Modular Curves over $\mathbb{Q}(i)$

Marlies Hoeksema

Master's thesis

Supervised by dr. Soumya Sankar

Department of Mathematics
Utrecht University
July 2024

Contents

1 Introduction

Let K be a number field and denote $G_K = \mathrm{Gal}(\overline{K}/K)$. A Galois representation of dimension n over a field F is a continuous homomorphism

$$\rho : G_K \to \mathrm{GL}_n(F).$$

We say that ρ is an ℓ-adic Galois representation if F is an extension of $\mathbb{Q}_\ell$. For an elliptic curve E we can define the following Galois representations:

$$\begin{aligned} \rho_{E,N} &: G_K \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(N) := \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \rho_{E,\ell^\infty} &: G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell) = \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ \rho_E &: G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim_N \mathrm{GL}_2(N). \end{aligned}$$

Define the reduction modulo N map $\pi_N : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(N)$. Any open subgroup $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ contains the kernel of π_N for some $N \geq 1$. The smallest N for which this holds is called the level of H. To every subgroup $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we can associate a modular curve X_H.

Definition 1.1. ([22, Definition 1.1.2] Let $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N. Then a point $P \in X_H(K)$ is called exceptional if the corresponding elliptic curve E/K is non-CM.

In 1977, Barry Mazur proposed the following program in [16], which is now known as Mazur's Program B:

"Given a number field K and a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$, classify all elliptic curves E/K whose associated Galois representation on torsion points maps $\mathrm{Gal}(\bar{K}/K)$ into $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$."
A way to do this is by counting K-rational points on the modular curve X_H associated to H. Since then, a lot of progress has been made on Mazur's Program B concerning elliptic curves defined over $\mathbb{Q}$. In 2022, Rouse, Sutherland and Zureick-Brown proved the following theorem:

Theorem 1.2 ([22, Theorem 1.1.6])**.** *Let ℓ be a prime, let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let $H = \rho_{E,\ell^\infty}(G_\mathbb{Q})$. Exactly one of the following is true:*

1. *The modular curve X_H is isomorphic to $\mathbb{P}^1$ or an elliptic curve of rank* 1*;*
2. *The modular curve X_H has an exceptional rational point;*
3. *$H \leq N_{ns}(3^3), N_{ns}(5^2), N_{ns}(7^2), N_{ns}(11^2)$ or $N_{ns}(\ell)$ for some $\ell \geq 19$;*
4. *H is a subgroup of one of the groups labeled* 49.147.9.1 *or* 49.196.9.1.

However, for modular curves over a general number field K there is currently not much written in the literature.
Inspired by the work of Rouse, Sutherland and Zureick-Brown in [22] and Sutherland and Zywina in [31], this thesis aims to progress Mazur's Program B for elliptic curves defined over $\mathbb{Q}(i)$. In this thesis, we will describe the arithmetically maximal subgroups corresponding to modular curves defined over $\mathbb{Q}(i)$ and attempt to compute all $\mathbb{Q}(i)$-points on one of these curves.

Every modular curve either has infinitely many points over a given number field K or it has finitely many points. We can list all subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ such that X_H has infinitely many K-points. We compute the maximal subgroups of these groups such that X_H has finitely many points over K; these are the arithmetically maximal subgroups. For all subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ such that X_H has finitely many K-points, there now exists a map

$$X_H \to X_G,$$

where G is an arithmetically maximal subgroup. We can use various point-counting techniques to find $X_H(K)$. The main technique discussed in this thesis is the Mordell-Weil sieve.

1.1 Main Results

Our main result is an enumeration of arithmetically maximal subgroups that correspond to modular curves defined over $\mathbb{Q}(i)$. Tables containing these groups can be found in the Appendix. We also proved the following theorem, regarding subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with infinitely many $\mathbb{Q}(i)$-points.

Theorem 1.3. *Up to conjugacy, there are at least* 452 *subgroups* $H \leq GL_2(\hat{\mathbb{Z}})$ *of prime power level such that the modular curve* X_H *has infinitely many* $\mathbb{Q}(i)$*-points. Out of these groups,* 438 *have genus* 0 *and* 14 *have genus* 1.

The 14 genus 1 groups stated in the theorem all have odd level and can be found in the Appendix. We were unable to enumerate all subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of genus 1 and even level such that X_H has infinitely many $\mathbb{Q}(i)$-points. However, up to conjugacy, the groups of genus 0 listed in the theorem are all possible genus 0 subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ such that $\#X_H(\mathbb{Q}(i)) = \infty$.

Theorem 1.4. *The arithmetically maximal subgroups for* $\mathbb{Q}(i)$ *of odd level are exactly the ones listed in the Appendix.*

1.2 Overview

In Chapter 2, we will give general results about modular curves, both defined over $\mathbb{Q}$ and over number fields.
Chapter 3 describes several point-counting techniques used over $\mathbb{Q}$, which (to an extend) can also be used in order to compute K-points.

Then, in Chapter 4, we will highlight one such point-counting technique, known as the Mordell-Weil sieve. We will describe both the classical and equationless version of this method and explain how it can be used over a general number field.
Lastly, in Chapter 5, we compute all arithmetically maximal subgroups that belong to modular curves defined over $\mathbb{Q}(i)$. We do so by first attempting to find all subgroups such that the corresponding modular curve has infinitely many points over $\mathbb{Q}(i)$ and then computing the maximal subgroups of those group.

2 Modular Curves

2.1 Modular Forms and Modular Groups

We define the modular group as the group of 2×2-matrices with determinant 1 denoted by

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

This group is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We will denote the upper half plane $\{\tau = x + iy \in \mathbb{C} \mid y > 0\}$ by $\mathbb{H}$. We say that a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is weakly modular of weight k if $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$ [8, Definition 1.1.1].

Definition 2.1. ([5, p. 10]) We can define an action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of meromorphic functions of $\mathbb{H}$ called the slash operator of weight k by $(f, \gamma) \mapsto f|_k\gamma$, where

$$(f|_k\gamma)(\tau) = (c\tau + d)^k f(\gamma\tau).$$

Let $\mathbb{D}$ denote the open unit disk $\{q \in \mathbb{C} \mid |q| < 1\}$. For a weakly modular function f of weight k, we can define a function $\tilde{f}$ on $\mathbb{D}^\times$ by $\tilde{f}(q) = f(\frac{\log q}{2\pi i})$. This is indeed well-defined, as $f(\tau + q) = f(\tau)$ for all $\tau \in \mathbb{H}$.

If we can extend $\tilde{f}$ to a holomorphic function on $\mathbb{D}$, then we say that f is holomorphic at ∞. In this case, $\tilde{f}$ has a Laurent expansion

$$\tilde{f}(q) \sum_{n \geq 0} a_n q^n.$$

Definition 2.2. ([8, Definition 1.1.2]) We say that a function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight k if

1. f is holomorphic on $\mathbb{H}$;
2. f is weakly modular of weight k;

3. f is holomorphic at ∞.

We denote the set of modular forms of weight k by $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$.

It follows that every modular form f of weight k has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i \tau n},$$

where $a_n(f) \in \mathbb{C}$ for all n. A cusp form of weight k is a modular form whose Fourier expansion has $a_0 = 0$. We denote the set of cusp forms of weight k by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$ [8, Definition 1.1.3].

Example 2.3. The Eisenstein series of weight k defined by $G_k : \mathbb{H} \to \mathbb{C}$, where

$$\tau \mapsto G_k(\tau) = \sum_{\substack{(m,n)\neq(0,0) \\ m,n\in\mathbb{Z}}} \frac{1}{(m\tau + n)^k}$$

is a modular form of weight k.

We can extend the concept of modular forms to subgroups of $\mathrm{SL}_2(\mathbb{Z})$, called congruence subgroups.

Definition 2.4. ([8, p. 13]) Let $N \geq 1$ be an integer, then we define the principal congruence subgroup of level N as

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then Γ is a congruence subgroup of level N if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}_{>0}$.

Example 2.5. We can define the following two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Let Γ be a a congruence subgroup of level N. We say that a function $f : \mathbb{H} \to \mathbb{C}$ is weakly modular of weight k with respect to Γ if it is meromorphic and $f|_k\gamma = f$ for all $\gamma \in \Gamma$ [8, p. 14].

Definition 2.6. ([8, Definition 1.2.3]) Let Γ be a congruence subgroup of level N. A modular form with respect to Γ is a function $f : \mathbb{H} \to \mathbb{C}$ such that

1. f is holomorphic on $\mathbb{H}$;

2. f is weakly modular of weight k with respect to Γ;

3. f is holomorphic at ∞.

We denote the space of modular form with respect to Γ of weight k by $\mathcal{M}_k(\Gamma)$. The cuspidal subspace of $\mathcal{M}_k(\Gamma)$ is denoted by $\mathcal{S}_k(\Gamma)$.

Definition 2.7. ([28, Definition 7.1]) The extended upper half plane is defined as the union $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

On the extended upper half plane we have the group action of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \begin{cases} \frac{a\tau+b}{c\tau+d} & \text{if } \tau \in \mathbb{H}^* \backslash \{\frac{-c}{d}\} \\ \frac{a}{c} & \text{if } \tau = \infty \\ \infty & \text{if } \tau = \frac{-c}{d}. \end{cases}$$

See for instance, [28, p.18]. We define an equivalence relation on $\mathbb{H}^*$ as follows: Two points in $\mathbb{H}^*$ are Γ-equivalent if they are in the same Γ-orbit under the action of $\mathrm{SL}_2(\mathbb{Z})$ defined on $\mathbb{H}^*$. [28, p.18]

Definition 2.8. ([28, p.18]) The quotient space of $\mathbb{H}^*$ under this equivalence relation is called the modular curve associated to Γ. The equivalence classes of points in $\mathbb{P}^1(\mathbb{Q})$ are called cuspidal points or cusps.

Let Γ be a congruence subgroup of level N, then the modular curve $\mathbb{H}^*/\Gamma$ is isomorphic to the moduli space of the stack $\mathcal{M}_\Gamma$ over Spec $\mathbb{Z}[1/N]$ parametrizing generalized elliptic curves over $\mathbb{Q}$ with Γ-level structure. More on this level structure will be explained in Section 2.4. More information on the stack M_Γ can be found in [7].

Example 2.9. We denote $Y(N) = \mathbb{H}/\Gamma(N)$, $Y_0(N) = \mathbb{H}/\Gamma_0(N)$ and $Y_1(N) = \mathbb{H}/\Gamma_1(N)$ [8, p.13]. Similarly, we denote $X(N) = \mathbb{H}^*/\Gamma(N)$, $X_0(N) = \mathbb{H}^*/\Gamma_0(N)$ and $X_1(N) = \mathbb{H}^*/\Gamma_1(N)$.

We define the genus of a congruence subgroup Γ to be the genus of the quotient $\mathbb{H}^*/\Gamma$. The number of subgroups of any genus is finite. All congruence subgroups of genus less than or equal to 24 have been enumerated by Cummins and Pauli in [6]. These groups can also be found in their online database.

Example 2.10. The congruence subgroup $\Gamma_0(9)$ is generated by

$$\left\langle \begin{pmatrix} 4 & 0 \\ 6 & 7 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 6 & 4 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 8 & 4 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} \right\rangle.$$

The corresponding modular curve $X_0(9)$ is isomorphic to $\mathbb{P}^1$.

We can now define the L-function of f, which we will later use to find the analytic rank of the Jacobian of a given modular curve.

Definition 2.11. ([8, p. 201]) Let f be a modular form of weight k for some congruence subgroup Γ. Then we define the L-function $L(f,s)$ of f as

$$L(f,s) := \sum_{n=1}^{\infty} a_n(f) n^{-s},$$

where $a_n(f)$ denotes the n-th coefficient of the q-expansion of f.

Definition 2.12. ([8, p. 16]) Let $N \in \mathbb{Z}_{>0}$, then we define a Dirichlet character modulo N as a function $\chi : \mathbb{Z} \to \mathbb{C}$ if there exists a group homomorphism $\chi' : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\chi(x) = \chi'(x \mod N)$ if $\gcd(N, x) = 1$ and $\chi(x) = 0$ otherwise.

The conductor of a Dirichlet character χ is the least integer $q \mid N$ such that $\chi(n + kq) = \chi(n)$ for all n and $n + kq$ coprime to N.

Example 2.13. The map $\phi_N : \mathbb{Z} \to \mathbb{C}$ defined by $x \mapsto \begin{cases} 1 & \text{if } \gcd(x, N) = 1 \\ 0 & \text{otherwise} \end{cases}$ is a Dirichlet character modulo N.

2.2 Hecke Operators

In order to introduce the concept of Hecke operators, we first define an action of the group $\mathrm{GL}_2^+(\mathbb{Q}) = \{\gamma \in \mathrm{GL}_2(\mathbb{Q}) \mid \det(\gamma) > 0\}$. We do this by defining

$$(f|_k\gamma)(\tau) = \frac{(\det\gamma)^k}{(c\tau + d)^k} f\left(\frac{a\tau + b}{c\tau + d}\right) \ \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}) \text{ and } \tau \in \mathbb{H}.$$

For a congruence subgroup Γ and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, let $\Gamma' = \Gamma \cap \alpha^{-1}\Gamma\alpha$. If f is modular form of weight k for Γ, then$f|_k\alpha$ is invariant under the right action of $\alpha^{-1}\Gamma\alpha$. Hence f is also a modular form of weight k for Γ'. This allows us to define

$$T_\alpha f = \sum_{[\gamma] \in \Gamma' \backslash \Gamma} f|_k\alpha\gamma.$$

Definition 2.14. ([8, p. 168-169]) Let N be a positive integer and let d be an integer such that $\gcd(d, N) = 1$. Let α denote a matrix in $\Gamma_0(N)$ with lower-right entry d. Then we can define the diamond operator $\langle d \rangle$ as the $\mathbb{C}$-linear endomorphism of $\mathcal{M}_k(\Gamma_1(N))$ such that $\langle d \rangle f = T_\alpha f$ for all $f \in \mathcal{M}_k(\Gamma_1(N))$.

Definition 2.15. ([8, p. 169]) Let p be a prime, then we define the Hecke operator T_p as the $\mathbb{C}$-linear endomorphism of $\mathcal{M}_k(\Gamma_1(N))$ such that $T_p f = \frac{1}{p} T_\alpha f$, where $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ for all $f \in \mathcal{M}_k(\Gamma_1(N))$.

For integers $N \geq 1$ and $k \in \mathbb{Z}$, we define the Hecke algebra $\mathbb{T}(\mathcal{M}_k(\Gamma_1(N)))$ that acts on $\mathcal{M}_k(\Gamma_1(N))$ as the commutative $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathcal{M}_k(\Gamma_1(N)))$ generated by

1. $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$;
2. T_p for p prime.

We can extend this notion of Hecke operators to T_m for a positive integer m in the following way: Set $T_1 :=$ id and $T_{p^r} := T_p T_p^{r-1} - p^{k-1}\langle p \rangle T_{p^{r-2}}$. We have $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$, for p, q distinct primes. Hence for $m = \prod p_i^{e_i}$, we can define

$T_m = \prod T_{p_i^{e_i}}$ [8, p. 179].

A Hecke eigenform is a modular form which is an eigenvector for all Hecke operators T_m, where m is a positive integer.

Let α_d denote the matrix $\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$. Then for any $d \mid N$, we can define the map

$$i_d : \mathcal{S}_k(\Gamma_1(Nd^{-1})) \times \mathcal{S}_k(\Gamma_1(Nd^{-1})) \to \mathcal{S}_k(\Gamma_1(N))$$

given by $(f, g) \mapsto f + g|_k\alpha_d$, where $(g|_k\alpha_d)(\tau) = d^{k-1}g(d\tau)$ [8, p. 188]. We can now define the notion of oldforms and newforms.

Definition 2.16. ([8, Definition 5.6.1]) The subspace of oldforms at level N is defined by $\mathcal{S}_k(\Gamma_1(N))^{\text{old}} = \sum_{p|N} i_p((\mathcal{S}_k(\Gamma_1(Np^{-1})))^2)$, where p is prime. We define the subspace of newforms at level N to be the orthogonal complement of the subspace of oldforms at level N with respect to the Petersson inner product, denoted by $\mathcal{S}_k(\Gamma_1(N))^{\text{new}} = (\mathcal{S}_k(\Gamma_1(N))^{\text{old}})^{\perp}$.

A definition of the Petersson inner product can be found in Chapter 5.4 of [8].

Definition 2.17. ([15]) Let $f \in \mathcal{S}_k^{\text{new}}(N, \chi)$ be a newform, then the Galois orbit of f is the set $[f] := \{\sigma(f) : \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}$.

Definition 2.18. ([8, p. 119], [1]) Let χ be a Dirichlet character modulo N. Then we define the χ-eigenspace of $\mathcal{M}_k(\Gamma_1(N))$ as $\mathcal{M}_k(\Gamma_0(N), \chi) := \{f \in \mathcal{M}_k(\Gamma_1(N)) \mid f|_k\gamma = \chi(d_\gamma)f \ \forall \gamma \in \Gamma_0(N)\}$, where d_γ denotes the lower right entry of γ. For the Galois orbit $[\chi]$, we can define

$$\mathcal{M}_k(\Gamma_0(N), [\chi]) := \bigoplus_{\chi' \in [\chi]} \mathcal{M}(\Gamma_0(N), \chi').$$

2.3 Galois Representations

Recall the definition of Galois representations given in the introduction:

Definition 2.19. Let K be a number field and denote $G_K = \text{Gal}(\overline{K}/K)$. A Galois representation of dimension n over a field F is a continuous homomorphism

$$\rho : G_K \to \text{GL}_n(F).$$

We say that ρ is an ℓ-adic Galois representation if F is an extension of $\mathbb{Q}_\ell$.

Let $N \geq 1$ be an integer, let K be a field with characteristic coprime to N. Suppose that (P_1, P_2) is a basis for $E[N](\overline{K})$, then we can define an isomorphism $E[N](\overline{K}) \to (\mathbb{Z}/N\mathbb{Z})^2$ by sending P_i to the standard basis vector e_i. Then this choice of basis gives rise to an isomorphism

$$\text{Aut}(E[N](\overline{K})) \to \text{GL}_2(N),$$

where $\mathrm{GL}_2(N) := \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, by defining

$$\iota(\phi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for $\phi \in \mathrm{Aut}(E[N](\overline{K}))$ such that

$$\phi(P_1) = aP_1 + cP_2$$

$$\phi(P_2) = bP_1 + dP_2.$$

The action of G_K on $E[N](\overline{K})$ induces a Galois representation $G_K \to \mathrm{GL}_2(N)$ defined by $\sigma \mapsto \iota(\sigma_N)$, where σ_N denotes the automorphism of $\mathrm{Aut}(E[N](\overline{K}))$ induced by σ. [22, p. 7]

Let E be an elliptic curve over a number field K, then we obtain the Galois representations seen in the introduction via the construction above [22, p. 1]:

$$\begin{aligned} \rho_{E,N} &: G_K \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(N) \\ \rho_{E,\ell^\infty} &: G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell) = \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ \rho_E &: G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim_N \mathrm{GL}_2(N). \end{aligned}$$

In the case that E is a non-CM elliptic curve the following theorem by Serre, also know as the open image theorem, is equivalent to the statement that $\rho_{E,N}$ is surjective for all but finitely many N.

Theorem 2.20. *(Serre, [26, p. 299, Theorem 3]) Let E be a non-CM elliptic curve. Then $\rho_E(G_K)$ is an open subgroup of $GL_2(\hat{\mathbb{Z}})$.*

2.4 Modular Curves

Let $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$. Recall that the level of H is the smallest integer $N \geq 1$ such that H contains the kernel of the map $\pi_N : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(N)$. If H has level N, then H is completely determined by $H(N) := \pi_N(H)$ [22, p. 7].
Let E be an elliptic curve defined over $\overline{K}$ for some field K and let H be a subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N.

Definition 2.21. ([22, p. 8]) An H-level structure of E is an equivalence class $[\iota]_H$ of isomorphisms $\iota : E[N](\overline{K}) \to (\mathbb{Z}/N\mathbb{Z})^2$, where ι is equivalent to ι' if there exists an $h \in H$ such that $\iota = h \circ \iota'$.

Two pairs $(E, [\iota]_H)$ and $(E', [\iota']_H)$ are equivalent if there exists an isomorphism $\phi : E \to E'$ such that for the induced isomorphism $\phi_N : E[N] \to E'[N]$ we have that $\iota \sim \iota' \circ \phi_N$. The set of these equivalence classes is denoted by $Y_H(\overline{K})$. We can define a G_K-action on this set via

$$(E, [\iota]_H) \mapsto (E^\sigma, [\iota \circ \sigma^{-1}]_H).$$

Definition 2.22. ([22, p. 8]) The set $Y_H(K)$ of K-rational points is exactly the set of elements of $Y_H(\overline{K})$ that are fixed by this action.

In other words, Y_H is defined as the modular curve that parametrizes elliptic curves with H-level structure. We denote the (Deligne-Mumford) compactification of Y_H by X_H. Similarly to Y_H, X_H parametrizes generalized elliptic curves with H-level structure [22, p. 8].
If $(E, [\iota]_H) \in Y_H(K)$, then for all $\sigma \in G_K$ there exists an isomorphism $\phi : E \to E^\sigma$ such that we have $\iota = h \circ \iota \circ \sigma^{-1} \circ \phi_N$ for some $h \in H$. It follows that $\iota \circ \phi_N \circ \sigma = h \circ \iota$, hence $\rho_{E,N}(G_K) \subset \mathrm{GL}_2(N)$ is conjugate to a subgroup of H. Indeed, classifying elliptic curves with a given Galois representation is equivalent to finding non-cuspidal rational points on modular curves. This is described in detail in Chapter 8 of [13]. Since the proof for this is scheme-theoretic, we will not discuss it further in this thesis.
For $H \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$, we can define Y_H and X_H as the modular curves parametrizing elliptic curves with ℓ-adic Galois image conjugate to a subgroup of H.

For an elliptic curve E and isomorphism i_E, we can define $A_E := \{\varphi_N \mid \varphi \in \mathrm{Aut}(E_{\overline{K}})\}$, where $\varphi_N = \iota_E(\varphi|_{E[N]})$. We can now also define $Y_H(\overline{K})$ as the set of pairs $(j(E), HgA_E)$, where $j(E)$ denotes the j-invariant of E and HgA_E is an element of the double coset $H\backslash \mathrm{GL}_2(N)/A_E$. Now, $Y_H(K)$ is exactly set of elements $(j(E), HgA_E)$ such that $Hg\rho_{E,N}(\sigma)A_E = HgA_E$ for all $\sigma \in G_K$ [22, p. 8].

While only non-cuspidal points parametrize elliptic curves with level structure, we are not exclusively concerned about them. In fact, information about the cusps can often be quite useful. In general, computing the number of cuspidal points on a modular curve is a lot easier than computing the number of non-cuspidal points. We will denote the set of cuspidal points of X_H by X_H^∞.
Define $\overline{H} := \langle H, -I \rangle \leq \mathrm{GL}_2(N)$ and let $U(N) := \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, -I \right\rangle$. We can now define the right G_K-action on $H\backslash \mathrm{GL}_2(N)/U(N)$ via $hgu \mapsto hg\chi_N(\sigma)u$, where $\chi_N(\sigma) := \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}$ is defined by $\sigma(\zeta_N) = \zeta_N^e$. It is known that X_H^∞ is in bijection with the subset of $H\backslash \mathrm{GL}_2(N)/U(N)$ that is fixed by this action [7, IV5.3, p.85]. So we have

$$\#X_H^\infty(K) = \#(H\backslash \mathrm{GL}_2(N)/U(N))^{G_K}. \tag{1}$$

We can make a connection between the number of cusps of the modular curve over $\mathbb{Q}$ and the number of cusps of the modular curve over a cyclotomic extension.

Corollary 2.23. *Let $K = \mathbb{Q}(\zeta_m)$ and let X_H be the modular curve corresponding to a subgroup $H \leq GL_2(\hat{\mathbb{Z}})$ of level N. If $\gcd(m, N) = 1$ then the number of cuspidal points on $X_H(K)$ is equal to the number of cuspidal points on $X_H(\mathbb{Q})$.*

Proof. Since $\gcd(m, N) = 1$, we have that

$$\chi_m(\mathrm{Gal}(\overline{K}/K)) = (\mathbb{Z}/N\mathbb{Z})^\times = \chi_m(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})).$$

□

There are several important subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ that one wants to consider. We have already seen examples of such groups, namely $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$. We define the Borel subgroup of level N, denoted by $B(N)$, as the subgroup of $\mathrm{GL}_2(N)$ consisting of the upper triangle matrices. We denote the split Cartan group of level N, consisting of diagonal matrices in $\mathrm{GL}_2(N)$ by $C_{\mathrm{sp}}(N)$. Its normalizer is denoted by N_{sp}. The corresponding modular curves are denoted by $X_{\mathrm{sp}}(N)$ and $X_{\mathrm{sp}}^{+}(N)$ respectively. Similarly, the non-split Cartan group of level N is denoted by $C_{\mathrm{ns}}(N)$, while its normalizer is denoted by $N_{\mathrm{ns}}(N)$. The modular curves corresponding to these groups are denoted by $X_{\mathrm{ns}}(N)$ and $X_{\mathrm{ns}}^{+}(N)$ respectively.

For consistency, we will uphold the same labelling system for these groups as described in [22]. This means that all subgroups H have a label of the form $N.i.g.n$, where N is the level of H, i is the index of $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : H] = [\mathrm{GL}_2(N) : \pi_N(H)]$ and g is the genus of H. Lastly, $n \geq 1$ is an ordinal chosen to distinguish subgroups where the first three quantities are the same. For a precise definition of n, see [22, p. 9-10].
As an example, take the subgroup H with the label 17.18.1.1, which corresponds to the modular curve $X_0(17)$. This is a subgroup of level 17, with index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : H] = 18$ and genus 1. Since it is the only modular curve with all three of these properties, we automatically label it with $n = 1$.

It is important here to note the connection between the subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that we use here and the congruence subgroups of $\mathrm{SL}_2(\hat{\mathbb{Z}})$ mentioned earlier. For every subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ there exists a congruence subgroup Γ_H of $\mathrm{SL}_2(\hat{\mathbb{Z}})$ such that $\Gamma_H = \pm H \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$. One needs to be aware that the level of H might not be equal to the level of Γ_H, while the genera of H and Γ_H will always be the same.

3 Point-Counting Techniques

In order to progress Mazur's Program B, one has to be able to count points on modular curves. In this chapter we will discuss several useful tools in doing so.

3.1 Counting points over finite fields

Let $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be a subgroup of level N and let X_H denote the corresponding modular curve. Let $q = p^e$ be a prime power coprime to N. The modular curve X_H has good reduction at all primes not dividing the level, as it has a smooth model over $\mathbb{Z}[1/N]$ [7, Chapter IV]. We can count the number of $\mathbb{F}_q$-points on X_H using the following formula

$$\#X_H(\mathbb{F}_q) = \#X_H^{\infty}(\mathbb{F}_q) + \#Y_H(\mathbb{F}_q),$$

where $X_H^{\infty}(\mathbb{F}_q)$ denotes the set of cusps on X_H over $\mathbb{F}_q$ [22, p.14]. Note that a cuspidal point cannot be Galois conjugate to a non-cupspidal point.

By Equation 1 we have

$$\#X_H^{\infty}(\mathbb{F}_q) = \#(H\backslash \mathrm{GL}_2(N)/U(N))^{G_{\mathbb{F}_q}},$$

so we can compute $\#X_H^{\infty}(\mathbb{F}_q)$ as the number of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$-orbits of the coset $[\overline{H}\backslash \mathrm{GL}_2(N)]$ that are fixed under the action of $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$, where $\overline{H} := \langle H, -I \rangle$.

We now want to compute the number of elements in the set of non-cuspidal points $Y_H(\mathbb{F}_q)$. Recall that this is exactly the number of elements in the coset $H\backslash \mathrm{GL}_2(N)/A_E$ that are fixed by the action $HgA_E \mapsto Hg\rho_{E,N}(\sigma)A_E$ for all $\sigma \in G_{\mathbb{F}_q}$, where $A_E := \{\varphi_N \mid \varphi \in \mathrm{Aut}(E_{\overline{\mathbb{F}_q}})\}$. So we want to compute

$$\#Y_H(\mathbb{F}_q) = \sum_{j(E) \in \mathbb{F}_q} \#(H\backslash \mathrm{GL}_2(N)/A_E)^{G_{\mathbb{F}_q}}.$$

Since $\pm I \in A_E$, we can replace $(H\backslash \mathrm{GL}_2(N)/A_E)^{G_{\mathbb{F}_q}}$ with $(\overline{H}\backslash \mathrm{GL}_2(N)/(A_E/\pm I))^{G_{\mathbb{F}_q}}$. Note that the quotient $A_E/\pm I$ is trivial in the case $j(E) \neq 0, 1728$, so it is enough to count the elements of $[\overline{H}\backslash \mathrm{GL}_2(N)]$ that are fixed by $G_{\mathbb{F}_q}$ using the action of the Frobenius endomorphism π on $E[N]$. Define $R_\pi = \mathrm{End}(E) \cap \mathbb{Q}[\pi]$, then $\pi|_{\mathrm{GL}_2(N)}$ is given by the matrix

$$A_\pi = A(a, b, \Delta) = \begin{pmatrix} \frac{a+bd}{2} & b \\ \frac{b(\Delta-d)}{4} & \frac{a-bd}{2} \end{pmatrix},$$

where $a = \mathrm{tr}\,\pi$, $\Delta = \mathrm{disc}(R_\pi)$, $d = \Delta \mod 2$ and $b = [R_\pi : \mathbb{Z}[\pi]]$ if $\mathbb{Z}[\pi] \neq \mathbb{Z}$ and $b = 0$ otherwise. It follows that $4q = a^2 - b^2\Delta$. [22, p.15]

Definition 3.1. Let E be elliptic curve over a field K of characteristic p. Then we say that E is supersingular if $E[p](K) = \{0\}$ and E is ordinary otherwise.

Let $\chi_{\overline{H}} : \mathrm{GL}_2(N) \to \mathbb{Z}_{\geq 0}$ denote the character of the permutation representation, where $\chi(G)$ is defined as the number of fixed points on $[\overline{H}\backslash \mathrm{GL}_2(N)]$ under the right action of G. Let Δ be an imaginary quadratic discriminant such that the norm equation $4q = a^2 - b^2\Delta$ has a solution with $a > 0$ coprime to q. Then there are $h(\Delta)$ ordinary j-invariants of elliptic curves over $\mathbb{F}_q$ with $\mathrm{disc}(R_\pi) = \Delta_j$, where $h(\Delta)$ denotes the class number of $\mathbb{Q}(\sqrt{\Delta})$ [32, Proposition 1]. Now, we can compute the number of $\mathbb{F}_q$-rational points on X_H corresponding to these ordinary j-invariants using the following equation: [22, p.15]

$$\#X_H^{\mathrm{ord}}(\mathbb{F}_q) = \sum_{\substack{0<a<2\sqrt{q} \\ \gcd(a,q)=1}} \sum_{\substack{4q=a^2-b^2\Delta \\ \Delta<-4}} h(\Delta)\chi_{\overline{H}}(A(a, b, \Delta)). \tag{2}$$

The following lemma allows us to count supersingular points on $X_H(\mathbb{F}_q)$. We denote these points by $X_H^{ss'}$.

Lemma 3.2. *([22, Lemma 5.1.1]) Let $q = p^e$ be a prime power, let $H \leq GL_2(N)$ with $\gcd(N, q) = 1$, let $h' = \lfloor h(-4p)/2 \rfloor$ and let $s_0 = 1$ for $p \equiv 2 \mod 3$ and $s_0 = 0$ otherwise. The number of $\mathbb{F}_q$-points on X_H corresponding to supersingular $j(E) \neq 0, 1728$ can be computed as follows:*

1. *If $p \leq 3$ then $\#X_H^{ss'}(\mathbb{F}_q) = 0$;*
2. *If e is odd and $p \equiv 1 \mod 4$ then*
$$\#X_H^{ss'}(\mathbb{F}_q) = (h' - s_0)\chi_{\overline{H}}(A(0, p^{(e-1/2)}, -4p));$$
3. *If e is odd and $p \equiv 3 \mod 4$ then*
$$\#X_H^{ss'}(\mathbb{F}_q) = h'\chi_{\overline{H}}(A(0, 2p^{(e-1/2)}, -p)) + (h' - s_0)\chi_{\overline{H}}(A(0, p^{(e-1/2)}, -4p));$$
4. *If e is even then*
$$\#X_H^{ss'}(\mathbb{F}_q) = \left(\frac{p - 6 + 2\left(\frac{-3}{p}\right) + 3\left(\frac{-4}{p}\right)}{12}\right)\chi_{\overline{H}}(A(2p^{e/2}, 0, 1)).$$

For $j(E) = 0, 1728$, we compute the weighted sum of $\chi_{\overline{H}}(A_\pi)$ over k-isomorphism classes of elliptic curves with $j(E) = 0, 1728$. By extending $\chi_{\overline{H}}$ to $\mathbb{Q}[\mathrm{GL}_2(N)]$, we can compute the number of $\mathbb{F}_q$-points of X_H above $j(E) = 0, 1728$ using

$$\#X_H^{j=0}(\mathbb{F}_q) = \chi_{\overline{H}}\Bigg(\sum_{\substack{j(E)=0 \\ p\neq 2}} \frac{A(a, b, \Delta)}{\#\mathrm{Aut}(E)}\Bigg),$$

$$\#X_H^{j=1728}(\mathbb{F}_q) = \chi_{\overline{H}}\Bigg(\sum_{\substack{j(E)=1728 \\ p\neq 3}} \frac{A(a, b, \Delta)}{\#\mathrm{Aut}(E)}\Bigg).$$

The values of a, b and Δ can be found in [22, Table 6, p. 17]. We can now count all $\mathbb{F}_q$-rational points on X_H using the formula

$$\#X_H(\mathbb{F}_q) = \#X_H^{\infty}(\mathbb{F}_q) + \#X_H^{\mathrm{ord}}(\mathbb{F}_q) + \#X_H^{ss'}(\mathbb{F}_q) + \#X_H^{j=0}(\mathbb{F}_q) + \#X_H^{j=1728}(\mathbb{F}_q).$$

Example 3.3. Let us count the number of points on the curve $X_{\mathrm{ns}}(7)$ over $\mathbb{F}_5$. The split Cartan group of level 7 is generated by the matrix $\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix}$. We count the number of cuspidal points $X_{\mathrm{ns}}^{\infty}(7)$ and find that there are none. Next, we compute the the number of $\mathbb{F}_5$-rational points over $X_{\mathrm{ns}}(7)$ that correspond to the ordinary j-invariants. Since $q = 5$, there are three different possibilities for the Frobenius matrices $A(a, b, \Delta)$, namely $A(1, 1, -19)$, $A(2, 1, -16)$ and $A(3, 1, -11)$. The corresponding class numbers are $1, 2$ and 1 respectively, while $\chi(A(1, 1, -19)) = 0$ and $\chi(A(2, 1, -16)) = \chi(A(2, 1, -11)) = 2$.
Since e is odd and $p \equiv 1 \mod 4$, Lemma 3.2 tells us that $\#X_{ns}^{ss'}(7) = 0$.
We find that

$$\#X_{ns}^{j=0}(7) = \chi(A(0, 1, -20)/2) = 0$$

and

$$\#X_{ns}^{j=1728}(7) = \chi(A(2, 2, -4)/4) = 2.$$

So we get $\#X_{\mathrm{ns}}(7) = 2 + 2 + 2 = 6$.

3.2 The Jacobian

Let X be a smooth variety over an (algebraically closed) field K. A prime divisor is an irreducible closed subvariety Z of codimension one defined over K. A divisor D is a linear combination $D = \sum_i n_i Z_i$ of prime divisors. We denote the set of divisors on X by $\mathrm{Div}\, X$. When all coefficients of this linear combination are non-negative, we say that D is a effective divisor. We define the degree of a divisor D by $\deg(D) = \sum_i n_i$. [11, p. 130]

Let $\kappa(X)$ denote the function field of X and let $f \in \kappa(X)^\times$. Let $\mathcal{O}_{X,Z}$ denote the local ring at Z and let $\mathfrak{m}$ be its maximal ideal. If there exists a $d \in \mathbb{Z}_{\geq 0}$ such that $f \in \mathfrak{m}^d$ and $f \notin \mathfrak{m}^{d+1}$, then we say that f has valuation $v_Z(f) = d$. Similarly, if $1/f \in \mathfrak{m}^d$ and $1/f \notin \mathfrak{m}^{d+1}$, we say that f has valuation $v_Z(f) = -d$. In the case that f and $1/f$ are both in the local ring at Z, we say that $v_Z(f) = 0$. We can now define a divisor $\mathrm{div} f (= (f)) = \sum_{Z \text{ prime divisor}} v_Z(f) Z$. We say that a divisor D is principal if there exists an $f \in \kappa(X)^\times$ such that $D = \mathrm{div} f$. We denote the set of principal divisors on X by $\mathrm{Princ}\, X$. [11, p. 131]

Two divisors D, D' are linearly equivalent if there exists a principal divisor (f) such that $(f) = D - D'$. In that case we denote linear equivalence by $D \sim D'$ [11, p. 131].

Proposition 3.4. *Let X be a smooth projective variety and let $f, g \in \kappa(X)^\times$.*

1. *If $(f) = 0$, then f is constant.*
2. *If $(f) = (g)$ then there exists a constant $a \in k^\times$ such that $f = ag$.*

Proof.

1. If $v_Z(f) = 0$ for all prime divisors Z, then f is regular on X. Therefore $f \in K$. [11, Theorem I3.4(a)].
2. If $(f) = (g)$, then $(f) - (g) = (f/g) = 0$. It follows from the first statement that $f/g = a$ for some constant $a \in k^\times$, hence $f = ag$.

□

We remark that all principal divisors have degree 0.

Definition 3.5. We define the Picard group of X by $\mathrm{Pic}\, X = \frac{\mathrm{Div}\, X}{\mathrm{Princ}\, X}$.

The kernel of the degree map $\deg : \mathrm{Pic}\, X \to \mathbb{Z}$ is called the Jacobian of X which we will denote by J_X [11, Remark II.6.10.3]. The map

$$X \to J_X$$

defined by $P \mapsto [P] - [O]$ for some $O \in X$ is called the Abel-Jacobi map. This map is a bijection if X is a curve of genus 1 [19, p. 2].

Let C be a curve over a number field K. Then the Jacobian J_C of C over K is an abelian variety. By the Mordell-Weil theorem, $J_C(K)$ is finitely generated, so it is of the form $J(K)_{\text{tors}} \oplus \mathbb{Z}^r$, where $0 \leq r < \infty$ denotes the algebraic rank of the Jacobian and $J(K)_{\text{tors}}$ is its torsion subgroup.

3.2.1 Over $\mathbb{Q}$

Besides the algebraic rank, the Jacobian also has a so-called analytic rank; we will discuss how to compute this in the next section. This analytic rank is conjectured to be the same as the algebraic rank, known as the Birch-Swinnerton-Dyer conjecture [4]. It has yet to be proven true in the general case, but we know that it holds if the analytic rank of the Jacobian is 0 or 1. Moreover, if $K = \mathbb{Q}$, we have the following theorem by Chabauty:

Theorem 3.6. *(Chabauty, [10, Theorem 1]) Let C be a curve of genus ≥ 2 over $\mathbb{Q}$. If $r \leq g - 1$, then $C(\mathbb{Q})$ is finite.*

Note that this theorem is actually a special case of Faltings' theorem:

Theorem 3.7. *(Faltings, [9, Theorem 7]) Let X be a smooth curve over a number field K. Then $X(K)$ is finite.*

The following theorem by Coleman can easily be used to find an upper bound for $\#C(\mathbb{Q})$.

Theorem 3.8. *(Coleman, [10, Theorem 2]) Let C be a curve over $\mathbb{Q}$ of genus ≥ 2 and let p be a prime of good reduction. Then*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

For any prime p of good reduction there exists an injection $J(\mathbb{Q})_{\text{tors}} \hookrightarrow J(\mathbb{F}_p)$. Note that $J(\mathbb{Q})_{\text{tors}}$ is always an abelian group, so oftentimes we can extract valuable information about $J(\mathbb{Q})_{\text{tors}}$ by computing $J(\mathbb{F}_|)$ for many primes of good reduction. If C is a hyperelliptic curve, the following equality holds: [18]

$$\#J(\mathbb{F}_p) = \frac{\#C(\mathbb{F}_p)^2 + \#C(\mathbb{F}_{p^2})}{2} - p.$$

3.2.2 Analytic rank of the Jacobian

Definition 3.9. ([15]) Let A be an abelian variety. Then the analytic rank of A is defined as the order of vanishing of its L-function at its central point.

Since the Birch-Swinnerton-Dyer conjecture holds for analytic rank ≤ 1, we will often be able to use this equality to find the algebraic rank of the Jacobian. For modular curves defined over $\mathbb{Q}$ it is easier to compute the analytic rank instead of the algebraic rank.

Let $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be a subgroup of level N and let X_H denote the corresponding modular curve. Let J_H denote the Jacobian of X_H. By [22, Theorem A.1.7], J_H is $\mathbb{Q}$-isogenous to $\prod_{n=1}^{m} A_{f_i}^{e_i}$, where $A_{f_i}^{e_i}$ denotes the modular abelian variety associated to the Galois orbit of an eigenform f_i of weight 2 for $\Gamma_1(N) \cap \Gamma_0(N^2)$. We can decompose the corresponding space of modular forms as

$$S_2(\Gamma_1(N) \cap \Gamma_0(N^2)) = \bigoplus_{\mathrm{cond}(\chi)|N} S_2(\Gamma_0(N^2), [\chi]),$$

where $[\chi]$ denotes the Galois orbit of the Dirichlet character χ [22, p. 18].

The following method of computing the analytic rank of the Jacobian is described in [22, Chapter 6]. Let $f \in S_2(\Gamma_0(N^2), [\chi])$, then we denote by $\mathbb{Q}(f)$ the rational field adjoined with the Fourier coefficients of f. We define the integral q-expansion of the trace form $\mathrm{Tr}(f)$ associated to f by

$$\mathrm{Tr}(f)(q) = \sum_{n \geq 1} \mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}(a_n(f))q^n,$$

where $\mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}(a_1(f)) = \dim f := [\mathbb{Q}(f) : \mathbb{Q}]$ and a_p is the Frobenius trace of $A_f/\mathbb{Q}$ for all primes p [1, Section 4.5]. Equivalently, a_p is the p-th Dirichlet coefficient of the L-function

$$L(A_f, s) = \prod_{f \in [f]} L(f, s).$$

Define $S(H) := \{[f_1], \ldots, [f_m]\}$ as the Galois orbits of eigenforms $f \in S_2(\Gamma_1(N) \cap \Gamma_0(N^2))$ with $\dim f \leq \dim J = g(H)$. Then there exists a sequence of non-negative integers $e(H) = (e_1, \ldots e_m)$ such that

$$L(J_H, s) = \prod_{i=1}^{m} L(A_{f_i}, s)^{e_i},$$

which satisfies $\sum_i e_i \dim f_i = g(H)$. For $B \in \mathbb{R}_{>0}$, define $T(B)$ to be the $n \times m$ integer matrix with i-th column

$$[a_1(\mathrm{Tr}(f_i)), a_2(\mathrm{Tr}(f_i)), a_3(\mathrm{Tr}(f_i)), a_5(\mathrm{Tr}(f_i)), \ldots, a_p(\mathrm{Tr}(f_i)), \ldots],$$

where p varies over the $n-1$ primes that are bounded by B and do not divide the level of H. Define $a(H; B) := [g(H), a_2(H), a_3(H), \ldots, a_p(H), \ldots]$, where $a_p(H)$ is the trace of the Frobenius endomorphism of J_H at a prime $p \leq B$ that does not divide the level of H. If we take $B \geq 1$, we have

$$T(B)e(H) = a(H; B)$$

and for B large enough, $e(H)$ is uniquely determined by $T(B)$ and $a(H; B)$ [29]. So we can compute the factors of $L(J_H, s)$ using the following algorithm:

1. We compute $S(H)$, which only depends on the genus and level of H;

2. We determine B by starting with a value that makes $T(B)$ a square matrix and increasing it until columns of $T(B)$ become linearly independent over $\mathbb{Q}$;

3. We compute $a(H; B)$ by computing the Frobenius traces $a_p(H) = p + 1 - \#X_H(\mathbb{F}_p)$ and we determine $e(H)$ from $T(B)e(H) = a(H; B)$ using linear algebra.

We can compute the analytic rank of J_H as $\sum e_i r_i$, where r_i denotes the sum of the analytic ranks of the eigenforms in the i-th Galois orbit $[f_i]$.

Example 3.10. We take the modular curve $X_{ns}(7)$ of genus 1. There is only one Galois orbit of an eigenform $f \in S_2(\Gamma_1(7) \cap \Gamma_0(49))$ with $\dim f \leq g = 1$, which has the label 49.a.a on LMFDB. We see that $a_1(\mathrm{Tr}(f)) \cdot e_1 = 1$ and that the analytic rank of the Jacobian $J_{C_{\mathrm{ns}}}$ is $e_1 \cdot r_1$, where r_1 denotes the analytic rank of $[f]$. We find that $r_1 = 0$, hence $J_{C_{\mathrm{ns}}}$ has rank 0.

3.2.3 Over a number field

Let K be a number field and let C be a curve defined over K. Let J_C denote the Jacobian of C.

Theorem 3.11. *([24, Theorem 1.2]) Let C have infinitely many K^{ab}-points. Then the module $\mathbb{Q} \otimes_{\mathbb{Z}} J_C(K^{ab})$ has infinite rank.*

Let C be a hyperelliptic curve defined by $y^2 = f(x)$ and let d be a squarefree integer. Then the quadratic twist of C by d, which we will denote by C^d, is defined by $dy^2 = f(x)$ [23].

Furthermore, let K be any number field and let C defined by $y^2 = f(x)$ be a hyperelliptic curve over K. Then there exists a short exact sequence

$$1 \to J[2] \to J(\overline{K}) \overset{x \mapsto 2 \cdot x}{\to} J(\overline{K}) \to 1,$$

where $J[2]$ denotes the 2-torsion of $J(\overline{K})$. Results on cohomology will now tell us that $J(K)/2J(K) \hookrightarrow H^1(\mathrm{Gal}(\overline{K}/K), J[2])$ [25, p. 1].
We can define a subgroup of $H^1(\mathrm{Gal}(\overline{K}/K), J[2])$ called the 2-Selmer group, denoted by $\mathrm{Sel}_2(J)$. In order to properly define this set, we first need to define the injective map $\delta_v : J(K_v)/2J(K_v) \to A_K^\times/(A_K^\times)^2$, where $A_K := K[x]/(f(x))$. [25, p.5]

Definition 3.12. ([25, Definition 2.2, p.]) The 2-Selmer group $\mathrm{Sel}_2(J)$ of J is the subgroup of $H^1(\mathrm{Gal}(\overline{K}/K), J[2])$ consisting of all cohomology classes whose restriction to $\mathrm{Gal}(\overline{K_v}/K_v)$ lies in the image of δ_v for all places v.

The dimension of the 2-Selmer group of J equals the rank of J plus the dimension of the set of elements of order 2 in the Tate-Shafarevich group [25, p. 1]. Computing $\mathrm{Sel}_2(J)$ can therefore gives us an upper bound on the rank of the Jacobian over a number field. Since the Tate-Shafarevich group can be hard to compute, it will be hard in most cases to achieve the exact rank in this manner, but this result is useful nonetheless.

The L-function of J_C is defined by

$$L(J_C, s) = \prod_{\mathfrak{p} \in \mathcal{O}_K} L_{\mathfrak{p}}(J_C, N\mathfrak{p}^{-s})^{-1},$$

where $\mathfrak{p}$ denotes a prime ideal and $L_{\mathfrak{p}}$ is a monic polynomial of degree $2 \cdot \dim J_C$ [14, p. 9].

Theorem 3.13. *([3, p. 4720]) Let C be a curve defined over $K = \mathbb{Q}(i)$ and let J_C be its Jacobian. Then rank $J_C(K) =$ rank $J_C(\mathbb{Q}) +$ rank $J_C^{-1}(\mathbb{Q})$, where J_C^{-1} denotes the quadratic twist of J_C by -1.*

By [12], the quadratic twist of J_C by d is equal to J_{C^d}.

4 The Mordell-Weil Sieve

In the previous chapter, we saw how to count points on a modular curve over a finite field and how to compute the analytic rank of the Jacobian. We can use this knowledge in our application of the Mordell-Weil sieve: a technique which is extremely useful for counting points on curves of higher genus.

4.1 Classical Mordell-Weil Sieve

Let C be a curve of genus ≥ 2 defined over $\mathbb{Q}$ and let $J(\mathbb{Q})$ denote its Jacobian. Suppose that we know an injective map $\iota : C \to J$ and the generators of $J(\mathbb{Q})$. Then there exists a commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_v C(\mathbb{Q}_v) \arrow[r, "\iota"] & \prod_v J(\mathbb{Q}_v)
\end{tikzcd},$$

where the lower arrow is induced by the top one and the vertical arrows are localizations. This means that if the intersection between the images of the bottom ι and α is empty, then $C(\mathbb{Q}) = \emptyset$. Conversely, any point in this intersection must come from a point in $C(\mathbb{Q})$; if $C(\mathbb{Q}) = \emptyset$ then the intersection must be empty. [2, p. 3]. As described below, we can use this principle to develop a method of showing that a specific curve has no rational points. This is the Mordell-Weil sieve.

The statement that $C(\mathbb{Q}) = \emptyset$ if the intersection of the images of α and the bottom ι is empty, does not just hold for the product over all places v; for any finite set S of places v it holds that the diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_{v \in S} C(\mathbb{Q}_v) \arrow[r, "\iota"] & \prod_{v \in S} J(\mathbb{Q}_v)
\end{tikzcd}$$

commutes. It has been conjectured by Bjorn Poonen that the converse also holds: If $C(\mathbb{Q}) = \emptyset$ then there exists a finite set S such that the images of α and the lower ι do not intersect [20, Conjecture 5.1].

For simplicity, we can take S to be finite a set of primes of good reduction. This makes it easier to actually compute the intersection. We note that as a consequence of Faltings' theorem, there exists an integer $N > 1$ such that $C(\mathbb{Q})$

embeds into $J(\mathbb{Q})/NJ(\mathbb{Q})$. We can therefore instead consider the following commutative diagram:

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q})/NJ(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "\beta=(\beta_{N,p})_{p\in S}"] & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)
\end{tikzcd}.$$

We define the set

$$A(S,N) = \{x \in J(\mathbb{Q})/NJ(\mathbb{Q}) \,:\, \alpha(x) \in \operatorname{im}(\beta_{N,p}) \,\forall\, p \in S\},$$

where $\beta_{N,p}$ denotes the composition of the Abel–Jacobi map $\iota : C(\mathbb{F}_p) \to J(\mathbb{F}_p)$ and the canonical epimorphism $J(\mathbb{F}_p) \to J(\mathbb{F}_p)/NJ(\mathbb{F}_p)$. Now $C(\mathbb{Q}) = \emptyset$ if $A(S,N) = \emptyset$ for S a finite set of primes of good reduction and N large enough [2, p. 4-5].

We can also modify this method to show that a curve can only have a specific set of rational points, as illustrated in the example below.

Example 4.1. Let X_H be the modular curve corresponding to the label 9.36.2.1. This curve has genus 2 and minimal Weierstrass equation

$$y^2 + (x^3+1)y = -5x^3 - 7.$$

The Jacobian of this curve has rank 0, and after computing $J(\mathbb{F}_p)$ for enough primes p, we find

$$J(\mathbb{Q}) = J(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}.$$

From the Weierstrass equation, we can see immediately that $X_H(\mathbb{Q})$ has at least two points, namely $(1:0:0)$ and $(0:1:0)$. We want to show that these are the only rational points on the curve.

Since every point in $J(\mathbb{Q})$ is 3-torsion, we can immediately see that we may take any $N \geq 3$, which gives us the following diagram:

$$\begin{tikzcd}
X_H(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_{p\in S} X_H(\mathbb{F}_p) \arrow[r, "\beta"] & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)
\end{tikzcd}.$$

We want to choose S such that

$$|A(S,N)| = |\{x \in \mathbb{Z}/3\mathbb{Z} \,:\, \alpha(x) \in \operatorname{im}(\beta_{N,p}) \,\forall\, p \in S\}| = 2.$$

We choose $S = \{5, 7\}$. Note that now we can choose N large enough such that the map $J(\mathbb{F}_p) \to J(\mathbb{F}_p)/NJ(\mathbb{F}_p)$ is injective for all $p \in S$.

Let $P_0 = (0:1:0)$ and let $\iota : X_H \to J$ be the map defined by $P \mapsto [P - P_0]$.

Because of the group structure of $J(\mathbb{Q})$, we know that $J(\mathbb{Q})$ contains the set $\{[0],[(1:0:0)-P_0],-[(1:0:0)-P_0]\}$. Let $p=7$, then

$$X_H(\mathbb{F}_7)=\{(0:1:0),(1:0:0),(0:0:1),(0:6:1)\},$$

hence $\iota(X_H(\mathbb{F}_7))=\{[0],[(1:0:0)-P_0],[(0:0:1)-P_0],[(0:6:1)-P_0]\}$. We see that $[(0:6:1)-P_0]=-[(0:0:1)-P_0]$, since the hyperelliptic involution of X_H swaps $(0:6:1)$ and $(0:0:1)$.
So neither $[(0:6:1)-P_0]$ nor $[(0:0:1)-P_0]$ maps to $-[(1:0:0)-P_0]$ under $\beta_{N,7}$. Therefore $\alpha([(1:0:0)-P_0])\notin \operatorname{im}(\beta_{N,7})$, which gives us $|A(S,N)|=2$. Note that we can use Equation 1 to show that both of these points are cusps.

One can check that this does indeed show that there can only be two points on the curve; we have chosen S to only contain primes of good reduction, from which it follows that the map $J(\mathbb{Q})\to J(\mathbb{F}_p)$ is injective for all $p\in S$. Since the diagram commutes, this means that there can be no point in $C(\mathbb{Q})$ whose image in $C(\mathbb{F}_p)$ reduces to $(0:1:0)$ or $(1:0:0)$.

4.1.1 Choice of S

Now that we know the general idea behind the sieve, we need to figure out an algorithm on how to best choose the set S and integer N such that $A(S,N)$ will be either empty or a specific set of points. In our example, we saw that choosing S first and basing N on that decision was the right choice.
While in the example we only really used information from the case that $p=7$, in general the Mordell-Weil sieve allows us to play different primes against one another. This is only possible if the orders of the groups $J(\mathbb{F}_p)$ have common factors. Note that this will always be the case if $J(\mathbb{Q})$ does not have trivial torsion, since then we have the inclusion $J(\mathbb{Q})_{\text{tors}}\hookrightarrow J(\mathbb{F}_p)$ for all primes p of good reduction. It is therefore helpful to fix a value B (in practice $B=100$ will suffice) and take S to be the set of primes p such that the divisors of $\#J(\mathbb{F}_p)$ are smaller or equal to B.

4.1.2 Choice of N

Now that we have chosen the set of primes S, following [2] we can forget about our original context and instead look at a much more general problem to find N. Let Γ be a finitely generated abstract abelian group of rank r and let $(G_i,\phi_i,X_i)_{i\in I}$ be a finite family of triples, where G_i is an abstract finite abelian group, $\phi_i:\Gamma\to G_i$ a surjective homomorphism and $X_i\subset G_i$ a subset. We can now generalize $A(S,N)$ by the following definition.

Definition 4.2. ([2, Definition 3.1]) Let $L\subset\Gamma$ be a subgroup of finite index and define $G_{L,i}=G_i/\phi_i(L)$. Define $X_{L,i}$ as the image of X_i in $G_{L,i}$. Let $\phi_{L,i}:\Gamma/L\to G_{L,i}$ be the induced homomorphism. Then we can define the set

$$A(L)=\{\gamma\in\Gamma/L\mid \phi_{L,i}(\gamma)\in X_{L,i}\text{ for all } i\in I\}$$

and its expected size

$$n(L) = \#(\Gamma/L) \prod_{i \in I} \frac{\#X_{L,i}}{\#G_{L,i}}.$$

In our application, we have $\Gamma = J(\mathbb{Q})$, $I = S$ and $X_p = C_p$. So we can rephrase the problem of finding a suitable N such that $A(S, N)$ is likely to be the size that we want, to finding a suitable N such that $A(N\Gamma)$ is easily computable and likely to be the desired size.

Since we need the map $C(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ to be injective, we will usually choose N to be quite large. This, however, can make our computations harder, which is why we use intermediate sets instead. We define the sequence $N_0 = 1$, $N_1 = q_1$, $N_2 = N_1 q_2$, $\ldots$, $N_m = N_{m-1} q_m = N$, where the q_j are prime divisors of N, and compute $A(N_j\Gamma)$ for each $j \in \{0, \ldots, m\}$. We want to choose the sequence (q_j) such that the $A(N_j\Gamma)$ are likely to be small, if not empty. An algorithm for finding such a suitable sequence using MAGMA is described in [2, p. 9]. As the value of N increases, $A(N\Gamma)$ will decrease in size.

All that is left to do now, is to compute the set $A(N\Gamma)$. We do so iteratively, by setting $A(N_0\Gamma) = A(\Gamma) = \{0\}$ and computing $A(N_j\Gamma)$ based on the assumption that we know $A(N_{j-1}\Gamma)$. First, we want to find the triples (G_i, ϕ_i, X_i) that can give us new information by looking at the G_i such that for its exponent e_i, we have $v_{q_j}(e_i) \geq v_{q_j}(N_j)$. For those i, we compute $G_{N_j\Gamma,i}$, $X_{N_j\Gamma,i}$ and $\phi_{N_j\Gamma,i} : \Gamma/N_j\Gamma \to G_{N_j\Gamma,i}$. We now regard all $\gamma \in A(N_{j-1}\Gamma)$ and see if their lifts in $\Gamma/N_j\Gamma$ are mapped into $X_{N_j\Gamma,i}$ by $\phi_{N_j\Gamma,i}$. A MAGMA algorithm to do this is described in [2, p. 10].

4.2 Equationless Mordell-Weil Sieve

Let $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N and let X_H be the modular curve corresponding to H. Without knowing the equations for X_H, we cannot use the classical Mordell-Weil Sieve to determine $X_H(\mathbb{Q})$, since we would need explicit points on $X_H(\mathbb{F}_p)$ in order to use that method. So, instead of using the Jacobian, we use the moduli interpretation by using another subgroup H' of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with level N' dividing N.

This equationless version of the Mordell-Weil can be described as follows: Suppose that H, H' are subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of levels N, N' respectively, such that $N' \mid N$. We want to count rational points on X_H, using the fact that we know the rational points on $X_{H'}$. If there exists a map $\pi : X_H \to X_{H'}$, we can consider the commutative diagram

$$\begin{tikzcd} X_H(\mathbb{Q}) \arrow[r, "\pi"] \arrow[d] & X_{H'}(\mathbb{Q}) \arrow[d, "\alpha"] \\ \prod_{p \in S} X_H(\mathbb{F}_p) \arrow[r, "\pi_S"] & \prod_{p \in S} X_{H'}(\mathbb{F}_p) \end{tikzcd} , \tag{3}$$

where S is a finite set of primes of good reduction. Similarly to the classical Mordell-Weil sieve, we know that $X_H(\mathbb{Q}) = \emptyset$ if the intersection of the images of α and π_S is empty.

Example 4.3. In [22], Sutherland, Rouse and Zureick-Brown used this equationless Mordell-Weil sieve to show that the curve X_H associated to the subgroup H with label 121.605.41.1. has no points over $\mathbb{Q}$. This curve has genus 41 and its Jacobian has analytic rank 41.
Reducing H modulo 11 gives a subgroup of $N_{\mathrm{ns}}(11)$, hence there exists a map

$$\pi : X_H \to X_{\mathrm{ns}}^{+}(11).$$

Note that π need not be injective. In fact, it is almost never injective. We know that $X_{\mathrm{ns}}^{+}(11)$ is an elliptic curve with Mordell-Weil group $X_{\mathrm{ns}}^{+}(11)(\mathbb{Q}) \cong \mathbb{Z}$, which allows one to create the commutative diagram as in Equation (4).
Let $p \neq 11$, be a prime. In order to show that a point on $X_H(\mathbb{F}_p)$ does not map to a point on $X_{H'}(\mathbb{F}_p)$, one needs to prove that $\rho_{E,121}(G_{\mathbb{F}_p})$ is a subgroup of H. Since this image is generated by the matrix of Frobenius, one only needs to check whether the reduction modulo 121 of the matrix A_π is conjugate to an element in H.
Define $S = \{13, 307\}$ and let R denote the generator of $X_{\mathrm{ns}}^{+}(11)(\mathbb{Q})$. Using MAGMA, one can find that any point of $X_H(\mathbb{Q})$ maps to $n \cdot R$, where $n \equiv 1$ or $5 \mod 7$, by taking $p = 13$. However, by taking $p = 307$ it follows that a point in $X_H(\mathbb{Q})$ must map to $n \cdot R$ in $X_{H'}(\mathbb{Q})$, where $n \equiv 2, 3, 4, 7, 10$ or $13 \mod 14$. So for $S = \{13, 307\}$, the intersection of the images of π_S and α must be empty, which gives $X_H(\mathbb{Q}) = \emptyset$. [22, p. 29-30].

As an observant reader might have already noticed, we cannot just use any subgroup H' for the equationless Mordell-Weil sieve. One needs to be able to find an H' of level divisible by N to obtain a map $X_H \to X_{H'}$. Preferably, $X_{H'}$ should be an elliptic curve, so that its Mordell-Weil group is finitely generated and we can use the generators to make claims about the possible points on X_H. However, it is not impossible to perform the equationless Mordell-Weil sieve on a curve X_H if $X_{H'}$ does not have genus 1.In some cases we may be able to deduce the number of X_H using only the known properties of the subgroups H and H' and the map $X_H \to X_H$. In this case, we do not even need the Mordell-Weil sieve at all. An example of this is illustrated below.

Example 4.4. Let H be the subgroup of level 18 generated by

$$H := \left\langle \begin{pmatrix} 5 & 15 \\ 15 & 14 \end{pmatrix}, \begin{pmatrix} 8 & 9 \\ 9 & 1 \end{pmatrix}, \begin{pmatrix} 13 & 12 \\ 12 & 7 \end{pmatrix} \right\rangle.$$

The corresponding curve X_H has label 18.72.5.1. Define

$$H' := \left\langle \begin{pmatrix} 2 & 3 \\ 6 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 6 \\ 6 & 8 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(9).$$

The curve $X_{H'}$ that corresponds to this group is defined by

$$y^2 + (x^3 + 1)y = -5x^3 - 7.$$

One can verify that $H \mod 9$ is a subset of H'.
We know from Example 4.1 that $X_{H'}$ has exactly two rational points, which are both cusps. Since any non-cuspidal points on $X_H(\mathbb{Q})$ must be mapped to non-cuspidal points on $X_{H'}(\mathbb{Q})$, we can conclude that all the possible points on $X_H(\mathbb{Q})$ must be cusps. Since the map $X_H \to X_{H'}$ has degree two, we deduce that $X_{H'}(\mathbb{Q})$ can have at most four cuspidal points. We compute the number of cusps on $X_H(\mathbb{Q})$ by counting the number of orbits of $H\backslash \mathrm{GL}_2(N)/U(N)$ fixed by the action $\chi_9(G_{\mathbb{Q}})$. We find that $\#(H\backslash \mathrm{GL}_2(N)/U(N))^{\chi_9(G_{\mathbb{Q}})} = 2$ and therefore $X_H(\mathbb{Q})$ contains two points.

Similarly to the classical case, one can also amend the equationless Mordell-Weil sieve to prove that a modular curve can only have a certain set of points. Information about the number of cusps and the points over finite fields can be used to determine a lower bound on the number of rational points on the curve. We can then use the equationless sieve to show that this is also an upper bound, as is shown in the example below.

Example 4.5. We consider the modular curve $X_{\mathrm{sp}}(9)$, which corresponds to the subgroup

$$\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(9)$$

Since the split Cartan group is contained in its normalizer, we know that there exists a map $X_{\mathrm{sp}}(9) \to X_{\mathrm{sp}}^{+}(9)$. Note that the normalizer of the split Cartan group is defined by

$$\left\langle \begin{pmatrix} 0 & 4 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 8 \\ 2 & 0 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(9).$$

The curve $X_{\mathrm{sp}}^{+}(9)$ is defined by the elliptic curve $y^2 + y = x^3$, which has the three rational points $\{(0:1:0), (0:0:1), (0:-1:1)\}$. Out of these points, only $(0:0:1)$ is a cusp. We count the number of cusps on $X_{\mathrm{sp}}(9)(\mathbb{Q})$ and find that there are two. Using the j-invariant map for $X_{\mathrm{sp}}^{+}(9)$, we find that $j((0:1:0)) = 8000$ and $j((0:-1:1)) = -32768$. We use this to compute elliptic curves

$$E_1 : y^2 + xy = x^3 - 9/1568x - 1/6272$$

and

$$E_2 : y^2 + xy = x^3 + 9/8624x + 1/34496$$

with these j-invariants respectively. We choose to look at the curves over $\mathbb{F}_{13}$, since E_1 and E_2 both have good reduction at this prime. Both of these elliptic curves have Frobenius matrix

$$\begin{pmatrix} 26 & -689 \\ 1 & -26 \end{pmatrix},$$

which modulo 9 reduces to

$$\begin{pmatrix} -1 & 4 \\ 1 & 1 \end{pmatrix}.$$

We check if this matrix is conjugate to an element of $C_{\mathrm{sp}}(9)$ and find that this is not the case. So $\#X_{\mathrm{sp}}(9)(\mathbb{Q}) = 2$ and both of these points are cusps.

4.3 Over Number Fields

Both the classical and the equationless Mordell-Weil sieve can be altered to work over a general number field K. For the classical Mordell-Weil sieve, we get the following commutative diagram:

$$\begin{tikzcd}
C(K) \arrow[r, "\iota"] \arrow[d] & J(K) \arrow[d, "\alpha"] \\
\prod_v C(K_v) \arrow[r, "\iota"] & \prod_v J(K_v)
\end{tikzcd} .$$

Again we can take a finite set S of places v of good reduction, giving us the commutative diagram

$$\begin{tikzcd}
C(K) \arrow[r, "\iota"] \arrow[d] & J(K) \arrow[d, "\alpha"] \\
\prod_{v\in S} C(K_v) \arrow[r, "\iota"] & \prod_{v\in S} J(K_v)
\end{tikzcd} .$$

Let $\mathfrak{p}$ be a prime ideal in K, then we can define $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, where $\mathcal{O}_K$ denotes the ring of integers of K. If $p \in \mathbb{Z}$ is a prime such that $p\mathcal{O}_K$ splits as $\mathfrak{p}\bar{\mathfrak{p}}$, we get that $C(\mathbb{F}_\mathfrak{p}) \cong C(\mathbb{F}_p)$, where $\mathbb{F}_p$ is defined in the usual sense. So if we define S to be a finite set of split primes p, we get a diagram quite similar to the one we had over $\mathbb{Q}$:

$$\begin{tikzcd}
C(K) \arrow[r, "\iota"] \arrow[d] & J(K) \arrow[d, "\alpha"] \\
\prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "\iota"] & \prod_{p\in S} J(\mathbb{F}_p)
\end{tikzcd} .$$

Again, $C(K)$ embeds into $J(K)$, so for an integer N large enough, we have the commutative diagram

$$\begin{tikzcd}
C(K) \arrow[r, "\iota"] \arrow[d] & J(K)/NJ(K) \arrow[d, "\alpha"] \\
\prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "\beta"] & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)
\end{tikzcd} .$$

We can now apply the same techniques for computing $A(S,N)$ as we did over $\mathbb{Q}$. Note that we do not need to exclusively work over split primes.

We can also apply the equationless Mordell-Weil sieve to find K-points on a modular curve. Since the map $X_H \to X_{H'}$ is defined over K, we again have the commutative diagram

$$\begin{tikzcd}
X_H(K) \arrow[r, "\pi"] \arrow[d] & X_{H'}(K) \arrow[d, "\alpha"] \\
\prod_{p\in S} X_H(\mathbb{F}_p) \arrow[r, "\pi_S"] & \prod_{p\in S} X_{H'}(\mathbb{F}_p)
\end{tikzcd} , \tag{4}$$

where we take S to be a finite set of split primes p.

Example 4.6. Recall the Example 4.1, where X_H is defined by

$$y^2 + (x^3 + 1)y = -5x^3 - 7.$$

We found that $\#X_H(\mathbb{Q}) = 2$. Now, we want to find $\#X_H(K)$, where $K = \mathbb{Q}(i)$, using the Mordell-Weil sieve.

First, we compute the the number of points on $X_H(K)$ up to a bounded height $B = 1000$, to see if we can find any points from that search. We only get back the two points over $\mathbb{Q}$ that we already found in our previous example. Our conjecture is that $X_H(K)$ contains only these two points.

We already know that for the Jacobian J_H of X_H, we have $J_H(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Let X_H^{-1} be the (-1)-twist of X_H and let $J_{H^{-1}}$ be the Jacobian of X_H^{-1}. Then the rank of $J_H(K)$ is equal to the sum of the ranks of $J_H(\mathbb{Q})$ and $J_{H^{-1}}(\mathbb{Q})$. We find that $J_{H^{-1}}(\mathbb{Q})$ has rank 2, which tells us that $J_H(K)$ must also have rank 2.

We compute the order of $[(1:0:0)-(0:1:0)]$ and find that it has order 3. Using the TorsionBound command in MAGMA, we find that $J_H(K)_{\mathrm{tors}} \cong \mathbb{Z}/3\mathbb{Z}$. Since (5) is a split prime, we have that for the primes $\mathfrak{p}$ dividing (5),

$$X_H(\mathbb{F}_{\mathfrak{p}}) = X_H(\mathbb{F}_5).$$

Similarly to what we did in the example over $\mathbb{Q}$ with $p = 7$, we find that a point that is contained in $\mathrm{im}(\alpha) \cap \mathrm{im}(\pi_5)$ cannot be the inverse of $[(1:0:0)-(0:1:0)]$. So any point in the image of π not coming from one of the two points we already found must map to a point of infinite order in $J_H(K)$.

We can use Equation 1 to compute the number of cusps on $X_H(K)$. By Corollary 2.23, we find that this must be equal to the number of cusps on $X_H(\mathbb{Q})$, which we know is 2. So any new points that we find must be non-cuspidal. We see that over $\mathbb{F}_5$ the curve has 6 points of which two are cusps. It follows that there can be at most 4 points on $X_H(K)$ that we have not yet found.

This also means that we may choose $N = 6$. We find that $\#A(5,6) = 5$ by computing $J(\mathbb{F}_5)/6J(\mathbb{F}_5)$. We increase the size of S by including all split primes up to and including 37 and compute $J(\mathbb{F}_p)/6J(\mathbb{F}_p)$ for these primes p. However, from this information, we are currently unable to deduce an upper bound for the size of $A(S,6)$. Adding non-split primes 7, 9 and 11 to S also did not provide us with any new information so far.

5 Arithmetically Maximal Subgroups

The goal of Mazur's Program B for $\mathbb{Q}(i)$ is to classify all elliptic curves defined over $\mathbb{Q}(i)$ whose Galois representation maps $\mathrm{Gal}(\overline{\mathbb{Q}(i)}/\mathbb{Q}(i))$ into $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

In order to do so, we want to define the notion of arithmetically maximal subgroups. The idea behind this is that every modular curve X_H falls into one of three categories: Either it has infinitely many points, the associated subgroup H is an arithmetically maximal subgroup, or it admits a map to a modular curve whose associated subgroup is an arithmetically subgroup.

5.1 Over $\mathbb{Q}$

Over $\mathbb{Q}$ we can define the arithmetically maximal subgroups as follows:

Definition 5.1. An open subgroup $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is said to be arithmetically maximal if

1. $\det(H) = \hat{\mathbb{Z}}^\times$;
2. H contains an element conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$;
3. $j(X_H(\mathbb{Q}))$ is finite and $j(X_G(\mathbb{Q}))$ is infinite for all $H < G \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

Note that conditions 1. and 3. ensure that our groups are indeed maximal. It is proven in [35, Proposition 3.5] that condition 2. implies that the curve X_H has non-cuspidal real points. So for a general number field K, we need not necessarily satisfy this condition. We now want to redefine the notion of arithmetically maximal subgroups over a number field in the following way.

Definition 5.2. We say that a subgroup $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N is arithmetically maximal if the following hold:

1. $[\hat{\mathbb{Z}} : \det(H)] = [K \cap \mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}]$, where $\mathbb{Q}^{\mathrm{cyc}}$ denotes the cyclotomic extension.
2. $j(X_H(K)) < \infty$ and $j(X_G(K)) = \infty$ for all $H \leq G \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

The first condition follows from the fact that we have

$$\sigma(\zeta_m) = \zeta_m^{\det(\rho_{E,m}(\sigma))}$$

for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, hence if $H = \rho_E(\mathrm{Gal}(\overline{K}/K)$, then

$$[\hat{\mathbb{Z}} : \det(H)] = [K \cap \mathbb{Q}^{\mathrm{cycl}} : \mathbb{Q}].$$

The second condition arises from the fact that for any group $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ with $X_H(K) < \infty$, we want that either H is arithmetically maximal or there exists a map $X_H \to X_G$, where G is an arithmetically maximal subgroup.

We can obtain these arithmetically maximal subgroups by enumerating all subgroups $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ such that $X_H(K)$ has infinitely many points and then computing the maximal subgroups of these groups. Note that we only have to look at curves that have genus 0 or 1, since by Falting's theorem any curve of higher genus can only have finitely many points.

5.2 Over $\mathbb{Q}(i)$

Let $K = \mathbb{Q}(i)$. Our goal is to determine all arithmetically maximal subgroups H over K. We follow a similar algorithm as described by Sutherland and Zywina in [31].
Let $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of level N and let $\Gamma \subset \mathrm{SL}_2(\hat{\mathbb{Z}})$ be a congruence subgroup from the Cummins and Pauli database, whose image in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ we will denote by Γ_N. Then we say that $H \leq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is an admissible subgroup for $\mathbb{Q}(i)$ if

1. $\Gamma_N = \pi_N(H) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$;
2. $[(\mathbb{Z}/N\mathbb{Z})^\times : \det(\pi_N(H))] = 1$ if $N = 2$ or $\gcd(N, 4) = 1$;
3. $[(\mathbb{Z}/N\mathbb{Z})^\times : \det(\pi_N(H))] = 2$ if $\gcd(N, 4) \neq 1$ and $N \neq 2$;

Note that the last two conditions come from the first property of arithmetical maximality over a number field.
Following [31], for each subgroup $\Gamma_N \subset \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ of genus 0 or 1 from the Cummins and Pauli database, we enumerate all possible groups $H \leq \mathrm{GL}_2(N)$ that satisfy the conditions listed above. Since $G := H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is normal in H, $\bar{H} \in N_G/G$ is isomorphic to $\det(H)$, where N_G denotes the normalizer of G in $\mathrm{GL}_2(N)$. So, we can enumerate all abelian subgroups A of order $\#\det(H)$ of N_G/G and check whether its inverse image has the properties listed above.
The modular curve X_H is defined over the invariant ring $\mathbb{Z}[1/N, \zeta_N]^{\det H}$ [21, p. 3]. So if N is odd and H is an admissible subgroup for $\mathbb{Q}(i)$, then X_H will be defined over $\mathbb{Q}$, whereas for admissible subgroups H with even level, X_H will be defined only over $\mathbb{Q}(i)$.

Theorem 5.3. *Up to conjugacy, there are* 441 *admissible subgroups of genus 0 and* 539 *admissible subgroups of genus 1.*

Proof. We amend the code provided by Sutherland and Zywina in [30] for their computations of admissible subgroups to fit our new conditions. In the case that N is odd, or $N = 2$, we define

```
function gl2QImagesFromSL2(H)
    GL2:=GL(2,BaseRing(H));
    SL2:=SL(2,BaseRing(H));
    assert H subset SL2;
    N:=Normalizer(GL2,H);
    Q,pi:=quo<N|H>;
    m:=#MultiplicativeGroup(BaseRing(H));
    S:=[Inverse(pi)(K‘subgroup) : K in
    Subgroups(Q:OrderEqual:=m,IsAbelian:=true)];
    return [G: G in S | gl2DetIndex(G) eq 1 and gl2Level(G) eq
    #BaseRing(H)];
end function;

function gl2QTwists(H)
```

```
    if Type(H) ne GrpMat then assert H eq CyclicGroup(1);
    return [];
    end if;
    assert -Identity(H) in H;
    N:=#BaseRing(H);
    if IsDivisibleBy(N,2) then
        if N eq 2 then
            G:=GL(2,Integers(4*#BaseRing(H)));
        else
            G:=GL(2,Integers(2*#BaseRing(H)));
        end if;
        _,pi:=ChangeRing(G,Integers(#BaseRing(H)));
        H:=sub<G|Kernel(pi),Inverse(pi)(H)>;
    else
        G:=GL(2,Integers(#BaseRing(H)));
    end if;
    S := [K`subgroup:K in Subgroups(H:IndexEqual:=2)|not
    -Identity(K`subgroup) in K`subgroup and
    gl2DetIndex(K`subgroup) eq 1];
    G:=GL(2,Integers(#BaseRing(H)));
    S := [S[i]:i in [1..#S] | #[j:j in [1..i-1]|
    IsConjugate(G,S[i],S[j])] eq 0];
    if #BaseRing(H) mod 2 eq 0 then
    S:=[ChangeRing(K,Integers(gl2Level(K))):K in S];
    end if;
    return S;
end function;
```

Note that the only thing that has changed here is that we removed the condition that H must contain an element conjugate to $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ or $\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$. In the case that $N \neq 2$ is even we amend it in the following way.

```
function gl2QImagesFromSL2(H)
    GL2:=GL(2,BaseRing(H));
    SL2:=SL(2,BaseRing(H));
    assert H subset SL2;
    N:=Normalizer(GL2,H);
    Q,pi:=quo<N|H>;
    m:=#MultiplicativeGroup(BaseRing(H)) div 2;
    S:=[Inverse(pi)(K`subgroup) : K in
    Subgroups(Q:OrderEqual:=m,IsAbelian:=true)];
    return [G: G in S | gl2DetIndex(G) eq 2 and gl2Level(G) eq
    #BaseRing(H)];
end function;
```

```
function gl2QTwists(H)
    if Type(H) ne GrpMat then assert H eq CyclicGroup(1);
    return [];
    end if;
    assert -Identity(H) in H;
    N:=#BaseRing(H);
    if IsDivisibleBy(N,2) then
        if N eq 2 then
            G:=GL(2,Integers(4*#BaseRing(H)));
        else
            G:=GL(2,Integers(2*#BaseRing(H)));
        end if;
        _,pi:=ChangeRing(G,Integers(#BaseRing(H)));
        H:=sub<G|Kernel(pi),Inverse(pi)(H)>;
    else
        G:=GL(2,Integers(#BaseRing(H)));
    end if;
    S := [K`subgroup:K in Subgroups(H:IndexEqual:=2)|not
    -Identity(K`subgroup) in K`subgroup and
    gl2DetIndex(K`subgroup) eq 2];
    G:=GL(2,Integers(#BaseRing(H)));
    S := [S[i]:i in [1..#S] | #[j:j in [1..i-1]|
    IsConjugate(G,S[i],S[j])] eq 0];
    if #BaseRing(H) mod 2 eq 0 then S:
    [ChangeRing(K,Integers(gl2Level(K))):K in S];
    end if;
    return S;
end function;
```

One can check that this indeed gives the stated amount of admissible subgroups. These groups are up to and including level 49. □

Now that we know the admissible subgroups up to conjugacy, we can check which of these groups give us a modular curve with infinitely many points.

5.2.1 Curves of genus 0

Let X_H be a modular curve of genus 0 defined over a number field K. Then X_H has a model of the form $ax^2 + by^2 = z^2$ for some $a, b \in K^\times$. If $X_H(K) \neq \emptyset$, then $X_H(K)$ is isomorphic to $\mathbb{P}^1_K$ [34, p. 7]. Let v be a place of K, then the Hilbert symbol of a and b at v is defined by

$$(a,b)_v := \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a } K_v\text{-point} \\ -1 & \text{otherwise} \end{cases}$$

Theorem 5.4. *([27, Theorem 4]) Let K be a number field and let $a, b \in K^\times$.*

Then

$$\prod_v (a,b)_v = 1.$$

Let $K = \mathbb{Q}(i)$. We will use the Hilbert product formula described above to prove whether our admissible subgroups of genus 0 have infinitely many K-points.

Theorem 5.5. *Let H be an admissible subgroup of level $N \neq 5$ and genus 0. Then $X_H(K)$ has infinitely many points.*

Proof. Since curves of genus 0 satisfy the Hasse principle, $X_H(K) \neq \emptyset$ if and only if $X_H(K_v) \neq \emptyset$ for all places v of K. We have that $X_H(K_\infty) = X_H(\mathbb{C}) \neq \emptyset$. Since a modular curve has good reduction on all primes not dividing the level, we know that $X_H(K_\mathfrak{p}) \neq \emptyset$ for $\mathfrak{p} \nmid (N)$. So suppose that $\mathfrak{p}$ divides (N). If $N = p^r$ for a non-split prime p and positive integer r, then the Hilbert product formula tells us that $X_H(K_\mathfrak{p}) \neq \emptyset$, hence $X_H(K) \neq \emptyset$. It now follows that $X_H(K)$ is isomorphic to $\mathbb{P}^1_K$.
If p is split, then either N is a power of 2, $N = 25$ or $N = 13$. If N is odd, we have $\det(\pi_N(H)) = (\mathbb{Z}/N\mathbb{Z})^\times$, which tells us that if $X_H(\mathbb{R}) \neq \emptyset$, then the curve has infinitely many rational points, and therefore infinitely many K-points, by [31, Proposition 3.1]. From [35, Proposition 3.5], we know that the existence of a point on $X_H(\mathbb{R})$ is equivalent to H containing an element that is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. For each subgroup H of level 13 or 25, we use MAGMA to verify that it indeed contains such a conjugate. For this, we use the following function from [30].

```
function GL2ContainsCC(H)
return #[h:h in H|Determinant(h) eq -1 and Trace(h) eq 0 and
GL2IsSubModule([#BaseRing(H)],GL2FixModule(sub<H|h>))] gt 0;
end function;
```

If N is even, then for every prime $\mathfrak{p}$ not dividing (N), we have $X_H(K_\mathfrak{p}) \neq \emptyset$. Since $(1+i)$ is the only prime dividing (2), the Hilbert product formula tells us that $X_H(K_{(1+i)}) \neq \emptyset$. So X_H has points everywhere locally and therefore $X_H(K) \neq \emptyset$. It again follows that $X_H(K)$ is isomorphic to $\mathbb{P}^1_K$. □

For our admissible subgroups of level 5, we cannot make such an argument, as 5 is a split prime. Instead, we need to check if these curves have points everywhere locally by checking if they have points over $\mathbb{Q}$. If this is not the case we can check for local points manually.

Proposition 5.6. *There are exactly 9 admissible subgroups H of level 5 and genus 0 such that $X_H(K)$ has infinitely many points.*

Proof. There are 12 admissible subgroups of level 5 and genus 0. For all admissible subgroups H of level 5, we use MAGMA to check whether or not H contains an element conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. This is the case for 9 groups.

There are exactly three admissible subgroups for which this condition does not hold. For those curves, we can find the corresponding models on LMFDB (see [15]). We check if these curves have points everywhere locally. Since these curves have points over $\mathbb{C}$ and have points at all primes $\mathfrak{p}$ not dividing (N), we only need to check whether points on $X_H(\mathbb{F}_5)$ lift to points on $X_H(\mathbb{Q}_5)$. None of the curves corresponding to the three subgroups have points on $\mathbb{F}_5$ that lift to $\mathbb{Q}_5$, since they are not points of $X_H(\mathbb{Z}/25\mathbb{Z})$. Hence $X_H(K) = \emptyset$. □

In [21], Rakvi enumerated all possible modular curves of genus 0 and even level that are defined over $\mathbb{Q}(i)$. Each of these curves X_H should correspond to an admissible subgroup H.

5.2.2 Curves of genus 1

While we can use Hilbert reciprocity to find the admissible subgroups that correspond to modular curves of genus 0 with infinitely many points, this same argument does not hold for subgroups of genus 1, as genus 1 curves need not satisfy the Hasse principle. Instead, we can look at the Jacobian of the curve to determine whether or not it could have infinitely many points over K.
Let H be an admissible subgroup of genus 1 and level N. Suppose that $X_H(K) \neq \emptyset$ and let J_H denote the Jacobian of X_H. Then there exists a bijection $X_H(K) \to J_H(K)$. Therefore, we can compute the rank of $J_H(K)$ to determine whether or not $X_H(K)$ has infinitely many points.

Lemma 5.7. *Let H be an admissible subgroup of genus 1 such that N is odd. Then $X_H(K) \neq \emptyset$.*

Proof. Since N is odd, we know that $\det(\pi_N(H)) = (\mathbb{Z}/N\mathbb{Z})^\times$ and therefore X_H is defined over $\mathbb{Q}$. So if H contains an element conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$, then H is one of the admissible subgroups of genus 1 mentioned in [31], hence $X_H(\mathbb{Q}) \neq \emptyset$. If H does not contain such an element, we check whether or not X_H has a cuspidal point over K. We find that any admissible subgroup $H \neq C_{\mathrm{ns}}(7)$ either contains an element conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ or has a cuspidal point over K.
Let H be the non-split Cartan group of level 7, then X_H is defined by the equation $-y^2 = 2x^4 - 14x^3 + 21x^2 + 28x + 7$ (see [17, p.2]). One can check that $(-1 : 4i : 1)$ is a point on this curve. □

Now that we know the modular curves corresponding to our admissible subgroups have at least one point over $\mathbb{Q}(i)$, we can apply the method described above to find all such curves which have infinitely many $\mathbb{Q}(i)$-points.

Theorem 5.8. *There are exactly 14 admissible subgroups H of odd level and genus 1 such that $X_H(K)$ has infinitely many points.*

Proof. These are exactly the 14 groups listed in Table 6. To find these groups, we use the code provided in [33], where we define the following function, taken from the JacobianOfXG(G) function, to find an elliptic curve isomorphic to the Jacobian of X_H:

```
function ellipticcurve(G);
 N:=#BaseRing(G);
   P:=PrimeDivisors(N);
   M:=1;
   for p in P do
       if   p eq 2 then M:=2^8*M;
       elif p eq 3 then M:=3^5*M;
       else             M:=p^2*M;
       end if;
   end for;

   D:=EllipticCurveDatabase();
   assert M lt LargestConductor(D);

   EE:= &cat[[EllipticCurve(D,N,i,1) : i in [1..
   NumberOfIsogenyClasses(D,N)]] : N in Divisors(M)];
   p:=5;
   while #EE ne 1 do
         while p in P do  p:=NextPrime(p); end while;
         ap:= (p+1)-NumberOfPointsOnXG(G,p);
         EE:= [E: E in EE | TraceOfFrobenius(E,p) eq ap];
         p:=NextPrime(p);
   end while;
   return EE[1];
end function;
```

Now for all our admissible subgroups H we determine whether or not X_H has infinitely many points by changing the base ring of the elliptic curve to $\mathbb{Q}(i)$ and computing its rank. □

We were unable to compute the admissible subgroups H of genus 1 and even level such that X_H has infinitely many $\mathbb{Q}(i)$-points. The models for these groups are not defined over $\mathbb{Q}$ and not known in literature. Since we were unable to compute these models ourselves, we could not check whether the curves contained a $\mathbb{Q}(i)$-point or not.

6 Appendix: Tables

Generators	Level	Index	Genus
$\begin{pmatrix}6&3\\0&1\end{pmatrix},\begin{pmatrix}3&5\\6&6\end{pmatrix},\begin{pmatrix}2&5\\6&5\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}6&3\\5&5\end{pmatrix}$	7	42	1
$\begin{pmatrix}5&5\\6&1\end{pmatrix},\begin{pmatrix}3&5\\6&6\end{pmatrix},\begin{pmatrix}2&5\\6&5\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}6&3\\5&5\end{pmatrix}$	7	42	1
$\begin{pmatrix}3&0\\2&1\end{pmatrix},\begin{pmatrix}4&0\\2&2\end{pmatrix},\begin{pmatrix}5&0\\6&6\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix}$	7	56	1
$\begin{pmatrix}4&0\\2&2\end{pmatrix},\begin{pmatrix}6&0\\1&1\end{pmatrix},\begin{pmatrix}5&0\\6&6\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix}$	7	56	1
$\begin{pmatrix}0&3\\2&0\end{pmatrix},\begin{pmatrix}4&0\\2&2\end{pmatrix},\begin{pmatrix}0&2\\6&0\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix}$	7	84	1
$\begin{pmatrix}10&8\\9&1\end{pmatrix},\begin{pmatrix}3&1\\1&8\end{pmatrix},\begin{pmatrix}3&5\\3&9\end{pmatrix},\begin{pmatrix}10&0\\0&10\end{pmatrix},\begin{pmatrix}10&9\\0&1\end{pmatrix},\begin{pmatrix}6&7\\1&5\end{pmatrix}$	11	55	1
$\begin{pmatrix}10&0\\0&10\end{pmatrix},\begin{pmatrix}1&8\\8&10\end{pmatrix},\begin{pmatrix}0&10\\1&0\end{pmatrix},\begin{pmatrix}2&5\\5&9\end{pmatrix},\begin{pmatrix}3&9\\9&9\end{pmatrix},\begin{pmatrix}10&3\\0&1\end{pmatrix}$	11	55	1
$\begin{pmatrix}11&0\\5&14\end{pmatrix},\begin{pmatrix}11&0\\0&1\end{pmatrix},\begin{pmatrix}9&0\\11&2\end{pmatrix},\begin{pmatrix}16&0\\0&16\end{pmatrix},\begin{pmatrix}4&0\\1&4\end{pmatrix},\begin{pmatrix}4&0\\15&13\end{pmatrix},\begin{pmatrix}11&0\\0&11\end{pmatrix},\begin{pmatrix}9&0\\4&8\end{pmatrix},\begin{pmatrix}16&0\\4&16\end{pmatrix}$	17	18	1
$\begin{pmatrix}1&0\\0&14\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}16&0\\0&16\end{pmatrix},\begin{pmatrix}1&0\\8&1\end{pmatrix},\begin{pmatrix}16&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\14&13\end{pmatrix},\begin{pmatrix}15&0\\8&8\end{pmatrix}$	17	36	1
$\begin{pmatrix}11&0\\0&1\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}16&0\\0&16\end{pmatrix},\begin{pmatrix}1&0\\8&1\end{pmatrix},\begin{pmatrix}16&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\14&13\end{pmatrix},\begin{pmatrix}15&0\\8&8\end{pmatrix}$	17	36	1
$\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}12&0\\16&2\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\2&1\end{pmatrix},\begin{pmatrix}16&0\\0&16\end{pmatrix},\begin{pmatrix}16&0\\0&1\end{pmatrix},\begin{pmatrix}13&0\\15&4\end{pmatrix}$	17	72	1
$\begin{pmatrix}13&0\\15&2\end{pmatrix},\begin{pmatrix}15&0\\3&11\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\2&1\end{pmatrix},\begin{pmatrix}16&0\\0&16\end{pmatrix},\begin{pmatrix}16&0\\0&1\end{pmatrix},\begin{pmatrix}13&0\\15&4\end{pmatrix}$	17	72	1
$\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}12&0\\16&2\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\2&1\end{pmatrix},\begin{pmatrix}16&0\\0&16\end{pmatrix},\begin{pmatrix}16&0\\0&1\end{pmatrix},\begin{pmatrix}13&0\\15&4\end{pmatrix}$	17	72	1
$\begin{pmatrix}6&44\\5&45\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}18&41\\34&32\end{pmatrix},\begin{pmatrix}29&7\\14&22\end{pmatrix},\begin{pmatrix}33&45\\3&5\end{pmatrix},\begin{pmatrix}25&21\\2&37\end{pmatrix},\begin{pmatrix}22&18\\11&1\end{pmatrix},\begin{pmatrix}22&0\\42&29\end{pmatrix}$	49	56	1

Table 1: Admissible subgroups of genus 1 corresponding to modular curves with infinitely many $\mathbb{Q}(i)$-points.

Generators	Level	Index	Genus
$\begin{pmatrix} 6 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 3 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	126	1
$\begin{pmatrix} 2 & 5 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	84	1
$\begin{pmatrix} 6 & 3 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	84	1
$\begin{pmatrix} 6 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	84	1
$\begin{pmatrix} 6 & 6 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 2 & 6 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	126	1
$\begin{pmatrix} 6 & 2 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	7	84	1
$\begin{pmatrix} 1 & 0 \\ 2 & 6 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 4 \end{pmatrix}$	7	168	1
$\begin{pmatrix} 1 & 0 \\ 2 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$	7	168	1
$\begin{pmatrix} 1 & 0 \\ 2 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 6 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$	7	168	3
$\begin{pmatrix} 1 & 0 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$	7	112	1
$\begin{pmatrix} 1 & 0 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$	7	112	1
$\begin{pmatrix} 1 & 0 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$	7	112	1
$\begin{pmatrix} 5 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 2 & 2 \end{pmatrix}$	7	168	1
$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$	7	168	3
$\begin{pmatrix} 6 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 2 & 2 \end{pmatrix}$	7	112	1
$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 2 & 2 \end{pmatrix}$	7	112	1
$\begin{pmatrix} 2 & 5 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 6 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 2 & 2 \end{pmatrix}$	7	112	1
$\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	252	1
$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 5 & 0 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	168	3
$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	168	1
$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$	7	168	3

Table 2: Arithmetically maximal subgroups of level 7

Generators	Level	Index	Genus
$\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}6&2\\0&2\end{pmatrix},\begin{pmatrix}2&0\\0&2\end{pmatrix},\begin{pmatrix}2&2\\0&4\end{pmatrix}$	7	56	1
$\begin{pmatrix}6&4\\2&0\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix},\begin{pmatrix}5&4\\2&6\end{pmatrix},\begin{pmatrix}5&2\\2&1\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix}$	7	42	1
$\begin{pmatrix}6&3\\0&1\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix},\begin{pmatrix}5&4\\2&6\end{pmatrix},\begin{pmatrix}5&2\\2&1\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix}$	7	42	1
$\begin{pmatrix}6&2\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&2\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix}$	7	168	3
$\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}6&2\\5&3\end{pmatrix},\begin{pmatrix}2&0\\0&2\end{pmatrix}$	7	168	3
$\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}6&2\\0&1\end{pmatrix},\begin{pmatrix}4&4\\0&1\end{pmatrix}$	7	168	3
$\begin{pmatrix}1&0\\0&6\end{pmatrix},\begin{pmatrix}0&3\\2&0\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix}$	7	84	1
$\begin{pmatrix}3&3\\5&3\end{pmatrix},\begin{pmatrix}1&0\\0&6\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix}$	7	56	1
$\begin{pmatrix}3&3\\5&3\end{pmatrix},\begin{pmatrix}0&3\\5&0\end{pmatrix},\begin{pmatrix}6&0\\0&6\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix}$	7	56	1

Table 3: Arithmetically maximal subgroups of level 7

Generators	Level	Index	Genus
$\begin{pmatrix}5&6\\0&1\end{pmatrix},\begin{pmatrix}8&0\\0&8\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\3&1\end{pmatrix},\begin{pmatrix}7&0\\3&4\end{pmatrix}$	9	36	1
$\begin{pmatrix}1&1\\8&1\end{pmatrix},\begin{pmatrix}0&2\\7&0\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix},\begin{pmatrix}7&0\\0&7\end{pmatrix}$	9	162	4
$\begin{pmatrix}4&4\\5&1\end{pmatrix},\begin{pmatrix}0&2\\7&3\end{pmatrix},\begin{pmatrix}5&6\\3&5\end{pmatrix},\begin{pmatrix}7&6\\3&7\end{pmatrix}$	9	162	4
$\begin{pmatrix}1&1\\8&1\end{pmatrix},\begin{pmatrix}0&2\\7&0\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix},\begin{pmatrix}7&0\\0&7\end{pmatrix}$	9	162	4
$\begin{pmatrix}1&1\\8&1\end{pmatrix},\begin{pmatrix}0&2\\7&0\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix},\begin{pmatrix}7&0\\0&7\end{pmatrix}$	9	162	4
$\begin{pmatrix}1&1\\8&1\end{pmatrix},\begin{pmatrix}0&2\\7&0\end{pmatrix},\begin{pmatrix}5&0\\0&5\end{pmatrix},\begin{pmatrix}7&0\\0&7\end{pmatrix}$	9	162	4
$\begin{pmatrix}8&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\8&0\end{pmatrix},\begin{pmatrix}8&0\\0&8\end{pmatrix},\begin{pmatrix}1&3\\3&1\end{pmatrix},\begin{pmatrix}7&6\\6&7\end{pmatrix}$	9	54	1
$\begin{pmatrix}8&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\8&0\end{pmatrix},\begin{pmatrix}8&0\\0&8\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\0&7\end{pmatrix}$	9	54	1
$\begin{pmatrix}0&8\\8&0\end{pmatrix},\begin{pmatrix}1&3\\3&1\end{pmatrix},\begin{pmatrix}8&0\\0&8\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}7&3\\3&4\end{pmatrix}$	9	36	2

Table 4: Arithmetically maximal subgroups of level 9

Generators	Level	Index	Genus
$\begin{pmatrix}8&0\\0&1\end{pmatrix}, \begin{pmatrix}1&3\\3&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}7&3\\3&4\end{pmatrix}$	9	36	2
$\begin{pmatrix}8&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\8&0\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}4&0\\0&7\end{pmatrix}$	9	54	1
$\begin{pmatrix}8&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\8&0\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}7&0\\0&7\end{pmatrix}, \begin{pmatrix}1&6\\3&1\end{pmatrix}$	9	54	2
$\begin{pmatrix}8&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\7&8\end{pmatrix}, \begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&8\\8&5\end{pmatrix}$	9	81	1
$\begin{pmatrix}8&1\\0&1\end{pmatrix}, \begin{pmatrix}4&6\\6&7\end{pmatrix}, \begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&8\\8&5\end{pmatrix}$	9	54	2
$\begin{pmatrix}0&1\\1&8\end{pmatrix}, \begin{pmatrix}4&6\\6&7\end{pmatrix}, \begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&8\\8&5\end{pmatrix}$	9	54	2
$\begin{pmatrix}8&4\\0&1\end{pmatrix}, \begin{pmatrix}5&0\\0&5\end{pmatrix}, \begin{pmatrix}7&2\\1&3\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}$	9	108	3
$\begin{pmatrix}8&4\\0&1\end{pmatrix}, \begin{pmatrix}5&0\\0&5\end{pmatrix}, \begin{pmatrix}1&5\\5&8\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}0&8\\1&0\end{pmatrix}$	9	81	1
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}7&0\\0&4\end{pmatrix}$	9	108	4
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}4&3\\6&7\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}7&0\\0&7\end{pmatrix}$	9	108	1
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}1&3\\6&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}7&3\\6&7\end{pmatrix}$	9	108	4
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}1&6\\3&14\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}7&3\\6&7\end{pmatrix}$	9	108	1
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}5&3\\3&5\end{pmatrix}, \begin{pmatrix}1&3\\3&4\end{pmatrix}, \begin{pmatrix}7&0\\0&7\end{pmatrix}$	9	108	4
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}2&0\\6&8\end{pmatrix}, \begin{pmatrix}1&6\\0&4\end{pmatrix}, \begin{pmatrix}4&3\\6&7\end{pmatrix}$	9	108	1
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}5&3\\3&5\end{pmatrix}, \begin{pmatrix}7&6\\0&7\end{pmatrix}, \begin{pmatrix}1&3\\6&1\end{pmatrix}$	9	108	4
$\begin{pmatrix}3&4\\7&6\end{pmatrix}, \begin{pmatrix}5&3\\3&5\end{pmatrix}, \begin{pmatrix}4&6\\0&1\end{pmatrix}, \begin{pmatrix}7&3\\6&4\end{pmatrix}$	9	108	1
$\begin{pmatrix}2&3\\0&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&3\\6&1\end{pmatrix}$	9	108	4
$\begin{pmatrix}8&3\\0&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}1&6\\3&4\end{pmatrix}, \begin{pmatrix}1&3\\6&1\end{pmatrix}$	9	108	4
$\begin{pmatrix}8&3\\0&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}7&3\\6&7\end{pmatrix}, \begin{pmatrix}1&3\\6&1\end{pmatrix}$	9	108	4
$\begin{pmatrix}2&3\\0&1\end{pmatrix}, \begin{pmatrix}8&0\\0&8\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}7&0\\0&4\end{pmatrix}$	9	108	4
$\begin{pmatrix}5&6\\0&1\end{pmatrix}, \begin{pmatrix}2&0\\6&8\end{pmatrix}, \begin{pmatrix}4&0\\1&7\end{pmatrix}, \begin{pmatrix}1&0\\3&1\end{pmatrix}$	9	108	1
$\begin{pmatrix}8&6\\0&1\end{pmatrix}, \begin{pmatrix}1&3\\3&2\end{pmatrix}, \begin{pmatrix}1&0\\3&4\end{pmatrix}, \begin{pmatrix}1&0\\3&1\end{pmatrix}$	9	108	1

Table 5: Arithmetically maximal subgroups of level 9

Generators	Level	Index	Genus
$\begin{pmatrix}10 & 9\\ 0 & 1\end{pmatrix}, \begin{pmatrix}8 & 6\\ 8 & 2\end{pmatrix}, \begin{pmatrix}3 & 7\\ 8 & 8\end{pmatrix}, \begin{pmatrix}5 & 4\\ 10 & 6\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	275	1
$\begin{pmatrix}10 & 9\\ 0 & 1\end{pmatrix}, \begin{pmatrix}8 & 6\\ 8 & 2\end{pmatrix}, \begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	220	8
$\begin{pmatrix}10 & 9\\ 0 & 1\end{pmatrix}, \begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}3 & 7\\ 8 & 8\end{pmatrix}, \begin{pmatrix}5 & 4\\ 10 & 6\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	165	5
$\begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}8 & 6\\ 8 & 2\end{pmatrix}, \begin{pmatrix}3 & 7\\ 8 & 8\end{pmatrix}, \begin{pmatrix}5 & 4\\ 10 & 6\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	110	1
$\begin{pmatrix}10 & 3\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 10\\ 1 & 0\end{pmatrix}, \begin{pmatrix}10 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}2 & 9\\ 9 & 8\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	275	1
$\begin{pmatrix}10 & 3\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 10\\ 1 & 0\end{pmatrix}, \begin{pmatrix}10 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	165	5
$\begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}0 & 10\\ 1 & 0\end{pmatrix}, \begin{pmatrix}10 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}2 & 9\\ 9 & 8\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	110	1
$\begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}10 & 3\\ 0 & 1\end{pmatrix}, \begin{pmatrix}10 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}2 & 9\\ 9 & 8\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	110	4
$\begin{pmatrix}7 & 0\\ 0 & 7\end{pmatrix}, \begin{pmatrix}3 & 1\\ 1 & 10\end{pmatrix}, \begin{pmatrix}10 & 3\\ 3 & 1\end{pmatrix}, \begin{pmatrix}2 & 9\\ 9 & 8\end{pmatrix}, \begin{pmatrix}10 & 0\\ 0 & 10\end{pmatrix}$	11	110	4

Table 6: Arithmetically maximal subgroups of level 11

Generators	Level	Index	Genus
$\begin{pmatrix}2 & 0\\0 & 2\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}, \begin{pmatrix}9 & 8\\0 & 3\end{pmatrix}$	13	182	8
$\begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}4 & 9\\0 & 7\end{pmatrix}, \begin{pmatrix}3 & 8\\0 & 10\end{pmatrix}, \begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}, \begin{pmatrix}3 & 5\\0 & 9\end{pmatrix}$	13	364	16
$\begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 1\\0 & 8\end{pmatrix}, \begin{pmatrix}1 & 7\\0 & 12\end{pmatrix}, \begin{pmatrix}3 & 7\\0 & 1\end{pmatrix}, \begin{pmatrix}10 & 12\\3 & 5\end{pmatrix}$	13	84	2
$\begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}4 & 9\\0 & 7\end{pmatrix}, \begin{pmatrix}3 & 8\\0 & 10\end{pmatrix}, \begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}, \begin{pmatrix}10 & 12\\3 & 5\end{pmatrix}$	13	84	2
$\begin{pmatrix}4 & 0\\0 & 4\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}, \begin{pmatrix}3 & 5\\0 & 9\end{pmatrix}$	13	364	16
$\begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}3 & 7\\0 & 1\end{pmatrix}, \begin{pmatrix}4 & 4\\1 & 11\end{pmatrix}$	13	84	2
$\begin{pmatrix}5 & 0\\0 & 5\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 11\\0 & 9\end{pmatrix}$	13	546	24
$\begin{pmatrix}1 & 11\\0 & 9\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}7 & 8\\2 & 8\end{pmatrix}$	13	84	2
$\begin{pmatrix}1 & 12\\0 & 5\end{pmatrix}, \begin{pmatrix}1 & 11\\0 & 9\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}7 & 8\\2 & 8\end{pmatrix}$	13	84	2
$\begin{pmatrix}6 & 0\\0 & 6\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}$	13	546	24
$\begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}11 & 9\\12 & 4\end{pmatrix}$	13	84	2
$\begin{pmatrix}9 & 0\\0 & 9\end{pmatrix}, \begin{pmatrix}9 & 4\\0 & 6\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}11 & 9\\12 & 4\end{pmatrix}$	13	84	2
$\begin{pmatrix}8 & 0\\0 & 8\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}9 & 2\\0 & 1\end{pmatrix}$	13	546	24
$\begin{pmatrix}9 & 2\\0 & 1\end{pmatrix}, \begin{pmatrix}8 & 5\\0 & 1\end{pmatrix}, \begin{pmatrix}12 & 0\\0 & 12\end{pmatrix}, \begin{pmatrix}12 & 6\\0 & 1\end{pmatrix}, \begin{pmatrix}11 & 9\\12 & 4\end{pmatrix}$	13	84	2

Table 7: Arithmetically maximal subgroups of level 13

Generators	Level	Index	Genus
$\begin{pmatrix}1&0\\0&6\end{pmatrix}, \begin{pmatrix}11&0\\0&14\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&0\\0&9\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\0&13\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&16\end{pmatrix}$	17	306	17
$\begin{pmatrix}11&0\\13&16\end{pmatrix}, \begin{pmatrix}1&0\\6&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&0\\6&9\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\15&13\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&16\end{pmatrix}$	17	36	1
$\begin{pmatrix}11&0\\5&14\end{pmatrix}, \begin{pmatrix}1&0\\6&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&0\\6&9\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\15&13\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&16\end{pmatrix}$	17	36	1
$\begin{pmatrix}1&0\\0&6\end{pmatrix}, \begin{pmatrix}1&0\\6&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&0\\6&9\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\15&13\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&16\end{pmatrix}$	17	36	1
$\begin{pmatrix}1&0\\0&12\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	612	33
$\begin{pmatrix}2&0\\0&12\end{pmatrix}, \begin{pmatrix}1&0\\9&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	72	1
$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\9&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	72	1
$\begin{pmatrix}1&0\\0&12\end{pmatrix}, \begin{pmatrix}1&0\\9&1\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	72	1
$\begin{pmatrix}1&0\\0&9\end{pmatrix}, \begin{pmatrix}11&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	612	33
$\begin{pmatrix}11&0\\0&9\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\9&1\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	72	1
$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}14&0\\0&6\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	1224	65
$\begin{pmatrix}15&0\\0&12\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	5
$\begin{pmatrix}15&0\\0&6\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	5
$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	1
$\begin{pmatrix}1&0\\0&8\end{pmatrix}, \begin{pmatrix}15&0\\0&6\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	1224	65
$\begin{pmatrix}15&0\\0&14\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	5
$\begin{pmatrix}1&0\\0&8\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	1
$\begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}11&0\\0&1\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	1224	65
$\begin{pmatrix}11&0\\0&13\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\15&1\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	5
$\begin{pmatrix}11&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\15&1\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	5
$\begin{pmatrix}1&0\\0&13\end{pmatrix}, \begin{pmatrix}1&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\15&1\end{pmatrix}, \begin{pmatrix}4&0\\0&2\end{pmatrix}, \begin{pmatrix}16&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}$	17	144	1
$\begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}9&0\\0&13\end{pmatrix}, \begin{pmatrix}13&0\\0&16\end{pmatrix}, \begin{pmatrix}16&0\\0&1\end{pmatrix}$	17	1224	65
$\begin{pmatrix}3&0\\16&2\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}9&0\\14&13\end{pmatrix}, \begin{pmatrix}13&0\\2&16\end{pmatrix}, \begin{pmatrix}16&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\15&1\end{pmatrix}$	17	144	5
$\begin{pmatrix}3&0\\4&9\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}9&0\\14&13\end{pmatrix}, \begin{pmatrix}13&0\\2&16\end{pmatrix}, \begin{pmatrix}16&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\15&1\end{pmatrix}$	17	144	5
$\begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&16\end{pmatrix}, \begin{pmatrix}9&0\\14&13\end{pmatrix}, \begin{pmatrix}13&0\\2&16\end{pmatrix}, \begin{pmatrix}16&0\\7&1\end{pmatrix}, \begin{pmatrix}1&0\\15&1\end{pmatrix}$	17	144	1

Table 8: Arithmetically maximal subgroups of level 17

Generators	Level	Index	Genus
$\begin{pmatrix}18&11\\0&1\end{pmatrix},\begin{pmatrix}14&1\\3&16\end{pmatrix},\begin{pmatrix}24&9\\0&1\end{pmatrix},\begin{pmatrix}14&0\\10&19\end{pmatrix},\begin{pmatrix}6&0\\20&16\end{pmatrix},\begin{pmatrix}10&22\\2&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	150	4
$\begin{pmatrix}3&16\\0&1\end{pmatrix},\begin{pmatrix}24&11\\18&1\end{pmatrix},\begin{pmatrix}14&0\\4&1\end{pmatrix},\begin{pmatrix}24&0\\0&24\end{pmatrix},\begin{pmatrix}21&10\\0&1\end{pmatrix},\begin{pmatrix}10&22\\2&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	150	8
$\begin{pmatrix}18&11\\0&1\end{pmatrix},\begin{pmatrix}19&16\\13&21\end{pmatrix},\begin{pmatrix}24&9\\0&1\end{pmatrix},\begin{pmatrix}24&5\\10&19\end{pmatrix},\begin{pmatrix}1&5\\10&21\end{pmatrix},\begin{pmatrix}10&22\\2&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	150	4
$\begin{pmatrix}18&11\\0&1\end{pmatrix},\begin{pmatrix}14&1\\3&16\end{pmatrix},\begin{pmatrix}24&9\\0&1\end{pmatrix},\begin{pmatrix}14&0\\10&19\end{pmatrix},\begin{pmatrix}6&0\\20&16\end{pmatrix},\begin{pmatrix}10&22\\2&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	150	8
$\begin{pmatrix}18&11\\0&1\end{pmatrix},\begin{pmatrix}9&11\\18&11\end{pmatrix},\begin{pmatrix}24&9\\0&1\end{pmatrix},\begin{pmatrix}14&20\\10&19\end{pmatrix},\begin{pmatrix}6&10\\5&11\end{pmatrix},\begin{pmatrix}10&22\\2&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	150	4
$\begin{pmatrix}24&24\\0&1\end{pmatrix},\begin{pmatrix}16&19\\5&18\end{pmatrix},\begin{pmatrix}1&21\\20&19\end{pmatrix},\begin{pmatrix}21&0\\10&6\end{pmatrix},\begin{pmatrix}10&17\\7&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	16
$\begin{pmatrix}4&14\\0&1\end{pmatrix},\begin{pmatrix}21&14\\20&3\end{pmatrix},\begin{pmatrix}6&16\\10&4\end{pmatrix},\begin{pmatrix}21&10\\0&1\end{pmatrix},\begin{pmatrix}10&17\\7&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}24&24\\0&1\end{pmatrix},\begin{pmatrix}1&24\\5&18\end{pmatrix},\begin{pmatrix}21&6\\20&19\end{pmatrix},\begin{pmatrix}11&10\\15&11\end{pmatrix},\begin{pmatrix}10&17\\7&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}4&14\\0&1\end{pmatrix},\begin{pmatrix}21&9\\5&18\end{pmatrix},\begin{pmatrix}11&1\\20&19\end{pmatrix},\begin{pmatrix}21&10\\0&1\end{pmatrix},\begin{pmatrix}21&0\\20&6\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}24&24\\0&1\end{pmatrix},\begin{pmatrix}21&9\\5&18\end{pmatrix},\begin{pmatrix}11&1\\20&19\end{pmatrix},\begin{pmatrix}1&10\\5&21\end{pmatrix},\begin{pmatrix}10&17\\7&17\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	16
$\begin{pmatrix}2&23\\0&1\end{pmatrix},\begin{pmatrix}24&0\\0&24\end{pmatrix},\begin{pmatrix}4&19\\0&1\end{pmatrix},\begin{pmatrix}16&20\\0&1\end{pmatrix},\begin{pmatrix}20&12\\22&7\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}7&13\\0&1\end{pmatrix},\begin{pmatrix}9&20\\20&4\end{pmatrix},\begin{pmatrix}24&4\\0&1\end{pmatrix},\begin{pmatrix}11&20\\20&6\end{pmatrix},\begin{pmatrix}20&12\\22&7\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}7&13\\0&1\end{pmatrix},\begin{pmatrix}14&10\\20&4\end{pmatrix},\begin{pmatrix}24&4\\0&1\end{pmatrix},\begin{pmatrix}6&20\\15&11\end{pmatrix},\begin{pmatrix}20&12\\22&7\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}7&13\\0&1\end{pmatrix},\begin{pmatrix}24&15\\20&4\end{pmatrix},\begin{pmatrix}24&4\\0&1\end{pmatrix},\begin{pmatrix}1&20\\10&16\end{pmatrix},\begin{pmatrix}20&12\\22&7\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}7&13\\0&1\end{pmatrix},\begin{pmatrix}4&5\\20&4\end{pmatrix},\begin{pmatrix}24&4\\0&1\end{pmatrix},\begin{pmatrix}21&20\\5&21\end{pmatrix},\begin{pmatrix}20&12\\22&7\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12
$\begin{pmatrix}2&23\\0&1\end{pmatrix},\begin{pmatrix}19&0\\20&4\end{pmatrix},\begin{pmatrix}4&19\\0&1\end{pmatrix},\begin{pmatrix}16&20\\0&20\end{pmatrix},\begin{pmatrix}21&0\\20&6\end{pmatrix},\begin{pmatrix}21&10\\10&6\end{pmatrix},$	25	300	12

Table 9: Arithmetically maximal subgroups of level 25

Generators	Level	Index	Genus
$\begin{pmatrix}20&15\\0&1\end{pmatrix},\begin{pmatrix}17&0\\18&8\end{pmatrix},\begin{pmatrix}16&9\\0&1\end{pmatrix},\begin{pmatrix}22&9\\10&25\end{pmatrix},\begin{pmatrix}19&0\\0&1\end{pmatrix},\begin{pmatrix}19&0\\18&10\end{pmatrix},\begin{pmatrix}10&0\\21&19\end{pmatrix},\begin{pmatrix}1&0\\9&1\end{pmatrix}$	27	108	4
$\begin{pmatrix}17&24\\0&1\end{pmatrix},\begin{pmatrix}20&0\\15&20\end{pmatrix},\begin{pmatrix}4&0\\6&22\end{pmatrix},\begin{pmatrix}22&9\\10&25\end{pmatrix},\begin{pmatrix}19&0\\0&1\end{pmatrix},\begin{pmatrix}19&0\\18&10\end{pmatrix},\begin{pmatrix}10&0\\21&19\end{pmatrix},\begin{pmatrix}1&0\\9&1\end{pmatrix}$	27	108	4
$\begin{pmatrix}17&24\\0&1\end{pmatrix},\begin{pmatrix}8&9\\6&20\end{pmatrix},\begin{pmatrix}1&18\\12&25\end{pmatrix},\begin{pmatrix}22&9\\10&25\end{pmatrix},\begin{pmatrix}19&0\\0&1\end{pmatrix},\begin{pmatrix}19&0\\18&10\end{pmatrix},\begin{pmatrix}10&0\\21&19\end{pmatrix},\begin{pmatrix}1&0\\9&1\end{pmatrix}$	27	108	4
$\begin{pmatrix}20&15\\0&1\end{pmatrix},\begin{pmatrix}14&18\\24&20\end{pmatrix},\begin{pmatrix}16&0\\9&1\end{pmatrix},\begin{pmatrix}7&16\\6&22\end{pmatrix},\begin{pmatrix}19&0\\0&1\end{pmatrix},\begin{pmatrix}19&0\\18&10\end{pmatrix},\begin{pmatrix}10&0\\21&19\end{pmatrix},\begin{pmatrix}1&0\\9&1\end{pmatrix}$	27	108	4

Table 10: Arithmetically maximal subgroups of level 27

Generators	Level	Index	Genus
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}11&19\\7&30\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	19
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}18&12\\7&30\end{pmatrix},\begin{pmatrix}10&40\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	19
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}39&40\\7&30\end{pmatrix},\begin{pmatrix}40&10\\11&39\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	19
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}46&33\\7&30\end{pmatrix},\begin{pmatrix}21&29\\41&9\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	19
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}4&26\\7&30\end{pmatrix},\begin{pmatrix}13&37\\33&17\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	26
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}32&47\\7&30\end{pmatrix},\begin{pmatrix}32&18\\3&47\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	19
$\begin{pmatrix}19&17\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}30&41\\0&1\end{pmatrix},\begin{pmatrix}25&5\\7&30\end{pmatrix},\begin{pmatrix}2&48\\22&28\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	392	19
$\begin{pmatrix}12&24\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}16&6\\0&1\end{pmatrix},\begin{pmatrix}29&21\\0&1\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	168	3
$\begin{pmatrix}34&23\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}22&43\\7&30\end{pmatrix},\begin{pmatrix}29&21\\0&1\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	168	3
$\begin{pmatrix}34&23\\0&1\end{pmatrix},\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}4&42\\42&4\end{pmatrix},\begin{pmatrix}29&21\\0&1\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	168	3
$\begin{pmatrix}37&25\\0&48\end{pmatrix},\begin{pmatrix}16&6\\0&1\end{pmatrix},\begin{pmatrix}11&19\\7&30\end{pmatrix},\begin{pmatrix}29&21\\0&1\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	112	1
$\begin{pmatrix}48&0\\0&48\end{pmatrix},\begin{pmatrix}16&6\\0&1\end{pmatrix},\begin{pmatrix}11&19\\7&30\end{pmatrix},\begin{pmatrix}29&21\\0&1\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	112	1
$\begin{pmatrix}12&29\\0&1\end{pmatrix},\begin{pmatrix}16&6\\0&1\end{pmatrix},\begin{pmatrix}11&19\\7&30\end{pmatrix},\begin{pmatrix}29&21\\0&1\end{pmatrix},\begin{pmatrix}31&19\\30&20\end{pmatrix},\begin{pmatrix}32&32\\45&19\end{pmatrix},\begin{pmatrix}22&28\\21&29\end{pmatrix}$	49	112	1

Table 11: Arithmetically maximal subgroups of level 49

References

[1] Alex J. Best et al. "Computing Classical Modular Forms". In: *Simons Symposia*. Springer International Publishing, 2021, pp. 131–213. ISBN: 9783030809140. DOI: 10.1007/978-3-030-80914-0_4. URL: http://dx.doi.org/10.1007/978-3-030-80914-0_4.

[2] Nils Bruin and Michael Stoll. "The Mordell–Weil sieve: proving nonexistence of rational points on curves". In: *LMS Journal of Computation and Mathematics* 13 (Aug. 2010), pp. 272–306. ISSN: 1461-1570. DOI: 10.1112/s1461157009000187. URL: http://dx.doi.org/10.1112/S1461157009000187.

[3] John Cannon et al. "HANDBOOK OF MAGMA FUNCTIONS". In: 2011. URL: https://api.semanticscholar.org/CorpusID:118154022.

[4] J. Coates and A. Wiles. "On the Conjecture of Birch and Swinnerton-Dyer". In: *Inventiones mathematicae* 39 (1977), pp. 223–252. URL: http://eudml.org/doc/142468.

[5] Henri Cohen. *An Introduction to Modular Forms*. 2018. arXiv: 1809.10907 [math.NT]. URL: https://arxiv.org/abs/1809.10907.

[6] C. Cummins and S. Pauli. "Congruence Subgroups of PSL(2, Z) of Genus Less than or Equal to 24". In: *Experimental Mathematics* 12 (Apr. 2012), pp. 243–255. DOI: 10.1080/10586458.2003.10504495.

[7] P. Deligne and M. Rapoport. "Les Schémas de Modules de Courbes Elliptiques". In: *Modular Functions of One Variable II*. Ed. by Pierre Deligne and Willem Kuijk. Berlin, Heidelberg: Springer Berlin Heidelberg, 1973, pp. 143–316. ISBN: 978-3-540-37855-6.

[8] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer New York, NY, 2005.

[9] Gerd Faltings. *Finiteness Theorems for Abelian Varieties over Number Fields*. Ed. by Gary Cornell and Joseph H. Silverman. New York, NY: Springer New York, 1986, pp. 9–26. ISBN: 978-1-4613-8655-1. DOI: 10.1007/978-1-4613-8655-1_2. URL: https://doi.org/10.1007/978-1-4613-8655-1_2.

[10] Stevan Gajović. *Curves with sharp Chabauty-Coleman bound*. 2020. arXiv: 2009.01084 [math.NT]. URL: https://arxiv.org/abs/2009.01084.

[11] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. Springer, 1977. URL: http://www.worldcat.org/oclc/2798099.

[12] Tomasz Jedrzejak. *Ranks of quadratic twists of Jacobians of generalized Mordell curves*. July 2023.

[13] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves. (AM-108), Volume 108*. Princeton: Princeton University Press, 1985. ISBN: 9781400881710. DOI: doi:10.1515/9781400881710. URL: https://doi.org/10.1515/9781400881710.

[14] Emmanuel Kowalski. *The rank of the Jacobian of modular curves: analytic methods*. 1998. URL: `https://api.semanticscholar.org/CorpusID:118063883`.

[15] The LMFDB Collaboration. *The L-functions and modular forms database*. `https://www.lmfdb.org`. [Online; accessed 26 July 2024]. 2024.

[16] B. Mazur. *Rational points on modular curves*. Ed. by Jean-Pierre Serre and Don Bernard Zagier. Berlin, Heidelberg: Springer Berlin Heidelberg, 1977, pp. 107–148. ISBN: 978-3-540-37291-2.

[17] Pietro Mercuri and Rene Schoof. *Modular forms invariant under non-split Cartan subgroups*. 2018. arXiv: `1805.06873 [math.NT]`.

[18] Steffen Müller. "Rational points on Jacobians of hyperelliptic curves". English. In: *Advances on Superelliptic Curves and Their Applications*. IOS Press, 2015.

[19] Nicola Pagani and Orsola Tommasi. *Geometry of genus one fine compactified universal Jacobians*. 2022. arXiv: `2012.09142 [math.AG]`. URL: `https://arxiv.org/abs/2012.09142`.

[20] Bjorn Poonen. *Heuristics for the Brauer-Manin obstruction for curves*. 2005. arXiv: `math/0507329 [math.NT]`.

[21] Rakvi. *Genus* 0 *Modular curves of prime power level with a point defined over number fields other than* . 2022. arXiv: `2208.02452 [math.NT]`.

[22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. "-adic images of Galois for elliptic curves over (and an appendix with John Voight)". In: *Forum of Mathematics, Sigma* 10 (2022). ISSN: 2050-5094. DOI: `10.1017/fms.2022.38`. URL: `http://dx.doi.org/10.1017/fms.2022.38`.

[23] Mohammad Sadek. *On Quadratic Twists of Hyperelliptic Curves*. 2012. arXiv: `1010.0732 [math.NT]`.

[24] Fumio Sairaiji and Takuya Yamauchi. "The Rank of Jacobian Varieties over the Maximal Abelian Extensions of Number Fields: Towards the Frey–Jarden Conjecture". In: *Canadian Mathematical Bulletin* 55.4 (2012), pp. 842–849. DOI: `10.4153/CMB-2011-140-5`.

[25] Daniel Barrera Salazar, Ariel Pacetti, and Gonzalo Tornaría. *On the* 2*-Selmer group of Jacobians of hyperelliptic curves*. 2023. arXiv: `2308.08663 [math.NT]`.

[26] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." fre. In: *Inventiones mathematicae* 15 (1971/72), pp. 259–331. URL: `https://www.wstein.org/sage_summer/bsd_comp/Serre-properties_galoisiennes_des_points_dordre_fini_des_courbes_elliptiques.pdf`.

[27] Parvati Shastri. *Reciprocity Laws: Artin-Hilbert*. URL: `https://www.bprim.org/sites/default/files/rlmain.pdf`.

[28] Aly Soliman. *A Beginner's Guide To Modular Curves.* URL: https://math.uchicago.edu/~may/REU2021/REUPapers/Soliman.pdf.

[29] K. Soundararajan. "Strong Multiplicity One for the Selberg Class". In: *Canadian Mathematical Bulletin* 47.3 (2004), pp. 468–474. DOI: 10.4153/CMB-2004-046-0.

[30] Andrew Sutherland and David Zywina. *MAGMA scripts associated to "Modular curves of prime-power level with infinitely many rational points".* 2016. URL: https://math.mit.edu/~drew/SZ16/?C=N;O=A.

[31] Andrew Sutherland and David Zywina. "Modular curves of prime-power level with infinitely many rational points". In: *Algebra and Number Theory* 11.5 (July 2017), pp. 1199–1229. ISSN: 1937-0652. DOI: 10.2140/ant.2017.11.1199. URL: http://dx.doi.org/10.2140/ant.2017.11.1199.

[32] Andrew V. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem". In: *Mathematics of Computation* 80.273 (May 2010), pp. 501–538. ISSN: 1088-6842. DOI: 10.1090/s0025-5718-2010-02373-7. URL: http://dx.doi.org/10.1090/S0025-5718-2010-02373-7.

[33] Andrew V. Sutherland. "Computing Images Of Galois Representations Attached To Elliptic Curves". In: *Forum of Mathematics, Sigma* 4 (2016), e4. DOI: 10.1017/fms.2015.33.

[34] Alexandr Zaitsev. *Forms of del Pezzo surfaces of degree 5 and 6.* 2023. arXiv: 2302.04937 [math.AG]. URL: https://arxiv.org/abs/2302.04937.

[35] David Zywina. *Possible indices for the Galois image of elliptic curves over Q.* 2022. arXiv: 1508.07663 [math.NT].