PRIMITIVE SOLUTIONS TO $x^2 + y^3 = z^{10}$

DAVID BROWN

ABSTRACT. We classify primitive integer solutions to $x^2 + y^3 = z^{10}$. The technique is to combine modular methods at the prime 5, number field enumeration techniques in place of modular methods at the prime 2, Chabauty techniques for elliptic curves over number fields, and local methods.

1. INTRODUCTION

We say a triple (s, t, u) of integers is *primitive* if $\gcd(s, t, u) = 1$. For $a, b, c \geq 3$ the equation $x^a + y^b = z^c$ is expected to have no primitive integer solutions with $xyz \neq 0$, while for $n \leq 9$ the equation $x^2 + y^3 = z^n$ has lots of such solutions; see for example [PSS07] for the case $n = 7$ and a review of previous work on generalized Fermat equations. The 'next' equation to solve is $x^2 + y^3 = z^{10}$ – it is the first of the form $x^2 + y^3 = z^n$ expected to have no non-obvious solutions.

Theorem 1.1. *The primitive integer solutions to $x^2 + y^3 = z^{10}$ are the 10 triples*

$$(\pm 1, 1, 0), (\pm 1, 0, 1), \pm(0, 1, 1), (\pm 3, -2, \pm 1).$$

It is clear that the only primitive solutions with $xyz = 0$ are the six above. To ease notation we set $S(\mathbb{Z}) = \{(a, b, c) : a^2 + b^3 = c^{10} \mid (a, b, c) \text{ is primitive}\}$.

One idea is to use Edwards's parameterization of $x^2+y^3 = z^5$. His thesis [Edw04] produces a list of 27 degree 12 polynomials $f_i \in \mathbb{Z}[x, y]$ such that if (x, y, z) is such a primitive triple, then there exist $i, s, t \in \mathbb{Z}$ such that

$$z = f_i(s, t)$$

and similar polynomials for x and y. This would reduce the problem to finding integral points on the 27 genus 5 hyperelliptic curves $-z^2 = f(s, t)$. This is a tempting approach, but the computational obstructions have not yet been overcome.

Alternatively, an elementry argument yields a parameterization of $x^2 + y^3 = z^2$, leading one to (independently) solve each of the two equations

$$y_1^3 + y_2^3 = z^5 \text{ or}$$
$$y_1^3 + 2y_2^3 = z^5.$$

Following [Bru00], a resultant/Chabauty argument resolves the first equation. For the second equation one must pass to a degree 3 number field, where one runs into a genus 2 curve whose

Date: March 29, 2010.

Jacobian has rank 3. There is less hope here for a classical Chabauty argument; [Sik] gives a solution along these lines, combining classical Chabauty methods with the elliptic Chabauty methods of [Bru03].

In a third direction one may consider the modular method used for example in [PSS07] to resolve the equation $x^2 + y^3 = z^7$. This method is most effective for large p; in particular, for a prime $p \geq 7$ the modular curve $X(p)$ has genus > 2 and conjecturally for $p \geq 17$ the curves $X_E(p)$ have no non-trivial $\mathbb{Q}$-points. Stated as a question by Mazur [Maz78, P. 133] for $p \geq 7$ and later relaxed to $p \geq 17$ (see [FM99, Table 5.3] for examples), this is now often called the Frey-Mazur conjecture. We note that direct application of this method to the equation $x^2 + y^3 = z^{10}$ at the prime 5 fails because $X(5)$ has genus 0.

The approach of this paper is to combine the traditional modular methods at the prime 5 described above and 'elementary' modular methods (based on number field enumeration) at the prime 2. Here the relevant modular curve is $X(10)$, which has genus 13. However it covers an elliptic curve X (with a modular interpertation) and the relevant twists $X_{(E,E')}(10)$ cover X over a degree 6 number field $K_{E,E'}$. For the pair (E, E') corresponding to the solution $(3, -2, 1)$ the elliptic curve X has rank 1 over $K_{E,E'}$ and one may apply the elliptic Chabauty methods of [Bru03]. Various local methods finish off the other cases.

The computer algebra package Magma [BCP97] is used in an essential way throughout.

Acknowledgements. I thank Bjorn Poonen for numerous conversations and for carefully reading earlier drafts of this paper and the participants of `mathoverflow.net` for help finding various references. Some computations were done on `sage.math.washington.edu`, which is supported by National Science Foundation Grant No. DMS-0821725.

2. A modular quotient of X(10)

Here we construct an elliptic quotient X of the full modular curve $X(10)$ whose twists X_E will be the center of our calculations.

Let E be an elliptic curve and p a prime. Following [PSS07, Section 4], we define $X_E(p)$ to be the compactified moduli space of elliptic curves E' plus symplectic isomorphisms (i.e. respecting Weil pairings) $E'[p] \cong E[p]$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Similarly, we define $X(p)$ to be the variant of the classical modular curve which parameterizes E' plus symplectic isomorphisms $E'[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules; in particular $X(p)$ is defined over $\mathbb{Q}$, is geometrically connected, and $X_E(p)_{\mathbb{C}}$ is isomorphic to $X(p)_{\mathbb{C}}$. Finally, for $p = 5$ we define (as in [PSS07, 4.4]) the variant $X_E^-(5)$ to be the compactified moduli space of elliptic curves E' plus anti-symplectic isomorphisms $E'[5] \cong E[5]$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules; here we define anti-symplectic to mean that the map induced by Weil pairings $\mu_5 \to \mu_5$ is the map $\zeta \mapsto \zeta^2$.

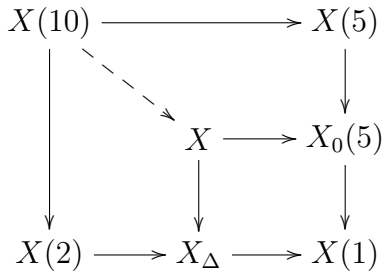
Remark 2.1 ([PSS07, 4.4]). Any isomorphism $E'[5] \cong E[5]$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules gives rise to a point on either $X_E(5)$ or $X_E^-(5)$. Indeed, for a positive integer N with $(N,5)=1$, the multiplication by N map $E \xrightarrow{[N]} E$ induces an isomorphism $E[5] \cong E[5]$ which changes the Weil pairing by N^2. Since $\mathbb{F}_5^*/(\mathbb{F}_5^*)^2 = \{1,2\}$, after composing with $[N]$ for some N, we arrive at an isomorphism $E'[5] \cong E[5]$ which either respects the Weil pairing or changes it by 2.

Recall that $X_0(p)$ is the modular curve whose points correspond to p-isogenies of elliptic curves up to twists. There are natural maps

$$X(p) \to X_0(p) \to X(1).$$

When $p=2$, $\mathrm{Gal}(X(2)/X(1)) \cong S_3$, and one can check by a direct calculation that the quotient of $X(2)$ by the normal subgroup A_3 is the degree 2 cover $X_\Delta \cong \mathbb{P}^1$ of $X(1) \cong \mathbb{P}^1$ given by $z \mapsto z^2 + 12^3$.

Definition 2.2. We define X to be the normalization of $X_\Delta \times_{X(1)} X_0(5)$. Denote by Y' the affine curve $Y(1) - \{12^3\}$, let $Y \subset X$ be the preimage of Y' in X, and let K be a number field; then a point in $Y(K)$ corresponds (up to twists) to a 5-isogeny $E \to E'$ defined over K with $j(E') \neq 12^3$ and a choice of a square root of $j(E) - 12^3 = c_6^2/\Delta_E$ in K (i.e. the fiber product $X_\Delta \times_{X(1)} X_0(5)$ is smooth away from cusps and the fiber of $12^3 \in X(1)$, which one can see via moduli using [DI95, Equation 9.1.2] or directly from the equations for X computed below).



Since A_3 is normal in S_3, the natural map $X_E(2) \to X(1)$ factors through a twist X_{Δ_E} of X_Δ mapping to $X(1)$ via $z \mapsto \Delta_E \cdot z^2 + 12^3$, and we define X_E to be the normalization of $X_{\Delta_E} \times_{X(1)} X_0(5)$. An easy calculation using [DI95, Equation 9.1.2] shows that X_E has genus 1; we omit the proof as this will be clear below when we compute explicit equations for X_E. Again, away from the cusps and the fiber over $12^3 \in X(1)$, the fiber product is smooth and so for a number field K and for Y_E the preimage of Y' in X_E, a point in $Y_E(K)$ corresponds (up to twists) to a 5-isogeny $E' \to E''$ defined over K such that $j(E) \neq 12^3$ and a choice of a square root of $(j(E') - 12^3)/\Delta_E = c_6^2/(\Delta_E \Delta_{E'})$ in K.

2.1. **Equations.** By [McM04, Table 3], equations for the map $Y_0(5) \xrightarrow{\pi_1} Y(1)$ sending a 5-isogeny $(E \to E')$ to $j(E)$ are given by

$$t \mapsto \frac{(t^2+250t+3125)^3}{t^5} = \frac{(t^2-500t-15625)^2(t^2+22t+125)}{t^5} + 12^3.$$

Equations for Y_E are thus obtained by setting equal the equations

$$\Delta_E \cdot z^2 + 12^3 = \frac{(t^2 - 500t - 15625)^2(t^2 + 22t + 125)}{t^5} + 12^3,$$

simplifying, and making the change of coordinates $y = zt^3/(t^2 - 500t - 15625)$. This gives

$$\Delta_E \cdot y^2 = t(t^2 + 22t + 125),$$

and the map $Y_E \xrightarrow{p_{\Delta_E}} X_{\Delta_E}$ is given by

$$(t, y) \mapsto \frac{y(t^2 - 500t - 15625)}{t^3}.$$

3. Modular Methods at 2

Following [PSS07, 4.6] we define for a primitive triple (a, b, c) the elliptic curve

$$E = E_{(a,b,c)} : Y^2 = X^3 + 3bX - 2a.$$

Remark 3.1. The elliptic curve E has j-invariant $12^3b^3/c^{10} = -12^3a^2/c^{10} + 12^3$; thus $j(E) - 12^3 = -12^3a^2/c^{10}$, which is -3 times a square.

Setting $E_0 := E_{(3,-2,1)}$, this remark proves the following.

Lemma 3.2. *To $(a, b, c) \in S(\mathbb{Z})$ one may associate a point on $X_{\Delta_{E_0}}(\mathbb{Q})$.*

In the following lemmas, we calculate $E_{(a,b,c)}[2]$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. The conclusion will be that the set of such possibilities is finite and explicitly computable. In fact, one can realize each possible Galois module as $E'[2]$ for E' an elliptic curve, with finitely many explicit possibilities for E'. One may thus associate to $E_{(a,b,c)}$ a point on one of the modular curves $X_{E'}(2)$ and then combine this with level lowering at the prime 5 to get a point on a twist of the genus 13 curve $X(10)$. Another idea is to use the explicit equations for the curve $X_{E'}(2)$ given in [RS01] to derive local information about the triple (a, b, c).

The idea is that knowledge of $E_{(a,b,c)}[2]$ is equivalent to knowledge of the splitting field L of the polynomial $f = X^3 + 3bX - 2a$, and we will find that L is unramified outside of $\{2, 3\}$. By Hermite's theorem, there are only finitely many fields of degree at most 3 and unramified outside of $\{2, 3, \infty\}$, and with the aid of a computer one can easily enumerate them and recognize each as the field of definition of the 2-torsion of an elliptic curve E' with good reduction outside of $\{2, 3\}$, effectively 'lowering the level' of $E_{(a,b,c)}$ at the prime 2 (an otherwise difficult task given that the usual level lowering theorems don't apply – the mod 2 representation is often ramified at 2). The details come in the next two lemmas.

Lemma 3.3 ('Level lowering' at 2)**.** *Let $(a, b, c) \in S(\mathbb{Z})$ be a primitive triple and suppose that $a \neq 0$. Then $f(x) = x^3 + 3bx - 2a$ is irrreducible.*

Proof. Let $K = \mathbb{Q}(E_{(a,b,c)}[2])$ be the splitting field of f. The discriminant of $E_{(a,b,c)}$ is -12^3c^{10}. By the standard Tate uniformization argument (that after base change to the maximal unramified extension $\mathbb{Q}_p^{\mathrm{un}}$ of $\mathbb{Q}_p$ there exists an analytic Galois equivariant isomorphism of $E_{(a,b,c)} \otimes \mathbb{Q}_p^{\mathrm{un}}$ with a Tate curve $\mathbb{G}_m/q^{\mathbb{Z}}$), $E_{(a,b,c)}[2]$ (and thus K) is unramified at a prime

$p > 3$ of multiplicative reduction if $2|v_p(\Delta_{E_{(a,b,c)}})$ (see [Ell01, Corollary 1.2] for a more detailed proof of this fact). Since $v_p(\Delta_{E_{(a,b,c)}}) = v_p(c^{10})$ for $p > 3$, we conclude that K is unramified outside of $\{2, 3\}$. Since f is reducible then K has degree 1 or 2. There are only finitely many such fields of degree ≤ 2, given by polynomials $x^2 + D$ with $D \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Let E_D be the elliptic curve given by $y^2 = x(x^2 + D)$. Then there exists a D as above and a point $P \in X_{E_D}(2)(\mathbb{Q})$ representing $E_{(a,b,c)}$ up to quadratic twist. Explicit equations paramaterizing such curves are given in [RS01]: there exist $u, v \in \mathbb{Q}$ such that $E_{(a,b,c)}$ is isomorphic to the curve $E_{u,v}\colon y^2 = x^3 + 3D(3v^2 - Du^2)x - 2(9D^2uv^2 - D^3u^3)$. The given model has discriminant $\Delta(E_{u,v}) = -2^6 3^6 D(v(v^2 + Du^2)D)^2$. As this may only change by a 12^{th} power, one concludes that for $D \neq 3$, $j(E_{u,v}) - 12^3 = c_6(E_{u,v})^2/\Delta(E_{u,v})$ is not -3 times a square and thus (by remark 3.1) cannot be isomorphic to $E_{(a,b,c)}$.

When $D = 3$, further analysis of the equation $j(E_{u,v}) = j(E_{(a,b,c)}) = 12^3 b^3/c^{10}$ produces rational points on one of the genus 2 curves given by $y^2 = x^5 - 3^5$ and $y^2 = x^5 - 3^7$; an application of Chabauty's method (recorded in the transcript of computations at [Bro]) determines the finite set of such points, and the only one corresponding to a primitive triple has $a = 0$. □

Lemma 3.4. *Let $(a, b, c) \in S(\mathbb{Z})$ be a primitive triple. Suppose that $f(x) = x^3 + 3bx - 2a$ is irreducible. Then $\mathbb{Q}(E_{(a,b,c)}[2]) \cong \mathbb{Q}(E_{(3,-2,1)}[2])$.*

Proof. The proof is the same as lemma 3.3, except that here the computer algebra package Sage (which implements the Jones database of number fields [Jon]) is used to enumerate all degree 3 number fields unramified outside of $\{2, 3, \infty\}$; a transcript of computations verifying this can be found at [Bro].

□

Remark 3.5. Lemmas 3.3 and 3.4 will be used in section 6 to give local information about possible values of $j(E_{(a,b,c)}) = 12^3 b^3/c^{10}$.

Remark 3.6. The mod 3 Galois representations arising from solutions to the equation $x^2 + y^3 = z^{15}$ are similarly ramified at the prime 3, so that Ribet's level lowering theorem again does not apply. Nonetheless, the techniques of the 'level lowering' lemmas 3.3 and 3.4 can be pushed (with more work and knowledge of the subfield structure of $\mathbb{Q}(E[3])$) to classify all mod 3 representations arising from this equation. It remains to be seen if the local information one obtains is actually useful in solvng this Fermat equation.

4. Modular Methods at 5

Let $(a, b, c) \in S(\mathbb{Z})$, let $E = E_{(a,b,c)}$, and recall that we defined E_0 to be $E_{(3,-2,1)}$. Following [PSS07, Section 6], we classify the possibilities for the Galois module $E[5]$.

Lemma 4.1. *$E[5]$ is irreducible as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module.*

Proof. If $E[5]$ is reducible then there exists a 5-isogeny defined over $\mathbb{Q}$. One can thus associate to E a point on $X_0(5)(\mathbb{Q})$. Together with lemma 3.2, this implies that E corresponds

to a point on $X_{E_0}(\mathbb{Q})$, which a Magma calculation reveals has rank 0. There are six torsion points and they have image $\{-102400/3, 20480/243, \infty\}$ in $X(1)$. For $(a,b,c) \in S(\mathbb{Z})$, $v_5(j(E_{(a,b,c)})) = v_5(12^3b^3/c^{10})$ is divisible by at least one of 3 or 10. On the other hand, for $j = -102400/3$ or $20480/243$ one has $v_5(j) \in \{1,2\}$. We conclude that these do not correspond to j-invariants of elliptic curves coming from $(a,b,c) \in S(\mathbb{Z})$. □

Let $\mathcal{E}$ be the following set of 13 elliptic curves over $\mathbb{Q}$ in the notation of [Cre97]:

24A1, 27A1, 32A1, 36A1, 54A1, 96A1, 108A1, 216A1, 216B1, 288A1, 864A1, 864B1, 864C1.

Lemma 4.2. *There exists an $E'' \in \mathcal{E}$ and a quadratic twist E' of E such that $E'[5] \cong E''[5]$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.*

Proof. This is identical to [PSS07, Lemma 6.1], with the remark that since 13 is not a square mod 5 one can again exclude the 14^{th} newform. □

Definition 4.3. For an elliptic curve E with j-invariant j, define K_E to be the number field $\mathbb{Q}(\alpha)$, with α a root of the polynomial

$$f(t) = (t^2 + 250t + 3125)^3 - jt^5.$$

As the field K_E only depends on $j(E)$, we will sometimes denote it by K_j.

By the explicit equations of 2.1, an elliptic curve E' has a 5-isogeny over $K_{E'}$ and gives rise to a point on $X_0(K_{E'})$. Moreover, by lemma 4.2, for E corresponding to a primitive triple $(a,b,c) \in S(\mathbb{Z})$ there exists an $E' \in \mathscr{E}$ such that $K_E = K_{E'}$ (since $E[5] \cong E'[5]$, E has a 5-isogeny over a field L if and only if E' does). Thus, E corresponds to a point in $X_0(5)(K_{E'})$. Combining this with lemma 3.2, we arrive at the key observation.

Lemma 4.4. *For $(a,b,c) \in S(\mathbb{Z})$, there exists an $E' \in \mathscr{E}$ such that $E_{(a,b,c)}$ corresponds to a point P_E in $X_{E_0}(K_{E'})$ whose image in $X_{\Delta_{E_0}}(K_{E'})$ in fact lands in $X_{\Delta_{E_0}}(\mathbb{Q})$.*

The image of P_E in $X(1)$ (i.e. $j(E)$) is rational too. As the field K_E depends only on the j-invariant of E, we note that the set of j-invariants of curves in $\mathcal{E}$ is

$$\{35152/9, 0, 1728, 9261/8, 21952/9, -3072, -6, -216, -13824, 1536\}.$$

5. Elliptic Chabauty

We now study the situation of lemma 4.4.

Proposition 5.1. *Let $j \in \{0, 1728, -13824\}$. Then*

$$j(X_{E_0}(K_j)) \cap X(1)(\mathbb{Q}) \in \{0, 1728, -13824, -102400/3, 20480/243, \infty\}.$$

The proof requires consideration of the following problem. Given an elliptic curve E over $\mathbb{Q}$, a map $E \xrightarrow{\pi} \mathbb{P}^1$ defined over $\mathbb{Q}$, and a number field K of degree $d > 1$ over $\mathbb{Q}$, one would like to determine the subset of $E(K)$ mapping to $\mathbb{P}^1(\mathbb{Q})$ under π. Let r be the rank of $E(K)$. Suppose further that $r < d$; then under this hypothesis a partial solution to this problem has been worked out in [Bru03], using a method analogous to Chabauty's method (see [PM07]

for a survey) in that one expands the map p-adic analytically locally (i.e. in terms of p-adic power series) and uses Newton polygons to analyze the solutions. This method has been completely implemented in Magma; see [Bru03] for a succinct description of the method and instructions for use of its Magma implementation.

To use this we need to understand the output of the Magma function

`Chabauty(MWmap, Ecov, p).`

The first argument `MWmap` is a map from an abstract abelian group into the Mordell-Weil group of E over K; we denote by A its domain and G its image. The second argument `Ecov` is a map from E to $\mathbb{P}^1$ which is defined over $\mathbb{Q}$. The third argument `p` is a prime of good reduction for E for which the map `Ecov` is also of good reduction. The function returns values N, V, R and L as follows (quoting the Magma documentation):

- N is an upper bound for the number of points $P \in G$ such that $\texttt{Ecov}(P) \in \mathbb{P}^1(\mathbb{Q})$.
- V is a set of elements of A that have images in $\mathbb{P}^1(\mathbb{Q})$.
- R is a number such that, if $[E(K) : G]$ is finite and prime to R then N is also a bound for the number of points $P \in E(K)$ with image in $\mathbb{P}^1(\mathbb{Q})$.
- L is extra information which we will not use.

An important point is that one does not need to know the entire Mordell-Weil group $E(K)$, only a subgroup G with index prime to R. In the following proof of proposition 5.1 we will not be able to compute all of $E(K)$.

Proof of proposition 5.1. Magma code verifying the following can be found at [Bro]. Below, for $P \in X_{E_0}$ a cusp (so that it represents a degenerate elliptic curve) we write $j(P) = \infty$.

Let $j = -13824$. The elliptic curve E_0 given by $y^2 = x^3 - 6x - 6$ corresponds to the primitive triple $(3, -2, 1) \in S(\mathbb{Z})$. It has j-invariant -13824 and Cremona label 1728r1. It is a quadratic twist of the elliptic curve $E \in \mathcal{E}$ with Cremona label 864b1, given by the equation $y^2 = x^3 - 24x - 48$. This is the most important case to consider in that there is actually a point on $X_{E_0}(K_E)$ corresponding to a triple $(a, b, c) \in S(\mathbb{Z})$.

A Magma computation reveals that $X_{E_0}(K_E)$ has rank 1. One can construct explicitly the point $P \in X_{E_0}(K_E)$ corresponding to a 5-isogeny of E over K_E. The `Chabauty` routine returns $N = 8$, $\#V = 8$, and $R = 40$. The images under `MWmap` of V are the known torsion points of lemma 4.1 and $\pm P$. Using Magma, one can check that the subgroup generated by P and the torsion is 2 and 5 saturated, so that the index $[X_{E_0}(K_E) : G]$ is prime to R; the brute force point search necessary to check that G generates the Mordell-Weil group is infeasible. The j-invariants of the (possibly degenerate) elliptic curves corresponding to these 8 points are $\{-13824, -102400/3, 20480/243, \infty\}$.

Let $j = 0$. A Magma computation reveals that $X_{E_0}(K_j)$ has rank 1. Let $E \in \mathcal{E}$ with $j(E) = 0$ (there are two such curves). One can construct explicitly the point $P \in X_{E_0}(K_j)$ corresponding to a 5-isogeny of E over K_j. The `Chabauty` routine returns $N = 10$, $\#V = 10$ and $R = 2$. Using Magma, one can check that the subgroup generated by P and the torsion

points is 2 saturated. The j-invariants of the (possibly degenerate) elliptic curves corresponding to the images in $X_{E_0}(K_j)$ under `MWmap` of V are $\{0, -102400/3, 20480/243, \infty\}$.

Let $j = 1728$. A Magma computation reveals that $X_{E_0}(K_j)$ has rank 0. The torsion subgroup has size 12, of which 4 points represent elliptic curves with j-invariant which is not a rational number. The j-invariants of the (possibly degenerate) curves they represent are $\{1728, -102400/3, 20480/243, \infty\}$.

□

Remark 5.2. We conclude that if $(a, b, c) \in S(\mathbb{Z})$ is a primitive triple such that $E_{(a,b,c)}[5] \cong E[5]$ for an elliptic curve E such that $j(E) \in \{0, 1728, -13824\}$, then (a, b, c) is one of the triples of theorem 1.1.

Remark 5.3. For other values of j one can compute that the rank of $X_{E_0}(K_j)$ is at most 3, but a brute force point search is too slow to explicitly determine a finite index subgroup.

6. Local Methods

Here we use local methods inspired by [PSS07, 7.4] to exclude the existence of any further primitive triples.

Proposition 6.1. *Let $E \in \mathcal{E}$ and suppose $j(E) \notin \{0, 1728, -13824\}$. Let E' be an elliptic curve such that $E[5] \cong E'[5]$. Then $j(E') \neq j(E_{(a,b,c)})$ for any primitive triple $(a, b, c) \in S(\mathbb{Z})$.*

Proof. MAGMA code verifying this (as described below) is available at [Bro]. □

Remark 6.2. Note that this completes the proof of theorem 1.1.

The idea is the following. For any morphism $X \xrightarrow{f} Y$ of varieties defined over $\mathbb{Q}$ and any prime p, one can (in principle) algorithmically determine the image $f(X(\mathbb{Q}_p))$ of the p-adic points. The existence of such an algorithm follows from an effective elimination of quantifiers; see [Mac76]. We explain how to do this for a map $\mathbb{P}^1 \to \mathbb{P}^1$ below. By lemma 4.2 and remark 2.1, $E_{(a,b,c)}$ gives rise to a point on either $X_E(5)$ or $X_E^-(5)$; the idea is then to apply this to the two maps $X_E(5) \to X(1)$ (resp. $X_E^-(5) \to X(1)$) and $S \to X(1)$. Explicit equations for the map $X_E(5) \to X(1)$ (resp. $X_E^-(5) \to X(1)$) are given in [RS95] (resp. the appendix), and the map $S \to X(1)$ sends a primitive triple to the j-invariant $j(E_{(a,b,c)}) = 12^3 b^3/c^{10}$. For each $E \in \mathcal{E}$ with $j(E) \notin \{0, 1728, -13824\}$, we will find a prime p such that the p-adic images of these two maps do not intersect; here we of course restrict the domain of S to primitive triples. Using the lemmas of section 3, one can also compare this to the local information coming from the maps $X_E(2) \to X(1)$.

Now we make this idea precise. Let $\mathbb{P}^1 \xrightarrow{\phi} \mathbb{P}^1$ be given by the pair of homogenous polynomials $f_1(s, t), f_2(s, t) \in \mathbb{Z}[s, t]$ and let p be a prime number. We partition the set $\mathbb{P}^1(\mathbb{Q}_p)$ into the two residue classes $R_1 = [\mathbb{Z}_p : 1]$ and $R_2 = [1 : p\mathbb{Z}_p]$ and instead study the single variable polynomials $f_i(R_j) \in \mathbb{Q}_p[x]$ (where now x will range over $\mathbb{Z}_p$). Let $f_i(R_j) = c_{ij} \cdot \prod_k (x - \alpha_{i,j,k})$. Using Newton polygons one can explicitly determine $\alpha_{i,j,k}$ to any desired precision, and from this is it straightforward to determine all values of $f_i(R_j)$ for $x \in \mathbb{Z}_p$.

Example 6.3. As a very simple example, suppose $X_E(5) \xrightarrow{\phi} X(1)$ is given by $[f_1, f_2]$ and suppose that $v_p(\alpha_{i,1,k}) = 4/3$ for each i, k. Then for $x \in \mathbb{Z}_p$, $v_p(x-\alpha_{i,1,k}) = \min\{v_p(x), 4/3\} \in \{0, 1, 4/3\}$. Thus, on the residue class $[\mathbb{Z}_p : 1]$, one has $v_p(f_i(x,1)) = v_p(c_{i,1}) \cdot \deg f_i \cdot \min\{v_p(x), 4/3\}$; setting $a_i = v_p(c_{i,1})$ we conclude that $\phi([\mathbb{Z}_p : 1]) \subset [p^{a_1}\mathbb{Z}_p^* : p^{a_2}\mathbb{Z}_p^*]$. Suppose now that $p = 3$ and $a_1 = a_2$. Since $\gcd(b, c) = 1$, $v_3(j(E_{(a,b,c)})) = v_3(12^3b^3/c^{10}) \neq 0$. We conclude that $v_3(j(E')) \neq v_3(j(E_{(a,b,c)}))$ for any $E' \in R_1 \subset X_E(5)(\mathbb{Q}_3)$ and $(a, b, c) \in S(\mathbb{Z}_p)$.

We have written MAGMA code (available at [Bro]) which takes as input an elliptic curve E and a prime p and returns, for each residue class R_i, a factorization $j = n \cdot \prod(x-\alpha_j)/\prod(x-\beta_j)$, where j is the affine part (i.e. the quotient f_1/f_2) of the map $X_E(5) \to X(1)$ restricted to the residue class R_i. There is an optional parameter 'anti'; when this is set to 'true' the routine instead returns this data for the map $X_E^-(5) \to X(1)$. Using this, we ran the local test described above for each $E \in \mathcal{E}$ with $j(E) \notin \{0, 1728, -13824\}$ and in each case found primes $p, p' \in \{2, 3, 5\}$ for which $X_E(5)$ (resp. $X_E^-(5)$) fails the local test at p (resp. p').

Appendix: Computing explicit equations for $X_E^-(5) \to X(1)$

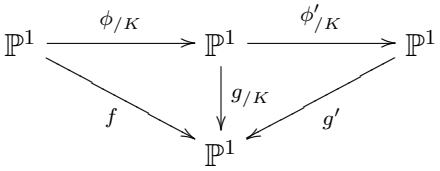
Here we explain how, for an elliptic curve E, one can deduce explicit equations for the map $X_E^-(5) \to X(1)$ given knowledge of equations for $X_{E'}(5)_{\overline{\mathbb{Q}}} \to X(1)_{\overline{\mathbb{Q}}}$, where E' is 2-isogenous to E over $\overline{\mathbb{Q}}$.

First we consider an abstract version of the problem: given a number field K and a morphism $g\colon P^1_{\overline{\mathbb{Q}}} \to P^1_{\overline{\mathbb{Q}}}$ such that there exists an automorphism ϕ of $P^1_{\overline{\mathbb{Q}}}$ such that $g \circ \phi$ is the base extension of a morphism $f\colon P^1_{\mathbb{Q}} \to P^1_{\mathbb{Q}}$, find such morphisms ϕ and f.

Lemma A.1. *Let $\mathbb{P}^1_{\overline{\mathbb{Q}}} \xrightarrow{\phi} \mathbb{P}^1_{\overline{\mathbb{Q}}}$ be an automorphism and suppose there exist distinct $Q_1, Q_2, Q_3 \in \mathbb{P}^1(\overline{\mathbb{Q}})$ such that for every i and for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\phi(Q_i^\sigma) = (\phi(Q_i))^\sigma$. Then ϕ is defined over $\mathbb{Q}$.*

Proof. Representing ϕ as a Möbius transformation $\frac{a_1 z + a_2}{a_3 z + a_4}$, one can, after scaling by a non-zero a_i, solve for the coefficients a_i in terms of coordinates of the points Q_j and $\phi(Q_j)$. It is then easy to see that $a_i^\sigma = a_i$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and thus $a_i \in \mathbb{Q}$. □

One can solve the abstract problem in the following situation: let $Q_1, Q_2, Q_3 \in \mathbb{P}^1(\overline{\mathbb{Q}})$ be 3 distinct points and suppose there exists an automorphism $\phi'\colon \mathbb{P}^1_K \to \mathbb{P}^1_K$ such that $\phi' \circ \phi$ and each Q_i satisfy the hypothesis of lemma A.1. Then $\phi' \circ \phi$ is defined over $\mathbb{Q}$. Setting $g' = g \circ (\phi')^{-1}$, we get a commutative diagram



Since one has $f = g' \circ \phi' \circ \phi$, we conclude that g' is defined over $\mathbb{Q}$ and differs from f by the $\mathbb{Q}$-automorphism $\phi^{-1} \circ (\phi')^{-1}$.

Now suppose E is given by the equation $y^2 = f(x)$. Let $K = \mathbb{Q}(E[2])$ be the splitting field of $f(x)$. Then the 2-torsion points of E are defined over K. Let $\{O, P_1, P_2, P_3\}$ be the 2-torsion points of E and define E_i to be $E/\langle P_i \rangle$, with $E \xrightarrow{\psi_i} E_i$ the quotient map and $\hat{\psi}_i$ the dual isogeny.

As in [PSS07, 4.4] the isogeny $E \xrightarrow{\psi_1} E_1$ changes the Weil pairing by 2 (since for a 2-isogeny ψ, $\langle \psi(P), \psi(Q) \rangle = \langle \hat{\psi} \circ \psi(P), Q \rangle = \langle 2P, Q \rangle = \langle P, Q \rangle^2$, where the first equality is [Sil09, III.8.2]). In particular, if E' is an elliptic curve and $E'[5] \cong E[5]$ is an anti-symplectic isomorphism (so that the map induced by the Weil pairing is $\zeta \mapsto \zeta^2$) then the composition $E'[5] \cong E[5] \xrightarrow{\psi_1} E_1[5]$ (where ψ_1 is the restriction to $E[5]$ of ψ_1) is symplectic. This induces an isomorphism $\phi\colon X_E^-(5)_K \cong X_{E_1}(5)_K$ over $X(1)_K$, which is the situation of the above discussion.

To apply this, let $Q_i \in X_E^-(5)(K)$ be three points induced by the isogenies ψ_i. By computing $j(E_i)$, it is easy to compute explicit points on $X_{E_1}(5)(K)$ which represent $\phi(Q_i)$. Let $\{r_1, r_2, r_3\}$ be the roots of $f(x)$. Since r_i is the x-coordinate of the 2-torsion point $P_i \in E(K)$, the Galois action on the ordered set $\{r_1, r_2, r_3\}$ agrees with the action on $\{E_1, E_2, E_3\}$, and thus also on $\{Q_1, Q_2, Q_3\}$. Our hypothesis is that we have an explicit identification of $X_{E_1}(5)$ with $\mathbb{P}^1$. Thus, if we define $\phi'\colon \mathbb{P}^1 \to \mathbb{P}^1$ to be the map sending $\phi(Q_i)$ to $[r_1 : 1] \in \mathbb{P}^1(K)$, then the hypothesis of lemma A.1 is satisfied for the composition $\phi' \circ \phi$.

One can explicilty compute E_i, $j(E_j)$, $\phi(Q_i) \in X_{E_1}(K)$, and the map ϕ'; equations for the map $j_{E_1}\colon X_{E_1}(5) \to X(1)$ are computed in [RS95]. The composition $j_{E_1} \circ (\phi')^{-1}$ is thus an explicitly computable model for the map $X_E^-(5) \to X(1)$. Magma code doing all of this explicitly is available at [Bro].

Remark A.2. Now let E be given by the equation $y^2 = x^3 + ax + b$. In [RS95] the equations for the map $X_E(5) \to X(1)$ are given as a function of the coefficients a and b of E. It it clear that the technique of this appendix can be refined to do the same for the map $X_E^-(5) \to X(1)$, since all of the numbers constructed (e.g. the j-invariants of the 2-isogenous curves E_i) depend algebraically on a and b. However writing out the resulting equations would double the length of this paper and is thus omitted.

References

[Bru03] Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. MR **2011330 (2004j:**11051) ↑

[Bru00] ———, *On powers as sums of two cubes*, Algorithmic number theory (Leiden, 2000), 2000, pp. 169–184. ↑

[Beu98] Frits Beukers, *The Diophantine equation* $Ax^p + By^q = Cz^r$, Duke Math. J. **91** (1998), no. 1, 61–88.MR1487980 (99f:11039) ↑

[Bro] David Brown, Electronic transcript of computations. Available at `http://www.math.berkeley.edu/~brownda/math/papers/235n/235nComputations.html`. ↑

[Buz00] Kevin Buzzard, *On level-lowering for mod 2 representations*, Math. Res. Lett. **7** (2000), no. 1, 95–110. MR **1748291 (2001a:**11080) ↑

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR **1628193 (99e:**11068) ↑

[Edw04] J. Edwards, *A complete solution to* $X^2 + Y^3 + Z^5$, J.reine angew **571** (2004), 213–236. ↑

[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.MR1348707 (96e:11042) ↑

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR **1357209 (97g:**11044) ↑

[Magma] 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. Computational algebra and number theory (London, 1993). Magma is available at `http://magma.maths.usyd.edu.au/magma/` .MR1484478 ↑1

[MP07] William McCallum and Bjorn Poonen, *On the Method of Chabauty and Coleman* (2007), available at `"http://math.berkeley.edu/~poonen/papers/chabauty.pdf"`. ↑
]

[McM04] Ken McMurdy, *Explicit parametrizations of ordinary and supersingular regions of* $X_0(p^n)$, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 165–179. MR **2058650 (2005e:**11074) ↑

[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. MR 2309145 ↑1, 1, 2, 2.1, 3, 4, 4, 6, 6
@article MR1694877, AUTHOR = Rubin, K. and Silverberg, A., TITLE = Mod 2 representations of elliptic curves, JOURNAL = Proc. Amer. Math. Soc., FJOURNAL = Proceedings of the American Mathematical Society, VOLUME = 129, YEAR = 2001, NUMBER = 1, PAGES = 53–57, ISSN = 0002-9939, CODEN = PAMYAR, MRCLASS = 11G05 (11F80), RNUMBER = MR1694877 (2001c:11064), MRREVIEWER = Matthew H. Baker,

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: `brownda@math.berkeley.edu`