HYPERELLIPTIC MODULAR CURVES $X_0(n)$ AND ISOGENIES OF ELLIPTIC CURVES OVER QUADRATIC FIELDS

PETER BRUIN AND FILIP NAJMAN

ABSTRACT. We study elliptic curves over quadratic fields with isogenies of certain degrees. Let n be a positive integer such that the modular curve $X_0(n)$ is hyperelliptic of genus ≥ 2 and such that its Jacobian has rank 0 over $\mathbb{Q}$. We determine all points of $X_0(n)$ defined over quadratic fields, and we give a moduli interpretation of these points. We show that, with finitely many exceptions up to $\overline{\mathbb{Q}}$-isomorphism, every elliptic curve over a quadratic field K admitting an n-isogeny is d-isogenous, for some $d \mid n$, to the twist of its Galois conjugate by a quadratic extension L of K; we determine d and L explicitly, and we list all exceptions. As a consequence, again with finitely many exceptions up to $\overline{\mathbb{Q}}$-isomorphism, all elliptic curves with n-isogenies over quadratic fields are in fact $\mathbb{Q}$-curves.

1. Introduction

The study of possible torsion groups of elliptic curves over number fields has seen a lot of progress in the last few decades. See, just to mention some, [21] for results over $\mathbb{Q}$, [13, 20] for results over quadratic fields, [11, 24] for results over cubic fields, and [12] for results over quartic fields. We also mention the uniform boundness conjecture, proved by Merel [23], which states that the order of the torsion group is bounded from above by an integer depending only on the degree of the number field.

Unfortunately, much less is known about the possible degrees of isogenies of elliptic curves over number fields. A complete classification of possible isogeny degrees is only known over $\mathbb{Q}$. Mazur [22] found all the isogenies of prime degree and gave a list of isogeny degrees which he believed to be complete, after which Kenku proved in a series of papers [15, 16, 17, 18] that the list is indeed complete.

The goal of this paper is to classify elliptic curves over quadratic fields with isogenies of certain degrees n and to investigate their properties. We will try to obtain as much information as possible on these curves. In particular, for many values of n, we classify all such curves and explicitly describe the isogenies.

We say that an elliptic curve E over a field K has an *n-isogeny* if it has an isogeny with cyclic kernel of order n defined over K. As usual, the (compact) modular curve over $\mathbb{Q}$ classifying elliptic curves with an n-isogeny will be denoted by $X_0(n)$, and the Jacobian of $X_0(n)$ will be denoted by $J_0(n)$.

To classify elliptic curves over quadratic fields admitting an n-isogeny, we determine all quadratic points on the curves $X_0(n)$ for n such that $X_0(n)$ is hyperelliptic of genus at least 2 and such that the group of $\mathbb{Q}$-rational points of $J_0(n)$ is finite. These assumptions are satisfied if and only if

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

Throughout this paper, unless stated otherwise, n will denote an integer in the above set.

Remark 1. The curve $X_0(37)$ is also hyperelliptic, but $J_0(37)(\mathbb{Q})$ has positive rank.

After obtaining all the quadratic points on the aforementioned modular curves, we study their moduli interpretation and derive interesting consequences from this. Quadratic points on $X_0(n)$ (except for the cusps) correspond to $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over quadratic fields with an n-isogeny. Hence studying these points gives us information about the properties of such elliptic curves.

Taking inverse images of $\mathbb{Q}$-points under the hyperelliptic map $X_0(n) \to \mathbb{P}^1(\mathbb{Q})$ gives an infinite set of points of $X_0(n)$ over quadratic fields. Apart from these, there are only finitely many quadratic points; we call these quadratic points *exceptional*.

We show that for all elliptic curves over quadratic fields K with a 28- or 40-isogeny, the quadratic field K is real, except in a few explicitly listed cases.

Recall that a $\mathbb{Q}$-*curve* over a number field $K \subset \overline{\mathbb{Q}}$ is an elliptic curve E over K that is $\overline{\mathbb{Q}}$-isogenous to all of its Galois conjugates ${}^\sigma E$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If K is quadratic and σ is the non-trivial automorphism of K, then E is a $\mathbb{Q}$-curve if and only if E is $\overline{\mathbb{Q}}$-isogenous to ${}^\sigma E$. We prove that all elliptic curves over quadratic fields obtained from points of $\mathbb{P}^1(\mathbb{Q})$ as above are in fact $\mathbb{Q}$-curves. The fact that there are only finitely many exceptional quadratic points means that, up to $\overline{\mathbb{Q}}$-isomorphism, there are only finitely many elliptic curves over quadratic fields with an n-isogeny that are not $\mathbb{Q}$-curves.

Let E be a $\mathbb{Q}$-curve without complex multiplication over a quadratic field K with an n-isogeny, arising from the inverse image of a point of $\mathbb{P}^1(\mathbb{Q})$ as above. Then E is not in general K-isogenous to its Galois conjugate ${}^\sigma E$, but it is by construction K-isogenous to a quadratic twist of ${}^\sigma E$. It follows that E becomes isogenous to ${}^\sigma E$ after base change to a quadratic extension L of K. We explicitly construct such an extension L. Moreover, we prove that E has even rank over L.

Similar results were proved in [5] for elliptic curves E over quadratic fields K with torsion group $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{13, 16, 18\}$. These follow from arithmetic properties of the relevant modular curves $X_1(n)$. In [5] it was also proved that for $n = 13$ and $n = 18$, the endomorphism ring of the restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}} E$ of such a curve E contains an order in a quadratic field, which implies that $\mathrm{Res}_{K/\mathbb{Q}} E(\mathbb{Q}) \simeq E(K)$ has even rank. We say that E has *false complex multiplication*; see [5] for a precise definition. In all the cases we consider, our construction implies that E has false complex multiplication over L in the sense of [5].

Remark 2. The difficulty that E is not K-isogenous to ${}^\sigma E$, but only to a twist of ${}^\sigma E$, does not happen for the elliptic curves with prescribed torsion studied in [5]. This is explained by the fact that $X_0(n)$ is only a coarse moduli space, while $X_1(n)$ is a fine moduli space.

We now give an overview of the structure of the paper.

In Section 2, we compute $J_0(n)(\mathbb{Q})$ and describe all the quadratic points on $X_0(n)$. We apply these results to show that for $n = 28$ and 40 almost all elliptic curves with n-isogenies are defined over real quadratic fields (Theorem 4). We also prove that the largest k such that there exist infinitely many K-isogeny classes over quadratic fields K containing k curves is $k = 16$ (Theorem 6).

In Section 3, we give a moduli interpretation of the action on $X_0(n)$ of the normalizer of $\Gamma_0(n)$ in $\mathrm{GL}_2(\mathbb{Q})^+$, and in particular of the hyperelliptic involution ι.

This is well known in the case where ι is an Atkin–Lehner involution, but we have chosen to present this material from a general perspective that also encompasses the non-Atkin–Lehner involutions in the cases $n = 40$ and 48.

In Sections 4 and 5, we show that the non-exceptional quadratic points on $X_0(n)$ give rise to $\mathbb{Q}$-curves (Theorem 12). We also show how to compute the fields of definition of the isogenies between the conjugates of such $\mathbb{Q}$-curves. This allows us to describe over which fields these elliptic curves acquire false complex multiplication, and by which rings.

In Section 6, we list all our computational results and give a moduli interpretation of the exceptional points.

The computer calculations were done using Magma [4]. In particular, we made use of plane models of $X_0(n)$ given by polynomials in $\mathbb{Q}[x, y]$, and the q-expansions of the modular functions x and y for every n. These data were obtained from M. Harrison's Small Modular Curve database, which is included in Magma.

Acknowledgments. We wish to thank Samir Siksek for enlightening discussions on this topic, and Chi-Yun Hsu, Ariyan Javanpeykar and Drew Sutherland for pointing out mistakes in earlier versions of the paper. We thank the referees for their comments, which greatly improved the exposition in the paper. Finally, we would like to thank Tarun Dalal, who found a number of mistakes in the article after it was published.

2. Quadratic points on $X_0(n)$

In this section we describe the set of all quadratic points on $X_0(n)$. We write $X = X_0(n)$ and $J = J_0(n)$. We write ι for the hyperelliptic involution of X, and we fix a hyperelliptic map $x\colon X \to \mathbb{P}^1$ and a cusp $C \in X(\mathbb{Q})$.

Using Magma's functionality for 2-descent [27], one proves in all the cases that we consider that J has rank 0 over $\mathbb{Q}$. One could alternatively prove that $J(\mathbb{Q})$ has rank 0 using L-functions [26, Section 3.10]. Thus in this section $J(\mathbb{Q})$ is finite.

2.1. **Finding the quadratic points.** We first observe that finding the quadratic points on X amounts to finding the rational points on the symmetric square $X^{(2)}$ of X, which classifies effective divisors of degree 2 on X. The map

$$\begin{aligned} \phi\colon X^{(2)} &\longrightarrow J \\ D &\longmapsto [D - C - \iota(C)] \end{aligned}$$

is an isomorphism onto its image, except above 0, and $\phi^{-1}\{0\}$ is isomorphic to $\mathbb{P}^1$. We have

$$X^{(2)}(\mathbb{Q}) = \phi^{-1}\{0\}(\mathbb{Q}) \cup \phi^{-1}(J(\mathbb{Q}) \setminus \{0\}).$$

Note that $\phi^{-1}(J(\mathbb{Q}) \setminus \{0\})$ is finite (since $J(\mathbb{Q})$ is finite by assumption), so the set of exceptional quadratic points on X is finite. Moreover, this set is easy to compute from $J(\mathbb{Q})$; we will do this explicitly in Section 6.

Let K be a quadratic field, let σ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$, and let P be a point in $X(K) \setminus X(\mathbb{Q})$ with rational x-coordinate. Then ι acts on P in the same way as σ. Let E be an elliptic curve over K in the $\overline{\mathbb{Q}}$-isomorphism class of elliptic curves (together with a subgroup) corresponding to P. As we will see, the moduli interpretation of ι (for example, ι is an Atkin–Lehner involution w_d for most values of n) implies that the curves E and ${}^{\sigma}E$ are $\overline{\mathbb{Q}}$-isogenous. Thus E is a $\mathbb{Q}$-curve.

This construction is similar to the one with hyperelliptic modular curves $X_1(n)$ [5, Section 4], but there is a fundamental difference. Namely, the curves $X_1(n)$ are fine moduli spaces, while $X_0(n)$ are only coarse moduli spaces. Consequently, the $\mathbb{Q}$-curves obtained from $X_1(n)$ in [5] are K-isogenous to their Galois conjugates, while our curves obtained from $X_0(n)$ are only K-isogenous to their Galois conjugates up to twist, meaning that E is K-isogenous to a twist of ${}^\sigma E$, or in other words that E and ${}^\sigma E$ are $\overline{\mathbb{Q}}$-isogenous. We refer to Elkies [7, Section 3] for a detailed exposition of the relevant properties of the curves $X_0(n)$.

By what we have seen, determining $X^{(2)}(\mathbb{Q})$ amounts to determining the finite group $J(\mathbb{Q})$, which we will do in the next proposition. Note that for all curves X that we consider, $X(\mathbb{Q})$ consists entirely of cusps. The *cuspidal subgroup* of $J(\mathbb{Q})$, denoted by C_J, is the subgroup of $J(\mathbb{Q})$ generated by the classes of the divisors $P_1 - P_2$, where P_1, P_2 are $\mathbb{Q}$-rational cusps of X.

Proposition 3. *Let n be an integer such that $X_0(n)$ is hyperelliptic of genus at least 2 and such that $J_0(n)(\mathbb{Q})$ has rank 0. Then $J_0(n)(\mathbb{Q})$ is equal to its cuspidal subgroup C_J.*

Proof. One can obtain an upper bound on the size of $J(\mathbb{Q})$ by using the fact that, for a prime p of good reduction, the prime-to-p part of $J(\mathbb{Q})$ injects into $J(\mathbb{F}_p)$. The function TorsionBound in Magma does exactly this. In all cases except $n \in \{30, 33, 39, 46, 48\}$, this immediately shows that $C_J = J(\mathbb{Q})$.

For $n \in \{30, 33, 39, 46, 48\}$, the bound obtained in this way is unfortunately larger than the order of the cuspidal subgroup. For $n = 30$ and $n = 48$, we only obtain that the index $(J(\mathbb{Q}) : C_J)$ is a divisor of 4, while for $n \in \{33, 39, 46\}$ the index is 1 or 2.

We deal with the cases $n = 33$ and $n = 39$ by studying the group structures of the reductions, not just their orders.

Let $n = 33$. One computes the group structure of C_J to be $(\mathbb{Z}/10\mathbb{Z})^2$. We compute

$$J(\mathbb{F}_5) \simeq \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$$

and

$$J(\mathbb{F}_7) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/10\mathbb{Z})^2.$$

Since $J(\mathbb{Q})$ injects into both of these groups, it follows that $J(\mathbb{Q}) = C_J$.

Similarly, in the case $n = 39$, one computes

$$\begin{aligned} C_J &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}, \\ J(\mathbb{F}_5) &\simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}, \\ J(\mathbb{F}_7) &\simeq (\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/28\mathbb{Z}, \end{aligned}$$

from which it follows that $J(\mathbb{Q}) = C_J$.

Let $n = 30$. We compute

$$\begin{aligned} C_J &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}, \\ J(\mathbb{F}_7) &\simeq (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/48\mathbb{Z}, \\ J(\mathbb{F}_{23}) &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus (\mathbb{Z}/24\mathbb{Z})^2. \end{aligned}$$

Therefore $J(\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$. Now the splitting field of $J[2]$ is $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$, and we can extract a basis for $J[2]$ from the classes of the divisors $P - Q$ where P and Q are Weierstrass points of X. By computing the Galois action with respect to this basis and taking invariants, one shows that $J(\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^3$. This implies that $J(\mathbb{Q}) = C_J$, as claimed.

Next, let $n = 46$. We compute C_J as

$$C_J \simeq \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}.$$

Using reduction modulo 3 and 5, one shows that $J(\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/22\mathbb{Z})^2$. The splitting field of $J[2]$ is $\mathbb{Q}(\sqrt{-23}, \alpha)$, where $\alpha^3 - \alpha - 1 = 0$. Computing the Galois action on $J[2]$ as above, we obtain $J(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$, from which we conclude that $J(\mathbb{Q}) = C_J$.

Finally, let $n = 48$. This case is harder, and we use the following method, proposed to us by Samir Siksek. We have

$$C_J \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z},$$
$$J(\mathbb{F}_5) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/8\mathbb{Z})^2.$$

By computing the Galois action on $J[2]$ as above, we obtain $J(\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^3$, and hence $J(\mathbb{Q})[2] \subseteq C_J$. Suppose that $J(\mathbb{Q}) \neq C_J$; then there exist $P \in C_J$ and $Q \in J(\mathbb{Q}) \setminus C_J$ such that $2Q = P$. This implies that $P + 2C_J$ is in the kernel of the map

$$C_J/2C_J \to J(\mathbb{Q})/2J(\mathbb{Q}),$$

and hence also in the kernel of

$$C_J/2C_J \to J(\mathbb{F}_5)/2J(\mathbb{F}_5). \tag{1}$$

An explicit calculation shows that the map (1) is injective. Thus P is in $2C_J$, say $P = 2R$ for some $R \in C_J$. It follows that $P = 2R$ and $2(Q - R) = 0$ in $J(\mathbb{Q})$. Since C_J contains the complete 2-torsion of $J(\mathbb{Q})$, it follows that $Q \in C_J$, which is a contradiction. We conclude that $J(\mathbb{Q}) = C_J$. □

2.2. **Fields of definition of elliptic curves with 28- or 40-isogenies.** We now prove that all but finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over quadratic fields with 28- or 40-isogenies are defined over real quadratic fields. This follows from the description of all quadratic points that we have just obtained.

Theorem 4. *With finitely many exceptions (up to $\overline{\mathbb{Q}}$-isomorphism), all elliptic curves over quadratic fields with a 28- or 40-isogeny are defined over real quadratic fields.*

Proof. The modular curves $X_0(28)$ and $X_0(40)$ admit the following equations (see for example [9, Section 4.3] or [8, Sections 4.3–4.4]):

$$X_0(28)\colon y^2 = f_{28}(x) = x^6 + 10x^4 + 25x^2 + 28,$$
$$X_0(40)\colon y^2 = f_{40}(x) = x^8 + 8x^6 - 2x^4 + 8x^2 + 1.$$

Let P be a non-exceptional quadratic point on $X_0(n)$, where $n = 28$ or 40. Then P is of the form $(x, \sqrt{f_n(x)})$ with $x \in \mathbb{Q}$. It clear that $f_n(x) > 0$, so P is defined over a real quadratic field. □

Remark 5. The exceptions mentioned in Theorem 4 do occur: there exist elliptic curves over *imaginary* quadratic fields with a 28- or 40-isogeny. There are finitely many $\overline{\mathbb{Q}}$-isomorphism classes of such curves, corresponding to the points in Tables 4 and 11.

2.3. **Number of elliptic curves in an isogeny class.** We now prove a result about isogeny classes of elliptic curves over quadratic fields. Kenku proved in [19] that any $\mathbb{Q}$-isogeny class of elliptic curves contains at most 8 curves. In [2], the authors find isogeny classes over $\mathbb{Q}(\sqrt{5})$ containing 10 curves. We show that the largest k such that there are infinitely many isogeny classes over quadratic fields containing k curves is $k = 16$, coming from points on $X_0(48)$. When counting isogeny classes, we count up to $\overline{\mathbb{Q}}$-isomorphism.

Theorem 6. *There are infinitely many isogeny classes of elliptic curves over quadratic fields containing* 16 *curves. For all $k > 16$, there are only finitely many isogeny classes of elliptic curves over quadratic fields containing k curves.*

Proof. Since $X_0(48)$ is hyperelliptic, it has infinitely many quadratic points. Since there are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over quadratic fields with complex multiplication, there are in fact infinitely many quadratic points on $X_0(48)$ corresponding to elliptic curves without complex multiplication. Let E_1 be an elliptic curve over a quadratic field K corresponding to such a point.

Let $f_{1,5}\colon E_1 \to E_5$ be a 16-isogeny (over K) to another curve E_5. Then $f_{1,5}$ factors as $f_{4,5} \circ f_{3,4} \circ f_{2,3} \circ f_{1,2}$, where $f_{i,i+1}$ is a 2-isogeny from E_i to E_{i+1} and E_2, E_3 and E_4 are elliptic curves over K. We note that E_2, E_3 and E_4 all have two distinct 2-isogenies over K. It follows that $E_2(K)$, $E_3(K)$ and $E_4(K)$ all have full 2-torsion. This implies that each of these curves has a third 2-isogeny, say to E_6, E_7 and E_8, respectively. We obtain the following isogeny diagram:

$$\begin{tikzcd}
E_1 \arrow[r, dash] & E_2 \arrow[r, dash] \arrow[d, dash] & E_3 \arrow[r, dash] \arrow[d, dash] & E_4 \arrow[r, dash] \arrow[d, dash] & E_5 \\
 & E_6 & E_7 & E_8 &
\end{tikzcd}$$

Each of the E_i is 3-isogenous (over K) to an elliptic curve E_i', and hence we get 16 elliptic curves in this isogeny class.

The second claim follows from results of Bars [3, Theorem 4.3]. $\square$

Remark 7. The elliptic curve E_1 is 12-isogenous to a twist of ${}^\sigma E_1$, so ${}^\sigma E_1$ is a twist of either E_3' or E_6'. It follows from the moduli interpretation of β_{48} (see §3.4) that the kernel of this isogeny is not in the kernel of a 48-isogeny, ruling out E_3'. We conclude that ${}^\sigma E_1$ is a twist of E_6'.

3. Moduli interpretation of the normalizer of $\Gamma_0(n)$

Let n be a positive integer, and let $B(\Gamma_0(n))$ denote the normalizer of $\Gamma_0(n)$ in the group $\mathrm{GL}_2(\mathbb{Q})^+$ of 2×2-matrices over $\mathbb{Q}$ with positive determinant. In this section, we describe a canonical action of $B(\Gamma_0(n))$ on $X_0(n)$, and we give a moduli interpretation of this action. From this we then derive a moduli interpretation of the hyperelliptic involution of $X_0(n)$. This lies at the basis of the constructions and results of the next two sections.

3.1. **The action of $B(\Gamma_0(n))$.** Let $\mathcal{C}_n$ be the category defined as follows. The objects of $\mathcal{C}_n$ are triples $(E \to S, C, \omega)$ consisting of an elliptic curve E over a $\mathbb{Q}$-scheme S, a cyclic subgroup scheme C of order n of E and a nowhere-vanishing global relative differential ω on E. A morphism $(E' \to S', C', \omega') \longrightarrow (E \to S, C, \omega)$ in $\mathcal{C}_n$ is a Cartesian diagram of schemes

$$\begin{array}{ccc} E' & \xrightarrow{\phi} & E \\ \downarrow & & \downarrow \\ S' & \longrightarrow & S \end{array}$$

that is compatible with the group structure and satisfies $\phi^* C = C'$ and $\phi^*\omega = \omega'$. We will usually omit S from the notation.

We let $B(\Gamma_0(n))$ act by equivalences of categories on $\mathcal{C}_n$ as follows. Let $\gamma \in B(\Gamma_0(n))$. First we consider the case where γ is a scalar matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ with $a \in \mathbb{Q}^\times$. For such γ, we define

$$\gamma(E, C, \omega) = (E, C, a^{-1}\omega).$$

Next we may assume that γ is of the form $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$. We put $\delta = \det\gamma = ad - bc$; this is a positive integer. After étale localization on S, we can choose an isomorphism

$$\phi\colon (\mathbb{Z}/n\delta\mathbb{Z})^2_S \xrightarrow{\sim} E[n\delta].$$

We may assume that the subgroup $\langle\phi(0, \delta)\rangle$ generated by $\phi(0, \delta)$ equals C. We put

$$C_\gamma = n\langle\phi(a, b), \phi(c, d)\rangle \subset E.$$

This is a subgroup of order δ whose structure (elementary divisors) is given by the Smith normal form of γ. Furthermore, we put

$$E' = E/C_\gamma$$

and

$$C' = (\langle\phi(c, d)\rangle + C_\gamma)/C_\gamma \subset E';$$

one easily sees that C' is cyclic of order n. There exists a unique differential ω' on E/C_γ whose pull-back to E equals ω. We define

$$\gamma(E, C, \omega) = (E', C', \omega').$$

Because $X_0(n)$ is the coarse moduli space of pairs (E, C) as above and the above construction commutes with scaling ω, any $\gamma \in B(\Gamma_0(n))$ induces an automorphism

$$\iota_\gamma\colon X_0(n) \xrightarrow{\sim} X_0(n).$$

This automorphism only depends on the image of γ in $B(\Gamma_0(n))/\Gamma_0(n)$. Thus we get an action of the latter group by automorphisms of the curve $X_0(n)$ over $\mathbb{Q}$.

3.2. **The complex perspective.** We now study an analogous construction over the complex numbers, where we can express elliptic curves using lattices.

Let $\mathcal{L}_\mathbb{Q}$ denote the set of all group homomorphisms $\psi\colon \mathbb{Q}^2 \to \mathbb{C}$ such that the group

$$L_\psi = \psi(\mathbb{Z}^2) = \mathbb{Z}\psi(1, 0) + \mathbb{Z}\psi(0, 1)$$

is a "positively-oriented" lattice in $\mathbb{C}$, in the sense that $\psi(1, 0)$ and $\psi(0, 1)$ are $\mathbb{R}$-linearly independent and $\psi(1, 0)/\psi(0, 1)$ has positive imaginary part.

We define a free left action of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathcal{L}_\mathbb{Q}$ as follows: given $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$ and $\psi\colon \mathbb{Q}^2 \to \mathbb{C}$ in $\mathcal{L}_\mathbb{Q}$, we define $\gamma\psi \in \mathcal{L}_\mathbb{Q}$ by

$$(\gamma\psi)(v) = \frac{1}{\det\gamma}\psi(v\gamma),$$

where $v\gamma$ denotes the usual right action of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathbb{Q}^2$ ("row vectors"). More concretely, the bases (ω_1, ω_2) of L_ψ and (ω_1', ω_2') of $L_{\gamma\psi}$ defined by

$$\omega_1 = \psi(1,0), \quad \omega_2 = \psi(0,1),$$
$$\omega_1' = (\gamma\psi)(1,0), \quad \omega_2' = (\gamma\psi)(0,1),$$

satisfy the relation

$$\omega_1' = \frac{1}{\det\gamma}(a\omega_1 + b\omega_2), \quad \omega_2' = \frac{1}{\det\gamma}(c\omega_1 + d\omega_2). \tag{2}$$

Lemma 8. (1) *Let ψ and ψ' be in $\mathcal{L}_\mathbb{Q}$. Then $L_\psi = L_{\psi'}$ if and only if the orbits $\mathrm{SL}_2(\mathbb{Z})\psi$ and $\mathrm{SL}_2(\mathbb{Z})\psi'$ are equal.*
(2) *Let ψ be in $\mathcal{L}_\mathbb{Q}$, and let γ and γ' be in $\mathrm{GL}_2(\mathbb{Q})^+$. Then $L_{\gamma\psi} = L_{\gamma'\psi}$ if and only if the cosets $\mathrm{SL}_2(\mathbb{Z})\gamma$ and $\mathrm{SL}_2(\mathbb{Z})\gamma'$ are equal.*

Proof. The first claim is easy to verify; the second one follows from the first and the fact that $\mathrm{GL}_2(\mathbb{Q})^+$ acts freely on $\mathcal{L}_\mathbb{Q}$. □

Now let n be a positive integer. We write $\mathcal{L}_n$ for the set of pairs of lattices (L, L') in $\mathbb{C}$ such that $L' \supseteq L$ and L'/L is cyclic of order n. Let γ_n be the matrix $\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We define a map

$$\begin{aligned} \pi_n \colon \mathcal{L}_\mathbb{Q} &\longrightarrow \mathcal{L}_n \\ \psi &\longmapsto (L_\psi, L_{\gamma_n\psi}). \end{aligned}$$

We note that $L_{\gamma_n\psi}$ is the lattice spanned by $\psi(1,0)$ and $\frac{1}{n}\psi(0,1)$.

Lemma 9. *The map π_n is a quotient map for the left action of the subgroup $\Gamma_0(n) \subset \mathrm{GL}_2(\mathbb{Q})^+$ on $\mathcal{L}_\mathbb{Q}$.*

Proof. It is straightforward to check that π_n is surjective. We have

$$\pi_n(\gamma\psi) = (L_{\gamma\psi}, L_{\gamma_n\gamma\psi}).$$

Hence $\pi_n(\gamma\psi) = \pi_n(\psi)$ if and only if $L_{\gamma\psi} = L_\psi$ and $L_{\gamma_n\gamma\psi} = L_{\gamma_n\psi}$. By Lemma 8, this condition is equivalent to $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma_n\gamma\gamma_n^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, which is in turn equivalent to $\gamma \in \Gamma_0(n)$. □

The above result yields a natural action of $B(\Gamma_0(n))$ on $\mathcal{L}_n$. Viewing elements of $\mathcal{L}_n$ as values of π_n, we can describe this action as

$$\gamma(L_\psi, L_{\gamma_n\psi}) = (L_{\gamma\psi}, L_{\gamma_n\gamma\psi}) \quad \text{for all } \gamma \in B(\Gamma_0(n)) \text{ and } \psi \in \mathcal{L}_\mathbb{Q}.$$

Furthermore, there is a map from $\mathcal{L}_\mathbb{Q}$ to the upper half-plane $\mathbb{H}$ sending ψ to $\psi(1,0)/\psi(0,1)$. This descends to a map from $\mathcal{L}_n$ to the non-compact analytic modular curve $\Gamma_0(n)\backslash\mathbb{H}$. From these observations and the relation (2), we obtain a commutative diagram

$$\begin{tikzcd} \mathcal{L}_\mathbb{Q} \arrow[r] \arrow[d, "\pi_n"] & \mathbb{H} \arrow[d] \\ \mathcal{L}_n \arrow[r] & \Gamma_0(n)\backslash\mathbb{H} \end{tikzcd}$$

in which the upper horizontal map is compatible with the action of $\mathrm{GL}_2(\mathbb{Q})^+$ and the lower horizontal map is compatible with the action of $B(\Gamma_0(n))$.

3.3. **Compatibility.** We now show that the constructions in the two preceding sections are compatible. This allows us to reinterpret the action of $B(\Gamma_0(n))$ on the analytic modular curve $\Gamma_0(n)\backslash\mathbb{H}$ as an action on objects of $\mathcal{C}_n$.

Let $\mathcal{C}_n^{\mathrm{an}}$ be the set of isomorphism classes of (analytified) objects of $\mathcal{C}_n$ over the base $S = \operatorname{Spec}\mathbb{C}$. The action of $B(\Gamma_0(n))$ on $\mathcal{C}_n$ induces an action on $\mathcal{C}_n^{\mathrm{an}}$. We define a map

$$\begin{aligned} F_n \colon \mathcal{L}_n &\longrightarrow \mathcal{C}_n^{\mathrm{an}} \\ (L, L') &\longmapsto (\mathbb{C}/L, L'/L, 2\pi i\,\mathrm{d}z). \end{aligned}$$

The following result shows that F_n respects the actions of $B(\Gamma_0(n))$ that we have defined on $\mathcal{L}_n$ and on $\mathcal{C}_n^{\mathrm{an}}$, respectively.

Proposition 10. *For all $\gamma \in B(\Gamma_0(n))$ and all $(L, L') \in \mathcal{L}_n$, we have*

$$F_n(\gamma(L, L')) = \gamma(F_n(L, L')).$$

Proof. Let $(L, L') \in \mathcal{L}$, and let $\psi \in \mathcal{L}_{\mathbb{Q}}$ be such that $\pi_n(\psi) = (L, L')$, so that $L = L_\psi$ and $L' = L_{\gamma_n\psi}$. In $\mathcal{C}_n^{\mathrm{an}}$, we then have

$$F_n(L, L') = (\mathbb{C}/L_\psi, L_{\gamma_n\psi}/L_\psi, 2\pi i\,\mathrm{d}z).$$

We first assume that γ is a scalar matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ with $a \in \mathbb{Q}^\times$. Then (2) implies

$$L_{\gamma\psi} = a^{-1}L_\psi = a^{-1}L \quad \text{and} \quad L_{\gamma_n\gamma\psi} = a^{-1}L_{\gamma_n\psi} = a^{-1}L'.$$

This implies

$$\begin{aligned} F_n(\gamma(L, L')) &= F_n(a^{-1}L, a^{-1}L') \\ &= (\mathbb{C}/a^{-1}L, a^{-1}L/a^{-1}L', 2\pi i\,\mathrm{d}z). \end{aligned}$$

On the other hand, we have

$$\gamma(F_n(L, L')) = (\mathbb{C}/L, L/L', a^{-1} \cdot 2\pi i\,\mathrm{d}z).$$

These two objects are isomorphic via the map $z \mapsto az$.

Next we assume that γ is of the form $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ and $\delta = ad - bc > 0$. Then the lattices $L = L_\psi$ and $L_{\gamma\psi}$ satisfy $L_{\gamma\psi} \supseteq L_\psi$ and $L_{\gamma\psi}/L_\psi$ has order δ. We define a group isomorphism

$$\begin{aligned} \phi \colon (\mathbb{Z}/n\delta\mathbb{Z})^2 &\xrightarrow{\sim} (\mathbb{C}/L)[n\delta] = \frac{1}{n\delta}L/L \\ (x \bmod n\delta, y \bmod n\delta) &\longmapsto \psi(x/n\delta, y/n\delta) \bmod L. \end{aligned}$$

A straightforward computation shows that both $\gamma(F_n(L, L'))$ and $F_n(\gamma(L, L'))$ are equal to $(\mathbb{C}/L_{\gamma\psi}, L_{\gamma_n\gamma\psi}/L_{\gamma\psi}, 2\pi i\,\mathrm{d}z)$ in $\mathcal{C}_n^{\mathrm{an}}$. This concludes the proof. □

3.4. **Moduli interpretation of the hyperelliptic involution.** We now describe an element $\gamma \in B(\Gamma_0(n))$ such that the hyperelliptic involution ι of $X_0(n)$ is the automorphism induced by γ as in §3.1, and we give a moduli interpretation of γ.

Suppose first that ι equals the Atkin–Lehner involution w_d for some $d \mid n$ with $\gcd(d, n/d) = 1$. This is the case for all n we consider except $n = 40$ and $n = 48$. For the matrix γ we can take any $\left(\begin{smallmatrix} ad & b \\ n & d \end{smallmatrix}\right)$ with $a, b \in \mathbb{Z}$ and $ad - b(n/d) = 1$.

In [25, Section 4] it is proved that for $n = 40$, the involution ι is induced by the action of the matrix $\beta_{40} = \left(\begin{smallmatrix} -10 & 1 \\ -120 & 10 \end{smallmatrix}\right) \in B(\Gamma_0(40))$ of determinant 20, and that for $n = 48$ it is induced by the matrix $\beta_{48} = \left(\begin{smallmatrix} -6 & 1 \\ -48 & 6 \end{smallmatrix}\right) \in B(\Gamma_0(48))$ of determinant 12.

By the description of the action of $B(\Gamma_0(n))$ in §3.1, the element γ equips every elliptic curve with a cyclic subgroup C of order n with a second cyclic subgroup C_γ of order δ, where $\delta = \det\gamma$, and hence with a δ-isogeny. If $\iota = w_d$, then we have

$C_\gamma = (n/d)C$; if $n = 40$, then C_γ is a subgroup of order 20 such that $C \cap C_\gamma$ has order 10; if $n = 48$, then C_γ is a subgroup of order 12 such that $C \cap C_\gamma$ has order 6.

4. Modular forms

Let n be a positive integer, and let $\gamma \in B(\Gamma_0(n))$. In this section, we construct a modular form A_γ of weight 2 for $\Gamma_0(n)$, based on the moduli interpretation of γ described in §3.1. The reason for introducing A_γ is that it allows us to explicitly compute the isogenies determined by the hyperelliptic involution of $X_0(n)$. This generalizes the methods of Elkies [7] to our setting.

More precisely, let $(E \to S, C, \omega)$ be an object of $\mathcal{C}_n$, and let C_γ be the cyclic subgroup of E determined by the moduli interpretation of γ as in §3.1. Let E' be the quotient E/C_γ, equipped with the differential induced from E. In the situation of Section 5 below, we know explicit expressions for E, E', δ and $A_\gamma(E,\omega)$. The subgroup C_γ can be computed from these data using an algorithm due to Elkies [7, Section 3]. We can then use Vélu's formulae [28] to compute rational functions defining an isogeny $E \to E'$ with kernel C_γ.

4.1. **Preliminaries.**

We begin by recalling the facts about modular forms that we need and introducing our notation.

A modular form of weight k for $\Gamma_0(n)$ can be viewed (à la Katz) as a rule that to every object $(E \to S, C, \omega)$ of $\mathcal{C}_n$, where we may restrict to the case where S is an affine scheme $\operatorname{Spec} A$, assigns an element $F(E \to S, C, \omega) \in A$ that satisfies $F(E \to S, C, \lambda\omega) = \lambda^{-k} F(E \to S, C, \omega)$ for all $\lambda \in A^\times$, is compatible with morphisms in $\mathcal{C}_n$ as in §3.1, and is regular at the cusps in a suitable sense; see Katz [14, Chapter 1] for details.

If E is the Tate curve over $\mathbb{C}((q))$ with parameter ζ, equipped with the canonical subgroup $C = \mu_n$ and the canonical differential $\omega = \frac{\mathrm{d}\zeta}{\zeta}$, then the q-expansion of F is $F(q) = F(E, C, \omega) \in \mathbb{C}((q))$. The space of modular forms of weight 2 for $\Gamma_0(n)$ is isomorphic to the space of logarithmic differentials on $X_0(n)$; see for example Katz [14, Appendix 1]. If F_α is the modular form of weight 2 attached to a logarithmic differential α, the relation between α and F_α can be expressed in terms of the q-expansion of F_α as $\alpha = F_\alpha(q)\frac{\mathrm{d}q}{q}$.

Over $\mathbb{C}$, modular forms F as above correspond to functions f on the upper half-plane $\mathbb{H}$: if $(E, C, \omega) = (\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \langle 1/n \rangle, 2\pi i\,\mathrm{d}z)$, then $F(E, C, \omega) = f(\tau)$. The logarithmic differential corresponding to a modular form f is $f(\tau)\frac{\mathrm{d}q}{q}$, where $q = \exp(2\pi i \tau)$.

The group $B(\Gamma_0(n))$ acts from the right on the space of modular forms of weight k for $\Gamma_0(n)$ via

$$(F|_k\gamma)(E, C, \omega) = F(\gamma(E, C, \omega)).$$

If α is a logarithmic differential on $X_0(n)$ and ι is the automorphism of $X_0(n)$ induced by γ, we have

$$F_\alpha|_2\gamma = (\det \gamma) F_{\iota^*\alpha}. \tag{3}$$

As usual, we write $\sigma_k(m)$ for the sum of the k-th powers of the positive divisors of m. Let $\mathbb{E}_4$ and $\mathbb{E}_6$ denote the standard Eisenstein series, normalized so that their

q-expansions are

$$\mathbb{E}_4(q) = \frac{1}{240} + \sum_{m=1}^{\infty} \sigma_3(m) q^m,$$
$$\mathbb{E}_6(q) = -\frac{1}{504} + \sum_{m=1}^{\infty} \sigma_5(m) q^m.$$

If E is elliptic curve given by a Weierstrass equation in x and y, equipped with the standard differential $\omega = \frac{\mathrm{d}x}{2y}$, these Eisenstein series are related to the usual coefficients c_4 and c_6 by

$$c_4 = 240\,\mathbb{E}_4(E,\omega) \quad \text{and} \quad c_6 = 504\,\mathbb{E}_6(E,\omega).$$

We view $\mathbb{E}_4$ and $\mathbb{E}_6$ as modular forms for $\Gamma_0(n)$. Furthermore, for every divisor d of n, let $\mathbb{E}_2^{(d)}$ be the modular form of weight 2 for $\Gamma_0(n)$ given by the q-expansion

$$\mathbb{E}_2^{(d)}(q) = \mathbb{E}_2(q) - d\,\mathbb{E}_2(q^d),$$

where

$$\begin{aligned}\mathbb{E}_2(q) &= -\frac{1}{24} + \sum_{m=1}^{\infty} \sigma_1(m) q^m \\ &= -\frac{1}{24} + \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2}.\end{aligned}$$

4.2. **The modular form A_γ.** Let n be a positive integer, and let $\gamma \in B(\Gamma_0(n))$. Let $(E \to S, C, \omega)$ be an object of $\mathcal{C}_n$, and let C_γ be the cyclic subgroup of E determined by the moduli interpretation of γ as in §3.1. We may assume that S is an affine scheme $\operatorname{Spec} R$ and that E is given by a short Weierstrass equation

$$E\colon y^2 = x^3 + a_4 x + a_6 \qquad (a_4, a_6 \in R,\ 4a_4^3 + 27a_6^2 \neq 0)$$

with $\omega = \mathrm{d}x/(2y)$. We put

$$A_\gamma(E \to S, C, \omega) = \sum_{P \in C_\gamma \setminus \{0\}} x(P) \in R.$$

One can check that this construction defines a modular form of weight 2 on $X_0(n)$.

Next, for all n in the set mentioned in the introduction, we will derive an explicit expression for A_γ in terms of Eisenstein series, where γ is the matrix inducing the hyperelliptic involution fixed in §3.4.

If n is not 40 or 48, the hyperelliptic involution of $X_0(n)$ equals the Atkin–Lehner involution w_d for some $d \mid n$ with $\gcd(d, n/d) = 1$. One can show that

$$A_\gamma = -2d\,\mathbb{E}_2^{(d)}; \tag{4}$$

see Elkies [7, Section 3].

In the remaining cases $n = 40$ and $n = 48$, the hyperelliptic involution of $X_0(n)$ is not an Atkin–Lehner involution. In these cases we have $\gamma = \beta_{40}$ and $\gamma = \beta_{48}$, respectively, as defined in §3.4.

Proposition 11. *The q-expansions of the modular forms $A_{\beta_{40}}$ and $A_{\beta_{48}}$ are*

$$A_{\beta_{40}}(q) = 40(\mathbb{E}_2^{(5)}(q) - 3\,\mathbb{E}_2^{(10)}(q) + \mathbb{E}_2^{(20)}(q)),$$
$$A_{\beta_{48}}(q) = 24(\mathbb{E}_2^{(3)}(q) - 3\,\mathbb{E}_2^{(6)}(q) + \mathbb{E}_2^{(12)}(q)).$$

Proof. The computation is inspired by Elkies's proof of (4). We compute the q-expansion by evaluating $A_{\beta_{40}}$ on the Tate curve $\mathbb{C}/q^{\mathbb{Z}}$ over $\mathbb{C}((q))$ with coordinate ζ, equipped with the standard subgroup μ_n and the differential $\mathrm{d}\zeta/\zeta$. The subgroup $C_{\beta_{40}}$ is cyclic of order 20, generated by $q^{1/2}\zeta_{20}$. The x-coordinates occurring in the definition of $A_{\beta_{40}}$ can then be viewed as values of the Weierstrass $\wp$-function. From the definition of $A_{\beta_{40}}$ and the classical formula

$$\wp(z;\tau) = (2\pi i)^2\left(-2\,\mathbb{E}_2(q) + \sum_{n=-\infty}^{\infty}\frac{q^n\zeta}{(1-q^n\zeta)^2}\right),$$

where $q = \exp(2\pi i\tau)$ and $\zeta = \exp(2\pi i z)$, we deduce

$$\begin{aligned} A_{\beta_{40}}(q) &= \sum_{\zeta\in C_{\beta_{40}}\setminus\{0\}}\left(-2\,\mathbb{E}_2(q) + \sum_{n\in\mathbb{Z}}\frac{q^n\zeta}{(1-q^n\zeta)^2}\right) \\ &= -38\,\mathbb{E}_2(q) + \sum_{\zeta\in C_{\beta_{40}}}\sum_{n\in\mathbb{Z}}\frac{q^n\zeta}{(1-q^n\zeta)^2}. \end{aligned}$$

It is a straightforward but tedious formal computation to show that

$$A_{\beta_{40}}(q) = -38\,\mathbb{E}_2(q) + \sum_{n\in\mathbb{Z}}\biggl(S_{10}(q^n) - S_{10}(q^{n+1/2}) + S_{20}(q^{n+1/2})\biggr),$$

where for $m \geq 1$ the rational function $S_m \in \mathbb{Q}(\zeta_m)(x)$ is defined by

$$S_m = \sum_{k=1}^{m-1}\frac{\zeta_m^k x}{(1-\zeta_m^k x)^2}.$$

By expanding in a Taylor series around $x = 0$, we obtain

$$S_m = m^2\sum_{l\geq 1} l x^{lm} - \sum_{l\geq 1} l x^l \in \mathbb{Q}[[x]],$$

and hence

$$S_m = m^2\frac{x^m}{(1-x^m)^2} - \frac{x}{(1-x)^2} \in \mathbb{Q}(x).$$

By substituting $x = \exp(t)$ and expanding in a Taylor series around $t = 0$, we get

$$S_m(1) = \frac{1-m^2}{12}.$$

Furthermore, it is easy to check that S_m is invariant under replacing x by $1/x$. We therefore obtain

$$\begin{aligned}
A_{\beta_{40}} &= -38\,\mathbb{E}_2(q) - \frac{99}{12} + 2\sum_{n\geq 1} S_{10}(q^n) - 2\sum_{n\geq 0} S_{10}(q^{n+1/2}) + 2\sum_{n\geq 0} S_{20}(q^{n+1/2}) \\
&= -38\,\mathbb{E}_2(q) - \frac{99}{12} + 2\sum_{n\geq 1}\left(100\frac{q^{10n}}{(1-q^{10n})^2} - \frac{q^n}{(1-q^n)^2}\right) \\
&\quad - 2\sum_{n\geq 0}\left(100\frac{q^{10n+5}}{(1-q^{10n+5})^2} - \frac{q^{n+1/2}}{(1-q^{n+1/2})^2}\right) \\
&\quad + 2\sum_{n\geq 0}\left(400\frac{q^{20n+10}}{(1-q^{20n+10})^2} - \frac{q^{n+1/2}}{(1-q^{n+1/2})^2}\right) \\
&= -40\,\mathbb{E}_2(q) + 200\,\mathbb{E}_2(q^{10}) - 200\sum_{n\geq 0}\frac{q^{10n+5}}{(1-q^{10n+5})^2} + 800\sum_{n\geq 0}\frac{q^{20n+10}}{(1-q^{20n+10})^2} \\
&= -40\,\mathbb{E}_2(q) + 200\,\mathbb{E}_2(q^{10}) - 200(\mathbb{E}_2(q^5) - \mathbb{E}_2(q^{10})) + 800(\mathbb{E}_2(q^{10}) - \mathbb{E}_2(q^{20})) \\
&= -40\,\mathbb{E}_2(q) - 200\,\mathbb{E}_2(q^5) + 1200\,\mathbb{E}_2(q^{10}) - 800\,\mathbb{E}_2(q^{20}).
\end{aligned}$$

which gives the first claimed equality; the second follows from the definition of $\mathbb{E}_2^{(d)}$.

Similarly, the hyperelliptic involution on $X_0(48)$ is induced by the action of the matrix $\beta_{48} = \left(\begin{smallmatrix} -6 & 1 \\ -48 & 6 \end{smallmatrix}\right)$ of determinant 12 on $\mathcal{C}_{40}$ and on $\mathcal{L}_{40}$. A calculation analogous to the one above gives the claimed identity. □

5. Moduli interpretation of quadratic points

Let n be such that $X_0(n)$ is hyperelliptic of genus ≥ 2 and such that $J_0(n)(\mathbb{Q})$ has rank 0. The purpose of this section is to give a moduli interpretation of the quadratic points of $X_0(n)$. In particular, we show that if E is an elliptic curve over a quadratic field K admitting an n-isogeny, then E is K-isogenous to a quadratic twist of its Galois conjugate, with finitely many exceptions up to $\overline{\mathbb{Q}}$-isomorphism. The following theorem summarizes the results of this section.

Theorem 12. *Let K be a quadratic field, and let E be an elliptic curve over K without complex multiplication coming from a non-exceptional point of $X_0(n)(K)$. Then there is a quadratic extension L of K (which can be explicitly computed) such that the following holds.*

1. *The curve E is a $\mathbb{Q}$-curve that is completely defined over L.*
2. *The curve E acquires even rank over L.*

5.1. **The moduli interpretation.** Let ι be the hyperelliptic involution on $X_0(n)$, and let γ be the element of $B(\Gamma_0(n))$ chosen in §3.4 so that γ induces the hyperelliptic involution ι. We put

$$\delta = \det \gamma.$$

We fix a non-zero meromorphic differential α on $X_0(n)$ satisfying

$$\iota^*\alpha = -\alpha.$$

Let f_α be the cusp form of weight 2 corresponding to α as in §4.1. Then we can uniquely express $\mathbb{E}_4$ and $\mathbb{E}_6$ as

$$\mathbb{E}_4 = g_4 f_\alpha^2 \quad \text{and} \quad \mathbb{E}_6 = g_6 f_\alpha^3,$$

where g_4, g_6 are meromorphic functions on $X_0(n)$.

Lemma 13. *The action of γ on $\mathbb{E}_4$ and $\mathbb{E}_6$ is given by*

$$\mathbb{E}_4|_4\gamma = (-\delta)^2\frac{\iota^* g_4}{g_4}\,\mathbb{E}_4 \quad \textit{and} \quad \mathbb{E}_6|_6\gamma = (-\delta)^3\frac{\iota^* g_6}{g_6}\,\mathbb{E}_6\,.$$

Proof. By (3) we have $f_\alpha|_2\gamma = \delta f_{\iota^*\alpha}$; our choice of α implies $f_{\iota^*\alpha} = f_{-\alpha} = -f_\alpha$. The claim now follows from the identities $\mathbb{E}_4|_4\gamma = (\iota^* g_4)(f_\alpha|_2\gamma)^2$ and $\mathbb{E}_6|_6\gamma = (\iota^* g_6)(f_\alpha|_2\gamma)^3$. □

For the rest of this section, we fix the following data. Let K be a quadratic field, and let σ be the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Let E be an elliptic curve over K together with a cyclic subgroup C of order n. Let P be the K-rational point of $X_0(n)$ determined by (E, C). We assume that E does not have complex multiplication, and furthermore that the K-rational point of $X_0(n)$ defined by the pair (E, C) is not in the finite set of exceptional quadratic points on $X_0(n)$.

We fix a non-zero global differential ω on E; this gives rise to a (non-uniquely determined) Weierstrass equation and to the usual c-coefficients c_4 and c_6, which only depend on ω. We define μ and λ in $K^\times$ by

$$\mu = \frac{21 g_6(P) c_4}{10 g_4(P) c_6} \quad \text{and} \quad \lambda = -\delta\frac{\sigma(\mu)}{\mu}.$$

We define an extension L of K (of degree 1 or 2) by

$$L = K(\sqrt{\lambda}).$$

We note that L can also be written as $K\big(\sqrt{-\delta\,\mathrm{Norm}_{K/\mathbb{Q}}(\mu)}\big)$ and is therefore either K itself or a V_4-extension of $\mathbb{Q}$.

Let E' be an elliptic curve over K, equipped with a non-zero global differential ω' (or equivalently given by a short Weierstrass equation), such that the c-coefficients of (E', ω') are

$$c_4' = \lambda^2\sigma(c_4) \quad \text{and} \quad c_6' = \lambda^3\sigma(c_6).$$

We note that E' is a quadratic twist of the Galois conjugate ${}^\sigma E$ of E, namely $E' = ({}^\sigma E)^{(\lambda)}$.

Proposition 14. *In the above situation, there exists a δ-isogeny $\mu\colon E \to E'$ with kernel C_γ satisfying $\mu^*\omega' = \omega$.*

Proof. Let ω'' be the differential induced by ω on E/C_γ, and let c_4'' and c_6'' be the c-coefficients corresponding to $(E/C_\gamma, \omega'')$. We have to prove that $(E/C_\gamma, \omega'')$ is isomorphic to (E', ω'). It is enough to show that $(c_4', c_6') = (c_4'', c_6'')$, or equivalently that each of the two modular forms $\mathbb{E}_4$ and $\mathbb{E}_6$ takes the same value on $(E/C_\gamma, \omega'')$ and (E', ω').

There is some cyclic subgroup C' in E/C_γ such that

$$\gamma(E, C, \omega) = (E/C_\gamma, C', \omega'').$$

Using Lemma 13 and the fact that $\mathbb{E}_4$ only depends on (E,ω) and g_4 only depends on P, we get

$$\begin{aligned}\mathbb{E}_4(E/C_\gamma,\omega'') &= \mathbb{E}_4(E/C_\gamma,C',\omega'')\\ &= (\mathbb{E}_4|_4\gamma)(E,C,\omega)\\ &= (-\delta)^2\left(\frac{\iota^* g_4}{g_4}\right)(P)\,\mathbb{E}_4(E,C,\omega)\\ &= (-\delta)^2\frac{g_4(\iota(P))}{g_4(P)}\,\mathbb{E}_4(E,\omega).\end{aligned}$$

This implies

$$c_4'' = (-\delta)^2\frac{g_4(\iota(P))}{g_4(P)}c_4.$$

Noting that $g_4(\iota(P)) = \sigma(g_4(P))$, we rewrite this as

$$c_4'' = (-\delta)^2\frac{\sigma(g_4(P)/c_4)}{g_4(P)/c_4}\sigma(c_4).$$

Likewise,

$$c_6'' = (-\delta)^3\frac{\sigma(g_6(P)/c_6)}{g_6(P)/c_6}\sigma(c_6).$$

The fact that E defines the point P on $X_0(n)$ implies that E is a twist of the curve defined by $y^2 = x^3 - 5g_4(P)x - \frac{7}{12}g_6(P)$, so there exists $\mu \in K^\times$ such that

$$240g_4(P) = \mu^2 c_4 \quad\text{and}\quad 504g_6(P) = \mu^3 c_6. \tag{5}$$

This implies

$$c_4'' = \left(-\delta\frac{\sigma(\mu)}{\mu}\right)^2\sigma(c_4) \quad\text{and}\quad c_6'' = \left(-\delta\frac{\sigma(\mu)}{\mu}\right)^3\sigma(c_6).$$

Furthermore, it follows from (5) that μ can be expressed as

$$\mu = \frac{21g_6(P)c_4}{10g_4(P)c_6},$$

as claimed. □

Proof of Theorem 12. We take L to be the field defined above. The first claim follows from Proposition 14 and our assumption that E does not have complex multiplication. To prove the second claim, we note that the curves $E^{(\lambda)}$ and ${}^\sigma E$ are K-isogenous, which implies

$$\begin{aligned}\operatorname{rk} E(L) &= \operatorname{rk} E(K) + \operatorname{rk} E^{(\lambda)}(K)\\ &= \operatorname{rk} E(K) + \operatorname{rk} {}^\sigma E(K).\end{aligned}$$

It remains to observe that $E(K)$ and ${}^\sigma E(K)$ are isomorphic. □

Remark 15. One can in fact show that E acquires "false complex multiplication" over L, in the sense of [5]. More precisely, let $M = \mathbb{Q}$ if $L = K$, and let M be one of the quadratic subfields of L other than K itself if $[L : K] = 2$. Then there is an action of the ring $\mathbb{Z}[\sqrt{m}]$ on the Weil restriction $A = \operatorname{Res}_{L/M} E$ and hence on the group $A(M) = E(L)$, where m is either δ or $-\delta$. In particular, since δ is not a square in any of the cases we consider in this paper, $E(L)$ has even rank. The rank of E will also be even over many extensions of L; see [6] for details.

Remark 16. The question over which field the isogenies between a $\mathbb{Q}$-curve and its Galois conjugates are defined was studied from a somewhat different perspective by González [10]. We leave it to the interested reader to compare the two approaches.

5.2. **An example.** We now give an example to show how to explicitly compute the field of definition of an n-isogeny on an elliptic curve over a quadratic field corresponding to a non-exceptional quadratic point on $X_0(n)$. We take $n = 22$ for simplicity, but the same method works in all cases.

The curve $X_0(22)$ has genus 2, and the Small Modular Curve database in Magma gives the equation

$$X_0(22)\colon y^2 - x^3 y = -x^4 + 5x^3 - 10x^2 + 12x - 8.$$

The hyperelliptic involution ι equals the Atkin–Lehner involution w_{11} and is induced by the matrix $\gamma = \left(\begin{smallmatrix} 11 & 5 \\ 22 & 11 \end{smallmatrix}\right)$. We fix the differential

$$\alpha = \frac{\mathrm{d}x}{(x-2)(2y-x^3)}.$$

Then we have

$$\mathbb{E}_2^{(11)} = -\frac{5x^3 + 2x^2 + 12x + 8}{12} f_\alpha.$$

Furthermore,

$$\mathbb{E}_4 = g_4 f_\alpha^2 \quad \text{and} \quad \mathbb{E}_6 = g_6 f_\alpha^3,$$

where g_4 and g_6 are the rational functions defined by

$$\begin{aligned} 240 g_4 &= 120(-x^3 + 6x^2 + 4x + 8)y \\ &\qquad + 121x^6 - 484x^5 + 604x^4 - 352x^3 - 400x^2 + 2496x - 2240, \\ -504 g_6 &= 36(-37x^6 + 236x^5 - 140x^4 + 1520x^3 + 368x^2 + 1408x - 448)y \\ &\qquad + 1331x^9 - 7986x^8 + 17304x^7 - 9832x^6 - 49632x^5 \\ &\qquad + 148704x^4 - 174720x^3 + 131712x^2 + 16128x - 179200. \end{aligned}$$

We consider the points with $x = -1$. These are defined over the quadratic field K of discriminant -143, and the points are $P = (-1, \beta)$ and $\iota(P) = {}^\sigma P = (-1, -1-\beta)$, where $\beta^2+\beta+36 = 0$. One of the elliptic curves in the family (consisting of quadratic twists) corresponding to the point P is

$$E\colon y^2 + xy + (1+\beta)y = x^3 - \frac{1}{2}x^2 + (74 - 28\beta)x + \frac{637 - 281\beta}{2}.$$

(The class number of K is 10, and E does not admit a global minimal model.) The element $\mu \in K^\times$ happens to be 1, so E and $({}^\sigma E)^{(-11)}$, with σ the non-trivial automorphism of K, are related by an 11-isogeny. Furthermore, if $C \subset E$ is the canonical cyclic subgroup of order 22 and ω is the standard differential, the modular form A_γ takes the value $-77/6$ on (E, C, ω). Using Elkies's algorithm, one computes that the kernel C_γ of this 11-isogeny is defined by the polynomial

$$\begin{aligned} P_{C_\gamma} &= x^5 + 6x^4 + (285 + 33\beta)x^3 - (1110 + 759\beta)x^2 \\ &\qquad + (40298 - 12496\beta)x - (13223 + 38324\beta). \end{aligned}$$

Using known algorithms, one can compute the rational functions defining the isogeny, but we will not write these down.

Finally, we note that both E and its quadratic twist by -11 have rank 0; this can be shown by a 2-descent. This implies that E has rank 0 over $L = K(\sqrt{-11})$, which is consistent with Theorem 12.

6. Exceptional points

6.1. **Notation.** In our tables, $\mathbb{Q}(\sqrt{d})$ is the field of definition of the exceptional elliptic curve, and w denotes $\sqrt{d}$. The coordinates denote the quadratic points on the given model of $X_0(n)$ that are not in $\phi^{-1}\{0\}(\mathbb{Q})$ in the notation of Section 2. The "CM" column indicates whether the corresponding elliptic curves have complex multiplication; an entry $-D$ means that they have complex multiplication by the imaginary quadratic order of discriminant $-D$.

As we are interested in the moduli interpretation of all the quadratic points on $X_0(n)$, it makes sense to determine the isogeny diagrams corresponding to the exceptional points. In our diagrams, the vertices are the points P on $X_0(n)$ instead of the corresponding elliptic curves with an n-isogeny. We use this notation as the points P take considerably less space to write down. We do not write down the functions that for a given point on $X_0(n)$ construct an elliptic curve with an n-isogeny; these functions are implemented in Magma.

Let P_1, P_2 be points on $X_0(n)$ forming an isogeny class whose isogeny diagram is of the form

$$P_1 \overset{n}{\text{———}} P_2.$$

In this case, we say that the isogeny diagram is *simple* and denote it by $\mathrm{S}(P_1, P_2, n)$.

Let P_1, P_2, P_3, P_4 be points on $X_0(n)$ forming an isogeny class whose isogeny diagram is of the form

$$\begin{tikzcd} P_1 \arrow[r, dash, "a"] \arrow[d, dash, "b"] & P_2 \arrow[d, dash, "b"] \\ P_3 \arrow[r, dash, "a"] & P_4 \end{tikzcd}$$

where the degrees a and b of the isogenies satisfy $ab = n$. In this case, we say that the isogeny diagram is a *square* and denote it by $\mathrm{SQ}(P_1, P_2, P_3, P_4, a, b)$.

For completeness, we give data on the modular curves $X_0(n)$ for all n in our list, even though some of them do not have exceptional points.

Table 1. $X_0(22)$

Model: $y^2 + (-x^3)y = -x^4 + 5x^3 - 10x^2 + 12x - 8$
Genus: 2
Hyperelliptic involution: w_{11}
Group structure: $J_0(22)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-7	$\left(\frac{1}{2}(w-1), \frac{1}{2}(w+11)\right)$	no
P_2	-7	$\left(\frac{1}{2}(w-1), -w-3\right)$	no
P_3	-7	$\left(\frac{1}{4}(-w+3), \frac{1}{16}(7w-13)\right)$	no
P_4	-7	$\left(\frac{1}{4}(-w+3), \frac{1}{4}(-3w+1)\right)$	no
P_5	-7	$\left(\frac{1}{2}(-w+1), \frac{1}{2}(w-5)\right)$	-7
P_6	-7	$\left(\frac{1}{2}(-w+1), 0\right)$	-7
P_7	33	$\left(\frac{1}{2}(-w-3), \frac{1}{2}(-3w-13)\right)$	no
P_8	33	$\left(\frac{1}{2}(-w-3), -6w-34\right)$	no
P_9	-47	$\left(\frac{1}{4}(w+1), \frac{1}{16}(-7w+1)\right)$	no
P_{10}	-47	$\left(\frac{1}{4}(w+1), \frac{1}{4}(-w-9)\right)$	no
P_{11}	-47	$\left(\frac{1}{6}(-w+5), \frac{1}{27}(w-41)\right)$	no
P_{12}	-47	$\left(\frac{1}{6}(-w+5), \frac{1}{6}(-w-7)\right)$	no
P_{13}	-2	$(w+1, -1)$	no
P_{14}	-2	$(w+1, w-4)$	no
P_{15}	-2	$\left(\frac{2}{3}(-2w+1), \frac{8}{3}(w-2)\right)$	no
P_{16}	-2	$\left(\frac{2}{3}(-2w+1), \frac{8}{27}(w-5)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

$\mathrm{SQ}(P_1, P_2, P_3, P_4, 11, 2)$, $\mathrm{SQ}(P_7, {}^\sigma P_7, P_8, {}^\sigma P_8, 11, 2)$, $\mathrm{SQ}(P_9, P_{10}, P_{11}, P_{12}, 11, 2)$, $\mathrm{SQ}(P_{13}, P_{14}, P_{15}, P_{16}, 11, 2)$.

Remark 17. The points P_7 and ${}^\sigma P_7$ are lifts of a $\mathbb{Q}$-point on $X_0(22)/w_2$, as are P_8 and ${}^\sigma P_8$.

Table 2. $X_0(23)$

Model: $y^2 + (-x^3 - x - 1)y = -2x^5 - 3x^2 + 2x - 2$
Genus: 2
Hyperelliptic involution: w_{23}
Group structure: $J_0(23)(\mathbb{Q}) \simeq \mathbb{Z}/11\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-5	$\left(\frac{1}{3}(2w-2), \frac{1}{9}(8w+70)\right)$	no
P_2	-5	$\left(\frac{1}{3}(2w-2), \frac{1}{27}(-22w-89)\right)$	no
P_3	-7	$\left(\frac{1}{4}(-w+3), \frac{1}{4}(-w-1)\right)$	no
P_4	-7	$\left(\frac{1}{4}(-w+3), \frac{1}{16}(-5w+23)\right)$	no
P_5	-11	$\left(\frac{1}{6}(-w+1), \frac{1}{54}(-19w+49)\right)$	no
P_6	-11	$\left(\frac{1}{6}(-w+1), \frac{1}{9}(2w+1)\right)$	no
P_7	-15	$\left(\frac{1}{4}(w+1), \frac{1}{16}(-3w+5)\right)$	no
P_8	-15	$\left(\frac{1}{4}(w+1), \frac{1}{4}(w+1)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

$\mathrm{S}(P_1, P_2, 23)$, $\mathrm{S}(P_3, P_4, 23)$, $\mathrm{S}(P_5, P_6, 23)$, $\mathrm{S}(P_7, P_8, 23)$.

Table 3. $X_0(26)$

Model: $y^2 + (-x^3 - 1)y = -2x^5 + 2x^4 - 5x^3 + 2x^2 - 2x$
Genus: 2
Hyperelliptic involution: w_{26}
Group structure: $J_0(26)(\mathbb{Q}) \simeq \mathbb{Z}/21\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-3	$\left(\frac{1}{2}(w+1), -1\right)$	-3
P_2	-3	$\left(\frac{1}{2}(w+1), 1\right)$	-12
P_3	-11	$\left(\frac{1}{2}(w-1), 7\right)$	no
P_4	-11	$\left(\frac{1}{6}(-w-1), \frac{1}{27}(7w+28)\right)$	no
P_5	-11	$\left(\frac{1}{6}(-w-1), \frac{1}{9}(-2w+1)\right)$	no
P_6	-11	$\left(\frac{1}{2}(w-1), -w-2\right)$	no
P_7	-23	$\left(\frac{1}{6}(-w+1), \frac{1}{27}(w+2)\right)$	no
P_8	-23	$\left(\frac{1}{4}(w+1), \frac{1}{16}(-w+3)\right)$	no
P_9	-23	$\left(\frac{1}{4}(w+1), \frac{1}{4}(-w-1)\right)$	no
P_{10}	-23	$\left(\frac{1}{6}(-w+1), \frac{1}{18}(w+11)\right)$	no
P_{11}	-1	$(w, 1)$	-4
P_{12}	-1	$(w, -w)$	-16

Isogeny diagrams of non-CM points, up to conjugation:

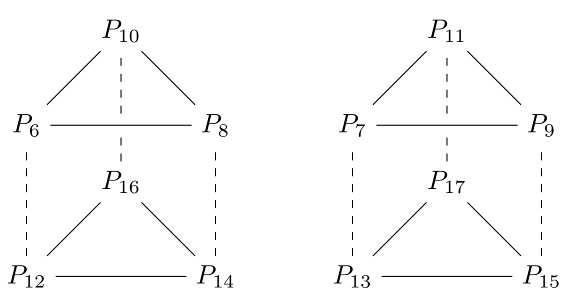
$\mathrm{SQ}(P_3, P_4, P_5, P_6, 2, 13)$, $\mathrm{SQ}(P_7, P_8, P_9, P_{10}, 2, 13)$.

TABLE 4. $X_0(28)$

Model: $y^2 + (-2x^3 + 3x^2 - 3x)y = x^4 - 3x^3 + 4x^2 - 3x + 1$
Genus: 2
Hyperelliptic involution: w_7
Group structure: $J_0(28)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-3	$\left(\frac{1}{2}(w+1), 0\right)$	-12
P_2	-3	$\left(\frac{1}{2}(w+1), 1\right)$	-12
P_3	-7	$\left(\frac{1}{2}(-w+1), \frac{1}{2}(w+1)\right)$	-7
P_4	-7	$\left(\frac{1}{4}(w+1), \frac{1}{8}(w+5)\right)$	-7
P_5	-7	$\left(\frac{1}{4}(-w+3), \frac{1}{8}(-w+3)\right)$	-28
P_6	-23	$\left(\frac{1}{4}(w+1), \frac{1}{8}(-w+19)\right)$	no
P_7	-23	$\left(\frac{1}{6}(-w+1), \frac{1}{54}(w+29)\right)$	no
P_8	-23	$\left(\frac{1}{8}(-w+5), \frac{1}{64}(-3w+7)\right)$	no
P_9	-23	$\left(\frac{1}{6}(w+5), \frac{1}{54}(-w+25)\right)$	no
P_{10}	-23	$\left(\frac{1}{4}(-w+3), \frac{1}{8}(w-11)\right)$	no
P_{11}	-23	$\left(\frac{1}{8}(w+3), \frac{1}{64}(3w+57)\right)$	no
P_{12}	-23	$\left(\frac{1}{4}(w+1), \frac{1}{8}(-w+3)\right)$	no
P_{13}	-23	$\left(\frac{1}{6}(-w+1), \frac{1}{6}(-w+7)\right)$	no
P_{14}	-23	$\left(\frac{1}{8}(-w+5), \frac{1}{16}(-w+13)\right)$	no
P_{15}	-23	$\left(\frac{1}{6}(w+5), \frac{1}{6}(w-1)\right)$	no
P_{16}	-23	$\left(\frac{1}{8}(w+3), \frac{1}{16}(w+3)\right)$	no
P_{17}	-23	$\left(\frac{1}{4}(-w+3), \frac{1}{8}(w+5)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:



In these diagrams the dashed lines represent 7-isogenies, while the full lines represent 4-isogenies.

TABLE 5. $X_0(29)$

Model: $y^2 + (-x^3 - 1)y = -x^5 - 3x^4 + 2x^2 + 2x - 2$
Genus: 2
Hyperelliptic involution: w_{29}
Group structure: $J_0(29)(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-1	$(w-1, 2w+4)$	no
P_2	-1	$(w-1, -1)$	no
P_3	-7	$\left(\frac{1}{4}(w+1), \frac{1}{16}(-11w-7)\right)$	no
P_4	-7	$\left(\frac{1}{4}(w+1), \frac{1}{8}(5w+9)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

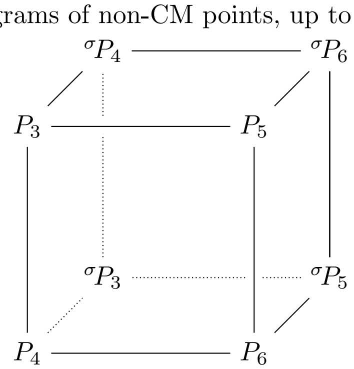
$\mathrm{S}(P_1, P_2, 29)$, $\mathrm{S}(P_3, P_4, 29)$.

Table 6. $X_0(30)$

Model:
$y^2 + (-x^4 - x^3 - x^2)y = 3x^7 + 19x^6 + 60x^5 + 110x^4 + 121x^3 + 79x^2 + 28x + 4$
Genus: 3
Hyperelliptic involution: w_{15}
Group structure: $J_0(30)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	5	$(-w-3, 71w+159)$	-15
P_2	5	$\left(\frac{1}{2}(-w-3), 4w+9\right)$	-60
P_3	-7	$\left(\frac{1}{2}(-w-3), w-3\right)$	no
P_4	-7	$\left(\frac{1}{4}(w-3), \frac{1}{32}(5w+9)\right)$	no
P_5	-7	$\left(\frac{1}{4}(-w-3), \frac{1}{16}(5w-9)\right)$	no
P_6	-7	$\left(\frac{1}{2}(w-3), \frac{1}{2}(w-15)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:



In this diagram, the horizontal lines are 5-isogenies, the vertical lines 2-isogenies and the diagonal lines 3-isogenies.

Remark 18. All the curves in the diagram are $\mathbb{Q}$-curves and are 6-isogenous to their Galois conjugates and arise from rational points on the curve $X_0(30)/w_6$.

TABLE 7. $X_0(31)$

Model: $y^2 + (-x^3 - x - 1)y = -2x^5 + x^4 + 4x^3 - 3x^2 - 4x - 1$
Genus: 2
Hyperelliptic involution: w_{31}
Group structure: $J_0(31)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-3	$\left(\frac{1}{2}(w-1), -2\right)$	no
P_2	-3	$\left(\frac{1}{2}(w-1), \frac{1}{2}(w+7)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

$\mathrm{S}(P_1, P_2, 31)$.

TABLE 8. $X_0(33)$

Model: $y^2 + (-x^4 - x^2 - 1)y = 2x^6 - 2x^5 + 11x^4 - 10x^3 + 20x^2 - 11x + 8$
Genus: 3
Hyperelliptic involution: w_{11}
Group structure: $J_0(33)(\mathbb{Q}) \simeq \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-2	$\left(-\frac{1}{2}w, \frac{1}{4}(-4w-5)\right)$	no
P_2	-2	$(w-1, -5w-5)$	no
P_3	-2	$\left(-\frac{1}{2}w, w+2\right)$	no
P_4	-2	$(w-1, 7w-2)$	no
P_5	-2	$(w, -w+1)$	-8
P_6	-2	$(w, w+2)$	-8
P_7	-7	$\left(\frac{1}{4}(-3w+1), \frac{1}{32}(9w+93)\right)$	no
P_8	-7	$\left(\frac{1}{2}(w+1), -1\right)$	no
P_9	-7	$\left(\frac{1}{4}(-3w+1), \frac{1}{4}(9w+33)\right)$	no
P_{10}	-7	$\left(\frac{1}{2}(w+1), -w+1\right)$	no
P_{11}	-11	$\left(\frac{1}{2}(-w+1), w+1\right)$	-11

Isogeny diagrams of non-CM points, up to conjugation:

$\mathrm{SQ}(P_1, P_2, P_3, P_4, 3, 11)$, $\mathrm{SQ}(P_7, P_8, P_9, P_{10}, 3, 11)$.

Table 9. $X_0(35)$

Model: $y^2 + (-x^4 - x^2 - 1)y = -x^7 - 2x^6 - x^5 - 3x^4 + x^3 - 2x^2 + x$
Genus: 3
Hyperelliptic involution: w_{35}
Group structure: $J_0(35)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	5	$\left(\frac{1}{2}(-w-1), w+3\right)$	-35

Isogeny diagrams of non-CM points, up to conjugation:

Table 10. $X_0(39)$

Model: $y^2 + (-x^4 - x^3 - x^2 - x - 1)y = -2x^7 + 2x^5 - 7x^4 + 2x^3 - 2x$
Genus: 3
Hyperelliptic involution: w_{39}
Group structure: $J_0(39)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-3	$\left(\frac{1}{2}(-w+1), \frac{1}{2}(-w+1)\right)$	-3
P_2	-3	$\left(\frac{1}{2}(-w+1), -1\right)$	-27
P_3	-7	$\left(\frac{1}{4}(-w+3), \frac{1}{3}2(-21w+7)\right)$	no
P_4	-7	$\left(\frac{1}{4}(w+3), \frac{1}{8}(3w+1)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

$$\mathrm{SQ}(P_3, {}^{\sigma}P_3, P_4, {}^{\sigma}P_4, 3, 13).$$

Remark 19. The points P_3 and ${}^{\sigma}P_3$ are lifts of a $\mathbb{Q}$-point on $X_0(39)/w_3$, as are P_4 and ${}^{\sigma}P_4$.

Table 11. $X_0(40)$

Model: $y^2 + (-x^4 - 1)y = 2x^6 - x^4 + 2x^2$
Genus: 3
Hyperelliptic involution: induced by $\beta_{40} = \left(\begin{smallmatrix} -10 & 1 \\ -120 & 10 \end{smallmatrix}\right)$
Group structure: $J_0(40)(\mathbb{Q}) \simeq \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-1	$(w, 2w+1)$	-16
P_2	-1	$(w, -2w+1)$	-16

Isogeny diagrams of non-CM points, up to conjugation:

Table 12. $X_0(41)$

Model: $y^2 + (-x^4 - x)y = -x^7 - 2x^6 + 2x^5 + 5x^4 + 2x^3 - 4x^2 - 5x - 2$
Genus: 3
Hyperelliptic involution: w_{41}
Group structure: $J_0(41)(\mathbb{Q}) \simeq \mathbb{Z}/10\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-1	$\left(\frac{1}{2}(-w-1), \frac{1}{4}(-3w-4)\right)$	no
P_2	-1	$\left(\frac{1}{2}(-w-1), \frac{1}{4}(w+1)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

$$\mathrm{S}(P_1, P_2, 41).$$

Table 13. $X_0(46)$

Model:

$$y^2 + (-x^6 - x^5 - x^3 - 1)y = -x^{11} + x^{10} + x^9 - 7x^8 + 21x^7 - 29x^6 + 33x^5 - 16x^4 + 6x^3 + 3x^2 + 2x - 2$$

Genus: 5
Hyperelliptic involution: w_{23}
Group structure:

$$J_0(46)(\mathbb{Q}) \simeq \mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$$

Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-7	$\left(\frac{1}{2}(w+1), w+3\right)$	-7
P_2	-7	$\left(\frac{1}{2}(w+1), \frac{1}{2}(w+11)\right)$	-7

Isogeny diagrams of non-CM points, up to conjugation:

Table 14. $X_0(47)$

Model:
$y^2+(-x^5-x^4-x^3-x^2-1)y = -2x^9+2x^8-7x^7+4x^6-5x^5-4x^4+7x^3-10x^2+7x-3$
Genus: 4
Hyperelliptic involution: w_{47}
Group structure: $J_0(47)(\mathbb{Q}) \simeq \mathbb{Z}/23\mathbb{Z}$
No exceptional points.

TABLE 15. $X_0(48)$

Model: $y^2 = x^8 + 14x^4 + 1$
Genus: 3
Hyperelliptic involution: induced by $\beta_{48} = \left(\begin{smallmatrix} -6 & 1 \\ -48 & 6 \end{smallmatrix}\right)$
Group structure: $J_0(48)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-1	$(w, 4)$	-16
P_2	-1	$(w, -4)$	-16

Isogeny diagrams of non-CM points, up to conjugation:

TABLE 16. $X_0(50)$

Model: $y^2 + (-x^3 - 1)y = -x^5 - 3x^3 - x$
Genus: 2
Hyperelliptic involution: w_{50}
Group structure: $J_0(50)(\mathbb{Q}) \simeq \mathbb{Z}/15\mathbb{Z}$
Exceptional conjugacy classes of points:

Name	d	Coordinates	CM
P_1	-1	$(w, -w)$	-4
P_2	-1	$(w, 1)$	-16
P_3	-7	$\left(\frac{1}{2}(w-1), 3\right)$	no
P_4	-7	$\left(\frac{1}{4}(-w-1), \frac{1}{16}(3w+15)\right)$	no
P_5	-7	$\left(\frac{1}{4}(-w-1), \frac{1}{8}(-w+3)\right)$	no
P_6	-7	$\left(\frac{1}{2}(w-1), \frac{1}{2}(-w+1)\right)$	no

Isogeny diagrams of non-CM points, up to conjugation:

$$\mathrm{SQ}(P_3, P_4, P_5, P_6, 2, 25)$$

TABLE 17. $X_0(59)$

Model:
$y^2 + (-x^6 - x^4 - x^2)y = -2x^{11} + 5x^{10} - 7x^9 + 10x^7 - 16x^6 + 10x^5 - x^4 - 6x^3 + 5x^2 - x - 2$
Genus: 5
Hyperelliptic involution: w_{59}
Group structure: $J_0(59)(\mathbb{Q}) \simeq \mathbb{Z}/29\mathbb{Z}$
No exceptional points.

Table 18. $X_0(71)$

Model:

$$y^2 + (-x^7 - x^5 - x^4 - x^3 - 1)y = x^{13} - x^{12} - 10x^{11} - 20x^{10} - 7x^9 + 27x^8 + 36x^7 - 31x^5 - 18x^4 + 7x^3 + 10x^2 + x - 3$$

Genus: 6
Hyperelliptic involution: w_{71}
Group structure: $J_0(71)(\mathbb{Q}) \simeq \mathbb{Z}/35\mathbb{Z}$
No exceptional points.

References

[1] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[2] J. Bober, A. Deines, A. Klages-Mundt, B. LeVeque, R. A. Ohana, A. Rabindranath, P. Sharaba, W. Stein, *A Database of Elliptic Curves over* $\mathbb{Q}(\sqrt{5})$*—First Report*, Proceedings of the Tenth Algorithmic Number Theory Symposium, ed. by E. W. Howe and K. S. Kedlaya (2012)

[3] F. Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), 154–165.

[4] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.19 (2013).

[5] J. G. Bosman, P. J. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN **2014** (2014), 2885–2923.

[6] P. J. Bruin and F. Najman, *The growth of the rank of Abelian varieties upon extensions*, Ramanujan J., electronically published on 5 December 2014.

[7] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), 21–76, AMS/IP Stud. Adv. Math., **7**, Amer. Math. Soc., Providence, RI, 1998.

[8] S. D. Galbraith, Equations for modular curves, D. Sc. thesis, University of Oxford, 1996.

[9] J. Gonzàlez Rovira, Equations of hyperelliptic modular curves, Annales de l'institut Fourier **41** (1991), 779–795.

[10] J. González, *Isogenies of polyquadratic* $\mathbb{Q}$*-curves to their Galois conjugates*, Arch. Math. **77** (2001), 383–390.

[11] D. Jeon, C. H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), 291–301.

[12] D. Jeon, C.H. Kim, E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12.

[13] S. Kamienny, *Torsion points on elliptic curves and* q*-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.

[14] N. M. Katz, p*-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Antwerp, 1972), 69–190, Lecture Notes in Math., **350**, Springer, Berlin, 1973.

[15] M. A. Kenku, *The modular curve* $X_0(39)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23.

[16] M. A. Kenku, *The modular curves* $X_0(65)$ *and* $X_0(91)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

[17] M. A. Kenku, *The modular curve* $X_0(169)$ *and rational isogeny* J. London Math. Soc. (2) **22** (1980), 239–244.

[18] M. A. Kenku, *On the modular curves* $X_0(125)$*,* $X_1(25)$ *and* $X_1(49)$, J. London Math. Soc. (2) **23** (1981), 415–427.

[19] M. Kenku, *On the number of* Q*-isomorphism classes of elliptic curves in each* Q*-isogeny class*, J. Number Theory **15** (1982), 199–202.

[20] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[21] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186.

[22] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[23] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

[24] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Lett. **23** (2016), 245–272.

[25] A. P. Ogg, *Hyperelliptic Modular Curves*, Bull. Soc. Math. France, **102** (1974), 449–462.

[26] W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).

[27] M. Stoll, *Implementing* 2*-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.

[28] J. Vélu, *Isogénies entre courbes elliptiques*, Comptes Rendus Acad. Sci. Paris A **273** (1971), 238–241.

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

Current address: Universiteit Leiden, Mathematisch Instituut, Postbus 9512, 2300 RA Leiden, Netherlands

Email address: `P.J.Bruin@math.leidenuniv.nl`

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

Email address: `fnajman@math.hr`