to \bigoplus_{v|\ell} k_v$ is injective with image Σ (Sections 9 and 10 show this for every field used). Let $\Theta_T = \bigoplus_{v|\ell} \mathbb{F}_\ell\, \delta_v(T)$ be the span of the local classes of T. For $v \mid \ell$ and $P_0 \in X_0(p)(K)$ let z_v be the parameter $x - x(P_0)$ at the reduction of $P_{0,v}$, or $y - y(P_0)$ if that reduction is a Weierstrass point, and let $c_{1,v} = (dj/dz_v)(P_{0,v})$.

Lemma 5.9 (known points)**.** *Let $P_0 \in X_0(p)(K)$ with $j(P_0) = j_* \in \mathbb{Q}$, and suppose that either*

(U) *$G_p(x, j_*) \bmod \ell$ is separable; put $e_0 = 0$; or*

(R) *j_* lies in region A or B at depth 1; put $e_0 = e - 1$.*

Then $v_\ell(c_{1,v}) = e_0$ at every $v \mid \ell$. For $v \mid \ell$ let $Q'_v \in X_0(p)(K_v)$ be a point in the residue disc of $P_{0,v}$ with $z_v(Q'_v) \equiv z_v(P_{0,v}) + \ell^{e_0+1}/c_{1,v} \pmod{\ell^2}$, and put $\vartheta_v = \delta_v(Q'_v) - \delta_v(P_{0,v})$ and $\vartheta = (\vartheta_v)_{v|\ell}$.

(i) *Suppose that $\delta_v(T) \neq 0$ for every $v \mid \ell$, that $\Sigma \cap \Theta_T = \mathbb{F}_\ell \cdot \delta(T)|_\ell$, and that $\vartheta \notin \Sigma + \Theta_T$.*

(ii) *Or suppose that K satisfies the hypotheses of Proposition 3.18 and that $\vartheta \notin \Sigma$.*

In either case P_0 is the only point $Q \in X_0(p)(K)$ with $j(Q) \in \mathbb{Q}$ such that, for every $v \mid \ell$, Q_v lies in the residue disc of $P_{0,v}$ and $v_\ell(z_v(Q_v) - z_v(P_{0,v})) \geq 2$.

In case (U) the last condition says that Q_v lies in the residue disc of $P_{0,v}$ for every v and $j(Q) \equiv j_* \pmod{\ell^2}$ (Lemma 4.6), and the point of that disc over $j_* + \ell$ is a valid choice of Q'_v. In case (R) it says that $j(Q)$ is at depth 1 of the same region and Q_v has the label of $P_{0,v}$ for every v (Lemma 4.5).

Proof. Fix $v \mid \ell$, write v also for the valuation v_ℓ on K_v, and write $z = z_v$, $h = z(Q_v) - z(P_{0,v})$ for a point Q_v of the disc, and $j(Q_v) - j_* = \sum_{m \geq 1} c_m h^m$. In case (U), $\tilde{\jmath}$ is étale at the reduction of $P_{0,v}$, so $v(c_1) = 0$ and $v(c_m) \geq 0$. In case (R), $j = j_c + z_i^e u(z_i)$ with z_i as in Lemma 4.5 and $v(z_i(P_{0,v})) = 1$. Expanding around $z_i(P_{0,v})$ (the change from z_i to z is a translation, or an invertible change of the same kind at a Weierstrass point) gives $v(c_1) = e - 1$ and $v(c_m) \geq \max(0, e - m)$. So in both cases $v(c_1) = e_0$ and $v(c_m) \geq \max(0, e_0 + 1 - m)$. Hence, if $s := v(h) \geq 2$, the linear term dominates: $v(j(Q_v) - j_*) = e_0 + s$ and $h \equiv (j(Q_v) - j_*)/c_1 \pmod{\ell^{2s-1}}$. Define $b_v \in \mathfrak{t}_v$ by $\langle b_v, \omega \rangle = \ell^{e_0}(\omega/dj)(P_{0,v})$ for regular differentials ω, which is integral as $v(c_1) = e_0$. As the logarithm is given by integrals of regular differentials, whose expansions at $P_{0,v}$ in z have integral coefficients,

$$\log[Q_v - P_{0,v}] \equiv (j(Q_v) - j_*)\, \ell^{-e_0} b_v \pmod{\ell^{2s-1}\mathfrak{t}_v}, \qquad 2s - 1 \geq s + 1.$$

Similarly $\log[Q'_v - P_{0,v}] \equiv \ell b_v \pmod{\ell^2 \mathfrak{t}_v}$.

Let $Q \neq P_0$ be as in the statement, and $s_v := v(z_v(Q_v) - z_v(P_{0,v})) \geq 2$. As K embeds in K_v, $Q_v \neq P_{0,v}$ and $v_\ell(j(Q) - j_*) = e_0 + s_v < \infty$, and $s := s_v$ is the same at every place because $j(Q) - j_*$ is rational. Write $j(Q) - j_* = \ell^{e_0+s} u$ with $u \in \mathbb{Z}_\ell^\times$, so that $\log D_v \equiv \ell^s u\, b_v \pmod{\ell^{s+1}\mathfrak{t}_v}$ for $D := [Q - P_0] \in J(K)$. Put $d = s - 1 \geq 1$. Then $\log D_v \in \ell^s \mathfrak{t}_v = \ell \lambda^d \mu^d \mathfrak{t}_v \subseteq \ell \lambda^d \mathfrak{t}_v$, so by (F1) of Lemma 3.16 there is a unique formal point $Y_v \in \widehat{J}(\ell \mathcal{O}_v)$ with $\lambda^d Y_v = D_v$, and $\log Y_v = \lambda^{-d} \log D_v \equiv \ell\, \mu^d u\, b_v \pmod{\ell \lambda \mathfrak{t}_v}$. Let $\varepsilon' \in \mathbb{Z}$ with $\varepsilon' \equiv \varepsilon^d \pmod{\ell}$, see (3.2), and $X_v = [Q'_v - P_{0,v}] \in \widehat{J}(\ell \mathcal{O}_v)$. Then $\log(Y_v - \varepsilon' u X_v) \in \ell \lambda \mathfrak{t}_v$, so $\delta_v(Y_v) = \varepsilon' u\, \delta_v(X_v) = \varepsilon' u\, \vartheta_v$ by (F1) and (F3), with the same scalar $\varepsilon' u \neq 0$ at every place.

In case (i) we apply Lemma 5.2 with $\varpi = \lambda$, $W_v = \langle T \rangle$, $\Gamma = \langle T \rangle$ and $m = d$. For (L): $\widehat{J}(\ell \mathcal{O}_v)$ is torsion-free, as K_v is unramified over $\mathbb{Q}_\ell$ and $\ell > 2$, so $J(K_v)[\lambda]$ injects into $\widetilde{J}(k_v)[\lambda] = \langle \tilde{T} \rangle$ by (F2), and $J(K_v)[\lambda] = \langle T \rangle$. If $\lambda Y = aT$ with $a \not\equiv 0 \pmod{\ell}$, then $T \in \lambda J(K_v)$ and $\delta_v(T) = 0$ by (F3), which is excluded, so $\lambda Y \in \langle T \rangle$ implies $\lambda Y = 0$ and $Y \in \langle T \rangle$. For (G): if $R_v \in \lambda J(K_v) + \langle T \rangle$ for every $v \mid \ell$, then $\delta(R)|_\ell \in \Sigma \cap \Theta_T = \mathbb{F}_\ell \cdot \delta(T)|_\ell$, so $\delta(R - aT)$ has trivial localization for some a, and $R - aT \in \lambda J(K)$ by the injectivity of the localization and Proposition 3.14(b). Lemma 5.2, with the points Y_v, gives $(\varepsilon' u\, \vartheta_v)_v \in \Sigma + \Theta_T$, so $\vartheta \in \Sigma + \Theta_T$, contrary to the hypothesis. In case (ii), Lemma 3.20 applies to D, $m = d$ and the points $W_v = Y_v$, and gives $(\delta_v^0(Y_v))_v \in \Sigma$. As Y_v is formal, $\pi_v(Y_v) = 0$ and $\delta_v^0(Y_v) = \delta_v(Y_v)$, so $\vartheta \in \Sigma$, contrary to the hypothesis. □

For the curves with complex multiplication, the known points over $j_c \in \{0, 1728\}$ are ramification points of j, and a point of a solution near them has depth $k \geq 2$ (Lemma 4.5(d)).

Lemma 5.10 (known points at ramification points)**.** *Let $\xi \in X_0(p)(K)$ with $j(\xi) = j_c$ for region A or B, and let $P \in X_0(p)(K)$ be the point of a solution (Proposition 2.12), with $j(P)$ at depth $k \geq 2$ of that region and P_v in the residue disc of ξ_v for every $v \mid \ell$. Let $(P_v^{(1)})_{v|\ell}$ be the points of Lemma 4.5(e), which form an admissible configuration at depth 1 with the labels of $(P_v)_v$.*

(i) *If* $\delta_v(T) \neq 0$ *for every* v *and* $\Sigma \cap \Theta_T = \mathbb{F}_\ell \cdot \delta(T)|_\ell$, *then* $(\delta_v(P_v^{(1)}))_v \in \Sigma + \Theta_T$.

(ii) *If* K *satisfies the hypotheses of Proposition 3.18, then* $(\delta_v(P_v^{(1)}))_v \in \Sigma$.

Proof. Let $D = [P - \xi] \in J(K)$. At $v \mid \ell$, let $z = z_i$ be the parameter at ξ_v, write $z(P_v) = \ell^k s_v$ with $s_v \in \mathcal{O}_v^\times$, and define $b_v \in \mathfrak{t}_v$ by $\langle b_v, \omega \rangle = (\omega/dz)(\xi_v)$ for regular differentials ω. The argument of the proof of Lemma 5.9, with $z(P_v)$ of valuation $k \geq 2$, gives $\log D_v \equiv \ell^k s_v b_v \pmod{\ell^{2k}\mathfrak{t}_v}$. So $D_v \in \widehat{J}(\ell^2 \mathcal{O}_v)$ and $\log D_v \in \ell\lambda^{k-1}\mathfrak{t}_v$. With $d = k - 1$, let Y_v be the formal point with $\lambda^d Y_v = D_v$. Then $\log Y_v \equiv \ell\mu^d s_v b_v \pmod{\ell\lambda\mathfrak{t}_v}$. The point $X_v = [P_v^{(1)} - \xi_v]$ has $\log X_v \equiv \ell s_v b_v \pmod{\ell^2\mathfrak{t}_v}$, so $\delta_v(Y_v) = \varepsilon'(\delta_v(P_v^{(1)}) - \delta_v(\xi_v))$ with $\varepsilon' \equiv \varepsilon^d \pmod{\ell}$. Under (i), Lemma 5.2, applied as in the proof of Lemma 5.9 with $m = d$, gives $(\delta_v(Y_v))_v \in \Sigma + \Theta_T$. Under (ii), Lemma 3.20 gives $(\delta_v(Y_v))_v = (\delta_v^0(Y_v))_v \in \Sigma$. Since $\delta(\xi)|_\ell \in \Sigma$, this gives (i) and (ii). The configuration $(P_v^{(1)})_v$ is admissible because $(P_v)_v$ is and admissibility depends only on the labels (Lemma 4.5(c)). □

So a disc test at depth 1 that has no class tuple in $\Sigma + \Theta_T$, respectively in Σ, among the configurations in the residue discs of the ξ_v, excludes the points of solutions near ξ at every depth $k \geq 2$.

5.6. **A sieve at good primes.** The Selmer classes that survive the disc test and the arguments above are removed by a test at a prime q of good reduction, which uses only that j_0 is rational.

Lemma 5.11 (sieve at good primes)**.** *Let* $p \in \{11, 17, 19, 23, 29\}$ *and* ℓ *the prime of the descent. Let* K' *be a number field and* $Q \in X_0(p)(K')$ *with* $j(Q) \in \mathbb{Q}$, *such that* Q *induces an isomorphism* $\operatorname{Spec} K' \to j^{-1}(j(Q))$. *Let* $q \notin \{2, 3, \ell, p\}$ *be a prime unramified in* K', *with* $q \neq 373$ *if* $p = 17$, *and let* $\tilde{\jmath} \in \mathbb{P}^1(\mathbb{F}_q)$ *be the reduction of* $j(Q)$. *For a place* $w \mid q$ *of* K' *let* k_w *be its residue field and* $f_w = [k_w : \mathbb{F}_q]$, *and write* $\sim$ *for reduction modulo* w. *Then* j *extends to a finite flat morphism of degree* $p + 1$ *from the smooth model* $\mathcal{X}$ *of* $X_0(p)$ *over* $\mathbb{Z}_{(q)}$ *to* $\mathbb{P}^1_{\mathbb{Z}_{(q)}}$, *with reduction* j_q, *and there is a map* $w \mapsto R(w)$ *from the places of* K' *above* q *to the closed points of the fibre* $j_q^{-1}(\tilde{\jmath})$ *with the following properties.*

(a) $\tilde{Q}_w$ *is a* k_w*-point of* $\mathcal{X}_{\mathbb{F}_q}$ *lying on* $R(w)$. *In particular* $\deg R(w)$ *divides* f_w.

(b) *For every closed point* R *of* $j_q^{-1}(\tilde{\jmath})$, $\sum_{R(w)=R} f_w = e_R \deg R$, *where* e_R *is the ramification index of* j_q *at* R.

(c) *Reduction induces an isomorphism* $J(K'_w)/\ell J(K'_w) \to \widetilde{J}(k_w)/\ell\widetilde{J}(k_w)$ *compatible with the local Kummer maps, so the component at* w *of* $\delta(R')$, *for* $R' \in J(K')$, *depends only on the image of* $\tilde{R}'_w$ *in* $\widetilde{J}(k_w)/\ell\widetilde{J}(k_w)$. *For* $p \neq 17$ *it is an unramified class, and its image in* $k_w^\times/k_w^{\times\ell}$ *is given as follows. In genus* 1, *for* $R' = Q$, *it is the class of* $\tilde{f}_T(\tilde{Q}_w)$ *if* $\tilde{Q}_w \notin \{\tilde{O}, \tilde{T}\}$, *the trivial class if* $\tilde{Q}_w = \tilde{O}$, *and the class of* $\delta(T)$ *if* $\tilde{Q}_w = \tilde{T}$. *In genus* 2, *for* $R' = [Q - \infty]$, *it is the class of* $\tilde{f}(\tilde{Q}_w)$ *if* $\tilde{Q}_w$ *is not a cusp, which holds when* $\tilde{\jmath} \neq \infty$.

(d) *If* $Q = P$ *is the point of a solution* (a, b, c) *(Proposition 2.12), then* $\tilde{\jmath} = \infty$ *if and only if* $q \mid c$, *and then* $a_q(E) \equiv \pm(q + 1) \pmod{p}$.

The hypothesis on Q forces $[K' : \mathbb{Q}] = p + 1$ and $j(Q) \notin \{0, 1728, \infty\}$, whose fibres are not reduced. The prime 373 is excluded for $p = 17$ because it divides $G_{17}(7, 0)$, where $7 = x_{17}^0$ is the x-coordinate of the cusp 0, so that modulo 373 a zero of j can meet the cusp 0 (see the proof). Here f_T is the function with divisor $\ell(T) - \ell(O)$ of Sections 3.2 and 3.3, $\delta(T)$ is

the class of $1/11$, respectively $-1/19$, and f is the modular unit of Section 2.3. For $p = 17$ the Kummer map is that of Lemma 3.9, and (c) is used in the form: if $2^m R' = Q - P_0 - \mathfrak{s}$ with $R', P_0 \in J(K')$ and $\mathfrak{s}$ torsion, then $2^m \tilde{R}'_w = \tilde{Q}_w - \tilde{P}_{0,w} - \tilde{\mathfrak{s}}_w$, and the class of $\tilde{R}'_w$ in $\widetilde{J}(k_w)/2\widetilde{J}(k_w)$ is the component at w of $\delta(R')$.

Proof. Let $\mathcal{X}$ be the scheme over $\mathbb{Z}_{(q)}$ defined by the model of $X_0(p)$ in Table 5 (genus 1) or by $y^2 = F(x)$ (genus 2). It is smooth, as its discriminant ($\pm$ a power of p in genus 1, $2^{12}p^k$ in genus 2) is prime to q. The divisor of j on $\mathcal{X}$ has no vertical component, because neither the numerator $\mathcal{A}_p + \mathcal{B}_p y$ of j nor $(x - x_p^0)^p$ in genus 1 vanishes identically on the special fibre: $\mathcal{B}_p$ has leading coefficient ± 1, or $\pm\frac{1}{2}$ in genus 2, and $1, y$ are linearly independent over $\mathbb{F}_q(x)$. The poles of j are the closures of the two cusps, whose reductions are distinct: in genus 1 they are O and a point of order dividing 5, 4 or 3, prime to q, and in genus 2 the two points at infinity, where $y/x^3 \to \mp 1$. The zeros of j are the closures of the points over 0, whose x-coordinates are roots of the monic integral polynomial $G_p(x, 0)$. So no zero reduces to a point at infinity, nor, in genus 1, to the cusp 0, whose x-coordinate is x_p^0, since $G_{11}(16, 0) = 11^{24}$, $G_{17}(7, 0) = 17^{18} \cdot 373^3$ and $G_{19}(5, 0) = 2^{15} \cdot 3^3 \cdot 19^{19}$ are prime to q. Hence j is a morphism $\mathcal{X} \to \mathbb{P}^1_{\mathbb{Z}_{(q)}}$. It is proper and quasi-finite since j_q is not constant (it involves y), so finite. It is flat of degree $p + 1$ because $\mathcal{X}$ and $\mathbb{P}^1_{\mathbb{Z}_{(q)}}$ are regular of dimension 2 [38, Theorem 23.1], [61, Tag 00R4].

Let B be the ring of the fibre of j over the $\mathbb{Z}_q$-point of $\mathbb{P}^1$ that extends $j(Q)$, a finite flat $\mathbb{Z}_q$-algebra of rank $p+1$. By the hypothesis on Q, $B \otimes \mathbb{Q}_q = K' \otimes \mathbb{Q}_q = \prod_{w|q} K'_w$, and $B \otimes \mathbb{F}_q$ is the ring of $j_q^{-1}(\tilde{\jmath})$. As B is flat and finite over $\mathbb{Z}_q$, $B \subseteq \prod_w \mathcal{O}_{K'_w}$, and as $\mathbb{Z}_q$ is henselian, $B = \prod_R B_R$ over the closed points R of $j_q^{-1}(\tilde{\jmath})$, with B_R local. Each B_R is free over $\mathbb{Z}_q$ of rank $\dim_{\mathbb{F}_q}(B_R \otimes \mathbb{F}_q) = e_R \deg R$, because the local ring of the fibre at R is the discrete valuation ring $\mathcal{O}_{\mathcal{X}_{\mathbb{F}_q},R}$ modulo the e_R-th power of its maximal ideal. Each factor K'_w of $B \otimes \mathbb{Q}_q$ is a factor of exactly one $B_R \otimes \mathbb{Q}_q$, and we let $R(w)$ be this R. As q is unramified in K', $[K'_w : \mathbb{Q}_q] = f_w$, and comparing ranks gives (b). The map $B_R \to \mathcal{O}_{K'_w} \to k_w$ has kernel the maximal ideal of B_R, as its image is a field. The composite $\operatorname{Spec} \mathcal{O}_{K'_w} \to \operatorname{Spec} B \to \mathcal{X}$ is the point of $\mathcal{X}(\mathcal{O}_{K'_w})$ extending Q, with special fibre $\tilde{Q}_w$, which gives (a).

(c) As J has good reduction at w and $q \neq \ell$, the kernel of reduction is a pro-q group, divisible by ℓ, and reduction is surjective onto $\widetilde{J}(k_w)$. The image of δ_w is then the group of unramified classes, which reduces isomorphically onto $k_w^\times / k_w^{\times \ell}$. In genus 1, f_T is regular away from O on $\mathcal{X}$ and its reduction has divisor $\ell(\tilde{T}) - \ell(\tilde{O})$. So if $\tilde{Q}_w \notin \{\tilde{O}, \tilde{T}\}$, then $f_T(Q)$ is a w-unit with reduction $\tilde{f}_T(\tilde{Q}_w)$. If $\tilde{Q}_w = \tilde{O}$, respectively $\tilde{T}$, then Q, respectively $Q - T$, lies in the kernel of reduction. In genus 2, $\delta([Q - \infty]) = f(Q)$ (Proposition 3.13), and f is a unit away from the cusps as $f \cdot (f \circ w_p) = p^{r_p/2}$. An element of $K(S, \ell)$ has valuation divisible by ℓ at w, so its image in $k_w^\times / k_w^{\times \ell}$ is well defined. When $\tilde{Q}_w$ is not a cusp, $f(Q)$ is a w-unit, and its image is the class of $f(\tilde{Q}_w)$. The cusps are the poles of j. (d) Since $j_0 = 1728b^3/c^p$ with $\gcd(b, c) = 1$ and $q \nmid 6$, j_0 is q-integral if and only if $q \nmid c$. If $q \mid c$, then the twist E' of the Frey curve has multiplicative reduction at q with $p \mid v_q(\Delta)$, so its mod p representation is unramified at q with Frobenius eigenvalues ± 1 and $\pm q$, and $a_q(E) \equiv \pm(q + 1) \pmod{p}$. □

The closed points of a fibre. Over $\tilde{\jmath} = \infty$ the closed points are the reductions of the two cusps, with $e = 1$ at ∞ (the origin O in genus 1) and $e = p$ at 0. So by (a) and (b) exactly one place w, of degree 1, has $\tilde{Q}_w = \tilde{\infty}$, and all other places reduce to the cusp 0. For $\tilde{\jmath} \neq \infty$, as in Section 2.3, the roots of $G_p(x, \tilde{\jmath})$ in $\bar{\mathbb{F}}_q$ are the x-coordinates of the geometric points R of $j_q^{-1}(\tilde{\jmath})$, each counted e_R times. If x separates these points, the closed points of the

fibre correspond to the irreducible factors of $G_p(x, \tilde{\jmath})$ over $\mathbb{F}_q$, with $\deg R$ the degree and e_R the multiplicity of the factor. In particular, if $G_p(x, \tilde{\jmath})$ is squarefree, then by (a) and (b) the places $w \mid q$ correspond bijectively to the irreducible factors F_w of $G_p(x, \tilde{\jmath})$, with $\deg F_w = f_w$ and $F_w(x(\tilde{Q}_w)) = 0$. Then $y(\tilde{Q}_w)$ is $(\tilde{\jmath}(\tilde{x} - x_p^0)^p - \mathcal{A}_p(\tilde{x}))/\mathcal{B}_p(\tilde{x})$ in genus 1 and $(\tilde{\jmath} - \mathcal{A}_p(\tilde{x}))/\mathcal{B}_p(\tilde{x})$ in genus 2, with $\tilde{x} = x(\tilde{Q}_w)$, whenever $\mathcal{B}_p(\tilde{x}) \neq 0$.

The test. Let σ be a class in the group of values of δ over K' that is unramified at the places above q. We say that σ *passes at* q if there are $\tilde{\jmath} \in \mathbb{P}^1(\mathbb{F}_q)$ and a map $w \mapsto R(w)$ to the closed points of $j_q^{-1}(\tilde{\jmath})$ with properties (a) and (b) such that, for every place $w \mid q$, the image of σ at w is the class, as in (c), of some k_w-point of $\mathcal{X}_{\mathbb{F}_q}$ lying on $R(w)$. By Lemma 5.11, $\delta(Q)$ (in genus 2, $\delta([Q - \infty])$) passes at every such q. Likewise, given $P_0 \in J(K')$, $m \geq 0$ and a torsion point $\mathfrak{s} \in J(K')$, a class σ passes at q for $(P_0, m, \mathfrak{s})$ if there are $\tilde{\jmath}$, $w \mapsto R(w)$ as above, k_w-points $\tilde{Q}_w$ on $R(w)$ and points $Y_w \in \tilde{J}(k_w)$ with $\ell^m Y_w = \tilde{Q}_w - \tilde{P}_{0,w} - \tilde{\mathfrak{s}}_w$ whose Kummer class is the image of σ at w. If $Q - P_0 = \ell^m R' + \mathfrak{s}$ with $R' \in J(K')$, then $\delta(R')$ passes at every such q for $(P_0, m, \mathfrak{s})$. Where x does not separate the points of the fibre, each place may take any k_w-point of the fibre (only (a) and the classes are used), which can only let more classes pass. At a place with $\ell \nmid \#k_w - 1$ only (a) and (b) constrain the place. The classes are the power residues $u^{(\#k_w - 1)/\ell}$ of representatives $u \in k_w^\times$. For P the point of a solution, (d) excludes $\tilde{\jmath} = \infty$ when $a_q(E) \not\equiv \pm(q + 1) \pmod{p}$, and every other value of $j_0 \bmod q$ is allowed.

Part II. The prime exponents

6. The exponent 11

Theorem A for $p = 11$ is proved at the prime 5, where $X_0(11)$ has good ordinary reduction and all the fields K_E are unramified (Freitas, Naskręcki and Stoll work at 2 [27, Lemma 7.3]). The disc test leaves ten known points and two further class tuples, which the sieve removes.

In this section $p = 11$, $\ell = 5$, $J = X_0(11)$ and $T = (5, 5)$ are as in Table 5, and δ is the Kummer map of Lemma 3.6. For $K = K_E$ let S be the set of primes above 11. Then Σ is the image of $K(S, 5)$ in $\prod_{v|5} K_v^\times / K_v^{\times 5}$, and the restriction map from $K(S, 5)$ is injective (Proposition 3.7). By [27, Proposition 2.4 and Lemma 2.3], some twist $E' = E_{a,b,c}^{(d)}$ with $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ has $E'[11] \simeq E[11]$ as Galois modules for one of the seven curves 27a1, 54a1, 96a1, 288a1, 864a1, 864b1, 864c1. By Proposition 2.3, E is not 27a1 or 288a1. So, by Proposition 2.12, a primitive solution (a, b, c) with $abc \neq 0$ gives a point $P \in J(K_E)$ for some

$$E \in \mathcal{E} = \{54a1, 96a1, 864a1, 864b1, 864c1\},$$

with $j(P) = j_0 = 1728b^3/c^{11}$.

6.1. Reduction at 5.

Lemma 6.1. *Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{11}$ with $abc \neq 0$, $E \in \mathcal{E}$, and E' an elliptic curve over $\mathbb{Q}$ with $j(E') = j_0$ and $E'[11] \simeq E[11]$ as Galois modules, symplectically or not.*

(i) *$5 \nmid c$, so $j_0 \in \mathbb{Z}_5$, and E' has good reduction at 5 with $a_5(E') = a_5(E)$.*

(ii) *$j_0 \bmod 5$ lies in $\mathcal{J}(E)$, where $\mathcal{J}(54a1) = \{2\}$, $\mathcal{J}(864a1) = \{4\}$ and $\mathcal{J}(96a1) = \mathcal{J}(864b1) = \mathcal{J}(864c1) = \{1, 3\}$. If $j_0 \equiv 3 \pmod 5$, then $1728 - j_0 = 25ws^2$ with $w \in \{1, 2\}$ and $s \in \mathbb{Z}_5$.*

Proof. The curves in $\mathcal{E}$ have conductors 54, 96 and 864, so their mod 11 representations are unramified at 5, with $a_5(E) = 3, 2, -1, 2, -2$ for 54a1, 96a1, 864a1, 864b1, 864c1. As $j_0 \neq 0, 1728$, E' is a quadratic twist of $E_{a,b,c}$ by some squarefree d. Suppose that $5 \mid d$. The Frey curve has good or multiplicative reduction at 5, as $5 \nmid \gcd(b, c)$, so the semisimplification of its mod 11 representation is trivial on the inertia group at 5. The mod 11 representation of E' restricted to inertia would then be the twist of this by the quadratic character of d, which is ramified at 5. But $E'[11] \simeq E[11]$ is unramified at 5, so $5 \nmid d$.

(i) If $5 \mid c$, then $5 \nmid b$, and E' has multiplicative reduction at 5 with $v_5(\Delta) = 11v_5(c)$. So its mod 11 representation is unramified at 5, and Frob_5 has eigenvalues η and 5η with $\eta = \pm 1$, and trace ± 6 modulo 11. But $a_5(E) \bmod 11 \in \{3, 2, 10, 9\}$ is never 5 or 6. So $5 \nmid c$, and E' has good reduction at 5. Then $a_5(E') \equiv a_5(E) \pmod{11}$, and since $|a_5(E')|, |a_5(E)| \leq 2\sqrt{5} < 5.5$, the two traces are equal.

(ii) The reduction of j_0 modulo 5 is the j-invariant of the reduction of E', a curve over $\mathbb{F}_5$ with trace $a_5(E)$. The traces of the elliptic curves over $\mathbb{F}_5$ are 0 for $j = 0$, ± 2 for $j = 1$, ± 3 for $j = 2$, ± 2 and ± 4 for $j = 3 = 1728$, and ± 1 for $j = 4$. This gives $\mathcal{J}(E)$. If $j_0 \equiv 3 \pmod 5$, then $1728 - j_0 = 1728a^2/c^{11}$ has even positive 5-adic valuation. So $(1728 - j_0)/25$ is ws^2 with $w \in \{1, 2\}$, a set of representatives of $\mathbb{Z}_5^\times/\mathbb{Z}_5^{\times 2}$, and $s \in \mathbb{Z}_5$. □

We cover the possible values of j_0 by sets of the kind (1) of Section 4.4: for $j_0 \not\equiv 3 \pmod 5$ the five *unramified discs* $j_1 + 25\mathbb{Z}_5$ with $j_1 \bmod 5 \in \mathcal{J}(E)$, and for $j_0 \equiv 3 \pmod 5$ the six sets $\{1728 - 25ws^2 : s \in s_1 + 5\mathbb{Z}_5\}$ with $w \in \{1, 2\}$ and $s_1 \in \{1, 2, 5\}$, which make up region B at 5 (Section 4.2). As s and $-s$ give the same j, the representatives 1, 2, 5 cover $s \equiv \pm 1, \pm 2, 0$. For $j_1 \bmod 5 \in \{1, 2, 4\}$ the polynomial $G_{11}(x, j_1)$ is squarefree modulo 5, with factors of degrees $6, 6$, respectively $1, 11$, respectively $1, 1, 5, 5$. So Lemma 4.6(a) applies in the unramified discs, and Lemma 4.6(c) in region B.

6.2. **The disc test.** By Lemma 2.14, there is exactly one point of $J(K_E)$ over each j-invariant of Table 9, since $\mathrm{Aut}(K_E) = 1$.

E	j-invariants of the known points	their sets of j-values	$v_5(\gamma_v)$
54a1	$9261/8$, $-132651/2$, $-1167051/512$	17, 12, $2 + 25\mathbb{Z}_5$	0
96a1	$97336/81$, $140608/3$	6, $11 + 25\mathbb{Z}_5$	0
	$21952/9$, $7301384/3$	region B, $w = 1$, $s \equiv \pm 1, \pm 2 \pmod 5$	1
864a1	-216	$9 + 25\mathbb{Z}_5$	0
864b1	-13824	$1 + 25\mathbb{Z}_5$	0
864c1	1536	$11 + 25\mathbb{Z}_5$	0

TABLE 9. The known points of $J(K_E)$ for $p = 11$, and the valuation of γ_v (Proposition 6.4) at every place above 5.

Proposition 6.2. *Let $E \in \mathcal{E}$ and $K = K_E$. In the sets of j-values of Section 6.1, the class tuples in Σ of admissible configurations over the representatives are exactly the following:*

(a) *the class tuples of the ten known points of Table 9, each in the set that contains its j-invariant;*

(b) *one further tuple for $E = 864a1$, in the disc $14 + 25\mathbb{Z}_5$, and one further tuple for $E = 96a1$, in the disc $11 + 25\mathbb{Z}_5$, which also contains a known point.*

The numbers of admissible configurations tested are 55 *for* 54a1, 500 *for* 864a1, *and* 576 *for each of* 96a1, 864b1, 864c1.

Proof. This is the computation of Section 4.4, with PARI/GP [43], in the programs of [32]. The classes δ_v are computed from f_T. In region B with $w = 2$ the fibre has four factors of degree 3 over $\mathbb{Q}_5$, and there is no admissible configuration for the fields whose places above 5 have degree 6. For 54a1 and 864a1 only unramified discs occur.

For $E = 54a1$, Table S1 gives a certificate that can be checked by hand. The classes of $K(S, 5)$ are unit classes at the two places v_1, v_2 above 5 (Proposition 3.7). Through (3.1), Σ is the span in $k_{v_1} \oplus k_{v_2} = \mathbb{F}_5 \oplus \mathbb{F}_{5^{11}}$ of the images of a basis of $K(S, 5)$ (Proposition A.4). It has dimension 9, and its annihilator is spanned by the functionals $\Upsilon_1, \Upsilon_2, \Upsilon_3$ of the table. The eleven points over j_1 at v_2 form one Frobenius orbit, and δ_{v_2} commutes with the Frobenius σ, since f_T has rational coefficients. So the class tuples of the disc $j_1 + 25\mathbb{Z}_5$ are the tuples $(a, \sigma^i c)$ in the notation of the table, and the table shows that Υ_1, Υ_2, Υ_3 vanish simultaneously only at the class tuples of the three known points, in the discs 2, 12 and $17 + 25\mathbb{Z}_5$. □

Proposition 6.3. *The two tuples of Proposition 6.2(b) are not class tuples of points $P \in J(K_E)$ coming from a primitive solution with $abc \neq 0$.*

Proof. Since the restriction of $K(S, 5)$ to the places above 5 is injective (Proposition 3.7), each tuple determines a unique element of $K(S, 5)$, which would be $\delta(P)$. By Proposition 2.12(a), P induces an isomorphism $\operatorname{Spec} K \to j^{-1}(j_0)$, so Lemma 5.11 applies with $K' = K$ and $Q = P$, and $\delta(P)$ passes at every prime $q \notin \{2, 3, 5, 11\}$ unramified in K. The Selmer class of the tuple for 864a1 first fails the test at $q = 31$, and that for 96a1 fails it at $q = 191$. In both cases $\tilde{\jmath} = \infty$ is excluded by Lemma 5.11(d). □

6.3. **The known points.**

Proposition 6.4. *Let $E \in \mathcal{E}$, $K = K_E$, and let $P_0 \in J(K)$ be one of the known points of Table 9, with set of j-values D. Then P_0 is the only point $Q \in J(K)$ with $j(Q) \in D \cap \mathbb{Q}$ whose class tuple at the places above 5 equals that of P_0.*

Proof. Let $\Theta_T = \bigoplus_{v|5} \mathbb{F}_5\, \delta_v(T)$. In region B we use the parameter s of Section 6.1, and on the unramified discs the parameter j. The following facts are computed for each known point:

(K1) at every place $v \mid 5$, $\delta_v(T) \neq 0$, and $\dim \Sigma + \dim \Theta_T - \dim(\Sigma + \Theta_T) = 1$, so $\Sigma \cap \Theta_T = \mathbb{F}_5\, \delta(T)|_5$;

(K2) at every place $v \mid 5$, the class of $P_{0,v}$ differs from the class of every other point of $J(K_v)$ over $j(P_0)$;

(K3) the valuation at P_0 of $\gamma_v = (dx/dj)/(2y + 1)$, respectively $(dx/ds)/(2y + 1)$, which is the derivative of the formal logarithm along the fibres with respect to the parameter, is as in Table 9;

(K4) the tangent class $\vartheta = (\vartheta_v)_{v|5}$ defined in Step 3 below is not in $\Sigma + \Theta_T$.

The dimensions in (K1) are $(\dim \Sigma, \dim \Theta_T, \dim(\Sigma + \Theta_T)) = (9, 2, 10)$ for 54a1, $(8, 4, 11)$ for 864a1 and $(8, 2, 9)$ for the other three curves.

Suppose that $Q \neq P_0$ has $j(Q) \in D \cap \mathbb{Q}$ and the class tuple of P_0. Since P_0 is the only K-point over $j(P_0)$, the difference τ of the parameters of Q and P_0 is not 0. In region B the sign of s is fixed by $s(Q) \equiv s(P_0) \pmod 5$, which is possible as $s(P_0) \not\equiv 0$ for the two points

in region B. Let $n = v_5(\tau)$, so $n \geq 2$ on the unramified discs and $n \geq 1$ in region B, and put $N = n$ on the unramified discs and $N = n+1$ in region B.

Step 1. By Lemma 4.6, each point of $J(K_v)$ over a j-value of D has the class of the point over $j(P_0)$ in the same residue disc (in region B, on the same branch). By (K2) and the equality of class tuples, Q_v and $P_{0,v}$ lie in the same residue disc (on the same branch) for every $v \mid 5$. On the unramified discs, $S = Q - P_0$ then has $S_v \in \widehat{J}(5^N\mathcal{O}_v)$. As a power series in τ, $\log S_v$ is $\gamma_v\tau + O(\tau^2)$ with integral coefficients up to the factors $1/k$ of the logarithm, so its terms of degree $k \geq 2$ have valuation at least $N+1$. In region B the branch has the form $x = x_R + 5sZ(5s)$ with Z integral (Lemma 4.6(c)). So $\gamma_v \in 5\mathcal{O}_v$, every coefficient of $\log S_v$ as a series in τ is divisible by 5, and the term of degree $k \geq 2$ has valuation at least $1 + kn - v_5(k) \geq n + 2 = N + 1$. In both cases $v_5(\gamma_v) = N - n$ by (K3), so $\log S_v \equiv \gamma_v\tau \pmod{5^{N+1}}$ has valuation exactly N, and $S_v \in \widehat{J}(5^N\mathcal{O}_v)$.

Step 2. We apply Lemma 5.2 with $A = J$, the point S in the role of D, $\varpi = [5]$, $\mathcal{P}$ the set of places above 5, $W_v = \Gamma = \langle T\rangle$ and $m = N - 1$. For (L): the formal group $\widehat{J}(5\mathcal{O}_v)$ is torsion-free, as K_v is unramified over $\mathbb{Q}_5$, and $\widetilde{J}(k_v)[5] = \langle\tilde{T}\rangle$, as the reduction is ordinary and $\#\widetilde{J}(\mathbb{F}_5) = 5$. So $J(K_v)[5] = \langle T\rangle$. If $5Y = aT$ with $a \not\equiv 0 \pmod 5$, then $T \in 5J(K_v)$ and $\delta_v(T) = 0$, contrary to (K1). So $5Y \in \langle T\rangle$ implies $Y \in \langle T\rangle$. For (G): if $R_v \in 5J(K_v) + \langle T\rangle$ for every $v \mid 5$, then $\delta(R)|_5 \in \Sigma \cap \Theta_T = \mathbb{F}_5\,\delta(T)|_5$ by (K1), so $R \in 5J(K) + \langle T\rangle$ by Proposition 3.7(b), (c). The logarithm is an isometry from $\widehat{J}(5^i\mathcal{O}_v)$ onto $5^i\mathcal{O}_v$ for $i \geq 1$, so $\widehat{J}(5^N\mathcal{O}_v) = 5^{N-1}\widehat{J}(5\mathcal{O}_v)$, and by Step 1 S_v has level at least $N - 1$ modulo $\langle T\rangle$. Let $Y_v \in \widehat{J}(5\mathcal{O}_v)$ be the point with $5^{N-1}Y_v = S_v$. Lemma 5.2 gives $(\delta_v(Y_v))_{v|5} \in \Sigma + \Theta_T$.

Step 3. By Step 1, $\log Y_v = 5^{1-N}\log S_v \equiv u\,5^{1-v_5(\gamma_v)}\gamma_v \pmod{25}$, where $u = \tau/5^n \bmod 5 \neq 0$ is the same at every place. On $\widehat{J}(5\mathcal{O}_v)$ the class δ_v is additive and depends only on the formal parameter modulo 25. Let $U(t)$ be the point with formal parameter t. Then $\delta_v(U(t))$ is the class of $h(t) = -t^5 f_T(U(t)) = 1 + 4t + \cdots$, which is linear in $t/5$ modulo 5, and $\log U(t) \equiv t \pmod{25}$ for $t \in 5\mathcal{O}_v$. So $\delta_v(Y_v) = u\,\vartheta_v$, where ϑ_v is the class of $h(t)$ at $t = 5^{1-v_5(\gamma_v)}\gamma_v$. By Step 2, $u\,\vartheta \in \Sigma + \Theta_T$, which contradicts (K4). □

6.4. **Proof of Theorem A for $p = 11$.**

Theorem 6.5. *Let $E \in \mathcal{E}$ and let (a,b,c) and E' be as in Lemma 6.1. Then $E =$ 864b1 and $(a,b,c) = (\pm 3, -2, 1)$.*

Proof. Let $P \in J(K_E)$ be the point of Proposition 2.12. Then j_0 lies in one of the sets of j-values of Section 6.1, the local points $(P_v)_{v|5}$ form an admissible configuration over j_0, and their class tuple lies in Σ (Proposition 3.7). By Propositions 4.9 and 6.2, this class tuple is the class tuple of a known point P_0 whose j-invariant lies in the same set, or one of the two tuples of Proposition 6.2(b), which Proposition 6.3 excludes. In the first case Proposition 6.4 gives $P = P_0$, so $j_0 = j(P_0)$ is one of the known j-invariants (2.5). By Lemma 2.15(b), $j_0 = -13824$ and $(a,b,c) = (\pm 3, -2, 1)$. Table 9 then gives $E =$ 864b1. □

Let (a,b,c) be a primitive solution of $x^2 + y^3 = z^p$ for an odd prime p. If $abc = 0$, then (a,b,c) is one of the six trivial solutions. If $a = 0$, then $b^3 = c^p$ with $\gcd(b,c) = 1$ forces $(b,c) = \pm(1,1)$. If $b = 0$, then $a^2 = c^p$ forces $c = 1$ and $a = \pm 1$. If $c = 0$, then $a^2 = -b^3$ forces $b = -1$ and $a = \pm 1$. Now let $p = 11$ and $abc \neq 0$. By [27, Proposition 2.4 and Lemma 2.3], some twist $E' = E^{(d)}_{a,b,c}$ has $E'[11] \simeq E[11]$, symplectically or not, for some $E \in \{27\text{a}1, 288\text{a}1\} \cup \mathcal{E}$. Proposition 2.3 excludes 27a1 and 288a1, and for $E \in \mathcal{E}$ Theorem 6.5 gives $(a,b,c) = (\pm 3, -2, 1)$. The class groups and S-units of the fields K_E are determined without GRH (Propositions A.3 and A.4), so the proof is unconditional. □

7. The exponent 17

For $p = 17$ we prove Theorem A at the prime $\ell = 2$, with the 2-descent of Section 3.4. New compared with $p = 11$ are the points near the cusps for 54a1 (Section 7.3) and the enumeration of Section 5.4, written out in full for 864b1 (Section 7.5). The disc test excludes 864a1; for 54a1, whose j_0 is near ∞, a linear form that vanishes on the image of the Selmer group excludes the points near the cusps; and for 864c1 and 864b1 the disc test leaves the discs of known points, which the enumeration closes, with a sieve at 13 for 864b1.

Here $J = X_0(17)$ and $T = (7, 13)$ are as in Table 5, with $J(\mathbb{Q}) = \langle T \rangle$. For a field $K = K_E$ of degree 18 we put $L = K(i)$. The map δ is that of Lemma 3.9, and Σ is the image of $\mathrm{Sel}^2(J/K)$ at the places above 2 (Proposition 3.11). By Theorem 2.1 and Proposition 2.2, the curves E to treat are 54a1, 864a1, 864b1 and 864c1. A primitive solution (a, b, c) with $abc \neq 0$ that gives a rational point on $X_E(17)$ yields a point $P \in J(K_E)$ with $j(P) = j_0 = 1728b^3/c^{17}$ (Proposition 2.12).

7.1. The 2-adic position of j_0.

Lemma 7.1. *Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{17}$ with $abc \neq 0$, let $E \in \{54a1, 864a1, 864b1, 864c1\}$, and suppose that some twist $E' = E^{(d)}_{a,b,c}$ has $E'[17] \simeq E[17]$. Put $j_0 = 1728b^3/c^{17}$.*

(a) *If $E = 54a1$, then c is even, b is odd, and $j_0 = 2^{-11}t^{-17}$ with $t \in \mathbb{Z}_2 \setminus \{0\}$, $v_2(t) = v_2(c) - 1$.*

(b) *If $E \in \{864a1, 864b1\}$, then j_0 lies in one of the sets $D_u = \{1728 + u \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\}$, $u \in \{-3, 1, -1, 3\}$, or in $D' = 512 + 2^{11}\mathbb{Z}_2$.*

(c) *If $E = 864c1$, then $j_0 \in j_1 + 2^{11}\mathbb{Z}_2$ with $j_1 \in \{-64, 960, 448, -576, -512\}$.*

Proof. (a) The curve 54a1 has multiplicative reduction at 2 and $v_2(j(54a1)) = -3$. Over the unramified quadratic extension of $\mathbb{Q}_2$ it is a Tate curve with parameter of valuation 3, prime to 17, so the inertia group at 2 acts on $54a1[17]$ through a group of order 17, and hence also on $E'[17]$. If E' had potentially good reduction at 2, inertia would act on $E'[17]$ through the Galois group of the extension of $\mathbb{Q}_2^{\mathrm{nr}}$ over which E' acquires good reduction. This group has order dividing 24 [54, §2], [35], which is prime to 17. So E' has potentially multiplicative reduction at 2, and $v_2(j_0) = 6 + 3v_2(b) - 17v_2(c) < 0$, whence $k = v_2(c) \geq 1$. Then b is odd by primitivity, and $j_0 = 2^{6-17k}w$ with $w \in \mathbb{Z}_2^\times$. Since 17 is odd and $\mathbb{Z}_2^\times \simeq \mathbb{Z}/2 \times \mathbb{Z}_2$, $w = w_1^{-17}$ for some $w_1 \in \mathbb{Z}_2^\times$, and $t = 2^{k-1}w_1$ works.

(b), (c) If E' had potentially multiplicative reduction at 2, the argument of (a) would show that inertia acts on $E'[17]$ through a group of order 17, as the valuation $-v_2(j_0) = 17v_2(c) - 6$ of its Tate parameter is prime to 17. But it acts on $E[17]$ through a group of order 8, since the curves of conductor 864 have potentially good reduction at 2, with inertia group the quaternion group. So E' has potentially good reduction at 2, and $E'[17] \simeq E[17]$ shows that E' and E have the same inertial field $\mathbb{Q}_2^{\mathrm{nr}}(E[17])$ at 2 [27, §3]. By [27, Theorem 3.1 and the remark after it], 864a1 and 864b1 have the inertial field of 288a1, and 864c1 that of 96a1, which is different. Table 1 of [27] gives the inertial field and the 2-adic position of j_0 for each class of (a mod 4, b mod 8) with a, b not both even. The field of 288a1 occurs exactly in lines 2 and 6, whose sets are D_u and D', and that of 96a1 in lines 3 and 5, with the sets of (c). □

7.2. The twist attached to 864a1.

Proposition 7.2. *Let $K = K_{864a1}$. No point $Q \in J(K) \setminus J(\mathbb{Q})$ has $j(Q) \in \mathbb{Q}$ in $D_{-3} \cup D_1 \cup D_{-1} \cup D_3 \cup D'$. Hence no primitive solution of $x^2 + y^3 = z^{17}$ with $abc \neq 0$ gives a rational point on $X_{864a1}(17)$.*

Proof. The fibre of j over 1728 is $(x^2 + 4x + 8)\, H_8(x)^2$ with H_8 irreducible of degree 8, and over 512 it is separable. We cover the sets of Lemma 7.1(b) by seven sets of the kind (2) of Section 4.4.

- The half-families of the four D_u with t even, represented by $j = 1728$.
- The half-families of the D_u with t odd. As the squares of 2-adic units form $1 + 8\mathbb{Z}_2$, these are the discs $j_1 + 2^{13}\mathbb{Z}_2$, $j_1 = 1728 + u \cdot 2^{10} \in \{-1344, 2752, 704, 4800\}$, treated as families with $e = 1$ and centre j_1.
- The two half-families of D', represented by $j = 512$ and 2560.

Conditions (i)–(iv) of Section 4.1 and (4.1) hold in every case: at 1728, with $\kappa = u \cdot 2^{10}$, at the eight roots of H_8 ($e_\xi = 2$, in the variable t, with $\nu_\xi = 2$ or 3) and at the two roots of $x^2 + 4x + 8$ ($e_\xi = 1$, in the variable t^2, with $\nu_\xi = 4$). At the points over each j_1 ($\kappa = 2^{13}$, $e = 1$) they hold with $\nu_\xi \geq 4$, and over 512 ($\kappa = 2^{11}$, $e = 1$) with $\nu_\xi \geq 2$. So the hypothesis of Proposition 4.9 holds with $k = 1$ for the half-families with t even and those of D', since $\nu_\xi + 1 \geq 3$, and with $k = 0$ for the discs about the j_1, since $\nu_\xi \geq 4$. In each case $r(x') \leq 5/2$ for every representative root x'. At the roots of H_8, where $\ell = 2$ divides $e_\xi = 2$, only Lemma 4.1 is used, through Lemma 4.4(a) and (c), and the representative is the centre. The sets $C_{D,v}$ are the same for the five discs that cover the D_u, and the same for the two halves of D'. In both cases they have 1, 2, 7, 1 elements at the places with $(e, f) = (4,1), (2,1), (4,2), (2,2)$, giving 14 class tuples per disc, and none of them lies in the image Σ of $\mathrm{Sel}^2(J/K)$. Since $j(T)$ and $j(2T)$ are not in these sets, the first statement follows from Proposition 4.9, and the second from Lemma 7.1(b) and Proposition 2.12. □

7.3. **The twist attached to 54a1.** For 54a1, Lemma 7.1(a) puts j_0 near ∞, and we work with the 2-adic points of the fibres near the cusps. Let $K = K_{54a1}$. By Table 6, 2 has two places in K: v_1 with $K_{v_1} = \mathbb{Q}_2$, and v_2 with K_{v_2} totally ramified of degree 17 over $\mathbb{Q}_2$. For a point Q reducing to O, over some finite extension of $\mathbb{Q}_2$, let $s = -x(Q)/y(Q)$ be its formal parameter. Then $Q \mapsto s$ is a bijection from the residue disc of O onto the open unit disc.

Lemma 7.3. (a) *For Q in the residue disc of O, $1/j(Q) = s\, g_1(s)$ with $g_1 \in 1 + s\mathbb{Z}[[s]]$.*
(b) *For Q in the residue disc of O, $1/j(-T - Q) = s^{17} g(s)$ with $g \in 1 + s\mathbb{Z}_2[[s]]$.*
(c) *If $v_2(\iota) > 0$, the fibre of $1/j$ over ι consists of one point in the residue disc of O and 17 points, counted with multiplicity, in the residue disc of $-T$.*

Proof. (a) Let $x(s) \in s^{-2}\mathbb{Z}[[s]]$ and $y(s) \in s^{-3}\mathbb{Z}[[s]]$ be the formal expansions [59, Chapter IV]. Then $s^{35}(\mathcal{A}_{17} + \mathcal{B}_{17} y)$ and $s^{34}(x - 7)^{17}$ lie in $1 + s\mathbb{Z}[[s]]$, so $1/j = s\, g_1(s)$ with $g_1 \in 1 + s\mathbb{Z}[[s]]$.

(b) Put $Q' = -T - Q = (x_3(s), y_3(s))$, computed with the addition law. Then $x_3, y_3 \in \mathbb{Z}[[s]]$, $x_3(0) = 7$, $y_3(0) = -21$, and $1/j(Q') = (x_3 - 7)^{17}/D(s)$ with $D = \mathcal{A}_{17}(x_3) + \mathcal{B}_{17}(x_3) y_3 \in \mathbb{Z}[[s]]$. We use Weierstrass preparation over $\mathbb{Z}_2$: a series whose first 2-adic unit coefficient is that of s^d is a monic polynomial of degree d times a unit of $\mathbb{Z}_2[[s]]$. Here $x_3 - 7 = 34s + 153s^2 + 595s^3 + \cdots$ has its first unit coefficient at s^2. Its zeros in the open disc are $s = 0$ (the point $-T$) and $s = s_T = 22/15$, the formal parameter of $2T$, at which $Q' = -T - 2T = T$. So $x_3 - 7 = s(s - s_T)u(s)$ with u a unit. The series D has $D(0) = 2^{17}17^{17}$, even coefficients up to s^{16} and an odd coefficient of s^{17}. Since j has degree 18, with poles of order 1 at O and 17 at $-T$, $j(T)$ is finite. So $D = j \cdot (x_3 - 7)^{17}$ vanishes to

order at least 17 at s_T, and hence $D = (s - s_T)^{17} w(s)$ with w a unit. So $1/j(Q') = s^{17} u^{17}/w$, and $g = u^{17}/w$ has $g(0) = 1$, since $u(0) = -255/11$ and $w(0) = -(255/11)^{17}$.

(c) For $v_2(\iota) > 0$, the series $s\, g_1(s) - \iota$ and $s^{17} g(s) - \iota$ have their first unit coefficients at s^1 and s^{17}, so the fibre has one point near O, 17 near $-T$ and, as $\deg j = 18$, no others. □

Lemma 7.4. *Let $t \in \mathbb{Z}_2 \setminus \{0\}$ and $j_0 = 2^{-11} t^{-17}$.*

(a) *The fibre $j^{-1}(j_0)$ has exactly one $\mathbb{Q}_2$-rational point R_1, and $R_1 \in 2J(\mathbb{Q}_2)$.*

(b) *$K_{v_2} = \mathbb{Q}_2(\alpha)$ with $\alpha^{17} = 2^{11}$, and the K_{v_2}-rational points of $j^{-1}(j_0)$ are R_1 and one point $R_2(t) = -T - Q(t)$, where $Q(t)$ has formal parameter $\varphi(\alpha t)$ and $\varphi \in s + s^2\mathbb{Z}_2[[s]]$ is the compositional inverse of $s\, g(s)^{1/17}$.*

(c) *If $t \equiv t' \pmod 4$, then $R_2(t) - R_2(t') \in 2J(K_{v_2})$. If $4 \mid t$, then $R_2(t) + T \in 2J(K_{v_2})$. So $\delta_{v_2}(R_2(t))$ depends only on $t \bmod 4$, and equals $\delta_{v_2}(T)$ when $4 \mid t$.*

Proof. Let $\iota = 1/j_0 = 2^{11} t^{17}$, of valuation at least 11. As $1/17 \in \mathbb{Z}_2$, the binomial series gives $h = g^{1/17} \in 1 + s\mathbb{Z}_2[[s]]$. The equation $s^{17} g(s) = \iota$ is $(s\, h(s))^{17} = \iota$, whose solutions in the open disc are $s = \varphi(\zeta\alpha t)$ with $\zeta^{17} = 1$, for a fixed root α of $X^{17} = 2^{11}$. They are distinct. For any finite extension M of $\mathbb{Q}_2$, the formal logarithm is an isomorphism from the points with $v_2(s) > 1$ onto $\{z \in M : v_2(z) > 1\}$, with $v_2(\log Y) = v_2(s(Y))$ [59, Theorem IV.6.4]. So every point with $v_2(s) > 2$ is divisible by 2 in $J(M)$.

(a) The point of the fibre near O has as parameter the unique root of $s\, g_1(s) = \iota$ in the open disc. It is Galois-invariant, so it lies in $J(\mathbb{Q}_2)$, and $v_2(s) = v_2(\iota) \geq 11 > 2$, so it lies in $2J(\mathbb{Q}_2)$. The 17 points near $-T$ are not $\mathbb{Q}_2$-rational, since $v_2(\zeta\alpha t) = 11/17 + v_2(t) \notin \mathbb{Z}$.

(b) $X^{17} - 2^{11}$ is irreducible over $\mathbb{Q}_2$, so $\mathbb{Q}_2(\alpha)$ is totally ramified of degree 17. So is K_{v_2} (Table 6). Thus $K_{v_2} = \mathbb{Q}_2(\pi)$ with $\pi^{17} = 2w$ for a unit w, which is a 17-th power by Hensel's lemma, as the residue field is $\mathbb{F}_2$. Hence K_{v_2} contains a root of $X^{17} - 2$, hence of $X^{17} - 2^{11}$, and $K_{v_2} \simeq \mathbb{Q}_2(\alpha)$. As $\mu_{17}(K_{v_2}) = 1$ (2 has order 8 modulo 17), exactly one of the 17 points near $-T$ is K_{v_2}-rational.

(c) If $t \equiv t' \pmod 4$, then $R_2(t) - R_2(t') = Q(t') - Q(t)$ has formal parameter of valuation $v_2(\varphi(\alpha t') - \varphi(\alpha t)) = 11/17 + v_2(t - t') > 2$, so it lies in $2J(K_{v_2})$. If $4 \mid t$, then $v_2(s(Q(t))) \geq 45/17 > 2$ and $R_2(t) \equiv -T \pmod{2J(K_{v_2})}$, and $\delta(-T) = \delta(T)$, as δ depends only on x. □

Proposition 7.5. *No primitive solution of $x^2 + y^3 = z^{17}$ with $abc \neq 0$ gives a rational point on $X_{54a1}(17)$.*

Proof. Suppose that one does, and let $P \in J(K)$ be the point of Proposition 2.12, with $j(P) = j_0 = 2^{-11} t^{-17}$ by Lemma 7.1(a). The image of P at v_1 is a $\mathbb{Q}_2$-point of the fibre, hence equal to $R_1 \in 2J(\mathbb{Q}_2)$, with class 0. The image at v_2 is a K_{v_2}-point of the fibre other than R_1: as $x(P)$ generates K (Proposition 2.12(b)), its image generates $K_{v_2} \neq \mathbb{Q}_2$. So it is $R_2(t)$, whose class is that of $R_2(t')$ for the representative $t' \in \{1, 2, 3\}$ of t mod 4, or that of T if $4 \mid t$. The pair of classes $(\delta_{v_2}(P), \delta_{v_1}(P))$ lies in the image of $\mathrm{Sel}^2(J/K)$ at the places above 2. It remains to show that none of the four possible pairs lies in this image. We give the pairs and the image, computed as in Appendix B.1, in explicit coordinates, and a linear form that separates them.

Coordinates. For a prime ℓ, let M be a totally ramified extension of $\mathbb{Q}_\ell$ of degree e, with uniformizer π_M (so its residue field is $\mathbb{F}_\ell$), and put $U_k = 1 + \pi_M^k \mathcal{O}_M$. If $\ell = 2$, the classes of π_M, of $1 + \pi_M^k$ for $k = 1, 3, \ldots, 2e - 1$, and of 5 form an $\mathbb{F}_2$-basis of $M^\times / M^{\times 2}$. If $\ell = 3$ and $\mu_3 \not\subset M$, the classes of $1 + \pi_M^k$ for $1 \leq k < 3e/2$ with $3 \nmid k$ form an $\mathbb{F}_3$-basis of $\mathcal{O}_M^\times / \mathcal{O}_M^{\times 3}$. Both follow from the action of the ℓ-th power map on the filtration: $(1 + x\pi_M^k)^\ell \equiv 1 + x^\ell \pi_M^{\ell k}$

(mod $U_{\ell k+1}$) if $k < e/(\ell-1)$, and $(1+x\pi_M^k)^\ell \equiv 1+\ell x\pi_M^k \pmod{U_{k+e+1}}$ if $k > e/(\ell-1)$. For $\ell = 2$ and $k = e$ one has $(1+x\pi_M^e)^2 \equiv 1+(x^2+ux)\pi_M^{2e} \pmod{U_{2e+1}}$, with $u \equiv 1$ the residue of $2/\pi_M^e$, and x^2+x vanishes on $\mathbb{F}_2$. So U_{2e} is generated modulo squares by $U_{2e+1} \subseteq M^{\times 2}$ and by $5 = 1+4$, and 5 is not a square in M because $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified. The coordinates of a class are computed from its unit part modulo $U_{\lfloor \ell e/(\ell-1)\rfloor+1}$ by removing at each step the lowest nontrivial term of the filtration: an index $k < \ell e/(\ell-1)$ with $\ell \nmid k$ contributes to the coordinate of $1+\pi_M^k$, and every other index is removed by an ℓ-th power, or by 5 at the index $2e$ when $\ell = 2$.

The classes and the image. Let β be the 17-th root of 2 in K_{v_2}. It exists and is unique by the proof of Lemma 7.4(b), and $\beta = 4\alpha^{-3}$. Let L_{v_1} and L_{v_2} be the completions of $L = K(i)$ at the places above v_1 and v_2. Then $L_{v_2} = K_{v_2}(i) = \mathbb{Q}_2(\Pi)$ with $\Pi = (1+i)/\beta^8$. Here $\Pi^{17} = 1+i$, so Π is a root of the Eisenstein polynomial $X^{34} - 2X^{17} + 2$, and $i = \Pi^{17} - 1$ and $\beta = -i\Pi^2$. We use the bases above for L_{v_2} with $\pi_M = \Pi$ ($e = 34$) and for $L_{v_1} = \mathbb{Q}_2(i)$ with $\pi_M = 1+i$ ($e = 2$). The latter basis consists of the classes of $1+i$, $2+i$, $-1+2i$ and 5. For a pair of classes $\sigma = (\sigma_{v_2}, \sigma_{v_1})$ we write $a_k(\sigma)$ for the coordinate of σ_{v_2} at $1+\Pi^k$, and $c_5(\sigma)$ and $c_5'(\sigma)$ for the coordinates of σ_{v_2} and σ_{v_1} at 5. Then:

- $\delta_{v_2}(T) = [5]$, since $x(T) - \theta = 8 - 2i$ is 5 times a square in $\mathbb{Q}_2(i)$ (Remark 3.12);
- the classes $\delta_{v_2}(R_2(t'))$, $t' = 1, 2, 3$, are given in the last rows of Table S2;
- the image Σ of $\mathrm{Sel}^2(J/K)$ in $L_{v_2}^\times/L_{v_2}^{\times 2} \times L_{v_1}^\times/L_{v_1}^{\times 2}$ has the basis $\sigma_1, \dots, \sigma_{11}$ of Table S2, and $\sigma_{11} = \delta(T)|_2$.

The linear form. Let $\chi = a_{43} + a_{57} + a_{63} + c_5 + c_5'$. Each basis vector in Table S2 has $\chi(\sigma_j) = 0$, so χ vanishes on Σ. Each of the four pairs $(\delta_{v_2}(R_2(t')), 0)$, $t' \in \{1, 2, 3\}$, and $(\delta_{v_2}(T), 0)$ has $\chi = c_5 = 1$. So none of these pairs lies in Σ. □

7.4. **The twist attached to 864c1.**

Proposition 7.6. *Let $K = K_{864c1}$ and let $P_0 \in J(K)$ be the point over $j(864c1) = 1536$. The only point $Q \in J(K) \setminus J(\mathbb{Q})$ with $j(Q) \in \mathbb{Q}$ in $\bigcup_{j_1}(j_1 + 2^{11}\mathbb{Z}_2)$, $j_1 \in \{-64, 960, 448, -576, -512\}$, is P_0. Hence no primitive solution of $x^2 + y^3 = z^{17}$ with $abc \neq 0$ gives a rational point on $X_{864c1}(17)$.*

Proof. The disc test. For each j_1 we apply Proposition 4.9 to the two half-families $j_1 + 2^{12}\mathbb{Z}_2$ and $j_1 + 2^{11} + 2^{12}\mathbb{Z}_2$, represented by j_1 and $j_1 + 2^{11}$. Conditions (i)–(iv) and (4.1) hold at every point over each j_1, with $\kappa = 2^{11}$, $e = 1$ and $\min \nu_\xi = 3$ for the four values from line 3 of [27, Table 1] and 2 for -512, and every representative root has $r(x') \le 5/2$. The numbers of class tuples are 16 for each half of the four discs of line 3 and 4 for each half of $-512 + 2^{11}\mathbb{Z}_2$. Exactly one class tuple lies in Σ, namely $\delta(P_0)|_2$, on the half $1536 + 2^{12}\mathbb{Z}_2$.

The known point. We apply the enumeration of Section 5.4 with $j_c = 1536$, $\kappa = 2^{12}$, $a = 2$ and $n_{\max} = 14$, with the data of Table S3. Here $\dim \Sigma = 11$, $\dim \Theta = 6$ and $\dim(\Sigma+\Theta) = 16$, so $\Sigma \cap \Theta = \{0, \delta(T)\}$ and Lemma 5.3 applies. The hypotheses of Lemma 5.4 hold at all 18 points over 1536, with ν above the separation at every place: $2y + x + 1$ and $x - 7$ are units and x is integral at P_0 at every place above 2, and $j(-P_0) \neq 1536$. The allowed conjugates $g_v P_{0,v}$ are those with the class of $P_{0,v}$, giving $2 \cdot 2 \cdot 4 \cdot 2 = 32$ tuples (g_v). For all $32 \cdot 2 \cdot 15 = 960$ branch data (u modulo 4, $0 \le n \le 14$) the class $\mathrm{cl}_m(S)$ of $S = Q - P_0$ is determined and lies outside $(\Sigma + \Theta)/\Theta$. By Lemma 5.3, $\tau = 0$, and $Q = P_0$.

No point of $J(\mathbb{Q})$ lies in the discs, as $v_2(j(T)), v_2(j(2T)) < 0$, and P_0 comes from no solution by Lemma 2.15(b). □

7.5. **The twist attached to 864b1.** Here the enumeration of Section 5.4 is carried out in full, for the known point that comes from the Catalan solutions $(\pm 3, -2, 1)$.

Proposition 7.7. *Let $K = K_{864\mathrm{b}1}$ and let $P_0 \in J(K)$ be the point over $j(864\mathrm{b}1) = -13824$. The only point $Q \in J(K) \setminus J(\mathbb{Q})$ with $j(Q) \in \mathbb{Q}$ in $D_{-3} \cup D_1 \cup D_{-1} \cup D_3 \cup D'$ is P_0. Hence every primitive solution of $x^2+y^3 = z^{17}$ with $abc \neq 0$ that gives a rational point on $X_{864\mathrm{b}1}(17)$ is $(\pm 3, -2, 1)$.*

Proof. The disc test. Let $Q \neq P_0$ be a point as in the statement. The sets of j-values, representatives and local data are those of Proposition 7.2, and the class tuples are computed over K. No class tuple of the sets covering the D_u lies in Σ. On each half of $D' = -13824 + 2^{11}\mathbb{Z}_2$ exactly two class tuples lie in Σ, namely $\delta(P_0)|_2$ and $\delta(P_0 + T)|_2$. So $j(Q) = -13824 + 2^{11}\tau$ with $\tau \in \mathbb{Z}_2 \setminus \{0\}$, and $(\delta_v(Q))_{v|2}$ is one of these two tuples.

The setting. We apply the enumeration of Section 5.4 with $j_c = -13824$ and $\kappa = 2^{11}$, so that the family is all of D'. We use the reference point P_0, these two class tuples and the data of Table S3. Here $\dim \Sigma = 11$, $\dim \Theta = 6$ and $\Sigma \cap \Theta = \{0, \delta(T)\}$, so Lemma 5.3 applies. The hypotheses of Lemma 5.4 hold at every point over -13824, with ν above the separation at every place. So $Q_v = \xi_v(\tau)$ for a centre $\xi_v = g_v P_{0,v}$ among the $2, 2, 8, 2$ points over -13824 whose x-coordinate generates K_v (Table S3), giving 64 tuples (g_v). We take $a = 3$ ($\tau_0 = 2^n u_0$ with $u_0 \in \{1, 3, 5, 7\}$), and a branch datum is a tuple (g_v), a class of $u = \tau/2^n \bmod 8$ and $n = v_2(\tau)$.

The fixed and branch terms. By Table S3, the branch term of (5.2) has level $\nu + n - 1$ at every place and for every centre, and the fixed term, for $g_v \neq 1$, has level 0, 1 or 2. So for $n \geq 6$ the second case of Section 5.4 applies: if $g_v \neq 1$ at some place, the branch terms there have level at least $\nu + n - c_v = \nu + n - 2 \geq 6$, above the fixed terms, and $(m, \mathrm{cl}_m(S))$ is that for $n = 6$. For the identity tuple, m grows with n and $\mathrm{cl}_m(S)$ stays the same.

The enumeration. We count the branch data with $n \leq 12$, which by the above cover every n. Those with $n \leq 5$ are counted from the representatives, and those with $6 \leq n \leq 12$ by scaling. There are $64 \cdot 4 \cdot 13 = 3328$ branch data with $n \leq 12$, of which 832 are allowed by the disc test, and all but 104 of these have a class outside $(\Sigma + \Theta)/\Theta$. The remaining 104 branch data all have $m = 1$ and the same class w_0. They are those in which the level $m = 1$ is attained only at the place of type $(4, 2)$. Table S4 sorts the 832 branch data by their centres, and Table S5 and its continuation give a basis of $\Sigma + \Theta$, the level and class of $2^{-d_v} \log_v(Q - P_0)$ at every place and centre, and the class of every branch datum.

The sieve. For these 104 branch data Lemma 5.3 gives $Q - P_0 = 2R' + \mathfrak{s}$ with $\mathfrak{s} \in J(K)_{\mathrm{tors}} = \langle T \rangle$ and $\delta(R') \in \{\sigma_0, \sigma_0 + \delta(T)\}$, the two Selmer classes whose restriction to the places above 2 lies in $w_0 + \Theta$ (Section 5.6). We apply Lemma 5.11 with $K' = K$, which is allowed since Q induces an isomorphism $\operatorname{Spec} K \to j^{-1}(j(Q))$ (Lemma 2.10). The prime 13 suffices. The places of K above 13 have residue degrees $1, 1, 4, 4, 4, 4$, so by Lemma 5.11(a) and (b) the reduction $\tilde{\jmath}$ of $j(Q)$ is ∞ or a value at which $G_{17}(x, \tilde{\jmath})$ is not squarefree modulo 13 or has irreducible factors of these degrees, that is, $\tilde{\jmath} \in \{0, 5, 8, 10, 12, \infty\}$. For each of the eight pairs $(\sigma, \mathfrak{s})$ with $\sigma \in \{\sigma_0, \sigma_0 + \delta(T)\}$ and $\mathfrak{s} \in \{0, T, 2T, 3T\}$, the class σ does not pass at 13 for $(P_0, 1, \mathfrak{s})$. So no $Q \neq P_0$ exists.

Finally, by Lemma 2.15(b) a primitive solution with $j_0 = -13824$ is $(\pm 3, -2, 1)$. □

An example. Take $n = 1$ and $u_0 = 1$, so $\tau_0 = 2$, with the centre $g_2 P_{0,v_1} \neq P_{0,v_1}$ at the place v_1 of type $(4, 1)$ and the centre $P_{0,v}$ at the places v_2, v_3, v_4 of types $(2, 1)$, $(2, 2)$, $(4, 2)$, numbered as in Table S5. At every place the point $\xi_v(2)$ has the class of $P_{0,v}$, so the class tuple is $\delta(P_0)|_2 \in \Sigma$, and the datum is allowed; it lies in the fourth row of

Table S4. At v_1 the fixed term $(g_2-1)\log_{v_1}(P_{0,v_1})$ has level 1 and the branch term has level $n+1=2$ (Table S3), so $d_{v_1}=1$, and the class of $2^{-1}\log_{v_1}(Q-P_0)$ is that of the fixed term, `0000001010` (Table S5(ii)). At v_2, v_3, v_4 the fixed term is 0, and d_v is the level of the branch term, $n+2=3$, $n+2=3$ and $n+1=2$. Each d_v is below the bound $\nu+a+n-2$ of Section 5.4, which is 4, 5, 5, 4 at $v_1,\dots,v_4$. So $m=1$, attained only at v_1, and $\mathrm{cl}_1(S)$ is the tuple w with the block `0000001010` at v_1 and zero blocks elsewhere. The basis of Table S5(i) is in echelon form, and reducing w by it means adding b_4 and b_5: this clears the block at v_1 and leaves a nonzero remainder, whose block at v_3 is `0000101110`. Hence $\mathrm{cl}_1(S)\notin(\Sigma+\Theta)/\Theta$, and the datum is excluded. The same levels and class occur for every u_0 and every n with $1\le n\le 12$, in the fourth row of the continuation of Table S5.

7.6. **Proof of Theorem A for $p=17$.** Let (a,b,c) be a primitive solution of $x^2+y^3=z^{17}$. If $abc=0$, then (a,b,c) is one of the six trivial solutions, as in the proof of Theorem A for $p=11$ (Section 6.4). If $abc\neq 0$, then by Theorem 2.1 it gives a rational point on $X_E(17)$ for some $E\in\{27\text{a}1, 54\text{a}1, 864\text{a}1, 864\text{b}1, 864\text{c}1\}$. Propositions 2.2, 7.5, 7.2 and 7.6 exclude 27a1, 54a1, 864a1 and 864c1, and Proposition 7.7 shows that 864b1 gives only $(\pm 3,-2,1)$. The 2-Selmer groups used in these propositions are determined without GRH (Proposition 3.11 and Appendix A). □

8. The exponent 19

Theorem A for $p=19$ is proved at the prime $\ell=3$. Here $J=X_0(19)$ and $T=(5,9)$ are as in Table 5, and δ is the Kummer map of the isogeny $\hat{\phi}$ with kernel μ_3 (Section 3.3). By Theorem 2.1, a primitive solution with $abc\neq 0$ gives a rational point on one of the eight twists of Table 4, attached to 54a1, 96a1, 864a1, 864b1, 864c1 (two twists) and 288a1 (two twists). For 54a1, 864a1, 864b1 and 864c1 the disc test (Proposition 8.1) and the enumeration at the known points (Proposition 8.3) suffice. New compared with $p=17$ are, for 288a1, known points at ramification points of j (Sections 8.5, 8.6 and 8.7); the cusps for 96a1 are treated as those for 54a1 at $p=17$ (Section 8.4).

8.1. **The 3-adic position of j_0.** For the curves without complex multiplication, Table 2 of [27] gives the 3-adic position of $j_0=1728b^3/c^{19}$ according to (a mod 9, b mod 3), and Table 3 of [27] the lines that go with each curve, through the inertial field at 3. Let $C_3=\{t^3 : t\in\mathbb{Z}_3\}$ be the set of cubes of $\mathbb{Z}_3$. For the five curves the tables give:

- 864b1, 864c1 (lines 3 and 5): $j_0\in 27+3^6\mathbb{Z}_3$, or $j_0\in 3^6C_3$, or $j_0\in 2\cdot 3^6C_3$;
- 54a1, 864a1 (lines 4 and 7): $j_0\in -216+3^6\mathbb{Z}_3$, or $j_0\in -108+3^5\mathbb{Z}_3$, or $j_0\in -27+3^5\mathbb{Z}_3$;
- 96a1 (line 1): $3\mid c$ and $j_0=3^{-16}t^{-19}$ with $t\in\mathbb{Z}_3\setminus\{0\}$.

The first two items are elementary consequences of the table, and a computation over all (a,b) modulo 3^8 confirms them. For instance, in line 3, $a=3a'$ with $3\nmid a'$ and $b\equiv 1 \pmod 3$, and $j_0-27=3^5(7b^3-a'^2)/(a^2+b^3)$ with $7b^3-a'^2\equiv 0 \pmod 3$. For 96a1, $c=3c'$ and $j_0=3^{-16}(2^6b^3)c'^{-19}$. The unit 2^6b^3 is a 19-th power in $\mathbb{Z}_3^\times$, which gives $v_3(t)=v_3(c)-1$.

We split these sets into families $\{j_c+\kappa t : t\in\mathbb{Z}_3\}$ or $\{\kappa t^3 : t\in\mathbb{Z}_3\}$ (Section 4.1). The set $27+3^6\mathbb{Z}_3$ splits into the three families $27+3^6t'+3^7\mathbb{Z}_3$ ($t'=0,1,2$). The set $3^6C_3\cup 2\cdot 3^6C_3$ splits into the four families $\pm 3^6u+3^8\mathbb{Z}_3$ ($u=1,2$), which are the values $3^6u\,t^3$ with $t\equiv\pm 1 \pmod 3$, and the two families $\{3^9u\,t^3 : t\in\mathbb{Z}_3\}$ ($u=1,2$). Lines 4 and 7 give 21 families: $-216+3^6t'+3^7\mathbb{Z}_3$ ($t'=0,1,2$), and $-108+3^5t'+3^7\mathbb{Z}_3$ and $-27+3^5t'+3^7\mathbb{Z}_3$ ($t'=0,\dots,8$).

8.2. **The disc test.**

Proposition 8.1. *Let E be one of the five curves without complex multiplication and $K = K_E$. For every family,* (i)–(iv) *and* (4.1) *hold at every root ξ of $G_{19}(x, j_c)$, with $\nu_\xi \geq 5/2$, and the hypotheses of Proposition 4.9 hold. The class tuples that lie in the image Σ of* $\mathrm{Sel}(K)$ *are:*

(a) *for* 864c1*: none, in any of the nine families;*

(b) *for* 864b1*: none in line 5; in each of the three families of line 3, exactly two, namely $\pm\delta(P_E)|_3$, where $j(P_E) = j(\text{864b1}) = -13824 \in 27 + 3^6\mathbb{Z}_3$;*

(c) *for* 864a1*: none, except in the family $-216 + 3^7\mathbb{Z}_3$, where exactly one tuple survives, $\delta(P_E)|_3$, with $j(P_E) = -216$;*

(d) *for* 54a1*: exactly one tuple on each of $-27+3^6\mathbb{Z}_3$, $378+3^6\mathbb{Z}_3$ and $-216+3^7\mathbb{Z}_3$, namely $\delta(P_E)|_3$, $\delta(P'_E)|_3$ and $\delta(P'_E - P_E)|_3$, where $j(P_E) = 9261/8$ and P'_E is the point over $j(\text{54a3}) = -132651/2$; none elsewhere.*

The point P'_E exists by Lemma 2.14, since 54a3 is 3-isogenous to 54a1. The j-invariants satisfy $9261/8 \equiv -27 + 2 \cdot 3^6$ and $-132651/2 \equiv 378 \pmod{3^7}$.

Proof. This is the computation of Section 4.4. In the families $\{3^9 u\, t^3 : t \in \mathbb{Z}_3\}$ the six roots of multiplicity 3 over $j_c = 0$ have $e_\xi = 3$, divisible by $\ell = 3$. There only Lemma 4.1 is used, through Lemma 4.4(a) and (c), which suffices because the representative of every family at $p = 19$ is its centre. For 864c1 the nine families have 14, 14, 14, 32, 32, 32, 32, 32, 32 class tuples, and none lies in Σ. Here Σ has dimension 11 in the product $\bigoplus_{v|3} \delta_v(J(K_v))$ of the local images, which has dimension $6 + 3 + 13 = 22$. For 54a1 the families of line 4 have 6 class tuples each and those of line 7 have 26. The surviving tuples are identified by comparison with the classes δ_v of the known points. □

Corollary 8.2. *No primitive solution of $x^2 + y^3 = z^{19}$ with $abc \neq 0$ gives a rational point on $X_{\text{864c1}}(19)$ or on $X^-_{\text{864c1}}(19)$.*

Proof. By Proposition 2.12 such a solution gives $P \in J(K) \setminus J(\mathbb{Q})$ with $j(P) = j_0$ in one of the nine families. Proposition 8.1(a) and Proposition 4.9 give a contradiction. □

8.3. **The known points.** The enumeration of Section 5.4 at $\ell = 3$ excludes the families of Proposition 8.1(b)–(d). In each case the completions of K above 3 are pairwise non-isomorphic, $T \notin 3J(K_v)$ at every place above 3, and $\Sigma \cap \Theta = \{0\}$, as that enumeration and Lemmas 5.6 and 5.7 require.

Proposition 8.3. (a) *Let $K = K_{\text{864a1}}$. The only point $Q \in J(K)$ with $j(Q) \in \mathbb{Q}$ in the 3-adic families allowed for* 864a1 *is P_E, with $j(P_E) = -216$.*

(b) *Let $K = K_{\text{864b1}}$. The only such point in the families allowed for* 864b1 *is P_E, with $j(P_E) = -13824$.*

(c) *Let $K = K_{\text{54a1}}$. The only such points in the families allowed for* 54a1 *are P_E and P'_E, with $j = 9261/8$ and $-132651/2$.*

Proof. By Proposition 8.1 it remains to treat the families that contain a surviving tuple. In all three fields the places above 3 have $(e, f) = (2, 1)$, $(6, 1)$, $(6, 2)$, and $\dim \Sigma = 11$. Table S7 lists the data of the five computations. In each of them the hypotheses of Lemma 5.8 hold at every centre, with ν above the separations, and every branch datum allowed by the disc test is determined, with its class outside $(\Sigma + \Theta)/\Theta$. The value $\tau = 0$ gives the known point itself, since $\mathrm{Aut}(K) = 1$. Then Lemma 5.7 completes the proof.

(a) For 864a1 we take $j_c = -216$ and $\kappa = 3^7$, and $n = 0, \dots, 10$. The conjugates of $P_{E,v}$ number $2, 2, 12$ at the three places, of which $2, 1, 6$ have the class of $P_{E,v}$. For $n \geq 4$ every branch term has level at least 5, above every fixed term (at most 2), so the outcome for $n \geq 4$ is that for $n = 4$, with all levels raised by $n - 4$ when every place uses the centre $P_{E,v}$.

(b) For 864b1 one family, with $j_c = -13824$ and $\kappa = 3^6$, covers the disc $27 + 3^6\mathbb{Z}_3$. The two surviving tuples $\pm\delta(P_E)|_3$ are treated with the reference points P_E and $-P_E$, that is, with $S = Q - P_E$ and $S = Q + P_E$, and $n = 0, \dots, 10$. At the two places with $e_v = 6$ we have $\nu = 3/2$, below the radius $N/e_v = 5/3$ of Lemma 4.8, so there Lemma 4.8 does not compare a point on a branch directly with its centre. Two points of one branch with $\tau \equiv \tau' \pmod 3$ satisfy $v_3(x - x') \geq \nu + 1 = 5/2$ by Lemma 4.4(b), so by Lemma 4.8, applied at either point, the class on a branch depends only on τ mod 3, and for $\tau \equiv 0$ it is the class of the centre. The classes at $\tau = 1, 2$, computed at every centre, are also those of the centres. So every point on a branch has the class of its centre.

(c) For 54a1 there are three families. On $-27 + 3^6\mathbb{Z}_3$ the reference point is P_E, and on $378 + 3^6\mathbb{Z}_3$ it is P'_E. On $-216 + 3^7\mathbb{Z}_3$ the surviving class is that of $R_0 = P'_E - P_E$, a point of $J(K)$ that does not lie over this family, and we use R_0 as the reference point, as in Section 5.4. No point of $J(K)$ lies over -216, since the fibre over -216 is $\operatorname{Spec} K_{864a1}$ and $K_{864a1} \not\simeq K_{54a1}$ (their discriminants differ, Table 6), so $\tau = 0$ does not occur there. The centres are the points over -216 whose x-coordinate generates K_v. They number $2, 2, 12$ at the three places, and $2, 1, 6$ of them have the class of R_0. □

8.4. **The twist attached to 96a1: points near the cusps.** For 96a1, j_0 is not 3-integral, and the argument of Section 5.3 runs with the cusps in place of a known point.

Proposition 8.4. *Let $K = K_{96a1}$. No point $Q \in J(K)$ has $j(Q) = 3^{-16}t^{-19}$ with $t \in \mathbb{Z}_3 \backslash \{0\}$. Hence no primitive solution of $x^2 + y^3 = z^{19}$ with $abc \neq 0$ gives a rational point on $X^-_{96a1}(19)$.*

Proof. Let $s = -x/y$ be the formal parameter at O. As at $p = 17$ (Lemma 7.3), for Q in the residue disc of O over a 3-adic field, $1/j(Q) = s\, g_1(s)$ and $1/j(-T - Q) = s^{19} g(s)$ with $g_1, g \in 1 + s\mathbb{Z}_3[[s]]$. Here $1/j$ is regular on the smooth model over $\mathbb{Z}_3$ near the cusps, with zeros of order 1 at O and 19 at $-T$. A uniformizer is s at O, and $Q' \mapsto s(-T - Q')$ at $-T$. A point with $v_3(j) < 0$ lies in the residue disc of a cusp.

By Table 6, $K \otimes \mathbb{Q}_3 = \mathbb{Q}_3 \times F$ with F totally ramified of degree 19. Since every 3-adic unit is a 19-th power, $F \simeq \mathbb{Q}_3(3^{1/19})$, so F contains exactly one 19-th root β of 3^{16} and no nontrivial 19-th root of unity. We write v_1 and v_2 for the places of K above 3 with completions $\mathbb{Q}_3$ and F. Let $j_0 = 3^{-16}t^{-19}$. Near O, $s\, g_1(s) = 3^{16}t^{19}$ has exactly one solution $s_1(t)$, giving $R_1(t) \in J(\mathbb{Q}_3)$. Near $-T$ there is no $\mathbb{Q}_3$-point, as $v_3(s)$ would be $16/19 + v_3(t)$. Let ψ be the compositional inverse of $s\, g(s)^{1/19}$. The solutions of $s^{19}g(s) = 3^{16}t^{19}$ are $s = \psi(\zeta\beta t)$ with $\zeta^{19} = 1$, and exactly one of them lies in F: $P_2(t) = -T - Q(t)$ with $s(Q(t)) = \psi(\beta t)$. If $Q \in J(K)$ has $j(Q) = j_0$, then $x(Q)$ generates K by Lemma 2.10, since the points of $J(\mathbb{Q})$ have $j \in \{\infty, j(T)\}$. So the image of Q at v_2 generates F and is $P_2(t)$, and its image at v_1 is $R_1(t)$.

The torsion of $J(K_v)$ of 3-power order is $\langle T \rangle$ at both places, since the formal groups have no 3-torsion, $\mu_3 \not\subset K_v$ and $\#\widetilde{J}(\mathbb{F}_3) = 6$. As $\delta_v(T) = 0$, we have $\Theta = 0$. The image of δ_v at each place above 3 is the group of unit classes, and $\mathrm{Sel}(K) = \mathcal{O}^\times_{K,\{19\}}/\mathcal{O}^{\times 3}_{K,\{19\}}$ has dimension 12 (Proposition 3.8(b), Corollary A.11), with image of rank 11 at 3. Now $\mathrm{Log}_{v_1}(R_1(t)) = \log s_1(t)$ has valuation $16 + 19n$, where $n = v_3(t)$. Also $\mathrm{Log}_{v_2}(P_2(t)) = -\mathcal{L}(t)$ with $\mathcal{L}(t) = \log \psi(\beta t) = \sum_k \gamma_k t^k$, $v_3(\gamma_1) = 16/19$ and $v_3(\gamma_k) \geq 29/19$ for $k \geq 2$. Here

$\psi(\beta t)=\beta t+\sum_{k\ge 2}p_k\beta^k t^k$ with $p_k\in\mathbb{Z}_3$, and the formal logarithm is $\sum_m a_m s^m/m$ with $a_m\in\mathbb{Z}_3$ and $a_1=1$, so $\gamma_1=\beta$ and $v_3(\gamma_k)\ge 16k/19-\max_{m\le k}v_3(m)\ge 29/19$ for $k\ge 2$.

So the comparison in the proof of Lemma 5.8 applies to $\mathcal{L}$ with $\nu=16/19$ and $a=1$. By Section 5.3, $3^k\Lambda_{v_2}$ contains the elements of F of valuation at least $k+10/19$, since $e_{v_2}=19$. For $t\equiv u \pmod 3$ with $u\in\{1,2\}$, $v_3(\mathcal{L}(t)-\mathcal{L}(u))\ge 35/19\ge 1+10/19$, so $\mathrm{Log}_{v_2}(P_2(t))\equiv\mathrm{Log}_{v_2}(P_2(u)) \pmod{3\Lambda_{v_2}}$. For $t=3^n u'$ with $n\ge 1$ and $u'\equiv u \pmod 3$, $v_3(3^{1-n}\mathcal{L}(t)-\mathcal{L}(3u))\ge 1+35/19\ge 2+10/19$, so $3^{1-n}\mathcal{L}(t)\equiv\mathcal{L}(3u) \pmod{9\Lambda_{v_2}}$. So, modulo torsion, $P_2(t)$ is 3^{n-1} times a point Y with $\mathrm{Log}_{v_2}Y\equiv\mathrm{Log}_{v_2}(P_2(3u)) \pmod{9\Lambda_{v_2}}$. We use the level and the class at a given level of Section 5.1, with $V=J(K_{v_2})$, $\varpi=[3]$, and levels taken modulo the torsion subgroup, so that the level of a point is the level of its logarithm in Λ_{v_2}. If $P_2(3u)$ has level 1, then so has Y, with the same class at level 1, and so $P_2(t)$ has level n and $\mathrm{cl}_n(P_2(t))=\mathrm{cl}_1(P_2(3u))$.

A computation of $R_1(t)$, $P_2(t)$ and their logarithms for $t=1,2,3,6$ (Appendix B.1, [32]) gives: for $u=1,2$ the level of $P_2(u)$ is 0, and for $t=3,6$ the level is 1 at v_2 and at least 34 at v_1. Since $\Lambda_{v_1}\supseteq 3\mathbb{Z}_3$ (Section 5.3), $R_1(t)$ has level at least $15+19n>n$ at v_1. So for $n=v_3(t)$ the level m of Q is n, attained at v_2 only, and by the previous paragraph the tuple of classes at level m is (class 0 at v_1, class of $P_2(u)$ at v_2) for $n=0$, and (class 0 at v_1, class of $P_2(3u)$ at level 1 at v_2) for $n\ge 1$. It remains to show that these tuples, for $u=1,2$, are not in Σ, with the coordinates of the proof of Proposition 7.5 and a linear form as there.

Let π be the 19-th root of 3 in F, so that $F=\mathbb{Q}_3(\pi)$ and $\beta=\pi^{16}$. At v_1 we use the isomorphism $\mathbb{Z}_3^\times/\mathbb{Z}_3^{\times 3}\to\mathbb{F}_3$, $u\mapsto a$, where $\pm u\equiv 1+3a \pmod 9$. The class of 4 has $a=1$. At v_2 we use the basis of the proof of Proposition 7.5 for $\ell=3$ and $e=19$, namely the classes of $1+\pi^k$ for $k\in\{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28\}$, and write b_k for the coordinate at $1+\pi^k$. Then:

- $\delta_{v_2}(P_2(1))=-[1+\pi^{16}]$ and $\delta_{v_2}(P_2(2))=[1+\pi^{16}]$. For $t=3$ and $t=6$ the classes at level 1 are those of $P_2(1)$ and $P_2(2)$ respectively, and all these points have class 0 at v_1;
- Σ is a graph: a unit class σ lies in Σ if and only if $(b_{16},b_{17},b_{19},b_{20},b_{22},b_{23},b_{25},b_{26},b_{28})=(a,b_1,b_2,b_4,b_5,b_7,b_8,b_{10},b_{11},b_{13},b_{14})$ times the matrix C of Table S8.

Let $\chi=-b_2-b_5+b_{16}+b_{17}+b_{19}$. The first three columns of C add up to the vector with entries 1 in the rows of b_2 and b_5 and 0 in the other rows. So χ vanishes on Σ, while $\chi(0,\mp[1+\pi^{16}])=\mp 1\ne 0$. Hence $(0,\pm[1+\pi^{16}])\notin\Sigma$.

But by Lemma 5.7 with $S=Q$, the tuple of classes of Q at level m lies in Σ, a contradiction. □

8.5. **The twists attached to 288a1.** Proposition 8.11 is proved in this subsection and the next two, in three steps. The disc test (Proposition 8.6) leaves, besides three families of line 8, three of the four families of line 2, whose j-values are close to 1728, the j-invariant of the two known points P_1, P_2. The sieve at good primes then shows that $\delta(P)$ is $\delta(P_1)$ or $\delta(P_2)$ and that j_0 lies on line 2 (Proposition 8.7). As 1728 is a branch value of j, the remaining j-values are treated by branches through ramification points (Section 8.7): the sign rule (Proposition 8.9) decides to which of P_1, P_2 the point is close, and the enumeration of Proposition 8.10, adapted from Section 5.4, excludes it.

Let $E=$ 288a1, the curve $y^2=x^3+3x$ with complex multiplication by $\mathbb{Z}[i]$, and $K=K_E$, the field of degree 20 of Proposition 2.9(a). The known points are the two points P_1, P_2 of $J(K)$ over $j(E)=1728$.

The field. The following facts supplement Proposition 2.9 and Table 6.

Proposition 8.5. (a) *The automorphism group of K has order 2. We write ι_K for its nontrivial element and K_{10} for the fixed field of ι_K. Besides $\mathbb{Q}$ and K, the field K has exactly one subfield of each of the degrees 2, 4, 5 and 10. The quadratic one is $\mathbb{Q}(\sqrt{19})$, and the one of degree 10 is K_{10}.*

(b) *The places of K above 2 have $(e, f) = (4, 1), (4, 2), (4, 2)$. The six places above 3 (Table 6) are fixed by ι_K. The two of residue degree 1, v_1 and v_2, have $K_{v_1} \simeq \mathbb{Q}_3(\sqrt{-3})$ and $K_{v_2} \simeq \mathbb{Q}_3(\sqrt{3})$. The completions at the other four, $v_3, \dots, v_6$, are isomorphic to $\mathbb{Q}_9(\sqrt{3})$, where $\mathbb{Q}_9$ is the unramified quadratic extension of $\mathbb{Q}_3$. So $\mu_3 \subset K_v$ for $v \neq v_2$, and $\mu_3 \not\subset K_{v_2}$.*

(c) *$G_{19}(x, 1728) = H_{10}(x)^2$, where $H_{10} \in \mathbb{Z}[x]$ is monic and irreducible of degree 10 and $H_{10} \equiv x(x+1)^3(x^2+1)^3 \pmod 3$. Exactly two roots of H_{10} lie in K, and both lie in K_{10}.*

Proof. These are computations with the defining polynomials of Appendix C.2 (Appendix B): the automorphisms and subfields in (a) with PARI's `nfgaloisconj` and `nfsubfields`, the places in (b) with `idealprimedec` in the maximal order, and (c) by factoring $G_{19}(x, 1728)$ over $\mathbb{Q}$ and H_{10} modulo 3, and with `nfroots` over K. □

The points over 1728. Each of the ten points of J over 1728 has ramification index 2. The automorphism $[i]$ acts on $E[19]$ as an element of $\mathbb{F}_{361} \setminus \mathbb{F}_{19}$, since $19 \equiv 3 \pmod 4$, and $[i]^2 = [-1]$, so the 20 subgroups of order 19 fall into ten orbits $\{C, [i]C\}$ under $\mathrm{Aut}(E)$. Let $P_1, P_2 \in J(K)$ be the two points over 1728 whose x-coordinates are the roots of H_{10} in K. A root ξ determines its point, which is $(\xi, y(\xi, 1728))$ with

$$y(x, j) = \frac{j(x-5)^{19} - \mathcal{A}_{19}(x)}{\mathcal{B}_{19}(x)},$$

because $\mathcal{B}_{19}$ is irreducible of degree 18 and so does not vanish at a number of degree 10. Both points lie in $J(K_{10})$. By Proposition 8.5(c), exactly one root of H_{10} in $\bar{\mathbb{Q}}_3$ lies in the maximal ideal, namely the root $\xi^{(0)} \in 3\mathbb{Z}_3$ that lifts the simple root 0 of H_{10} modulo 3. We number the two points so that $x(P_1)$ is mapped to $\xi^{(0)}$ at v_1. A computation shows that $x(P_2)$ is then mapped to $\xi^{(0)}$ at v_2. One of P_1, P_2 is the point given by (E, C_0), with C_0 as in Proposition 2.9. A solution with $abc \neq 0$ has $j_0 \neq 1728$, so it gives neither point.

The Selmer group. By Proposition 3.8, $\dim \mathrm{Sel}(K) = 11$, $\delta\colon J(K)/3J(K) \to \mathrm{Sel}(K)$ is injective, and the restriction of $\mathrm{Sel}(K)$ to the places above 3 has kernel spanned by $\delta(T)$, the class of $-1/19$. The local images $\delta_v(J(K_v))$ at $v_1, \dots, v_6$ have dimensions $3, 2, 5, 5, 5, 5$, in groups $K_v^\times/K_v^{\times 3}$ of dimensions $4, 3, 6, 6, 6, 6$. The image Σ of $\mathrm{Sel}(K)$ in the 25-dimensional space $\bigoplus_{v|3} \delta_v(J(K_v))$ has dimension 10. This holds without GRH (Corollary A.11).

The 3-adic position of j_0. Let (a, b, c) be a primitive solution with $abc \neq 0$ that gives a rational point on one of the two twists. By Theorem 2.1, $3 \nmid c$, and by [27, Tables 2 and 3] the pair ($a \bmod 9, b \bmod 3$) lies in line 2, 6 or 8 of [27, Table 2]. These lines give:

- line 2 ($9 \mid a$):
$$j_0 = 1728 - \varsigma\, 3^7 \tau^2 \qquad \text{with } \varsigma \in \{1, -1\},\ \varsigma \equiv c \pmod 3,\ \tau \in \mathbb{Z}_3 \setminus \{0\}; \tag{8.1}$$
- line 6 ($a \equiv \pm 4 \pmod 9$, $3 \mid b$): $j_0 \in 4 \cdot 3^6 C_3$, with C_3 as in Section 8.1;
- line 8 ($a \equiv \pm 2 \pmod 9$, $b \equiv 1 \pmod 3$): $j_0 \in 54 + 3^5\mathbb{Z}_3$.

For line 2 write $a = 9a'$, and write $1/c = \varsigma\, w^2$ with $\varsigma = \pm 1$ and $w \in \mathbb{Z}_3^\times$, which is possible because every 3-adic unit is ± 1 times a square. Then $1728 - j_0 = 1728a^2/c^{19} = 2^6 3^7 a'^2/c^{19} =$

$\varsigma\,3^7\tau^2$ with $\tau = 8a'w/c^9$, and $\tau \neq 0$ because $a \neq 0$. Moreover $\varsigma \equiv c \pmod 3$. Lines 6 and 8 follow from the table as in Section 8.1, and a computation modulo 3^8 confirms all three lines.

We cover these sets by sixteen families. Line 8 gives the nine families $54+3^5t'+3^7\mathbb{Z}_3$ with $0 \le t' \le 8$. Line 6 gives the families $\pm 2916 + 3^8\mathbb{Z}_3$, which contain the values $4\cdot 3^6t^3$ with $t \equiv \pm 1 \pmod 3$ (as $t^3 \equiv \pm 1 \pmod 9$), and $\{4\cdot 3^9t^3 : t \in \mathbb{Z}_3\}$. Line 2 gives $-459+3^8\mathbb{Z}_3$ and $3915+3^8\mathbb{Z}_3$, which contain the values (8.1) with $3 \nmid \tau$ for $\varsigma = 1$ and $\varsigma = -1$ (as $\tau^2 \in 1+3\mathbb{Z}_3$), and the two families $\{1728 - \varsigma\,3^9t^2 : t \in \mathbb{Z}_3\}$, which are the values with $3 \mid \tau$.

Proposition 8.6. *For each of the sixteen families,* (i)–(iv) *and* (4.1) *hold at every root ξ of $G_{19}(x, j_c)$, with $\nu_\xi \ge 5/2$, and the hypotheses of Proposition 4.9 hold. The class tuples that lie in Σ are the following.*

(a) *None on the three families of line 6, none on the six families of line 8 with $t' \not\equiv 1 \pmod 3$, and none on $3915+3^8\mathbb{Z}_3$.*

(b) *On each of the three families of line 8 with $t' \equiv 1 \pmod 3$, whose union is $297+3^6\mathbb{Z}_3$: the same two tuples $\pm h$. The tuple h is not the restriction to the places above 3 of any element of the subgroup of $\mathrm{Sel}(K)$ generated by $\delta(P_1)$, $\delta(P_2)$ and $\delta(T)$.*

(c) *On $-459+3^8\mathbb{Z}_3$: exactly one tuple, $\delta(P_1)|_3$.*

(d) *On $\{1728 - \varsigma\,3^9t^2 : t \in \mathbb{Z}_3\}$, for either sign ς: the same ten tuples, among them $0 = \delta(T)|_3$, $\delta(P_1)|_3$ and $\delta(P_2)|_3$. The other seven are not restrictions of elements of the subgroup generated by $\delta(P_1)$, $\delta(P_2)$ and $\delta(T)$.*

Proof. This is the computation of Section 4.4. The families have 57122 class tuples each on line 8, 16384 each on line 6, and 256, 4802, 1024 and 1024 on the families $-459+3^8\mathbb{Z}_3$, $3915+3^8\mathbb{Z}_3$, $\{1728-3^9t^2\}$ and $\{1728+3^9t^2\}$ of line 2. The smallest value of ν_ξ is $7/2$ on line 8 and $5/2$ on lines 2 and 6. As in Proposition 8.1, only Lemma 4.1 is used, through Lemma 4.4(a) and (c), at the six roots of multiplicity 3 over the centre $j_c = 0$ of $\{4\cdot 3^9t^3\}$. These have $\nu_\xi = 5/2$ and separation $1/2$, and the two simple roots have $\nu_\xi = 15/2$ and separation $3/2$. In the families $\{1728 - \varsigma\,3^9t^2\}$ the ten roots of H_{10} have $e_\xi = 2$, with $\nu_\xi = 9/2$ at $\xi^{(0)}$ and $5/2$ at the other nine. The identification of the surviving tuples uses $\delta(T)|_3 = 0$ (as $19 \equiv 1 \pmod 9$) and the classes $\delta_v(P_1)$, $\delta_v(P_2)$. □

8.6. **A sieve at good primes.** The sieve of Section 5.6 leaves only the Selmer classes of P_1 and P_2 (Proposition 8.7). At $p = 19$ the following criterion shows when the closed points of a fibre modulo q are read off from the factorization of $G_{19}(x, \tilde{\jmath})$. Two distinct geometric points of J with the same x-coordinate are a point R and $-R \neq R$. If both lie in the fibre over $\tilde{\jmath}$, then $j_q(R) - j_q(-R) = \mathcal{B}_{19}(x)(2y+1)/(x-5)^{19}$ vanishes at R, with $2y+1 \neq 0$, and $(2y+1)^2 = 4(x^3+x^2-9x-15)+1$ on J. So if no root r of $G_{19}(x,\tilde{\jmath})$ has both $\mathcal{B}_{19}(r) = 0$ and $4(r^3+r^2-9r-15)+1 \neq 0$, then x separates the geometric points of the fibre, and its closed points are described by the factorization of $G_{19}(x,\tilde{\jmath})$ over $\mathbb{F}_q$ as in Section 5.6.

Proposition 8.7. *Let (a,b,c) be a primitive solution of $x^2+y^3=z^{19}$ with $abc \neq 0$ that gives a rational point on $X_{288\mathrm{a}1}(19)$ or on $X^-_{288\mathrm{a}1}(19)$, and let $P \in J(K)$ be the point of Proposition 2.12. Then $\delta(P) \in \{\delta(P_1), \delta(P_2)\}$, and j_0 lies on line 2 of* [27, Table 2].

Proof. By Proposition 2.12(a), P induces an isomorphism $\operatorname{Spec} K \to j^{-1}(j_0)$, so Lemma 5.11 applies with $K' = K$ and $Q = P$ at every prime $q \notin \{2,3,19\}$, at which K is unramified. The class $\delta(P)$ lies in $\mathrm{Sel}(K)$, and by Propositions 8.6 and 4.9 its restriction to the places above 3 is one of the tuples of Proposition 8.6(b)–(d). These are twelve distinct tuples: the two tuples $\pm h$, and the ten tuples of (d), one of which is $\delta(P_1)|_3$. The restriction map has

kernel $\langle\delta(T)\rangle$ (Proposition 3.8(c)), so each tuple is the restriction of exactly three elements of $\mathrm{Sel}(K)$, and $\delta(P)$ is one of these 36 classes.

We apply the test of Section 5.6 at the primes $q = 13$, 23, 43 and 67; among the primes $5 \le q \le 67$ with $q \ne 19$, these four suffice. The prime 13 has one place above it in K, of degree 20. The primes 23 and 43 have ten places each, of degree 2, and 67 has two places of degree 1 and nine of degree 2. Taking the primes in this order, the test excludes 24, 5, 3 and 2 of the 36 classes, and the two classes that pass at all four primes are $\delta(P_1)$ and $\delta(P_2)$. So $\delta(P) \in \{\delta(P_1), \delta(P_2)\}$. By Proposition 8.6, no tuple survives on line 6, and on line 8 only the tuples $\pm h$ survive, which differ from $\delta(P_1)|_3$ and $\delta(P_2)|_3$. So j_0 lies on line 2. □

8.7. **The ramification points over 1728.** It remains to exclude the solutions on line 2. The families are $\{1728 + \kappa t^2 : t \in \mathbb{Z}_3\}$ with $\kappa = \pm 3^7$, and every root of H_{10} has $e_\xi = 2$, prime to $\ell = 3$, so Lemma 4.2 gives the branches through these roots (Remark 4.3).

Data at the roots of H_{10}. For $\kappa = \pm 3^7$, conditions (i)–(iv) and (4.1) hold at every root ξ of H_{10}, for the family $\{1728 + \kappa t^2\}$ with $e = e_\xi = 2$. Here $\nu_\xi = 7/2$ at $\xi^{(0)}$, and $v_3(\xi^{(0)} - \xi') = 0$ for every other root ξ'. At each of the other nine roots ξ, $\nu_\xi = 3/2$ and $\max_{\xi' \ne \xi} v_3(\xi - \xi') = 1$. At every root, ξ and $y_\xi = y(\xi, 1728)$ are integral, and $2y_\xi + 1$ and $\mathcal{B}_{19}(\xi)$ are units. We write $R_\xi = (\xi, y_\xi)$ for the point of J over 1728 with x-coordinate ξ, and c_ξ for the coefficient c of Section 4.1 at ξ, so that $\nu_\xi = v_3(c_\xi)/2$.

Lemma 8.8 (ramified branches)**.** *Let $\kappa \in \{3^7, -3^7\}$, let $v \mid 3$ be a place of K, let $\xi \in \bar{\mathbb{Q}}_3$ be a root of H_{10}, put $\nu = \nu_\xi$, and let $\gamma \in \bar{\mathbb{Q}}_3$ with $\gamma^2 = c_\xi$.*

(a) *There is a power series $\varphi_\xi \in \mathbb{Q}_3(\xi, \gamma)[[t]]$ with linear term γt, converging on $|t| \le 1$ with Gauss norm $|\gamma| = 3^{-\nu}$ attained only at its linear term, such that the following holds for every $\tau \in \mathbb{Z}_3 \setminus \{0\}$. The points of J over $1728 + \kappa\tau^2$ with $v_3(x - \xi) \ge \nu$ are exactly $R_\xi(\tau)$ and $R_\xi(-\tau)$, where $R_\xi(t) = (\xi + \varphi_\xi(t), y(\xi + \varphi_\xi(t), 1728 + \kappa t^2))$, and these two points are distinct.*

(b) *Let $\xi \in K_v$. If $\gamma \in K_v$, then $R_\xi(\tau) \in J(K_v)$ for every $\tau \in \mathbb{Z}_3$. If $\gamma \notin K_v$, then $R_\xi(\tau) \notin J(K_v)$ for every $\tau \in \mathbb{Z}_3 \setminus \{0\}$. If $\xi \notin K_v$, no point of $J(K_v)$ over $1728 + \kappa\tau^2$ has $v_3(x - \xi) \ge \nu$.*

(c) *Let $\xi, \gamma \in K_v$. For $\tau \in \mathbb{Z}_3$, $R_\xi(\tau) - R_\xi$ lies in the formal group, and*

$$\mathcal{L}_\xi(\tau) \coloneqq \mathrm{Log}_v R_\xi(\tau) - \mathrm{Log}_v R_\xi = \sum_{k \ge 1} b_k \tau^k, \qquad v_3(b_1) = \nu, \quad v_3(b_k) > \nu \ (k \ge 2).$$

If $\tau = 3^n u$ and $\tau_0 = 3^{n_0} u_0$ with $u, u_0 \in \mathbb{Z}_3^\times$, $u \equiv u_0 \pmod{3^a}$, and either $n = n_0$ or $n, n_0 \ge a$, then $v_3(3^{-n}\mathcal{L}_\xi(\tau) - 3^{-n_0}\mathcal{L}_\xi(\tau_0)) \ge \nu + a$.

(d) *Let $\xi, \gamma \in K_v$, and let $\tau, \tau' \in \mathbb{Z}_3$ with $\nu + v_3(\tau - \tau') \ge 2$. Then $\delta_v(R_\xi(\tau)) = \delta_v(R_\xi(\tau'))$.*

Proof. Let $M = \mathbb{Q}_3(\xi)$ and let $F(X, Y)$ be the polynomial of Section 4.1 at ξ, that is, $G_{19}(\xi + Y, 1728 + \kappa X)$ divided by its coefficient of $X^0 Y^2$.

(a) As $3 \nmid 2$, Lemma 4.2 applies with $e = 2$ and $r = 1$. It gives two power series φ_0, φ_1 with coefficients in $M(\gamma)$, converging on $|t| \le 1$, with Gauss norm $|\gamma|$ attained only at their linear terms γt and $-\gamma t$. For $\tau \in \mathbb{Z}_3$ the values $\varphi_0(\tau)$, $\varphi_1(\tau)$ are the roots of $F(\tau^2, Y)$ with $|Y| \le |\gamma|$, and $|\varphi_0(\tau) - \varphi_1(\tau)| = |\gamma||\tau|$. The last equality is where $\ell \nmid e$ is used: in the proof of Lemma 4.2, $\varphi_k = \gamma t\, w_k$ with $|w_k - (-1)^k| < 1$ on the disc, and $|2| = 1$. As recalled in Section 4.1, $\varphi_1(t) = \varphi_0(-t)$. Put $\varphi_\xi = \varphi_0$. By Lemma 4.4(a) and (b), for $\tau \in \mathbb{Z}_3$ the roots x of $G_{19}(x, 1728 + \kappa\tau^2)$ with $v_3(x - \xi) \ge \nu$ are $\xi + \varphi_\xi(\tau)$ and $\xi + \varphi_\xi(-\tau)$, and they are distinct

if $\tau \neq 0$. Each of them is the x-coordinate of exactly one point of the fibre, namely $R_\xi(\pm\tau)$, because $\mathcal{B}_{19}$ is a unit on the disc $v_3(x-\xi) > 0$.

(b) Put $s = \gamma t$. The polynomial $F(s^2/c_\xi, sW)$ is divisible by s^2, because F has no terms X^0Y^0 and X^0Y^1, and $F(s^2/c_\xi, sW)/s^2$ lies in $M[s, W]$ and equals $W^2 - 1$ at $s = 0$. As $2 \neq 0$, there is a unique power series $W_\xi \in M[[s]]$ with $W_\xi(0) = 1$ that solves $F(s^2/c_\xi, sW)/s^2 = 0$. Then $\gamma t\, W_\xi(\gamma t)$ is a formal solution of $F(t^2, Y) = 0$ with linear term γt, so it is φ_ξ, since by the same argument the formal solution with this linear term is unique. If $\gamma \in K_v$, the coefficients of φ_ξ lie in K_v, so $R_\xi(\tau) \in J(K_v)$ for $\tau \in \mathbb{Z}_3$. If $\gamma \notin K_v$, let ρ be an automorphism of $\bar{\mathbb{Q}}_3$ over K_v with $\rho(\gamma) = -\gamma$. For $\tau \in \mathbb{Z}_3$, $\rho(\varphi_\xi(\tau)) = -\gamma\tau\, W_\xi(-\gamma\tau) = \varphi_\xi(-\tau)$, so ρ exchanges $R_\xi(\tau)$ and $R_\xi(-\tau)$, which are distinct for $\tau \neq 0$ by (a), so neither lies in $J(K_v)$. If $\xi \notin K_v$, then by Lemma 4.4(c) every root of $G_{19}(x, 1728 + \kappa\tau^2)$ in K_v lies in the disc about a root in K_v, and these discs are disjoint from the disc about ξ by Lemma 4.4(a).

(c) We argue as in the proof of Lemma 5.8, comparison included, with φ_ξ in place of X_ξ. As $\mathcal{B}_{19}$ is a unit near ξ, $R_\xi(\tau)$ lies in the residue disc of R_ξ, where $z = x - \xi$ is a coordinate because $2y_\xi + 1$ is a unit. Then $t_\xi(\tau) \coloneqq t(R_\xi(\tau) - R_\xi) = \mathcal{T}(\varphi_\xi(\tau))$ with $\mathcal{T} \in z\mathcal{O}_v[[z]]$ and $\mathcal{T}'(0)$ a unit. By (a), t_ξ has Gauss norm $|\gamma|$, attained only at its linear term, and so has $\mathcal{L}_\xi = \log \circ t_\xi$, since $3^{v_3(k)}|\gamma|^k < |\gamma|$ for $k \geq 2$, as $v_3(k) \leq (k-1)/2 < (k-1)\nu$ for $\nu > 1/2$.

(d) By Lemma 4.4(b), every coefficient of φ_ξ has valuation at least ν, so $v_3(x(R_\xi(\tau)) - x(R_\xi(\tau'))) \geq \nu + v_3(\tau - \tau') \geq 2$. Both points lie in the residue disc of R_ξ, and $R_\xi(\tau')$ has integral coordinates with $2y + 1$ a unit. As $e_v = 2$, the bound $v_3 \geq 2$ is the bound $v_v \geq 4 = \lfloor 3e_v/2 \rfloor + 1$ of Lemma 4.8, which gives the equality of the classes. □

Proposition 8.9 (the sign rule)**.** *Let $\varsigma \in \{1, -1\}$. Put $P_0 = P_1$ and $v = v_1$ if $\varsigma = 1$, and $P_0 = P_2$ and $v = v_2$ if $\varsigma = -1$. Let $Q \in J(K)$ with $j(Q) \in \mathbb{Q}$ and $j(Q) = 1728 - \varsigma\, 3^7\tau^2$ for some $\tau \in \mathbb{Z}_3 \setminus \{0\}$. Then $\delta_v(Q) = \delta_v(P_0)$. Consequently, if $\delta(Q) \in \{\delta(P_1), \delta(P_2)\}$, then $\delta(Q) = \delta(P_0)$.*

Proof. Put $\kappa = -\varsigma\, 3^7$, and call a root $\xi \in K_v$ of H_{10} a *centre* at v if c_ξ is a square in K_v. (In Section 8.7 a centre is thus a root of H_{10}, not a point of $J(K_v)$ as in Section 5.4.) We use two computed facts. First, for $\kappa = -3^7$ the only centre at v_1, and the only centre at v_2, is the image of $x(P_1)$. For $\kappa = 3^7$ it is the image of $x(P_2)$. So at the place v of the statement the only centre is the image of $x(P_0)$, which is $\xi^{(0)}$, with $\nu = 7/2$. Second, $\delta_{v_1}(P_1) = 0 \neq \delta_{v_1}(P_2)$ and $\delta_{v_2}(P_2) = 0 \neq \delta_{v_2}(P_1)$.

Let Q_v be the image of Q in $J(K_v)$. By Lemma 4.4(c), $x(Q_v)$ lies in the disc about a root $\xi \in K_v$ of H_{10}. By Lemma 8.8(a) and (b), $Q_v \in \{R_\xi(\tau), R_\xi(-\tau)\}$ and ξ is a centre, so $\xi = \xi^{(0)}$ is the image of $x(P_0)$, and $R_\xi = P_{0,v}$. As $\nu + v_3(\pm\tau - 0) \geq 7/2 \geq 2$, Lemma 8.8(d) with $\tau' = 0$ gives $\delta_v(Q) = \delta_v(R_\xi(0)) = \delta_v(P_0)$. The last statement follows, since $\delta_v(P_0)$ differs from the class at v of the other point. □

Proposition 8.10. *Let ς and P_0 be as in Proposition 8.9. There is no point $Q \in J(K)$ with $j(Q) \in \mathbb{Q} \setminus \{1728\}$, $j(Q) = 1728 - \varsigma\, 3^7\tau^2$ for some $\tau \in \mathbb{Z}_3$, and $\delta(Q) = \delta(P_0)$.*

Proof. Suppose that such a Q exists, and put $S = Q - P_0 \in J(K)$. We derive a contradiction with Lemma 5.7 by the enumeration of Section 5.4, adapted to the ramification of j over 1728.

The hypotheses of Lemma 5.7. The hypothesis $T \notin 3V_v$ of Lemma 5.6 holds at every place $v \mid 3$, by the remark after that lemma. The lattices Λ_v are $3\mathcal{O}_{K_v}$ at v_1, $\pi\mathcal{O}_{K_v}$ at v_2 (for a uniformizer π), and sublattices of index 3 of $\pi\mathcal{O}_{K_v}$ at $v_3, \dots, v_6$. The groups Θ_v, spanned by the classes of the points of $C \simeq \mu_3$ (Section 3.3), have dimensions $1, 0, 1, 1, 1, 1$ at $v_1, \dots, v_6$, so $\dim \Theta = 5$. As $\dim \Sigma = 10$ and $\dim(\Sigma + \Theta) = 15$, we have $\Sigma \cap \Theta = \{0\}$.

The local form of Q. Put $\kappa = -\varsigma\, 3^7$. Since $j(Q) \neq 1728$, $\tau \neq 0$, and replacing τ by $-\tau$ we may assume $\tau = 3^n u$ with $n \geq 0$ and $u \equiv u_0 \pmod 9$ for some $u_0 \in \{1, 2, 4\}$. With centres as in the proof of Proposition 8.9, Lemma 4.4(c) and Lemma 8.8(a) and (b) give, for every $v \mid 3$, a centre ξ_v at v and a sign ϱ_v with $Q_v = R_{\xi_v}(\varrho_v \tau)$, and then

$$\operatorname{Log}_v S = \operatorname{Log}_v(R_{\xi_v} - P_{0,v}) + \mathcal{L}_{\xi_v}(\varrho_v \tau). \tag{8.2}$$

This is the formula of Section 5.4 with reference point P_0, and we write $x(P_0)$ also for its image in K_v. At v_1 and at v_2 the only centre is the image of $x(P_0)$ (proof of Proposition 8.9). At each of $v_3, \dots, v_6$ all ten roots of H_{10} are centres, one with $\nu = 7/2$ and nine with $\nu = 3/2$, and all of them are used. As the completions at $v_3, \dots, v_6$ are isomorphic, the centres are not restricted to conjugates of $P_{0,v}$.

Representatives and allowed pairs. Put $\tau_0 = 3^{\min(n,3)} u_0$. Then $v_3(\tau - \tau_0) \geq 2$: for $n \leq 3$ because $u \equiv u_0 \pmod 9$, and for $n \geq 4$ because $v_3(\tau - \tau_0) = 3$. By Lemma 8.8(d), $\delta_v(R_\xi(\varrho\tau)) = \delta_v(R_\xi(\varrho\tau_0))$ for every centre ξ and sign ϱ. As $\delta(Q) = \delta(P_0)$, the pair (ξ_v, ϱ_v) is *allowed*: $\delta_v(R_{\xi_v}(\varrho_v\tau_0)) = \delta_v(P_0)$.

Levels and classes. Let d_v be the level of $\operatorname{Log}_v S$ in Λ_v, and consider the class of $3^{-d_v} \operatorname{Log}_v S$ modulo $3\Lambda_v$, an element of $\delta_v(V_v)/\Theta_v$ by Lemma 5.6. For $n \leq 3$ these are computed from (8.2) at τ_0, for every allowed pair at every place. They are the same for every τ in the class of τ_0 whenever $d_v < \lfloor \nu + n + 1 \rfloor$. By Lemma 8.8(c) with $a = 2$, $\mathcal{L}_\xi(\varrho\tau) - \mathcal{L}_\xi(\varrho\tau_0)$ has valuation at least $\nu + n + 2$, and elements of valuation at least c lie in $3^{\lfloor c-1 \rfloor}\Lambda_v$, since $\Lambda_v \supseteq 3\mathcal{O}_{K_v}$. This is the bound $\lfloor \nu + a + n - c_v \rfloor$ of Section 5.4 with $a = 2$ and $c_v = 1$, and $d_v < \lfloor \nu + n + 1 \rfloor$ holds in every case. For $n \geq 4$ the values are obtained from $n = 3$. At the centre $x(P_0)$ the fixed term vanishes, and by Lemma 8.8(c) with $n, n_0 \geq 2$ the level increases by $n - 3$ while the class does not change. This uses that $d_v - 3 < \lfloor \nu + 1 \rfloor$ at $n = 3$, which holds in every case. At the other centres the fixed term has level at most 2, below the level $\lfloor \nu + n - 1 \rfloor \geq 4$ of the branch term, so d_v and the class are those of the fixed term. So the local outcomes are computed at representatives with $n \leq 3$ only, and for every $n \geq 4$ they are those at $n = 3$, with the level at the centre $x(P_0)$ raised by $n - 3$.

The computation. The level of $\bar{S}$ is $m = \min_v d_v$, and by Lemma 5.7 the class $\operatorname{cl}_m(S)$, read off at the places with $d_v = m$, lies in $(\Sigma + \Theta)/\Theta$. In this proof, in place of the branch data of Section 5.4, a *branch datum* is a choice of u_0, of $n \leq 12$, and of one local outcome (d_v and the class) at each place, among the distinct outcomes of the allowed pairs at that place. For $P_0 = P_1$ there are 53184 branch data, and in each of them $\operatorname{cl}_m(S)$ lies outside $(\Sigma + \Theta)/\Theta$. For $P_0 = P_2$ and $n = 0$ no pair at v_1 is allowed, for each of the three values of u_0. For $P_0 = P_2$ and $1 \leq n \leq 12$ there are 44928 branch data, and in each of them the class lies outside $(\Sigma + \Theta)/\Theta$. In every branch datum all the d_v and classes are determined. The centres $x(P_0)$ contribute $d_v = n + 2$ at v_1 and $n + 1$ at $v_2, \dots, v_6$ for P_1, and $d_v = n$ at $v_1, v_3, \dots, v_6$ and $n + 3$ at v_2 for P_2. The local computations are made with the error bounds of Appendix B.1. For $n \geq 4$ every contribution of a centre $x(P_0)$ is at least 4, above every fixed term. So, as in the second case of Section 5.4, a branch datum with $n \geq 4$ has the outcome of the one with $n = 4$ and the same choices: m and all d_v are raised by $n - 4$ when every place uses the centre $x(P_0)$, and otherwise m and $\operatorname{cl}_m(S)$ are unchanged. Hence the enumeration up to $n = 12$ covers every n. Table S9 and its continuation give a basis of $\Sigma + \Theta$ and the local outcomes at each place, from which every branch datum can be checked. So $\operatorname{cl}_m(S) \notin (\Sigma + \Theta)/\Theta$ in every branch datum, which contradicts Lemma 5.7. □

Proposition 8.11. *No primitive solution of $x^2 + y^3 = z^{19}$ with $abc \neq 0$ gives a rational point on $X_{288a1}(19)$ or on $X^-_{288a1}(19)$.*

Proof. Let $P \in J(K)$ be the point of Proposition 2.12 of such a solution. By Proposition 8.7, $\delta(P) \in \{\delta(P_1), \delta(P_2)\}$ and j_0 lies on line 2, so $j_0 = 1728 - \varsigma\, 3^7 \tau^2$ with $\varsigma = \pm 1$ and $\tau \in \mathbb{Z}_3 \setminus \{0\}$, by (8.1). By Proposition 8.9, $\delta(P) = \delta(P_0)$, where $P_0 = P_1$ if $\varsigma = 1$ and $P_0 = P_2$ if $\varsigma = -1$. As $j_0 \in \mathbb{Q} \setminus \{1728\}$, this contradicts Proposition 8.10 with $Q = P$. □

8.8. **Proof of Theorem A for $p = 19$.** Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{19}$. If $abc = 0$, it is one of the trivial solutions, found as in Section 7.6. Suppose that $abc \neq 0$ and $(a, b, c) \neq (\pm 3, -2, 1)$. By Theorem 2.1, the solution gives a rational point on one of eight twists. This is impossible for the two twists attached to 288a1 by Proposition 8.11, for the two attached to 864c1 by Corollary 8.2, and for the one attached to 96a1 by Proposition 8.4. For 864a1, 864b1 and 54a1, Propositions 2.12, 8.1, 4.9 and 8.3 give $j_0 \in \{-216, -13824, 9261/8, -132651/2\}$. These are known j-invariants, so by Lemma 2.15(b) the solution is $(\pm 3, -2, 1)$, which was excluded. The proof holds without GRH, since the Selmer groups are determined without it (Corollary A.11). □

9. The exponent 23

We prove Theorem B(a), the case $p = 23$, with descent prime $\ell = 11$. For 864a1, 864b1 and 864c1 the disc test and Lemma 5.9(i) suffice (Section 9.3). For 27a1 and 288a1 the second descent of Section 3.7 replaces Lemma 5.9(i) (Sections 9.4, 9.5, 9.6 and 9.7).

9.1. **The position of j_0 at ℓ.** For $p \in \{23, 29\}$ the trace of Frobenius of E at ℓ determines the residues of j_0 modulo ℓ that the disc test needs, here and in Section 10.

For an elliptic curve E with good reduction at ℓ let $a_\ell(E)$ be its trace of Frobenius, and let

$$\mathcal{J}(E) := \{\bar{\jmath} \in \mathbb{F}_\ell : \text{ some elliptic curve over } \mathbb{F}_\ell \text{ with } j\text{-invariant } \bar{\jmath} \text{ has trace } a_\ell(E)\}.$$

Lemma 9.1. *Let $p \in \{23, 29\}$, with $\ell = 11$, respectively $\ell = 7$, and let (a, b, c), E and $E' = E^{(d)}_{a,b,c}$ be as in Theorem 2.1, so that $E'[p] \simeq E[p]$.*

(i) *$\ell \nmid c$, E' has good reduction at ℓ, and $a_\ell(E') = a_\ell(E)$.*

(ii) *j_0 is ℓ-integral and $j_0 \bmod \ell \in \mathcal{J}(E)$, with $a_\ell(E)$ and $\mathcal{J}(E)$ as in Table 10.*

(iii) *$v_\ell(j_0) = 3v_\ell(b)$ and $v_\ell(1728 - j_0) = 2v_\ell(a)$. So $j_0 \equiv 0 \pmod{\ell}$ if and only if $\ell \mid b$, and $j_0 \equiv 1728 \pmod{\ell}$ if and only if $\ell \mid a$.*

	$p = 23$, $\ell = 11$					$p = 29$, $\ell = 7$					
E	864a1	864b1	864c1	27a1	288a1	864a1	864b1	864c1	54a1	96a1	27a1
$a_\ell(E)$	3	-6	-2	0	0	-3	-3	1	-1	-4	-1
$\mathcal{J}(E)$	$\{4, 10\}$	$\{3\}$	$\{7, 9\}$	$\{0, 1\}$	$\{0, 1\}$	$\{1\}$	$\{1\}$	$\{0, 3\}$	$\{0, 3\}$	$\{0, 2\}$	$\{0, 3\}$

Table 10. Traces at ℓ and the allowed residues of j_0 modulo ℓ. Modulo 11, $1728 \equiv 1$, and modulo 7, $1728 \equiv 6$.

Proof. (i) The curves E have good reduction at ℓ, since their conductors divide 864. If $\ell \mid c$, then $\ell \nmid ab$, and E', a twist by $d \mid 6$, has multiplicative reduction at ℓ: $c_4 = -144bd^2$ is a unit and $v_\ell(\Delta) = p\, v_\ell(c)$. So, as in the proof of Lemma 6.1(i), $a_\ell(E) \equiv \pm(\ell + 1) \pmod{p}$. But $|a_\ell(E)| \leq 2\sqrt{\ell}$, and no integer in $[-6, 6]$ is congruent to ± 12 modulo 23, nor one in $[-5, 5]$ to ± 8 modulo 29. So $\ell \nmid c$. The model $Y^2 = X^3 + 3bd^2X - 2ad^3$ of E' has

discriminant $-1728d^6c^p$, a unit at ℓ. Finally $a_\ell(E') \equiv a_\ell(E) \pmod p$, as $E'[p] \simeq E[p]$, and $|a_\ell(E') - a_\ell(E)| \leq 4\sqrt{\ell} < p$.

(ii) The residue $j_0 \bmod \ell$ is the j-invariant of the reduction of E', whose trace is $a_\ell(E)$ by (i). The traces of all elliptic curves over $\mathbb{F}_\ell$, grouped by j-invariant, give $\mathcal{J}(E)$ (Appendix B).

(iii) We have $j_0 = 1728b^3/c^p$ and $1728 - j_0 = 1728(c^p - b^3)/c^p = 1728a^2/c^p$, and $\ell \nmid 1728c$. □

9.2. **The fields and their Selmer groups.** From now on $p = 23$ and $\ell = 11$. For $E \in \{864\text{a}1, 864\text{b}1, 864\text{c}1\}$ we assume that $11 \nmid h_{K_E}$, the hypothesis of Theorem B(a). For 27a1 and 288a1 it holds by Proposition A.12. So Proposition 3.14 applies to all five fields $K = K_E$, with S the set of places above 23. For each field, a computation in [32] gives the $12 + \#S$ elements u_i of Remark 3.15, with linearly independent images in $\bigoplus_{v|11} k_v \simeq \mathbb{F}_{11}^{24}$. So the localization $K(S, 11) \to \mathbb{F}_{11}^{24}$ is injective, as Section 5.5 assumes, with image Σ of dimension $12 + \#S$ (Proposition 9.2(a), Section 9.4). The disc test *allows* a configuration if its class tuple lies in Σ, and the element of $K(S, 11)$ with this localization is its *Selmer class*.

9.3. **The curves without complex multiplication.** For $E \in \{864\text{a}1, 864\text{b}1, 864\text{c}1\}$ let $P_E \in X_0(23)(K_E)$ be the point over $j(E)$ given by the identity embedding (Lemma 2.14). It is the only K_E-point over $j(E)$, as $\mathrm{Aut}(K_E) = 1$. A configuration has the *residue points* of a point $P \in X_0(p)(K)$ if at every place $v \mid \ell$ its point lies in the residue disc of P_v.

Proposition 9.2. *Let $E = 864a1$, $864b1$, $864c1$, and assume that $11 \nmid h_{K_E}$.*

(a) $\dim K(S, 11) = 15, 14, 15$, *the localization is injective, and Σ has codimension $9, 10, 9$ in $\mathbb{F}_{11}^{24}$. The class of $\delta(T) = 23^6$ is nonzero at every place above 11,* $\dim \Theta_T = 1, 3, 3$, $\Sigma \cap \Theta_T = \mathbb{F}_{11} \cdot \delta(T)|_{11}$, *and $\delta(P_E)|_{11} \in \Sigma$.*

(b) *The residues allowed by Lemma 9.1 are $\mathcal{J}(E) = \{4, 10\}$, $\{3\}$, $\{7, 9\}$, and $G_{23}(x, j_1) \bmod 11$ is separable for these residues. Over the representatives $j_1 = r + 11t$ ($r \in \mathcal{J}(E)$, $0 \le t \le 10$) there are 24, 3072, 44 admissible configurations in each disc, in all 528, 33792, 968. Exactly one of them has its class tuple in Σ. It lies in the disc of $j(E)$, where $j(E) \equiv 26, 91, 84 \pmod{121}$, and it has the residue points of P_E at every place above 11.*

(c) *The tuple ϑ of Lemma 5.9 for $P_0 = P_E$, in case* (U), *is not in $\Sigma + \Theta_T$.*

Proof. These are finite computations with the basis of $K(S, 11)$ and the points over the representatives j_1, whose classes are computed as in Section 4.4 and Appendix B.1. The numbers of configurations in (b) follow from the degrees of the places above 11 (Table 7): 24, $3! \cdot 8^3 = 3072$ and $2! \cdot 22 = 44$ per disc. For (c), Q'_v is the point of the residue disc of $P_{E,v}$ over $j(E) + 11$, a valid choice by the remark after Lemma 5.9.

For $E = 864a1$, Table S11 prints the disc test of (b) in a form checkable by hand. In a normal basis of k_v, the 528 class tuples are the cyclic shifts of the 22 printed classes, and each of them except $\delta_v(P_E)$ is nonzero under one of the vectors Υ_1, Υ_2, Υ_3 of the basis of the annihilator of Σ printed there. □

Theorem 9.3. *Assume that $11 \nmid h_{K_E}$ for $E \in \{864a1, 864b1, 864c1\}$. Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{23}$ with $abc \neq 0$ such that $E'[23] \simeq E[23]$ for a quadratic twist E' of its Frey curve by some $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ and one of these three curves E. Then $E = 864b1$ and $(a, b, c) = (\pm 3, -2, 1)$.*

Proof. Let $P \in X_0(23)(K_E)$ be the point of Proposition 2.12. By Lemma 9.1, $j_0 \bmod 11 \in \mathcal{J}(E)$. By Proposition 4.9, applied to the disc $j_1 + 121\mathbb{Z}_{11}$ that contains j_0, the class tuple of $(P_v)_{v|11}$ lies in Σ and is that of an admissible configuration over j_1 with the residue points of $(P_v)_v$. By Proposition 9.2(b) this configuration is the one of P_E, so $j_0 \equiv j(E) \pmod{121}$ and P_v lies in the residue disc of $P_{E,v}$ for every $v \mid 11$. By Lemma 5.9, case (U), with the hypotheses (i) given by Proposition 9.2(a),(c), $P = P_E$ and $j_0 = j(E) \in \{-216, -13824, 1536\}$. By Lemma 2.15, $j_0 = -13824$, $E = 864b1$ and $(a, b, c) = (\pm 3, -2, 1)$. □

9.4. **Tools for the curves with complex multiplication.** For the curves 27a1 and 288a1 with complex multiplication, $\Sigma \cap \Theta_T$ is too large for Lemma 5.9(i) (see below), and some of the known points lie at ramification points of j, over 0 and 1728. In this subsection we check the hypotheses of the second descent for K_{27a1} and K_{288a1} and set up a logarithm measuring division by λ modulo T. Section 9.5 turns them into a criterion (Lemma 9.5) for dividing $[P - \beta]$ by λ near a known point β. For each curve, the disc test in the ramified regions and a sieve at one good prime, 89 for 27a1 and 43 for 288a1, leave only configurations that carry the Selmer class of a known point (Propositions 9.6 and 9.10). These are excluded with Lemma 9.5 in Lemmas 9.7, 9.8 and 9.12, and Propositions 9.9 and 9.13 assemble the cases.

Let K be K_{27a1} or K_{288a1}. Above 11 there are two places of degree one and eleven of degree two, and 23 is totally ramified with residue degree one (Table 7). For a solution attached to 27a1 or 288a1, Lemma 9.1 and Table 10 give $j_0 \equiv 0$ or $1728 \pmod{11}$, so j_0 lies in region A or B of (4.2), at depth $v_{11}(b)$ or $v_{11}(a)$ (Section 4.2). In both fields $\dim K(S, 11) = 13$, Σ has codimension 11 in $\mathbb{F}_{11}^{24}$ and $\dim \Theta_T = 13$, while $\dim(\Sigma \cap \Theta_T)$

is 4 for K_{27a1} and 2 for K_{288a1}, so hypothesis (i) of Lemma 5.9 fails. The hypotheses of Proposition 3.18 hold: $11 \nmid h_K$ by Proposition A.12, (H_v) holds at the places above 11 since they have degree one or two (Section 3.6), and the ray class group modulo the place above 23 has 11-rank at most one by Remark 3.19.

The logarithm. For $R \in J(K_v)$ with $\pi_v(R) = 0$ put $\mathrm{Log}_v(R) \coloneqq \log_\lambda(m'R)/m'$ with $m' = \#\widetilde{J}(k_v)/11$, that is, $m' = 20$ at the places of degree one and $m' = 1520$ at those of degree two. By Lemma 3.17, $m'R$ is formal, and Log_v is additive, vanishes on torsion and agrees with $\log_\lambda$ on $\widehat{J}(11\mathcal{O}_v)$. Hence, for such R, $R \in \lambda^d J(K_v)$ if and only if $v_{11}(\mathrm{Log}_v R) \geq d+1$. In that case every R' with $\lambda^d R' = R$ has

$$\delta_v^0(R') = \varepsilon^d \, N_v\big(\mathrm{Log}_v(R)/11^{d+1} \bmod 11\big),$$

by Lemma 3.16(F3) and Lemma 3.17, since two such points R' differ by an element of $\langle T \rangle + J(K_v)'$, on which δ_v^0 vanishes. Here $\varepsilon = 4$ by (3.2).

For a set S' of places above 11 let $k_{S'} \coloneqq \bigoplus_{v \in S'} k_v \subseteq \mathbb{F}_{11}^{24}$.

In the following lemma, π_v is the map of Lemma 3.17.

Lemma 9.4. *Let $p = 23$ and $\ell = 11$, and let Q be a point of $X_0(23)_{\bar{\mathbb{F}}_{11}}$ with $\tilde{\jmath}(Q) \in \{0, 1728\}$. Then $Q \in X_0(23)_{\mathbb{F}_{11}}(\mathbb{F}_{121})$, and the image of $[Q - \tilde{\infty}]$ in $\widetilde{J}(\mathbb{F}_{121})/\lambda\widetilde{J}(\mathbb{F}_{121}) \simeq \mathbb{Z}/11$ is $6\tilde{T}$. In particular $\pi_v([Q_1 - Q_2]) = 0$ for any two K_v-points Q_1, Q_2 whose reductions lie over 0 or 1728.*

Proof. There are 8 points over 0 and 12 over 1728, all in $X_0(23)_{\mathbb{F}_{11}}(\mathbb{F}_{121})$, and six of them are Weierstrass points. The hyperelliptic involution is w_{23} (Section 2.3), and $Q + w_{23}(Q) \sim (\tilde{\infty}) + (\tilde{0})$ for every point Q, so $[Q - \tilde{\infty}] + [w_{23}(Q) - \tilde{\infty}] = \tilde{T}$. At a Weierstrass point W this gives $2[W - \tilde{\infty}] = \tilde{T}$, hence the claim for W. For the other fourteen points the claim is a computation in $\widetilde{J}(\mathbb{F}_{121})$, of order $16720 = 11 \cdot 1520$ (Section 3.6). It suffices to show that $1520([Q - \tilde{\infty}] - 6\tilde{T}) = 0$, since an element of order prime to 11 lies in $\lambda\widetilde{J}(\mathbb{F}_{121})$. Put $D_\infty = (\tilde{\infty}) + (\tilde{0})$. Since $1520 \cdot 6 \equiv 1$ and $760 \equiv 1 \pmod{11}$, and $11(\tilde{0}) - 11(\tilde{\infty})$ is the divisor of f, the class $1520([Q - \tilde{\infty}] - 6\tilde{T})$ is that of $1520(Q) - 760D_\infty$.

Write $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$. The fourteen points are $(x, \pm y)$ with (x, y) one of

$$(8,4),\ (10\alpha, 4\alpha),\ (\alpha+1, 4\alpha+4),\ (4\alpha+2, 4),\ (7\alpha+9, 4),\ (10\alpha+9, 6\alpha+5),\ (\alpha+10, 5\alpha+10).$$

Of these, $(8,7)$, $(10\alpha, 7\alpha)$, $(\alpha+1, 4\alpha+4)$, $(4\alpha+2, 4)$ and $(7\alpha+9, 4)$ lie over 0, and the other nine over 1728. The Riemann–Roch space of $760D_\infty$ consists of the functions $g_1(x) + g_2(x)y$ with $\deg g_1 \leq 760$ and $\deg g_2 \leq 757$. For each of the fourteen points $Q = (x_0, y_0)$ we computed over $\mathbb{F}_{121}$ such a function, with $\deg g_1 = 760$ and $\deg g_2 = 756$, for which $g_1(x_0 + t) + g_2(x_0 + t)Y(t)$ vanishes to order 1520 in t, where $Y(t)$ is the power series with $Y(0) = y_0$ and $Y^2 = F(x_0 + t)$. The function then has a zero of order at least 1520 at Q and poles bounded by $760D_\infty$, and both divisors have degree 1520, so its divisor is $1520(Q) - 760D_\infty$. □

9.5. **Dividing by $\boldsymbol{\lambda}$ near a known point.** Lemma 3.20 is used in Sections 9.6 and 9.7 in the following form. There, $K = K_E$ with $E = 27a1$ or $288a1$, and $P \in X_0(23)(K)$ is the point (Proposition 2.12) of a primitive solution with $abc \neq 0$ such that some twist E' of its Frey curve has $E'[23] \simeq E[23]$. So $j(P)$ lies in region A or B (Section 9.4), and $(P_v)_{v|11}$ has the labels and the class tuple of an allowed configuration (Proposition 4.9).

Suppose that this configuration carries the Selmer class of a known point $\beta \in X_0(23)(K)$, that is, its class tuple is $\delta(\beta)|_{11}$. By the injectivity of the localization, $\delta([P - \infty]) = \delta([\beta - \infty])$,

so $D \coloneqq [P-\beta]$ lies in $\lambda J(K)$ (Proposition 3.14(b)). At each place $v \mid 11$ we choose a point $Y_v \in X_0(23)(K_v)$ in the residue disc of P_v and write

$$D_v = D_v^{\mathrm{b}} + D_v^{\mathrm{f}}, \qquad D_v^{\mathrm{b}} \coloneqq [P_v - Y_v] \in \widehat{J}(11\mathcal{O}_v), \qquad D_v^{\mathrm{f}} \coloneqq [Y_v - \beta_v]. \tag{9.1}$$

We call D_v^{f} the *fixed term* at v and D_v^{b} the *branch term*, as in Section 5.4. Put $S' \coloneqq \{v \mid 11 : Y_v \neq \beta_v\}$, so that $D_v^{\mathrm{f}} = 0$ for $v \notin S'$.

Lemma 9.5. *Let K be $K_{27\mathrm{a}1}$ or $K_{288\mathrm{a}1}$. Let $D \in J(K)$, let $n \geq 1$ be an integer and S' a set of places above 11, and suppose that for every $v \mid 11$*

$$D_v = D_v^{\mathrm{b}} + D_v^{\mathrm{f}} \qquad \text{with} \qquad D_v^{\mathrm{b}} \in \lambda^n \widehat{J}(11\mathcal{O}_v), \quad D_v^{\mathrm{f}} \in J(K_v),$$

where $D_v^{\mathrm{f}} = 0$ if $v \notin S'$, and $\pi_v(D_v^{\mathrm{f}}) = 0$ and $\delta_v(D_v^{\mathrm{f}}) = 0$ if $v \in S'$. Let $\lambda^{-n} D_v^{\mathrm{b}} \in \widehat{J}(11\mathcal{O}_v)$ be the unique formal point whose image under λ^n is D_v^{b} (Lemma 3.16(F1),(F3)), and put $\vartheta_v^{\mathrm{b}} \coloneqq \delta_v(\lambda^{-n} D_v^{\mathrm{b}}) \in k_v$ and $\vartheta^{\mathrm{b}} \coloneqq (\vartheta_v^{\mathrm{b}})_{v \mid 11}$.

(a) *For $v \in S'$, $D_v^{\mathrm{f}} \in \lambda J(K_v)$. Let $d_v \in \{1, 2, \ldots, \infty\}$ be the level of D_v^{f} modulo $\langle T \rangle$ for the endomorphism λ (Section 5.1), that is, the largest d with $D_v^{\mathrm{f}} \in \lambda^d J(K_v) + \langle T \rangle$.*

(b) *Let m be an integer with $1 \leq m \leq n$ and $m \leq d_v$ for every $v \in S'$. For $v \in S'$ let $R_v \in J(K_v)$ be a point with $\lambda^m R_v \in D_v^{\mathrm{f}} + \langle T \rangle$, and for $v \notin S'$ put $R_v = 0$. Then, for $v \in S'$, $\delta_v^0(R_v) = 0$ if $d_v > m$, $\delta_v^0(R_v) \neq 0$ if $d_v = m$, and $\delta_v^0(R_v) = \varepsilon^m N_v\big(\operatorname{Log}_v(D_v^{\mathrm{f}})/11^{m+1} \bmod 11\big)$.*

(c) *With m and R_v as in (b), put $W_v \coloneqq \lambda^{-m} D_v^{\mathrm{b}} + R_v$, where $\lambda^{-m} D_v^{\mathrm{b}} \coloneqq \lambda^{n-m}(\lambda^{-n} D_v^{\mathrm{b}})$. Then Lemma 3.20 applies to D, m and the points W_v, and gives $(\delta_v^0(W_v))_{v \mid 11} \in \Sigma$, where*

$$(\delta_v^0(W_v))_{v \mid 11} = \begin{cases} (\delta_v^0(R_v))_{v \mid 11} & \text{if } m < n, \\ \vartheta^{\mathrm{b}} + (\delta_v^0(R_v))_{v \mid 11} & \text{if } m = n, \end{cases} \qquad \text{and} \qquad (\delta_v^0(R_v))_{v \mid 11} \in k_{S'}.$$

Proof. By Section 9.4, K satisfies the hypotheses of Proposition 3.18 and of Lemma 3.20.

(a) Both δ_v and π_v vanish on D_v^{f}, and (δ_v, π_v) is injective on $J(K_v)/\lambda J(K_v)$ (Lemma 3.17).

(b) A point R_v exists because $m \leq d_v$. If $d_v > m$, then $D_v^{\mathrm{f}} \in \lambda^{m+1} R' + \langle T \rangle$ for some $R' \in J(K_v)$, so $\lambda^m(R_v - \lambda R') \in \langle T \rangle$ and $R_v - \lambda R' \in J(K_v)[\lambda^\infty] = \langle T \rangle$. As δ_v^0 vanishes on $\lambda J(K_v)$ and on T (Lemma 3.17), $\delta_v^0(R_v) = 0$. Suppose that $d_v = m$ and $\delta_v^0(R_v) = 0$, and put $a = \pi_v(R_v)$. Then $\delta_v(R_v - aT) = \delta_v^0(R_v) = 0$ and $\pi_v(R_v - aT) = 0$, so $R_v - aT \in \lambda J(K_v)$ by Lemma 3.17, and $D_v^{\mathrm{f}} \in \lambda^m R_v + \langle T \rangle \subseteq \lambda^{m+1} J(K_v) + \langle T \rangle$, contradicting $d_v = m$. For the formula, π_v is the coordinate along $\langle T \rangle$ in the decomposition $J(K_v) = J(K_v)' \oplus \langle T \rangle \oplus \widehat{J}(11\mathcal{O}_v)$ of Lemma 3.17, whose summands are $\mathcal{O}$-stable. So neither D_v^{f} (as $\pi_v(D_v^{\mathrm{f}}) = 0$) nor $\lambda^m R_v$ (as $\lambda T = 0$) has a component along $\langle T \rangle$, and $\lambda^m R_v \in D_v^{\mathrm{f}} + \langle T \rangle$ gives $\lambda^m R_v = D_v^{\mathrm{f}}$. The formula is then the one of Section 9.4 for Log_v, with $R = D_v^{\mathrm{f}}$, $R' = R_v$ and $d = m$.

(c) For every $v \mid 11$, $D_v^{\mathrm{b}} \in \lambda^m J(K_v)$, and $D_v^{\mathrm{f}} \in \lambda^m J(K_v) + \langle T \rangle$ as $m \leq d_v$ for $v \in S'$. So $D_v \in \lambda^m J(K_v) + \langle T \rangle$, and $\lambda^m W_v = D_v^{\mathrm{b}} + \lambda^m R_v \in D_v + \langle T \rangle$. Hence Lemma 3.20 gives $(\delta_v^0(W_v))_v \in \Sigma$. If $m < n$, then $\lambda^{-m} D_v^{\mathrm{b}} \in \lambda J(K_v)$, so $\delta_v^0(\lambda^{-m} D_v^{\mathrm{b}}) = 0$. If $m = n$, then $\delta_v^0(\lambda^{-n} D_v^{\mathrm{b}}) = \delta_v(\lambda^{-n} D_v^{\mathrm{b}}) = \vartheta_v^{\mathrm{b}}$, as π_v vanishes on formal points. □

9.6. **The curve 27a1.** Let $K = K_{27\mathrm{a}1}$ and ι_K its nontrivial automorphism. The known points are ξ and $\iota_K \xi$, the two K-points over $j = 0$, which come from the trivial solutions $(\pm 1, 0, 1)$, and P_0 and $\iota_K P_0$, the two K-points over $j(27\mathrm{a}2) = -12288000 = 1728 - 11^2 \cdot 101568$, where $101568 \equiv 5 \pmod{11}$. Here, and for 27a1 in Section 10, ξ denotes a point, not a root of a fibre polynomial as in Section 4; the x-coordinates of ξ and $\iota_K \xi$ are the roots in K of the

polynomial h of degree 8 with $G_{23}(x,0) = h^3$. There are no K-points over 1728. The class tuples of the known points lie in Σ. Let S_0 be the set of places $v \mid 11$ with $\delta_v(\xi) = \delta_v(\iota_K\xi)$.

For a configuration $(R_v)_{v|11}$ in a ramified region, let $\rho(R_v)$ be the point over j_c in the residue disc of R_v (one of the ρ_i of Lemma 4.5), and call $(\rho(R_v))_v$ its *ramification points*.

Proposition 9.6. (a) *S_0 consists of three places of degree two, and at each $v \in S_0$ the points ξ_v and $\iota_K\xi_v$ lie in different residue discs.*

(b) *The disc test in the ramified regions (Proposition 4.9, with $2 \cdot 11! \cdot 2^{11}$ admissible configurations for each $\bar{w}$ and each of the two depth cases, Section 4.4) allows the following configurations:*

- *region A, depth 1: four, all with $\bar{w} = 6$, carrying two Selmer classes;*
- *region A, depth ≥ 2: for every $\bar{w}$, 13824 configurations, whose ramification points form one of 16 patterns: for $\beta \in \{\xi, \iota_K\xi\}$ with β' the other one and $S' \subseteq S_0$, $\rho(R_v) = \beta'_v$ for $v \in S'$ and $\rho(R_v) = \beta_v$ otherwise, and the Selmer class is $\delta(\beta)$;*
- *region B, depth 1: 64 with $\bar{w} = 5$, carrying the Selmer classes $\delta(P_0)$ and $\delta(\iota_K P_0)$ (32 each), and 8 with $\bar{w} = 6$, carrying two Selmer classes;*
- *region B, depth ≥ 2: none.*

(c) *None of the four Selmer classes of the allowed configurations of region A at depth 1 and of region B at depth 1 with $\bar{w} = 6$ passes at $q = 89$ (Section 5.6), whatever the value of j_0 mod 89.*

(d) *$\Sigma \cap k_{S'} = 0$ for every nonempty $S' \subseteq S_0$.*

(e) *No admissible configuration at depth 1 of region A (any $\bar{w}$) whose ramification points form one of the 16 patterns of* (b)*, with its set S', has its class tuple in $\Sigma + k_{S'}$. There are 8640 such configurations for each pattern, over all ten values of $\bar{w}$.*

(f) *For each of the 64 allowed configurations of region B at depth 1 with $\bar{w} = 5$, let $\beta \in \{P_0, \iota_K P_0\}$ be the known point whose Selmer class it carries. For $v \mid 11$ let Y_v be the K_v-point over $j(\beta)$ with the label of the configuration at v, and let $S' = \{v : Y_v \neq \beta_v\}$ and $D_v^{\mathrm{f}} = [Y_v - \beta_v]$ for $v \in S'$. Then $\pi_v(D_v^{\mathrm{f}}) = 0$, $\delta_v(D_v^{\mathrm{f}}) = 0$ and $v_{11}(\mathrm{Log}_v D_v^{\mathrm{f}}) = 2$ for every $v \in S'$. Put $\vartheta^{\mathrm{f}} = \big(N_v(\mathrm{Log}_v(D_v^{\mathrm{f}})/121 \bmod 11)\big)_{v \in S'}$, extended by 0, and $\vartheta' = (\delta_v(\beta) - \delta_v(\rho(Y_v)))_{v|11}$. If $S' = \emptyset$, which happens for two configurations (those of P_0 and $\iota_K P_0$), then $\vartheta' \notin \Sigma$. For each of the other 62, $\vartheta^{\mathrm{f}} \notin \Sigma$ and $u\vartheta' + \vartheta^{\mathrm{f}} \notin \Sigma$ for every $u \in \mathbb{F}_{11}^\times$.*

Proof. These are computations. Items (a), (d) and (e) are linear algebra over $\mathbb{F}_{11}$ with the class tuples of the points over $j = 0$ and of the admissible configurations at depth 1. Item (b) is the disc test in the ramified regions, by the meet-in-the-middle search of Section 4.4. Item (c) is the test of Section 5.6 in the residue fields of the places above 89, the smallest prime that works (Remark 9.14). Item (f) uses the 11-adic logarithms of Appendix B.1, which have a proven error bound. Tables S12 and S14 and their continuations give the data from which (a), (b) for region A at depth ≥ 2, (d), (e) and (f) can be checked. □

In (b) and (e), each of the $16 = 2 \cdot 2^3$ patterns (choices of β and S') is that of $2^2 \cdot (3!)^3 = 864$ admissible configurations for each $\bar{w}$, since two of the eight points over 0 are defined over $\mathbb{Q}_{11}$ and the other six form three conjugate pairs (Lemma 4.5(b),(c)). Near each of the two, the fibre has one $\mathbb{Q}_{11}$-point and one conjugate pair, and near each pair it has three orbits of size 2, so the 13 orbits go one to each place. Given the pattern, what remains is the point of the conjugate pair at each of two places of degree two (2^2), and, for each of the three pairs,

which of its three orbits goes to which of the three places where the pattern uses that pair $((3!)^3)$. This gives $16 \cdot 864 = 13824$ and $10 \cdot 864 = 8640$.

Lemma 9.7 (27a1, region A, depth ≥ 2)**.** *Let P be as in Section 9.5, with $E = 27a1$. Then $j(P)$ is not in region A at a depth $k \geq 2$.*

Proof. Suppose that $j(P)$ is in region A at depth $k \geq 2$. By Proposition 4.9 and Proposition 9.6(b), the ramification points $\rho(P_v)$ form one of the 16 patterns, given by $\beta \in \{\xi, \iota_K\xi\}$ and a set $S' \subseteq S_0$, and $\delta([P-\infty]) = \delta([\beta-\infty])$. We apply Lemma 9.5 to $D = [P-\beta]$, with $Y_v = \rho(P_v)$ in (9.1). Then $D_v^{\mathrm{f}} = 0$ for $v \notin S'$ and $D_v^{\mathrm{f}} = [\beta_v' - \beta_v]$ for $v \in S'$, where β' is the other known point over 0. By Proposition 9.6(a), S' is the set $\{v : Y_v \neq \beta_v\}$ of (9.1). The hypotheses of Lemma 9.5 hold with $n = k-1$. By Lemma 4.5(e) and Lemma 3.16(F1),(F3), $D_v^{\mathrm{b}} = [P_v - \rho(P_v)] \in \lambda^{k-1}\widehat{J}(11\mathcal{O}_v)$ and $\vartheta_v^{\mathrm{b}} = \varepsilon^{k-1}(\delta_v(P_v^{(1)}) - \delta_v(\rho(P_v)))$, where $P_v^{(1)}$ is the point of Lemma 4.5(e) for $Q = P_v$. For $v \in S'$, $\delta_v(D_v^{\mathrm{f}}) = \delta_v(\beta') - \delta_v(\beta) = 0$ as $S' \subseteq S_0$, and $\pi_v(D_v^{\mathrm{f}}) = 0$ because β_v' and β_v are K_v-points over 0 (Lemma 9.4). Moreover $\delta_v(\rho(P_v)) = \delta_v(\beta)$ for every v, as $\rho(P_v) = \beta_v$ for $v \notin S'$ and $S' \subseteq S_0$. So $\vartheta^{\mathrm{b}} = \varepsilon^{k-1}((\delta_v(P_v^{(1)}))_v - \delta(\beta)|_{11})$. Let d_v ($v \in S'$) be as in Lemma 9.5(a).

If $m := \min_{v\in S'} d_v < k-1$ (so $S' \neq \emptyset$), then by Lemma 9.5(b),(c) with this $m < n$, the tuple $(\delta_v^0(R_v))_v$ lies in $\Sigma \cap k_{S'}$, and it is nonzero, since $\delta_v^0(R_v) \neq 0$ at a place v with $d_v = m$. This contradicts Proposition 9.6(d).

Otherwise $d_v \geq k-1$ for all $v \in S'$, and Lemma 9.5(c) with $m = n = k-1$ gives $\vartheta^{\mathrm{b}} + (\delta_v^0(R_v))_v \in \Sigma$, so $\vartheta^{\mathrm{b}} \in \Sigma + k_{S'}$. As $\delta(\beta)|_{11} \in \Sigma$ and $\varepsilon \neq 0$, the class tuple of $(P_v^{(1)})_v$ lies in $\Sigma + k_{S'}$. The points $P_v^{(1)}$ have the labels of the P_v, so by Lemma 4.5(c),(d) this is the class tuple of an admissible configuration at depth 1 of region A whose ramification points form the pattern of β and S'. This contradicts Proposition 9.6(e). □

Lemma 9.8 (27a1, region B, depth 1, $\bar{w} = 5$)**.** *Let P be as in Section 9.5, with $E = 27a1$. Then $j(P)$ is not in region B at depth 1 with $\bar{w} = 5$.*

Proof. Suppose that it is. By Proposition 4.9 and Proposition 9.6(b), $(P_v)_v$ has the labels and the class tuple of one of the 64 allowed configurations of region B at depth 1 with $\bar{w} = 5$, and $\delta([P-\infty]) = \delta([\beta-\infty])$ for the point $\beta \in \{P_0, \iota_K P_0\}$ whose Selmer class that configuration carries. Let Y_v, S', D_v^{f}, ϑ^{f} and ϑ' be as in Proposition 9.6(f) for this configuration. Then Y_v lies in the residue disc of P_v, and we apply Lemma 9.5 to $D = [P-\beta]$ with these Y_v in (9.1). Its hypotheses on the D_v^{f} hold by Proposition 9.6(f).

The branch terms $D_v^{\mathrm{b}} = [P_v - Y_v]$. Let $n_\beta = v_{11}(j(P) - j(\beta))$. As $j(P)$ and $j(\beta)$ are both of the form $1728 - 121w$ with $w \equiv 5 \pmod{11}$, $n_\beta \geq 3$. And $n_\beta < \infty$, since $j(\beta)$ is not the j-invariant of a Frey curve (Lemma 2.15). Put $u_1 := (j(P) - j(\beta))/11^{n_\beta} \in \mathbb{Z}_{11}^\times$ and $w_0 := (j(\beta) - 1728)/121$. Let $\rho(Y_v) = \rho_i$, and let z_i and u_i be as in Lemma 4.5(a) on its residue disc. Write $z_i = 11s$ and $j - 1728 = 121\,\Omega(s)$ with $\Omega(s) = s^2 u_i(11s)$. Then $\Omega(s(Y_v)) = w_0$, so $w_0 \equiv s(Y_v)^2 u_i(0) \pmod{11}$, and $\Omega'(s) \equiv 2su_i(0) \pmod{11}$ is a unit at $s(Y_v)$. Since P_v and Y_v have the same label, $s(P_v) \equiv s(Y_v) \pmod{11}$, and $\Omega(s(P_v)) - \Omega(s(Y_v)) = 11^{n_\beta - 2}u_1$ gives

$$s(P_v) - s(Y_v) \equiv 11^{n_\beta-2}\, u_1/\Omega'(s(Y_v)) \pmod{11^{n_\beta-1}}.$$

Write $\omega_\lambda = (b_0 + b_1 z_i + \cdots)\, dz_i$ on the disc. Integrating ω_λ from Y_v to P_v, as in the proof of Lemma 5.9, gives

$$\log_\lambda D_v^{\mathrm{b}} \equiv 11^{n_\beta - 1}\, \frac{u_1}{2w_0}\, s(Y_v)\, b_0 \pmod{11^{n_\beta}},$$

while $\log_\lambda[Y_v - \rho(Y_v)] \equiv 11\, s(Y_v)\, b_0 \pmod{121}$. So $\log_\lambda D_v^{\mathrm{b}} \equiv 11^{n_\beta-2}\,(u_1/2w_0)\log_\lambda[Y_v - \rho(Y_v)] \pmod{11^{n_\beta}}$. Hence $D_v^{\mathrm{b}} \in \lambda^{n_\beta-2}\widehat{J}(11\mathcal{O}_v)$, and by Lemma 3.16(F1),(F3) the formal point $\lambda^{-(n_\beta-2)}D_v^{\mathrm{b}}$ has class $\varepsilon^{n_\beta-2}u(\delta_v(Y_v) - \delta_v(\rho(Y_v)))$, where $u \coloneqq u_1/(2w_0) \bmod 11 \in \mathbb{F}_{11}^\times$ is the same at every place. As $\delta_v(Y_v) = \delta_v(P_v) = \delta_v(\beta)$ (Lemma 4.5(d)), the hypothesis on D_v^{b} in Lemma 9.5 holds with $n = n_\beta - 2$ and $\vartheta^{\mathrm{b}} = \varepsilon^{n_\beta-2}u\,\vartheta'$.

Conclusion. By Proposition 9.6(f) ($\pi_v(D_v^{\mathrm{f}}) = 0$ and $v_{11}(\mathrm{Log}_v D_v^{\mathrm{f}}) = 2$) and Section 9.4, $d_v = 1$ for $v \in S'$, and for $m = 1$ Lemma 9.5(b) gives $\delta_v^0(R_v) = \varepsilon\vartheta_v^{\mathrm{f}}$ for $v \in S'$. If $S' = \emptyset$, Lemma 9.5(c) with $m = n = n_\beta - 2$ gives $\varepsilon^{n_\beta-2}u\,\vartheta' \in \Sigma$, so $\vartheta' \in \Sigma$. If $S' \neq \emptyset$, Lemma 9.5(c) with $m = 1$ gives $\varepsilon\vartheta^{\mathrm{f}} \in \Sigma$ if $n_\beta \geq 4$ (then $m < n$), and $\varepsilon(u\vartheta' + \vartheta^{\mathrm{f}}) \in \Sigma$ if $n_\beta = 3$ (then $m = n$). Each contradicts Proposition 9.6(f). □

Proposition 9.9. *No primitive solution of $x^2 + y^3 = z^{23}$ with $abc \neq 0$ has a twist E' of its Frey curve with $E'[23] \simeq 27\mathrm{a}1[23]$.*

Proof. Let $K = K_{27\mathrm{a}1}$, so that $11 \nmid h_K$ (Proposition A.12), and let $P \in X_0(23)(K)$ be the point of such a solution. By Lemma 9.1 and Table 10, $j(P) = j_0$ lies in region A or B. By Proposition 4.9, its configuration has the labels and the class tuple of a configuration allowed in Proposition 9.6(b), in the same region, at the same depth (1 or ≥ 2) and with the same $\bar{w}$. By the injectivity of the localization, $\delta([P - \infty])$ is the Selmer class of that configuration. By Proposition 9.6(c) and Lemma 5.11, P is not in region A at depth 1, nor in region B at depth 1 with $\bar{w} = 6$. Here $89 \nmid c$ by Lemma 5.11(d), since $a_{89}(27\mathrm{a}1) = 0 \not\equiv \pm 90 \pmod{23}$. By Lemmas 9.7 and 9.8, P is not in region A at a depth ≥ 2, nor in region B at depth 1 with $\bar{w} = 5$. The other combinations of region, depth and $\bar{w}$ allow no configuration, so P does not exist. □

9.7. **The curve 288a1.** Let $K = K_{288\mathrm{a}1}$ (Proposition 2.9(b)). The known points are η_1 and η_2, the two K-points over $j = 1728$, which come from the trivial solutions $(0, 1, 1)$ and $(0, -1, -1)$. Both are fixed by ι_K. There are no K-points over 0. The class tuples of η_1 and η_2 lie in Σ.

Proposition 9.10. (a) *The disc test in the ramified regions allows the following configurations. Region A, depth 1: 16, all with $\bar{w} = 8$, carrying two Selmer classes. Region A, depth ≥ 2: none. Region B, depth 1: 4 with $\bar{w} = 1$ and 16 with $\bar{w} = 7$, carrying two Selmer classes each. Region B, depth ≥ 2: 3072 for every $\bar{w}$, carrying the Selmer class $\delta(\eta_2)$ if $\bar{w}$ is a square modulo 11 and $\delta(\eta_1)$ otherwise.*

(b) *None of the six Selmer classes of the configurations allowed at depth 1 passes at $q = 43$ (Section 5.6), whatever the value of j_0 mod 43.*

(c) *For each of the 30720 configurations allowed in region B at depth ≥ 2 (3072 for each of the ten values of $\bar{w}$), let $\beta = \eta_g$ be the known point whose Selmer class it carries, $(\rho(R_v))_v$ its ramification points, $(R_v^{(1)})_v$ the admissible configuration at depth 1 with its labels, $S' = \{v : \rho(R_v) \neq \beta_v\}$, and $D_v^{\mathrm{f}} = [\rho(R_v) - \beta_v]$ for $v \in S'$. Then $\delta_v(D_v^{\mathrm{f}}) = 0$, $\pi_v(D_v^{\mathrm{f}}) = 0$ and $v_{11}(\mathrm{Log}_v D_v^{\mathrm{f}}) = 2$ for every $v \in S'$. Put $\vartheta^{\mathrm{f}} = \big(N_v(\mathrm{Log}_v(D_v^{\mathrm{f}})/121 \bmod 11)\big)_{v\in S'}$, extended by 0. If $S' = \emptyset$, the class tuple of $(R_v^{(1)})_v$ is not in Σ. If $S' \neq \emptyset$, then $\vartheta^{\mathrm{f}} \notin \Sigma$ and $\big(\delta_v(R_v^{(1)}) - \delta_v(\rho(R_v))\big)_v + \vartheta^{\mathrm{f}} \notin \Sigma$.*

Proof. As for Proposition 9.6: (a) is the disc test, (b) the test of Section 5.6 at the places above 43, the smallest prime that works (Remark 9.14), and (c) uses linear algebra over $\mathbb{F}_{11}$ and the 11-adic logarithms of Appendix B.1. Table S16 gives the data from which (a) for region B at depth ≥ 2 and (c) can be checked. □

In (a) and (c), each pattern of ramification points is that of $2 \cdot 2 \cdot (2!)^5 = 2^7$ admissible configurations, since two of the twelve points over 1728 are defined over $\mathbb{Q}_{11}$ and the other ten form five conjugate pairs. Given the pattern, one chooses which of the two $\mathbb{Q}_{11}$-points near one of them goes to which place of degree one (2), the point of the conjugate pair near the other (2), and, for each of the five pairs, which of its two orbits goes to which of its two places ($(2!)^5$). The $3072 = 24 \cdot 2^7$ configurations for each $\bar{w}$ form 24 patterns.

Remark 9.11. A fixed term $\pm[\eta_1 - \eta_2]$ in Proposition 9.10(c) can occur only at the two places, both of degree two, where $\delta_v(\eta_1) = \delta_v(\eta_2)$. At the other eleven, $v_{11}(\mathrm{Log}_v[\eta_1 - \eta_2]) = 1$ with leading digit $\delta_v(\eta_1) - \delta_v(\eta_2)$, as Lemma 3.16(F3) with N_v the identity (Appendix B.1) predicts.

Lemma 9.12 (288a1, region B, depth ≥ 2)**.** *Let P be as in Section 9.5, with $E = 288\mathrm{a}1$. Then $j(P)$ is not in region B at a depth $k \geq 2$.*

Proof. Suppose that $j(P)$ is in region B at depth $k \geq 2$. By Proposition 4.9 and Proposition 9.10(a), $(P_v)_v$ has the labels and the class tuple of a configuration allowed in region B at depth ≥ 2, and $\delta([P - \infty]) = \delta([\beta - \infty])$ for the known point $\beta = \eta_g$ whose Selmer class that configuration carries. Let S', D_v^{f} and ϑ^{f} be as in Proposition 9.10(c), and apply Lemma 9.5 to $D = [P - \beta]$, with $Y_v = \rho(P_v)$ in (9.1). As in the proof of Lemma 9.7, $D_v^{\mathrm{b}} = [P_v - \rho(P_v)] \in \lambda^{k-1}\widehat{J}(11\mathcal{O}_v)$ and $\vartheta_v^{\mathrm{b}} = \varepsilon^{k-1}(\delta_v(P_v^{(1)}) - \delta_v(\rho(P_v)))$, where $P_v^{(1)}$ is the point of Lemma 4.5(e) for $Q = P_v$. So the hypothesis on D_v^{b} holds with $n = k - 1$. By Proposition 9.10(c), the hypotheses on the D_v^{f} hold, and $d_v = 1$ for $v \in S'$ (Section 9.4), and for $m = 1$ Lemma 9.5(b) gives $\delta_v^0(R_v) = \varepsilon\vartheta_v^{\mathrm{f}}$ for $v \in S'$.

If $S' = \emptyset$, then $\rho(P_v) = \beta_v$ for all v, and Lemma 9.5(c) with $m = n = k - 1$ gives $\vartheta^{\mathrm{b}} = \varepsilon^{k-1}((\delta_v(P_v^{(1)}))_v - \delta(\beta)|_{11}) \in \Sigma$. As $\delta(\beta)|_{11} \in \Sigma$, the class tuple of $(P_v^{(1)})_v$ lies in Σ. If $S' \neq \emptyset$, Lemma 9.5(c) with $m = 1$ gives $\varepsilon\vartheta^{\mathrm{f}} \in \Sigma$ if $k \geq 3$ (then $m < n$), and $\varepsilon((\delta_v(P_v^{(1)}) - \delta_v(\rho(P_v)))_v + \vartheta^{\mathrm{f}}) \in \Sigma$ if $k = 2$ (then $m = n$). By Lemma 4.5(c),(d), the class tuple of $(P_v^{(1)})_v$ is that of the admissible configuration at depth 1 with the labels of $(P_v)_v$, so each case contradicts Proposition 9.10(c). □

Proposition 9.13. *No primitive solution of $x^2 + y^3 = z^{23}$ with $abc \neq 0$ has a twist E' of its Frey curve with $E'[23] \simeq 288\mathrm{a}1[23]$.*

Proof. Let $K = K_{288\mathrm{a}1}$, so that $11 \nmid h_K$ (Proposition A.12), and let $P \in X_0(23)(K)$ be the point of such a solution. As in the proof of Proposition 9.9, $j(P)$ lies in region A or B, and $\delta([P - \infty])$ is the Selmer class of a configuration allowed in Proposition 9.10(a) with the labels and the class tuple of $(P_v)_v$. By Proposition 9.10(b) and Lemma 5.11, P is not at depth 1. Here $43 \nmid c$ by Lemma 5.11(d), as $a_{43}(288\mathrm{a}1) = 0 \not\equiv \pm 44 \pmod{23}$. Region A at depth ≥ 2 allows no configuration, and region B at depth ≥ 2 is excluded by Lemma 9.12, so P does not exist. □

Remark 9.14. The primes 89 and 43 are the smallest that work, since the classes enter the test at q only through the places $w \mid q$ with $11 \mid \#k_w - 1$. Below 89, the only primes $q \nmid 2 \cdot 3 \cdot 11 \cdot 23$ at which $K_{27\mathrm{a}1}$ has such a place are 43 and 67, each with a single one, of degree 24, and there all four classes pass. For $K_{288\mathrm{a}1}$ no prime $q < 43$ has such a place.

9.8. **Proof of Theorem B(a).** Under the hypothesis of Theorem B(a), let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{23}$ with $abc \neq 0$. By Theorem 2.1 some twist E' of its Frey curve has $E'[23] \simeq E[23]$ with $E \in \{27\mathrm{a}1, 288\mathrm{a}1, 864\mathrm{a}1, 864\mathrm{b}1, 864\mathrm{c}1\}$. Propositions 9.9

and 9.13 exclude 27a1 and 288a1, and Theorem 9.3 gives $(a,b,c) = (\pm 3, -2, 1)$ for the other three. The primitive solutions with $abc = 0$ are the trivial ones listed in Theorem B(a) (Section 1.1), and $3^2 + (-2)^3 = 1^{23}$. This proves Theorem B(a). □

10. The exponent 29

For $p = 29$, Theorem B(b), the descent prime is $\ell = 7$ and the proof follows the argument of Section 9. Every configuration that the disc test allows has, at every place above 7, the residue points or labels of a known point (Table 11), so Lemma 5.9 finishes the argument without a sieve. For 27a1, Lemma 5.10(ii) replaces the division by λ of Section 9.5 (Proposition 10.2).

E	discs	configurations	allowed	the allowed configurations
864a1	$j \equiv 1 \pmod 7$: 7 discs	3150	1	residue points of P_{-216}
864b1	$j \equiv 1$: 7 discs	3150	1	residue points of P_{-13824}
864c1	$j \equiv 3$: 7 discs	78,750,000	1	residue points of P_{1536}
	region A, $\bar{w} = \pm 1$, depths $1, \geq 2$	45,000,000	0	
54a1	$j \equiv 3$: 7 discs	78,750,000	2	residue points of $P_{-1167051/512}$, $P_{-132651/2}$
	region A, $\bar{w} = \pm 1$, depths $1, \geq 2$	45,000,000	1	depth 1, $\bar{w} = 6$: labels of $P_{9261/8}$
96a1	$j \equiv 2$: 7 discs	3150	3	residue points of $P_{140608/3}$, $P_{97336/81}$, $P_{7301384/3}$
	region A, $\bar{w} \in \{2,3,4,5\}$, depths $1, \geq 2$	3600	1	depth 1, $\bar{w} = 4$: labels of $P_{21952/9}$
27a1	$j \equiv 3$: 7 discs	78,750,000	2	residue points of P_0, of $\iota_K P_0$
	region A, $\bar{w} = \pm 1$, depth 1	22,500,000	0	
	region A, $\bar{w} = \pm 1$, depth ≥ 2	22,500,000	144	residue points of ξ (72), of $\iota_K \xi$ (72)

Table 11. The disc test at 7 for $p = 29$. The last column describes the allowed configurations by the residue points (Section 9.3) or the labels (Lemma 4.5) of known points; a number in parentheses is the number of allowed configurations of that kind.

For $E \neq$ 27a1 we assume that $7 \nmid h_{K_E}$, the hypothesis of Theorem B(b). The places above 7 have degree 5 or 15, so $\bigoplus_{v|7} k_v \simeq \mathbb{F}_7^{30}$. Let S be the set of places above 29. As in Section 9.2, a computation in [32] gives the $15 + \#S$ elements u_i of Remark 3.15, with linearly independent images in $\mathbb{F}_7^{30}$, so the localization $K(S,7) \to \mathbb{F}_7^{30}$ is injective. Its image Σ, the allowed configurations and their Selmer classes are defined as in Section 9.2. By Table 10, the residue $1728 \equiv 6$ never occurs, and region A ($7 \mid b$) occurs for 864c1, 54a1, 96a1 and 27a1.

Known points (Section 2.6). For E without complex multiplication they are the points $P_j \in X_0(29)(K_E)$, one over the j-invariant j of each curve isogenous to E, as $\mathrm{Aut}(K_E) = 1$ (Lemma 2.14). For 27a1 they are P_0 and $\iota_K P_0$ over $j(27a2) = -12288000$, and the two K-points ξ, $\iota_K \xi$ over 0, from the trivial solutions $(\pm 1, 0, 1)$. Modulo 49: for 864a1, 864b1, 864c1, $-216 \equiv 29$, $-13824 \equiv 43$, $1536 \equiv 17$. For 54a1, $9261/8 = 7^3 \cdot 27/8$ is in region A at depth 1 with $\bar{w} = 6$, $-1167051/512 \equiv 17$ and $-132651/2 \equiv 45$. For 96a1, $21952/9 = 7^3 \cdot 64/9$ is in region A at depth 1 with $\bar{w} = 4$, $140608/3 \equiv 9$, $97336/81 \equiv 16$ and $7301384/3 \equiv 30$. For 27a1, $-12288000 \equiv 24$.

Proposition 10.1. *For each of the six fields K_E, assume that $7 \nmid h_{K_E}$ (for $E =$ 27a1 this holds by Proposition A.12).*

(a) *The localization* $K(S,7) \to \mathbb{F}_7^{30}$ *is injective, every* $\delta_v(T)$ *is nonzero (here* $\delta(T) = 29^3$*), and the class tuple of every known point lies in* Σ*. For* $E =$ 864a1, 864b1, 864c1, 54a1, 96a1, 27a1*:* $\dim K(S,7) = 17, 17, 17, 17, 17, 16$*,* Σ *has codimension* $13, 13, 13, 13, 13, 14$*,* $\dim \Theta_T = 2, 2, 6, 6, 2, 6$ *and* $\dim(\Sigma \cap \Theta_T) = 1, 1, 1, 1, 1, 4$*.*

(b) *The disc test (Proposition 4.9) gives Table 11. For the values of* $\bar{w}$ *not listed there, region A has no admissible configuration.*

(c) *For every known point* P_0 *of the curves without complex multiplication, and for* P_0 *and* $\iota_K P_0$ *in the case of* 27a1*, the tuple* ϑ *of Lemma 5.9 is not in* $\Sigma + \Theta_T$*. The case is* (U) *(*$e_0 = 0$*), except for* $P_{9261/8}$ *and* $P_{21952/9}$*, where it is* (R) *with* $e_0 = 2$*.*

(d) *For* 27a1*: no admissible configuration at depth* 1 *of region A has its class tuple in* $\Sigma + \Theta_T$*.*

Proof. These are finite computations, with the basis of $K(S,7)$ above and the classes of points located by Hensel's lemma (Appendix B.1): linear algebra over $\mathbb{F}_7$ for (a), (c), (d), and the disc test of Proposition 4.9 for (b).

For $E =$ 864a1, Table S17 prints the disc test of (b) so that it can be checked by hand. Over each of the seven representatives $j_1 \equiv 1 \pmod 7$, an admissible configuration puts one of the two Frobenius orbits of 15 points at each place above 7, so its class tuple is $(\sigma^i a_1 \,|\, \sigma^k b_2)$ or $(\sigma^i a_2 \,|\, \sigma^k b_1)$, with $0 \le i, k \le 14$ and a_1, b_1, a_2, b_2 the classes printed for its disc. For the four marked vectors Υ_r, the tuple $\big(\Upsilon_r(\sigma^i a \,|\, 0)\big)_r$ never equals $\big(-\Upsilon_r(0 \,|\, \sigma^k b)\big)_r$, except for $(\sigma^0 a_1 \,|\, \sigma^0 b_2)$ at $j_1 = 29$, where $(a_1 \,|\, b_2) = \delta(P_{-216})|_7 \in \Sigma$. So some Υ_r is nonzero on every other class tuple, and the test allows only the residue points of P_{-216}. □

Proposition 10.2. *Let* $P \in X_0(29)(K_{27a1})$ *be the point of a primitive solution of* $x^2 + y^3 = z^{29}$ *with* $abc \neq 0$ *(Proposition 2.12). Then* $j(P)$ *is not in region A.*

Proof. Let $K = K_{27a1}$. It satisfies the hypotheses of Proposition 3.18: $7 \nmid h_K$ by Proposition A.12, the places above 7 have degree 5, where (H_v) holds (Section 3.6), and 29 is totally ramified with residue degree one, so Remark 3.19 applies. By Proposition 4.9 and Table 11, $j(P)$ is not at depth 1 of region A. If it were at depth $k \ge 2$, then by Table 11 P_v would lie in the residue disc of ξ_v for every $v \mid 7$, or in that of $\iota_K \xi_v$ for every v. Then Lemma 5.10(ii) would put the class tuple of an admissible configuration at depth 1 in Σ, contradicting Proposition 10.1(d). □

Theorem 10.3. *Assume that the class numbers of the five fields* K_E *of degree* 30 *attached to* $E =$ 54a1, 96a1, 864a1, 864b1, 864c1 *are prime to* 7*. Then every primitive solution* (a, b, c) *of* $x^2 + y^3 = z^{29}$ *with* $abc \neq 0$ *is* $(\pm 3, -2, 1)$*.*

Proof. Let (a, b, c) be a primitive solution with $abc \neq 0$, E and E' as in Theorem 2.1, $K = K_E$, and $P \in X_0(29)(K)$ the point of Proposition 2.12. By Lemma 9.1, $7 \nmid c$, j_0 is 7-integral and $\bar{j}_0 := j_0 \bmod 7$ lies in $\mathcal{J}(E) \subseteq \{0, 1, 2, 3\}$.

If $\bar{j}_0 \neq 0$, then by Proposition 4.9 and Table 11, j_0 is congruent modulo 49 to the j-invariant j_* of a known point P_0 in an unramified residue, and P_v lies in the residue disc of $P_{0,v}$ for every $v \mid 7$. So $P = P_0$ and $j_0 = j_*$ by Lemma 5.9, case (U). If E has no complex multiplication, the hypotheses (i) of Lemma 5.9 hold by Proposition 10.1(a),(c): by (a), $\Sigma \cap \Theta_T$ has dimension 1 and contains $\delta(T)|_7 \neq 0$, so $\Sigma \cap \Theta_T = \mathbb{F}_7\, \delta(T)|_7$. For 27a1 its hypotheses (ii) hold by the proof of Proposition 10.2 and by Proposition 10.1(c), since $\vartheta \notin \Sigma + \Theta_T$ implies $\vartheta \notin \Sigma$.

If $\bar{j}_0 = 0$, then j_0 is in region A at depth $v_7(b)$. By Proposition 10.2, $E \neq$ 27a1. By Proposition 4.9 and Table 11, E is 54a1 or 96a1, the depth is 1, and P has the labels of

$P_0 = P_{9261/8}$, respectively $P_{21952/9}$, at every place. Lemma 5.9 in case (R), with hypotheses (i), gives $P = P_0$ and $j_0 = j(P_0)$.

In all cases j_0 is a known j-invariant (2.5), so $(a, b, c) = (\pm 3, -2, 1)$ by Lemma 2.15. □

10.1. **Proof of Theorem B(b).** Under the hypothesis of Theorem B(b), Theorem 10.3 shows that every primitive solution of $x^2 + y^3 = z^{29}$ with $abc \neq 0$ is $(\pm 3, -2, 1)$. The primitive solutions with $abc = 0$ are the trivial ones listed in Theorem B(b) (Section 1.1), and $3^2 + (-2)^3 = 1^{29}$. This proves Theorem B(b). □

Part III. The exponent 25

11. The reduction of Freitas and Stoll

We state here what Part III takes from the work of Freitas and Stoll [28], an arXiv preprint, on the equation

$$x^2 + y^3 = z^{25}. \tag{11.1}$$

Their reduction (Theorem 11.6) shows that a primitive solution (a, b, c) with $abc \neq 0$ comes from one of eight binary forms h_i at coprime integers (u, v) that satisfy a congruence condition at 2 and 3 and a condition on the class of a factor $H_i(u, v)$ of $h_i(u, v)$ modulo fifth powers. Freitas and Stoll use GRH once, through Stoll's determination of the rational points of a curve of genus 4 [64, Theorem 9.1]. We prove that result without GRH (Proposition 11.4), and we supplement one step of their sieve at the primes above 5 (Lemma 11.3). We cite [28] by the numbering of its version 1 (arXiv:2506.10667, June 2025). Part III has its own notation (Section 11.7); in particular K now denotes a sextic field, not a field K_E.

11.1. **Edwards' forms.** Freitas and Stoll write $h = [\eta_0, \dots, \eta_{12}]$ for the binary form $h(u, v) = \sum_{k=0}^{12} \binom{12}{k} \eta_k u^k v^{12-k}$, and define 27 forms $h_1, \dots, h_{27}$, printed in [28, Table 3]; Table S18 in the Supplement prints the eight that we need. With

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

the forms f_i, g_i, h_i have integral coefficients and degrees 30, 20, 12, and $f_i^2 + g_i^3 + h_i^5 = 0$.

Theorem 11.1 (Edwards [21]; see [28, Theorem 2.1])**.** *If x_1, y_1, z_1 are coprime integers with $x_1^2 + y_1^3 + z_1^5 = 0$, then there are $i \in \{1, \dots, 27\}$, coprime integers u, v and a sign such that $x_1 = \pm f_i(u, v)$, $y_1 = g_i(u, v)$ and $z_1 = h_i(u, v)$.*

For a primitive solution (a, b, c) of (11.1), Theorem 11.1 applied to $(a, b, -c^5)$ gives i and coprime u, v with $a = \pm f_i(u, v)$, $b = g_i(u, v)$ and $-c^5 = h_i(u, v)$, and the solution *comes from* h_i and (u, v).

11.2. **The eight remaining forms.** The reduction leaves eight forms, indexed by $\mathcal{I} = \{5, 6, 13, 14, 16, 22, 23, 24\}$. Apart from h_7, h_{11}, h_{19}, which are excluded by [28, Lemma 4.1], twelve of the 27 forms are irreducible over $\mathbb{Q}(\sqrt{5})$, namely h_i for $i \in \mathcal{I} \cup \{8, 9, 15, 21\}$. We call these the *twelve forms*. For each of them there is a sextic field K over which h_i is a constant times the product of an irreducible quadratic form and an irreducible form H_i of degree 10 [28, §9]. For $i \in \{5, 6, 16, 22, 24\}$ the field is in [28, Table 2], and h_{13}, h_{23}, h_{14} use the fields of h_5, h_6, h_{16} (Lemma 11.8). We normalize H_i so that $H_i(t, 1)$ is monic in t. For $i \in \mathcal{I}$ the *known pair* (u_i, v_i) of h_i is that of Table 12, and $\pm(u_i, v_i)$ are the expected solutions of $H_i(u, v) = H_i(u_i, v_i)\, w^5$ with $w \in K$ [28, Table 1 and the list before Proposition 9.1].

i	i'	(u_i, v_i)	classes at 2	classes at 3	known pair
5	5	$(0,1)$	$(2u,1)$, $(1,2v)$	$(3u,1)$, $(3u+2,1)$, $(1,3v)$	gives $(\pm 3, -2, 1)$
13	5	$(0,1)$	$(1,v)$	$(3u+1,1)$, $(3u,1)$, $(1,3v)$	excluded at 2
6	6	$(0,1)$	$(u,1)$	$(1, 81v+51)$	excluded at 3
23	6	$(0,1)$	$(1,v)$	$(1, 81v+66)$	excluded at 2 and 3
16	16	$(0,1)$	$(2u,1)$, $(1,2v)$	$(3u+2,1)$, $(3u+1,1)$, $(1,3v)$	excluded at 3
14	16	$(1,-1)$	$(2u,1)$, $(1,2v)$	$(3u+1,1)$, $(3u,1)$, $(1,3v)$	excluded at 2 and 3
22	22	$(1,0)$	$(1, 8v+6)$	$(u,1)$	excluded at 2 and 3
24	24	$(1,0)$	$(u,1)$	$(3u+1,1)$, $(3u,1)$, $(1,3v)$	excluded at 2

TABLE 12. The eight forms of Theorem 11.6, the index i' of the curve used for h_i (Lemma 11.8), and the residue classes of [28, Table 5], in which (u, v) must lie at 2 and at 3: $(2u, 1)$ means $u \equiv 0 \bmod 2$ and v odd, $(1, 8v+6)$ means u odd and $v \equiv 6u \bmod 8$, $(1, 81v + 51)$ means $3 \nmid u$ and $v \equiv 51u \bmod 81$, and similarly for the others. The last column shows where the known pair (u_i, v_i) fails these conditions, or the solution it gives.

11.3. **The sieve at the primes above 5.** For the twelve forms, Freitas and Stoll show that $H_i(u, v)$ is a unit of K times a fifth power, and they sieve the 125 classes of units modulo fifth powers by local conditions at 11, 31, 101 and above 5 [28, §9]. Their sieve discards every $(u : v)$ at which the ramified prime above 5 divides $H_i(u, v)$. For h_{15}, h_{21}, h_{24} this prime does divide $H_i(u, v)$ at some pairs that satisfy every local condition at 2, 3 and 5 imposed by a primitive solution. For example, take $i = 15$ and $(u, v) = (60490, 1)$. Then $(f_{15}, g_{15}, h_{15})(u, v)$ has no common prime factor, $h_{15}(u, v)$ is prime to 6, $v_5(h_{15}(u, v)) = 5$ and $-h_{15}(u, v)/5^5 \equiv 7 \pmod{25}$, so $-h_{15}(u, v)$ is a fifth power in $\mathbb{Q}_2$, $\mathbb{Q}_3$, $\mathbb{Q}_5$. Yet the ramified prime divides $H_{15}(u, v)$ to the exponent 25. Here, in the notation of Section 11.1,

$$h_{15} = 567u^{12} - 5508u^{11}v - 8910u^{10}v^2 - 5940u^9v^3 - 4455u^8v^4 + 7128u^7v^5 - 10692u^6v^6 \\ - 11880u^5v^7 - 4455u^4v^8 - 660u^3v^9 - 462u^2v^{10} + 348uv^{11} + 55v^{12},$$

its field K, that of h_{24} in Table S18, is defined by $U^6 - 10U^3 - 6U + 5$, and $5\mathcal{O}_K = \mathfrak{q}_1^5\mathfrak{q}_2$, where $\mathfrak{q}_1$ is the ramified prime. Lemma 11.3 uses a condition at 5 valid for all twelve forms and reaches the conclusion of [28, §9].

In Part III, a pair (u, v) of coprime integers is *admissible* for h_i (a notion unrelated to the admissible configurations of Parts I and II) if $f_i(u, v)$, $g_i(u, v)$, $h_i(u, v)$ have no common prime factor and $-h_i(u, v) = c^5$ for an integer c. A primitive solution that comes from h_i and (u, v) gives an admissible pair. The forms h_8 and h_{16} share their field K, as do h_9 and h_5, and so do h_{15}, h_{21} and h_{24}. Let $\mathcal{O} = \mathcal{O}_K$. Over K we write $h_i = n_i\, q_i\, H_i$ with $n_i \in \mathbb{Z}$ the content of h_i, and q_i, H_i binary forms of degrees 2 and 10 with coefficients in $\mathcal{O}$ that generate the unit ideal. This H_i differs from that of Section 11.2 by a factor in $K^\times$, which leaves the statement of Lemma 11.3 unchanged. For a prime $\mathfrak{q}$ of K and $x \in K^\times$ let $[x]_\mathfrak{q}$ be the class of x in $K_\mathfrak{q}^\times / K_\mathfrak{q}^{\times 5}$, and for a prime $\mathfrak{q} \nmid 30$ of norm $\equiv 1 \pmod 5$ let $\chi_\mathfrak{q} \colon (\mathcal{O}/\mathfrak{q})^\times \to \mathbb{Z}/5$ be a fifth-power residue character. A root of h_i modulo 5 is a point of $\mathbb{P}^1(\mathbb{F}_5)$ at which the reduction of h_i vanishes.

Lemma 11.2. *For each of the twelve forms h_i and its field K, the following hold.*

(a) *K has signature $(2, 2)$ and class number 1, and $5\mathcal{O} = \mathfrak{q}_1^5\mathfrak{q}_2$ with $\mathfrak{q}_1 \neq \mathfrak{q}_2$ of residue degree 1. The content n_i is 4 for $i = 22$, 3 for $i \in \{6, 23\}$, and 1 otherwise.*

(b) *The reduction of h_i modulo 5 is the tenth power of a linear form times a quadratic form prime to it. Let r_i be the root of the linear form. Then $v_5(h_i(u,v)) = 2$ for every $(u,v) \in \mathbb{Z}_5^2$ reducing to r_i. The quadratic form has the roots $(0:1)$, $(4:1)$ for $i \in \{15, 21\}$ and $(0:1)$, $(2:1)$ for $i = 24$, and no root in $\mathbb{P}^1(\mathbb{F}_5)$ for the other nine forms.*

(c) *The resultant of q_i and H_i is divisible by no prime of K other than those above 2, 3 and 5, and not by $\mathfrak{q}_2$.*

(d) *Let $p \in \{2, 3\}$ and let $(u,v) \in \mathbb{Z}_p^2$, not both divisible by p, be such that $f_i(u,v)$, $g_i(u,v)$, $h_i(u,v)$ are not all divisible by p and $v_p(h_i(u,v)) \equiv 0 \pmod 5$. Then $h_i(u,v)$ is a p-adic unit, except for $i = 22$ at $p = 2$ and $i \in \{6, 23\}$ at $p = 3$. In these three cases, for every prime $\mathfrak{q}$ of K above p, one of $n_i q_i(u,v)$ and $H_i(u,v)$ has $\mathfrak{q}$-adic valuation divisible by 5.*

(e) *For $i \in \{15, 21, 24\}$ and a simple root $(\tilde{r} : 1)$ of h_i modulo 5, $q_i(\tilde{r}, 1) \notin \mathfrak{q}_1$ and $H_i(\tilde{r}, 1) \notin \mathfrak{q}_2$.*

(f) *There are units $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathcal{O}^\times$ whose fifth-power residue characters at the primes of K above 11, 31, 41, 61, 71 and 101 have rank 3 over $\mathbb{F}_5$.*

Proof. These are finite computations with PARI/GP in the fields K (Appendix B), with the class number of Proposition A.13. Part (d) repeats the local computation of [28, §4 and §9] at 2 and 3. □

For the sieve at 5 let $\mathcal{V}_i$ be the set of pairs $([x_1]_{\mathfrak{q}_1}, [x_2]_{\mathfrak{q}_2})$ obtained from all $(u,v) \in (\mathbb{Z}/25\mathbb{Z})^2$ with $(u,v) \not\equiv (0,0) \pmod 5$, except those that reduce to r_i and, over a simple root of h_i modulo 5, those with $25 \nmid h_i(u,v)$. Here $x_1 = x_2 = H_i(u,v)$ if $(u:v)$ does not reduce to a root of h_i modulo 5, and $x_1 = (n_i q_i(u,v))^{-1}$, $x_2 = H_i(u,v)$ if it reduces to a simple root, all evaluated at integer representatives. For $i \in \mathcal{I}$ let $\varepsilon^{(i)} \in \mathcal{O}^\times$ and $w_i \in \mathcal{O}$ be such that $H_i(u_i, v_i) = \varepsilon^{(i)} w_i^5$.

Lemma 11.3. *Let $i \in \mathcal{I} \cup \{8, 9, 15, 21\}$, and let (u,v) be an admissible pair for h_i. Then $i \notin \{8, 9, 15, 21\}$, and $H_i(u,v) \in H_i(u_i, v_i)\,(K^\times)^5$, where (u_i, v_i) is the known pair of h_i. In particular $H_{24}(u,v) = H_{24}(1,0)\,w^5$ with $w \in K^\times$ for $i = 24$.*

Proof. Write h, q, H, n for h_i, q_i, H_i, n_i, and $-h(u,v) = c^5$. As q and H are irreducible over K, h has no zero in $\mathbb{P}^1(\mathbb{Q})$, so $c \neq 0$, and $H(u,v)$ divides $h(u,v)$ in $\mathcal{O}$. For a prime $\mathfrak{q}$ of K above ℓ, $v_{\mathfrak{q}}(h(u,v)) = 5\,e(\mathfrak{q}/\ell)\,v_\ell(c) \equiv 0 \pmod 5$. If binary forms A, B over $\mathcal{O}$ of degrees m, m' have resultant $R \neq 0$, there are binary forms C_1, D_1, C_2, D_2 over $\mathcal{O}$ with $C_1 A + D_1 B = R\,v^{m+m'-1}$ and $C_2 A + D_2 B = R\,u^{m+m'-1}$, so a prime dividing $A(u,v)$ and $B(u,v)$ divides R, as u, v are coprime.

Step 1: $H(u,v)$ is a unit times a fifth power. Let $\mathfrak{q}$ be a prime of K. If $\mathfrak{q}$ lies above no prime in $\{2, 3, 5\}$, or $\mathfrak{q} = \mathfrak{q}_2$, then $\mathfrak{q} \nmid n$ and $\mathfrak{q}$ does not divide the resultant of q and H (Lemma 11.2(a), (c)), so $v_{\mathfrak{q}}(H(u,v))$ is 0 or $v_{\mathfrak{q}}(h(u,v))$, divisible by 5. If $\mathfrak{q}$ lies above $p \in \{2, 3\}$, Lemma 11.2(d) applies, since $(f, g, h)(u,v)$ is p-adically primitive and $v_p(h(u,v)) = 5 v_p(c)$. Either $h(u,v)$ is a p-adic unit, and then so is $H(u,v)$, or one of $v_{\mathfrak{q}}(nq(u,v))$, $v_{\mathfrak{q}}(H(u,v))$ is divisible by 5, and then so is the other, as they add up to $v_{\mathfrak{q}}(h(u,v))$. Let $\mathfrak{q} = \mathfrak{q}_1$ and let $r \in \mathbb{P}^1(\mathbb{F}_5)$ be the reduction of $(u:v)$. If $r = r_i$, then $v_5(h(u,v)) = 2$ by Lemma 11.2(b), contradicting $5 \mid v_5(h(u,v))$. If h does not vanish at r modulo 5, then $5 \nmid h(u,v)$ and $\mathfrak{q}_1 \nmid H(u,v)$. If r is a simple root of h modulo 5, then $i \in \{15, 21, 24\}$, $n = 1$ and $q(u,v) \notin \mathfrak{q}_1$ by Lemma 11.2(e), so $v_{\mathfrak{q}_1}(H(u,v)) = v_{\mathfrak{q}_1}(h(u,v)) \equiv 0 \pmod 5$. So the ideal $H(u,v)\mathcal{O}$ is a fifth power, and as K has class number 1, $H(u,v) = \varepsilon w^5$ with $\varepsilon \in \mathcal{O}^\times$ and $w \in \mathcal{O}$.

Step 2: the classes at $\mathfrak{q}_1$ and $\mathfrak{q}_2$. We have $r \neq r_i$. From $H(u,v) = \varepsilon w^5$ and $h(u,v) = nq(u,v)H(u,v) = (-c)^5$ we get $[\varepsilon]_\mathfrak{q} = [H(u,v)]_\mathfrak{q} = [(nq(u,v))^{-1}]_\mathfrak{q}$ for every prime $\mathfrak{q}$. If h does not vanish at r modulo 5, then $H(u,v)$ is a unit at $\mathfrak{q}_1$ and $\mathfrak{q}_2$. If r is a simple root, then $5 \mid v_5(h(u,v)) > 0$, so $25 \mid h(u,v)$, and $q(u,v)$ is a unit at $\mathfrak{q}_1$ and $H(u,v)$ a unit at $\mathfrak{q}_2$ by Lemma 11.2(e). For $\mathfrak{q} \in \{\mathfrak{q}_1, \mathfrak{q}_2\}$ the class of a unit x of $\mathcal{O}_\mathfrak{q}$ depends only on x modulo $\mathfrak{q}^{2e(\mathfrak{q})}$, because $1 + \mathfrak{q}^{2e(\mathfrak{q})}\mathcal{O}_\mathfrak{q}$ consists of fifth powers by Lemma 13.5. Since $25\mathcal{O} = \mathfrak{q}_1^{10}\mathfrak{q}_2^2$, these classes depend only on (u,v) modulo 25. Hence $([\varepsilon]_{\mathfrak{q}_1}, [\varepsilon]_{\mathfrak{q}_2}) \in \mathcal{V}_i$.

Step 3: the sieve. The field K has signature $(2,2)$ and $\mu(K) = \{\pm 1\}$, so $\mathcal{O}^\times/\mathcal{O}^{\times 5} \simeq (\mathbb{Z}/5)^3$, with basis the classes of $\varepsilon_1, \varepsilon_2, \varepsilon_3$ by Lemma 11.2(f). So $\varepsilon = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\eta^5$ with $0 \le a_j \le 4$ and $\eta \in \mathcal{O}^\times$. Let $p \in \{11, 31, 101\}$ and let $\mathfrak{q} \mid p$ be a prime of K of norm $\equiv 1 \pmod 5$ with $\mathfrak{q} \nmid H(u,v)$. Then $\mathfrak{q} \nmid w$ and $\chi_\mathfrak{q}(\varepsilon) = \chi_\mathfrak{q}(H(u,v))$. The right side depends only on $(u:v) \in \mathbb{P}^1(\mathbb{F}_p)$, as $H(\lambda u, \lambda v) = \lambda^{10} H(u,v)$. So (a_1, a_2, a_3) lies in the set $\mathcal{S}(i)$ of exponent vectors such that (1) for each $p \in \{11, 31, 101\}$ some point of $\mathbb{P}^1(\mathbb{F}_p)$ gives the same character values at every such prime above p at which H does not vanish, and (2) the pair of classes at $\mathfrak{q}_1$ and $\mathfrak{q}_2$ lies in $\mathcal{V}_i$. A computation (Appendix B) shows that $\mathcal{S}(i)$ is empty for $i \in \{8, 9, 15, 21\}$, and that for the other eight forms it has exactly one element, the exponent vector of $\varepsilon^{(i)}$. So there is no admissible pair for $i \in \{8, 9, 15, 21\}$, and for the other forms $\varepsilon/\varepsilon^{(i)}$ is a fifth power in $\mathcal{O}^\times$, and $H(u,v)/H(u_i,v_i) = (\varepsilon/\varepsilon^{(i)})(w/w_i)^5 \in (K^\times)^5$. □

11.4. **Stoll's curve of genus four, and two facts from §7 of Freitas and Stoll.**

Proposition 11.4. *Let $D_0 \colon y^2 = F_0(x)$, where*

$$F_0(x) = 81x^{10} - 1650x^9 + 16725x^8 - 99000x^7 + 395250x^6 - 1039500x^5 + 1961250x^4 - 2475000x^3 + 2128125x^2 - 1031250x + 215625,$$

be the curve of genus 4 of [28, §8]. *Then $D_0(\mathbb{Q})$ consists of the two points $(1 : \pm 9 : 0)$ at infinity.*

Proof. The substitution $x = 1 - 2x'$, $y = 32y'$ transforms D_0 into Stoll's model $D \colon y'^2 = f(x')$ with

$$f(x) = 81x^{10} + 420x^9 + 1380x^8 + 1860x^7 + 3060x^6 - 66x^5 + 3240x^4 - 1740x^3 + 1320x^2 - 480x + 69,$$

and matches the points at infinity. We follow Stoll's proof [64, §9], with the class groups of Proposition A.13 in its second step and all four sign patterns in its third.

Let θ be a root of f and $k = \mathbb{Q}(\theta)$, of degree 10 and signature $(0,5)$, isomorphic to the field of a root of $t^{10} + 75t^6 - 50t^5 + 100t^3 + 625t^2 + 1250t + 645$. Let S be the set of primes of k above 2, 3, 5. The class group of k is cyclic of order 6, generated by the class of a prime in S (Proposition A.13), so $k(S,2) = \mathcal{O}_{k,S}^\times/\mathcal{O}_{k,S}^{\times 2}$ has dimension 12. It has an explicit basis of S-units, independent modulo squares by their quadratic residue characters.

Step 1: a two-cover descent. For a field $\Omega \supseteq \mathbb{Q}$ let $\mu_\Omega \colon D(\Omega) \to (k \otimes \Omega)^\times/((k \otimes \Omega)^{\times 2}\,\Omega^\times)$ send P to the class of $x(P) - \theta$, and the points at infinity to 1. Since $N_{k/\mathbb{Q}}(x(P) - \theta) = y(P)^2/81$ and D has good reduction outside 2, 3, 5, $\mu_\mathbb{Q}(P)$ is the class of some $\xi \in k(S,2)$ with $N(\xi) \in \mathbb{Q}^{\times 2}$ whose image in $(k \otimes \mathbb{Q}_p)^\times/(k \otimes \mathbb{Q}_p)^{\times 2}\mathbb{Q}_p^\times$ lies in $\mu_{\mathbb{Q}_p}(D(\mathbb{Q}_p))$ for every p. The images $\mu_{\mathbb{Q}_p}(D(\mathbb{Q}_p))$ for $p = 2, 3, 29$ leave only the classes of elements of $\mathbb{Q}^\times$, so $\mu_\mathbb{Q}(P) = 1$ for $P \in D(\mathbb{Q})$. These images are computed by covering $\mathbb{P}^1(\mathbb{Q}_p)$ with discs on which the classes of $x - \theta$ at all primes of k above p are constant (Appendix B). At $p = 2$ the only disc of $D(\mathbb{Q}_2)$ on which $\mu_{\mathbb{Q}_2}$ is trivial is $\{v_2(x) \le -3\}$ with the points at infinity. So a rational point P not at infinity has $v_2(x(P)) \le -3$ and $x(P) - \theta = \lambda\beta^2$ with $\lambda \in \mathbb{Q}^\times$, $\beta \in k^\times$.

The field k has an automorphism of order 2, and over k, f is the product of two linear factors and two quartic factors that this automorphism exchanges. Let g be one of the quartic factors, made monic. In a splitting field the roots of g are $\rho_1(\theta), \dots, \rho_4(\theta)$ for automorphisms ρ_j, so $g(x(P)) = \lambda^4\big(\prod_j \rho_j(\beta)\big)^2$, where the product is fixed by the automorphisms fixing k, as they permute the $\rho_j|_k$. Hence $g(x(P)) \in k^{\times 2}$.

Step 2: an elliptic curve over k. Let $\mathcal{Y}\colon y^2 = g(x)$, of genus 1 over k with the k-rational points ∞_1, ∞_2 at infinity ($y/x^2 \to 1$, resp. -1), and let E be its Jacobian. Then $E(k)[2] \simeq \mathbb{Z}/2$, generated by a point T_2. The extension k' of k of degree 2 generated by a root of the quadratic factor of the 2-division polynomial of E has class group $(\mathbb{Z}/3)^2$ (Proposition A.13(e)), of odd order. So the 2-Selmer group of E over k is cut out by local conditions at the seven primes of k above 2, 3, 5 inside a group of dimension 21 built from explicit bases of $k(S,2)$ and $k'(S,2)$. The local images at these primes, spanned by explicit local points, have dimensions 3, 10, 1, 1, 2, 2, 2, and the Selmer group has dimension 6 (Appendix B).

Step 3: the 2-adic argument. Let $A = R_{k/\mathbb{Q}}E$ and $i\colon \mathcal{Z} \to A$, $Q \mapsto [Q - \infty_1]$, where $\mathcal{Z}$ is the curve over $\mathbb{Q}$ of points of $\mathcal{Y}$ with rational x-coordinate. The primes of k above 2 are v_1, v_2, with $(e,f) = (2,1)$, $(2,4)$, and $A(\mathbb{Q}_2) = E(k_{v_1}) \times E(k_{v_2})$. By Step 1, a rational point P of D not at infinity gives $(x(P), \eta) \in \mathcal{Z}(\mathbb{Q})$ with $\eta^2 = g(x(P))$. Put $s = 1/(4x) \in 2\mathbb{Z}_2$. Then $g(x)/x^4 \equiv 1$ modulo $\mathfrak{p}^6$ at v_1 and v_2, so $\eta = \pm x^2 u_v(s)$ at $v \in \{v_1, v_2\}$, with $u_v(s) \equiv 1 \pmod{\mathfrak{p}^3}$ the square root given by the binomial series. The signs give four families of points of $\mathcal{Z}(\mathbb{Q}_2)$, exchanged in pairs by $y \mapsto -y$, so it suffices to treat X_{++}, with signs $(+,+)$, which contains ∞_1 at $s = 0$, and X_{+-}. In the parameter s the formal parameter of a minimal model of E at v is 2 times a power series in s with integral coefficients vanishing at 0. So $i(X_{++}(s))$ lies in the subgroup $K_{v_2(s)+1}$ of $A(\mathbb{Q}_2)$, where K_n is the product of the $2n$-th kernels of reduction at v_1, v_2. Here $K_{n+j} = 2^j K_n$ for $n \geq 2$, and points whose parameters differ by an element of $2^m\mathbb{Z}_2$ differ by an element of K_{m+1}. Stoll's Lemmas 3.1, 3.3, 3.4 and 3.7 [64, §3] apply in the parameter s, not in his parameter $t = 2s$, where this integrality fails. The level of $B \in A(\mathbb{Q}_2)$ is $\sup\{n\colon B \in 2^n A(\mathbb{Q}_2)\}$, as in Section 5.1 with $\varpi = [2]$ and $W = 0$, and n_m denotes the largest level of a point $i(X_{++}(s))$ with $v_2(s) = m$. We use Lemma 3.7 at $m = 3$ in the form that needs $2m - 1 \geq n_m + 2$. By the values below, $n_3 = 3$, so the condition holds. Stoll's lemmas show that for the sets $q(\cdot)$ of [64, §2] (for multiplication by 2) the points of $X_{++} \smallsetminus \{\infty_1\}$ give only the sets at $s = \pm 2, \pm 4, \pm 8$ and $\{0\}$. The points of X_{+-} are $P^* + R(s)$, where $P^* \in A(\mathbb{Q}_2)$ is 0 at v_1 and $[\infty_2 - \infty_1]$ at v_2 and $R(s) \in K_{v_2(s)+1}$, and they give only the sets at $s = \pm 2, \pm 4$ and $q(P^*)$. A computation at these points (Appendix B) shows the following. The 2-Selmer group injects into $A(\mathbb{Q}_2)/2A(\mathbb{Q}_2)$, and $A(\mathbb{Q}_2)$ has no point of order 4. The levels of $i(X_{++}(s))$ at $s = 2, -2, 4, -4, 8, -8$ are 1, 1, 2, 2, 3, 3. The union of the sets $q(\cdot)$ for $X_{++} \smallsetminus \{\infty_1\}$ has 16 elements and meets the image of the Selmer group in $\{0, \pi(T_2)\}$, where π is reduction modulo $2A(\mathbb{Q}_2)$. The union for X_{+-} has 17 elements and meets the image of the Selmer group in $\{0\}$. Moreover $\pi(T_2) \neq 0$ and the points of both families have image 0 under π, so $q(i(Q) + T_2) = \{\pi(T_2)\}$ for them. So [64, Theorem 2.1], which uses only that $A(\mathbb{Q})$ is finitely generated, applies to A, multiplication by 2, $\Gamma = \{0, T_2\}$, $\mathcal{Z}$, i and the set $(X_{++} \smallsetminus \{\infty_1\}) \cup X_{+-}$, and $i(Q)$ is torsion for every rational point Q in these families. The component at v_1 of such a point lies in the torsion-free group K_2, so $i(Q)$ is a torsion point of $E(k)$ vanishing in $E(k_{v_1})$, hence $i(Q) = 0$, $Q = \infty_1$, and $D(\mathbb{Q})$ consists of the points at infinity. □

Lemma 11.5. (a) *The curve* $5Y^2 = X^4 - 10X^2 + 5$ *has exactly the rational points* $(0, \pm 1)$, *and the elliptic curve* $y^2 = x^3 + x^2 - 83x + 88$ *has Mordell–Weil group* $\mathbb{Z}/2$, *generated by* $(8, 0)$.

(b) *Let* $M_4\colon y^2 = 3x(x^4 - 10x^2 + 5)(x^5 + 10x^4 - 10x^3 - 20x^2 + 5x + 2)$ *be the curve of genus* 4 *of* [28, §7]. *The class* $[(1, 12) - (0, 0)]$ *has infinite order in the Jacobian of* M_4.

Proof. (a) Put $x_H = X$ and $y_H = 5Y$, so that the curve is $y_H^2 = 5(x_H^4 - 10x_H^2 + 5)$. The rational maps

$$(x_H, y_H) \mapsto \Big(\frac{50 - 10y_H}{x_H^2}, \frac{500x_H^2 + 100y_H - 500}{x_H^3}\Big),$$
$$(x_1, y_1) \mapsto \Big(\frac{500 - 10x_1}{y_1}, 5 - \frac{10x_1^3 - 1000x_1^2 + 25000x_1}{y_1^2}\Big)$$

are inverse birational maps between this curve and $E_1\colon y_1^2 = x_1^3 - 50x_1^2 - 500x_1 + 25000$, isomorphic to $E\colon y^2 = x^3 + x^2 - 83x + 88$ by $x_1 = 4x + 18$, $y_1 = 8y$, so the smooth projective models have the same number of rational points. With $x = X_2 + 8$ the curve E becomes $y^2 = X_2(X_2^2 + 25X_2 + 125)$, which is 2-isogenous to $E'\colon y^2 = X_2(X_2^2 - 50X_2 + 125)$. In the descent via 2-isogeny [60, §§III.5–6], $2^{\operatorname{rank} E(\mathbb{Q})} = \#\alpha(E(\mathbb{Q}))\,\#\alpha'(E'(\mathbb{Q}))/4$, where $\alpha(E(\mathbb{Q}))$ consists of the squarefree divisors d of 125 for which $N^2 = dM^4 + 25M^2e^2 + (125/d)e^4$ has an integer solution with $e \neq 0$ and $\gcd(M, e) = 1$, and similarly for E' with -50 in place of 25. Both images contain 1 and 5. For E and $d \in \{-1, -5\}$ the right side is $\equiv 3$ or $7 \pmod 8$ whenever M and e are not both even, and for E' and $d \in \{-1, -5\}$ all three coefficients are negative. So both images are $\{1, 5\}$ and $E(\mathbb{Q})$ has rank 0. The discriminant of E is $2^4 \cdot 5^9$, and $\#E(\mathbb{F}_3) = 6$, $\#E(\mathbb{F}_7) = 10$. Torsion of order prime to ℓ injects into $E(\mathbb{F}_\ell)$ for $\ell = 3, 7$ [59, Proposition VII.3.1], so $E(\mathbb{Q}) = \{\infty, (8, 0)\}$. The curve $y_H^2 = 5(x_H^4 - 10x_H^2 + 5)$ has no rational point at infinity, since 5 is not a square, so its rational points are $(0, \pm 5)$, that is $(X, Y) = (0, \pm 1)$.

(b) Under $x \mapsto 1/x$, $y \mapsto y/x^5$ the curve M_4 becomes $C_4\colon y^2 = f_4(x)$ with

$$f_4(x) = 30x^9 + 75x^8 - 360x^7 - 300x^6 + 756x^5 + 330x^4 - 360x^3 - 60x^2 + 30x + 3,$$

and the class $[(1, 12) - (0, 0)]$ becomes $P_4 = [(1, 12) - \infty]$. The discriminant of f_4 is $2^{72}3^{16}5^{12}$, so C_4 has good reduction at every $\ell \geq 7$. As the kernel of reduction on the Jacobian over $\mathbb{Z}_\ell$ is pro-ℓ, a point of finite order N reduces to a point of order N/ℓ^j for some $j \geq 0$. By Cantor's algorithm, the reduction of P_4 has order $1240 = 2^3 \cdot 5 \cdot 31$ modulo 7 and $70 = 2 \cdot 5 \cdot 7$ modulo 11 (Appendix B). If P_4 had finite order N, then $N = 1240 \cdot 7^a = 70 \cdot 11^b$, which is impossible by comparing the powers of 2. □

11.5. **The reduction.**

Theorem 11.6 (Freitas and Stoll [28])**.** (A) *Every primitive solution of* (11.1) *other than the trivial solutions* $(\pm 1, -1, 0)$, $(\pm 1, 0, 1)$, $(0, 1, 1)$, $(0, -1, -1)$ *comes from* h_i *and coprime integers* (u, v) *for some* $i \in \mathcal{I}$.

(B) *If a primitive solution comes from* h_i *and* (u, v) *with* $i \in \mathcal{I}$, *then*

(a) (u, v) *lies in one of the residue classes listed for* i *at* 2, *and in one of those listed at* 3, *in Table 12* ([28, Table 5])*;*

(b) $H_i(u, v)/H_i(u_i, v_i) \in (K^\times)^5$, *where* (u_i, v_i) *is the known pair of* h_i.

(C) *The pair* $\pm(u_i, v_i)$ *gives a primitive solution of* (11.1) *only for* $i = 5$, *and then the solution is one of* $(\pm 3, -2, 1)$.

Where this is proved. By Theorem 11.1 every primitive solution comes from some h_i and coprime (u, v). The forms h_7, h_{11}, h_{19} give no primitive solution [28, Lemma 4.1]. The forms that factor over $\mathbb{Q}$ into irreducible factors of degrees 1, 1 and 10, or 4 and 8, and those that factor over $\mathbb{Q}(\sqrt{5})$ into two irreducible factors of degree 6, give only the trivial solutions listed [28, §§6–8 and Table 1]. Of the twelve forms, h_8, h_9, h_{15}, h_{21} give no primitive solution by Lemma 11.3. This proves (A). Condition (a) expresses that $(a, b, -c^5)$ is a primitive solution 2-adically and 3-adically [28, §4 and Table 5], and (b) is Lemma 11.3. Part (C) is the list of solutions of $H_i(u, v) = w^5$ in [28, §9] that precedes [28, Proposition 9.1], together with the proof of that proposition. The pairs $\pm(0, 1)$ for $i = 5$ give $(f_5, g_5, h_5)(0, 1) = (-3, -2, -1)$, so $a = \pm 3$, $b = -2$ and $c = 1$.

The following five inputs are established here.

(i) Stoll's determination of $D_0(\mathbb{Q})$ [64, Theorem 9.1], used in [28, §8], is Proposition 11.4.

(ii) Every class group, unit group and S-unit group used in [28, §§6–9] is determined in Proposition A.13 (the fields of Table 16 and the five sextic fields of §9).

(iii) The descents of [28] that use these groups were recomputed from them (Appendix B): the 2-descents on the Jacobians of $C_1 \colon y^2 = x^5 + 2^8 \cdot 5^3$ and $C_2 \colon y^2 = x^5 + 2^6 \cdot 5^3$ in §6 (rank 1 and rank 0, so that $C_2(\mathbb{Q}) = \{\infty\}$), the two-cover descents of M_3 and M_4 and the 2-Selmer bound rank ≤ 1 for the Jacobian of M_4 in §7, the two-cover descents of $D_{\pm 1}$ and $D_{\pm 2}$ in §8, and the sieve of §9, supplemented by Lemma 11.3.

(iv) The two facts of [28, §7] used to determine $M_3(\mathbb{Q})$ and $M_4(\mathbb{Q})$ are Lemma 11.5.

(v) Two results of [28] were obtained with Magma's Mordell–Weil, Chabauty and rank-bound routines: $C_1(\mathbb{Q}) = \{\infty, (-4, \pm 176)\}$ [28, §6] and $\operatorname{rank} J_{-1}(\mathbb{Q}), \operatorname{rank} J_{-2}(\mathbb{Q}) \leq 2$ [28, §8]. They were recomputed without Magma and without GRH, from (iii) and the groups $k_{\pm 1}(S, 2)$, $k_{\pm 2}(S, 2)$ of Proposition A.13 (Appendix B.2, (M1) and (M2)).

□

The statements of [28] that the proof of Theorem C uses without a new proof are the following, with their places in [28].

- The forms $h_1, \ldots, h_{27}$ and the definitions of f_i and g_i (§2 and Table 3), and the factorization types of the h_i over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{5})$ (§3 and Table 4).
- Lemma 4.1, which excludes h_7, h_{11}, h_{19}, and the residue classes of (u, v) at 2 and 3 (§4 and Table 5).
- For h_1, h_{20}, h_{25} (type $[1, 1, 10]$): the reduction to the curves C_1, C_2 and the translation of their points back to (u, v) (§6).
- For h_3, h_4, h_{12}, h_{17}, h_{18}, h_{27} (type $[4, 8]$): the reduction to the curves M_i, Table 8, the deductions from the points of M_3 and M_4, and the Chabauty argument at 11 (§7).
- For h_2, h_{10}, h_{26} (two factors of degree 6 over $\mathbb{Q}(\sqrt{5})$): the reduction to the curves D_j and $\tilde{D}_j$, Lemma 8.1, the odd index in Lemma 8.2, Proposition 8.3 and the Chabauty argument at 7 (§8).
- For the twelve forms: the factorization over a sextic field (§9), the fields of Table 2, the known pairs (Table 1 and the list before Proposition 9.1), and, for part (C), the proof of Proposition 9.1.

Remark 11.7. Freitas and Stoll [28, Theorem 1.1] derive the primitive solutions from the statement that $H_i(u, v) = H_i(u_i, v_i)\, w^5$ has no solutions other than $\pm(u_i, v_i)$ for $i \in \{5, 6, 16, 22, 24\}$. Sections 12, 13, 14 and 15 prove instead that no coprime (u, v)

other than $\pm(0,1)$ for $i = 5$ satisfies both (a) and (b) of Theorem 11.6(B). For h_{22} these sections use only that the class listed at 2 contains the 2-adic pairs that pass the local test of [28, §4].

11.6. **The paired forms.** Three of the eight forms are, up to a constant factor, linear changes of variables of others. We treat each such h_i on the curve of a form $h_{i'}$ with $i' \in \{5, 6, 16, 22, 24\}$ (Section 12.1).

Lemma 11.8. *Put* $\Psi_{23}(u,v) = (u/2, v)$, $\Psi_{13}(u,v) = (-u/2, u/2 + v)$ *and* $\Psi_{14}(u,v) = (-u - v, -u + v)$. *Then*

$$h_{23} = 64\, h_6 \circ \Psi_{23}, \qquad h_{13} = 64\, h_5 \circ \Psi_{13}, \qquad h_{14} = \tfrac{1}{64}\, h_{16} \circ \Psi_{14}.$$

Let $i \in \{13, 23, 14\}$, *let* $i' = 5, 6, 16$ *respectively, and let* $\Psi = \Psi_i$. *Over the field* K *of* $h_{i'}$ *the form* h_i *has an irreducible factor of degree* 10, *namely a constant multiple of* $H_{i'} \circ \Psi$. *If coprime integers* (u, v) *satisfy condition (b) of Theorem 11.6(B) for* i, *then every* $(u', v') \in \mathbb{Q}^2 \smallsetminus \{0\}$ *representing* $\Psi(u : v) \in \mathbb{P}^1(\mathbb{Q})$ *satisfies* $H_{i'}(u', v')/H_{i'}(u_{i'}, v_{i'}) \in (K^\times)^5$. *Moreover* $\Psi(u_i : v_i) = (0 : 1) = (u_{i'} : v_{i'})$, *and each* Ψ_i *induces a bijection of* $\mathbb{P}^1(\mathbb{Q}_5)$ *that maps residue classes of* $\mathbb{P}^1(\mathbb{Z}_5)$ *modulo* 5^k *to residue classes modulo* 5^k.

Proof. The identities of forms follow by expanding. Since Ψ is invertible and $K[u, v]$ is a unique factorization domain, the factorization of $h_{i'}$ over K pulls back to that of h_i, so H_i is a constant multiple of $H_{i'} \circ \Psi$. If (u, v) satisfies (b) for i, then

$$\frac{H_{i'}(\Psi(u,v))}{H_{i'}(\Psi(u_i, v_i))} = \frac{H_i(u,v)}{H_i(u_i, v_i)} \in (K^\times)^5.$$

We have $\Psi_{23}(0,1) = \Psi_{13}(0,1) = (0,1)$ and $\Psi_{14}(1,-1) = (0,-2)$, and $H_{16}(0,-2) = 2^{10} H_{16}(0,1)$. Multiplying (u', v') by a nonzero rational number multiplies $H_{i'}(u', v')$ by its tenth power, which is a fifth power. Finally, the matrices of Ψ_{23}, Ψ_{13}, Ψ_{14} have entries in $\mathbb{Z}[1/2]$ and determinants $1/2$, $-1/2$, -2, so they lie in $\mathrm{GL}_2(\mathbb{Z}_5)$. □

For every $i \in \mathcal{I}$ we put $\Psi_i = \mathrm{id}$ if $i = i'$, and we write $(u_0 : v_0) \coloneqq (u_{i'} : v_{i'})$ for the known pair of $h_{i'}$. By Lemma 11.8, a solution as in Theorem 11.6 gives $(u' : v') = \Psi_i(u : v)$ with

$$H_{i'}(u', v')/H_{i'}(u_0, v_0) \in (K^\times)^5. \tag{11.2}$$

11.7. **Conventions for Part III.** Throughout Part III, $\zeta = \zeta_5$ is a fixed primitive fifth root of unity and $\pi \coloneqq 1 - \zeta$. For a prime $\mathfrak{p}$ of a number field such as F or L we write $F_\mathfrak{p}$ (or $L_\mathfrak{p}$) for the completion, $\mathcal{O}_\mathfrak{p}$ for its valuation ring, $e(\mathfrak{p})$ and $f(\mathfrak{p})$ for the ramification index and residue degree, and $v_\mathfrak{p}$ for the normalized valuation, so that $v_\mathfrak{p} = e(\mathfrak{p}) v_5$ when $\mathfrak{p}$ lies above 5. On $\mathbb{Z}_5[\zeta]$, a discrete valuation ring with uniformizer π and residue field $\mathbb{F}_5$, we write v_π for the normalized valuation and a bar for reduction modulo π. For a power series $\varphi = \sum_n \varphi_n s^n$ with coefficients in a finite extension of $\mathbb{Q}_5$ with valuation v, and a rational number m_0, the *Gauss valuation* of φ on the closed disc $\{v(s) \geq m_0\}$ is $\inf_n(v(\varphi_n) + n m_0)$. It is multiplicative, and it is the minimum of $v(\varphi(s))$ over the disc (over an algebraic closure).

Some symbols of Table 3 have a different meaning in Part III: K is the sextic field of Section 11.2, P_0 is the known point of a curve $\mathcal{C}\colon Y^2 = X^5 + \beta$ over a field L of degree 12 (Lemma 12.3). The symbols $J_\mathcal{C}$ and T_π are defined in Section 12.2, $\Sigma_\mathfrak{P}$ in Proposition 12.6, Λ in Section 13.2, γ_n in Section 13.5, and the quotient curve $\mathcal{D}$ with $J_\mathcal{D}$ and T'_π in Section 15.1. Moreover ℓ_1, ℓ_2 denote linear forms (Section 12.1), not primes, and in Section 11 the letter λ denotes a nonzero number, not an Eisenstein prime.

12. Genus-2 curves and the descent by $1-\zeta$

To a solution we attach a point on a curve $\mathcal{C}\colon Y^2 = X^5+\beta$ over a field L of degree 12 (Lemma 12.3), and we confine it by the descent by $\pi = 1-\zeta$ over $F = L(\zeta)$. A 2-descent on $\mathcal{C}$ would need the class and unit groups of $L(\beta^{1/5})$, of degree 60 [28, §9]. Since $\beta/5$ is a square in L, the kernel of π is generated by a divisor class defined over F, a field of degree 48, and the descent takes values in $F^\times/F^{\times 5}$ (Lemma 12.4).

Throughout, $i' \in \{5,6,16,22,24\}$ is fixed, K is the sextic field of $h_{i'}$, $H = H_{i'}$, and (u_0,v_0) is $(0,1)$ for $i' \in \{5,6,16\}$ and $(1,0)$ for $i' \in \{22,24\}$ (Section 11.6).

12.1. **The curves.** Over K the form $h_{i'}$ is a constant times $(u-\theta_1 v)(u-\theta_2 v)\,H(u,v)$, where θ_1,θ_2 are conjugate over K and $H(t,1)$ is monic of degree 10 in t (Section 11.2). The field $L = K(\theta_1)$ (Table S19) has degree 12 and signature $(4,4)$. We fix a labelling of θ_1,θ_2 and put $\ell_j = \ell_j(u,v) = u-\theta_j v$.

Lemma 12.1. *There are $A,B,C \in L$ with*

$$H(u,v) = A\,\ell_1^{10} + B\,\ell_1^5\ell_2^5 + C\,\ell_2^{10}, \qquad A+B+C = 1, \qquad B^2 = -121\,AC.$$

Consequently $\Delta := B^2-4AC = -125\,AC = 5\,(5B/11)^2$.

Proof. Such a decomposition, with a relation between B^2 and AC, is [28, Remark 2.2], and reflects that $h_{i'}$ is $\mathrm{GL}_2(\mathbb{C})$-equivalent to Klein's form $uv(u^{10}+11u^5v^5-v^{10})$, for which $(A,B,C) = (1,11,-1)$. With $A = H(\theta_2,1)/(\theta_2-\theta_1)^{10}$, $C = H(\theta_1,1)/(\theta_1-\theta_2)^{10}$ and $B = 1-A-C$, a computation in L gives the identity of forms and $B^2 = -121AC$. □

Remark 12.2. In [28, Remark 2.2] the relation is printed as $(B/11)^2 = AC$. The Klein form shows that it is $(B/11)^2 = -AC$.

Let $\alpha := H(u_0,v_0) \in K^\times$ (so $\alpha = 1$ when $(u_0,v_0) = (1,0)$), let d be the positive integer in Table 13, and put

$$\beta := d^{10}(4\alpha A)^4\Delta \in \mathcal{O}_L, \qquad \mathcal{C}\colon\ Y^2 = X^5+\beta.$$

Here d is the least positive integer for which β is integral. As $\Delta/5$ is a square in L, the element $\sqrt{\beta} = d^5(4\alpha A)^2(5B/11)\sqrt{5}$ lies in $M := L(\sqrt{5})$. The curve $\mathcal{C}$ has genus 2 and one point ∞ at infinity.

Lemma 12.3. *Let $(u',v') \in \mathbb{Q}^2 \smallsetminus \{0\}$ satisfy $H(u',v')/\alpha \in (K^\times)^5$, and let $w \in K$ be the fifth root of $H(u',v')/\alpha$ in K. Then ℓ_1,ℓ_2,w are nonzero at (u',v'), and*

$$P_{(u':v')} := \Big(\, d^2(4\alpha A)\,\frac{w}{\ell_2^2}\,,\ d^5(4\alpha A)^2\Big(2A\frac{\ell_1^5}{\ell_2^5}+B\Big)\Big) \tag{12.1}$$

is a point of $\mathcal{C}(L)$ that depends only on $(u':v') \in \mathbb{P}^1(\mathbb{Q})$. The point $P_0 := P_{(u_0:v_0)}$ is the known point.

Proof. The fifth root is unique because K, of degree 6, does not contain ζ. Since $h_{i'}$ is irreducible over $\mathbb{Q}$, neither H nor $\ell_1\ell_2$ vanishes at a rational point of $\mathbb{P}^1$. By Lemma 12.1, $(2A\ell_1^5+B\ell_2^5)^2 = 4A\,H+\Delta\,\ell_2^{10}$, and substituting $H = \alpha w^5$ gives $Y^2 = X^5+\beta$ for the pair (12.1). Multiplying (u',v') by a nonzero rational number multiplies w by its square and ℓ_1, ℓ_2 by the number itself, and leaves (12.1) unchanged. □

By (11.2), a primitive solution coming from h_i and (u,v) with $i \in \mathcal{I}$ gives the *point of the solution* $P := P_{\Psi_i(u:v)} \in \mathcal{C}(L)$ on the curve of i'.

12.2. **The descent by $1-\zeta$.** Let $F := L(\zeta)$. A computation shows $\sqrt{5} \notin L$, so $[F : L] = 4$, F is totally imaginary of degree 48, and $[F : M] = 2$ for $M = L(\sqrt{5})$, where $\sqrt{5} = 2(\zeta+\zeta^4)+1$. The group $\mathrm{Gal}(F/L)$ is generated by $\sigma\colon \zeta \mapsto \zeta^2$, and $\mathrm{Gal}(F/M)$ by $\tau := \sigma^2\colon \zeta \mapsto \zeta^{-1}$.

Push-forward by the automorphism $(X, Y) \mapsto (\zeta X, Y)$ of $\mathcal{C}$ gives an automorphism $[\zeta]$ of $J_\mathcal{C}$, so $J_\mathcal{C}$ is a $\mathbb{Z}[\zeta]$-module over F. The endomorphism $\pi = 1 - \zeta$ is an isogeny of degree $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\pi) = 5$, since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4 = 2 \dim J_\mathcal{C}$. Put $P_\pm = (0, \pm\sqrt{\beta})$ and $T_\pi := [P_+ - \infty] \in J_\mathcal{C}(F)$. The function $Y - \sqrt{\beta}$ has divisor $5P_+ - 5\infty$ and is invariant under the automorphism.

Lemma 12.4. *Let F_* be F or a completion $F_\mathfrak{p}$ of F.*

(a) *$J_\mathcal{C}[\pi]$ has order 5 and is generated by T_π.*

(b) *There is an injective homomorphism $\kappa_{F_*}\colon J_\mathcal{C}(F_*)/\pi J_\mathcal{C}(F_*) \to F_*^\times/F_*^{\times 5}$ with $\kappa_{F_*}([Q - \infty]) = Y(Q) - \sqrt{\beta}$ for every point $Q \in \mathcal{C}(F_*)$ other than P_+ and ∞, and with $\kappa_{F_*}(T_\pi) = (-2\sqrt{\beta})^{-1}$. These maps commute with the maps induced by $F \hookrightarrow F_\mathfrak{p}$.*

(c) *For a prime $\mathfrak{p}$ of F the image $W_\mathfrak{p} := \kappa_{F_\mathfrak{p}}(J_\mathcal{C}(F_\mathfrak{p}))$ has dimension 1 over $\mathbb{F}_5$ if $\mathfrak{p} \nmid 5$, and $1 + [F_\mathfrak{p} : \mathbb{Q}_5]/2$ if $\mathfrak{p} \mid 5$. If $\mathfrak{p} \nmid 5$ and $\mathcal{C}$ has good reduction at $\mathfrak{p}$, then $W_\mathfrak{p}$ consists of the classes of units.*

Proof. The curve $\mathcal{C}$ is the cyclic cover $X^5 = (Y - \sqrt{\beta})(Y + \sqrt{\beta})$ of degree 5 of the Y-line, totally ramified above $Y = \pm\sqrt{\beta}$ and ∞, and 5 does not divide the degree 2 of $Y^2 - \beta$. For such covers Poonen and Schaefer show that $J_\mathcal{C}[1 - \zeta]$ is generated by the classes of differences of ramification points, and that the "$x - T$" map is an injective homomorphism on $J_\mathcal{C}(F_*)/(1 - \zeta)J_\mathcal{C}(F_*)$ [45] (see also [51]). The first statement gives (a), as $[P_- - \infty] = -T_\pi$ (X has divisor $P_+ + P_- - 2\infty$). Here the "$x - T$" map is evaluation of $Y - \sqrt{\beta}$ on divisors, normalized at ∞ by the uniformizer X^2/Y. Its value on $T_\pi = -[P_- - \infty]$ is $(Y(P_-) - \sqrt{\beta})^{-1}$. For (c), $\#J_\mathcal{C}(F_\mathfrak{p})/\pi J_\mathcal{C}(F_\mathfrak{p}) = \#J_\mathcal{C}(F_\mathfrak{p})[\pi] \cdot \|\det d\pi\|_\mathfrak{p}^{-1}$, where $\|\cdot\|_\mathfrak{p}$ is the normalized absolute value of $F_\mathfrak{p}$ and $d\pi$ is the action of π on the tangent space [50, §3]. On the basis $\mathrm{d}X/Y$, $X\,\mathrm{d}X/Y$ of invariant differentials $[\zeta]$ acts by ζ and ζ^2, so $\det d\pi = (1 - \zeta)(1 - \zeta^2)$, of 5-adic valuation 1/2. With $\#J_\mathcal{C}(F_\mathfrak{p})[\pi] = 5$ and the injectivity in (b) this gives the dimensions. The last statement is the usual description of the local image at primes of good reduction not above the degree of the isogeny [50, §3]. □

For a finite set S of primes of F containing the primes above 5 and those at which $\mathcal{C}$ has bad reduction, let $F(S, 5) := \{c \in F^\times/F^{\times 5}\colon v_\mathfrak{p}(c) \equiv 0 \bmod 5 \text{ for } \mathfrak{p} \notin S\}$ and $\mathrm{Sel} := \{c \in F(S, 5)\colon \mathrm{loc}_\mathfrak{p}(c) \in W_\mathfrak{p} \text{ for } \mathfrak{p} \in S\}$, where $\mathrm{loc}_\mathfrak{p}$ is the map to $F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 5}$. Since F has no real places, Lemma 12.4 shows that Sel is the π-Selmer group of $J_\mathcal{C}$ over F, and that $\kappa := \kappa_F$ maps $J_\mathcal{C}(F)/\pi J_\mathcal{C}(F)$ injectively into Sel. For a prime $\mathfrak{p}$ of F we write $\kappa_\mathfrak{p} := \kappa_{F_\mathfrak{p}}$. We take for S the primes of F above 2, 3, 5 and above the rational primes that lie below a prime dividing β. Primes $\mathfrak{p} \nmid 5$ of good reduction in S leave Sel unchanged, as $W_\mathfrak{p}$ is then the set of classes of units, those with valuation divisible by 5 (Lemma 12.4(c)).

We determine Sel through its eigenspaces for $\mathrm{Gal}(F/L)$: those fixed by $\tau = \sigma^2$ come from S-units of L and M, and the dimensions of the other two follow by duality. The next lemma is stated for a general cyclic group G, as it also serves $\mathrm{Gal}(F/M)$ in Section 15.

Let $L_0 \subseteq F$ be a subfield with $F = L_0(\zeta)$ and $G = \mathrm{Gal}(F/L_0)$ cyclic, and let $\omega\colon G \to \mathbb{F}_5^\times$ be the character by which G acts on μ_5. For a character $\chi\colon G \to \mathbb{F}_5^\times$ let $E_\chi \subseteq F^\times/F^{\times 5}$ be the subspace on which $g \in G$ acts as multiplication by $\chi(g)$, let A_χ be the Galois module $\mathbb{F}_5$ on which $\mathrm{Gal}(\bar{\mathbb{Q}}/L_0)$ acts through G by $\omega\chi^{-1}$, and let $\chi^* = \omega\chi^{-1}$. For a place w of L_0 let

i'	forms	d	primes below S	$\#S$	$\dim \mathrm{Sel}_1$	$\dim(\mathrm{Sel}_1 \oplus \mathrm{Sel}_4)$	(δ_2, δ_3)	$\dim \mathrm{Sel}$	(e, f) above 5
22	22	50	$2, 3, 5$	8	4	6	$(-4, -2)$	6	$(20, 2)$, $(4, 2)$
6	$6, 23$	42300	$2, 3, 5, 47$	21	4	8	$(-4, -4)$	8	$(20, 2)$, $(4, 2)$
16	$16, 14$	41425	$2, 3, 5, 1657$	19	2	3	$(-2, -1)$	3	$(20, 2)$, $(4, 2)$
24	24	25	$2, 3, 5$	9	4	7	$(-3, -2)$	9	$(20, 1)^2$, $(4, 1)^2$
5	$5, 13$	57025	$2, 3, 5, 2281$	55	1	4	$(-1, -2)$	5	$(20, 2)$, $(4, 2)$

TABLE 13. The five curves $\mathcal{C}$ and their π-Selmer groups over F. Sel_a is the eigenspace on which σ acts by a, $\delta_2 = \dim \mathrm{Sel}_2 - \dim \mathrm{Sel}_1$, $\delta_3 = \dim \mathrm{Sel}_3 - \dim \mathrm{Sel}_4$ (Lemma 12.5), and the last column gives $(e(\mathfrak{p}), f(\mathfrak{p}))$ for the primes $\mathfrak{p} \mid 5$ of F (exponent 2: two primes).

$E_{\chi,w}$ be the χ-eigenspace of $\bigoplus_{v|w} F_v^\times / F_v^{\times 5}$, with the pairing $\langle x, y\rangle_w = \prod_{v|w} (x_v, y_v)_v$ given by the Hilbert symbols of degree 5 at the places v of F above w.

Lemma 12.5. (a) *$F^\times/F^{\times 5} = \bigoplus_\chi E_\chi$, and E_1 is the image of $L_0^\times/L_0^{\times 5}$, which maps injectively. Restriction induces isomorphisms $H^1(L_0, A_\chi) \to E_\chi$ and $H^1(L_{0,w}, A_\chi) \to E_{\chi,w}$, and $\mathrm{Hom}(A_\chi, \mu_5) \simeq A_{\chi^*}$.*

(b) *The pairing $\langle\,,\rangle_w$ is trivial on $E_{\chi,w} \times E_{\psi,w}$ unless $\chi\psi = \omega$, and it is perfect on $E_{\chi,w} \times E_{\chi^*,w}$, where it is $[F : L_0]$ times the local Tate pairing of $H^1(L_{0,w}, A_\chi) \times H^1(L_{0,w}, A_{\chi^*})$.*

(c) *Let $W_w \subseteq \bigoplus_{v|w} F_v^\times/F_v^{\times 5}$ be G-stable and maximal isotropic for $\langle\,,\rangle_w$. Then $W_w = \bigoplus_\chi W_{\chi,w}$ with $W_{\chi,w} = W_w \cap E_{\chi,w}$, and $W_{\chi^*,w}$ is the annihilator of $W_{\chi,w}$.*

(d) *Let $\mathrm{Sel} \subseteq F^\times/F^{\times 5}$ be cut out by local conditions W_w as in (c) for all places w of L_0, equal to the unramified classes for almost all w, and let $\mathrm{Sel}_\chi = \mathrm{Sel} \cap E_\chi$. Then $\mathrm{Sel} = \bigoplus_\chi \mathrm{Sel}_\chi$, and*

$$\dim \mathrm{Sel}_{\chi^*} - \dim \mathrm{Sel}_\chi = h^0(L_0, A_{\chi^*}) - h^0(L_0, A_\chi) + \sum_w (\dim W_{\chi^*,w} - h^0(L_{0,w}, A_{\chi^*})),$$

where h^0 denotes the dimension of H^0 and the sum runs over all places of L_0.

Proof. (a) The order of G divides 4, so $H^j(G, B) = 0$ for $j \geq 1$ and every $\mathbb{F}_5[G]$-module B. By inflation–restriction $H^1(L_0, A) \to H^1(F, A)^G$ is an isomorphism for every $\mathbb{F}_5$-module A with an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/L_0)$. Over F, A_χ is μ_5, and $g \in G$ acts on $H^1(F, A_\chi) = F^\times/F^{\times 5}$ by $x \mapsto \chi(g)^{-1} g(x)$, with invariants E_χ. For $\chi = 1$ this gives $L_0^\times/L_0^{\times 5} \simeq E_1$, and the same argument over $F \otimes_{L_0} L_{0,w}$ gives the local statement. The decomposition holds as $\mathbb{F}_5[G]$ is split semisimple, $\mathbb{F}_5$ containing the fourth roots of unity. Finally $\mathrm{Hom}(A_\chi, \mu_5)$ is $\mathbb{F}_5$ with the action $\omega \cdot (\omega\chi^{-1})^{-1} = \chi$, and $\omega\chi^{*-1} = \chi$, so it is A_{χ^*}.

(b) Since $(gx, gy)_{gv} = (x, y)_v^{\omega(g)}$, for $x \in E_{\chi,w}$ and $y \in E_{\psi,w}$ we get $\langle x, y\rangle_w^{\chi(g)\psi(g)} = \langle x, y\rangle_w^{\omega(g)}$ for all g, so $\langle x, y\rangle_w = 1$ unless $\chi\psi = \omega$. The pairing on $\bigoplus_{v|w} F_v^\times/F_v^{\times 5}$ is perfect, so its restriction to $E_{\chi,w} \times E_{\chi^*,w}$ is perfect. For $x \in H^1(L_{0,w}, A_\chi)$ and $y \in H^1(L_{0,w}, A_{\chi^*})$ we have $\sum_{v|w} \mathrm{inv}_v(\mathrm{res}\, x \cup \mathrm{res}\, y) = \sum_{v|w} [F_v : L_{0,w}] \,\mathrm{inv}_w(x \cup y) = [F : L_0] \,\mathrm{inv}_w(x \cup y)$.

(c) The decomposition of W_w follows from its G-stability. Isotropy and (b) give $W_{\chi,w} \perp W_{\chi^*,w}$, so $\dim W_{\chi,w} + \dim W_{\chi^*,w} \leq \dim E_{\chi,w}$. Summing over the pairs $\{\chi, \chi^*\}$ gives $\dim W_w \leq \frac{1}{2} \sum_\chi \dim E_{\chi,w}$, with equality by maximality. So equality holds for each pair, and $W_{\chi^*,w}$ is the annihilator of $W_{\chi,w}$.

(d) The decomposition of Sel follows from those of $F^\times/F^{\times 5}$ and of the W_w. By (a) and (c), Sel_χ and Sel_{χ^*} are the Selmer groups of A_χ and $A_{\chi^*} = \mathrm{Hom}(A_\chi, \mu_5)$ for the local conditions

$(W_{\chi,w})_w$ and $(W_{\chi^*,w})_w$. By (b), these are exact annihilators of each other under the local Tate pairing, since $[F : L_0]$ is prime to 5. The displayed formula is the Greenberg–Wiles formula [18, Theorem 2.19], which holds over any number field. □

We apply the lemma with $L_0 = L$ and $G = \langle\sigma\rangle$. Then $\omega(\sigma) = 2$, and we write E_a, Sel_a for the eigenspaces with $\chi(\sigma) = a$. So E_1 is paired with E_2 and E_4 with E_3, and $E_1 \oplus E_4$, the part fixed by $\tau = \sigma^2$, is the image of $M^\times/M^{\times 5}$. The local conditions of Sel satisfy the hypotheses of Lemma 12.5(c), (d). They are G-stable because $\sigma(\sqrt{\beta}) = -\sqrt{\beta}$: for a point Q of $\mathcal{C}$ over $F_\mathfrak{p}$ we have $Y(\sigma Q) - \sqrt{\beta} = \sigma(Y(Q) + \sqrt{\beta}) = \sigma(X(Q)^5/(Y(Q) - \sqrt{\beta}))$, so $\kappa(\sigma Q) = -\sigma(\kappa(Q))$ and $\sigma(W_\mathfrak{p}) = W_{\sigma\mathfrak{p}}$. They are maximal isotropic: with respect to the principal polarization the dual isogeny of π is $1 - \zeta^{-1} = -\zeta^{-1}\pi$, which has the same kernel and the same local images. So by Tate local duality $W_\mathfrak{p}$ is its own annihilator under the pairing induced by the Weil pairing on $J_\mathcal{C}[\pi]$, which is a nonzero multiple of the Hilbert pairing, and $\dim W_\mathfrak{p}$ is half of $\dim F_\mathfrak{p}^\times/F_\mathfrak{p}^{\times 5}$ by Lemma 12.4(c). At the primes outside S they are the unramified classes, and F has no real places.

Proposition 12.6. *Let $i' \in \{5, 6, 16, 22, 24\}$.*

(a) *The eigenspaces of* Sel *and its dimension are as in Table 13, and* Sel *is spanned by the classes of* $\dim$ Sel *explicit S-units of F.*

(b) *The classes $\kappa(P_0 - \infty)$ and $\kappa(T_\pi)$ are independent elements of* Sel.

(c) *The primes of F above 5 with ramification index 20 are one prime $\mathfrak{P}$ with $f(\mathfrak{P}) = 2$ if $i' \neq 24$, and two primes $\mathfrak{P}_1, \mathfrak{P}_2$ with $f = 1$, exchanged by σ, if $i' = 24$. At each of them $\kappa_\mathfrak{P}(T_\pi) \neq 0$.*

(d) *The map* $\mathrm{loc}_\mathfrak{P}\colon \mathrm{Sel} \to W_\mathfrak{P}$ *is injective if $i' \neq 24$, and* $\mathrm{loc}_{\mathfrak{P}_1} \times \mathrm{loc}_{\mathfrak{P}_2}\colon \mathrm{Sel} \to W_{\mathfrak{P}_1} \times W_{\mathfrak{P}_2}$ *is injective if $i' = 24$.*

Proof. The local images $W_\mathfrak{p}$, $\mathfrak{p} \in S$, are the spans of the classes of explicit points of $\mathcal{C}(F_\mathfrak{p})$, since these spans reach the dimension of Lemma 12.4(c).

The class groups of L and of M have order 1 or 2 (Proposition A.13). Let S_L and S_M be the sets of primes of L and M below those in S. The ramification indices of F/L are prime to 5, so $E_1 \cap F(S, 5)$ is the image of $L(S_L, 5)$, defined like $F(S, 5)$, and similarly $(E_1 \oplus E_4) \cap F(S, 5)$ is the image of $M(S_M, 5)$. Since the class numbers are prime to 5, $L(S_L, 5) = \mathcal{O}^\times_{L,S_L}/\mathcal{O}^{\times 5}_{L,S_L}$ and $M(S_M, 5) = \mathcal{O}^\times_{M,S_M}/\mathcal{O}^{\times 5}_{M,S_M}$, of dimensions $r_1 + r_2 - 1 + \#S_L$ and $r_1 + r_2 - 1 + \#S_M$, as L and M have real places, so that their only roots of unity are ± 1. For each we have that many explicit elements, S-units by their ideal factorizations and independent modulo fifth powers by their fifth-power residue characters at primes of small norm, hence a basis. With these bases, Sel_1 and $\mathrm{Sel}_1 \oplus \mathrm{Sel}_4$ are kernels of explicit linear maps over $\mathbb{F}_5$, and their dimensions are those of Table 13 (Appendix B). Lemma 12.5(d), evaluated with the local images, gives δ_2 and δ_3 (Table 13), hence $\dim \mathrm{Sel}_2$, $\dim \mathrm{Sel}_3$ and $\dim$ Sel.

There are $\dim$ Sel explicit S-units of F [32] whose classes satisfy all the local conditions and are independent in $F^\times/F^{\times 5}$ by fifth-power residue symbols, so they span Sel. The description of the primes above 5 in (c) is the decomposition of 5 in F (Table 13), and the rest of (b)–(d) is linear algebra over $\mathbb{F}_5$ on these classes. At the primes with $e = 20$, a basis of $\Sigma_\mathfrak{P} := \mathrm{loc}_\mathfrak{P}(\mathrm{Sel})$ is printed in Section S6. □

12.3. **The descent class of the point of a solution.** The descent class of the point of a solution is the value of an explicit binary quintic form in (u, v), which allows a sieve over $\mathbb{P}^1(\mathbb{Q}_p)$.

Lemma 12.7. *Let* $\sqrt{\Delta} := (5B/11)\sqrt{5}$ *and* $\rho := (\sqrt{\Delta}-B)/(2A) \in M$*, a root of* Az^2+Bz+C*. For* (u', v') *as in Lemma 12.3,*

$$\kappa(P_{(u':v')} - \infty) = \Phi(u', v') := \textit{the class of } 32\,\alpha^2 A^3(\ell_1^5 - \rho\,\ell_2^5) \textit{ in } F^\times/F^{\times 5}.$$

The same formula gives $\kappa_{F_\mathfrak{p}}(Q-\infty)$ *for the point* $Q \in \mathcal{C}(F_\mathfrak{p})$ *defined by (12.1) from* $(u', v') \in F_\mathfrak{p}^2$ *and any* $w \in F_\mathfrak{p}^\times$ *with* $w^5 = H(u', v')/\alpha$*.*

Proof. We have $Y - \sqrt{\beta} = d^5(4\alpha A)^2(2A\ell_1^5/\ell_2^5 + B - \sqrt{\Delta}) = d^5(4\alpha A)^2 \cdot 2A\,(\ell_1^5 - \rho\ell_2^5)/\ell_2^5$, and d^5, ℓ_2^5 are fifth powers. □

The form $\ell_1^5 - \rho\ell_2^5$ is homogeneous of degree 5, so Φ is a function on $\mathbb{P}^1$. Its class at a prime $\mathfrak{p} \mid p$ is locally constant on $\mathbb{P}^1(\mathbb{Q}_p)$ away from the zeros of $\ell_1^5 - \rho\ell_2^5$, and is computed on residue classes as follows. Let $k_\mathfrak{p} = \lfloor 5e(\mathfrak{p})/4 \rfloor + 1$ if $\mathfrak{p} \mid 5$ and $k_\mathfrak{p} = 1$ otherwise. Then $1 + \mathfrak{p}^{k_\mathfrak{p}}\mathcal{O}_\mathfrak{p} \subseteq F_\mathfrak{p}^{\times 5}$ (for $\mathfrak{p} \mid 5$ by Lemma 13.5). On a residue class $\{(t_0 + p^k U : 1) : U \in \mathbb{Z}_p\}$ (and similarly on $\{(1 : t_0 + p^k U)\}$), with $t_0 \in \mathbb{Z}$, expand Φ at t_0 as

$$\Phi(t_0 + p^k U) = \sum_{n=0}^{5} \varphi_n\,(p^k U)^n,$$

where $\varphi_n \in F$ is the n-th Taylor coefficient of Φ at t_0, so that $\varphi_0 = \Phi(t_0)$. If $v_\mathfrak{p}(\varphi_n) + nk\,e(\mathfrak{p}) \geq v_\mathfrak{p}(\varphi_0) + k_\mathfrak{p}$ for $1 \leq n \leq 5$ (the *constancy criterion* at $\mathfrak{p}$), then $\Phi/\varphi_0 \in 1 + \mathfrak{p}^{k_\mathfrak{p}}\mathcal{O}_\mathfrak{p}$ on the residue class, so Φ has the class of φ_0 at $\mathfrak{p}$ there.

12.4. **The sieve.** For a primitive solution from h_i and (u, v), $i \in \mathcal{I}$, with point $P = P_{\Psi_i(u:v)}$, the class $\kappa(P - \infty) = \Phi(\Psi_i(u, v))$ lies in Sel, and its local classes above p are those of $\Phi \circ \Psi_i$ at some $(u : v) \in \mathbb{P}^1(\mathbb{Q}_p)$, in the classes of Table 12 for $p = 2, 3$. We use $p = 2$ and 3, where condition (a) restricts $(u : v)$; $p = 5$, where the local groups are largest (Lemma 12.4(c)); and, for h_{24}, the six smallest primes $p \geq 11$ above which F has at least four primes, namely 11, 13, 17, 19, 23 and 29 (other sets also suffice, for instance 11, 31 and 41).

For each p used we compute the set $\mathcal{L}_p$ of these vectors of local classes above p. We split $\mathbb{P}^1(\mathbb{Z}_p)$ into residue classes, and each class into its p subclasses, until the constancy criterion holds at every prime of F above p. Near a p-adic zero of $\ell_1^5 - \rho\ell_2^5$ in one of the completions this never happens, so we stop at residue classes modulo p^{30}. A residue class modulo p^{30} on which the criterion holds only at some of the primes above p contributes the classes at those primes and no condition at the others. This can only enlarge $\mathcal{L}_p$, so the test is valid for any stopping depth, and the depth 30 suffices for Proposition 12.8. For $i' = 24$ it leaves ten undecided residue classes at $p = 5$ and two at each of $p = 11$ and $p = 23$. Finally we keep the elements of Sel whose local vectors lie in $\mathcal{L}_p$ for every p used.

Proposition 12.8. *For every* $i \in \mathcal{I}$*, exactly one element of* Sel *(for the curve attached to* i'*) passes the local tests at the primes listed below, namely* $\kappa(P_0 - \infty)$*. The primes are:* 5 *alone for* $i \in \{5, 13, 6, 23, 16, 14\}$*;* 2, 3, 5 *for* $i = 22$*; and* 2, 3, 5, 11, 13, 17, 19, 23, 29 *for* $i = 24$*. Consequently, for a solution as above,* $\kappa(P - \infty) = \kappa(P_0 - \infty)$*, that is,* $[P - P_0] \in \pi J_\mathcal{C}(F)$*.*

Proof. The elements passing the tests were found by enumerating all $5^{\dim \mathrm{Sel}}$ elements, 3125, 390625, 125, 15625 and 1953125 for $i' = 5$, 6, 16, 22, 24 (Appendix B). For the paired forms the 5-adic test is the same as for the partner, since Ψ_i permutes $\mathbb{P}^1(\mathbb{Q}_5)$ (Lemma 11.8) and the test at 5 uses all of $\mathbb{P}^1(\mathbb{Z}_5)$. The last statement holds as $\kappa(P - \infty)$ passes every test and κ is injective. □

Proposition 12.9. *Let $\mathcal{R}$ be the set of $(u':v')\in\mathbb{P}^1(\mathbb{Q}_5)$ at which the local classes of Φ at all primes of F above 5 equal those of $\kappa(P_0-\infty)$. Write $(u':v')=(t:1)$ if $i'\in\{5,6,16\}$ and $(u':v')=(1:t)$ if $i'\in\{22,24\}$, so that the known point has $t=0$. Then $\mathcal{R}=\{t\in 25\mathbb{Z}_5\}$ for $i'\in\{5,6,16,24\}$ and $\mathcal{R}=\{t\in 5\mathbb{Z}_5\}$ for $i'=22$. Moreover the constancy criterion holds on $\mathcal{R}$ (on each of the five classes $t\in 5j+25\mathbb{Z}_5$, $0\le j\le 4$, for $i'=22$), so that $\kappa_{\mathfrak{p}}(P_t-P_0)=0$ for every point $P_t\in\mathcal{C}(F_{\mathfrak{p}})$ defined by (12.1) with $t\in\mathcal{R}$, at every prime $\mathfrak{p}\mid 5$.*

Proof. This is part of the computation at $p=5$ for Proposition 12.8. For $i'\in\{5,6,16,22\}$ the refinement of $\mathbb{P}^1(\mathbb{Z}_5)$ ends with 30 residue classes, on each of which the criterion holds at both primes of F above 5. Those on which the local classes of Φ equal those of $\kappa(P_0-\infty)$ make up $\mathcal{R}$: the class $t\in 25\mathbb{Z}_5$, and for $i'=22$ the five classes $t\in 5j+25\mathbb{Z}_5$. For $i'=24$ the refinement ends with 1150 residue classes. On all but ten of them the criterion holds at the four primes of F above 5, and among these only the class $t\in 25\mathbb{Z}_5$ carries the local classes of $\kappa(P_0-\infty)$. The remaining ten are residue classes modulo 5^{30} of points $(a:1)$ with $a\in\mathbb{Z}_5$. They contain no point of $\mathcal{R}$, since on each of them the criterion holds at three of the four primes, and at the prime with $e=20$ among these the class differs from that of $\kappa(P_0-\infty)$. □

By Propositions 12.8 and 12.9 and Lemma 11.8, the point P of a solution coming from h_i has parameter $t\in\mathcal{R}$. For the paired forms, $t\in 25\mathbb{Z}_5$ means $u/v\in 25\mathbb{Z}_5$ for $i=23$ and $i=13$, and $(u+v)/(u-v)\in 25\mathbb{Z}_5$ for $i=14$.

13. The 5-adic argument

The 5-adic tools of this section decide the disc left by the sieve of Section 12, for the curves $\mathcal{C}$ and for the curves $\mathcal{D}$ of Section 15.

13.1. **Stoll's criterion for the descent by $\boldsymbol{\pi}$.** Throughout this section $\mathcal{X}\colon Y^2=X^5+\beta_0$ is a curve over a subfield of F with $\beta_0\in F^\times$ and $\sqrt{\beta_0}\in F$, namely a curve $\mathcal{C}$ or $\mathcal{D}$. Lemma 12.4 and its proof apply to $\mathcal{X}$, and we use its notation: $J_{\mathcal{X}}$ is the Jacobian, $T_\pi=[(0,\sqrt{\beta_0})-\infty]$ generates $J_{\mathcal{X}}[\pi]$, κ, $\kappa_{\mathfrak{p}}$ are the descent maps, $W_{\mathfrak{p}}$ the local images, and Sel is the π-Selmer group over F (Proposition 12.6, or Proposition 15.2 for $\mathcal{D}$). For a set $\mathcal{P}$ of primes of F above 5, $\mathrm{loc}_{\mathcal{P}}$ is the product of the maps $\mathrm{loc}_{\mathfrak{p}}$, $\mathfrak{p}\in\mathcal{P}$, and $\Sigma_{\mathcal{P}}:=\mathrm{loc}_{\mathcal{P}}(\mathrm{Sel})$.

We apply Proposition 5.1 to $J_{\mathcal{X}}$ over F with $\ell=5$ and $\varpi=\pi$ (Section 5.1), $\mathcal{H}=F^\times/F^{\times 5}$, $\delta=\kappa$, $\delta_{\mathcal{P}}=\kappa_{\mathcal{P}}=\prod_{\mathfrak{p}\in\mathcal{P}}\kappa_{\mathfrak{p}}$, $\Gamma=J_{\mathcal{X}}[\pi]=\langle T_\pi\rangle$ and $\iota(Q)=[Q-Q_0]$ for a point $Q_0\in\mathcal{X}(F)$. We use the primes $\mathfrak{P}$ with $e(\mathfrak{P})=20$, where $J_{\mathcal{X}}(F_{\mathfrak{P}})/\pi J_{\mathcal{X}}(F_{\mathfrak{P}})$ is largest (Lemma 12.4(c)).

13.2. **The lattice and the level.** Proposition 5.1 needs the classes of the local points R with $\pi^n R=D$, which we compute from the coordinates of $\log D$ in a basis of the logarithm lattice. Let $\mathfrak{P}$ be a prime of F above 5 with $\kappa_{\mathfrak{P}}(T_\pi)\ne 0$. Put $r:=[F_{\mathfrak{P}}:\mathbb{Q}_5]/2$, so that $\dim W_{\mathfrak{P}}=r+1$ (Lemma 12.4(c)). Let $\omega_0=\mathrm{d}X/Y$, $\omega_1=X\,\mathrm{d}X/Y$, and let

$$\log\colon J_{\mathcal{X}}(F_{\mathfrak{P}})\to F_{\mathfrak{P}}^2,\qquad D\mapsto\Big(\int_0^D\omega_0,\int_0^D\omega_1\Big)$$

be the logarithm of the 5-adic Lie group $J_{\mathcal{X}}(F_{\mathfrak{P}})$ for the invariant differentials attached to ω_0, ω_1. It is a homomorphism with kernel the torsion subgroup, and its image $\Lambda:=\log J_{\mathcal{X}}(F_{\mathfrak{P}})$ is a $\mathbb{Z}_5$-lattice of rank $4r$ in $F_{\mathfrak{P}}^2$. Pulling back ω_0 and ω_1 by $(X,Y)\mapsto(\zeta X,Y)$ multiplies them by ζ and ζ^2, so $\log([\zeta]D)=\zeta\cdot\log D$, where $\mathbb{Z}_5[\zeta]$ acts on $F_{\mathfrak{P}}^2$ through $\zeta\mapsto\mathrm{diag}(\zeta,\zeta^2)$. Since $1-\zeta^2=(1-\zeta)(1+\zeta)$ with $1+\zeta$ a unit, $\pi^j\mathcal{O}_{\mathfrak{P}}^2=(1-\zeta)^j\mathcal{O}_{\mathfrak{P}}^2$ for every $j\in\mathbb{Z}$.

The *level* of $D \in J_{\mathcal{X}}(F_{\mathfrak{P}})$ is that of Section 5.1 with $\varpi = \pi$ and $W = 0$, namely $\operatorname{lev}(D) \coloneqq \sup\{n \geq 0 \colon D \in \pi^n J_{\mathcal{X}}(F_{\mathfrak{P}})\}$.

Lemma 13.1. *Let $G_1, \dots, G_r \in J_{\mathcal{X}}(F_{\mathfrak{P}})$ be such that $\kappa_{\mathfrak{P}}(G_1), \dots, \kappa_{\mathfrak{P}}(G_r), \kappa_{\mathfrak{P}}(T_\pi)$ form a basis of $W_{\mathfrak{P}}$.*

(a) *The 5-primary torsion of $J_{\mathcal{X}}(F_{\mathfrak{P}})$ is $\langle T_\pi \rangle$, and every torsion point of $J_{\mathcal{X}}(F_{\mathfrak{P}})$ has level 0 or ∞.*

(b) *$\log G_1, \dots, \log G_r$ form a $\mathbb{Z}_5[\zeta]$-basis of Λ.*

(c) *Let $D \in J_{\mathcal{X}}(F_{\mathfrak{P}})$ with $\kappa_{\mathfrak{P}}(D) = 0$, and write $\log D = \sum_k a_k \log G_k$ with $a_k \in \mathbb{Z}_5[\zeta]$. Then $\operatorname{lev}(D) = \min_k v_\pi(a_k)$. If $\nu \coloneqq \operatorname{lev}(D)$ is finite, there is $R \in J_{\mathcal{X}}(F_{\mathfrak{P}})$ with $\pi^\nu R = D$ and*

$$\kappa_{\mathfrak{P}}(R) = \sum_k \overline{\pi^{-\nu} a_k}\, \kappa_{\mathfrak{P}}(G_k) \notin \mathbb{F}_5 \kappa_{\mathfrak{P}}(T_\pi).$$

The class $\operatorname{cl}(D)$ of $\kappa_{\mathfrak{P}}(R)$ in $W_{\mathfrak{P}}/\mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$ is nonzero and independent of the choices, and $\mathcal{Q}(D) \subseteq (\kappa_{\mathfrak{P}}(R) + \mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)) \cup \mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$, with $\mathcal{Q}$ as in Proposition 5.1 for $\mathcal{P} = \{\mathfrak{P}\}$.

Proof. Let $\mathfrak{M}$ be the quotient of $J_{\mathcal{X}}(F_{\mathfrak{P}})$ by its torsion of order prime to 5, a finitely generated $\mathbb{Z}_5[\zeta]$-module. Points of order prime to 5 are divisible by 5, which is π^4 times a unit, so $\mathfrak{M}/\pi\mathfrak{M} = J_{\mathcal{X}}(F_{\mathfrak{P}})/\pi J_{\mathcal{X}}(F_{\mathfrak{P}})$, which $\kappa_{\mathfrak{P}}$ maps isomorphically onto $W_{\mathfrak{P}}$. The torsion submodule $\mathfrak{M}_{\mathrm{tors}}$ is the 5-primary torsion of $J_{\mathcal{X}}(F_{\mathfrak{P}})$, and its π-torsion lies in $J_{\mathcal{X}}[\pi] = \langle T_\pi \rangle$, of order 5. So $\mathfrak{M}_{\mathrm{tors}} \simeq \mathbb{Z}_5[\zeta]/\pi^j$, with T_π generating $\pi^{j-1}\mathfrak{M}_{\mathrm{tors}}$, and $j = 1$, since otherwise $T_\pi \in \pi\mathfrak{M}$ and $\kappa_{\mathfrak{P}}(T_\pi) = 0$. A torsion point is cT_π plus a point of order prime to 5, so it has image $c\,\kappa_{\mathfrak{P}}(T_\pi) \neq 0$ if $c \neq 0$, and lies in every $\pi^n J_{\mathcal{X}}(F_{\mathfrak{P}})$ otherwise. This proves (a).

Now $\mathfrak{M} \simeq \mathbb{Z}_5[\zeta]^{r'} \oplus \langle T_\pi \rangle$ with $r' + 1 = \dim \mathfrak{M}/\pi\mathfrak{M} = r + 1$. By Nakayama's lemma $G_1, \dots, G_r, T_\pi$ generate $\mathfrak{M}$, so the $\log G_k$ generate Λ, which is free of rank r over $\mathbb{Z}_5[\zeta]$. This is (b).

For (c), $D - \sum_k a_k G_k$ lies in the kernel of log, so $D = \sum a_k G_k + cT_\pi$ in $\mathfrak{M}$ with $c \in \mathbb{F}_5$. The map $\kappa_{\mathfrak{P}}$ vanishes on $\pi J_{\mathcal{X}}(F_{\mathfrak{P}})$, so $\kappa_{\mathfrak{P}}(aG) = \bar{a}\,\kappa_{\mathfrak{P}}(G)$ for $a \in \mathbb{Z}_5[\zeta]$. Applying $\kappa_{\mathfrak{P}}$ gives $0 = \sum \bar{a}_k \kappa_{\mathfrak{P}}(G_k) + c\,\kappa_{\mathfrak{P}}(T_\pi)$, so all $\bar{a}_k$ and c are 0. Since $\mathfrak{M} = \bigoplus_k \mathbb{Z}_5[\zeta] G_k \oplus \langle T_\pi \rangle$ and $\pi^n\mathfrak{M} = \bigoplus_k \pi^n \mathbb{Z}_5[\zeta] G_k$ for $n \geq 1$, we get $D \in \pi^n\mathfrak{M}$ if and only if $v_\pi(a_k) \geq n$ for all k, which gives the formula for $\operatorname{lev}(D)$. If ν is finite, $R_1 \coloneqq \sum \pi^{-\nu} a_k G_k$ satisfies $\pi^\nu R_1 = D + t$ with t of order prime to 5. Writing $t = \pi^\nu t'$ with t' of order prime to 5, the point $R = R_1 - t'$ satisfies $\pi^\nu R = D$ and $\kappa_{\mathfrak{P}}(R) = \kappa_{\mathfrak{P}}(R_1)$, as displayed. Some $\overline{\pi^{-\nu} a_k}$ is nonzero, so $\kappa_{\mathfrak{P}}(R) \notin \mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$. If $\pi^n R' = D$, then $n \leq \nu$, and if $n = \nu$, then $R' - R \in J_{\mathcal{X}}(F_{\mathfrak{P}})[\pi^\nu] = \langle T_\pi \rangle$ by (a), so $\kappa_{\mathfrak{P}}(R') \in \kappa_{\mathfrak{P}}(R) + \mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$. If $n < \nu$, then $R' - \pi^{\nu-n} R \in \langle T_\pi \rangle$, so $\kappa_{\mathfrak{P}}(R') \in \mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$. This proves the independence of the choices and the description of $\mathcal{Q}(D)$. □

We extend lev and cl to $F_{\mathfrak{P}}^2 = \Lambda \otimes \mathbb{Q}$. For $\gamma = \sum a_k \log G_k$ with $a_k \in \mathbb{Q}_5(\zeta)$ put $\operatorname{lev}(\gamma) = \min_k v_\pi(a_k)$, and if $\operatorname{lev}(\gamma) = \nu$ let $\operatorname{cl}_\nu(\gamma)$ be the class of $\sum \overline{\pi^{-\nu} a_k}\, \kappa_{\mathfrak{P}}(G_k)$ modulo $\mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$. Then $\operatorname{lev}(\gamma + \gamma') \geq \min(\operatorname{lev}\gamma, \operatorname{lev}\gamma')$, with $\operatorname{cl}_\nu(\gamma + \gamma') = \operatorname{cl}_\nu(\gamma)$ if $\operatorname{lev}(\gamma') > \operatorname{lev}(\gamma) = \nu$. Moreover $\operatorname{lev}(5^m s_0 \gamma) = \operatorname{lev}(\gamma) + 4m$ and $\operatorname{cl}_{\nu+4m}(5^m s_0 \gamma) = \overline{(-1)^m s_0}\, \operatorname{cl}_\nu(\gamma)$ for $s_0 \in \mathbb{Z}_5^\times$, because $5 \equiv -\pi^4 \bmod \pi^5$, as $5 = \prod_{a=1}^4 (1 - \zeta^a) = \pi^4 \prod_{a=1}^4 (1 + \zeta + \cdots + \zeta^{a-1})$ and $\prod_{a=1}^4 a = 24 \equiv -1 \bmod 5$.

Lemma 13.2. *Suppose $e(\mathfrak{P}) = 20$ and $\pi^N \mathcal{O}_{\mathfrak{P}}^2 \subseteq \Lambda$ for an integer $N \geq 0$. Then $\operatorname{lev}(\gamma) \geq \lfloor v_{\mathfrak{P}}(\gamma)/5 \rfloor - N$ for every $\gamma \in F_{\mathfrak{P}}^2$, where $v_{\mathfrak{P}}(\gamma)$ is the smaller of the valuations of the two coordinates.*

Proof. We have $v_{\mathfrak{P}}(\pi) = e(\mathfrak{P})/4 = 5$, so $\gamma \in \pi^{\lfloor v_{\mathfrak{P}}(\gamma)/5 \rfloor} \mathcal{O}_{\mathfrak{P}}^2 \subseteq \pi^{\lfloor v_{\mathfrak{P}}(\gamma)/5 \rfloor - N} \Lambda$. □

For every lattice Λ that we use at a prime with $e = 20$, the inverse of a basis matrix of Λ has entries of valuation at least -1 (Appendix B), so $5\mathcal{O}_{\mathfrak{P}}^2 = \pi^4\mathcal{O}_{\mathfrak{P}}^2 \subseteq \Lambda$ and Lemma 13.2 holds with $N = 4$. In one case we use the stronger inclusion with $N = 1$ (Proposition 15.5).

13.3. **The logarithm.**

Lemma 13.3. *Let F' be a finite extension of $F_{\mathfrak{P}}$ with valuation $v_{F'}$, let $\mathbb{B} = \{s\colon v_{F'}(s) \geq m_0\}$ be a closed disc over F', and let $s \mapsto Q_s = (X(s), Y(s))$ be given by power series converging on $\mathbb{B}$, with $Y(s)^2 = X(s)^5 + \beta_0$ and $Y(s) \neq 0$ on $\mathbb{B}$. Then, for $s, s' \in \mathbb{B}$ (with coordinates in finite extensions of F'),*

$$\log[Q_s - Q_{s'}] = \int_{s'}^{s} \Big(\frac{X'(s_1)}{Y(s_1)}, \frac{X(s_1)X'(s_1)}{Y(s_1)}\Big)\mathrm{d}s_1,$$

the termwise integral of the power series.

Proof. This is the usual justification of tiny integrals (compare [16]). The Jacobian has complex multiplication by $\mathbb{Z}[\zeta]$, so it has potentially good reduction [54]. Let $F'' \supseteq F'$ be a finite extension over which it has good reduction, with abelian scheme $\mathcal{J}$ over $\mathcal{O}_{F''}$. The rigid analytic map $s \mapsto [Q_s - Q_{s'}]$ from $\mathbb{B}$ to $J_{\mathcal{X}}^{\mathrm{an}}$ extends, after an admissible blowing-up of the formal model of $\mathbb{B}$, to a morphism of formal models into the formal completion of $\mathcal{J}$ [7]. After a finite extension of F'' the model of $\mathbb{B}$ has reduced, hence geometrically reduced, special fibre [8, Theorem 2.1], and we may pass to the completion of an algebraic closure. The preimage in $\mathbb{B}$ of a dense open affine part of a component of the special fibre is then a connected affinoid subdomain of the disc with irreducible canonical reduction, so a closed disc with finitely many open discs of the same radius removed [29, Chapter 2, pp. 13–43]. Its canonical reduction, birational to the component, is the affine line minus finitely many points. So the special fibre is a connected curve with rational components, each mapped to a point, since morphisms from rational curves to abelian varieties are constant. As s' maps to 0, the image of $\mathbb{B}$ lies in the residue polydisc of 0, on which log is the formal logarithm, given by convergent power series in formal coordinates. Hence $s \mapsto \log[Q_s - Q_{s'}]$ is a power series converging on $\mathbb{B}$, with derivative the pull-back of (ω_0, ω_1) and value 0 at s', and such a power series is determined by its derivative and one value. □

For the points used to build lattices we use a closed formula. Let

$$\mathscr{F}_1(\chi) = \sum_{n\geq 0} \mathfrak{a}_n\chi^n, \quad \mathscr{F}_2(\chi) = \sum_{n\geq 0} \mathfrak{a}'_n\chi^n, \qquad \mathfrak{a}_n = \frac{(1/2)_n}{(6/5)_n}, \quad \mathfrak{a}'_n = \frac{(1/2)_n}{(7/5)_n},$$

be the hypergeometric series ${}_2F_1(\frac{1}{2}, 1; \frac{6}{5}; \chi)$ and ${}_2F_1(\frac{1}{2}, 1; \frac{7}{5}; \chi)$, where $(\,\cdot\,)_n$ is the rising factorial, for instance $(1/2)_n = \prod_{j=0}^{n-1}(\frac{1}{2} + j)$.

Lemma 13.4. *Let F' be a finite extension of $\mathbb{Q}_5$, let $\beta_0 \in F'^{\times}$, and let $Q = (X_Q, Y_Q)$ be a point of $Y^2 = X^5 + \beta_0$ over F' with $Y_Q \neq 0$ and $\chi(Q) \coloneqq X_Q^5/Y_Q^2$ satisfying $v_5(\chi(Q)) > -1$. Then*

$$\log[Q - \infty] = \Big(\frac{X_Q}{Y_Q}\,\mathscr{F}_1(\chi(Q)),\ \frac{X_Q^2}{2Y_Q}\,\mathscr{F}_2(\chi(Q))\Big).$$

Moreover $v_5(\mathfrak{a}_n) \geq n$ and $v_5(\mathfrak{a}'_n) \geq n$, so truncating the two series after the terms of degree n_1 changes the two coordinates by elements of 5-adic valuation at least $(n_1 + 1)(1 + v_5(\chi(Q))) + v_5(X_Q/Y_Q)$, respectively $(n_1 + 1)(1 + v_5(\chi(Q))) + v_5(X_Q^2/2Y_Q)$.

Proof. The recursions $(5n+1)\mathfrak{a}_n = \frac{5}{2}(2n-1)\mathfrak{a}_{n-1}$ and $(5n+2)\mathfrak{a}'_n = \frac{5}{2}(2n-1)\mathfrak{a}'_{n-1}$, with $5n+1$, $5n+2$ prime to 5, show that $v_5(\mathfrak{a}_n) = v_5(\mathfrak{a}'_n) = n + v_5(1\cdot 3\cdots(2n-1)) \geq n$. This gives convergence for $v_5(\chi) > -1$ and the truncation bounds. On the curve, $\mathrm{d}\chi/\mathrm{d}X = 5\chi(1-\chi)/X$, $\mathrm{d}(X/Y)/\mathrm{d}X = (1-\frac{5}{2}\chi)/Y$ and $\mathrm{d}(X^2/2Y)/\mathrm{d}X = (X/Y)(1-\frac{5}{4}\chi)$. The recursions are equivalent to $(1-\frac{5}{2}\chi)\mathscr{F}_1 + 5\chi(1-\chi)\mathscr{F}'_1 = 1$ and $(1-\frac{5}{4}\chi)\mathscr{F}_2 + \frac{5}{2}\chi(1-\chi)\mathscr{F}'_2 = 1$, which give

$$\frac{\mathrm{d}}{\mathrm{d}X}\Big(\frac{X}{Y}\mathscr{F}_1(\chi)\Big) = \frac{1}{Y}, \qquad \frac{\mathrm{d}}{\mathrm{d}X}\Big(\frac{X^2}{2Y}\mathscr{F}_2(\chi)\Big) = \frac{X}{Y}.$$

For the constant of integration, over a finite extension containing a fifth root $\beta_0^{1/5}$ and $\sqrt{\beta_0}$, write $X = \beta_0^{1/5}\tilde{X}$ and $Y = \sqrt{\beta_0}\,\tilde{Y}$, so that $\tilde{Y}^2 = \tilde{X}^5 + 1$ and $\chi = \tilde{X}^5/(\tilde{X}^5+1)$. If $v_5(\tilde{X}) \neq 0$, then $v_5(\chi) \geq 0$. If $v_5(\tilde{X}) = 0$, then $\tilde{X}^5+1 = (\tilde{X}+1)^5 - 5(\tilde{X}+1)^4 + 10(\tilde{X}+1)^3 - 10(\tilde{X}+1)^2 + 5(\tilde{X}+1)$, so $v_5(\chi) > -1$ if and only if $v_5(\tilde{X}+1) < 1/5$. Hence $\{v_5(\chi) > -1\}$ is the preimage on the curve of $\mathcal{V} = \mathbb{P}^1 \smallsetminus \{\tilde{X} \colon v_5(\tilde{X}+1) \geq 1/5\}$, an open disc around $\tilde{X} = \infty$ that contains none of the five roots of $\tilde{X}^5 = -1$ (they satisfy $v_5(\tilde{X}+1) \geq 1/4$). With $\Theta = 1/(\tilde{X}+1)$, so that $\mathcal{V} = \{v_5(\Theta) > -1/5\}$, we get $(\tilde{Y}\Theta^3)^2 = \Theta\,(1 - 5\Theta + 10\Theta^2 - 10\Theta^3 + 5\Theta^4)$, and on $\mathcal{V}$ the second factor is 1 plus terms of positive valuation, so it has an analytic square root. So the preimage of $\mathcal{V}$ is an open disc with parameter $\sqrt{\Theta}$, containing ∞ at $\sqrt{\Theta} = 0$, on which X/Y, X^2/Y, χ are analytic. The first two vanish at ∞, so the right-hand side of the formula is analytic on this disc, vanishes at ∞ and has differential (ω_0, ω_1). By Lemma 13.3, applied to a closed subdisc containing ∞ and Q (its proof applies to any analytic map from a closed disc to the curve), it equals $\log[Q - \infty]$. □

Every point to which we apply Lemma 13.4 satisfies $v_5(\chi(Q)) \geq -2/5$. For a divisor $Q + \bar{Q}$ with Q defined over a quadratic extension F'' of $F' = F_{\mathfrak{P}}$ and $\bar{Q}$ its conjugate, $\log[Q + \bar{Q} - 2\infty] = \mathrm{Tr}_{F''/F'} \log[Q - \infty]$.

13.4. **Fifth roots, families and tails.** To apply the criterion to every point of a disc we write its points as an analytic family, which needs fifth roots of power series, and we bound the tail of the power series of its logarithm.

Lemma 13.5. *Let F' be a finite extension of $\mathbb{Q}_5$ and $\varepsilon \in F'$ with $v_5(\varepsilon) > 5/4$. Then $w = \sum_{k\geq 0} \binom{1/5}{k}\varepsilon^k$ converges, $w^5 = 1+\varepsilon$, and $v_5(w-1) \geq v_5(\varepsilon) - 1$. If $\zeta \notin F'$, then w is the only fifth root of $1+\varepsilon$ in F'. The same holds for a power series ε whose Gauss valuation on a closed disc exceeds $5/4$, with valuations replaced by Gauss valuations.*

Proof. The coefficient $\binom{1/5}{k} = \prod_{j=0}^{k-1}(1-5j)/(5^k k!)$ has v_5 equal to $-k - v_5(k!) \geq -k - (k-1)/4$, so the k-th term has valuation at least $k(v_5(\varepsilon) - 5/4) + 1/4$, which tends to infinity, and which for $k \geq 2$ is at least $v_5(\varepsilon) - 1$, the valuation of the term $k = 1$. The fifth roots of $1+\varepsilon$ differ by fifth roots of unity. □

Let $\mathfrak{P}$ be a prime of F above 5 with $e(\mathfrak{P}) = 20$, let $v = v_{\mathfrak{P}}$, and let $\mathfrak{p}_L$ be the prime of L below $\mathfrak{P}$. With the parameter t of Proposition 12.9, each family of local points of $\mathcal{C}$ is $s \mapsto P_{t(s)}$ with $t(s) = t_0 + 25s$, $t_0 \in 5\mathbb{Z}$, and s in the closed disc $\{v(s) \geq -10\}$ of radius $5^{1/2}$. The disc is larger than $\mathbb{Z}_5$ so that the Cauchy estimate on it bounds derivatives with a margin of 10 in v. The family is defined by (12.1) with

$$w(s) = w(t_0)\,(1+\varepsilon(s))^{1/5}, \qquad \varepsilon(s) \coloneqq \frac{H(t(s))}{H(t_0)} - 1,$$

where $H(t)$ means $H(t,1)$ or $H(1,t)$ as in Proposition 12.9, and $w(t_0)$ is a fifth root of $H(t_0)/\alpha$ in $L_{\mathfrak{p}_L}$, with $w(0) = 1$. The polynomial $\varepsilon(s)$ has coefficients in L. When its Gauss

valuation on the disc exceeds $5e(\mathfrak{P})/4 = 25$, Lemma 13.5 makes $w(s)$ a power series with coefficients in $L_{\mathfrak{p}_L}$ converging on the disc, and $s \mapsto P_{t(s)}$ is analytic there.

Lemma 13.6. *In this situation let $P \in \mathcal{C}(L)$ be the point of Lemma 12.3 for a rational $(u' : v')$ with parameter $t = t_0 + 25s$, $s \in \mathbb{Z}_5$. Then $P = P_{t(s)}$ in $\mathcal{C}(F_{\mathfrak{P}})$.*

Proof. Both points are given by (12.1) with the same (u', v'), and their values of w are fifth roots of $H(u', v')/\alpha$ in $L_{\mathfrak{p}_L}$ (the global w lies in $K \subseteq L_{\mathfrak{p}_L}$). Such a fifth root is unique as $\zeta \notin L_{\mathfrak{p}_L}$ (Table S20). □

Lemma 13.7. *Let $\Omega(s) = \sum_{n\geq 0} \Omega_n s^n$ be a power series with coefficients in $F_{\mathfrak{P}}^2$ whose Gauss valuation on the disc $\{v(s) \geq -10\}$ is at least 20, and let $\sum_{n\geq 1} \gamma_n s^n$ be its termwise integral. Then*

$$v(\gamma_n) \geq 20 + 10(n-1) - 20v_5(n) \qquad (n \geq 1).$$

If moreover $\pi^N \mathcal{O}_{\mathfrak{P}}^2 \subseteq \Lambda$, then $\operatorname{lev}(\gamma_n) \geq 2(n-1) - 4v_5(n) + 4 - N$. For $N = 4$ this bound is at least 4 for every $n \geq 3$, and at least 6 for $n = 4$ and every $n \geq 6$.

Proof. We have $v(\Omega_{n-1}) - 10(n-1) \geq 20$ and $\gamma_n = \Omega_{n-1}/n$, with $v(n) = 20v_5(n)$. By Lemma 13.2, $\operatorname{lev}(\gamma_n) \geq \lfloor (20 + 10(n-1) - 20v_5(n))/5 \rfloor - N = 4 + 2(n-1) - 4v_5(n) - N$. If $5 \nmid n$ the last bound is $2(n-1)$ for $N = 4$. If $n = 5^j n'$ with $j \geq 1$ and $5 \nmid n'$, it is $2(5^j n' - 1) - 4j$, which is 4 for $n = 5$ and at least 14 otherwise. □

The Gauss valuation of the integrand $\Omega = (X'/Y, XX'/Y)$ is bounded as follows (values in Table S20). That of ε, computed from its coefficients, bounds that of $w(s) - w(t_0)$ by Lemma 13.5. The linear forms $\ell_j(t(s))$ are dominated by their constant terms, which bounds $X - X(t_0)$ and $Y - Y(t_0)$. The Cauchy estimate gives $v(X') \geq v(X - X(t_0)) + 10$. If the Gauss valuation of $Y - Y(t_0)$ exceeds $v(Y(t_0))$, then $1/Y$ has Gauss valuation $-v(Y(t_0))$ and Y has no zero on the disc.

13.5. **Deciding a disc.**

Proposition 13.8. *Let $Q_0 \in \mathcal{X}(F)$, let $\mathfrak{P}$ be a prime of F above 5, and let $\mathcal{U}$ be a set of $F_{\mathfrak{P}}$-points of $\mathcal{X}$. Put $D_Q = [Q - Q_0]$. Assume:*

(i) $\operatorname{loc}_{\mathfrak{P}} \colon \mathrm{Sel} \to W_{\mathfrak{P}}$ *is injective, and* $\kappa_{\mathfrak{P}}(T_\pi) \neq 0$;

(ii) $\kappa_{\mathfrak{P}}(D_Q) = 0$ *for every* $Q \in \mathcal{U}$;

(iii) *for every $Q \in \mathcal{U}$ with $Q \neq Q_0$, the level of D_Q is finite and $\operatorname{cl}(D_Q)$ does not meet $\Sigma_{\mathfrak{P}} + \mathbb{F}_5 \kappa_{\mathfrak{P}}(T_\pi)$.*

Then every F-rational point of $\mathcal{X}$ whose image lies in $\mathcal{U}$ is Q_0.

Proof. We check the hypotheses of Proposition 5.1 with $\mathcal{P} = \{\mathfrak{P}\}$ and $\iota(Q) = D_Q$. Hypothesis (1) is our (i). For (2), $\kappa_{\mathfrak{P}}(T_\pi) \in \Sigma_{\mathfrak{P}}$ because $T_\pi \in J_{\mathcal{X}}(F)$. Let $Q \in \mathcal{U}$ and $\mathfrak{s} = cT_\pi$ with $c \in \mathbb{F}_5$. If $Q \neq Q_0$ and $c = 0$, then $D_Q \in \pi J_{\mathcal{X}}(F_{\mathfrak{P}})$ by (ii), and by Lemma 13.1(c) and (iii), $\mathcal{Q}(D_Q) \cap \Sigma_{\mathfrak{P}} \subseteq \mathbb{F}_5 \kappa_{\mathfrak{P}}(T_\pi)$. If $c \neq 0$, then $\kappa_{\mathfrak{P}}(D_Q + cT_\pi) = c\,\kappa_{\mathfrak{P}}(T_\pi) \neq 0$, so $D_Q + cT_\pi \notin \pi J_{\mathcal{X}}(F_{\mathfrak{P}})$ and $\mathcal{Q}(D_Q + cT_\pi) = \{c\,\kappa_{\mathfrak{P}}(T_\pi)\}$. If $Q = Q_0$, then $\mathcal{Q}(cT_\pi) \subseteq \kappa_{\mathfrak{P}}(J_{\mathcal{X}}(F_{\mathfrak{P}})[5^\infty]) = \mathbb{F}_5 \kappa_{\mathfrak{P}}(T_\pi)$ by Lemma 13.1(a). So D_Q is torsion for every F-rational Q with image in $\mathcal{U}$, while for $Q \neq Q_0$ it has finite positive level and is not torsion by Lemma 13.1(a). □

At two primes a condition on the classes of the torsion points becomes part of hypothesis (i).

Proposition 13.9. *In the situation of Proposition 13.8, let $\mathfrak{P}_1, \mathfrak{P}_2$ be two primes of F above 5, write $\kappa_1 = \kappa_{\mathfrak{P}_1}$ and $\kappa_2 = \kappa_{\mathfrak{P}_2}$, and let $\mathcal{P} = \{\mathfrak{P}_1, \mathfrak{P}_2\}$. Assume:*

(i) $\mathrm{loc}_{\mathcal{P}}\colon \mathrm{Sel} \to W_{\mathfrak{P}_1} \times W_{\mathfrak{P}_2}$ *is injective,* $\kappa_1(T_\pi) \neq 0 \neq \kappa_2(T_\pi)$*, and* $\Sigma_{\mathcal{P}}$ *meets* $\mathbb{F}_5\kappa_1(T_\pi) \times \mathbb{F}_5\kappa_2(T_\pi)$ *only in the diagonal* $\{(c\kappa_1(T_\pi), c\kappa_2(T_\pi))\colon c \in \mathbb{F}_5\}$*;*

(ii) $\kappa_1(D_Q) = \kappa_2(D_Q) = 0$ *for every* $Q \in \mathcal{U}$*;*

(iii) *for every* $Q \in \mathcal{U}$ *with* $Q \neq Q_0$*,* D_Q *has the same finite level* ν *at* $\mathfrak{P}_1$ *and at* $\mathfrak{P}_2$*, and for* $R_k \in J_{\mathcal{X}}(F_{\mathfrak{P}_k})$ *with* $\pi^\nu R_k = D_Q$ *the pair* $(\kappa_1(R_1), \kappa_2(R_2))$ *does not lie in* $\Sigma_{\mathcal{P}} + \mathbb{F}_5\kappa_1(T_\pi) \times \mathbb{F}_5\kappa_2(T_\pi)$*.*

Then every F*-rational point of* $\mathcal{X}$ *whose image lies in* $\mathcal{U}$ *is* Q_0*.*

Proof. We argue as for Proposition 13.8 with $\mathcal{P} = \{\mathfrak{P}_1, \mathfrak{P}_2\}$, and hypothesis (1) of Proposition 5.1 is part of (i). Now $\delta_{\mathcal{P}}(\Gamma) = \kappa_{\mathcal{P}}(\langle T_\pi \rangle)$ is the diagonal. For $Q \neq Q_0$ and $\mathfrak{s} = 0$, Lemma 13.1(c) at each prime shows that $\mathcal{Q}(D_Q)$ lies in the union of $(\kappa_1(R_1), \kappa_2(R_2)) + \mathbb{F}_5\kappa_1(T_\pi) \times \mathbb{F}_5\kappa_2(T_\pi)$ and $\mathbb{F}_5\kappa_1(T_\pi) \times \mathbb{F}_5\kappa_2(T_\pi)$. By (iii) and (i) its intersection with $\Sigma_{\mathcal{P}}$ lies in the diagonal. For $\mathfrak{s} = cT_\pi \neq 0$ the only element of $\mathcal{Q}(D_Q + \mathfrak{s})$ is the diagonal element $(c\kappa_1(T_\pi), c\kappa_2(T_\pi))$. For $Q = Q_0$ the set $\mathcal{Q}(\mathfrak{s})$ lies in $\mathbb{F}_5\kappa_1(T_\pi) \times \mathbb{F}_5\kappa_2(T_\pi)$, which meets $\Sigma_{\mathcal{P}}$ only in the diagonal. This is hypothesis (2), and we conclude as for Proposition 13.8. □

In the applications $\mathcal{U}$ is the image of a disc $s \mapsto Q_s$ ($s \in \mathbb{Z}_5$) with Q_0 at $s = 0$ and $\log[Q_s - Q_0] = \sum_{n\geq 1} \gamma_n s^n$ (Lemma 13.3). Suppose $\mathrm{lev}(\gamma_1) = \nu_1$ and $\mathrm{lev}(\gamma_n) > \nu_1$ for all $n \geq 2$. For $s = 5^m s_0$ with $s_0 \in \mathbb{Z}_5^\times$, every term $\gamma_n s^n$ with $n \geq 2$ has level $\mathrm{lev}(\gamma_n) + 4mn > \nu_1 + 4m$, and these terms tend to 0. So D_{Q_s} has level exactly $\nu_1 + 4m$ and $\mathrm{cl}(D_{Q_s}) = \overline{(-1)^m s_0}\,\vartheta$, where

$$\vartheta := \mathrm{cl}_{\nu_1}(\gamma_1). \tag{13.1}$$

So condition (iii) of Proposition 13.8 reduces to $\vartheta \notin \Sigma_{\mathfrak{P}} + \mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$.

14. The forms decided by the first descent

For the forms h_6, h_{23}, h_{16}, h_{14} and h_{24} the first descent suffices. A solution that comes from one of them gives a point $P \in \mathcal{C}(L)$ with $\kappa(P - \infty) = \kappa(P_0 - \infty)$ in the 5-adic disc of Proposition 12.9 around the known point P_0. Proposition 13.8 (for h_{24}, Proposition 13.9) shows that $P = P_0$: the class of the first coefficient of the logarithm on the disc is not in the span of the image of the Selmer group and the class of the torsion point T_π.

14.1. **Local data.** The local computations at a prime $\mathfrak{P}$ are done in the model $Y^2 = X^5 + \eta^{10}\beta$ of the curve, the image of the isomorphism $(X, Y) \mapsto (\eta^2 X, \eta^5 Y)$, for a power η of an element of F that is a uniformizer at $\mathfrak{P}$. This change of variables commutes with $(X, Y) \mapsto (\zeta X, Y)$ and multiplies log by a fixed diagonal matrix, so it changes neither levels nor classes, which are defined by divisibility by π in the group of points. The Gauss valuations and the inclusion $\pi^N \mathcal{O}_{\mathfrak{P}}^2 \subseteq \Lambda$ refer to the model used. Table S20 gives the data at the primes with $e = 20$ and the bounds for the families, for this section and Section 15.

14.2. **Forms 6, 23, 16 and 14.**

Theorem 14.1. *No primitive solution of* (11.1) *comes from* h_6*,* h_{23}*,* h_{16} *or* h_{14}*.*

Proof. Let a primitive solution come from h_i and (u, v) with $i \in \{6, 23, 16, 14\}$, so that (a) and (b) of Theorem 11.6(B) hold. Let $i' = 6$ for $i \in \{6, 23\}$ and $i' = 16$ for $i \in \{16, 14\}$, and let $P = P_{\Psi_i(u:v)} \in \mathcal{C}(L)$ (Lemmas 11.8 and 12.3). By Proposition 12.8, $\kappa(P - \infty) = \kappa(P_0 - \infty)$, and Proposition 12.9 gives $\Psi_i(u : v) = (t : 1)$ with $t \in 25\mathbb{Z}_5$. Write $t = 25s$ with $s \in \mathbb{Z}_5$. By Table S20 and Lemma 13.5, $s \mapsto P_{25s}$ is an analytic family on $\{v(s) \geq -10\}$, and by Lemma 13.6, $P = P_{25s}$ in $\mathcal{C}(F_{\mathfrak{P}})$.

We apply Proposition 13.8 at $\mathfrak{P}$ with $\mathcal{X}=\mathcal{C}$, $Q_0=P_0$ and $\mathcal{U}=\{P_{25s}\colon s\in\mathbb{Z}_5\}$. Condition (i) is Proposition 12.6, and condition (ii) is Proposition 12.9. For (iii), Lemma 13.3 gives $\log[P_{25s}-P_0]=\sum_{n\ge1}\gamma_n s^n$. The levels of $\gamma_1,\dots,\gamma_5$ (Lemma 13.1(c)) are $\operatorname{lev}(\gamma_1)=4$ and $\operatorname{lev}(\gamma_n)>4$ for $2\le n\le5$ (Table S20). For $n\ge6$, Lemma 13.7, with the integrand bound of Table S20 and $N=4$, gives $\operatorname{lev}(\gamma_n)\ge6$. By (13.1), condition (iii) reduces to $\vartheta=\mathrm{cl}_4(\gamma_1)\notin\Sigma_{\mathfrak{P}}+\mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$, which holds by Tables S21 and S22. Hence $P=P_0$, and as $[P_{25s}-P_0]$ has finite level for every $s\ne0$, we get $s=0$, that is $\Psi_i(u:v)=(0:1)$, and so $(u:v)=(u_i:v_i)$, which is $(0:1)$ for $i\in\{6,23,16\}$ and $(1:-1)$ for $i=14$. By Table 12 this pair violates condition (a), at 3 for $i=6$ and $i=16$, and at 2 and 3 for $i=23$ and $i=14$. □

14.3. **Form 24.** For $i'=24$ the Selmer group has dimension 9 and its image at either prime $\mathfrak{P}_1$, $\mathfrak{P}_2$ with $e=20$ has rank 8 (Table S20), so we use both primes in Proposition 13.9.

Theorem 14.2. *No primitive solution of* (11.1) *comes from* h_{24}.

Proof. Let a primitive solution come from h_{24} and (u,v), and let $P=P_{(u:v)}\in\mathcal{C}(L)$ for $i'=24$. By Propositions 12.8 and 12.9, $\kappa(P-\infty)=\kappa(P_0-\infty)$ and $(u:v)=(1:t)$ with $t=25s$, $s\in\mathbb{Z}_5$. By Lemma 13.6, $P=P_{25s}$ in $\mathcal{C}(F_{\mathfrak{P}_1})$ and in $\mathcal{C}(F_{\mathfrak{P}_2})$. We apply Proposition 13.9 with $\mathcal{X}=\mathcal{C}$, $Q_0=P_0$ and $\mathcal{U}=\{P_{25s}\colon s\in\mathbb{Z}_5\}$. In condition (i), the injectivity is Proposition 12.6, and a basis of $\Sigma_{\mathcal{P}}$, printed in Table S23, shows that $\Sigma_{\mathcal{P}}$ meets $\mathbb{F}_5\kappa_1(T_\pi)\times\mathbb{F}_5\kappa_2(T_\pi)$ exactly in the diagonal. Condition (ii) is Proposition 12.9. For (iii), at each $\mathfrak{P}_k$ we have $\log[P_{25s}-P_0]=\sum\gamma_n^{(k)}s^n$ with $\operatorname{lev}(\gamma_1^{(k)})=3$ and $\operatorname{lev}(\gamma_2^{(k)})\ge7$, and $\operatorname{lev}(\gamma_n^{(k)})\ge4$ for $n\ge3$ by Lemma 13.7. So for $s=5^m s_0$ with $s_0\in\mathbb{Z}_5^\times$ the divisor $D=[P_{25s}-P_0]$ has level $3+4m$ at both primes, and its classes are $\overline{(-1)^m s_0}\,(\vartheta_1,\vartheta_2)$ modulo $\mathbb{F}_5\kappa_1(T_\pi)\times\mathbb{F}_5\kappa_2(T_\pi)$, where $\vartheta_k=\mathrm{cl}_3(\gamma_1^{(k)})$. The scalar is the same at both primes, as it comes from s_0 and the global identity $5=\pi^4\cdot(\text{unit})$. The pair $(\vartheta_1,\vartheta_2)$ does not lie in $\Sigma_{\mathcal{P}}+\mathbb{F}_5\kappa_1(T_\pi)\times\mathbb{F}_5\kappa_2(T_\pi)$ (Table S23). Hence $P=P_0$, and as D has finite level for every $s\ne0$, we get $s=0$, so $(u:v)=(1:0)$, which violates condition (a) at 2 (Table 12). □

15. The forms decided by a second descent, and the proof of Theorem C

To complete the proof of Theorem C it remains to treat h_{22}, h_5 and h_{13}, that is, the curves $\mathcal{C}$ with $i'\in\{22,5\}$. For these curves Proposition 13.8 on $\mathcal{C}$ near P_0 fails: for $i'=5$ the family $t=25s$ has $\operatorname{lev}(\gamma_1)=4$, and $\mathrm{cl}_4(\gamma_1)$ lies in $\Sigma_{\mathfrak{P}}$ but not in the span of $\kappa_{\mathfrak{P}}(P_0-\infty)$ and $\kappa_{\mathfrak{P}}(T_\pi)$. We pass to a quotient $\mathcal{D}$ of a π-covering of $\mathcal{C}$ (lifting points to coverings is an old idea [13, 56]). The curve $\mathcal{D}$ again has an automorphism of order 5, so the tools of Sections 12 and 13 apply to it. In this section $i'\in\{22,5\}$.

15.1. **The quotient curve.** In this section ξ denotes $Y(P_0)-\sqrt{\beta}\in M^\times$, so $\kappa(P_0-\infty)$ is the class of ξ.

Proposition 15.1. *Let* $P=(X,Y)\in\mathcal{C}(L)$ *with* $X\ne0$ *and* $\kappa(P-\infty)=\kappa(P_0-\infty)$.

(a) *There is a unique* $Z\in M$ *with* $Y-\sqrt{\beta}=\xi Z^5$.

(b) *The point* (X_2,Y_2) *with*

$$X_2=-2\xi\sqrt{\beta}\,\frac{Z^3}{X^2},\qquad Y_2=2\xi\beta\,\frac{Y-3\sqrt{\beta}}{Y+\sqrt{\beta}}$$

lies on $\mathcal{D}_0\colon Y_2^2=X_2^5+4\xi^2\beta^2$, *a curve over* M.

(c) $Y_2 - 2\xi\beta = -8\xi^2\beta\sqrt{\beta}\, Z^5/X^5$. *In particular the class of* $Y_2 - 2\xi\beta$ *in* $F^\times/F^{\times 5}$ *is that of* $-8\xi^2\beta\sqrt{\beta}$, *independently of* P.

Proof. (a) The elements $Y - \sqrt{\beta}$ and ξ lie in M, and their quotient q is z^5 with $z \in F$. As $[F : M] = 2$, $q^2 = N_{F/M}(z)^5$, so $q = (q^2)^3/q^5 = \big(N_{F/M}(z)^3/q\big)^5$ is a fifth power in M, and the fifth root is unique as $\zeta \notin M$.

(b) From $X^5 = Y^2 - \beta = (Y - \sqrt{\beta})(Y + \sqrt{\beta})$ we get $X^{10} = (Y - \sqrt{\beta})^2(Y + \sqrt{\beta})^2$, and from (a), $Z^{15} = (Y - \sqrt{\beta})^3/\xi^3$. In particular $Y + \sqrt{\beta} \neq 0$. Hence

$$X_2^5 = -32\xi^5\beta^2\sqrt{\beta}\,\frac{Z^{15}}{X^{10}} = -32\xi^2\beta^2\sqrt{\beta}\,\frac{Y - \sqrt{\beta}}{(Y + \sqrt{\beta})^2},$$

and $Y_2^2 - X_2^5 = 4\xi^2\beta^2\big((Y - 3\sqrt{\beta})^2 + 8\sqrt{\beta}(Y - \sqrt{\beta})\big)/(Y + \sqrt{\beta})^2 = 4\xi^2\beta^2$.

(c) We have $Y_2 - 2\xi\beta = 2\xi\beta\big((Y - 3\sqrt{\beta}) - (Y + \sqrt{\beta})\big)/(Y + \sqrt{\beta}) = -8\xi\beta\sqrt{\beta}/(Y + \sqrt{\beta})$, and $Y + \sqrt{\beta} = X^5/(Y - \sqrt{\beta}) = X^5/(\xi Z^5)$. □

We rescale $\mathcal{D}_0$ to an integral model. Let $d' = 2^{m_1}5^{m_2}$, where $0 \le m_1, m_2 \le 6$ and $m_1 + m_2$ is as large as possible such that $4\xi^2\beta^2/d'^{10}$ is integral. This gives $d' = 20$ for $i' = 22$ and $d' = 4$ for $i' = 5$. Then the map $(X_2, Y_2) \mapsto (X_2/d'^2, Y_2/d'^5)$ identifies $\mathcal{D}_0$ with

$$\mathcal{D}\colon\ Y^2 = X^5 + \beta', \qquad \beta' := 4\xi^2\beta^2/d'^{10}, \qquad \sqrt{\beta'} = 2\xi\beta/d'^5 \in M.$$

Let $P_0' \in \mathcal{D}(M)$ be the image of P_0 (with $Z = 1$), $J_\mathcal{D}$ the Jacobian of $\mathcal{D}$, and $T_\pi' = [(0, \sqrt{\beta'}) - \infty] \in J_\mathcal{D}(M)$. Let κ', $W_\mathfrak{p}'$ and $\mathrm{Sel}(J_\mathcal{D})$ be the objects of Section 12.2 for $\mathcal{D}$ over F. For P as in Proposition 15.1 let $P' \in \mathcal{D}(M)$ be the image of (X_2, Y_2). By Proposition 15.1(c), $\kappa'(P' - \infty) = \kappa'(P_0' - \infty)$, that is,

$$[P' - P_0'] \in \pi J_\mathcal{D}(F). \tag{15.1}$$

15.2. **The Selmer groups of the quotients.**

Proposition 15.2. *Let* S' *be the set of primes of* F *above* 2, 3, 5 *for* $i' = 22$, *and above* 2, 3, 5, 2281 *for* $i' = 5$. *It is the set* S *of Section 12.2 for the same* i', *and it contains all primes at which* $\mathcal{D}$ *has bad reduction and all primes above* 5. *Then* $\mathrm{Sel}(J_\mathcal{D})$ *lies in the image of* $M^\times/M^{\times 5}$, *and its dimension is* 8 *for* $i' = 22$ *and* 4 *for* $i' = 5$. *The classes* $\kappa'(P_0' - \infty)$ *and* $\kappa'(T_\pi')$ *are independent elements of* $\mathrm{Sel}(J_\mathcal{D})$. *At the prime* $\mathfrak{P}$ *of* F *above* 5 *with* $e(\mathfrak{P}) = 20$ *we have* $\kappa'_\mathfrak{P}(T_\pi') \neq 0$, *and* $\mathrm{loc}_\mathfrak{P}\colon \mathrm{Sel}(J_\mathcal{D}) \to W_\mathfrak{P}'$ *is injective. Moreover* τ *fixes* $\mathfrak{P}$, *the space* $W_\mathfrak{P}'$ *is* τ*-stable with eigenspaces for* $\tau = +1$ *and* $\tau = -1$ *of dimensions* 11 *and* 10 *for* $i' = 22$, *and* 10 *and* 11 *for* $i' = 5$, *and* $\Sigma_\mathfrak{P}' := \mathrm{loc}_\mathfrak{P}(\mathrm{Sel}(J_\mathcal{D}))$ *lies in the* $(+1)$*-eigenspace.*

Proof. The local images $W_\mathfrak{p}'$, $\mathfrak{p} \in S'$, are the spans of the classes of explicit local points, as in Proposition 12.6. For $i' = 5$ the points of $\mathcal{D}(F_\mathfrak{P})$ that we found span 19 of the 21 dimensions of $W_\mathfrak{P}'$, and we completed the span with the classes of divisors $Q + \bar{Q}$, with Q a point over the unramified quadratic extension of $F_\mathfrak{P}$ and $\bar{Q}$ its conjugate. The class of such a divisor is the norm of $Y(Q) - \sqrt{\beta'}$.

We apply Lemma 12.5 with $L_0 = M$ and $G = \langle\tau\rangle$, where $\omega(\tau) = -1$, so the $(+1)$-eigenspace E_+, the image of $M^\times/M^{\times 5}$, is paired with the (-1)-eigenspace E_-. The local conditions are τ-stable, as $\mathcal{D}$ and $\sqrt{\beta'}$ are defined over M, so that $\kappa'(\tau Q) = \tau(\kappa'(Q))$, and maximal isotropic as for $\mathcal{C}$ (Section 12.2). The class number of M is prime to 5 (Proposition A.13), so $E_+ \cap F(S', 5)$ is the image of $\mathcal{O}_{M,S_M}^\times/\mathcal{O}_{M,S_M}^{\times 5}$, with an explicit basis of S_M-units as in Proposition 12.6, and $\mathrm{Sel}(J_\mathcal{D}) \cap E_+$ is the kernel of a linear map, of dimension 8 for $i' = 22$ and 4 for $i' = 5$, spanned by explicit elements of M. Lemma 12.5(d), evaluated with the

local images, gives $\dim(\mathrm{Sel}(J_{\mathcal{D}})\cap E_-)-\dim(\mathrm{Sel}(J_{\mathcal{D}})\cap E_+)=-8$ for $i'=22$ and -4 for $i'=5$ (Appendix B). So $\mathrm{Sel}(J_{\mathcal{D}})\cap E_-=0$, and the remaining statements are linear algebra over $\mathbb{F}_5$ on these classes. A basis of $\Sigma'_{\mathfrak{P}}$ is printed in Tables S25 and S26. □

The eigenspace statement puts the classes of odd level on $\mathcal{D}$ outside $\Sigma'_{\mathfrak{P}}$.

Lemma 15.3. *Let $\mathfrak{P}$ be as in Proposition 15.2. Let $D\in J_{\mathcal{D}}(F_{\mathfrak{P}})$ be fixed by τ, of finite level $\nu\geq 1$, and let $R\in J_{\mathcal{D}}(F_{\mathfrak{P}})$ with $\pi^\nu R=D$. Then $\tau(\kappa'_{\mathfrak{P}}(R))\equiv(-1)^\nu\kappa'_{\mathfrak{P}}(R)$ modulo $\mathbb{F}_5\kappa'_{\mathfrak{P}}(T'_\pi)$. Consequently, if ν is odd, then $\mathrm{cl}(D)$ does not meet $\Sigma'_{\mathfrak{P}}+\mathbb{F}_5\kappa'_{\mathfrak{P}}(T'_\pi)$.*

Proof. As $\mathcal{D}$ and $\sqrt{\beta'}$ are defined over M and τ fixes $\mathfrak{P}$, τ acts on $J_{\mathcal{D}}(F_{\mathfrak{P}})$ and on $F_{\mathfrak{P}}^\times/F_{\mathfrak{P}}^{\times 5}$ with $\kappa'_{\mathfrak{P}}(\tau D')=\tau(\kappa'_{\mathfrak{P}}(D'))$. Moreover $\tau\circ[\zeta]=[\zeta^{-1}]\circ\tau$, so $\tau\pi\tau^{-1}=1-[\zeta]^{-1}=-[\zeta]^{-1}\pi$. Applying τ to $\pi^\nu R=D$ gives $\pi^\nu((-1)^\nu[\zeta]^{-\nu}\tau R)=D=\pi^\nu R$, so $(-1)^\nu[\zeta]^{-\nu}\tau R-R\in J_{\mathcal{D}}(F_{\mathfrak{P}})[\pi^\nu]=\langle T'_\pi\rangle$ (Lemma 13.1(a)). Since $\kappa'_{\mathfrak{P}}([\zeta]D')=\kappa'_{\mathfrak{P}}(D')$, applying $\kappa'_{\mathfrak{P}}$ gives the congruence. Now $\kappa'_{\mathfrak{P}}(T'_\pi)$ is fixed by τ, as $T'_\pi\in J_{\mathcal{D}}(M)$, and $\Sigma'_{\mathfrak{P}}$ lies in the $(+1)$-eigenspace. So if $\kappa'_{\mathfrak{P}}(R)\in\Sigma'_{\mathfrak{P}}+\mathbb{F}_5\kappa'_{\mathfrak{P}}(T'_\pi)$ and ν is odd, then $\kappa'_{\mathfrak{P}}(R)$ is both fixed and negated by τ modulo $\mathbb{F}_5\kappa'_{\mathfrak{P}}(T'_\pi)$, so $2\kappa'_{\mathfrak{P}}(R)\in\mathbb{F}_5\kappa'_{\mathfrak{P}}(T'_\pi)$, contradicting Lemma 13.1(c). □

15.3. **The lifted family.** We lift the family of Section 13.4 on the disc $t=25s$ to $\mathcal{D}$. Let $\mathfrak{p}_M$ be the prime of M below $\mathfrak{P}$, so $\zeta\notin M_{\mathfrak{p}_M}$ (Table S20). For the family $s\mapsto P_{25s}=(X(s),Y(s))$ put

$$Z(s)\coloneqq\big(1+\varepsilon_Z(s)\big)^{1/5},\qquad \varepsilon_Z(s)\coloneqq\frac{Y(s)-\sqrt{\beta}}{\xi}-1.$$

The Gauss valuation of ε_Z on $\{v(s)\geq -10\}$ is at least $30>25$ (Table S20), so $Z(s)$ is a power series with coefficients in $M_{\mathfrak{p}_M}$ converging on the disc. Proposition 15.1(b) with $Z=Z(s)$, followed by the rescaling, defines an analytic family $s\mapsto P'_s\in\mathcal{D}(M_{\mathfrak{p}_M})$ with P'_0 at $s=0$. By Proposition 15.1(c), $\kappa'_{\mathfrak{P}}(P'_s-P'_0)=0$ for every s.

Lemma 15.4. *Let $P\in\mathcal{C}(L)$ satisfy the hypotheses of Proposition 15.1, with $P=P_{25s}$ in $\mathcal{C}(F_{\mathfrak{P}})$ for some $s\in\mathbb{Z}_5$, and let $P'\in\mathcal{D}(M)$ be its image. Then $P'=P'_s$ in $\mathcal{D}(F_{\mathfrak{P}})$.*

Proof. The global Z and $Z(s)$ are fifth roots of $(Y(s)-\sqrt{\beta})/\xi$ in $M_{\mathfrak{p}_M}$, equal as $\zeta\notin M_{\mathfrak{p}_M}$. □

15.4. **Form 22.** For $i'=22$ the disc of Proposition 12.9 is $t\in 5\mathbb{Z}_5$, with $(u:v)=(1:t)$. We treat the annulus $t\in 5\mathbb{Z}_5\smallsetminus 25\mathbb{Z}_5$ on $\mathcal{C}$ and the disc $t\in 25\mathbb{Z}_5$ on $\mathcal{D}$.

Proposition 15.5. *Let $i'=22$. No point of $\mathcal{C}(F)$ lies in $\mathcal{U}=\{P_t\colon t\in 5\mathbb{Z}_5\smallsetminus 25\mathbb{Z}_5\}\subseteq\mathcal{C}(F_{\mathfrak{P}})$.*

Proof. Write $\mathcal{U}$ as the union of the families $\mathcal{U}_j=\{P_{5j+25s}\colon s\in\mathbb{Z}_5\}$, $j=1,\dots,4$, of Section 13.4 with $t_0=5j$, for which $H(1,5j)/\alpha$ has exactly one fifth root $w(5j)$ in $L_{\mathfrak{p}_L}$. We apply Proposition 13.8 with $\mathcal{X}=\mathcal{C}$ and $Q_0=P_0\notin\mathcal{U}$. Condition (i) is Proposition 12.6, and (ii) is Proposition 12.9. For (iii), let $D_j=[P_{5j}-P_0]$. With the logarithms of Lemma 13.4, $\mathrm{lev}(D_j)=1$ and $\mathrm{cl}(D_j)$ does not meet $\Sigma_{\mathfrak{P}}+\mathbb{F}_5\kappa_{\mathfrak{P}}(T_\pi)$ (Table S24). By Lemma 13.3, $\log[P_{5j+25s}-P_{5j}]=\sum_{n\geq 1}\gamma_n^{(j)}s^n$. For this curve the lattice satisfies $\pi\mathcal{O}_{\mathfrak{P}}^2\subseteq\Lambda$ (Appendix B), and Lemma 13.7, with the integrand bound of Table S20 and $N=1$, gives $\mathrm{lev}(\gamma_n^{(j)})\geq 2n+1-4v_5(n)\geq 3$ for every $n\geq 1$. Hence $[P_{5j+25s}-P_0]=D_j+[P_{5j+25s}-P_{5j}]$ has level exactly 1 and class $\mathrm{cl}(D_j)$, for every $s\in\mathbb{Z}_5$. So Proposition 13.8 applies, and as $P_0\notin\mathcal{U}$ no F-rational point lies in $\mathcal{U}$. □

Theorem 15.6. *No primitive solution of (11.1) comes from h_{22}.*

Proof. Let a primitive solution come from h_{22} and (u, v), and let $P = P_{(u:v)} \in \mathcal{C}(L)$. By Propositions 12.8 and 12.9, $\kappa(P - \infty) = \kappa(P_0 - \infty)$ and $(u : v) = (1 : t)$ with $t \in 5\mathbb{Z}_5$. By Proposition 15.5 and Lemma 13.6, $t = 25s$ with $s \in \mathbb{Z}_5$ and $P = P_{25s}$ in $\mathcal{C}(F_{\mathfrak{P}})$. As $X(P) \neq 0$ (Lemma 12.3), Proposition 15.1 gives $P' \in \mathcal{D}(M)$, and $P' = P'_s$ by Lemma 15.4.

We apply Proposition 13.8 with $\mathcal{X} = \mathcal{D}$ at $\mathfrak{P}$, with $Q_0 = P'_0$ and $\mathcal{U} = \{P'_s \colon s \in \mathbb{Z}_5\}$. Condition (i) is Proposition 15.2, and (ii) holds by construction of the family. For (iii), $\log[P'_s - P'_0] = \sum_{n\geq 1} \gamma_n s^n$ (Lemma 13.3), with $\operatorname{lev}(\gamma_1) = 3$ and $\operatorname{lev}(\gamma_2) = 7$ by computation, and $\operatorname{lev}(\gamma_n) \geq 4$ for $n \geq 3$ by Lemma 13.7 (with Table S20 and $N = 4$). So for $s = 5^m s_0 \neq 0$ the level of $[P'_s - P'_0]$ is $3 + 4m$, which is odd. This divisor is fixed by τ, since P'_s and P'_0 have coordinates in $M_{\mathfrak{p}_M}$, the fixed field of τ in $F_{\mathfrak{P}}$. So Lemma 15.3 shows that $\operatorname{cl}([P'_s - P'_0])$ does not meet $\Sigma'_{\mathfrak{P}} + \mathbb{F}_5\kappa'_{\mathfrak{P}}(T'_\pi)$. Hence $P' = P'_0$, and as $[P'_s - P'_0]$ has finite level for every $s \neq 0$, we get $s = 0$ and $(u : v) = (1 : 0)$, which violates condition (a) of Theorem 11.6 at 2 and at 3 (Table 12). □

15.5. **Forms 5 and 13.**

Theorem 15.7. *Every primitive solution of* (11.1) *with* $abc \neq 0$ *that comes from* h_5 *is one of the Catalan solutions* $(\pm 3, -2, 1)$*, and none comes from* h_{13}*.*

Proof. Let a primitive solution with $abc \neq 0$ come from h_i and (u, v), $i \in \{5, 13\}$, and let $P = P_{\Psi_i(u:v)} \in \mathcal{C}(L)$ for $i' = 5$. By Propositions 12.8 and 12.9 and Lemma 13.6, $\kappa(P - \infty) = \kappa(P_0 - \infty)$, $\Psi_i(u : v) = (t : 1)$ with $t = 25s$, $s \in \mathbb{Z}_5$, and $P = P_{25s}$ in $\mathcal{C}(F_{\mathfrak{P}})$. As $X(P) \neq 0$, Proposition 15.1 and Lemma 15.4 give $P' = P'_s \in \mathcal{D}(M)$. The argument of the second paragraph of the proof of Theorem 15.6, with the levels $\operatorname{lev}(\gamma_1) = 3$, $\operatorname{lev}(\gamma_2) = 7$ computed for $i' = 5$ and with Table S26, gives $s = 0$. So $\Psi_i(u : v) = (0 : 1)$, that is, $(u : v) = (0 : 1)$. For $i = 5$ this pair gives the Catalan solutions (Theorem 11.6(C)). For $i = 13$ it violates condition (a) at 2 (Table 12). □

15.6. **Proof of Theorem C.**

Proof of Theorem C. Let (a, b, c) be a primitive solution of (11.1). If $abc = 0$, it is one of the trivial solutions listed in Theorem C. If $abc \neq 0$, it comes from h_i and coprime (u, v) with $i \in \mathcal{I}$, satisfying (a) and (b) (Theorem 11.6). No primitive solution comes from h_6, h_{23}, h_{16} or h_{14} (Theorem 14.1), from h_{24} (Theorem 14.2), from h_{22} (Theorem 15.6) or from h_{13} (Theorem 15.7). A primitive solution coming from h_5 is $(\pm 3, -2, 1)$ (Theorem 15.7), and $3^2 + (-2)^3 = 1 = 1^{25}$. So every primitive solution with $abc \neq 0$ is a Catalan solution. □

Part IV. **The exponents 13 and 26, and those that remain**

16. The exponent 13: the descent

For $p = 13$ the curve $X_0(13)$ has genus 0, so Parts I and II do not apply. Freitas, Naskręcki and Stoll reduce the equation to points on twists of $X_1(13)$, of genus 2, over fields of degree 14, and observe that a 2-descent on them needs a number field of degree 84 [27, §§8, 9]. The diamond automorphism σ of order 3 of $X_1(13)$ survives the twist, and we descend by $\lambda = 1 - \sigma$ instead. The order-3 diamond operators act trivially on the kernel of λ, so the cubic part of the twist disappears from it, and the descent needs only a quadratic extension of $K_E(\omega)$, of degree 56 (Proposition 16.3). The class groups of these fields, one for each of the four curves E, enter through their 3-parts, which are trivial under GRH (Proposition 16.5). The rest of the proof, a 3-adic analysis in the manner of Sections 4 and 5, uses no hypothesis

(Section 17). In this part λ denotes $1-\sigma$, not the Eisenstein prime of Section 3.5, and ω is a primitive cube root of unity.

16.1. **The reduction.** Let $\Phi(v)=(v^2+3v+9)(v^4+3v^3+5v^2-4v-4)^3$. With the coordinate v on $X_0(13)\simeq\mathbb{P}^1$ of [27, §8.1], the j-map is $j=\Phi(v)/(v-1)$, so the v-coordinates of the points over $j_1\neq\infty$ are the roots of

$$G_{j_1}(v):=\Phi(v)-j_1(v-1),$$

which is monic of degree 14. The cusps are $v=1$ and $v=\infty$. Let $C_3=\{t^3:t\in\mathbb{Z}_3\}$.

Theorem 16.1 (Freitas, Naskręcki and Stoll)**.** *Let (a,b,c) be a primitive solution of $x^2+y^3=z^{13}$ with $abc\neq0$. Then for some $d'\in\{\pm1,\pm2,\pm3,\pm6\}$ the twist $E'=E^{(d')}_{a,b,c}$ satisfies $E'[13]\simeq E[13]$ as $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules for some $E\in\{96\mathrm{a}1,864\mathrm{a}1,864\mathrm{b}1,864\mathrm{c}1\}$, and $j_0=1728b^3/c^{13}$ lies in the following subsets of $\mathbb{Q}_3$:*

- *for $E=96\mathrm{a}1$: $3\mid c$ and $j_0=3^{-10}t^{-13}$ with $t\in\mathbb{Z}_3\setminus\{0\}$ and $v_3(t)=v_3(c)-1$;*
- *for $E=864\mathrm{a}1$: $-216+3^6\mathbb{Z}_3$, $-108+3^5\mathbb{Z}_3$ or $-27+3^5\mathbb{Z}_3$;*
- *for $E=864\mathrm{b}1$, $864\mathrm{c}1$: $27+3^6\mathbb{Z}_3$, 3^6C_3 or $2\cdot3^6C_3$.*

Proof. By [27, Proposition 2.4 and Lemma 8.1] the mod 13 representation of $E_{a,b,c}$ is irreducible, and by [27, Lemma 2.3] some twist E' has $E'[13]\simeq E[13]$ for one of the seven curves of [27, Lemma 2.3]. For $p=13$, Theorem 5.1 of [27], whose list depends on p modulo 24, leaves the curves $X_E(13)$ with $E\in\{27\mathrm{a}1,96\mathrm{a}2,288\mathrm{a}1,288\mathrm{a}2,864\mathrm{a}1,864\mathrm{b}1,864\mathrm{c}1\}$, and Lemma 8.2 of [27] (in §8.2 there) removes 27a1, 288a1 and 288a2. The curve 96a2 is 2-isogenous to 96a1, so $96\mathrm{a}2[13]\simeq96\mathrm{a}1[13]$, and we work with 96a1. The 3-adic sets come from Tables 2 and 3 of [27] (line 1 for 96a1, lines 4 and 7 for 864a1, lines 3 and 5 for 864b1 and 864c1) exactly as in Section 8.1, with 13 in place of 19; a computation over all (a,b) modulo 3^7 confirms lines 3, 4, 5 and 7, and line 1 is derived in the next sentence. For 96a1, $c=3c'$ and $j_0=3^{-10}(2^6b^3)c'^{-13}$, and the unit 2^6b^3 is a 13-th power in $\mathbb{Z}_3^\times$, since $x\mapsto x^{13}$ is a bijection of $\mathbb{Z}_3^\times\simeq\{\pm1\}\times(1+3\mathbb{Z}_3)$. □

We split these sets into *leaves*, on which the local classes below are constant: for 96a1, the nine sets $t\equiv t'\pmod 9$; for 864a1, $-216+3^6t'+3^7\mathbb{Z}_3$, $-108+3^5t'+3^6\mathbb{Z}_3$ and $-27+3^5t'+3^6\mathbb{Z}_3$ ($t'=0,1,2$); for 864b1 and 864c1, $27+3^6t'+3^7\mathbb{Z}_3$ ($t'=0,1,2$), the four sets $\pm3^6u+3^8\mathbb{Z}_3$ and the four sets $\pm3^9u+3^{11}\mathbb{Z}_3$ ($u=1,2$), and the two sets $\{3^{12}u\,t^3:t\in\mathbb{Z}_3\}$ ($u=1,2$). Since the cubes of $\mathbb{Z}_3^\times$ are $\pm(1+9\mathbb{Z}_3)$, these partition $3^6C_3\cup2\cdot3^6C_3$.

16.2. **The curves X_ψ.** Let E be one of the four curves and $j_E=j(E)$, that is $21952/9$, -216, -13824, 1536. The polynomial G_{j_E} is irreducible, and its roots are the v-coordinates of the points of $X_0(13)$ attached to the subgroups of order 13 of $E[13]$, as in Proposition 2.8(a). So

$$K=K_E=\mathbb{Q}(v_0),\qquad G_{j_E}(v_0)=0,$$

is the field of Definition 2.7, of degree 14; it has no quadratic subfield and no automorphism other than the identity. Let $\psi\colon\mathrm{Gal}(\bar{\mathbb{Q}}/K)\to\mathbb{F}_{13}^\times$ be the character by which Galois acts on the subgroup C_E of order 13 attached to v_0. Put

$$d=(v_0+2)^2+4,\qquad\gamma=\frac{v_0-3\omega}{v_0-3\omega^2}\in K(\omega),$$

and let X_ψ be the smooth projective curve over K with function field generated by v, Y, Z subject to

$$dY^2 = (v+2)^2 + 4, \qquad \gamma\Big(\frac{Z-\omega}{Z-\omega^2}\Big)^3 = \frac{v-3\omega}{v-3\omega^2}. \tag{16.1}$$

This is the model of [27, §8.1] for the twist of $X_1(13)$ by ψ modulo ±1, through the diamond operators $(\mathbb{Z}/13)^\times/\{\pm1\}$, which form a cyclic group of order 6. It is a cyclic cover of degree 3 of the conic $D\colon dY^2 = (v+2)^2+4$, which has the K-point $(v_0, 1)$, and the map v is the map to $X_0(13)$. The automorphisms

$$\sigma\colon Z \mapsto -\frac{Z+1}{Z}, \qquad \iota\colon Y \mapsto -Y$$

are the diamond operators of orders 3 and 2, σ multiplies $w = (Z-\omega)/(Z-\omega^2)$ by ω, and ι is the hyperelliptic involution. The cover $X_\psi \to D$ is ramified exactly at the four points over $v = 3\omega, 3\omega^2$, where $w = 0$ or ∞, so X_ψ has genus 2. The point $Q_0 = (v_0, 1, \infty)$ is the point given by E and C_E, and $\iota Q_0 = (v_0, -1, \infty)$. The point Q_0 determines d and γ: a curve of the shape (16.1) that has a K-point with $v = v_0$, $Y = 1$, $Z = \infty$ must have $d \equiv (v_0+2)^2+4$ modulo squares and $\gamma \equiv (v_0 - 3\omega)/(v_0 - 3\omega^2)$ modulo cubes. We write J for the Jacobian of X_ψ; σ acts on it with $\sigma^2 + \sigma + 1 = 0$, so $\mathbb{Z}[\zeta_3] \subseteq \mathrm{End}_K(J)$ with $\zeta_3 \mapsto \sigma$.

Lemma 16.2. *Let E' be an elliptic curve over $\mathbb{Q}$ with $j(E') \notin \{0, 1728\}$ and an isomorphism $E'[13] \simeq E[13]$ of Galois modules, and let C' be the image of C_E. Then (E', C') gives a point $Q \in X_\psi(K)$ with $j(Q) = j(E')$, and $v(Q)$ generates K. In particular its image in $K_\mathfrak{p}$ generates $K_\mathfrak{p}$ over $\mathbb{Q}_3$ for every prime $\mathfrak{p} \mid 3$ of K.*

Proof. The point exists by [27, §8.1]: $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ acts on C' through ψ. The coordinate $v(Q)$ is the point of $X_0(13)$ given by (E', C'). As $\mathrm{Aut}(E'_{\bar{\mathbb{Q}}}) = \{\pm1\}$, an element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ fixes $v(Q)$ if and only if it maps C' to itself, and since the isomorphism is Galois-equivariant, C' and C_E have the same stabilizer. So $\mathbb{Q}(v(Q)) = \mathbb{Q}(v_0) = K$. □

The *known points* of $X_\psi(K)$ are the points over the j-invariants of curves isogenous to E by isogenies of degree prime to 13. For the three curves of conductor 864 they are the six points $\sigma^a Q_0$, $\sigma^a \iota Q_0$; for 96a1 the four curves of the isogeny class give four orbits of six points each. Their classes span the subspace K_0 of the Selmer group of Proposition 16.4, of dimension 1 for the curves of conductor 864 and 3 for 96a1.

16.3. **The descent by $\mathbf{1-\sigma}$.** Let $F = K(\omega)$, of degree 28. Let $R_1, R_2 = (3\omega, \pm Y_1, \omega)$ be the two points of X_ψ over $v = 3\omega$, where $dY_1^2 = 3\omega - 1$; their conjugates R_3, R_4 lie over $3\omega^2$. Put

$$L = L_E := F\big(\sqrt{d(3\omega-1)}\big) = K(\omega, Y_1),$$

of degree 56, and let τ be its automorphism over F. On D let $m = (Y-1)/(v-v_0)$ be the slope of the line through $(v_0, 1)$, a coordinate with $m(\iota Q_0) = \infty$ and $m(Q_0) = (v_0+2)/d$, and put

$$m_{1,2} = \frac{\pm Y_1 - 1}{3\omega - v_0}, \qquad g_1 = \frac{m - m_1}{m - m_2}.$$

Proposition 16.3. *Let $\lambda = 1 - \sigma \in \mathrm{End}_K(J)$ and $M = J[\lambda]$.*

(a) *$M \simeq \mathbb{F}_3^2$ is spanned by $[R_1 - R_2]$ and $[R_3 - R_4]$, and $M \simeq \mathrm{Ind}_F^K \mathbb{F}_3(\chi)$, where χ is the quadratic character of L/F.*

(b) *$H^1(K, M) \simeq (L^\times/L^{\times 3})^-$, the subgroup on which τ acts by -1, which is the kernel of the norm to F modulo cubes.*

(c) $J(K)[\lambda] = 0$.

(d) *For a suitable choice of the isomorphism in* (b)*, the Kummer map of* λ*, followed by this isomorphism, sends* $[P - \iota Q_0]$ *to the class of* $g_1(m(P))$*, for* $P \in X_\psi(K')$ *over any field* $K' \supseteq K$ *(with* $L \otimes_K K'$ *in place of* L*).*

Proof. (a) The fixed points of σ are the points with $w \in \{0, \infty\}$, which are $R_1, \dots, R_4$. For a cyclic cover of prime degree of a curve of genus 0 with r branch points, the kernel of $1 - \sigma$ has dimension $r - 2$ over $\mathbb{F}_3$ and is spanned by the differences of the ramification points [45]. Here $r = 4$, and w has divisor $R_1 + R_2 - R_3 - R_4$, so $[R_1 - R_2]$ and $[R_3 - R_4]$ span M. The group $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ fixes $\{R_1, R_2\}$ and acts on $[R_1 - R_2]$ through the sign of Y_1, that is through χ, and $\omega \mapsto \omega^2$ exchanges the two pairs. (b) By Shapiro's lemma $H^1(K, M) \simeq H^1(F, \mathbb{F}_3(\chi))$, and $\mathbb{F}_3(\chi) \simeq \mu_3 \otimes \chi$ as $\mu_3 \subseteq F$. As $[L : F] = 2$ is prime to 3, inflation and restriction identify this with the χ-part of $H^1(L, \mu_3) = L^\times / L^{\times 3}$. (c) $M^{\mathrm{Gal}(\bar{\mathbb{Q}}/K)} = \mathbb{F}_3(\chi)^{\mathrm{Gal}(\bar{\mathbb{Q}}/F)} = 0$, as $\chi \neq 1$: $[L : \mathbb{Q}] = 56$. (d) The function g_1 on X_ψ has divisor $3(R_1 - R_2)$, because $m - m_1$ vanishes on D at the image of R_1, over which $X_\psi \to D$ is totally ramified, and $m - m_2$ likewise at R_2, while their poles at $m = \infty$ cancel. Over F the cover is a μ_3-cover of $D \simeq \mathbb{P}^1$. By [45], or over K by the Weil-pairing description of [51], the Kummer map of λ is then, up to sign, evaluation of g_1 on divisors, with values in $(L \otimes K')^\times$ modulo cubes; it is normalized at ιQ_0, where $g_1 = 1$. □

So $[L_E : \mathbb{Q}] = 56$, compared with the field of degree 84 needed by a 2-descent [27, §9]: on $J[2]$ the order-3 diamond operators act nontrivially, and the cubic part of ψ remains. For a finite place v of K let $W_v \subseteq H^1(K_v, M)$ be the image of $J(K_v)/\lambda J(K_v)$. By [50, §3], as in the proof of Lemma 12.4(c), $\#W_v = \#J(K_v)[\lambda] \cdot \| \det d\lambda \|_v^{-1}$, and $\det d\lambda = (1 - \zeta_3)(1 - \zeta_3^2) = 3$, because σ acts on the invariant differentials through the two primitive cube roots of unity. With (a) this gives

$$\dim_{\mathbb{F}_3} W_v = h_v + \begin{cases} [K_v : \mathbb{Q}_3] & \text{if } v \mid 3, \\ 0 & \text{otherwise,} \end{cases} \tag{16.2}$$

where $h_v = \dim J(K_v)[\lambda]$ is the number of primes of L above v minus the number of primes of F above v. The curve X_ψ has good reduction outside 2, 3 and 13, so the Selmer group $\mathrm{Sel}^\lambda(J/K)$ is the set of classes in

$$L(S, 3)^- = \{\alpha \in (L^\times / L^{\times 3})^- : \ v_{\mathfrak{P}}(\alpha) \equiv 0 \pmod 3 \text{ for all primes } \mathfrak{P} \nmid 2 \cdot 3 \cdot 13 \text{ of } L\}$$

whose restrictions lie in W_v for every v above 2, 3, 13.

16.4. **The Selmer groups.**

Proposition 16.4. *Suppose that the class number of* L_E *is prime to* 3*. Then* $\mathrm{Sel}^\lambda(J/K)$ *has the dimension in Table 14, its restriction to* $\bigoplus_{v|3} W_v$ *is injective, and it contains the classes of the known points, which span* K_0*. Without the hypothesis, the classes listed span a subgroup of* $\mathrm{Sel}^\lambda(J/K)$ *of that dimension.*

Proof. Let S_L be the set of primes of L above 2, 3, 13. By Dirichlet's S-unit theorem $\mathcal{O}_{L,S}^\times / \mathcal{O}_{L,S}^{\times 3}$ has dimension $\#S_L + 28$, since L is totally complex of degree 56 and $\mu_3 \subseteq L$. PARI's `bnfunits` gives $\#S_L + 28$ elements. Their valuations outside S_L are 0: every factor of their compact representation is integral, and the valuations are checked exactly at every prime dividing the norm of a factor. Their cubic residue characters at 83 to 87 auxiliary primes of degree 1 have full rank. So they are a basis of $\mathcal{O}_{L,S}^\times / \mathcal{O}_{L,S}^{\times 3}$, with no hypothesis. If $3 \nmid h_L$, then $\mathrm{Cl}_S(L)[3] = 0$ and every $\alpha \in L(S, 3)$ is an S-unit times a cube, so these

elements span $L(S,3)$, and $L(S,3)^-$ is the kernel of $\tau+1$ on their span. The local images W_v are spanned by the classes of $g_1(m')$ for slopes $m' \in K$ of explicit K_v-points, whose number is $\dim W_v$ of (16.2) (Table S32). Linear algebra over $\mathbb{F}_3$ gives $\mathrm{Sel}^\lambda(J/K)$ and the restriction (Table S33). The known classes are computed with Proposition 16.3(d). For 96a1, let $c_1 = \delta(Q_0)$ and let c_2, c_3, c_4 be the classes of points over 7301384/3, 97336/81, 140608/3. Then $c_1^2c_2^2c_3^2c_4$ is a cube in L, and the restrictions of c_1, c_2, c_3 to the places above 3 are independent, which gives $\dim K_0 = 3$. Without the hypothesis the computed classes still lie in $L(S,3)^-$ and satisfy the local conditions, and they are independent. □

E	$\lvert\operatorname{disc} K_E\rvert$	(e,f) above 3	$\operatorname{disc} L_E$	$\#S_L$	$\dim L(S,3)^-$	$\dim \mathrm{Sel}$	$\dim K_0$	$\mathrm{Cl}(L_E)$ (GRH)
96a1	$2^{18}3^{12}13^{13}$	$(13,1),(1,1)$	$2^{84}3^{52}13^{54}$	15	18	4	3	$\mathbb{Z}/2$
864a1	$2^{18}3^{14}13^{13}$	$(6,1),(2,1),(3,2)$	$2^{84}3^{60}13^{54}$	17	20	2	1	$\mathbb{Z}/4\times\mathbb{Z}/4\times\mathbb{Z}/2$
864b1	$2^{18}3^{14}13^{13}$	$(6,1),(2,1),(3,2)$	$2^{84}3^{60}13^{54}$	19	20	4	1	$\mathbb{Z}/2$
864c1	$2^{18}3^{14}13^{13}$	$(2,1),(6,1),(3,2)$	$2^{84}3^{60}13^{54}$	19	20	2	1	$\mathbb{Z}/2$

TABLE 14. The fields K_E of degree 14 and L_E of degree 56 for $p = 13$. The discriminants are those of the maximal orders, which are proved maximal. $\#S_L$ is the number of primes of L_E above 2, 3, 13. The dimension of $L(S,3)^-$ equals $\sum_v \dim W_v$ over the places above 2, 3, 13, which is $2+14+2$ for 96a1 and $2+18+0$ for the others (Table S32). $\dim \mathrm{Sel}$ is the dimension of $\mathrm{Sel}^\lambda(J/K)$ under the hypothesis of Theorem D, and K_0 the span of the known classes. The class groups are PARI's values, correct under GRH; Proposition 16.5 proves under GRH that their orders divide 2, 32, 2, 2.

In every case the Selmer group is larger than the span of the known points, by 1, 1, 3, 1 dimensions, so the local analysis cannot be replaced by a comparison with K_0. We do not know whether these extra classes come from points of infinite order or from the Tate–Shafarevich group.

Proposition 16.5. *Assume GRH. Then the class numbers of the four fields L_E divide* 2, 32, 2, 2 *respectively, so they are prime to* 3.

Proof. Let $B_E = 3433, 4931, 4888, 5171$ for $E =$ 96a1, 864a1, 864b1, 864c1. This is the least integer T satisfying the inequality of [3, Corollary 2.2], with its exact constants, for the discriminant, the signature $(0,28)$ and the decomposition of the primes below T in L_E; so under GRH the prime ideals of norm less than B_E generate $\mathrm{Cl}(L_E)$ [3, Corollary 2.2]. For each prime ideal $\mathfrak{P}$ of norm at most B_E (517, 685, 613, 665 prime ideals), we have an exact certificate $\mathfrak{P}\cdot\mathfrak{g}^e = (\alpha)$, where $\mathfrak{g}$ runs over fixed ideals and α is given explicitly, in factored form for three of the fields. Each α is proposed by PARI's `bnfisprincipal`, and the equality of ideals is checked by exact arithmetic. For 96a1, 864b1, 864c1 there is one ideal $\mathfrak{g}$, in the class of a prime of norm 7, 3, 3 whose square is principal (certified the same way), so $\mathrm{Cl}(L_E)$ is generated by one class of order at most 2. For 864a1 there are three ideals $\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$, and the certificates for primes $\mathfrak{P}_{19}$, $\mathfrak{P}_{13}$, $\mathfrak{P}_{283}$ above 19, 13, 283 in the classes of $\mathfrak{g}_1$, $\mathfrak{g}_2$, $\mathfrak{g}_2\mathfrak{g}_3$, together with certificates that $\mathfrak{P}_{19}^4$, $\mathfrak{P}_{13}^4$ and $\mathfrak{P}_{283}^2\mathfrak{P}_{13}^2$ are principal, show that $\mathfrak{g}_1^4$, $\mathfrak{g}_2^4$ and $\mathfrak{g}_3^2$ are principal, so $\#\mathrm{Cl}(L_E)$ divides 32. Table S34 gives the counts. □

17. The exponent 13: the 3-adic analysis

By Lemma 16.2, a solution gives a point $Q \in X_\psi(K)$ with $j(Q) = j_0$ in one of the sets of Theorem 16.1, and the class $\delta(Q)$ of $g_1(m(Q))$, the image of $[Q - \iota Q_0]$, lies in $\mathrm{Sel}^\lambda(J/K)$. We

show that Q is a known point. The local classes at 3 leave only discs that contain a known point, and none for 864c1 (Proposition 17.4); in these discs the 3-adic logarithm decides, near j_E for 864a1 and 864b1 (Proposition 17.7) and near the cusps for 96a1 (Proposition 17.9). Throughout, $\mathfrak{p}$ runs over the primes of K above 3, $n_\mathfrak{p}=[K_\mathfrak{p}:\mathbb{Q}_3]$, $W=\bigoplus_\mathfrak{p} W_\mathfrak{p}$, and $\mathrm{loc}\colon \mathrm{Sel}^\lambda(J/K)\to W$ is the restriction. It is injective when the class number of L_E is prime to 3 (Proposition 16.4), as we assume from now on. Let $\Theta_\mathfrak{p}\subseteq W_\mathfrak{p}$ be the image of the torsion of $J(K_\mathfrak{p})$ and $\Theta=\bigoplus_\mathfrak{p}\Theta_\mathfrak{p}$.

17.1. **Local classes at 3.**

Lemma 17.1. *Let M' be a finite extension of $\mathbb{Q}_3$ and $z\in M'$ with $v_3(z)>3/2$. Then $1+z$ is a cube in M'. Consequently, if $\mathfrak{P}$ is a prime of L above 3 and $g,g'\in L_\mathfrak{P}$ satisfy $v_3(g'-g)-v_3(g)>3/2$, then g and g' have the same valuation and the same class in $L_\mathfrak{P}^\times/L_\mathfrak{P}^{\times 3}$.*

Proof. The coefficient $\binom{1/3}{k}$ has 3-adic valuation $-k-v_3(k!)\ge -k-(k-1)/2$, so the binomial series for $(1+z)^{1/3}$ has terms of valuation at least $k(v_3(z)-3/2)+1/2$ and converges. Apply this to $z=(g'-g)/g$. □

Lemma 17.2. *Let $(v,Y)\in D(K_\mathfrak{p})$ with $v\ne 3\omega, 3\omega^2$. It lifts to a point of $X_\psi(K_\mathfrak{p})$ if and only if $(v-3\omega)/(\gamma(v-3\omega^2))$ is a cube in $F\otimes_K K_\mathfrak{p}$, and then its three lifts form one orbit of σ and have the same class $\delta_\mathfrak{p}$, the class of $g_1(m)$.*

Proof. The points over (v,Y) have $Z=(\omega-\omega^2 w)/(1-w)$ with $w^3=c:=(v-3\omega)/(\gamma(v-3\omega^2))$, and Z is $K_\mathfrak{p}$-rational exactly when $w\in F\otimes K_\mathfrak{p}$ and $w\bar w=1$, where the bar is $\omega\mapsto\omega^2$. As $\gamma\bar\gamma=1$, $c\bar c=1$. If $c=w_0^3$, then $w_0\bar w_0$ is a cube root of unity in $K_\mathfrak{p}$; it is 1 if $\omega\notin K_\mathfrak{p}$, and if $\omega\in K_\mathfrak{p}$ then $F\otimes K_\mathfrak{p}=K_\mathfrak{p}\times K_\mathfrak{p}$ with the bar exchanging the factors, $c=(c_1,1/c_1)$, and $w=(w_1,1/w_1)$ with $w_1^3=c_1$ works. The lifts differ by the cube roots of unity, that is by σ, and g_1 is a function of m, so their classes agree (Proposition 16.3(d)). □

Near $(v_0,1)$ both factors of $g_1(m)$ are small, and we use instead

$$g_1(m)=g_1(m(Q_0))\cdot\frac{(Y+1)(3\omega-v_0)-(Y_1+1)(v-v_0)}{(Y+1)(3\omega-v_0)-(1-Y_1)(v-v_0)},$$

an identity of functions on D: both sides have divisor R_1-R_2 on D (in the image), and they agree at $(v_0,1)$, where m is the tangent slope.

Lemma 17.3. (a) *Let $j_c\in\mathbb{Q}$ and $\kappa\in\mathbb{Q}$ with $v_3(\kappa)>0$, and suppose that* (i)–(iv) *of Section 4.1 and* (4.1) *hold at every root ξ of G_{j_c}, for $F(X,Y)=G_{j_c+\kappa X}(\xi+Y)$ with $e_\xi=1$. Then for $t\in\mathbb{Z}_3$ the roots of $G_{j_c+\kappa t}$ are the values $\xi+\varphi_\xi(t)$ of the branches, with $v_3(\varphi_\xi(t)-\varphi_\xi(t'))\ge\nu_\xi+v_3(t-t')$. If Q is as in Lemma 16.2 with $j(Q)=j_c+\kappa t$, then the image of $v(Q)$ in $K_\mathfrak{p}$ lies on the branch of a root $\xi\in K_\mathfrak{p}$ with $\mathbb{Q}_3(\xi)=K_\mathfrak{p}$.*

(b) *For the leaves $\{3^{12}u\,t^3\}$, the image of $v(Q)$ in $K_\mathfrak{p}$ lies within $3^{-\nu}$ of a root $\rho\in K_\mathfrak{p}$ of $v^4+3v^3+5v^2-4v-4$, where $\nu=v_3(3^{12}u(\rho-1)/\Phi^{[3]}(\rho))/3$ and $\Phi^{[3]}$ is the third Hasse derivative, or $\omega\in K_\mathfrak{p}$ and $v(Q)$ is close to 3ω or $3\omega^2$.*

(c) *For* 96a1, *the image of $1/v(Q)$ in $K_{\mathfrak{p}_1}$, where $\mathfrak{p}_1$ is the prime with $e=13$, is the value at t of the unique $K_{\mathfrak{p}_1}$-rational branch through $1/v=0$ (the remaining root, near $v=1$, lies in $\mathbb{Q}_3$ and does not generate $K_{\mathfrak{p}_1}$, so Lemma 16.2 excludes it), and the image of $v(Q)$ in $K_{\mathfrak{p}_2}=\mathbb{Q}_3$, for the other prime $\mathfrak{p}_2$, satisfies $v_3(v(Q)-1)\ge 10$.*

Proof. (a) is Lemma 4.4 for the polynomial G_j in place of $G_p(x,j)$, with $e=1$. By Lemma 16.2 the image of $v(Q)$ generates $K_\mathfrak{p}$, and it lies in the disc of a root $\xi \in K_\mathfrak{p}$ (Lemma 4.4(c)); the branch has coefficients in $\mathbb{Q}_3(\xi)$, so $K_\mathfrak{p} = \mathbb{Q}_3(v(Q)) \subseteq \mathbb{Q}_3(\xi) \subseteq K_\mathfrak{p}$. (b) Over $j=0$ the fibre consists of 3ω, $3\omega^2$ (simple roots of Φ) and the roots ρ of $v^4+3v^3+5v^2-4v-4$, with multiplicity 3. Here $e_\rho = 3$ is divisible by $\ell = 3$, so only Lemma 4.1 is used, as at $p=19$ (Proposition 8.1): the roots near ρ satisfy $v_3(v-\rho) = \nu + v_3(t)$, and by the separation condition and Krasner's lemma a root in $K_\mathfrak{p}$ lies near a root $\rho \in K_\mathfrak{p}$. If $\omega \notin K_\mathfrak{p}$, a point of $K_\mathfrak{p}$ has $v_3(v-3\omega) \le 3/2$, because $v-3\omega$ and its conjugate $v-3\omega^2$ have the same valuation and differ by $3(\omega^2-\omega)$; the root near 3ω has $v_3(v-3\omega) \ge 21/2$. (c) With $q = 1/v$ and $s = 1/j = 3^{10}t^{13}$, the equation $G_j(v)=0$ becomes $q^{13}(1-q) - s\,\tilde\Phi(q) = 0$ with $\tilde\Phi(q) = q^{14}\Phi(1/q)$, $\tilde\Phi(0)=1$. Lemma 4.2 with $e=13$, which is prime to 3, gives 13 branches $q = \varphi_0(\zeta_{13}^k t)$ with $|\varphi_0(t)| = 3^{-10/13}|t|$. The field $K_{\mathfrak{p}_1}$ is totally ramified of degree 13 with residue field $\mathbb{F}_3$, so its units are 13-th powers and $3^{1/13} \in K_{\mathfrak{p}_1}$, while $\zeta_{13} \notin K_{\mathfrak{p}_1}$: exactly one branch is $K_{\mathfrak{p}_1}$-rational. In $K_{\mathfrak{p}_2} = \mathbb{Q}_3$ the 13 roots near $q=0$ have $v_3(q) = 10/13 + v_3(t) \notin \mathbb{Z}$, and the remaining root is $v = 1 + 13s + \cdots$ by Lemma 4.2 with $e=1$. □

The hypotheses (i)–(iv) and (4.1) are checked exactly in $\mathbb{Q}(\xi)$ at every prime above 3, for every leaf and every root, and for the discs of the known points below; in (b) the separation and $\nu_{3\omega} = 21/2$ are checked in the same way.

For a leaf $\mathcal{L}$ and $\mathfrak{p} \mid 3$ we define a set $D_\mathfrak{p}(\mathcal{L}) \subseteq W_\mathfrak{p}$. If $\mathcal{L}$ is not one of the leaves $\{3^{12}u\,t^3\}$ of Lemma 17.3(b), it is the set of classes of the points of $X_\psi(K_\mathfrak{p})$ over the discs of Lemma 17.3 about the roots that generate $K_\mathfrak{p}$. If $\mathcal{L}$ is one of these leaves and $\omega \in K_\mathfrak{p}$, it is all of $W_\mathfrak{p}$, since Lemma 17.3(b) then allows a point near 3ω or $3\omega^2$. If $\mathcal{L}$ is one of these leaves and $\omega \notin K_\mathfrak{p}$, it is the set of classes of the points of $X_\psi(K_\mathfrak{p})$ over the discs about the roots $\rho \in K_\mathfrak{p}$ of $v^4+3v^3+5v^2-4v-4$. These sets are computed by covering each disc by balls of v-values, deciding on each ball whether the conic points lift (Lemma 17.2), and evaluating g_1 on the ball, which has a constant class once its radius exceeds its valuation by more than $3/2$ (Lemma 17.1); a ball that does not decide is split by the residue of t modulo 3.

Proposition 17.4. *Let Q be as in Lemma 16.2 with $j(Q)$ in a leaf $\mathcal{L}$. Then $\operatorname{loc}\delta(Q) \in \prod_\mathfrak{p} D_\mathfrak{p}(\mathcal{L})$. The leaves for which some element of $\mathrm{Sel}^\lambda(J/K)$ satisfies this are exactly:*

(a) *for* 96a1, *the three leaves with $3 \mid t$, with only the element $-\delta(Q_0)$;*
(b) *for* 864a1, *the leaf $-216+3^7\mathbb{Z}_3$, with only 0 and $\delta(Q_0)$;*
(c) *for* 864b1, *the three leaves $27+3^6t'+3^7\mathbb{Z}_3$, which make up $-13824+3^6\mathbb{Z}_3$, with only 0 and $\delta(Q_0)$;*
(d) *for* 864c1, *none.*

Proof. The first statement follows from Lemmas 17.3, 17.2 and 17.1 and Proposition 16.3(d). The rest compares the sets $D_\mathfrak{p}(\mathcal{L})$ with the $3^{\dim \mathrm{Sel}}$ elements of $\mathrm{Sel}^\lambda(J/K)$. Table S35 gives, for each of the $9+9+13+13$ leaves, the sizes of the sets $D_\mathfrak{p}(\mathcal{L})$ and the result. □

So 864c1 contributes no solution, and for the other curves it remains to treat the discs of (a)–(c), each of which contains the j-invariant of a known point: the cusp $v=\infty$ (where $j=\infty$, that is, $t=0$) for 96a1, and j_E for 864a1 and 864b1.

17.2. **Logarithms and levels.** Let $\mathrm{Log}_\mathfrak{p}\colon J(K_\mathfrak{p}) \to K_\mathfrak{p}^2$ be the logarithm of the 3-adic Lie group $J(K_\mathfrak{p})$ with respect to the invariant differentials ω_1, ω_2 dual to the basis $\mathrm{d}W/y$, $W\mathrm{d}W/y$ of a sextic model $y^2 = f_W(W)$ of X_ψ, with $W = 1/Z$. Its kernel is the torsion and its image $\Lambda_\mathfrak{p}$ is a lattice of rank $2n_\mathfrak{p}$ over $\mathbb{Z}_3$. The automorphism σ acts on (ω_1,ω_2) by the

matrix $\left(\begin{smallmatrix}-1 & -1\\ 1 & 0\end{smallmatrix}\right)$, so $\Lambda_{\mathfrak{p}}$ is a free module of rank $n_{\mathfrak{p}}$ over $\mathbb{Z}_3[\zeta_3]$, a discrete valuation ring with uniformizer λ. We measure levels with $\varpi=\lambda$ as in Section 5.1: the level of $S\in J(K_{\mathfrak{p}})$ modulo torsion is the largest k with $\operatorname{Log}_{\mathfrak{p}} S\in\lambda^k\Lambda_{\mathfrak{p}}$.

Lemma 17.5. (a) *The map $J(K_{\mathfrak{p}})\to\Lambda_{\mathfrak{p}}$ induces an isomorphism $W_{\mathfrak{p}}/\Theta_{\mathfrak{p}}\simeq\Lambda_{\mathfrak{p}}/\lambda\Lambda_{\mathfrak{p}}\simeq\mathbb{F}_3^{n_{\mathfrak{p}}}$, and $\dim\Theta_{\mathfrak{p}}=h_{\mathfrak{p}}$. If the classes of $G_1,\dots,G_s\in J(K_{\mathfrak{p}})$ span $W_{\mathfrak{p}}$, then the $\operatorname{Log}_{\mathfrak{p}} G_i$ generate $\Lambda_{\mathfrak{p}}$ over $\mathbb{Z}_3[\zeta_3]$.*

(b) *Let $u\in\Lambda_{\mathfrak{p}}\setminus\{0\}$, let k be the least valuation of its coordinates in a $\mathbb{Z}_3$-basis, and $u_1=3^{-k}u$. If $u_1\notin\lambda\Lambda_{\mathfrak{p}}$, the level of u is $2k$ and its class at that level is $(-1)^k$ times the class of u_1; otherwise the level is $2k+1$ and the class is $(-1)^k$ times that of $(1-\sigma^2)u_1/3$.*

Proof. (a) As $\Lambda_{\mathfrak{p}}$ is torsion-free, the snake lemma for multiplication by λ on $0\to J(K_{\mathfrak{p}})_{\mathrm{tors}}\to J(K_{\mathfrak{p}})\to\Lambda_{\mathfrak{p}}\to 0$ gives $W_{\mathfrak{p}}\to\Lambda_{\mathfrak{p}}/\lambda\Lambda_{\mathfrak{p}}$ onto with kernel $\Theta_{\mathfrak{p}}$, and $\dim\Theta_{\mathfrak{p}}=(n_{\mathfrak{p}}+h_{\mathfrak{p}})-n_{\mathfrak{p}}$ by (16.2). The rest is Nakayama's lemma. (b) $\lambda^2=-3\zeta_3$ and $\zeta_3\equiv 1\pmod\lambda$, so $u=(-1)^k\zeta_3^{2k}\lambda^{2k}u_1$ with $u_1\notin\lambda^2\Lambda_{\mathfrak{p}}$, and $\lambda^{-1}=(1-\zeta_3^2)/3$. □

The logarithms are computed from integrals of $(\mathrm{d}W, W\,\mathrm{d}W)/y$ along branches of y: if $X=(W_X,y_X)$ is a point and $f_W(W_X+h)/f_W(W_X)=1+\sum_{k=1}^{6}p_kh^k$, then on the disc $v_3(h)>\rho_X=\max_k(-v_3(p_k)/k)$ the points $A=(W_X+h,y)$ on the branch $y=y_X(1+\sum p_kh^k)^{1/2}$ satisfy

$$\operatorname{Log}_{\mathfrak{p}}[A-X]=\int_{W_X}^{W_X+h}(1,W)\,\frac{\mathrm{d}W}{y},\tag{17.1}$$

integrated termwise. Indeed X_ψ has potentially good reduction at 3, being a twist of $X_1(13)$ by a character of finite order, and the open disc lies in one residue disc of a smooth model over a finite extension, on which Log is the formal logarithm; both sides of (17.1) are analytic on the disc with the same derivative and vanish at $h=0$. A general point of $J(K_{\mathfrak{p}})$ is multiplied by an integer k, using Cantor's algorithm, until it is represented by $A-\iota A'$ with A and $\iota A'$ on one such branch, and its logarithm is $1/k$ times the integral. For each $\mathfrak{p}$ the lattice $\Lambda_{\mathfrak{p}}$ is computed from the logarithms of $Q_0-\iota Q_0$ and of points whose classes span $W_{\mathfrak{p}}$, by Lemma 17.5(a), as a Hermite normal form modulo 3^{60}, and $\Theta_{\mathfrak{p}}$ is read off from it. Appendix B.1 explains the error bounds, and Table S36 gives the dimensions of $\Theta_{\mathfrak{p}}$ and the levels used below.

The division argument is Lemma 5.2 with $\varpi=\lambda$, W_v the torsion of $J(K_{\mathfrak{p}})$ and $\Gamma=0$.

Lemma 17.6. *Suppose that $\operatorname{loc}(\mathrm{Sel}^{\lambda}(J/K))\cap\Theta=0$. Let $S\in J(K)$ and $m\ge 0$ with $\operatorname{Log}_{\mathfrak{p}} S\in\lambda^m\Lambda_{\mathfrak{p}}$ for every $\mathfrak{p}\mid 3$. Then the tuple of the classes at level m of $\operatorname{Log}_{\mathfrak{p}} S$, with 0 at the primes where the level exceeds m, lies in $(\operatorname{loc}(\mathrm{Sel}^{\lambda}(J/K))+\Theta)/\Theta$.*

Proof. Condition (L) of Lemma 5.2 holds since λY torsion implies Y torsion. For (G), let $R\in J(K)$ with $R\in\lambda J(K_{\mathfrak{p}})+J(K_{\mathfrak{p}})_{\mathrm{tors}}$ for every $\mathfrak{p}$. Then $\operatorname{loc}\delta(R)\in\operatorname{loc}(\mathrm{Sel})\cap\Theta=0$, so $\delta(R)=0$ by the injectivity of loc (Proposition 16.4), and $R\in\lambda J(K)$. Lemma 5.2 and Lemma 17.5(a) give the statement. □

17.3. **The discs of the known points for 864a1 and 864b1.** Let $E\in\{864\mathrm{a}1, 864\mathrm{b}1\}$ and $\mathcal{D}=j_E+\kappa\mathbb{Z}_3$ the disc of Proposition 17.4(b), (c), with $\kappa=3^7$, 3^6. Let Q be as in Lemma 16.2 with $j(Q)=j_E+\kappa\tau$, $\tau\in\mathbb{Z}_3\cap\mathbb{Q}$.

If $\tau=0$, then $v(Q)$ is a root in K of G_{j_E}, the minimal polynomial of v_0; as $\mathrm{Aut}(K)=1$, $v(Q)=v_0$, and Q is one of the six known points σ^aQ_0, $\sigma^a\iota Q_0$. Let $\tau\neq 0$. By Proposition 17.4,

$\delta(Q) = c'\delta(Q_0)$ with $c' \in \{0,1\}$, so

$$S \coloneqq [Q - \iota Q_0] - c'[Q_0 - \iota Q_0] \in \lambda J(K).$$

At each $\mathfrak{p}$ the image of Q lies on a branch $\tau \mapsto \sigma^a Q_X(\tau)$ through a *centre* X, a $K_\mathfrak{p}$-point of X_ψ over a root of G_{j_E} that generates $K_\mathfrak{p}$ (Lemma 17.3(a), and Lemma 4.2 with $e = 1$ for the cubic equation of W over v). Since $Q_0 + \iota Q_0$ and $\sigma^a(Q_0 + \iota Q_0)$ are linearly equivalent,

$$\operatorname{Log}_\mathfrak{p} S = F_{X,a,c'} + \sigma^a\, l_X(\tau), \qquad l_X(\tau) \coloneqq \operatorname{Log}_\mathfrak{p}[Q_X(\tau) - X] = \sum_{k\geq 1} \gamma_k \tau^k, \tag{17.2}$$

with the *fixed term* $F_{X,a,c'} = \sigma^a \operatorname{Log}_\mathfrak{p}[X - \iota Q_0] - (\sigma^a - 1)L_0/2 - c'L_0$, where $L_0 = \operatorname{Log}_\mathfrak{p}[Q_0 - \iota Q_0]$. The coefficients γ_k have valuation at least an explicit ν_l, by (17.1) composed with the branch. So for $\tau = 3^n u$ the level and class of $\operatorname{Log}_\mathfrak{p} S$ depend only on n and u mod 9 once they are determined at one representative. Beyond an explicit n they are given by $F_{X,a,c'}$ alone, or, if $F_{X,a,c'} = 0$, by $3^n u\,\gamma_1$, with level $2n + \operatorname{lev}(\gamma_1)$ and class $(-1)^n(u \bmod 3)$ times that of γ_1. These are the fixed and branch terms of Section 5.4, now with $\varpi = \lambda$.

Proposition 17.7. *For $E =$ 864a1 and $E =$ 864b1, $\operatorname{loc}(\operatorname{Sel}^\lambda(J/K)) \cap \Theta = 0$, and every choice of centres $(X_\mathfrak{p})$, of a, of $c' \in \{0,1\}$ and of the class of $\tau = 3^n u$ ($n \geq 0$, u mod 9) gives, through Lemma 17.6, a tuple outside $(\operatorname{loc}(\operatorname{Sel}) + \Theta)/\Theta$, or a level 0 at some $\mathfrak{p}$, which contradicts $S \in \lambda J(K)$. So the only points of $X_\psi(K)$ as in Lemma 16.2 over $\mathcal{D}$ are the six known points.*

Proof. For both curves $\dim \Theta = 4$, and $\operatorname{loc}(\operatorname{Sel}) + \Theta$ has dimension $2 + 4$, resp. $4 + 4$, so the sum is direct. The enumeration runs over the three primes above 3 and covers 1512 cases for each curve, all excluded (Table S36); its structure is that of Section 5.4. Beyond the last explicit n the tuple is constant, or constant up to the sign $(-1)^n u$, so finitely many n decide all. □

The known points carry no other solution: $j_0 = -216$ would need $c^{13} = -8b^3$ with $\gcd(b,c) = 1$, which is impossible, and $j_0 = -13824$ gives $(a,b,c) = (\pm 3, -2, 1)$ by Lemma 2.15(a), whose proof does not depend on p.

17.4. **The cusps for 96a1.** Let $E =$ 96a1, so that K has the primes $\mathfrak{p}_1$ ($e = 13$) and $\mathfrak{p}_2$ ($e = f = 1$) above 3, and $h_{\mathfrak{p}_1} = h_{\mathfrak{p}_2} = 0$, so $\Theta = 0$. On the leaves with $3 \mid t$ the class tuple is that of $-\delta(Q_0)$, which lies in $\operatorname{loc}(\operatorname{Sel})$ for every Selmer group, so these leaves need a division argument. Here the known point is a cusp, that is, a point over $j = \infty$.

Lemma 17.8. *For every point C of X_ψ, $2[C - \iota Q_0] - [Q_0 - \iota Q_0] = [C - \iota C]$. If C is a cusp, this class is torsion of order dividing 19^2.*

Proof. $Q_0 + \iota Q_0$ and $C + \iota C$ are linearly equivalent, which gives the identity. If C is a cusp, so is ιC, and over $\bar{K}$, where $X_\psi \simeq X_1(13)$ compatibly with the maps to $X_0(13)$, the class $[C - \iota C]$ lies in the cuspidal subgroup $\mathcal{C}$ of $J_1(13)$, which is finite by the theorem of Manin and Drinfeld. The cusps of $X_1(13)$ are defined over $\mathbb{Q}(\zeta_{13})^+$, so for primes $q \equiv \pm 1 \pmod{13}$ the ℓ-part of $\mathcal{C}$ injects into $J_1(13)(\mathbb{F}_q)$ for $\ell \neq q$. As $\#J_1(13)(\mathbb{F}_{79}) = 2^4 \cdot 19^2$ and $\#J_1(13)(\mathbb{F}_{337}) = 19^4$, $\#\mathcal{C}$ divides 19^2. □

Proposition 17.9. *Let $E =$ 96a1. No point Q as in Lemma 16.2 lies over $j = 3^{-10}t^{-13}$ with $3 \mid t$, $t \neq 0$.*

Proof. Let $t = 3^n u$ with $n \geq 1$, $3 \nmid u$, and $S = 2[Q - \iota Q_0] - [Q_0 - \iota Q_0]$. At each $\mathfrak{p}$, Q lies on the branch of a cusp $C_\mathfrak{p}$ (Lemma 17.3(c)), which is $K_\mathfrak{p}$-rational by the computation

recorded after the proof. By Lemma 17.8, $S = 2[Q - C_{\mathfrak{p}}] + [C_{\mathfrak{p}} - \iota C_{\mathfrak{p}}]$, and the second term is torsion of order prime to 3. So $\mathrm{Log}_{\mathfrak{p}} S = 2\,\mathrm{Log}_{\mathfrak{p}}[Q - C_{\mathfrak{p}}]$ has no fixed term, and is $2\sigma^a l_X(t)$ at $\mathfrak{p}_1$ and $2\sigma^a l_X(t^{13})$ at $\mathfrak{p}_2$, for a centre X over the cusp. At $\mathfrak{p}_1$ the tangent vector γ_1 of each of the two centres has level 0, so $\mathrm{Log}_{\mathfrak{p}_1} S$ has level $2n$ and class $\pm(u \bmod 3)\,\mathrm{cl}(\gamma_1)$; at $\mathfrak{p}_2$ the level is $18 + 26n$. In particular S has infinite order. Lemma 17.6, with $m = 2n$, puts $\pm(\mathrm{cl}(\gamma_1), 0)$ in loc(Sel), and for both centres it is not there (Table S36). The 72 cases ($n = 1, 2, 3$, u mod 9, two centres at each prime) are all excluded, and beyond $n = 1$ the cases repeat up to sign. □

At $\mathfrak{p}_1$ all six cusps over $v = \infty$ are $K_{\mathfrak{p}_1}$-rational with class $2\delta_{\mathfrak{p}_1}(Q_0)$, and at $\mathfrak{p}_2$ the six cusps over $v = 1$ have class $0 = \delta_{\mathfrak{p}_2}(Q_0)$, in agreement with Lemma 17.8. The factor 2 in the definition of S is needed. With $S' = [Q - \iota Q_0] - 2[Q_0 - \iota Q_0]$ the fixed term is $-\frac{3}{2}\,\mathrm{Log}_{\mathfrak{p}}[Q_0 - \iota Q_0]$; for $v_3(t) \geq 2$ it alone attains the least level, at $\mathfrak{p}_1$, and the tuple is $\pm \mathrm{loc}\,\delta(Q_0)$, which lies in every Selmer group.

17.5. **Proof of Theorem D.** Let (a, b, c) be a primitive solution of $x^2 + y^3 = z^{13}$ with $abc \neq 0$, and assume that the class numbers of the four fields L_E are prime to 3. By Theorem 16.1 and Lemma 16.2 it gives a point $Q \in X_\psi(K_E)$ for one of the four curves, with $j(Q) = j_0$ in one of the leaves, and $\delta(Q) \in \mathrm{Sel}^\lambda(J/K)$ of Proposition 16.4. By Proposition 17.4, $E \neq$ 864c1; for 96a1, $3 \mid t$, which Proposition 17.9 excludes; for 864a1 and 864b1, $j_0 \in j_E + \kappa\mathbb{Z}_3$, and Proposition 17.7 shows that Q is a known point, so $j_0 = j_E$. The case $j_0 = -216$ is impossible and $j_0 = -13824$ gives the Catalan solutions. The solutions with $abc = 0$ are the trivial ones. Under GRH the hypothesis holds by Proposition 16.5. For $n = 26$, a primitive solution (x, y, z) gives the solution (x, y, z^2) for 13, and $z^2 \in \{0, 1\}$, which gives the list of Theorem D (Corollary E). □

18. The exponents that remain

Up to 36, only the exponent 31 remains open; the exponents 13, 23, 26 and 29 are settled under GRH. We explain why the methods of this paper do not reach 31, and then discuss the non-split Cartan curves, the hypotheses of Theorems B and D, and the infinite family of Bennett, Chen, Dahmen and Yazdani.

18.1. **The exponent 31.** For $p = 31$ the reduction of Freitas, Naskręcki and Stoll leaves the twists attached to 54a1 (through 54a2), 96a1, 288a1, 864a1, 864b1 and 864c1 [27, Theorem 5.1 and Lemma 6.1(1)]. The curve $X_0(31)$ has genus 2, and the cuspidal subgroup of $J_0(31)$ has order $\ell = 5$. The Hecke algebra is the ring of integers of $\mathbb{Q}(\sqrt{5})$, in which 5 ramifies: the Eisenstein prime $\lambda = (\sqrt{5})$ satisfies $\lambda^2 = (5)$. So the parts of Sections 3 and 5 that use the splitting $\mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda \times \mathcal{O}_\mu$ would need an argument for a ramified Eisenstein prime. For one twist there is a further obstruction, which holds without GRH.

Remark 18.1. Let $E =$ 864b1, the curve $y^2 = x^3 - 24x + 48$, and let $K = K_E$ be the field of degree 32 attached to E and $p = 31$. Then 5 divides the class number of K, so the descent of Proposition 3.14, which needs $\ell \nmid h_K$, is not available for this twist at $p = 31$.

We sketch the proof. The curve E has j-invariant -13824, the j-invariant of the Frey curves of the Catalan solutions, and good supersingular reduction at 31, since $a_{31}(E) = 0$. Its mod 31 representation $\bar{\rho}_E$ is surjective onto $\mathrm{GL}_2(\mathbb{F}_{31})$. The field K is the field of definition of a line $C \subset E[31]$, so G_K acts on C and on $E[31]/C$ through characters a and d, and $\rho = a/d$ maps G_K onto $\mathbb{F}_{31}^\times$. Then ρ^6 has order 5, and it is unramified at every place of K. At places above primes $q \notin \{2, 3, 31\}$ this holds because E has good reduction at q. At

places above 2 and 3 the reduction of E is potentially good, so the image of inertia has order dividing 24 [54], and a homomorphism from it to a group of order 5 is trivial. At 31 the image of inertia in $\mathrm{GL}_2(\mathbb{F}_{31})$ is a non-split Cartan subgroup [52, §1.11, Proposition 12], which meets the stabilizer of C only in the scalars, where $a = d$. The real places map to the identity because ρ^6 has odd order. So the fixed field of the kernel of ρ^6 is an unramified cyclic extension of K of degree 5, and by class field theory 5 divides the class number of K.

18.2. **Non-split Cartan curves.** The twists attached to curves with complex multiplication could also be treated through non-split Cartan modular curves, as in Proposition 2.2. The curve 288a1 has complex multiplication by $\mathbb{Z}[i]$, and 19 is inert in $\mathbb{Q}(i)$, so the image of its mod 19 representation lies in the normalizer of a non-split Cartan subgroup. As in the proof of Proposition 2.2, a primitive solution with $abc \neq 0$ that gives a rational point on $X_{288\mathrm{a}1}(19)$ or on $X^-_{288\mathrm{a}1}(19)$ gives a non-cuspidal rational point of $X^+_{\mathrm{ns}}(19)$ with j-invariant j_0. Balakrishnan, Müller and Vonk have announced in a conference lecture, without a preprint so far, that the non-cuspidal rational points of $X^+_{\mathrm{ns}}(19)$ are CM points [41]. With Lemma 2.15(a) this would give a second proof for these two twists, which Section 8.5 excludes without it. In the same way a primitive solution on a twist attached to 27a1 or 288a1 at $p = 23$, or to 27a1 at $p = 29$, gives a rational point on $X^+_{\mathrm{ns}}(p)$, since p is inert in the field of complex multiplication, and a determination of $X^+_{\mathrm{ns}}(23)(\mathbb{Q})$ and $X^+_{\mathrm{ns}}(29)(\mathbb{Q})$ would remove these twists.

18.3. **The hypotheses of Theorems B and D.** Theorem B becomes unconditional once its hypotheses on the class numbers of the eight fields of degree 24 and 30 are proved, and Theorem D once the class numbers of the four fields L_E of degree 56 are proved prime to 3. For the eight fields of Theorem B the criterion of Belabas, Diaz y Diaz and Friedman (Proposition A.1) applies as it stands. A numerical evaluation of (A.1) indicates that the criterion would need bounds X up to about 10^{12} at $p = 23$ and between about 10^{13} and 10^{15} at $p = 29$, against at most $3.2 \cdot 10^8$ for the fields of Table 15. For the fields L_E the certificates of Proposition 16.5 already cover every prime ideal below the bound B_E of Belabas, Diaz y Diaz and Friedman under GRH; without GRH one needs instead a bound such as that of Proposition A.1, which we have not evaluated for these fields. The rest of the proof of Theorem D, including the S-unit groups, uses no hypothesis.

18.4. **An infinite family.** Bennett, Chen, Dahmen and Yazdani prove that for every prime $p \equiv 1 \pmod 8$ the only primitive solutions of $x^2 + y^3 = z^{3p}$ with $xyz \neq 0$ are $(\pm 3, -2, 1)$ [4, Theorem 1.1], which they state for $a^3 + b^{3p} = c^2$, with $x = c$, $y = -a$, $z = b$. It follows from their Propositions 1.2 and 1.3: for primes $p \equiv 1, 3 \pmod 8$ with $p \geq 17$ there is no other solution with x odd, and for primes $p \equiv 1 \pmod 4$ with $p \geq 17$ none with x even [4]. Their family, whose smallest exponent is $51 = 3 \cdot 17$, meets ours only there, and Corollary E also covers it. Conversely, Corollary E gives all multiples of 11, 17 and 19, and, under the hypothesis of Theorem B(a), respectively (b), of 23 and 29, and, under that of Theorem D, of 13. Among them are $3p$ for $p = 11$, 13, 19, 23 and 29, which are not in their family.

Appendix A. Class groups and units without GRH

We prove here without GRH the statements on class groups and S-units that the descents use: $\ell \nmid h_{K_E}$ for the μ_ℓ-descents of Sections 3.2 and 3.3 and for the fields of the CM curves at $p = 23$ and 29, the class groups of the fields $K_E(i)$ of the 2-descent of Section 3.4, and the corresponding statements for the fields of Part III and of the reduction of Freitas and

Stoll (Appendix A.7). With them, Lemma 3.5 identifies each group $K(S,\ell)$ with an explicit group of S-units.

Each statement is proved with explicit elements (generators of principal ideals, relations between prime ideals, S-units), except for one real number per field, which is enclosed by ball arithmetic. The elements were found with PARI's `bnfinit`, `bnfisprincipal` and `bnfunits`, whose output is proved correct only under GRH, and the proofs use only the elements themselves. The programs of [32] produce these elements and check them; the coefficients a_j below and the bases of S-units of the fields $L_{i'}$ and $M_{i'}$ of Appendix A.7 are stored there. The orders used were proved maximal with PARI's `nfcertify`.

A.1. **The explicit-formula criterion.** Minkowski's bound for the fields K_E of degrees 18 and 20 exceeds 10^{11}, so we use the following unconditional criterion, deduced by Belabas, Diaz y Diaz and Friedman from Weil's explicit formula in the form given by Poitou [44]. Let K be a number field of degree n with r_1 real places and discriminant d_K, and let γ be Euler's constant. Let $c > 0$, $J \geq 1$ and $a_0, \dots, a_{J-1} \in \mathbb{R}$, not all zero. Let $h(y) = \sum_{j<J} a_j \cos(2\pi j y/c)$ for $|y| \leq c/2$ and $h(y) = 0$ otherwise, and $g = h * h$. Put $k(x) = r_1/(1+\cosh x) + n/\sinh x$ for $x > 0$ and

$$R = r_1 + n(\gamma + \log 4\pi) - \log|d_K| - \int_0^\infty \Big(1 - \frac{g(x)}{g(0)}\Big) k(x)\,dx + \sum_{\mathfrak{p}} \sum_{\substack{m \geq 1 \\ \mathrm{N}\,\mathfrak{p}^m < e^c}} \frac{4\log \mathrm{N}\,\mathfrak{p}}{\mathrm{N}\,\mathfrak{p}^m + 1} \frac{g(m \log \mathrm{N}\,\mathfrak{p})}{g(0)}, \tag{A.1}$$

where $\mathfrak{p}$ runs over the prime ideals of K.

Proposition A.1 ([3, Theorem 5.1])**.** *If $R > 0$, then the classes of the prime ideals of K of norm less than e^c generate the class group of K.*

This is [3, Theorem 5.1] with $T = e^c$ and the test function $f = g/g(0)$ restricted to $[0,\infty)$: since $2\cosh^2(x/2) = 1 + \cosh x$, their inequality (16) is $R > 0$. The hypotheses of that theorem hold: f is supported on $[0,c]$ with $f(0) = 1$, its Fourier cosine transform is $\hat{h}^2/g(0) \geq 0$, and $f(x)/\cosh(x/2)$ is even, continuous, compactly supported and piecewise real-analytic.

We evaluate (A.1) in ball arithmetic (Arb [33], through python-flint), with g given by a closed formula. The integral is enclosed by Arb's numerical integration on $[\epsilon, c]$, with a Lipschitz bound on $[0,\epsilon]$ and the tail on $[c,\infty)$ computed exactly. The prime sum runs over the prime ideals obtained by factoring every rational prime below $X = e^c$ in the maximal order. The coefficients a_j, found by numerical optimization, are exact decimal numbers with eight digits, so R is a well-defined real number. Its enclosures have radius at most $7.1 \cdot 10^{-6}$, and Table 15 lists their lower bounds. The smallest lower bound is 0.257677, for $K_{864\mathrm{b}1}$ at $p = 19$. The prime ideals of norm less than X are then placed in a known subgroup of $\mathrm{Cl}(K)$ by the following induction on the norm.

Lemma A.2. *Let G be a finite set of prime ideals of K, $H \subseteq \mathrm{Cl}(K)$ the subgroup generated by their classes, and $X > 1$. Suppose that each prime ideal $\mathfrak{p}$ of K with $\mathrm{N}\,\mathfrak{p} < X$ satisfies one of the following:* (i) *$(\alpha) = \mathfrak{p}\prod_{\mathfrak{q}\in G}\mathfrak{q}^{a_\mathfrak{q}}$ for some $\alpha \in K^\times$ and integers $a_\mathfrak{q}$;* (ii) *there is $\beta \in \mathfrak{p}$ with $|\mathrm{N}\,\beta| = \mathrm{N}\,\mathfrak{p}\cdot q$, where q is prime to $\mathrm{N}\,\mathfrak{p}$ and every prime power exactly dividing q is smaller than $\mathrm{N}\,\mathfrak{p}$. Then the class of every prime ideal of norm less than X lies in H.*

Proof. By induction on $\mathrm{N}\,\mathfrak{p}$. In case (i) the class of $\mathfrak{p}$ lies in H. In case (ii), $(\beta) = \mathfrak{p}\mathfrak{a}$ with $\mathrm{N}\,\mathfrak{a} = q$, and every prime factor of $\mathfrak{a}$ has norm smaller than $\mathrm{N}\,\mathfrak{p}$, so its class lies in H by induction, and so does that of $\mathfrak{p}$. □

In the applications, (i) is used for all prime ideals of norm at most 1000 (at most 100 for the field k' of Proposition A.13(e)), with the identity checked by comparing Hermite normal forms. For the others (ii) is used, or (i) where no β was found. If moreover $R > 0$ for this X, then $\mathrm{Cl}(K) = H$ by Proposition A.1. We refer to this as *the criterion with G and X*. To bound $\#H$, we give for each $\mathfrak{q} \in G$ an element $a \in \mathcal{O}_K$ with $(a) = \mathfrak{q}^{m_\mathfrak{q}}$; then $\#H$ divides $\prod_\mathfrak{q} m_\mathfrak{q}$.

A.2. **The fields of degree 12.** For $p = 11$ the descent of Section 3.2 needs $5 \nmid h_K$ for the five fields K_E of degree 12, and a basis of $K(S, 5)$, with S the primes above 11.

Proposition A.3. *The five fields K_E of degree 12 ($p = 11$) have class number 1 (for 54a1 and 96a1) or dividing 2 (for 864a1, 864b1, 864c1). In particular 5 does not divide their class numbers.*

Proof. Here $n = 12$, $r_1 = 2$, $|d_K|$ is as in Table 6, $X = 10^5$, and h is the indicator function of $[-c/2, c/2]$ ($J = 1$, $a_0 = 1$). Then $R > 0$ by Table 15. Every prime ideal $\mathfrak{p}$ of norm less than 10^5 satisfies $\mathfrak{p} = \mathfrak{g}^e(\alpha)$ with $e \in \{0, 1\}$, where $\mathfrak{g} = (1)$ for the first two fields, and for the other three $\mathfrak{g}$ is a fixed ideal, not necessarily prime, whose square is principal. □

Proposition A.4. *Let K be one of the five fields of degree 12 and S the set of primes above 11. The $6 + \#S$ elements used to compute $\mathrm{Sel}^{\hat\psi}(J'/K)$ in Proposition 3.7 are S-units, and together with -1 they generate $\mathcal{O}_{K,S}^\times$ up to an index prime to 5. Hence their classes form a basis of $K(S, 5)$.*

Proof. Each element and its inverse have coordinates on an integral basis whose denominators are powers of 11, and norms that are $\pm$ powers of 11, so they are S-units. Their images in $\bigoplus_\mathfrak{q}(\mathcal{O}_K/\mathfrak{q})^\times/(\mathcal{O}_K/\mathfrak{q})^{\times 5}$, for eight or nine prime ideals $\mathfrak{q}$ with $\mathrm{N}\,\mathfrak{q} \equiv 1 \pmod 5$ lying above rational primes $q \le 71$, have rank $6 + \#S$, the S-unit rank. So no nontrivial product of them is a fifth power in K, and since the only fifth roots of ± 1 in K are ± 1, the index of the group they generate with -1 is prime to 5. Since $5 \nmid h_K$ (Proposition A.3) and $\mu_5 \not\subset K$, Lemma 3.5 shows that their classes form a basis of $K(S, 5) = \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 5}$. □

A.3. **The fields of degree 18.** The 2-descent of Section 3.4 runs over the fields $K_E(i)$, whose class groups Appendix A.4 controls through two facts on the fields K_E of degree 18.

Proposition A.5. *The fields K_E of degree 18 for $E \in \{864a1, 864b1, 864c1\}$ have class number 1.*

Proof. Here $n = 18$, $r_1 = 2$ and $|d_K| = 2^{24}3^{20}17^{17}$. Apply the criterion with $G = \emptyset$, $J = 20$ and $X = 10^6$, 10^6, $4 \cdot 10^6$ respectively (Table 15). □

Proposition A.6. *Let $K = K_{54a1}$ of degree 18 ($p = 17$), with defining polynomial as in Appendix C.2 and root ϑ, and let S'' be the set of places consisting of the infinite places, the two primes above 2, the prime above 17, $\mathfrak{q}_0 = (11, \vartheta - 7)$ and $\mathfrak{q}_1 = (37, \vartheta - 18)$. Then the classes of the primes of S'' generate $\mathrm{Cl}(K)$.*

Proof. Here $|d_K| = 2^{16}3^{20}17^{17}$. Apply the criterion with G the finite primes of S'', $J = 20$ and $X = 3 \cdot 10^6$ (Table 15). □

A.4. **Chevalley's formula and the fields $K_E(i)$.** We control the class group of $L = K(i)$, of degree 36, from K with Chevalley's ambiguous class number formula [15] (see [36, Theorem 1] for the classical case and [30, Chapter II, §6] for S-class groups). Let L/K be a cyclic extension of prime degree ℓ with group G, and S a finite set of places of K containing

n	K	$[K:\mathbb{Q}]$	X	$\mathrm{N}\mathfrak{p} < X$	$\mathrm{N}\mathfrak{p} > B$	$R >$	generators (exponents)	conclusion
11	54a1	12	10^5	9595	—	13.085492	—	$h = 1$
	96a1	12	10^5	9675	—	6.254350	—	$h = 1$
	864a1	12	10^5	9614	—	5.688776	$\mathfrak{g}$ (2)	$h \mid 2$
	864b1	12	10^5	9527	—	0.886518	$\mathfrak{g}$ (2)	$h \mid 2$
	864c1	12	10^5	9683	—	2.527361	$\mathfrak{g}$ (2)	$h \mid 2$
17	864a1	18	10^6	78566	78378	1.763978	—	$h = 1$
	864b1	18	10^6	78498	78311	2.188267	—	$h = 1$
	864c1	18	$4 \cdot 10^6$	283405	283219	0.834767	—	$h = 1$
	54a1	18	$3 \cdot 10^6$	217220	217043	1.488264	primes of S''	$\mathrm{Cl}(K) = \langle S'' \rangle$
19	54a1	20	$2 \cdot 10^7$	1270510	1270345	1.314076	—	$h = 1$
	96a1	20	$3 \cdot 10^7$	1859537	1859343	0.635184	—	$h = 1$
	864a1	20	$8 \cdot 10^7$	4667820	4667622	0.532766	$\mathfrak{q}_{864a1}$ (2)	$h \mid 2$
	864b1	20	$3.2 \cdot 10^8$	17277460	17277291	0.257677	$\mathfrak{q}_{864b1}$ (2)	$h \mid 2$
	864c1	20	$4 \cdot 10^7$	2434931	2434751	0.649884	$\mathfrak{q}_{864c1}$ (2)	$h \mid 2$
	288a1	20	10^6	78309	78098	1.837294	four primes (2 each)	$h \mid 2^4$
23	27a1	24	10^6	78245	78093	10.407623	$\mathfrak{q}_5$ (3)	$h \mid 3$
	288a1	24	$3 \cdot 10^7$	1855542	1855355	0.539967	$\mathfrak{q}_2, \mathfrak{q}_2', \mathfrak{q}_2''$ (2), $\mathfrak{q}_3$ (4), $\mathfrak{q}_7$ (4)	$h \mid 2^7$
29	27a1	30	10^6	78478	78321	1.729112	$\mathfrak{q}_2$ (3)	$h \mid 3$
25	K_5	6	10^3	163	0	10.985976	—	$h = 1$
	K_6	6	10^3	163	0	12.595593	—	$h = 1$
	K_{16}	6	10^3	159	0	10.706858	—	$h = 1$
	K_{22}	6	10^3	162	0	11.938416	—	$h = 1$
	K_{24}	6	10^3	154	0	10.983394	—	$h = 1$
	L_5	12	10^4	1319	1159	7.295487	$\mathfrak{q}_2$ (2)	$h \mid 2$
	L_6	12	10^4	1160	1002	13.886526	—	$h = 1$
	L_{16}	12	10^4	1237	1078	9.238815	$\mathfrak{q}_2$ (2)	$h \mid 2$
	L_{22}	12	10^4	1233	1076	14.812176	—	$h = 1$
	L_{24}	12	10^4	1257	1100	9.842936	$\mathfrak{q}_2$ (2)	$h \mid 2$
	M_5	24	$2 \cdot 10^5$	18025	17862	2.204795	$\mathfrak{q}_2$ (2)	$h \mid 2$
	M_6	24	10^4	1107	964	8.601433	—	$h = 1$
	M_{16}	24	$5 \cdot 10^4$	5065	4930	4.986347	$\mathfrak{q}_2$ (2)	$h \mid 2$
	M_{22}	24	10^4	1182	1052	10.460123	—	$h = 1$
	M_{24}	24	$5 \cdot 10^4$	4863	4708	5.283617	$\mathfrak{q}_2$ (2)	$h \mid 2$
	k'	20	$2 \cdot 10^5$	17985	17964	1.929993	$\mathfrak{G}_1, \mathfrak{G}_2$ (3)	$\mathrm{Cl}(K) \simeq (\mathbb{Z}/3)^2$

TABLE 15. The class group computations of Appendix A: the exponent n; the field K (the field K_E for the curve E when n is prime, the fields of Appendix A.7 when $n = 25$); its degree; the bound $X = e^c$ of Proposition A.1; the number of prime ideals $\mathfrak{p}$ of norm less than X, and of those of norm greater than B, which are handled by relations, where $B = 1000$, except $B = 100$ for k'; the lower bound for R given by ball arithmetic; the ideals $\mathfrak{q}$ whose classes generate $\mathrm{Cl}(K)$ (with the exponent m such that $\mathfrak{q}^m$ is principal; a dash means that $\mathrm{Cl}(K)$ is trivial), as in Propositions A.3, A.5, A.6, A.9, A.12 and A.13; and the conclusion, with $h = \#\,\mathrm{Cl}(K)$. For $n = 11$ every prime ideal is written directly as $\mathfrak{g}^e(\alpha)$, and $J = 1$; in all other rows $J = 20$. For k' the relations reduce every prime ideal to the 21 of norm at most 100.

the infinite places. Let Cl_S be the S-class group (for K the class group modulo the classes of the primes in S, for L modulo those of the primes above S), h_S its order, and $\mathcal{O}_{K,S}^\times$ the group of S-units. Then

$$\#\,\mathrm{Cl}_S(L)^G = h_S(K)\cdot \frac{\prod_{v\notin S} e_v \cdot \prod_{v\in S} n_v}{\ell\cdot[\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S}^\times \cap \mathrm{N}_{L/K}\, L^\times]}, \tag{A.2}$$

where e_v is the ramification index and n_v the local degree of L/K at v. For $L = K(i)$ and $\ell = 2$, Hasse's norm theorem identifies $\mathcal{O}_{K,S}^\times \cap \mathrm{N}_{L/K}\, L^\times$ with the S-units ε whose Hilbert symbols $(\varepsilon, -1)_v$ are 1 at every place v that does not split in L and, if $v \notin S$, ramifies. By the product formula the image of $\mathcal{O}_{K,S}^\times$ under $\varepsilon \mapsto ((\varepsilon,-1)_v)_v$, with v running over these places, lies in a hyperplane of $\bigoplus_v \{\pm 1\}$.

Proposition A.7. (a) *For $E \in \{864\mathrm{a}1, 864\mathrm{b}1, 864\mathrm{c}1\}$ and $L = K_E(i)$, the class group of L has odd order.*

(b) *For $K = K_{54\mathrm{a}1}$, $L = K(i)$ and S'' as in Proposition A.6, the S''-class group of L has odd order.*

Proof. (a) Take S to be the infinite places. The places of K that ramify in L are the two real places and exactly one prime above 2, the one with $(e, f) = (2, 2)$. The units of K realize every sign pattern at the two real places, so the Hilbert symbol map on $\mathcal{O}_K^\times$ has rank 2, the maximum allowed by the product formula, and (A.2) gives $\#\,\mathrm{Cl}(L)^G = 1\cdot 2^3/(2\cdot 2^2) = 1$ by Proposition A.5. A nontrivial finite 2-group with an action of $G \simeq \mathbb{Z}/2$ has a nontrivial fixed point, so $\mathrm{Cl}(L)[2^\infty] = 0$.

(b) The places of S'' that do not split in L are the two real places, the two primes above 2 (both ramified) and $\mathfrak{q}_0$ (inert, since -1 is not a square in $\mathbb{F}_{11}$). The prime above 17 and $\mathfrak{q}_1$ split, and no place outside S'' ramifies. Fifteen explicit S''-units of K, namely -1, nine units and five further S''-units, have Hilbert symbols of rank 4 at these five places, the maximum. By Proposition A.6, $h_{S''}(K) = 1$, and (A.2) gives $\#\,\mathrm{Cl}_{S''}(L)^G = 2^5/(2\cdot 2^4) = 1$. As in (a), $\mathrm{Cl}_{S''}(L)[2^\infty] = 0$. □

Proposition A.8. (a) *For $E \in \{864\mathrm{a}1, 864\mathrm{b}1, 864\mathrm{c}1\}$, $L = K_E(i)$ and S the primes above 2 and 17, $L(S,2) = \mathcal{O}_{L,S}^\times/\mathcal{O}_{L,S}^{\times 2}$ has dimension 28, and the 28 elements used to compute $\mathrm{Sel}^2(J/K_E)$ are S-units forming a basis of it.*

(b) *For $K = K_{54\mathrm{a}1}$, $L = K(i)$ and S the primes above 2 and 17, $L(S,2)$ has dimension 23, and the 23 elements used to compute $\mathrm{Sel}^2(J/K)$ form a basis of it.*

In particular the Selmer groups of Proposition 3.11 are determined without GRH.

Proof. (a) By Proposition A.7(a), $\mathrm{Cl}_S(L)[2] = 0$, so the exact sequence $0 \to \mathcal{O}_{L,S}^\times/2 \to L(S,2) \to \mathrm{Cl}_S(L)[2] \to 0$ gives $L(S,2) = \mathcal{O}_{L,S}^\times/2$. As L is totally complex of degree 36 with $\mu(L) = \mu_4$ and has ten primes above 2 and 17, this group has dimension $17 + 1 + 10 = 28$. Each of the 28 elements is a product of integer powers of explicit elements of L and has valuation zero at every prime not above 2 or 17, as the factorizations of the norms and denominators of the factors show. The quadratic residue characters of the 28 elements at 32 to 38 primes of L of degree one have $\mathbb{F}_2$-rank 28, so they are independent modulo squares and form a basis.

(b) By Proposition A.7(b), $L(S'',2) = \mathcal{O}_{L,S''}^\times/2$, of dimension $18 + 7 = 25$, as L has seven primes above the finite places of S''. An element of $L(S'',2)$ lies in $L(S,2)$ if and only if its valuations at the three primes of L above $\mathfrak{q}_0, \mathfrak{q}_1$ are even. Two explicit S''-units of L have parity vectors $(1,0,0)$ and $(0,1,1)$ there, so $\dim L(S,2) \le 23$. The 23 elements used for the

descent have even valuation at every prime outside S, and their quadratic residue characters show that they are independent modulo squares, so they form a basis.

The proofs of Propositions 7.6 and 7.7 use a second basis of $L(S,2)$, consisting of S-units expressed in a different defining polynomial of L. Its elements are supported on S and their quadratic residue characters have full rank, so it is a basis as well and gives the same Selmer group. □

A.5. **The fields of degree 20.** The descent of Section 3.3 runs over the six fields K_E of degree 20 of Table 6, including K_{288a1} (Proposition 2.9). Each has signature $(2,9)$, so its unit rank is 10 and its only roots of unity are ± 1.

Proposition A.9. *Let $K = K_E$ be one of the six fields of degree 20.*

(a) *If $E \in \{54a1, 96a1\}$, then K has class number 1.*

(b) *If $E \in \{864a1, 864b1, 864c1\}$, then $\mathrm{Cl}(K)$ is generated by the class of one prime ideal $\mathfrak{q}_E$ whose square is principal, so the class number of K divides 2. Here $\mathfrak{q}_E$ is the prime above 3 with $(e,f) = (6,1)$ for 864a1, the prime above 3 with $(e,f) = (2,1)$ for 864b1, and the prime above 2 with $(e,f) = (4,1)$ for 864c1. In each case it is the only prime of K of its type.*

(c) *If $E = 288a1$, then $\mathrm{Cl}(K)$ is generated by the classes of four prime ideals whose squares are principal: the prime above 2 with $(e,f) = (4,1)$, the two primes above 2 with $(e,f) = (4,2)$, and the prime above 3 of degree 1 whose completion contains μ_3 (the place v_1 of Proposition 8.5). So $\mathrm{Cl}(K)$ is an elementary abelian 2-group of order dividing 16.*

In particular 3 does not divide the class number of any of the six fields.

Proof. Let G be the set of prime ideals named in the statement ($G = \emptyset$ in (a)). For each $\mathfrak{q} \in G$ an element $a \in \mathcal{O}_K$ with $v_\mathfrak{q}(a) = 2$ and $|\mathrm{N}\, a| = \mathrm{N}\, \mathfrak{q}^2$ gives $(a) = \mathfrak{q}^2$. Apply the criterion with G, $J = 20$ and the bound X of Table 15. □

Proposition A.10. *Let $K = K_E$ be one of the six fields of degree 20, and S the set of primes of K above 3 and 19, so $\#S = 5, 4, 5, 5, 5, 7$ for $E = 54a1, 96a1, 864a1, 864b1, 864c1, 288a1$. The $10 + \#S$ elements used to compute $\mathrm{Sel}(K)$ in Proposition 3.8 are S-units, and their classes form a basis of $\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 3}$. This group equals $K(S,3)$, of dimension $10 + \#S$.*

Proof. The elements are given as products of integer powers of explicit elements of K. At each prime of K above a prime $l \notin \{3, 19\}$ dividing the norm or the denominator of a factor, the valuation of each element, computed factor by factor, is 0. All such l are at most 35677 and proved prime. At the other primes outside S every factor is a unit. So the elements are S-units.

We use 19 to 28 primes $\mathfrak{q}$ of degree one of K, above primes $q \equiv 1 \pmod 3$ between 10007 and 10657, at which all the factors are units. The cubic residue characters $u \mapsto u^{(q-1)/3} \in \mu_3(\mathbb{F}_q)$ at these primes have $\mathbb{F}_3$-rank $10 + \#S$ on the elements. Since $3 \nmid h_K$ (Proposition A.9) and $\mu_3 \not\subset K$, Lemma 3.5 shows that the classes of the elements form a basis of $\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times 3} = K(S,3)$. □

Corollary A.11. *Proposition 3.8 holds without GRH for the six fields of degree 20. In particular the groups $\mathrm{Sel}(K)$ and their images Σ at the places above 3, used in Section 8, are determined without GRH.*

Proof. The proof of Proposition 3.8 computes $\mathrm{Sel}(K)$ inside $K(S,3)$ from the local conditions at the places above 3, which are spanned by classes of explicit points of $J(K_v)$. Its

only global input is a basis of $K(S,3)$, given by Proposition A.10. The group $\mathrm{Sel}(K) = \mathcal{O}_{K,S_{19}}^{\times}/\mathcal{O}_{K,S_{19}}^{\times 3}$ used for $K_{96\mathrm{a}1}$ in Proposition 8.4, with S_{19} the primes above 19, is described in Proposition 3.8(b), whose proof uses only Proposition 3.8(a), $3 \nmid h_K$ and Lemma 3.5. □

A.6. **The fields of the curves with complex multiplication at $p = 23$ and 29.** The descents of Sections 9 and 10 need $\ell \nmid h_K$, with $\ell = 11$ for $p = 23$ and $\ell = 7$ for $p = 29$. For the fields of the curves without complex multiplication this is the hypothesis of Theorem B (Section 18).

Proposition A.12. *Let $K = K_E$ be as in Proposition 2.8.*

(a) *For $p = 23$ and $E = 27\mathrm{a}1$, $\mathrm{Cl}(K)$ is generated by the class of a prime ideal $\mathfrak{q}_5$ of degree one above 5, and $\mathfrak{q}_5^3$ is principal. Either of the two prime ideals of degree one above 5 can be taken, since the automorphism ι_K of K exchanges them. So the class number of K is 1 or 3, and 11 does not divide it.*

(b) *For $p = 29$ and $E = 27\mathrm{a}1$, $\mathrm{Cl}(K)$ is generated by the class of one of the fifteen prime ideals $\mathfrak{q}_2$ above 2, which all have residue degree 2, and $\mathfrak{q}_2^3$ is principal. So the class number of K is 1 or 3, and 7 does not divide it.*

(c) *For $p = 23$ and $E = 288\mathrm{a}1$, $\mathrm{Cl}(K)$ is generated by the classes of the three prime ideals $\mathfrak{q}_2, \mathfrak{q}_2', \mathfrak{q}_2''$ above 2, which all have $(e,f) = (4,2)$, of one of the six prime ideals $\mathfrak{q}_3$ above 3, which all have $(e,f) = (2,2)$, and of a prime ideal $\mathfrak{q}_7$ of degree one above 7. The ideals $\mathfrak{q}_2^2$, $\mathfrak{q}_2'^2$, $\mathfrak{q}_2''^2$, $\mathfrak{q}_3^4$ and $\mathfrak{q}_7^4$ are principal. So the class number of K divides 2^7, and 11 does not divide it.*

In particular the hypothesis $\ell \nmid h_K$ of Proposition 3.14 and Remark 3.19 holds for these three fields without GRH.

Proof. The field K is defined by $G_p(x, -12288000)$ in (a) and (b) and by $m_{288}^{(23)}$ in (c) (Proposition 2.8 and Appendix C.2). It has degree 24, 30, 24 and signature $(2,11)$, $(2,14)$, $(2,11)$, and its discriminant is $-3^{28}23^{23}$, $3^{34}29^{29}$, $-2^{36}3^{12}23^{23}$ respectively. Let G be the set of prime ideals named in the statement, with $m_{\mathfrak{q}} = 3$ in (a) and (b), and $m_{\mathfrak{q}} = 2,2,2,4,4$ in (c), so $\prod_{\mathfrak{q}} m_{\mathfrak{q}}$ is 3, 3 and 2^7. Apply the criterion with G, $J = 20$ and $X = 10^6$ in (a) and (b), $3 \cdot 10^7$ in (c) (Table 15). In (a), ι_K acts on $\mathrm{Cl}(K)$ as an automorphism and maps the class of $\mathfrak{q}_5$ to that of the other prime of degree one above 5, which therefore also generates $\mathrm{Cl}(K)$. □

A.7. **The fields of Part III and of the reduction of Freitas and Stoll.** Part III uses class groups and units of the fields L and $M = L(\sqrt{5})$ of its descents (Section 12), of the sextic fields K of [28, §9] (Lemma 11.3), and of the fields of the 2-descents of Freitas and Stoll [28] and Stoll [64, Theorem 9.1] (Proposition 11.4 and Lemma 11.5). For $i' \in \{5,6,16,22,24\}$ let $K_{i'}$, $L_{i'}$ and $F_{i'} = L_{i'}(\zeta_5)$ be the fields of Tables S18 and S19, and $M_{i'} = L_{i'}(\sqrt{5})$. Let $S_{i'}$ be the set of rational primes $\{2,3,5\}$ for $i' \in \{22,24\}$, $\{2,3,5,1657\}$ for $i' = 16$, $\{2,3,5,47\}$ for $i' = 6$ and $\{2,3,5,2281\}$ for $i' = 5$, and for a field K' let $K'(S_{i'},5)$ be the group of classes in $K'^{\times}/K'^{\times 5}$ with valuation divisible by 5 at every prime of K' not above $S_{i'}$.

Proposition A.13. (a) *For $i' \in \{6,22\}$ the fields $L_{i'}$ and $M_{i'}$ have class number 1. For $i' \in \{5,16,24\}$ the class group of $L_{i'}$, and that of $M_{i'}$, is generated by the class of one prime ideal above 2 whose square is principal, of type $(e,f) = (4,1)$ in L_5 and L_{24}, $(4,2)$ in L_{16}, and $(4,2)$ in M_5, M_{16}, M_{24}. In particular 5 does not divide the class numbers of these ten fields.*

(b) *The five sextic fields $K_{i'}$ have class number* 1. *Each has signature* $(2, 2)$, *and three explicit units of $K_{i'}$ whose fifth-power residue characters have $\mathbb{F}_5$-rank* 3 *span $\mathcal{O}^\times_{K_{i'}}/\mathcal{O}^{\times 5}_{K_{i'}}$, of dimension* 3.

(c) *For $K' \in \{L_{i'}, M_{i'}\}$, the $r_1+r_2-1+\#S'$ elements of K' used in Proposition 12.6, where S' is the set of primes of K' above $S_{i'}$, are S'-units, and their classes form a basis of $K'(S_{i'}, 5) = \mathcal{O}^\times_{K',S'}/\mathcal{O}^{\times 5}_{K',S'}$. The same holds, with the same S', for the $23 = 15 + 8$ and $46 = 15 + 31$ elements of M_{22} and M_5 used for the second descent (Proposition 15.2).*

(d) *For the eight fields K of Table 16,* $\mathrm{Cl}(K)$ *is the group given there, $\mu(K) = \{\pm 1\}$, the classes of the primes of S generate* $\mathrm{Cl}(K)$, *and $r_1 + r_2 + \#S$ explicit S-units form a basis of $K(S, 2) = \mathcal{O}^\times_{K,S}/\mathcal{O}^{\times 2}_{K,S}$, where S is the set of primes of K above the rational primes of Table 16.*

(e) *The field k' of the proof of Proposition 11.4, of degree* 20, *signature* $(0, 10)$ *and discriminant $2^{20}5^{38}$, has $\mathrm{Cl}(k') \simeq (\mathbb{Z}/3)^2$, generated by the classes of prime ideals $\mathfrak{G}_1$, $\mathfrak{G}_2$ of norms* 9 *and* 29 *whose cubes are principal. With S the set of the eleven primes of k' above* 2, 3 *and* 5, *explicit S-units form a basis of $k'(S, 2) = \mathcal{O}^\times_{k',S}/\mathcal{O}^{\times 2}_{k',S}$, of dimension* 21.

K	used in	M_K	$\mathrm{N}\,\mathfrak{p} \le M_K$	$\mathrm{Cl}(K)$	S above	$\dim K(S,2)$
$\mathbb{Q}(\sqrt[5]{10})$	[28, §6], $y^2 = x^5 + 2^8 5^3$	348.0	73	1	2, 5	5
$\mathbb{Q}(\sqrt[5]{20})$	[28, §6], $y^2 = x^5 + 2^6 5^3$	348.0	68	1	2, 5	5
K_4	[28, §7], M_3, M_4	4.2	1	1	2, 3, 5	7
K_5	[28, §7], M_3, M_4	214.7	46	1	2, 3, 5	10
$\mathbb{Q}(\sqrt{5})$	[28, §7], $y^2 = x^3 + x^2 - 83x + 88$	1.1	0	1	2, 5	4
$k_{\pm 1}$	[28, §8], $D_{\pm 1}$	169698.8	15504	$\mathbb{Z}/2$	2, 3, 5, 7	16
$k_{\pm 2}$	[28, §8], $D_{\pm 2}$	169698.8	15599	$\mathbb{Z}/2$	2, 3, 5, 7, 43	20
k	[64, Theorem 9.1], D_0	169698.8	15534	$\mathbb{Z}/6$	2, 3, 5	12

TABLE 16. The fields of the 2-descents of Freitas and Stoll (Proposition A.13(d)): Minkowski's bound M_K and the number of prime ideals of norm at most M_K, each written in terms of the generators of $\mathrm{Cl}(K)$; the class group; the rational primes below S; and the dimension of $K(S, 2) = \mathcal{O}^\times_{K,S}/\mathcal{O}^{\times 2}_{K,S}$. Here K_4 and K_5 are defined by $t^4 - 5t^2 + 5$ and $t^5 - 25t^3 + 125t - 110$, and $k_{\pm 1}$, $k_{\pm 2}$ and k by $t^{10} + 75t^6 - 20t^5 + 150t^3 + 625t^2 + 500t + 145$, $t^{10} + 75t^6 - 10t^5 + 625t^2 + 250t + 25$ and $t^{10} + 75t^6 - 50t^5 + 100t^3 + 625t^2 + 1250t + 645$.

The field $M_{i'} = L_{i'}(\sqrt{5})$ has degree 24 because $\sqrt{5} \notin L_{i'}$. The fields of (d) are the fields $\mathbb{Q}[x]/(g)$ for the irreducible factors g of the defining polynomials of the curves named in Table 16.

Proof. (a), (b). Apply the criterion with G the named prime ideal ($m_{\mathfrak{q}} = 2$) or $G = \emptyset$, $J = 20$ and the bounds X of Table 15: 10^3 for the sextic fields, 10^4 for the fields $L_{i'}$, and between 10^4 and $2 \cdot 10^5$ for the fields $M_{i'}$. The three units of (b) are integral of norm ± 1. Since $K_{i'}$ has a real place, $\mu(K_{i'}) = \{\pm 1\}$ and $\mathcal{O}^\times_{K_{i'}}/\mathcal{O}^{\times 5}_{K_{i'}} \simeq (\mathbb{Z}/5)^3$, so three units independent modulo fifth powers span it.

(c) Each element is supported on S', as the factorization of the ideal it generates shows, and the number of elements is $r_1 + r_2 - 1 + \#S'$. Their fifth-power residue characters at

between 15 and 50 primes of K' of degree one have full rank. The fields $L_{i'}$ and $M_{i'}$ have real places, so $\mu_5 \not\subset K'$, and $5 \nmid h_{K'}$ by (a), so Lemma 3.5 applies.

(d) Minkowski's bound M_K is given in Table 16. The first five fields have a real place, and in the three totally complex fields of degree 10 no cyclotomic polynomial Φ_m with $m > 2$ and $\varphi(m) \mid 10$ has a root, so $\mu(K) = \{\pm 1\}$ for all eight. For each prime ideal $\mathfrak{p}$ of norm at most M_K an identity $\mathfrak{p} = (a_\mathfrak{p}) \prod_i \mathfrak{g}_i^{e_i}$ with fixed ideals $\mathfrak{g}_i$ is checked by comparing Hermite normal forms, and $\mathfrak{g}_i^{c_i} = (b_i)$ is checked in the same way. So $\mathrm{Cl}(K)$ is a quotient of $\prod_i \mathbb{Z}/c_i$. For the lower bound, fix a prime ℓ dividing some c_i. The elements b_i with $\ell \mid c_i$, together with $r_1 + r_2 - 1$ units and, for $\ell = 2$, also -1, are independent modulo ℓ-th powers, as their ℓ-th power residue characters at primes of degree one show. They lie in $K(\emptyset, \ell)$, and the exact sequence $0 \to \mathcal{O}_K^\times/\mathcal{O}_K^{\times\ell} \to K(\emptyset,\ell) \to \mathrm{Cl}(K)[\ell] \to 0$ gives $\dim \mathrm{Cl}(K)[\ell] \geq \#\{i : \ell \mid c_i\}$. The primes of S are written as $(a)\prod_i \mathfrak{g}_i^{e_i}$ in the same way, and their classes generate $\mathrm{Cl}(K)$, so $\mathrm{Cl}_S(K) = 0$. The given elements are S-units, as the factorizations of the ideals they generate show, and their quadratic residue characters have rank $r_1 + r_2 + \#S$, which is the dimension of $\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ because $\mu(K) = \{\pm 1\}$. Finally $K(S,2) = \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S}^{\times 2}$ because $\mathrm{Cl}_S(K)[2] = 0$.

(e) Apply the criterion with $G = \{\mathfrak{G}_1, \mathfrak{G}_2\}$, $m_\mathfrak{q} = 3$, $J = 20$ and $X = 2 \cdot 10^5$ (Table 15), with (i) of Lemma A.2 for the 21 prime ideals of norm at most 100. So $\mathrm{Cl}(k')$ is a quotient of $(\mathbb{Z}/3)^2$. Let $\mathfrak{G}_i^3 = (\gamma_i)$. The field has unit rank 9 and $\mu(k') = \mu_4$, and nine units together with γ_1, γ_2 have cubic residue characters of $\mathbb{F}_3$-rank 11 at 36 primes of norm up to 541. They lie in $k'(\emptyset, 3)$, and the exact sequence $0 \to \mathcal{O}_{k'}^\times/\mathcal{O}_{k'}^{\times 3} \to k'(\emptyset,3) \to \mathrm{Cl}(k')[3] \to 0$ gives $\dim \mathrm{Cl}(k')[3] \geq 2$. So $\mathrm{Cl}(k') \simeq (\mathbb{Z}/3)^2$, of odd order, and $k'(S,2) = \mathcal{O}_{k',S}^\times/\mathcal{O}_{k',S}^{\times 2}$, of dimension $9 + 11 + 1 = 21$. The given elements are S-units, as the factorizations of the ideals they generate show, and their quadratic residue characters have rank 21. □

Appendix B. Computations

Table S31 in the Supplement lists the computational statements and what is computed for each. The computations used PARI/GP 2.17.3 [43], PARI/GP 2.19.0 (for the fields of degree 56 of Part IV), SageMath 10.9 [49] (for (M1), the repetition in a second system and the minimal models and one archimedean constant in the repetition of [27, §7.1], all in Appendix B.2), Python 3.12 with python-flint 0.8 (FLINT 3.3 and Arb [23, 33]) and NumPy, and one program in C. Most computations take between a second and a few minutes on one processor core. The class group and S-unit computations for the fields of degree 56 of Part IV, which propose the S-units of Proposition 16.4 and the generators α of Proposition 16.5, ran for several days on a server. Apart from these, the longest are the class group certificates for the fields of degree 20 (Appendix A.5), which treat about 27.6 million prime ideals in 8.6 hours. For the class groups of the fields of degree 56 we adapted PARI's search for relations, since in these fields almost every relation found is fixed up to sign by the automorphism τ of Section 16.3 and so gives only units of F; the checks that PARI applies to the result are unchanged.

B.1. **Exactness and error control.** The computations are exact except for the ℓ-adic points and logarithms in the four settings below, which carry proven error bounds, and the real numbers R of Appendix A.1, which are enclosed in ball arithmetic.

Exact computations. Everything else is computed with integers, rationals, number fields given by explicit polynomials (through their maximal orders, proved maximal as in Appendix A) and finite rings: the q-expansions and the j-maps, the branch conditions of Section 4.1 (valuations of explicit elements), the Selmer groups with Σ, Θ, Θ_T, their dimensions and

all membership tests (linear algebra over $\mathbb{F}_\ell$ with entries computed from explicit elements), the counts of configurations, the sieves and the orders of $\widetilde{J}$ over finite fields. In Part III the following are also exact: the identities of Lemmas 11.8 and 12.1 and Proposition 15.1 (of polynomials or rational functions) and the refinements of $\mathbb{P}^1(\mathbb{Z}_p)$ into residue classes in Propositions 12.8 and 12.9, with the criterion of Section 12.3 and the Taylor coefficients φ_n of Φ at each representative (Section 12.4), followed by an enumeration of the $5^{\dim \mathrm{Sel}}$ elements of Sel. For $p = 23$ and 29, $y^2 - F(x)$ vanishes in the q-expansions to order at least 400, and $j - (\mathcal{A}_p + \mathcal{B}_p y)$ and $f - (f_0 + f_1 y)$ to order at least 390. The class groups of the fields K_E at $p = 23$ and 29 other than those of Proposition A.12 are PARI's values, correct under GRH, which enter Theorem B as hypotheses. PARI gives the same values for two different defining polynomials of each field. The S-units of F in Part III are explicit elements, in factored form, so the Selmer groups computed from them over F are contained in the true ones, and Lemma 12.5 and Proposition 12.6 show that they are equal. These elements are checked to be S-units by factoring the ideals they generate, or their norms and denominators.

Genus one: $p = 11$, 17, 19. Roots of polynomials in the completions K_v are located by a search over residue classes and checked with Hensel's inequality $v(G(\tilde{x})) > 2v(G'(\tilde{x}))$, which gives a root x with $v(x - \tilde{x}) \geq v(G(\tilde{x})) - v(G'(\tilde{x}))$. This precision is far above the constancy radius of Section 4.3: for example it is at least 120 in the normalized valuation of K_{v_2} in Proposition 7.5, where about 3 in v_2-units suffices, and at least 50 in the 5-adic tests, where 2 suffices. So by Lemmas 4.7, 4.8 and 4.6 the class of the root is computed exactly from the approximation. In the computations at the known points (Propositions 7.6, 7.7, 8.3 and 8.10) each local quantity (points of $J(K_v)$, their sums, Log_v) is carried as a pair (z, N). Here z is an exact element of K, or of a number field of degree n_v approximating K_v, and N is a proven lower bound for the valuation of the error, propagated through addition, multiplication, inversion, the group law and the map from the formal group to J. The formal logarithm is truncated with a proven bound for the tail: $v(c_k t^k) \geq km - e_v \log_2 k$ for $v(t) = m > e_v$ at $\ell = 2$, and similarly at $\ell = 3$. Coordinates of Log_v on $\mathcal{O}_v$ are taken modulo a power of ℓ well below the proven precision, and a level or class is used only if it lies below that precision. The lattice Λ_v is spanned by the logarithms of explicit points: either points whose classes span $\delta_v(J(K_v))$, which suffices by Nakayama's lemma (Section 5.2 and Lemma 5.6), or points of the formal group with parameters $\omega_j \pi^i$ (ω_j lifts of a basis of the residue field, π a uniformizer) together with points whose reductions generate $\widetilde{J}(k_v)$. The group Θ_v is read off from the relations modulo ℓ. For 864b1 at $p = 17$ the proven precision of Log_v is at least 59 binary digits and the lattice coordinates are determined modulo 2^{47}, while the levels used are at most 7. For 864c1 the coordinates are taken modulo 2^{40}.

Genus two: $p = 23$, 29. A class $\delta_v(Q)$ depends only on $f(Q)$ modulo ℓ^2, hence on $x(Q)$ and $y(Q)$ modulo ℓ^2. For $p = 23$ and the curves without complex multiplication the completions are modelled as $(\mathbb{Z}/11^M)[x]/(g_v)$, where $G_{23}(x, j_E) \equiv \prod_v g_v \pmod{11^M}$ is a Hensel-lifted factorization, checked by multiplying out, with $M = 3$ and with $M = 5$, which give the same class tuples. For $p = 29$ they are modelled as the finite rings $\mathcal{O}_K/v^{10}$, with classes computed by discrete logarithms in $(\mathcal{O}_K/v^2)^\times$. Roots of $G_p(x, j_1)$ are found in the residue field and lifted by Newton's iteration to roots modulo the working precision. Since G_p' is a unit at the roots in the unramified discs, and $v(G_p(\tilde{x})) > 2v(G_p'(\tilde{x}))$ in the ramified region at $p = 29$, Hensel's lemma gives a true root congruent to it modulo a power of ℓ well above ℓ^2. Every inverse is checked by multiplication, so the class tuples are exact. For 27a1 and 288a1 at $p = 23$ the fibre points in the ramified regions are simple roots, lifted by Newton's iteration,

and by Hensel's lemma each lifted value agrees with a true root to the stated precision: for 27a1 in exact integer arithmetic modulo 11^{40}, with at least 24 correct digits, and for 288a1 with PARI's p-adic numbers, which carry their precision, with at least 37 correct digits at the input of the class map. The disc tests enumerate all admissible configurations over each representative. For the fields with $2 \cdot 11! \cdot 2^{11}$ configurations per disc the meet-in-the-middle search of Section 4.4 splits the places into seven and six, or eight and five, and rechecks each configuration found; each such search takes at most eighteen minutes on one processor core.

For 27a1 ($p = 23$) the logarithms Log_v were computed in integer arithmetic modulo 11^N ($N = 40$ and 60). For $X \in J(K_v)$ the multiple $m'X$, with $m' = \#\widetilde{J}(k_v)/11$ as in Section 9.4, is computed with Cantor's algorithm on a model with a Weierstrass point W at infinity, as $m'X + D$ for an auxiliary divisor $D = (Q_1) + (Q_2) - 2(W)$. Every element inverted is a unit, so an input error of 11^{-e} gives an output error of at most 11^{-e}. The result is a divisor $(P_1) + (P_2) - 2(W)$, and $\log_\lambda(m'X) = \int_{Q_1}^{P_1} \omega_\lambda + \int_{Q_2}^{P_2} \omega_\lambda$ is a sum of integrals within residue discs, computed from the power series of ω_λ truncated at degree 45. The omitted terms have valuation at least 47, and the divisions by $n \le 46$ lose at most one digit on terms of valuation at least 11. The total error is at most 11^{-24}, and the tests use Log_v only modulo 11^3 (its valuation, at most 2, and its leading digit). For 288a1 the same construction was carried out with PARI's p-adic numbers, from inputs known modulo 11^{250}, with series truncated after 150 terms (omitted terms of valuation at least 149), and every logarithm used is correct modulo 11^{149}. For $p = 23$ the maps N_v of Lemma 3.16(F3) are the identity of k_v, that is, $\delta_v(R) = \log_\lambda(R)/11 \bmod 11$ for $R \in \widehat{J}(11\mathcal{O}_v)$. From the polynomials f_0, f_1 of Lemma 2.5(c) (Appendix C.1) one checks that $f_0' + (x+3)f_1$ and $f_1'F + f_1F'/2 + (x+3)f_0$ vanish modulo 11, that is, $df/f \equiv -\omega_\lambda \pmod{11}$. So if $Q, Q' \in X_0(23)(K_v)$ lie in one residue disc, $u = f(Q)/f(Q')$ satisfies $\log u \equiv -\log_\lambda[Q - Q'] \pmod{121}$, and its class $(u^{q_v-1} - 1)/11 \equiv (q_v - 1)\log(u)/11$ is $\log_\lambda[Q - Q']/11 \bmod 11$. Such differences span $\widehat{J}(11\mathcal{O}_v)/\lambda\widehat{J}(11\mathcal{O}_v) \simeq k_v$. At a point Q with $(\omega_\lambda/dx)(\tilde{Q}) \neq 0$, the points Q' of its residue disc with $x(Q') = x(Q) + 11c$, for $c = 1$ and $c = t$ with $k_v = \mathbb{F}_{11}(t)$, give leading digits $c \cdot (\omega_\lambda/dx)(\tilde{Q})$, which span k_v. For $p = 29$ the proofs use only that N_v exists.

Part III. A local image $W_\mathfrak{p}$ is computed as the span of the classes of explicit divisors. At primes not above 5 these are points with $Y \in F$ and $Y^2 - \beta$ a fifth power in $F_\mathfrak{p}$, tested exactly. At primes above 5 they are points with a chosen $X \in F$ and Y computed by Newton's method to a precision exceeding $v_\mathfrak{p}(Y - \sqrt{\beta}) + k_\mathfrak{p}$, which determines the class of $Y - \sqrt{\beta}$ (Section 12.3). Classes in $F_\mathfrak{p}^\times / F_\mathfrak{p}^{\times 5}$ are given by the valuation modulo 5 and discrete logarithms in $(\mathcal{O}_F/\mathfrak{p}^{k_\mathfrak{p}})^\times$. In every case the span reached the dimension of Lemma 12.4(c), so it is all of $W_\mathfrak{p}$. For each row of Table S20, let $G_1, \dots, G_r$ be the points (and, for $\mathcal{D}$ with $i' = 5$, two divisors of degree 2) whose classes, together with $\kappa_\mathfrak{P}(T_\pi)$, span $W_\mathfrak{P}$. Their logarithms are computed with Lemma 13.4, with error bounded by its truncation bound and the 5-adic precision of the arithmetic, which PARI tracks. The logarithms used are known to at least 24 5-adic digits, and in most computations to more than 80. The lattice basis matrix has size $4r \times 4r$ over $\mathbb{Q}_5$. Its inverse, computed within this precision, has entries of valuation at least -1, which gives $5\mathcal{O}_\mathfrak{P}^2 \subseteq \Lambda$, and for $\mathcal{C}$ with $i' = 22$ also $\pi\mathcal{O}_\mathfrak{P}^2 \subseteq \Lambda$. The vector γ_1 was computed as an element of F^2, as the derivative at $s = 0$ of the family (Lemma 13.3), and $\gamma_2, \gamma_3, \dots$ from the power series of the family. The level and the class of γ_1 need its lattice coordinates only modulo 5^2, and the levels of $\gamma_2, \dots, \gamma_5$ only modulo 5^6, far below the precision reached. For $i' = 24$ the logarithms of the generators were computed from tiny integrals (Lemma 13.3) of explicit divisors representing $5[G_k - \infty]$, with the number of

terms chosen from an explicit lower bound for the decay of the terms. The proofs use only logarithms so obtained, with explicit error bounds.

The exponent 13. The completions $K_{\mathfrak{p}}$ at the primes above 3 in Section 17 are modelled with PARI's 3-adic numbers as coefficients in a basis of $\mathcal{O}_{\mathfrak{p}}$, so PARI tracks the precision of every local quantity. Roots of polynomials over K are computed in exact arithmetic in K and certified by Hensel's lemma to $v_3 \geq 190$. Every Newton iteration used to find a root in local arithmetic has its precision lowered to what Hensel's lemma certifies. In Cantor's algorithm on $J(K_{\mathfrak{p}})$ every decision that a coefficient is nonzero is certified at the current precision. The series in (17.1) is summed either to a number of terms chosen from the margin $v_3(h) - \rho_X$, so that the omitted terms have $v_3 \geq 40$, or to a fixed number of terms (300 or 400) with an explicit bound for the tail. The logarithms of the generators of the lattices $\Lambda_{\mathfrak{p}}$ are known with errors of valuation at least 51 at the primes of 864a1 and 864b1, and at least 35 and 330/13 at the primes of 96a1 with $e = 1$ and $e = 13$. After scaling by a power of 3 (at most 3^4), let 3^s be the index of the lattice in $\mathbb{Z}_3^{2n_{\mathfrak{p}}}$ and $3^{e'}$ the exponent of the quotient; in every case $s \leq 36$ and $e' \leq 2$. The program checks that $60 > s + 2$, so that the Hermite normal form modulo 3^{60} is that of $\Lambda_{\mathfrak{p}}$, and that the valuations of the scaled errors exceed e' by at least 1, so that these errors lie in $3\Lambda_{\mathfrak{p}}$ and, by Nakayama's lemma, do not change the lattice. A level or class is used only when its error bound determines it. The largest level used is 44, at the prime of 96a1 with $K_{\mathfrak{p}} = \mathbb{Q}_3$, where the logarithms compared have error bound 23 (enough, since a level $2k$ needs only precision $k + 1$, Section 17.2).

B.2. **Repetition.** Every computation on which a proof depends, except (M1) and (M2) below and some of those for $p = 13$, was carried out by two separately written programs, with the same results. These programs, and the SageMath programs below, have a common origin (see the Declarations). They share the definitions in the text but use different models of the fields (K_E, $K_E(i)$, L and F), other S-unit generators, other coordinates for the local classes (Hilbert symbols, residue characters or explicit bases of the unit filtration instead of discrete logarithms), other generators of the local images, other root finders, and other constructions of the lattices Λ_v and Λ. The table below lists the decisive computations and how each was repeated: by a second program, in a second computer algebra system (SageMath), or, where there is no second program, by running the same program again.

Computation	Second program	SageMath	Run again
Mordell–Weil groups behind Proposition 2.3	yes	minimal models only	–
Elliptic Chabauty of [27, §7.1]	yes	no	–
Selmer groups, disc tests and sieves for $p = 11$, 17, 19, 23, 29	yes	one case for each p	–
Known points at $p = 17$, 19: Propositions 7.6, 7.7, 8.3 and 8.10	yes	no	–
Known points at $p = 23$, 29: Propositions 9.6, 9.10 and 10.1	yes	parts of Propositions 9.6 and 10.1	–
Class group certificates of Appendix A	yes	no	–
Part III: Selmer groups, sieve and discs, Propositions 12.6, 12.8 and 12.9	yes	parts, for $i' = 16$	–
Part III: logarithms, lattices and levels, Sections 14 and 15	yes	no	–
(M1) and (M2) in Theorem 11.6	in part	(M1) in part	–
Part IV: Selmer groups, Proposition 16.4	yes	no	–
Part IV: the bound B_E of Proposition 16.5	yes	no	–

Computation	Second program	SageMath	Run again
Part IV: the certificates of Proposition 16.5 for 96a1	yes	no	–
Part IV: the other certificates of Proposition 16.5	no	no	no
Part IV: 3-adic logarithms, lattices and levels, Propositions 17.7 and 17.9	yes, in SageMath	yes	–
Part IV: enumerations, Propositions 17.4, 17.7 and 17.9	no	no	yes

A dash in the last column means that the computation was repeated, in whole or in part, by a second program.

The j-maps for $p = 17$ and 19 were checked against the classical modular polynomials ($\Phi_p(j(P), j(w_pP)) = 0$ at random points over finite fields), and for $p = 19$ also against the analytic modular parametrization. The models of $X_0(23)$ and $X_0(29)$ were rebuilt from other bases of $S_2(\Gamma_0(p))$. At $p = 23$ and 29 the class tuples were also computed ℓ-adically with PARI's p-adic numbers, which carry their precision. In the lines of [27, Tables 1 and 2] used in Section 4, the description of j was confirmed by a direct computation; the assignment of the lines to the curves E is used as published. The class group certificates were repeated with a second enumeration of the prime ideals, a second evaluation of R and a second check of the relations. At $p = 23$, one program obtained four 11-adic logarithms in Proposition 9.10(c): those of the fixed terms $\Gamma_v = \pm[\eta_1 - \eta_2]$ at the two places of degree two where $\delta_v(\eta_1) = \delta_v(\eta_2)$. The other program excluded the same configurations without them. A third program computes $\mathrm{Log}_v X$ as $\log_\lambda (m(X + A) - mA)/m$ for an auxiliary class A defined over the unramified extension of $\mathbb{Q}_{11}$ of degree 6, in arithmetic modulo 11^{30}. It finds $v_{11}(\mathrm{Log}_v \Gamma_v) = 2$ at both places, with the same leading digits as the first program, and $v_{11}(\mathrm{Log}_v[\eta_1 - \eta_2]) = 1$ at the other eleven places, with leading digit $\delta_v(\eta_1) - \delta_v(\eta_2)$ (Remark 9.11).

Repetition in SageMath. One decisive case of each of the prime exponents 11, 17, 19, 23 and 29, and part of one case of the exponent 25, was computed again in SageMath [49], by programs written from the text of this paper, not from the PARI programs. They take from [32] the defining polynomials of the fields, the j-maps and the bases of $K(S, \ell)$, of $L(S, 2)$ and, for $p = 25$, of Sel. The two S-unit bases for 27a1 and some auxiliary elements and embeddings of the fields were computed again with PARI and then checked in SageMath. The programs prove that the basis elements are S-units for $p = 11$, 23, 29, and for $p = 17$, 19 except at the places above the prime factors of two, respectively one, large unfactored divisors of the denominators with which the elements are written. At those places they check only that the norm of each basis element is prime to the divisor. For $p = 25$ they do not check that the basis elements are S-units. In every case they prove that the basis elements are independent. That these generate the whole group rests on Appendix A, and for $p = 25$ on Proposition 12.6(a). Everything else in the cases below is recomputed, with the completions constructed by MacLane's algorithm or as unramified extensions in FLINT. For $p = 23$, 29 the models, the j-maps and the functions f are checked against q-expansions. The statements confirmed in this way are the following. For 864a1 at $p = 11$: Proposition 6.2 (500 configurations, two tuples in Σ) and Proposition 6.3 (the first failure is at $q = 31$). For 864a1 at $p = 17$: $\dim \mathrm{Sel}^2(J/K) = 11$ with injective restriction at 2 (Proposition 3.11), and the class sets and class tuples of Proposition 7.2. For 864c1 at $p = 19$: $\dim \mathrm{Sel}(K) = 12$ (Proposition 3.8), and the ranks and the class tuples of the nine families in Proposition 8.1(a)

and its proof. For 27a1 at $p=23$: Proposition 9.6(a), (c), (d), (e) and the numbers of configurations, patterns and Selmer classes in (b), by a search through all admissible configurations. For 27a1 at $p=29$: the dimensions of Proposition 10.1(a), the numbers in its rows of Table 11, and (d). For the curve with $i'=16$ at $p=25$: Proposition 12.6(b)–(d) at $\mathfrak{P}$ for the span of the three basis elements of Sel, the single element of this span passing the test at 5, namely $\kappa(P_0-\infty)$ (Proposition 12.8), and the 30 residue classes and $\mathcal{R}=25\mathbb{Z}_5$ (Proposition 12.9 and its proof). The branch conditions of Section 4.1 for $p=17$ and 19 were not repeated in SageMath.

The two Magma computations of [28]. Freitas and Stoll determine $C_1(\mathbb{Q})$, for $C_1\colon y^2=x^5+2^8\cdot5^3$, with Magma's Mordell–Weil and Chabauty routines [28, §6], and bound the ranks of $J_{-1}(\mathbb{Q})$ and $J_{-2}(\mathbb{Q})$ by 2 with Magma's rank bound [28, §8]. Here J_j is the Jacobian of the curve $\tilde{D}_j\colon y^2=F_j(x)$ of genus 4 of [28, p. 15], with $\deg F_j=10$ and square leading coefficient. In Magma versions before V2.29 the saturation step of the class group algorithm could be switched off by an error [22, §1]. We recomputed both results without Magma and without GRH: the first, (M1) below, with SageMath 10.9 and PARI/GP, and the second, (M2), with PARI/GP.

(M1) Let J be the Jacobian of C_1 and $P=[(-4,176)-\infty]$. By the 2-descent of (iii) in the proof of Theorem 11.6, $\operatorname{rank}J(\mathbb{Q})=1$. The group $J(\mathbb{Q})$ is torsion-free: $\#J(\mathbb{F}_3)=10$ and $J(\mathbb{Q})[2]=0$ leave only 5-torsion. The automorphism $(x,y)\mapsto(\zeta_5x,y)$ makes J a $\mathbb{Z}[\zeta_5]$-module. If $T\in J(\mathbb{Q})$ had order 5, then $M=\mathbb{Z}[\zeta_5]T\simeq\mathbb{Z}[\zeta_5]/(1-\zeta_5)^r$, $1\le r\le4$, would be Galois-stable, and Galois would act on its socle $(1-\zeta_5)^{r-1}M$ by χ_5^{r-1}, where χ_5 is the cyclotomic character modulo 5. The socle lies in $J[1-\zeta_5]$, of order 5, spanned by $[(0,\sqrt{2^85^3})-\infty]$, on which Galois acts through $\mathbb{Q}(\sqrt5)$, that is by χ_5^2. So $r=3$, and $125=\#M$ would divide $\#J(\mathbb{F}_q)$ for every prime $q\equiv1 \bmod 5$ of good reduction, whereas $\#J(\mathbb{F}_{11})=80$. For each prime $\ell\in\{2,3,5,7,11,19\}$ a prime $q\in\{11,29,3,139,31,191\}$ respectively with $P \bmod q\notin\ell J(\mathbb{F}_q)$ shows that ℓ does not divide $[J(\mathbb{Q}):\langle P\rangle]$. The sieve uses the 26 primes $q<660$ with $\operatorname{ord}(P \bmod q)\mid N$, where $N=2^3\cdot3^2\cdot5^2\cdot7\cdot11\cdot19$. For each of them $\#J(\mathbb{F}_q)$ has no prime factor outside $\{2,3,5,7,11,19\}$, so the image of $J(\mathbb{Q})$ in $J(\mathbb{F}_q)$ is $\langle P \bmod q\rangle$, and the sieve leaves $[Q-\infty]\in\{0,\pm P\}+NJ(\mathbb{Q})$ for $Q\in C_1(\mathbb{Q})$. As $2\cdot5^2\cdot7\mid N$ and $\#J(\mathbb{F}_7)=50$, $NJ(\mathbb{Q})$ lies in the kernel of reduction modulo 7^2. With $I_j=\int_\infty^{(-4,176)}x^j\,dx/2y$ and $\omega=I_1\,dx/2y-I_0\,x\,dx/2y$, whose integral vanishes on $J(\mathbb{Q})$, we have $v_7(I_0)=1$ and $v_7(I_1+4I_0)=2$, so by Strassmann's theorem $\int_\infty^Q\omega$ has at most one zero in the residue disc of ∞ and at most one in each disc $\{v_7(x+4)\ge2\}$ around $(-4,\pm176)$. A point Q with $[Q-(-4,\pm176)]$ in the kernel of reduction modulo 7^2 lies in that disc, since on the residue disc $\int_{(-4,176)}^Q dx/2y\equiv(x+4)/352 \bmod 7^2$. Hence $C_1(\mathbb{Q})=\{\infty,(-4,\pm176)\}$. The integrals I_j were computed with the Coleman integration of SageMath [1] and, independently, as $\frac15$ of the tiny integral from ιQ_2 to Q_1, where ι is the hyperelliptic involution and $5P=[Q_1+Q_2-2\infty]$ with $Q_2\equiv\iota Q_1 \bmod 7$. The two agree modulo 7^{40}, and only $I_j \bmod 7^3$ is used.

(M2) The algebra $A=\mathbb{Q}[x]/(F_j)$ is $k_{\pm1}$ for $j=-1$ and $k_{\pm2}$ for $j=-2$. We use the map $J_j(\mathbb{Q})/2J_j(\mathbb{Q})\to A^\times/\mathbb{Q}^\times A^{\times2}$, $[\sum P_i-2(\infty_++\infty_-)]\mapsto\prod(x(P_i)-\theta)$, of [45, §11] (see also [63]). Its kernel lies in the subgroup generated by $2J_j(\mathbb{Q})$ and the class of $[\infty_+-\infty_-]$: it is contained in the preimage under the connecting map δ of the class of the $J_j[2]$-torsor $\{x\in\operatorname{Pic}^1:2x=[\infty_++\infty_-]\}$, and this class is $\delta([\infty_+-\infty_-])$ because ∞_+ is rational. Now $[\infty_+-\infty_-]=\pm2[Q_{j,1}-2(\infty_++\infty_-)]$ lies in $2J_j(\mathbb{Q})$, where $Q_{j,1}$ is the effective divisor of degree 4 given by (a,b) in Mumford form [28, p. 16]: for an explicit quintic $R\equiv b \bmod a$, R^2-F_j is a constant times a^2, so $y-R(x)$ has divisor $2Q_{j,1}-3\infty_\pm-5\infty_\mp$. So the map

is injective, and so is the same map over every $\mathbb{Q}_p$. As $J_j(\mathbb{Q})[2] = 0$ (F_j is irreducible of degree 10), rank $J_j(\mathbb{Q})$ is at most the dimension of the 2-Selmer group. Let S' be the set of primes above 2, 3, 5, 7 (and 43 for $j = -2$). The Selmer group lies in the image of $A(S', 2)$, of dimension 16 and 20 by Proposition A.13(d); we use a basis of explicit S'-units, checked to be S'-units and independent modulo squares. The conditions are: $N(\xi) \in \mathbb{Q}^{\times 2}$; unramified at the primes above 7 (and 43); and at $p = 2$, 3, 5 membership in the local image, spanned by the classes of explicit points and divisors of degree 2 and 4 until its dimension $\dim J_j(\mathbb{Q}_p)[2] + 4[p = 2]$, namely 5, 2, 0, is reached. $A \otimes \mathbb{R} \simeq \mathbb{C}^5$ gives no condition. Both Selmer groups have dimension 2 and are spanned by the classes of $Q_{j,1}$ and $Q_{j,2}$, so rank $J_j(\mathbb{Q}) \leq 2$.

In (M1) the point counts over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ for $q < 400$ were made twice (character sums and SageMath's point counting), the orders $\#J(\mathbb{F}_q)$ were checked against the Frobenius polynomial and by multiplying random points, and the 7-adic integrals were computed by the two methods above, but the saturation, the sieve and the Strassmann bounds were computed by one program. (M2) is one PARI/GP program with independent consistency checks: many further local points and divisors never enlarge the local images beyond the dimensions above, each local image together with the image of $\mathbb{Q}_p^\times$ is maximal isotropic for the Hilbert symbol pairing, and the S'-unit basis is checked without PARI's class group routines.

Apart from (M1) and (M2), Part III uses no Magma computation of [28] other than finite computations (polynomial identities and factorizations, residue classes, finite fields and power series), which are used as published; the Chabauty computations at 11 in §7 and at 7 in §8 and the odd index modulo 29 in §8 of [28] are among these finite computations.

The exponent 13. The Selmer groups of Proposition 16.4 were computed by two separately written programs, with different auxiliary primes, and the two give the same dimensions, restrictions and known classes. At the primes above 3 both programs use discrete logarithms in $(\mathcal{O}/\mathfrak{P}^N)^\times$, with different N and different uniformizers. At four places the second program confirms $\dim W_v$ through the points of the first program, which it checks to be exact local points: the place above 2 with $(e, f) = (4, 2)$ for 96a1, 864a1 and 864b1, and the place above 3 with $(e, f) = (2, 1)$ for 864c1. The relation among the four known classes of 96a1 was checked exactly, by finding a cube root in L. The bound B_E was computed twice for every field, by PARI and by a separate program. The 3-adic logarithms, lattices and levels at the eight primes above 3 used in Propositions 17.7 and 17.9 were recomputed in SageMath 10.9 by a separately written program, which computes the cube classes of the lattice generators with PARI. The location of the roots in Proposition 17.4 was checked at 855 sampled roots. The certificates of Proposition 16.5 for 96a1 were checked again by a separately written program, with exact arithmetic. The other certificates and the enumerations of Propositions 17.4, 17.7 and 17.9 were computed by one program each, and the enumerations were run a second time, with the same results. For 96a1, 864a1 and 864b1, the classes that a point outside the span K_0 of the known points would have to produce were also collected into a finite set, using only the local data; none of the 54, 6 and 78 elements, respectively, of $\mathrm{Sel}^\lambda(J/K)$ outside K_0 restricts into it. In lines 3, 4, 5 and 7 of [27, Table 2], the description of j was confirmed for $p = 13$ for all (a, b) modulo 3^7; the assignment of these lines to the curves is used as published.

The Magma computations of [27, §7.1]. Proposition 2.3 uses the treatment of the CM twists at $p = 11$ in [27, §7.1], whose computations are made in Magma by the file `section7.magma` of Stoll's script [62]. They do not assume GRH: the script assumes GRH only when it

recomputes the Selmer groups of [27, §7.2], which it does not do as published, and according to its documentation Magma computes class groups and Selmer groups unconditionally unless a bound for them is set [9]. Freitas, Naskręcki and Stoll also state, after their Theorem 7.1, that GRH is used only for the class groups of five fields of degree 36.

We have checked the Mordell–Weil groups of [27, §7.1] independently, without GRH and without Magma, so also without Magma's class group computations (see [22, §1] above). Let α be a root of $4x^3-4x^2-28x+41$ and $K_\alpha = \mathbb{Q}(\alpha)$, a cubic field of discriminant -44 and class number 1. For $c \in \{1,\ 4-\alpha,\ 3,\ 3(4-\alpha)\}$ let E_c be the curve $u^2 = c(x-\alpha)(4x^3+7x^2-6x+19)$ of genus one over K_α, an elliptic curve with origin $(\alpha, 0)$; these are the four curves of [27, §7.1], with $c = -d$ and $c = -d(4-\alpha)$ for $d = -1, -3$. The 2-descents on all four curves take place in the field $L_\alpha = K_\alpha(\beta)$, where β is a root of $4x^3 + 7x^2 - 6x + 19$, which is irreducible over K_α. The field L_α has degree 9, signature $(1, 4)$ and discriminant $2^{10}11^7$, its ring of integers is proved maximal, and its class number is 1: each of the 64 prime ideals of norm below the Minkowski bound 347.7 is generated by an explicit element. With explicit S-units of L_α, for S the primes above 2, 3 and 11, the 2-Selmer groups of E_c over K_α have dimensions 1, 1, 2, 2, and the images of explicit points span them. The torsion of $E_c(K_\alpha)$ is trivial, by the orders of the reductions modulo primes of norm 7, 13 and 17, so $\operatorname{rank} E_c(K_\alpha) = 1,\ 1,\ 2,\ 2$. The subgroup generated by the explicit points has odd index, by the descent; its index is prime to every odd prime $\ell \le 997$, by reduction modulo primes of K_α of degree one and norm at most 83,497; and its index is less than 20, 24, 226 and 261, by Thongjunthug's lower bound for the canonical height [65], with the archimedean constants enclosed in ball arithmetic. So the explicit points generate, and $E_c(K_\alpha) \simeq \mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Z}^2$, $\mathbb{Z}^2$, of rank less than $[K_\alpha : \mathbb{Q}] = 3$, as elliptic Chabauty requires [11]. Likewise the group of rational points of $y^2 = 4x^3 - 4x^2 - 28x + 41$, a model of 121b1, is $\mathbb{Z} \cdot (4, 11)$ (this is proved below). These computations were made by two separately written programs in PARI/GP; the second finds its generators and units without PARI's class group routines. For 121b1 the first program checks only the rank, the torsion and the saturation at primes up to 200. The archimedean constants were enclosed in ball arithmetic, with python-flint, by the second program only; the first takes the constant at the complex place from SageMath and gives nearly the same index bounds. The minimal models used in the height bound were found with SageMath and checked in PARI/GP.

We have also repeated the elliptic Chabauty step of [27, §7.1] in PARI/GP, on these generators. For $c = 1,\ 4-\alpha,\ 3,\ 3(4-\alpha)$ the points of $E_c(K_\alpha)$ with $x \in \mathbb{P}^1(\mathbb{Q})$ are exactly the two points with $x = \infty,\ 5/4,\ -2,\ 4$ respectively, in agreement with [27, §7.1] and Stoll's script; we write them $\pm P_c$. In each case a Mordell–Weil sieve, by reduction modulo the primes of K_α above 863 for $c = 1$, above 53 for $c = 4-\alpha$, above 863 and 7 for $c = 3$, and above 53 and 863 for $c = 3(4-\alpha)$, shows that such a point lies in $P_c + H_c$ or in $-P_c + H_c$, where H_c is the subgroup of points that reduce to the origin modulo every prime above $p = 863,\ 53,\ 863,\ 53$ respectively. This prime p splits completely in K_α, with embeddings $\sigma_1, \sigma_2, \sigma_3 \colon K_\alpha \to \mathbb{Q}_p$. On each of the two cosets, $\sigma_1(x) - \sigma_2(x)$ and $\sigma_1(x) - \sigma_3(x)$ (with $1/x$ in place of x for $c = 1$) are p-adic power series in the coordinates with respect to a basis of H_c, divisible by p, and their linear terms divided by p have rank equal to that of $E_c(K_\alpha)$ modulo p. So $\pm P_c$ are the only points of their cosets with rational x. Our program in PARI/GP computes these linear terms both p-adically and by exact arithmetic in K_α, and a separately written program in Python, with its own arithmetic in finite fields and modulo p^2, gives the same sieve sets and linear terms.

Over $x = \infty,\ 4,\ 5/4,\ -2$ lie the seven rational points $O, \pm P, \pm 3P, \pm 4P$ of $y^2 = 4x^3-4x^2-28x+41$, where $P = (4, 11)$, and Freitas, Naskręcki and Stoll find the j-invariants at these

points with the formula of Dose, Fernández, González and Schoof [20, §1], a step that is not in Stoll's script. With $y = 2Y+1$ the curve becomes $Y^2+Y = X^3-X^2-7X+10$, on which that formula is written, and $P = (4, 5)$. We evaluated the formula exactly at the seven points O, $\pm P$, $\pm 3P$, $\pm 4P$, in PARI/GP and again by a separately written program. It gives $j = 287496$, 54000, -12288000, 1728, 0 at O, P, $-P$, $3P$, $4P$ (discriminants -16, -12, -27, -4, -3), and $j(-3P) = -2^9\cdot 3^3\cdot 5^3\cdot 13\cdot 71^3\cdot 181^3/43^{11}$ and $j(-4P) = 2^{18}\cdot 3^3\cdot 5^3\cdot 7\cdot 11^3\cdot 23^3\cdot 29^3\cdot 103^3/67^{11}$, which are not CM. As a check of the formula, it gives at $-P$, O, P, $2P$, $3P$, $4P$, $5P$ the j-invariants of the orders of discriminant -27, -16, -12, -67, -4, -3, -163, and $j = 1728$ at $(5/4, 7/8) = 3P$ as Dose, Fernández, González and Schoof state. The integral values other than 0 and 1728 differ from -13824, so they come from no primitive solution with $abc \neq 0$ (Lemma 2.15(a)). If $j(-3P)$ or $j(-4P)$ were $1728b^3/c^{11}$ with b, c coprime, then $|c| = 43$, resp. 67, and $b^3 = \mp 2^3\cdot 5^3\cdot 13\cdot 71^3\cdot 181^3$, resp. $\pm 2^{12}\cdot 5^3\cdot 7\cdot 11^3\cdot 23^3\cdot 29^3\cdot 103^3$, which are not cubes. Only $j(3P) = 1728$ and $j(4P) = 0$ remain; they come from the trivial solutions with $a = 0$ and with $b = 0$. So every computation of [27, §7.1] has been repeated without Magma and without GRH. The published inputs are the equation of $X_{\mathrm{ns}}^+(11)$ [37, Proposition II.4.3.8.1], that of its double cover $X_{\mathrm{ns}}(11)$ [20, Proposition 1], the formula for j [20, §1] and the covering argument of [27, §7.1]. That the group of rational points of $y^2 = 4x^3 - 4x^2 - 28x + 41$ is $\mathbb{Z}\cdot(4, 11)$ is proved as follows: the torsion is trivial; the rank is 1 by Gross–Zagier and Kolyvagin [31, 34], as the curve has complex multiplication and so is modular, its root number is -1 and $L'(121\mathrm{b}1, 1) \approx 0.86237$, computed in ball arithmetic, and a 2-descent gives the same rank independently; and the index of $\mathbb{Z}\cdot(4, 11)$ is 1 by Silverman's bound for the difference between the Weil and canonical heights [58, Theorem 1.1] and a search for points of small height.

The programs, their inputs and outputs, and the data behind each statement of Table S31 (Selmer bases, class sets, lattices and levels, S-unit bases, the coefficients of Appendix A.1, and the j-maps and defining polynomials of Appendix C) are available at [32].

Appendix C. Data

This appendix prints data that the proofs use and that are too long for the body: defining polynomials of $K_{288\mathrm{a}1}$ for $p = 19$ and 23 (Table 17), the modular units f for $p = 23$ and 29, and a second model of $K_{54\mathrm{a}1}$ for $p = 17$. The other fields and the forms of Part III are printed in the Supplement (Appendix C.2).

C.1. **The j-maps and the modular units.** The polynomials $\mathcal{A}_p$ and $\mathcal{B}_p$ of Lemma 2.5 for $p = 17$, 19, 23 and 29, whose coefficients have up to 21 digits, are given in [32]. For $p = 11$ they are printed in [27, §7.2]. They determine the fibre polynomials G_p of (2.4), and hence the fields $K_E = \mathbb{Q}[x]/(G_p(x, j_E))$ of Proposition 2.8 for $E \neq 288\mathrm{a}1$. The modular units $f = f_0 + f_1 y$ of Lemma 2.5(c) are, for $p = 23$,

$$\begin{aligned} f_0 &= \tfrac{1}{2}x^{11} - 17x^{10} + 235x^9 - \tfrac{3345}{2}x^8 + 6279x^7 - \tfrac{20815}{2}x^6 - 1637x^5 \\ &\quad + \tfrac{49169}{2}x^4 - \tfrac{36235}{2}x^3 + \tfrac{1729}{2}x^2 + 4920x - 11367, \\ f_1 &= -\tfrac{1}{2}x^8 + 15x^7 - \tfrac{357}{2}x^6 + 1050x^5 - \tfrac{5985}{2}x^4 + 2670x^3 \\ &\quad + \tfrac{7975}{2}x^2 - 6043x - 1640, \end{aligned}$$

and for $p = 29$,

$$\begin{aligned} f_0 &= \tfrac{1}{2}x^7 - \tfrac{13}{2}x^6 + \tfrac{45}{2}x^5 + \tfrac{25}{2}x^4 - \tfrac{269}{2}x^3 + \tfrac{29}{2}x^2 + 150x + 83, \\ f_1 &= -\tfrac{1}{2}x^4 + \tfrac{11}{2}x^3 - \tfrac{31}{2}x^2 - 7x + 50. \end{aligned}$$

k	$m_{288}^{(19)}$	$F_{288\mathrm{a}1}$	$m_{288}^{(23)}$
24			1
23			−24
22			230
21			−1426
20	1	1	8878
19		−8	−50 830
18	61 560	38	238 418
17		−114	−1 026 168
16	−1 525 826 160	304	3 950 227
15		−2926	−13 959 666
14	1 833 137 422 848	30 666	42 655 478
13		−179 474	−124 719 064
12	−5 874 735 961 013 760	738 777	300 116 282
11		−3 019 898	−678 269 770
10	−166 315 930 060 566 528	14 240 652	1 299 851 808
9		−61 774 396	−2 183 341 838
8	−255 992 490 477 137 977 344	208 696 570	3 308 502 229
7		−528 087 672	−4 220 494 020
6	21 172 552 815 177 276 456 960	999 253 928	4 772 392 912
5		−1 410 881 024	−5 417 780 272
4	−958 223 223 674 312 627 257 344	1 466 149 060	3 812 752 780
3		−1 085 621 088	−5 723 159 184
2	−10 356 520 397 660 515 346 153 472	537 538 272	1 078 993 296
1		−157 224 096	−4 267 545 696
0	−87 484 249 994 340 285 136 502 784	20 206 944	−1 082 377 584

TABLE 17. Defining polynomials of the fields $K_{288\mathrm{a}1}$ (Proposition 2.9): for $p = 19$, the minimal polynomial $m_{288}^{(19)}$ of $s(C_0)$ and a second defining polynomial $F_{288\mathrm{a}1}$ of the same field of degree 20; for $p = 23$, the polynomial $m_{288}^{(23)}$ of degree 24. Each column lists the coefficient of the k-th power of the variable. Empty entries are 0.

C.2. **Further defining polynomials.** As $j(288\mathrm{a}1) = 1728$ is a branch value of j, the field $K_{288\mathrm{a}1}$ is not of the form $\mathbb{Q}[x]/(G_p(x, 1728))$. For instance $G_{19}(x, 1728)$ is the square of a polynomial of degree 10. Table 17 gives the polynomials $m_{288}^{(19)}$ and $m_{288}^{(23)}$ of Proposition 2.9, and for $p = 19$ a second defining polynomial $F_{288\mathrm{a}1}$ with smaller coefficients.

For $p = 17$, Proposition A.6 uses the model $K_{54\mathrm{a}1} = \mathbb{Q}[x]/(F_{54\mathrm{a}1}) = \mathbb{Q}(\vartheta)$ with

$$\begin{aligned} F_{54\mathrm{a}1}(x) = {} & x^{18} - 3x^{17} - 68x^{15} + 408x^{14} + 1224x^{13} - 15028x^{12} + 42636x^{11} - 11934x^{10} \\ & - 196758x^9 + 446556x^8 - 228684x^7 - 486608x^6 + 657696x^5 + 366180x^4 \\ & - 1461116x^3 + 1558101x^2 - 1227471x + 642932, \end{aligned}$$

and this field is isomorphic to $\mathbb{Q}[x]/(G_{17}(x, j(54\mathrm{a}1)))$.

Tables S27, S28, S29 and S30 give defining polynomials with smaller coefficients of the other fields K_E with $p \geq 17$, and Tables S18 and S19 the forms h_i of [28, Table 3] and the fields of Part III.

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. Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic number theory (ANTS IX), Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 16–31.
2. Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Quadratic Chabauty for modular curves: algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152, arXiv:2101.01862.
3. Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197, https://doi.org/10.1090/S0025-5718-07-02003-0.
4. Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani, *On the equation* $a^3 + b^{3n} = c^2$, Acta Arith. **163** (2014), no. 4, 327–343, https://doi.org/10.4064/aa163-4-3.
5. ———, *Generalized Fermat equations: a miscellany*, Int. J. Number Theory **11** (2015), no. 1, 1–28, https://doi.org/10.1142/S179304211530001X.
6. Siegfried Bosch and Werner Lütkebohmert, *Degenerating abelian varieties*, Topology **30** (1991), no. 4, 653–698.
7. ———, *Formal and rigid geometry. I. Rigid spaces*, Math. Ann. **295** (1993), no. 2, 291–317.
8. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Formal and rigid geometry. IV. The reduced fibre theorem*, Invent. Math. **119** (1995), no. 2, 361–398.
9. Wieb Bosma, John J. Cannon, Claus Fieker, and Allan Steel, *Handbook of Magma functions*, version 2.25, https://magma.maths.usyd.edu.au/magma/handbook/.
10. David Brown, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, Int. Math. Res. Not. IMRN (2012), no. 2, 423–436.
11. Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.
12. ———, *The primitive solutions to* $x^3 + y^9 = z^2$, J. Number Theory **111** (2005), no. 1, 179–189.
13. Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370.
14. Kęstutis Česnavičius, *p-Selmer growth in extensions of degree p*, J. Lond. Math. Soc. (2) **95** (2017), no. 3, 833–852, arXiv:1408.1151.
15. Claude Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Univ. Tokyo Sect. I **2** (1933), 365–476.
16. Robert F. Coleman, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.
17. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.
18. Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154.

19. 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.
20. Valerio Dose, Julio Fernández, Josep González, and René Schoof, *The automorphism group of the non-split Cartan modular curve of level* 11, J. Algebra **417** (2014), 95–102, https://doi.org/10.1016/j.jalgebra.2014.05.036, arXiv:1403.6254.
21. 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.
22. Andreas-Stephan Elsenhans and John Voight, *Computing class groups and unit groups in Magma*, 2025, preprint, arXiv:2510.05501.
23. The FLINT team, *FLINT: Fast Library for Number Theory*, 2025, version 3.3.0, https://flintlib.org.
24. Nuno Freitas and Alain Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Mem. Amer. Math. Soc. **277** (2022), no. 1361, arXiv:1607.01218v5; theorem numbers as in this version.
25. Nuno Freitas and Diana Mocanu, *Local points on twists of* $X(p)$ *with applications*, 2025, preprint, arXiv:2509.04294v4.
26. Nuno Freitas, Diana Mocanu, and Ignasi Sánchez-Rodríguez, *Revisiting the equation* $x^2 + y^3 = z^p$, 2025, preprint, arXiv:2512.10781.
27. Nuno Freitas, Bartosz Naskręcki, and Michael Stoll, *The generalized Fermat equation with exponents* 2*,* 3*,* n, Compos. Math. **156** (2020), no. 1, 77–113, https://doi.org/10.1112/S0010437X19007693, arXiv:1703.05058.
28. Nuno Freitas and Michael Stoll, *The generalized Fermat equation* $x^2 + y^3 = z^{25}$, 2025, preprint, arXiv:2506.10667v1.
29. Jean Fresnel and Marius van der Put, *Rigid analytic geometry and its applications*, Progr. Math., vol. 218, Birkhäuser, Boston, 2004.
30. Georges Gras, *Class field theory: from theory to practice*, Springer Monogr. Math., Springer-Verlag, Berlin, 2003.
31. Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.
32. Manvir Jaswal, *Programs and data for "New exponents for the generalized Fermat equation* $x^2 + y^3 = z^n$ *"*, 2026, Zenodo, https://doi.org/10.5281/zenodo.23088537.
33. Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292.
34. Victor A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser, Boston, MA, 1990, pp. 435–483.
35. Alain Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), no. 4, 353–385.
36. Franz Lemmermeyer, *The ambiguous class number formula revisited*, J. Ramanujan Math. Soc. **28** (2013), no. 4, 415–421, arXiv:1309.1071.
37. Gérard Ligozat, *Courbes modulaires de niveau* 11, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., vol. 601, Springer, Berlin, 1977, pp. 149–237.
38. Hideyuki Matsumura, *Commutative ring theory*, Cambridge Stud. Adv. Math., vol. 8, Cambridge University Press, Cambridge, 1986.
39. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186.
40. ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.
41. J. Steffen Müller, *Rational points on* $X_{\mathrm{ns}}^+(19)$ *(joint work with J. S. Balakrishnan and J. Vonk)*, 2026, announcement of results in a lecture at the conference ChaBONNty, Max Planck Institute for Mathematics, Bonn, 1 July 2026; slides at https://martinluedtke.github.io/chabonnty-slides/mueller.pdf.
42. Jürgen Neukirch, *Algebraic number theory*, Grundlehren Math. Wiss., vol. 322, Springer-Verlag, Berlin, 1999.
43. The PARI Group, *PARI/GP version 2.17.3*, Univ. Bordeaux, 2025, https://pari.math.u-bordeaux.fr/.
44. Georges Poitou, *Sur les petits discriminants*, Séminaire Delange–Pisot–Poitou. Théorie des nombres **18** (1976/77), no. 1, Exp. No. 6, 1–17, http://www.numdam.org/item/SDPP_1976-1977__18_1_A6_0/.
45. Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.

46. 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.
47. Ashleigh Ratcliffe and Bogdan Grechuk, *Generalized Fermat equation: a survey of solved cases*, Expo. Math. **43** (2025), no. 4, Paper No. 125688, arXiv:2412.11933v2.
48. Michel Raynaud, *Schémas en groupes de type $(p,\dots,p)$*, Bull. Soc. Math. France **102** (1974), 241–280.
49. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026, https://www.sagemath.org.
50. Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114.
51. ———, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471.
52. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
53. ———, *Algebraic groups and class fields*, Grad. Texts in Math., vol. 117, Springer-Verlag, New York, 1988.
54. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
55. Samir Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793.
56. Samir Siksek and Michael Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3+y^4+z^5=0$*, Bull. Lond. Math. Soc. **44** (2012), no. 1, 151–166.
57. ———, *The generalised Fermat equation $x^2+y^3=z^{15}$*, Arch. Math. (Basel) **102** (2014), no. 5, 411–421.
58. Joseph H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743.
59. ———, *The arithmetic of elliptic curves*, second ed., Grad. Texts in Math., vol. 106, Springer, New York, 2009.
60. Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, second ed., Undergrad. Texts Math., Springer, Cham, 2015.
61. The Stacks Project Authors, *The Stacks Project*, https://stacks.math.columbia.edu, 2026.
62. Michael Stoll, *Magma scripts for the computations in "The generalized Fermat equation with exponents 2, 3, n"*, files dated 13 June 2019, https://www.mathe2.uni-bayreuth.de/stoll/magma/index.html#GenFermat.
63. ———, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277.
64. ———, *Chabauty without the Mordell–Weil group*, Algorithmic and experimental methods in algebra, geometry, and number theory, Springer, Cham, 2017, pp. 623–663, arXiv:1506.04286v2.
65. Thotsaphon Thongjunthug, *Computing a lower bound for the canonical height on elliptic curves over number fields*, Math. Comp. **79** (2010), no. 272, 2431–2449.
66. Zhong-Peng Zhou, *The inter-universal Teichmüller theory and new Diophantine results over rational numbers. II*, 2025, preprint, arXiv:2510.05448v1.

Toronto, Canada
Email address: manvirjaswal@icloud.com