TWISTS OF $X(7)$ AND PRIMITIVE SOLUTIONS TO $x^2 + y^3 = z^7$

BJORN POONEN, EDWARD F. SCHAEFER, AND MICHAEL STOLL

ABSTRACT. We find the primitive integer solutions to $x^2 + y^3 = z^7$. A nonabelian descent argument involving the simple group of order 168 reduces the problem to the determination of the set of rational points on a finite set of twists of the Klein quartic curve X. To restrict the set of relevant twists, we exploit the isomorphism between X and the modular curve $X(7)$, and use modularity of elliptic curves and level lowering. This leaves 10 genus-3 curves, whose rational points are found by a combination of methods.

1. INTRODUCTION

1.1. **Main result.** Fix integers $p, q, r \geq 1$. An integer solution (x, y, z) to $x^p + y^q = z^r$ is called *primitive* if $\gcd(x, y, z) = 1$. The main goal of this paper is to prove:

Theorem 1.1. *The primitive integer solutions to $x^2 + y^3 = z^7$ are the 16 triples*

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1), \quad (\pm 71, -17, 2),$$
$$(\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \quad (\pm 21063928, -76271, 17)\,.$$

1.2. **Previous work on generalized Fermat equations.** We temporarily return to the discussion of $x^p + y^q = z^r$ for a fixed general triple (p, q, r).

Let $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1$. There is a naïve heuristic that for each triple of integers (x, y, z) with $|x| \leq B^{1/p}$, $|y| \leq B^{1/q}$, $|z| \leq B^{1/r}$, the probability that $x^p + y^q = z^r$ is $1/B$: this leads to the guesses that the set of primitive integer solutions is finite when $\chi < 0$ and infinite when $\chi > 0$. In fact, these statements are theorems, proved by Darmon and Granville [DG95] and Beukers [Beu98], respectively.[1]

The method of *descent*, in one form or another, is the key ingredient used in the proofs of these theorems. Descent relates the primitive integer solutions to the rational points (possibly over some number field) on one or more auxiliary curves, whose Euler characteristic $2 - 2g$ is a positive integer multiple of χ. This connection is made clear in [Dar97], for example. In Section 3, we will explain it in detail in the context of the special case $(p, q, r) = (2, 3, 7)$.

Suppose $\chi > 0$. Then $2 - 2g > 0$, so $g = 0$. Thus the auxiliary curves that have rational points are isomorphic to $\mathbb{P}^1$. The conclusion is that the primitive integer solutions fall into a

Date: July 16, 2006.

2000 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G10, 11G18, 11G30, 14G05.

Key words and phrases. generalized Fermat equation, Jacobian, Mordell-Weil sieve, Chabauty, modular curve, Klein quartic, descent.

This article has appeared in *Duke Math. J.* **137** (2007), no. 1, 103–158.

[1] In fact, they prove results more generally for equations $Ax^p + By^q = Cz^r$ where A, B, C are nonzero integer constants.

finite number of parametrized families. These parametrizations have been found explicitly for every (p, q, r) with $\chi > 0$, as we now indicate. The case where some exponent is 1 is trivial, and the case where the multiset $\{p, q, r\}$ equals $\{2, 2, n\}$ for some $n \geq 2$ is elementary. The only remaining possibilities are $\{2, 3, 3\}$, $\{2, 3, 4\}$, $\{2, 3, 5\}$; these were completed by Mordell, Zagier, and Edwards, respectively. See [Edw04] for details.

If $\chi = 0$, then $2 - 2g = 0$, so $g = 1$. There are only the cases $\{2, 3, 6\}$, $\{2, 4, 4\}$, $\{3, 3, 3\}$, and the auxiliary curves turn out to be elliptic curves E over $\mathbb{Q}$, and descent proves that $E(\mathbb{Q})$ is finite in each case. (The finiteness should not be surprising, since these elliptic curves have very low conductor.) One then easily finds that the only nontrivial primitive solution, up to permutations and sign changes, is $1^6 + 2^3 = 3^2$. Many, if not all, of these cases are classical: Fermat invented the method of descent to handle $(4, 4, 2)$, and Euler[2]resolved $(3, 3, 3)$. If $\chi < 0$, then $g > 1$. Each auxiliary curve has finitely many rational points, by [Fal83], and hence we obtain the Darmon-Granville result that for each (p, q, r) there are at most finitely many nontrivial primitive solutions. For many (p, q, r) these solutions have been determined explicitly. These are summarized in Table 1.

1.3. **Why $x^2 + y^3 = z^7$ is particularly difficult.** We give several reasons to explain why the $(2, 3, 7)$ equation presents a particular challenge.

1.3.1. *It corresponds to the negative value of χ closest to 0.* When (p, q, r) is such that χ is negative but close to 0, the naïve heuristic mentioned earlier predicts that the set of primitive integer solutions should be relatively large and that some solutions should involve large integers. The existence of solutions, especially large solutions, naturally tends to make proving the nonexistence of others a difficult task.

From this point of view, the triple $\{p, q, r\}$ with $\chi < 0$ that should be most difficult is the one with χ closest to 0: this is $\{2, 3, 7\}$. Indeed the equation $x^2 + y^3 = z^7$ has several solutions, and some of them involve large integers. Now that this equation is solved, we know the complete list of solutions for every (p, q, r) for which $\chi < 0$ and for which nontrivial primitive solutions (excluding $1^n + 2^3 = 3^2$) are known to exist.

1.3.2. *The exponents are prime.* The triple $\{2, 3, 8\}$ analyzed by Bruin has a value of χ almost as close to 0 as $(2, 3, 7)$ does, and also has large solutions, so it also is difficult. But at least it could be studied by using Zagier's parametrizations for the case $\{2, 3, 4\}$ (with $\chi > 0$).

1.3.3. *The exponents are pairwise relatively prime.* For descent, one requires finite étale covers, and (geometrically) abelian étale covers can be easily constructed in cases where two of the exponents share a common factor. In contrast, for $\{2, 3, 7\}$, the smallest nontrivial Galois étale covering has a nonabelian Galois group of size 168. Before the present work, no pairwise coprime (p, q, r) with $\chi < 0$ had been studied successfully.

[2]Euler's argument had a small flaw, but it was later fixed by others.

$\{2,3,7\}$	See Theorem 1.1.
$\{2,3,8\}$	[Bru99, Bru03]: $1549034^2 + 33^8 = 15613^3$, $96222^3 + 43^8 = 30042907^2$
$\{2,3,9\}$	[Bru04]: $13^2 + 7^3 = 2^9$
$(2,2\ell,3)$	[Che04], for prime $7 < \ell < 1000$ with $\ell \neq 31$
$\{2,4,5\}$	[Bru03]: $7^2 + 2^5 = 3^4$, $11^4 + 3^5 = 122^2$
$\{2,4,6\}$	[Bru99]
$(2,4,7)$	[Ghi02]
$(2,4,\ell)$	[Ell04], for prime $\ell \geq 211$
$(2,n,4)$	follows easily from [BS04];
	$(4,n,4)$ was done earlier in [Dar93]
$\{2,n,n\}$	[DM97]; others for small n
$\{3,3,4\}$	[Bru00]
$\{3,3,5\}$	[Bru00]
$\{3,3,\ell\}$	[Kra98], for prime $17 \leq \ell \leq 10000$
$\{3,n,n\}$	[DM97]; others for small n
$\{2n,2n,5\}$	[Ben04]
$\{n,n,n\}$	[Wil95, TW95], building on work of many others

TABLE 1. We list exponent triples (p,q,r) such that $\chi < 0$ and the primitive integer solutions to $x^p + y^q = z^r$ have been determined. The notation $\{p,q,r\}$ means that the solutions have been determined for every permutation of (p,q,r): this makes a difference only if at least two of p,q,r are even. For each (p,q,r) listed, all solutions up to sign changes and permutations are given, except that solutions of the form $1^n + 2^3 = 3^2$ are omitted. Heuristics suggest that probably there are no more solutions for (p,q,r) with $\chi < 0$: in fact a cash prize awaits anyone who finds a new solution [Dar97].

1.4. **Historical remarks.** The equation $x^2 + y^3 = z^7$ seems to have appeared first (with coefficients) in the paper [Kle1879]. There it arose as the relation between certain covariants of the Klein quartic form $x^3y + y^3z + z^3x$. For interesting connections to the Schwarz triangle group $\Sigma(2,3,7)$ and to the resolution of surface singularities, see [Bri81].

2. NOTATION

If k is a field, then $\overline{k}$ denotes an algebraic closure, and $\mathcal{G}_k = \mathrm{Gal}(\overline{k}/k)$. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let $\zeta = e^{2\pi i/7} \in \overline{\mathbb{Q}}$.

If X is a scheme over a ring R, and R' is an R-algebra, then $X_{R'}$ denotes $X \underset{\operatorname{Spec} R}{\times} \operatorname{Spec} R'$. If X is a variety over $\mathbb{Q}$, and R is a localization of $\mathbb{Z}$, then X_R will denote a smooth model of X over R (assuming it exists), and $X(R)$ means $X_R(R)$. Conversely, if X_R is a scheme over such a ring R, then X will denote the generic fiber, a scheme over $\mathbb{Q}$.

We say that a k-variety Y is a *twist* of a k-variety X if $Y_{\overline{k}} \simeq X_{\overline{k}}$. Twists of morphisms are defined similarly.

If M is a $\mathcal{G}_{\mathbb{Q}}$-module, and k is an extension of $\mathbb{Q}$, then M_k denotes the same group with the action of $\mathcal{G}_k$ via the restriction map $\mathcal{G}_k \to \mathcal{G}_{\mathbb{Q}}$. In particular, $M_{\overline{\mathbb{Q}}}$ denotes the abelian group with no Galois action.

3. The theory behind the initial descent

This section explains the theory that reduces the original problem to the problem of determining the rational points on a finite list of auxiliary curves, which turn out to have genus 3.

The argument is essentially the same as that in [DG95] (see also [Dar97]), though we do have one small theoretical innovation: By sticking with punctured affine surfaces instead of Darmon's "M-curves" (which are essentially the stack quotients of the surfaces by a $\mathbb{G}_m$-action), we can use the standard theory of descent for finite étale covers of varieties à la Chevalley-Weil and avoid having to use or develop more general statements for ramified coverings or for stacks. Keeping the stacks in the back of one's mind, however, still simplifies the task of *finding* the étale covers of the punctured surfaces; we will use them for this purpose.

Another difference in our presentation is that we word the argument so as to obtain a finite list of curves over $\mathbb{Q}$ instead of a single curve over a larger number field; this is important for the practical computations.

Equations for the varieties and morphisms of this section will appear in later sections of our paper.

3.1. **Scheme-theoretic interpretation of the problem.** Start with the subscheme $x^2 + y^3 = z^7$ in $\mathbb{A}^3_{\mathbb{Z}}$ and let $S_{\mathbb{Z}}$ be the (quasi-affine) scheme obtained by deleting the subscheme $x = y = z = 0$. Then $S(\mathbb{Z})$ is the set of primitive integer solutions to $x^2 + y^3 = z^7$.

3.2. **An étale cover of $S_{\mathbb{C}}$.** In order to apply the method of descent, we need a finite étale cover of $S_{\mathbb{Z}}$, or at least of $S_{\mathbb{Z}[1/N]}$ for some $N \geq 1$. We first find a finite étale cover of $S_{\mathbb{C}}$.

The multiplicative group $\mathbb{G}_m$ acts on $S_{\mathbb{C}}$: namely, λ acts by $(x, y, z) \mapsto (\lambda^{21}x, \lambda^{14}y, \lambda^6 z)$. The subfield of the function field $\mathbb{C}(S_{\mathbb{C}})$ invariant under $\mathbb{G}_m$ is $\mathbb{C}(j)$ where $j := 1728\, y^3/z^7$, so the quotient of $S_{\mathbb{C}}$ by $\mathbb{G}_m$ should be birational to $\mathbb{P}^1$ with coordinate j. (The reason for the factor 1728 and for the name j will become clear later on.) But $\mathbb{G}_m$ does not act freely on $S_{\mathbb{C}}$: the points where one of x, y, z vanishes have nontrivial stabilizers. Therefore, it is best to consider the stack quotient $[S_{\mathbb{C}}/\mathbb{G}_m]$, which looks like $\mathbb{P}^1$ except that the points $j = 1728$, $j = 0$, $j = \infty$ are replaced by a $\frac{1}{2}$-point, a $\frac{1}{3}$-point, and a $\frac{1}{7}$-point, respectively. (This stack is

essentially the same as the "M-curve" of [Dar97].) The induced morphism $[S_{\mathbb{C}}/\mathbb{G}_m] \xrightarrow{j} \mathbb{P}^1$ is a ramified map of degree 1, with ramification indices 2, 3, 7 above 1728, 0, ∞, respectively.

The strategy for constructing a finite étale cover $\tilde{X}_{\mathbb{C}}$ of $S_{\mathbb{C}}$ will be first to construct a finite étale cover $X_{\mathbb{C}}$ of $[S_{\mathbb{C}}/\mathbb{G}_m]$ and then to base extend by $S_{\mathbb{C}} \to [S_{\mathbb{C}}/\mathbb{G}_m]$. A finite étale cover of $[S_{\mathbb{C}}/\mathbb{G}_m]$ is a finite cover of $\mathbb{P}^1$ whose ramification is accounted for by the ramification of $[S_{\mathbb{C}}/\mathbb{G}_m] \to \mathbb{P}^1$: in other words, a finite cover of $\mathbb{P}^1$ ramified only above 1728, 0, and ∞, and with ramification indices 2, 3, 7, respectively. In fact, we will seek such a cover that is generically Galois. Such covers can be specified analytically by giving the monodromy above the three branch points, and are automatically algebraic, by the Riemann Existence Theorem. Specifically, the Galois group should be a *Hurwitz group*: a finite group generated by elements a, b, c of orders 2, 3, 7, respectively, such that $abc = 1$. In principle we could use any Hurwitz group (even the monster group is a possibility [Wil01]), but to make future computations practical, we choose the smallest Hurwitz group: the simple group $G := \mathrm{PSL}_2(\mathbb{F}_7)$ of order 168, with generators $a = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $b = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$, $c = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

We next identify the covering curve $X_{\mathbb{C}}$. Since $[S_{\mathbb{C}}/\mathbb{G}_m]$ is obtained from $\mathbb{P}^1$ by deleting three points and reinserting a $\frac{1}{2}$-point, a $\frac{1}{3}$-point, and a $\frac{1}{7}$-point, its topological Euler characteristic satisfies

$$\begin{aligned}\chi([S_{\mathbb{C}}/\mathbb{G}_m]) &= \chi(\mathbb{P}^1) - (1+1+1) + \left(\frac{1}{2}+\frac{1}{3}+\frac{1}{7}\right) \\ &= \frac{1}{2}+\frac{1}{3}+\frac{1}{7}-1 \\ &= -\frac{1}{42}.\end{aligned}$$

The genus g of its degree-168 cover $X_{\mathbb{C}}$ satisfies

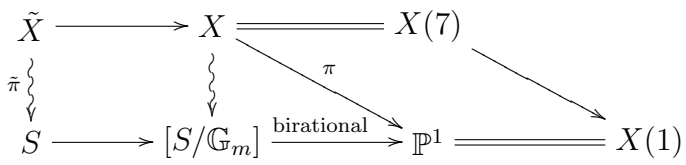
$$2-2g = \chi(X_{\mathbb{C}}) = 168\,\chi([S_{\mathbb{C}}/\mathbb{G}_m]) = -4.$$

Hence $X_{\mathbb{C}}$ is a curve of genus 3 with 168 automorphisms; the only such curve over $\mathbb{C}$ is the *Klein quartic curve* defined in $\mathbb{P}^2$ by the homogeneous equation

$$x^3y + y^3z + z^3x = 0.$$

See [Kle1879] and [Elk99] for many facts about X and G. The base extension of $X_{\mathbb{C}}$ by $S_{\mathbb{C}} \to [S_{\mathbb{C}}/\mathbb{G}_m]$ is the punctured cone $\tilde{X}_{\mathbb{C}}$ above $X_{\mathbb{C}}$, obtained by removing the origin from the surface in $\mathbb{A}^3$ defined by the same quartic polynomial.

3.3. **An étale cover of $S_{\mathbb{Z}[1/42]}$.** Let X and $\tilde{X}$ be the varieties over $\mathbb{Q}$ defined by the same equations, and let X_R and $\tilde{X}_R$ be the corresponding smooth models over $R := \mathbb{Z}[1/42]$. We identify G with $\mathrm{Aut}(X_{\mathbb{C}}) = \mathrm{Aut}(X_{\overline{\mathbb{Q}}})$, so $\mathcal{G}_{\mathbb{Q}}$ acts on G. The degree-168 étale map $\tilde{X}_{\mathbb{C}} \to S_{\mathbb{C}}$ arises from an étale map $\tilde{\pi}\colon \tilde{X}_R \to S_R$; the associated morphism $X \to \mathbb{P}^1$ is given explicitly in Section 7.3.



$$(a,b,c) \longmapsto j := \frac{1728\,b^3}{c^7} \longmapsto E_{(a,b,c)}\colon Y^2 = X^3 + 3b\,X - 2a$$

FIGURE 1. The wavy arrows denote étale morphisms. All vertical and diagonal morphisms are finite of degree 168. The schemes may be considered over $\mathbb{C}$, or more generally over any ring in which 42 is invertible.

3.4. **Descent.** Descent theory (cf. [CW30] and [Sko01, §5.3]) tells us the following:

- The set of classes in the Galois cohomology set $\mathrm{H}^1(\mathbb{Q}, G)$ that are unramified outside 2, 3, and 7 is finite. ("Unramified outside $\{2,3,7\}$" means that the image in $\mathrm{H}^1(\mathbb{Q}_p^{\mathrm{unr}}, G)$ is the neutral element for every *finite* prime $p \notin \{2,3,7\}$.)
- Each such class corresponds to an isomorphism class of twists $\tilde{\pi}'\colon \tilde{X}' \to S$ of $\tilde{\pi}\colon \tilde{X} \to S$. Choosing a cocycle in the class lets one construct a twist within the isomorphism class.
- The set $S(R)$ is the disjoint union of the sets $\tilde{\pi}'(\tilde{X}'(R))$ so obtained.

In fact, each such cocycle twists the upper half of the square

$$\begin{array}{ccc} \tilde{X} & \longrightarrow & X \\ {\scriptstyle\tilde{\pi}}\downarrow & & \downarrow{\scriptstyle\pi} \\ S & \xrightarrow{j} & \mathbb{P}^1 \end{array} \qquad \text{to yield} \qquad \begin{array}{ccc} \tilde{X}' & \longrightarrow & X' \\ {\scriptstyle\tilde{\pi}'}\downarrow & & \downarrow{\scriptstyle\pi'} \\ S & \xrightarrow{j} & \mathbb{P}^1. \end{array}$$

Since $\operatorname{Pic} R$ is trivial, each map $\tilde{X}'(R) \to X'(R) = X'(\mathbb{Q})$ is surjective. Hence $S(\mathbb{Z}) \subseteq S(R) = \bigcup j^{-1}(\pi'(X'(\mathbb{Q})))$, where the union is over our finite list of twists X' of X. So to solve the original equation, it would suffice to:

(1) Find equations for each twist X' and map π' arising from a cocycle unramified outside 2, 3, 7.
(2) Determine $X'(\mathbb{Q})$ for each X'. (Since X' is a genus-3 curve, $X'(\mathbb{Q})$ is finite by [Fal83].)

The first task reduces to a finite computation in principle, because Hermite's theorem on number fields with bounded ramification is effective. The second task is not known to reduce to a finite computation, and in fact for one of the curves X' that arises, we are unable to complete this task! (See Section 12.1.)

But since we want $S(\mathbb{Z})$ and not all of $S(R)$, we can get by with computing only the rational points inside certain "residue classes" on each curve. Say that X' *passes the local*

test if the subset $\pi'(X'(\mathbb{Q}_p)) \cap j(S(\mathbb{Z}_p))$ of $\mathbb{P}^1(\mathbb{Q}_p)$ is nonempty for all primes p. We will do the following:

(1) For each X' passing the local test, find an equation for X' and π'.
(2) For each such X', determine $\{P \in X'(\mathbb{Q}) : \pi'(P) \in j(S(\mathbb{Z}_p)) \text{ for all primes } p\}$.

4. The modular interpretation

In Section 4.3 we observe that the map $X \to \mathbb{P}^1$ is isomorphic to the map of modular curves $X(7) \to X(1)$. In later sections this will be used to help catalogue the needed twists of X. Indeed, each twist of $X(7)$ is a moduli space classifying elliptic curves with an exotic level-7 structure, so we reduce to a problem of enumerating level structures.

4.1. **Definition of $X(7)$.** If E is an elliptic curve over a field k of characteristic zero, let $E[7]$ be the $\mathcal{G}_k$-module of $\overline{k}$-points in the kernel of the multiplication-by-7 map $[7]\colon E \to E$. The Weil pairing gives an isomorphism $\bigwedge^2 E[7] \simeq \mu_7$. Let M be the $\mathcal{G}_\mathbb{Q}$-module $\mu_7 \times \mathbb{Z}/7\mathbb{Z}$.[3] There is a canonical isomorphism $\bigwedge^2 M \simeq \mu_7$ mapping $(\zeta^1, 0) \wedge (\zeta^0, 1)$ to ζ. When we write $\phi\colon M_k \overset{\wedge}{\simeq} E[7]$, we mean that ϕ is a *symplectic isomorphism*, that is, an isomorphism of $\mathcal{G}_k$-modules such that $\bigwedge^2 \phi\colon \bigwedge^2 M_k \to \bigwedge^2 E[7]$ is the identity $\mu_7 \to \mu_7$.

For a field k of characteristic zero, let $\mathcal{Y}(7)(k)$ be the set of isomorphism classes of pairs (E, ϕ) where E is an elliptic curve over k and $\phi\colon M_k \overset{\wedge}{\simeq} E[7]$. It is possible to extend $\mathcal{Y}(7)$ to a functor from $\mathbb{Q}$-schemes to sets, with essentially the same definition. The functor $\mathcal{Y}(7)$ is representable by a smooth affine curve $Y(7)$ over $\mathbb{Q}$. The curve $Y(7)$ can be completed to a smooth projective curve $X(7)$ over $\mathbb{Q}$.

Remark 4.1. The $\mathbb{Q}$-variety $X(7)$ extends to a smooth projective curve over $\mathbb{Z}[1/7]$ with geometrically integral fibers. It too is a fine moduli space, representing a certain functor.

Warning 4.2. Some authors use instead the set of isomorphism classes of pairs (E, ϕ) where $\phi\colon (\mathbb{Z}/7\mathbb{Z})^2 \simeq E[7]$ is an isomorphism of Galois modules not necessarily respecting the symplectic structures. This leads to an irreducible scheme over $\mathbb{Q}$ that over $\mathbb{Q}(\zeta)$ decomposes into 6 disjoint components, each isomorphic to our $X(7)_{\mathbb{Q}(\zeta)}$.

4.2. **Automorphisms of $X(7)$ over $\overline{\mathbb{Q}}$.** Let $Y(1)$ be the (coarse) moduli space of elliptic curves over $\mathbb{Q}$. The j-invariant gives an isomorphism $Y(1) \simeq \mathbb{A}^1$. Let $X(1) \simeq \mathbb{P}^1$ be the usual compactification of $Y(1)$. The forgetful functor mapping a pair (E, ϕ) to E induces a morphism $Y(7) \to Y(1)$ and hence also a morphism $X(7) \to X(1)$.

The isomorphism $M_{\overline{\mathbb{Q}}} \simeq (\mathbb{Z}/7\mathbb{Z})^2$ mapping (ζ^a, b) to the column vector $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ identifies $\bigwedge^2 M_{\overline{\mathbb{Q}}} \simeq (\mu_7)_{\overline{\mathbb{Q}}}$ with $\bigwedge^2 (\mathbb{Z}/7\mathbb{Z})^2 \overset{\det}{\simeq} \mathbb{Z}/7\mathbb{Z}$. Therefore the group of symplectic automorphisms of $M_{\overline{\mathbb{Q}}}$ equals

$$\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}}) = \mathrm{Aut}_\wedge((\mathbb{Z}/7\mathbb{Z})^2) = \mathrm{SL}_2(\mathbb{F}_7),$$

[3] Writing $M = \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ instead of $M = \mathbb{Z}/7\mathbb{Z} \times \mu_7$ does not change it (even considering symplectic structure). Our reason for this is so that when $M_{\overline{\mathbb{Q}}}$ is identified with column vectors, the action on $\mathrm{SL}_2(\mathbb{F}_7)$ on $M_{\overline{\mathbb{Q}}}$ agrees with its usual action on $X(7)$, as groups *equipped with a $\mathcal{G}_\mathbb{Q}$-action.*

which we view as acting on the left on column vectors. If $g \in \mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}})$, then g acts on the left on $Y(7)_{\overline{\mathbb{Q}}}$ by mapping each pair (E, ϕ) to $(E, \phi \circ g^{-1})$; this automorphism of $Y(7)_{\overline{\mathbb{Q}}}$ extends to an automorphism of $X(7)_{\overline{\mathbb{Q}}}$. Thus we obtain a homomorphism

$$\mathrm{SL}_2(\mathbb{F}_7) \to \mathrm{Aut}\, X(7)_{\overline{\mathbb{Q}}}.$$

Since $\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}})$ acts transitively on the set of ϕ corresponding to a given E over $\overline{\mathbb{Q}}$, the covering $X(7)_{\overline{\mathbb{Q}}} \to X(1)_{\overline{\mathbb{Q}}}$ is generically Galois, and $\mathrm{SL}_2(\mathbb{F}_7)$ surjects onto the Galois group of the covering. Pairs (E, ϕ) and (E, ϕ') are isomorphic if and only if $\phi' = \alpha \circ \phi$ for some $\alpha \in \mathrm{Aut}(E)$; but $\mathrm{Aut}(E)$ is generated by $[-1]$ for most E, so the kernel of $\mathrm{SL}_2(\mathbb{F}_7) \to \mathrm{Gal}(X(7)_{\overline{\mathbb{Q}}}/X(1)_{\overline{\mathbb{Q}}})$ is generated by the scalar matrix $-1 \in \mathrm{SL}_2(\mathbb{F}_7)$. In other words, there is an isomorphism $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{Gal}(X(7)_{\overline{\mathbb{Q}}}/X(1)_{\overline{\mathbb{Q}}})$.

4.3. **The Klein quartic as $X(7)$.** There exists an isomorphism of $\mathbb{Q}$-varieties $X \to X(7)$ [Elk99]. The group of automorphisms of X over $\mathbb{Q}$ has order 3, so the isomorphism $X \simeq X(7)$ is not unique; we will take the the particular isomorphism in [Elk99] for which the homogeneous coordinates x, y, z correspond on $X(7)$ to cusp forms whose q-expansions begin

$$\begin{aligned}
\mathsf{x} &= q^{4/7}(-1 + 4q - 3q^2 - 5q^3 + 5q^4 + 8q^6 - 10q^7 + 4q^9 - 6q^{10} + \dots), \\
\mathsf{y} &= q^{2/7}(1 - 3q - q^2 + 8q^3 - 6q^5 - 4q^6 + 2q^8 + 9q^{10} + \dots), \text{ and} \\
\mathsf{z} &= q^{1/7}(1 - 3q + 4q^3 + 2q^4 + 3q^5 - 12q^6 - 5q^7 + 7q^9 + 16q^{10} + \dots).
\end{aligned}$$

Taking the quotient of each curve by its $\overline{\mathbb{Q}}$-automorphism group, we obtain the commutative parallelogram at the right in Figure 1. Comparing the branch points and ramification indices of $X(7) \to X(1)$ with $X \to \mathbb{P}^1$ determines the values of the isomorphism $X(1) \to \mathbb{P}^1$ at 3 points; it follows that the isomorphism is the standard one given by the j-invariant.

4.4. **Twists of $X(7)$.** Since $\mathcal{G}_\mathbb{Q}$ acts on $M_{\overline{\mathbb{Q}}}$, it acts also on $\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}})$. The homomorphism $\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}}) \to \mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}})$ is $\mathcal{G}_\mathbb{Q}$-equivariant, so we obtain a map of cohomology sets

$$\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}})) \to \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}})).$$

This map, which is not a bijection, can be reinterpreted as

$$\{\text{symplectic twists of } M\} \to \{\text{twists of } X(7)\}. \tag{4.3}$$

(A *symplectic twist* of M is a $\mathcal{G}_\mathbb{Q}$-module M' with an isomorphism $\bigwedge^2 M' \simeq \mu_7$ such that there is an isomorphism $\iota\colon M_{\overline{\mathbb{Q}}} \to M'_{\overline{\mathbb{Q}}}$ such that $\bigwedge^2 \iota$ is the identity $\mu_7 \to \mu_7$ over $\overline{\mathbb{Q}}$.) In (4.3), let $X_{M'}(7)$ be the image of M'. Thus $X_{M'}(7)$ is the smooth projective model of the smooth affine curve whose points classify pairs (E, ϕ) where E is an elliptic curve and $\phi\colon M' \overset{\wedge}{\simeq} E[7]$.

Since $\mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}})$ acts as automorphisms of $X(7)_{\overline{\mathbb{Q}}}$ over $X(1)_{\overline{\mathbb{Q}}}$, there is a canonical morphism $X_{M'}(7) \to X(1)$. In the moduli interpretation, this is the forgetful functor mapping (E, ϕ) to E.

If $a \in \mathbb{F}_7^\times$, composing $\bigwedge^2 M' \simeq \mu_7$ with the a^{th}-power map $\mu_7 \to \mu_7$ gives a new isomorphism $\bigwedge^2 M' \simeq \mu_7$. Let M'^a be M' with this new symplectic structure. If $a = b^2\alpha$ for some

$b \in \mathbb{F}_7^\times$, then multiplication-by-b induces $M'^a \overset{\wedge}{\simeq} M'^\alpha$. Thus only the image of a in $\mathbb{F}_7^\times/\mathbb{F}_7^{\times 2}$ matters: we lose nothing by considering $a = \pm 1$ only.

If M' is a symplectic twist of M, and $M'' = M' \otimes \chi$ for some quadratic character $\chi\colon \mathcal{G}_\mathbb{Q} \to \{\pm 1\}$, then the elements of $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}}))$ corresponding to M' and M'' have the same image in $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}}))$, because $\{\pm 1\}$ is in the kernel of $\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}}) \to \mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}})$.

4.5. **Twists of $X(7)$ associated to elliptic curves.** Let E be an elliptic curve over $\mathbb{Q}$. Define $X_E(7) := X_{E[7]}(7)$ and $X_E^-(7) := X_{E[7]^{-1}}(7)$.

If F is a quadratic twist of E, then $X_E(7) \simeq X_F(7)$ and $X_E^-(7) \simeq X_F^-(7)$.

Lemma 4.4. *If F' is a quadratic twist of an elliptic curve F such that $F[7] \simeq E[7]$ as $\mathcal{G}_\mathbb{Q}$-modules* without symplectic structure*, then the point $j(F') \in X(1)(\mathbb{Q})$ is in the image of $X_E(7)(\mathbb{Q}) \to X(1)(\mathbb{Q})$ or $X_E^-(7)(\mathbb{Q}) \to X(1)(\mathbb{Q})$.*

Proof. By the discussion above, we need to have $F[7] \overset{\wedge}{\simeq} E[7]$ or $F[7] \overset{\wedge}{\simeq} E[7]^{-1}$, and so F gives rise to a rational point on $X_E(7)$ or on $X_E^-(7)$. Therefore, $j(F') = j(F)$ is in the image of $X_E(7)(\mathbb{Q}) \to X(1)(\mathbb{Q})$ or of $X_E^-(7)(\mathbb{Q}) \to X(1)(\mathbb{Q})$. □

Warning 4.5. Not every twist of $X(7)$ can be written as $X_E(7)$ or $X_E^-(7)$ for an elliptic curve E over $\mathbb{Q}$. For example, let $M' := \mu_7^{\otimes 2} \times \mu_7^{\otimes -1}$, equipped with a symplectic structure $\bigwedge^2 M' \simeq \mu_7$, and let $X' = X_{M'}(7)$. If X' were isomorphic to $X_E^-(7)$, it would also be isomorphic to $X_E(7)$, since $\mathrm{Aut}(M')$ acts transitively on the symplectic structures on M'. This is impossible, because $X'(\mathbb{Q}) = \emptyset$: indeed, $X'(\mathbb{F}_2) = \emptyset$, since there are no elliptic curves E over $\mathbb{F}_2$ (not even degenerate ones corresponding to cusps) with $E[7] \simeq \mu_7^{\otimes 2} \times \mu_7^{\otimes -1}$, that is, with the 2-power Frobenius acting on $E[7]$ as multiplication-by-4.

In fact, $X(7)$ itself is another example of a twist that cannot be written as $X_E(7)$ or $X_E^-(7)$ (at least if one requires E to be a *nondegenerate* elliptic curve over $\mathbb{Q}$): again $\mathrm{Aut}(M)$ acts transitively on the symplectic structures on M, and although this time $X(7)$ has rational points, they are all cusps [Elk99].

4.6. **Primitive solutions and elliptic curves.** Suppose $(a, b, c) \in S(\mathbb{Z})$ and a, b, c are nonzero. Then $j := 1728\, b^3/c^7$ is not 1728, 0, or ∞. The corresponding point on $X(1)$ is represented by the elliptic curve

$$E = E_{(a,b,c)}\colon Y^2 = X^3 + 3b\, X - 2a$$

and its quadratic twists. The twist X' of X in Section 3.4 for which $j \in \pi'(X'(\mathbb{Q}))$ corresponds to the twist $X_E(7)$ of $X(7)$. Therefore to find the relevant twists of $X(7)$, it suffices to catalogue the possibilities for the $\mathcal{G}_\mathbb{Q}$-module $E[7]$, up to quadratic twist. Restrictions on $E[7]$ will be deduced from the following.

Lemma 4.6. *If $(a, b, c) \in S(\mathbb{Z})$ and a, b, c are nonzero, then $1728\, b^3/c^7$ is the j-invariant of an elliptic curve E over $\mathbb{Q}$ such that*

(a) *The conductor N of E is of the form $2^r 3^s \prod_{p \in T} p$ where $r \leq 6$, $s \leq 3$, and T is a finite set of primes ≥ 5.*

(b) $E[7]$ *is finite at* 7 *in the sense of* [Ser87, p. 189].

Proof.

(a) Since $\gcd(a,b,c) = 1$ and $a^2 + b^3 = c^7$, the integers a, b, c are *pairwise* relatively prime. We need to bound the p-adic valuation $v_p(N)$ for each prime p.

Case 1: $p \geq 5$

Associated to the Weierstrass equation for $E_{(a,b,c)}$ are the quantities

$$c_4 = -12^2\, b\,, \qquad c_6 = 12^3\, a\,, \qquad \Delta = -12^3\, c^7\,.$$

(See [Sil92, III.§1] for definitions.) Suppose $p \geq 5$ is a prime dividing N. Then $p \mid \Delta$. But $\gcd(b,c) = 1$, so $p \nmid c_4$. By [Sil92, VII.5.1(b)], E has multiplicative reduction at p, and $v_p(N) = 1$.

Case 2: $p = 3$

If $3 \nmid c$, then $v_3(N) \leq v_3(\Delta) \leq 3$. Therefore suppose $3 \mid c$. Then $3 \nmid a, b$. Let $t = a/b \in \mathbb{Z}_3$. Then $a^2 + b^3 \equiv 0 \pmod{3^7}$ implies $(a,b) \equiv (-t^3, -t^2) \pmod{3^7}$. The right hand side of the Weierstrass equation is now congruent to $(X-t)(X-t)(X+2t)$ modulo 3^7, so the substitution $X \mapsto x + t$ results in a cubic polynomial congruent to $x^3 + 3tx^2$ modulo 3^7. Hence we can twist by $-1/3$ to obtain an elliptic curve E' such that

$$v_3(c_4') = v_3(-12^2 b) - 2 = 0 \quad \text{and} \quad v_3(\Delta') = v_3(-12^3 c^7) - 6 > 0.$$

Thus E' has multiplicative reduction, and $v_3(N') = 1$.

Case 3: $p = 2$

If $2 \nmid c$, then $v_2(N) \leq v_2(\Delta) \leq 6$. Therefore suppose $2 \mid c$. Twisting by -1 if necessary, we may assume $a \equiv 1 \pmod 4$. As in the previous paragraph, we have $(a,b) \equiv (-t^3, -t^2) \pmod{2^7}$ for some $t \in \mathbb{Z}_2$ and we can find a model $y^2 = f(x)$ where $f(x) \equiv x^3 + 3tx^2 \pmod{2^7}$. Now $a \equiv 1 \pmod 4$ implies $t \equiv -1 \pmod 4$, so the further substitution $y \mapsto y' + x$ shows that the model is not minimal at 2. Thus we arrive at a model E' with

$$v_2(c_4') = v_2(-12^2 b) - 4 = 0 \quad \text{and} \quad v_2(\Delta') = v_2(-12^3 c^7) - 12 > 0,$$

and hence $v_2(N') = 1$.

(b) If $7 \nmid c$, then E has good reduction at 7, so $E[7]$ is finite at 7. If $7 \mid c$, then $v_7(j) = -7v_7(c)$ is a negative multiple of 7, so by the theory of Tate curves, $E[7]$ is finite at 7. (The twists applied in part (a) affect the behavior at 2 and 3 independently, and do not interfere with the behavior at other primes.) □

5. Reducible 7-torsion

By Lemma 4.6 we need only catalogue the possibilities for $E[7]$ (up to quadratic twist) such that $E[7]$ is unramified outside $\{2, 3, 7\}$. In this section we assume moreover that $E[7]$ is reducible as a $\mathcal{G}_{\mathbb{Q}}$-module.

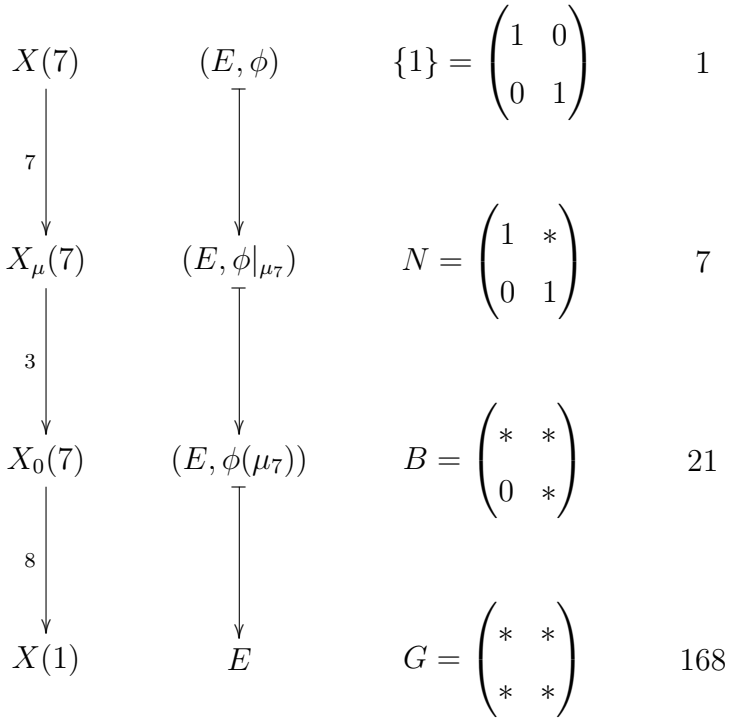


FIGURE 2. Modular curves of level 7.

5.1. **Intermediate modular curves.** Let $Y_\mu(7)$ over $\mathbb{Q}$ be the affine curve parametrizing pairs (E, ψ) where E is an elliptic curve and $\psi\colon \mu_7 \hookrightarrow E[7]$ is an injection. Let $X_\mu(7)$ be the smooth projective curve having $Y_\mu(7)$ as an affine subset.

Remark 5.1. The curve $X_\mu(7)$ is a twist of the classical modular curve $X_1(7)$, the completion of the curve $Y_1(7)$ parametrizing (E, P) where P is a point of exact order 7 on E: giving P is equivalent to giving an injection $\mathbb{Z}/7\mathbb{Z} \hookrightarrow E[7]$. In a less obvious way, $X_\mu(7)$ is also isomorphic to $X_1(7)$: if (E, ψ) as above is defined over k, one can map it to the pair (E', P') where E' is the elliptic curve $E/\psi(\mu_7)$ over k and $P' \in E'[7](k)$ is the image of a point $P \in E[7](\overline{k})$ whose Weil pairing with $\psi(\zeta)$ gives ζ.

Define $Y_0(7)$ as the (coarse) moduli space parametrizing pairs (E, C) where C is a (cyclic) order-7 subgroup of E, and define $X_0(7)$ as the completed curve.

The columns of Figure 2 show

- the morphisms relating the modular curves, labelled by their degrees,
- the moduli interpretations of these morphisms,
- the subgroup $\mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}}/Z_{\overline{\mathbb{Q}}})$ of $\mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}}/X(1)_{\overline{\mathbb{Q}}}) = G$ corresponding to each intermediate curve Z, and
- the orders of these subgroups.

The notation $B = \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ means that B equals the image of $\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_7)\}$ in $\mathrm{PSL}_2(\mathbb{F}_7) \simeq G$.

5.2. **The Galois action on G and its subgroups.** Since $M = \mu_7 \times \mathbb{Z}/7\mathbb{Z}$, we have

$$\mathrm{End}(M_{\overline{\mathbb{Q}}}) \simeq \begin{pmatrix} \mathrm{End}(\mu_7) & \mathrm{Hom}(\mathbb{Z}/7\mathbb{Z}, \mu_7) \\ \mathrm{Hom}(\mu_7, \mathbb{Z}/7\mathbb{Z}) & \mathrm{End}(\mathbb{Z}/7\mathbb{Z}) \end{pmatrix} \simeq \begin{pmatrix} \mathbb{Z}/7\mathbb{Z} & \mu_7 \\ \mu_7^{\otimes -1} & \mathbb{Z}/7\mathbb{Z} \end{pmatrix},$$

which is the matrix ring $\mathrm{M}_2(\mathbb{F}_7)$ with a nontrivial $\mathcal{G}_{\mathbb{Q}}$-action. This $\mathcal{G}_{\mathbb{Q}}$-action induces a $\mathcal{G}_{\mathbb{Q}}$-action on $\mathrm{PSL}_2(\mathbb{F}_7)$ making $\mathrm{PSL}_2(\mathbb{F}_7) \simeq G$ an isomorphism of $\mathcal{G}_{\mathbb{Q}}$-*groups* (groups equipped with a continuous action of $\mathcal{G}_{\mathbb{Q}}$).

In particular, $N \simeq \mu_7$ as $\mathcal{G}_{\mathbb{Q}}$-groups, and B is a semidirect product of the subgroup $H := \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \simeq \mathbb{F}_7^{\times}/\{\pm 1\} \simeq \mathbb{Z}/3\mathbb{Z}$ (with trivial $\mathcal{G}_{\mathbb{Q}}$-action) by N. Thus we have a split exact sequence of $\mathcal{G}_{\mathbb{Q}}$-groups

$$0 \to \mu_7 \to B \to \mathbb{Z}/3\mathbb{Z} \to 0. \tag{5.2}$$

The generators $g := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $N \simeq \mu_7$ and $h := \left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ of $H \simeq \mathbb{Z}/3\mathbb{Z}$ satisfy $h^{-1}gh = g^2$. Under the isomorphism in Section 4.3, g and h correspond to the automorphisms $(x : y : z) \mapsto (\zeta^4 x : \zeta^2 y : \zeta z)$ and $(x : y : z) \mapsto (y : z : x)$ of X, according to [Elk99].

5.3. **Nonabelian cohomology of B.** Let E be an elliptic curve over $\mathbb{Q}$ such that $E[7]$ is reducible as a $\mathcal{G}_{\mathbb{Q}}$-module. Thus there is a $\mathcal{G}_{\mathbb{Q}}$-stable order-7 subgroup $C \subset E[7]$. Choosing $\phi\colon M_{\overline{\mathbb{Q}}} \overset{\wedge}{\simeq} E[7]_{\overline{\mathbb{Q}}}$ such that $\phi(\mu_7) = C$ shows that the twist $X_E(7)$ of $X(7)$ arises from a cocycle taking values in the subgroup B of G. In this subsection, we calculate $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, B)$; in the next subsection, we use the results to write down equations for all $X_E(7)$ corresponding to E with reducible $E[7]$.

From the exact sequence (5.2) of $\mathcal{G}_{\mathbb{Q}}$-groups, we obtain the exact sequence of pointed sets [Ser02, Proposition 38, p. 51]

$$\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, \mu_7) \to \mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, B) \xrightarrow{s} \mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z}).$$

Define s as shown. Since the last map in (5.2) admits a section, s admits a section; in particular s is surjective.

Suppose ξ is a cocycle representing a class $[\xi] \in \mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$. Since $\mathbb{Z}/3\mathbb{Z}$ acts on μ_7, ξ determines a twist ${}_{\xi}\mu_7$ of μ_7. A cohomologous cocycle would determine a (noncanonically) isomorphic twist. Via the section of $B \to \mathbb{Z}/3\mathbb{Z}$, we may view ξ also as a B-valued cocycle. By [Ser02, Corollary 2, p. 52], there is a natural surjective map $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, {}_{\xi}\mu_7) \to s^{-1}([\xi])$. We now calculate $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, {}_{\xi}\mu_7)$.

Case 1: $[\xi] = 0$.
Then $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, {}_{\xi}\mu_7) = \mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, \mu_7) \simeq \mathbb{Q}^{\times}/\mathbb{Q}^{\times 7}$.

Case 2: $[\xi] \neq 0$.

Then $[\xi] \in \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathbb{Z}/3\mathbb{Z}) = \mathrm{Hom}_{\mathrm{conts}}(\mathcal{G}_\mathbb{Q}, \mathbb{Z}/3\mathbb{Z})$ corresponds to a cyclic cubic extension K of $\mathbb{Q}$ with a choice of generator $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. From the Hochschild-Serre spectral sequence [Ser02, p. 15] we can extract the exact sequence

$$\begin{aligned} \mathrm{H}^1(\mathrm{Gal}(K/\mathbb{Q}), ({}_\xi\mu_7)^{\mathcal{G}_K}) \to \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, {}_\xi\mu_7) \to \mathrm{H}^1(\mathcal{G}_K, {}_\xi\mu_7)^{\mathrm{Gal}(K/\mathbb{Q})} \\ \to \mathrm{H}^2(\mathrm{Gal}(K/\mathbb{Q}), ({}_\xi\mu_7)^{\mathcal{G}_K}). \end{aligned} \tag{5.3}$$

The first and last terms are zero, since $\mathrm{Gal}(K/\mathbb{Q})$ and ${}_\xi\mu_7$ have relatively prime orders. In the third term, $\mathrm{H}^1(\mathcal{G}_K, {}_\xi\mu_7)$ equals $K^\times/K^{\times 7}$ with a twisted action of $\mathrm{Gal}(K/\mathbb{Q})$; thus $\mathrm{H}^1(\mathcal{G}_K, {}_\xi\mu_7)^{\mathrm{Gal}(K/\mathbb{Q})}$, instead of equalling the subgroup of $K^\times/K^{\times 7}$ *fixed* by the usual action of τ, equals the subgroup $(K^\times/K^{\times 7})^{\tau=2}$ of $K^\times/K^{\times 7}$ consisting of elements on which τ has the same effect as squaring. (The 2 comes from the action of $\mathbb{Z}/3\mathbb{Z}$ on μ_7, that is, from the fact that $h^{-1}gh = g^2$.) Thus (5.3) gives

$$\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, {}_\xi\mu_7) \simeq \mathrm{H}^1(\mathcal{G}_K, {}_\xi\mu_7)^{\mathrm{Gal}(K/\mathbb{Q})} \simeq (K^\times/K^{\times 7})^{\tau=2}.$$

5.4. **Twists of $X(7)$ corresponding to reducible $E[7]$.** We now write down twists of $X \simeq X(7)$ whose classes in $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, G)$ represent the image of $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, B) \to \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, G)$.

Case 1: $[\xi] = 0$.

Given $a \in \mathbb{Q}^\times$, fix $\alpha \in \overline{\mathbb{Q}}$ with $\alpha^7 = a$. The substitution $(x, y, z) = (\alpha^4\bar{x}, \alpha^2\bar{y}, \alpha\bar{z})$ transforms $X_{\overline{\mathbb{Q}}}$ into the plane curve

$$(\alpha^4\bar{x})^3(\alpha^2\bar{y}) + (\alpha^2\bar{y})^3(\alpha\bar{z}) + (\alpha\bar{z})^3(\alpha^4\bar{x}) = 0,$$

which, if we divide by a and drop the bars, is the same as

$$X' \colon ax^3y + y^3z + z^3x = 0. \tag{5.4}$$

Let $\beta \colon X_{\overline{\mathbb{Q}}} \to X'_{\overline{\mathbb{Q}}}$ be the isomorphism we just described. If we identify the automorphism $(x : y : z) \mapsto (\zeta^4 x : \zeta^2 y : \zeta z)$ of $X_{\overline{\mathbb{Q}}}$ with $g := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in N$ and with $\zeta \in \mu_7$, then the cocycle $\sigma \mapsto \beta^{-1}({}^\sigma\beta) \in N$ is identified with the cocycle $\sigma \mapsto {}^\sigma\alpha^{-1}/\alpha^{-1} \in \mu_7$. Thus the image of a^{-1} under

$$\mathbb{Q}^\times \to \mathbb{Q}^\times/\mathbb{Q}^{\times 7} \simeq \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mu_7) \simeq \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, N) \to \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, G)$$

corresponds to the twist X' of X. In particular, all twists of X arising in Case 1 have the form (5.4), where a runs through positive integers representing the elements of $\mathbb{Q}^\times/\mathbb{Q}^{\times 7}$.

The same curves can be written in other ways. Suppose that X' is a curve given by

$$ax^3y + by^3z + cz^3x = 0$$

for some $a, b, c \in \mathbb{Z}_{>0}$. If p is a prime such that p^2 divides a, then multiplying by p and substituting $x = \bar{x}/p$ leads to an isomorphic curve of the same type but with a smaller value of abc. Similar reductions apply if p^2 divides b or c. Hence eventually we can reduce to a curve where a, b, and c are squarefree. Moreover we may assume that $\gcd(a, b, c) = 1$ and that $a \geq b$ and $a \geq c$.

Case 2: $[\xi] \neq 0$.

We will write the action of τ on K on the right, so that we can use notation such as $a^{2\tau-3} := (a^\tau)^2/a^3$ for $a \in K^\times$. Let $\ell \in K\bar{x} + K\bar{y} + K\bar{z}$ be a linear form such that ℓ, ℓ^τ, and $\ell^{\tau\tau}$ form a K-basis for $K\bar{x} + K\bar{y} + K\bar{z}$. Let $a \in K^\times$ be such that its image in $K^\times/K^{\times 7}$ lies in $(K^\times/K^{\times 7})^{\tau=2}$. Thus $a^{\tau-2} = b^7$ for some $b \in K^\times$. Applying $\tau^2 + 2\tau + 4$ and using $\tau^3 = 1$ yields $a^{-7} = b^{7\tau^2+14\tau+28}$. Since $\mu_7(K) = \{1\}$, it follows that $a^{-1} = b^{\tau^2+2\tau+4}$.

Choose $\alpha \in \overline{\mathbb{Q}}$ such that $\alpha^7 = a$. Define elements $\alpha_\tau := b\alpha^2$ and $\alpha_{\tau\tau} := b^{\tau+2}\alpha^4$ of $\overline{\mathbb{Q}}$. (There is no action of τ on α, so we interpret α_τ and $\alpha_{\tau\tau}$ as new labels.) Then $\alpha_\tau^7 = a^\tau$ and $\alpha_{\tau\tau}^7 = a^{\tau\tau}$.

A calculation shows that the substitution $(x, y, z) = (\alpha_{\tau\tau}\ell^{\tau\tau}, \alpha_\tau\ell^\tau, \alpha\ell)$ transforms $X_{\overline{\mathbb{Q}}}$ into the plane curve

$$X_{c,\ell}\colon\ c^{\tau\tau}\ell^{3\tau\tau+\tau} + c^\tau\ell^{3\tau+1} + c\ell^{3+\tau\tau} = 0, \tag{5.5}$$

where $c = b^{\tau+2}a \in K^\times$. By symmetry, the coefficients of the polynomial in $\bar{x}$, $\bar{y}$, $\bar{z}$ defining $X_{c,\ell}$ are fixed by τ, and hence are in $\mathbb{Q}$. A chase through definitions (similar to that in Case 1, but more tedious) shows that the B-valued cocycle defined by the constructed isomorphism $X_{\overline{\mathbb{Q}}} \to (X_{c,\ell})_{\overline{\mathbb{Q}}}$ represents the element of $s^{-1}([\xi])$ coming from the image of a^{-1} in $(K^\times/K^{\times 7})^{\tau=2}$.

In summary, all twists of X arising in Case 2 have the form $X_{c,\ell}$ for some cyclic cubic extension K, some choice of $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, some choice of ℓ, and some choice of $c \in K^\times$. Changing ℓ does not change $X_{c,\ell}$.

Changing a to $\tilde{a} = d^7a$ for some $d \in K^\times$, so that the corresponding values of b and c are $\tilde{b} = d^{\tau-2}b$ and $\tilde{c} = d^{\tau^2+3}c$, does not change $X_{c,\ell}$. Thus multiplying c by an element of $K^{\times(\tau^2+3)}$ does not change $X_{c,\ell}$. (This amounts to changing ℓ into $d\ell$, resulting in a linear substitution on $(\bar{x}, \bar{y}, \bar{z})$ with rational coefficients.) Multiplying c by an element of $K^{\times(\tau^2+\tau+1)} \subseteq \mathbb{Q}^\times$ simply multiplies the equation of $X_{c,\ell}$ by an element of $\mathbb{Q}^\times$, so this also does not change $X_{c,\ell}$. Since the difference of $\tau^2 + \tau + 1$ and $\tau^2 + 3$ equals $\tau - 2$, and since 7 is a multiple of $\tau - 2$ in $\mathbb{Z}[\tau]/(\tau^3 - 1)$, multiplying c by an element of $K^{\times 7}$ or more generally, an element of $K^{\times(\tau-2)}$, does not change $X_{c,\ell}$. Since the natural map $(K^\times/K^{\times 7})^{\tau=2} \to K^\times/K^{\times(\tau-2)}$ is an isomorphism, it suffices to let c run through representatives of the elements of $(K^\times/K^{\times 7})^{\tau=2}$.

5.5. **Ramification conditions.** In our application, we know by Lemma 4.6 that $E[7]$ is unramified outside $\{2, 3, 7\}$, just as M is. Therefore any isomorphism $M_{\overline{\mathbb{Q}}} \overset{\wedge}{\simeq} E[7]_{\overline{\mathbb{Q}}}$ will be unramified outside $\{2, 3, 7\}$. The choice of isomorphism gives the cocycle defining the twist $X_E(7)$ of $X(7)$, so the cocycle will be unramified outside $\{2, 3, 7\}$, and then so will be all the cocycles in Section 5.3.

Case 1: $[\xi] = 0$.

The twist has the form (5.4) for some $a \in \mathbb{Z}_{>0}$. We need consider only a whose image in $\mathbb{Q}^\times/\mathbb{Q}^{\times 7} \simeq \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mu_7)$ is unramified outside $\{2, 3, 7\}$. Equivalently, the field $\mathbb{Q}(a^{1/7})$ should be unramified outside $\{2, 3, 7\}$. Concretely, this means that the only primes occurring in the factorization of a are among 2, 3, and 7.

Case 2: $[\xi] \neq 0$.

The number field K must be unramified above all finite places outside $\{2,3,7\}$. By the Kronecker-Weber theorem, the only such cyclic cubic extensions are the four degree-3 subfields of the $(\mathbb{Z}/3\mathbb{Z})^2$-extension $\mathbb{Q}(\zeta+\zeta^{-1},\zeta_9+\zeta_9^{-1})$, where $\zeta=e^{2\pi i/7}$ (as usual) and $\zeta_9=e^{2\pi i/9}$. Let $\mathcal{O}_K$ be the ring of integers of K. The element $a\in K^\times$ must be such that $K(a^{1/7})$ is unramified above finite places outside $\{2,3,7\}$. Since each K has class number 1, it is possible to multiply a by an element of $K^{\times 7}$ to assume that $a\in\mathcal{O}_K[1/42]^\times$. Then the element c of Case 2 of Section 5.4 lies in $\mathcal{O}_K[1/42]^\times$, and we can finally reduce to the finite group $(\mathcal{O}_K[1/42]^\times/\mathcal{O}_K[1/42]^{\times 7})^{\tau=2}$, generators for which are easily computed for each (K,τ).

6. Irreducible 7-torsion: level lowering

Now we list the possibilities for irreducible $E[7]$, up to quadratic twist. 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 6.1. *Suppose that E is as in Lemma 4.6, and that $E[7]$ is an irreducible $\mathcal{G}_\mathbb{Q}$-module. Then there exists a quadratic twist E' of some $E''\in\mathcal{E}$ such that $E[7]\simeq E'[7]$ as $\mathcal{G}_\mathbb{Q}$-modules.*

Proof. By [BCDT01], there is a weight-2 newform f on $\Gamma_0(N)$ associated to E, where N is the conductor of E. By Lemma 4.6, $N=2^r3^s\prod_{p\in T}p$ for some $r\le 6$, $s\le 3$ and finite set T of primes ≥ 5. Let $N'=2^r3^s$. Since $E[7]$ is irreducible, Theorem 1.1 of [Rib90] lets us lower the level of f by eliminating 7 (if present) and then the other primes ≥ 5: more precisely, there is a weight-2 newform f' on $\Gamma_0(N')$ such that "$f'\equiv f \pmod 7$." The congruence is to be interpreted as follows: "The $\mathbb{Z}$-algebra generated by the Fourier coefficients of f' is an order $\mathcal{O}_{f'}$ in some number field, and there is a prime ideal $\mathfrak{p}\subset\mathcal{O}_{f'}$ of norm 7 such that $a_p(f') \bmod \mathfrak{p} = a_p(f) \bmod 7$ for all but finitely many p." Replacing f' by a quadratic twist does not change $\mathcal{O}_{f'}$.

We now consult William Stein's Modular Forms Database [Ste] (or use Magma [Magma]), and get all weight-2 newforms f' of level dividing $2^6 3^3$. If two of them are quadratic twists of each other, we can check this by looking at sufficiently many coefficients, because the twisting factor is in $\{\pm1,\pm2,\pm3,\pm6\}$, and the order of vanishing of a difference of modular forms at the cusp ∞ can be bounded in terms of its level. We find that each f' is a quadratic twist of one of 14 newforms f''. Now 13 of these 14 newforms have $\mathcal{O}_{f''}=\mathbb{Z}$ and are associated to the elliptic curves $E''\in\mathcal{E}$. (Warning: the labelling of isogeny classes of [Ste] is different from that of [Cre97] at some levels.) The 14^{th} has $\mathcal{O}_{f''}$ an order containing $\sqrt{13}$ in $\mathbb{Q}(\sqrt{13})$ (in fact it is $\mathbb{Z}[\sqrt{13}]$); such an order has no prime of norm 7, so we can discard this last newform.

Thus $f\equiv f' \pmod 7$ where f' is associated to an elliptic curve E' having a quadratic twist $E''\in\mathcal{E}$. By the Eichler-Shimura relation (see [Eic54] for the relation in the context we need), the congruence implies that for all but finitely many p, the traces of the Frobenius automorphism at p acting on $E[7]$ and $E'[7]$ are equal. By the Chebotarev density theorem, the $\mathcal{G}_\mathbb{Q}$-representations $E[7]$ and $E'[7]$ have the same trace. They also have the same

determinant, namely the cyclotomic character. So the Brauer-Nesbitt theorem [CR88, Theorem 30.16] implies that the semisimplifications of $E[7]$ and $E'[7]$ are isomorphic. But $E[7]$ is irreducible and hence semisimple, so $E[7] \simeq E'[7]$ as $\mathcal{G}_{\mathbb{Q}}$-modules. □

Corollary 6.2. *Suppose $(a, b, c) \in S(\mathbb{Z})$ and a, b, c are nonzero. If $E_{(a,b,c)}[7]$ is irreducible, then $j = 1728\, b^3/c^7 \in X(1)(\mathbb{Q})$ is the image of a rational point on one of the 26 curves $X_E(7)$ or $X_E^-(7)$ with $E \in \mathcal{E}$.*

Proof. Combine Lemmas 4.4 and 6.1. □

7. Explicit equations

Each twist of $X = X(7)$ is a nonhyperelliptic curve of genus 3, and hence has a model as a smooth plane curve of degree 4. In this section we find equations for the homogeneous forms defining the twists that we need, and also the equations for their canonical morphisms to $\mathbb{P}^1 = X(1)$. The strategy is to exploit the 168 symmetries.

7.1. **Covariants of ternary quartic forms.** The standard left action of $\mathrm{GL}_n(\mathbb{C})$ on $V = \mathbb{C}^n$ induces a right action of $\mathrm{GL}_n(\mathbb{C})$ on the $\mathbb{C}$-algebra $\mathbb{C}[x_1, \dots, x_n] = \mathrm{Sym}\ V^*$. If $g \in \mathrm{GL}_n(\mathbb{C})$ and $F \in \mathbb{C}[x_1, \dots, x_n]$, let F^g be the result of applying g to F, so $F^g(v) = F({}^g v)$ for all $v \in V$. Let $\mathbb{C}[x_1, \dots, x_n]_d = \mathrm{Sym}^d V^*$ be the subspace of $\mathbb{C}[x_1, \dots, x_n]$ consisting of homogeneous polynomials of degree d.

Fix n and d. A *covariant* of *order* j and *degree* δ is a function $\Psi\colon \mathbb{C}[x_1, \dots, x_n]_d \to \mathbb{C}[x_1, \dots, x_n]_j$ such that

(1) The coefficient of a fixed monomial $x_1^{i_1} \dots x_n^{i_n}$ in $\Psi(F)$ depends polynomially on the coefficients of F, as F varies.
(2) For each $g \in \mathrm{SL}_n(\mathbb{C})$, we have $\Psi(F^g) = \Psi(F)^g$.
(3) For each $t \in \mathbb{C}^\times$, we have $\Psi(tF) = t^\delta \Psi(F)$.

In the same way, a *contravariant* of *order* j and *degree* δ is a polynomial map $\Psi\colon \mathrm{Sym}^d V^* \to \mathrm{Sym}^j V$ that is equivariant with respect to the right action of $\mathrm{SL}_n(\mathbb{C})$ on the two spaces and is homogeneous of degree δ in the coefficients. (The right action of $\mathrm{SL}_n(\mathbb{C})$ on V is the contragredient of the action on V^*.) In other words, for all $F \in \mathrm{Sym}^d V^*$ and $g \in \mathrm{SL}_n(\mathbb{C})$ we have $\Psi(F^g) = \Psi(F)^{g^{-t}}$, where g^{-t} is the inverse transpose of g. Our choice of basis for V induces an isomorphism $V \to V^*$, so we may express each contravariant as a polynomial in the same variables $x_1, \dots, x_n$.

From now on, we take $n = 3$ and $d = 4$, and use x, y, z in place of x_1, x_2, x_3. We will list some covariants, which we will call Ψ_0, Ψ_4, Ψ_6, Ψ_{14}, and Ψ_{21}, and a contravariant, which we will call Ψ_{-4}. They will be of orders 0, 4, 6, 14, 21, 4 and of degrees 3, 1, 3, 8, 12, 2, respectively.

First of all, define $\Psi_4(F) = F$. Then $\Psi_6(F)$ is essentially the Hessian of F:

$$\Psi_6(F) = -\frac{1}{54}\begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x\,\partial y} & \frac{\partial^2 F}{\partial x\,\partial z} \\ \frac{\partial^2 F}{\partial y\,\partial x} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y\,\partial z} \\ \frac{\partial^2 F}{\partial z\,\partial x} & \frac{\partial^2 F}{\partial z\,\partial y} & \frac{\partial^2 F}{\partial z^2} \end{vmatrix}$$

The constant $-1/54$ is there so that Ψ_6 has integer coefficients with gcd 1. Next, $\Psi_{14}(F)$ is obtained in a similar way:

$$\Psi_{14}(F) = \frac{1}{9}\begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x\,\partial y} & \frac{\partial^2 F}{\partial x\,\partial z} & \frac{\partial \Psi_6(F)}{\partial x} \\ \frac{\partial^2 F}{\partial y\,\partial x} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y\,\partial z} & \frac{\partial \Psi_6(F)}{\partial y} \\ \frac{\partial^2 F}{\partial z\,\partial x} & \frac{\partial^2 F}{\partial z\,\partial y} & \frac{\partial^2 F}{\partial z^2} & \frac{\partial \Psi_6(F)}{\partial z} \\ \frac{\partial \Psi_6(F)}{\partial x} & \frac{\partial \Psi_6(F)}{\partial y} & \frac{\partial \Psi_6(F)}{\partial z} & 0 \end{vmatrix}$$

And $\Psi_{21}(F)$ is essentially the Jacobian determinant of the other three:

$$\Psi_{21}(F) = \frac{1}{14}\begin{vmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} & \frac{\partial F}{\partial z} \\ \frac{\partial \Psi_6(F)}{\partial x} & \frac{\partial \Psi_6(F)}{\partial y} & \frac{\partial \Psi_6(F)}{\partial z} \\ \frac{\partial \Psi_{14}(F)}{\partial x} & \frac{\partial \Psi_{14}(F)}{\partial y} & \frac{\partial \Psi_{14}(F)}{\partial z} \end{vmatrix}$$

The *invariant* $\Psi_0(F)$ can be obtained as follows. Consider the following differential operator.

$$D = \begin{vmatrix} \frac{\partial}{\partial x_1} & \frac{\partial}{\partial y_1} & \frac{\partial}{\partial z_1} \\ \frac{\partial}{\partial x_2} & \frac{\partial}{\partial y_2} & \frac{\partial}{\partial z_2} \\ \frac{\partial}{\partial x_3} & \frac{\partial}{\partial y_3} & \frac{\partial}{\partial z_3} \end{vmatrix}$$

Then

$$\Psi_0(F) = \frac{1}{5184} D^4(F(x_1, y_1, z_1)F(x_2, y_2, z_2)F(x_3, y_3, z_3))\,.$$

Alternatively, one can find an explicit formula in Salmon's book [Sal1879, p. 264], where he gives also a formula for the contravariant $\Psi_{-4}(F)$. We do not reproduce it here, but in Section 7.2 we will give the result for the special curves we will have to deal with.

(The covariants Ψ_j do not generate the $\mathbb{C}$-algebra of covariants, but they are all we will need. In fact, they do generate the specialization of the algebra of covariants for each ternary quartic $\mathrm{GL}_3(\mathbb{C})$-equivalent to $x^3y + y^3z + z^3x$.)

Let $F_0 = x^3y + y^3z + z^3x$ be the polynomial defining X. Each $g \in G \subset \mathrm{GL}_3(\mathbb{C})$ must act on F_0 as multiplication by a scalar, so there is a character $\chi\colon G \to \mathbb{C}^\times$ describing the action of G on F_0. But G is simple and nonabelian, so χ is trivial. In other words, F_0 belongs to $\mathbb{C}[x, y, z]^G$, the ring of G-invariants. For $j \in \{0, 4, 6, 14, 21\}$, let $\Phi_j = \Psi_j(F_0) \in \mathbb{C}[x, y, z]_j$. Since Ψ_j is a covariant, $\Phi_j \in \mathbb{C}[x, y, z]^G$. In fact, the Φ_j generate $\mathbb{C}[x, y, z]^G$ as a $\mathbb{C}$-algebra. Moreover, $\Phi_0 = 1$, the polynomials Φ_4, Φ_6, Φ_{14} are algebraically independent, and Φ_{21}^2 can

be expressed as a polynomial in the others. We give this relation modulo Φ_4, since this is all we need:

$$\Phi_{21}^2 - \Phi_{14}^3 \equiv -1728\,\Phi_0\Phi_6^7 \pmod{\Phi_4}. \tag{7.1}$$

Lemma 7.2. *If $F = F_0^g$ for some $g \in \mathrm{GL}_3(\mathbb{C})$, then*

$$\Psi_{21}(F)^2 - \Psi_{14}(F)^3 \equiv -1728\,\Psi_0(F)\Psi_6(F)^7 \pmod{F}.$$

Proof. Write $g = tg'$ with $t \in \mathbb{C}^\times$ and $g' \in \mathrm{SL}_3(\mathbb{C})$, and apply it to (7.1). The result follows, since the two sides of (7.2) are covariants of the same degree 24 and order 42. (This was the point of including the trivial factor Φ_0 in (7.2).) □

Lemma 7.3. *Let $F = F_0^g$ for some $g \in \mathrm{GL}_3(\mathbb{C})$. No two of $\Psi_6(F)$, $\Psi_{14}(F)$, $\Psi_{21}(F)$ vanish simultaneously at a point of the curve $F = 0$ in $\mathbb{P}^2_{\mathbb{C}}$.*

Proof. We may assume $F = F_0$, in which case the result is in [Kle1879, §6]: see [Elk99, p. 66]. □

7.2. **Equations for $X_E(7)$ and $X_E^-(7)$.** In order to use Corollary 6.2, we need explicit equations for the 26 curves described there. Halberstadt and Kraus [HK03] find an explicit equation for $X_E(7)$ in terms of the coefficients of E. If E is given as $Y^2 = X^3 + a\,X + b$, the equation is

$$a\,x^4{+}7b\,x^3z{+}3\,x^2y^2{-}3a^2\,x^2z^2{-}6b\,xyz^2{-}5ab\,xz^3{+}2\,y^3z{+}3a\,y^2z^2{+}2a^2\,yz^3{-}4b^2\,z^4 = 0\,. \tag{7.4}$$

The following result will let us deduce an equation for $X_E^-(7)$ from (7.4), using very little additional work.

Proposition 7.5. *If F is a ternary quartic form describing $X_{M'}(7)$, then $\Psi_{-4}(F)$ is a ternary quartic form describing $X_{M'}^-(7)$.*

Proof. Given M', the curve $X_{M'}(7)$ can be constructed as follows. Fix a symplectic isomorphism $\phi\colon M_{\overline{\mathbb{Q}}} \xrightarrow{\sim} M'_{\overline{\mathbb{Q}}}$. Then $\sigma \mapsto \xi_\sigma = \phi^{-1} \circ {}^\sigma\phi$ defines a 1-cocycle on $\mathcal{G}_{\mathbb{Q}}$ with values in $\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}})$. We have

$$\mathrm{Aut}_\wedge(M_{\overline{\mathbb{Q}}}) \twoheadrightarrow G = \mathrm{Aut}(X_{\overline{\mathbb{Q}}}) \hookrightarrow \mathrm{GL}_3(\overline{\mathbb{Q}}),$$

in which the last homomorphism is the 3-dimensional representation (V, ρ) of [Elk99, p. 54] giving the action of $\mathrm{Aut}(X_{\overline{\mathbb{Q}}})$ on the dual of the space of holomorphic differentials on X, and giving also the automorphisms of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ that restrict to the automorphisms of the canonically embedded curve $X_{\overline{\mathbb{Q}}}$. Under this composition, ξ maps to a cocycle $\bar{\xi}\colon \mathcal{G}_{\mathbb{Q}} \to \mathrm{GL}_3(\overline{\mathbb{Q}})$, which can be written as $\sigma \mapsto g^{-1} \cdot {}^\sigma g$ for some $g \in \mathrm{GL}_3(\overline{\mathbb{Q}})$, since $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, \mathrm{GL}_3) = 0$. If $\sim$ denotes "equal up to scalar multiple", then

$${}^\sigma\left(F_0^{g^{-1}}\right) = ({}^\sigma F_0)^{\left({}^\sigma g^{-1}\right)} = F_0^{\bar{\xi}_\sigma^{-1} g^{-1}} \sim F_0^{g^{-1}}$$

since $\bar{\xi}_\sigma^{-1}$ induces an automorphism of $X_{\overline{\mathbb{Q}}}$. Thus $F_0^{g^{-1}} = 0$ defines a twist X' of X in $\mathbb{P}^2$. The cocycle $\mathcal{G}_{\mathbb{Q}} \to \mathrm{Aut}(X_{\overline{\mathbb{Q}}})$ defining this twist (obtained from the isomorphism $X_{\overline{\mathbb{Q}}} \to X'_{\overline{\mathbb{Q}}}$ given

by g) is the same as the cocycle defining $X_{M'}(7)$, so $X' \simeq X_{M'}(7)$. After replacing F by F^b for some $b \in \mathrm{GL}_3(\mathbb{Q})$ (which we may do, without loss of generality), we have $F_0^{g^{-1}} \sim F$.

The element $\iota = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ defines an anti-symplectic automorphism of M over $\mathbb{Q}$. A calculation based on the explicit description of (V, ρ) in [Elk99, p. 54] shows that $\operatorname{Aut} M_{\overline{\mathbb{Q}}} \to \mathrm{GL}_3(\overline{\mathbb{Q}})$ is equivariant with respect to conjugation by ι on the left and $g \mapsto g^{-t}$ on the right. In particular, the image of G in $\mathrm{SL}_3(\overline{\mathbb{Q}})$ is stable under inverse transpose, so the contravariance of Ψ_{-4} implies that $\Psi_{-4}(F_0)$ is a G-invariant ternary quartic form. All such are multiples of F_0 [Elk99, pp.55–56], so $\Psi_{-4}(F_0) \sim F_0$.

Now we repeat the first paragraph of this proof using the anti-symplectic isomorphism $\phi\iota \colon M_{\overline{\mathbb{Q}}} \to M'_{\overline{\mathbb{Q}}}$ in place of ϕ, to construct $X^-_{M'}(7)$. The image of the cocycle

$$\sigma \mapsto (\phi\iota)^{-1} \circ {}^{\sigma}(\phi\iota) = \iota^{-1}\xi_\sigma\iota$$

under $\operatorname{Aut} M_{\overline{\mathbb{Q}}} \to \mathrm{GL}_3(\overline{\mathbb{Q}})$ is

$$\sigma \mapsto \bar{\xi}_\sigma^{-t} = \left(g^{-1} \cdot {}^{\sigma}g\right)^{-t} = h^{-1} \cdot {}^{\sigma}h,$$

where $h := g^{-t}$, so the polynomial defining $X^-_{M'}(7)$ is

$$F_0^{h^{-1}} \sim \Psi_{-4}(F_0)^{h^{-1}} \sim \Psi_{-4}(F_0^{h^t}) = \Psi_{-4}(F_0^{g^{-1}}) \sim \Psi_{-4}(F).$$

□

A formula for Ψ_{-4} is given in [Sal1879, p. 264]. Applying it to (7.4), we obtain an equation for $X^-_E(7)$:

$$\begin{aligned}(7.6)\quad & -a^2\,x^4 + a(3a^3 + 19b^2)\,y^4 + 3\,z^4 + 6a^2\,y^2z^2 + 6a\,z^2x^2 - 6(a^3 + 6b^2)\,x^2y^2 - 12ab\,y^2zx \\ & + 18b\,z^2xy + 2ab\,x^3y - 12b\,x^3z - 2(4a^3 + 21b^2)\,y^3z + 2a^2b\,y^3x - 8a\,z^3y = 0\end{aligned}$$

7.3. **Equations for the degree-168 morphism to $\mathbb{P}^1$.** Recall that each twist X' of $X = X(7)$ comes equipped with a canonical degree-168 morphism to $\mathbb{P}^1 = X(1)$ that is invariant under $\operatorname{Aut}(X'_{\overline{\mathbb{Q}}})$. The morphism with these properties is unique if we require that its branch points (with ramification indices 2, 3, 7) be at 1728, 0, ∞, respectively, on $\mathbb{P}^1$.

Lemma 7.7. *Let X' be a twist of X defined by a ternary quartic form F. Then the canonical morphism is*

$$\begin{aligned}\pi' : \qquad X' &\longrightarrow \mathbb{P}^1 \\ (x : y : z) &\longmapsto \frac{\Psi_{14}(F)^3}{\Psi_0(F)\,\Psi_6(F)^7}\,,\end{aligned}$$

where as usual we use the parameter j on $\mathbb{P}^1$.

Proof. We need only to check this for X, in which case it is (2.13) in [Elk99]. □

7.4. **The local test.** Let X' be a twist of the Klein quartic X. Then X' is given by an equation $F = 0$, where $F = F_0^g \in \mathbb{Q}[x, y, z]_4$ for some $g \in \mathrm{GL}_3(\overline{\mathbb{Q}})$. By Lemma 7.7, there is a morphism $\pi' \colon X' \to \mathbb{P}^1$, given by

$$(x : y : z) \mapsto \frac{\Psi_{14}(F)^3}{\Psi_0(F)\,\Psi_6(F)^7}\,.$$

We showed in Section 3.4 that every $(a, b, c) \in S(\mathbb{Z})$ maps to a point in $\pi'(X'(\mathbb{Q}))$ for some twist X' whose class in $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, G)$ is unramified outside 2, 3, and 7. Now suppose we have such a twist. Then π' extends to a morphism $X'_R \to \mathbb{P}^1_R$, so $\pi'(X'(\mathbb{Q})) = \pi'(X'(R)) \subseteq \mathbb{P}^1_R(R)$, and the corresponding solutions to $x^2 + y^3 = z^7$ will have $\gcd(x, y, z)$ divisible by at most primes in $\{2, 3, 7\}$. For each of the remaining primes $p = 2, 3, 7$, we search for residue classes that give rise to p-primitive solutions. (We say that (x, y, z) in $\mathbb{Z}^3$ or $\mathbb{Z}_p^3$ is *p-primitive* if at least one of x, y, z is not divisible by p.)

Let us define a *residue class* in $\mathbb{P}^2(\mathbb{Q}_p)$ to be a subset that, after permuting the homogeneous coordinates, equals $\{(1 : a + p^k u : b + p^l v) : u, v \in \mathbb{Z}_p\}$ for some fixed $a, b \in \mathbb{Z}_p$ and integers $k, l \geq 0$. We have an initial partition of $\mathbb{P}^2(\mathbb{Q}_p)$ into the three residue classes $(1 : \mathbb{Z}_p : \mathbb{Z}_p)$, $(p\mathbb{Z}_p : 1 : \mathbb{Z}_p)$ and $(p\mathbb{Z}_p : p\mathbb{Z}_p : 1)$. For each given residue class, we rewrite F in terms of u and v. If this expression has the form $p^e(\alpha + pF_1(u, v))$ with $\alpha \in \mathbb{Z}_p^\times$ and $e \in \mathbb{Z}$, then the residue class does not meet $X'(\mathbb{Q}_p)$, so we can discard it. Otherwise, we compute the covariants $\Psi_6(F)$, $\Psi_{14}(F)$ and $\Psi_{21}(F)$ in terms of u and v. The minimum of the p-adic valuations of the coefficients gives us a lower bound for the p-adic valuation of the covariants on our residue class, and if the constant term has the unique coefficient with minimal valuation, we even know the p-adic valuation of the corresponding covariant exactly. Let W_6, W_{14} and W_{21} be these lower bounds for $v_p(\Psi_6(F))$, $v_p(\Psi_{14}(F))$ and $v_p(\Psi_{21}(F))$, respectively, and let $w = v_p(1728\Psi_0(F))$.

One of the solutions to $a^2 + b^3 = c^7$ corresponding to the point $(x : y : z) \in X'(\mathbb{Q})$ is given by

$$a = (1728\Psi_0(F))^3\Psi_{21}(F)\,, \qquad b = -(1728\Psi_0(F))^2\Psi_{14}(F)\,, \qquad c = -1728\Psi_0(F)\Psi_6(F)\,,$$

evaluated at (x, y, z). This can be scaled to a p-primitive solution if and only if

$$\min\{v_p(a)/21, v_p(b)/14, v_p(c)/6\} \in \mathbb{Z}\,.$$

So we define

$$w_6 = (W_6 + 3w)/21\,, \qquad w_{14} = (W_{14} + 2w)/14\,, \qquad w_{21} = (W_{21} + w)/6\,.$$

If $\min\{w_6, w_{14}, w_{21}\}$ is an integer *and* the minimum comes from a covariant whose valuation on the residue class is known exactly, then there will be a p-adic point on X' giving rise to a p-primitive solution (at least if the given residue class contains a p-adic point on X', which we can check using Hensel's Lemma). In the same way, if $\min\{w_6, w_{14}, w_{21}\}$ is not an integer *and* the minimum comes from a covariant whose valuation on the residue class is known exactly, then no p-adic point in this residue class can produce a p-primitive solution. If the minimum comes only from a lower bound, we split the residue class into p (or p^2) subclasses

and repeat. In this way, we can decide fairly quickly whether any given twist gives rise to primitive solutions everywhere locally. If so, we say that "X' passes the local test."

This algorithm terminates, since by Lemma 7.3 no two of $\Psi_6(F)$, $\Psi_{14}(F)$ and $\Psi_{21}(F)$ vanish simultaneously on $X'(\mathbb{Q}_p)$.

7.5. **The list.** Putting together the twists coming from the reducible and irreducible cases, respectively, we obtained an initial finite list of twists. We then ran the local test on each of the curves. There are exactly 10 twists that pass the local test. They are given in Table 2. We have put some effort into simplifying these equations (trying to minimize the invariant $\Psi_0(F)$ and to reduce the size of the coefficients); the equations given are usually not those coming from formula (7.4) directly.

$$
\begin{aligned}
C_1&\colon 6x^3y + y^3z + z^3x = 0\\
C_2&\colon 3x^3y + y^3z + 2z^3x = 0\\
C_3&\colon 3x^3y + 2y^3z + z^3x = 0\\
C_4&\colon 7x^3z + 3x^2y^2 - 3xyz^2 + y^3z - z^4 = 0\\
C_5&\colon -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0\\
C_6&\colon x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 18xyz^2 + 9y^2z^2 - 9z^4 = 0\\
C_7&\colon -3x^4 - 6x^3z + 6x^2y^2 - 6x^2yz + 15x^2z^2 - 4xy^3 - 6xyz^2 - 4xz^3 + 6y^2z^2 - 6yz^3 = 0\\
C_8&\colon 2x^4 - x^3y - 12x^2y^2 + 3x^2z^2 - 5xy^3 - 6xy^2z + 2xz^3 - 2y^4 + 6y^3z + 3y^2z^2 + 2yz^3 = 0\\
C_9&\colon 2x^4 + 4x^3y - 4x^3z - 3x^2y^2 - 6x^2yz + 6x^2z^2 - xy^3 - 6xyz^2 - 2y^4 + 2y^3z\\
&\qquad - 3y^2z^2 + 6yz^3 = 0\\
C_{10}&\colon x^3y - x^3z + 3x^2z^2 + 3xy^2z + 3xyz^2 + 3xz^3 - y^4 + y^3z + 3y^2z^2 - 12yz^3 + 3z^4 = 0
\end{aligned}
$$

TABLE 2. Equations for the plane quartic curves C_1 through C_{10}.

Curves C_1, C_2, and C_3 come from the case that $E[7]$ is reducible. As it happens, they all correspond to twists that involve only the cyclic subgroup of order 7. Curves C_4 through C_{10} are of the form $X_E(7)$ for $E = 27\text{A}1$, $96\text{A}1$, $288\text{A}1$, $864\text{A}1$, $864\text{B}1$, $864\text{C}1$, $54\text{A}2$, respectively. (The curve C_{10} is also $X_E^-(7)$ for $E = 54\text{A}1$, because 54A1 and 54A2 are 3-isogenous, and 3 is not a square modulo 7.)

7.6. **Local conditions for C_5.** If $P_1, P_2 \in \mathbb{P}^2(\mathbb{Q}_p)$ then we write "$P_1 \equiv P_2 \pmod p$" to mean that the images of P_1 and P_2 under the reduction map $\mathbb{P}^2(\mathbb{Q}_p) = \mathbb{P}^2(\mathbb{Z}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ are equal. Define

$$
\begin{aligned}
C_5(\mathbb{Q}_2)_{\text{subset}} &:= \{\, P \in C_5(\mathbb{Q}_2) : P \equiv (1:0:0) \text{ or } (1:1:1) \pmod 2 \,\}\\
C_5(\mathbb{Q}_3)_{\text{subset}} &:= \{\, P \in C_5(\mathbb{Q}_3) : P \equiv (0:1:0) \pmod 3 \,\}\\
C_5(\mathbb{Q})_{\text{subset}} &:= \{\, P \in C_5(\mathbb{Q}) : P \in C_5(\mathbb{Q}_2)_{\text{subset}} \text{ and } P \in C_5(\mathbb{Q}_3)_{\text{subset}} \,\}.
\end{aligned}
$$

Lemma 7.8. *Let p be 2 or 3. If $P \in C_5(\mathbb{Q}_p)$ and the image of P in $\mathbb{P}^1(\mathbb{Q}_p)$ is in $j(S(\mathbb{Z}_p))$, then $P \in C_5(\mathbb{Q}_p)_{\text{subset}}$.*

Proof. We do the computations for the "local test", keeping track of the residue classes that are not excluded. For example, when $p = 3$, the reduction mod 3 of the equation $F_5 = 0$ of C_5 is

$$(x - z)(x^2y + y^2z + xyz + xz^2 + yz^2) = 0\,,$$

which describes a line and a cuspidal cubic intersecting at the cusp $(0 : 1 : 0)$. The invariant $\Psi_0(F_5)$ equals -24, so in the notation of Section 7.4, $w = 4$. For all residue classes corresponding to smooth points on the reduction, we find that the minimum of w_6, w_{14} and w_{21} is determined and non-integral. So $(0 : 1 : 0)$ is the only residue class that may contain points leading to 3-primitive solutions. The argument for $p = 2$ is similar. □

Because of Lemma 7.8, it will suffice to determine $C_5(\mathbb{Q})_{\text{subset}}$ instead of $C_5(\mathbb{Q})$. Eventually we will prove $C_5(\mathbb{Q})_{\text{subset}} = \emptyset$.

8. Known rational points on the 10 curves

For the remainder of the proof, all we need to retain from Sections 3–7 are the equations for C_1 through C_{10}, the local conditions for C_5 given by Lemma 7.8, and the formula in Lemma 7.7. (The latter is needed only to recover the solutions to $x^2 + y^3 = z^7$ from the relevant rational points on the 10 curves).

Table 3 gives the rank of the Mordell-Weil group of the Jacobian of each curve (these numbers will be proved correct in Section 11), and lists rational points on C_1 through C_{10} discovered by a naïve search. We will prove that the list is complete for each curve except possibly C_5.[4] For C_5, we will prove instead that $C_5(\mathbb{Q})_{\text{subset}} = \emptyset$, which will suffice for our purposes. Then Theorem 1.1 will follow.

For each rational point, Table 3 next gives the corresponding value of $j\colon C_i \to \mathbb{P}^1$ calculated by Lemma 7.7. If $j \notin \{1728, 0, \infty\}$, it gives also the Cremona label [Cre] for an elliptic curve of that j-invariant, and all primitive solutions (a, b, c) to $a^2 + b^3 = c^7$ with $1728\,b^3/c^7 = j$. If the conductor N is out of the range of Cremona's database, we use $N*$ as a substitute for the Cremona label.

Remark 8.1. The last two points on C_6 are interchanged by the involution $z \mapsto -z$ of C_6, and hence map to the same j-invariant.

9. Overview of the strategy for determining the rational points

In order to determine the sets of rational points on $C_1, \ldots, C_{10}$, we will need to determine the Mordell-Weil ranks of their corresponding Jacobians $J_1, \ldots, J_{10}$ over $\mathbb{Q}$. The curves C_1, C_2 and C_3 are μ_7-twists of X rather than more general twists. So there are more methods available for dealing with them than for the other curves.

[4] Almost certainly the list is complete for C_5 too, since Noam Elkies ran an algorithm based on his paper [Elk00] to prove that there are no additional points $(x : y : z)$ with integer homogeneous coordinates satisfying $|x|, |y|, |z| \le 10^7$.

	Rank	Points	j-invariant	Cremona	Primitive solutions
C_1	1	$(1:0:0)$	∞		$(\pm1,-1,0)$
		$(0:1:0)$	∞		$(\pm1,-1,0)$
		$(0:0:1)$	∞		$(\pm1,-1,0)$
		$(1:-1:2)$	$-13^3221173^32^{-2}3^{-1}43^{-7}$	258F2	—
C_2	1	$(1:0:0)$	∞		$(\pm1,-1,0)$
		$(0:1:0)$	∞		$(\pm1,-1,0)$
		$(0:0:1)$	∞		$(\pm1,-1,0)$
		$(1:1:-1)$	$-7^42^{-1}3^{-1}$	294A1	—
		$(1:-2:-1)$	$-13^326293^32^{-2}3^{-1}113^{-7}$	678D2	—
C_3	1	$(1:0:0)$	∞		$(\pm1,-1,0)$
		$(0:1:0)$	∞		$(\pm1,-1,0)$
		$(0:0:1)$	∞		$(\pm1,-1,0)$
		$(1:1:-1)$	$-7^344647^32^{-1}3^{-1}29^{-7}$	174B2	—
C_4	2	$(1:0:0)$	0		$(\pm1,0,1)$
		$(0:1:0)$	0		$(\pm1,0,1)$
		$(0:1:1)$	$-2^{15}3\cdot5^3$	27A2	—
C_5	3	$(1:0:0)$	$2^613^33^{-1}$	96A2	—
		$(0:1:0)$	$2^323^33^{-4}$	96A4	—
		$(0:0:1)$	$2^397^33^{-1}$	96A3	—
		$(1:1:1)$	$2^67^33^{-2}$	96A1	—
C_6	2	$(0:1:0)$	2^63^3		$\pm(0,1,1)$
		$(1:-1:0)$	2^63^3		$\pm(0,1,1)$
		$(0:1:1)$	$2^93^311^3421^3113^{-7}$	32544B1	$(\pm15312283,9262,113)$
		$(0:1:-1)$	$2^93^311^3421^3113^{-7}$	32544B1	$(\pm15312283,9262,113)$
C_7	2	$(0:1:0)$	-2^33^3	864A1	—
		$(0:0:1)$	$2^93^37^3101^35^{-7}13^{-7}$	56160H1	$(\pm2213459,1414,65)$
		$(0:1:1)$	$-2^63^313^35867^317^{-7}$	14688D1	$(\pm21063928,-76271,17)$
C_8	2	$(0:0:1)$	-2^93^3	864B1	$(\pm3,-2,1)$
		$(2:-1:0)$	$2^33\cdot547^366029^3977^{-7}$	844128*	—
C_9	2	$(0:0:1)$	2^93	864C1	—
		$(1:1:0)$	$2^33^9163^38779^37^{-7}79^{-7}$	477792*	—
C_{10}	2	$(1:0:0)$	$-3^317^32^{-1}$	54A3	$(\pm71,-17,2)$
		$(1:1:0)$	$-3\cdot73^32^{-9}$	54A2	—

TABLE 3. Known rational points on C_1 through C_{10}.

First observe that each of these three curves is a Galois cover of $\mathbb{P}^1$, over $\mathbb{Q}$, with Galois group μ_7; in fact, C_1, C_2 and C_3 are birational to the (singular) projective plane curves

$$u^7 = v^2(6\,v - w)w^4\,, \qquad u^7 = v^2(18\,v - w)w^4 \quad \text{and} \quad u^7 = v^2(12\,v - w)w^4\,,$$

respectively. To see this, rescale and/or permute the variables to obtain an equation of the form $x^3y + y^3z + A\,z^3x = 0$ (with $A = 6, 18, 12$); then $(u : v : w) = (xyz : -z^3 : x^2y)$ does the transformation.

The curves (and their Jacobians) are therefore amenable to the techniques developed by Schaefer [Sch98] and Poonen and Schaefer [PS97]: the Jacobians have complex multiplication by $\mathbb{Z}[\zeta]$. We will do a $1-\zeta$ descent for each of these Jacobians.

For $C_4, \ldots, C_{10}$, we need to develop a new method of determining the Mordell-Weil ranks of their Jacobians over $\mathbb{Q}$. We do this in Section 11.

For the curves $C_1, \ldots, C_{10}$ other than C_5, the rank of $J_i(\mathbb{Q})$ is less than 3, the dimension of J_i. In each case, a combination of Chabauty and Mordell-Weil sieve computations determines the set of rational points (see Section 12). For C_5, the rank of $J_5(\mathbb{Q})$ is 3, so we will deal with that curve separately in Section 13.1.

10. $(1-\zeta)$-descent on J_1, J_2, and J_3

We now do a descent using the endomorphism $1-\zeta$ of J_i over $L := \mathbb{Q}(\zeta)$ for $i = 1, 2, 3$. See [Sch98] and [PS97] for details. The descent map is given by the function $f = v/w$ and takes values in

$$H = L(\{2,3,7\},7) = \{\theta \in L^\times/L^{\times 7} : L(\sqrt[7]{\theta})/L \text{ is unramified outside } \{2,3,7\}\}\,.$$

The group H is an $\mathbb{F}_7$-vector space of dimension 7.

For each prime $\mathfrak{p}$ of L, let $\rho_\mathfrak{p}$ be the composition $H \hookrightarrow L^\times/L^{\times 7} \to L_\mathfrak{p}^\times/L_\mathfrak{p}^{\times 7}$. Let $\pi = 1-\zeta \in L$. Let $\mathfrak{q}$ be a prime of L above 2. For each i, we found that

$$\rho_\pi^{-1} f\left(\frac{J_i(L_\pi)}{(1-\zeta)J_i(L_\pi)}\right) \cap \rho_\mathfrak{q}^{-1} f\left(\frac{J_i(L_\mathfrak{q})}{(1-\zeta)J_i(L_\mathfrak{q})}\right) = \langle 2,3\rangle \subset H;$$

in particular the intersection is of dimension 2. In addition, we found two independent elements in $J_i(L)/(1-\zeta)J_i(L)$. Therefore, the Selmer group $S^{1-\zeta}(L, J_i)$ and $J_i(L)/(1-\zeta)J_i(L)$ are of dimension 2. Since $\dim J_i(L)[1-\zeta] = 1$, the rank of $J_i(\mathbb{Q})$ is 1.

For $i = 1, 2, 3$ and $\mathfrak{p} \in \{\pi, \mathfrak{q}\}$, we found a basis of $J_i(L_\mathfrak{p})/(1-\zeta)J_i(L_\mathfrak{p})$ consisting of divisor classes of the form $[P - \infty]$ or $[P + \overline{P} - 2\infty]$ where ∞ is the single point with $w = 0$ and P is defined over $L_\mathfrak{p}$, or P is defined over a quadratic extension of $L_\mathfrak{p}$ and $\overline{P}$ is its conjugate. In Table 4 we describe each such divisor class by giving the value of v/w at P. The last column of Table 4 does the same for $J_i(L)/(1-\zeta)J_i(L)$.

For each i, we have $J_i[1-\zeta] \subseteq J_i(\mathbb{Q})$ and $\dim J(\mathbb{Q})[7] = 1$, so $\dim J_i(\mathbb{Q})/7J_i(\mathbb{Q}) = 2$. We will use this in Section 11.2.

10.1. **Side application to twists of the degree-7 Fermat curve.** Our calculation of $C_1(\mathbb{Q})$, $C_2(\mathbb{Q})$, $C_3(\mathbb{Q})$ will have consequences for rational points on certain curves $c_1X^7 + c_2Y^7 + c_3Z^7 = 0$ in $\mathbb{P}^2$. These are not needed for the proof of our main theorem, but are of interest in their own right.

A rational point on a curve

$$u^7 = v^2(Av - w)w^4\,,$$

i	$\dfrac{J_i(L_\pi)}{(1-\zeta)J_i(L_\pi)}$	$\dfrac{J_i(L_\mathfrak{q})}{(1-\zeta)J_i(L_\mathfrak{q})}$	$\dfrac{J_i(L)}{(1-\zeta)J_i(L)}$
1	0 $(3+6\pi^3+2\pi^4)/6^5$ $(3+\pi^3+5\pi^4+\pi^5)/6^5$ $\pi^7(1+5\pi^6+5\pi^7)/6^5$	$-1/2$	0 $-1/2$
2	$1/27$ $\pi^7(1+3\pi^7)/864$ $(4+\pi^4)/864$ $(4+\pi^4+\pi^5)/864$	$1/27$	0 $1/27$
3	0 $\pi^7(1+\pi^6)/1944$ $(3+\sqrt{3}\pi^3+\pi^4/\sqrt{3})/1944$ $(2+\pi^{3/2}+\pi^{5/2}+3\pi^3+\pi^{7/2}$ $-\pi^4+\pi^{9/2}+2\pi^5+2\pi^6)/1944$	$1/8$	0 $1/8$

TABLE 4. Data needed for $(1-\zeta)$-descents for C_1, C_2 and C_3.

---

can be represented by $u, v, w \in \mathbb{Z}$ with $\gcd(v, w) = 1$. Then $\gcd(v, Av - w) = 1$; therefore there exist integers a, b, r, s, t such that

$$v = r^7\,, \quad Av - w = as^7\,, \quad w = bt^7,$$

and ab^4 is a 7^{th} power, and a and b are divisible only by primes dividing A. Therefore, we obtain a point on the covering curve

$$A\,r^7 - a\,s^7 - b\,t^7 = 0\,.$$

Conversely, a rational point on this curve maps down to a rational point on the original curve.

Section 12 determines the rational points on $u^7 = v^2(Av - w)w^4$ for $A = 6, 12, 18$. Assuming this, we can list the rational points on the covering curves arising from these. After simplifying their equations (by multiplying by constants, and making the coefficients 7^{th}-power free), and eliminating those that over some $\mathbb{Q}_p$ fail to have points, we obtain the following:

Corollary 10.1. *The following curves in $\mathbb{P}^2_{\mathbb{Q}}$ have $\mathbb{Q}_p$-points for all $p \le \infty$, but the only rational points are the ones with $X, Y, Z \in \{-1, 0, 1\}$:*

$$X^7 + Y^7 + 12\,Z^7 = 0\,, \quad X^7 + Y^7 + 18\,Z^7 = 0\,, \quad X^7 + Y^7 + 48\,Z^7 = 0\,,$$
$$X^7 + Y^7 + 144\,Z^7 = 0\,, \quad X^7 + Y^7 + 162\,Z^7 = 0\,, \quad X^7 + Y^7 + 324\,Z^7 = 0\,,$$
$$X^7 + 2\,Y^7 + 3\,Z^7 = 0\,, \quad X^7 + 2\,Y^7 + 81\,Z^7 = 0\,, \quad X^7 + 3\,Y^7 + 4\,Z^7 = 0\,,$$
$$X^7 + 3\,Y^7 + 16\,Z^7 = 0\,, \quad X^7 + 4\,Y^7 + 9\,Z^7 = 0\,, \quad X^7 + 9\,Y^7 + 16\,Z^7 = 0\,,$$
$$X^7 + 16\,Y^7 + 81\,Z^7 = 0.$$

11. 2-descent on Jacobians of twists of X

11.1. **Theory.** To compute the ranks of $J_4(\mathbb{Q}), \ldots, J_{10}(\mathbb{Q})$, we will use the 2-descent described in this section. It is similar to the descent described in [PS97].

The Klein quartic X has 24 Weierstrass points, each of weight 1 (ordinary flexes). These can be partitioned into eight sets of three with the following property. Choose one set of three and denote the points W_1, W_2, W_3. The tangent line at W_i intersects X with multiplicity 3 at W_i and multiplicity 1 at W_{i+1} (with subscripts considered modulo 3). We will call such a set of three Weierstrass points a *triangle*. The set of eight triangles is a Galois-stable set.

By abuse of notation, let T_i denote both a triangle and the effective degree-3 divisor that is the sum of its points. For $1 \leq i < j \leq 8$, we can find a function with divisor $2T_i - 2T_j$ whose numerator and denominator are cubics. Therefore the divisor class $[T_i - T_j]$ is killed by 2. Since the points in each T_i are not collinear, an application of the Riemann-Roch theorem shows that $T_i - T_j$ is not principal. Thus the order of $[T_i - T_j]$ is exactly two.

Proposition 11.1. *The $[T_i - T_1]$ for $i = 1, \ldots, 8$ sum to 0, and any six of them with $i \neq 1$ form a basis for* $\mathrm{Jac}(X)[2]$. *Let $Q_1 = [\sum_{i=1}^{8} a_i T_i]$ and $Q_2 = [\sum_{i=1}^{8} b_i T_i]$ with $\sum a_i = \sum b_i = 0$. Let e_2 be the 2-Weil pairing. Then $e_2(Q_1, Q_2) = (-1)^{\sum_{i=1}^{8} a_i b_i}$.*

Proof. Over some finite and totally ramified extension K of $\mathbb{Q}_7$, the Klein quartic X acquires good reduction and has all its automorphisms defined. So if O_K is the valuation ring of K, then X extends to a smooth curve over O_K. The special fiber X_s is the hyperelliptic curve branched above the eight points in $\mathbb{P}^1(\mathbb{F}_7)$. Then $\mathrm{Aut}(X)$ injects into $\mathrm{Aut}(X_\mathrm{s})$ and injects into the automorphism group of $\mathbb{P}^1_{\mathbb{F}_7}$, which is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_7)$ (see [Elk99]). At a Weierstrass point W_i of X, there is a regular differential vanishing to order 3 (it corresponds to the tangent line in the canonical model). One can scale the differential by an element of K so that it extends to a regular differential on the model X over O_K, and reduces to a nonzero differential on X_s, vanishing at least to order 3 at the reduction of the point. This means that Weierstrass points of X reduce to Weierstrass points of the hyperelliptic curve X_s.

The differential in characteristic 0 has divisor $3W_i + W_{i+1}$, where W_i, W_{i+1} are two points in a triangle. The reduction must be $3W_i' + W_{i+1}'$ where W_i', W_{i+1}' are Weierstrass points. But the only possibility for W_{i+1}' that makes this the divisor of a differential on the hyperelliptic curve is $W_{i+1}' = W_i'$. Repeating this argument shows that the points of a triangle all reduce to the same Weierstrass point on X_s. Applying the automorphisms, and using the fact that $\mathrm{PSL}_2(\mathbb{F}_7)$ acts transitively on the set $\mathbb{P}^1(\mathbb{F}_7)$ of hyperelliptic branch points for X_s, shows that the eight triangles reduce to the eight Weierstrass points on X_s. Now the 2-torsion point $[T_i - T_j]$ reduces to the 2-torsion point $[3P_i - 3P_j] = [P_i - P_j]$ where P_i (for example) is the reduction of any point in T_i. The map $\mathrm{Jac}(X)[2] \to \mathrm{Jac}(X_\mathrm{s})[2]$ is an isomorphism of groups preserving the Weil pairing, because X has good reduction.

The desired statements for X and the T_i now follow from their analogues for the genus-3 hyperelliptic curve X_s and its Weierstrass points, which are well known (cf. Propositions 6.2 and 7.1 in [PS97]). □

This correspondence between X with its T_i and a genus-3 hyperelliptic curve with its Weierstrass points will enable us to translate many of the results in [PS97] to our situation. That article involves descent on cyclic covers of the projective line using ramification points of the covering. For hyperelliptic curves, these are the Weierstrass points. In this section, for brevity, we will sometimes cite an equivalent proof in [PS97] which is easily translated. First we need to find a function corresponding to the $x - T$ map in [PS97].

Let C be a twist of X with a rational point $P \in C(\mathbb{Q})$. In addition, assume that for each triangle T_i, there is a cubic whose intersection divisor with C is $2T_i + 3P + R_i$ where R_i is an effective divisor of degree 3, defined over $\mathbb{Q}$ and supported on three non-collinear $\overline{\mathbb{Q}}$-points. A calculation shows that this holds for $C_4, \ldots, C_{10}$. Let J be the Jacobian of C.

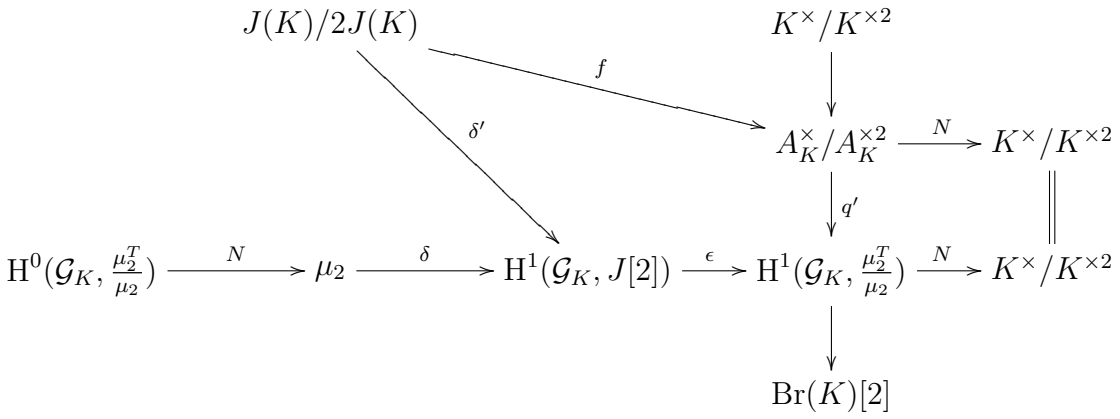
Choose functions $f_1, \ldots, f_8$ with $\mathrm{div}(f_i) = 2T_i + 3P + R_i - 3\Omega$ (where Ω is a canonical divisor defined over $\mathbb{Q}$) and such that if $\sigma \in \mathcal{G}_\mathbb{Q}$, and ${}^\sigma T_i = T_j$ then ${}^\sigma f_i = f_j$. Then $\mathrm{div}(f_i/f_j) = 2T_i - 2T_j + R_i - R_j$. Since $2T_i - 2T_j$ is principal, so is $R_i - R_j$. The R_i are effective, of degree 3, and are supported on three non-collinear points. The Riemann-Roch theorem then implies that $R_i = R_j$. Let R be the common value of the R_i.

Let $T = \{T_i\}_{i=1}^8$. Let K be $\mathbb{Q}$ or $\mathbb{Q}_p$ (we allow $p = \infty$, in which case $\mathbb{Q}_p := \mathbb{R}$). Let $\overline{A}_K$ be the algebra of maps from T to $\overline{K}$. The group $\mathcal{G}_K$ acts on $\overline{A}_K$ through its action on T and $\overline{K}$. Let A_K be the algebra of $\mathcal{G}_K$-invariants in $\overline{A}_K$; it is isomorphic as K-algebra to a product of finite extensions of K corresponding to the $\mathcal{G}_K$-orbits of T. We call D a *good divisor* if it is a divisor of degree 0, defined over K, whose support is disjoint from the support of $\mathrm{div}(f_i)$ for every i. If D is a good divisor, then we define $f(D) = (T_i \mapsto f_i(D))$. Then f is a homomorphism from the group of good divisors to $A_K^\times$. The divisor of each f_i is the sum of a double and a $\mathbb{Q}$-rational divisor. So by Weil reciprocity, f sends good principal divisors to $A_K^{\times 2} K^\times$. Since C has a rational point, every element of $J(K)$ is represented by a good divisor. Therefore, f induces a well-defined homomorphism $f\colon J(K)/2J(K) \to A_K^\times / A_K^{\times 2} K^\times$. In order to determine the kernel and image of this map, it will help to find a cohomological interpretation of it.

Let μ_2^T be the 2-torsion in $\overline{A}_K^\times$; it equals the $\mathcal{G}_K$-module of maps from T to μ_2. Let μ_2^T/μ_2 be the quotient by the set of constant maps. Let q be the canonical surjection $\mu_2^T \to \mu_2^T/\mu_2$. Define $\epsilon\colon J[2] \to \mu_2^T/\mu_2$ by $\epsilon(Q) = (T_i \mapsto e_2(Q, [T_i - T_1]))$. Let $N\colon \mu_2^T \to \mu_2$ be the restriction of the norm map $\overline{A}_K \to \overline{K}$. A straightforward computation involving Proposition 11.1 shows that the following is a commutative diagram of $\mathcal{G}_K$-modules with exact rows and columns.

$$\begin{array}{ccccccccc}
 & & & & \mu_2 & & & & \\
 & & & & \downarrow & & & & \\
 & & & & \mu_2^T & \xrightarrow{N} & \mu_2 & \longrightarrow & 1 \\
 & & & & \downarrow{\scriptstyle q} & & \| & & \\
0 & \longrightarrow & J[2] & \xrightarrow{\epsilon} & \dfrac{\mu_2^T}{\mu_2} & \xrightarrow{N} & \mu_2 & \longrightarrow & 1
\end{array}$$

We now compute the long exact sequences of $\mathcal{G}_K$-cohomology for the rows and columns. Since $\mathrm{H}^1(\mathcal{G}_K, \overline{K}^\times)$ and $\mathrm{H}^1(\mathcal{G}_K, \overline{A}_K^\times)$ are both 0, we have $\mathrm{H}^1(\mathcal{G}_K, \mu_2) \simeq K^\times/K^{\times 2}$ and $\mathrm{H}^1(\mathcal{G}_K, \mu_2^T) \simeq A_K^\times/A_K^{\times 2}$ by Kummer isomorphisms. We obtain the following diagram with exact rows and columns.



The map q' is the composition of the Kummer isomorphism of $A_K^\times/A_K^{\times 2}$ with $\mathrm{H}^1(\mathcal{G}_K, \mu_2^T)$ and the map induced by q. The map δ' comes from taking cohomology of

$$0 \longrightarrow J[2] \longrightarrow J \xrightarrow{2} J \longrightarrow 0.$$

Proposition 11.2. *The maps $\epsilon \circ \delta'$ and $q' \circ f$ are the same as maps from $J(K)/2J(K)$ to $\mathrm{H}^1(\mathcal{G}_K, \mu_2^T/\mu_2)$ (i.e., the diagram above commutes).*

Proof. Pick an element of $J(K)$. Since C has a rational point, that element is represented by a good divisor D. Pick $D' \in \operatorname{Div} C_{\overline{K}}$ whose support is disjoint from the supports of the $\operatorname{div}(f_i)$ and such that $2[D'] = [D]$. Then $\delta'([D])$ is the class of the cocycle $\sigma \mapsto [{}^\sigma D' - D']$ in $\mathrm{H}^1(\mathcal{G}_K, J[2])$. So $\epsilon \circ \delta'([D])$ is the class of the cocycle $\xi_\sigma := (T_i \mapsto e_2([{}^\sigma D' - D'], [T_i - T_1]))$ in $\mathrm{H}^1(\mathcal{G}_K, \mu_2^T/\mu_2)$. Let g be a function, defined over $K(D')$, whose divisor is $2D' - D$. Then $\operatorname{div}({}^\sigma g/g) = 2({}^\sigma D' - D')$. We also have $\operatorname{div}(f_i/f_1) = 2(T_i - T_1)$. By definition,

$$e_2([{}^\sigma D' - D'], [T_i - T_1]) = \frac{(f_i/f_1)({}^\sigma D' - D')}{({}^\sigma g/g)(T_i - T_1)}.$$

Therefore, we have

$$\xi_\sigma = \left(T_i \mapsto \frac{(f_i/f_1)({}^\sigma D' - D')}{({}^\sigma g/g)(T_i - T_1)}\right).$$

For each i, the divisor $E = 2T_i - \operatorname{div}(f_i)$ is the same. Let $l = \sqrt{g(E)}$. By Weil reciprocity, the square of $\eta_\sigma := f_1({}^\sigma D' - D')({}^\sigma g/g)(-T_1)\, {}^\sigma l/l$ is 1, so $\eta_\sigma \in \mu_2$. Since ξ_σ is in the quotient μ_2^T/μ_2, we can multiply the expression for ξ_σ by the constant map $(T_i \mapsto \eta_\sigma)$ to get

$$\xi_\sigma = \left(T_i \mapsto \frac{f_i({}^\sigma D' - D'){}^\sigma l/l}{({}^\sigma g/g)(T_i)}\right) = (T_i \mapsto {}^\sigma\nu/\nu)$$

where $\nu = f_i(D')l/g(T_i)$. Now

$$\nu^2 = \frac{f_i(2D')}{g(2T_i - E)} = \frac{f_i(\operatorname{div}(g) + D)}{g(\operatorname{div}(f_i))} = f_i(D)$$

by Weil reciprocity. It follows that ξ_σ is the image of $f(D)$ under q', since q' is the composition of the Kummer map $A_K^\times/A_K^{\times 2} \to \mathrm{H}^1(\mathcal{G}_K, \mu_2^T)$ and q, the map induced by the quotient map. □

Proposition 11.3. *We have $\delta'([R-3P]) = \delta(-1)$.*

Proof. By definition of $R = R_1$, $2T_1+3P+R$ is the intersection of C with a cubic, and hence is linearly equivalent to the intersection of C with any other cubic, which we may take to be the union of the tangent lines at the three points of T_1. Thus $[2T_1 + 3P + R] = [4T_1]$, so $[R-3P] = [2T_1-6P]$. Therefore $\delta'([R-3P])$ is the class including the cocycle $(\sigma \mapsto [{}^\sigma T_1 - T_1])$ in $\mathrm{H}^1(\mathcal{G}_K, J[2])$. From Proposition 11.1, we have $\epsilon([{}^\sigma T_1 - T_1]) = {}^\sigma M - M \in \mu_2^T$ where M is the map sending T_1 to 1 and T_i to -1 for $i > 1$. Also $N(M) = -1$. Hence, by definition, $\delta(-1)$ is the class of the cocycle $(\sigma \mapsto [{}^\sigma T_1 - T_1])$ in $\mathrm{H}^1(\mathcal{G}_K, J[2])$. □

Proposition 11.4. *The kernel of $f\colon J(K)/2J(K) \to A_K^\times/A_K^{\times 2}K^\times$ is generated by $[R-3P]$. This element is trivial in $J(K)/2J(K)$ if and only if the $\mathcal{G}_K$-set T has an orbit of odd size.*

Proof. The maps $\delta'\colon J(K)/2J(K) \to \mathrm{H}^1(\mathcal{G}_K, J[2])$ and $q'\colon A_K^\times/A_K^{\times 2}K^\times \to \mathrm{H}^1(\mathcal{G}_K, \mu_2^T/\mu_2)$ are injective. By Propositions 11.2 and 11.3,

$$\ker f = (\delta')^{-1}(\ker \epsilon) = (\delta')^{-1}(\delta(\mu_2)) = (\delta')^{-1}(\delta'(\langle [R-3P] \rangle)) = \langle [R-3P] \rangle,$$

The proof of the second half of the proposition is essentially identical to the proof of [PS97, Lemma 11.2]. □

To simplify notation, we let $A = A_{\mathbb{Q}}$ and $A_p = A_{\mathbb{Q}_p}$. In Section 11.2.1 we will show how to compute the $\mathcal{G}_{\mathbb{Q}}$-orbits of T; it will turn out that for each of $C_4, \ldots, C_{10}$, there is no orbit of odd size. Therefore, the kernel of the map f from $J(\mathbb{Q})/2J(\mathbb{Q})$ to $A^\times/A^{\times 2}\mathbb{Q}^\times$ has size 2 and is generated by $[R-3P]$.

Let $A \simeq \prod A_i$ where the A_i are number fields. Let p be a prime of $\mathbb{Q}$. Let a be an element of $A^\times$ and a_i its image in A_i. We say that $a \in A^\times/A^{\times 2}$ is unramified at p if for each i, the field extension $A_i(\sqrt{a_i})/A_i$ is unramified at primes over p. Let S be a set of places of $\mathbb{Q}$ including 2, the infinite prime, and all primes at which J has bad reduction excluding the odd primes at which the Tamagawa number is odd. Let $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S$ be the image in $A^\times/A^{\times 2}\mathbb{Q}^\times$ of the elements of $A^\times/A^{\times 2}$ that are unramified outside of primes in S.

Denote by H the kernel of the norm from $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S$ to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

Proposition 11.5. *The image of $f\colon J(\mathbb{Q}) \to A^\times/A^{\times 2}\mathbb{Q}^\times$ is contained in H.*

Proof. The divisor of f is the sum of the double of a divisor and a rational divisor. This was the condition necessary for the proofs of the essentially identical results in [PS97, Props. 12.1 & 12.4]. The exclusion of primes with odd Tamagawa numbers is explained in [SS04, Prop. 3.2]. □

Let p be a prime of $\mathbb{Q}$, finite or infinite. We have the following commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q})/\ker(f) & \xrightarrow{f} & H \\ \downarrow & & \downarrow \rho_p \\ J(\mathbb{Q}_p)/\ker(f_p) & \xrightarrow{f_p} & A_p^\times/A_p^{\times 2}\mathbb{Q}_p^\times \end{array}$$

where f_p is the map f for the case $K = \mathbb{Q}_p$, and ρ_p is the composition $H \hookrightarrow A^\times/A^{\times 2}\mathbb{Q}^\times \to A_p^\times/A_p^{\times 2}\mathbb{Q}_p^\times$.

Recall that the 2-Selmer group $\mathrm{Sel}^2(J,\mathbb{Q})$ is the set of elements in $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, J[2])$, unramified outside S, which map to the image of $J(\mathbb{Q}_p) \to \mathrm{H}^1(\mathcal{G}_{\mathbb{Q}_p}, J[2])$ for all $p \in S$. Define the *fake* 2-*Selmer group* to be

$$\mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q}) = \{\theta \in H \mid \rho_p(\theta) \in f(J(\mathbb{Q}_p)) \text{ for all } p \in S\}.$$

Proposition 11.6. *The sequence* $\mu_2 \xrightarrow{\delta} \mathrm{Sel}^2(J,\mathbb{Q}) \xrightarrow{\epsilon} \mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q}) \to 0$ *is exact.*

Proof. See the proof of [PS97, Thm. 13.2]. □

For the curves $C_4, \ldots, C_{10}$, we find that $\delta'([R-3P])$ is nonzero. By Propositions 11.3 and 11.6, $\dim_{F_2} \mathrm{Sel}^2(J,\mathbb{Q}) = 1 + \dim_{\mathbb{F}_2} \mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q})$.

To compute $\mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q})$, we first find A. Let Λ be a subset of $\{1,\ldots,8\}$ such that the set $\{T_j\}_{j\in\Lambda}$ contains one representative of each $\mathcal{G}_\mathbb{Q}$-orbit of T. Let $A_j = \mathbb{Q}(T_j)$. Then we can find an isomorphism

$$A \simeq \prod_{j\in\Lambda} A_j.$$

The composition of f and this isomorphism is $\prod_{j\in\Lambda} f_j$.

Next we find a basis of $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S$; an algorithm for doing this is given in [PS97, §12]. To find a function f_j, we find a cubic form defined over A_j, with the property that the curve defined by the cubic meets C at P with multiplicity (at least) 3 and at each of the three points of T_j with multiplicity (at least) 2. The jth component of f can then be taken to be this cubic divided by any cubic form defined over $\mathbb{Q}$ (for example, z^3).

Then we find a basis for each $J(\mathbb{Q}_p)/\ker(f)$. It helps to know the dimension in advance. For p odd, we have $\#J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \#J(\mathbb{Q}_p)[2]$. We also have $\#J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 2^3\#J(\mathbb{Q}_2)[2]$ and $\#J(\mathbb{R})/2J(\mathbb{R}) = \#J(\mathbb{R})[2]/2^3$ (cf. [PS97, Lemma 12.10]). We can use Proposition 11.4 to determine whether $J(\mathbb{Q}_p)/\ker(f)$ has the same or half the size of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. Then we determine the intersection of all $\rho_p^{-1}(f(J(\mathbb{Q}_p)))$ for $p \in S$. That intersection is equal to $\mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q})$, which in our cases is half the size of $\mathrm{Sel}^2(J,\mathbb{Q})$.

We have

$$\dim \mathrm{Sel}^2(J,\mathbb{Q}) = \mathrm{rank}\, J(\mathbb{Q}) + \dim J(\mathbb{Q})[2] + \dim Ш(J,\mathbb{Q})[2].$$

In each of our cases, the number of independent elements we found so far in $J(\mathbb{Q})/2J(\mathbb{Q})$ equals $\dim \mathrm{Sel}^2(J,\mathbb{Q})$, so $Ш(J,\mathbb{Q})[2] = 0$. Subtracting $\dim J(\mathbb{Q})[2]$ gives us $\mathrm{rank}\, J(\mathbb{Q})$.

11.2. **Results.** In this section we use the 2-descent developed in the previous section to determine the ranks of $J_4(\mathbb{Q}), \ldots, J_{10}(\mathbb{Q})$. In each case, we find that $\rho_2^{-1}(f(J_i(\mathbb{Q}_2)/\ker f))$ is the same as the image of the subgroup of $J_i(\mathbb{Q})$ generated by the known rational points. Therefore, in each case, $\mathrm{Sel}^2_{\mathrm{fake}}(J_i, \mathbb{Q}) = \rho_2^{-1}(f(J_i(\mathbb{Q}_2)/\ker f))$. Recall that in each case, the $\mathcal{G}_{\mathbb{Q}}$-set T has no orbit of odd size, so the dimension of $\mathrm{Sel}^2(J_i, \mathbb{Q}) \simeq J_i(\mathbb{Q})/2J_i(\mathbb{Q})$ equals $1 + \dim \mathrm{Sel}^2_{\mathrm{fake}}(J_i, \mathbb{Q})$.

11.2.1. *Computing the rank of* $J_4(\mathbb{Q})$. In this section, we give a detailed description of the computation of the rank of $J_4(\mathbb{Q})$. For the curves $C_5, \ldots, C_{10}$, we give only the data necessary to check the computations in Table 5.

Let $g(x, y, z) = 0$ be the model of C_4 given in Table 2. For any smooth plane curve, the flex points are the points on the curve where the Hessian vanishes. We dehomogenize both g and the Hessian with respect to z and get two polynomials in $u = x/z$ and $v = y/z$. We compute their resultant to eliminate v, and get $h_6(u)h_{18}(u)$ where

$$h_6(u) = 7\,u^6 - u^3 + 1$$

and

$$h_{18}(u) = 343\,u^{18} + 23667\,u^{15} + 127743\,u^{12} + 72128\,u^9 - 29379\,u^6 + 2184\,u^3 + 1$$

are irreducible. This tells us that the $\mathcal{G}_{\mathbb{Q}}$-orbits of triangles will be of size 2 and 6. To determine a polynomial giving us the field of definition of a triangle in the size-2 orbit, we begin by taking a zero u_1 of h_6, and solve the equations given by g and its Hessian to find an explicit $v_1 \in \mathbb{Q}(u_1)$ such that (u_1, v_1) is a flex; let T_1 be the triangle it belongs to. We then construct the tangent line to C_4 at this flex to find the next point in T_1 and repeat once more to find the third point of T_1, expressing all coordinates as rational functions of u_1. The sum of the three u-coordinates must lie in the (quadratic) field of definition $\mathbb{Q}(T_1)$ of T_1, and this sum is found to generate $\mathbb{Q}(\sqrt{-3})$, so $\mathbb{Q}(T_1) = \mathbb{Q}(\sqrt{-3})$. A similar computation with a zero of h_{18} shows that if T_2 is a triangle in the other orbit, then $\mathbb{Q}(T_2) = \mathbb{Q}(\sqrt[6]{189})$. So $A \simeq \mathbb{Q}(\alpha) \times \mathbb{Q}(\beta)$ where $\alpha = \sqrt{-3}$ and $\beta = \sqrt[6]{189}$. Let $S = \{\infty, 2, 3, 7\}$. The subgroup of $\mathbb{Q}(\alpha)^\times/\mathbb{Q}(\alpha)^{\times 2}$ that is unramified outside S has basis $\{-1, 2, n_1, n_2, n_3\}$ where

$$n_1 = \alpha\,, \quad n_2 = \frac{\alpha + 5}{2}\,, \quad n_3 = \frac{-\alpha + 5}{2}\,.$$

Their norms are $1, 4, 3, 7, 7$, respectively. The subgroup of $\mathbb{Q}(\beta)^\times/\mathbb{Q}(\beta)^{\times 2}$ that is unramified outside S has basis $\{-1, \varepsilon_2, \varepsilon_3, \varepsilon_4, m_1, m_2, m_3, m_4, m_5\}$ where

$$\varepsilon_2 = \frac{1}{54}(\beta^5 - 3\beta^4 + 3\beta^3 + 9\beta^2 - 45\beta + 27)\,, \quad \varepsilon_3 = \frac{1}{54}(\beta^5 + 3\beta^4 + 3\beta^3 - 9\beta^2 - 45\beta - 27)\,,$$

$$\varepsilon_4 = \frac{1}{6}(\beta^3 + 15)\,, \quad m_1 = \frac{1}{18}(-\beta^4 - 6\beta^2 + 9\beta - 36)\,,$$

$$m_2 = \frac{1}{54}(-\beta^5 - 3\beta^3 + 9\beta^2 + 18\beta + 81)\,, \quad m_3 = \frac{1}{54}(\beta^5 + 3\beta^4 + 3\beta^3 + 27\beta^2 + 9\beta + 81)\,,$$

$$m_4 = \frac{1}{54}(\beta^5 + 3\beta^3 + 9\beta^2 + 36\beta - 27)\,, \quad m_5 = \frac{1}{18}(\beta^4 - 9\beta)\,.$$

Their norms are $1, 1, 1, 1, 64, 64, 64, -48, 7$, respectively.

Now let us find the image of $\langle -1, 2, 3, 7\rangle \subseteq \mathbb{Q}^\times$ in $A^\times/A^{\times 2}$. In $\mathbb{Q}(\alpha)$ we have

$$2 = 2\,, \qquad 3 = -\alpha^2\,, \qquad 7 = n_2 n_3\,.$$

In $\mathbb{Q}(\beta)$ we have

$$2 = -m_1^{-1} m_2 m_3\,, \quad 3 = \varepsilon_4^{-1} m_1^{-4} m_4^6 \quad \text{and} \quad 7 = \varepsilon_4^3 m_5^6\,.$$

So in $A^\times/A^{\times 2}\mathbb{Q}^\times$ we have

$$-1 \equiv (-1,-1)\,, \quad 2 \equiv (2, -m_1 m_2 m_3)\,, \quad 3 \equiv (-1, \varepsilon_4)\,, \quad 7 \equiv (n_2 n_3, \varepsilon_4)$$

are all trivial. So $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S$ has basis

$$\{(-1,1), (n_1,1), (n_2,1), (1,\varepsilon_2), (1,\varepsilon_3), (1,m_1), (1,m_2), (1,m_3), (1,m_4), (1,m_5)\}\ .$$

These have norms $1, 3, 7, 1, 1, 64, 64, 64, -48, 7$, respectively. So the kernel H of the norm from this group to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ has basis

$$\{(-1,1), (n_2, m_5), (1,\varepsilon_2), (1,\varepsilon_3), (1,m_1), (1,m_2), (1,m_3)\}\,.$$

This group H contains the fake 2-Selmer group.

Now we must find the function f. We will express f as a pair (f_2, f_6), where f_2 is defined over $\mathbb{Q}(\sqrt{-3})$ and f_6 is defined over $\mathbb{Q}(\sqrt[6]{189})$. By linear algebra, we can find a cubic $f_2(x,y,z)$, defined over the field $\mathbb{Q}(u_1)$, with the property that the intersection divisor of $f_2 = 0$ with $g = 0$ includes $2T_1 + 3(0:1:1)$. We can scale the solution in such a way that the coefficients lie in the field $\mathbb{Q}(\sqrt{-3})$. We get

$$\begin{aligned} f_2(x,y,z) = {} & 238\,x^3 + 84\,x^2 y + (9\alpha+3)xy^2 + (12\alpha+4)y^3 + (21\alpha-21)x^2 z - (57\alpha+33)xyz \\ & + (-12\alpha+24)y^2 z + (42\alpha-42)xz^2 + (-6\alpha+12)yz^2 + (6\alpha-40)z^3\,. \end{aligned}$$

Doing the same for T_2 yields

$$\begin{aligned} f_6(x,y,z) = {} & 2142\,x^3 + (-51\beta^4 + 1071\beta + 756)x^2 y + (4\beta^5 + 42\beta^4 - 21\beta^3 - 882\beta + 189)x^2 z \\ & + (-8\beta^5 - 9\beta^3 + 189)xy^2 + (8\beta^5 + 6\beta^4 + 57\beta^3 - 126\beta - 1323)xyz \\ & + (2\beta^5 + 6\beta^4 - 42\beta^3 - 126\beta + 378)xz^2 + (-12\beta^3 + 252)y^3 \\ & + (2\beta^5 - 9\beta^4 + 12\beta^3 + 189\beta)y^2 z + (-6\beta^5 + 6\beta^4 + 6\beta^3 - 126\beta)yz^2 \\ & + (4\beta^5 + 3\beta^4 - 6\beta^3 - 63\beta - 252)z^3\,. \end{aligned}$$

To compute $\mathrm{Sel}^2_{\mathrm{fake}}(J_4, \mathbb{Q})$, we first do global computations. Since the $\mathcal{G}_\mathbb{Q}$-orbits of the 8 triangles have sizes 2 and 6, we have $\dim J_4(\mathbb{Q})[2] = 1$. Since no orbit has odd size, Proposition 11.4 gives

$$\dim J_4(\mathbb{Q})/\ker(f) = \dim J_4(\mathbb{Q})/2J_4(\mathbb{Q}) - 1 = \dim J_4(\mathbb{Q})/2J_4(\mathbb{Q}) - \dim J_4(\mathbb{Q})[2] = \operatorname{rank} J_4(\mathbb{Q}).$$

The image in H, under f, of the subgroup of $J_4(\mathbb{Q})$ generated by the three known rational points is $\langle (-n_2, m_5), (1, \varepsilon_2)\rangle$. So $\operatorname{rank} J_4(\mathbb{Q}) \geq 2$.

The eight triangles break into four $\mathcal{G}_{\mathbb{Q}_2}$-orbits of size 2. Each pair is conjugate over $\mathbb{Q}_2(\sqrt{-3})$. Therefore, we have $\dim J_4(\mathbb{Q}_2)[2] = 4$ and $\dim J_4(\mathbb{Q}_2)/2J_4(\mathbb{Q}_2) = 7$. Since there

is no orbit of odd size, Proposition 11.4 gives $\dim J_4(\mathbb{Q}_2)/\ker f = 6$. We need to find a basis. Let $A_2 = A \otimes_{\mathbb{Q}} \mathbb{Q}_2$. The map f induces a map

$$J_4(\mathbb{Q}_2) \longrightarrow A_2^\times / A_2^{\times 2}\mathbb{Q}_2^\times \simeq (\mathbb{Q}_2(\sqrt{-3})^\times/\mathbb{Q}_2(\sqrt{-3})^{\times 2})^4 \,/\, (\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2})\,,$$

To find a basis of $J_4(\mathbb{Q}_2)/\ker f$, we look for $\mathbb{Q}_2$-rational divisors of degree 0 and determine their images under f. It is a straightforward exercise in algebraic number theory to determine whether their images are independent in $(\mathbb{Q}_2(\sqrt{-3})^\times/\mathbb{Q}_2(\sqrt{-3})^{\times 2})^4/(\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2})$. The following form a basis of $J_4(\mathbb{Q}_2)/\ker f$:

$$\begin{gathered}[(0:1:0)-(0:1:1)]\,, \quad [(1:0:0)-(0:1:1)]\,,\\ [(2:-1:O(2))-(0:1:1)]\,, \quad [(1:0:1+O(2))-(0:1:1)]\,,\\ [(4:-3:O(2))-(0:1:1)]\,, \quad [(5:4:1+O(2))-(0:1:1)]\,.\end{gathered}$$

We compute the image of $J_4(\mathbb{Q}_2)/\ker f$ in $(\mathbb{Q}_2(\sqrt{-3})^\times/\mathbb{Q}_2(\sqrt{-3})^{\times 2})^4/(\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2})$, and compute that its inverse image under $\rho_2|_H$ has basis $\{(-n_2, m_5), (1, \varepsilon_2)\}$. Thus

$$2 \geq \dim \mathrm{Sel}^2_{\mathrm{fake}}(J_4, \mathbb{Q}) \geq \dim J_4(\mathbb{Q})/\ker f = \operatorname{rank} J_4(\mathbb{Q}) \geq 2,$$

and equality holds everywhere. (We did not need the conditions on $\mathrm{Sel}^2_{\mathrm{fake}}(J_4, \mathbb{Q})$ coming from other primes.)

11.2.2. *Table with* 2*-descent data.* We computed the fake 2-Selmer groups for $C_5, \ldots, C_{10}$ in ways similar to that explained in detail for C_4. Table 5 can be used to check the fake 2-Selmer group computations for $C_5, \ldots, C_{10}$. In the column labelled *octic*, we present the coefficients of $t^8, \ldots, 1$ for a polynomial defining the 8-dimensional algebra A. We also give the dimensions of $J(\mathbb{Q}_2)[2]$ and $J(\mathbb{Q})[2]$. Basis elements of $J(\mathbb{Q}_2)/\ker f$ are represented by $\mathbb{Q}_2$-rational degree 0 divisors. Lastly, we give the rank of $J(\mathbb{Q})$.

Regarding $\dim J(\mathbb{Q}_2)[2]$, note that 2-torsion points are represented by a partition of the set of 8 flex triangles into two sets of even cardinality. So we have the trivial 2-torsion point 0, corresponding to the trivial factorization of the octic polynomial over $\mathbb{Q}_2$, points corresponding to factors of degree 2, and finally points corresponding to a factorization of the octic polynomial into two factors of degree 4 over $\mathbb{Q}_2$ *or into two factors of degree* 4 *that are conjugate over some quadratic extension of* $\mathbb{Q}_2$. For example, $\dim J_5(\mathbb{Q}_2)[2] = 2$, even though the octic polynomial is irreducible over $\mathbb{Q}_2$. This phenomenon came up already when dealing with C_4 above: the fact that the octic polynomial defining the algebra split into four quadratic factors over $\mathbb{Q}_2$ defining the same quadratic extension $\mathbb{Q}_2(\sqrt{-3})$ gives rise to an additional independent point in $J_4(\mathbb{Q}_2)[2]$.

12. Chabauty and Mordell-Weil sieve

We discuss the Mordell-Weil sieve first since this is often performed before the Chabauty computation.

i	octic	dim $J_i(\mathbb{Q}_2)[2]$	basis of $J_i(\mathbb{Q}_2)/\ker(f)$	dim $J_i(\mathbb{Q})[2]$	rank
5	$1,2,0,0,-21,$ $0,84,-30,-123$	2	$[(1:1:1)-(0:1:0)]$ $[(1:1:5+O(2^3))-(0:1:0)]$ $[(2:2:3+O(2^3))-(0:1:0)]$ $[(-1:1:3+O(2^3))-(0:1:0)]$	0	3
6	$1,0,-42,0,567,$ $0,-1890,0,-567$	1	$[(0:1:0)-(0:1:1)]$ $[(-1:1:0)-(0:1:1)]$ $[(4:1:-1+O(2^2))-(0:1:1)]$	1	2
7	$1,2,-14,-98,-217,$ $-182,196,548,529$	2	$[(0:0:1)-(0:1:0)]$ $[(2:2:-1+O(2^3))-(0:1:0)]$ $[(2:-2:1+O(2^3))-(0:1:0)]$ $[(2:-1:3+O(2^3))-(0:1:0)]$	0	2
8	$1,0,0,56,-210,$ $336,-224,24,21$	2	$[(2:-1:0)-(0:0:1)]$ $[(0:2:1+O(2^3))-(0:0:1)]$ $[(-2:1:10+O(2^4))-(0:0:1)]$ $[(1:-3:1+O(2^3))-(0:0:1)]$	0	2
9	$1,-2,-14,14,119,$ $182,112,16,-11$	2	$[(1:1:0)-(0:0:1)]$ $[(0:2:-3+O(2^3))-(0:0:1)]$ $[(4:2:1+O(2^3))-(0:0:1)]$ $[(2:1:6+O(2^4))-(0:0:1)]$	0	2
10	$1,-3,0,14,0,$ $-84,112,-24,-12$	0	$[(-1:1:2+O(2^3))-(1:1:0)]$ $[(0:1:-1+O(2^3))-(1:1:0)]$ $[(1:-4:4+O(2^3))-(1:1:0)]$	0	2

TABLE 5. Data needed for 2-descents for $C_5,\dots,C_{10}$.

12.1. **Mordell-Weil sieve theory.** Let C be a curve over $\mathbb{Q}$ and J be its Jacobian. (The assumption that the ground field is $\mathbb{Q}$ is for simplicity only; other global fields would do just as well.) Suppose that we know an embedding $C \to J$ over $\mathbb{Q}$. What we call the *Mordell-Weil sieve* is a method introduced by Scharaschkin [Sch04] that uses reduction modulo p for several primes p to show that certain points in $J(\mathbb{Q})$ cannot lie on the image of C. Suppose also that we know explicit generators for $J(\mathbb{Q})$. Then the desired set $C(\mathbb{Q})$ is the set of points of $J(\mathbb{Q})$ that lie on C. This set is difficult to compute: indeed, it is not known whether there exists an algorithm to solve this problem in general.

Therefore we pick a prime p of good reduction for C (and J), and we approximate the condition that a point $P \in J(\mathbb{Q})$ lie on C with the weaker condition that the reduction of P in $J(\mathbb{F}_p)$ lie in $C(\mathbb{F}_p)$. For each p, this weaker condition allows us to "sieve out" certain cosets of a finite-index subgroup in $J(\mathbb{Q})$. The conditions at different p can interact nontrivially, because the orders of $J(\mathbb{F}_p)$ may share prime factors. If we are lucky, after using these sieve conditions at a few primes, no points on $J(\mathbb{Q})$ remain; in this case one concludes that $C(\mathbb{Q})$

is empty. In fact, there is a heuristic that predicts that when $C(\mathbb{Q}) = \emptyset$, sieving with a suitable set of p will rule out all points of $J(\mathbb{Q})$ [Poo06]. This obstruction to the existence of rational points is closely related to the Brauer-Manin obstruction: see [Sch04] and in particular [Sto06b].

Remarks 12.1.

(1) With care, one can obtain sieve conditions also at primes p of bad reduction. Namely, let $\mathcal{C}$ be the minimal proper regular model of C over $\mathbb{Z}_p$, and let $\mathcal{J}$ be the Néron model of J over $\mathbb{Z}_p$. Suppose we have an Albanese embedding $C \hookrightarrow J$ associated to a rational point on C. Let $\mathcal{C}^{\mathrm{smooth}}$ be the smooth locus of the structure morphism $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_p$; thus $\mathcal{C}^{\mathrm{smooth}}$ is obtained from $\mathcal{C}$ by deleting the singular points on the special fiber $\mathcal{C}_{\mathbb{F}_p}$. By the Néron property, the morphism $C \hookrightarrow J$ extends to a $\mathbb{Z}_p$-morphism $\mathcal{C}^{\mathrm{smooth}} \hookrightarrow \mathcal{J}$. Points in $C(\mathbb{Q})$ extend to $\mathbb{Z}_p$-points of $\mathcal{C}^{\mathrm{smooth}}$, so we need only examine the set of points $J(\mathbb{Q})$ whose reduction in $\mathcal{J}(\mathbb{F}_p)$ lies in the image of $\mathcal{C}^{\mathrm{smooth}}(\mathbb{F}_p)$.
(2) Sometimes it is more convenient to work in a homomorphic image Φ of $\mathcal{J}(\mathbb{F}_p)$ instead of $\mathcal{J}(\mathbb{F}_p)$ itself.
(3) Working in $\mathcal{J}(\mathbb{Z}/p^n\mathbb{Z})$ for $n > 1$ also might give more information than $\mathcal{J}(\mathbb{F}_p)$ alone.
(4) We assumed that we know generators for $J(\mathbb{Q})$, but it may be enough to know generators for a subgroup $\mathcal{Q}$ of finite index. For instance, if one can prove that the index $(J(\mathbb{Q}) : \mathcal{Q})$ is prime to the order of $J(\mathbb{F}_p)$, then $\mathcal{Q}$ and $J(\mathbb{Q})$ will have the same image in $J(\mathbb{F}_p)$.
(5) If $C(\mathbb{Q})$ is known *a priori* to be nonempty, obviously no complete obstruction to rational points can be obtained. In this case, one can try to use the sieve information as input to a Chabauty argument, to restrict the possibilities for residue classes. The Chabauty argument still requires that the p-adic closure of $J(\mathbb{Q})$ be provably of dimension less than $\dim J$, however, and this usually requires $\operatorname{rank} J(\mathbb{Q}) < \dim J$.

The first examples of this method were given in [Sch04]. The method was refined and implemented for genus 2 curves over $\mathbb{Q}$ in [Fly04].

12.2. **Chabauty theory.** Here we explain Chabauty's method [Cha41], as made explicit by Coleman [Col85]. Let C be a smooth projective curve. Let J be its Jacobian. Assume that $C(\mathbb{Q})$ is nonempty (this is true for all of our C_i); choose $P \in C(\mathbb{Q})$. Identify C with a subvariety of J by mapping each $T \in C$ to $T \mapsto [T - P]$. Assume that $J(\mathbb{Q})$ has rank $r < g$, where $g = \dim J$ is the genus of C. Let p be a finite prime. If ω is a holomorphic 1-form on $J_{\mathbb{Q}_p}$ or its pullback to $C_{\mathbb{Q}_p}$, then following [Bou98, III.§7.6] we define a homomorphism $\lambda_\omega \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p$ by $Q \mapsto \int_0^Q \omega$. (This integral can be defined on a neighborhood of 0 using the formal group, and then extended linearly to all of $J(\mathbb{Q}_p)$.) Say that ω kills an element or subset S of $J(\mathbb{Q}_p)$ if $\lambda_\omega|_S = 0$. By linear algebra, we can find (to any desired p-adic precision) at least $g - r > 0$ independent forms ω killing $J(\mathbb{Q})$ and hence $C(\mathbb{Q})$. The method consists of bounding the number of common zeros of the corresponding integrals λ_ω on $C(\mathbb{Q}_p)$, and hoping that enough points in $C(\mathbb{Q})$ are found to meet the bound, in which case these points

are all of them. If the method fails, we can try again with a different p, or combine the argument with a Mordell-Weil sieve.

Let us explain how to do a Chabauty computation in practice. Let C be the smooth projective model of the affine plane quartic curve $g(u,v)=0$. For the computation, we need $G_1,\dots,G_r \in J(\mathbb{Q})$ which generate a subgroup of finite index in $J(\mathbb{Q})$. Usually we obtain this information when we determine r. Choose a (small) prime p at which C, and hence J, has good reduction. Pick a uniformizing parameter t of C at P that is also a uniformizer at P modulo p. For each i, we calculate $m_i \in \mathbb{Z}_{>0}$ such that m_iG_i reduces to 0 mod p, and find a divisor of the form $D_i - 3P$ linearly equivalent to m_iG_i, where $D_i = P_{i,1}+P_{i,2}+P_{i,3}$ is an effective divisor of degree 3, defined over $\mathbb{Q}$. If P does not reduce to a Weierstrass point mod p, then it follows that each $P_{i,j}$ is congruent to P modulo p.

A basis for the space of holomorphic differentials on C is given by

$$\omega_1 = \frac{dv}{g_u}\,, \quad \omega_2 = \frac{u\,dv}{g_u} \quad \text{and} \quad \omega_3 = \frac{v\,dv}{g_u}\,.$$

We express ω_j as an element of $\mathbb{Q}[[t]]\,dt$ and integrate formally to obtain $\lambda_j = \int_0^t \omega_j \in t\,\mathbb{Q}[[t]]$. Then for all i and j, we compute

$$\begin{aligned}\lambda_{\omega_j}(m_iG_i) &= \int_0^{m_iG_i} \iota_*\omega_j = \int_0^{[D_i-3P]} \iota_*\omega_j = \int_P^{P_{i,1}} \omega_j + \int_P^{P_{i,2}} \omega_j + \int_P^{P_{i,3}} \omega_j \\ &= \lambda_j(t(P_{i,1})) + \lambda_j(t(P_{i,2})) + \lambda_j(t(P_{i,3}))\,.\end{aligned}$$

The series converge, since the $t(P_{i,k})$ are of positive p-adic valuation (this is because $P_{i,k}$ has the same reduction mod p as P). Computing the kernel of $\omega \longmapsto (\lambda_\omega(m_1G_1),\dots,\lambda_\omega(m_rG_r))$, we find $s = 3-r$ independent holomorphic differentials $\eta_1,\dots,\eta_s$ such that the corresponding 1-forms on $J_{\mathbb{Q}_p}$ kill $J(\mathbb{Q})$. We rescale each so that it reduces to a nonzero differential $\tilde{\eta}_i$ modulo p. Let $Q \in C(\mathbb{F}_p)$ and let $\nu = \min_i v_Q(\tilde{\eta}_i)$. If $p > \nu+1$, there can be at most $\nu+1$ rational points on C reducing to Q mod p: see, e.g., [Sto06a].

For $i = 1,3,7,8,9,10$, we want to do Chabauty arguments using the prime 7, at which C_i has bad reduction. However, the given model of C_i in $\mathbb{P}^2_{\mathbb{Z}_7}$ is a minimal proper regular model over $\mathbb{Z}_7$, and the special fiber $\tilde{C}_i$ has just one component, which is of (geometric) genus 0. Let $\mathcal{J}_i$ be the Néron model of J_i over $\mathbb{Z}_7$. Let $\tilde{J}_i = \mathcal{J}_i \times_{\mathbb{Z}_7} \mathbb{F}_7$ be the special fiber of $\mathcal{J}_i$. Since $\tilde{C}_i$ has just one component, $\tilde{J}_i$ is connected. Let $\tilde{C}_i^{\mathrm{smooth}}$ be the smooth part of $\tilde{C}_i$. We write $J_i(\mathbb{F}_7)$ for $\tilde{J}_i(\mathbb{F}_7)$, and write $C_i(\mathbb{F}_7)$ for $\tilde{C}_i^{\mathrm{smooth}}(\mathbb{F}_7)$, which is a subset of $J_i(\mathbb{F}_7)$. In all the cases we consider, we find that $J_i(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. We can proceed as in the case of good reduction; the differentials reduce to holomorphic differentials on $\tilde{C}_i^{\mathrm{smooth}}$ in this case.

12.3. **Results.** For brevity, we give full detail for the Chabauty and Mordell-Weil sieve arguments for just one curve. We chose C_2 since our argument for C_2 involves a shortcut that apparently is not described elsewhere in the literature. Afterwards we sketch the Chabauty arguments for the remaining curves.

Define the *known part* $J_i(\mathbb{Q})_{\mathrm{known}}$ of $J_i(\mathbb{Q})$ as the subgroup generated by the rational points in Table 3 and the element $[R-3P]$ mentioned in Propositions 11.3 and 11.4.

12.3.1. *Determining $C_2(\mathbb{Q})$.* We will show that

$$C_2(\mathbb{Q}) = \{(1:0:0), (0:1:0), (0:0:1), (1:-2:-1), (1:1:-1)\}\,.$$

We work with $p = 5$; we have $J_2(\mathbb{F}_5) \simeq \mathbb{Z}/126\mathbb{Z}$. The reduction of $J_2(\mathbb{Q})_{\text{known}}$ is the cyclic subgroup of order 63. We use $P = (1:-2:-1)$ as a basepoint. The five known rational points of C_2 reduce to different points in $C_2(\mathbb{F}_5)$, which has size 6.

We first have to find the space of 5-adic differentials that vanish on $J_2(\mathbb{Q})$. Dehomogenize by setting $z = 1$; then a basis of the space of holomorphic differentials on C_2 is given by

$$\omega_1 = \frac{dy}{9\,x^2y + 2}\,, \quad \omega_2 = \frac{x\,dy}{9\,x^2y + 2}\,, \quad \omega_3 = \frac{y\,dy}{9\,x^2y + 2}\,.$$

(As line sections, we have $\omega_1 \leftrightarrow z$, $\omega_2 \leftrightarrow x$, $\omega_3 \leftrightarrow y$. This point of view is useful when determining the zeros of differentials.) The point $G = [(1:0:0) - (1:-2:-1)] \in J_2(\mathbb{Q})$ is of infinite order, and $9G$ is in the kernel of reduction mod 5. We find an effective divisor D of degree 3 such that $9G = [D - 3P]$. We choose $t = x + 1$ as a uniformizer at P; then we can express x, y, and the differentials in terms of t as follows.

$$\begin{aligned}
x &= -1 + t \\
y &= 2 - \frac{20}{3^2}\,t + \frac{226}{3^5}\,t^2 + \frac{1024}{3^8}\,t^3 - \frac{7702}{3^{10}}\,t^4 + \dots \\
\omega_1 &= \Big(-\frac{1}{3^2} - \frac{53}{3^5}\,t - \frac{478}{3^7}\,t^2 - \frac{6530}{3^{10}}\,t^3 - \frac{1135}{3^{14}}\,t^4 + \dots\Big)\,dt \\
\omega_2 &= \Big(\frac{1}{3^2} + \frac{26}{3^5}\,t + \frac{1}{3^7}\,t^2 - \frac{6376}{3^{10}}\,t^3 - \frac{527795}{3^{14}}\,t^4 + \dots\Big)\,dt \\
\omega_3 &= \Big(-\frac{2}{3^2} - \frac{46}{3^5}\,t - \frac{122}{3^7}\,t^2 + \frac{2618}{3^{10}}\,t^3 + \frac{107380}{3^{14}}\,t^4 + \dots\Big)\,dt
\end{aligned}$$

We obtain the logarithms λ_{ω_i} in terms of t by formal integration of the latter three power series:

$$\begin{aligned}
\lambda_1 &= -\frac{1}{3^2}\,t - \frac{53}{2\cdot 3^5}\,t^2 - \frac{478}{3^8}\,t^3 - \frac{3265}{2\cdot 3^{10}}\,t^4 - \frac{227}{3^{14}}\,t^5 + \dots \\
\lambda_2 &= \frac{1}{3^2}\,t + \frac{13}{3^5}\,t^2 + \frac{1}{3^8}\,t^3 - \frac{1594}{3^{10}}\,t^4 - \frac{105559}{3^{14}}\,t^5 + \dots \\
\lambda_3 &= -\frac{2}{3^2}\,t - \frac{23}{3^5}\,t^2 - \frac{122}{3^8}\,t^3 + \frac{1309}{2\cdot 3^{10}}\,t^4 + \frac{21476}{3^{14}}\,t^5 + \dots
\end{aligned}$$

If t_1, t_2, t_3 are the values of t at the three points in D, then

$$\lambda_{\omega_i}(9G) = \lambda_i(t_1) + \lambda_i(t_2) + \lambda_i(t_3) = \sum_{j=1}^{\infty} \lambda_{i,j}(t_1^j + t_2^j + t_3^j)\,,$$

where $\lambda_i(t) = \sum_{j\ge 1} \lambda_{i,j} t^j$. We obtain the power sums $t_1^j + t_2^j + t_3^j$ from the coefficients of the characteristic polynomial $(X - t_1)(X - t_2)(X - t_3) \in \mathbb{Q}[X]$. The 5-adic valuation of each t_i is positive (at least 1/3), and so the series above converge in $\mathbb{Q}_5$. We obtain

$$\lambda_{\omega_1}(9G) = -2\cdot 5^3 + O(5^4)\,, \quad \lambda_{\omega_2}(9G) = -16\cdot 5 + O(5^4)\,, \quad \lambda_{\omega_3}(9G) = -27\cdot 5 + O(5^4)\,.$$

We see that

$$\tilde{\eta_1} = \tilde{\omega_1} = \frac{dy}{2 - x^2 y} \leftrightarrow z \quad \text{and} \quad \tilde{\eta_2} = \tilde{\omega_2} + 2\tilde{\omega_3} = \frac{(x + 2y)\, dy}{2 - x^2 y} \leftrightarrow x + 2y$$

are reductions mod 5 of differentials killing $J_2(\mathbb{Q})$. Since the common zero of z and $x + 2y$ in $\mathbb{P}^2(\mathbb{F}_5)$ is not on C, we have $\min\{v_Q(\tilde{\eta_1}), v_Q(\tilde{\eta_2})\} = 0$ at all $Q \in C(\mathbb{F}_5)$. Thus each of the six residue classes contains at most one rational point. Since five of the six do contain a rational point, it remains to show that there is no rational point reducing to the sixth, which is $(2 : 2 : 1) \in C_2(\mathbb{F}_5)$.

To that end, we pick $Q \in C_2(\mathbb{Q}_5)$ reducing to $(2 : 2 : 1)$; we take $Q = (\frac{3+\sqrt{-39}}{6} : 2 : 1)$, where we choose the square root that is -1 mod 5. We first need to find $\lambda_\omega([Q - P])$ for a basis of differentials ω killing $J_2(\mathbb{Q})$. In principle, we can find this by first computing $21[Q - P] = [D' - 3P]$ in the kernel of reduction as above, but in this case, there is a trick, taught to us by Joseph Wetherell, that allows us to simplify the computation.

Note that $[(2 : 2 : 1) - \tilde{P}] \in J_2(\mathbb{F}_5)$ is in the reduction of $J_2(\mathbb{Q})_{\text{known}}$; we find that $G' = [(0 : 1 : 0) + (1 : 1 : -1) - (1 : 0 : 0) - P] \in J_2(\mathbb{Q})$ has this image. If ω kills $J_2(\mathbb{Q})$, then $\lambda_\omega([Q - P]) = \lambda_\omega([Q - P] - G')$, where now $[Q - P] - G'$ is in the kernel of reduction, and we can compute the logarithm as before. With

$$\eta_1 = \omega_1 - 50\,\omega_2 + O(5^3) \quad \text{and} \quad \eta_2 = \omega_2 - 33\,\omega_3 + O(5^3)\,,$$

we obtain the values $\lambda_{\eta_1}([Q - P]) = -12 \cdot 5 + O(5^3)$ and $\lambda_{\eta_2}([Q - P]) = -14 \cdot 5 + O(5^3)$. We now compute $\lambda_{\eta_i}([Q' - Q])$ for points Q' in the residue class of Q. Taking $T = y - 2$ as a uniformizer at Q, we obtain for points Q' such that $T(Q') = 5\tau$:

$$\lambda_{\eta_1}([Q' - P]) = \lambda_{\eta_1}([Q' - Q]) + \lambda_{\eta_1}([Q - P]) = -12 \cdot 5 + 4 \cdot 5\,\tau + 5^2\,\tau^2 + O(5^3)$$
$$\lambda_{\eta_2}([Q' - P]) = \lambda_{\eta_2}([Q' - Q]) + \lambda_{\eta_2}([Q - P]) = 11 \cdot 5 + 9 \cdot 5\,\tau - 3 \cdot 5^2\,\tau^2 + O(5^3)$$

We see that $\lambda_{\eta_1}([Q' - P]) - \lambda_{\eta_2}([Q' - P]) = 2 \cdot 5 + O(5^2)$ and so never vanishes. This proves that there is no rational point on C_2 reducing to $(2 : 2 : 1)$.

12.3.2. *Determining $C_1(\mathbb{Q})$.* We show that

$$C_1(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0), (0 : 0 : 1), (1 : -1 : 2)\}\,.$$

As described in Section 12.2, we have $J_1(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. From Section 10, we see that $\dim_{\mathbb{F}_7} J_1(\mathbb{Q})/7J_1(\mathbb{Q}) = 2$. The reduction of $J_1(\mathbb{Q})_{\text{known}}$ has dimension 2, so that is also the reduction of the whole $J_1(\mathbb{Q})$.

Using $(1 : -1 : 2)$ as a basepoint, we find that there are exactly four points of $C_1(\mathbb{F}_7)$ in the reduction of $J(\mathbb{Q})$. They are the reductions of the four known rational points on C_1. So it suffices to show that there is only one point of $C_1(\mathbb{Q})$ in each of those residue classes.

Proceeding as for C_2, we find reductions of differentials killing $J_1(\mathbb{Q})$:

$$\tilde{\eta_1} \leftrightarrow x + 2y\,, \qquad \tilde{\eta_2} \leftrightarrow x - z\,.$$

The common zero of $x + 2y$ and z in $\mathbb{P}^2(\mathbb{F}_7)$ is not on C_1, so there is at most one rational point per residue class, as desired.

12.3.3. *Determining* $C_3(\mathbb{Q})$. We show that

$$C_3(\mathbb{Q}) = \{(1:0:0), (0:1:0), (0:0:1), (1:1:-1)\}\,.$$

We have $J_3(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. From Section 10 we see that $\dim_{\mathbb{F}_7} J_3(\mathbb{Q})/7J_3(\mathbb{Q}) = 2$. The reduction of $J_3(\mathbb{Q})_{\text{known}}$ has dimension 2, so that is also the reduction of the whole $J_3(\mathbb{Q})$.

Using $(1:1:-1)$ as a basepoint, we find that there are exactly four points of $C_3(\mathbb{F}_7)$ in the reduction of $J_3(\mathbb{Q})$. Again, they are the reductions of the four known rational points on C_3. So it suffices to show that there is only one point of $C_3(\mathbb{Q})$ in each of those residue classes.

Proceeding as before, we find reductions of differentials killing $J_3(\mathbb{Q})$:

$$\tilde{\eta_1} \leftrightarrow 2x - y\,, \qquad \tilde{\eta_2} \leftrightarrow x + 2z\,.$$

The common zero of $2x - y$ and $x + 2z$ in $\mathbb{P}^2(\mathbb{F}_7)$ is not on C_3, so we are done.

12.3.4. *Determining* $C_4(\mathbb{Q})$. We show that

$$C_4(\mathbb{Q}) = \{(1:0:0), (0:1:0), (0:1:1)\}\,.$$

We have $J_4(\mathbb{F}_5) \simeq (\mathbb{Z}/6\mathbb{Z})^3$. The reduction of $J_4(\mathbb{Q})_{\text{known}}$ is isomorphic to $(\mathbb{Z}/6\mathbb{Z})^2$. Since $J_4(\mathbb{Q})$ and $J_4(\mathbb{Q})_{\text{known}}$ are both isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$, and $J_4(\mathbb{Q})_{\text{known}}$ has odd index in $J_4(\mathbb{Q})$, the whole $J_4(\mathbb{Q})$ must also reduce to the same $(\mathbb{Z}/6\mathbb{Z})^2$ subgroup. We use $(1:0:0)$ as a basepoint. Then the only elements in $C_4(\mathbb{F}_5)$ in the reduction of $J_4(\mathbb{Q})$ are the reductions of the three known rational points. So it suffices to show that there is only one point of $C_4(\mathbb{Q})$ in each of those residue classes.

Since the rank is 2, we have only one differential, $\tilde{\eta} \leftrightarrow x + y$. It does not vanish at any of the three relevant points of $C_4(\mathbb{F}_5)$; this proves the claim.

12.3.5. *Determining* $C_6(\mathbb{Q})$. We show that

$$C_6(\mathbb{Q}) = \{(0:1:0), (1:-1:0), (0:1:1), (0:1:-1)\}\,.$$

We use $P = (0:1:-1)$ as a basepoint. We have an isomorphism $\mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z} \to J_6(\mathbb{Q})_{\text{known}}$ taking the standard generators $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ to $[R-3P]$, $[(0:1:0)-P]$, $[(1:-1:0)-P]$, respectively. From the 2-descent, we know that $J_6(\mathbb{Q})_{\text{known}}$ has odd index in $J_6(\mathbb{Q})$, which also is isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$. We have $J_6(\mathbb{F}_{11}) \simeq (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$. The reduction of $J_6(\mathbb{Q})_{\text{known}}$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})$, with $[R-3P]$, $[(0:1:0)-P]$, $[(1:-1:0)-P]$ mapping to the standard generators. By the above, $J_6(\mathbb{Q})$ has the same reduction as $J_6(\mathbb{Q})_{\text{known}}$. There are five points in $C_6(\mathbb{F}_{11})$ lying in the reduction of $J_6(\mathbb{Q})$; four of those are the reductions of the four known rational points. The fifth is the reduction of

$$m\,[R-3P] + n\,[(0:1:0)-P] + p\,[(1:-1:0)-P]$$

with $(m,n,p) = (1,4,2)$.

We have $J_6(\mathbb{F}_{23}) \simeq \mathbb{Z}/32\mathbb{Z} \times (\mathbb{Z}/16\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$. The mod 23 reduction of $J_6(\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/16\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$, with $[R-3P]$, $[(0:1:0)-P]$, $[(1:-1:0)-P]$ mapping to the standard

generators. We find that if $(m,n,p) \in \mathbb{Z}^3$ satisfy $(m \bmod 8, n \bmod 8, p \bmod 4) = (1,4,2)$ then the mod 23 reduction of

$$m\,[R-3P] + n\,[(0:1:0)-P] + p\,[(1:-1:0)-P]$$

is not in $C_6(\mathbb{F}_{23})$. Because $J_6(\mathbb{Q})_{\text{known}}$ has odd index in $J_6(\mathbb{Q})$, the points of $J_6(\mathbb{Q})$ reducing to the fifth point of $C_6(\mathbb{F}_{11})$ of the previous paragraph do not reduce mod 23 to points in $C_6(\mathbb{F}_{23})$. So it suffices to show that there is only one point of $C_6(\mathbb{Q})$ in each of the four residue classes of the four known rational points modulo 11.

The differential is $\tilde{\eta} \leftrightarrow x + 5y$; it does not vanish at the four relevant points of $C_6(\mathbb{F}_{11})$. This proves the claim.

12.3.6. *Determining $C_7(\mathbb{Q})$.* We show that

$$C_7(\mathbb{Q}) = \{(0:1:0), (0:0:1), (0:1:1)\}.$$

We have $J_7(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. The group $J_7(\mathbb{Q})$ has rank 2 and no 7-torsion. The reduction of $J_7(\mathbb{Q})_{\text{known}}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, so that is also the reduction of the whole $J_7(\mathbb{Q})$.

We use $(0:1:0)$ as a basepoint. Then the only elements in $C_7(\mathbb{F}_7)$ in the reduction of $J_7(\mathbb{Q})$ are the reductions of the three known rational points. So it suffices to show that there is only one point of $C_7(\mathbb{Q})$ in each of those residue classes.

Our differential mod 7 is $\tilde{\eta} \leftrightarrow x - 2z$. It does not vanish at $(0:0:1)$ and at $(0:1:1)$, but it has a simple zero at $(0:1:0)$. So we see that there is at most one rational point in each of the two first residue classes, but there may be two in the third. Since we are using $(0:1:0)$ as a basepoint, the information over $\mathbb{Q}_7$ tells us that any point of $C_7(\mathbb{Q})$ in the residue class of $(0:1:0)$ is in $7J_7(\mathbb{Q})$.

We have $J_7(\mathbb{F}_{13}) \simeq (\mathbb{Z}/14\mathbb{Z})^3$. The reduction of $J_7(\mathbb{Q})_{\text{known}}$ is isomorphic to $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. From the 2-descent, we know that the index of $J_7(\mathbb{Q})_{\text{known}}$ in $J_7(\mathbb{Q})$ is odd. Thus, the reduction of the whole $J_7(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Only one point of $C_7(\mathbb{F}_{13})$ has trivial image in $J(\mathbb{F}_{13}) \otimes \mathbb{Z}/7\mathbb{Z}$, namely $(0:1:0)$. A holomorphic differential killing $J_7(\mathbb{Q})$ reduces mod 13 to $\tilde{\omega} \leftrightarrow x - 2y$, which does not vanish at $(0:1:0)$. So there is only one point of $C_7(\mathbb{Q})$ in this residue class. (Incidentally, $\tilde{\omega}$ vanishes at one of the other interesting residue classes, namely $(0:0:1)$. So information obtained from $\mathbb{Q}_{13}$ alone would also not be sufficient.)

12.3.7. *Determining $C_8(\mathbb{Q})$.* We show that

$$C_8(\mathbb{Q}) = \{(0:0:1), (2:-1:0)\}.$$

We have $J_8(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. The group $J_8(\mathbb{Q})$ has rank 2 and no 7-torsion. The reduction of $J_8(\mathbb{Q})_{\text{known}}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, so that is also the reduction of the whole $J_8(\mathbb{Q})$.

We use $(0:0:1)$ as a basepoint. Then the only elements in $C_8(\mathbb{F}_7)$ in the reduction of $J_8(\mathbb{Q})$ are the reductions of the two known rational points. So it suffices to show that there is only one point of $C_8(\mathbb{Q})$ in each of those residue classes.

Our differential mod 7 is $\tilde{\eta} \leftrightarrow x - y - 3z$. It does not vanish at $(0:0:1)$ and at $(2:-1:0)$. This proves the claim.

12.3.8. *Determining* $C_9(\mathbb{Q})$. We show that

$$C_9(\mathbb{Q}) = \{(0:0:1), (1:1:0)\}.$$

We use $P = (0:0:1)$ as a basepoint. We have $J_9(\mathbb{Q})_{\text{known}} \simeq \mathbb{Z}^2$, generated by $[(1:1:0)-P]$ and $[R-3P]$. The group $J_9(\mathbb{Q})$ has rank 2 and no 7-torsion.

We have $J_9(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$, with $[(1:1:0)-P]$ and $[R-3P]$ reducing to $\mathbb{F}_7$-independent points, so their reductions form a basis also for the reduction of $J_9(\mathbb{Q})$.

There are four points of $C_9(\mathbb{F}_7)$ in the reduction of $J_9(\mathbb{Q})$: the reductions of $m[(1:1:0)-P]+n[R-3P]$ with $(m,n) = (0,0), (1,0), (2,1), (4,3)$. Clearly $(m,n) = (0,0)$ and $(1,0)$ correspond to the reductions of the two known rational points. So we must eliminate the possibilities of $(m,n) = (2,1)$ and $(4,3)$. We do this by working over $\mathbb{F}_{13}$. We have $J_9(\mathbb{F}_{13}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/170\mathbb{Z}$. The classes $(m,n) = (2,1)$ and $(4,3)$ in $(\mathbb{Z}/7\mathbb{Z})^2$ map to classes in $J_9(\mathbb{F}_{13}) \otimes \mathbb{Z}/7\mathbb{Z}$. that are not in the image of $C_9(\mathbb{F}_{13})$ in $J_9(\mathbb{F}_{13}) \otimes \mathbb{Z}/7\mathbb{Z}$.

Our differential mod 7 is $\tilde{\eta} \leftrightarrow x - y - 2z$. It does not vanish at $(0:0:1)$, so there is only one rational point in this residue class. But $\tilde{\eta}$ has a simple zero at the other point, $(1:1:0)$. So we have to do another Chabauty computation to show that $(1:1:0)$ is the only point of $C_9(\mathbb{Q})$ in $[(1:1:0)-P]+7J_9(\mathbb{Q})$.

We will use $p = 11$. We have $J_9(\mathbb{F}_{11}) \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/140\mathbb{Z}$. We know from the 2-descent that the index of $J_9(\mathbb{Q})_{\text{known}}$ in $J_9(\mathbb{Q})$ is odd. The reduction modulo 11 of $J_9(\mathbb{Q})_{\text{known}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/70\mathbb{Z}$ and so must be the reduction of the whole $J_9(\mathbb{Q})$. Only three points of $C_9(\mathbb{F}_{11})$ are in the reduction of $J_9(\mathbb{Q})$. Only one of them has the same image in $J_9(\mathbb{F}_{11}) \otimes \mathbb{Z}/7\mathbb{Z}$ as $[(1:1:0)-P]+7J_9(\mathbb{Q})$, and that is the reduction of $(1:1:0)$. So it suffices to show that there is only one point of $C_9(\mathbb{Q})$ with reduction equal to $(1:1:0)$ modulo 11. The differential mod 11 is $\tilde{\omega} \leftrightarrow x - 5y + 4z$, and it does not vanish at $(1:1:0)$. So there is only one point of $C_9(\mathbb{Q})$ in this mod 11 residue class.

12.3.9. *Determining* $C_{10}(\mathbb{Q})$. We show that

$$C_{10}(\mathbb{Q}) = \{(1:0:0), (1:1:0)\}.$$

We have $J_{10}(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. The group $J_{10}(\mathbb{Q})$ has rank 2 and no 7-torsion. The reduction of $J_{10}(\mathbb{Q})_{\text{known}}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, so that is also the reduction of the whole $J_{10}(\mathbb{Q})$. We use $(1:0:0)$ as a basepoint. Then the only elements in $C_{10}(\mathbb{F}_7)$ in the reduction of $J_{10}(\mathbb{Q})$ are the reductions of the two known rational points. So it suffices to show that there is only one point of $C_{10}(\mathbb{Q})$ in each of those residue classes. The differential mod 7 is $\tilde{\eta} \leftrightarrow x + y + 3z$; it does not vanish at either of the two relevant points in $C_{10}(\mathbb{F}_7)$, proving the claim.

13. Mordell-Weil sieve for C_5

In this section we prove that $C_5(\mathbb{Q})_{\text{subset}} = \emptyset$. The method used is the Mordell-Weil sieve described in Section 12.1.

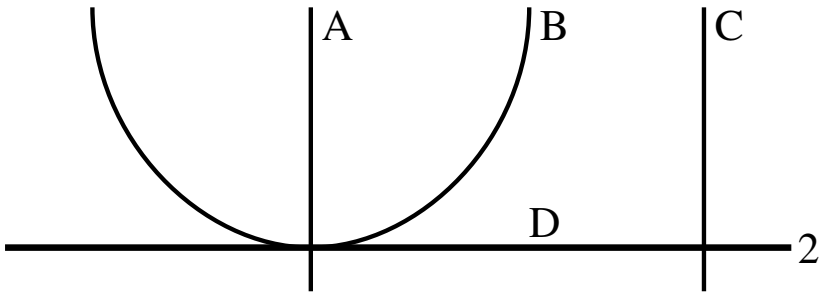


FIGURE 3. The special fiber of C_5 at 3.

13.1. **The strategy for C_5.** Because $C_5(\mathbb{Q})$ is nonempty and $\operatorname{rank} J_5(\mathbb{Q}) = \dim J_5$, we cannot expect to determine $C_5(\mathbb{Q})$ using only the methods described in Section 12.1. On the other hand, by Lemma 7.8 we need only the subset $C_5(\mathbb{Q})_{\text{subset}}$ of rational points lying in certain residue classes, so there is hope of proving $C_5(\mathbb{Q})_{\text{subset}} = \emptyset$.

To succeed, we must use the 2-adic and 3-adic conditions defining $C_5(\mathbb{Q})_{\text{subset}}$, since neither alone is enough to exclude all the rational points on C_5. This means that we must use the sieve information at the bad primes 2 and 3. In fact, we will use only the component groups of the Néron models at 2 and 3. We will discover that the only primes dividing the orders of these groups are 2 and 7 (respectively), so we will sieve also at primes p of good reduction chosen so that $J_5(\mathbb{F}_p)$ has large 2-primary and/or 7-primary parts.

Let P_0, P_1, P_2, P_3 (in this order) be the four rational points on C_5 listed in Table 3. Let $Q_i \in J(\mathbb{Q})$ be the class of the divisor $P_i - P_0$. Let $\mathcal{Q}$ be the subgroup of $J(\mathbb{Q})$ generated by the Q_i. We will show that $(J_5(\mathbb{Q}) : \mathcal{Q})$ is prime to 14, and we will use groups Φ of order divisible only by 2 and 7 in the sieve. We will determine the set of $(n_1, n_2, n_3) \in \mathbb{Z}^3$ such that $n_1Q_1 + n_2Q_2 + n_3Q_3$ satisfies the sieve conditions.

13.2. **Sieve information at 3.** We will compute the minimal proper regular model $\mathcal{C}$ of C_5 over $\mathbb{Z}_3$, and then the component group of the Néron model of its Jacobian. Our exposition will be terse, since [FLS$^+$01] contains a detailed account of the general method. We will use the same label for a component and for its strict transform(s) after blowing up. Subscripts on components denote multiplicities, and a component without a subscript has multiplicity 1.

Start with the model in $\mathbb{P}^2_{\mathbb{Z}_3}$ defined by the ternary quartic. Its special fiber has two irreducible components A and B, and is regular except at the point s where A intersects B.

Blowing up s gives a regular $\mathbb{Z}_3$-scheme $\mathcal{C}$. Its special fiber, shown in Figure 3, has four irreducible components, all isomorphic to $\mathbb{P}^1_{\mathbb{F}_3}$.

The intersection matrix is

	A	B	C	D_2
A	-3	1	0	1
B	1	-5	0	2
C	0	0	-2	1
D_2	1	2	1	-2

(The diagonal entries are computed using the condition that the inner product of each row with the multiplicity vector $(1, 1, 1, 2)$ is 0.)

Let $\mathcal{J}$ be the Néron model of J_5 over $\mathbb{Z}_3$. Then the component group Φ of $\mathcal{J}_{\overline{\mathbb{F}}_3}$ is obtained as follows. View the multiplicity vector as a $\mathbb{Z}$-linear map $\mathbb{Z}^4 \to \mathbb{Z}$. Take the quotient of its kernel by the span of the rows of the intersection matrix. We get an isomorphism $\Phi \simeq \mathbb{Z}/7\mathbb{Z}$.

We will use the homomorphic image $\Phi = \mathbb{Z}/7\mathbb{Z}$ of $\mathcal{J}(\mathbb{F}_3)$ for the sieve. The points P_0, P_1, P_2, P_3 map to components B, C, B, A respectively. If $P \in C_5(\mathbb{Q})$, then the corresponding point on the special fiber lies on A, B, or C (it must be a component of multiplicity 1), and the class of $P - P_0$ in $J(\mathbb{Q})$ maps to the element 3, 0, or 1 in $\mathbb{Z}/7\mathbb{Z}$ accordingly (for a particular choice of isomorphism $\Phi \simeq \mathbb{Z}/7\mathbb{Z}$). In particular, Q_1, Q_2, Q_3 map to $1, 0, 3$ in $\mathbb{Z}/7\mathbb{Z}$.

If moreover $P \in C_5(\mathbb{Q})_{\text{subset}}$, then the image of P in $\mathcal{C}(\mathbb{F}_3)$ is not on A^{smooth} or B^{smooth} in the regular model since smooth points on these components in the regular model map to points in the plane quartic model other than $s = (0 : 1 : 0)$. Therefore the image of P lies on C, and $P - P_0$ maps to 1 in $\mathbb{Z}/7\mathbb{Z}$. Thus if $n_1Q_1 + n_2Q_2 + n_3Q_3 = [P - P_0]$, then

$$n_1 + 3n_3 \equiv 1 \pmod 7. \tag{13.1}$$

13.3. **Sieve information at 2.** We repeat the computations of the previous section, but at the prime 2.

The fiber at 2 of the original plane model consists of a conic A and a line B_2. They are tangent at the point $s_1 := (1 : 0 : 0)$. Because of the multiplicity, no points on B_2 are smooth. But the whole $\mathbb{Z}_2$-scheme is regular except at the points s_1 and $s_2 := (1 : 1 : 1)$ on the special fiber.

Blowing up s_1 yields a model whose special fiber has new components C and D_2, and a new non-regular point s_3 at the intersection of A, B_2, C, D_2. Blowing up s_2 produces new components E and F and a new non-regular point s_4 at the intersection of B_2, E, F. (For the sake of definiteness, label E and F so that $P_3 \in C_5(\mathbb{Q})$ reduces to a point on F.) Blowing up s_3 produces new components G_2 and H_4, and a new non-regular point s_5 at the intersection of A, G_2, H_4. Blowing up s_4 produces a new component I_2, and no new non-regular points. Blowing up s_5 produces new components J_3 and K_4 and a new non-regular point s_6 at the intersection of A, J_3, K_4. Blowing up s_6 produces new components L_4 and M_4 (let L_4 be the one that intersects A) and a new non-regular point s_7 at the intersection of L_4 and M_4. Blowing up s_7 produces new components N_4 and O_4 (let N_4 be the one that intersects L_4)

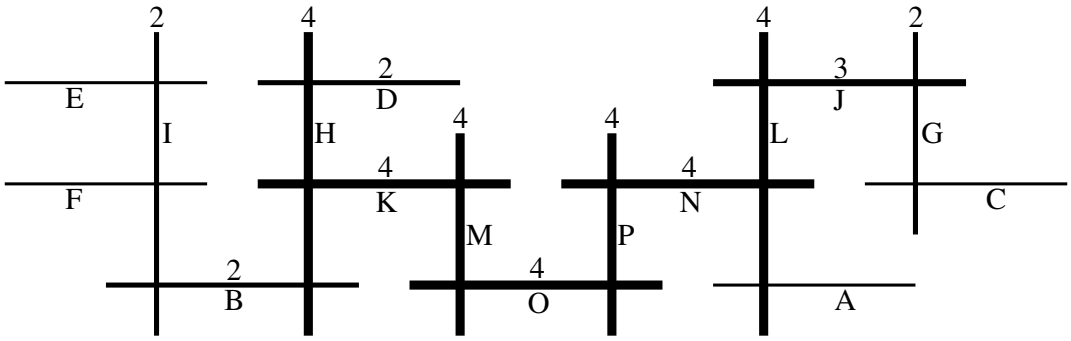


FIGURE 4. The special fiber of C_5 at 2.

---

and a new non-regular point s_8 at the intersection of N_4 and O_4. Blowing up s_8 produces a new component P_4 and no new non-regular points.

The resulting $\mathbb{Z}_2$-scheme $\mathcal{C}$ is regular, and its special fiber has 16 components, all isomorphic to $\mathbb{P}^1_{\mathbb{F}_2}$: see Figure 4. All the intersection numbers are 0 or 1, except the self-intersection numbers, which are -4 for A, -3 for B_2, and -2 for each other component. The points P_0, P_1, P_2, P_3 map to components C, A, A, F respectively.

Let $\mathcal{J}$ be the Néron model of J_5 over $\mathbb{Z}_2$. We find that the component group Φ of $\mathcal{J}_{\overline{\mathbb{F}}_2}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. If $P \in C_5(\mathbb{Q})$, then the corresponding point on the special fiber lies on one of A, C, E, F, and the class of $P - P_0$ in $J(\mathbb{Q})$ maps to $(0,3)$, $(0,0)$, $(1,0)$, $(1,2)$ in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ accordingly (for a particular choice of isomorphism $\Phi \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$). In particular, Q_1, Q_2, Q_3 map to $(0,3)$, $(0,3)$, $(1,2)$ respectively.

If moreover $P \in C_5(\mathbb{Q})_{\text{subset}}$, then P does not reduce to a point on A. Thus

$$n_1(0,3) + n_2(0,3) + n_3(1,2) \equiv (0,0) \text{ or } (1,0) \text{ or } (1,2) \pmod 4. \tag{13.2}$$

13.4. **Sieve information at 23.** Using Magma's `ClassGroup` function, we find that

$$J_5(\mathbb{F}_{23}) \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^4\mathbb{Z}} \times \frac{\mathbb{Z}}{2^4\mathbb{Z}} \times \frac{\mathbb{Z}}{2^5\mathbb{Z}}.$$

Magma also lists the points of $C_5(\mathbb{F}_{23})$ and computes their images in $J_5(\mathbb{F}_{23})$. The condition that the image of $n_1Q_1 + n_2Q_2 + n_3Q_3$ in $J_5(\mathbb{F}_{23})/4J_5(\mathbb{F}_{23})$ be in the image of $C_5(\mathbb{F}_{23})$ forces (n_1, n_2, n_3) to be congruent to one of

000, 001, 002, 010, 011, 021, 030, 100, 101, 102, 110, 113, 220, 303, 312, 322

modulo 4 (we have omitted parentheses and commas within each triple, for readability). Combining this with (13.2), we find that only

$$000, 001, 021, 220$$

are possible. In particular n_1 and n_2 are both even.

13.5. **Sieve information at** 97**.** We have $J_5(\mathbb{F}_{97}) \simeq (\mathbb{Z}/98\mathbb{Z})^3$. The condition that the image of $n_1Q_1 + n_2Q_2 + n_3Q_3$ in $J_5(\mathbb{F}_{97})$ be in the image of $C_5(\mathbb{F}_{97})$ imposes congruence conditions on (n_1, n_2, n_3) modulo 98. Combining these conditions with (13.1) and the condition that n_1 and n_2 be even proves that (n_1, n_2, n_3) is congruent modulo 14 to one of the following:

$$(2, 10, 9), \quad (6, 2, 10), \quad (6, 10, 10), \quad (8, 0, 7).$$

13.6. **Sieve information at** 13**.** The group $J_5(\mathbb{F}_{13})$ is cyclic of order $2 \cdot 7 \cdot 157$. The image of $C_5(\mathbb{F}_{13})$ in $J_5(\mathbb{F}_{13})/14J_5(\mathbb{F}_{13})$ has size 6, and the resulting conditions on (n_1, n_2, n_3) modulo 14 contradict those in the previous paragraph.

13.7. **End of proof.** Finally we must verify that $(J_5(\mathbb{Q}) : \mathcal{Q})$ is prime to 14. By the results in Table 5, $J_5(\mathbb{Q}) \simeq \mathbb{Z}^3$. The image of $\mathcal{Q}$ under $J_5(\mathbb{Q}) \to J_5(\mathbb{F}_{23})/2J_5(\mathbb{F}_{23})$ has $\mathbb{F}_2$-dimension 3, so $2 \nmid (J_5(\mathbb{Q}) : \mathcal{Q})$. The image of $\mathcal{Q}$ under

$$J_5(\mathbb{Q}) \to \frac{J_5(\mathbb{F}_{13})}{7\,J_5(\mathbb{F}_{13})} \times \frac{J_5(\mathbb{F}_{97})}{7\,J_5(\mathbb{F}_{97})}$$

has $\mathbb{F}_7$-dimension 3, so $7 \nmid (J_5(\mathbb{Q}) : \mathcal{Q})$. Thus $C_5(\mathbb{Q})_{\text{subset}} = \emptyset$. This completes the proof of Theorem 1.1.

Acknowledgements

M.S. thanks the University of California at Berkeley for inviting him to visit the Department of Mathematics for two months in 2002; many of the ideas in this paper evolved during this period. Thanks go also to the Deutsche Forschungsgemeinschaft for providing the financial means to pay for this visit through a Heisenberg Fellowship. We thank Ken Ribet for suggesting some of the references in the proof of Lemma 6.1, Jonathan Wahl for suggesting the article [Bri81], and Brian Conrad for a comment regarding modular curves over $\mathbb{Z}$. B.P. and E.S. thank Nils Bruin and the Pacific Institute for the Mathematical Sciences for their hospitality in the summer of 2004: some calculations were doublechecked and some writing was done there. B.P. thanks also the Isaac Newton Institute for a visit in the summer of 2005. B.P. was partially supported by NSF grants DMS-9801104 and DMS-0301280, and a Packard Fellowship. E.S. was partially supported by the NSA grant MDA904-03-1-0030. Computations were done using the software Magma [Magma] and PARI/GP [PARI2].

References

[Ben04] Michael A. Bennett, *The equation $x^{2n} + y^{2n} = z^5$* (2004). Preprint.

[BS04] Michael A. Bennett and Chris M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.MR2031121

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

[Bou98] Nicolas Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998. Translated from the French; Reprint of the 1989 English translation.MR1728312 (2001g:17006)

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).MR1839918 (2002d:11058)

[Bri81] Egbert Brieskorn, *The unfolding of exceptional singularities*, Nova Acta Leopoldina (N.F.) **52** (1981), no. 240, 65–93. Leopoldina Symposium: Singularities (Thüringen, 1978). MR **642697 (83k:**32020)

[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.MR1711307 (2001d:11035)

[Bru00] ———, *On powers as sums of two cubes*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 169–184.MR1850605 (2002f:11029)

[Bru03] ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.MR2011330 (2004j:11051)

[Bru04] ———, *Visualising Sha[2] in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic).MR2047096

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French).MR0004484 (3,14d)

[Che04] Imin Chen, *On the equation* $s^2 + y^{2p} = \alpha^3$ (July 1, 2004). Preprint.

[CW30] C. Chevalley and A. Weil, *Un théorème d'arithmétique sur les courbes algébriques*, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1930), 570–572.

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.MR808103 (87f:11043)

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

[Cre] ———, *Elliptic curve data*. Available at `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`

[CR88] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1988. Reprint of the 1962 original; A Wiley-Interscience Publication.MR1013113 (90g:16001)

[Dar93] Henri Darmon, *The equation* $x^4 - y^4 = z^p$, C. R. Math. Rep. Acad. Sci. Canada **15** (1993), no. 6, 286–290.MR1260076 (94m:11037)

[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)

[DM97] Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.MR1468926 (98h:11076)

[Dar97] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 1, 3–14.MR1479291 (98h:11034a)

[Edw04] Johnny Edwards, *A complete solution to* $X^2 + Y^3 + Z^5 = 0$, J. Reine Angew. Math. **571** (2004), 213–236.MR2070150

[Eic54] Martin Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Arch. Math. **5** (1954), 355–366 (German).MR0063406 (16,116d)

[Elk99] Noam D. Elkies, *The Klein quartic in number theory*, The eightfold way, 1999, pp. 51–101.MR1722413 (2001a:11103)

[Elk00] ———, *Rational points near curves and small nonzero* $|x^3 - y^2|$ *via lattice reduction*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 33–63.MR1850598 (2002g:11035)

[Ell04] Jordan S. Ellenberg, *Galois representations attached to* $\mathbb{Q}$*-curves and the generalized Fermat equation* $A^4 + B^2 = C^p$, Amer. J. Math. **126** (2004), no. 4, 763–787.MR2075481

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366 (German); English transl., *Finiteness theorems for abelian varieties over number fields* (1986), 9–27. Erratum in: Invent. Math. **75** (1984), 381.MR718935 (85g:11026a)

[Fly04] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466.MR2103661

[FLS+01] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697 (electronic).MR1836926 (2002d:11072)

[Ghi02] Dragos Ghioca, September 1, 2002. e-mail message.

[HK03] Emmanuel Halberstadt and Alain Kraus, *Sur la courbe modulaire $X_E(7)$*, Experiment. Math. **12** (2003), no. 1, 27–40 (French, with French summary).MR2002672 (2004m:11090)

[Kle1879] Felix Klein, *Über die Transformationen siebenter Ordnung der elliptischen Funktionen*, Math. Annalen **14** (1879), 428–471 (German); English transl., Felix Klein, *On the order-seven transformation of elliptic functions* **35** (1999), 287–331.MR1722419 (2001i:14042); reprinted in Felix Klein, *Gesammelte mathematische Abhandlungen*, Springer-Verlag, Berlin, 1973. Dritter Band: Elliptische Funktionen, insbesondere Modulfunktionen, hyperelliptische und Abelsche Funktionen, Riemannsche Funktionentheorie und automorphe Funktionen, Anhang verschiedene Verzeichnisse; Herausgegeben von R. Fricke, H. Vermeil und E. Bessel-Hagen (von F. Klein mit ergänzenden Zusätzen versehen) Reprint der Erstauflagen [Verlag von Julius Springer, Berlin, 1923].MR0389520 (52 #10351).

[Kra98] Alain Kraus, *Sur l'équation $a^3 + b^3 = c^p$*, Experiment. Math. **7** (1998), no. 1, 1–13 (French).MR1618290 (99f:11040)

[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

[PARI2] The PARI group, *PARI/GP, version 2*, Bordeaux, 2005. available from `http://pari.math.u-bordeaux.fr`.

[Poo06] Bjorn Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experimental Math. **15** (2006), no. 4, 415–420.

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.MR1465369 (98k:11087)

[Rib90] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.MR1047143 (91g:11066)

[Sal1879] G. Salmon, *A treatise on the higher plane curves*, 3rd ed., Hodges, Foster, and Figgis, Dublin, 1879.

[Sch98] Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471.MR1612262 (99h:11063)

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231 (electronic).MR2021618 (2004g:11045)

[Sch04] Victor Scharaschkin, *The Brauer-Manin obstruction for curves* (December 2004). Preprint.

[Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230 (French).MR885783 (88g:11022)

[Ser02] ———, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.MR1867431 (2002i:12004)

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.MR 95m:11054

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.MR1845760 (2002d:14032)

[Ste] William A. Stein, *Modular forms database*. Available at `http://modular.math.washington.edu/Tables/index.html` .

[Sto06a] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR 2264661

[Sto06b] ———, *Finite descent and rational points on curves*, November 22, 2006. Preprint.

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.MR1333036 (96d:11072)

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.MR1333035 (96d:11071)

[Wil01] Robert A. Wilson, *The Monster is a Hurwitz group*, J. Group Theory **4** (2001), no. 4, 367–374.MR1859175 (2002f:20022)

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

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053, USA
E-mail address: `eschaefe@math.scu.edu`

School of Engineering and Science, International University Bremen, P.O.Box 750561, 28725 Bremen, Germany.
E-mail address: `m.stoll@iu-bremen.de`