Equations and Rational Points of the Modular Curves $X_0^+(p)$

Pietro Mercuri

Abstract

Let $p$ be an odd prime number and let $X_0^+(p)$ be the quotient of the classical modular curve $X_0(p)$ by the action of the Atkin-Lehner operator $w_p$. In this paper we show how to compute explicit equations for the canonical model of $X_0^+(p)$. Then we show how to compute the modular parametrization, when it exists, from $X_0^+(p)$ to an isogeny factor $E$ of dimension 1 of its jacobian $J_0^+(p)$. Finally we show how use this map to determine the rational points on $X_0^+(p)$ up to a large fixed height.

1 Introduction

The classical problem to determine the rational points of the modular curve $X_0(p)$, when $p$ is a prime number, has been solved by Mazur in his paper [Maz76] in 1975. In his work, Mazur proved, for $p > 37$, that the only rational points of the curve $X_0(p)$ are cusps and CM points. In the same paper Mazur also refers to the interesting case of the modular curve $X_0^+(p)$. This curve is the quotient of $X_0(p)$ by the Atkin-Lehner involution $w_p$. See Galbraith [Gal99, Section 2]. For these curves a similar result is expected: for sufficiently large $p$ the only rational points of the curve $X_0^+(p)$ are cusps and CM points.

The genus $g$ of $X_0^+(p)$ growth with $p$, so for a fixed $g$ we have only finitely many curves. The cases $g$ equal to 0 or 1 are well known. If $g$ is equal to 0, then $X_0^+(p)$ is isomorphic to $\mathbb{P}^1$ and there are infinitely many rational points. If $g$ is equal to 1, then $X_0^+(p)$ is an elliptic curve whose Mordell-Weil group is torsion-free and has rank 1. Let us focus on the case $g > 1$. Galbraith in his papers [Gal96] and [Gal99] describes a method to find explicit equations for the curves $X_0^+(p)$. If $X_0^+(p)$ is hyperelliptic he uses an ad hoc technique. We recall that by [HH96] that the curve $X_0^+(p)$ is hyperelliptic if and only if $g = 2$. If $X_0^+(p)$ is not hyperelliptic, Galbraith uses the canonical embedding $\varphi: X_0^+(p) \hookrightarrow \mathbb{P}^{g-1}$ to find equations for the curves. He finds explicit equations for all curves $X_0^+(p)$ with $g \leq 5$. Here we present the following result.

Result 1.1. We use the method of Galbraith to find explicit equations for the canonical model of all the modular curves $X_0^+(p)$ with genus $g = 6$ or 7.
Equations for the thirteen curves of genus 6 or 7 are listed in Section 6. The equations that we find have very small coefficients and have good reduction for each prime number $\ell \neq p$.

The technique used here play an important role in [Mer15] in finding explicit equations defining the modular curves $X^+_n(p)$. These curves are the modular curves associated to the normalizer of a nonsplit Cartan subgroup of the general linear group over a finite field with $p$ elements. Few is still known about them and they are harder to study with respect to modular curves $X^+_0(p)$ considered here.

Galbraith uses the equations of the curves $X^+_0(p)$ to look for rational points $P$ up to some bounds on the naive projective height $H$. See Silverman [Sil86, Chapter VIII, Section 5] for more details about the naive height on projective space. Using a projection onto a plane model, possibly singular, we check that if $X^+_0(p)$ has genus $g = 6$ or $7$, then it has no rational points $P$, except the cusps and the CM points, for which $H(P) \leq 10^4$. When the jacobian variety $J^+_0(p)$ of $X^+_0(p)$ has an isogeny factor over $\mathbb{Q}$ of dimension 1, we improve this bound significantly. In particular we prove the following result.

**Result 1.2.** For the primes $p = 163, 197, 229, 269$ and $359$, the only rational points $P$ on $X^+_0(p)$ of naive height $H(P) \leq 10^{10000}$ are cusps or CM points.

## 2 The method to get explicit equations

In this section we show how to get explicit equations of the canonical model for modular curves. The final output is a list of quadrics with very small integer coefficients.

Let $\Gamma$ be a congruence subgroup of $\text{SL}_2(\mathbb{Z})$, let $S_2(\Gamma)$ be the $\mathbb{C}$-vector space of the cusp forms of weight 2 with respect to $\Gamma$, and let $f_1, \ldots, f_g$ be a $\mathbb{C}$-basis of $S_2(\Gamma)$ where $g$ is the genus of the modular curve $X(\Gamma)$. If $g > 2$, we use the canonical embedding to get the canonical model for $X(\Gamma)$. We know that $X(\Gamma)$ is isomorphic as compact Riemann surfaces to $\Gamma \backslash \mathcal{H}^*$, where $\mathcal{H}^*$ is the extended complex upper half plane. We also know that $S_2(\Gamma)$ is isomorphic to the $\mathbb{C}$-vector space of holomorphic differentials $\Omega^1(X(\Gamma))$ with respect to the map $f(\tau) \mapsto f(\tau)d\tau$. See Diamond and Shurman [DS05] for more details about these results. Using these isomorphisms, the canonical embedding can be expressed in the following way

$$\varphi: X(\Gamma) \rightarrow \mathbb{P}^{g-1}(\mathbb{C})$$

$$\Gamma \tau \mapsto (f_1(\tau): \ldots: f_g(\tau)),$$

where $\tau \in \mathcal{H}^*$. The Enriques-Petri Theorem (see Griffith, Harris [GH78], Chapter 4, Section 3, pag. 535) states that the canonical model of a complete nonsingular non-hypereelliptic curve is entirely cut out by quadrics and cubics. Moreover, it is cut out by quadrics if it is neither trigonal, nor a quintic plane curve with genus exactly 6.

When $X(\Gamma)$ can be defined over $\mathbb{Q}$, we can look for equations defined over $\mathbb{Q}$. The Enriques-Petri Theorem is proved over algebraically closed fields, but its proof
can be suitable modified to work over \( \mathbb{Q} \). Alternatively, if we find equations defined over \( \mathbb{Q} \), then we can check by MAGMA that their zero locus \( Z \) is an algebraic curve with the same genus as \( X(\Gamma) \). An application of the Hurwitz genus formula for genus \( g > 1 \), to the morphism \( \varphi: X(\Gamma) \to Z \) implies that \( \varphi \) is an isomorphism.

Finding equations for \( Z \) is equivalent to finding generators of the homogeneous ideal \( I \) defining it in \( \mathbb{P}^{e-1} \). Let \( I_d \) be the set of homogeneous elements of \( I \) of degree exactly \( d \). We explain how to find generators of \( I \) that belong to \( I_d \) for a fixed \( d \). By the Enriques-Petri Theorem and by Hasegawa and Hashimoto [HH96], we know that if \( g > 2 \), the ideal \( I \) is generated by elements in \( I_d \) for \( d = 2, 3 \). Now, we fix the degree \( d \) and we suppose that we know the first \( m \) Fourier coefficients of the \( \varphi \)-expansions of a basis \( \mathcal{B} = \{ f_1, \ldots, f_g \} \) of \( \Omega^1(X(\Gamma)) \), where \( m > d(2g - 2) \). This condition on \( m \) guarantees that if we have a polynomial \( F \) with rational coefficients and \( g \) unknowns such that \( F(f_1, \ldots, f_g) \equiv 0 \) (mod \( q^{m+1} \)), then \( F(f_1, \ldots, f_g) = 0 \). See [BGGP05] Section 2.1, Lemma 2.2, pag 1329] for more details. We also assume that the Fourier coefficients of the basis \( \mathcal{B} \) are algebraic integers.

There is a number field \( K \), of degree \( D \) over \( \mathbb{Q} \), which contains all the coefficients of all the elements of \( \mathcal{B} \). Moreover, if the Fourier coefficients are algebraic integers, they have integer coordinates with respect to a suitable chosen basis of \( K \) over \( \mathbb{Q} \). If \( a_n(f_i) \) is the \( n \)-th Fourier coefficient of \( f_i \), we denote the \( k \)-th coordinate of \( a_n(f_i) \) in \( K \) by \( c(i, n, k) \in \mathbb{Z} \), where \( k = 1, \ldots, D \). We can associate to \( \mathcal{B} \) a matrix \( M \) whose integer entries are the coordinates of the Fourier coefficients where each row \( i \) corresponds to an element \( f_i \) of \( \mathcal{B} \). An explicit way to set the entries of \( M = (u_{ij}) \) is to choose \( u_{ij} = c(i, n, k) \), where \( j = (n - 1)D + k \), for \( i = 1, \ldots, g \), \( n = 1, \ldots, m \) and for \( k = 1, \ldots, D \). The matrix \( M \) has \( g \) rows and \( mD \) columns, where \( m \) is the number of the first Fourier coefficients used and \( g \) is the cardinality of the basis. Since \( m > d(2g - 2) \) and \( g > 0 \), we always have \( m \geq g \), hence the rank of \( M \) is \( g \). To find equations defining \( X(\Gamma) \) we compute all the monomials \( F_j \) of degree \( d \) where the indeterminates are the elements of \( \mathcal{B} \). The elements of a \( \mathbb{Z} \)-basis of the space \( S \) of the solutions of the homogeneous linear system in the unknowns \( F_j \) are the coefficients of the desired equations.

We are interested in reducing the size of the coefficients of these equations and minimizing the number of primes \( \ell \) such that the model has bad reduction modulo \( \ell \). To reduce the size of the coefficients, we apply the LLL-algorithm first to \( M \) and then to the \( \mathbb{Z} \)-basis of \( S \). We know that if the rank of \( M \) modulo \( \ell \) is less than \( g \), then the canonical model of the curve that we find, is singular modulo \( \ell \). We say that \( M \) is optimal, if the rank of \( M \) modulo \( \ell \) is exactly \( g \) for each prime \( \ell \). In Algorithm 2.2 below, within a more general setting, we describe how to modify \( \mathcal{B} \) to make \( M \) optimal.

Now, we describe how to find the primes \( \ell \) such that the canonical model has bad reduction. Let \( I_{\text{Jac}} \) be the ideal generated by the polynomials defining the curve and by all the determinants of order \( g - 2 \) of the jacobian matrix of the curve. We compute the elimination ideals \( J_i := I_{\text{Jac}} \cap \mathbb{Q}[x_i] \), for \( i = 1, \ldots, g \). If \( J_i \neq 0 \), it turns out to be generated by \( \lambda x_i^n \) with \( \lambda, n \in \mathbb{Z}_{>0} \). The curve has bad reduction modulo any prime \( \ell \) such that \( \ell \mid \lambda \).
2.1 Algorithm

Let \( g \) and \( m \) be positive integers such that \( g \leq m \) and let \( v_1, \ldots, v_g \in \mathbb{Z}^m \) be linearly independent vectors over \( \mathbb{Q} \). We describe a method to find a basis over \( \mathbb{Z} \) of the lattice \( L := \text{span}_{\mathbb{Q}}[v_1, \ldots, v_g] \cap \mathbb{Z}^m \). Let \( L' := \text{span}_{\mathbb{Z}}[v_1, \ldots, v_g] \), so \( L' \) is a subgroup of \( L \), and let \( J := [L : L'] \). We want to modify \( L' \) and its basis until we have \( J = 1 \) and so \( L' = L \).

**Lemma 2.1.** Let the notation as above and let \( p \) be a prime number. We have that \( v_1, \ldots, v_g \) are linearly dependent in \( \mathbb{Z}^m / p\mathbb{Z}^m \) if and only if \( p \mid [L : L'] \).

**Proof.** We have that \( p \mid [L : L'] = \#(L/L') \) if and only if there is an element of \( L/L' \) of order exactly \( p \). This is equivalent to have an element \( v \in L \setminus L' \) such that \( pv \in L' \). The condition \( v \in L \) implies that there are \( \alpha_1, \ldots, \alpha_g \in \mathbb{Q} \) such that \( v = \alpha_1 v_1 + \ldots + \alpha_g v_g \). The condition \( pv \in L' \) implies that \( p\alpha_1, \ldots, p\alpha_g \) are integers. The independence over \( \mathbb{Q} \) implies that \( p\alpha_1, \ldots, p\alpha_g \) are not all zero. Finally, the condition \( v \notin L' \) implies that \( p\alpha_1, \ldots, p\alpha_g \) are not all zero modulo \( p \). \( \square \)

Let \( M \in \mathbb{Z}^{m \times g} \) be the matrix whose columns are the vectors \( v_1, \ldots, v_g \). It follows from Lemma 2.1 above that if a prime \( p \) divides the index \( J \), then \( p \) divides the determinant \( \Delta \) of any \( g \times g \) submatrix of \( M \).

**Algorithm 2.2.**

**Step 0** Choose a \( g \times g \) submatrix of \( M \) with nonzero determinant \( \Delta \).

Set \( \mathcal{P} := \{ \text{prime numbers dividing } \Delta \} \). Go to Step 1.

**Step 1** If \( \mathcal{P} = \emptyset \) the algorithm terminates. If \( \mathcal{P} \neq \emptyset \) go to Step 2.

**Step 2** Let \( p \in \mathcal{P} \). If \( v_1, \ldots, v_g \) are linearly dependent in \( \mathbb{Z}^m / p\mathbb{Z}^m \), we have that \( p \mid J \), and go to Step 3. Else set \( \mathcal{P} := \mathcal{P} \setminus \{ p \} \) and go to Step 1.

**Step 3** If \( v_1, \ldots, v_g \) are linearly dependent in \( \mathbb{Z}^m / p\mathbb{Z}^m \), up to reordering the \( v_i \)'s, there are, \( \alpha_1, \ldots, \alpha_g \in \mathbb{Z} \) such that \( v_1 + \alpha_2 v_2 + \ldots + \alpha_g v_g = pv \). We replace \( v_1 \) by \( v = \frac{1}{p}(v_1 + \alpha_2 v_2 + \ldots + \alpha_g v_g) \in L \setminus L' \) and go to Step 2.

**Remark 2.3.** To reduce the number of primes to check, one can apply Gauss elimination to make \( \Delta \) minimal.

**Remark 2.4.** The algorithm terminates in finitely many steps. In fact the substitution \( v_1 \mapsto \frac{1}{p}(v_1 + \alpha_2 v_2 + \ldots + \alpha_g v_g) \) implies that

\[
\Delta = \det(v_1, \ldots, v_g) \mapsto \det \left( \frac{1}{p} \left( v_1 + \sum_{i=2}^{g} \alpha_i v_i \right), v_2, \ldots, v_g \right) = \frac{1}{p} \det(v_1, \ldots, v_g) = \frac{\Delta}{p}.
\]

Hence, after finitely many iterations of the algorithm the rank of \( M \) modulo \( p \) is \( g \) for each prime \( p \).
3 Computing the expected rational points

We have a simple moduli interpretation of certain rational points of the modular curves $X_0^+(p)$. The expected rational points on $X_0^+(p)$ are the points corresponding to the unique cusp or to elliptic curves with complex multiplication such that $p$ is split or ramified inside the endomorphism ring of the elliptic curve itself. We call a rational point exceptional if it is not one of the expected ones.

Here we describe a way to find numerically the expected rational points on a modular curve $X_0^+(p)$, for $p$ an odd prime. We assume to know the first $m$ Fourier coefficients of a basis $f_1, \ldots, f_6$ of $\Omega(X_0^+(p))$, where $g$ is the genus of the modular curve. It is well known, see Stark [Sta66], that the orders in imaginary quadratic number fields with class number 1 are the ones with discriminant

$$\Delta = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$ 

The corresponding orders can be written in the form $Z + Z\tau$, where

$$\tau = \begin{cases} \frac{1+i\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is odd}, \\ \frac{i\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is even}. \end{cases}$$ 

Let $E$ be an elliptic curve with complex multiplication such that the discriminant $\Delta_E$ of its endomorphism ring $O_E$ is a class number 1 discriminant. This means that $\Delta_E$ is in the list above. If $\Delta_E$ is a square modulo $p$ we can associate to $E$ a point on $X_0^+(p)$, see Galbraith [Gal99]. The unique cusp is always rational. Let $\{1, \tau_E\}$ be the basis of the order $O_E$ such that $\tau_E$ is defined as above. There is a suitable element $\hat{\tau}$ in the $\text{SL}_2(Z)$-orbit of $\tau_E$ in $\mathcal{H}$ such that $P = (f_1(\hat{\tau}) : \ldots : f_6(\hat{\tau}))$ is a rational point for the modular curve. If we know $\hat{\tau}$, we can evaluate $f_1(\hat{\tau}), \ldots, f_6(\hat{\tau})$ numerically using the $q$-expansions. If $m$ is large enough, it is quite easy recognize the rational coordinates of $P$. To compute the coordinates of the cusp it is enough take $\hat{\tau} = i\infty$, this means to set $q = 0$ in the $q$-expansions. Now we explain how to compute $\hat{\tau}$ for the CM points.

We recall the moduli interpretation of the points of $X_0^+(p)$. Let $E'$ be an elliptic curve and let $C$ be a cyclic subgroup of order $p$ of the $p$-torsion subgroup $E'[p]$. We know that a point on $X_0^+(p)$ is an unordered pair $\{(E', C), (E'/C, E'[p]/C)\}$, where $E'/C$ is the unique elliptic curve, up to isomorphism, that is the image of the unique isogeny of $E'$ with kernel $C$. Over $\mathbb{C}$ this is $\{(C/\Lambda, \frac{1}{p}Z + \Lambda), (C/\Lambda', \frac{1}{p}Z + \Lambda')\}$ for some $\tau \in \mathcal{H}$ such that $\Lambda = Z + \tau Z$ and $\Lambda' = Z + \frac{1}{p}\tau Z$. If $\Delta_E$ is a square modulo $p$, we know there is a principal prime ideal $\mathfrak{p}$ of $O_E$ such that $(p) = \mathfrak{p}\mathfrak{p}$. Let $\alpha$ and $\tilde{\alpha}$ be generators of $\mathfrak{p}$ and $\mathfrak{p}$ respectively. The cyclic subgroups $C$ and $E'[p]/C$ are the kernels of the multiplication by $\alpha$ and $\tilde{\alpha}$. Let $(E', C) = (C/\Lambda_E, \frac{1}{p}Z + \Lambda_E)$, where $\Lambda_E = Z + \tau_E Z$. The point $((C/\Lambda_E, \frac{1}{p}Z + \Lambda_E), (C/\Lambda_E, \frac{1}{p}Z + \Lambda_E))$ is rational on $X_0^+(p)$.

Now, we want to find $\hat{\tau}$ such that $(C/\Lambda_E, \frac{1}{p}Z + \Lambda_E) = (C/\hat{\Lambda}, \frac{1}{p}Z + \hat{\Lambda})$, where $\hat{\Lambda} = Z + \hat{\tau} Z$. Let $c, d \in Z$ such that $\alpha = c\tau_E + d$. Then we can find $a, b \in Z$ such
that \(ad - bc = 1\) and so we have a matrix \( \hat{\gamma} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \). The transformation \( \hat{\gamma} = \gamma \tau_E \) correspond to the isogeny \( z + \Lambda_E \mapsto \frac{z}{\alpha} + \hat{\Lambda} \) for every \( z + \Lambda_E \in \mathbb{C}/\Lambda_E \). Hence \( \frac{1}{\alpha} + \Lambda_E \mapsto \frac{1}{\alpha}Z + \hat{\Lambda} \) and the group \( \frac{1}{\alpha}Z + \Lambda_E \) maps to \( \frac{1}{\alpha}Z + \hat{\Lambda} \) and we are done.

4 Computing the modular parametrization

In this section we assume to know the first \( m \) Fourier coefficients of the modular forms involved, where \( m \) is "large enough" for our purposes. Let \( p \) be a prime number and let \( J_0(p) \) be the jacobian variety of the modular curve \( X_0(p) \). If there is an isogeny factor \( E \) over \( \mathbb{Q} \) of dimension 1 of \( J_0(p) \), we know there is a non-constant morphism \( \phi: X_0(p) \to E \) defined over \( \mathbb{Q} \). Let \( f \) be the normalized eigenform in \( S_2(\Gamma_0(p)) \) associated to the isogeny class of \( E \). Let \( T \) be the Hecke algebra over \( \mathbb{Z} \) and let \( I_f = \{ T \in T : Tf = 0 \} \). We know that if the Fourier coefficients of \( f \) belong to \( \mathbb{Q} \), the associated abelian variety \( J_0(p)/I_f J_0(p) \) is an elliptic curve called optimal curve (or strong Weil curve). See Diamond and Shurman [DS05] Sections 6.5 and 6.6] for more details about these topics. If \( E = J_0(p)/I_f J_0(p) \), then we call \( \phi \) the modular parametrization with respect to \( X_0(p) \). The degree of the morphism \( \phi \) is called the modular degree. Using the identification of \( X_0(p) \) with \( \Gamma_0(p) \backslash \mathcal{H}^* \), we can write

\[
\phi: \Gamma_0(p)\backslash \mathcal{H}^* \to E(\mathbb{C})
\]

\[
\Gamma_0(p)\tau \mapsto \phi(\tau) = (\phi_1(\tau), \phi_2(\tau)),
\]

where \( \tau \in \mathcal{H}^* \) and \( \phi_1(\tau) \) and \( \phi_2(\tau) \) are Fourier series with rational coefficients in the indeterminate \( q = e^{2\pi i \tau} \).

**Lemma 4.1.** If \( E \) is an elliptic curve over \( \mathbb{Q} \) of conductor a prime \( p \) and with negative sign of the functional equation of the associated \( L \)-function, then the modular parametrization \( \phi: X_0(p) \to E \) factors as \( \phi = \phi_+ \circ \pi_p \), where \( \pi_p: X_0(p) \to X_0^+ (p) \) is the natural projection and \( \phi_+: X_0^+ (p) \to E \) is the modular parametrization with respect to \( X_0^+ (p) \). Moreover \( \phi_+ \) is defined over \( \mathbb{Q} \).

**Proof.** Just apply Galois Theory to the associated function fields and use invariance under the Atkin-Lehner involution of the differentials of \( X_0^+ (p) \). \( \square \)

Let \( X_0^+ (p) \) a modular curve of genus \( g \) with an isogeny factor \( E \) over \( \mathbb{Q} \) of dimension 1 of the jacobian variety \( J_0^+ (p) \). We denote by \( f_1, \ldots, f_g \) some \( g \) linearly independent newforms of \( S_2(\Gamma_0(p)) \) with eigenvalue +1 with respect to the Atkin-Lehner operator \( w_p \). This is a basis of \( S_2(\Gamma_0^+(p)) \). The modular parametrization \( \phi_+: X_0^+ (p) \to E \) is locally given by four homogeneous polynomials \( p_x, q_x, p_y, q_y \in \mathbb{Z}[x_1, \ldots, x_g] \), such that \( p_x \) and \( q_x \) have the same degree, \( p_y \) and \( q_y \) have the same
degree and

\[
\begin{align*}
\phi_x(\tau) &= \frac{p_x(f_1(\tau), \ldots, f_g(\tau))}{q_x(f_1(\tau), \ldots, f_g(\tau))}, \\
\phi_y(\tau) &= \frac{p_y(f_1(\tau), \ldots, f_g(\tau))}{q_y(f_1(\tau), \ldots, f_g(\tau))},
\end{align*}
\]

(1)

for every \(\tau\) representative of \(\Gamma_0(p)\tau\) chosen in a suitable open set of \(X_0(p)\).

To find these polynomials explicitly we use some linear algebra. The main difficulty is that we don’t know exactly the degrees of the polynomials \(p_x, q_x, p_y, q_y\), but we know the degree of the morphism \(\phi_x\). In Cremona [Cre92] or in the LMFDB online database [lmfdb] we can find the value of \(\deg \phi\) and we have \(\deg \phi_x = \frac{1}{2}\deg \phi\). For increasing degrees from 1 to \(\deg \phi_x\), we apply the following procedure to look for nontrivial relations. We rewrite the first equation as

\[p_x(f_1(\tau), \ldots, f_g(\tau)) - q_x(f_1(\tau), \ldots, f_g(\tau))\phi_x(\tau) = 0.\]

Let \(r = \left(\frac{g + d_x - 1}{d_x}\right)\) be the number of monomials of degree \(d_x\). Let \(I = \{F_1, \ldots, F_r\}\) be the set of the monomials obtained as product of \(d_x\) elements of the basis \(f_1, \ldots, f_g\), where repetitions are allowed, and let \(J = \{G_1, \ldots, G_r\}\) be the set with the same elements of \(I\) multiplied by \(\phi_x\). Since the Fourier coefficients of \(\phi_x, f_1, \ldots, f_g\) are algebraic numbers, the coefficients of the elements of \(I\) and \(J\) are also algebraic numbers and there is a number field \(K_f\) of finite degree over \(\mathbb{Q}\), which contains all these Fourier coefficients. Multiplying the elements of \(I\) and \(J\) by a suitable algebraic number, we can assume that the Fourier coefficients belong to the ring of integers of \(K_f\) and that they have integer coordinates with respect to a suitable basis of \(K_f\). Hence, there are \(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r \in \mathbb{Z}\) such that

\[
\begin{align*}
\alpha_1 F_1 + \ldots + \alpha_r F_r + \beta_1 G_1 + \ldots + \beta_r G_r &= 0, \\
\alpha_1 F_1 + \ldots + \alpha_r F_r &\neq 0, \\
\beta_1 G_1 + \ldots + \beta_r G_r &\neq 0.
\end{align*}
\]

These \(\alpha_i\)’s and \(\beta_i\)’s are the coefficients of \(p_x\) and \(q_x\) respectively. Different choices of \(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r\) correspond to the same map defined on different open sets. The same method is applied to the second equation of (1) to find the coefficients of \(p_y\) and \(q_y\).

**Remark 4.2.** We find the optimal curve with conductor \(p\) in Cremona’s tables in [Cre92] or in the LMFDB online database [lmfdb]. We use PARI to compute the \(q\)-expansions of the two components \(\phi_x(\tau)\) and \(\phi_y(\tau)\) of the modular parametrization of \(X_0(p)\).

## 5 An estimation on heights

Let \(n\) be a positive integer and let \(X\) be a complete nonsingular curve defined over \(\mathbb{Q}\) in \(\mathbb{P}^{n-1}\) and with an elliptic curve \(E\) as isogeny factor over \(\mathbb{Q}\) of its jacobian variety.
In this section we suppose to know a Weierstrass equation of \( E \), an explicit formula for the morphism \( \phi : X \to E \) defined over \( \mathbb{Q} \) and generators for the Mordell-Weil group of \( E \). Writing \( \phi \) in more explicit terms, we have
\[
\phi(x_1, \ldots, x_n) = \left( \frac{p_1(x_1, \ldots, x_n)}{q_1(x_1, \ldots, x_n)}, \frac{p_2(x_1, \ldots, x_n)}{q_2(x_1, \ldots, x_n)} \right),
\]
where \( p_1, q_1 \) are homogeneous polynomials with integer coefficients of degree \( d_1 \) and \( p_2, q_2 \) are homogeneous polynomials with integer coefficients of degree \( d_2 \). Let \( r \) be the number of monomials of degree \( d \), and let \( \alpha_i \) and \( \beta_i \) for \( i = 1, \ldots, r \), be the coefficients of \( p_1 \) and \( q_1 \) respectively. Moreover, let \( \alpha := \log \max \{ \sum_i |\alpha_i|, \sum_i |\beta_i| \} \) a constant that we use in the Proposition 5.1 below.

In the paper [Sil90], Silverman gives an estimate of the difference between the canonical height and the Weil height on an elliptic curve. We use the Theorem 1.1 of [Sil90] to prove the following proposition.

**Proposition 5.1.** Let the notation be as above and let \( Q \in \mathbb{P}^{r-1} \). Let \( H(Q) \) be the naive height of \( Q \) and let \( h(Q) := \log H(Q) \). If \( Q \in X(\mathbb{Q}) \), then \( \phi(Q) \in E(\mathbb{Q}) \) and
\[
\hat{h}(\phi(Q)) \leq \mu(E) + 1.07 + \frac{1}{2}(\alpha + d_\phi h(Q)),
\]
where the quantity \( \mu(E) \) is defined in Theorem 1.1 of [Sil90], the function \( \hat{h} \) is the canonical height on \( E \), the number \( d_\phi \) is the degree of the homogeneous polynomials \( p_1 \) and \( q_1 \) defined above and \( \alpha \) is the constant defined above.

**Proof.** Let \( Q \) be a rational point on \( X \). Let \( (x_1 : \ldots : x_n) \) its coprime integers coordinates in \( \mathbb{P}^{r-1} \). We denote by \( P \) the image of this rational point under \( \phi \), hence we have \( \phi(x_1, \ldots, x_n) = P = (P_x, P_y) \), where
\[
P_x = \frac{p_1(x_1, \ldots, x_n)}{q_1(x_1, \ldots, x_n)}.
\]

If \( |x_i| \leq H(Q) \), by the definition of height we have
\[
H(P_x) \leq H(Q)^{d_\phi} \max \left\{ \sum_i |\alpha_i|, \sum_i |\beta_i| \right\}.
\]
Taking the logarithm in the previous inequality we get \( h(P_x) \leq \alpha + d_\phi h(Q) \). Now, using the second inequality in Theorem 1.1 of [Sil90], we are done. \( \square \)

**Remark 5.2.** Since \( \phi \) is defined over \( \mathbb{Q} \), every rational point on the curve \( X \) must go in a rational point on the elliptic curve \( E \). Therefore, to find rational points on \( X \), it is enough to search in the preimage \( \phi^{-1}(P) \) letting \( P \) run over the rational points of \( E \).

**Remark 5.3.** In all our cases the Mordell-Weil group has rank 1 and is torsion-free, so it is generated by one point. One can find a generator in Cremona’s tables in [Cre92] or in the LMFDB online database [lmfdb].
Remark 5.4. If the Mordell-Weil group of $E$ has rank 1 with generator $P_0$ and is torsion-free, every rational point $P$ of $E$ has the form $P = kP_0$ for some $k \in \mathbb{Z}$. In this case we have
\[
\hat{h}(P) = \hat{h}(kP_0) = k^2 \hat{h}(P_0) \leq \mu(E) + 1.07 + \frac{1}{2}(\alpha + d, h(Q)),
\]
by properties of the canonical height. See [Sil86, Chapter VIII, Section 9] for more details about the canonical height.

6 Tables

In 6.1 we list the equations for the canonical model of the modular curves $X^*_0(p)$ for primes $p$ such that the genus $g$ is 6 or 7. We also list the expected rational points. The models all have good reduction modulo every prime $\ell \neq p$. In 6.2 we give an explicit morphism $\phi_+ : X^*_0(p) \to E$, whenever the jacobian variety $J^*_0(p)$ of $X^*_0(p)$ admits a 1-dimensional isogeny factor $E$ over $\mathbb{Q}$.

6.1 Equations

Here we list the genus, the equations of the canonical model and the expected rational points with the corresponding discriminants.

- Curve $X^*_0(163)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
&x_1x_3 + x_2x_4 + x_2x_5 - x_2x_6 = 0 \\
x_1^2 - x_1x_2 - x_1x_5 + x_2x_5 + x_3^2 + x_3x_4 = 0 \\
x_2x_4 - x_2x_5 + x_3x_5 = 0 \\
-x_1^2 + x_1x_2 - x_1x_4 + x_2x_4 + x_3x_6 = 0 \\
x_1x_3 + x_1x_5 + x_1x_6 + x_2x_3 - x_2x_5 + x_4x_5 = 0 \\
-x_1^2 + x_1x_2 + x_1x_3 + x_1x_4 - x_1x_5 + x_1x_6 + x_2x_5 - x_3^2 + x_4^2 + x_5x_6 = 0.
\end{align*}
\]

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| (0 : 0 : 1 : 0 : 1 : 0) | cusp | (0 : 1 : 1 : 0 : 1 : 0) | -12 |
| (24 : 10 : 13 : 15 : -50 : 42) | -163 | (0 : 1 : 0 : 0 : 0 : 0) | -11 |
| (1 : 0 : 1 : -2 : 0 : -1) | -67 | (0 : 0 : 1 : -1 : 0 : 0) | -8 |
| (1 : 1 : 2 : -2 : 2 : 0) | -28 | (1 : 1 : 0 : 0 : 0 : 0) | -7 |
| (1 : 1 : 0 : 1 : 1 : -1) | -27 | (2 : -1 : 3 : -4 : -1 : -2) | -3 |
| (0 : 0 : 0 : 0 : 1 : 0) | -19 | | |

9
• Curve $X^+_0(193)$. Genus $g = 7$. Equations of the canonical model in $\mathbb{P}^6$

\[
\begin{align*}
-x_1^2 - x_1x_4 - x_1x_5 - x_1x_7 + x_2x_7 + x_3^2 + x_3x_4 = 0 \\
x_1x_2 + x_1x_4 - x_1x_5 + x_1x_7 - x_2x_3 - x_2x_4 - x_2x_7 + x_3x_5 = 0 \\
x_1x_2 - x_1x_5 - x_2x_7 + x_3x_6 = 0 \\
-x_1x_2 - x_1x_3 + 2x_1x_5 + x_1x_6 + 2x_2x_3 + 2x_2x_4 - x_3^2 + x_4^2 + x_4x_5 = 0 \\
x_1^2 - x_1x_2 + 2x_1x_4 + x_1x_5 + 2x_1x_6 + x_1x_7 - x_2x_3 - x_3^2 + x_4^2 + x_4x_6 = 0 \\
x_1x_3 - x_1x_4 - x_1x_5 - 2x_1x_6 - x_1x_7 - 2x_2x_3 - 2x_2x_4 + 2x_2x_7 + x_3^2 - x_4^2 + x_4x_7 = 0 \\
x_1^2 + x_1x_3 + x_1x_4 - 2x_1x_5 + x_1x_7 - x_2x_3 - 3x_2x_4 - x_2x_5 - x_2x_7 - x_3^2 - x_4^2 = 0 \\
x_1^2 + 2x_1x_2 - x_1x_4 - x_1x_5 - 2x_1x_6 - x_1x_7 - x_2x_3 - x_2x_4 + x_2x_7 + x_3^2 - x_4^2 + x_3x_6 = 0 \\
-x_1x_3 + x_1x_4 + x_2x_3 + 2x_2x_4 - x_2x_7 - x_3^2 + x_4^2 + x_3x_7 = 0 \\
-x_1x_4 - x_1x_5 + x_1x_7 + x_2x_3 - x_2x_4 - x_2x_6 + 2x_2x_7 - x_3x_7 - x_4^2 + x_5^2 = 0.
\end{align*}
\]

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| (0 : 0 : 0 : 0 : 0 : 1) | cusp | (1 : 0 : -1 : 0 : 0 : 0) | -12 |
| (1 : 1 : -1 : 2 : 0 : -1) | -67 | (0 : 1 : 0 : 0 : 0 : 1) | -8 |
| (0 : 0 : 0 : 1 : -1 : -1 : 1) | -43 | (0 : 1 : 0 : 0 : 0 : 0) | -7 |
| (0 : 1 : 2 : -2 : 0 : 0 : 0) | -28 | (1 : 0 : 0 : 1 : 0 : -1 : 1) | -4 |
| (0 : 1 : 0 : 0 : 1 : 0 : 0) | -27 | (3 : 2 : 3 : 0 : 2 : 0 : 0) | -3 |
| (1 : 0 : 0 : -1 : 0 : -1 : 1) | -16 |

• Curve $X^+_0(197)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
-x_1x_2 + x_1x_4 - x_1x_5 - x_1x_6 + x_2x_3 = 0 \\
x_1^2 - x_1x_3 - x_1x_4 + x_1x_5 + x_2x_4 = 0 \\
2x_1x_2 - 2x_1x_3 - 2x_1x_4 + 3x_1x_5 + x_1x_6 - x_2^2 - x_3x_6 + x_3^2 + x_3x_4 + x_4^2 = 0 \\
x_1^2 + x_1x_3 + x_1x_4 + x_1x_6 - x_2^2 - x_3x_6 + x_4^2 + x_4x_5 = 0 \\
x_1x_2 - x_1x_3 - x_1x_4 + x_3x_5 + x_4x_6 = 0 \\
-x_1x_2 - x_1x_3 + x_1x_4 - x_1x_6 + x_2x_3 - x_2x_6 - x_3x_5 + x_3x_6 + x_5^2 = 0.
\end{align*}
\]

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| (0 : 0 : 0 : 0 : 1) | cusp | (1 : 1 : 1 : 0 : 0 : 0) | -19 |
| (1 : -1 : 3 : 2 : 6 : -6) | -163 | (1 : 0 : 0 : 0 : -1 : 1) | -16 |
| (1 : 1 : 1 : 1 : 0 : 1) | -43 | (1 : 0 : 0 : 1 : 0 : 1) | -7 |
| (1 : 0 : 2 : -1 : 0 : -1) | -28 | (1 : 0 : 2 : 0 : 1 : -1) | -4 |

• Curve $X^+_0(211)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
-x_1^2 - x_1x_4 - x_1x_5 + x_2x_3 - x_2x_6 + x_3x_4 = 0 \\
-x_1x_3 - x_1x_4 - x_1x_5 + x_2x_3 - x_2x_6 + x_3x_5 = 0 \\
x_1^2 - x_1x_2 + x_1x_3 + x_1x_4 - x_2x_3 + x_3x_6 = 0 \\
2x_1^2 - 2x_1x_2 + x_1x_3 + 2x_1x_4 + x_1x_5 - 2x_2x_3 - x_2x_4 + 2x_2x_6 + x_3^2 = 0 \\
x_1x_3 + x_1x_4 + 2x_1x_5 - x_1x_6 - 2x_2x_3 - x_3x_5 + 2x_2x_4 + x_4^2 = 0 \\
x_1^2 - 2x_1x_2 + x_1x_3 + 2x_1x_4 + x_1x_5 - x_1x_6 - 2x_2x_3 - x_2x_4 + x_3x_5 + 2x_2x_6 - x_4x_6 + x_5^2 = 0.
\end{align*}
\]
Rational point | Disc. | Rational point | Disc. | Rational point | Disc. |
|----------------|------|----------------|------|----------------|------|
| (0 : 0 : 0 : 0 : 0 : 1) | cusp | (0 : 1 : 1 : 0 : 0 : 1) | −12 | (0 : 0 : 1 : 0 : 0 : 0) | −8 | (0 : 1 : 0 : 0 : 0 : 0) | −7 | (2 : −3 : −2 : 4 : 1) | −3 |

- Curve $X_0^*(223)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
-x_1^2 + x_1x_3 - x_2x_3 - x_2x_4 + x_2x_5 = 0 \\
x_1^2 + 2x_1x_3 - x_1x_4 + x_1x_5 + x_3^2 + 2x_2x_4 + x_2x_6 + x_5^2 = 0 \\
-x_1^2 + x_1x_2 - x_1x_3 + x_1x_4 - x_2x_4 + x_2x_6 + x_3x_4 = 0 \\
x_1^2 - x_1x_2 + 2x_1x_3 - x_1x_6 + x_3^2 + 2x_2x_4 + 2x_3x_5 = 0 \\
-x_1^2 - x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 - x_3x_5 = 0 \\
-2x_1^2 - 2x_1x_3 + 3x_1x_4 + 2x_1x_5 + x_1x_6 + x_2^2 + 4x_2x_6 - x_3x_6 - x_4^2 - x_4x_6 + x_5^2 = 0.
\end{align*}
\]

| Rational point | Disc. | Rational point | Disc. | Rational point | Disc. |
|----------------|------|----------------|------|----------------|------|
| (0 : 0 : 0 : 0 : 0 : 1) | cusp | (0 : 1 : 1 : 0 : 0 : 1) | −12 | (0 : 0 : 1 : 0 : 0 : 0) | −8 | (0 : 1 : 0 : 0 : 0 : 0) | −7 | (2 : −3 : −2 : 4 : 1) | −3 |

- Curve $X_0^*(229)$. Genus $g = 7$. Equations of the canonical model in $\mathbb{P}^6$

\[
\begin{align*}
-x_1x_5 + x_2x_4 - x_2x_6 + x_2x_7 = 0 \\
x_1x_2 - x_1x_3 - x_1x_4 - x_1x_5 + x_2x_3 + x_2x_4 - x_2x_6 + x_3^2 + x_4x_7 = 0 \\
x_1x_5 + x_2^2 + x_2x_3 + x_2x_4 - x_2x_5 - x_2x_6 + x_3x_5 = 0 \\
x_1x_2 - x_1x_3 - x_1x_4 - x_1x_6 - x_2^2 + x_2x_4 + x_3^2 + x_3x_6 = 0 \\
x_1x_2 + x_1x_3 - x_1x_6 - x_1x_7 - x_2^2 - x_2x_3 + x_2x_6 + x_3x_7 = 0 \\
x_1x_2 + x_1x_3 + x_1x_5 + x_1x_6 + x_1x_7 - x_2x_3 - x_2x_4 + x_2x_6 - x_3^2 + x_4^2 = 0 \\
x_1x_3 + x_1x_6 - x_2^2 - x_2x_3 - x_2x_4 + x_2x_5 + x_3x_4 = 0 \\
x_1x_2 + x_1x_5 + x_1x_7 + x_2x_4 - x_2x_5 + x_5x_6 = 0 \\
x_1x_2 - 2x_1x_5 - x_1x_6 - x_1x_7 + x_2x_3 + 2x_2x_4 - x_2x_6 - x_2x_7 + x_3^2 - x_4x_6 + x_5x_7 = 0 \\
x_1x_5 - x_2x_3 - x_2x_4 - x_3^2 - x_4x_7 + x_6^2 = 0.
\end{align*}
\]
• Curve $X_0^+ (233)$. Genus $g = 7$. Equations of the canonical model in $\mathbb{P}^6$

$$
\begin{align*}
-x_1 x_2 - x_1 x_3 - x_1 x_4 + x_2^2 - x_2 x_3 - x_2 x_5 - x_2 x_6 + x_2 x_7 &= 0 \\
x_1 x_2 + x_1 x_4 - x_2^2 + x_2 x_6 + x_3 x_5 &= 0 \\
x_1^2 - 2x_1 x_2 - x_1 x_3 + x_1 x_5 + 2x_2^2 - 2x_2 x_3 - x_2 x_4 - 2x_2 x_5 - x_2 x_6 + x_3 x_6 &= 0 \\
-2x_1 x_3 - x_1 x_6 + x_2^2 - x_2 x_4 - x_2 x_5 + x_3 x_7 &= 0 \\
x_1^2 - 2x_1 x_2 + x_1 x_4 + x_1 x_5 + 2x_2^2 - 2x_2 x_3 - 2x_2 x_5 - x_2 x_6 + x_3 x_4 + x_4^2 &= 0 \\
x_1 x_3 + x_1 x_6 - x_2^2 + x_2 x_3 + x_2 x_5 + x_4 x_5 &= 0 \\
x_1 x_2 + x_1 x_3 - x_1 x_7 - x_2^2 + x_2 x_3 - x_2 x_4 + x_2 x_5 + x_2 x_6 + x_4 x_6 &= 0 \\
-x_1 x_2 - x_1 x_3 - x_1 x_4 + x_1 x_5 - x_1 x_6 - x_1 x_7 + 2x_2^2 - x_2 x_3 - x_2 x_4 - 2x_2 x_5 - x_2 x_6 + x_3^2 &= 0 \\
-x_1^2 + x_1 x_2 + 2x_1 x_3 - x_1 x_5 + x_1 x_7 - 2x_2^2 + 2x_2 x_3 + x_2 x_4 + 2x_2 x_5 + x_3 x_7 + x_3 x_6 &= 0 \\
-x_1^2 + x_1 x_2 - x_1 x_5 + x_2 x_4 - x_2 x_6 + x_3 x_7 + x_6^2 &= 0.
\end{align*}
$$

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| $0:0:0:0:1:0$ | cusp  | $0:0:1:0:0:0$ | $-8$  |
| $1:0:2:-2:1:0$ | $-28$ | $1:0:0:-1:0:0$ | $-7$  |
| $0:0:1:-1:0:0$ | $-19$ | $1:1:0:-2:1:1$ | $-4$  |
| $1:1:0:0:1:0$ | $-16$ | | |

• Curve $X_0^+ (241)$. Genus $g = 7$. Equations of the canonical model in $\mathbb{P}^6$

$$
\begin{align*}
x_1^2 + x_1 x_4 - x_2^2 - x_2 x_4 + x_2 x_6 &= 0 \\
x_1 x_5 - x_2 x_3 - x_2 x_5 + x_2 x_7 &= 0 \\
x_1 x_2 + 2x_1 x_3 + x_1 x_6 - x_1 x_7 - x_2^2 + x_3^2 &= 0 \\
x_1 x_3 - x_1 x_7 + x_2 x_4 + x_3 x_4 &= 0 \\
-x_1 x_4 - x_1 x_5 - x_2 x_4 + x_2 x_5 - x_3 x_5 - x_2^2 + x_4 x_5 &= 0 \\
x_1^2 + x_1 x_2 - x_1 x_3 + x_1 x_4 + x_1 x_5 + x_1 x_7 + x_2 x_3 - 2x_2 x_4 - x_2 x_5 + x_3 x_5 - x_3 x_6 + x_4 x_6 &= 0 \\
-x_1^2 + x_1 x_3 + x_1 x_4 - x_1 x_6 + x_2^2 + x_2 x_3 - x_2 x_4 + x_3 x_5 - x_3 x_6 - x_3 x_7 + x_4 x_7 &= 0 \\
x_1 x_2 + x_1 x_3 - 3x_1 x_4 - x_1 x_5 + x_1 x_6 + x_2^2 + x_2 x_4 - x_3 x_5 + x_3 x_6 - x_4 x_5 + x_5^2 &= 0 \\
x_1^2 - x_1 x_3 + x_1 x_4 + x_1 x_5 - x_1 x_6 + x_2^2 + x_2 x_3 - 2x_2 x_4 - x_2 x_5 + x_3 x_5 - x_3 x_6 - x_3 x_7 + x_5 x_6 &= 0 \\
x_1^2 + x_1 x_2 - x_1 x_3 + x_1 x_4 + 2x_1 x_5 + x_1 x_7 + x_2 x_3 - 2x_2 x_4 - 2x_2 x_5 + x_3 x_7 + x_5 x_6 + x_6^2 &= 0.
\end{align*}
$$

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| $0:0:0:0:0:1$ | cusp  | $1:1:0:1:0:0$ | $-12$ |
| $1:0:-2:-1:0:0$ | $-67$ | $0:0:1:1:0:0$ | $-8$  |
| $0:1:-1:0:1:0$ | $-27$ | $1:-1:-2:0:0:-2$ | $-4$  |
| $1:1:0:0:0:0$ | $-16$ | $3:1:-4:-6:-3:4:2$ | $-3$  |
• Curve $X_6^+(257)$. Genus $g = 7$. Equations of the canonical model in $\mathbb{P}^6$

\[
\begin{align*}
-x_1^2 - x_1x_2 + x_1x_4 - x_2^2 - x_2x_4 + x_2x_5 &= 0 \\
-x_1^2 - 2x_1x_2 + x_1x_3 + x_1x_4 - x_1x_5 - 2x_2^2 - x_2x_4 + x_2x_6 &= 0 \\
x_1x_2 - x_1x_5 - x_2x_3 + x_2x_7 &= 0 \\
x_1x_2 - x_1x_3 + x_1x_6 + x_2^2 + x_2x_4 + x_3x_4 &= 0 \\
-x_1x_3 - x_1x_4 + x_1x_7 + x_2^2 - x_2x_4 + x_3x_5 &= 0 \\
x_1^2 + x_1x_2 + x_1x_3 - x_1x_4 + 2x_2^2 - x_2x_3 + 2x_2x_4 - x_3x_6 + x_4x_7 &= 0 \\
x_1^2 + x_1x_2 - 2x_1x_4 + x_1x_5 - x_1x_7 + 2x_2^2 - x_2x_3 + 2x_3x_4 + x_3^2 - x_3x_6 - x_3x_7 + x_4x_6 &= 0 \\
x_1^2 - x_1x_3 - x_1x_4 - x_1x_5 - x_1x_6 + x_1^2 - x_2x_4 + x_3x_5 - x_3x_6 + x_3x_7 + x_3^2 &= 0 \\
x_1^2 + x_1x_3 - 2x_1x_4 - 2x_1x_7 + x_3^2 - x_3x_6 + x_3x_7 + x_3x_8 + x_3x_9 &= 0 \\
-x_1x_2 + 2x_1x_3 - 2x_1x_6 - x_1x_7 - 2x_4^2 - x_2x_4 - x_3x_6 + x_3x_7 + x_3x_8 &= 0.
\end{align*}
\]

| Rational point Disc. | Rational point Disc. |
|-----------------------|-----------------------|
| $x : 0 : 0 : 0 : 0 : 1$ | cusp                  |
| $0 : 0 : 1 : 0 : 0 : 1$ | $-11$                 |
| $0 : 1 : 0 : 0 : -1 : 0$ | $-67$                |
| $0 : 1 : 1 : 0 : 1 : 0$ | $-16$                 |
| $2 : -1 : 0 : 1 : 0 : 1$ | $-4$                  |

• Curve $X_6^+(269)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
x_1x_4 + x_2^2 + x_2x_3 + x_3^2 + x_3x_5 &= 0 \\
x_1x_2 - x_1x_5 + x_2^2 + x_2x_4 + x_3x_5 + x_3x_6 &= 0 \\
x_1x_2 + 2x_1x_4 + x_1x_6 + x_2^2 + x_3x_4 + x_4^2 &= 0 \\
x_1x_2 - x_1x_4 + x_1x_5 - x_2^2 - x_2x_3 + x_2x_4 + x_3x_4 + x_4x_5 &= 0 \\
x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6 - x_2x_3 - x_2x_4 + x_4x_6 &= 0 \\
-x_1x_2 - x_1x_3 - 2x_1x_4 - x_1x_5 - x_1x_6 - 2x_2^2 - x_2x_4 - x_3x_6 + x_3x_7 + x_3^2 &= 0.
\end{align*}
\]

| Rational point Disc. | Rational point Disc. |
|-----------------------|-----------------------|
| $0 : 0 : 0 : 0 : 0 : 1$ | cusp                  |
| $1 : -1 : 0 : -1 : 1 : 2$ | $-67$                |
| $1 : 1 : 0 : -1 : -1 : 0$ | $-43$                 |
| $1 : 1 : 2 : -3 : 0 : 0$ | $-4$                  |

• Curve $X_6^+(271)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
x_1^2 + 2x_1x_2 + x_1x_3 - x_1x_6 - x_2x_4 - 2x_2x_5 - x_2x_6 + x_3x_5 &= 0 \\
x_1^2 + x_1x_2 - x_1x_4 - x_1x_6 - x_2x_3 - x_2x_4 - x_3x_5 - x_3x_6 &= 0 \\
x_1^2 - 2x_1x_2 - x_1x_3 + x_1x_6 + x_2x_3 + x_2x_4 + x_3x_5 &= 0 \\
x_1x_2 - x_1x_4 - x_1x_6 - 2x_2x_3 + x_2x_4 + x_3^2 + x_4x_5 &= 0 \\
x_1^2 + 3x_1x_2 + 2x_1x_3 + x_1x_5 - 3x_1x_6 - 2x_2x_4 - x_3x_5 + x_3^2 &= 0 \\
-x_1x_2 - x_1x_3 - x_1x_4 - x_1x_5 + x_1x_6 - x_2x_3 + x_2x_4 + x_2x_5 + x_2x_6 + x_3x_4 + x_3x_6 &= 0.
\end{align*}
\]

| Rational point Disc. | Rational point Disc. |
|-----------------------|-----------------------|
| $0 : 0 : 0 : 0 : 0 : 1$ | cusp                  |
| $0 : 1 : 0 : 0 : 0 : 1$ | $-19$                 |
| $0 : 1 : 1 : 0 : 1 : 0$ | $-12$                 |
| $3 : -2 : -5 : 4 : -4 : -3$ | $-4$                  |
• Curve $X_0^+(281)$. Genus $g = 7$. Equations of the canonical model in $\mathbb{P}^6$

\[
\begin{align*}
-x_1x_2 + x_1x_3 + x_2x_4 - x_3x_4 + x_3x_6 &= 0 \\
-x_1x_6 - x_2x_3 - x_2x_6 + x_2x_5 + x_3x_7 &= 0 \\
x_1x_2 + x_1x_7 + 2x_3x_4 - x_3x_5 + x_5^2 &= 0 \\
-x_1x_7 - 2x_1x_3 - x_2x_3 - x_1x_5 - x_2x_3 + 2x_1x_5 + x_4x_5 &= 0 \\
x_1x_2 - x_1x_3 + x_2x_3 + 2x_3x_4 + x_4x_6 &= 0 \\
x_1x_3 + 2x_1x_4 + x_1x_6 + x_1x_5 - x_2^2 + x_2x_3 + x_2x_5 + x_3x_4 - 2x_3x_5 + x_4x_7 &= 0 \\
x_1x_2 + 2x_1x_3 + x_2x_4 + x_1x_5 + x_1x_7 + x_2x_3 - x_2x_5 - x_3x_5 + x_5^2 &= 0 \\
x_1x_2 - x_1x_3 + x_2^2 - x_2x_3 - x_2x_4 - x_2x_5 + x_3x_5 + x_4x_6 &= 0 \\
x_1x_2 - x_1x_3 - x_1x_5 - x_1x_7 + x_2^2 + x_2x_6 + x_3x_5 + x_3x_7 &= 0 \\
x_1x_2 - x_1x_3 + x_1x_6 - x_2x_3 - x_2x_4 - x_2x_7 + 2x_3x_4 + x_5^2 &= 0.
\end{align*}
\]

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| (0 : 0 : 0 : 0 : 0 : 1) | cusps | (1 : 0 : 0 : 0 : 0 : 0) | −16 |
| (2 : −5 : −5 : −1 : 1 : 5 : −3) | −163 | (1 : 0 : 0 : 1 : 0 : 0 : −1) | −8 |
| (0 : 1 : −1 : 1 : 1 : 1 : −1) | −43 | (0 : 0 : 1 : 0 : 0 : 0 : −1) | −7 |
| (0 : 0 : 1 : −2 : 0 : −2 : −1) | −28 | (1 : 2 : −2 : 2 : 0 : −2) | −4 |

• Curve $X_0^+(359)$. Genus $g = 6$. Equations of the canonical model in $\mathbb{P}^5$

\[
\begin{align*}
x_1x_2 - x_1x_5 + x_1x_6 + x_3x_4 &= 0 \\
x_1^2 + x_1x_2 + x_1x_3 - 2x_1x_4 - x_1x_5 + x_2x_4 + x_3x_5 &= 0 \\
x_2^2 - 3x_1x_2 - x_1x_3 + 2x_1x_4 + 2x_1x_5 - x_1x_6 + x_2^2 - x_2x_3 - x_2x_4 - x_3^2 + x_3x_6 &= 0 \\
x_1^2 + 3x_1x_2 + x_1x_3 - 2x_1x_4 - 2x_1x_5 + x_1x_6 - x_2^2 + x_2x_4 + x_3^2 + x_4x_5 &= 0 \\
x_2^2 - 2x_1x_2 - 2x_1x_3 + 3x_1x_4 + 3x_1x_5 - x_6 + x_2^2 - 2x_2x_4 - x_2x_5 - x_3^2 + x_4x_6 &= 0 \\
x_1^2 + 2x_1x_3 - 2x_1x_4 - 2x_1x_5 + x_2^2 + x_2x_4 - x_2x_6 + x_3^2 &= 0.
\end{align*}
\]

| Rational point | Disc. | Rational point | Disc. |
|----------------|-------|----------------|-------|
| (0 : 0 : 0 : 0 : 0 : 1) | cusps | (1 : 0 : 0 : 0 : 0 : 0) | −28 |
| (2 : −5 : −5 : −1 : 1 : 5 : −3) | −163 | (1 : 0 : 0 : 1 : 0 : 0 : −1) | −19 |
| (0 : 1 : −1 : 1 : 1 : 1 : −1) | −67 | (0 : 0 : 1 : 0 : 0 : 0 : −1) | −7 |
| (0 : 0 : 1 : −2 : 0 : −2 : −1) | −43 |

6.2 Modular parametrization

Here we list the isogeny factor $E$ of $J^+_0(p)$, a generator $P_0$ of the Mordell Weil group, an explicit formula for the modular parametrization $\phi_+: X^+_0(p) \to E$ and the modular degree $\deg(\phi_+)$ of the morphism $\phi_+$.

• Curve $X^+_0(163)$. Elliptic curve $E : y^2 + y = x^3 - 2x + 1$.

Mordell-Weil generator $P_0 = (1, 0)$. Modular degree $\deg(\phi_+) = 3$.

Modular parametrization: $\phi_+(x_1 : x_2 : x_3 : x_4 : x_5 : x_6) = (P_x, P_y)$,

\[
P_x = \frac{-2x_3 - x_4 + x_5 - x_6}{-x_3 + x_5}; \quad P_y = \frac{x_1^2 + x_1x_2 + 2x_1x_3 + 2x_1x_4 + 2x_1x_6 - x_2^2 + x_4^2}{x_1x_3 - x_1x_5}. 
\]
• Curve $X_0^+(197)$. Elliptic curve $E : y^2 + y = x^3 - 5x + 4$.
Mordell–Weil generator $P_0 = (1, 0)$. Modular degree deg($\phi_+$) = 5.
Modular parametrization: $\phi_+(x_1 : x_2 : x_3 : x_4 : x_5 : x_6) = (P_x, P_y)$.

\[
\begin{align*}
\text{Numerator}(P_x) &= -38x_1^2 - 25x_1x_2 - 6x_1x_3 + 13x_1x_4 - 61x_1x_5 + 11x_1x_6 + 22x_2^2 + \\
&\quad + 10x_2x_5 + 20x_2x_6 + 17x_3x_5 - 11x_3x_6,
\end{align*}
\]

\[
\begin{align*}
\text{Denominator}(P_x) &= -36x_1^2 - 34x_1x_2 + 11x_1x_3 + 30x_1x_4 - 27x_1x_5 - 8x_1x_6 + 12x_2^2 + \\
&\quad + 5x_2x_5 + 11x_2x_6,
\end{align*}
\]

\[
\begin{align*}
\text{Numerator}(P_y) &= 1715x_1^4 - 899x_1^2x_2 - 2691x_1^2x_3 - 1013x_1^2x_4 - 2889x_1^2x_5 - 81x_1^2x_6 + \\
&\quad + 1875x_1x_5^2 + 2476x_1x_2x_5 + 1176x_1x_2x_6 - 669x_1x_3x_5 + 1224x_1x_3x_6 + \\
&\quad + 2205x_1x_5x_6 - 1306x_1x_6^2 - 384x_1^2x_5 - 384x_2x_5x_6,
\end{align*}
\]

\[
\begin{align*}
\text{Denominator}(P_y) &= 961x_1^3 - 49x_1^2x_2 + 3875x_1^2x_3 - 632x_1^2x_4 + 1195x_1^2x_5 + 356x_1^2x_6 + \\
&\quad + 593x_1x_2^2 + 655x_1x_2x_5 + 432x_1x_2x_6 - 839x_1x_3^2 - 1680x_1x_3x_4 + \\
&\quad + 154x_1x_5x_6 + 384x_1x_5^2.
\end{align*}
\]

• Curve $X_0^+(229)$. Elliptic curve $E : y^2 + xy = x^3 - 2x - 1$.
Mordell–Weil generator $P_0 = (-1, 1)$. Modular degree deg($\phi_+$) = 4.
Modular parametrization: $\phi_+(x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7) = (P_x, P_y)$.

\[
\begin{align*}
\frac{P_x}{x_2 - x_5 + x_6} = \frac{-x_2 - x_5 + x_6}{x_2 + x_5}, \\
\text{Numerator}(P_y) &= x_1^2 + 3x_1x_2 + 7x_1x_3 + 6x_1x_4 + x_1x_5 - x_1x_6 - 4x_1x_7 + \\
&\quad - 2x_2x_3 - 2x_2x_4 + 3x_2x_6 - 2x_2^2 + x_4x_6 - 2x_4x_7 - x_6x_7, \\
\text{Denominator}(P_y) &= x_1^2 + 5x_1x_2 + x_1x_4 + 2x_1x_5 - x_1x_6 - x_1x_7 - x_3^2 - x_4x_7 + x_6^2.
\end{align*}
\]

• Curve $X_0^+(269)$. Elliptic curve $E : y^2 + y = x^3 - 2x - 1$.
Mordell–Weil generator $P_0 = (-1, 0)$. Modular degree deg($\phi_+$) = 3.
Modular parametrization: $\phi_+(x_1 : x_2 : x_3 : x_4 : x_5 : x_6) = (P_x, P_y)$.

\[
\begin{align*}
\frac{P_x}{x_2} = \frac{x_4 + x_6}{x_2}, \\
\frac{P_y}{x_1x_2} = \frac{x_1x_5 - x_2x_3 + x_3x_4}{x_1x_2}.
\end{align*}
\]

• Curve $X_0^+(359)$. Elliptic curve $E : y^2 + xy + y = x^3 - x^2 - 7x + 8$.
Mordell–Weil generator $P_0 = (2, -1)$. Modular degree deg($\phi_+$) = 4.
Modular parametrization: $\phi_+(x_1 : x_2 : x_3 : x_4 : x_5 : x_6) = (P_x, P_y)$.

\[
\begin{align*}
\frac{P_x}{x_2} &= -4x_1^2 + 3x_1x_2 - 4x_1x_3 - x_1x_5 + 3x_1x_6 + x_2x_4 + x_4^2 + \\
&\quad - 2x_2^2 + x_1x_5 - 2x_1x_3 + x_1x_6, \\
\frac{P_y}{x_1x_2} &= -5x_1^2 + 4x_1x_2 - 6x_1x_3 + 5x_1x_4 + 4x_1x_6 - x_2x_4 - x_2x_5 - x_2x_6 + x_3^2 + 2x_4^2, \\
&\quad + 3x_1x_5 - 2x_1x_4 - 2x_1x_5 + x_2x_4.
\end{align*}
\]
References

[ALe70] A.O.L. Atkin and J. Lehner, *Hecke Operators on \( \Gamma_0(m) \)*, Math. Ann. 185 (1970), 134-160.

[BGGP05] M.H. Baker, E. Gonzalez-Jimenez, J. Gonzalez and B. Poonen *Finiteness results for modular curves of genus at least 2*, American Journal of Mathematics, Vol. 127, No. 6 (2005), 1325-1387.

[BPR11] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on \( X_0^+(p^r) \)*, http://arxiv.org/pdf/1104.4641.pdf (2011).

[Cre92] J.E. Cremona, *Algorithms for modular elliptic curves* (2nd ed.), Cambridge University Press, Cambridge (1997).

[DS05] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer, New York (2005).

[Gal96] S.D. Galbraith, *Equations For Modular Curves*, Ph.D. thesis (1996).

[Gal99] S.D. Galbraith, *Rational Points on \( X_0^+(p) \)*, Experimental Mathematics Vol. 8 No. 4 (1999).

[GH78] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, John Wiley & Sons, New York, Toronto (1978).

[HH96] Y. Hasegawa and K. Hashimoto, *Hyperelliptic modular curves \( X_0^+(N) \) with square-free levels*, Acta Arithmetica LXXVII.2 (1996).

[Hee52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Zeit. (1952), 227-253.

[lmfdb] The database of L-functions, modular forms, and related objects, http://www.lmfdb.org/.

[Maz76] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47 (1976), 33-186.

[Maz77] B. Mazur, *Rational Points on Modular Curves*, Modular Functions of One Variable V (Proc. Internat. Conference, Univ. Bonn, Bonn, 1977), Lecture Notes in Math. 601, Springer-Verlag, Berlin (1977), 107-148.

[Mer15] P. Mercuri, *Equations of Modular Curves Associated to Normalizers of non-split Cartan Subgroups*, preprint 2016.

[Mom87] F. Momose, *Rational points on the modular curves \( X_0^+(N) \)*, J. Math. Soc. Japan Vol. 39 No. 2 (1978), 269-286.
[Ogg73] A.P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (St. Louis, MO, 1972), Proc. Sympos. Pure Math. 24, Amer. Math. Soc., Providence (1973), 221-231.

[Sd73] B. Saint-Donat, *On Petri’s analysis of the linear system of quadrics through a canonical curve*, Math. Ann. 206 (1973), 157-175.

[Shi95] M. Shimura, *Defining Equations of Modular Curves $X_0(N)$*, Tokyo J. Math. Vol. 18 No. 2 (1995), 443-456.

[Sil86] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York (1986).

[Sil90] J.H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Mathematics of Computation, Vol. 55 No. 192 (1990), 723-743.

[Sta66] H.M. Stark, *On complex quadratic fields with class number equal to one*, Trans. Amer. Math. Soc. 122 (1966), 112-119.

[Ste] W.A. Stein, The Modular Forms Database, [http://modular.math.washington.edu/Tables/](http://modular.math.washington.edu/Tables/)