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 first develop new local criteria to decide if two elliptic curves with certain types of potentially good reduction at 2 and 3 can have symplectically or anti-symplectically isomorphic p-torsion modules. Using these criteria we produce the minimal list of twists of $X(p)$ that have to be considered, based on local information at 2 and 3; this list depends on $p \bmod 24$. Recent results on mod p representations with image in the normalizer of a split Cartan subgroup allow us to reduce the list further in some cases.

Our second main result is the complete solution of the equation when $p = 11$, which previously was the smallest unresolved p. One relevant new ingredient is the use of the 'Selmer group Chabauty' method introduced by the third author in recent work, 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*, where an *integral solution* is a triple $(a, b, c) \in \mathbb{Z}^3$ such that $a^2 + b^3 = \pm c^n$; such a solution is *trivial* if $abc = 0$ and *primitive* if a, b and c are coprime. 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 non-trivial solutions

Date: June 10, 2019.

2010 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11G05, 11G07, 11G30, 14G05, 14G25.

are known for $n \geq 7$, namely (up to sign changes)

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

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.

We note that an explicit version of the *abc* conjecture with a sufficiently good exponent would give an effective way of obtaining all solutions to equation (1.1). Namely, suppose that we know $\gamma > 0$ and $\varepsilon < \frac{5}{61}$ such that for all coprime integers A, B, C with $A + B = C$, we have that

$$\max\{|A|, |B|, |C|\} \leq \gamma\Bigl(\prod_{p \mid ABC} p\Bigr)^{1+\varepsilon},$$

where the product is over the prime divisors of ABC. Assume that $a^2 + b^3 = \pm c^n$ with coprime a, b, c and set $M = \max\{|a|^2, |b|^3, |c|^n\}$. We then obtain that

$$M \leq \gamma\Bigl(\prod_{p \mid a^2b^3c^n} p\Bigr)^{1+\varepsilon} = \gamma\Bigl(\prod_{p \mid abc} p\Bigr)^{1+\varepsilon} \leq \gamma|abc|^{1+\varepsilon} \leq \gamma M^{(1/2+1/3+1/n)(1+\varepsilon)},$$

so $M^{1/6-1/n-(5/6+1/n)\varepsilon} \leq \gamma$. Since $\varepsilon < \frac{5}{61}$, the exponent on the left is positive as soon as $n \geq 11$, and we get an effective bound on M in this case. Since equation (1.1) has been solved completely for $n \leq 10$, this then would give a complete solution. Whether this would result in a practical approach very much depends on the quality of the bound γ in relation to ε. (This is well-known to the experts; see for example [Coh07, Prop. 14.6.5 and Exercise 2 on p. 493].)

Our approach follows and refines the arguments of [PSS07] by combining new ideas around the modular method with recent approaches to the determination of the set of 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; see the discussion below. Nevertheless, in the first part of this paper we will apply a refinement of it to obtain optimal 2-adic and 3-adic 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.

The modular method.

The *modular method* for solving Diophantine equations typically proceeds in the following steps.

1. To a putative solution associate a *Frey elliptic curve* E.

2. Use modularity and level lowering results to show that (for a suitable prime p) the Galois representation on the p-torsion $E[p]$ is isomorphic to the mod-$\mathfrak{p}$ representation associated to a newform f of weight 2 and small level N (for a suitable prime ideal $\mathfrak{p}$ above p of the field of coefficients of f),

$$\overline{\rho}_{E,p} \simeq \overline{\rho}_{f,\mathfrak{p}} \,. \tag{1.2}$$

3. For each of the possible newforms, show that they cannot occur, or find all possible associated solutions.

The most challenging step is often the very last, where we want to obtain a contradiction or list the corresponding solutions. In the proof of Fermat's Last Theorem (where the modular method was born) we have $N = 2$ and there are no candidate newforms f, giving a simple contradiction. In essentially every other application of the method there are candidates for f, therefore more work is needed to complete the argument. More precisely, we must show, for each newform f at the concrete small levels, that $\overline{\rho}_{E,p} \not\simeq \overline{\rho}_{f,\mathfrak{p}}$. This is for example the obstruction to proving FLT over $\mathbb{Q}(\sqrt{5})$; see [FS15]. Thus it is crucial to have methods for distinguishing Galois representations.

One such method is known as 'the symplectic argument'; it originated in [HK02] and it uses a 'symplectic criterion' (see Theorem 4.1) to decide if an isomorphism of the p-torsion of two elliptic curves having a common prime of (potentially) multiplicative reduction preserves the Weil pairing. In practice, it sometimes succeeds in distinguishing between the mod p Galois representations of elliptic curves having at least two primes of potentially multiplicative reduction. Extending the symplectic criteria to include elliptic curves with other types of reduction will clearly allow to attack many more Diophantine equations. The main challenge in doing this comes from the fact that, in the presence of potentially good reduction, the inertia action either does not carry enough information or is hard to describe explicitly.

In the first part of this paper, we prove new symplectic criteria (Theorems 4.6 and 4.7) for certain cases of potentially good reduction at 2 and 3 and apply them to our concrete equation $x^2 + y^3 = z^p$. Previously the only such criterion available was [HK02, Prop. A.2], which contains a large list of hypotheses making it hard to apply.

Remark 1.3. While completing this paper, the methods of this first part have been generalized in work of the first author [Fre16, FK19]; furthermore, our symplectic results together with their more general variants have already allowed for applications to further Fermat-type equations, including the equation $x^3 + y^3 = z^p$; see [Fre16, BBF18, FK16].

Note that equation (1.1) admits, for all p, the Catalan solution mentioned above, but also the *trivial solutions* $(\pm1, 1, 0)$, $(\pm1, 0, 1)$, $\pm(0, 1, 1)$. We remark that the existence of these solutions is a powerful obstruction to the success of the modular method alone. Indeed, if by evaluating the Frey curve at these solutions we obtain a non-singular curve, then we will find the modular form corresponding to it via modularity among the forms with 'small' level. This means that we do obtain a 'real' isomorphism in (1.2), which for arbitrary p we cannot discard with current methods (except under highly favorable conditions). Nevertheless, we will apply our refinement of the symplectic argument together with a careful analysis of (1.2) restricted to certain decomposition groups to obtain finer local information, valid for an arbitrary exponent p. This information is then used as input for global methods in the second part when tackling concrete exponents.

More precisely, our goal is to reduce the study of 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 $X(p)$. For this, we apply our new symplectic criteria to reduce the list of twists that have to be considered (in the case of irreducible p-torsion on the Frey elliptic curve, which always holds for $p \neq 7, 13$) that was obtained in [PSS07]. 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 results here are 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.

Rational points on curves.

In the second part of the paper, our main goal is to give a proof of the following.

Theorem 1.4. *Assume the Generalized Riemann Hypothesis. Then the only non-trivial primitive integral solutions of the equation*

$$x^2 + y^3 = z^{11} \tag{1.5}$$

are the Catalan solutions $(a, b, c) = (\pm 3, -2, 1)$.

This appears to be only the second 'hyperbolic' instance (i.e., with $1/p + 1/q + 1/r < 1$) of the Generalized Fermat Equation with pairwise distinct prime exponents p, q, r that could be solved completely. (The first instance was $\{p, q, r\} = \{2, 3, 7\}$, which was solved in [PSS07].)

We use several ingredients to obtain this result. One is the work of Fisher [Fis14], who obtained an explicit description of the relevant twists of $X(11)$ (which we determine in the first part). These curves have genus 26 and are therefore not amenable to any direct methods for determining their 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 one of the relevant twists of $X(11)$ 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 to solve equation (1.5) 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 [Sto17], applied in the Elliptic Curve Chabauty setting. We note that we need the Generalized Riemann Hypothesis (GRH) 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 would like to stress that future improvements of the methods for computing class groups could result in removing the dependence of our result from GRH.

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.

We have used the Magma computer algebra system [BCP97] for the necessary computations.

Acknowledgments.

The work reported on in this paper was supported by the Deutsche Forschungsgemeinschaft, 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 and Jean-Pierre Serre for pointing us to Ligozat's work on the splitting of $J(11)$. We also thank an anonymous referee for some useful comments.

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 when K is a p-adic field or a number field. For a modular form f and a prime $\mathfrak{p}$ in its field of coefficients we write $\overline{\rho}_{f,\mathfrak{p}}$ for its associated mod $\mathfrak{p}$ Galois representation.

2. Irreducibility and level lowering

Suppose that $(a, b, c) \in \mathbb{Z}^3$ is a solution to the equation

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

Recall that (a, b, c) is *trivial* if $abc = 0$ and *non-trivial* otherwise. An integral 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 $G_{\mathbb{Q}}$-module, where E is one of the following seven elliptic curves (specified by their Cremona label):*

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

For the convenience of the reader, we give equations of these elliptic curves.

$$\begin{aligned} 27a1 &: y^2 + y = x^3 - 7 & 864a1 &: y^2 = x^3 - 3x + 6 \\ 54a1 &: y^2 + xy = x^3 - x^2 + 12x + 8 & 864b1 &: y^2 = x^3 - 24x + 48 \\ 96a1 &: y^2 = x^3 + x^2 - 2x & 864c1 &: y^2 = x^3 + 24x - 16 \\ 288a1 &: y^2 = x^3 + 3x \end{aligned}$$

Proof. By the proof of [PSS07, Lemma 4.6], a twist $E_{(a,b,c)}^{(d)}$ 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.) Write E for this twist $E_{(a,b,c)}^{(d)}$.

Using level lowering as in the proof of [PSS07, Lemma 6.1], we find that $\overline{\rho}_{E,p} \simeq \overline{\rho}_{E',p}$ where E' is an elliptic curve of conductor 27, 54, 96, 288 or 864, or else $\overline{\rho}_{E,p} \simeq \overline{\rho}_{f,\mathfrak{p}}$, 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 $\rho(I_3) \simeq S_3$, where $I_3 \subset D_3$ is the inertia group. Since p does not divide $6 = \# S_3$, we also have that $\overline{\rho}(I_3) \simeq S_3$. 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 $\overline{\rho}_{E,p} \simeq \overline{\rho}_{f,\mathfrak{p}}$ 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. $\square$

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

Proposition 2.4. *Let $(a, b, c) \in \mathbb{Z}^3$ 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. First assume $p \neq 13$, so $p = 11$ 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 that

(i) $p = 11, 19, 43, 67, 163$ and the corresponding curves have integral j-invariant, or else
(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

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

integral points on the elliptic curves $y^2 = x^3 \pm 1$ (which both have finite Mordell-Weil group) have $x \in \{0, \pm 1, 2\}$. It remains to observe that the Frey curve associated to the Catalan solution (which is, up to quadratic twist, $864b1$) is the only curve in its isogeny class, so it has irreducible mod p Galois representations for all p (see [LMFDB, Elliptic curves over $\mathbb{Q}$]). If we are in case (ii), then the 17-adic valuation of the j-invariant contradicts (2.2).

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

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 an isogeny of degree 2. 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 $L = \mathbb{Q}_\ell^{\mathrm{unr}}(E[p])$. The field L does not depend on p and is the smallest extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$ over which E acquires good reduction; see [ST68, §2, Corollary 3]. We call L the *inertial field* of $E/\mathbb{Q}_\ell$ or of E at ℓ, when E is defined over $\mathbb{Q}$.

We write $L_{2,96}$ and $L_{2,288}$ for the inertial fields at 2 of the elliptic curves with Cremona labels $96a1$ and $288a1$, respectively, and we write $L_{3,27}$ and $L_{3,54}$ for the inertial fields at 3 of the elliptic curves with Cremona labels $27a1$ and $54a1$. The following theorem shows that these are all the inertial fields that can arise from certain types of elliptic curves.

Let H_8 denote the quaternion group and $\mathrm{Dic}_{12} \simeq C_3 \rtimes C_4$ the dicyclic group of 12 elements. The properties of H_8 and of Dic_{12} that are used below can easily be verified using a suitable computer algebra system like for example Magma.

Theorem 3.1. *Let $E/\mathbb{Q}_\ell$ be an elliptic curve with potentially good reduction, conductor N_E and inertial field L. Assume further one of the following two sets of hypotheses.*

(1) $\ell = 2, \quad \mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}}) \simeq H_8$ *and* $v_2(N_E) = 5$;
(2) $\ell = 3, \quad \mathrm{Gal}(L/\mathbb{Q}_3^{\mathrm{unr}}) \simeq \mathrm{Dic}_{12}$ *and* $v_3(N_E) = 3$.

Then $L = L_{2,96}$ or $L_{2,288}$ in case (1) and $L = L_{3,27}$ or $L_{3,54}$ in case (2).

Proof. For a finite extension $K/\mathbb{Q}_\ell$ we denote the Weil subgroup of the absolute Galois group G_K by W_K. We write W_ℓ for $W_{\mathbb{Q}_\ell}$. We let $r_K \colon K^\times \to W_K^{\mathrm{ab}}$ denote the reciprocity map from local class field theory. It allows us to identify a character χ of W_K with the character $\chi^A = \chi \circ r_K$ of $K^\times$.

There is a representation $\rho_E\colon W_\ell \to \mathrm{GL}_2(\mathbb{C})$ of conductor $\ell^{v_\ell(N_E)}$ attached to E; see [Roh94, Section 13] and [DDT94, Remark 2.14]. This representation is either principal series or supercuspidal; see [Pac13, Section 2], noting that the Steinberg representation corresponds to infinite inertia.

Hypotheses (1) and (2) both imply that E acquires good reduction over a non-abelian extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$, hence ρ_E is a supercuspidal representation. More precisely, $\rho_E = \mathrm{Ind}_{W_M}^{W_\ell} \chi$ where $M/\mathbb{Q}_\ell$ is a quadratic extension, W_M is the Weil group of M and $\chi\colon W_M \to \mathbb{C}^\times$ is a character. If $M/\mathbb{Q}_\ell$ is unramified, then $\rho_E|_{I_\ell} \simeq \chi \oplus \chi^s$, where $\chi^s(g) := \chi(sgs^{-1})$ and $s \in W_\ell$ lifts the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$. Thus inertia has abelian image, a contradiction. Therefore $M/\mathbb{Q}_\ell$ is ramified, and we have that $\rho_E|_{I_\ell} = \mathrm{Ind}_{I_M}^{I_\ell}(\chi|_{I_M})$, where $I_M \subset W_M$ is the inertia subgroup.

Write ϵ_M for the quadratic character of $G_{\mathbb{Q}_\ell}$ fixing M. Then $(\chi^A|_{\mathbb{Q}_\ell^\times})\cdot\epsilon_M^A = \|\cdot\|^{-1}$ as characters of $\mathbb{Q}_\ell^\times$, where $\|\cdot\|$ is the norm character. Furthermore, the conductor exponents of ρ_E and χ are related by $\mathrm{cond}(\rho_E) = \mathrm{cond}(\chi) + \mathrm{cond}(\epsilon_M)$; see [Gér78, 2.8].

We denote the maximal ideal of M by $\mathfrak{p}$.

Suppose hypothesis (1). From [Pac13, Corollary 4.1] it follows that $M = \mathbb{Q}_2(d)$, where $d = \sqrt{-1}$ or $d = \sqrt{-5}$, hence $\mathrm{cond}(\epsilon_M) = 2$ and $\mathrm{cond}(\chi) = 5 - 2 = 3$.

Since $\mathrm{cond}(\chi) = 3$, we have that $\chi^A|_{\mathcal{O}_M^\times}$ factors via $(\mathcal{O}_M/\mathfrak{p}^3)^\times$, which has order 4 and is generated by $2 + d$. The condition $\chi^A|_{\mathbb{Z}_2^\times} = \epsilon_M^A$ implies $\chi^A(-1) = -1$, thus $\chi^A(2 + d) = \pm i$. We conclude that there are only two possibilities for $\chi|_{I_M}$, which are related by conjugation, hence giving the same induction $\rho_E|_{I_2}$. Thus, for each possible extension M there is only one field L, so there are at most two possible fields L.

Finally, from [Kra90, p. 357, Corollary] we see that the curves $96a1$ and $288a1$ satisfy hypothesis (1), and a direct computation in Magma using the 3-torsion fields shows that $L_{2,96} \neq L_{2,288}$. This proves the theorem in case (1).

Now suppose hypothesis (2). We have $M = \mathbb{Q}_3(d)$, where $d = \sqrt{\pm 3}$, both fields satisfying $v_3(\mathrm{disc}(M)) = 1$. Thus $3 = \mathrm{cond}(\chi) + v_3(\mathrm{disc}(M))$ implies that χ is of conductor $\mathfrak{p}^2$.

For both possible extensions M the character $\chi^A|_{\mathcal{O}_M^\times}$ factors through $(\mathcal{O}_M/\mathfrak{p}^2)^\times$, which is generated by -1 and $1 + d$ of orders 2 and 3, respectively. The condition $\chi^A|_{\mathbb{Z}_3^\times} = \epsilon_M^A$ implies that $\chi^A(-1) = -1$ and the conductor forces $\chi^A(1 + d) = \zeta_3^c$ with $c = 1$ or 2. Again, for each possible extension M there is only one field L, so there are at most two possible fields L.

Finally, from [Kra90, p. 355, Corollary], we see that the curves $27a1$ and $54a1$ satisfy hypothesis (2), and again a direct computation with Magma (but now with 5-torsion fields as we need $\ell \neq p$) shows that $L_{3,27} \neq L_{3,54}$. This concludes the proof. □

In a similar way as in the preceding proof, using Magma to compute with the 3-torsion fields over $\mathbb{Q}_2$, one checks that $96a1$ and $864c1$ have the same inertial field at 2; the same is true for $288a1$, $864a1$ and $864b1$. Similarly, working with the 5-torsion over $\mathbb{Q}_3$, we also check that $27a1$, $864b1$ and $864c1$ have the same inertial field at 3; the same is true for $54a1$ and $864a1$.

i_2	a mod 4	b mod 8	d	curves	$v_2(N_E)$	j
1	1	-1	$1, -3$	$54a1$	1	$2^{6-p}t^{-p}$
	-1	-1	$-1, 3$	$54a1$	1	$2^{6-p}t^{-p}$
2	0	1	$\pm 1, \pm 3$	$288a1, 864a1, 864b1$	5	$12^3 - 3 \cdot 2^{10}t^2$
	0	-3	$\pm 1, \pm 3$	$288a1, 864a1, 864b1$	5	$12^3 + 2^{10}t^2$
	0	3	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$	5	$12^3 - 2^{10}t^2$
	0	-1	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$	5	$12^3 + 3 \cdot 2^{10}t^2$
3	2	1	$\pm 1, \pm 3$	$96a1, 864c1$	5	$-2^6 + 2^{11}t$
	2	-3	$\pm 1, \pm 3$	$96a1, 864c1$	5	$15 \cdot 2^6 + 2^{11}t$
	2	3	$\pm 2, \pm 6$	$96a1, 864c1$	5	$7 \cdot 2^6 + 2^{11}t$
	2	-1	$\pm 2, \pm 6$	$96a1, 864c1$	5	$-9 \cdot 2^6 + 2^{11}t$
4	1	0	$-2, 6$	$27a1$	0	$2^{15}t^3$
	-1	0	$2, -6$	$27a1$	0	$2^{15}t^3$
5	± 1	2	$\pm 2, \pm 6$	$96a1, 864c1$	5	$-2^9 + 2^{11}t$
6	± 1	-2	$\pm 2, \pm 6$	$288a1, 864a1, 864b1$	5	$2^9 + 2^{11}t$
7	1	4	$-2, 6$	impossible	0	$(2^{12} + 2^{13}t)$
	-1	4	$2, -6$	impossible	0	$(2^{12} + 2^{13}t)$

TABLE 1. 2-adic conditions. Here $E = E^{(d)}_{(a,b,c)}$.
j gives the possible values of the associated j-invariant, with $t \in \mathbb{Z}_2$.

Moreover, 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 fields at 2 and 3 of $E^{(d)}_{(a,b,c)}$ match those of the seven curves in Lemma 2.3. Indeed, the inertial field of $E^{(d)}_{(a,b,c)}$ at 2 can be computed from the 3-torsion field with only a finite amount of precision for the Weierstrass model of $E^{(d)}_{(a,b,c)}/\mathbb{Q}_2$. More precisely, there exists k such that if $(x, y, z) \equiv (a, b, c) \bmod 2^k$, then $E^{(d)}_{(a,b,c)}$ and $E^{(d)}_{(x,y,z)}$ have the same inertial field at 2. We run over all congruence classes for x, y, z modulo 2^k (with x, y not both even) and compute the inertial field in each case. We can use a version of Lemma 7.5 to show that $k = 3$ is sufficient. Analogously we compute the inertial fields at 3 using 5-torsion (here $k = 2$ is sufficient).

The 2-adic information can be found in Table 1. The last row 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 3.2. *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.*

i_3	a mod 9	b mod 3	d	curves	$v_3(N_E)$	j
1	1	-1	$-3, 6$	$96a1$	1	$3^{3-p}t^{-p}$
	-1	-1	$3, -6$	$96a1$	1	$3^{3-p}t^{-p}$
2	0	1	$\pm1, \pm2, \pm3, \pm6$	$288a1$	2	$12^3 - 3^7t^2$
	0	-1	$\pm1, \pm2, \pm3, \pm6$	$288a1$	2	$12^3 + 3^7t^2$
3	±3	1	$\pm1, \pm2, \pm3, \pm6$	$27a1, 864b1, 864c1$	3	$3^3 + 3^6t$
4	±3	-1	$\pm1, \pm2, \pm3, \pm6$	$54a1, 864a1$	3	$-8 \cdot 3^3 + 3^6t$
5	±1	0	$\pm1, \pm2, \pm3, \pm6$	$27a1, 864b1, 864c1$	3	3^6t^3
	±2	0	$\pm1, \pm2, \pm3, \pm6$	$27a1, 864b1, 864c1$	3	$2 \cdot 3^6t^3$
6	±4	0	$\pm1, \pm2, \pm3, \pm6$	$288a1$	2	$4 \cdot 3^6t^3$
7	±1	1	$\pm1, \pm2, \pm3, \pm6$	$54a1, 864a1$	3	$-4 \cdot 3^3 + 3^5t$
	±4	1	$\pm1, \pm2, \pm3, \pm6$	$54a1, 864a1$	3	$-3^3 + 3^5t$
8	±2	1	$\pm1, \pm2, \pm3, \pm6$	$288a1$	2	$2 \cdot 3^3 + 3^5t$

TABLE 2. 3-adic conditions. j is as in Table 1, with $t \in \mathbb{Z}_3$ and $E = E^{(d)}_{(a,b,c)}$

$i_2 \backslash i_3$	1	2, 6, 8	3, 5	4, 7
1	–	–	–	$54a1$
2, 6	–	$288a1$	$864b1$	$864a1$
3, 5	$96a1$	–	$864c1$	–
4	–	–	$27a1$	–

TABLE 3. Curves E determined by (a mod 36, b mod 24).

Proof. Table 1 shows that $b \equiv 4$ mod 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. □

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 i_2 of Table 1 determines the row and the line number i_3 of Table 2, the column.

A Magma script that performs the necessary computations for the results in this section is available as `section3.magma` at [Sto].

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 $r(a\phi) = a^2 r(\phi)$. So up to scaling ϕ, only the class of $r(\phi)$ modulo squares matters. We say that ϕ is a *symplectic isomorphism* if $r(\phi)$ is a square in $\mathbb{F}_p^\times$, and an *anti-symplectic isomorphism* if $r(\phi)$ is a non-square. Fix a non-square $r_p \in \mathbb{F}_p^\times$. We say that ϕ is *strictly symplectic*, if $r(\phi) = 1$, and *strictly anti-symplectic*, if $r(\phi) = r_p$. 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 strictly symplectic (respectively, strictly anti-symplectic) isomorphism $\phi\colon E'[p] \to E[p]$. 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, Definition 4.1]. As explained there, the existence of a non-trivial primitive solution (a, b, c) of (2.1) implies that some twisted Frey curve $E_{(a,b,c)}^{(d)}$ 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 resolution 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 prime to p, 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 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 $X^-_{288a1}(p) \simeq X_{288a2}(p)$.

We now recall a criterion from [KO92] to decide, under certain hypotheses, whether $E[p]$ and $E'[p]$ are symplectically isomorphic, which will be useful later.

Theorem 4.1 ([KO92, Proposition 2])**.** *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 $E[p]$ and $E'[p]$ 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 [Fre16]), which we will then apply to our Diophantine problem in Theorem 5.1.

We will need the following auxiliary result.

Lemma 4.2. *Let E and E' be two elliptic curves defined over a field K and 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 these 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. This is [Fre16, Lemma 1]. □

4.1. A little bit of 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; these are the two Galois groups occurring in Theorem 3.1. We now consider them as subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$.

Write D_n for the dihedral group with $2n$ elements and S_n and A_n for the symmetric and alternating groups 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. **The symplectic criteria.**

Let E, E' be elliptic curves over $\mathbb{Q}_\ell$ with potentially good reduction and respective inertial fields $L = \mathbb{Q}_\ell^{\mathrm{unr}}(E[p])$ and $L' = \mathbb{Q}_\ell^{\mathrm{unr}}(E'[p])$. Suppose that $E[p]$ and $E'[p]$ are isomorphic as $G_{\mathbb{Q}_\ell}$-modules; in particular, $L = L'$. Write $I = \mathrm{Gal}(L/\mathbb{Q}_\ell^{\mathrm{unr}})$ and recall that I_ℓ denotes the inertia subgroup of $G_{\mathbb{Q}_\ell}$.

If I is not abelian, then Lemma 4.2 applied with $K = \mathbb{Q}_\ell^{\mathrm{unr}}$ says that $E[p]$ and $E'[p]$ cannot be both symplectically and anti-symplectically isomorphic I_ℓ-modules. Since the symplectic type of an isomorphism $\phi\colon E[p] \to E'[p]$ does not depend on whether it is considered as an isomorphism of $G_{\mathbb{Q}_\ell}$-modules of of I_ℓ-modules, we can conclude 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. 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 [FK19]. We note that [FK19], which originated as a continuation of the work done here, contains criteria similar to those stated below, and also improvements of the second parts of Theorems 4.6 and 4.7.

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 preserves the Weil pairing. 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 $\gamma_E\colon I \to \mathrm{Aut}(\overline{E})$, so that $\overline{E}[p]$ is an I-module via $\psi \circ \gamma_E$ in a natural way. Then φ is actually an isomorphism of I-modules: 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 field 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.

Since the map $\gamma_E \colon I \to \mathrm{Aut}(\overline{E})$ is injective, we have $H_8 \subset \mathrm{Aut}(\overline{E})$. From [Sil09, Thm.III.10.1 and Ex. A.1 on p. 414] we see that $\mathrm{Aut}(\overline{E}) \simeq \mathrm{SL}_2(\mathbb{F}_3)$ and $j(\overline{E}) = 0$. Similarly, we conclude that $j(\overline{E}') = 0$. Thus, $\overline{E}$ and $\overline{E}'$ are isomorphic over $\overline{\mathbb{F}}_2$.

So we can fix minimal models of E/L and E'/L both reducing to the same $\overline{E}$.

There is only one (hence normal) subgroup H of $\mathrm{SL}_2(\mathbb{F}_3)$ isomorphic to H_8. Therefore we have that $\psi(\gamma_E(I)) = \psi(\gamma_{E'}(I)) = \psi(H)$ 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 matrix in both cases. 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 that are not in 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 automorphism 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 fixes the order 8 subgroup pointwise 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 field and that $I \simeq \mathrm{Dic}_{12}$. 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. Reducing the number of relevant twists

Using the results of 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 $(a,b,c) \in \mathbb{Z}^3$ be a non-trivial primitive solution 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 $X(p)$, depending on the residue class of p mod 24.*

p mod 24	*twists of* $X(p)$
1	$X_{27a1}(p),\ X_{54a1}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)$
5	$X_{27a1}(p),\ X_{54a2}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{288a2}(p),$ $X_{864a1}(p),\ X^-_{864a1}(p),\ X_{864b1}(p),\ X^-_{864b1}(p),\ X_{864c1}(p),\ X^-_{864c1}(p)$
7	$X_{27a1}(p),\ X_{54a2}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)$
11	$X_{27a1}(p),\ X_{54a1}(p),\ X_{96a1}(p),\ X_{288a1}(p),\ X_{288a2}(p),$ $X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)$
13	$X_{27a1}(p),\ X_{96a2}(p),\ X_{288a1}(p),\ X_{288a2}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)$
17	$X_{27a1}(p),\ X_{54a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)$
19	$X_{27a1}(p),\ X_{54a1}(p),\ X_{96a2}(p),\ X_{288a1}(p),\ X_{288a2}(p),$ $X_{864a1}(p),\ X^-_{864a1}(p),\ X_{864b1}(p),\ X^-_{864b1}(p),\ X_{864c1}(p),\ X^-_{864c1}(p)$
23	$X_{27a1}(p),\ X_{288a1}(p),\ X_{864a1}(p),\ X_{864b1}(p),\ X_{864c1}(p)$

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. 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):

$$\begin{tikzcd}[row sep=small]
27a2 \arrow[r, dash, "3"] & 27a1 \arrow[r, dash, "3"] & 27a3 \arrow[r, dash, "3"] & 27a4 & 54a2 \arrow[r, dash, "3"] & 54a1 \arrow[r, dash, "3"] & 54a3 \\
& 96a2 \arrow[dr, dash, "2"] & & & & & \\
& & 96a1 \arrow[r, dash, "2"] & 96a4 & 288a1 \arrow[r, dash, "2"] & 288a2 & \\
& 96a3 \arrow[ur, dash, "2"'] & & & & &
\end{tikzcd}$$

whereas the isogeny classes of the last three curves are trivial; see [Cre97, Table 1] or [LMFDB]. Since $27a3$ is the quadratic twist by -3 of $27a1$, we have 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 $p \equiv 5, 7, 17, 19$ mod 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 $I = \mathrm{Gal}(L/\mathbb{Q}_2^{\mathrm{unr}}) \simeq H_8$. As explained at the beginning of section 4.2, the fact that H_8 is non-abelian implies that 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 in the case that $(2/p) = 1$ the isomorphism $E^{(d)}_{(a,b,c)}[p] \simeq E[p]$ can only be symplectic. So when $p \equiv 1, 7, 17, 23 \bmod 24$, 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. $\square$

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 $E/\mathbb{Q}_\ell$ can be obtained as the Frey curve evaluated at an ℓ-adically primitive solution of (2.1). Note that, for $\ell \in \{2, 3\}$ and $p \geq 5$, any ℓ-adic unit is a p-th power in $\mathbb{Q}_\ell$. For $\ell = 2$, we have the following triples (a, b, E), where $a, b \in \mathbb{Z}_2$ are coprime with $a^2 + b^3 \in \mathbb{Z}_2^\times$ and $E/\mathbb{Q}_2$ is the curve obtained as the associated (local) Frey curve:

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

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. This means that Theorem 5.1 is the optimal result obtainable from local information at 2 and 3.

Lemma 5.2. *Let $p \geq 3$ be a prime such that $(2/p) = -1$. Then, up to unramified quadratic twist, the p-torsion $G_{\mathbb{Q}_2}$-modules of the following curves admit exclusively the following isomorphism types:*

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

where $+$ means symplectic and $-$ anti-symplectic. Moreover, let a, b be coprime integers satisfying the congruences in line i_2 of Table 1 and write $E = E_{(a,b,c)}^{(d)}/\mathbb{Q}_2$, where d is any of the possible values in the same line. Then, up to unramified quadratic twist, the p-torsion $G_{\mathbb{Q}_2}$-modules of the following curves admit exclusively the following isomorphism types:

$i_2 = 2$ with $d = \pm 1, \pm 3$ or $i_2 = 6$:	$E \overset{+}{\simeq} 288a1$,	$E \overset{-}{\simeq} 864a1$,	$E \overset{+}{\simeq} 864b1$
$i_2 = 2$ with $d = \pm 2, \pm 6$:	$E \overset{-}{\simeq} 288a1$,	$E \overset{+}{\simeq} 864a1$,	$E \overset{-}{\simeq} 864b1$
$i_2 = 3$ with $d = \pm 1, \pm 3$ or $i_2 = 5$:	$E \overset{+}{\simeq} 96a1$,	$E \overset{+}{\simeq} 864c1$	
$i_2 = 3$ with $d = \pm 2, \pm 6$:	$E \overset{-}{\simeq} 96a1$,	$E \overset{-}{\simeq} 864c1$	

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 compared in the statement. We have seen in Section 3 that E and E' have the same inertial field at 2. From Theorem 4.6 we know that there is an isomorphism of I_2-modules $\phi \colon E[p] \to E'[p]$. We can then use [FK19, Theorem 9] to decide whether this isomorphism is symplectic or anti-symplectic. We will now 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 $L_p = \mathbb{Q}_2(E[p])$ for the p-torsion field of E and let U_p be the maximal unramified extension of $\mathbb{Q}_2$ contained in L_p. Note that all the curves in the statement acquire good reduction over L_3 and have trace of Frobenius $a_{L_3} = -4$ (this can be checked using Magma). Therefore, we know that

$$\overline{\rho}_{E,p}|_{I_2} \simeq \overline{\rho}_{E',p}|_{I_2} \quad \text{and} \quad \overline{\rho}_{E,p}|_{G_{L_3}} \simeq \overline{\rho}_{E',p}|_{G_{L_3}}.$$

Note that $G_{U_3} = G_{L_3} \cdot I_2$. We now apply [Cen16, Theorem 2] to find that there is a basis in which $\overline{\rho}_{E,p}(\mathrm{Frob}_{L_3})$ is the scalar matrix $-2 \cdot \mathrm{Id}_2$. Thus the same is true in all bases;

therefore $\overline{\rho}_{E,p}(\mathrm{Frob}_{L_3})$ commutes with all matrices in $\overline{\rho}_{E,p}(I_2)$. Since the same is true for E', the isomorphism between $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ on the subgroups I_2 and G_{L_3} extends to G_{U_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 $\mathrm{Gal}(L_3/\mathbb{Q}_2)$ is isomorphic to the semi-dihedral group with 16 elements, hence $H_8 \simeq I \subset G_3$ with index 2, thus $[U_3 : \mathbb{Q}_2] = 2$. Therefore, because the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are irreducible, they differ at most by the quadratic character χ fixing U_3, that is, we have

$$\overline{\rho}_{E,p} \simeq \overline{\rho}_{E',p} \quad \text{or} \quad \overline{\rho}_{E,p} \simeq \overline{\rho}_{E',p} \otimes \chi.$$

The last statement follows from Theorem 4.6 (1). $\square$

When (E, E') is any of the pairs of curves in the first part of the statement of Lemma 5.2, the unramified quadratic twist is actually never necessary, whereas it is necessary for some of the Frey curves in the second part. This can be checked on the 3-torsion by an explicit computation; the result for arbitrary p follows from this.

Since the isomorphism class of $X_E(p)$ (or $X_E^-(p)$) depends only on the symplectic Galois module $E[p]$ up to quadratic twist, Lemma 5.2 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 $(2/p) = -1$. In this latter case, the Frey curve gives rise to 'primitive' 2-adic points on $X_E^-(p)$ for $E \in \{96a1, 288a1, 864a1, 864b1, 964c1\}$.

Lemma 5.3. *Let $p \geq 5$ be a prime such that $(3/p) = -1$. Then, up to unramified quadratic twist, the p-torsion $G_{\mathbb{Q}_3}$-modules of the following curves admit exclusively the following isomorphism types:*

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

where $+$ means symplectic and $-$ anti-symplectic. Moreover, let a, b be coprime integers satisfying the congruences in line i_3 of Table 2 and write $E = E^{(d)}_{(a,b,c)}/\mathbb{Q}_3$, where d is any of the possible values in the same line. Then, up to unramified quadratic twist, the p-torsion $G_{\mathbb{Q}_3}$-modules of the following curves admit exclusively the following isomorphism types:

$$\begin{array}{llll}
i_3 = 3 \text{ or } 5 \text{ with } d = \pm 1, \pm 2: & E \overset{-}{\simeq} 27a1, & E \overset{+}{\simeq} 864b1, & E \overset{-}{\simeq} 864c1 \\
i_3 = 3 \text{ or } 5 \text{ with } d = \pm 3, \pm 6: & E \overset{+}{\simeq} 27a1, & E \overset{-}{\simeq} 864b1, & E \overset{+}{\simeq} 864c1 \\
i_3 = 4 \text{ or } 7 \text{ with } d = \pm 1, \pm 2: & E \overset{-}{\simeq} 54a1, & E \overset{+}{\simeq} 864a1 & \\
i_3 = 4 \text{ or } 7 \text{ with } d = \pm 3, \pm 6: & E \overset{+}{\simeq} 54a1, & E \overset{-}{\simeq} 864a1 &
\end{array}$$

Furthermore, if instead $p \geq 5$ satisfies $(3/p) = 1$, then all the previous isomorphisms are symplectic.

Proof. The proof proceeds in the same way as for the previous lemma, replacing 2 and 3 by 3 and 5, respectively. We now use Theorem 11 of [FK19] to obtain the result on the level of inertia. We then see that $G_{U_3} = G_{L_5} \cdot I_3$ and that all the curves in the statement acquire good reduction over L_5 and have trace of Frobenius $a_{L_5} = -18$. We conclude as before that $\overline{\rho}_{E,p}$ and $\overline{\rho}_{E',p}$ are isomorphic when restricted to G_{U_5}. In the present case we have $[U_5 : \mathbb{Q}_3] = 4$, so it a priori conceivable that the representations differ by an unramified quartic twist. However, this is not possible, because both representations have the same determinant. We conclude that they differ at most by an unramified quadratic twist. $\square$

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 $X_E^{\pm}(p)$ 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 $X_{54a1}^{\pm}(p)$ and 3-adic points on $X_{96a1}^{\pm}(p)$. 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 2-adic and 3-adic arguments. Note that in some cases it is possible to use local arguments at other primes to rule out some further twists. For example, in [FK19, Section 32] it is shown that the twist $X_{864a1}^{-}(p)$ can be excluded for $p = 19$ and 43 and that $X_{864b1}^{-}(p)$ can be excluded for $p = 19$, 43 and 67, working at a suitable prime of good reduction.

Proposition 5.4. *Let $\ell \neq p$ be primes with $p \geq 3$ and $\ell \not\equiv 1 \bmod p$. Let E_1 and E_2 be Tate curves over $\mathbb{Q}_\ell$ with Tate parameters q_1 and q_2. Write $e_1 = v_\ell(q_1)$ and $e_2 = v_\ell(q_2)$ and suppose that $p \nmid e_1 e_2$.*

Then $E_1[p]$ and $E_2[p]$ are isomorphic $G_{\mathbb{Q}_\ell}$-modules.

Proof. Fix a primitive pth root of unity $\zeta \in \overline{\mathbb{Q}}_\ell$. Since $p \nmid e_1 e_2$, we can find integers n and m (with $p \nmid n$) satisfying $e_2 = n e_1 + p m$. Write $a = q_2 / q_1^n \ell^{mp}$; then a is a unit in $\mathbb{Q}_\ell$. Since by assumption $p \neq \ell$ and $\ell \not\equiv 1 \bmod p$, every unit is a pth power, hence there is $\alpha \in \mathbb{Q}_\ell$ satisfying $\alpha^p = a$. Thus $q_2 = q_1^n (\ell^m \alpha)^p$ with $p \nmid n$. Fix $\gamma_1 \in \overline{\mathbb{Q}}_\ell$ with $\gamma_1^p = q_1$. Setting $\gamma_2 = \gamma_1^n \ell^m \alpha$, we have $\gamma_2^p = q_2$. By the theory of the Tate curve, we can use $(\zeta q_i^{\mathbb{Z}}, \gamma_i q_i^{\mathbb{Z}})$ as an $\mathbb{F}_p$-basis for the p-torsion of E_i. We claim that the isomorphism $\phi\colon E_1[p] \to E_2[p]$ of $\mathbb{F}_p$-vector spaces given by the matrix

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$$

with respect to these bases is actually an isomorphism of $G_{\mathbb{Q}_\ell}$-modules. To see this, consider $\sigma \in G_{\mathbb{Q}_\ell}$. Then $\sigma(\zeta) = \zeta^r$ for some $r \in \mathbb{F}_p^\times$ and $\sigma(\gamma_1) = \zeta^s \gamma_1$ for some $s \in \mathbb{F}_p$, which implies that $\sigma(\gamma_2) = \zeta^{ns} \gamma_2$. We then have

$$\phi(\sigma(\zeta q_1^{\mathbb{Z}})) = \phi(\zeta^r q_1^{\mathbb{Z}}) = \zeta^{nr} q_2^{\mathbb{Z}} = \sigma(\zeta^n q_2^{\mathbb{Z}}) = \sigma(\phi(\zeta q_1^{\mathbb{Z}}))$$

and

$$\phi(\sigma(\gamma_1 q_1^{\mathbb{Z}})) = \phi(\zeta^s \gamma_1 q_1^{\mathbb{Z}})) = \zeta^{ns} \gamma_2 q_2^{\mathbb{Z}} = \sigma(\gamma_2 q_2^{\mathbb{Z}}) = \sigma(\phi(\gamma_1 q_1^{\mathbb{Z}}))$$

as desired. $\square$

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

Proof. Note that $2 \not\equiv 1 \bmod p$ and $3 \not\equiv 1 \bmod p$, so Proposition 5.4 applies for $\ell = 2$ and $\ell = 3$.

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 $v_2(q_E) = -v_2(j_E) = -6 + pv_2(c)$.

Since $p \neq 3$, 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 $\mathbb{Q}_2$. $\square$

A Magma script that performs the necessary computations for the results in this section is available as `section5.magma` at [Sto].

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 $\mathbb{Z}[i]$. $\square$

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 $X^+_{\mathrm{sp}}(p)$, 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 [Shi94, 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 weight 2 and level M_f dividing p^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 [Shi94, 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 $J_{\text{ns}}^{(d)}(p)$ have positive rank.

To conclude this section, we mention that when $p = 13$, we are in the split case for both CM curves. During the work on this paper, it was an open question whether the set of rational points on $X_{\text{sp}}^+(13)$ consists of cusps and CM points. (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.

After our work was finished, Steffen Müller announced at a workshop in Banff that in joint work with Balakrishnan, Dogra, Tuitman and Vonk the set $X_{\text{ns}}^+(13)(\mathbb{Q})$ could be determined using 'Quadratic Chabauty' techniques. This work has now appeared as [BDM+19]. Since there is an accidental isomorphism $X_{\text{ns}}^+(13) \simeq X_{\text{sp}}^+(13)$ and there are no unexpected points, this gives another proof of Lemma 8.2.

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 $12^3 - j = 12^3 a^2/c^{11}$ 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.

Some of the results in this section rely on computations that require a computer algebra system. We provide a script `section7.magma` at [Sto] (which relies on `localtest.magma`, also provided there) that can be loaded into Magma and performs these computations.

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; see [DFGS14, Remark 1]. 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 (see [Lig77, Proposition II.4.3.8.1])

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

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 using Magma 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. 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, with a (geometric) point defined over 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 [Sto17]. 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

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

We define the following set of subsets of $\mathbb{P}^1(\mathbb{Q}_2)$.

$$\begin{aligned} \mathcal{D} = \bigl\{ & 15 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2,\ 2^9 + 2^{11}\mathbb{Z}_2,\ -2^9 + 2^{11}\mathbb{Z}_2,\ \{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}, \\ & \{12^3 - 3 \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 - 2^{10}t^2 : t \in \mathbb{Z}_2\}, \\ & \{12^3 + 2^{10}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 + 3 \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\} \bigr\} \end{aligned} \tag{7.2}$$

Note that according to Table 1 all elements in these sets are 2-adically good j-invariants, and for each set, all fibers of the j-map $X_0(11) \to \mathbb{P}^1$ over points in the set are isomorphic over $\mathbb{Q}_2$ (excluding $j = 12^3$ and $j = \infty$).

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 $D \in \mathcal{D}$, depending on E.*

$$\begin{aligned} 54a1\colon & \{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}\,. \\ 96a1\colon & 15 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2,\ -2^9 + 2^{11}\mathbb{Z}_2\,. \\ 864a1\colon & \{12^3 - 2^{10}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 + 3 \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\}\,. \\ 864b1\colon & \{12^3 - 3 \cdot 2^{10}t^2 : t \in \mathbb{Z}_2\},\ \{12^3 + 2^{10}t^2 : t \in \mathbb{Z}_2\},\ 2^9 + 2^{11}\mathbb{Z}_2\,. \\ 864c1\colon & 15 \cdot 2^6 + 2^{11}\mathbb{Z}_2,\ -2^6 + 2^{11}\mathbb{Z}_2,\ -2^9 + 2^{11}\mathbb{Z}_2\,. \end{aligned}$$

Proof. This follows from the information in Table 1, together with Lemma 5.2, which allows us to distinguish between $X_E(p)$ and $X_E^-(p)$ (note that 2 is a non-square mod 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 $E \in \mathcal{E}$.

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

$$\begin{aligned}
F(x,j) = {} & (x^4 - 52820x^3 + 1333262x^2 + 4971236x + 9789217)^3 \\
& + (1486x^{11} + 43119747x^{10} + 38323813979x^9 + 5072626276355x^8 \\
& \qquad + 164063633585170x^7 + 1134855511654843x^6 - 4074814667347831x^5 \\
& \qquad - 29669709666741936x^4 + 6839041777752481x^3 + 159480622275659333x^2 \\
& \qquad + 199736619430410535x - 104748564078368391)j \\
& - (x-16)^{11} j^2 = 0\,.
\end{aligned} \tag{7.4}$$

We now state a technical lemma for later use.

Lemma 7.5. *Let K be a field complete with respect to an absolute value $|\cdot|$. Consider a polynomial $F = \sum_{i,j\ge 0} f_{ij} x^i y^j \in K[x,y]$. Fix an integer $e \ge 1$ such that the characteristic of K does not divide e. We assume that $f_{0j} = 0$ for $0 \le j < e$ and that $f_{0e} = 1$. For $j \ge 0$, we set $F_j(t) = \sum_{i\ge 0} f_{ij} t^i \in K[t]$, so that $F(x,y) = \sum_{j\ge 0} F_j(x) y^j$. Assume that $F_0(t) = -ct +$ higher order terms, with $c \neq 0$. For a real number $r > 0$ and a polynomial $f(t) = a_n t^n + \ldots + a_1 t + a_0 \in K[t]$, we set $|f|_r = \max\{r^i |a_i| : 0 \le i \le n\}$.*

There are exactly e formal power series $\phi_0, \ldots, \phi_{e-1} \in L[\![t]\!]$, where L is the splitting field of $X^e - c$ over K, such that $\phi_j(0) = 0$ and $F(t^e, \phi_j(t)) = 0$. If $\zeta \in L$ is a primitive eth root of unity, then we can label the ϕ_j in such a way that $\phi_j(t) = \phi_0(\zeta^j t)$.

If $r > 0$ is such that $|F_m(t^e)|_r < |F_0(t^e)|_r^{(e-m)/e}$ for $0 < m < e$, $|F_e(t^e) - 1|_r < 1$ and $|F_0(t^e)|_r^{(m-e)/e} |F_m(t^e)|_r < 1$ for $m > e$, then the ϕ_j converge on the closed disk of radius r in L, and we have $|\phi_j(\tau)| \le |F_0(t^e)|_r^{1/e}$ for all τ in this disk. If in addition $|F_0(t^e) + ct^e|_r < |F_0(t^e)|_r$, then $|\phi_j(\tau)| = |c|^{1/e} |\tau|$ for all these τ.

Proof. We consider the equation $F(t^e, y) = 0$ over the field of Laurent series $L(\!(t)\!)$. The assumptions $f_{0j} = 0$ for $0 \le j < e$, $f_{0e} = 1$ and $f_{10} = -c \neq 0$ imply that the Newton

Polygon of $F(t^e, y)$ has a segment of length e and slope $-e$, and that all other slopes are ≥ 0. This already shows that there are at most e power series with the required properties. Also, the reduction modulo t of $t^{-e}F(t^e, tz)$ is $z^e - c$, which is a separable polynomial splitting over L into linear factors. So by Hensel's Lemma, there are exactly e solutions $z \in L[\![t]\!]$. Let $\phi_0 = tz_0$ for one such solution z_0. Clearly, each solution z gives rise to exactly one power series ϕ_j. Since the original equation is invariant under the substitution $t \mapsto \zeta^j t$, $\phi_j(t) := \phi_0(\zeta^j t)$ is a solution for each $0 \leq j < e$. Since $\gamma = z_0(0) \neq 0$ (it is an eth root of c), we have $\phi_0(t) = \gamma t + \ldots$, and so all these ϕ_j are pairwise distinct.

Now consider the completion of the polynomial ring $L[t]$ with respect to $|\cdot|_r$. This is the Tate Algebra T_r of power series converging on the closed disk of radius r (in the algebraic closure of L). The assumptions on r guarantee that the Newton Polygon of $F(t^e, y)$, considered over T_r, again has a unique segment of length e and slope corresponding to the absolute value $|F_0(t^e)|_r^{1/e}$, whereas all other slopes correspond to larger absolute values. As can be seen by letting r tend to zero, the corresponding solutions must be given by the ϕ_j. The claim that $|\phi_j(\tau)| \leq |F_0(t^e)|_r^{1/e}$ follows from $|\phi_j|_r = |F_0(t^e)|_r^{1/e}$. For the last claim, note that $|F_0(t^e)|_r = |c|r^e$ and that if $|\phi_j(\tau)| < |c|^{1/e}$, then the term $-c\tau^e$ would be dominant in $F(\tau^e, \phi_j(\tau))$, which gives a contradiction. □

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 7.6. *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 different from $\{2^{-5}t^{-11} : t \in \mathbb{Z}_2\}$, and let $\varphi\colon \mathbb{Z}_2 \to D$ be the parameterization in terms of t as given in (7.2). Let $P \in X_0(11)(K)$ be such that $j(P) \in D$. Then P is in the image of an analytic map $\phi\colon \mathbb{Z}_2 \to X_0(11)(K)$ such that $j \circ \phi = \varphi$, and the square class of $x(\phi(z)) - \theta \in L^\times$ is constant for $z \in \mathbb{Z}_2$.*

Proof. By the information in Table 1 the $\mathbb{Q}_2$-isomorphism type of the fiber of j above D is constant, say given by the disjoint union of $\operatorname{Spec} K_i$ for certain 2-adic fields K_i. We note that all K_i 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 can then take $K = K_i$, since we will use a purely valuation-theoretic criterion for the second statement, so the choice of field will be largely irrelevant. In the following, $F(x, j) = 0$ is the relation between the x-coordinate on $X_0(11)$ and the associated j-invariant given in (7.4).

If D is not one of the last four sets in (7.2), then we solve $F(x_0 + \phi_0, \varphi(t)) = 0$ for a power series ϕ_0 with $\phi_0(0) = 0$, where $x_0 \in K$ is any root of $F(x, \varphi(0))$. For each possible D and x_0, Lemma 7.5 allows us to deduce that such a power series ϕ_0 exists, that it converges on an open disk containing $\mathbb{Z}_2$ and that it satisfies $v_2(\phi_0(\tau)) > 4/3$ for all $\tau \in \mathbb{Z}_2$. Since we obtain as many power series as there are roots of $F(x, z) = 0$ for any $z \in D$ (this is because the fibers over D of the j-map are all isomorphic, so the number of roots in K is constant) and since the y-coordinate of a point on $X_0(11)$ is uniquely determined by its x-coordinate and its image under the j-map (unless $b(x) = 0$, but this never happens for the points we are considering), we obtain analytic maps $\phi\colon \mathbb{Z}_2 \to X_0(11)(K)$ whose images cover all points P as in the statement. Also, $v_2(x(\phi(\tau)) - x_0) = v_2(\phi_0(\tau)) > 4/3 = 2 + v_2(x_0 - \theta)$, which implies (compare [Sto01, Lemma 6.3]) that $x(\phi(\tau)) - \theta$ is in the same square class as $x_0 - \theta$.

If D is one of the last four sets in (7.2), then we proceed in a similar way. Note that the four parameterizations $\varphi(t) = 12^3 + a2^{10}t^2$ all have 2-adic units a and so can be converted one into another by scaling t by a 2-adic unit (in some extension field of $\mathbb{Q}_2$). Since we only care about valuations in the argument, it is sufficient to just work with one of them. In the same way as before, we consider $F(x_0 + \phi_0(t), \varphi(t)) = 0$ as an equation to be solved for a power series ϕ_0 with $\phi_0(0) = 0$, where $x_0 \in K$ is such that $F(x_0, 12^3) = 0$. We apply Lemma 7.5 again, this time with $e = 2$, and the remaining argument is similar to the previous case. $\square$

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

Lemma 7.7. *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 $D \in \mathcal{D}$, depending on E.*

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

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

$$\begin{tikzcd} X_0(11)(K_E) \arrow[r] \arrow[d] & \mathrm{Sel}_2(X_0(11)/K_E) \arrow[r, hook] \arrow[d] & \dfrac{L_E^\times}{L_E^{\times 2}} \arrow[d] \\ X_0(11)(K_{E,2}) \arrow[r] & \dfrac{X_0(11)(K_{E,2})}{2X_0(11)(K_{E,2})} \arrow[r, hook] & \dfrac{L_{E,2}^\times}{L_{E,2}^{\times 2}}\,. \end{tikzcd}$$

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 7.6, the square class we obtain for a point in $X_0(11)(K_{E,2})$ mapping into a fixed set 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. $\square$

It remains to deal with the remaining five sets 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 [Sto17].

Lemma 7.8. *Let $E \in \mathcal{E}$ and let $D \in \mathcal{D}$ be one of the sets associated to E in Lemma 7.7. 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 7.7 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 have 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 $j(P) \in D$. $\square$

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 $t = -x/y$ to be a uniformizer at the point at infinity on $X_0(11)$ and write $\mathcal{K}_\nu = \{P \in \mathcal{K} : v_2(t(P)) > \nu\}$.

Lemma 7.9. *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 $\mathcal{K} \cap X_0(11)(K)$.

Proof. Note that the points T of order 2 on $X_0(11)$ satisfy $v_2(t(T)) = 1/3$ (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 P with $v_2(t(P)) > 1/3$, so log is injective on this set. Explicitly, we find that for $P \in \mathcal{K}$ with $t(P) = \tau$,

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

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 $\mathcal{K} \cap X_0(11)(K)$. $\square$

Lemma 7.10. *Let K be some 2-adic field such that $X_0(11)(K)[2] = 0$ and consider an analytic map $\phi\colon \mathbb{Z}_2 \to \mathcal{K} \cap X_0(11)(K)$. We assume that ϕ actually converges on the open disk $D_{-c} = \{\tau \in \mathbb{C}_2 : v_2(\tau) > -c\}$ for some $c > 0$ and that there is some $\nu \in \mathbb{Q}_{>1/3}$ such that $|t(\phi(\tau))| = |2|^\nu\,|\tau|$ for all $\tau \in D_{-c}$. (This implies that $\phi(0)$ is the point at infinity.) We set $\mu = \lceil \nu - \frac{1}{3} \rceil - 1 \in \mathbb{Z}_{\geq 0}$.*

Then for each $\tau \in \mathbb{Z}_2 \setminus \{0\}$ there is a unique $Q_\tau \in \mathcal{K} \cap X_0(11)(K)$ such that $\phi(\tau) = 2^{\mu + v_2(\tau)} Q_\tau$. If $\tau \in \mathbb{Z}_2^\times$, then $Q_\tau \equiv Q_1 \bmod 2X_0(11)(K)$. If $\nu - \mu + \min\{1, c, \nu - \frac{1}{3}\} > \frac{4}{3}$, then this remains true for arbitrary $\tau \in \mathbb{Z}_2 \setminus \{0\}$. Otherwise, we have that $Q_\tau \equiv Q_2 \bmod 2X_0(11)(K)$ if $\tau \in 2\mathbb{Z}_2 \setminus \{0\}$.

Proof. Fix $0 \neq \tau \in \mathbb{Z}_2$ and write $n = v_2(\tau)$. By assumption, we have that $\phi(\tau) \in \mathcal{K}_{\nu+n}$. Since $\nu > 1/3 + \mu$, this implies that $\phi(\tau)$ is divisible by $2^{\mu+n}$ in $\mathcal{K} \cap X_0(11)(K)$ by Lemma 7.9. Since $X_0(11)(K)[2] = 0$, there is then a unique point $Q_\tau \in \mathcal{K} \cap X_0(11)(K)$ such that $\phi(\tau) = 2^{\mu+n} Q_\tau$. We now consider

$$\log \phi(\tau) = \gamma\big(\tau + a_2\tau^2 + a_3\tau^3 + \ldots\big)\,.$$

We know by assumption and by Lemma 7.9 and its proof that $|\log \phi(\tau)| = |t(\phi(\tau))| = |2|^\nu\,|\tau|$ whenever $v_2(\tau) > -\min\{c, \nu - \frac{1}{3}\}$ (for $\tau \in \mathbb{C}_2$). This implies that $v_2(\gamma) = \nu$ and that

$$v_2(a_k) \geq (k-1)\min\{c, \nu - \tfrac{1}{3}\} \qquad \text{for all } k \geq 2.$$

Writing $\tau = 2^n u$ with $u \in \mathbb{Z}_2^\times$, we then have that

$$\log Q_\tau = 2^{-\mu-n} \log \phi(\tau) = \gamma 2^{-\mu}(u + 2^n a_2 u^2 + 2^{2n} a_3 u^3 + \ldots)$$

and so

$$\log(Q_\tau - Q_1) = \log Q_\tau - \log Q_1 = \gamma 2^{-\mu}\big((u-1) + a_2(2^n u^2 - 1) + a_3(2^{2n}u^3 - 1) + \ldots\big)\,.$$

If $n = 0$, then $v_2(\log(Q_\tau - Q_1)) \geq \nu - \mu + 1 > \frac{4}{3}$, and if $\nu - \mu + \min\{1, c, \nu - \frac{1}{3}\} > \frac{4}{3}$, then $v_2(\log(Q_\tau - Q_1)) \geq \nu - \mu + \min\{1, v_2(a_2), v_2(a_3), \ldots\} > \frac{4}{3}$, so in both cases, Lemma 7.9 shows that $Q_\tau - Q_1$ is divisible by 2 in $\mathcal{K} \cap X_0(11)(K)$. If $n \geq 1$, then we find that

$$\log(Q_\tau - Q_2) = \gamma 2^{-\mu}\big((u-1) + 2a_2(2^{n-1}u^2 - 1) + 2^2 a_3(2^{2n-2}u^3 - 1) + \ldots\big)\,,$$

and we see that this has 2-adic valuation $> \frac{4}{3}$, so $Q_\tau - Q_2$ is divisible by 2. $\square$

Remark 7.11. We will apply this lemma in the following setting. We consider one of the remaining sets $D \in \mathcal{D}$ and a point $P \in X_0(11)(K_E)$ such that $j(P) \in D$. Then there is an analytic map $\psi\colon \mathbb{Z}_2 \xrightarrow{\simeq} D \to X_0(11)(K_{E,2})$ such that $\psi(0) = P$ and such that the second map in this composition inverts the j function. We set $\phi(\tau) = \psi(\tau) - P$; then ϕ is an analytic map into $\mathcal{K} \cap X_0(11)(K_{E,2})$, which satisfies a polynomial relation $\Phi(\tau, t(\phi(\tau))) = 0$, where $\Phi \in K_E[x, y]$ has degree 3 in x and degree 12 in y (this is because $j\colon X_0(11) \to \mathbb{P}^1$ has degree 12 and $t\colon X_0(11) \to \mathbb{P}^1$ has degree 3). We find Φ explicitly by interpolation: we compute the pairs $(j(Q), t(Q))$ for all points $Q = nP + T$, where $-5 \leq n \leq 5$ and $T \in X_0(11)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z}$. This gives us enough information to determine the 52 coefficients of Φ (up to scaling). We then use Lemma 7.5 to show that ϕ actually converges for $v_2(\tau) > -c$ for some $c > 1/3$ and that $v_2(t(\phi(\tau))) = \nu + v_2(\tau)$ for $v_2(\tau) > -c$ (where $\nu = 2$, 3 or 5/11 in the concrete cases considered). Finally, we check that Q_1 does not map into the image of the Selmer group (and that Q_2 does not, either, in the last case). This then verifies condition (*) for D, E and P.

Lemma 7.12. *Let $E \in \mathcal{E}$ and let $D \in \mathcal{D}$ be one of the sets associated to E in Lemma 7.7. Then the point P given in the table below satisfies (*) for E and D. Here* $\operatorname{can}(E)$ *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
$96a1$	$15 \cdot 2^6 + 2^{11}\mathbb{Z}_2$	$-\operatorname{can}(96a2)$	no
$96a1$	$-2^6 + 2^{11}\mathbb{Z}_2$	$\operatorname{can}(96a1)$	yes
$864b1$	$2^9 + 2^{11}\mathbb{Z}_2$	$\operatorname{can}(864b1)$	yes
$864c1$	$-2^9 + 2^{11}\mathbb{Z}_2$	$\operatorname{can}(864c1)$	yes

Proof. The points P given in the table have the property that their image in $G = L_{E,2}^\times / L_{E,2}^{\times 2}$ 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 use Fisher's explicit description of $X_E(11)$ and the j-map on it [Fis14] to obtain a partition of $X_{96a1}(11)(\mathbb{Q}_2)$ into 2-adic disks; 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 in $X_0(11)(K_{E,2})$ above D that we have to consider is the disk D' containing the image of the canonical point. We then follow the approach outlined in Remark 7.11 above to verify (*) for each of the last three entries in the table.

Next we consider the other disk D for $E = 96a1$; this is the second entry in the table. There are four disks D' in $X_0(11)(K_{E,2})$ 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 these 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 $j = 2^{-5}\tau^{-11}$ and solving for the x and y-coordinates in $\mathbb{Q}(\sqrt[11]{2})((\tau))$. We use the alternative uniformizer $t' = -(x-5)/(y-5)$ at the origin (the standard uniformizer t does not work well in this case, because it is 2-adically small on the other branch above $j = \infty$), which has the additional benefit that it is of degree 2 instead of 3 as a function on $X_0(11)$, leading to a smaller polynomial Φ. The statements of Lemmas 7.9 and 7.10 are unaffected by this change of uniformizer. Using the approach of Remark 7.11, we find that the series ϕ of Lemma 7.10 converges for $v_2(\tau) > -5/11$ and satisfies $v_2(\phi(\tau)) = 5/11 + v_2(\tau)$. We can also check that for $\tau = 1$ and for $\tau = 2$ we obtain a point whose image in G is not in the image of the Selmer group, so (*) is verified in this case, too. $\square$

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.

Remark 7.13. According to work by Ligozat [Lig77], the Jacobian $J(11)$ of $X(11)$ splits up to isogeny (and over $\mathbb{Q}(\sqrt{-11})$) into a product of eleven copies of $X_0(11)$, ten copies of a second elliptic curve and five copies of a third elliptic curve (which is $X^+_{\mathrm{ns}}(11) = 121b1$). The powers of these three elliptic curves correspond to isotypical components of the representation of the automorphism group of the j-map $X(11) \to \mathbb{P}^1$ on the Lie algebra of $J(11)$; the splitting into these three powers therefore persists over $\mathbb{Q}$ after twisting. Our approach uses the 11-dimensional factor (it can be identified with the kernel of the trace map from $R_{K_E/\mathbb{Q}} X_0(11)_{K_E}$ to $X_0(11)$, up to isogeny). It would be nice if one could use the 5-dimensional factor instead in the hope of eliminating the dependence on GRH, but so far we have not found a description that would allow us to work over a smaller field.

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

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

which shows that it indeed gives a cyclic covering of $\mathbb{P}^1_v$ by $\mathbb{P}^1_z$. If d is a squarefree 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

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

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 $\mathbb{Q}(\omega)$. We denote the curve in row i of the table by C_i.

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 C_1 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 curves C_2, C_3 and C_4, a 2-descent on the Jacobian as in [Sto01] gives an upper bound of 2 for the rank. C_2 and C_4 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 C_3 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 C_2 and C_4.

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 six curves that do have rational points then give points on $X_0(13)$ with $v = \infty$, 0, -4, 1, -12, $-8/5$ and j-invariants

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

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 C_2 and C_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 in each orbit of rational points under the action of the automorphism group, there is a point that lifts to the 2-covering of the curve that lifts the two points at infinity. So it is enough to look at rational points on this 2-covering.

We first consider 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; 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 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 and that the difference of the two points at infinity has infinite order, so the Mordell-Weil rank of E over L is 1. 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 $(a, b, c) \in \mathbb{Z}^3$ 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 (at least) 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 C_{27a1} and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for C_{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 C_{27a1}, or the primes above 5 for C_{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 (the same for both primes), 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 $(a, b, c) \in \mathbb{Z}^3$ 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 $E[13]$, where E is 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. ☐

A Magma script that performs the necessary computations for the results in this section is available as `section8.magma` at [Sto]. It relies on `X1_13_opt.magma`, which is available at the same location.

9. Possible extensions

Since $X_0(17)$ and $X_0(19)$ are elliptic curves like $X_0(11)$, the approach taken in this paper to treat the case $p = 11$ has a chance to also work for $p = 17$ and/or $p = 19$. Since $X_0(17)$ has a rational point of order 4 and $X_0(19)$ has a rational point of order 3, suitable Selmer groups can be computed with roughly comparable effort (requiring arithmetic information of number fields of degree 36 or 40). This is investigated in ongoing work by the authors. For $p = 13$, results beyond those obtained in the preceding section are likely harder to obtain than for $p = 17$ or $p = 19$, since $X_0(13)$ is a curve of genus 0. We can try to work with twists of $X_1(13)$, which is a curve of genus 2; our approach would require us to find the (relevant) points on such a twist over a field of degree 14. The standard method of 2-descent on the Jacobian of such a curve would require working with a number field of degree $6 \cdot 14 = 84$, which is beyond the range of feasibility of current algorithms (even assuming GRH).

References

[BDM+19] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, DOI 10.4007/annals.2019.189.3.6. ↑6

[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

[BBF18] Michael A. Bennett, Carmen Bruni, and Nuno Freitas, *Sums of two cubes as twisted perfect powers, revisited*, Algebra Number Theory **12** (2018), no. 4, 959–999, DOI 10.2140/ant.2018.12.959. MR3830208 ↑1.3

[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

[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, 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 Math. Sigma **4** (2016), e6, 80, DOI 10.1017/fms.2016.1. MR3482281 ↑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

[Cen16] Tommaso Giorgio Centeleghe, *Integral Tate modules and splitting of primes in torsion fields of elliptic curves*, Int. J. Number Theory **12** (2016), no. 1, 237–248, DOI 10.1142/S1793042116500147. MR3455277 ↑5

[Che98] Imin Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 1–38, DOI 10.1112/S0024611598000392. MR1625491 ↑6

[Coh07] Henri Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007. MR2312338 ↑1

[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, https://dspace.library.uu.nl/handle/1874/29640. ↑2

[DDT94] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154. MR1474977 ↑3

[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, DOI 10.4310/MRL.2000.v7.n2.a1 (French, with English and French summaries). MR1764312 ↑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 ↑5

[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 $X^2 + Y^3 + Z^5 = 0$*, 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

[Fre16] Nuno Freitas, *On the Fermat-type equation $x^3 + y^3 = z^p$*, Comment. Math. Helv. **91** (2016), no. 2, 295–304, DOI 10.4171/CMH/386. MR3493372 ↑1.3, 4, 4

[FK16] Nuno Freitas and Alain Kraus, *An application of the symplectic argument to some Fermat-type equations*, C. R. Math. Acad. Sci. Paris **354** (2016), no. 8, 751–755, DOI 10.1016/j.crma.2016.06.002 (English, with English and French summaries). MR3528327 ↑1.3

[FK19] ______, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Memoirs of the AMS (to appear) (2019), available at https://arxiv.org/abs/1607.01218. ↑1.3, 4.2, 5, 5

[FS15] Nuno Freitas and Samir Siksek, *Fermat's last theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895, DOI 10.2140/ant.2015.9.875. MR3352822 ↑1

[Gér78] Paul Gérardin, *Facteurs locaux des algèbres simples de rang* 4. *I*, Reductive groups and automorphic forms, I (Paris, 1976/1977), Publ. Math. Univ. Paris VII, vol. 1, Univ. Paris VII, Paris, 1978, pp. 37–77 (French). MR680785 ↑3

[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 (French, with English summary). MR1915212 ↑1

[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 (French, with English summary). MR1080288 ↑2, 3

[KO92] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), no. 2, 259–275, DOI 10.1007/BF01444715 (French). MR1166121 ↑4, 4.1

[Lig77] Gérard Ligozat, *Courbes modulaires de niveau* 11, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 149–237. Lecture Notes in Math., Vol. 601 (French). MR0463118 ↑7.1, 7.13

[LMFDB] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2017. http://www.lmfdb.org. ↑2, 5

[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 ↑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, DOI 10.1090/S0002-9939-2013-11532-7. MR3056552 ↑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, 1, 1, 2, 2, 2, 2, 4, 5, 8.1

[Roh94] David E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic curves and related topics, CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 125–157. MR1260960 ↑3

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, DOI 10.2307/1970722. MR0236190 ↑3, 4.2

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. MR1291394 ↑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*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑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

[Sto17] ______, *Chabauty without the Mordell-Weil group*, Algorithmic and experimental methods in algebra, geometry, and number theory, Springer, Cham, 2017, pp. 623–663. MR3792746 ↑1, 7.2, 7.2

[Sto] ______, *Magma scripts for the computations.* http://www.mathe2.uni-bayreuth.de/stoll/magma/index.html#GenFermat. ↑3, 5, 7, 8.2

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

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom

Email address: `nunobfreitas@gmail.com`

Faculty of Mathematics and Computer Science, Adam Mickiewicz University in Poznań, Uniwersytetu Poznańskiego 4, 61-614 Poznań, Poland

Email address: `nasqret@gmail.com`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

Email address: `Michael.Stoll@uni-bayreuth.de`

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