THE GENERALIZED FERMAT EQUATION WITH EXPONENTS 2, 3, n

NUNO FREITAS, BARTOSZ NASKRĘCKI, AND MICHAEL STOLL

Abstract. We study the Generalized Fermat Equation $x^2 + y^3 = z^p$, to be solved in coprime integers, where $p \geq 7$ is prime. Using modularity and level lowering techniques, the problem can be reduced to the determination of the sets of rational points satisfying certain 2-adic and 3-adic conditions on a finite set of twists of the modular curve $X(p)$. We use information on mod-p Galois representations over 2-adic and 3-adic fields to produce the minimal list of such twists that are compatible with local information at 2 and 3; this list depends on p mod 24. Using recent results on mod p representations with image in the normalizer of a split Cartan subgroup, the list can be further reduced in some cases.

Our second main result is the complete solution of the equation when $p = 11$, which was the smallest unresolved p. One relevant new ingredient is the use of the 'Selmer group Chabauty' method introduced by the third author in a recent preprint, applied in an Elliptic Curve Chabauty context, to determine relevant points on $X_0(11)$ defined over certain number fields of degree 12. This result is conditional on GRH, which is needed to show correctness of the computation of the class groups of five specific number fields of degree 36.

We also give some partial results for the case $p = 13$.

1. Introduction

This paper considers the Generalized Fermat Equation

$$x^2 + y^3 = \pm z^n \,. \tag{1.1}$$

Here $n \geq 2$ is an integer, and we are interested in *non-trivial primitive integral solutions*, i.e., triples (a, b, c) of nonzero coprime integers such that $a^2 + b^3 = \pm c^n$. If n is odd, the sign can be absorbed into the nth power, and there is only one equation to consider, whereas for even n, the two sign choices lead to genuinely different equations.

It is known that for $n \leq 5$ there are infinitely many primitive integral solutions, which come in finitely many families parameterized by binary forms evaluated at pairs of coprime integers satisfying some congruence conditions, see for example [Edw04] for details. It is also known that for (fixed) $n \geq 6$ there are only finitely many coprime integral solutions, see [DG95] for $n \geq 7$; the case $n = 6$ reduces to two elliptic curves of rank zero. Some solutions are known for $n \geq 7$, namely (up to sign changes)

$$13^2 + 7^3 = 2^9, \quad 71^2 + (-17)^3 = 2^7 \quad 21063928^2 + (-76271)^3 = 17^7,$$
$$2213459^2 + 1414^3 = 65^7, \quad 15312283^2 + 9262^3 = 113^7,$$
$$30042907^2 + (-96222)^3 = 43^8, \quad 1549034^2 + (-15613)^3 = -33^8,$$

Date: May 17, 2016.

and for every n, there is the 'Catalan solution' $3^2 + (-2)^3 = 1^n$. It appears likely (and is in fact a special case of the 'Generalized Fermat Conjecture') that these are the only non-trivial primitive integral solutions for all $n \geq 6$. This has been verified for $n = 7$ [PSS07], $n = 8$ [Bru99, Bru03], $n = 9$ [Bru05], $n = 10$ [Bro12, Sik13] and $n = 15$ [SS14]. Since any integer $n \geq 6$ is divisible by 6, 8, 9, 10, 15, 25 or a prime $p \geq 7$, it suffices to deal with $n = 25$ and with $n = p \geq 11$ a prime, given these results. The case $n = 25$ is considered in ongoing work by the authors of this paper; the results will be described elsewhere. So we will from now on assume that $n = p \geq 7$ (or ≥ 11) is a prime number.

Our approach follows and refines the arguments of [PSS07] by combining new ideas around the modular method with recent methods to find rational points on curves. We note that the existence of trivial solutions with $c \neq 0$ and of the Catalan solutions prevents a successful application of the modular method alone. Nevertheless, in the first part of this paper we will apply a refinement of it to obtain local information, valid for an arbitrary prime exponent p. This information is then used as input for global methods in the second part when tackling concrete exponents. We now give a more detailed description of these two parts.

In the first part, we reduce solving equation (1.1) to the problem of determining the sets of rational points (satisfying some congruence conditions at 2 and 3) on a small number of twists of the modular curve $X(p)$. We first develop new criteria to decide if two elliptic curves with certain type of potentially good reduction at 2 and 3 have symplectically isomorphic p-torsion modules. Then we apply these criteria to reduce the list obtained in [PSS07] of twists that have to be considered (in the case of irreducible p-torsion on the Frey elliptic curve, which always holds for $p \neq 7, 13$). For this we also make use of fairly recent results regarding elliptic curves over $\mathbb{Q}$ such that the image of the mod p Galois representation is contained in the normalizer of a split Cartan subgroup. Our main result here is summarized in Table 4, which says that, depending on the residue class of p mod 24, there are between four and ten twists that have to be considered.

In the second part, we give a proof of the fact that the only non-trivial primitive solutions in the case $p = 11$ are the Catalan solutions $(a, b, c) = (\pm 3, -2, 1)$, subject to the Generalized Riemann Hypothesis (and the correctness of our computations, which we have done with the help of the Magma computer algebra system [BCP97]). We use several ingredients to obtain this result. One is the explicit description of the relevant twists of $X(11)$ by Fisher [Fis14]. These twists have genus 26 and are therefore not amenable to any direct methods for determining the rational points. We can (and do) still use Fisher's description to obtain local information, in particular on the location in $\mathbb{Q}_2$ of the possible j-invariants of the Frey curves. The second ingredient is the observation that any rational point on a twist $X_E(11)$ maps to a point on the elliptic curve $X_0(11)$ that is defined over a certain number field K of degree (at most) 12 that only depends on E and such that the image of this point under the j-map is rational. This is the setting of 'Elliptic Curve Chabauty' [Bru03]; this approach was already taken in an earlier unsuccessful attempt by David Zureick-Brown. To carry this out in the usual way, one needs to find generators of the group $X_0(11)(K)$ (or at least of a subgroup of finite index), which proved to be infeasible in some of the cases. We get around this problem by invoking the third ingredient, which is 'Selmer Group Chabauty' as described in [Sto15], applied in the Elliptic Curve Chabauty setting. We note that we need the Generalized Riemann Hypothesis to ensure the correctness of the class group

computation for the number fields of degree 36 arising by adjoining to K the x-coordinate of a point of order 2 on $X_0(11)$. In principle, the class group can be verified unconditionally by a finite computation, which, however, would take too much time with the currently available implementations.

We also give some partial results for $p = 13$, showing that the Frey curves cannot have reducible 13-torsion and that the two CM curves in the list of Lemma 2.3 below can only give rise to trivial solutions.

Acknowledgments.

The work reported on in this paper was supported by the German Science Foundation (DFG), grant Sto 299/11-1, in the framework of the Priority Programme SPP 1489. The first author was also partly supported by the grant *Proyecto RSME-FBBVA* 2015 *José Luis Rubio de Francia*. We thank David Zureick-Brown for sharing his notes with us.

Notation.

Let K be a field of characteristic zero or a finite field. We write G_K for its absolute Galois group. If E/K is an elliptic curve, we denote by $\overline{\rho}_{E,p}$ the Galois representation of G_K arising from the p-torsion on E. We write N_E for the conductor of E. Let H_8 denote the quaternion group and $\mathrm{Dic}_{12} \simeq C_3 \rtimes C_4$ the dicyclic group with 12 elements.

2. Irreducibility and level lowering

Suppose that (a, b, c) is a solution to the equation

$$x^2 + y^3 = z^p, \qquad \text{with } p \geq 7 \text{ prime.} \tag{2.1}$$

We will say (a, b, c) is *trivial* if $abc = 0$ and *non-trivial* otherwise. A non-trivial solution is *primitive* if $\gcd(a, b, c) = 1$ and *non-primitive* otherwise. Note that Equation (2.1) admits for all p the trivial primitive solutions $(\pm 1, 1, 0)$, $(\pm 1, 0, 1)$, $\pm(0, 1, 1)$ and the pair of non-trivial primitive solutions $(\pm 3, 2, 1)$, which we refer to as the *Catalan solution(s)*.

As in [PSS07], we can consider a putative solution (a, b, c) of (2.1) and the associated Frey elliptic curve

$$E_{(a,b,c)} \colon y^2 = x^3 + 3bx - 2a \qquad \text{of discriminant } \Delta = -12^3 c^p.$$

This curve has invariants

$$c_4 = -12^2 b, \quad c_6 = -12^3 a, \quad j = \frac{12^3 b^3}{c^p}. \tag{2.2}$$

We begin with a generalization and refinement of Lemma 6.1 in [PSS07].

Lemma 2.3. *Let $p \geq 7$ and let (a, b, c) be coprime integers satisfying $a^2 + b^3 = c^p$ and $c \neq 0$. Assume that the Galois representation on $E_{(a,b,c)}[p]$ is irreducible. Then there is a quadratic twist $E^{(d)}_{(a,b,c)}$ of $E_{(a,b,c)}$ with $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ such that $E^{(d)}_{(a,b,c)}[p]$ is isomorphic to $E[p]$ as a $G_{\mathbb{Q}}$-Galois module, where E is one of the following seven elliptic curves (specified by their Cremona label):*

$$27a1,\ 54a1,\ 96a1,\ 288a1,\ 864a1,\ 864b1,\ 864c1\,.$$

Proof. By the proof of [PSS07, Lemma 4.6], a twist $E^{(d)}_{(a,b,c)}$ with $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ of the Frey curve has conductor dividing $12^3 N'$, where N' is the product of the primes ≥ 5 dividing c. In fact, carrying out Tate's algorithm for $E_{(a,b,c)}$ locally at 2 and 3 shows that the conductor can be taken to be $2^r 3^s N'$ with $r \in \{0, 1, 5\}$ and $s \in \{1, 2, 3\}$. (This uses the assumption that the solution is primitive.)

Using level lowering as in the proof of [PSS07, Lemma 6.1], we find that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ where E' is an elliptic curve of conductor 27, 54, 96, 288 or 864, or else $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,\mathfrak{p}}$, where f is a newform of level 864 with field of coefficients $\mathbb{Q}(\sqrt{13})$ and $\mathfrak{p} \mid p$ in this field. Let f be one of these newforms and write $\rho = \rho_{f,\mathfrak{p}}|_{D_3}$ for the restriction of the Galois representation attached to f to a decomposition group at 3. We apply the Loeffler-Weinstein algorithm[1] [LW12, LW15] to determine ρ and we obtain $\rho(I_3) \simeq S_3$. Since p does not divide $6 = \#S_3$ we also have $\overline{\rho}(I_3) \simeq S_3$. On the other hand, it is well known that when $\overline{\rho}_{E,p}(I_3)$ has order 6, it must be cyclic (see [Kra90, page 354]). Thus we cannot have $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,\mathfrak{p}}$ for any of these newforms f.

We then check that each elliptic curve with conductor 27, 54, 96, 288 or 864 is isogenous (via an isogeny of degree prime to p) to a quadratic twist (with d in the specified set) of one of the seven curves mentioned in the statement of the lemma. □

The following proposition shows that the irreducibility assumption in the previous lemma is automatically satisfied in most cases.

Proposition 2.4. *Let (a, b, c) be a non-trivial primitive solution of (2.1) for $p \geq 11$. Write $E = E_{(a,b,c)}$ for the associated Frey curve. Then $\overline{\rho}_{E,p}$ is irreducible.*

Proof. If $p = 11$ or $p \geq 17$, then by Mazur's results [Maz78], there is only a finite list of j-invariants of elliptic curves over $\mathbb{Q}$ that have a reducible mod p Galois representation (see also [Dah08, Theorem 22]). More precisely, either we have

(i) $p = 11, 19, 43, 67, 163$ and the corresponding curves have integral j-invariant, or
(ii) $p = 17$ and the j-invariant is $-17^2 \cdot 101^3/2$ or $-17 \cdot 373^3/2^{17}$.

Suppose that $\overline{\rho}_{E,p}$ is reducible, hence the Frey curve $E_{(a,b,c)}$ corresponds to one of the curves in (i) or (ii). Note that $\gcd(a, b) = 1$. Suppose we are in case (i). Since $p \geq 11$ and the j-invariant is integral, it follows that $c = \pm 1$, which implies that we either have one of the trivial solutions $(\pm 1, 0, 1)$, $\pm(0, 1, 1)$ or the 'Catalan solution' $(\pm 3, -2, 1)$, since the only integral points on the elliptic curves $y^2 = x^3 \pm 1$ (which both have finite Mordell-Weil group) have $x \in \{0, -1, 2\}$. It remains to observe that the Frey curve associated to the Catalan solution (which is, up to quadratic twist, 864*b*1) is the only curve in its isogeny class, so it has irreducible mod p Galois representations for all p. If we are in case (ii), then then the 17-adic valuation of the j-invariant contradicts (2.2).

For $p = 13$ the claim is shown in Lemma 8.1 in Section 8 below. □

[1] This is implemented in Magma via the commands `pi:=LocalComponent(ModularSymbols(f), 3); WeilRepresentation(pi)`.

We remark that the results of [PSS07] show that the statement of Proposition 2.4 is also true for $p = 7$.

Note that some of the seven curves in Lemma 2.3 are realized by twists of the Frey curve evaluated at known solutions. Indeed,

$$E^{(6)}_{(1,0,1)} = 27a1, \quad E_{(0,1,1)} = 288a1, \quad E^{(2)}_{(0,-1,-1)} = 288a2, \quad E^{(-2)}_{(3,-2,1)} = 864b1$$

and $288a2$ and $288a1$ are related by a degree 2 isogeny. The solutions $(\pm 1, 1, 0)$ give rise to singular Frey curves. Note also that $E^{(-d)}_{(-a,b,c)} = E^{(d)}_{(a,b,c)}$, so that $(-1, 0, 1)$ and $(-3, -2, 1)$ do not lead to new curves.

3. Local conditions and representations of inertia

Let ℓ be a prime. We write $\mathbb{Q}_\ell^{\mathrm{unr}}$ for the maximal unramified extension of $\mathbb{Q}_\ell$ and $I_\ell \subset G_{\mathbb{Q}_\ell}$ for the inertia subgroup. Let E be an elliptic curve over $\mathbb{Q}_\ell$ with potentially good reduction. Let $p \geq 3$, $p \neq \ell$ and $L = \mathbb{Q}_\ell^{\mathrm{unr}}(E[p])$ be the smallest extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$ over which E acquires good reduction. The extension L does not depend on p, see [Kra90]. For two elliptic curves E and E' defined over $\mathbb{Q}$ with potentially good reduction at ℓ and such that $L = \mathbb{Q}_\ell^{\mathrm{unr}}(E[p]) = \mathbb{Q}_\ell^{\mathrm{unr}}(E'[p]) = L'$ we say that *E and E' have the same inertial type at ℓ*.

We write $L_{2,96}$ and $L_{2,288}$ for the field $L/\mathbb{Q}_2^{\mathrm{unr}}$ corresponding respectively to the elliptic curves with Cremona labels $96a1$ and $288a1$. A direct computation shows that $L_{2,96} \not\simeq L_{2,288}$.

Proposition 3.1. *Let $E/\mathbb{Q}_2$ be an elliptic curve with potentially good reduction satisfying $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}}) \simeq H_8$. Suppose further that E has conductor 2^5. Then $L = L_{2,96}$ or $L = L_{2,288}$.*

Proof. There is a representation $\rho_E \colon W_2 \to \mathrm{GL}_2(\mathbb{C})$ of conductor 2^5 attached to E, where $W_2 \subset G_{\mathbb{Q}_2}$ is the Weil subgroup. The hypothesis implies that the inertia subgroup has finite image and acts irreducibly, hence ρ_E is a supercuspidal representation. In particular, we have

$$\rho_E = \mathrm{Ind}_{W_M}^{W_2} \chi \qquad \text{and} \qquad \rho_E\big|_{I_2} = \mathrm{Ind}_{I_M}^{I_2}(\chi\big|_{I_2}),$$

where $M/\mathbb{Q}_2$ is a ramified quadratic extension, $\chi \colon W_M \to \mathbb{C}^\times$ is a character and $I_M \subset W_M$ are the inertia and Weil groups of M. Furthermore, $\varepsilon_M \chi = \|\cdot\|^{-1}$ as characters of $\mathbb{Q}_2^\times$, where ε_M is the character associated to the quadratic extension $M/\mathbb{Q}_2$, $\|\cdot\|$ is the norm character and we use local class field theory to identify characters of W_2 with characters of $\mathbb{Q}_2^\times$.

The conductor exponents of ρ_E and χ are related by $\mathrm{cond}(\rho_E) = \mathrm{cond}(\chi) + \mathrm{cond}(\varepsilon_M)$. It follows from [Pac13, Corollary 4.1] that $M = \mathbb{Q}_2(d)$ where $d = \sqrt{-1}$ or $d = \sqrt{-5}$, hence $\mathrm{cond}(\varepsilon_M) = 2$ and $\mathrm{cond}(\chi) = 5 - 2 = 3$.

Write $\mathfrak{p}$ for the maximal ideal of M. Since $\mathrm{cond}(\chi) = 3$, we have that $\chi|_{I_M}$ factors via $(\mathcal{O}_M/\mathfrak{p}^3)^\times$, which has order 4 and is generated by $2 + d$. The condition $\chi|_{\mathbb{Z}_2^\times} = \varepsilon_M$ implies $\chi(-1) = -1$, thus $\chi(2 + d) = \pm i$. We conclude there are only two possibilities for $\chi|_{I_2}$, which are related by conjugation, hence giving the same induction $\rho_E|_{I_2}$. Thus, we find two possible fields L, one for each choice of M. Finally, we note that the curves $96a1$ and $288a1$ satisfy the hypotheses of the proposition. □

j	a	b	d	curves	$v_2(N_E)$
1	$a \equiv 1 \bmod 4$	$b \equiv 1 \bmod 2$	$1, -3$	$54a1$	1
2	$a \equiv 3 \bmod 4$	$b \equiv 1 \bmod 2$	$-1, 3$	$54a1$	1
3	$a \equiv 0 \bmod 4$	$b \equiv 1 \bmod 4$	$\pm 1, \pm 3$	$288a1, 864a1, 864b1$	5
4	$a \equiv 0 \bmod 4$	$b \equiv 3 \bmod 4$	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$	5
5	$a \equiv 2 \bmod 4$	$b \equiv 1 \bmod 4$	$\pm 1, \pm 3$	$96a1, 864c1$	5
6	$a \equiv 2 \bmod 4$	$b \equiv 3 \bmod 4$	$\pm 2, \pm 6$	$96a1, 864c1$	5
7	$a \equiv 1 \bmod 4$	$b \equiv 0 \bmod 8$	$-2, 6$	$27a1$	0
8	$a \equiv 3 \bmod 4$	$b \equiv 0 \bmod 8$	$2, -6$	$27a1$	0
9	$a \equiv 1 \bmod 2$	$b \equiv 2 \bmod 8$	$\pm 2, \pm 6$	$96a1, 864c1$	5
10	$a \equiv 1 \bmod 2$	$b \equiv 6 \bmod 8$	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$	5
11	$a \equiv 1 \bmod 2$	$b \equiv 4 \bmod 8$	$\pm 2, \pm 6$	impossible	0

TABLE 1. 2-adic conditions

We write $L_{3,54}$ and $L_{3,27}$ for the field $L/\mathbb{Q}_3^{\mathrm{unr}}$ corresponding respectively to the elliptic curves with Cremona labels $54a1$ and $27a1$. With similar arguments as in the proof of the previous proposition one can show the following.

Proposition 3.2. *Let $E/\mathbb{Q}_3$ be an elliptic curve with potentially good reduction satisfying $\mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}}) \simeq \mathrm{Dic}_{12}$. Suppose further that E has conductor 3^3. Then $L = L_{3,54}$ or $L = L_{3,27}$.*

One can check that the curves $96a1$ and $864c1$ and the curves $288a1$, $864a1$ and $864b1$ have the same inertial type at 2; similarly, one checks that the curves $54a1$ and $864a1$ and the curves $27a1$, $864b1$ and $864c1$ have the same inertial type at 3.

Using Magma we reprove and refine Lemma 2.3 by determining the 2-adic and 3-adic conditions on a, b and the twists $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ such that the inertial types at 2 and 3 of $E^{(d)}_{(a,b,c)}$ match those of the seven curves in Lemma 2.3. The 2-adic information can be found in Table 1. The last line is interesting: in this case, the twists of the Frey curve that have good reduction at 2 have trace of Frobenius at 2 equal to ± 2, so level lowering can never lead to a curve of conductor 27 (which is the only possible odd conductor dividing 12^3), since these curves all have trace of Frobenius equal to 0. The 3-adic conditions can be found in Table 2. The first column in each table is just a line number; it will be useful as reference in a later section. The remaining columns contain the indicated data.

Corollary 3.3. *Let $p \geq 11$ be a prime number. Let $(a, b, c) \in \mathbb{Z}^3$ be coprime and satisfy $a^2 + b^3 = c^p$. Then $b \not\equiv 4 \bmod 8$, and if $c \neq 0$, then c is not divisible by 6.*

Proof. Table 1 shows that $b \equiv 4 \bmod 8$ is impossible. If $c \neq 0$, then we have a twisted Frey curve $E^{(d)}_{(a,b,c)}$, which if $6 \mid c$ would have to be p-congruent to $54a1$ and to $96a1$ at the same time; this is impossible. □

i	a	b	d	curves	$v_3(N_E)$
1	$a \equiv 1 \bmod 3$	$b \equiv -1 \bmod 3$	$-3, 6$	$96a1$	1
2	$a \equiv -1 \bmod 3$	$b \equiv -1 \bmod 3$	$3, -6$	$96a1$	1
3	$a \equiv 0 \bmod 9$	$b \equiv \pm 1 \bmod 3$	$\pm 1, \pm 2, \pm 3, \pm 6$	$288a1$	2
4	$a \equiv \pm 3 \bmod 9$	$b \equiv 1 \bmod 3$	$\pm 1, \pm 2, \pm 3, \pm 6$	$27a1, 864b1, 864c1$	3
5	$a \equiv \pm 3 \bmod 9$	$b \equiv -1 \bmod 3$	$\pm 1, \pm 2, \pm 3, \pm 6$	$54a1, 864a1$	3
6	$a \equiv \pm 1 \bmod 3$	$b \equiv 0 \bmod 3$	$\pm 1, \pm 2, \pm 3, \pm 6$	$27a1, 864b1, 864c1$	3
7	$a \equiv \pm 2 \bmod 9$	$b \equiv 1 \bmod 3$	$\pm 1, \pm 2, \pm 3, \pm 6$	$288a1$	2
8	$a \equiv \pm 1, \pm 4 \bmod 9$	$b \equiv 1 \bmod 3$	$\pm 1, \pm 2, \pm 3, \pm 6$	$54a1, 864a1$	3

TABLE 2. 3-adic conditions

$j \backslash i$	$1, 2$	$3, 7$	$4, 6$	$5, 8$
$1, 2$	–	–	–	$54a1$
$3, 4, 10$	–	$288a1$	$864b1$	$864a1$
$5, 6, 9$	$96a1$	–	$864c1$	–
$7, 8$	–	–	$27a1$	–

TABLE 3. Curves E determined by ($a \bmod 36, b \bmod 24$).

We observe that the residue classes of a mod 36 and b mod 24 determine the corresponding curve in Lemma 2.3 uniquely, as given in Table 3. The line number j of Table 1 determines the row and the line number i of Table 2, the column.

4. Symplectic and anti-symplectic isomorphisms of p-torsion

Let p be a prime. Let K be a field of characteristic zero or a finite field of characteristic $\neq p$. Fix a primitive p-th root of unity $\zeta_p \in \bar{K}$. For E an elliptic curve defined over K we write $E[p]$ for its p-torsion G_K-module, $\overline{\rho}_{E,p} \colon G_K \to \mathrm{Aut}(E[p])$ for the corresponding Galois representation and $e_{E,p}$ for the Weil pairing on $E[p]$. We say that an $\mathbb{F}_p$-basis (P, Q) of $E[p]$ is *symplectic* if $e_{E,p}(P, Q) = \zeta_p$.

Now let E/K and E'/K be two elliptic curves over some field K and let $\phi \colon E[p] \to E'[p]$ be an isomorphism of G_K-modules. Then there is an element $r(\phi) \in \mathbb{F}_p^\times$ such that

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E,p}(P, Q)^{r(\phi)} \quad \text{for all } P, Q \in E[p].$$

Note that for any $a \in \mathbb{F}_p^\times$ we have $r(a\phi) = a^2 r(\phi)$. We say that ϕ is a *symplectic isomorphism* if $r(\phi) = 1$ or, more generally, $r(\phi)$ is a square in $\mathbb{F}_p^\times$. Fix a non-square $r_p \in \mathbb{F}_p^\times$. We say that ϕ is a *anti-symplectic isomorphism* if $r(\phi) = r_p$ or, more generally, $r(\phi)$ is a non-square in $\mathbb{F}_p^\times$. Finally, we say that $E[p]$ and $E'[p]$ are *symplectically* (or *anti-symplectically*) *isomorphic*, if there exists a symplectic (or anti-symplectic) isomorphism of G_K-modules between them.

Note that it is possible that $E[p]$ and $E'[p]$ are both symplectically and anti-symplectically isomorphic; this will be the case if and only if $E[p]$ admits an anti-symplectic automorphism.

Note that an isogeny $\phi\colon E \to E'$ of degree n not divisible by p restricts to an isomorphism $\phi\colon E[p] \to E'[p]$ such that $r(\phi) = n$. This can be seen from the following computation, where $\hat{\phi}$ is the dual isogeny, and where we use that fact that ϕ and $\hat{\phi}$ are adjoint with respect to the Weil pairing.

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E,p}(P, \hat{\phi}\phi(Q)) = e_{E,p}(P, nQ) = e_{E,p}(P, Q)^n.$$

In particular, ϕ induces a symplectic isomorphism on p-torsion if $(n/p) = 1$ and an anti-symplectic isomorphism if $(n/p) = -1$.

For an elliptic curve $E/\mathbb{Q}$ there are two modular curves $X_E^+(p) = X_E(p)$ and $X_E^-(p)$ defined over $\mathbb{Q}$ that parameterize pairs (E', ϕ) consisting of an elliptic curve E' and a symplectic (respectively, anti-symplectic) isomorphism $E'[p] \to E[p]$ (in the strict sense, i.e., such that $r(\phi) = 1$ or $r(\phi) = r_p$). These two curves are twists of the standard modular curve $X(p)$ that classifies pairs (E', ϕ) such that $\phi\colon E'[p] \to M$ is a symplectic isomorphism, with $M = \mu_p \times \mathbb{Z}/p\mathbb{Z}$ and a certain symplectic pairing on M, compare [PSS07]. As explained there, the existence of a non-trivial primitive solution (a, b, c) of (2.1) implies that some twisted Frey curve $E^{(d)}_{(a,b,c)}$ gives rise to a rational point on one of the modular curves $X_E(p)$ or $X_E^-(p)$ where E is one of the seven elliptic curves in Lemma 2.3. Thus the solution of Equation (2.1) for any particular $p \geq 11$ is reduced to the determination of the sets of rational points on 14 modular curves $X_E(p)$ and $X_E^-(p)$.

We remark that taking quadratic twists by d of the pairs (E', ϕ) induces canonical isomorphisms $X_{E^{(d)}}(p) \simeq X_E(p)$ and $X^-_{E^{(d)}}(p) \simeq X_E^-(p)$. Also note that each twist $X_E(p)$ has a 'canonical rational point' representing $(E, \mathrm{id}_{E[p]})$. On the other hand, it is possible that the twist $X_E^-(p)$ does not have any rational point. If E' is isogenous to E by an isogeny ϕ of degree n, then $(E', \phi|_{E'[p]})$ gives rise to a rational point on $X_E(p)$ when $(n/p) = +1$ and on $X_E^-(p)$ when $(n/p) = -1$.

In this section we will study carefully when isomorphisms of the torsion modules of elliptic curves preserve the Weil pairing. This will allow us to discard some of these 14 modular curves by local considerations. Of course, from the last paragraph of section 2 it follows that it is impossible to discard $X_{27a1}(p)$, $X_{288a1}(p)$ or $X_{864b1}(p)$, since they have rational points arising from the known solutions. Moreover, if $(2/p) = -1$ we also have a rational point on $X^-_{288a1}(p) \simeq X_{288a2}(p)$.

Let E and E' be elliptic curves over $\mathbb{Q}$ with isomorphic p-torsion. In [HK02] the authors give criteria for deciding under certain hypotheses if $E[p]$ and $E'[p]$ are symplectically isomorphic. We recall one such criterion, which will be of use later.

Theorem 4.1 ([HK02, Proposition A.1])**.** *Let E, E' be elliptic curves over $\mathbb{Q}$ with minimal discriminants Δ, Δ'. Let p be a prime such that $\overline{\rho}_{E,p} \simeq \overline{\rho}_{E',p}$. Suppose that E and E' have multiplicative reduction at a prime $\ell \neq p$ and that $p \nmid v_\ell(\Delta)$. Then $p \nmid v_\ell(\Delta')$, and the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are symplectically isomorphic if and only if $v_\ell(\Delta)/v_\ell(\Delta')$ is a square mod p.*

The objective of this section is to deduce similar results for certain types of additive reduction at ℓ (see also [HK02, Proposition A.2]), which we will then apply to our Diophantine problem in Theorem 5.1.

We will need the following simple criterion.

Lemma 4.2. *Let E and E' be two elliptic curves defined over a field K with isomorphic p-torsion. Fix symplectic bases for $E[p]$ and $E'[p]$. Let $\phi\colon E[p] \to E'[p]$ be an isomorphism of G_K-modules and write M_ϕ for the matrix representing ϕ with respect to the fixed bases.*

Then ϕ is a symplectic isomorphism if and only if $\det(M_\phi)$ is a square mod p; otherwise ϕ is anti-symplectic.

Moreover, if $\overline{\rho}_{E,p}(G_K)$ is a non-abelian subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, then $E[p]$ and $E'[p]$ cannot be simultaneously symplectically and anti-symplectically isomorphic.

Proof. Let $P, Q \in E[p]$ and $P', Q' \in E'[p]$ be the fixed symplectic bases. We have that

$$e_{E',p}(\phi(P), \phi(Q)) = e_{E',p}(P', Q')^{\det(M_\phi)} = {\zeta_p}^{\det(M_\phi)} = e_{E,p}(P, Q)^{\det(M_\phi)},$$

so $r(\phi) = \det(M_\phi)$. This implies the first assertion.

We now prove the second statement. Let $\beta\colon E[p] \to E'[p]$ be another isomorphism of G_K-modules. Then $\beta^{-1}\phi = \lambda$ is in the centralizer of $\overline{\rho}_{E,p}(G_K)$. Since $\overline{\rho}_{E,p}(G_K)$ is non-abelian, λ is represented by a scalar matrix, see [HK02, Lemme A.3]. Therefore $\det(M_\beta)$ and $\det(M_\phi)$ are in the same square class mod p. □

4.1. **A little group theory.**

Recall that H_8 denotes the quaternion group and $\mathrm{Dic}_{12} \simeq C_3 \rtimes C_4$ is the dicyclic group of 12 elements. Write D_n for the dihedral group with $2n$ elements and S_n for the symmetric group on n letters. We write $C(G)$ for the center of a group G. If H is a subgroup of G, then we write $N_G(H)$ for its normalizer and $C_G(H)$ for its centralizer in G.

Lemma 4.3. *Let $p \geq 3$ and $G = \mathrm{GL}_2(\mathbb{F}_p)$. Let $H \subset G$ be a subgroup isomorphic to H_8. Then the group $\mathrm{Aut}(H)$ of automorphisms of H satisfies*

$$N_G(H)/C(G) \simeq \mathrm{Aut}(H) \simeq S_4.$$

Moreover,

(a) *if $(2/p) = 1$, then all the matrices in $N_G(H)$ have square determinant;*
(b) *if $(2/p) = -1$, then the matrices in $N_G(H)$ with square determinant correspond to the subgroup of $\mathrm{Aut}(H)$ isomorphic to A_4.*

Proof. There is only one faithful two-dimensional representation of H_8 over $\mathbb{F}_p$ (H_8 has exactly one irreducible two-dimensional representation and any direct sum of one-dimensional representations factors over the maximal abelian quotient), so all subgroups H as in the statement are conjugate. We can therefore assume that H is the subgroup generated by

$$g_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix},$$

where $\alpha, \beta \in \mathbb{F}_p^\times$ satisfy $\alpha^2 + \beta^2 = -1$. It is easy to see that the elements of H span the $\mathbb{F}_p$-vector space of 2×2 matrices, which implies that $C_G(H) = C(G)$.

Now the action by conjugation induces a canonical group homomorphism $N_G(H) \to \mathrm{Aut}(H)$ with kernel $C_G(H) = C(G)$, leading to an injection $N_G(H)/C(G) \to \mathrm{Aut}(H)$. To see that this map is also surjective (and hence an isomorphism), note that $N_G(H)$ contains the matrices

$$n_1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad n_2 = \begin{pmatrix} \alpha & \beta - 1 \\ \beta + 1 & -\alpha \end{pmatrix}$$

and that the subgroup of $N_G(H)/C(G)$ generated by the images of H and of these matrices has order 24. Since it can be easily checked that $\mathrm{Aut}(H_8) \simeq S_4$, the first claim follows.

Note that A_4 is the unique subgroup of S_4 of index 2. The determinant induces a homomorphism $S_4 \simeq N_G(H)/C(G) \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ whose kernel is either S_4 or A_4. Since $H \subset \mathrm{SL}_2(\mathbb{F}_p)$ and all matrices in $C(G)$ have square determinant, it remains to compute $\det(n_1)$ and $\det(n_2)$. But $\det(n_1) = 2$ and

$$\det(n_2) = -\alpha^2 - (\beta - 1)(\beta + 1) = -\alpha^2 - \beta^2 + 1 = 2$$

as well. The result is now clear. □

Lemma 4.4. *Let $p \geq 5$ and $G = \mathrm{GL}_2(\mathbb{F}_p)$. Let $H \subset G$ be a subgroup isomorphic to Dic_{12}. Then the group of automorphisms of H satisfies*

$$N_G(H)/C(G) \simeq \mathrm{Aut}(H) \simeq D_6.$$

Moreover,

(a) *if $(3/p) = 1$, then all the matrices in $N_G(H)$ have square determinant;*
(b) *if $(3/p) = -1$, then the matrices in $N_G(H)$ with square determinant correspond to the subgroup of inner automorphisms in $\mathrm{Aut}(H)$.*

Proof. The proof is similar to that of Lemma 4.3. Again, there is a unique conjugacy class of subgroups isomorphic to Dic_{12} in G, so we can take H to be the subgroup generated by

$$g_1 = \begin{pmatrix} \alpha & \beta \\ \beta & 1 - \alpha \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where $\alpha, \beta \in \mathbb{F}_p$ satisfy $\beta^2 = -\alpha^2 + \alpha - 1$ with $\beta \neq 0$. As before, one sees that $C_G(H) = C(G)$, so we again have an injective group homomorphism $N_G(H)/C(G) \to \mathrm{Aut}(H) \simeq D_6$.

The normalizer $N_G(H)$ contains the matrix

$$M = \begin{pmatrix} 2\alpha - 1 & 2\beta \\ 2\beta & 1 - 2\alpha \end{pmatrix}$$

and the images of H and M generate a subgroup of order 12 of $N_G(H)/C(G)$, which shows that the homomorphism is also surjective.

Since $H \subset \mathrm{SL}_2(\mathbb{F}_p)$, the determinant of any element of $N_G(H)$ that induces an inner automorphism of H is a square. Also, the inner automorphism group of H has order 6, so the homomorphism $D_6 \simeq N_G(H)/C(G) \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ induced by the determinant is either trivial

or has kernel equal to the group of inner automorphisms. This depends on whether the determinant of M,

$$\det(M) = -4\alpha^2 + 4\alpha - 1 - 4\beta^2 = 3,$$

is a square in $\mathbb{F}_p$ or not. □

4.2. **Criteria for symplecticity.**

Let E, E' be elliptic curves over $\mathbb{Q}_\ell$ with potentially good reduction and set $L = \mathbb{Q}_\ell^{\mathrm{unr}}(E[p])$ and $L' = \mathbb{Q}_\ell^{\mathrm{unr}}(E'[p])$, where $\mathbb{Q}_\ell^{\mathrm{unr}}$ denotes the maximal unramified extension of $\mathbb{Q}_\ell$. Suppose that $E[p]$ and $E'[p]$ are isomorphic as $G_{\mathbb{Q}_\ell}$-modules. Then in particular they have the same inertial type, thus $L = L'$. Write $I = \mathrm{Gal}(L/\mathbb{Q}_\ell^{\mathrm{unr}})$ and $I_\ell = G_{\mathbb{Q}_\ell^{\mathrm{unr}}}$. If I is not abelian, then it follows from Lemma 4.2 and its proof that $E[p]$ and $E'[p]$ are symplectically isomorphic as $G_{\mathbb{Q}_\ell}$-modules if and only if they are symplectically isomorphic as I_ℓ-modules. Moreover, they cannot be both symplectically and anti-symplectically isomorphic. In Theorem 4.6 we provide a criterion to decide between the two possibilities when $\ell = 2$ and $I \simeq H_8$. In Theorem 4.7 we do the same for $\ell = 3$ and $I \simeq \mathrm{Dic}_{12}$.

We now introduce notation and recall facts from [ST68, Section 2] and [HK02, Appendice A]. Let p and ℓ be primes such that $p \geq 3$ and $\ell \neq p$. Let $E/\mathbb{Q}_\ell$, L and I be as above. Write $\overline{E}$ for the elliptic curve over $\overline{\mathbb{F}}_\ell$ obtained by reduction of a minimal model of E/L and $\varphi\colon E[p] \to \overline{E}[p]$ for the reduction morphism, which is a symplectic isomorphism of (trivial) G_L-modules. Let $\mathrm{Aut}(\overline{E})$ be the automorphism group of $\overline{E}$ over $\overline{\mathbb{F}}_\ell$ and write $\psi\colon \mathrm{Aut}(\overline{E}) \to \mathrm{GL}(\overline{E}[p])$ for the natural injective morphism. The action of I on L induces an injective morphism $\gamma_E\colon I \to \mathrm{Aut}(\overline{E})$. Moreover, for $\sigma \in I$ we have

$$\varphi \circ \overline{\rho}_{E,p}(\sigma) = \psi(\gamma_E(\sigma)) \circ \varphi. \tag{4.5}$$

Theorem 4.6. *Let $p \geq 3$ be a prime. Let E and E' be elliptic curves over $\mathbb{Q}_2$ with potentially good reduction. Suppose they have the same inertial type and that $I \simeq H_8$. Then $E[p]$ and $E'[p]$ are isomorphic as I_2-modules. Moreover,*

(1) *if $(2/p) = 1$, then $E[p]$ and $E'[p]$ are symplectically isomorphic I_2-modules;*
(2) *if $(2/p) = -1$, then $E[p]$ and $E'[p]$ are symplectically isomorphic I_2-modules if and only if $E[3]$ and $E'[3]$ are symplectically isomorphic I_2-modules.*

Proof. Note that $L = \mathbb{Q}_2^{\mathrm{unr}}(E[p])$ is the smallest extension of $\mathbb{Q}_2^{\mathrm{unr}}$ over which E acquires good reduction and that the reduction map φ is an isomorphism between the $\mathbb{F}_p$-vector spaces $E[p](L)$ and $\overline{E}[p](\overline{\mathbb{F}}_2)$. By hypothesis E' also has good reduction over L and φ' is an isomorphism. Applying equation (4.5) to both E and E' we see that $E[p]$ and $E'[p]$ are isomorphic I_2-modules, if we can show that $\psi\circ\gamma_E$ and $\psi\circ\gamma_{E'}$ are isomorphic as representations into $\mathrm{GL}(\overline{E}[p])$ and $\mathrm{GL}(\overline{E}'[p])$, respectively.

We have that $j(\overline{E}) = j(\overline{E}') = 0$ (see the proof of [DD15, Theorem 3.2]), thus E and E' are isomorphic over $\overline{\mathbb{F}}_2$. So we can fix minimal models of E/L and E'/L both reducing to the same $\overline{E}$. Note that $\mathrm{Aut}(\overline{E}) \simeq \mathrm{SL}_2(\mathbb{F}_3)$ (see [Sil09, Thm.III.10.1]) and that there is only one (hence normal) subgroup H of $\mathrm{SL}_2(\mathbb{F}_3)$ isomorphic to H_8. Therefore $\psi(\gamma_E(I)) = \psi(\gamma_{E'}(I)) = \psi(H)$ in $\mathrm{GL}(\overline{E}[p])$, and there must be an automorphism $\alpha \in \mathrm{Aut}(\psi(H))$ such that $\psi \circ \gamma_E =$

$\alpha \circ \psi \circ \gamma_{E'}$. The first statement of Lemma 4.3 shows that there is $g \in \mathrm{GL}(\overline{E}[p])$ such that $\alpha(x) = gxg^{-1}$ for all $x \in \psi(H)$; thus $\psi \circ \gamma_E$ and $\psi \circ \gamma_{E'}$ are isomorphic representations.

Fix a symplectic basis of $\overline{E}[p]$, thus identifying $\mathrm{GL}(\overline{E}[p])$ with $\mathrm{GL}_2(\mathbb{F}_p)$. Let M_g denote the matrix representing g and observe that $M_g \in N_{\mathrm{GL}_2(\mathbb{F}_p)}(\psi(H))$. Lift the fixed basis to bases of $E[p]$ and $E'[p]$ via the corresponding reduction maps φ and φ'. The lifted bases are symplectic. The matrices representing φ and φ' with respect to these bases are the identity. From (4.5) it follows that $\overline{\rho}_{E,p}(\sigma) = M_g \overline{\rho}_{E',p}(\sigma) M_g^{-1}$ for all $\sigma \in I$. Moreover, M_g represents some I_2-module isomorphism $\phi\colon E[p] \to E'[p]$, and from Lemma 4.2 we have that $E[p]$ and $E'[p]$ are symplectically isomorphic if and only if $\det(M_g)$ is a square mod p.

Part (1) then follows from Lemma 4.3 (a).

We now prove (2). From Lemma 4.3 (b) we see that $E[p]$ and $E'[p]$ are symplectically isomorphic if and only if α is an automorphism in $A_4 \subset \mathrm{Aut}(\psi(H)) \simeq S_4$. Note that these are precisely the inner automorphisms or automorphisms of order 3. Note also that all the elements in $S_4 \setminus A_4$ are not inner and have order 2 or 4. For each p the map $\alpha_p = \psi^{-1} \circ \alpha \circ \psi$ defines an automorphisms of $\gamma_E(I) = H \subset \mathrm{Aut}(\overline{E})$ satisfying $\alpha_p \circ \gamma_{E'} = \gamma_E$.

We note that the unique automorphism of $\mathrm{SL}_2(\mathbb{F}_3)$ which is the identity on the order 8 subgroup is the identity. Since γ_E, $\gamma_{E'}$ are independent of p, it follows that α_p is the same for all p. Since α and α_p have the same order and are simultaneously inner or not it follows that this property is independent of the prime p satisfying $(2/p) = -1$. This shows that $E[p]$ and $E'[p]$ are symplectically isomorphic I_2-modules if and only if $E[\ell]$ and $E'[\ell]$ are symplectically isomorphic I_2-modules for one (hence all) ℓ satisfying $(2/\ell) = -1$. In particular, we can take $\ell = 3$, and the result follows. □

Theorem 4.7. *Let $p \geq 5$ be a prime. Let E and E' be elliptic curves over $\mathbb{Q}_3$ with potentially good reduction. Suppose they have the same inertial type and $I \simeq \mathrm{Dic}_{12}$. Then $E[p]$ and $E'[p]$ are isomorphic as I_3-modules. Moreover,*

(1) *if $(3/p) = 1$, then $E[p]$ and $E'[p]$ are symplectically isomorphic I_3-modules;*
(2) *if $(3/p) = -1$, then $E[p]$ and $E'[p]$ are symplectically isomorphic I_3-modules if and only if $E[5]$ and $E'[5]$ are symplectically isomorphic I_3-modules.*

Proof. This proof is analogous to the proof of Theorem 4.6, with 3 and 5 taking over the roles of 2 and 3, respectively.

In this case $\mathrm{Aut}(\overline{E}) \simeq \mathrm{Dic}_{12}$ [Sil09, Thm.III.10.1], so $\psi(\gamma_E(I)) = \psi(\gamma_{E'}(I)) = \psi(\mathrm{Aut}(\overline{E}))$. We use Lemma 4.4 instead of Lemma 4.3 to conclude that α is given by a matrix M_g. Lemma 4.4 (a) concludes the proof of (1) and Lemma 4.4 (b) the proof of (2). □

5. Application to the Frey curves

Using the results in the previous section we will now show that one can discard some of the 14 twists of $X(p)$, depending on the residue class of p mod 24.

Theorem 5.1. *Let $p \geq 11$ be prime and let (a, b, c) be a non-trivial primitive solution (a, b, c) of $x^2 + y^3 = z^p$. Then the associated Frey curve $E^{(d)}_{(a,b,c)}$ gives rise to a rational point on one of the following twists of $X(p)$.*

- *If* $p \equiv 1 \bmod 24$*:*

$$X_{27a1}(p),\ X_{54a1}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)\,.$$

- *If* $p \equiv 5 \bmod 24$*:*

$$X_{27a1}(p),\ X_{54a2}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{288a2}(p),$$
$$X_{864a1}(p),\ X^-_{864a1}(p),\ X_{864b1}(p),\ X^-_{864b1}(p),\ X_{864c1}(p),\ X^-_{864c1}(p)\,.$$

- *If* $p \equiv 7 \bmod 24$*:*

$$X_{27a1}(p),\ X_{54a2}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)\,.$$

- *If* $p \equiv 11 \bmod 24$*:*

$$X_{27a1}(p),\ X_{54a1}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{288a2}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)\,.$$

- *If* $p \equiv 13 \bmod 24$*:*

$$X_{27a1}(p),\ X_{96a2}(p),\ X_{288a1}(p),\ X_{288a2}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)\,.$$

- *If* $p \equiv 17 \bmod 24$*:*

$$X_{27a1}(p),\ X_{54a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)\,.$$

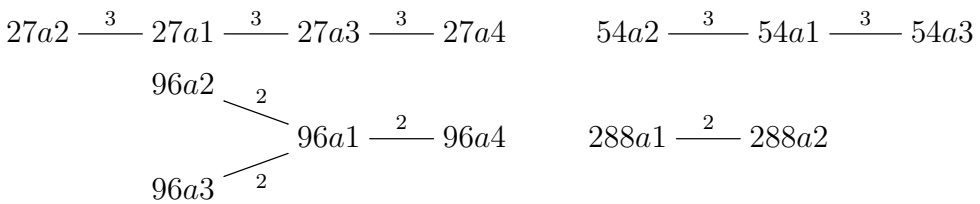
- *If* $p \equiv 19 \bmod 24$*:*

$$X_{27a1}(p),\ X_{54a1}(p),\ X_{96a2}(p),\ X_{288a1}(p),\ X_{288a2}(p),$$
$$X_{864a1}(p),\ X^-_{864a1}(p),\ X_{864b1}(p),\ X^-_{864b1}(p),\ X_{864c1}(p),\ X^-_{864c1}(p)\,.$$

- *If* $p \equiv 23 \bmod 24$*:*

$$X_{27a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)\,.$$

Proof. Note that among the seven elliptic curves in Lemma 2.3, $27a1$ and $288a1$ have complex multiplication by $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$, respectively, where ω is a primitive cube root of unity. We note also that the isogeny classes of the first four curves in the list of Lemma 2.3 have the following structure (the edges are labeled by the degree of the isogeny):



whereas the isogeny classes of the last three curves are trivial (see [Cre97, Table 1]). We also note that $27a3$ is the quadratic twist by -3 of $27a1$, so that $X_{27a1}(p) \simeq X_{27a3}(p)$. If $(3/p) = -1$, then the 3-isogeny between these curves induces an anti-symplectic isomorphism of the mod p Galois representations, and we have that $X_{27a1}(p) \simeq X_{27a3}(p) \simeq X^-_{27a1}(p)$. So when $p \equiv 5, 7, 17, 19 \bmod 24$, we only have one twist of $X(p)$ coming from $27a1$. (For the other CM curve, $288a1$, this argument does not apply, since it is its own -1-twist.)

For the twists associated to the curves $54a1$ and $96a1$ we apply Theorem 4.1. From Table 1 we see that the Frey curve $E^{(d)}_{(a,b,c)}$ has multiplicative reduction at $\ell = 2$ if and only if c is even and $d = \pm 1, \pm 3$, in which case its minimal discriminant is $\Delta = 2^{-6}3^3d^6c^p$ (compare the proof of [PSS07, Lemma 4.6]); in particular, $v_2(\Delta) \equiv -6 \bmod p$. Then the Frey curve

must be p-congruent to $E = 54a1$ (which is the only curve in our list that has multiplicative reduction at 2). On the other hand, $\Delta_E = -2^3 3^9$, so that the isomorphism between $E^{(d)}_{(a,b,c)}[p]$ and $E[p]$ is symplectic if and only if $(-2/p) = 1$. So for $p \equiv 1, 11, 17, 19 \bmod 24$, we get rational points at most on $X_{54a1}(p)$, whereas for $p \equiv 5, 7, 13, 23 \bmod 24$, we get rational points at most on $X^-_{54a1}(p)$ (which is $X_{54a2}(p)$ when $(3/p) = -1$). Similarly, Table 2 shows that the Frey curve has multiplicative reduction at $\ell = 3$ if and only if c is divisible by 3. In this case $d = \pm 3, \pm 6$ and the minimal discriminant is $\Delta = 2^6 3^{-3} c^p$ (see again the proof of [PSS07, Lemma 4.6]), so $v_3(\Delta) \equiv -3 \bmod p$. Since $E = 96a1$ is the only curve in our list that has multiplicative reduction at 3, the Frey curve must be p-congruent to it. Since $\Delta_E = 2^6 3^2$, we find that the isomorphism between $E^{(d)}_{(a,b,c)}[p]$ and $E[p]$ is symplectic if and only if $(-6/p) = 1$. So for $p \equiv 1, 5, 7, 11 \bmod 24$ we get rational points at most on $X_{96a1}(p)$, whereas for $p \equiv 13, 17, 19, 23 \bmod 24$, we get rational points at most on $X^-_{96a1}(p)$ (which is X_{96a2} when $(2/p) = -1$).

Now we consider the curves E with conductor at 2 equal to 2^5; these are $96a1$, $288a1$, $864a1$, $864b1$ and $864c1$. They all have potentially good reduction at 2 and $I = \mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}}) \simeq H_8$. Since H_8 is non-abelian, by the proof of Lemma 4.2 the isomorphism of mod p Galois representations is symplectic if and only if it is symplectic on the level of inertia groups. It follows from Theorem 4.6 (1) that when $(2/p) = 1$ the isomorphism $E^{(d)}_{(a,b,c)}[p] \simeq E[p]$ can only be symplectic. So for $p \equiv 1, 7, 17, 23 \bmod 24$, we can exclude the 'minus' twists $X^-_E(p)$ for $E \in \{96a1, 288a1, 864a1, 864b1, 864c1\}$.

We can use a similar argument over $\mathbb{Q}_3$ for the curves E in our list whose conductor at 3 is 3^3, namely $27a1$, $54a1$, $864a1$, $864b1$ and $864c1$. They all have potentially good reduction and $I \simeq \mathrm{Dic}_{12}$. By Theorem 4.7 (1) we conclude that the isomorphism $E^{(d)}_{(a,b,c)}[p] \simeq E[p]$ must be symplectic when $(3/p) = 1$. Thus we can exclude the twists $X^-_E(p)$ for E in the set $\{27a1, 54a1, 864a1, 864b1, 864c1\}$ when $p \equiv 1, 11, 13, 23 \bmod 24$.

Finally, from the isogeny diagrams we see that $X_{96a2}(p) \simeq X^-_{96a1}(p)$ and $X_{288a2}(p) \simeq X^-_{288a1}(p)$ when $(2/p) = -1$; and also $X_{54a2}(p) \simeq X^-_{54a1}(p)$ when $(3/p) = -1$. This concludes the proof. □

We have already observed that $X_E(p)$ for $E \in \{27a1, 288a1, 288a2, 864b1\}$ always has a rational point coming from a primitive solution of (2.1), so these twists cannot be excluded. In a similar way, we see that we cannot exclude $X_E(p)$ by local arguments over $\mathbb{Q}_\ell$ with $\ell = 2$ or 3, if E can be obtained as a Frey curve coming from an ℓ-adically primitive solution of (2.1). Note that any ℓ-adic unit is a p-th power in $\mathbb{Q}_\ell$ (for $\ell \in \{2, 3\}$ and $p \geq 5$). For $\ell = 2$, we have the following triples (a, b, E) (such that $a, b \in \mathbb{Z}_2$ are coprime and $a^2 + b^3 \in \mathbb{Z}_2^\times$).

$$(253, -40, 27a2), \quad (10, -7, 96a1), \quad (46, -13, 96a2), \quad (1, 2, 864c1).$$

For $\ell = 3$, we only obtain $(13, 7, 54a1)$ and $(3, -1, 864a1)$. The remaining combinations (E, ℓ), namely

$$(27a2, 3),\ (54a1, 2),\ (54a2, 2),\ (54a2, 3),\ (54a3, 2),\ (54a3, 3),\ (96a1, 3),$$
$$(96a2, 3),\ (96a3, 2),\ (96a3, 3),\ (96a4, 2),\ (96a4, 3),\ (864a1, 2),\ (864c1, 3),$$

do not arise in this way. This can be verified by checking whether there is $d \in \mathbb{Q}_\ell^\times$ such that $a = c_6(E)d^3$ and $b = -c_4(E)d^2$ are coprime ℓ-adic integers such that $a^2 + b^3$ is an ℓ-adic unit.

In the remainder of this section we will show that there are nevertheless always 2-adic and 3-adic points corresponding to primitive solutions on the twists $X_E^{\pm}(p)$ listed in Theorem 5.1.

Lemma 5.2. *Let $p \geq 7$ be a prime such that $(2/p) = -1$. Then the p-torsion $G_{\mathbb{Q}_2}$-modules of the following curves admit exclusively the following isomorphism types:*

$$96a1 \overset{+}{\simeq} 864c1, \quad 288a1 \overset{+}{\simeq} 864b1, \quad 288a1 \overset{-}{\simeq} 864a1, \quad 864b1 \overset{-}{\simeq} 864a1,$$

where $+$ means symplectic and $-$ anti-symplectic. Moreover, let a, b be coprime integers satisfying the congruences in line j of Table 1 and write $E = E^{(d)}_{(a,b,c)}/\mathbb{Q}_2$, where d is any of the possible values in the same line. Then, up to quadratic twist, the p-torsion $G_{\mathbb{Q}_2}$-modules of the following curves admit exclusively the following isomorphism types:

$$\begin{array}{lccc}
j = 3, 10\colon & E \overset{+}{\simeq} 288a1, & E \overset{+}{\simeq} 864b1, & E \overset{-}{\simeq} 864a1 \\
j = 4\colon & E \overset{-}{\simeq} 288a1, & E \overset{-}{\simeq} 864b1, & E \overset{+}{\simeq} 864a1 \\
j = 5, 9\colon & E \overset{+}{\simeq} 96a1, & E \overset{+}{\simeq} 864c1 & \\
j = 6\colon & E \overset{-}{\simeq} 96a1, & E \overset{-}{\simeq} 864c1 &
\end{array}$$

Furthermore, if instead $p \geq 3$ satisfies $(2/p) = 1$, then all the previous isomorphisms are symplectic.

Proof. Let E and E' be any choice of curves that are being compared in the statement. From Theorem 4.6 we know there is an isomorphism of I_2-modules $\phi\colon E[p] \to E'[p]$. Moreover, from part (2) we know that $E[p]$ and $E'[p]$ are (exclusively) symplectically or anti-symplectically isomorphic if and only if $E[3]$ and $E'[3]$ are. We computed (for $p = 3$) the matrix M_ϕ in Lemma 4.2 using Magma to conclude that the results in the statement hold at the level of inertia. To finish the proof we will show that the I_2-module isomorphism between $E[p]$ and $E'[p]$ extends to the whole of $G_{\mathbb{Q}_2}$ up to unramified quadratic twist.

Write $L = \mathbb{Q}_2^{\mathrm{unr}}(E[n])$ and $I = \mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}})$ as usual (recall that L is independent of $n \geq 3$). Write also $L_n = \mathbb{Q}_2(E[n])$ for the field fixed by the representation on the n-torsion. Let U_n be the maximal unramified extension inside L_n. The group I can be naturally identified with the subgroup of $G_n = \mathrm{Gal}(L_n/\mathbb{Q}_2)$ that fixes U_n. In what follows we implicitly use this identification. In particular, $\overline{\rho}_{E,n}|_I \simeq \overline{\rho}_{E',n}|_I$.

Note that all the curves in the statement obtain good reduction over L_3 and that they all have the trace of Frobenius $a_{L_3} = -4$. Thus $\overline{\rho}_{E,n}|_{G_{L_3}} \simeq \overline{\rho}_{E',n}|_{G_{L_3}}$.

Since all the curves involved have conductor 2^5, their discriminants are cubes in $\mathbb{Q}_2$. Thus, by [DD08, Table 1] we conclude that $G_3 = \mathrm{Gal}(L_3/\mathbb{Q}_2)$ is isomorphic to the semi-dihedral group with 16 elements, hence $H_8 \simeq I \subset G_3$ with index 2, thus $[U_3 : \mathbb{Q}_2] = 2$. (Note that explicit Magma computations can also prove these statements, since we only have to consider a finite list of curves).

The field $L_{3p} = U_p \cdot L_3$ satisfies $[L_{3p} : L_p] \leq 2$ with equality holding if and only if $U_p \cap U_3 = \mathbb{Q}_2$. Moreover, the groups $N = \mathrm{Gal}(L_{3p}/L_3)$ and $I = \mathrm{Gal}(L_{3p}/U_{3p})$ generate $G_{U_3} := \mathrm{Gal}(L_{3p}/U_3)$.

We apply [Cen15, Theorem 2] to find that there is a basis in which $\overline{\rho}_{E,p}(\mathrm{Frob}_2)$ is the scalar matrix $-2 \cdot \mathrm{Id}_2$. Thus the same is true in all bases; therefore $\overline{\rho}_{E,p}(\mathrm{Frob}_2)$ commutes with all

matrices in $\overline{\rho}_{E,p}(I)$. Since the same is true for E', the isomorphism between $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ on the subgroups I and N extends to G_{U_3}.

Since the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are irreducible and $[U_3 : \mathbb{Q}_2] = 2$, they differ at most by the quadratic character fixing U_3.

Since $U_3 \subset L_3$, we have that $\mathrm{Gal}(U_3/\mathbb{Q}_2)$ is a quotient of G_3. Thus if the 3-torsion representations are already isomorphic, we do not need to take the quadratic twist. The explicit computations show that this is what happens when comparing the curves $96a1$, $288a1$, $864a1$, $864b1$, $864c1$ among themselves, but that this is not always the case when comparing them against $E^{(d)}_{(a,b,c)}$.

The last statement follows from Theorem 4.6 (1). □

Since the isomorphism class of $X_E(p)$ (or $X^-_E(p)$) depends only on the symplectic Galois module $E[p]$, the lemma implies that over $\mathbb{Q}_2$, $X^{\pm}_{96a1}(p) \simeq X^{\pm}_{864c1}(p)$ and $X^{\pm}_{288a1}(p) \simeq X^{\pm}_{864b1}(p)$ (writing $X^+_E(p) = X_E(p)$), and also that $X^{\pm}_{288a1}(p) \simeq X^{\pm}_{864a1}(p)$ when $(2/p) = 1$, whereas $X^{\pm}_{288a1}(p) \simeq X^{\mp}_{864a1}(p)$ when $(2/p) = -1$. Furthermore, in the latter case, we obtain 'primitive' 2-adic points on $X^-_E(p)$ for $E \in \{96a1, 288a1, 864a1, 864b1, 964c1\}$.

Lemma 5.3. *Let $p \geq 7$ be a prime such that $(3/p) = -1$. Then the p-torsion $G_{\mathbb{Q}_3}$-modules of the following curves admit exclusively the following isomorphism types:*

$$27a1 \overset{+}{\simeq} 864c1, \quad 27a1 \overset{-}{\simeq} 864b1, \quad 864b1 \overset{-}{\simeq} 864c1, \quad 54a1 \overset{-}{\simeq} 864a1,$$

where $+$ means symplectic and $-$ anti-symplectic. Moreover, let a, b be coprime integers satisfying the congruences in line i of Table 2 and write $E = E^{(d)}_{(a,b,c)}/\mathbb{Q}_3$. Then the p-torsion $G_{\mathbb{Q}_3}$-modules of the following curves admit exclusively the following isomorphism types:

$$\begin{array}{llll}
i = 4, 6, & d = \pm 1, \pm 2: & E \overset{-}{\simeq} 27a1, \quad E \overset{+}{\simeq} 864b1, & E \overset{-}{\simeq} 864c1 \\
i = 4, 6, & d = \pm 3, \pm 6: & E \overset{+}{\sim} 27a1, \quad E \overset{-}{\sim} 864b1, & E \overset{-}{\sim} 864c1 \\
i = 5, 8, & d = \pm 1, \pm 2: & E \overset{-}{\sim} 54a1, \quad E \overset{+}{\sim} 864a1 & \\
i = 5, 8, & d = \pm 3, \pm 6: & E \overset{+}{\sim} 54a1, \quad E \overset{-}{\sim} 864a1 &
\end{array}$$

Furthermore, if instead $p \geq 7$ satisfies $(3/p) = 1$, then all the previous isomorphisms are symplectic.

Proof. This is similar to the previous lemma, where we replace 2 and 3 by 3 and 5 respectively. Arguing as above, we see that $I = \mathrm{Gal}(L_{5p}/U_{5p})$ and $N = \mathrm{Gal}(L_{5p}/L_5)$ generate $G_{U_5} := \mathrm{Gal}(L_{5p}/U_5)$. Moreover, since all the curves in the statement acquire good reduction over L_5 and have trace of Frobenius $a_{L_5} = -18$, we conclude in the same way as before that $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are isomorphic when restricted to G_{U_5}. Since $[U_5 : \mathbb{Q}_3] = 4$, it could be possible that the representations differ by a quartic twist, but explicit computations show that we can always make the representations on the 5-torsion isomorphic after a quadratic twist. □

The statements of this lemma can be translated in terms of isomorphisms over $\mathbb{Q}_3$ and 'primitive' $\mathbb{Q}_3$-points in the same way as for the previous lemma.

These results already show that all the curves $X^{\pm}_E(p)$ listed in Theorem 5.1 have 'primitive' 2-adic and 3-adic points (and therefore cannot be ruled out by local considerations at 2 and 3),

with the possible exception of 2-adic points on $X^{\pm}_{54a1}(p)$ and 3-adic points on $X^{\pm}_{96a1}(p)$. The next proposition and corollary show that these curves also have these local 'primitive' points. This then implies that the information in Theorem 5.1 is optimal in the sense that we cannot exclude more of the twists using purely local arguments.

Proposition 5.4. *Let $\ell \neq p$ be primes with $p \geq 3$. Let E_1 and E_2 be Tate curves over $\mathbb{Q}_\ell$ with parameters q_1 and q_2. Assume that $q_1^{r_1} = q_2^{r_2} s^p$ with $s \in \mathbb{Q}_\ell$ and $r_1, r_2 \in \mathbb{Z}$ with $p \nmid r_i$. Write $e_1 = v_\ell(\Delta_{E_1})$ and $e_2 = v_\ell(\Delta_{E_2})$ for the ℓ-adic valuations of the minimal discriminants. Suppose that $p \nmid e_1 e_2$. Then the I_ℓ-modules $E_1[p]$ and $E_2[p]$ are isomorphic. If in addition $\ell = 2$ or 3, then $E_1[p]$ and $E_2[p]$ are even isomorphic as $G_{\mathbb{Q}_\ell}$-modules.*

Proof. Since $p \nmid e_1 e_2$, we can find coprime integers n and m satisfying $e_2 = ne_1 + pm$.

Let $\gamma_1, \gamma_2 \in \overline{\mathbb{Q}}_\ell$, $\alpha \in \mathbb{Q}_\ell^{\mathrm{unr}}$ satisfy $\gamma_1^p = q_1$, $\alpha^p = q_2/q_1^n \ell^{mp}$ and $\gamma_2 = \gamma_1^n \ell^m \alpha$ (hence $\gamma_2^p = q_2$).

Fix a primitive p-th root of unity ζ. The theory of the Tate curve implies that we can use $\zeta q_1^{\mathbb{Z}}, \gamma_1 q_1^{\mathbb{Z}}$ and $\zeta q_2^{\mathbb{Z}}, \gamma_2 q_2^{\mathbb{Z}}$ as $\mathbb{F}_p$-bases for the p-torsion of E_1 and E_2, respectively. In terms of these bases we have

$$\overline{\rho}_{E_i,p} = \begin{pmatrix} \chi_p & h_i \\ 0 & 1 \end{pmatrix},$$

where χ_p is the mod p cyclotomic character and $h_i \colon G_{\mathbb{Q}_\ell} \to \mathbb{F}_p$ becomes a non-trivial group homomorphism when restricted to I_ℓ.

Write K_p for the p-torsion field of E_1; the relation between q_1 and q_2 implies that K_p is also the p-torsion field of E_2, that is, $\overline{\rho}_{E_1,p}$ and $\overline{\rho}_{E_2,p}$ have the same kernel. In particular, the inertia subgroup of $\mathrm{Gal}(K_p/\mathbb{Q}_\ell)$ is cyclic of order p and is generated by the element σ such that $\sigma(\zeta) = \zeta$ and $\sigma(\gamma_1) = \zeta\gamma_1$; thus $\sigma(\gamma_2) = \zeta^n \gamma_2$. We can directly check that $M_b \overline{\rho}_{E_1,p}(\sigma) = \overline{\rho}_{E_2,p}(\sigma) M_b$, where

$$\overline{\rho}_{E_1,p}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \overline{\rho}_{E_2,p}(\sigma) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \quad M_b = \begin{pmatrix} n & b \\ 0 & 1 \end{pmatrix} \text{ for any } b \in \mathbb{F}_p.$$

The first statement follows.

We will now prove the second statement. Write τ for a Frobenius element at ℓ. Let $n_\alpha \in \mathbb{F}_p^\times$ be defined by $\tau(\alpha)/\alpha = \zeta^{n_\alpha}$. We have that $\tau(\zeta) = \zeta^\ell$, $\tau(\gamma_1) = \zeta^{h_1(\tau)}\gamma_1$ and

$$\tau(\gamma_2) = \tau(\gamma_1^n \ell^m \alpha) = \ell^m \tau(\alpha) \zeta^{h_1(\tau)n} \gamma_1^n = \frac{\tau(\alpha)}{\alpha} \zeta^{h_1(\tau)n} \gamma_1^n \ell^m \alpha = \zeta^{n_\alpha + h_1(\tau)n} \gamma_2$$

We have to show that $M_b \overline{\rho}_{E_1,p}(\tau) = \overline{\rho}_{E_2,p}(\tau) M_b$ for some choice of $b \in \mathbb{F}_p$, where

$$\overline{\rho}_{E_1,p}(\tau) = \begin{pmatrix} \ell & h_1(\tau) \\ 0 & 1 \end{pmatrix}, \quad \overline{\rho}_{E_2,p}(\tau) = \begin{pmatrix} \ell & h_1(\tau)n + n_\alpha \\ 0 & 1 \end{pmatrix}.$$

The condition $M_b \overline{\rho}_{E_1,p}(\tau) = \overline{\rho}_{E_2,p}(\tau) M_b$ translates to the condition that $b \in \mathbb{F}_p$ satisfies $b(1-\ell) = n_\alpha$, which is always possible if we can invert $1 - \ell$ in $\mathbb{F}_p$. For odd p and $\ell = 2$, 3 this is the case. □

Corollary 5.5. *There are primitive 2-adic points on $X^{\pm}_{54a1}(p)$ for $p \geq 3$. There are primitive 3-adic points on $X^{\pm}_{96a1}(p)$ for $p \geq 5$. The signs $\pm$ here are as given by the entries in Table 4 (which for the curves considered here summarizes Theorem 5.1).*

Proof. Let W denote the curve $54a1$. From Table 1 we see that for the Frey curve $E = E_{a,b,c}$ to be p-congruent to W we must have $v_2(c) > 0$ and $v_2(a) = v_2(b) = 0$. Note that we can always find $a, b, c \in \mathbb{Q}_2$ satisfying the previous conditions and $a^2 + b^3 = c^p$.

Up to unramified quadratic twist the curves $W/\mathbb{Q}_2$ and $E/\mathbb{Q}_2$ are Tate curves with parameters q_W and q_E respectively. We have $v_2(q_W) = v_2(\Delta_W) = 3$ and $v_2(q_E) = -v_2(j_E) = -6+pv_2(c)$.

We want to find $r_1, r_2 \in \mathbb{Z}$ not divisible by p such that $q_E^{r_1}/q_W^{r_2} = s^p$, $s \in \mathbb{Q}_2$. Since every unit in $\mathbb{Q}_2$ is a p-th power, we only have to find r_i such that $v_2(q_E^{r_1}/q_W^{r_2})$ is a multiple of p. This is always possible. From the previous proposition we conclude that (up to quadratic twist) $E[p]$ and $W[p]$ are isomorphic $G_{\mathbb{Q}_2}$-modules. Therefore we get 2-adic points on $X^+_{54a1}(p)$ or $X^-_{54a1}(p)$ according to the signs in Table 4.

For the curve $96a1$ we argue in the same way, but over $\mathbb{Q}_3$ instead of $\mathbb{Q}_2$. □

6. Ruling out twists coming from CM curves

In [BPR13, Corollary 1.2] it is shown that for $p \geq 11$, $p \neq 13$, the image of the mod p Galois representation of any elliptic curve E over $\mathbb{Q}$ is never contained in the normalizer of a split Cartan subgroup unless E has complex multiplication. This allows us to deduce the following.

Lemma 6.1. *Let $p \geq 17$ be a prime number.*

(1) *If $p \equiv 1 \bmod 3$, then the only primitive solutions of (2.1) coming from rational points on $X^{\pm}_{27a1}(p)$ are the trivial solutions $(\pm 1)^2 + 0^3 = 1^p$.*
(2) *If $p \equiv 1 \bmod 4$, then the only primitive solutions of (2.1) coming from rational points on $X^{\pm}_{288a1}(p)$ are the trivial solutions $0^2 + (\pm 1)^3 = (\pm 1)^p$ (with the same sign on both sides).*

Proof. If a primitive solution (a, b, c) gives rise to a Frey curve E' such that $E'[p] \cong E[p]$ for $E = 27a1$, then the image of Galois in $\mathrm{GL}(E'[p]) \cong \mathrm{GL}(E[p])$ is contained in the normalizer of a split Cartan subgroup, since E has complex multiplication by $\mathbb{Z}[\omega]$ and p splits in this ring when $p \equiv 1 \bmod 3$. It follows that E' also has complex multiplication, which implies that $c = \pm 1$. Since the Frey curve of the Catalan solution does not have CM, the solution must be trivial, and then only the given solution corresponds to the right curve E. The other case is similar, using the fact that $288a1$ has CM by $\mathbb{Z}[i]$. □

A separate computation for the case $p = 13$, see Lemma 8.2 below, shows that Lemma 6.1 remains valid in that case, even though the result of [BPR13] does not apply.

We can therefore further reduce the list of twists of $X(p)$ that have to be considered. This results in Table 4, where an entry '+' (resp., '−') indicates that the twist $X_E(p)$ (resp., $X^-_E(p)$) cannot (so far) be ruled out to have rational points giving rise to a non-trivial primitive solution of (2.1).

Unfortunately, there is no similar result on mod p Galois representations whose image is contained in the normalizer of a non-split Cartan subgroup. Such a result would allow us to eliminate the curves $27a1$ and $288a1$ also in the remaining cases.

p mod 24	$27a1$	$54a1$	$96a1$	$288a1$	$864a1$	$864b1$	$864c1$
1		+	+		+	+	+
5	+	−	+		+−	+−	+−
7		−	+	+	+	+	+
11	+	+	+	+−	+	+	+
13			−		+	+	+
17	+	+			+	+	+
19		+	−	+−	+−	+−	+−
23	+			+	+	+	+

TABLE 4. Twists of $X(p)$ remaining after local considerations and using information on $X^+_{\mathrm{split}}(p)$, according to p mod 24. This table is valid for $p \geq 11$.

In Section 7.1 below we show how one can deal with the non-split case when $p = 11$, by considering the twists $X^{(-1)}_{\mathrm{ns}}(p)$ and $X^{(-3)}_{\mathrm{ns}}(p)$ of the double cover $X_{\mathrm{ns}}(p) \to X^+_{\mathrm{ns}}(p)$, where $X_{\mathrm{ns}}(p)$ classifies elliptic curves such that the image of the mod p Galois representation is contained in a non-split Cartan subgroup and $X^+_{\mathrm{ns}}(p)$ does the same for the normalizer of a non-split Cartan subgroup. It turns out that for $p = 11$ the two curves $X^{(-1)}_{\mathrm{ns}}(11)$ and $X^{(-3)}_{\mathrm{ns}}(11)$ are not directly amenable to a Chabauty argument; instead one can use suitable coverings and Elliptic Curve Chabauty. The following argument shows that the failure of the Chabauty condition is a general phenomenon.

By a result of Chen [Che98] (see also [dSE00]) the Jacobian variety $J_0(p^2)$ of $X_0(p^2)$ is isogenous to the product $\mathrm{Jac}(X_{\mathrm{ns}}(p)) \times \mathrm{Jac}(X_0(p))^2$. On the other hand, a theorem of Shimura [Shi71, Thm. 7.14] implies that $J_0(p^2)$ is isogenous to the product $\prod_f A_f^{m_f}$, where f runs over a system of representatives of the Galois orbits of newforms of level M_f dividing p^2 and weight 2, A_f is the abelian variety over $\mathbb{Q}$ associated to f defined by Shimura, and $p^{3-m_f} = M_f$. It follows that $\mathrm{Jac}(X_{\mathrm{ns}}(p))$ is isogenous to the product of the A_f such that f is a newform in $S_2(\Gamma_0(p^2))$. Similarly, the Jacobian of $X^+_{\mathrm{ns}}(p)$ corresponds to the product of the A_f for the subset of f invariant under the Atkin-Lehner involution W at level p^2.

If $p \equiv -1 \bmod 4$, we need to exclude rational points on the twists $X^{\pm}_{288a1}(p)$; solutions associated to this curve will give rise to rational points on the (-1)-twist $X^{(-1)}_{\mathrm{ns}}(p)$ of the double cover $X_{\mathrm{ns}}(p) \to X^+_{\mathrm{ns}}(p)$. Similarly, for $p \equiv -1 \bmod 3$, we need to exclude rational points on the twist $X_{27a1}(p)$, and solutions associated to that curve will give rise to rational points on $X^{(-3)}_{\mathrm{ns}}(p)$. To be able to use Chabauty's method, we would need to have a factor of the Jacobian $J^{(d)}_{\mathrm{ns}}(p)$ (for $d = -1$ and/or $d = -3$) of Mordell-Weil rank strictly less than its dimension. Since all these factors have real multiplication (defined over $\mathbb{Q}$), the Mordell-Weil rank is always a multiple of the dimension, so we actually need a factor of rank zero.

By the above, we know that $J^{(d)}_{\mathrm{ns}}(p)$ splits up to isogeny as the product of the twists $A^{(d)}_f$ for newforms f such that $f|_W = -f$ and the untwisted A_f for f such that $f|_W = f$. The L-series of $A^{(d)}_f$ is the product of $L({}^\sigma f_\chi, s)$, where ${}^\sigma f$ runs through the newforms in the Galois orbit and χ is the quadratic character associated to d, see [Shi71, Section 7.5]. By a theorem of Weil [Wei67, Satz 1] all these L-series have root number -1 when $f|_W = -f$ and $d < 0$ is

squarefree (note that $C = 1$ from $f|_W = -f$, ε is trivial, χ is real, so $g(\chi) = g(\bar{\chi})$, and $A = p^2$, so that $\chi(-A) = \chi(-1) = -1$), so $L(A_f^{(d)}, s)$ vanishes at least to order $\dim A_f^{(d)}$ at $s = 1$. For the f that are invariant under W we also have that the root number of $L({}^{\sigma}f, s)$ is -1, so $L(A_f, s)$ also vanishes to order at least $\dim A_f$. Assuming the Birch and Swinnerton-Dyer conjecture, it follows that all factors of $J_{\mathrm{ns}}^{(d)}(p)$ have positive rank.

To conclude this section, we mention that when $p = 13$, we are in the split case for both CM curves, but we have the problem that there is no proof so far that the set of rational points on $X_{\mathrm{sp}}^{+}(13)$ consists of cusps and CM points, although this is almost certainly the case. (The curve is of genus 3 and its Jacobian has Mordell-Weil rank 3, see [Bar14] and [BPS16].) We tried an approach similar to that used in Section 7.1 below, but did not succeed. However, a different approach using twists of $X_1(13)$ is successful; see Lemma 8.2 below.

7. The Generalized Fermat Equation with exponents 2, 3, 11

We now consider the case $p = 11$. In this section we will prove the following theorem.

Theorem 7.1. *Assume the Generalized Riemann Hypothesis. Then the only primitive integral solutions of the equation $x^2 + y^3 = z^{11}$ are the trivial solutions $(\pm 1, 0, 1)$, $\pm(0, 1, 1)$, $(\pm 1, -1, 0)$ and the Catalan solutions $(\pm 3, -2, 1)$.*

We note at this point that the Generalized Riemann Hypothesis is only used to verify the correctness of the computation of the class groups of five specific number fields of degree 36.

In the following we will say that $j \in \mathbb{Q}$ is *good* if it is the j-invariant of a Frey curve associated to a primitive integral solution of $x^2 + y^3 = z^{11}$, which means that $j = (12b)^3/c^{11}$ and $12^3 - j = 12^3a^2/c^{11}$ with coprime integers a, b, c. In a similar way, we say that $j \in \mathbb{Q}_2$ is 2-*adically good* if it has this form for coprime 2-adic integers a, b, c.

By Theorem 5.1, it suffices to find the rational points on the twisted modular curves $X_E(11)$ for the elliptic curves $E \in \mathcal{E}'$, where

$$\mathcal{E}' = \{27a1, 54a1, 96a1, 288a1, 288a2, 864a1, 864b1, 864c1\},$$

such that their image on the j-line is good.

7.1. The CM curves.

In the case $p = 11$, we can deal with the CM curves $E \in \{27a1, 288a1, 288a2\}$ in the following way. Note that since $(-1/11) = (-3/11) = -1$, the images of both relevant Galois representations are contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(2, \mathbb{F}_{11})$. Elliptic curves with this property are parameterized by the modular curve $X_{\mathrm{ns}}^{+}(11)$, which is the elliptic curve $121b1$ of rank 1. It has as a double cover the curve $X_{\mathrm{ns}}(11)$ parameterizing elliptic curves E such that the image of the mod 11 Galois representation is contained in a non-split Cartan subgroup. Elliptic curves whose mod 11 representation is isomorphic to that of $288a1$ (or $288a2$) or $27a1$ will give rise to rational points on the quadratic twists $X_{\mathrm{ns}}^{(-1)}(11)$ and $X_{\mathrm{ns}}^{(-3)}(11)$ of this double cover. These curves are of genus 4; the Jacobian of $X_{\mathrm{ns}}(11)$ is isogenous to the product of the four elliptic curves $121a1$, $121b1$, $121c1$ and $121d1$, so that the Jacobian of the twist $X_{\mathrm{ns}}^{(d)}(11)$ splits into the four elliptic curves $121b1$, $121a1^{(d)}$, $121c1^{(d)}$

and $121d1^{(d)}$. Unfortunately, for $d=-1$ and $d=-3$ all of these curves have rank 1, so the obvious approach does not work. However, we can use a covering collection combined with the Elliptic Curve Chabauty method [Bru03], as follows. An equation for $X_{\mathrm{ns}}^+(11)$ is

$$y^2 = 4x^3 - 4x^2 - 28x + 41$$

and the double cover $X_{\mathrm{ns}}(11) \to X_{\mathrm{ns}}^+(11)$ is given by

$$t^2 = -(4x^3 + 7x^2 - 6x + 19)$$

(this is an equation for $121c1$), see [DFGS14, Proposition 1]. Therefore our twists are given by

$$X_{\mathrm{ns}}^{(-1)}(11)\colon \begin{cases} y^2 = 4x^3 - 4x^2 - 28x + 41 \\ t^2 = 4x^3 + 7x^2 - 6x + 19 \end{cases}$$

and

$$X_{\mathrm{ns}}^{(-3)}(11)\colon \begin{cases} y^2 = 4x^3 - 4x^2 - 28x + 41 \\ t^2 = 3(4x^3 + 7x^2 - 6x + 19)\,. \end{cases}$$

Let α be a root of $f_1(x) = 4x^3-4x^2-28x+41$ and set $K=\mathbb{Q}(\alpha)$. Write $f_1(x) = (x-\alpha)g_1(x)$ in $K[x]$. Since $E_1 = 121b1$ has Mordell-Weil group $E_1(\mathbb{Q})$ isomorphic to $\mathbb{Z}$, with generator $P=(4,11)$, it follows that each rational point on E_1 gives rise to a K-rational point with rational x-coordinate on one of the two curves

$$\begin{cases} y_1^2 = x - \alpha \\ y_2^2 = g_1(x) \end{cases} \quad \text{and} \quad \begin{cases} y_1^2 = (4-\alpha)(x-\alpha) \\ y_2^2 = (4-\alpha)g_1(x)\,. \end{cases}$$

(Here we use that the map $E_1(\mathbb{Q}) \to K^\times/K^{\times 2}$ that associates to a point P the square class of $x(P)-\alpha$ is a homomorphism.) So a rational point on $X_{\mathrm{ns}}^{(d)}(11)$ will give a K-rational point with rational x-coordinate on

$$u^2 = -d(x-\alpha)(4x^3+7x^2-6x+19) \quad \text{or} \quad u^2 = -d(4-\alpha)(x-\alpha)(4x^3+7x^2-6x+19)\,.$$

These are elliptic curves over K, which turn out to both have Mordell-Weil rank 1 for $d=-1$ and rank 2 for $d=-3$. Since the rank is strictly smaller than the degree of K in all cases, Elliptic Curve Chabauty applies, and we find that the x-coordinates of the rational points on $X_{\mathrm{ns}}^{(-1)}(11)$ and $X_{\mathrm{ns}}^{(-3)}(11)$ are $\infty, 5/4, 4, -2$, corresponding to O, $\pm 3P$, $\pm P$ and $\pm 4P$ on E_1. (These computations have been done using Magma [BCP97].) We compute the j-invariants of the elliptic curves represented by these points using the formula in [DFGS14] and find that only the curves corresponding to $3P$ and to $4P$ give rise to solutions of (2.1); they are the trivial solutions with $a=0$ or $b=0$.

7.2. **Dealing with the remaining curves.**

We now set $\mathcal{E} = \{54a1, 96a1, 864a1, 864b1, 864c1\}$; this is the set of curves E such that we still have to consider $X_E(11)$.

We will denote any of the canonical morphisms

$$X(11) \to X(1) \simeq \mathbb{P}^1\,, \quad X_E(11) \simeq_{\bar{\mathbb{Q}}} X(11) \to X(1) \simeq \mathbb{P}^1 \quad \text{and} \quad X_0(11) \to X(1) \simeq \mathbb{P}^1$$

by j and we will also use j to denote the corresponding coordinate on $\mathbb{P}^1$.

Recall that $X_0(11)$ is an elliptic curve. Let $P \in X_E(11)(\mathbb{Q})$ be a rational point; then under the composition $X_E(11) \simeq X(11) \to X_0(11)$ (where the isomorphism is defined over $\bar{\mathbb{Q}}$) P will be mapped to a point P' on $X_0(11)$ whose image $j(P') = j(P)$ on the j-line is rational. Since the j-map from $X_0(11)$ has degree 12, it follows that P' is defined over a number field K of degree at most 12. More precisely, the points in the fiber above $j(P') = j(P)$ in $X_0(11)$ correspond to the twelve possible cyclic subgroups of order 11 in $E[11]$, so the Galois action on the fiber depends only on E and is the same as the Galois action on the fiber above the image $j(E)$ on the j-line of the canonical point of $X_E(11)$. In particular, we can easily determine the isomorphism type of this fiber. It turns out that for our five curves E, the fiber is irreducible, given by a field $K = K_E$ of degree 12. The problem can therefore be reduced to the determination of the set of K_E-points P' on $X_0(11)$ such that $j(P') \in \mathbb{Q}$ and is good. This kind of problem is the setting for the Elliptic Curve Chabauty method as introduced in [Bru03] that we have already used in Section 7.1 above. To apply the method, we need explicit generators of a finite-index subgroup of the group $X_0(11)(K_E)$. This requires knowing the rank of this group, for which we can obtain an upper bound by computing a suitable Selmer group. We use the 2-Selmer group, whose computation requires class and unit group information for the cubic extension L_E of K_E obtained by adjoining the x-coordinate of a point of order 2 on $X_0(11)$ (no field K_E has a non-trivial subfield, so no point of order 2 on $X_0(11)$ becomes rational over K_E). To make the relevant computation feasible, we assume the Generalized Riemann Hypothesis. With this assumption the computation of the 2-Selmer groups is done by Magma in reasonable time (up to a few hours). However, we now have the problem that we do not find sufficiently many independent points in $X_0(11)(K_E)$ to reach the upper bound. This is where an earlier attempt in 2006 along similar lines by David Zureick-Brown got stuck. We get around this stumbling block by making use of 'Selmer Group Chabauty' as described in [Sto15]. This method allows us to work with the Selmer group information without having to find sufficiently many points in $X_0(11)(K_E)$.

The idea of the Selmer Group Chabauty method (when applied with the 2-Selmer group) is to combine the global information from the Selmer group with local, here specifically 2-adic, information. So we first study our situation over $\mathbb{Q}_2$. Away from the branch points 0, 12^3 and ∞ of $j\colon X_0(11) \to \mathbb{P}^1_j$, the $\mathbb{Q}_2$-isomorphism type of the fiber is locally constant in the 2-adic topology. In a suitable neighborhood of a branch point, the isomorphism type of the fiber will only depend on the class of the value of a suitable uniformizer on $\mathbb{P}^1_j$ at the branch point modulo cubes (for 0), squares (for 12^3) or eleventh powers (for ∞). We use the standard model given by

$$y^2 + y = x^3 - x^2 - 10x - 20$$

for the elliptic curve $X_0(11)$, with j-invariant map given by $j = (a(x) + b(x)y)/(x - 16)^{11}$, where

$$\begin{aligned} a(x) = {} & 743x^{11} + 21559874x^{10} + 19162005343x^9 + 2536749758583x^8 \\ & + 82165362766027x^7 + 576036867160006x^6 - 1895608370650736x^5 \\ & - 14545268641576841x^4 + 420015065507429x^3 + 74593328129816300x^2 \\ & + 108160113602504237x - 39176677684144739 \end{aligned}$$

and

$$b(x) = (x^5 + 4518x^4 + 1304157x^3 + 65058492x^2 + 271927184x - 707351591) \\ \cdot (x^5 + 192189x^4 + 3626752x^3 - 3406817x^2 - 37789861x - 37315543)\,.$$

Lemma 7.2. *The set $\mathcal{D}$ below is a partition of the subset of $\mathbb{P}^1(\mathbb{Q}_2)$ consisting of 2-adically good j-invariants into pairwise disjoint subsets D such that the isomorphism type over $\mathbb{Q}_2$ of the fiber of $j\colon X_0(11) \to \mathbb{P}^1$ is constant on $D \setminus \{0, 12^3, \infty\}$.*

$$\begin{aligned}\mathcal{D} = \big\{&7 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ 15 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -9 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2,\\ &2^9 + 2^{11}\mathbb{Z}_2,\ -2^9 + 2^{11}\mathbb{Z}_2,\ 2^{12} + 2^{13}\mathbb{Z}_2,\ \{2^{15}t^3 : t \in \mathbb{Z}_2\},\ \{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}\\ &\{12^3 - 3 \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 - 2^{10}t^2 : t \in \mathbb{Z}_2\},\\ &\{12^3 + 2^{10}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 + 3 \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\}\big\}\end{aligned}$$

Proof. We eliminate y from the equation of $X_0(11)$ and the relation between j and x, y. This results in

$$\begin{aligned}&(x^4 - 52820x^3 + 1333262x^2 + 4971236x + 9789217)^3\\ &\quad + (1486x^{11} + 43119747x^{10} + 38323813979x^9 + 5072626276355x^8\\ &\qquad + 164063633585170x^7 + 1134855511654843x^6 - 4074814667347831x^5\\ &\qquad - 29669709666741936x^4 + 6839041777752481x^3 + 15948062227565933 3x^2\\ &\qquad + 199736619430410535x - 104748564078368391)j\\ &\quad - (x - 16)^{11}j^2 = 0\,.\end{aligned}$$

The y-coordinate is then uniquely determined by x and j (at least when $b(x) \neq 0$, but $b(x) = 0$ never occurs when $j \in \mathbb{Q}_2$), so we can use this relation between x and j to determine the isomorphism type of the fiber. First consider $j_0 \in \mathbb{P}^1(\mathbb{Q}_2) \setminus \{0, 12^3, \infty\}$. Using a variant of Krasner's Lemma or similar arguments, we can find an explicit 2-adic disk $D(j_0)$ centered at j_0 such that the isomorphism type of the fiber of j is constant on $D(j_0)$. Working with Puiseux series in j, $j-12^3$, or j^{-1}, we obtain in a similar way sets D of the form $\{\alpha t^3 : t \in \mathbb{Z}_2\}$, $\{12^3 + \alpha t^2 : t \in \mathbb{Z}_2\}$, or $\{\alpha t^{-11} : t \in \mathbb{Z}_2\}$ with the property that the isomorphism type of the fiber of j is constant on D except for the branch point. Combining these results, we obtain an explicit partition of $\mathbb{P}^1_j(\mathbb{Q}_2) \setminus \{0, 12^3, \infty\}$ into sets above which the isomorphism type of the fiber is constant. Comparing the isomorphism types (or working with the 11-division polynomial instead of with the above relation, which corresponds to working on $X_1(11)$ instead of $X_0(11)$), we can collapse some of the disks into one disk. We then remove from this partition the subsets on which j is not 2-adically good (for each subset D, this condition is either satisfied for all $j \in D$ or for no $j \in D$). Note that the condition means explicitly that either $v_2(j) \geq 6$, $v_2(j)$ is divisible by 3 and $v_2(12^3 - j)$ is even, or else $v_2(j)$ is strictly negative and $v_2(j) \equiv 6 \bmod 11$. This results in the set $\mathcal{D}$ as given in the statement. □

Lemma 7.3. *Let $E \in \mathcal{E}$ and let $P \in X_E(11)(\mathbb{Q}_2)$ such that $j(P)$ is 2-adically good. Then $j(P)$ is in one of the following sets $D \in \mathcal{D}$.*

$$\begin{aligned}
54a1&: \{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}\,.\\
96a1&: 15\cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2,\ -2^9 + 2^{11}\mathbb{Z}_2\,.\\
864a1&: \{12^3 - 3\cdot 2^{16}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 + 2^{16}t^2 : t \in \mathbb{Z}_2\}\,.\\
864b1&: \{12^3 - 2^{16}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 + 3\cdot 2^{16}t^2 : t \in \mathbb{Z}_2\},\ 2^9 + 2^{11}\mathbb{Z}_2\,.\\
864c1&: 15\cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2,\ -2^9 + 2^{11}\mathbb{Z}_2\,.
\end{aligned}$$

Note that this result is consistent with the fact that the only pair of curves in $\mathcal{E}$ that are symplectically 11-congruent over $\mathbb{Q}_2$ is $(96a1, 864c1)$; compare Lemma 5.2.

Proof. We use the explicit description of $X_E(11)$ together with the map to the j-line provided by Fisher [Fis14]. This gives a model of $X_E(11)$ as a smooth projective curve in $\mathbb{P}^4$, which we can use to obtain a partition of $X_E(11)(\mathbb{Q}_2)$ into 2-adic disks, on which we evaluate the j-map to find out which of the sets in $\mathcal{D}$ contain the image of a point P as in the statement. For $E = 54a1$ (where this procedure results in a large number of disks in $X_E(11)(\mathbb{Q}_2)$), this can be simplified by observing that the given $D \in \mathcal{D}$ is the only set in $\mathcal{D}$ such that the isomorphism type of the fiber is that above $j(E)$ (which is $\operatorname{Spec}\mathbb{Q}_2 \amalg \operatorname{Spec}\mathbb{Q}_2(2^{1/11})$). □

The next step is the computation of the 2-Selmer groups of $X_0(11)$ over the fields K_E, where E runs through the curves in $\mathcal{E}$. This is where we assume GRH. Table 5 lists defining polynomials for the fields K_E and gives the $\mathbb{F}_2$-dimension of the Selmer group.

E	polynomial defining K_E	$\dim_{\mathbb{F}_2} \mathrm{Sel}_2 / K_E$
$54a1$	$x^{12} - 6x^{10} + 6x^9 - 6x^8 - 126x^7 + 104x^6 + 468x^5 + 258x^4 - 456x^3 - 1062x^2 - 774x - 380$	4
$96a1$	$x^{12} - 4x^{11} - 264x^7 + 66x^6 - 132x^5 - 2112x^4 - 1320x^3 - 660x^2 - 6240x - 8007$	5
$864a1$	$x^{12} - 6x^{11} + 110x^9 - 132x^8 - 528x^7 + 1100x^6 + 330x^5 - 2508x^4 + 2134x^3 - 594x^2 + 456x - 371$	5
$864b1$	$x^{12} - 6x^{11} + 22x^9 + 99x^8 - 396x^7 + 440x^6 - 132x^5 - 6501x^4 + 33506x^3 - 23760x^2 - 92418x + 193081$	3
$864c1$	$x^{12} - 44x^9 - 264x^8 - 264x^7 - 2266x^6 - 4488x^5 - 264x^4 - 17644x^3 - 7128x^2 + 144x - 15191$	3

TABLE 5. Fields K_E and dimensions of Selmer groups, for $E \in \mathcal{E}$.

Recall that θ denotes the x-coordinate of a point of order 2 on $X_0(11)$, so θ is a root of the 2-division polynomial

$$4x^3 - 4x^2 - 40x - 79$$

of $X_0(11)$. We denote the 2-adic valuation on $\bar{\mathbb{Q}}_2$ by v_2, normalized so that $v_2(2) = 1$. Then $v_2(\theta) = -2/3$.

Lemma 7.4. *Let K be a finite extension of $\mathbb{Q}_2$ such that $X_0(11)(K)[2] = 0$ and set $L = K(\theta)$. Let $D \in \mathcal{D}$, but $D \neq \{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}$. Let $\phi\colon D \to X_0(11)(K)$ be an analytic section of j. Then the square class of $x(\phi(z)) - \theta \in L^\times$ is constant for $z \in D$.*

Proof. By Lemma 7.2 the $\mathbb{Q}_2$-isomorphism type of the fiber of j above D is constant, say given by the disjoint union of $\operatorname{Spec} K_j$ for certain 2-adic fields K_j. Then the power series defining ϕ will have coefficients in some K_j. We now use the fact that $\xi - \theta$ and $\xi' - \theta$ are in the same class modulo squares when $v_2(\xi - \xi') > 2 + v_2(\xi - \theta)$, compare [Sto01, Lemma 6.3]. Note that this condition is independent of the field considered, so we can assume that $K = K_j$. (We note that all K_j coming up in this way have the property that $X_0(11)(K_j)[2] = 0$, since the ramification indices are not divisible by 3.) We obtain K_j as one of the completions of the field K_E at a place above 2, where E is an elliptic curve with $j(E)$ equal to the 'center' (or any other rational point if the center is a branch point) of D. We obtain a 'generic' ϕ by solving the relation between x and j for x as a power series in t with coefficients in K_E, with j replaced by $j(E) + at^b$, where a and b are taken from the description $D = \{j(E) + at^b : t \in \mathbb{Z}_2\}$. This series is unique up to an automorphism of K_E. We then check that the 2-adic valuations of all coefficients of powers t^n with $n \geq 1$ in all completions K_j are $> 4/3$. Since $x(t)$ is always 2-adically integral when $t \in \mathbb{Z}_2$ (since $D \subset \mathbb{Z}_2$ and the relation is monic in x), we then have $v_2(x(0) - x(t)) > 4/3 = 2 - 2/3 = 2 + v_2(x(0) - \theta)$ for all $t \in \mathbb{Z}_2$, which implies the claim. □

We now use the information coming from the Selmer group together with the preceding lemma to rule out most of the disks listed in Lemma 7.3.

Lemma 7.5. *Let $E \in \mathcal{E}$ and let $P \in X_E(11)(\mathbb{Q})$ such that $j(P)$ is 2-adically good. Then $j(P)$ is in one of the following sets $D \in \mathcal{D}$.*

$$
\begin{aligned}
54a1&\colon \{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}\,.\\
96a1&\colon 15 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2\,.\\
864a1&\colon \text{none}\,.\\
864b1&\colon 2^9 + 2^{11}\mathbb{Z}_2\,.\\
864c1&\colon -2^9 + 2^{11}\mathbb{Z}_2\,.
\end{aligned}
$$

Note that the curve $864a1$ can already be ruled out at this stage.

Proof. In view of Lemma 7.3, there is nothing to prove when $E = 54a1$. So we let E be one of the other four curves. Any rational point on $X_E(11)$ whose image on the j-line is good will map to a point in $X_0(11)(K_E)$ with the same j-invariant, and so will give rise to a point in $X_0(11)(K_E \otimes_{\mathbb{Q}} \mathbb{Q}_2)$ whose j-invariant is in one of the sets D listed in Lemma 7.3, depending on E. Recall that $L_E = K_E(\theta)$. We write $K_{E,2} = K_E \otimes_{\mathbb{Q}} \mathbb{Q}_2$ and $L_{E,2} = L_E \otimes_{\mathbb{Q}} \mathbb{Q}_2$;

$K_{E,2}$ and $L_{E,2}$ are étale algebras over $\mathbb{Q}_2$. Then we have the commutative diagram

$$\begin{array}{ccccc} X_0(11)(K_E) & \longrightarrow & \mathrm{Sel}_2(X_0(11)/K_E) & \hookrightarrow & \dfrac{L_E^\times}{L_E^{\times 2}} \\ \downarrow & & \downarrow & & \downarrow \\ X_0(11)(K_{E,2}) & \longrightarrow & \dfrac{X_0(11)(K_{E,2})}{2X_0(11)(K_{E,2})} & \hookrightarrow & \dfrac{L_{E,2}^\times}{L_{E,2}^{\times 2}}. \end{array}$$

The composition of the two horizontal maps in the bottom row sends a point (ξ, η) to the square class of $\xi - \theta$ in $L_{E,2}^\times$. By Lemma 7.4, the set of square classes we obtain for points in $X_0(11)(K_{E,2})$ mapping into D does not depend on the image point in D. It therefore suffices to compute the square class for the points above some representative point (for example, the 'center' if it is not a branch point) of D. Doing this, we find that the square classes we obtain are not in the image of the Selmer group except for the sets given in the statement. Since by the diagram above a point in $X_0(11)(K_E)$ has to map into the image of the Selmer group, this allows us to exclude these D. □

It remains to deal with the remaining five disks D. All but one of them do actually contain the image of a point in $X_0(11)(K_E)$, so we have to use a more sophisticated approach. The idea for the following statement comes from [Sto15].

Lemma 7.6. *Let $E \in \mathcal{E}$ and let $D \in \mathcal{D}$ be one of the sets associated to E in Lemma 7.5. Assume that there is a point $P \in X_0(11)(K_E)$ with the following property.*

(*) *For any point $Q \in X_0(11)(K_{E,2})$ with $Q \neq P$ and $j(Q) \in D$, there is $n \geq 0$ such that $Q = P + 2^n Q'$ with $Q' \in X_0(11)(K_{E,2})$ such that the image of Q' in $L_{E,2}^\times / L_{E,2}^{\times 2}$ is not in the image of the Selmer group.*

Then if $j(P) \in D$, P is the only point $Q \in X_0(11)(K_E)$ with $j(Q) \in D$, and if $j(P) \notin D$, then there is no such point.

Proof. For each $E \in \mathcal{E}$, we verify that the middle vertical map in the diagram in the proof of Lemma 7.5 is injective, by checking that the rightmost vertical map is injective on the image of the Selmer group. Note that the Selmer group is actually computed as a subgroup of the upper right group. Since $X_0(11)(K_E)/2X_0(11)(K_E)$ maps injectively into the Selmer group, this means that a K_E-rational point that is divisible by 2 in $X_0(11)(K_{E,2})$ is already divisible by 2 in $X_0(11)(K_E)$. Since $X_0(11)$ has no K_E-rational points of exact order 2 (none of the fields K_E has non-trivial subfields, so $\theta \notin K_E$, since $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$), there is a unique 'half' of a point, if there is any. So if $P \neq Q \in X_0(11)(K_E)$ has j-invariant in D, then the point Q' in the relation in property (*) is also K_E-rational. But then its image in $L_{E,2}^\times / L_{E,2}^{\times 2}$ must be in the image of the Selmer group, which gives a contradiction to (*). The only remaining possibility for a point $Q \in X_0(11)(K_E)$ with $j(Q) \in D$ is then P, and this possibility only exists when $j(P) \in D$. □

It remains to exhibit a suitable point P for the remaining pairs (E, D) and to show that it has property (*). We first have a look at the 2-adic elliptic logarithm on $X_0(11)$. Let

$\mathcal{K} \subset X_0(11)(\bar{\mathbb{Q}}_2)$ denote the kernel of reduction. We take $\tau = x/y$ to be a uniformizer at the point at infinity on $X_0(11)$ and write $\mathcal{K}_\nu = \{P \in \mathcal{K} : v_2(\tau(P)) > \nu\}$.

Lemma 7.7. *The 2-adic elliptic logarithm* $\log\colon \mathcal{K} \to \bar{\mathbb{Q}}_2$ *induces a group isomorphism between* $\mathcal{K}_{1/3}$ *and the additive group* $D_{1/3} = \{\lambda \in \bar{\mathbb{Q}}_2 : v_2(\lambda) > 1/3\}$.

In particular, if K *is a 2-adic field and* $P \in \mathcal{K}_{4/3} \cap X_0(11)(K)$*, then* P *is divisible by* 2 *in* $X_0(11)(K)$.

Proof. Note that the points T of order 2 on $X_0(11)$ satisfy $v_2(\tau(T)) = 1/3$ (the x-coordinate has valuation $-2/3$ and the y-coordinate is $-1/2$). We also note that $X_0(11)$ is supersingular at 2, so $X_0(11)(\bar{\mathbb{F}}_2)$ consists of points of odd order. This implies that the kernel of log on $\mathcal{K}$ consists exactly of the points of order a power of 2. There are no such points with $v_2(\tau) > 1/3$, so log is injective on this set. Explicitly, we find that for $P \in \mathcal{K}$ with $\tau(P) = \tau$,

$$\log P = \tau - \frac{1}{3}\tau^3 - \frac{1}{2}\tau^4 - \frac{19}{5}\tau^5 + \tau^6 + \frac{5}{7}\tau^7 + \frac{27}{2}\tau^8 + \dots;$$

for $v_2(\tau) > 1/3$ the first term is dominant, so the image is $D_{1/3}$ as claimed.

Now let $P \in \mathcal{K}_{4/3} \cap X_0(11)(K)$. Note that restricting log gives us an isomorphism between $\mathcal{K}_{1/3} \cap X_0(11)(K)$ and $D_{1/3} \cap K$. Since $v_2(\tau) > 4/3$, the image of P in $D_{1/3} \cap K$ is divisible by 2 in $D_{1/3} \cap K$, so P must be divisible by 2 in $X_0(11)(K)$. □

Lemma 7.8. *Let* $\phi\colon 2\mathbb{Z}_2 \to \mathcal{K} \cap X_0(11)(K)$ *be an analytic map with* $\phi(0)$ *the point at infinity, where* K *is some 2-adic field. If* $P_1 = \phi(2) \in X_0(11)(K)$ *is not divisible by* 2 *and*

$$\log \phi(t) = a_1 t + a_2 t^2 + a_3 t^3 + \dots$$

with $a_j \in K$ *such that* $v_2(a_j) > 1/3 - j$ *for all* $j \geq 1$*, then for every* $t \in 2\mathbb{Z}_2$*, we can write* $\phi(P) = 2^{v_2(t)-1}P'$ *with* $P' \in X_0(11)(K)$ *such that* $P' - P_1$ *is divisible by* 2 *in* $X_0(11)(K)$.

Proof. Write $t = 2^{\nu+1}u$ with $u \in \mathbb{Z}_2^\times$ and $\nu \geq 0$. Then

$$\log \phi(t) = 2^\nu \left(a_1 \cdot 2u + a_2 \cdot 2^{\nu+2}u^2 + a_3 \cdot 2^{2\nu+3}u^3 + \dots\right),$$

which has 2-adic valuation $> \nu + 1/3$ and so $\phi(t)$ is divisible by 2^ν in $X_0(11)(K)$ by Lemma 7.7. We write $\phi(t) = 2^\nu P'$; then

$$\log(P' - P_1) = 2^{-\nu}\log\phi(t) - \log\phi(2) = 2(u-1)\left(a_1 + 2(u+1)a_2 + 4(u^2+u+1)a_3 + \dots\right).$$

Since $v_2(u-1) \geq 1$, the 2-adic valuation of this is $> 4/3$, so $P' - P_1$ is divisible by 2 in $X_0(11)(K)$ by Lemma 7.7 again. □

Lemma 7.9. *Let* $E \in \mathcal{E}$ *and let* $D \in \mathcal{D}$ *be one of the sets associated to* E *in Lemma 7.5. Then the point* P *given in the table below satisfies (*) for* E *and* D*. Here* $\mathrm{can}(E)$ *stands for the image on* $X_0(11)$ *of the canonical point on* $X_E(11)$.

E	D	P	$j(P) \in D \setminus \{0, 12^3, \infty\}$
$54a1$	$\{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}$	$(16, 60)$	no
$96a1$	$15 \cdot 2^6 + 2^{11}\mathbb{Z}_2$	$-\mathrm{can}(96a2)$	no
$96a1$	$-2^6 + 2^{11}\mathbb{Z}_2$	$\mathrm{can}(96a1)$	yes
$864b1$	$2^9 + 2^{11}\mathbb{Z}_2$	$\mathrm{can}(864b1)$	yes
$864c1$	$-2^9 + 2^{11}\mathbb{Z}_2$	$\mathrm{can}(864c1)$	yes

Proof. The points P given in the table have the property that their image in $G = L_{E,1}^{\times}/L_{E,2}^{\times 2}$ agrees with the image of those points in $j^{-1}(D) \cap X_0(11)(K_{E,2})$ whose image is in the image of the Selmer group. This means that for any point Q in one of the 2-adic disks above D such that Q maps into the image of the Selmer group, we have that $P - Q$ is divisible by 2 in $X_0(11)(K_{E,2})$.

We first consider the last three cases. In the last two cases only one (out of sixteen) of the disks above D maps into the image of the Selmer group; this must be the disk containing the image of the canonical point. For $96a1$ we find that there is only one residue disk in $X_{96a1}(11)(\mathbb{Q}_2)$ that maps to D. Its image in $X_0(11)(K_{96a1,2})$ must be one of the disks above D and this disk contains the image of the canonical point; the other disks above D can be excluded. So in each of these three cases the only disk above D that we have to consider is the disk D' containing the image of the canonical point. We parameterize this disk, taking the image of the canonical point as the center; this results in a pair of power series with coefficients in K_E giving the x- and y-coordinates. We write $\psi\colon 2\mathbb{Z}_2 \to X_0(11)(K_{E,2})$ for this parameterization. We know from Lemma 7.4 that all differences $Q - \mathrm{can}(E)$ for $Q \in D'$ are divisible by 2 in $X_0(11)(K_{E,2})$. This gives us an analytic map $\phi\colon 2\mathbb{Z}_2 \to \mathcal{K} \cap X_0(11)(K_{E,2})$ such that $2\phi(t) = \psi(t) - \mathrm{can}(E)$. For $E = 96a1$, the points $\psi(t) - \mathrm{can}(E)$ are actually divisible by 4, so here we take ϕ such that $4\phi(t) = \psi(t) - \mathrm{can}(E)$. We now consider $\log \phi(t)$ and verify that this power series satisfies the conditions in Lemma 7.8 for each component of $K_{E,2}$. We also check that $P_1 = \phi(2)$ does not map into the image of the Selmer group. This, together with the conclusion of Lemma 7.8, verifies (*).

Next we consider the other disk D for $E = 96a1$. There are four disks D' above D such that the image of D' in G is in the image of the Selmer group; this image is the same as that of P. Taking the difference with P and halving, we find that on three of the remaining disks the image in G of the resulting points is not in the image of the Selmer group. On the fourth disk, the image is zero, so the points are again divisible by 2. After halving again, we find that the resulting points have image in G not in the image of the Selmer group. This verifies (*) for this case (with $n \leq 2$).

Finally, we look at $E = 54a1$. There is one unramified branch above $j = \infty$ with the point at infinity of $X_0(11)$ sitting in the center of the disk, and there is one point (with coordinates $(16, 60)$) with ramification index 11. We can parameterize the disk relevant to us by setting $j = 2^6 t^{-11}$ and solving for the x and y-coordinates in $\mathbb{Q}(\sqrt[11]{2})(\!(t)\!)$. We find that the series giving the logarithm of this point minus $(16, 60)$ satisfies the valuation conditions of Lemma 7.8, and we can also check that for $t = 2$ we obtain a point whose image in G is not in the image of the Selmer group, so (*) is verified in this case, too. Note that it suffices to look only at the component over $\mathbb{Q}_2(\sqrt[11]{2})$; the other component always gives a point that is quite a bit more often divisible by 2, so the image in the corresponding component of G is always zero. □

To conclude the proof of Theorem 7.1, it now only remains to observe that the j-invariants $21952/9$ of $96a1$ and 1536 of $864c1$ are not good (the condition on the 3-adic valuation is violated), so the only remaining point in $X_{96a1}(11)(\mathbb{Q})$ and in $X_{864c1}(11)(\mathbb{Q})$ does not lead to a primitive integral solution of our Generalized Fermat Equation. The only remaining point in $X_{864b1}(11)(\mathbb{Q})$ is the canonical point; it corresponds to the Catalan solutions.

8. The Generalized Fermat Equation with exponents 2, 3, 13

In this section, we collect some partial results for the case $p = 13$. More precisely, we show that the Frey curve associated to any putative solution must have irreducible 13-torsion Galois module and that only trivial solutions can be associated to the two CM curves in the list of Lemma 2.3.

8.1. **Eliminating reducible 13-torsion.**

The case $p = 13$ is special in the sense that it is a priori possible to have Frey curves with reducible 13-torsion Galois modules. In this respect, it is similar to $p = 7$, compare [PSS07]. To deal with this possibility, we note that such a Frey curve E will have a Galois-stable subgroup C of order 13 and so gives rise to a rational point P_E on $X_0(13)$, which is a curve of genus 0. The Galois action on C is via some character $\chi\colon G_{\mathbb{Q}} \to \mathbb{F}_{13}^\times$, which can be ramified at most at 2, 3 and 13. Associated to χ is a twist $X_\chi(13)$ of $X_1(13)$ that classifies elliptic curves with a cyclic subgroup of order 13 on which the Galois group acts via χ; the Frey curve E corresponds to a rational point on $X_\chi(13)$ that maps to P_E under the canonical covering map $X_\chi(13) \to X_0(13)$. The covering $X_1(13) \to X_0(13)$ is Galois of degree 6 with Galois group naturally isomorphic to $\mathbb{F}_{13}^\times/\{\pm 1\}$; the coverings $X_\chi(13) \to X_0(13)$ are twisted forms of it, corresponding to the composition

$$G_{\mathbb{Q}} \xrightarrow{\chi} \mathbb{F}_{13}^\times \longrightarrow \mathbb{F}_{13}^\times/\{\pm 1\} \simeq \mathbb{Z}/6\mathbb{Z}\,,$$

which is an element of $H^1(\mathbb{Q}, \mathbb{Z}/6\mathbb{Z}; \{2, 3, 13\})$ (where $H^1(K, M; S)$ denotes the subgroup of $H^1(K, M)$ of cocycle classes unramified outside S). We can describe this group in the form

$$\begin{aligned} H^1(\mathbb{Q}, \mathbb{Z}/6\mathbb{Z}; \{2, 3, 13\}) &= H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}; \{2, 3, 13\}) \oplus H^1(\mathbb{Q}, \mathbb{Z}/3\mathbb{Z}; \{2, 3, 13\}) \\ &\simeq \langle -1, 2, 3, 13\rangle_{\mathbb{Q}^\times/\mathbb{Q}^{\times 2}} \oplus \langle \omega, \tfrac{4+\omega}{3-\omega}\rangle_{\mathbb{Q}(\omega)^\times/\mathbb{Q}(\omega)^{\times 3}}\,, \end{aligned}$$

where ω is a primitive cube root of unity. One can check that a model of $X_1(13)$ is given by

$$y^2 = (v + 2)^2 + 4\,, \qquad z^3 - vz^2 - (v + 3)z - 1 = 0\,;$$

the map to $X_0(13) \simeq \mathbb{P}^1$ is given by the v-coordinate. The second equation can be written in the form

$$\Big(\frac{z - \omega}{z - \omega^2}\Big)^3 = \frac{v - 3\omega}{v - 3\omega^2}\,,$$

which shows that the second equation gives a cyclic covering of $\mathbb{P}^1_v$ by $\mathbb{P}^1_z$. If d is a square-free integer representing an element in $\langle -1, 2, 3, 13\rangle_{\mathbb{Q}^\times/\mathbb{Q}^{\times 2}}$ and γ represents an element of $\langle \omega, \frac{4+\omega}{3-\omega}\rangle_{\mathbb{Q}(\omega)^\times/\mathbb{Q}(\omega)^{\times 3}}$, then the corresponding twist is

$$X_\chi(13)\colon dy^2 = (v + 2)^2 + 4\,, \qquad \gamma\Big(\frac{z - \omega}{z - \omega^2}\Big)^3 = \frac{v - 3\omega}{v - 3\omega^2}\,.$$

We note that the first equation defines a conic that has no real points when $d < 0$ and has no 3-adic points when $3 \mid d$. This restricts us to $d \in \{1, 2, 13, 26\}$. We find hyperelliptic equations for the 36 remaining curves (recall that $X_1(13)$ has genus 2), It turns out that only eight of them have ℓ-adic points for $\ell \in \{2, 3, 13\}$. We list them in Table 6. In the table we give d and δ, where $\gamma = \delta/\bar{\delta}$ and the bar denotes the non-trivial automorphism of $\mathbb{Q}(\omega)$.

no.	d	δ	f
1	1	1	$x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$
2	2	ω	$16x^6 + 24x^5 + 18x^4 + 76x^3 + 138x^2 + 72x + 16$
3	2	$\omega + 4$	$208x^6 - 312x^5 + 234x^4 - 988x^3 + 1794x^2 - 936x + 208$
4	2	$-3\omega - 4$	$16x^6 - 24x^5 + 106x^4 - 252x^3 + 226x^2 - 72x + 16$
5	13	$3\omega - 1$	$x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$
6	26	$\omega + 4$	$16x^6 - 24x^5 + 18x^4 - 76x^3 + 138x^2 - 72x + 16$
7	26	ω	$208x^6 + 312x^5 + 234x^4 + 988x^3 + 1794x^2 + 936x + 208$
8	26	$-3\omega - 4$	$16x^6 - 24x^5 + 106x^4 - 252x^3 + 226x^2 - 72x + 16$

TABLE 6. Curves $X_\chi(13)$ with local points, given as $y^2 = f(x)$.

We see that the last four curves are isomorphic to the first four. This is because of the canonical isomorphism $X_1(13) \simeq X_\mu(13)$, where the latter classifies elliptic curves with a subgroup isomorphic to μ_{13}. On the level of $X_0(13)$, this comes from the Atkin-Lehner involution, which in terms of our coordinate v is given by $v \mapsto (v+12)/(v-1)$.

The first curve is $X_1(13)$; it is known that its Jacobian has Mordell-Weil rank zero and that the only rational points on $X_1(13)$ are six cusps (there are no elliptic curves over $\mathbb{Q}$ with a rational point of order 13). For the other three curves, a 2-descent on the Jacobian as in [Sto01] gives an upper bound of 2 for the rank. The second and the fourth curve each have six more or less obvious rational points; their differences generate a subgroup of rank 2 of the Mordell-Weil group, so their Jacobians indeed have rank 2. On the third curve one does not find small rational points, and indeed it turns out that its 2-Selmer set is empty, which proves that it has no rational points. See [BS09] for how to compute the 2-Selmer set. It remains to consider the second and the fourth curves.

We note that the j-invariant map on $\mathbb{P}^1_v \simeq X_0(13)$ is given by

$$j = \frac{(v^2+3v+9)(v^4+3v^3+5v^2-4v-4)^3}{v-1}\,.$$

The obvious orbits of points on the curves no. 1, 2, 4, 5, 6, 8 then give points with $v = \infty$, 0, -4, 1, -12, $-8/5$ and j-invariants

$$\infty\,,\quad 12^3/3\,,\quad -\frac{12^3\cdot 13^4}{5}\,,\quad \infty\,,\quad -\frac{12^3\cdot 4079^3}{3}\,,\quad -\frac{12^3\cdot(17\cdot 29)^3\cdot 13}{5^{13}}\,,$$

respectively. None of these correspond to primitive solutions of $x^2+y^3=z^{13}$, except $j=\infty$, which is related to the trivial solutions $(\pm 1, -1, 0)$. So to rule out solutions whose Frey curves have reducible 13-torsion, it will suffice to show that there are no rational points on curves no. 2 and 4 other than the orbit of six points containing the points at infinity.

Computing the 2-Selmer sets, we find in both cases that its elements are accounted for by the points in the known orbit. So modulo the action of the automorphism group, it is enough to consider only the 2-covering of the curve that lifts the two points at infinity.

We first look at the second curve, which we denote C_2. Its polynomial f splits off three linear factors over K, where K is the field obtained by adjoining one of the roots α of f to $\mathbb{Q}$. The relevant 2-covering then maps over K to the curve $y^2 = (x - \alpha)g(x)$, where g is the remaining cubic factor. This is an elliptic curve (with two K-points at infinity and one with $x = \alpha$). Computing its 2-Selmer group (this involves obtaining the class group of a number field of degree 18, which we can do without assuming GRH; the computation took a few days), we find that it has rank 1. We know three K-points on the elliptic curve (coming from the points at infinity and from $(\alpha, 0)$); they map surjectively onto the Selmer group. So we can do an Elliptic Curve Chabauty computation, which tells us that the only K-points whose x-coordinate is rational are the two points at infinity. This in turn implies that the known rational points on C_2 are the six points in the orbit of the points at infinity.

Now we consider the fourth curve, C_4. Here the field generated by a root of f is actually Galois (with group S_3). We work over its cubic subfield L. Over L, f splits as 16 times the product of three monic quadratic factors h_1, h_2, h_3, and we consider the elliptic curve E given as $y^2 = h_1(x)h_2(x)$, with one of the points at infinity as the origin. This curve has full 2-torsion over L, so a 2-descent is easily done unconditionally. We find that the 2-Selmer group has rank 3, so the Mordell-Weil rank of E over L is 1 (the difference of the two points at infinity has infinite order). An Elliptic Curve Chabauty computation then shows that the only K-points on E with rational x-coordinate are those at infinity and those with x-coordinate -3. Since there are no rational points on C_4 with x-coordinate -3, this shows as above for C_2 that the only rational points are the six points in the orbit of the points at infinity.

This proves the following statement.

Lemma 8.1. *Let (a, b, c) be a non-trivial primitive solution of $x^2 + y^3 = z^{13}$. Then the 13-torsion Galois module $E_{(a,b,c)}[13]$ of the associated Frey curve is irreducible.*

8.2. **Dealing with the CM curves.**

13 is congruent to 1 both mod 3 and mod 4, so the 13-torsion Galois representations on $27a1$ and on $288a1$ both have image contained in the normalizer of a split Cartan subgroup. But unfortunately the general result of [BPR13] does not apply in this case. We can, however, use the approach taken in Section 8.1 above. Since we are in the split case, the curves have cyclic subgroups of order 13 defined over a quadratic field K, which is $\mathbb{Q}(\omega)$ for $27a1$ (with ω a primitive cube root of unity) and $\mathbb{Q}(i)$ for $288a1$. We find the twist of $X_1(13)$ over K that corresponds to the Galois representation over K on this cyclic subgroup. Finding the twist is not entirely trivial, since the points on $X_0(13)$ corresponding to $27a1$ or to $288a1$ are branch points for the covering $X_1(13) \to X_0(13)$ (of ramification degree 3, respectively 2). In the case of $27a1$ we use a little trick: the isogenous curve $27a2$ has isomorphic Galois representation, but j-invariant $\neq 0$, so the corresponding point in $X_0(13)(K)$ lifts to a unique twist, which must be the correct one also for $27a1$. Since cube roots of unity are in K, we can make a coordinate change so that the automorphism of order 3 is given by multiplying the x-coordinate by ω. We obtain the following simple model over $K = \mathbb{Q}(\omega)$ of the relevant twist of $X_1(13)$:

$$C_{27a1} \colon y^2 = x^6 + 22x^3 + 13\,.$$

The points coming from $27a1$ are the two points at infinity, and the points coming from $27a2$ are the six points whose x-coordinate is a cube root of unity.

For $288a1$, we figure out the quadratic part of the sextic twist (the cubic part is unique in this case) by looking at the Galois action on the cyclic subgroup explicitly. We find that the correct twist of $X_1(13)$ is

$$C_{288a1}\colon y^2 = 12ix^5 + (30i+33)x^4 + 66x^3 + (-30i+33)x^2 - 12ix\,.$$

Here the points coming from $288a1$ are the ramification points $(0,0)$ and $(-1,0)$ and the (unique) point at infinity. There are six further points over $\mathbb{Q}(i)$ on this curve, forming an orbit under the automorphism group, of which $\big((4i-3)/6, 35/36\big)$ is a representative.

As a first step, we compute the 2-Selmer group of the Jacobian J of each of the two curves. In both cases, we find an upper bound of 2 for the rank of $J(K)$. The differences of the known points on the curve generate a group of rank 2, so we know a subgroup of finite index of $J(K)$. It is easy to determine the torsion subgroup, which is $\mathbb{Z}/3\mathbb{Z}$ for $27a1$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $288a1$. Using the reduction modulo several good primes of K, we check that our subgroup is saturated at the primes dividing the group order of the reductions for the primes above 7 for $27a1$, or the primes above 5 for $288a1$. We also use this reduction information for a bit of Mordell-Weil sieving (compare [BS10]) to show that any point in $C_{27a1}(\mathbb{Q}(\omega))$ with rational j-invariant must reduce modulo both primes above 7 to the image of one of the known eight points, and that any point in $C_{288a1}(\mathbb{Q}(i))$ with rational j-invariant must reduce modulo both primes above 5 to the image of one of the three points coming from $288a1$ (the other six points have j in $\mathbb{Q}(i) \setminus \mathbb{Q}$).

It remains to show that these points are the only points in their residue classes mod 7, respectively, mod 5. For this, we use the criterion in [Sik13, Theorem 2]. We compute the integrals to sufficient precision and then check that the pair of differentials killing $J(K)$ is 'transverse' mod 7 (or 5) at each of the relevant points, which comes down to verifying the assumption in Siksek's criterion. Note that we apply Chabauty's method for a genus 2 curve when the rank is 2; this is possible because we are working over a quadratic field. See the discussion in [Sik13, Section 2].

We obtain the following result.

Lemma 8.2. *Let (a,b,c) be a non-trivial primitive solution of $x^2 + y^3 = z^{13}$. Then the 13-torsion Galois module $E_{(a,b,c)}[13]$ of the associated Frey curve is, up to quadratic twist, symplectically isomorphic to $E[13]$ for some $E \in \{96a2, 864a1, 864b1, 864c1\}$.*

Proof. By Lemma 8.1, $E_{(a,b,c)}[13]$ is irreducible, so by Theorem 5.1, it is symplectically isomorphic to $E[13]$ for E one of the given curves or one of the CM curves $27a1$, $288a1$ or $288a2$. These latter three are excluded by the computations reported on above. □

References

[Bar14] Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300, DOI 10.1016/j.jnt.2014.05.017. MR3253304 ↑6

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984, DOI 10.5802/aif.2781 (English, with English and French summaries). MR3137477 ↑6, 6, 8.2

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑1, 7.1

[Bro12] David Brown, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, Int. Math. Res. Not. IMRN **2** (2012), 423–436. MR2876388 (2012k:11036) ↑1

[Bru99] Nils Bruin, *The Diophantine equations* $x^2 \pm y^4 = \pm z^6$ *and* $x^2 + y^8 = z^3$, Compositio Math. **118** (1999), no. 3, 305–321, DOI 10.1023/A:1001529706709. MR1711307 (2001d:11035) ↑1

[Bru03] ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49, DOI 10.1515/crll.2003.076. MR2011330 (2004j:11051) ↑1, 7.1, 7.2

[Bru05] ———, *The primitive solutions to* $x^3 + y^9 = z^2$, J. Number Theory **111** (2005), no. 1, 179–189, DOI 10.1016/j.jnt.2004.11.008. MR2124048 (2006e:11040) ↑1

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum of Mathematics, Sigma **4** (2016), no. e6, 80 pages, DOI 10.1017/fms.2016.1. ↑6

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8. MR2521292 (2010e:11059) ↑8.1

[BS10] ———, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. MR2685127 ↑8.2

[Cen15] Tommaso Centeleghe, *Integral Tate modules and splitting of primes in torsion fields of elliptic curves*, Accepted for publication by Int. J. of Number Theory (2015). ↑5

[Che98] Imin Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 1–38. ↑6

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068) ↑5

[Dah08] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, PhD thesis, Utrecht University, 2008, http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html. ↑2

[DG95] 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, DOI 10.1112/blms/27.6.513. MR1348707 (96e:11042) ↑1

[dSE00] Bart de Smit and Bas Edixhoven, *Sur un résultat d'Imin Chen*, Math. Res. Lett. **7** (2000), no. 2-3, 147–153. ↑6

[DD08] Tim Dokchitser and Vladimir Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 516–524, DOI 10.1112/blms/bdn034. MR2418807 (2009k:11093) ↑5

[DD15] ———, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4339–4358, DOI 10.1090/S0002-9947-2014-06271-5. MR3324930 ↑4.2

[DFGS14] 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, DOI 10.1016/j.jalgebra.2014.05.036. MR3244639 ↑7.1

[Edw04] Johnny Edwards, *A complete solution to* $X\mathrm{sp}2 + Y\mathrm{sp}3 + Z\mathrm{sp}5 = 0$, J. Reine Angew. Math. **571** (2004), 213–236, DOI 10.1515/crll.2004.043. MR2070150 (2005e:11035) ↑1

[Fis14] Tom Fisher, *On families of 7- and 11-congruent elliptic curves*, LMS J. Comput. Math. **17** (2014), no. 1, 536–564, DOI 10.1112/S1461157014000059. MR3356045 ↑1, 7.2

[HK02] Emmanuel Halberstadt and Alain Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234, DOI 10.1515/crll.2002.058. MR1915212 (2003h:11068) ↑4, 4.1, 4, 4, 4.2

[Kra90] Alain Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), no. 4, 353–385, DOI 10.1007/BF02567933. MR1080288 (91j:11045) ↑2, 3

[LW12] David Loeffler and Jared Weinstein, *On the computation of local components of a newform*, Math. Comp. **81** (2012), no. 278, 1179–1200, DOI 10.1090/S0025-5718-2011-02530-5. MR2869056 (2012k:11064) ↑2

[LW15] ———, *Erratum: "On the computation of local components of a newform" [MR2869056]*, Math. Comp. **84** (2015), no. 291, 355–356, DOI 10.1090/S0025-5718-2014-02867-6. MR3266964 ↑2

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230 (80h:14022) ↑2

[Pac13] Ariel Pacetti, *On the change of root numbers under twisting and applications.*, Proc. Amer. Math. Soc. **141** (2013), no. 8, 2615–2628. ↑3

[PSS07] 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, DOI 10.1215/S0012-7094-07-13714-1. MR2309145 (2008i:11085) ↑1, 2, 2, 2, 2, 4, 5, 8.1

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488) ↑4.2

[Shi71] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1. ↑6

[Sik13] Samir Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793, DOI 10.2140/ant.2013.7.765. MR3095226 ↑1, 8.2

[SS14] Samir Siksek and Michael Stoll, *The generalised Fermat equation $x^2 + y^3 = z^{15}$*, Arch. Math. (Basel) **102** (2014), no. 5, 411–421, DOI 10.1007/s00013-014-0639-z. MR3254783 ↑1

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005) ↑4.2, 4.2

[Sto01] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 (2002b:11089) ↑7.2, 8.1

[Sto15] ———, *Chabauty without the Mordell-Weil group*, June 13, 2015. Preprint, `arXiv:1506.04286`. ↑1, 7.2, 7.2

[Wei67] André Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156 (German). MR0207658 (34 #7473) ↑6

Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, B.C., Canada V6T 1Z2

E-mail address: `nunobfreitas@gmail.com`

School of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, UK; Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland

E-mail address: `nasqret@gmail.com`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: `Michael.Stoll@uni-bayreuth.de`

URL: `http://www.computeralgebra.uni-bayreuth.de`