MATHEMATICS OF COMPUTATION
https://doi.org/10.1090/mcom/3407
Article electronically published on December 28, 2018

QUADRATIC POINTS ON MODULAR CURVES

EKIN OZMAN AND SAMIR SIKSEK

Abstract. In this paper we determine the quadratic points on the modular curves $X_0(N)$, where the curve is non-hyperelliptic, the genus is 3, 4, or 5, and the Mordell–Weil group of $J_0(N)$ is finite. The values of N are 34, 38, 42, 44, 45, 51, 52, 54, 55, 56, 63, 64, 72, 75, 81.

As well as determining the non-cuspidal quadratic points, we give the j-invariants of the elliptic curves parametrized by those points, and determine if they have complex multiplication or are quadratic $\mathbb{Q}$-curves.

1. Introduction

Let N be a positive integer. By the work of Mazur [26], we have a complete understanding of rational points on the modular curves $X_1(N)$; namely if $X_1(N)$ is of genus ≥ 1, then the only rational points are cuspidal. Merel's celebrated uniform boundedness theorem [28] asserts that for $d \geq 1$, there is some bound B_d such that if K is a number field of degree $\leq d$, and $N \geq B_d$ is prime, then the only K-rational points on $X_1(N)$ are cuspidal. There are more precise results for small fixed degrees d. Kamienny [19] showed that if $N \geq 17$ is prime, then $X_1(N)$ has no quadratic points, and the corresponding result for cubic points was proved by Parent [32,33]. This has recently been extended to degrees 4, 5, 6 by Derickx, Kamienny, Stein, and Stoll [10].

The situation concerning low-degree points on the family $X_0(N)$ is much less happy. In fact we only have complete results for the case of rational points. Mazur [27] proved that the only rational points on $X_0(N)$ are cusps when N is prime and greater than 163. Later, these results were extended to composite levels and completed by Kenku (see [22] and the references therein). Results of Bars [3] and Harris and Silverman [17] assert that if $X_0(N)$ has genus ≥ 2, then it has finitely many quadratic points, except for 28 values of N. A result of Aigner [1] gives all the solutions in quadratic fields to the Fermat equation $x^4 + y^4 = z^4$ which is isomorphic to $X_0(64)$. Recently, Bruin and Najman [5] parametrized all quadratic points on $X_0(N)$ explicitly for those values of N where $X_0(N)$ is hyperelliptic and $J_0(N)$ has Mordell–Weil rank 0; namely those values of N belonging to the set

$$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}.$$

Received by the editor June 21, 2018, and, in revised form, August 16, 2018, and October 2, 2018.

2010 *Mathematics Subject Classification.* Primary 11G05, 14G05, 11G18.

Key words and phrases. Modular curves, quadratic points, Mordell–Weil, Jacobian.

The first-named author was partially supported by Bogazici University Research Fund Grant Number 10842 and TUBITAK Research Grant 117F045.

The second-named author was supported by an EPSRC LMF: L-Functions and Modular Forms Programme Grant EP/K034383/1.

In this paper we focus on non-hyperelliptic $X_0(N)$ of genera 3, 4, 5 where the Mordell–Weil group $J_0(N)(\mathbb{Q})$ is finite. We determine the quadratic points on these modular curves, and supply the modular interpretation of the points. In the forthcoming second part of this work [31] we deal with those values of N for which the genus is 3, 4, 5 but $J_0(N)(\mathbb{Q})$ is infinite, using a version of Chabauty for symmetric powers of curves as in [36].

Lemma 1.1. *The values of N for which $X_0(N)$ is non-hyperelliptic, of genus g where $3 \leq g \leq 5$, and for which $J_0(N)(\mathbb{Q})$ is finite are*

genus 3: 34, 45, 64;
genus 4: 38, 44, 54, 81;
genus 5: 42, 51, 52, 55, 56, 63, 72, 75.

Let X be a curve defined over $\mathbb{Q}$. A point $P \in X$ is called *quadratic* if the field $\mathbb{Q}(P)$ is a quadratic extension of $\mathbb{Q}$.

Main Theorem. *For the values of N listed in Lemma* 1.1 *the quadratic points on $X_0(N)$ are as given in the tables of Section* 8.

For the non-cuspidal quadratic points, we compute j-invariants of the elliptic curves parametrized by them. In addition, we check whether those points are related via any Atkin–Lehner involutions and decide whether or not they have complex multiplication or are $\mathbb{Q}$-curves.

One motivation for this work is the current interest in the Fermat equation over quadratic fields and similar Diophantine problems. The approach via modularity and level-lowering requires the irreducibility of the mod p representation of a Frey elliptic curve defined over the given quadratic field, K say. This Frey elliptic curve often has extra level structure in the form of a K-rational 2 or 3-isogeny. If the mod p representation is reducible, then the Frey curve gives rise to a K-rational point on $X_0(2p)$ or $X_0(3p)$, and thus having a parametrization of quadratic points is useful in establishing irreducibility for small values of p. The results of the current paper have already proved useful in that context [16].

A theoretical approach to the problem. Let $X/\mathbb{Q}$ be a non-hyperelliptic curve of genus ≥ 3 with $J(\mathbb{Q})$ finite, where J is the Jacobian of X, and suppose for convenience that X has at least one rational point P_0. For example X could be any of the curves $X_0(N)$ for the values of N in Lemma 1.1. There is a straightforward theoretical method (see for instance [15]) of computing all effective degree 2 rational divisors on X, and hence all points defined over quadratic extensions, provided we are able to enumerate all the elements of $J(\mathbb{Q})$. Let $X^{(2)}$ denote the second symmetric product of X. A $\mathbb{Q}$-rational point on $X^{(2)}$ can be represented by an unordered pair $\{P_1, P_2\}$, where P_1, P_2 are either both rational points on X, or are defined over a quadratic field and Galois conjugate. Let $D = P_1 + P_2$ and let $\iota : X^{(2)}(\mathbb{Q}) \to J(\mathbb{Q})$ be the map which sends D to $[D - 2P_0]$. Since X is not hyperelliptic, ι is injective. By pulling back the finitely many points in $J(\mathbb{Q})$, it is theoretically possible to determine $X^{(2)}(\mathbb{Q})$, and hence the quadratic points of X, as follows. For any $\mathbb{Q}$-rational point on $X^{(2)}$, the corresponding degree 2 divisor D is linearly equivalent to $D' + 2P_0$ for some $[D']$ in $J(\mathbb{Q})$ (where D' is a rational degree 0 divisor on X). Thus, for each $[D']$ in $J(\mathbb{Q})$, we need to enumerate the effective degree 2 divisors linearly equivalent to $D' + 2P_0$. For each $[D']$ in $J(\mathbb{Q})$ we compute the Riemann–Roch space $L(D' + 2P_0)$. As the curve is non-hyperelliptic

the dimension of this space is either 0 or 1. If it has dimension 0, then there is no effective degree 2 divisor D linearly equivalent to $D'+2P_0$. If it has dimension 1, we let f be a non-zero element of this space, and then $D'+2P_0+\mathrm{div}(f)$ is the unique effective degree 2 divisor linearly equivalent to $D'+2P_0$. There are potentially two problems with this approach:

- It is often not convenient or practical to compute $J(\mathbb{Q}) = J(\mathbb{Q})_{\mathrm{tors}}$.
- Even if we can compute $J(\mathbb{Q})$, it can be a large group, and the Riemann–Roch computations might not be practical for some of the more complicated elements $[D']$ of $J(\mathbb{Q})$.

Our approach. For the modular curves of interest to us we first compute the rational cuspidal subgroup $C = C_0(N)(\mathbb{Q})$ (see below for definition) and bound its index inside $J(\mathbb{Q})$, where $J = J_0(N)$. We therefore know a positive integer I such that $I \cdot J(\mathbb{Q}) \in C$. It follows that the effective degree 2 divisors D we seek satisfy $[D - 2P_0] = I \cdot [D']$, where $[D'] \in J(\mathbb{Q})$. We then employ a version of the Mordell–Weil sieve to help us eliminate most possibilities for D'. Only then do we use Riemann–Roch to recover the divisors D.

Programs. The computations described in this paper have been performed using the `Magma` computer algebra package [4]. Our `Magma` code is available with the `arXiv` version of the paper at `https://arxiv.org/abs/1806.08192`.

The generalized Ogg conjecture. For now let N be any positive integer. Let $C_0(N)$ be the subgroup of $J_0(N)(\overline{\mathbb{Q}})$ generated by classes of differences of cusps; this is known as the cuspidal subgroup. Write $C_0(N)(\mathbb{Q})$ for the subgroup of $C_0(N)$ of points stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; this is known as the rational cuspidal subgroup, and is contained in $J_0(N)(\mathbb{Q})$. The Manin–Drinfel′d theorem [25], [12] in fact asserts that $C_0(N) \subseteq J_0(N)(\overline{\mathbb{Q}})_{\mathrm{tors}}$, and thus $C_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tors}}$. A conjecture of Ogg, proved by Mazur [26], says that $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ for N prime. A "generalized Ogg conjecture" (stated for example in [35]) asserts that this equality holds for all positive N. Our computations verify the conjecture for most of the values of N mentioned in the statement of Main Theorem.

Theorem 1.2. *The generalized Ogg conjecture holds for* $N = 34, 38, 44, 45, 51, 52, 54, 56, 64, 81$.

For recent partial results towards the generalized Ogg conjecture see [35], [23], [29], [41].

2. Choices of $X_0(N)$: Proof of Lemma 1.1

Ogg [30] has shown that the values of N for which $X_0(N)$ is hyperelliptic are

$$22,\ 23,\ 26,\ 28,\ 29,\ 30,\ 31,\ 33,\ 35,\ 37,\ 39,\ 40,\ 41,\ 46, 47,\ 48,\ 50,\ 59,\ 71.$$

The genus of $X_0(N)$ grows with N and there are only finitely many values of N for any given genus g. Using the explicit formula for the genus (e.g., [11, Section 3.9]), which is also the dimension formula for $S_2(N)$, we found the values of N for which $X_0(N)$ is non-hyperelliptic and has genus $3 \le g \le 5$ to be

genus 3: 34, 43, 45, 64;
genus 4: 38, 44, 53, 54, 61, 81;
genus 5: 42, 51, 52, 55, 56, 57, 63, 65, 67, 72, 73, 75.

We need to decide on the values of N in this list for which $J_0(N)$ has rank 0. For this we briefly recall standard facts about the decomposition of $J_0(N)$ as a product of abelian varieties of GL_2-type; for more details see for example Stein's thesis [38].

Let $f_1, \ldots, f_k$ be representatives of the Galois-conjugacy classes of Hecke eigenforms in $S_2(N)$. Let K_i be the (totally real) number field generated by the coefficients of f_i, and let d_i be its degree. Attached to each f_i (or more precisely to its Galois-conjugacy class) is an abelian variety $\mathcal{A}_i/\mathbb{Q}$ of dimension d_i whose endomorphism ring contains an order in K_i. In particular the rank of $\mathcal{A}_i(\mathbb{Q})$ is a multiple of d_i. The modular Jacobian $J_0(N)$ is isogenous to $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$. Thus $J_0(N)(\mathbb{Q})$ is finite if and only if the $\mathcal{A}_i$ all have rank 0. Let $\mathcal{A}$ be any of the $\mathcal{A}_i$. We write $L(\mathcal{A}, s)$ for the L-function of $\mathcal{A}$. The conjecture of Birch and Swinnerton-Dyer asserts that the rank of $\mathcal{A}(\mathbb{Q})$ is equal to the order of vanishing of $L(\mathcal{A}, s)$ at $s = 1$. A deep theorem of Kolyvagin and Logachev [21] asserts that if $L(\mathcal{A}, 1) \neq 0$, then $\mathcal{A}(\mathbb{Q})$ has rank 0. In fact an algorithm of Stein [38, Chapter 3] allows us to compute the exact value $L(\mathcal{A}, 1)/\Omega_{\mathcal{A}} \in \mathbb{Q}$, where $\Omega_{\mathcal{A}}$ is the real volume of $\mathcal{A}$. Using the `Magma` "modular abelian varieties package", which is an implementation by Stein of his algorithms [39], [38] we computed the ratios $L(\mathcal{A}, 1)/\Omega_{\mathcal{A}}$ and found them all to be non-zero for the values of N listed in the statement of Lemma 1.1. Thus we know that $J(\mathbb{Q})$ is finite for those values. It remains to show that $J(\mathbb{Q})$ is infinite for the remaining values 43, 53, 61, 57, 65, 67, 73; for these we claim the ranks respectively are 1, 1, 1, 1, 1, 2, 2. For each of these values of N, there is only one factor $\mathcal{A}$ for which $L(\mathcal{A}, 1) = 0$, and thus the rank of $J_0(N)$ is equal to the rank of $\mathcal{A}$. For $N = 43$, 53, 61, 57, 65 this factor $\mathcal{A}$ happens to be a rank 1 elliptic curve, completing the proof in those cases. For $N = 67$ and 73 this factor is simply $J_0^+(N)$ which in both cases is 2-dimensional, and it remains to show that this has rank 2 in both cases. For both values, a model for the genus 2 curve $X_0^+(N)$ is given by Galbraith [13, page 43]. Using the `Magma` implementation of Stoll's 2-descent algorithm [40] we checked that the rank of $J_0^+(N)$ is indeed 2 in both cases.

3. Computing equations for the $X_0(N)$, Atkin–Lehner involutions, j-maps, and cusps

Let N be such that the modular curve $X_0(N)$ has genus $g \geq 3$ and is non-hyperelliptic. Then the canonical map embeds $X_0(N)$ into projective space $\mathbb{P}^{g-1}$ as a smooth curve of degree $2g-2$, and it is this model that we work with. An algorithm for writing down the model is given by Galbraith [13]. Although equations for $X_0(N)$ for most of the N we consider are already given by Galbraith, we need to redo his computations so that we can explicitly construct the Atkin–Lehner involutions on the models, and also the j-map $X_0(N) \to X(1)$. We start by briefly recalling Galbraith's method.

Let $S_2(N)$ be the space of weight 2 cuspforms of level N with q-expansion coefficients belonging to $\mathbb{Q}$; this has dimension $g = \mathrm{genus}(X_0(N))$. The cuspforms in $S_2(N)$ can be identified with the regular differentials on $X_0(N)/\mathbb{Q}$ via the map $f(q) \mapsto 2\pi i f(q) dq/q$. Fix a $\mathbb{Q}$-basis for $f_0, \ldots, f_{g-1}$ for $S_2(N)$; such a basis may be computed as q-expansions to a desired precision via the modular symbols algorithm [8], [39]. Now let $F \in \mathbb{Q}[x_0, \ldots, x_{g-1}]$ be homogeneous of degree d. Then $F(f_0, \ldots, f_{g-1})$ is a cuspform of weight $2d$ and level N. Write

$$I = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

By Sturm's Theorem (e.g., [39, Theorem 9.18]), $F(f_0, \dots, f_{g-1}) = 0$ if and only if the q-expansion $F(f_0(q), \dots, f_{g-1}(q)) = O(q^r)$ with $r = \lfloor dI/6 \rfloor + 1$. Thus determining the vector space of all homogeneous F of degree d such that $F(f_0, \dots, f_{g-1}) = 0$ is a straightforward linear algebra computation, and carrying this out for $d \mid (2g-2)$ ensures that we have a system of equations that cuts out a model for $X_0(N)$ in $\mathbb{P}^{g-1}$. For the values of N in Lemma 1.1 we carried this out and, conveniently, found a model for $X_0(N)$ that has good reduction away from the primes dividing N. The equations for these models are given in our tables at the end.

Next we would like to work out the Atkin–Lehner involutions on $X_0(N)$. Let $m \mid N$ such that $\gcd(m, N/m) = 1$ and $m \neq 1$. The modular symbols algorithm gives the action of the Atkin–Lehner operator w_m as a linear operator of order 2 on $S_2(N)$ and hence as an order 2 matrix of size $g \times g$ with entries in $\mathbb{Q}$. Now the linear automorphism on $\mathbb{P}^{g-1}$ induced by this matrix restricts to the Atkin–Lehner involution w_m on $X_0(N)$.

Next we describe how we obtain the map $j : X_0(N) \to X(1)$; this is not described in [13] but similar computations are found in [2] and [15]. We start with largest divisor $n \mid N$ for which we already know the following:

(i) equations for $X_0(n)$;
(ii) generators $u_1, \dots, u_s$ for the function field of $X_0(n)$ together with their q-expansions at the cusp at infinity (these will in general be Laurent series);
(iii) the map $X_0(n) \to X(1)$.

In fact, for all values of N that we consider, we found that the `Magma` "small modular curves" package gives (i), (ii), (iii) with n the largest proper divisor of N. The idea is to construct the degeneracy map $X_0(N) \to X_0(n)$ whence composition with $X_0(n) \to X(1)$ gives the desired $j : X_0(N) \to X(1)$. For this it is sufficient to construct the pull-backs of $u_1, \dots, u_s$ to $X_0(N)$ which we denote by $U_1, \dots, U_s$. Fix $1 \leq i \leq s$ and let $U = U_i$ and $u = u_i$. Then U is a rational function on $X_0(N)$, and hence can be written as

$$U = \frac{F(x_0, \dots, x_{g-1})}{G(x_0, \dots, x_{g-1})},$$

where F, G are homogeneous in $\mathbb{Q}[x_0, \dots, x_{g-1}]$ of equal degree d. These satisfy

$$F(f_0(q), \dots, f_{g-1}(q)) - u(q) \cdot G(f_0(q), \dots, f_{g-1}(q)) = 0, \tag{3.1}$$

where $u(q)$ is the known q-expansion for u. Fix a degree d. Let V_d be the vector space of all homogeneous $\mathbb{Q}[x_0, \dots, x_{g-1}]$ of degree d and let V'_d be the subspace belonging to the homogeneous ideal generated by the equations of $X_0(N)$. Note that if $H \in V'_d$, then $H(f_0(q), \dots, f_{g-1}(q)) = 0$. Thus we may think of (3.1) as a linear equation in $(F, G) \in V_d/V'_d \times V_d/V'_d$, and we would like to find a non-trivial solution (for a suitable choice of d). Fixing d and a large "precision" m we consider the linear system of equations

$$F(f_0(q), \dots, f_{g-1}(q)) - u(q)G(f_0(q), \dots, f_{g-1}(q)) = O(q^m), \tag{3.2}$$

in $(F, G) \in V_d/V'_d \times V_d/V'_d$. By choosing d large enough we were always able to find a non-trivial solution (F, G) and thus a highly plausible guess for $U = F/G$ (we took $m = 500$ in all our examples). Next we checked that the guesses $U_1, \dots, U_s$ do in fact give a map $X_0(N) \to X_0(n)$ and we composed this with the known $X_0(n) \to X(1)$ to obtain a proposed j-function $X_0(N) \to X(1)$ which for now we denote by j'. We did not prove the correctness of the degeneracy map $X_0(N) \to X_0(n)$ (which we do

not use later), but we did prove the correctness of the proposed j-function on $X_0(N)$ as we now explain. For now we think of j and j' as elements of the function field of $X_0(N)$. The above procedure gives $j' = H_1(x_0, \ldots, x_{g-1})/H_2(x_0, \ldots, x_{g-1})$, where H_1, H_2 are homogeneous in $\mathbb{Q}[x_0, \ldots, x_{g-1}]$ of equal degree. The q-expansion for j' is given by $j'(q) = H_1(f_1(q), \ldots, f_{g-1}(q))/H_2(f_1(q), \ldots, f_{g-1}(q))$ and by computing enough terms we checked that $j(q) - j'(q) = O(q^m)$ for some large m, where

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

is the usual expansion of the j-function. Note that here we cannot simply apply Sturm's Theorem to deduce $j = j'$ as we have not shown that $j - j'$ is a modular form (i.e., holomorphic at all the cusps of $X_0(N)$), so we adopt a different approach. Let D and D' be the divisor of poles for j and j', respectively. By [11, pages 106–107], for $N > 2$,

$$\deg(D) = \deg(j) = \frac{N^2}{\varphi(N)} \cdot \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right),$$

where φ denotes the Euler totient-function. Since we know j' we can compute D' explicitly and we checked that $\deg(D') = \deg(D)$ in all cases. Now if $j \neq j'$, then the divisor of poles for $j - j'$ is bounded by $D + D'$ and so has degree at most $2\deg(D)$. But the order of vanishing of $j - j'$ at the cusp ∞ is at least m. Since the divisor of zeros has the same degree as the divisor of poles we deduce that $m \leq 2\deg(D)$. In all cases m exceeded $2\deg(D) + 1$ by a huge margin, proving $j = j'$.

We note in passing that the `Magma` "small modular curves" package is a wonderful resource, but that the justification for the modular curves data is only very briefly sketched in the `Magma` handbook. Whilst we make use of this package to guess the j-function on $X_0(N)$ our subsequent proof of the correctness of our guess is independent of it.

Finally, as we have the j-map we can compute the cusps; these are merely the poles of j.

4. An extension problem for finite abelian groups

Let C, A_1, A_2 be finite abelian groups and suppose $\iota_j : C \to A_j$ are injective homomorphisms. In this section we address the following question: *is there an isomorphism $\psi : A_1 \to A_2$ such that $\psi \circ \iota_1 = \iota_2$?* This is a problem we will need to address later on where C happens to be the rational cuspidal subgroup of $J_0(N)$ and A_1, A_2 are candidates for $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ obtained from local information. Let p be a prime, and write $C[p^\infty]$, $A_1[p^\infty]$, and $A_2[p^\infty]$ for the p-power torsion in C, A_1, and A_2. Clearly the question has a positive answer if and only if the corresponding question for $C[p^\infty]$, $A_1[p^\infty]$, and $A_2[p^\infty]$ has a positive answer for every prime p dividing the orders of the groups A_1, A_2. Thus we may suppose that C, A_1, A_2 are p-power torsion finite abelian groups for some prime p.

Of course the question has a negative answer if A_1 is not isomorphic to A_2. Thus first we make sure that A_1, A_2 are isomorphic and write down an explicit isomorphism $\psi_0 : A_1 \to A_2$. Next we can write down the automorphism group of A_2 and deduce the set of all isomorphisms $A_1 \to A_2$; any such isomorphism will be a composition of ψ_0 with an automorphism of A_2. These steps can be carried out using for example algorithms explained in [7] and implemented in `Magma`.

Now we may simply test the isomorphisms $\psi : A_1 \to A_2$ and see if there is one that satisfies $\psi \circ \iota_1 = \iota_2$. This strategy does provide a theoretical answer to our question. In our application we have found it impractical as the automorphism groups $\mathrm{Aut}(A_i)$ are enormous. As an illustration we point out that if $A = (\mathbb{Z}/p\mathbb{Z})^n$, then $\mathrm{Aut}(A) \cong \mathrm{GL}_n(\mathbb{F}_p)$. Thus whilst $\#A = p^n$, we have $\#\,\mathrm{Aut}(A) = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

Write $B_i = A_i/\iota_i(C)$ and let $\pi_i : A_i \to B_i$ be the quotient maps. Any isomorphism $\psi : A_1 \to A_2$ satisfying $\psi \circ \iota_1 = \iota_2$ induces an isomorphism $\mu : B_1 \to B_2$ that makes the diagram (4.1) commute, where the two rows are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C & \xrightarrow{\iota_1} & A_1 & \xrightarrow{\pi_1} & B_1 & \longrightarrow & 0 \\ & & \| & & \psi\downarrow & & \mu\downarrow & & \\ 0 & \longrightarrow & C & \xrightarrow{\iota_2} & A_2 & \xrightarrow{\pi_2} & B_2 & \longrightarrow & 0 \end{array} \tag{4.1}$$

Thus we know that our question has a negative answer if B_1, B_2 are not isomorphic. We suppose that they are isomorphic and we enumerate all isomorphisms $\mu : B_1 \to B_2$ (by computing the automorphism group of B_2). In our application the groups B_i tend to be rather small and so there are far fewer isomorphisms $B_1 \to B_2$ than isomorphisms $A_1 \to A_2$. For each μ we now ask the following: is there an isomorphism $\psi : A_1 \to A_2$ that makes the diagram (4.1) commute? In essence we can interpret both exact sequences as extensions of B_2 by C and we are asking if they are equivalent extensions. However we are interested in answering this question in the category of finite abelian groups and would like to avoid computing $\mathrm{Ext}(B_2, C)$ (which classifies all extensions of B_2 by C including the non-abelian ones) as well as avoiding the computation of the images of the two sequences in this group. The following proposition gives us an efficient way of answering the question in the category of finite abelian groups.

Proposition 4.1. *Let*

$$0 \to C \xrightarrow{\iota_i} A_i \xrightarrow{\pi_i} B_i \to 0$$

be exact sequences of finite abelian groups for $i = 1, 2$. Let $\mu : B_1 \to B_2$ be an isomorphism. Let $x_1, \ldots, x_r$ be any elements of A_1 such that A_1 is generated by $\iota_1(C)$ together with $x_1, \ldots, x_r$. Let $y_1, \ldots, y_r \in A_2$ satisfy $\pi_2(y_j) = \mu(\pi_1(x_j))$ for $j = 1, \ldots, r$ (these must exist as π_2 is surjective). Write $\mathbf{x} = (x_1, \ldots, x_r) \in A_1^r$ and $\mathbf{y} = (y_1, \ldots, y_r) \in A_2^r$. Let $\mathcal{A} = \mathbb{Z}^r \times C$. Let $\tau : \mathcal{A} \to A_1$ be given by

$$\tau(\mathbf{m}, c) = \mathbf{m} \cdot \mathbf{x} + \iota_1(c) \qquad \text{for } \mathbf{m} \in \mathbb{Z}^r \text{ and } c \in C;$$

here $(m_1, \ldots, m_r) \cdot (x_1, \ldots, x_r)$ is shorthand for the linear combination $m_1x_1 + \cdots + m_rx_r$. Let $(\mathbf{n}_1, c_1), \ldots, (\mathbf{n}_s, c_s)$ be a set of generators for the kernel of τ. Define a homomorphism

$$\eta : C^r \to A_2^s, \qquad \mathbf{t} \mapsto (\iota_2(\mathbf{n_1} \cdot \mathbf{t}), \ldots, \iota_2(\mathbf{n_s} \cdot \mathbf{t})),$$

and let

$$\kappa = (\mathbf{n}_1 \cdot \mathbf{y} + \iota_2(c_1), \ldots, \mathbf{n}_s \cdot \mathbf{y} + \iota_2(c_s)) \in A_2^s.$$

Then there exists an isomorphism $\psi : A_1 \to A_2$ making the diagram (4.1) commute if and only if $\kappa \in \mathrm{Image}(\eta)$.

Proof. Suppose κ belongs to the image of η. We will show the existence of a homomorphism $\psi : A_1 \to A_2$ making the diagram (4.1) commute. It then easily follows that ψ must be an isomorphism (this fact is known as the *short-five lemma*).

As κ is in the image of η, so is $-\kappa$. Thus there is some $\mathbf{t} = (t_1, \ldots, t_r) \in C^r$ such that

$$\mathbf{n}_j \cdot \mathbf{y} + \iota_2(c_j) = -\iota_2(\mathbf{n}_j \cdot \mathbf{t}), \qquad j = 1, \ldots, s. \tag{4.2}$$

Let

$$\sigma : \mathcal{A} \to A_2, \qquad \sigma(\mathbf{m}, c) = \mathbf{m} \cdot \mathbf{y} + \iota_2(\mathbf{m} \cdot \mathbf{t}) + \iota_2(c) \qquad \text{for } \mathbf{m} \in \mathbb{Z}^r \text{ and } c \in C.$$

Recall that $(\mathbf{n}_1, c_1), \ldots, (\mathbf{n}_s, c_s)$ are generators for the kernel of $\tau : \mathcal{A} \to A_1$. Condition (4.2) ensures that the kernel of τ is contained in the kernel of $\sigma : \mathcal{A} \to A_2$. Thus we obtain a well-defined homomorphism $\mathcal{A}/\operatorname{Ker}(\tau) \to \mathcal{A}/\operatorname{Ker}(\sigma) \to A_2$. By hypothesis A_1 is generated by $x_1, \ldots, x_r$ and $\iota_1(C)$, thus $\tau : \mathcal{A} \to A_1$ is surjective. We let ψ be the composition

$$A_1 \xrightarrow{\sim} \mathcal{A}/\operatorname{Ker}(\tau) \to \mathcal{A}/\operatorname{Ker}(\sigma) \to A_2.$$

It follows from the definitions of τ and σ that ψ sends $\iota_1(c)$ to $\iota_2(c)$ for any $c \in C$, and sends x_j to $y_j + \iota_2(t_j)$ for $j = 1, \ldots, r$. In particular, the left-hand square of (4.1) commutes. Moreover

$$\pi_2(\psi(x_j)) = \pi_2(y_j + \iota_2(t_j)) = \pi_2(y_j) = \mu(\pi_1(x_j)),$$

where the last equality comes from our original definition of the y_j. Since $x_1, \ldots, x_j$ together with $\iota_1(C)$ generate A_1 the right-hand square of (4.1) also commutes.

Now conversely suppose there is an isomorphism $\psi : A_1 \to A_2$ making (4.1) commute. Thus $\pi_2(\psi(x_j)) = \mu(\pi_1(x_j)) = \pi_2(y_j)$. By the exactness of the bottom row, $\psi(x_j) = y_j + \iota_2(t_j)$ for some $t_j \in C$. Now let $(\mathbf{n}_i, c_i)$ be as in the statement of the theorem. Thus $\mathbf{n}_i \cdot \mathbf{x} + \iota_1(c_i) = 0$. Letting $\mathbf{t} = (t_1, \ldots, t_r)$ and applying ψ we have

$$\mathbf{n}_i \cdot \mathbf{y} + \iota_2(\mathbf{n}_i \cdot \mathbf{t}) + \iota_2(c_i) = 0.$$

It follows that $\kappa = \eta(-\mathbf{t})$, completing the proof. □

5. The Mordell–Weil information

Now let N be one of the values of N in Lemma 1.1. In this section we explain how we compute the structure of the rational cuspidal subgroup $C_0(N)(\mathbb{Q})$ as well as deducing a small integer I such that $I \cdot J_0(N)(\mathbb{Q})_{\text{tors}} \subseteq C_0(N)(\mathbb{Q})$.

5.1. `Magma` **computations in Jacobians of curves.** It is more convenient computationally to work with places of a curve than with points defined over various extensions of the base field. Let X be a smooth projective curve over a perfect field F. A place $\mathcal{P}$ of X is simply a set of distinct points $\{P_1, \ldots, P_n\} \subset X(\overline{F})$ that is stable under the action of $\operatorname{Gal}(\overline{F}/F)$ and forms a single orbit under that action. The size n is called the degree of $\mathcal{P}$. It also happens to be the degree of $F(P_i)/F$ for any i. It is often convenient to think of $\mathcal{P}$ as the effective degree n rational divisor $P_1 + \cdots + P_n \in \operatorname{Div}(X/F)$, and indeed any rational divisor can be written uniquely as an integral linear combination of places. We shall make use of the "algebraic function fields" package within `Magma`, which carries out computations in $\operatorname{Div}(X/F)$ and more importantly in the quotient $\operatorname{Pic}(X/F)$ and its degree 0 part $\operatorname{Pic}^0(X/F) \cong J(F)$ (for this latter isomorphism to hold we need to suppose the existence of a degree 1 place on X). For the theory behind these algorithms see Hess' paper [18]. When $F = \mathbb{Q}$ or a number field some of the computations we would like to do become impractical, particularly in the genus 5 cases. However `Magma` computations in $\operatorname{Pic}^0(X/F)$ are much more efficient when F is a finite field, and

in fact the `Magma` implementation of Hess' algorithm does compute the structure of $\mathrm{Pic}^0(X/F) \cong J(F)$ in all the cases of interest to us, where F is a finite field of characteristic p, with p a prime of good reduction for our model $X = X_0(N)$. Our strategy is to carry out as much of the computations over finite fields as possible. A particularly useful fact for us is the following. Let X be a curve defined over a number field K, let $p > 2$ be a rational prime, and let $\mathfrak{p}$ be a prime of K above p of ramification degree 1 and of good reduction for X. Then a theorem of Katz [20, appendix] asserts that the composition of natural maps $J(K)_{\mathrm{tors}} \hookrightarrow J(K) \to J(\mathbb{F}_{\mathfrak{p}})$ is an injection. In particular we may identify $J(K)_{\mathrm{tors}}$ as a subgroup of $J(\mathbb{F}_{\mathfrak{p}})$.

5.2. **A closer look at the rational cuspidal subgroup.** To ease notation we shall write X and J for $X_0(N)$ and $J_0(N)$. Let d^2 be the largest square divisor of N, and let $K = \mathbb{Q}(\zeta_d)$ be the dth cyclotomic field. The cusps of X are all defined over K. Let these be $P_0, \ldots, P_k$ with P_0 defined over $\mathbb{Q}$ (there are always at least two rational cusps: the ∞ cusp and the 0 cusp). Henceforth P_0 will be the basepoint for the Abel–Jacobi map $X \to J$. Let

$$\mathcal{D} = \sum_{i=1}^{k} \mathbb{Z} \cdot (P_i - P_0).$$

This is the subgroup of $\mathrm{Div}^0(X/K)$ supported on the cusps. Write $G = \mathrm{Gal}(K/\mathbb{Q})$; this acts naturally on $\mathcal{D}$ and we denote by $\mathcal{D}^G$ the subgroup of divisors that are stable under G (these are the degree 0, $\mathbb{Q}$-rational divisors supported on the cusps). Write

$$C' = \{[D] \ : \ D \in \mathcal{D}^G\}$$

for the image of $\mathcal{D}$ in $J(\mathbb{Q})$. Now G also acts on the subgroup

$$\mathcal{E} = \sum_{i=1}^{k} \mathbb{Z} \cdot [P_i - P_0]$$

of $J(K)$. The group $\mathcal{E}^G \subset J(\mathbb{Q})$ is precisely the rational cuspidal subgroup $C = C_0(N)(\mathbb{Q})$. Of course C' is contained inside C, and it is natural to ask if they are equal.

Lemma 5.1. *Let N be one of the values in Lemma* 1.1. *Then $C = C'$. In other words, every degree* 0 *rational divisor class supported on the cusps is the class of a degree* 0 *rational divisor supported on the cusps.*

The lemma will bring some simplifications to our later computations comparing C with the torsion subgroup. We note in passing that as $X(\mathbb{Q}) \neq \emptyset$, it is known [34, Section 3] that every degree 0 rational divisor class is the class of a degree 0 rational divisor. However, applying this to a degree 0 rational divisor class supported on the cusps does yield a degree 0 rational divisor defining the same class, but that divisor need not be supported on the cusps.

Proof of Lemma 5.1. Since we have the cusps as points on X with coordinates in K, we can compute $\mathcal{E}^G$.

Now let $p \nmid 2N$ be a rational prime and let $\mathfrak{p}$ be a prime of K above p. In particular $p \nmid d$ and so $\mathfrak{p}$ is an unramified prime. It follows from the aforementioned

theorem of Katz that the reduction modulo $\mathfrak{p}$ map $\pi : J(K)_{\mathrm{tors}} \to J(\mathbb{F}_{\mathfrak{p}})$ is injective. For $\sigma \in G$ we let

$$\mu_\sigma : \mathcal{D} \to J(\mathbb{F}_{\mathfrak{p}}), \qquad D \mapsto \pi(D^\sigma - D).$$

It follows from the injectivity of π that $[D]^\sigma = [D]$ if and only if $\mu_\sigma(D) = 0$. Let

$$\mathcal{F} = \bigcap_{\sigma \in G} \mathrm{Ker}(\mu_\sigma).$$

This is precisely the subgroup of $\mathcal{D}$ of divisors representing rational divisor classes. The image of $\mathcal{F}$ in $J(\mathbb{F}_{\mathfrak{p}})$ lands in fact inside $J(\mathbb{F}_p)$ and is isomorphic to C. The image of $\mathcal{E}^G$ inside $J(\mathbb{F}_{\mathfrak{p}})$ is contained in the image of $\mathcal{F}$ and is isomorphic to C'. For each N we made a suitable choice of p, $\mathfrak{p}$ and computed both these images and checked that they are equal. Thus $C = C'$. □

Having established the equality $C = C'$, we have another more convenient way of thinking of C. Let $\mathcal{P}_0, \ldots, \mathcal{P}_r$ be the cusp places on $X/\mathbb{Q}$, with $\mathcal{P}_0 = P_0$ as before a cusp place of degree 1. From the equality $C = C'$ we now know that

$$C = \sum_{i=1}^{r} \mathbb{Z}(\mathcal{P}_i - \deg(\mathcal{P}_i) \cdot \mathcal{P}_0).$$

Thus for any $p \nmid N$, to compute the image of C in $J(\mathbb{F}_p)$ we merely take the subgroup generated by the reductions of $\mathcal{P}_i - \deg(\mathcal{P}_i) \cdot \mathcal{P}_0$.

5.3. **The real torsion subgroup of $J_0(N)$.** Let N be a positive integer and let g be the genus of $X_0(N)$. The torsion subgroup of $J_0(N)(\mathbb{C})$ is isomorphic to $(\mathbb{Q}/\mathbb{Z})^{2g}$. So the group $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a product of $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{2g}\mathbb{Z}$ with $d_1 \mid d_2 \mid \cdots \mid d_{2g}$. However $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is contained in the torsion subgroup of $J_0(N)(\mathbb{R})$ and we can use this to deduce that $d_1, \ldots, d_g \in \{1, 2\}$, and often in fact to cut down the number of possibilities for $d_1, \ldots, d_g$ as we shall see below.

We shall need the following theorem of Snowden [37], which tells us the number of connected components of $X_0(N)(\mathbb{R})$.

Theorem 5.2 (Snowden)**.** *Let N be a positive integer. If N is a power of 2, then $X_0(N)$ has one real component. Otherwise let n be the number of odd prime divisors of N. Let $\epsilon = 1$ if $8 \mid N$ and $\epsilon = 0$ otherwise. Then $X_0(N)$ has $2^{n+\epsilon-1}$ real components.*

We shall also need the following well-known theorem, which perhaps first appeared in a paper of Gross and Harris [14].

Theorem 5.3. *Let $X/\mathbb{R}$ be a smooth curve with $X(\mathbb{R}) \neq \emptyset$. Let g be the genus of X, m the number of its real components, and J its Jacobian. Then*

$$J(\mathbb{R}) \cong (\mathbb{R}/\mathbb{Z})^g \times (\mathbb{Z}/2\mathbb{Z})^{m-1}.$$

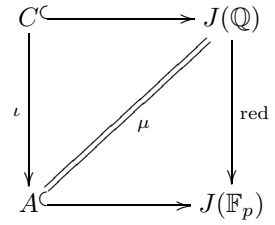
Thus

$$J(\mathbb{R})_{\mathrm{tors}} \cong (\mathbb{Q}/\mathbb{Z})^g \times (\mathbb{Z}/2\mathbb{Z})^{m-1}.$$

Proof. By [14, Proposition 3.2], the number of connected components of $J(\mathbb{R})$ is 2^{m-1}. The theorem follows from [14, Section 1]. □

5.4. **Computing the possibilities for $J_0(N)(\mathbb{Q})$.** We return to N being one of the values in Lemma 1.1, and we continue writing $X = X_0(N)$, $J = J_0(N)$, and $C = C_0(N)(\mathbb{Q})$. Recall that $J(\mathbb{Q})$ is finite for all values of N we are considering. Thus $C \subseteq J(\mathbb{Q})_{\mathrm{tors}} = J(\mathbb{Q})$. In particular, the reduction modulo p map $J(\mathbb{Q}) \to J(\mathbb{F}_p)$ is injective for $p \nmid 2N$. Let $\mathcal{A}'_p$ be a set of homomorphisms $\iota : C \to A$, where A is a subgroup of $J(\mathbb{F}_p)$ containing the image of C under the reduction mod p map, and ι is the restriction of the mod p map to C. Thus we know that for *some* $\iota \in \mathcal{A}'_p$, we have a commutative diagram

(5.1)

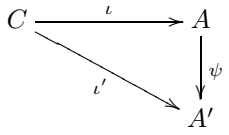


where μ is an isomorphism. Let g be the genus of X, and let m be the number of real components of J which may be computed from Theorem 5.2. By Theorem 5.3, we know that

$$J(\mathbb{Q}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}, \qquad d_1 \mid d_2 \mid \cdots \mid d_k,$$

where $k \le g$ or $g+1 \le k \le g+m-1$ and $d_1, \ldots, d_{k-g} \in \{1, 2\}$. Thus we eliminate from $\mathcal{A}'_p$ all $\iota : C \to A$, where the isomorphism class of A is incompatible with this information, to obtain a subset $\mathcal{A}_p$.

Let $p_1, \ldots, p_s$ be distinct primes $\nmid 2pN$. We let $\mathcal{A}_{p;\,p_1,\ldots,p_s}$ be the set of $\iota : C \to A$ in $\mathcal{A}_p$ such that the following holds: for each $p' \in \{p_1, \ldots, p_s\}$ there is some $\iota' : C \to A'$ in $\mathcal{A}_{p'}$ and an isomorphism $\psi : A \to A'$ making the diagram



commute. The existence of the isomorphism can be efficiently decided using the method explained in Section 4. It is clear that there must be some $\iota : C \to A$ in $\mathcal{A}_{p;p_1\ldots,p_s}$ and an isomorphism $\mu : A \to J(\mathbb{Q})$ such that the diagram (5.1) commutes. Observe that $\mathcal{A}_{p;p_1,\ldots,p_s}$ must contain some $\iota_0 : C \to A_0$, where A_0 is the image of C under the reduction mod p map.

Our hope is to find suitable p, $p_1, \ldots, p_s$ such that $\mathcal{A}_{p;p_1,\ldots,p_s}$ contains precisely one element, in which case this is necessarily ι_0, and we can then deduce that $J(\mathbb{Q}) = C$. In any case we know that $J(\mathbb{Q})/C$ is isomorphic to the cokernel of some ι in $\mathcal{A}_{p;p_1,\ldots,p_s}$ which allows us to deduce a positive integer I such that $I \cdot J(\mathbb{Q}) \subseteq C$.

Lemma 5.4. *Let N be one of the values given in Lemma* 1.1. *Then C and $J(\mathbb{Q})/C$ are as given in the tables of Section* 8.

Proof of Lemma 5.4 *and Theorem* 1.2. We wrote a `Magma` script which for each value of N computed $\mathcal{A}_{p;p_1,\ldots,p_s}$, where p is the smallest rational prime not dividing $2N$, and $p_1, \ldots, p_s$ are the primes ≤ 17 not dividing $2pN$. This allowed us to deduce the information in the tables except for two cases, where $N = 45, 64$. For those two cases we were able to improve on the information given by this method and deduce that $J(\mathbb{Q}) = C$. We explain this below in Sections 5.5 and 5.6. □

5.5. **The Mordell–Weil group for $J_0(45)$.** Let $N = 45$. The procedure explained above tells us that $C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, and

$$\begin{aligned} J(\mathbb{Q}) \cong\ & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \\ \text{or}\quad & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \\ \text{or}\quad & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}. \end{aligned}$$

We would like to show that $J(\mathbb{Q}) = C$, and for this it is enough to show that $J(\mathbb{Q})[2] = C[2] = (\mathbb{Z}/2\mathbb{Z})^3$. However for all primes $p \nmid N$ we tried $J(\mathbb{F}_p)[2] = (\mathbb{Z}/2\mathbb{Z})^6$ or $(\mathbb{Z}/2\mathbb{Z})^4$, and so it does not seem to be possible to prove the desired conclusion using reduction modulo primes. Instead we will compute the entire mod 2 representation of J,

$$\overline{\rho}_{J,2} \ :\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Sp}_6(\mathbb{F}_2),$$

and use this to deduce that $J(\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^3$.

The curve $X = X_0(45)$ is a smooth plane quartic. Our model for it is

$$X \ :\ x^3z - x^2y^2 + xyz^2 - y^3z - 5z^4 = 0$$

in $\mathbb{P}^2$. A procedure for computing the mod 2 representation of Jacobians of smooth plane quartics is explained by Bruin, Poonen, and Stoll [6, Section 12] and we apply that method to our situation. We wrote down the equations for the 28 bitangents to X. We found that the field of definition of these bitangents is $K = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ and so $\mathbb{Q}(J[2]) = K$. In particular $\overline{\rho}_{J,2}$ factors through $\mathrm{Gal}(K/\mathbb{Q})$, and we continue to denote the corresponding representation $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Sp}_6(\mathbb{F}_2)$ by $\overline{\rho}_{J,2}$. Each bitangent L meets X in a divisor $(L.X)$ which has the form $2D_L$, where D_L is an effective degree 2 divisor. We wrote down the set Σ of all quadruples $\{L_1, \ldots, L_4\}$ such that $D_{L_1} + \cdots + D_{L_4} \sim 2\omega_X$, where ω_X is the canonical divisor on X. As predicted by [6] this set Σ has cardinality 315. Next we construct the graph $\mathcal{G}$ whose vertices are the quadruples $Q \in \Sigma$, and where $Q \neq Q'$ are connected by an edge if and only if $Q \cap Q' \neq \emptyset$. We computed the automorphism group $\mathrm{Aut}(\mathcal{G})$ using `Magma` (this routine is an implementation of the algorithm described in [24]), and found it to be isomorphic to $\mathrm{Sp}_6(\mathbb{F}_2)$ as predicted by [6]. Now the action of $\mathrm{Gal}(K/\mathbb{Q})$ on the lines naturally gives a representation $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(\mathcal{G}) \cong \mathrm{Sp}_6(\mathbb{F}_2)$, and this is precisely $\overline{\rho} = \overline{\rho}_{J,2} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Sp}_6(\mathbb{F}_2)$ (up to conjugation inside $\mathrm{Sp}_6(\mathbb{F}_2)$). Let τ_1, τ_2, τ_3 be the elements of $\mathrm{Gal}(K/\mathbb{Q})$ satisfying

$$\begin{cases} \tau_1(\sqrt{-3}) = \sqrt{-3}, \\ \tau_1(\sqrt{5}) = -\sqrt{5}, \end{cases} \qquad \begin{cases} \tau_2(\sqrt{-3}) = -\sqrt{-3}, \\ \tau_2(\sqrt{5}) = \sqrt{5}, \end{cases} \qquad \tau_3 = \tau_1\tau_2.$$

Write $M_i = \overline{\rho}(\tau_i)$. We found that

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Write $V_i = \mathrm{Ker}(M_i - I)$, where $I \in \mathrm{Sp}_6(\mathbb{F}_2)$ is the identity matrix. Thus V_i is isomorphic to the subspace of $J[2]$ fixed by τ_i. We found that V_1, V_2, V_3 are 4-dimensional, but $V_1 \cap V_2 \cap V_3$ is 3-dimensional. This proves that $J(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^3$, and completes the proof that $J(\mathbb{Q}) = C$.

It is worth observing that if p is any prime of good reduction, then the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ must either be the identity or one of the τ_i; in the former case $J(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^6$ and in the latter case $J(\mathbb{F}_p)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$. This explains why we have been unable to use the reduction mod p maps to precisely pin down $J(\mathbb{Q})[2]$.

5.6. **The Mordell–Weil group for $J_0(64)$.** Let $N = 64$. The procedure explained above gives us

$$C \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2$$

and

$$J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2 \qquad \text{or} \qquad (\mathbb{Z}/4\mathbb{Z})^3.$$

We want to show that $J(\mathbb{Q}) = C$. For this it is enough to show that $J(\mathbb{Q})[4] = C$. The cusps of $X_0(64)$ are defined over $K = \mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. Let $L = \mathbb{Q}(\sqrt{2})$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and $H = \mathrm{Gal}(K/L) \subset G$. The method explained in Subsection 5.2 computes $C_0(64)(K)$ (the full cuspidal group) and then $C = C_0(64)(\mathbb{Q})$ is obtained by taking G-invariants. Instead we take H-invariants to obtain $C_0(64)(L)$ and find $C_0(64)(L) \cong (\mathbb{Z}/4\mathbb{Z})^3$. Note that this is contained in $J(L)[4]$. However, from Theorems 5.2 and 5.3 we know that $J(\mathbb{R})[4] \cong (\mathbb{Z}/4\mathbb{Z})^3$. As $L \subset \mathbb{R}$ we deduce $J(L)[4] = C_0(64)(L) \cong (\mathbb{Z}/4\mathbb{Z})^4$. Hence $J(\mathbb{Q})[4] \subseteq C_0(64)(K)$. Now taking G-invariants we have $J(\mathbb{Q})[4] \subseteq C_0(64)(K)^G = C$. This proves that $J(\mathbb{Q}) = C$.

6. The Mordell–Weil sieve

Let $X/\mathbb{Q}$ be a curve of genus ≥ 3 with Jacobian J, and suppose X is not hyperelliptic. In this section we explain a version of the Mordell–Weil sieve for quadratic points on X, under the assumption that $J(\mathbb{Q})$ has rank 0, but without assuming full knowledge of $J(\mathbb{Q})$. Let $P_0 \in X(\mathbb{Q})$. We use this to fix a map $X^{(2)} \to J$ given by $D \mapsto [D - 2P_0]$.

Let $\mathcal{K}$ be a (known) set of rational effective divisors of degree 2. Let G be a subgroup of $J(\mathbb{Q})$ and I a positive integer such that $I \cdot J(\mathbb{Q}) \subseteq G$; again we assume that G and I are known, but that $J(\mathbb{Q})$ is perhaps unknown. We will use our partial knowledge of the Mordell–Weil group to sieve for unknown rational effective degree 2 divisors. Let $p \geq 3$ be a prime of good reduction for X. Let

$$\mathcal{V}_p = \{\tilde{D} \in X^{(2)}(\mathbb{F}_p) \ : \ D \in \mathcal{K}\}, \qquad \mathcal{U}_p = X^{(2)}(\mathbb{F}_p) \setminus \mathcal{V}_p.$$

Lemma 6.1. *Let $D' \in X^{(2)}(\mathbb{Q})$ and suppose $\tilde{D}' \in \mathcal{V}_p$. Then $D' \in \mathcal{K}$.*

Proof. By definition of $\mathcal{V}_p$ we have $\tilde{D}' = \tilde{D}$ for some $D \in \mathcal{K}$. Thus the divisor class $[D' - D]$ is in the kernel of the reduction map $J(\mathbb{Q}) \to J(\mathbb{F}_p)$. However, $J(\mathbb{Q})$ is torsion. By the injectivity of torsion [20, appendix] under mod p reduction we conclude that $D \sim D'$. It will be enough to show that $D = D'$. Suppose otherwise; then the Riemann–Roch space $\mathcal{L}(D)$ has dimension at least 2. Let $f \in \mathcal{L}(D)$ be a non-constant function. Then $f : X \to \mathbb{P}^1$ has degree 2, contradicting the assumption that X is non-hyperelliptic. □

Lemma 6.2. *Let $p_1, \ldots, p_r$ be primes ≥ 3 of good reduction for X. Let $\phi_i : G \to J(\mathbb{F}_{p_i})$ be the composition for the inclusion $G \hookrightarrow J(\mathbb{Q})$ with the reduction modulo p_i map $J(\mathbb{Q}) \to J(\mathbb{F}_{p_i})$. If $D \in X^{(2)}(\mathbb{Q}) \setminus \mathcal{K}$, then*

$$I \cdot [D - 2P_0] \in \bigcap_{i=1}^{r} \phi_i^{-1} \left(\left\{ I \cdot [\tilde{D} - 2\tilde{P}_0] \ : \ \tilde{D} \in \mathcal{U}_{p_i} \right\} \right). \tag{6.1}$$

Proof. Since $I \cdot J(\mathbb{Q}) \subseteq G$, we know that $I \cdot [D - 2P_0] \in G$. By Lemma 6.1, we know that the reduction $\tilde{D}$ of D modulo p_i belongs to $\mathcal{U}_{p_i}$. The proof follows easily. □

7. Proof of Main Theorem

Let N be one of the values in Lemma 1.1. Thanks to Lemma 5.4, we know a set that contains all the possibilities for $J(\mathbb{Q})/C$. We take I to be the least common multiple of the exponents of these groups. Thus $I \cdot J(\mathbb{Q}) \subseteq C$. In each case we know the rational points on X and thus we have some collection $\mathcal{K}_0$ of effective degree 2 divisors of the form $P + Q$, where P, Q are rational points on X. We searched for quadratic points on P on X and took $\mathcal{K}$ to be the union of $\mathcal{K}_0$ together with $P + P^\sigma$, where P runs through the quadratic points we have found, and P^σ is a Galois conjugate of P. We took $\mathcal{K}$ as our known set of degree 2 divisors on X. We then applied Lemma 6.2 for a suitable choice of primes $p_1, \ldots, p_r \geq 3$ of good reduction, and with $G = C$, to deduce a subset of $\mathcal{S} \subseteq J(\mathbb{Q})$ given by (6.1) that contains the possibilities for $I \cdot [D - 2P_0]$ for $D \in X^{(2)}(\mathbb{Q}) \setminus \mathcal{K}$. We found, for $N \neq 42, 72$, that $\mathcal{S} = \emptyset$, and thus $X^{(2)}(\mathbb{Q}) = \mathcal{K}$. The two values $N = 42, 72$ needed virtually identical arguments to complete the proof that $X^{(2)}(\mathbb{Q}) = \mathcal{K}$. We illustrate this now by giving a detailed account of the computation for $X_0(72)$.

The curve $X_0(72)$ has eight cusps of degree 1 and four cusp pairs defined over quadratic fields. Let these be $P_0, \dots, P_7$ and Q_i, Q_i', where $i = 1, 2, 3, 4$ and Q_i, Q_i' are Galois conjugates. The modular symbols algorithm shows that $J_0(72)$ is isogenous to a product $E_1^2 \times E_2^2 \times E_3$, where E_1, E_2, E_3 are respectively the elliptic curves with Cremona labels `24A1`, `36A1`, `72A1`. As these three elliptic curves have rank 0 so does $J_0(72)$. We write $X = X_0(72)$ and $J = J_0(72)$. Let $\mathcal{K}$ consist of the known degree 2 effective rational divisors: $Q_i + Q_i'$ for $i = 1, \dots, 4$ and $P_i + P_j$, where $0 \le i, j \le 7$. Thus $\mathcal{K}$ has 40 elements. From our tables in Section 8 we have

$$C = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \qquad J(\mathbb{Q})/C = 0 \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z}.$$

We take $G = C$ and $I = 2$. We applied Lemma 6.2 with just one prime $p = 5$. We found that $\#X^{(2)}(\mathbb{F}_5) = 64$. Of these 64 divisors, 40 are reductions of elements in $\mathcal{K}$ and the 2×5 matrix $A(\tilde{D})$ has rank 2 for all 40. Thus $\#\mathcal{U}_5$ has 24 elements. However, only two elements of the set $\{2[\tilde{D} - 2\tilde{P}_0] \ : \ \tilde{D} \in \mathcal{U}_5\}$ are in the image of $\phi_5 \ : \ G \hookrightarrow J(\mathbb{F}_5)$. We let A_1, A_2 be their preimages in G (which we represent as divisors of degree 0 on X). Thus if $D \in X^{(2)}(\mathbb{Q}) \setminus \mathcal{K}$, then $2D \sim A_i + 4P_0$. We found that the Riemann–Roch spaces $L(A_i + 4P_0)$ are both 2-dimensional. Suppose $i = 1$ and let f, g be a $\mathbb{Q}$-basis for $L(A_1 + 4P_0)$. Thus $2D = A_1 + \operatorname{div}(\alpha f + \beta g)$ for some $(\alpha, \beta) \in \mathbb{P}^1(\mathbb{Q})$. We consider the 1-dimensional family of 0-dimensional subschemes $A_1 + \operatorname{div}(\alpha f + \beta g)$ of $X^{(2)}$ parametrized by $(\alpha, \beta) \in \mathbb{P}^1$. Computing and factoring the discriminant of this subscheme (as a homogeneous expression in α, β) shows that none of the elements of this 1-dimensional family has the form $2D$ with $D \in X^{(2)}(\mathbb{Q})$. This shows that no element $D \in X^{(2)}(\mathbb{Q})$ satisfies $2D \sim A_1 + 4P_0$. An identical argument also allows us to deduce a contradiction for $i = 2$. This shows that $X^{(2)}(\mathbb{Q}) = \mathcal{K}$. Therefore there are no non-cuspidal quadratic points on $X_0(72)$.

Remark. In the above computation for $X_0(72)$ we have applied the Mordell–Weil sieve with just one prime $p = 5$. In fact we have found in this case that using additional primes does not allow us to eliminate A_1, A_2 using just the Mordell–Weil sieve and it is instructive to ponder the reason for this. In both cases $i = 1$, 2, the discriminant mentioned above has three quadratic factors which give divisors D belonging to $X^{(2)}(\mathbb{Q}(\sqrt{-1}))$, $X^{(2)}(\mathbb{Q}(\sqrt{3}))$, and $X^{(2)}(\mathbb{Q}(\sqrt{-3}))$ such that $2D \sim A_i + 4P_0$. Since any prime $p \ge 5$ must split in at least one of the fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{-3})$ it follows that for any such p (and for $i = 1$, 2) there is some $\tilde{D} \in X^{(2)}(\mathbb{F}_p)$ such that $2\tilde{D} \sim \tilde{A}_i + 4\tilde{P}_0$. This fact can be easily used to show that A_1, A_2 belong to the intersection in (6.1) regardless of which primes $p_1, \dots, p_r \ge 5$ are chosen.

8. Tables

Table 8.1. $X_0(34)$

Genus: 3

Model: $x^3z - x^2y^2 - 3x^2z^2 + 2xz^3 + 3xy^2z - 3xyz^2 + 4xz^3 - y^4 + 4y^3z - 6x^2z^2 + 4yz^3 - 2z^4$

$J_0(34)(\mathbb{Q}) = C \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-1	$(\theta+1, 0, 1)$	287496	-16	YES
P_2	-1	$(\frac{\theta+1}{2}, \frac{\theta+1}{2}, 1)$	1728	-4	YES
P_3	-1	$(\theta, -\theta, 1)$	1728	-4	YES
P_4	-2	$(\frac{\theta}{2}, -\frac{\theta}{2}, 1)$	8000	-8	YES
P_5	-15	$(\frac{\theta+11}{8}, \frac{1}{2}, 1)$	$\frac{2041\theta+11779}{8}$	NO	YES
P_6	-15	$(\frac{\theta+23}{16}, \frac{\theta+7}{16}, 1)$	$\frac{-531847853404479\theta-7319387769191}{34359738368}$	NO	YES

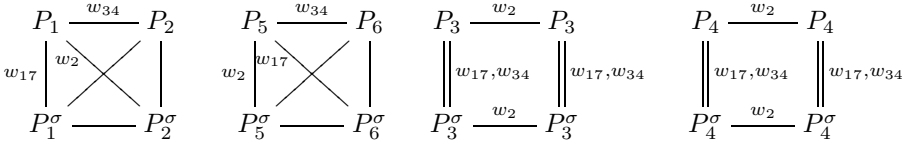


Table 8.2. $X_0(38)$

Genus: 4

Model: $x_1x_3 - x_2^2 - x_2x_4 - x_3^2 - x_3x_4 - x_4^2$,
$x_1^2x_4 + x_1x_4^2 - x_2^3 + 3x_2^2x_3 + 2x_2^2x_4 - 3x_2x_3^2 - 4x_2x_3x_4 - 2x_2x_4^2 + x_3^3 + 2x_3^2x_4 + 2x_3x_4^2 + x_4^3$

$J_0(38)(\mathbb{Q}) = C \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-3	$(\frac{\theta+1}{2}, 0, \frac{\theta-1}{2}, 1)$	0	-3	YES
P_2	-3	$(0, \frac{-\theta+1}{2}, 0, 1)$	54000	-12	YES
P_3	-2	$(\frac{\theta+1}{3}, \frac{-\theta+1}{3}, \frac{\theta-1}{3}, 1)$	8000	-8	YES

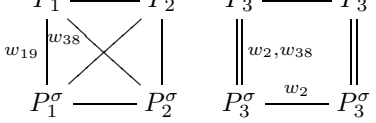


TABLE 8.3. $\boldsymbol{X_0(42)}$

Genus: 5

Model: $x_1x_3 - x_2^2 + x_3x_4$,

$x_1x_5 - x_2x_5 - x_3^2 + x_4x_5 - x_5^2$,

$x_1x_4 - x_2x_3 + x_2x_4 - x_3^2 + x_3x_4 + x_3x_5 - x_4^2 - 2x_4x_5$

$C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ and $J_0(42)(\mathbb{Q})/C \cong 0$ or $\mathbb{Z}/2\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-3	$(\frac{-\theta+1}{2}, \frac{\theta+1}{2}, \frac{\theta-1}{2}, \frac{\theta+1}{2}, 1)$	54000	-12	YES
P_2	-3	$(2, \frac{\theta+1}{2}, \frac{\theta-1}{2}, -1, 1)$	0	-3	YES

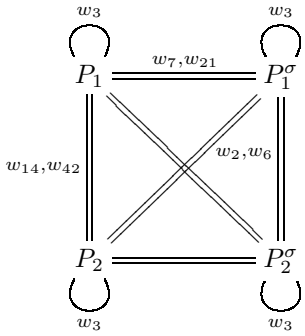


TABLE 8.4. $\boldsymbol{X_0(44)}$

Genus: 4

Model: $x_1^2x_4 - x_2^3 + x_3^2x_4 - 2x_4^3$, $x_1x_3 - x_2^2 + 2x_2x_4 - 3x_4^2$

$J_0(44)(\mathbb{Q}) = C \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-7	$(\frac{-\theta+1}{2}, \frac{\theta+1}{2}, 1, 1)$	-3375	-7	YES
P_2	-7	$(\frac{\theta-1}{2}, \frac{\theta+1}{2}, -1, 1)$	16581375	-28	NO
P_3	-7	$(1, \frac{-\theta+1}{2}, \frac{\theta+1}{2}, 1)$	16581375	-28	NO
P_4	-7	$(-1, \frac{\theta+1}{2}, \frac{\theta-1}{2}, 1)$	-3375	-7	YES
P_5	-7	$(\theta-2, -2, -\theta-2, 1)$	-3375	-7	NO
P_6	-7	$(-\theta+2, -2, \theta+2, 1)$	-3375	-7	NO

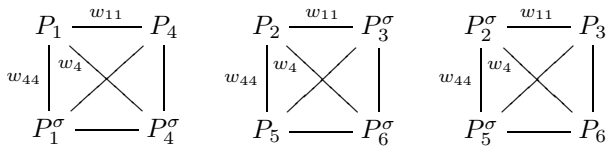


TABLE 8.5. $\boldsymbol{X_0(45)}$

Genus: 3

Model: $x^3z - x^2y^2 + xyz^2 - y^3z - 5z^4$

$J_0(45)(\mathbb{Q}) = C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-11	$(\frac{\theta-1}{2}, 1, 1)$	-32768	-11	YES
P_2	-11	$(-1, \frac{-\theta+1}{2}, 1)$	-32768	-11	YES
P_3	13	$(2, \frac{-\theta-5}{2}, 1)$	$\frac{12506376645279330\theta - 4509238226399579}{64}$	NO	YES
P_4	13	$(\frac{-\theta+5}{2}, -2, 1)$	$\frac{461373\theta - 1664219}{4}$	NO	YES
P_5	-39	$(\frac{\theta+13}{8}, \frac{-\theta-5}{4}, 1)$	$\frac{27341062250\theta + 43419758443}{1024}$	NO	YES
P_6	-39	$(\frac{\theta+5}{4}, \frac{-\theta-13}{8}, 1)$	$\frac{-6035506678349769 5\theta - 1556546639145161477}{70368744177664}$	NO	YES

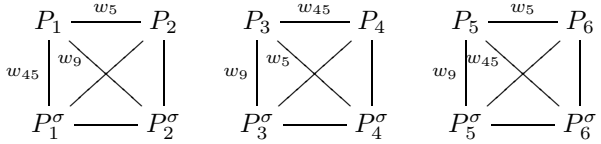


TABLE 8.6. $\boldsymbol{X_0(51)}$

Genus: 5

Model: $x_1x_3 - x_2^2 + x_2x_4 - x_3^2 - x_3x_5 - x_4^2$,

$x_1x_4 - x_2x_3 - x_3^2 - x_4x_5$,

$x_1x_5 - x_2x_4 - 2x_3^2 + x_3x_5 + x_4^2 - 2x_4x_5$

$J_0(51)(\mathbb{Q}) = C \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-2	$(0, \theta/2, \theta/2, 1, 1)$	8000	-8	YES
P_2	-2	$(\frac{-\theta+1}{9}, \frac{2\theta-1}{9}, \frac{2\theta-1}{9}, \frac{\theta+4}{9}, 1)$	8000	-8	NO
P_3	17	$(\frac{\theta+5}{2}, \frac{-\theta-3}{4}, \frac{\theta+3}{4}, 0, 1)$	$-6719569920\theta - 2770550784$	-51	NO

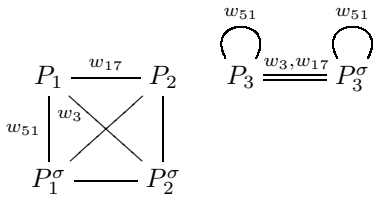


TABLE 8.7. $\boldsymbol{X_0(52)}$

Genus: 5

Model: $x_1x_3 - x_2^2 - x_3^2 - x_4^2$,
$x_1x_4 - x_2x_3 + x_2x_5 - x_4x_5$,
$x_1x_5 - x_2x_4 - 2x_3^2 + x_3x_5 - x_5^2$

$J_0(52)(\mathbb{Q}) = C \cong \mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-1	$(\theta+1, 1, 0, \theta, 1)$	287496	-16	YES
P_2	-1	$(\frac{-\theta+1}{2}, 0, \frac{-\theta+1}{2}, 0, 1)$	287496	-16	YES
P_3	-1	$(\theta+1, -1, 0, -\theta, 1)$	1728	-4	YES
P_4	-3	$(0, -1, \frac{\theta+1}{2}, \frac{\theta-1}{2}, 1)$	54000	-12	YES
P_5	-3	$(0, 1, \frac{\theta+1}{2}, \frac{-\theta+1}{2}, 1)$	54000	-12	YES

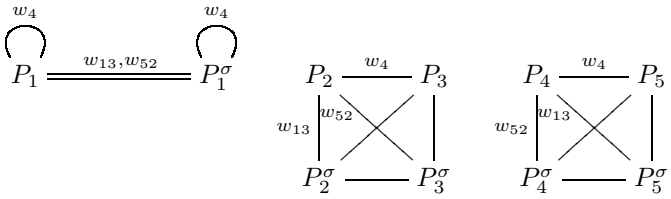


TABLE 8.8. $\boldsymbol{X_0(54)}$

Genus: 4

Model: $x_1^2x_3 - x_1x_3^2 - x_2^3 + x_2^2x_4 - 3x_2x_4^2 + x_3^3 + 3x_4^3$,
$x_1x_4 - x_2x_3 + x_3x_4$

$J_0(54)(\mathbb{Q}) = C \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-2	$(-2, \theta+1, \theta, 1)$	8000	-8	YES

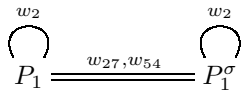


TABLE 8.9. $\boldsymbol{X_0(55)}$

Genus: 5

Model: $x_1x_3 - x_2^2 + x_2x_4 - x_2x_5 - x_3^2 + 3x_3x_4 + x_3x_5 - 2x_4^2 - 4x_5^2$,
$x_1x_4 - x_2x_3 + 2x_2x_4 - 2x_2x_5 - 2x_3^2 + 4x_3x_4 + 5x_3x_5 - 2x_4^2 - 4x_4x_5 - 3x_5^2$,
$x_1x_5 - 2x_2x_5 - x_3^2 + 2x_3x_4 + x_3x_5 - x_4^2$

$C \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ and $J_0(55)(\mathbb{Q})/C \cong 0, \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-11	$(\frac{-\theta-1}{2}, 2, 2, \frac{-\theta+5}{2}, 1)$	-32768	-11	YES
P_2	-19	$(\frac{\theta-3}{2}, \frac{-\theta+3}{2}, 2, \frac{-T+1}{2}, 1)$	-884736	-19	YES
P_3	-19	$(-2, \frac{\theta+3}{2}, \frac{-\theta+5}{2}, 1, 1)$	-884736	-19	YES
P_4	-159	$(\frac{5\theta-9}{32}, 1/8, \frac{-5\theta+19}{32}, \frac{-5\theta+27}{32}, 1)$	$\frac{-3069246457756\theta-1607809480031}{4096}$	NO	YES
P_5	-159	$(\frac{\theta+7}{2}, -4, \frac{-\theta-5}{2}, \frac{-\theta+1}{2}, 1)$	$\frac{25951242954109990556\theta-21462567617768426467 1}{72057594037927936}$	NO	YES

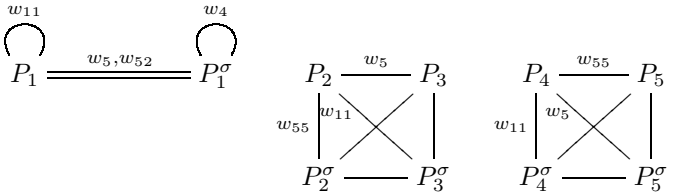


TABLE 8.10. $\boldsymbol{X_0(56)}$

Genus: 5

Model: $x_1x_3 - x_2^2 - x_3^2 + x_3x_5 - 3x_4^2$,
$x_1x_4 - x_2x_3 + x_2x_5 - x_3x_4$,
$x_1x_5 - x_2x_4 - x_3^2 + 2x_3x_5 - x_4^2 - x_5^2$

$J_0(56)(\mathbb{Q}) = C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-7	$(-1, \frac{3\theta+7}{8}, \frac{-\theta+3}{4}, \frac{\theta-3}{8}, 1)$	-3375	-7	NO
P_2	-7	$(-1, \frac{-\theta+1}{2}, \frac{\theta+1}{2}, -1, 1)$	16581375	-28	NO
P_3	-7	$(-1, \frac{-3\theta-7}{8}, \frac{-\theta+3}{4}, \frac{-\theta+3}{8}, 1)$	16581375	-28	YES
P_4	-7	$(-1, \frac{\theta-1}{2}, \frac{\theta+1}{2}, 1, 1)$	-3375	-7	YES

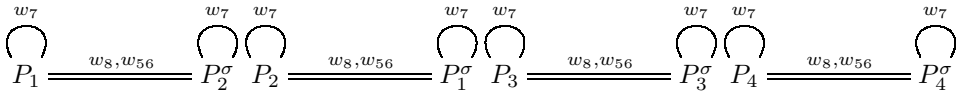


TABLE 8.11. $\boldsymbol{X_0(63)}$

Genus: 5

Model: $x_1x_3 - x_2^2 + x_2x_5 - x_3x_4 - x_5^2$,
$x_1x_4 - x_2x_3 - x_3x_5$,
$x_1x_5 - x_2x_4 - x_3^2$

$C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ and $J_0(63)(\mathbb{Q})/C \cong 0$ or $\mathbb{Z}/2\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-3	$\left(\frac{-\theta+1}{2}, \frac{-\theta-1}{2}, \frac{\theta-1}{2}, \frac{\theta-1}{2}, 1\right)$	0	-3	YES
P_2	-3	$\left(\frac{\theta+1}{2}, \frac{-\theta-1}{2}, 1, \frac{-\theta-1}{2}, 1\right)$	-12288000	-27	YES
P_3	-3	$\left(-1, \frac{\theta-1}{2}, \frac{\theta-1}{2}, 1, 1\right)$	-12288000	-27	YES
P_4	-3	$(0, \frac{-\theta+1}{2}, 0, 0, 1)$	-12288000	-27	YES

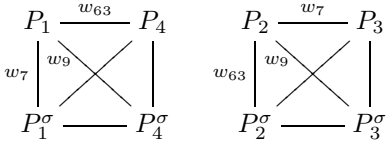


TABLE 8.12. $\boldsymbol{X_0(64)}$

Genus: 3

Model: $x^3z + 4xz^3 - y^4$

$J_0(64)(\mathbb{Q}) = C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-7	$(-\theta-1, -2, 1)$	-3375	-7	NO
P_2	-7	$(-\theta-1, 2, 1)$	16581375	-28	YES
P_3	-7	$(\frac{-\theta-1}{2}, \frac{\theta+1}{2}, 1)$	-3375	-7	YES
P_4	-7	$(\frac{\theta-1}{2}, \frac{\theta-1}{2}, 1)$	16581375	-28	NO

$P_1 \overset{w_{64}}{\text{———}} P_4^\sigma \qquad P_2 \overset{w_{64}}{\text{———}} P_2^\sigma \qquad P_3 \overset{w_{64}}{\text{———}} P_3^\sigma$

TABLE 8.13. $\boldsymbol{X_0(72)}$

Genus: 5

Model: $x_1x_3 - x_2^2 - x_4^2 - 4x_5^2$,
$x_1x_4 - x_2x_3 + x_2x_5 + x_4x_5 - 3x_5^2$,
$x_1x_5 - x_2x_4 - x_3x_5$

$C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and $J_0(72)(\mathbb{Q})/C \cong 0$ or $\mathbb{Z}/2\mathbb{Z}$

There are no non-cuspidal quadratic points on $X_0(72)$.

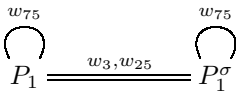
TABLE 8.14. $\boldsymbol{X_0(75)}$

Genus: 5

Model: $x_1x_3 - x_2^2 + x_2x_5 - x_3x_4 - x_5^2$,
$x_1x_4 - x_2x_3 - x_3x_5$,
$x_1x_5 - x_2x_4 - x_3^2$

$C \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}$ and $J_0(75)(\mathbb{Q})/C \cong 0$ or $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	5	$\left(\frac{-3\theta+1}{2}, \frac{\theta-3}{2}, \frac{-3\theta-1}{2}, \frac{\theta-3}{2}, 1\right)$	$1463291412480\theta - 327201914880$	-75	YES
P_2	-11	$\left(-2, \frac{t-1}{2}, \frac{t+1}{2}, \frac{t-1}{2}, 1\right)$	-12288000	-11	YES
P_3	-11	$\left(\frac{-\theta-1}{2}, \frac{\theta-1}{2}, 2, \frac{\theta-1}{2}, 1\right)$	-12288000	-11	YES



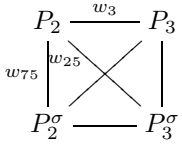


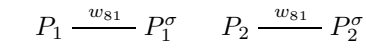
TABLE 8.15. $\boldsymbol{X_0(81)}$

Genus: 4

Model: $x_1^2x_4 - x_1x_4^2 - x_2^3 - 3x_3^3 + x_4^3$,
$x_1x_3 - x_2^2 - 2x_3x_4$

$J_0(81)(\mathbb{Q}) = C \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-2	$(\frac{-\theta}{2}, \frac{\theta-1}{2}, \frac{\theta}{2}, , 1)$	8000	-8	YES
P_2	-11	$(\frac{-\theta-1}{2}, \frac{-\theta+1}{2}, 1, 1)$	-32768	-11	YES



Acknowledgments

The second-named author would like to thank Martin Derickx, Steve Donnelly, Derek Holt, and David Zureick-Brown for useful conversations. The authors would like to thank Ozlem Ejder and Jeremy Rouse for pointing out that $X_0(64)$ is isomorphic to the Fermat quartic and pointing us in the direction of Aigner's paper [1]. The authors are grateful to the referee for suggesting several significant improvements and simplifications. The authors would also like to thank the Istanbul Center for Mathematical Sciences (IMBM) for hosting their collaboration during April 2018.

References

[1] A. Aigner, *Uber die Möglichkeit von $x^4 + y^4 = z^4$ in quadratischen Körpern*, Jber. Deutsch. Math.-Verein. **43** (1934), 226–229. 1, 23

[2] B. S. Banwait and J. E. Cremona, *Tetrahedral elliptic curves and the local-global principle for isogenies*, Algebra Number Theory **8** (2014), no. 5, 1201–1229, DOI 10.2140/ant.2014.8.1201. MR3263141 ↑5

[3] F. Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), no. 1, 154–165, DOI 10.1006/jnth.1998.2343. MR1688168 ↑1

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478 ↑3

[5] P. Bruin and F. Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), no. 1, 578–602, DOI 10.1112/S1461157015000157. MR3389884 ↑1

[6] N. Bruin, B. Poonen, and M. Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80, DOI 10.1017/fms.2016.1. MR3482281 ↑12

[7] J. J. Cannon and D. F. Holt, *Automorphism group computation and isomorphism testing in finite groups*, J. Symbolic Comput. **35** (2003), no. 3, 241–267, DOI 10.1016/S0747-7171(02)00133-5. MR1962794 ↑7

[8] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1992. MR1201151 ↑4

[9] M. Derickx, *Torsion points on elliptic curves over number fields of small degree*, PhD thesis, Leiden University, 2016.

[10] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, *Torsion Points on Elliptic Curves over Number Fields of Small Degree*, `arXiv:1707.00364v1`. 1

[11] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196 ↑3, 6

[12] V. G. Drinfel′d, *Two theorems on modular curves* (Russian), Funkcional. Anal. i Priložen. **7** (1973), no. 2, 83–84. MR0318157 ↑3

[13] S. D. Galbraith, *Equations for modular curves*, DPhil thesis, University of Oxford, 1996. 4, 5

[14] B. H. Gross and J. Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 2, 157–182. MR631748 ↑10, 11

[15] N. Freitas, B. V. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206, DOI 10.1007/s00222-014-0550-z. MR3359051 ↑2, 5

[16] N. Freitas and S. Siksek, *Fermat's last theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895, DOI 10.2140/ant.2015.9.875. MR3352822 ↑2

[17] J. Harris and J. Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), no. 2, 347–356, DOI 10.2307/2048726. MR1055774 ↑1

[18] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445, DOI 10.1006/jsco.2001.0513. MR1890579 ↑9

[19] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689 ↑1

[20] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502, DOI 10.1007/BF01394256. MR604840 ↑9, 14

[21] V. A. Kolyvagin and D. Yu. Logachëv, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz **1** (1989), no. 5, 171–196; English transl., Leningrad Math. J. **1** (1990), no. 5, 1229–1253. MR1036843 ↑4

[22] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), no. 3, 415–427, DOI 10.1112/jlms/s2-23.3.415. MR616546 ↑1

[23] S. Ling, *On the $\mathbf{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$*, Israel J. Math. **99** (1997), 29–54, DOI 10.1007/BF02760675. MR1469086 ↑3

[24] B. D. McKay, *Practical graph isomorphism*, Proceedings of the Tenth Manitoba Conference on Numerical Mathematics and Computing, Vol. I (Winnipeg, Man., 1980), Congr. Numer. **30** (1981), 45–87. MR635936 ↑12

[25] Ju. I. Manin, *Parabolic points and zeta functions of modular curves* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. MR0314846 ↑3

[26] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287 ↑1, 3

[27] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230 ↑1

[28] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (French), Invent. Math. **124** (1996), no. 1-3, 437–449, DOI 10.1007/s002220050059. MR1369424 ↑1

[29] M. Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. **37** (2014), no. 2, 273–318, DOI 10.3836/tjm/1422452795. MR3304683 ↑3

[30] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR0364259 ↑3

[31] E. Ozman and S. Siksek, *Quadratic points on modular curves II*, in progress. 2

[32] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres* (French, with French summary), J. Reine Angew. Math. **506** (1999), 85–116, DOI 10.1515/crll.1999.009. MR1665681 ↑1

[33] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques* (French, with English and French summaries), Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749. MR1779891 ↑1

[34] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR1465369 ↑9

[35] Y. Ren, *Rational torsion subgroups of modular Jacobian varieties*, J. Number Theory **190** (2018), 169–186, DOI 10.1016/j.jnt.2018.02.009. MR3805452 ↑3

[36] S. Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236, DOI 10.2140/ant.2009.3.209. MR2491943 ↑2

[37] A. Snowden, *Real components of modular curves*, `arXiv:1108.3131`. 10

[38] W. A. Stein, *Explicit approaches to modular abelian varieties*, ProQuest LLC, Ann Arbor, MI, 2000. Thesis (Ph.D.)–University of California, Berkeley. MR2701042 ↑4

[39] W. Stein, *Modular forms, a Computational Approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells. MR2289048 ↑4, 5

[40] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 ↑4

[41] H. Yoo, *The index of an Eisenstein ideal and multiplicity one*, Math. Z. **282** (2016), no. 3-4, 1097–1116, DOI 10.1007/s00209-015-1579-4. MR3473658 ↑3

Department of Mathematics, Bogazici University, Bebek, Istanbul, 34342, Turkey
Email address: `ekin.ozman@boun.edu.tr`

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
Email address: `samir.siksek@gmail.com`