Pietro Mercuri

Rational Points on Modular Curves

Dottorato in Matematica, Roma «La Sapienza» (2014).

<http://www.bdim.eu/item?id=tesi_2014_MercuriPietro_1>

SAPIENZA
UNIVERSITÀ DI ROMA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

DIPARTIMENTO DI MATEMATICA
GUIDO CASTELNUOVO

TESI DI DOTTORATO IN MATEMATICA

Rational Points on Modular Curves

Relatore
Prof. RENÉ SCHOOF

Autore
PIETRO MERCURI

DOTTORATO DI RICERCA VITO VOLTERRA
XXVI CICLO
ANNO ACCADEMICO 2013/2014

A mio nonno

Contents

Acknowledgements

I would to give a special thank to René Schoof for the opportunity he gave me to work togheter in these years. It is a pleasure to thank Bas Edixhoven and Burcu Baran for the willingness to help me to develop this work. I would also to thank Andrea Siviero and Alberto Gioia for their support during my stay in Leiden. Finally, I would to thank Daniela Colabuono and my family for their continual sustain and encouragement, and for allowing me the freedom to pursue my own interests.

Introduction

An important theorem proved by Serre [44] in 1972 states

Theorem 0.1 (Serre)**.** *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. There is a positive constant C_E, depending on E, such that the representation*

$$\rho_{E,p}\colon \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

of the absolute Galois group $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*, is surjective for all prime numbers $p > C_E$.*

Here $\rho_{E,p}$ is the representation of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that we get identifying the group $\mathrm{GL}_2(\mathbb{F}_p)$ with the automorphism group $\operatorname{Aut}(E[p])$ of p-torsion points $E[p]$ of elliptic curve E.

From Theorem 0.1 follows naturally the formulation of *Serre's uniformity conjecture* over $\mathbb{Q}$.

Conjecture 0.2 (Serre's uniformity conjecture)**.** *There is a positive constant C such that the representation*

$$\rho_{E,p}\colon \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

of the absolute Galois group $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*, is surjective for every elliptic curve E over $\mathbb{Q}$ without complex multiplication and for all prime numbers $p > C$.*

The word "uniformity" refers to the independence of the constant C from the chosen elliptic curve, in contrast with the previous theorem.

After the results of Serre [44], Mazur [35], Bilu and Parent [10], and Bilu, Parent and Rebolledo [11], we know that Conjecture 0.2 follows from the following conjecture.

Conjecture 0.3. *There is a positive constant C such that, for all prime numbers $p > C$, the modular curve $X^+_{ns}(p)$ of level p associated to the normalizer of a non-split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$*, have no rational points, except the complex multiplication points.*

The modular curves $X^+_{ns}(p)$ are moduli spaces that parametrize elliptic curves with some p-torsion data. The complex multiplication points correspond to elliptic curves with complex multiplication and these play a special role.

The methods used to study the modular curves $X_0(p)$ of level p associated to a Borel subgroup and the modular curves $X_s^+(p)$ of level p associated to the normalizer of a split Cartan subgroup don't work for curves $X_{ns}^+(p)$. And at the moment, to my knowledge, there are not good ideas to study $X_{ns}^+(p)$ in general.

All the modular curves $X_{ns}^+(p)$ with prime level $p < 11$ have genus zero and have infinitely many rational points, so the constant C of Conjecture 0.3 is at least 11. The papers of Ligozat [33] in 1977 and Baran [7] in 2012 focus on particular cases of these non-split Cartan modular curves. Ligozat studies the genus 1 curve $X_{ns}^+(11)$, proving that it has infinitely many rational points, and Baran studies the genus 3 curve $X_{ns}^+(13)$. The Ligozat result relies on elliptic curves theory, so his method is not applicable in general to curves with higher genus, but the approach of Baran, that is more numerical, could be generalized.

In this thesis we extend the techniques of Baran [7] to $X_{ns}^+(p)$ for each prime p. For larger p the main problem is the fact that the genus of $X_{ns}^+(p)$, and hence the required number of calculations, grows rapidly with p. For example, we know that the genus of $X_{ns}^+(p)$ exceeds 5 when the level is a prime $p > 13$. We show an application of these techniques explicitly on the genus 6 modular curve $X_{ns}^+(17)$.

In the first chapter we recall some well known results that we use in the chapters two and three.

In the second chapter we explain how to compute the Fourier coefficients of a $\mathbb{Q}$-basis of modular forms of weight 2 with respect to the congruence subgroup $\Gamma_{ns}^+(p)$ starting from those of a basis of cusp forms of weight 2 with respect to $\Gamma_1(p)$. This method, that uses the representation theory of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, extends the method of Baran's paper [7].

In the third chapter we describe a way to get explicit equations of projective models for $X_{ns}^+(p)$ and $X_0^+(p) := X_0(p)/w_p$, where w_p is the Atkin-Lehner operator. This method uses the Fourier coefficients of the associated modular forms of weight 2 and the canonical embedding. The works of Galbraith [23] and [24] on the modular curves $X_0^+(p)$ have been useful to implement this method.

We study the modular curves $X_0^+(p)$ for two main reasons. First, these curves have not been studied thoroughly and there are no methods, at the moment, to determine the rational points. We only know, by Faltings' theorem, that they are finitely many, for levels p such that the genus is greater than 1. Second, in the study of these curves arise difficulties very similar to those ones that arise in the study of $X_{ns}^+(p)$, but the curves $X_0^+(p)$ are simpler than the non-split Cartan curves. Hence, the study of modular curves $X_0^+(p)$ could suggest techniques that one can extend to the study of $X_{ns}^+(p)$.

Following this philosophy, we describe a method that allows to check if there are rational points whose coordinates, in a suitable model of $X_0^+(p)$, are rational numbers with numerators and denominator bounded by 10^{10000} in absolute value. Using this method we checked, for some primes p, that there are no rational points on $X_0^+(p)$ up to the bound above, except the rational cusp and the complex multiplication points. At the moment this method works only for modular curves $X_0^+(p)$ that admit a non-constant morphism over $\mathbb{Q}$ to a genus 1 curve.

In the end of the third chapter we give some tables with some examples of the application of our techniques. We list explicit equations for a projective model of $X_0^+(p)$ when

$$p = 163, 193, 197, 211, 223, 229, 233, 241, 257, 269, 271, 281, 283,$$

and $X_{ns}^+(17)$. We list also the genus, the expected rational points and, when it is possible, the results of the search of rational points. The modular curves $X_0^+(p)$ with level a prime $p < 163$ have genus $g < 6$ and they have already been studied, see Galbraith [23] and [24].

All computations have been done using the software packages PARI and MAGMA.

Chapter 1

Background

1.1 Introduction

In this chapter we recall the definitions and the main results of topics we use in the following chapters. Each section is devoted to a different topic and include some related references.

1.2 Characters and Gauss sums

Our main references for this section are Serre [42], Diamond and Shurman [18], Shimura [45] (Section 3.6) and Berndt, Evans and Williams [9].

Definition 1.1. Let G be an finite abelian group written moltiplicatively. A *character* of G is a homomorphism from G to the multiplicative group $\mathbb{C}^*$. The *dual* of G is the group, in multiplicative notation, $\mathrm{Hom}(G, \mathbb{C}^*)$ of all characters of G with the pointwise multiplication as group operation. We denote the dual of G by $\hat{G}$. The dual group $\hat{\hat{G}}$ of $\hat{G}$ is also called the *bidual* of G.

The character identically equal to one, denoted by $\mathbb{1}$, is called the *trivial character* and is the identity element of $\hat{G}$. Since the group G is finite, we have that $\chi(g)$ is a root of unity for all $g \in G$. This implies that the group inverse χ^{-1} of χ in $\hat{G}$ is the complex conjugate $\overline{\chi}$ defined as $\overline{\chi}(g) := \overline{\chi(g)}$ for all $g \in G$. The relation between a group G and its dual $\hat{G}$ is showed by the following theorem.

Proposition 1.2. **a)** *The groups G and $\hat{G}$ are non-canonically isomorphic.*

b) *Let $\hat{\hat{G}}$ the dual group of $\hat{G}$. The map*

$$\begin{aligned} \iota \colon G &\to \hat{\hat{G}} \\ g &\mapsto \phi_g, \end{aligned}$$

defined by $\phi_g(\chi) := \chi(g)$, is a canonical group isomorphism.

For the proof see Serre [42].

Theorem 1.3 (Orthogonality relations)**.** *Let n be the order of G. Then*

$$\sum_{g\in G}\chi(g) = \begin{cases} n & \text{if } \chi = \mathbb{1} \\ 0 & \text{if } \chi \neq \mathbb{1}, \end{cases}$$

for each $\chi \in \hat{G}$ and

$$\sum_{\chi\in\hat{G}}\chi(g) = \begin{cases} n & \text{if } g = 1 \\ 0 & \text{if } g \neq 1, \end{cases}$$

for each $g \in G$.

Proof. Let us start proving the first relation. If $\chi = \mathbb{1}$ the equality is trivial. If $\chi \neq \mathbb{1}$, choose $h \in G$ such that $\chi(h) \neq 1$. Then

$$\chi(h)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(h)\chi(g) = \sum_{g\in G}\chi(hg) = \sum_{g\in G}\chi(g),$$

where in the last equality we use the substitution $gh \mapsto g$. Therefore

$$(\chi(h) - 1)\sum_{g\in G}\chi(g) = 0,$$

and, since $\chi(h) - 1 \neq 0$, we are done.

For the second relation we apply the first one to the group $\hat{G}$ and the formula follows from the isomorphism between $\hat{\hat{G}}$ and G. □

Definition 1.4. A *Dirichlet character modulo N* is a character of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$, where N is a positive integer.

Let d a positive divisor of a positive integer N. We can lift every Dirichlet character χ' modulo d to a Dirichlet character χ modulo N in the following way

$$\chi(n \mod N) := \chi'(n \mod d).$$

In other terms, if $\pi_{N,d}\colon (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$ is the classical projection, we define $\chi := \chi' \circ \pi_{N,d}$.

Definition 1.5. For each Dirichlet character χ modulo N there is a smallest positive divisor d of N such that $\chi = \chi' \circ \pi_{N,d}$ for some Dirichlet character χ' modulo d. This number d is called the *conductor* of χ. If the conductor of χ is N itself, we say that χ is *primitive*.

The fact that d is the conductor for a Dirichlet character χ modulo N is equivalent to the condition that χ is trivial on the normal subgroup

$$\ker(\pi_{N,d}) = \{n \in (\mathbb{Z}/N\mathbb{Z})^* : n \equiv 1 \mod d\}.$$

Usually one extend the Dirichlet characters to maps defined on the whole $\mathbb{Z}$ and with range $\mathbb{C}$. If χ is a Dirichlet character modulo N, this is done defining $\chi(n) = 0$ for all $n \in \mathbb{Z}$ such that $\gcd(n, N) > 1$. We point out that, if χ is a Dirichlet character modulo N, we have

$$\chi(0) = \begin{cases} 1 & N = 1 \\ 0 & N > 1. \end{cases}$$

Definition 1.6. Let N a positive integer and χ a Dirichlet character modulo N. The *Gauss sum* of the character χ is the complex number

$$G(\chi) := \sum_{n=1}^{N-1} \chi(n)\zeta_N^n,$$

where $\zeta_N = e^{\frac{2\pi i}{N}}$.

The following lemma states the basic properties of Gauss sums.

Lemma 1.7. *Let χ be a primitive Dirichlet character modulo N, then the Gauss sum $G(\chi)$ satisfies the following*

a) $\sum_{n=1}^{N-1} \chi(n)\zeta_N^{nk} = \overline{\chi}(k)G(\chi)$ *for all integers k;*

b) $G(\chi)G(\overline{\chi}) = \chi(-1)N$;

c) $\overline{G(\chi)} = \chi(-1)G(\overline{\chi})$;

d) $|G(\chi)|^2 = N$.

Proof. **a)** Let k be a fixed integer. If $k = 0$ the formula is trivial, so we assume $k \neq 0$.

If $\gcd(N, k) = 1$ then, using the substitution $nk \mapsto n$, we have

$$\sum_{n=1}^{N-1} \chi(n)\zeta_N^{nk} = \sum_{n=1}^{N-1} \chi(nk^{-1})\zeta_N^n = \chi(k^{-1}) \sum_{n=1}^{N-1} \chi(n)\zeta_N^n = \overline{\chi}(k)G(\chi),$$

where k^{-1} is the inverse of k modulo N.

Otherwise, if $\gcd(N, k) = d > 1$, we have

$$\overline{\chi}(k)G(\chi) = 0,$$

because $\overline{\chi}(k) = 0$. Let $N = dN'$ and $k = dk'r$, where r is the minimal divisor of k such that $\gcd(k', N) = 1$. In this case we have $\zeta_N^{nk} = \zeta_{N'}^{nhk'}$ and $\gcd(k', N') = 1$. Hence

$$\sum_{n=1}^{N-1} \chi(n)\zeta_N^{nk} = \sum_{n=1}^{N-1} \chi(n)\zeta_{N'}^{nhk'} = \overline{\chi}(k') \sum_{n=1}^{N-1} \chi(n)\zeta_{N'}^{nh} = \overline{\chi}(k') \sum_{n'=1}^{N'-1} \zeta_{N'}^{n'h} \sum_{\substack{n=1 \\ n \equiv n'(N')}}^{N-1} \chi(n) = 0,$$

where in the second equality we use the substitution $nk' \mapsto n$ and the last is true because χ is primitive and we are done.

b) We have

$$G(\chi)G(\overline{\chi}) = \sum_{n=1}^{N-1} G(\chi)\overline{\chi}(n)\zeta_N^n = \sum_{n=1}^{N-1}\sum_{m=1}^{N-1}\chi(m)\zeta_N^{mn}\zeta_N^n =$$
$$= \sum_{m=1}^{N-1}\chi(m)\sum_{n=1}^{N-1}\zeta_N^{n(m+1)} = \chi(-1)N,$$

where the second equality is true by part a) and the last equality is true because

$$\sum_{k=1}^{N-1}\zeta_N^{ka} = \begin{cases} N & \text{if } a \equiv 0 \mod N \\ 0 & \text{if } a \not\equiv 0 \mod N. \end{cases}$$

c) We have

$$\overline{G(\chi)} = \sum_{n=1}^{N-1}\overline{\chi}(n)\zeta_N^{-n} = \chi(-1)G(\overline{\chi}),$$

where the second equality is true by part a).

d) We have

$$|G(\chi)|^2 = G(\chi)\overline{G(\chi)} = \chi(-1)G(\chi)G(\overline{\chi}) = N,$$

where the second equality is true by part c) and the third by part b).

□

1.3 Complex representations of $\mathrm{GL}_2(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$

Our main references for this section are Piatetski-Shapiro [40] and Fulton and Harris [22].

Let $q = p^r$ with p an odd prime, $\mathbb{F}_q$ the finite field with q elements and $G = \mathrm{GL}_2(\mathbb{F}_q)$ the *general linear group* over $\mathbb{F}_q$, i.e. the multiplicative group of matrices with entries in $\mathbb{F}_q$ and with non-zero determinant.

We assume to fix a $\mathbb{F}_p$-basis, therefore, the following definitions hold up to the conjugation by the change of basis matrix. Let

$$\mathrm{SL}_2(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{F}_q, ad - bc = 1 \right\},$$

be the *special linear group* and let

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}; a, b, d \in \mathbb{F}_q; ad \neq 0 \right\},$$

be the *Borel* subgroup of G.

We start with the description of the conjugacy classes of G.

Lemma 1.8. *The conjugacy classes of G are:*

a) $q-1$ *classes, each with one element, represented by* $r_1(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$;

b) $q-1$ *classes, each with* q^2-1 *elements, represented by* $r_2(a) = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$;

c) $\frac{(q-1)(q-2)}{2}$ *classes, each with* q^2+q *elements, represented by* $r_3(a,d) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, *with* $a \neq d$;

d) $\frac{q(q-1)}{2}$ *classes, each with* q^2-q *elements, represented by* $r_4(\lambda) = \begin{pmatrix} 0 & -\mathrm{Norm}(\lambda) \\ 1 & \mathrm{Tr}(\lambda) \end{pmatrix}$, *where* λ *is a root of a monic quadratic irreducible polynomial over* $\mathbb{F}_q$.

Proof. Every element $g \in G$ has two eigenvalues that satisfy the same quadratic equation

$$\det(g - xI) = 0,$$

i.e. the characteristic equation of g. So, either they belong both to $\mathbb{F}_q$ or they don't belong to $\mathbb{F}_q$.

If they belong both to $\mathbb{F}_q$, by Jordan canonical form we have three different conjugacy classes: if the two eigenvalues are equal and the minimal polynomial is different from the characteristic polynomial we have the $q-1$ classes represented by $r_1(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, where $a \in \mathbb{F}_q^*$; if the two eigenvalues are equal and the minimal polynomial is equal to the characteristic polynomial we have the $q-1$ classes represented by $r_2(a) = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, where $a \in \mathbb{F}_q^*$; and if the two eigenvalues are different we have the $\frac{(q-1)(q-2)}{2}$ classes represented by $r_3(a,d) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, where $a, d \in \mathbb{F}_q^*$ and $a \neq d$.

If the two eigenvalues don't belong to $\mathbb{F}_q$, they belong to the unique, up to field isomorphism, quadratic extension $\mathbb{F}_{q^2}$. Since $\mathbb{F}_q$ is a finite field, then it is perfect and the eigenvalues are distinct. Let λ be one of the eigenvalues of g and v a non-zero element of $\mathbb{F}_q^2$. We have that $\{v, gv\}$ is a basis, in fact if v and gv would be linearly dependent over $\mathbb{F}_q$ we would have $gv = \alpha v$ with $\alpha \in \mathbb{F}_q$, but this is impossible because the eigenvalues of g are not in $\mathbb{F}_q$. Therefore g is in the conjugacy class of $r_4(\lambda) = \begin{pmatrix} 0 & -\mathrm{Norm}(\lambda) \\ 1 & \mathrm{Tr}(\lambda) \end{pmatrix}$, where $\mathrm{Norm}(\lambda) = \det g$ and $\mathrm{Tr}(\lambda) = \mathrm{Tr}\, g$. Since $r_4(\lambda)$ and $r_4(\lambda')$ are conjugate if and only if λ and λ' are roots of the same monic quadratic polynomial and since the elements of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ are $q^2 - q$, we have $\frac{q(q-1)}{2}$ conjugacy classes of this kind.

Since $r_1(a)$ belongs to the center of G, then each class represented by $r_1(a)$ has one element. The centralizer of $r_2(a)$ is $\left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}, x \in \mathbb{F}_q^*, y \in \mathbb{F}_q \right\}$, hence each class

represented by $r_2(a)$ has

$$[G : C_G(r_2(a))] = \frac{(q-1)^2 q(q+1)}{q(q-1)} = q^2 - 1$$

elements. The centralizer of $r_3(a,d)$ is $\left\{\begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix}, x, z \in \mathbb{F}_q^*\right\}$, hence each class represented by $r_3(a,d)$ has

$$[G : C_G(r_3(a,d))] = \frac{(q-1)^2 q(q+1)}{(q-1)^2} = q^2 + q$$

elements. Finally, the elements of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ are $q^2 - q$, so each class represented by $r_4(\lambda)$ has $q^2 - q$ elements. □

Now, we know how many irreducible representations we have to find. We know that there is a bijection between the characters μ of B and the ordered pairs (μ_1, μ_2) of Dirichlet characters $\mu_1, \mu_2 \colon \mathbb{F}_q^* \to \mathbb{C}^*$. Therefore, we have

$$\mu(\beta) = \mu_1(a)\mu_2(d),$$

for some Dirichlet characters μ_1, μ_2 and for all $\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B$.

By Piatetski-Shapiro [40] Chapter 2, Section 8, we know that the induced representation $\mathrm{Ind}_B^G \mu$ of G is irreducible if and only if $\mu_1 \neq \mu_2$, where μ corresponds to the pair (μ_1, μ_2). In this case the representation is denoted by ρ_{μ_1,μ_2} and there are $\frac{(q-1)(q-2)}{2}$ irreducible representations of this kind. On the other hand, if $\mu_1 = \mu_2$ we have $\mathrm{Ind}_B^G \mu \cong \rho_{1,\mu_1} \oplus \rho_{q,\mu_1}$, where ρ_{1,μ_1} is an irreducible representation of dimension 1 and ρ_{q,μ_1} is an irreducible representation of dimension q. There are $q-1$ irreducible representations for each kind.

Finally, we know, by Piatetski-Shapiro [40] Chapter 2, Section 13, that the remaining $\frac{q(q-1)}{2}$ irreducible representations are parametrized by Dirichlet characters $\theta \colon \mathbb{F}_{q^2}^* \to \mathbb{C}^*$ such that they don't factor through the norm map and a character of $\mathbb{F}_q$, i.e. there are not Dirichlet characters $\chi \colon \mathbb{F}_q^* \to \mathbb{C}^*$ such that $\theta = \chi \circ \mathrm{Norm}$, where $\mathrm{Norm} \colon \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ is the usual norm map. Moreover, the characters θ and θ^{-1} give isomorphic representations.

We resume the result in the following proposition.

Proposition 1.9. *With the notation as above we have that the group G has $q^2 - 1$ irreducible representations:*

a) *there are $q-1$ of dimension 1, they are denoted by ρ_{1,μ_1};*

b) *there are $q-1$ of dimension q, they are denoted by ρ_{q,μ_1};*

c) *there are $\frac{(q-1)(q-2)}{2}$ of dimension $q+1$, they are denoted by ρ_{μ_1,μ_2};*

d) *there are* $\frac{q(q-1)}{2}$ *of dimension* $q-1$*, they are denoted by* ρ_θ *and* θ *and* θ^{-1} *give isomorphic representations.*

We call the first three kinds of representations the *principal series* representations and the last one the *cuspidal* representations or *discrete series* representations.

From the irreducible representations of G we get, by restriction, the irreducible representations of $\mathrm{SL}_2(\mathbb{F}_q)$. They are classified by the following proposition.

Proposition 1.10. *With the notation as above we have that the group* $\mathrm{SL}_2(\mathbb{F}_q)$ *has* $q+4$ *irreducible representations:*

a) *there is one of dimension 1, it is the restriction of* ρ_{1,μ_1}*, every* μ_1 *gives the same representation;*

b) *there is one of dimension q, it is the restriction of* ρ_{q,μ_1}*, every* μ_1 *gives the same representation;*

c) *there are* $\frac{q-3}{2}$ *of dimension* $q+1$*, they are the restriction of* $\rho_{\mu_1,\mathbb{1}}$*, when* $\mu_1^2 \neq \mathbb{1}$ *and* μ_1 *and* μ_1^{-1} *give the same representation;*

d) *there is one of dimension* $\frac{q+1}{2}$*, it is one of the two irreducible subrepresentations of the restriction of* $\rho_{\mu_1,\mathbb{1}}$*, when* $\mu_1^2 = \mathbb{1}$ *but* $\mu_1 \neq \mathbb{1}$*;*

e) *there is one of dimension* $\frac{q+1}{2}$*, it is one of the two irreducible subrepresentations of the restriction of* $\rho_{\mu_1,\mathbb{1}}$*, when* $\mu_1^2 = \mathbb{1}$ *but* $\mu_1 \neq \mathbb{1}$*;*

f) *there are* $\frac{q-1}{2}$ *of dimension* $q-1$*, they are the restriction of* ρ_θ*, when* $\theta^2 \neq \mathbb{1}$ *and* θ *and* θ^{-1} *give the same representation and it depends only on the values of* θ *on* $(q+1)$*-th roots of unity of* $\mathbb{F}_{q^2}$*;*

g) *there is one of dimension* $\frac{q-1}{2}$*, it is one of the two irreducible subrepresentations of the restriction of* ρ_θ*, when* $\theta^2 = \mathbb{1}$ *but* $\theta \neq \mathbb{1}$*;*

h) *there is one of dimension* $\frac{q-1}{2}$*, it is one of the two irreducible subrepresentations of the restriction of* ρ_θ*, when* $\theta^2 = \mathbb{1}$ *but* $\theta \neq \mathbb{1}$*.*

1.4 Divisors and Riemann-Roch theorem

Our main reference for this section is Diamond and Shurman [18].

Definition 1.11. Let C be a compact Riemann surface. A *divisor* on C is a finite formal sum of integer multiples of points of C

$$D = \sum_{P \in C} n_P P,$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ except for finitely many P's. The free abelian group of points of C is the abelian group $\mathrm{Div}(C)$ of all divisors on C. Given two divisors

$D = \sum n_P P$ and $D' = \sum n'_P P$, we write $D \geq D'$ if $n_P \geq n'_P$ for all $P \in C$. The *degree* of a divisor D is

$$\deg(D) = \sum_{P \in C} n_P.$$

The map $\deg\colon \mathrm{Div}(C) \to \mathbb{Z}$ is a surjective homomorphism of abelian groups. We denote by $\mathrm{Div}^0(C)$ the kernel of the degree map.

Every non-zero meromorphic function f on C has an associated divisor

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P,$$

where $\mathrm{ord}_P(f)$ is the usual order of a meromorphic function at the point P of the Riemann surface C. We know by the theory of Riemann surfaces that the degree of $\mathrm{div}(f)$ is always zero.

Let D be a divisor on C, we define the *linear space* of D, also called *Riemann-Roch space* of D, denoted by $L(D)$, the $\mathbb{C}$-vector space

$$L(D) := \{f \text{ meromorphic function on } C \text{ such that } f \equiv 0 \text{ or } \mathrm{div}(f) \geq -D\}.$$

The idea of these spaces is to consider meromorphic functions with prescribed poles and zeroes or, more precisely, with at most the prescribed poles and at least the prescribed zeroes. The fact that $L(D)$ is a vector space follows by the property

$$\mathrm{ord}_P(f_1 + f_2) \geq \min\{\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)\},$$

for every $P \in C$ and for all meromorphic functions on C. Further, the dimension of these spaces is always finite and we denote it by $\ell(D)$. The computation of this dimension $\ell(D)$ is the aim of Riemann-Roch theorem below.

Let C be a compact Riemann surface of genus $g \geq 2$. Let $\Omega^1(C)$ be the $\mathbb{C}$-vector space of holomorphic differentials on C.

Theorem 1.12 (Riemann, Roch)**.** *Let D be a divisor on a curve C of genus g and let K the canonical divisor of C. Then*

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1.$$

For the proof see Griffith and Harris [25] (pag. 243) or, for a more algebraic setting, see Hartshorne [27] Theorem IV.1.3 (pag. 295).

Corollary 1.13. *Let C be a compact Riemann surface of genus g as above, let K be a canonical divisor on C and D a divisor on C. Then*

a) $\ell(K) = g$*;*

b) $\deg(K) = 2g - 2$*;*

c) *if* $\deg(D) < 0$ *then* $\ell(D) = 0$*;*

d) *if* $\deg(D) > 2g-2$ *then* $\ell(D) = \deg(D) - g + 1$.

Proof. **a)** Since $\operatorname{div}(f) \geq 0$ only for constant functions on C, then $\ell(0) = 1$. Hence, choosing $D = 0$ in Riemann-Roch formula, we have $\ell(K) = g$.

b) Choosing $D = K$ in Riemann-Roch formula and using **a)** we have $\deg(K) = 2g - 2$.

c) We suppose $\ell(D) > 0$, then there is a non-zero $f \in L(D)$. Hence $\operatorname{div}(f) \geq -D$ and taking degrees we find $\deg(D) \geq 0$ that is a contradiction.

d) The condition $\deg(D) > 2g - 2$ implies, by **b)** and **c)**, that $\ell(K - D) = 0$. Hence by Riemann-Roch theorem we have $\ell(D) = \deg(D) - g + 1$.

□

We end this section with the definition of Picard group.

Definition 1.14. Let C be a compact Riemann surface. A divisor D on C is *principal* if there is a meromorphic function f such that $\operatorname{div}(f) = D$. Two divisors D, D' on C are *linearly equivalent*, and we denote this by $D \sim D'$, if $D - D'$ is principal.

It is simple to check that the linear equivalence is an equivalence relation.

Definition 1.15. The *Picard group* of C, also called the *group class divisor* of C, denoted by $\operatorname{Pic}(C)$, is the quotient of $\operatorname{Div}(C)$ by its subgroup of pricipal divisors. The *degree zero part of the divisor class group* of C, denoted by $\operatorname{Pic}^0(C)$ is the quotient of $\operatorname{Div}^0(C)$ by its subgroup of pricipal divisors of degree zero.

1.5 The canonical map and the canonical curve

Our main references for this section are Griffith and Harris [25] and Hartshorne [27].

Definition 1.16. Let C be a Riemann surface of genus $g \geq 2$. Let $\Omega^1(C)$ be the $\mathbb{C}$-vector space of holomorphic differentials of C and let $\omega_1, \ldots, \omega_g$ be a basis of $\Omega^1(C)$. We call the map defined as

$$\begin{aligned} \varphi \colon C &\to \mathbb{P}^{g-1}(\mathbb{C}) \\ P &\mapsto [\omega_1(P), \ldots, \omega_g(P)], \end{aligned}$$

the *canonical map* and its image $\varphi(C)$ is called the *canonical curve*.

Remark 1.17. The canonical map is well defined by Riemann-Roch theorem, see Hartshorne [27] Lemma IV.5.1 (pag. 341).

To understand the next results of this section, it is useful recall two important kinds of algebraic curves.

Definition 1.18. Let C be a complex algebraic curve. The curve C is called *hyperelliptic* if there is a map $\psi_2 : C \to \mathbb{P}^1(\mathbb{C})$ of degree 2. The curve C is called *trigonal* if there is a map $\psi_3 : C \to \mathbb{P}^1(\mathbb{C})$ of degree 3.

Now we can recall the following proposition that states when the canonical map is injective.

Proposition 1.19. *With the notation as above we have that if $g \geq 2$ then the canonical map φ is injective if and only if C is not hyperelliptic. In this case we call φ the canonical embedding.*

For the proof see Hartshorne [27] Proposition IV.5.2 (pag. 341).

Since we are interested in curves with genus $g \geq 6$, either the curve C is hyperelliptic or the canonical map is injective. The following theorem classifies the different kinds of canonical curves.

Theorem 1.20 (Max Noether, Enriques, Petri)**.** *With the notation as above we have that if $g \geq 3$ and if C is not hyperelliptic, then*

a) *the canonical curve $\varphi(C)$ is entirely cut out by quadric and cubic hypersurfaces;*

b) *the canonical curve $\varphi(C)$ is entirely cut out by quadric hypersurfaces except when it is either trigonal or a plane quintic, where this last case could happen only when $g = 6$.*

For the proof see Griffith and Harris [25] (pag. 535) or Saint-Donat [41].

The following proposition tells us that, in our cases, i.e. when the genus $g \geq 6$, the canonical curve is never a complete intersection.

Proposition 1.21. *With the notation as above we have that if C has genus $g \geq 6$ then the canonical curve $\varphi(C)$ is not a complete intersection.*

Proof. If C is hyperelliptic it is enough to recall, by Hartshorne [27] Proposition IV.5.2 (pag. 341), that a hyperelliptic curve can never be a complete intersection because the canonical map is not an embedding.

If C is not hyperelliptic we know by Noether-Enriques-Petri theorem that $\varphi(C)$ cannot be contained in a hyperplane. Let $d_1, \ldots, d_{g-2}$ be the degrees of the $g-2$ hypersurfaces of complete intersection, where $d_i \geq 2$ for $i = 1, \ldots, g-2$. By Bézout theorem their intersection has degree $d = \prod_{i=1}^{g-2} d_i$. Denoting by K a canonical divisor of C, we know that $\deg(\varphi(C)) = \deg(K) = 2g-2$. We simply observe that in the lowest case, i.e. $d_1 = \cdots = d_{g-2} = 2$, we have $2g-2 < d = 2^{g-2}$ for all $g \geq 6$ and we are done. □

Finally, the proposition below gives us a lower bound for the number of quadrics we need to describe the canonical curve in the generic case.

Proposition 1.22. *With the notation as above we have that if C is not hyperelliptic, if $g \geq 6$ and if the canonical curve $\varphi(C)$ is neither trigonal nor a plane quintic, where this last case could happen only when $g = 6$, then we need at least*

$$\binom{g+1}{2} - 3(g-1)$$

quadric hypersurfaces to cut out the canonical curve $\varphi(C)$.

Proof. Let $X = \varphi(C)$ be the canonical curve of genus $g \geq 6$ and $\mathbb{P} = \mathbb{P}^{g-1}$. We have the short exact sequence

$$0 \to \mathcal{I}_X \to \mathcal{O}_{\mathbb{P}} \to \mathcal{O}_X \to 0,$$

where $\mathcal{I}_X$ is the ideal sheaf of X. Twisting by $\mathcal{O}_{\mathbb{P}}(2)$ we have the short exact sequence

$$0 \to \mathcal{I}_X(2) \to \mathcal{O}_{\mathbb{P}}(2) \to \mathcal{O}_X(2) \to 0,$$

and taking cohomology we have

$$0 \to H^0(\mathbb{P}, \mathcal{I}_X(2)) \to H^0(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(2)) \to H^0(X, \mathcal{O}_X(2)) \to H^1(\mathbb{P}, \mathcal{I}_X(2)) \to 0,$$

by Hartshorne [27] Theorem III.5.1 (pag. 225). We know, again by Hartshorne [27] Theorem III.5.1 (pag. 225), that

$$\dim H^0(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(2)) = \binom{g+1}{2},$$

is the number of homogenous monomials of degree 2 in g indeterminates. Reminding that $\mathcal{O}_X(2)$ is the invertible sheaf corresponding to divisor $2K$, where K is a canonical divisor of X, using Riemann-Roch theorem letting $D = -K$, and by Corollary 1.13, we have

$$\dim H^0(X, \mathcal{O}_X(2)) = \ell(2K) = 3(g-1).$$

Hence we can conclude

$$\dim H^0(\mathbb{P}, \mathcal{I}_X(2)) \geq \binom{g+1}{2} - 3(g-1).$$

□

1.6 Elliptic curves

Our main reference for this section is Silverman [47].

Definition 1.23. Let K be a field. An *elliptic curve over K*, denoted by E/K, is a nonsingular projective cubic plane curve with a distinguished K-rational point O called *basepoint*. The set of K-rational points of E is denoted by $E(K)$.

A *generalized Weierstrass equation* is an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

or, written in non-homogenous coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define the following quantities related to a Weierstrass equation

$$\begin{aligned}
b_2 &:= a_1^2 + 4a_2,\\
b_4 &:= 2a_4 + a_1a_3,\\
b_6 &:= a_3^2 + 4a_6,\\
b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &:= b_2^2 - 24b_4,\\
c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &:= \frac{c_4^3}{\Delta},
\end{aligned}$$

Definition 1.24. The Δ defined above is called the *discriminant* of the Weierstrass equation. The j defined above is called the *j-invariant*.

Proposition 1.25. *An elliptic curve over a field K could be defined as a generalized Weierstrass equation*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$, where the basepoint is $O = (0 : 1 : 0)$.

For the proof see Silverman [47] Proposition 3.1 (pag. 63).

Remark 1.26. The condition $a_1, a_2, a_3, a_4, a_6 \in K$ tells us that E is defined over K and the condition $\Delta \neq 0$ is equivalent to the nonsingularity of given cubic. In the non-homogenous form the basepoint O goes to infinity.

Let E/K an elliptic curve over K and $\bar{K}$ an algebraic closure of K. If char $\bar{K} \neq 2$, using the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$, we can write the Weierstrass equation as

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where $b_2, b_4, b_6 \in K$ are defined above, and we have

$$b_8 = \frac{b_2b_6 - b_4^2}{4}.$$

If $\operatorname{char} \bar{K} \neq 2, 3$, we can use the substitution $(x, y) \mapsto \left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$ and get the simpler Weierstrass equation

$$y^2 = x^3 - 27c_4x - 54c_6,$$

where $c_4, c_6 \in K$ are defined above, and we have

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

Remark 1.27. In this last case of characteristic not 2 or 3, one usually writes the Weierstrass equation of E/K as

$$y^2 = x^3 + ax + b,$$

with $a, b \in K$ and

$$\Delta = -16(4a^3 + 27b^2),$$
$$j = \frac{1728(4a)^3}{\Delta}.$$

We can get this form from the previous one using the trasformation $(x, y) \mapsto (36x, 216y)$ and taking $a = -\frac{c_4}{48}$ and $b = -\frac{c_6}{864}$.

Now we explain how one can define a group structure on an elliptic curve. We start with a lemma and a proposition.

Lemma 1.28. *Let $\bar{K}$ an algebraically closed field, C a curve of genus $g = 1$ over $\bar{K}$ and let P and Q points on C. Then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. If $(P) \sim (Q)$ there is a function f in the function field $\bar{K}(C)$ of C such that $\operatorname{div}(f) = (P) - (Q)$. But, since $g = 1$, we have $\ell((Q)) = 1$ by Corollary 1.13.d to Riemann-Roch theorem. Hence $f \in L((Q))$, but constant functions are in $L((Q))$ too, so f is constant and $P = Q$.

The converse is trivial observing that constant functions are always in $\bar{K}(C)$. □

Proposition 1.29. *Let $\bar{K}$ an algebraically closed field, E an elliptic curve over $\bar{K}$ with basepoint O. Then*

a) *for each divisor $D \in \operatorname{Div}^0(E)$ there is a unique point $P \in E(\bar{K})$ such that*

$$D \sim (P) - (O);$$

b) *the map $\psi\colon \operatorname{Div}^0(E) \to E$ defined by the association of part a) induces a bijection of sets*

$$\operatorname{Pic}^0(E) \cong E(\bar{K}).$$

Proof. **a)** Since E has genus $g = 1$, we have $\ell(D + (O)) = 1$ by Corollary 1.13.d to Riemann-Roch theorem. If $f \in \bar{K}(E)$ is a non-zero element of $L(D + (O))$, we have

$$\operatorname{div}(f) \geq -D - (O),$$

and

$$\deg(\operatorname{div}(f)) = 0.$$

Hence there is a point $P \in E(\bar{K})$ such that

$$\operatorname{div}(f) = -D - (O) + (P),$$

and this implies that

$$D \sim (P) - (O).$$

So, we have the existence, to prove the uniqueness we suppose that $P' \in E(\bar{K})$ is a point with the same property of P. It follows that

$$(P) \sim D + (O) \sim (P'),$$

and, by Lemma 1.28, we have $P = P'$.

b) That the map ψ is surjective is trivial because $\psi((P)-(O)) = P$ for all $P \in E(\bar{K})$. Now we have to prove that $\psi(D) = \psi(D')$ if and only if $D \sim D'$ for every $D, D' \in \operatorname{Div}^0(E)$. So, let $D, D' \in \operatorname{Div}^0(E)$ and $P, P' \in E(\bar{K})$ such that $\psi(D) = P$ and $\psi(D') = P'$. By definition of ψ we have

$$(P) - (P') \sim D - D',$$

it follows that $P = P'$ implies $D \sim D'$ and that $D \sim D'$ implies $(P) \sim (P')$ and by Lemma 1.28 we can conclude that $P = P'$.

□

Definition 1.30. Let $\bar{K}$ an algebraically closed field and E an elliptic curve over $\bar{K}$ with basepoint O. We define the group law on E as the one induced by the bijection of Proposition 1.29.b. With this group law the elliptic curve is an abelian group with neutral element the basepoint O.

The main fact about the group operation is the following theorem.

Theorem 1.31. *Let $\bar{K}$ an algebraically closed field and E an elliptic curve over $\bar{K}$ with basepoint O. The map sum of the group structure defined above on the elliptic curve and the map that sends an element in its inverse, with respect to the group law, are morphisms.*

For the proof see Silverman [47] Theorem 3.6 (pag. 68) or Hartshorne [27] Proposition IV.4.8 (pag. 321). Because of group structure, the most important morphisms between elliptic curves are those which respect this group structure. So, it is useful the following definition.

Definition 1.32. Let E_1 and E_2 be elliptic curves. A morphism

$$\phi\colon E_1 \to E_2,$$

such that $\phi(O) = O$ is called *isogeny*. If ϕ is non-constant then E_1 and E_2 are called *isogenous*.

All the isogenies are group homomorphisms. By Hartshorne [27] Proposition II.6.8, we know that a morphism between nonsingular curves is either constant or surjective and it is a finite morphism. If $\bar{K}(E_1)$ and $\bar{K}(E_2)$ are the function fields of E_1 and E_2 respectively, the finiteness of the morphism ϕ implies that the field extension $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$ of the pullback of $\bar{K}(E_2)$ under ϕ, has finite degree. This degree is called the *degree* of ϕ and we denote it by $\deg\phi$. The degree of a constant morphism is defined to be zero.

We denote the set of endomorphisms of E over K by $\mathrm{End}_K(E)$. It is a ring with the addition defined pointwise using the group law on E and with the composition as multiplication.

Definition 1.33. Let $\bar{K}$ an algebraically closed field, E an elliptic curve over $\bar{K}$ and N a non-zero integer. The *N-torsion subgroup* of E, denoted by $E[N]$, is the set of points of order N in E, i.e. the set

$$E[N] := \{P \in E(\bar{K}) : [N]P = O\},$$

and this is a subgroup of $E(\bar{K})$.

Theorem 1.34. *Let $\bar{K}$ an algebraically closed field with characteristic zero, E an elliptic curve over $\bar{K}$ and N a non-zero integer. Then*

a) *we have a group isomorphism*

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z};$$

b) *the endomorphism ring $\mathrm{End}_{\bar{K}}(E)$, is isomorphic either to $\mathbb{Z}$ or to an order in an imaginary quadratic field.*

For the proof see Silverman [47] Corollary 6.4 (pag. 89) for part a) and Silverman [47] Corollary 9.4 (pag. 102) for part b).

Definition 1.35. We say that an elliptic curve E/K has complex multiplication, often shortened in CM, if the endomorphism ring of E is strictly larger than $\mathbb{Z}$, i.e. if $\mathrm{char}\, K = 0$, we say that E has CM when $\mathrm{End}_K(E)$ is isomorphic to an order in an imaginary quadratic field.

1.7 Weil height and canonical height

Our main reference for this section is Silverman [47].

In this section we recall the definitions of Weil height on projective spaces and canonical height on elliptic curves. After this we recall a theorem, included in Silverman [48], that estimates the difference between the Weil height and the canonical height on elliptic curves. We use this theorem in Section 3.6.

Let us start introducing heights on projective space. Let $M_{\mathbb{Q}}$ be the set of all standard absolute values on $\mathbb{Q}$. It contains one archimedean absolute value, the classical one

$$|x|_\infty = \max\{x, -x\}, \qquad \text{for every } x \in \mathbb{Q},$$

and one non-archimedean absolute value for each prime p such that

$$\left|\frac{a}{b}p^n\right|_p = p^{-n}, \qquad \text{for every } a, b \in \mathbb{Z} \text{ coprime with } p.$$

Let K be a number field and let M_K be the set of standard absolute values on K, i.e. the absolute values on K such that their restriction to $\mathbb{Q}$ is an element of $M_{\mathbb{Q}}$. If $P = (x_0 : \cdots : x_n)$ is a point of projective space $\mathbb{P}^n(K)$, we define the *height of P relatively to K*, or simply the *height* of P, as

$$H_K(P) := \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{n_v},$$

where n_v is local degree of K at v, i.e. $n_v = [K_v : \mathbb{Q}_v]$, where K_v and $\mathbb{Q}_v$ are the completions with respect to the absolute value v of K and $\mathbb{Q}$ respectively.

Remark 1.36. That the function H_K is well defined, i.e. it is independet of the coordinates of P, follows immediatly by the product formula

$$\prod_{v \in M_K} |x|_v^{n_v} = 1,$$

for all $x \in K^*$.

If $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n\left(\overline{\mathbb{Q}}\right)$, we define the *absolute height* of P, or again simply the *height* of P, as

$$H(P) := H_K(P)^{\frac{1}{[K:\mathbb{Q}]}},$$

where K is a number field such that $P \in \mathbb{P}^n(K)$.

If we have an element $x \in K$, we define

$$H_K(x) := H_K((x : 1)),$$

and similarly, if $x \in \overline{\mathbb{Q}}$, we define

$$H(x) := H((x : 1)).$$

Definition 1.37. The *Weil height* is the function

$$\begin{aligned} h\colon \mathbb{P}^n\left(\overline{\mathbb{Q}}\right) &\to \mathbb{R} \\ P &\mapsto h(P) := \log H(P), \end{aligned}$$

which, more explicitly, is

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log\big(\max\{|x_0|_v, \ldots, |x_n|_v\}\big),$$

for some K that contains the coordinates $x_0, \ldots, x_n$ of P, where M_K is the set of standard absolute values on K and n_v is the local degree of K as above.

In the theorem 1.41 below it will be useful the archimedean part of Weil height, so we denote it by h_∞ and it is, explicitly,

$$h_\infty(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty} n_v \log\big(\max\{|x_0|_v, \ldots, |x_n|_v\}\big),$$

where M_K^∞ is the subset of M_K of all standard archimedean absolute values on K.

Remark 1.38. We are interested in the case $K = \mathbb{Q}$, when this happens the previous heights become simpler. If $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ such that $x_0, \ldots, x_n \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$ then

$$\begin{aligned} H_{\mathbb{Q}}(P) = H(P) &= \max\{|x_0|_\infty, \ldots, |x_n|_\infty\} \\ h_\infty(P) = h(P) &= \log\big(\max\{|x_0|_\infty, \ldots, |x_n|_\infty\}\big), \end{aligned}$$

this is because, for each prime p, we have $|x_i|_p < 1$ but exactly one that is equal to 1.

Now we move our attention toward elliptic curves. Let E/K be an elliptic curve over a number field K, we can define a height on it called the canonical height. In order to do this we recall that to every non-constant element f of the function field $\bar{K}(E)$ we can associate a surjective morphism, denoted again by f, such that

$$\begin{aligned} f\colon E &\to \mathbb{P}^1(\bar{K}) \\ P &\mapsto \begin{cases} (1:0) & \text{if } P \text{ is a pole of } f \\ (f(P):1) & \text{otherwise.} \end{cases} \end{aligned}$$

Now we define the *height on E relatively to f*, or simply the *height* on E, as the function

$$\begin{aligned} h_f\colon E(\bar{K}) &\to \mathbb{R} \\ P &\mapsto h_f(P) := h(f(P)), \end{aligned}$$

where h is the Weil height defined above.

Definition 1.39. Let K a number field, E/K an elliptic curve and $f \in K(E)$ a non-constant even function. The *canonical height*, sometimes called *Néron-Tate height*, is the function

$$\begin{aligned} \hat{h}\colon E(\bar{K}) &\to \mathbb{R} \\ P &\mapsto \hat{h}(P) := \frac{1}{\deg f} \lim_{n\to\infty} 4^{-n} h_f(\lfloor 2^n \rfloor P). \end{aligned}$$

Remark 1.40. The canonical height exists and is well defined, i.e. it is independent of the choice of f, by Silverman [47] Proposition 9.1.

The following theorem gives us an estimate of the difference between the two heights.

Theorem 1.41. *Let K a number field and E/K an elliptic curve given by the Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, a_2, a_3, a_4, a_6 \in K$. Let Δ_E the discriminant of E and j_E the j-invariant of E. Let μ the function defined as

$$\mu(E) := \frac{1}{12}h(\Delta_E) + \frac{1}{12}h_\infty(j_E) + \frac{1}{2}h_\infty\left(\frac{a_1^2 + 4a_2}{12}\right) + \frac{1}{2}\log \varepsilon_E,$$

where

$$\varepsilon_E := \begin{cases} 2 & \text{if } a_1^2 + 4a_2 \neq 0 \\ 1 & \text{if } a_1^2 + 4a_2 = 0. \end{cases}$$

Then for all $P \in E(\bar{K})$ we have

$$-\frac{1}{24}h(j_E) - \mu(E) - 0.973 \leq \hat{h}(P) - \frac{1}{2}h(P_x) \leq \mu(E) + 1.07,$$

where P_x is the x-coordinate of P.

For the proof of this theorem see Silverman [48].

1.8 Modular forms and automorphic forms

Our main reference for this section is Diamond and Shurman [18].

Before to define modular forms, we recall some preliminaries notions.

Definition 1.42. We call the *complex upper half-plane* the set

$$\mathcal{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\},$$

we call *cusps* the elements of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ and we call the *extended complex half-plane* the set

$$\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\},$$

i.e. the complex half-plane with the cusps.

The term "cusp" and the reason to their use come from the geometric side of this theory and we will explain this later. Usually we denote by z elements of $\mathbb{C}$, by τ elements of $\mathcal{H}$ and by s the cusps.

We have the multiplicative matrix group

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

acts on $\mathcal{H}^*$. In fact we define

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} &\to \mathcal{H} \\ (\gamma, \tau) &\mapsto \gamma\tau := \frac{a\tau + b}{c\tau + d}, \end{aligned}$$

if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and this action is well defined because

$$\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}\,\tau}{|c\tau + d|^2}.$$

But this action extends to cusps $\mathbb{P}^1(\mathbb{Q})$ and so we have an action on $\mathcal{H}^*$.

Remark 1.43. Actually, we can define, on $\mathcal{H}$, an action of

$$\mathrm{GL}_2(\mathbb{R})^+ = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}; ad - bc > 0 \right\},$$

in the same way, i.e. $g\tau = \frac{a\tau+b}{c\tau+d}$ for every $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+$. But we cannot extend this action to $\mathcal{H}^*$.

It is known, for example by Apostol [1], that the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

generate $\mathrm{SL}_2(\mathbb{Z})$. These matrices correspond to trasformations $\tau \mapsto \tau + 1$ and $\tau \mapsto -\frac{1}{\tau}$ on $\mathcal{H}$ respectively. We also have that T generates the stabilizer of ∞.

Definition 1.44. Let N be a positive integer. The *principal congruence subgroup of level N* is the subgroup $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ defined as

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

where the congruence relation is taken entrywise. A *congruence subgroup* Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subset \Gamma$ for some positive integer N. In this case we say that Γ is a *congruence subgroup of level N*.

Remark 1.45. It is trivial that $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Since $\Gamma(N)$ is the kernel of the natural group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 1.46. *For every positive integer N, the natural group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective and the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite.*

Proof. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ is a lift of an element $\bar{\gamma} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have that $\gcd(c, d, N) = 1$. In fact, if $\gcd(c, d, N) = k > 1$ then $1 = \det \gamma = ad - bc = k(ad' - bc')$, but $k > 1$ and $ad' - bc' \in \mathbb{Z}$, contradiction.

Actually we can choose c and d such that $\gcd(c, d) = 1$. If $\gcd(c, d) = k' > 1$, assuming $c \neq 0$, we can choose, by Chinese Remainder Theorem, $d'' = d + tN$ where

$$t \equiv \begin{cases} 1 \mod p & \text{if } p \text{ is a prime such that } p \mid k' \\ 0 \mod p & \text{if } p \text{ is a prime such that } p \mid c \text{ but } p \nmid k'. \end{cases}$$

If $c = 0$ in a similar way we can choose $d'' = 1$.

But fixed c and d coprime, it follows by Bézout identity that there are x and y such that $ax - by = 1$. If

$$x \equiv a + t \mod N,$$

then

$$y \equiv c^{-1}((a + t)d - 1) \mod N.$$

It is well known that if (x, y) is a solution for $ax - by = 1$, then also $(x - k''c, y - k''d)$ is a solution for it, for all $k'' \in \mathbb{Z}$; so if we take

$$k'' \equiv c^{-1}t \mod N,$$

we have

$$\begin{aligned} x - k''c &\equiv a + t - t \equiv a \mod N \\ y - k''d &\equiv c^{-1}((a + t)d - 1) - c^{-1}td \equiv c^{-1}(ad - 1) \equiv b \mod N. \end{aligned}$$

Hence, choosing $a' = x - k''c$ and $b' = y - k''d$, we have a lift $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and we proved the surjectivity of the map.

To show that the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite, it is enough to observe that $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ by surjectivity just proved. □

It follows, by the previous lemma, that every congruence subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$. Two of the most important congruence subgroup are

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

and

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

where the $*$ means "any". It is clear that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$ and this shows that they are congruence subgroups indeed.

Definition 1.47. Let $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 1\}$ be the complex upper half-plane and $f\colon \mathcal{H} \to \mathbb{C}$ a complex valued function on it. For every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and for every integer k, we define the *weight-k operator* $[\gamma]_k$ as

$$(f[\gamma]_k)(\tau) := (c\tau + d)^{-k} f(\gamma\tau),$$

if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\tau \in \mathcal{H}$.

Remark 1.48. Since the factor $c\tau+d$ has not zeroes or poles for $\tau \in \mathcal{H}$ and $c, d \in \mathbb{Z}$, if f is meromorphic, then $f[\gamma]_k$ is meromorphic too. For the same reason we have that if f is holomorphic, then $f[\gamma]_k$ is holomorphic.

Remark 1.49. One can define the weight-k operator for more general matrices in the following way

$$(f[\gamma]_k)(\tau) := \det(\gamma)^{\frac{k}{2}}(c\tau + d)^{-k} f(\gamma\tau),$$

for every $\gamma \in \mathrm{GL}_2(\mathbb{R})^+$, where $\mathrm{GL}_2(\mathbb{R})^+$ is the group of matrices with real entries and positive determinant. Sometimes it is convenient to put the normalization factor $\det(\gamma)^{k-1}$ instead of $\det(\gamma)^{\frac{k}{2}}$, but we work mainly with forms of weight 2 so this choice doesn't matter in our work.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Since $\Gamma(N) \subset \Gamma$, we konw that there is a minimal $h \in \mathbb{Z}_{>0}$ such that the matrix $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$. Hence, if a function f satisfies the relation $f[\gamma]_k = f$ for all $\gamma \in \Gamma$, i.e. f is weight-k invariant with respect to Γ, we have that f is $h\mathbb{Z}$-periodic and this impies that f has a Fourier expansion to the infinity. The reason is the following. Denoting by $D = \{z \in \mathbb{C} : |z| \leq 1\}$ the complex unit disk and by $D' = D \setminus \{0\}$ the punctured unit disk, we know, by complex analysis, that the map

$$\begin{aligned} \mathcal{H} &\to D' \\ \tau &\mapsto e^{\frac{2\pi i \tau}{h}} = q, \end{aligned}$$

is $h\mathbb{Z}$-periodic, holomorphic and surjective. Hence there is a map

$$\begin{aligned} g\colon D' &\to \mathbb{C} \\ q &\mapsto g(q) := f\left(\frac{h \log q}{2\pi i}\right), \end{aligned}$$

that is well defined, by periodicity of f, and meromorphic, if f it is. We also have that g is holomorphic is f it is. This impies that g has a Laurent expansion at zero $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for all $q \in D'$. Since $|q| = e^{-2\pi \operatorname{Im}\tau}$, we have

$$\lim_{\operatorname{Im}\tau \to +\infty} q = 0,$$

so we say that f is *meromorphic at* ∞ if g extends meromorphically at $q = 0$, i.e. if the Laurent expansion has only finitely many non-zero a_n with $n < 0$. Similarly, we say that f is *holomorphic at* ∞ if g extends holomorphically at $q = 0$, i.e. if the Laurent expansion is such that $a_n = 0$ for $n < 0$. This Laurent expansion is often called *q-expansion* in this setting.

Remark 1.50. If f is weight-k invariant with respect to a congruence subgroup Γ, then $f[\alpha]_k$ is weight-k invariant with respect to $\alpha^{-1}\Gamma\alpha$, for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. That $\alpha^{-1}\Gamma\alpha$ is a congruence subgroup is trivial.

Definition 1.51. Let $f\colon \mathcal{H} \to \mathbb{C}$ a function, Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and k an integer. We call f a *automorphic form of weight k with respect to* Γ if

1. f is meromorphic on $\mathcal{H}$;
2. $f[\gamma]_k = f$ for all $\gamma \in \Gamma$;
3. $f[\alpha]_k$ is meromorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

The $\mathbb{C}$-vector space of all automorphic forms of weight k with respect to the congruence subgroup Γ is denoted by $\mathcal{A}_k(\Gamma)$.

Last condition, also called *meromorphy at cusps*, makes sense by remark 1.50 and is necessary to keep finite dimensional the vector space of automorphic forms. A modular form is just a holomorphic automorphic form, holomorphic also at cusps. More formally

Definition 1.52. Let $f\colon \mathcal{H} \to \mathbb{C}$ a function, Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and k an integer. We call f a *modular form of weight k with respect to* Γ if

1. f is holomorphic on $\mathcal{H}$;
2. $f[\gamma]_k = f$ for all $\gamma \in \Gamma$;
3. $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

The $\mathbb{C}$-vector space of all modular forms of weight k with respect to the congruence subgroup Γ is denoted by $\mathcal{M}_k(\Gamma)$.

A cusp form is a modular form that vanishes at cusps, or more formally

Definition 1.53. Let f a modular form of weight k with respect to the congruence subgroup Γ. We call f a *cusp form* if $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. The $\mathbb{C}$-vector space of all cusp forms of weight k with respect to the congruence subgroup Γ is denoted by $\mathcal{S}_k(\Gamma)$ and this is a subspace of $\mathcal{M}_k(\Gamma)$.

Remark 1.54. The third condition of definitions 1.51 and 1.52 and the condition of definition 1.53 are written independently of the congruence subgroup Γ, but it is enough to check the condition for the finitely many representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma$.

Remark 1.55. Let f a modular form of weight k with respect to the congruence subgroup Γ. For a fixed cusp s, possibly $s = \infty$, we don't have a unique Fourier expansion of f at s. If $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\alpha\infty = s$, we have the Fourier expansion of f at s defined as the Fourier expansion of $f[\alpha]_k$ at ∞. But if $\beta = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ with $j \in \mathbb{Z}$, we have $\pm\alpha\beta\infty = s$ too and $(f[\pm\alpha\beta]_k)(\tau) = (\pm 1)^k (f[\alpha]_k)(\tau + j)$. So, if h is the smallest positive integer such that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \alpha^{-1}\Gamma\alpha$, we have

$$(f[\alpha]_k)(\tau) = \sum_{n=0}^{\infty} a_n q^n,$$

where $q = e^{\frac{2\pi i \tau}{h}}$, but, since $e^{\frac{2\pi i(\tau+j)}{h}} = e^{\frac{2\pi i j}{h}} q$, we have also

$$(f[\pm\alpha\beta]_k)(\tau) = (\pm 1)^k \sum_{n=0}^{\infty} a_n \zeta_h^{nj} q^n,$$

where $\zeta_h = e^{\frac{2\pi i}{h}}$ is the h-th root of unity. All these expansions are admissible Fourier expansions for f at s. Hence, if k is odd, the value of f at s is not well defined, but it makes sense to ask whether f vanishes at s, i.e. to ask whether $a_0 = 0$.

1.9 Modular curves

The main reference for this section is Diamond and Shurman [18].

There are three different ways to define a modular curves: the complex analytic, the algebraic and the moduli space setting. We briefly recall these three points of view.

Using the complex analysis we can define the modular curves as Riemann surfaces.

Definition 1.56. Let $\mathcal{H}^*$ the extended upper half-plane and Γ a congruence subgroup of level N as in Section 1.8 above. We define

$$Y(\Gamma) := \Gamma\backslash\mathcal{H},$$
$$X(\Gamma) := \Gamma\backslash\mathcal{H}^*.$$

If $\Gamma = \Gamma(N), \Gamma_0(N), \Gamma_1(N)$ we denote the sets above respectively by $Y(N), Y_0(N)$, $Y_1(N)$ and $X(N), X_0(N), X_1(N)$.

Proposition 1.57. *Let $\mathcal{H}^*$ the extended upper half-plane and Γ a congruence subgroup of level N as in Section 1.8 above. The set $Y(\Gamma)$ have a structure of connected Riemann surface and the set $X(\Gamma)$ have a structure of compact connected Riemann surface.*

For the proof see Diamond and Shurman [18] Chapter 2.

Remark 1.58. The reason to introduce the cusps is to get the compactness property.

This point of view allows to use many transcendental tools to study modular curves. For example we know that ratios of modular forms of same weight with respect to the congruence subgroup Γ are well defined functions on the modular curve $X(\Gamma)$.

The algebraic setting allows to define the modular curves over algebraic extensions of $\mathbb{Q}$ or $\mathbb{Q}$ itself in some cases. Using this point of view, one can study algebraic and arithmetic properties of modular curves. This approach uses Galois theory and the correspondence between isomorphism classes over K of projective algebraic curves over K and conjugacy classes over K of function fields over K, where K is a field. See Diamond and Shurman [18] Chapter 7 for more details.

Nevertheless, the more interesting point of view is to see the modular curves as moduli spaces of elliptic curves with some torsion data.

Let E an elliptic curve over $\bar{\mathbb{Q}}$ and N a positive integer. By Section 1.6, we know there is a group isomorphism

$$\phi\colon E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and let N be a positive integer. We define a relation on the set of ordered pairs (E, ϕ), where E is an elliptic curve over $\bar{\mathbb{Q}}$ and ϕ is the isomorphism above for the fixed N, i.e. it is a choice of a basis for the N-torsion points of E. We have

$$(E, \phi) \sim (E', \phi')$$

if and only if the following two conditions hold:

1. there is a curve isomorphism
$$\iota\colon E \to E';$$
2. there is a matrix $h \in H$ such that the following diagram commutes
$$\begin{array}{ccc} E[N] & \xrightarrow{\phi} & \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle h} \\ E'[N] & \xrightarrow[\phi']{} & \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}\,. \end{array}$$

It is simple to check that the relation just defined is an equivalence relation.

Definition 1.59. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and let N be a positive integer. The modular curve associated to H is the set

$$S(H) := \{(E, \phi)\}/\sim,$$

where the pairs (E, ϕ) and the equivalence relation $\sim$ are defined above.

We know that the set $S(H)$ has a structure of algebraic curve defined over an algebraic extension of $\mathbb{Q}$ and a structure of Riemann surface when it is defined over $\mathbb{C}$, and these structures are the same we talk above. We can compactify $S(H)$ adding the cusps and we denote the new curve as X_H. The cusps could be seen as generalized elliptic curves. See Deligne and Rapoport [17] for more details about this topic.

We can define what a rational point on $S(H)$ is, using the action of absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on pairs (E, ϕ). If $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ we define this action as $(E, \phi)^\sigma := (E^\sigma, \phi^\sigma)$. Here E^σ is the action of σ on coefficients of Weierstrass equation defining E and the action on ϕ is $\phi^\sigma := \phi \circ \sigma^{-1}$.

If E is defined over $\mathbb{Q}$, the action of $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on E is just the action of σ on $E(\bar{\mathbb{Q}})$, i.e. if $P = (x, y) \in E(\bar{\mathbb{Q}})$ then $P^\sigma := (\sigma(x), \sigma(y))$. It follows that if $P \in E[N]$ then $P^\sigma \in E[N]$.

Definition 1.60. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, let N be a positive integer and let $S(H)$ the modular curve associated to H as above. A point on $S(H)$ is *rational* if it is invariant with respect to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, i.e. if $(E, \phi)^\sigma \sim (E, \phi)$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. A point on $S(H)$ is *integral* if the j-invariant of the isomorphism class of E corresponding to that point belongs to $\mathbb{Z}$.

Using the description above, the rationality condition just defined become:

1. there is a curve isomorphism

$$\iota \colon E \to E^\sigma;$$

2. there is a matrix $h \in H$ such that the following diagram commutes

$$\begin{array}{ccc} E[N] & \xrightarrow{\phi} & \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle h} \\ E^\sigma[N] & \xrightarrow[\phi^\sigma]{} & \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \,. \end{array}$$

It is trivial that the two conditions are satisfied if and only if E is defined over $\mathbb{Q}$, hence we have $E^\sigma = E$ and $\iota = \mathrm{id}_E$, and $\phi \circ \sigma^{-1} \circ \phi^{-1} \in H$.

1.10 Order of automorphic forms and differentials

The main reference for this section is Diamond and Shurman [18].

We are able to compute the order of an automorphic form f at a point $\Gamma\tau$ of the modular curve $X(\Gamma)$ from the knowledge of the order of the form f itself at a point τ of the extended upper half-plane $\mathcal{H}^*$, where τ is any representative of $\Gamma\tau$.

Let Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, let f an automorphic form of even weight k with respect to Γ, let τ a point of $\mathcal{H}$ such that $\Gamma\tau$ has period $e \in \{1, 2, 3\}$ in $X(\Gamma)$ and let $s \in \mathbb{Q} \cup \{\infty\}$ such that Γs is a cusp of $X(\Gamma)$. By Diamond and Shurman [18] (Section 3.2) or Shimura [45] (Section 2.4) we know that

$$\mathrm{ord}_{\Gamma\tau}(f) = \frac{\mathrm{ord}_\tau(f)}{e},$$

for every $\tau \in \mathcal{H}$ and

$$\mathrm{ord}_{\Gamma s}(f) = \mathrm{ord}_s(f),$$

for every cusp s and the orders are well defined, i.e. they are independent of the chosen representative inside the orbit. We remark that there are not irregular cusps when k is even.

In this setting we can define the meromorphic differentials in the following way.

Definition 1.61. Let Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $X(\Gamma)$ the associated modular curve. We call *meromorphic differentials on $X(\Gamma)$ of degree n*, for a positive integer n, the elements of the set

$$\Omega^n(X(\Gamma)) := \{f(\tau)(d\tau)^n, f \in \mathcal{A}_{2n}(\Gamma)\}.$$

The elements $\omega = \omega(f) = f(\tau)(d\tau)^n$, where f is an automorphic form of weight $2n$ with respect to Γ and τ varies in $\mathcal{H}$, are differentials on $\mathcal{H}$ that are well defined as differentials on $X(\Gamma)$. It is obvious that $\Omega^n(X(\Gamma))$ is a $\mathbb{C}$-vector space isomorphic to $\mathcal{A}_{2n}(\Gamma)$.

Remark 1.62. The Definition 1.61 above of meromorphic differentials is equivalent to the usual one of meromorphic differentials on a Riemann surface. See Diamond and Shurman [18] Section 3.3 for details.

The discussion above allows to define and compute the order of a meromorphic differential $\omega(f)$ at a point $\Gamma\tau$ of $X(\Gamma)$ from the order of the associated form f at a point τ of $\mathcal{H}^*$, where τ is any representative of $\Gamma\tau$.

Let Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, let f an automorphic form of even weight k with respect to Γ, let $\omega = \omega(f)$ the meromorphic differential on $X(\Gamma)$ of degree $\frac{k}{2}$ associated to f, let τ a point of $\mathcal{H}$ such that $\Gamma\tau$ has period $e \in \{1, 2, 3\}$ in $X(\Gamma)$ and let $s \in \mathbb{Q} \cup \{\infty\}$ such that Γs is a cusp of $X(\Gamma)$. By Diamond and Shurman [18] (Section 3.3) or Shimura [45] (Section 2.4) we know that

$$\mathrm{ord}_{\Gamma\tau}(\omega) = \mathrm{ord}_{\Gamma\tau}(f) - \frac{k}{2}\left(1 - \frac{1}{e}\right) = \frac{\mathrm{ord}_\tau(f)}{e} - \frac{k}{2}\left(1 - \frac{1}{e}\right),$$

for every $\tau \in \mathcal{H}$ and

$$\mathrm{ord}_{\Gamma s}(\omega) = \mathrm{ord}_{\Gamma s}(f) - \frac{k}{2} = \mathrm{ord}_s(f) - \frac{k}{2},$$

for every cusp s and the orders are well defined, i.e. they are independent of the chosen representative inside the orbit. When $k = 2$ they become

$$\begin{aligned} \mathrm{ord}_{\Gamma\tau}(\omega) &= \frac{\mathrm{ord}_\tau(f) + 1}{e} - 1 \\ \mathrm{ord}_{\Gamma s}(\omega) &= \mathrm{ord}_s(f) - 1. \end{aligned}$$

Moreover, when $k = 2$ we have also the following result.

Corollary 1.63. *Let Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $X(\Gamma)$ the associated modular curve. Then*

$$\Omega^1_{hol}(X(\Gamma)) \cong \mathcal{S}_2(\Gamma),$$

where Ω^1_{hol} is the $\mathbb{C}$-vector space of holomorphic differentials of degree 1.

1.11 Twist of cusp forms

Our main references for this section are Shimura [45] and Atkin and Li [3].

Let $\mathcal{S}_k(\Gamma_1(N))$ be the set of cusp forms of weight k with respect to $\Gamma_1(N)$ and let

$$\begin{aligned} \mathcal{S}_k(N,\phi) &= \left\{ f \in \mathcal{S}_k(\Gamma_1(N)) \text{ s.t. } f[\gamma]_k = \phi(d)f, \text{ for every } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\} = \\ &= \left\{ f \in \mathcal{S}_k(\Gamma_1(N)) \text{ s.t. } \langle d \rangle f = \phi(d)f, \text{ for every } d \in (\mathbb{Z}/N\mathbb{Z})^* \right\}, \end{aligned}$$

where ϕ is a Dirichlet character modulo N and $\langle d \rangle$ is the usual diamond operator.

We recall the main definitions about twisting.

Definition 1.64. Let f be a modular form of level N and weight k with q-expansion $\sum_{n=0}^{\infty} a_n(f)q^n$ and χ a Dirichlet character modulo a positive integer M possibly different from the level N. We call $\sum_{n=0}^{\infty} a_n(f)\chi(n)q^n$ the twist form of f by χ and we denote it with $f \otimes \chi$. This means that $f \otimes \chi$ has a q-expansion with Fourier coefficient $a_n(f \otimes \chi) = a_n(f)\chi(n)$ for all $n \in \mathbb{Z}_{\geq 0}$.

Definition 1.65. Let h be a modular form. We call h *primitive* if there are not a modular form f and a non-trivial Dirichlet character χ such that $h = f \otimes \chi$.

We recall, without proof, the main result that we need about twisting of modular forms in Shimura [45] Proposition 3.64 (pag. 92). See also Atkin and Li [3] (Section 3).

Proposition 1.66. *Let N, s, r be positive integers with $s|N$ and let $M = \mathrm{lcm}(N, r^2, rs)$. Let ϕ and χ be primitive Dirichlet characters modulo s and r respectively. Let $f \in \mathcal{S}_k(N,\phi)$. Then $f \otimes \chi \in \mathcal{S}_k(M, \phi\chi^2)$.*

In our case $N = s = r = p$ where p is a prime number and $k = 2$. In this case $M = p^2$ and both ϕ and χ are characters modulo p. We want to know, given $f \in \mathcal{S}_2(p, \phi)$ and χ a primitive character modulo p, when the twist form $h = f \otimes \chi$ belongs to $\mathcal{S}_2(\Gamma_0(p^2)) = \mathcal{S}_2(p^2, \mathbb{1})$, where $\mathbb{1}$ is the trivial character modulo p. This is true if and only if $\phi\chi^2 = \mathbb{1}$ or equivalently when $\chi^2 = \phi^{-1}$.

If ϕ is the trivial character we have $h \in \mathcal{S}_2(\Gamma_0(p^2))$ if and only if $\chi^2 = \mathbb{1}$ and, since χ is primitive, this implies that χ is the quadratic character modulo p. This means that a twist of an element of $\mathcal{S}_2(\Gamma_0(p))$ by the non-trivial quadratic character modulo p is an element of $\mathcal{S}_2(\Gamma_0(p^2))$.

Now we assume ϕ is not trivial. Given an element $f \in \mathcal{S}_2(p, \phi)$ we can obtain two twists: $h = f \otimes \chi$ and $h' = f \otimes \chi'$, where $\chi^2 = \chi'^2 = \phi^{-1}$, hence $\chi' = \chi\xi$ where ξ is the non-trivial quadratic character modulo p.

Let $\sigma \in \mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$ an element of the absoute Galois group of $\mathbb{Q}$. Since we have the q-expansions of f and h at a rational cusp, then σ acts on f and h just acting on their Fourier coefficients. So it is obvious that $h^\sigma = f^\sigma \otimes \chi^\sigma$, that is Galois conjugates of h correspond to twist of Galois conjugates of f by Galois conjugates of χ. In particular if the character $\chi' = \chi\xi$ is a Galois conjugate of χ there is only one twisted Galois conjugacy class, otherwise there are two twisted Galois conjugacy classes: the class of $f \otimes \chi$ and the class of $f \otimes \chi'$.

By Atkin and Li [3] Corollary 3.1 (pag. 231), we know exactly when a twist form of a newform is again a newform. In our case $N = Q = q = p$ where p is a prime number, $F_\chi = f \otimes \chi$ is the twist form of $f \in \mathcal{S}_2(p, \phi)$ by the character χ such that $\mathrm{cond}\,\chi = p$. It follows that $\varepsilon = \varepsilon_Q = \phi$ and $M = 1$. Finally if we choose $Q' = p^2$ and $f \otimes \chi \in \mathcal{S}_2(\Gamma_0(p^2))$, that means $\phi\chi^2 = \mathbb{1}$, we can conclude that if f is a newform then $f \otimes \chi$ is a newform.

1.12 Serre's uniformity conjecture

In this section we illustrate the link between the Serre's uniformity conjecture and the modular curves. The main references for this section are Serre [44], Mazur [37] and Galbraith [24].

The *Serre's uniformity conjecture* over $\mathbb{Q}$ is the following.

Conjecture 1.67 (Serre's uniformity conjecture)**.** *There is a positive constant C such that, the representation*

$$\rho_{E,p} \colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*, is surjective for every elliptic curve E over $\mathbb{Q}$ without complex multiplication and for all prime numbers $p > C$.*

Here $\rho_{E,p}$ is the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that we get identifying the group $\mathrm{GL}_2(\mathbb{F}_p)$ with the automorphism group $\mathrm{Aut}(E[p])$ of p-torsion points $E[p]$ of the elliptic curve E. The word "uniformity" refers to the independence of constant C from the chosen elliptic curve.

Using the moduli space description of modular curves, we know, by Serre [44], that this conjecture follows from the following one.

Conjecture 1.68. *Let H be a proper subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that $\det\colon H \to \mathbb{F}_p^*$ is surjective. There is a positive constant C_H such that, for all primes $p > C_H$, the only rational points on the modular curve $X_H(p)$ of level p, defined over $\mathbb{Q}$, are the "expected points".*

We explain what the "expected points" are, after we state Theorem 1.69 below. Again by Serre [44], Section 2, we know the following theorem.

Theorem 1.69. *Let p be a prime number. If H is a subgroup of $G = \mathrm{GL}_2(\mathbb{F}_p)$ such that $\det\colon H \to \mathbb{F}_p^*$ is surjective, then we have only five possible cases:*

1. *$H = G$;*
2. *H is contained in a Borel subgroup of G;*
3. *H is contained in a normalizer of a split Cartan subgroup of G;*
4. *H is contained in a normalizer of a non-split Cartan subgroup of G;*
5. *H is the inverse image of an exceptional subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$, i.e. H is the inverse image of a subgroup H_1 of $\mathrm{PGL}_2(\mathbb{F}_p)$ that is isomorphic either to the symmetric group S_4, or to the alternating groups A_4 or A_5.*

Hence, it is enough to check the Conjecture 1.68 for H isomorphic to one of the maximal subgroups above: Borel, normalizer of split Cartan, normalizer of non-split Cartan and exceptional subgroup. If H is isomorphic to a Borel subgroup we denote the associated modular curve of level p by $X_0(p)$, if H is isomorphic to the normalizer of a split Cartan subgroup we denote the associated modular curve of level p by $X_s^+(p)$, and if H is isomorphic to the normalizer of a non-split Cartan subgroup we denote the associated modular curve of level p by $X_{ns}^+(p)$.

Depending on which maximal subgroup we consider, the expected rational points are characterized in a little bit different way. A nice point of view is that of Mazur [37] which we recall.

Let $E/\mathbb{C}$ an elliptic curve over the complex field with complex multiplication. Hence, E has a complex quadratic order as endomorphism ring $O_E := \mathrm{End}_{\mathbb{C}} E$. We denote by Δ_E the discriminant of O_E, by K the fraction field of O_E and by c the conductor of O_E, i.e. the index $[O_K : O_E]$ where O_K is the ring of integers of K.

If E is isomorphic to the complex torus $\mathbb{C}/\Lambda_\tau$, where Λ_τ is a lattice of $\mathbb{C}$ with basis $\{1, \tau\}$ for a fixed $\tau \in \mathcal{H}$, we have $O_E \cong \mathbb{Z}[\tau]$.

If the level of $X_H(p)$ is the prime number p, then the ideal pO_E of O_E over the prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$ could have only three different behaviours:

1. the ideal pO_E ramifies, so there is a prime ideal $\mathfrak{q}$ such that $pO_E = \mathfrak{q}^2$, in this case $\ker(\varphi_\mathfrak{q})$ is a subgroup of order p of group of the p-torsion points $E[p]$ of E, where $\varphi_\mathfrak{q}$ is a generator of the principal ideal $\mathfrak{q}$, and the pair $(E, \ker(\varphi_\mathfrak{q}))$ is a point on $X_0(p)$;

2. the ideal pO_E splits into two prime ideals $pO_E = \mathfrak{p}\bar{\mathfrak{p}}$, in this case $\ker(\varphi_{\mathfrak{p}})$ and $\ker(\varphi_{\bar{\mathfrak{p}}})$ are cyclic subgroups of order p of group of the p-torsion points $E[p]$ of E, where $\varphi_{\mathfrak{p}}$ and $\varphi_{\bar{\mathfrak{p}}}$ are generators of principal ideals $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ respectively, and the pair $(E, \{\ker(\varphi_{\mathfrak{p}}), \ker(\varphi_{\bar{\mathfrak{p}}})\})$ is a point on $X_s^+(p)$;

3. the ideal pO_E is inert, so it is still prime in O_E, in this case O_E/pO_E is a field that we can consider as a subfield of the endomorphism ring of p-torsion points $E[p]$ of E and the pair $(E, O_E/pO_E)$ is a point on $X_{ns}^+(p)$.

To get rational points on modular curves we need that the elliptic curve associated to that point is defined over $\mathbb{Q}$, i.e. we need that its j-invariant belongs to $\mathbb{Q}$. Let E be an elliptic curve with complex multiplication, let O_E be its endomorphism ring and let j_E be its j-invariant, we know, by complex multiplication theory, that

$$[\mathbb{Q}(j_E) : \mathbb{Q}] = h_{O_E},$$

where h_{O_E} is the class number of the order O_E. Hence, E is defined over $\mathbb{Q}$ if and only if O_E has class number one. So, the points above are rational if and only if the class number of the quadratic order O_E is one.

Definition 1.70. Let H be one of the maximal subgroup of G of Theorem 1.69. The *expected rational points* on a modular curve $X_H(p)$, whose level is a prime p, are:

1. the unique two cusps and the elliptic curves with complex multiplication such that the class number of O_E is one and p ramifies in O_E, if H is isomorphic to a Borel subgroup;

2. the unique rational cusp among the $\frac{p+1}{2}$ cusps of the curve and the elliptic curves with complex multiplication such that the class number of O_E is one and p splits in O_E, if H is isomorphic to the normalizer of a split Cartan subgroup;

3. the elliptic curves with complex multiplication such that the class number of O_E is one and p is inert in O_E, if H is isomorphic to the normalizer of a non-split Cartan subgroup.

There are no expected rational points in the case of H is the inverse image of an exceptional subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$.

The non-cuspidal expected rational points are also called *complex multiplication points* or *CM points*.

By Heegner [28], Stark [49] or Baker [5], we know that there are only 13 complex quadratic orders with class number one and their discriminants are

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

This implies that, for each prime number p, there are 13 non-cuspidal rational points to allocate among the curves $X_0(p)$, $X_s^+(p)$ and $X_{ns}^+(p)$. Since p ramifies in a quadratic order if and only if p divides the discriminant of the order, these 13 non-cuspidal rational points will be distributed only between $X_s^+(p)$ and $X_{ns}^+(p)$, when $p > 163$. Further, the CM points are always integral according to Definition 1.60.

What is the present status of Serre's uniformity conjecture? We know that Serre himself proved that it is true for H is the inverse image of an exceptional subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ taking $C_H = 13$. See Mazur [35] Introduction (pag. 36). Few years later, Mazur [35] and [36] proved that the conjecture is true for H isomorphic to a Borel subgroup taking $C_H = 37$. More recently, by the works of Bilu and Parent [10], and Bilu, Parent and Rebolledo [11], we know that the Serre's conjecture is true for H isomorphic to a normalizer of a split Cartan subgroup taking $C_H = 13$. So, to prove it, it is enough to prove the following conjecture.

Conjecture 1.71. *There is a positive constant C_{ns} such that, for all prime numbers $p > C_{ns}$, the modular curve $X_{ns}^+(p)$ of level p associated to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, have not rational points, except the expected points.*

So the problem is translated in an arithmetic geometry question. At the moment, to my knowledge, there are not promising approaches to attack this conjecture, but there are some papers that give some numerical evidence for it. The curves $X_{ns}^+(p)$ with level a prime $p < 11$ have genus zero and they have infinitely many rational points. Ligozat [33] in 1977 studies the genus 1 curve $X_{ns}^+(11)$, proving that it has infinitely many rational points, and Baran [7] in 2012 studies the genus 3 curve $X_{ns}^+(13)$. Bilu and Bajolet [4] in 2012 proved that the curve $X_{ns}^+(p)$ with level a prime $11 < p < 71$ has no integral points but the CM points.

In the following chapters we extend the method of Baran to all modular curves $X_{ns}^+(p)$ with level a prime $p > 13$. For larger p the main problem is the fact that the genus of $X_{ns}^+(p)$ and hence the required number of calculations grows rapidly with p. For example, we know that the genus of $X_{ns}^+(p)$ exceeds 5 when the level is a prime $p > 13$. We show an application of these techniques explicitly on the genus 6 modular curve $X_{ns}^+(17)$.

Chapter 2

How compute Fourier coefficients of non-split Cartan invariant forms

2.1 Introduction

In this chapter we denote by p a rational prime, by $\mathbb{F}_p$ the finite field with p elements and by $G = \mathrm{GL}_2(\mathbb{F}_p)$ the general linear group over $\mathbb{F}_p$.

Let $f \in \mathcal{S}_2(\Gamma_s(p))$ be the image of a newform in $\mathcal{S}_2(\Gamma_0^+(p^2))$. We know, by Baran [7] Proposition 3.6, that the G-subrepresentation generated by the $\mathbb{C}[G]$-span of f is an irreducible representation. But it is not true that every such a representation is a cuspidal one. This is the case only when f is not a twist of a lower level form, i.e. when f is primitive. We know f could arise as a twist of an element $t \in \mathcal{S}_2(\Gamma_1(p))$. Sometimes it is useful to distiguish when $t \in \mathcal{S}_2(\Gamma_0(p))$ and when $t \in \mathcal{S}_2(\Gamma_1(p)) \setminus \mathcal{S}_2(\Gamma_0(p))$, i.e. when the character ϕ of t is trivial or when it is not.

We want to get a form $h \in \mathcal{S}_2(\Gamma_{ns}(p))$ form one $f \in \mathcal{S}_2(\Gamma_s(p))$. In order to do this we use a representation-theoretical point of view.

2.2 Characterization of split and non-split Cartan invariant elements

Let p a rational prime, $\mathbb{F}_p$ the finite field with p elements and $G = \mathrm{GL}_2(\mathbb{F}_p)$ the general linear group over $\mathbb{F}_p$. We can associate a G-representation to every newform of $\mathcal{S}_2(\Gamma_0(p^2))$, as we explain in Section 2.3 below, so we use the group representation theory on G and our main reference is Piatetski-Shapiro [40].

We assume to fix a $\mathbb{F}_p$-basis and we choose a simple form for the subgroups of G that we define below. Therefore, the following definitions hold up to the conju-

gation by the change of basis matrix. Let

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}; a, b, d \in \mathbb{F}_p; ad \neq 0 \right\},$$

be the Borel subgroup of G, let

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}; u \in \mathbb{F}_p \right\},$$

be the unipotent subgroup of G, let

$$C_s = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}; a, d \in \mathbb{F}_p^* \right\},$$
$$C_s^+ = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}; a, d \in \mathbb{F}_p^* \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}; b, c \in \mathbb{F}_p^* \right\},$$

be the split Cartan subgroup and his normalizer respectively and let

$$C_{ns} = \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}; a, b \in \mathbb{F}_p; a^2 - b^2\xi \neq 0 \right\},$$
$$C_{ns}^+ = C_{ns} \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns},$$

be the non-split Cartan subgroup and his normalizer respectively, where ξ is a fixed quadratic non-residue of $\mathbb{F}_p$.

Let

$$\mu \colon B \to \mathbb{C},$$

be a character of B. We know that

$$\mu(\beta) = \mu_1(a)\mu_2(d), \text{ for every } \beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B,$$

where $\mu_1, \mu_2 \colon \mathbb{F}_p^* \to \mathbb{C}$ are two charcters of $\mathbb{F}_p^*$.

We know the complex irreducible representations of G are of four kinds and three of them arise from induced representations from B. The irreducible representations which don't arise from B are called cuspidal representations and their link with the newforms is already explained by Baran in [7]. Hence we focus our attention to representations arising from B and we give an explicit description of them.

Let $g_\infty, g_0, g_1, \ldots, g_{p-1}$ be a set of representatives of G/B, where

$$g_\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$g_k = \begin{pmatrix} k & k+1 \\ -1 & -1 \end{pmatrix}, \text{ for } k = 0, 1, \ldots, p-1.$$

Hence we have

$$G = B \sqcup \left(\bigsqcup_{k=0}^{p-1} g_k B \right).$$

Let V be a complex one dimensional representation of B such that $\beta \cdot v = \mu(\beta)v$ for every $v \in V$ and for every $\beta \in B$ and let $W = \mathrm{Ind}_B^G V$ the complex representation induced by V from B to G. We can see W as a $\mathbb{C}[G]$-module using

$$W = \mathbb{C}[G] \otimes_{\mathbb{C}[B]} V,$$

where

$$\begin{aligned} z \cdot (x \otimes v) &= x \otimes (zv), \\ g \cdot (x \otimes v) &= (gx) \otimes v, \\ (x\beta) \otimes v &= x \otimes \mu(\beta)v, \end{aligned}$$

for every $x, g \in G$, for every $v \in V$, for every $z \in \mathbb{C}$ and for every $\beta \in B$. To understand in explicit terms the action $g \cdot (x \otimes v)$, when $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, it is enough to compute the action on the basis, i.e. it is enough to compute $g \cdot (g_k \otimes 1) = (gg_k) \otimes 1$, for $k = \infty, 0, 1, \ldots, p-1$. The reader can easily check that if $c = 0$, i.e. $g \in B$, we have

$$\begin{aligned} gg_\infty &= \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = g_\infty g, \\ gg_k &= \begin{pmatrix} \frac{ak-b}{d} & \frac{ak-b}{d} + 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} d & d-a \\ 0 & a \end{pmatrix} = g_{\frac{ak-b}{d}} \begin{pmatrix} d & d-a \\ 0 & a \end{pmatrix}, \text{ for } k \neq \infty, \end{aligned}$$

otherwise, if $c \neq 0$, we have

$$\begin{aligned} gg_\infty &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -\frac{a}{c} & -\frac{a}{c} + 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} -c & \frac{ad}{c} - d - b \\ 0 & -\frac{ad}{c} + b \end{pmatrix} = g_{-\frac{a}{c}} \begin{pmatrix} -c & \frac{ad}{c} - d - b \\ 0 & -\frac{ad}{c} + b \end{pmatrix}, \\ gg_{\frac{d}{c}} &= \begin{pmatrix} \frac{ad}{c} - b & \frac{ad}{c} + a - b \\ 0 & c \end{pmatrix} = g_\infty \begin{pmatrix} \frac{ad}{c} - b & \frac{ad}{c} + a - b \\ 0 & c \end{pmatrix}, \\ gg_k &= \begin{pmatrix} -\frac{ak-b}{ck-d} & -\frac{ak-b}{ck-d} + 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} d - ck & d - a + c\frac{ak-b}{ck-d} \\ 0 & a - c\frac{ak-b}{ck-d} \end{pmatrix} = \\ &= g_{-\frac{ak-b}{ck-d}} \begin{pmatrix} d - ck & d - a + c\frac{ak-b}{ck-d} \\ 0 & a - c\frac{ak-b}{ck-d} \end{pmatrix}, \text{ for } k \neq \infty, \frac{d}{c}. \end{aligned}$$

It follows that if $c = 0$ we have

$$\begin{aligned} gg_\infty \otimes 1 &= g_\infty \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \otimes 1 = g_\infty \otimes \mu_1(a)\mu_2(d), \\ gg_k \otimes 1 &= g_{\frac{ak-b}{d}} \begin{pmatrix} d & d-a \\ 0 & a \end{pmatrix} \otimes 1 = g_{\frac{ak-b}{d}} \otimes \mu_1(d)\mu_2(a), \text{ for } k \neq \infty, \end{aligned}$$

otherwise, if $c \neq 0$, we have

$$
\begin{aligned}
gg_\infty \otimes 1 &= g_{-\frac{a}{c}} \begin{pmatrix} -c & \frac{ad}{c} - d - b \\ 0 & -\frac{ad}{c} + b \end{pmatrix} \otimes 1 = g_{-\frac{a}{c}} \otimes \mu_1(-c)\mu_2\left(-\frac{ad}{c} + b\right), \\
gg_{\frac{d}{c}} \otimes 1 &= g_\infty \begin{pmatrix} \frac{ad}{c} - b & \frac{ad}{c} + a - b \\ 0 & c \end{pmatrix} \otimes 1 = g_\infty \otimes \mu_1\left(\frac{ad}{c} - b\right)\mu_2(c), \\
gg_k \otimes 1 &= g_{-\frac{ak-b}{ck-d}} \begin{pmatrix} d - ck & d - a + c\frac{ak-b}{ck-d} \\ 0 & a - c\frac{ak-b}{ck-d} \end{pmatrix} \otimes 1 = \\
&= g_{-\frac{ak-b}{ck-d}} \otimes \mu_1(d - ck)\mu_2\left(a - c\frac{ak-b}{ck-d}\right), \text{ for } k \neq \infty, \frac{d}{c}.
\end{aligned}
$$

We have the fact that W is a $(p+1)$-dimensional complex representation that is irreducible if $\mu_1 \neq \mu_2$ and it splits in two irreducible representations, of dimension one and p respectively, if $\mu_1 = \mu_2$.

We want a formula that takes as input an element invariant with respect to the action of C_s^+ and gives as output an element invariant with respect to the action of C_{ns}^+. The way we get this is to characterize the C_s^+-invariant elements and the C_{ns}^+-invariant ones, i.e. we characterize the subspaces $W^{C_s^+}$ and $W^{C_{ns}^+}$.

In the remainder of this section we prove the following proposition.

Proposition 2.1. *Let $C_s, C_{ns}, C_s^+, C_{ns}^+$ be the Cartan subgroups and their normalizer as above, let $\mathbb{1}, \mu_1, \mu_2 \colon \mathbb{F}_p^* \to \mathbb{C}$ be characters of $\mathbb{F}_p^*$, where $\mathbb{1}$ is the trivial character. Let $\mu \colon B \to \mathbb{C}$ be a character of B such that for all $\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B$ we have $\mu(\beta) = \mu_1(a)\mu_2(d)$. Let $W = \operatorname{Ind}_B^G V = \mathbb{C}[G] \otimes_{\mathbb{C}[B]} V$, where V is the $\mathbb{C}$-representation of B of dimension one defined by the character μ as above. Let $g_\infty, g_0, \ldots, g_{p-1}$ be the above basis of W and let $v \in W$ an element with coordinates $z_\infty, z_0, \ldots, z_{p-1}$ with respect to this basis. Then*

a) *if $\mu_1 \neq \mu_2$ we have*

$$
\begin{aligned}
\dim W^{C_s} &= \delta(\mu_1\mu_2, \mathbb{1}), \\
\dim W^{C_{ns}} &= \delta(\mu_1\mu_2, \mathbb{1}), \\
\dim W^{C_s^+} &= \delta(\mu_1\mu_2, \mathbb{1})\delta(\mu_1(-1), 1), \\
\dim W^{C_{ns}^+} &= \delta(\mu_1\mu_2, \mathbb{1})\delta(\mu_1(-1), 1),
\end{aligned}
$$

and the characterization of his Cartan-invariant elements is the following

$$v \in W^{C_s} \text{ if and only if } \begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1\left(\frac{1}{k}\right) z_1, \quad k = 1, \dots, p-1, \end{cases} \tag{2.1}$$

$$v \in W^{C_{ns}} \text{ if and only if } \begin{cases} z_\infty = \mu_1 (1-\xi)\, z_1 \\ z_k = \mu_1\left(\frac{1-\xi}{k^2-\xi}\right) z_1, \quad k = 0, \dots, p-1, \end{cases} \tag{2.2}$$

$$v \in W^{C_s^+} \text{ if and only if } \mu_1(-1) = 1 \text{ and } \begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1\left(\frac{1}{k}\right) z_1, \quad k \neq \infty, 0, \end{cases} \tag{2.3}$$

$$v \in W^{C_{ns}^+} \text{ if and only if } \mu_1(-1) = 1 \text{ and } \begin{cases} z_\infty = \mu_1 (1-\xi)\, z_1 \\ z_k = \mu_1\left(\frac{1-\xi}{k^2-\xi}\right) z_1, \quad k \neq \infty; \end{cases} \tag{2.4}$$

b) *if $\mu_1 = \mu_2$ then $W = W_1 \oplus W_p$, where W_1 and W_p are irreducible representations of dimension one and p respectively such that W_1 is characterized by the following condition*

$$v \in W_1 \text{ if and only if } z_\infty = z_0 = \cdots = z_{p-1}, \tag{2.5}$$

and such that

$$\begin{aligned} \dim W_1^{C_s} &= \delta(\mu_1, \mathbb{1}), \\ \dim W_1^{C_{ns}} &= \delta(\mu_1, \mathbb{1}), \\ \dim W_1^{C_s^+} &= \delta(\mu_1, \mathbb{1}), \\ \dim W_1^{C_{ns}^+} &= \delta(\mu_1, \mathbb{1}), \\ \dim W_p^{C_s} &= \delta\left(\mu_1^2, \mathbb{1}\right) + \delta(\mu_1, \mathbb{1}), \\ \dim W_p^{C_{ns}} &= \delta\left(\mu_1^2, \mathbb{1}\right) - \delta(\mu_1, \mathbb{1}), \\ \dim W_p^{C_s^+} &= \delta\left(\mu_1^2, \mathbb{1}\right) \delta(\mu_1(-1), 1), \\ \dim W_p^{C_{ns}^+} &= \delta\left(\mu_1^2, \mathbb{1}\right) \delta(\mu_1(-1), 1) - \delta(\mu_1, \mathbb{1}), \end{aligned}$$

moreover, if $\mu_1 \neq \mathbb{1}$, the characterization of W_p's Cartan-invariant elements is the following

$$v \in W_p^{C_s} \text{ if and only if } \begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1\left(\frac{1}{k}\right) z_1, \quad k \neq \infty, 0, \end{cases} \tag{2.6}$$

$$v \in W_p^{C_{ns}} \text{ if and only if } \begin{cases} z_\infty = \mu_1 (1-\xi)\, z_1 \\ z_k = \mu_1\left(\frac{1-\xi}{k^2-\xi}\right) z_1, \quad k \neq \infty, \end{cases} \tag{2.7}$$

$$v \in W_p^{C_s^+} \text{ if and only if } \mu_1(-1) = 1 \text{ and } \begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1\left(\frac{1}{k}\right) z_1, \quad k \neq \infty, 0, \end{cases} \tag{2.8}$$

$$v \in W_p^{C_{ns}^+} \text{ if and only if } \mu_1(-1) = 1 \text{ and } \begin{cases} z_\infty = \mu_1 (1-\xi)\, z_1 \\ z_k = \mu_1\left(\frac{1-\xi}{k^2-\xi}\right) z_1, \quad k \neq \infty, \end{cases} \tag{2.9}$$

otherwise, if $\mu_1 = \mathbb{1}$, *it is*

$$v \in W_p^{C_s} \text{ if and only if } z_1 = \cdots = z_{p-1} = -z_\infty - z_0, \tag{2.10}$$

$$v \in W_p^{C_s^+} \text{ if and only if } z_1 = \cdots = z_{p-1} = -z_\infty = -z_0. \tag{2.11}$$

Proof. **a)** We suppose $\mu_1 \neq \mu_2$. Let $v = \sum_{k\in\mathbb{P}^1(\mathbb{F}_p)} g_k \otimes z_k \neq 0$, where $g_k, k \in \mathbb{P}^1(\mathbb{F}_p)$ are the above elements that form a basis for W and $z_k \in \mathbb{C}$ are the coordinates with respect to this basis. So $v \in W^{C_s}$ if and only if

$$g\left(\sum_{k\in\mathbb{P}^1(\mathbb{F}_p)} g_k \otimes z_k\right) = \sum_{k\in\mathbb{P}^1(\mathbb{F}_p)} g_k \otimes z_k, \text{ for every } g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in C_s.$$

Since

$$g\left(\sum_{k\in\mathbb{P}^1(\mathbb{F}_p)} g_k \otimes z_k\right) = \sum_{k\in\mathbb{P}^1(\mathbb{F}_p)} gg_k \otimes z_k =$$

$$= g_\infty \otimes \mu_1(a)\mu_2(d)z_\infty + \sum_{k=0}^{p-1} g_{\frac{ak}{d}} \otimes \mu_1(d)\mu_2(a)z_k =$$

$$= g_\infty \otimes \mu_1(a)\mu_2(d)z_\infty + \sum_{k=0}^{p-1} g_k \otimes \mu_1(d)\mu_2(a)z_{\frac{dk}{a}}, \text{ using the substitution } k \mapsto \frac{dk}{a},$$

it follows that $v \in W^{C_s}$ if and only if

$$\begin{cases} \mu_1(a)\mu_2(d)z_\infty = z_\infty \\ \mu_1(d)\mu_2(a)z_{\frac{dk}{a}} = z_k, \quad k = 0, \ldots, p-1 \end{cases}, \text{ for every } a, d \in \mathbb{F}_p^*.$$

If we choose $d = a$ then we get $\mu_2 = \mu_1^{-1}$, because at least one of $z_k, k \in \mathbb{P}^1(\mathbb{F}_p)$ is not zero and because the previous system must hold for every $a \in \mathbb{F}_p^*$. Therefore

$$\begin{cases} \mu_1\left(\frac{a}{d}\right)z_\infty = z_\infty \\ \mu_1\left(\frac{d}{a}\right)z_{\frac{dk}{a}} = z_k, \quad k = 0, \ldots, p-1 \end{cases}, \text{ for every } a, d \in \mathbb{F}_p^*,$$

and if we denote $r = \frac{d}{a}$ we have

$$\begin{cases} \mu_1\left(\frac{1}{r}\right)z_\infty = z_\infty \\ \mu_1(r)\, z_{rk} = z_k, \quad k = 0, \ldots, p-1 \end{cases}, \text{ for every } r \in \mathbb{F}_p^*.$$

Since we supposed $\mu_1 \neq \mu_1^{-1}$ it follows that μ_1 is not the trivial character, therefore we obtain

$$\begin{cases} z_\infty = z_0 = 0 \\ \mu_1(r)\, z_{rk} = z_k, \quad k = 1, \ldots, p-1 \end{cases}, \text{ for every } r \in \mathbb{F}_p^*.$$

So if we choose $k = 1$ we can write

$$\begin{cases} z_\infty = z_0 = 0 \\ z_r = \mu_1\left(\frac{1}{r}\right) z_1, \quad r = 1, \dots, p-1, \end{cases}$$

or equivalently $v \in W^{C_s}$ if and only if $v = \sum_{k=1}^{p-1} g_k \otimes \mu_1\left(\frac{1}{k}\right) z_1$.

Using the same argument when $g = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$, with $b, c \in \mathbb{F}_p^*$ and assuming $\mu_2 \neq \mu_1^{-1}$, we get

$$\begin{cases} z_\infty = \mu_1\left(-\frac{b}{c}\right) z_0 \\ z_0 = \mu_1\left(-\frac{c}{b}\right) z_\infty \\ z_k = \mu_1\left(-\frac{b}{ck^2}\right) z_{\frac{b}{ck}}, \quad k = 1, \dots, p-1 \end{cases}, \text{ for every } b, c \in \mathbb{F}_p^*.$$

Now if we suppose $v \in W^{C_s}$ and denoting $s = \frac{b}{c}$ we get

$$\begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1(r)\, z_{rk} \\ z_k = \mu_1\left(-\frac{s}{k^2}\right) z_{\frac{s}{k}} \end{cases}, \text{ for every } k, r, s \in \mathbb{F}_p^*,$$

and equaling the right hand side of the last two equations, denoting $\kappa = rk$ and $\rho = \frac{s}{rk^2}$, we obtain

$$\begin{cases} z_\infty = z_0 = 0 \\ z_\kappa = \mu_1(-\rho)\, z_{\rho\kappa} \end{cases}, \text{ for every } \kappa, \rho \in \mathbb{F}_p^*,$$

so, choosing $\rho = 1$, we have the extra condition $\mu_1(-1) = 1$ on the character.

For C_{ns} we make the same computations and if $g = \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}$, with $b \neq 0$ (the case $b = 0$ is trivial), we have

$$\begin{cases} z_\infty = \mu_1\left(\frac{a^2}{b} - b\xi\right)\mu_2(b) z_{\frac{a}{b}} \\ z_{-\frac{a}{b}} = \mu_1(-b)\,\mu_2\left(-\frac{a^2}{b} + b\xi\right) z_\infty \\ z_{\frac{ak-b\xi}{a-bk}} = \mu_1(a-bk)\,\mu_2\left(a - b\frac{ak-b\xi}{bk-a}\right) z_k, \quad k \neq \infty, \frac{a}{b}, \end{cases}$$

for every $a \in \mathbb{F}_p$ and for every $b \in \mathbb{F}_p^*$ such that $a^2 + b^2\xi \neq 0$. So we must have $z_\infty \neq 0$ and, choosing $a = 0$, this implies that

$$z_\infty = \mu_1(-b\xi)\,\mu_2(b) z_0 = \mu_1\left(b^2\xi\right)\mu_2\left(b^2\xi\right) z_\infty,$$

for every $b \in \mathbb{F}_p^*$ and therefore we have again the condition $\mu_2 = \mu_1^{-1}$. Using this condition and denoting $r = -\frac{a}{b}$ we get

$$\begin{cases} z_\infty = \mu_1\left(r^2 - \xi\right) z_{-r} \\ z_r = \mu_1\left(\frac{1}{r^2-\xi}\right) z_\infty \\ z_{\frac{rk+\xi}{r+k}} = \mu_1\left(\frac{(r+k)^2}{r^2-\xi}\right) z_k, \quad k \neq \infty, -r, \end{cases}, \text{ for every } r \in \mathbb{F}_p,$$

and with the substitution $k \mapsto \frac{kr-\xi}{r-k}$ we have

$$\begin{cases} z_\infty = \mu_1\left(r^2-\xi\right) z_{-r} \\ z_r = \mu_1\left(\frac{1}{r^2-\xi}\right) z_\infty \\ z_k = \mu_1\left(\frac{r^2-\xi}{(r-k)^2}\right) z_{\frac{rk-\xi}{r-k}}, \quad k \neq \infty, r \end{cases}, \text{ for every } r \in \mathbb{F}_p.$$

As for the split Cartan case if we take $g = \begin{pmatrix} a & -b\xi \\ b & -a \end{pmatrix}$, with $b \neq 0$, denoting again $r = -\frac{a}{b}$ and assuming $\mu_2 = \mu_1^{-1}$ we get

$$\begin{cases} z_\infty = \mu_1\left(\xi - r^2\right) z_r \\ z_r = \mu_1\left(\frac{1}{\xi-r^2}\right) z_\infty \\ z_{\frac{rk-\xi}{k-r}} = \mu_1\left(\frac{(r-k)^2}{\xi-r^2}\right) z_k, \quad k \neq \infty, r, \end{cases}, \text{ for every } r \in \mathbb{F}_p.$$

As before, joining these conditions with the previous ones which characterize $W^{C_{ns}}$, we obtain again the extra condition on the character $\mu_1(-1) = 1$. If we want to express all the coordinates in terms of one of them, for example z_1, we can write

$$\begin{cases} z_\infty = \mu_1(1-\xi) z_1 \\ z_k = \mu_1\left(\frac{1-\xi}{k^2-\xi}\right) z_1, \quad k = 0, \ldots, p-1. \end{cases}$$

So if $\mu_1 \neq \mu_2$ then W is irreducible and we have

$$\begin{aligned} \dim W^{C_s} &= \delta(\mu_1\mu_2, \mathbb{1}), \\ \dim W^{C_s^+} &= \delta(\mu_1\mu_2, \mathbb{1})\delta(\mu_1(-1), 1), \\ \dim W^{C_{ns}} &= \delta(\mu_1\mu_2, \mathbb{1}), \\ \dim W^{C_{ns}^+} &= \delta(\mu_1\mu_2, \mathbb{1})\delta(\mu_1(-1), 1), \end{aligned}$$

where δ is the usual Kronecker's delta and $\mathbb{1} : \mathbb{F}_p^* \to \mathbb{C}$ is the trivial character of $\mathbb{F}_p^*$.

b) Now we study the case $\mu_2 = \mu_1$. By Piatetski-Shapiro [40] we know W splits in two not isomorphic irreducible representations with dimension one and p respectively. We denote the former by W_1 and the latter by W_p, so $W = W_1 \oplus W_p$. In this case the action of an element g of G on the basis become

$$\begin{aligned} gg_\infty \otimes 1 &= g_\infty \otimes \mu_1(\det g), \\ gg_k \otimes 1 &= g_{\frac{ak-b}{d}} \otimes \mu_1(\det g), \text{ for } k \neq \infty, \end{aligned}$$

if $c = 0$ and

$$\begin{aligned} gg_\infty \otimes 1 &= g_{-\frac{a}{c}} \otimes \mu_1(\det g), \\ gg_{\frac{d}{c}} \otimes 1 &= g_\infty \otimes \mu_1(\det g), \\ gg_k \otimes 1 &= g_{-\frac{ak-b}{ck-d}} \otimes \mu_1(\det g), \text{ for } k \neq \infty, \frac{d}{c}, \end{aligned}$$

if $c \neq 0$. It is immediate to observe that the only one dimensional representation is defined by the condition $z_\infty = z_0 = \cdots = z_{p-1}$. Hence $gv = \mu_1(\det g)v$ for every $g \in G$ and $v \in W_1$ and from this we deduce

$$\begin{aligned}\dim W_1^{C_s} &= \delta(\mu_1, \mathbb{1}),\\ \dim W_1^{C_s^+} &= \delta(\mu_1, \mathbb{1}),\\ \dim W_1^{C_{ns}} &= \delta(\mu_1, \mathbb{1}),\\ \dim W_1^{C_{ns}^+} &= \delta(\mu_1, \mathbb{1}).\end{aligned}$$

If $v \in W$ and $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in C_s$ we get $v \in W^{C_s}$ if and only if

$$\begin{cases} z_\infty = \mu_1(ad)\, z_\infty \\ z_{\frac{ak}{d}} = \mu_1(ad)\, z_k, \quad k \neq \infty, \end{cases}, \text{ for every } a, d \in \mathbb{F}_p^*.$$

Substituting $k \mapsto \frac{dk}{a}$ we obtain

$$\begin{cases} z_\infty = \mu_1(ad)\, z_\infty \\ z_k = \mu_1(ad)\, z_{\frac{dk}{a}}, \quad k \neq \infty, \end{cases}, \text{ for every } a, d \in \mathbb{F}_p^*.$$

and choosing $a = d$ we get $\mu_1^2(a) = 1$ for every $a \in \mathbb{F}_p^*$ and therefore $\mu_1^2 = \mathbb{1}$. We have two cases $\mu_1 \neq \mathbb{1}$ or $\mu_1 = \mathbb{1}$. In the first case choosing $a = d$ we get $z_\infty = z_0 = 0$ and denoting $r = \frac{d}{a}$ we get $z_k = \mu_1(a^2 r) z_{rk} = \mu_1(r) z_{rk}$. Hence $v \in W^{C_s}$ if and only if

$$\begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1(r) z_{rk}, \quad k \neq \infty, 0, \end{cases}, \text{ for every } r \in \mathbb{F}_p^*,$$

or in terms of z_1

$$\begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1\left(\frac{1}{k}\right) z_1, \quad k \neq \infty, 0. \end{cases}$$

On the other hand if $\mu_1 = \mathbb{1}$, again denoting $r = \frac{d}{a}$, we have

$$\begin{cases} z_k = z_{rk}, \quad k \neq \infty, 0, \text{ for every } r \in \mathbb{F}_p^*. \end{cases}$$

So we can write

$$\dim W_p^{C_s} = \delta\left(\mu_1^2, \mathbb{1}\right) + \delta(\mu_1, \mathbb{1}).$$

For C_s^+ we take $g = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \in G$ and in the same way we have

$$\begin{cases} z_\infty = \mu_1(-bc)\, z_0 \\ z_0 = \mu_1(-bc)\, z_\infty \\ z_{\frac{b}{ck}} = \mu_1(-bc)\, z_k, \quad k \neq \infty, 0, \end{cases}, \text{ for every } b, c \in \mathbb{F}_p^*.$$

Substituting $k \mapsto \frac{b}{ck}$ we obtain

$$\begin{cases} z_\infty = \mu_1(-bc)\, z_0 \\ z_0 = \mu_1(-bc)\, z_\infty \\ z_k = \mu_1(-bc)\, z_{\frac{b}{ck}}, \quad k \neq \infty, 0, \end{cases}, \text{ for every } b, c \in \mathbb{F}_p^*.$$

If we add to these the conditions the characterize W^{C_s} and denoting $s = \frac{b}{c}$ we have, if $\mu_1 \neq \mathbb{1}$,

$$\begin{cases} z_\infty = z_0 = 0 \\ z_k = \mu_1(r) z_{rk}, \quad k \neq \infty, 0, \\ z_k = \mu_1(-s)\, z_{\frac{s}{k}}, \quad k \neq \infty, 0, \end{cases}$$

for every $r, s \in \mathbb{F}_p^*$ and choosing $s = k = 1$ we obtain again the extra condition $\mu_1(-1) = 1$. But when $\mu_1 = \mathbb{1}$ we have

$$\begin{cases} z_\infty = z_0 \\ z_k = z_{rk}, \quad k \neq \infty, 0, \\ z_k = z_{\frac{s}{k}}, \quad k \neq \infty, 0, \end{cases}$$

for every $r, s \in \mathbb{F}_p^*$, so we can write

$$\dim W_p^{C_s^+} = \delta\left(\mu_1^2, \mathbb{1}\right) \delta(\mu_1(-1), 1).$$

And now the last part of these computations. We take $g = \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix} \in C_{ns}$, we suppose $b \neq 0$, the case $b = 0$ is trivial, and we denote $r = -\frac{a}{b}$. We have

$$\begin{cases} z_\infty = \mu_1(\det g)\, z_{-r} \\ z_r = \mu_1(\det g)\, z_\infty \\ z_{\frac{rk+\xi}{r+k}} = \mu_1(\det g)\, z_k, \quad k \neq \infty, -r, \end{cases}, \text{ for every } r \in \mathbb{F}_p^*.$$

Substituting $k \mapsto \frac{rk-\xi}{r-k}$ we obtain

$$\begin{cases} z_\infty = \mu_1(\det g)\, z_{-r} \\ z_r = \mu_1(\det g)\, z_\infty \\ z_k = \mu_1(\det g)\, z_{\frac{rk-\xi}{r-k}}, \quad k \neq \infty, r, \end{cases}, \text{ for every } r \in \mathbb{F}_p^*.$$

Using the first two equations we have $z_r = \mu_1^2(\det g) z_{-r}$, for every $r \in \mathbb{F}_p^*$ and for every $g \in C_{ns}$, hence if we take $r = 0$ we get $\mu_1^2 = \mathbb{1}$ (because if $z_0 = 0$ then $v = 0$). Now if $\mu_1 = \mathbb{1}$ we have $z_\infty = z_0 = \ldots, z_{p-1}$ that is W_1. So we suppose $\mu_1 \neq \mathbb{1}$ and we rewrite the conditions in terms of z_1

$$\begin{cases} z_\infty = \mu_1(1-\xi)\, z_1 \\ z_k = \mu_1\left((1-\xi)(k^2-\xi)\right) z_1, \quad k \neq \infty. \end{cases}$$

Hence we have

$$\dim W_p^{C_{ns}} = \delta\left(\mu_1^2, \mathbb{1}\right) - \delta(\mu_1, \mathbb{1}).$$

Finally for $g = \begin{pmatrix} a & -b\xi \\ b & -a \end{pmatrix}$ we get similarly $z_\infty = z_0 = \ldots, z_{p-1}$ if $\mu_1 = \mathbb{1}$ and again the extra condition $\mu_1(-1) = 1$ if $\mu_1 \neq \mathbb{1}$. So we have

$$\dim W_p^{C_{ns}^+} = \delta\left(\mu_1^2, \mathbb{1}\right)\delta(\mu_1(-1), 1) - \delta(\mu_1, \mathbb{1}),$$

completing the part of interest for us of the dimension table in Edixhoven [20] and the proof.

□

2.3 From representations to cusp forms

In this section we explain the relation between cusp forms and representations of $G = \mathrm{GL}_2(\mathbb{F}_p)$ and $\mathrm{SL}_2(\mathbb{F}_p)$. This allows to apply the results of Section 2.2 above to cusp forms.

Let $X(p)$, for p prime number, be the modular curve which parametrizes elliptic curves with full p-level structure. This modular curve is defined over the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. There is a natural isomorphism

$$X(p)_{\mathbb{C}} \cong \coprod_{\mu_p^*} \mathcal{H}^*/\Gamma(p),$$

where μ_p^* is the set of primitive p-th roots of unity, $X(p)_{\mathbb{C}}$ is the analytification of $X(p)$, the group $\Gamma(p)$ is the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level p and $\mathcal{H}^*$ is the extended upper half-plane. This isomorphism is defined over $\mathbb{C}$.

Using the previous isomorphism and Corollary 1.63 we get the isomorphism

$$\Omega^1_{hol}(X(p)_{\mathbb{C}}) \cong \bigoplus_{\mu_p^*} \mathcal{S}_2(\Gamma(p)), \tag{2.12}$$

between the $\mathbb{C}$-vector space of holomorphic differentials on $X(p)_{\mathbb{C}}$ and the direct sum of the $\mathbb{C}$-vector space of cusp forms of weight 2 with respect to $\Gamma(p)$, indexed by the set μ_p^* of primitive p-th roots of unity.

By Section 1.8 we know there is an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{S}_2(\Gamma(p))$ using the weight-2 operator. This action is actually an action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\mathcal{S}_2(\Gamma(p))$. We have that isomorphism (2.12) above is G-equivariant if we identify the right hand with the complex G-representation space $\mathrm{Ind}_{\mathrm{SL}_2(\mathbb{F}_p)}^G \mathcal{S}_2(\Gamma(p))$. We denote this representation space as $V(p)$.

We have that

$$\Omega^1_{hol}(X_s^+(p)_{\mathbb{C}}) \cong V(p)^{C_s^+}$$
$$\Omega^1_{hol}(X_{ns}^+(p)_{\mathbb{C}}) \cong V(p)^{C_{ns}^+},$$

where $V(p)^{C_s^+}$ is the subrepresentation of elements of $V(p)$ that are invariant with respect to the action of C_s^+ and similarly for $V(p)^{C_{ns}^+}$.

We know by Baran [7] Proposition 3.6, that the $\mathbb{C}[G]$-span V_f of a newform $f \in \mathcal{S}_2(\Gamma_0^+(p^2))$, where p is an odd prime, is an irreducible representation. This follows from the strong multiplicity one property.

It is well known that the irreducible representations of G are the cuspidal ones and the principal series. The cuspidal representations are parametrized by characters θ of $\mathbb{F}_{p^2}^*$ that don't factor through the norm map and a character of $\mathbb{F}_p^*$, i.e. there are not characters $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$ such that $\theta = \chi \circ \mathrm{Norm}$, where $\mathrm{Norm}\colon \mathbb{F}_{p^2}^* \to \mathbb{F}_p^*$ is the usual norm map. The principal series representations are parametrized by pairs (μ_1, μ_2) of characters of $\mathbb{F}_p^*$. For more details see Section 1.3 above or Piatetski-Shapiro [40] or Fulton and Harris [22].

We recall, from Section 1.11, that a modular form is primitive if it is not a twist of a lower level modular form. Let f be a newform of $\mathcal{S}_2(\Gamma_0(p^2))$, we know that, if f is primitive then V_f is a cuspidal irreducible representation, on the other hand if f is a twist by χ of a lower level newform $g \in \mathcal{S}_2(\Gamma_1(p))$ then V_f is a principal series irreducible representation. More precisely, if $g \in \mathcal{S}_2(\Gamma_0(p))$ then V_f has dimension p and $\mu_2 = \mu_1^{-1} = \mu_1 = \chi$, but if $g \in \mathcal{S}_2(\Gamma_1(p))$ and $g \notin \mathcal{S}_2(\Gamma_0(p))$ then V_f has dimension $p+1$ and $\mu_2 = \mu_1^{-1} \neq \mu_1 = \chi$. The irreducible representations of G with dimension 1 never occur in this context.

Starting with the knowledge of the Fourier coefficients of a basis of newforms for $\mathcal{S}_2(\Gamma_0^+(p^2))$, we are able to compute the Fourier coefficients of a basis for $\mathcal{S}_2(\Gamma_{ns}^+(p))$.

The first step is to observe that there is an isomorphism $\mathcal{S}_2(\Gamma_0^+(p^2)) \cong \mathcal{S}_2(\Gamma_s^+(p))$ that doesn't change the Fourier coefficients. We show this in the following lemma.

Lemma 2.2. *Let* $w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ *for every positive integer* N *and let* p *a prime. The map*

$$\begin{aligned} \iota\colon \mathcal{S}_2(\Gamma_0^+(p^2)) &\to \mathcal{S}_2(\Gamma_s^+(p)) \\ f &\mapsto \iota(f) := pf[w_p]_2 \end{aligned}$$

is an isomorphism and the Fourier coefficients of f *and* $\iota(f)$ *are the same.*

Proof. We start proving that the map ι is well defined. By

$$\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}\begin{pmatrix} a & pb \\ pc & d \end{pmatrix} = \begin{pmatrix} d & -c \\ -p^2 b & a \end{pmatrix}\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix},$$

for every $a, b, c, d \in \mathbb{Z}$ such that $ad - p^2bc = 1$, it follows that

$$f\left[w_p \begin{pmatrix} a & pb \\ pc & d \end{pmatrix}\right]_2 = f\left[\begin{pmatrix} d & -c \\ -p^2 b & a \end{pmatrix} w_p\right]_2 = f[w_p]_2.$$

Moreover, by

$$f\left[\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right]_2 = f,$$

for every non-zero integer a, and by

$$\begin{pmatrix} 0 & -1 \\ p^2 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}\begin{pmatrix} pa & b \\ c & pd \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} b & -a \\ p^2 d & -c \end{pmatrix}\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix},$$

for every $a, b, c, d \in \mathbb{Z}$ such that $p^2 ad - bc = 1$, it follows that

$$f\left[w_p \begin{pmatrix} pa & b \\ c & pd \end{pmatrix}\right]_2 = f\left[w_{p^2} w_p \begin{pmatrix} pa & b \\ c & pd \end{pmatrix}\right]_2 = f\left[\begin{pmatrix} b & -a \\ p^2 d & -c \end{pmatrix} w_p\right]_2 = f[w_p]_2.$$

So ι is well defined.

The $\mathbb{C}$-linearity of ι follows by definition of weight-2 operator.

That $\iota(f) = 0$ implies $f = 0$ follows trivially by $\frac{1}{p\tau^2} \neq 0$ for all $\tau \in \mathcal{H}$. Thus, ι is injective.

To prove that ι is also surjective, we show that if $g \in \mathcal{S}_2(\Gamma_s^+(p))$ then $g[w_p]_2 \in \mathcal{S}_2(\Gamma_0^+(p^2))$. If this is true we can define $f := \frac{1}{p} g[w_p]_2 \in \mathcal{S}_2(\Gamma_0^+(p^2))$ and we have $\iota(f) = g$, because w_p is an involution. Hence, we assume $g \in \mathcal{S}_2(\Gamma_s^+(p))$. By

$$\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}\begin{pmatrix} a & b \\ p^2 c & d \end{pmatrix} = \begin{pmatrix} d & -pc \\ -pb & a \end{pmatrix}\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix},$$

for every $a, b, c, d \in \mathbb{Z}$ such that $ad - p^2 bc = 1$, it follows that

$$g\left[w_p \begin{pmatrix} a & b \\ p^2 c & d \end{pmatrix}\right]_2 = g\left[\begin{pmatrix} d & -pc \\ -pb & a \end{pmatrix} w_p\right]_2 = g[w_p]_2.$$

Furthermore, we have

$$g\left[w_p w_{p^2}\right]_2 = g\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} w_p\right]_2 = g[w_p]_2,$$

and we are done.

Finally, we prove the Fourier coefficients invariance. Since $f \in \mathcal{S}_2(\Gamma_0^+(p^2))$, we have

$$f(\tau) = (f[w_{p^2}]_2)(\tau) = \frac{1}{p^2\tau^2} f\left(-\frac{1}{p^2\tau}\right),$$

for every $\tau \in \mathcal{H}$ and where the second equality holds by definition of weight-2 operator for matrices with not unitary determinant, see Remark 1.49. Hence, substituting τ with $-\frac{1}{p\tau}$ we have

$$f\left(-\frac{1}{p\tau}\right) = \frac{1}{p^2 \frac{1}{p^2\tau^2}} f\left(-\frac{1}{-p^2 \frac{1}{p\tau}}\right) = \tau^2 f\left(\frac{\tau}{p}\right).$$

It follows that

$$(f[w_p]_2)(\tau) = \frac{1}{p\tau^2} f\left(-\frac{1}{p\tau}\right) = \frac{1}{p} f\left(\frac{\tau}{p}\right).$$

This means that if $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$, where $q = e^{2\pi i \tau}$, then

$$\iota(f)(\tau) = p(f[w_p]_2)(\tau) = \sum_{n=1}^{\infty} a_n q^n,$$

where $q = e^{\frac{2\pi i \tau}{p}}$, i.e. f and $\iota(f)$ have the same Fourier coefficients, but different q's. □

Now, it is enough to show how to compute the Fourier coefficients of a basis for $\mathcal{S}_2(\Gamma_{ns}^+(p))$ from the coefficients of a basis of newforms for $\mathcal{S}_2(\Gamma_s^+(p))$.

We don't explain how to do this when f is a primitive newform and hence V_f is a cuspidal representation, becuase it is already described in Baran [7]. So, we focus on the case of f twist of a newform $g \in \mathcal{S}_2(\Gamma_1(p))$.

If f is a twist of a newform $g \in \mathcal{S}_2(\Gamma_1(p))$, there is a non-trivial Dirichlet character $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$ such that $f = g \otimes \chi$. We know that the pair of characters corresponding to V_f is (χ, χ^{-1}).

Let $f = g \otimes \chi$ be a twist of a newform $g \in \mathcal{S}_2(\Gamma_1(p))$ and a non-trivial Dirichlet character $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$, and let

$$g(\tau) = \sum_{n=1}^{\infty} a_n q^n,$$

the Fourier expansion of g, where $q = e^{\frac{2\pi i \tau}{p}}$. We denote by ε_g the eigenvalue of g with respect to the Atkin-Lehner involution w_p, i.e. $g[w_p]_2 = \varepsilon_g g$ and $\varepsilon_g = \pm 1$. Let

$$\mathfrak{g}_\infty(\tau) := p\varepsilon_g \sum_{n=1}^{\infty} a_n q^{pn},$$

where the a_n's are the Fourier coefficients of g and $q = e^{\frac{2\pi i \tau}{p}}$ and let

$$\mathfrak{g}_k(\tau) := \sum_{n=1}^{\infty} a_n \zeta_p^{-kn} q^n,$$

for $k = 0, \ldots, p-1$, where $\zeta_p = e^{\frac{2\pi i}{p}}$ is a p-th root of unity, the a_n's are the Fourier coefficients of g and $q = e^{\frac{2\pi i \tau}{p}}$. Of course, we have $\mathfrak{g}_0 = g$.

We construct the $\mathbb{C}$-vector space $V_{\mathfrak{g}}$ freely generated by $\mathfrak{g}_\infty, \mathfrak{g}_0, \ldots, \mathfrak{g}_{p-1}$. This space has dimension $p+1$ over $\mathbb{C}$.

Using the same notation of Section 2.2 above, we consider the complex one dimensional representation V of the Borel subgroup B such that $\beta \cdot v = \chi(\beta)v$ for every $v \in V$ and for every $\beta \in B$, where χ is the character used to twist g and get f. Furthermore, we consider the complex representation $W = \mathrm{Ind}_B^G V$ induced by V from B to G. We see W as a $\mathbb{C}[G]$-module using

$$W = \mathbb{C}[G] \otimes_{\mathbb{C}[B]} V.$$

A basis of this representation W is $g_\infty, g_0, \ldots, g_{p-1}$, where

$$g_\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$g_k = \begin{pmatrix} k & k+1 \\ -1 & -1 \end{pmatrix}, \text{ for } k = 0, 1, \ldots, p-1.$$

Proposition 2.3. *Let W be the complex G-representation defined above. Then $V_{\mathfrak{g}}$ is a complex $\mathrm{SL}_2(\mathbb{F}_p)$-representation isomorphic to $\mathrm{Res}^G_{\mathrm{SL}_2(\mathbb{F}_p)} W$.*

Proof. The map $(g_k \otimes 1) \mapsto \mathfrak{g}_k$ for $k = \infty, 0, \ldots, p-1$ is $\mathbb{C}$-linear, so it is enough to check that is also $\mathrm{SL}_2(\mathbb{F}_p)$-equivariant. By definition of $\mathrm{SL}_2(\mathbb{F}_p)$ action we can check the equivariance only for the generators $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ of $\mathrm{SL}_2(\mathbb{Z})$.

We described the action of G on W in the Section 2.2 above and we can assume that $\mu_2 = \mu_1^{-1} = \chi^{-1}$, where μ_1, μ_2 are the character parametrizing the representation W and χ is the character we used to twist g. So we get

$$\begin{aligned}
T g_\infty \otimes 1 &= g_\infty \otimes 1, \\
T g_k \otimes 1 &= g_{k-1} \otimes 1, \quad \text{if } k \neq \infty, \\
S g_\infty \otimes 1 &= g_0 \otimes 1, \\
S g_0 \otimes 1 &= g_\infty \otimes 1, \\
S g_k \otimes 1 &= g_{-\frac{1}{k}} \otimes \chi^2(k), \quad \text{if } k \neq \infty, 0.
\end{aligned}$$

On the modular form side, for each $\tau \in \mathcal{H}$, we have

$$\begin{aligned}
(\mathfrak{g}_\infty[T]_2)(\tau) &= p\varepsilon_g \sum_{n=1}^{\infty} a_n e^{\frac{2\pi i(\tau+1)pn}{p}} = p\varepsilon_g \sum_{n=1}^{\infty} a_n e^{\frac{2\pi i\tau pn}{p}} = \mathfrak{g}_\infty(\tau), \\
(\mathfrak{g}_k[T]_2)(\tau) &= \sum_{n=1}^{\infty} a_n \zeta_p^{-kn} e^{\frac{2\pi i(\tau+1)n}{p}} = \sum_{n=1}^{\infty} a_n \zeta_p^{-kn} e^{\frac{2\pi i\tau n}{p}} \zeta_p^n = \\
&= \sum_{n=1}^{\infty} a_n \zeta_p^{-(k-1)n} e^{\frac{2\pi i\tau n}{p}} = \mathfrak{g}_{k-1}(\tau), \quad \text{if } k \neq \infty, \\
(\mathfrak{g}_\infty[S]_2)(\tau) &= \frac{1}{\tau^2} \sum_{n=1}^{\infty} a_n e^{-\frac{2\pi i n}{p\tau}} = p\varepsilon_g \sum_{n=1}^{\infty} a_n e^{2\pi i\tau n} = \mathfrak{g}_0(\tau),
\end{aligned}$$

where the second equality hold by $g[w_p]_2 = \varepsilon_g g$, with $\varepsilon_g = \pm 1$, depending on g. By

$$(\mathfrak{g}_\infty[S]_2)(\tau) = \mathfrak{g}_0(\tau),$$

we have

$$(\mathfrak{g}_0[S]_2)(\tau) = \mathfrak{g}_\infty(\tau),$$

acting by S on both sides and using that S is an involution. And finally we have

$$(\mathfrak{g}_k[S]_2)(\tau) = \chi^2(k)\mathfrak{g}_{-\frac{1}{k}}(\tau), \qquad \text{if } k \neq \infty, 0.$$

□

Therefore, by Proposition 2.1 and by Proposition 2.3 above we get the following formulas.

Corollary 2.4. *Let $f = g \otimes \chi \in \mathcal{S}_2(\Gamma_s^+(p))$ be a twist of a newform $g \in \mathcal{S}_2(\Gamma_1(p))$ and a non-trivial character $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$. Let ξ be a fixed quadratic non-residue of $\mathbb{F}_p$ and let $\mathfrak{g}_\infty, \mathfrak{g}_0, \ldots, \mathfrak{g}_{p-1}$ be the basis of representation $V_\mathfrak{g}$ defined above. Then*

$$h(\tau) := \mathfrak{g}_\infty(\tau) + \sum_{k=0}^{p-1} z_k \mathfrak{g}_k(\tau),$$

is a cusp form $h \in \mathcal{S}_2(\Gamma_{ns}^+(p))$ if and only if

$$\begin{cases} z_\infty = z, \\ z_k = \chi^{-1}\left(k^2 - \xi\right) z, \quad k \neq \infty, \end{cases}$$

where $z \in \mathbb{C}$ is an arbitrary constant.

By Corollary 2.4 we have that the the cusp forms of $\mathcal{S}_2(\Gamma_{ns}^+(p))$ are the forms h such that

$$h(\tau) := z\left(\mathfrak{g}_\infty(\tau) + \sum_{k=0}^{p-1} \chi^{-1}\left(k^2 - \xi\right)\mathfrak{g}_k(\tau)\right),$$

with the notation as above, for some $f = g \otimes \chi \in \mathcal{S}_2(\Gamma_s^+(p))$ twist of a newform $g \in \mathcal{S}_2(\Gamma_1(p))$ and a non-trivial character $\chi\colon \mathbb{F}_p^* \to \mathbb{C}^*$. In terms of Fourier coefficients, if

$$g(\tau) = \sum_{n=1}^{\infty} a_n q^n,$$

is the Fourier expansion of g, where $q = e^{\frac{2\pi i \tau}{p}}$, and

$$h(\tau) = \sum_{n=1}^{\infty} b_n q^n,$$

is the Fourier expansion of h, where again $q = e^{\frac{2\pi i \tau}{p}}$, we have

$$b_n = \begin{cases} \left(\sum_{k=0}^{p-1} \chi^{-1}\left(k^2 - \xi\right)\zeta_p^{-kn}\right) a_n & \text{if } p \nmid n, \\ p\varepsilon_g a_{\frac{n}{p}} + \left(\sum_{k=0}^{p-1} \chi^{-1}\left(k^2 - \xi\right)\zeta_p^{-kn}\right) a_n & \text{if } p \mid n, \end{cases}$$

where ξ is the fixed quadratic non-residue of $\mathbb{F}_p$ and $\zeta_p = e^{\frac{2\pi i}{p}}$ is a p-th root of unity.

Chapter 3

Explicit equations and other explicit computations

3.1 Introduction

According to Serre's uniformity conjecture we have an explicit description of the finitely many rational points on modular curves $X_0^+(p)$ and $X_{ns}^+(p)$. See Section 1.12 for more details about rational points on modular curves. The expected rational points on $X_0^+(p)$ are the cusp and the points corresponding to elliptic curves with complex multiplication such that p is split or ramifies in their endomorphism ring. We point out that the curve $X_0^+(p)$ has, for every prime p, only one cusp and it is always rational; see for example Ogg [39]. Differently, the expected rational points on $X_{ns}^+(p)$ are the points corresponding to elliptic curves with complex multiplication such that p is inert in their endomorphism ring; we point out that cusps are never rational in this case. We call an *exceptional* rational point every rational point that is not included in the expected ones.

Usually one can look for exceptional rational points numerically where the height of points is the natural upper bound to choose for this search. If one use a simple brute force enumeration, the value of height, that allows to finish the search in reasonable time, depends on genus of curve, i.e. it depends on the number of variables, and it is very small. Often, it does not reach two digits number in examples we treat. Hence the numerical evidence for Serre's conjecture is very low. In some particular cases, that we explain below in this section, we are able to improve this bound up to 10000 digits number in best istances. To explain this method, we need some data that we briefly recall.

In the table below we list dimensions of rational eigenspaces of Hecke algebra acting on $\mathcal{S}_2(X_0(p))$, for all prime number $p \leq 300$ such that the genus of the modular curve $X_0^+(p)$ is at least 6. For the complete list, up to 300, see [12].

The prime p is the level, + and − are the dimensions of spaces of newforms with eigenvalue +1 and −1 respectively, with respect to usual Atkin-Lehner operator w_p. If these spaces split, we write the dimension of each component. The number of

components is also the number of Galois-conjugacy classes of newforms and the corresponding dimensions are the cardinalities of these classes.

p	$+$	$-$
163	6 = 1 + 5	7
193	7 = 2 + 5	8
197	6 = 1 + 5	10
211	6 = 3 + 3	11 = 2 + 9
223	6 = 2 + 4	12
229	7 = 1 + 6	11
233	7	12 = 1 + 11
241	7	12
257	7	14
269	6 = 1 + 5	16
271	6	16
277	10 = 1 + 9	12 = 3 + 9
281	7	16
283	9	14
293	8	16

We focus on the +-space, i.e. the jacobian of $X_0^+(p)$. Since to each Galois-conjugacy class we can associate an abelian variety which dimension is equal to the cardinality of corresponding class, if there is a one-element class then the associated abelian variety is, in fact, an elliptic curve and we denote it by $E_{(p,+)}$. We know by Eichler-Shimura theory (see Knapp [30] Theorem 11.74 and Section 3.5 Lemma 3.6 below) that there is an algebraic map from $X_0^+(p)$ to $E_{(p,+)}$. We call it the E-map and we denote it by π_E. It follows that the rational points of $X_0^+(p)$ belong to the inverse image of rational points of $E_{(p,+)}$.

Using Cremona's tables in [15] or the LMFDB online database [34] to know the Mordell-Weil generators of $E_{(p,+)}$, we are able to enumerate the rational points of this elliptic curve. Usually we can look for rational points on $X_0^+(p)$ up to a fixed height, the E-map allows to make bigger this upper bound, without increase in time. In Section 3.6 below we explain in detail how we can do this.

In the non-split case, by Chen [14] or Edixhoven [20], we know that the jacobian $J_{ns}^+(p)$ of $X_{ns}^+(p)$ is isogenous to the new part of jacobian $J_0^+(p^2)$ of $X_0^+(p^2)$, i.e. there is an isogeny $\phi\colon J_{ns}^+(p) \to J_0^+(p^2)^{new}$. Hence, if there is a newform $f \in \mathcal{S}_2(X_0(p^2))$ with integer Fourier coefficients and w_p-eigenvalue equal to $+1$, then, as we explained above, there are an elliptic curve $E_{(p^2,+)}$ and a map from $X_0^+(p^2)$ to this elliptic curve $E_{(p^2,+)}$. The explicit computation of E-map $\pi_E\colon X_{ns}^+(p) \to E_{(p^2,+)}$ is harder because, now, π_E is the composition of the map from the modular curve $X_{ns}^+(p)$ to its jacobian with the isogeny ϕ, and this fact increase the degree of polynomials we look for.

Using online Stein tables [50] we list the modular curves $X_0(p^2)$, where p is a prime number, such that $p^2 < 1000$ and the genus of $X_0^+(p^2)$ is at least 6. In

particular p^2 is the level, p is the prime factor, + and − are the dimensions of spaces of newforms with eigenvalue +1 and −1 respectively, with respect to usual Atkin-Lehner operator w_p. If these spaces split, we write the dimension of each component.

p^2	p	+	−
289	17	$7 = 1 + 1 + 2 + 3$	$10 = 1 + 2 + 3 + 4$
361	19	$9 = 1 + 1 + 3 + 4$	$13 = 1 + 1 + 2 + 2 + 2 + 2 + 3$
529	23	$12 = 2 + 2 + 4 + 4$	$20 = 2 + 2 + 2 + 2 + 2 + 2 + 3 + 5$
841	29	$26 = 2 + 2 + 2 + 3 + 3 + 6 + 8$	$32 = 2 + 2 + 2 + 6 + 8 + 12$
961	31	$28 = 2 + 2 + 8 + 16$	$35 = 2 + 2 + 2 + 2 + 3 + 4 + 8 + 12$

In this chapter we explain how we make explicit calculations to get equations for a projective model of some modular curves.

Then we explain how to compute the prescribed rational points and how to improve the basic upper bound using the E-map to look for exceptional rational points.

In the end of this chapter we attach tables of some examples. In particular, given a modular curve X, we list in Section 3.7 some explicit equations for a projective model of it, its expected rational points and the upper bound used to look for exceptional ones. The considered modular curves are $X = X_0^+(p)$ for $p = 163, 193, 197, 211, 223, 229, 233, 241, 257, 269, 271, 277, 281, 283, 293$, and $X = X_{ns}^+(p)$ for $p = 17$.

3.2 How many Fourier coefficients do we need?

In this section we explain how many Fourier coefficients we should use to prove the found equations are correct and not only numerically approximated. This number depends only on degree of equations, genus and number of elliptic points of the modular curve.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, let $f_1, \ldots, f_g$ be a basis of $\mathcal{S}_2(\Gamma)$ where g is the genus of $X(\Gamma)$ and let

$$F = \sum_{i_1=1}^{g} \cdots \sum_{i_d=1}^{g} c_{i_1,\ldots,i_d} f_{i_1} \ldots f_{i_d},$$

a linear combination of products of d elements of this basis, so $F \in \mathcal{S}_{2d}(\Gamma)$. Let $\mathcal{A}_k(\Gamma)$ be the field of automorphic forms of weight k with respect to Γ, let $\mathbb{C}(X(\Gamma))$ be the field of meromorphic functions of $X(\Gamma)$ and h a nonzero element of it. We know that $\mathcal{A}_k(\Gamma) \simeq \mathbb{C}(X(\Gamma))h$ for every $k \in \mathbb{Z}$. Hence, given the above basis $f_1, \ldots, f_g$, we can choose $f_1 = f$ and write $f_i = h_i f$ where $h_i \in \mathbb{C}(X(\Gamma))$ for $i = 2, \ldots, g$. It follows that we can write

$$F = h_F f^d,$$

where $h_F \in \mathbb{C}(X(\Gamma))$ and it is explicitly

$$h_F = \sum_{i_1=1}^{g} \cdots \sum_{i_d=1}^{g} c_{i_1,\ldots,i_d} h_{i_1} \ldots h_{i_d},$$

where $h_1 = 1$.

We want to find a divisor D_F and a positive integer m such that $h_F \in L(D_F)$ and such that if $h_F \in L(D_F - m(\infty))$ then $h_F = 0$ and hence $F = 0$. We have

$$\operatorname{div}(h_F) = \operatorname{div}(F) - d \cdot \operatorname{div}(f),$$

moreover we know also that

$$\operatorname{div}(F) \geq \sum_{i=1}^{\varepsilon_\infty} Q_i,$$

because F is a cusp form, where ε_∞ is the number of cusps of $X(\Gamma)$ and

$$\operatorname{div}(f) = K + \sum_{P \in Y(\Gamma)} \left(1 - \frac{1}{e_P}\right) P + \sum_{i=1}^{\varepsilon_\infty} Q_i,$$

where $K = \operatorname{div}(\omega)$ is a canonical divisor, $\omega = \omega(f) = f(\tau)d\tau$ is the holomorphic differential associated to f and $e_P \in \{1, 2, 3\}$ is the period of the point P. The divisor is well defined because the number of cusps and elliptic points is finite and for P not elliptic we have that the corresponding summand in the second sum is zero. So we can write

$$\operatorname{div}(h_F) \geq (1 - d) \sum_{i=1}^{\varepsilon_\infty} Q_i - d \cdot K - d \sum_{P \in Y(\Gamma)} \left(1 - \frac{1}{e_P}\right) P,$$

hence $h_F \in L(D_F)$ with

$$D_F = (d - 1) \sum_{i=1}^{\varepsilon_\infty} Q_i + d \cdot K + d \sum_{P \in Y(\Gamma)} \left(1 - \frac{1}{e_P}\right) P.$$

Now we suppose $h_F \in L(D_F - m(\infty))$. If $\deg(D_F - m(\infty)) < 0$ then $L(D_F - m(\infty))$ is trivial and we are done. So it suffices to observe that

$$\deg(D_F - m(\infty)) = d - 1 + 2d(g - 1) + d \sum_{P \in Y(\Gamma)} \left(1 - \frac{1}{e_P}\right) - m,$$

to get a lower bound for m

$$m \geq d(2g - 1) + d \sum_{P \in Y(\Gamma)} \left(1 - \frac{1}{e_P}\right),$$

where $e_P \in \{1, 2, 3\}$ is the period of P for every point of the modular curve $X(\Gamma)$ that is not a cusp, d is the degree of F as homogenous polynomial in the elements of a basis of $\mathcal{S}_2(\Gamma)$, and g is the genus of $X(\Gamma)$. Denoting by ε_2 and ε_3 the number of elliptic points on $X(\Gamma)$ of period 2 and 3 respectively, we can rewrite the lower bound in the following way

$$m \geq d\left(2g - 1 + \frac{1}{2}\varepsilon_2 + \frac{2}{3}\varepsilon_3\right). \tag{3.1}$$

When we cannot compute exactly ε_2 and ε_3 we can use as upper bound the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ for both of them. In our cases we have always $d = 2$ and $g \geq 6$.

Let p a rational prime and r a positive integer. We recall the Baran formulas, included in [8] Proposition 7.10, to count the number of elliptic points of period 2 and 3 on $X^+_{ns}(p^r)$, when $p^r \neq 2$, denoted by ε_2 and ε_3 respectively. They are

$$\varepsilon_2(X^+_{ns}(p^r)) = \begin{cases} \frac{1}{2}p^r\left(1 - \frac{1}{p}\right) & \text{if } p \equiv 1 \mod 4, \\ 1 + \frac{1}{2}p^r\left(1 + \frac{1}{p}\right) & \text{if } p \equiv 3 \mod 4, \\ 2^{r-1} & \text{if } p = 2, \end{cases}$$

$$\varepsilon_3(X^+_{ns}(p^r)) = \begin{cases} 1 & \text{if } p \equiv 2 \mod 3, \\ 0 & \text{otherwise.} \end{cases}$$

Hence to compute the quadrics defining $X^+_{ns}(17)$ we need at least 32 Fourier coefficients because the degree is $d = 2$, the genus is $g = 6$ and the number of elliptic points is $\varepsilon_2 = 8$ and $\varepsilon_3 = 1$.

When $\Gamma = \Gamma^+_0(p)$, where p is a prime greater than 3, we can bound from above ε_2 and ε_3 by $\frac{p+1}{2}$ since

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1,$$
$$[\Gamma^+_0(p) : \Gamma_0(p)] = 2,$$

imply

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma^+_0(p)] = \frac{p+1}{2}.$$

So, if $d = 2$, the condition on m become

$$m > 4g - 2 + \frac{7}{6}(p + 1).$$

For example, if $p = 163$ we have $g = 6$, hence to compute the quadrics defining $X^+_0(163)$ it is enough to consider 214 Fourier coefficients.

3.3 Method to get explicit equations

Our method to get explicit equations is not supposed to be the best way to do it, but it allows to obtain very nice equations, i.e. equations with very small integer coefficients in absolute value.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let $f_1, \ldots, f_g$ be a $\mathbb{Q}$-basis of $\mathcal{S}_2(\Gamma)$ where g is the genus of $X(\Gamma)$.

To get a projective model of $X(\Gamma)$ we use the canonical embedding. We recall the main results about this in Section 1.5. In the modular curve setting the canonical embedding could be express, by Section 1.10, in the following way

$$\begin{aligned} \varphi\colon X(\Gamma) &\to \mathbb{P}^{g-1}(\mathbb{C}) \\ \Gamma\tau &\mapsto [f_1(\tau), \ldots, f_g(\tau)], \end{aligned}$$

where $X(\Gamma)$ is defined over $\mathbb{C}$.

We know by Theorem 1.20 the possible forms of equations defining the canonical curve and in this section we assume that we are in the general case, i.e. we assume that it is not hyperelliptic, trigonal or a quintic plane. The hyperelliptic case is already treated in Galbraith [23] Section 4.

If we know that $X(\Gamma)$ is defined over $\mathbb{Q}$, we can look for equations defined over $\mathbb{Q}$. We cannot use Theorem 1.20, because it is proved on algebraically closed fields, but we can use it over $\mathbb{C}$ to find equations defined over $\mathbb{C}$. Then, if these equations are defined over $\mathbb{Q}$, we can check by MAGMA that their zero locus Z is an algebraic curve with correct genus, i.e. the genus of $X(\Gamma)$ and Z is the same. Finally using Hurwitz genus formula, for genus $g > 1$, we can conclude that Z is isomorphic to $X(\Gamma)$ over $\mathbb{Q}$.

In the remainder of this section we suppose to know d, the degree of the homogenous equations that we want to find, and m Fourier coefficients of the q-expansions of $f_1, \ldots, f_g$, where m satisfies the condition (3.1) of Section 3.2.

Our method consists of three steps: to build up the matrix of coefficients with entries in $\mathbb{Z}$, to get better equations, and to write down the equations. The second step is not necessary to find the equations but it is the key step to get nicer models.

1. Building up the matrix with entries in $\mathbb{Z}$

   Using a $\mathbb{Q}$-basis of newforms we can build up M, the matrix of coefficients. Let us denote by $\mathcal{B} = \{f_1, \ldots, f_g\}$ this $\mathbb{Q}$-basis. Since the Fourier coefficients of elements of $\mathcal{B}$ are algebraic numbers, there is a number field $\mathfrak{F}$, of degree D over $\mathbb{Q}$, which contains all coefficients of all elements of $\mathcal{B}$.

   We can always multiply by a constant to clean out all denominators of the coordinates, with respect to the basis of $\mathfrak{F}$ over $\mathbb{Q}$, of every coefficient of each element of $\mathcal{B}$.

   Now, we can produce the matrix $M = (a_{ij})$ that has g rows and mD columns, where m is the number of Fourier coefficients used and g is the cardinality of the basis. The matrix M is filled taking, for each row, the entries $a_{i1}, \ldots, a_{iD}$ equal to the coordinates, with respect to the basis of $\mathfrak{F}$ over $\mathbb{Q}$, of the first coefficient of f_i, the i-th element of $\mathcal{B}$, and so on up to the row is full.

2. Improving equations

   Once we have the matrix M with integer entries, we look for prime numbers p such that rank of M is not maximal, i.e. lower than g because we have

always $m \geq g$ by condition (3.1) on m above. We want to get rid of these primes, because if they stay, the models we find will be singular modulo these primes. So we call these primes *bad primes*.

We describe how to do this in Algorithm 3.1 below within a more general setting.

Without bad primes we apply the LLL-algorithm to reduce considerably the size of matrix entries and we get the matrix M_L.

3. Finding explicit equations

Now, we rewrite the rows of M_L as q-series of modular forms and compute all monomials of degree d where the indeterminates are these forms. We build up M', the new matrix of coefficients, that has $\binom{g+d-1}{d}$ rows (i.e. the number of homogenous monomials of degree d) and dmD columns.

Finally we compute the kernel of M' and these are the coefficients of the desired equations.

Sometimes, it could be a good idea apply LLL-algorithm also to the matrix of coefficients of found equations to reduce further such coefficients.

Algorithm 3.1. Let $v_1, \ldots, v_g \in \mathbb{Z}^m$ be $\mathbb{Q}$-linearly independent vectors, where g and m are positive integers such that $g \leq m$. We want to find a $\mathbb{Z}$-basis of

$$V := \mathrm{span}_{\mathbb{Q}}\{v_1, \ldots, v_g\} \cap \mathbb{Z}^m.$$

Let $W := \mathrm{span}_{\mathbb{Z}}\{v_1, \ldots, v_g\}$, so W is a subgroup of V, and let $J := [V : W]$.

Let $M \in \mathbb{Z}^{m \times g}$ the matrix whose columns are the vectors $v_1, \ldots, v_g$. If Δ is a minor of M then Δ is an integer and $J \mid \Delta$.

We want to modify W until we have $J = 1$, i.e. $W = V$.

Step 0 We choose the principal maximal minor Δ of M. We set

$$S_\Delta := \{\text{prime numbers that divide } \Delta\},$$

now go to Step 1.

Step 1 If $S_\Delta = \emptyset$ the algorithm terminate.

If $S_\Delta \neq \emptyset$ then go to Step 2.

Step 2 We choose the minimal prime number $p \in S_\Delta$. We solve the system of linear congruences

$$\sum_{i=1}^{g} a_i v_i \equiv 0 \mod p. \tag{3.2}$$

If the system (3.2) above has unique solution, the trivial one, i.e. the rank of M is maximal modulo p, we have $p \nmid J$. Hence, we set

$$S_\Delta := S_\Delta \setminus \{p\},$$

and go to Step 1.

If the system (3.2) above admits non-trivial solutions, i.e. the rank of M is not maximal modulo p, then go to Step 3

Step 3 Let $r := \mathrm{rk}(M \mod p)$, we have $k := g - r \in \mathbb{Z}_{>0}$ solutions that are linearly independent over the finite field $\mathbb{F}_p$. We find a $\mathbb{F}_p$-basis $b_1, \ldots, b_k \in \mathbb{F}_p^g$ such that if we take the matrix B with columns the b_j's we can choose k rows, denoted by $i_1, \ldots, i_k$, such that $1 \leq i_1 < \cdots < i_k \leq g$ and such that the submatrix $k \times k$ of B determined by these rows has each element of the principal diagonal equal to 1.

For $j = 1, \ldots, k$, let $b_j = (\bar{a}_1^j, \ldots, \bar{a}_g^j)$ and we set

$$w_j := \frac{1}{p} \sum_{i=1}^{g} \bar{a}_i^j v_i.$$

Hence, by our choice of B, we have $\bar{a}_{i_j}^j = 1$ for $j = 1, \ldots, k$, and we set

$$v_{i_j} := w_j,$$

for $j = 1, \ldots, k$ and then go to Step 0.

Remark 3.2. In the Step 0 of Algorithm 3.1 above it is not necessary to choose the principal maximal minor, it is good enough any maximal minor. Further, if one choose more than one maximal minor $\Delta_1, \ldots, \Delta_n$, one can take $S_\Delta := \gcd\{\Delta_1, \ldots, \Delta_n\}$.

Now we prove that the problem solved by Algorithm 3.1 above is equivalent to get of rid of bad primes as we want in our procedure to find explicit equations.

Lemma 3.3. *With the same notation of Algorithm 3.1 above. We have $W = V$ if and only if* $\mathrm{rk}(M \mod p)$ *is maximal for every prime number p.*

Proof. First we suppose there is a prime p such that $\mathrm{rk}(M \mod p)$ is not maximal. This is equivalent to say that $v_1, \ldots, v_g$ are $\mathbb{F}_p$-linearly dependent, i.e. there are $\alpha_1, \ldots, \alpha_g \in \mathbb{Z}$, not all zero modulo p, such that $\alpha_1 v_1 + \cdots + \alpha_g v_g = pw$, where $w \in \mathbb{Z}^n$ is a non-zero vector because the v_i's are $\mathbb{Q}$-linearly independent. So, w belongs to V but not to W and therefore $W \subsetneq V$.

For the other direction we assume there is an element $w \in V \setminus W$. In this case there are $\alpha_1, \ldots, \alpha_g \in \mathbb{Q} \setminus \mathbb{Z}$ such that $\alpha_1 v_1 + \cdots + \alpha_g v_g = w$. Let D be the least common denominator of $\alpha_1, \ldots, \alpha_g$, we know that $D > 1$, so we can write

$$D_1 v_1 + \cdots + D_g v_g = Dw,$$

where the D_i's are the integers $D\alpha_i$, for $i = 1, \ldots, g$. This implies that $v_1, \ldots, v_g$ are $\mathbb{F}_p$-linearly dependent for every prime p that divides D. □

The next lemma shows that Algorithm 3.1 finish in finitely many steps, i.e. a bad prime is no more bad after finitely many steps and, if $\bar{a}^j_{i_j} = 1$, no new bad primes are introduced.

Lemma 3.4. *Let M be the matrix in Algorithm 3.1 above and let p be the prime number chose in Step 2. After finitely many iterations of the algorithm the rank of M is maximal modulo p and no new bad primes are introduced.*

Proof. We denote by $M_{(t)}$ the matrix M after t iterations of the algorithm and we use a similar notation for each matrix involved. We suppose that $M_{(t)}$ has not maximal rank modulo the prime p. Without loss of generality we can assume that the rows $i_1, \ldots, i_k$ of Step 3 are the first k rows and the submatrix $k \times k$ including these rows is the identity matrix I_k. So, we can write the matrix $B_{(t)}$ as the block matrix

$$B_{(t)} = \left(\frac{I_k}{B'_{(t)}}\right).$$

Let $T_{(t)}$ the $g \times g$ matrix

$$T_{(t)} = \left(\begin{array}{c|c} \frac{1}{p} I_k & 0 \\ \hline \frac{1}{p} B'_{(t)} & I_{g-k} \end{array}\right),$$

therefore we can write

$$M_{(t+1)} := M_{(t)} T_{(t)}.$$

Now, it is simple to see that for a maximal minor $\Delta_{(t+1)}$ of $M_{(t+1)}$, i.e. a minor of order g, we have

$$\Delta_{(t+1)} = \Delta_{(t)} \det T = \frac{1}{p^k} \Delta_{(t)},$$

where $\Delta_{(t)}$ is the maximal minor of $M_{(t)}$ corresponding to the same rows of $\Delta_{(t+1)}$, and this prove the lemma. □

Remark 3.5. From the proof of Lemma 3.4 above follows that if $\bar{a}^j_{i_j} \neq \pm 1$, i.e. the top left block of matrix $T_{(t)}$ has, at least, one element divisible by a prime number q, then the matrix $M_{(t+1)} := M_{(t)} T_{(t)}$ has not maximal rank modulo q. So, in this way, we introduce bad primes and the algorithm will not finish. Hence the condition $\bar{a}^j_{i_j} = \pm 1$ is necessary to the finiteness of algorithm, but we choose $\bar{a}^j_{i_j} = 1$ just for simplicity of exposition.

3.4 Computing the expected rational points

In this section we illustrate a trivial way to find numerically the expected rational points on a modular curve of kind $X_0^+(p)$ or $X_{ns}^+(p)$, for p prime. We assume to have explicit equations for a projective model of the modular curve considered and to know as many Fourier coefficients as necessary of the basis $f_1, \ldots, f_g$ of newforms used to find the explicit equations, where g is the genus of the modular curve. It

is obvious that the coordinates of the rational points will depend on the equations used to describe the curve.

It is well known that the class number one discriminants, for orders in imaginary quadratic number fields, are

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

see, for example, Stark [49], Baker [5] or Baran [6] and [8]. By classical algebraic number theory we know that to every discriminant Δ corresponds a square-free number D that defines a quadratic number field $K\left(\sqrt{D}\right)$ containing the order O_Δ associated to Δ. The index $[O_K : O_\Delta]$, where O_K is the ring of integers of K, is usually denoted by f and if $f = 1$ we call the discriminant Δ a *fundamental discriminant*. We recall the relation between Δ and D

$$\Delta = \begin{cases} Df^2 & \text{if } D \equiv 1 \mod 4 \\ 4Df^2 & \text{if } D \equiv 2, 3 \mod 4, \end{cases}$$

and since $\Delta \equiv 0, 1 \mod 4$ we can also recover D from Δ (let $\Delta = Ds$ where s is the square part of Δ, if $D \equiv 1 \mod 4$ then $f = \sqrt{s}$, else $f = \frac{\sqrt{s}}{2}$). We recall also that a basis of O_Δ is $1, \tau$ where

$$\tau = \begin{cases} \left(\frac{1+\sqrt{D}}{2}\right) f & \text{if } D \equiv 1 \mod 4 \\ \sqrt{D} f & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

We table below these data for the class number one discriminants (some τ's are not the same of the previous formula but are equivalent).

Δ	D	f	$(D \mod 4)$	τ
-3	-3	1	1	$\frac{1}{2} + \frac{\sqrt{3}}{2}i$
-4	-1	1	3	i
-7	-7	1	1	$\frac{1}{2} + \frac{\sqrt{7}}{2}i$
-8	-2	1	2	$\sqrt{2}i$
-11	-11	1	1	$\frac{1}{2} + \frac{\sqrt{11}}{2}i$
-12	-3	2	1	$\sqrt{3}i$
-16	-1	2	3	$2i$
-19	-19	1	1	$\frac{1}{2} + \frac{\sqrt{19}}{2}i$
-27	-3	3	1	$\frac{1}{2} + \frac{3\sqrt{3}}{2}i$
-28	-7	2	1	$\sqrt{7}i$
-43	-43	1	1	$\frac{1}{2} + \frac{\sqrt{43}}{2}i$
-67	-67	1	1	$\frac{1}{2} + \frac{\sqrt{67}}{2}i$
-163	-163	1	1	$\frac{1}{2} + \frac{\sqrt{163}}{2}i$

Let E be an elliptic curve with complex multiplication such that the discriminant Δ_E of its endomorphism ring O_E is a class number one discriminant, i.e. Δ_E

is equal to one of the list above. This implies that E is unique up to isomorphism. It is known that it produces a rational point on $X_0^+(p)$ or $X_{ns}^+(p)$. More specifically, if the prime p splits or ramifies in $\mathcal{O}_E$ then E corresponds to a rational point on $X_0^+(p)$, see Galbraith [24], else, i.e. if p is inert in $\mathcal{O}_E$, we have that E corresponds to a rational point on $X_{ns}^+(p)$, see Mazur [37]. In the case $X_0^+(p)$ we have also that the unique cusp is always rational. See Ogg [39] for more details about this.

From the previous discussion it follows that we can find how much the expected rational points are on the modular curve $X_0^+(p)$ or $X_{ns}^+(p)$. It is enough to check if p divides the class number one discriminants, and if p is a square or not in the associated orders. Once we have found the class number one discriminants that generate rational points, we know the corresponding $\tau_E \in \mathcal{H}$. See the table above for some explicit τ_E's. A suitable element of the orbit of τ_E under the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ will be the τ such that $(f_1(\tau) : \cdots : f_g(\tau))$ is a rational point for the modular curve, where g is the genus of the modular curve and $f_1, \ldots, f_g$ is the basis of newforms used to find the explicit equations defining the curve in $\mathbb{P}^{g-1}$. Moreover, the point $(f_1(\tau) : \cdots : f_g(\tau))$ has rational coordinates in the projective model of the modular curve.

We focus on the case $X_{ns}^+(p)$. Let Γ_{ns}^+ be the lifting in $\mathrm{SL}_2(\mathbb{Z})$ of C_{ns}^+. We know that

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_{ns}^+] = [\mathrm{GL}_2(\mathbb{F}_p) : C_{ns}^+],$$

for every prime p. Therefore, we can explicitly get, for example using MAGMA, all the finitely many representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_{ns}^+$. We can do this computing the representatives of $\mathrm{GL}_2(\mathbb{F}_p)/C_{ns}^+$ and then finding the lifting in $\mathrm{SL}_2(\mathbb{Z})$ for each representative. To have more computational stability it is better to choose the lifting $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, with the lower entries c and d as small as possible (in absolute value). This is because the convergence of series is better when $|c\tau + d|$ is small.

Now we use these representatives to get the corresponding elements in the orbit of τ_E, i.e. for each representative γ we compute $\gamma\tau_E$. Then we compute $(f_1(\gamma\tau_E) : \cdots : f_g(\gamma\tau_E))$ for every γ representative of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_{ns}^+$ and, if one use enough Fourier coefficients, it is quite simple recognize the rational points within this set of points. Often it is useful to divide by one non-zero coordinate before to search the rational points.

For the case $X_0^+(p)$ we can work in a similar way.

3.5 Computation of E-map

In this section we suppose to know m Fourier coefficients of the modular forms involved, where m is "large enough" for our purposes.

Let E be an elliptic curve over $\mathbb{Q}$ with conductor a positive integer N. By Mod-

ularity Theorem, we know that there is a map, called *modular parametrization*,

$$\begin{aligned} \phi\colon X_0(N) &\to E(\mathbb{C}) \\ \Gamma_0(N)\tau &\mapsto \phi(\tau) = (\phi_x(\tau), \phi_y(\tau)), \end{aligned}$$

where τ is a representative of $\Gamma_0(N)\tau$ and $\phi_x(\tau)$ and $\phi_y(\tau)$ are power series with rational coefficients in the indeterminate $q = e^{2\pi i\tau}$.

Lemma 3.6. *If E is an elliptic curve over $\mathbb{Q}$ with conductor a positive integer N and with negative sign of functional equation of the associated zeta function, then the modular parametrization $\phi\colon X_0(N) \to E(\mathbb{C})$ factors as $\phi = \pi_E \circ \pi_{w_N}$, where $\pi_{w_N}\colon X_0(N) \to X_0^+(N)$ is the natural projection and $\pi_E\colon X_0^+(N) \to E$ is the E-map.*

Given the modular curve $X_0^+(N)$ of genus g_+, we denote by $f_1, \dots, f_{g_+}$ a basis of newforms of $\mathcal{S}_2(\Gamma_0(N))$ with eigenvalues $+1$ with respect to the Atkin-Lehner operator w_N. If there is the E-map $\pi_E\colon X_0^+(N) \to E$ for an elliptic curve E with conductor N, then there are four (not unique) homogenous polynomials $p_x, q_x, p_y, q_y \in \mathbb{Z}[x_1, \dots, x_{g_+}]$, such that p_x and q_x have the same degree, p_y and q_y have the same degree and

$$\begin{cases} \phi_x(\tau) = \frac{p_x(f_1(\tau),\dots,f_{g_+}(\tau))}{q_x(f_1(\tau),\dots,f_{g_+}(\tau))} \\ \phi_y(\tau) = \frac{p_y(f_1(\tau),\dots,f_{g_+}(\tau))}{q_y(f_1(\tau),\dots,f_{g_+}(\tau))}, \end{cases}$$

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

To find explicitly these polynomials we use some linear algebra and we proceed similarly to Section 3.3. The main difficulty is that we don't know the degrees of the polynomials. To describe the method we used, we suppose to know the degree d of p_x and q_x and apply this method to the first equation of the system above.

We can rewrite the first equation of the system above as

$$p_x(f_1(\tau), \dots, f_{g_+}(\tau)) - q_x(f_1(\tau), \dots, f_{g_+}(\tau))\phi_x(\tau) = 0.$$

Let $\mathcal{I}$ be the set of the monomials obtained as product of d elements of the basis $f_1, \dots, f_{g_+}$, where repetitions are allowed, and let $\mathcal{J}$ be the set with the same elements of $\mathcal{I}$ multiplied by ϕ_x. Since the Fourier coefficients of $\phi_x, f_1, \dots, f_{g_+}$ are algebraic numbers, also the coefficients of elements of $\mathcal{I}$ and $\mathcal{J}$ are algebraic numbers and there is a number field $\mathfrak{F}$, of degree D over $\mathbb{Q}$, which contains all these Fourier coefficients. Multiplying the elements of $\mathcal{I}$ and $\mathcal{J}$ by a suitable algebraic number, we can assume the Fourier coefficients belonging to ring of integers of $\mathfrak{F}$. Now we can build up the matrix A with $2r$ rows, where r is the number $\binom{g_+ + d - 1}{d}$ of monomials of degree d, and mD columns. The matrix A is filled taking, for a fixed row i, the first D entries equal to the coordinates, with respect to the basis of the number field $\mathfrak{F}$ over $\mathbb{Q}$, of the first coefficient of i-th element of $\mathcal{I}$. Then, we repeat this to the next D entries and so on up to fill the row and again for the first r

rows. The last r rows are filled in the same way but using $\mathcal{J}$ in place of $\mathcal{I}$. So we get the matrix A with integer entries.

Computing the kernel of the tranpose of the matrix A^T we should be able to determine the polynomials p_x and q_x. Usually this kernel will not be trivial and we have to look for columns of kernel that have both the first r rows not all zero and the last r rows not all zero. If there is at least one column with this property, the first r entries of the column are the coefficients of p_x and the last r entries of the column are the coefficients of q_x. If there are more than one column with the requested property, they represent the same map, but defined on different open sets.

3.6 How to use the E-map to find rational points

Let X be a modular curve with an elliptic curve E as component in its jacobian. In this section we suppose to know a Weierstrass equation of E, an analytic expression for the E-map π_E and the generators for the Mordell-Weil group of E. Moreover, for every point of the projective space $\mathbb{P}^n(\mathbb{Q})$ we choose his representative with coordinates $(x_0 : \cdots : x_n)$ such that $x_i \in \mathbb{Z}$ for $i = 0, \ldots, n$ and $\gcd(x_0, \ldots, x_n) = 1$.

We know that π_E is rational, hence every rational point on the modular curve X must go in a rational point on the elliptic curve E. Therefore, to find rational points on X, it is enough to search in the preimage $\pi_E^{-1}(P)$ letting P vary between the rational points of E.

Remark 3.7. In all our cases the Mordell-Weil group has rank one, so we have only one generator, denoted by P_0, that we found using Cremona's tables in [15] or the LMFDB online database [34].

By the above remark, we restrict ourself to the case that the Mordell-Weil group has rank one and its generator is P_0. This implies that every rational point P of E has the form $P = kP_0$ with $k \in \mathbb{Z}$.

Writing π_E in more explicit terms we have

$$\pi_E(x_1, \ldots, x_g) = \left(\frac{p_x(x_1, \ldots, x_g)}{q_x(x_1, \ldots, x_g)}, \frac{p_y(x_1, \ldots, x_g)}{q_y(x_1, \ldots, x_g)} \right),$$

where p_x, q_x are homogenous polynomials with integer coefficients of degree d_x and p_y, q_y are homogenous polynomials with integer coefficients of degree d_y.

The following proposition tells us the range within m must vary to get, if they exist, all rational points on X up to a fixed upper bound for their integer coordinates.

Proposition 3.8. *With the notation as above, if we want to find a rational point on X such that its coordinates in the projective model are not greater than a fixed positive integer δ, we have to compute the multiples kP_0 of the Mordell-Weil generator up to*

$$|k| = k_\delta := \sqrt{\frac{\mu(E) + 1.07 + \frac{\alpha}{2} + d_x \log \sqrt{\delta}}{\hat{h}(P_0)}},$$

where $\mu(E)$ is the function defined in Theorem 1.41, $\hat{h}$ is the canonical height on E, d_x is the degree of the numerator and denominator polynomials of the E-map π_E and α are defined in the proof.

Proof. Let $\Gamma\tau$ be a rational point on X such that its coordinates in the projective model are $x_1, \ldots, x_g \in \mathbb{Z}$ and $\gcd(x_1, \ldots, x_g) = 1$. We denote by P the image of this rational point under the E-map π_E, i.e.

$$\pi_E(x_1, \ldots, x_g) = P = (P_x, P_y),$$

where

$$P_x = \frac{p_x(x_1, \ldots, x_g)}{q_x(x_1, \ldots, x_g)},$$

for some p_x, q_x homogenous polynomials of degree d_x with integer coefficients a_i's and b_i's respectively.

Let β be a positive real number. We know that the set $\{t \in \mathbb{P}^1(\mathbb{Q}) : H(t) \leq \beta\}$ is finite. Since π_E has finite degree, the set $\pi_E^{-1}(\{P \in E(\mathbb{Q}) : H(P_x) \leq \beta\})$ is finite too.

We start showing that if $|x_i| \leq \delta$ for $i = 1, \ldots, g$ then there is a positive real number β such that every well defined $\pi_E(x_1, \ldots, x_g) = P$ with such x_i's has $H(P_x) \leq \beta$.

By the definition of height and using the condition on the x_i's, we have

$$H(P_x) = \max\{|p_x(x_1, \ldots, x_g)|, |q_x(x_1, \ldots, x_g)|\} \leq \delta^{d_x} \max\left\{\sum_i |a_i|, \sum_i |b_i|\right\},$$

so it is enough to define

$$\beta := \delta^{d_x} \max\left\{\sum_i |a_i|, \sum_i |b_i|\right\}.$$

To get the bound on k we take the logarithm in the previous inequality

$$h(P_x) \leq \alpha + d_x \log \delta,$$

where

$$\alpha := \log \max\left\{\sum_i |a_i|, \sum_i |b_i|\right\}.$$

If $P = kP_0$, where P_0 is the Mordell-Weil generator, we have

$$\hat{h}(P) = \hat{h}(kP_0) = k^2 \hat{h}(P_0)$$

by properties of canonical height. Now, by Theorem 1.41, we have

$$\begin{aligned} \hat{h}(P) - \frac{1}{2} h(P_x) &\leq \mu(E) + 1.07 \\ k^2 &\leq \frac{\mu(E) + 1.07 + \frac{\alpha}{2} + d_x \log \sqrt{\delta}}{\hat{h}(P_0)} \\ |k| &\leq \sqrt{\frac{\mu(E) + 1.07 + \frac{\alpha}{2} + d_x \log \sqrt{\delta}}{\hat{h}(P_0)}}. \end{aligned}$$

□

3.7 List of explicit equations

List of explicit equations for a projective model of $X_0^+(p)$ when

$$p = 163, 193, 197, 211, 223, 229, 233, 241, 257, 269, 271, 281, 283.$$

We list the level, the genus, the expected rational points and, when they exist, we list also the elliptic curve E used, an analytic expression for the E-map π_E, the Mordell-Weil generator P_0, the bound δ used and the corresponding k_δ. For the definition of last two values see Proposition 3.8 above.

Level $p = 163$.
Genus $g = 6$.
Equations

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

Rational points and corresponding discriminants

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

Elliptic curve

$$E : y^2 + y = x^3 - 2x + 1.$$

E-map

$$\begin{aligned} \pi_E \colon X &\to E \\ (x_1, x_2, x_3, x_4, x_5, x_6) &\mapsto (P_x, P_y) \\ P_x &= \frac{-2x_3 - x_4 + x_5 - x_6}{-x_3 + x_5} \\ P_y &= \frac{-x_1^2 + x_1x_2 + 2x_1x_3 + 2x_1x_4 + 2x_1x_6 - x_3^2 + x_4^2}{x_1x_3 - x_1x_5}. \end{aligned}$$

Mordell-Weil generator $P_0 = (1, 0)$.
Bound $\delta = 10^{10000}$.
$k_\delta = 247$.

Level $p = 193$.
Genus $g = 7$.
Equations

$$\begin{cases} -x_1^2 - x_1x_4 - x_1x_6 - x_1x_7 + x_2x_7 + x_3^2 + x_3x_4 = 0 \\ x_1x_2 + x_1x_4 - x_1x_5 + x_1x_7 - x_2x_3 - x_2x_4 - x_2x_7 + x_3x_5 = 0 \\ x_1x_2 - x_1x_5 - x_2x_7 + x_3x_6 = 0 \\ -x_1x_2 - x_1x_3 + 2x_1x_5 + x_1x_6 + 2x_2x_3 + 2x_2x_4 - x_3^2 + x_4^2 + x_4x_5 = 0 \\ x_1^2 - x_1x_2 + 2x_1x_4 + x_1x_5 + 2x_1x_6 + x_1x_7 - x_2x_7 - x_3^2 + x_4^2 + x_4x_6 = 0 \\ x_1x_3 - x_1x_4 - x_1x_5 - 2x_1x_6 - x_1x_7 - 2x_2x_3 - 2x_2x_4 + 2x_2x_7 + x_3^2 - x_4^2 + x_4x_7 = 0 \\ x_1^2 + x_1x_3 + x_1x_4 - 2x_1x_5 + x_1x_7 - x_2x_3 - 3x_2x_4 - x_2x_5 - x_2x_7 - x_4^2 + x_5^2 = 0 \\ -x_1^2 + 2x_1x_2 - x_1x_4 - x_1x_5 - 2x_1x_6 - x_1x_7 - x_2x_3 - x_2x_4 + x_2x_7 + x_3^2 - x_4^2 + x_5x_6 = 0 \\ -x_1x_3 + x_1x_5 + x_1x_6 + 2x_2x_3 + 2x_2x_4 - x_2x_7 - x_3^2 + x_4^2 + x_5x_7 = 0 \\ -x_1x_4 - x_1x_5 - x_1x_7 + x_2x_3 - x_2x_4 - x_2x_6 + 2x_2x_7 - x_3x_7 - x_4^2 + x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

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

Level $p = 197$.
Genus $g = 6$.
Equations

$$\begin{cases} -x_1x_2 + x_1x_4 - x_1x_5 - x_1x_6 + x_2x_3 = 0 \\ x_1^2 - x_1x_3 - x_1x_4 + x_1x_5 + x_2x_4 = 0 \\ 2x_1x_2 - 2x_1x_3 - 2x_1x_4 + x_1x_5 + x_1x_6 - x_2^2 - x_2x_6 + x_3^2 + x_3x_4 + x_4^2 = 0 \\ -x_1^2 + x_1x_2 + x_1x_3 + x_1x_6 - x_2^2 - x_2x_6 + x_4x_5 = 0 \\ x_1x_2 - x_1x_3 - x_1x_4 + x_3x_5 + x_4x_6 = 0 \\ -x_1x_2 + x_1x_3 + x_1x_4 - x_1x_6 + x_2x_5 - x_2x_6 - x_3x_5 + x_3x_6 + x_5^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0:0:0:0:0:1)$	cusp
$(1:-1:3:2:6:-6)$	-163
$(1:1:1:1:0:1)$	-43
$(1:0:2:-1:0:-1)$	-28
$(1:1:1:0:0:0)$	-19
$(1:0:0:0:-1:1)$	-16
$(1:0:0:1:0:1)$	-7
$(1:0:2:0:1:-1)$	-4

Elliptic curve

$$E : y^2 + y = x^3 - 5x + 4.$$

E-map

$$\begin{aligned} \pi_E \colon X &\to E \\ (x_1, x_2, x_3, x_4, x_5, x_6) &\mapsto (P_x, P_y) \end{aligned}$$

$$\begin{aligned} \text{Numerator}(P_x) &= -38x_1^2 - 25x_1x_2 - 6x_1x_3 + 13x_1x_4 - 61x_1x_5 + 11x_1x_6 + 22x_2^2 + \\ &\quad + 10x_2x_5 + 20x_2x_6 + 17x_3x_5 - 11x_3x_6 \\ \text{Denominator}(P_x) &= -36x_1^2 - 34x_1x_2 + 11x_1x_3 + 30x_1x_4 - 27x_1x_5 - 8x_1x_6 + 12x_2^2 + \\ &\quad + 5x_2x_5 + 11x_2x_6 \\ \text{Numerator}(P_y) &= 1715x_1^3 - 899x_1^2x_2 - 2691x_1^2x_3 - 1013x_1^2x_4 - 2889x_1^2x_5 - 81x_1^2x_6 + \\ &\quad + 1875x_1x_2^2 + 2476x_1x_2x_5 + 1176x_1x_2x_6 - 669x_1x_3x_5 + 1224x_1x_3x_6 + \\ &\quad + 2205x_1x_5x_6 - 1306x_1x_6^2 - 384x_2^2x_5 - 384x_2x_5x_6 \\ \text{Denominator}(P_y) &= 961x_1^3 - 49x_1^2x_2 + 3875x_1^2x3 - 632x_1^2x_4 + 1195x_1^2x_5 + 356x_1^2x_6 + \\ &\quad + 593x_1x_2^2 + 655x_1x_2x_5 + 432x_1x_2x_6 - 839x_1x_3^2 - 1680x_1x_3x_4 + \\ &\quad + 154x_1x_3x_5 + 384x_1x_5^2. \end{aligned}$$

Mordell-Weil generator $P_0 = (1, 0)$.
Bound $\delta = 10^{10000}$.
$k_\delta = 408$.

Level $p = 211$.
Genus $g = 6$.
Equations

$$\begin{cases} -x_1^2 - x_1x_4 - x_1x_5 + x_2x_3 - x_2x_6 + x_3x_4 = 0 \\ -x_1x_3 - x_1x_4 - x_1x_5 + x_2x_3 - x_2x_6 + x_3x_5 = 0 \\ x_1^2 - x_1x_2 + x_1x_3 + x_1x_4 - x_2x_3 + x_3x_6 = 0 \\ 2x_1^2 - 2x_1x_2 + x_1x_3 + 3x_1x_4 + x_1x_5 - 2x_2x_3 - x_2x_4 + 2x_2x_6 + x_4^2 = 0 \\ x_1x_3 + x_1x_4 + 2x_1x_5 - x_1x_6 - 2x_2x_3 - x_2x_5 + 2x_2x_6 + x_4x_5 = 0 \\ x_1^2 - 2x_1x_2 + x_1x_3 + 2x_1x_4 + x_1x_5 - x_1x_6 - 2x_2x_3 - x_2x_4 + x_2x_5 + 2x_2x_6 - x_4x_6 + x_5^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(1 : 0 : -1 : -1 : 1 : -1)$	-67
$(2 : 1 : 2 : 0 : 0 : -2)$	-28
$(1 : 0 : 1 : -1 : -1 : -1)$	-27
$(0 : 1 : 1 : 0 : 0 : 1)$	-12
$(0 : 0 : 1 : 0 : 0 : 0)$	-8
$(0 : 1 : 0 : 0 : 0 : 0)$	-7
$(2 : -3 : -1 : -2 : 4 : 1)$	-3

Level $p = 223$.
Genus $g = 6$.
Equations

$$\begin{cases} -x_1^2 + x_1x_4 - x_2x_3 - x_2x_4 + x_2x_5 = 0 \\ x_1^2 + 2x_1x_3 - x_1x_4 + x_1x_5 + x_2^2 + 2x_2x_4 + x_2x_6 + x_3^2 = 0 \\ -x_1^2 - x_1x_2 - x_1x_3 + x_1x_4 - x_2x_4 + x_2x_6 + x_3x_4 = 0 \\ x_1^2 - x_1x_2 + 2x_1x_5 - x_1x_6 + x_2^2 + x_2x_4 + 2x_2x_6 + x_3x_5 = 0 \\ -x_1^2 - x_1x_2 + x_1x_3 + x_1x_4 + x_2x_6 - x_3x_6 + x_4x_5 = 0 \\ -2x_1^2 - 2x_1x_2 + x_1x_3 + 3x_1x_4 + 2x_1x_5 + x_1x_6 + x_2^2 + 4x_2x_6 - x_3x_6 - x_4^2 - x_4x_6 + x_5^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(2 : -2 : 2 : 3 : 6 : 7)$	-163
$(1 : 0 : -2 : 1 : 0 : 1)$	-67
$(1 : 0 : 0 : 1 : 0 : 1)$	-27
$(0 : 1 : 1 : -1 : 0 : 0)$	-12
$(0 : 0 : 0 : 1 : 0 : -1)$	-11
$(2 : -3 : -3 : -1 : -6 : 2)$	-3

Level $p = 229$.
Genus $g = 7$.
Equations

$$\begin{cases} -x_1x_5 + x_2x_4 - x_2x_6 + x_2x_7 = 0 \\ x_1x_2 - x_1x_3 - x_1x_4 - x_1x_5 + x_2x_3 + x_2x_4 - x_2x_6 + x_3^2 + x_3x_4 = 0 \\ -x_1x_5 + x_2^2 + x_2x_3 + x_2x_4 - x_2x_5 - x_2x_6 + x_3x_5 = 0 \\ x_1x_2 - x_1x_3 - x_1x_4 - x_1x_6 - x_2^2 + x_2x_4 + x_3^2 + x_3x_6 = 0 \\ x_1x_2 + x_1x_3 - x_1x_6 - x_1x_7 - x_2^2 - x_2x_3 + x_2x_6 + x_3x_7 = 0 \\ -2x_1x_2 + x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 - x_2x_3 - x_2x_4 + x_2x_6 - x_3^2 + x_4^2 = 0 \\ -x_1x_3 + x_1x_6 - x_2^2 - x_2x_3 - x_2x_4 + x_2x_5 + x_4x_5 = 0 \\ -x_1x_2 + x_1x_5 + x_1x_7 + x_2x_4 - x_2x_5 + x_5x_6 = 0 \\ x_1x_2 - 2x_1x_5 - x_1x_6 - x_1x_7 + x_2x_3 + 2x_2x_4 - x_2x_5 - x_2x_6 + x_3^2 - x_4x_6 + x_5x_7 = 0 \\ x_1x_5 - x_2x_3 - x_2x_4 - x_3^2 - x_4x_7 + x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0:0:0:0:0:0:1)$	cusp
$(1:1:0:1:1:0:0)$	-43
$(1:0:1:0:0:1:0)$	-27
$(0:0:0:0:1:0:0)$	-19
$(0:0:1:-1:0:-1:0)$	-16
$(0:1:-1:0:0:0:0)$	-12
$(1:0:0:0:0:0:0)$	-11
$(2:0:1:-1:0:1:0)$	-4
$(2:-3:-1:0:-6:-4:0)$	-3

Elliptic curve

$$E : y^2 + xy = x^3 - 2x - 1.$$

E-map

$$\pi_E \colon X \to E$$
$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \mapsto (P_x, P_y)$$

$$P_x = \frac{-x_2 - x_5 + x_6}{x_2 + x_5}$$

$$\begin{aligned} \text{Numerator}(P_y) = {} & x_1^2 + 3x_1x_2 + 7x_1x_3 + 6x_1x_4 + x_1x_5 - x_1x_6 - 4x_1x_7 - 2x_2x_3 - 2x_2x_4 + \\ & + 3x_2x_6 - 2x_3^2 + x_4x_6 - 2x_4x_7 - x_6x_7 \end{aligned}$$

$$\text{Denominator}(P_y) = x_1^2 + 5x_1x_2 + x_1x_4 + 2x_1x_5 - x_1x_6 - x_1x_7 - x_3^2 - x_4x_7 + x_6^2.$$

Mordell-Weil generator $P_0 = (-1, 1)$.
Bound $\delta = 10^{10000}$.
$k_\delta = 210$.

Level $p = 233$.
Genus $g = 7$.
Equations

$$\begin{cases} -x_1x_2 - x_1x_3 - x_1x_4 + x_2^2 - x_2x_3 - x_2x_5 - x_2x_6 + x_2x_7 = 0 \\ x_1x_2 + x_1x_4 - x_2^2 + x_2x_6 + x_3x_5 = 0 \\ x_1^2 - 2x_1x_2 - x_1x_3 + x_1x_5 + 2x_2^2 - 2x_2x_3 - x_2x_4 - 2x_2x_5 - x_2x_6 + x_3x_6 = 0 \\ -2x_1x_3 - x_1x_6 + x_2^2 - x_2x_3 - x_2x_4 - x_2x_5 + x_3x_7 = 0 \\ x_1^2 - 2x_1x_2 + x_1x_4 + x_1x_5 + 2x_2^2 - 2x_2x_3 - 2x_2x_5 - x_2x_6 + x_3x_4 + x_4^2 = 0 \\ x_1x_3 + x_1x_6 - x_2^2 + x_2x_3 + x_2x_5 + x_4x_5 = 0 \\ x_1x_2 + x_1x_3 - x_1x_7 - x_2^2 + x_2x_3 - x_2x_4 + x_2x_5 + x_2x_6 + x_4x_6 = 0 \\ -x_1x_2 - x_1x_3 - x_1x_4 + x_1x_5 - x_1x_6 - x_1x_7 + 2x_2^2 - x_2x_3 - x_2x_4 - 2x_2x_5 - x_2x_6 + x_5^2 = 0 \\ -x_1^2 + x_1x_2 + 2x_1x_3 - x_1x_5 + x_1x_6 + x_1x_7 - 2x_2^2 + 2x_2x_3 + x_2x_4 + 2x_2x_5 + x_4x_7 + x_5x_6 = 0 \\ -x_1^2 + x_1x_2 - x_1x_5 + x_2x_4 - x_2x_6 + x_5x_7 + x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(1 : 0 : 2 : -2 : 1 : 0 : 2)$	-28
$(0 : 0 : 1 : -1 : 0 : 0 : 0)$	-19
$(1 : 1 : 0 : 0 : 1 : 0 : 1)$	-16
$(0 : 0 : 1 : 0 : 0 : 0 : 0)$	-8
$(1 : 0 : 0 : 0 : -1 : 0 : 0)$	-7
$(1 : 1 : 0 : -2 : 1 : 2 : 1)$	-4

Level $p = 241$.
Genus $g = 7$.
Equations

$$\begin{cases} x_1^2 + x_1x_4 - x_2^2 - x_2x_4 + x_2x_6 = 0 \\ x_1x_5 - x_2x_3 - x_2x_5 + x_2x_7 = 0 \\ x_1x_2 + 2x_1x_3 + x_1x_6 - x_1x_7 - x_2^2 + x_3^2 = 0 \\ x_1x_3 - x_1x_7 + x_2x_4 + x_3x_4 = 0 \\ -x_1x_4 - x_1x_5 - x_2x_4 + x_2x_5 - x_3x_5 - x_4^2 + x_4x_5 = 0 \\ -x_1^2 + x_1x_2 - x_1x_3 + x_1x_4 + x_1x_5 + x_1x_7 + x_2x_3 - 2x_2x_4 - x_2x_5 + x_3x_5 - x_3x_6 + x_4x_6 = 0 \\ -x_1^2 - x_1x_3 + x_1x_4 - x_1x_6 + x_2^2 + x_2x_3 - x_2x_4 + x_3x_5 - x_3x_6 - x_3x_7 + x_4x_7 = 0 \\ -x_1x_2 + x_1x_3 - 3x_1x_4 - x_1x_5 + x_1x_6 + x_2^2 + x_2x_4 - x_3x_5 + x_3x_6 - x_4^2 + x_5^2 = 0 \\ -x_1^2 - x_1x_3 + x_1x_4 + x_1x_5 - x_1x_6 + x_2^2 + x_2x_3 - 2x_2x_4 - x_2x_5 + x_3x_5 - x_3x_6 - x_3x_7 + x_5x_6 = 0 \\ -x_1^2 + x_1x_2 - x_1x_3 + x_1x_4 + 2x_1x_5 + x_1x_7 + x_2x_3 - 2x_2x_4 - 2x_2x_5 + x_5x_7 + x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(1 : 0 : -2 : -1 : 0 : 0 : 0)$	-67
$(0 : 1 : -1 : 0 : 0 : 1 : -1)$	-27
$(1 : 1 : 0 : 0 : 0 : 0 : 0)$	-16
$(1 : 1 : 0 : 0 : 1 : 0 : 0)$	-12
$(0 : 0 : 0 : 1 : 1 : 0 : 0)$	-8
$(1 : -1 : -2 : 0 : 0 : 0 : -2)$	-4
$(3 : 1 : -4 : -6 : -3 : 4 : 2)$	-3

Level $p = 257$.
Genus $g = 7$.
Equations

$$\begin{cases} -x_1^2 - x_1x_2 + x_1x_4 - x_2^2 - x_2x_4 + x_2x_5 = 0 \\ -x_1^2 - 2x_1x_2 + x_1x_3 + x_1x_4 - x_1x_5 - 2x_2^2 - x_2x_4 + x_2x_6 = 0 \\ -x_1x_2 - x_1x_6 - x_2x_3 + x_2x_7 = 0 \\ x_1x_2 - x_1x_3 + x_1x_6 + x_2^2 + x_2x_4 + x_3x_4 = 0 \\ -x_1x_3 - x_1x_4 + x_1x_6 - x_1x_7 + x_2^2 - x_2x_3 + x_2x_4 + x_3x_5 = 0 \\ x_1^2 + x_1x_2 - x_1x_3 - x_1x_4 + 2x_2^2 - x_2x_3 + 2x_2x_4 - x_3x_6 + x_4x_5 = 0 \\ x_1^2 + x_1x_2 - 2x_1x_4 + x_1x_5 - x_1x_7 + 2x_2^2 - x_2x_3 + x_2x_4 + x_3^2 - x_3x_6 - x_3x_7 + x_4x_6 = 0 \\ x_1^2 - x_1x_3 - x_1x_4 - x_1x_5 - x_1x_6 + x_2^2 - x_2x_3 + x_2x_4 - x_3^2 - x_3x_6 + x_3x_7 + x_5^2 = 0 \\ x_1^2 + x_1x_3 - 2x_1x_4 - 2x_1x_7 + x_2^2 - x_2x_3 + x_2x_4 + x_3^2 - x_3x_6 - x_3x_7 + x_4x_7 + x_5x_6 = 0 \\ -2x_1x_2 + 2x_1x_3 - 2x_1x_6 - x_1x_7 - 2x_2^2 - x_2x_4 - x_3x_6 + x_4x_7 - x_5x_7 + x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(1 : 0 : 0 : 1 : 0 : 0 : -1)$	-67
$(0 : 1 : 0 : -1 : 0 : 1 : 0)$	-16
$(0 : 0 : 1 : 0 : 0 : 0 : 1)$	-11
$(0 : 0 : 0 : 1 : 0 : 0 : 0)$	-8
$(2 : -1 : 0 : 1 : 0 : 1 : 0)$	-4

Level $p = 269$.
Genus $g = 6$.
Equations

$$\begin{cases} x_1x_4 + x_2^2 + x_2x_3 + x_3^2 + x_3x_5 = 0 \\ -x_1x_2 - x_1x_5 + x_2^2 + x_2x_3 + x_2x_5 + x_3x_6 = 0 \\ x_1x_2 + 2x_1x_4 + x_1x_6 + x_3^2 + x_3x_4 + x_4^2 = 0 \\ x_1x_2 - x_1x_4 + x_1x_5 - x_2^2 - x_2x_3 + x_2x_4 + x_3x_4 + x_4x_5 = 0 \\ x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6 - x_2x_3 - x_2x_5 + x_4x_6 = 0 \\ -x_1x_2 - x_1x_3 - 2x_1x_4 - x_1x_5 - x_1x_6 - x_2^2 + 2x_2x_5 - x_2x_6 - x_3^2 + x_5^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0:0:0:0:0:1)$	cusp
$(1:-1:0:-1:1:2)$	-67
$(1:1:0:-1:-1:0)$	-43
$(1:1:0:-1:0:0)$	-16
$(1:0:0:0:0:0)$	-11
$(1:-1:2:-3:0:0)$	-4

Elliptic curve

$$E : y^2 + y = x^3 - 2x - 1.$$

E-map

$$\begin{aligned} \pi_E \colon X &\to E \\ (x_1, x_2, x_3, x_4, x_5, x_6) &\mapsto (P_x, P_y) \\ P_x &= \frac{x_4 + x_6}{x_2} \\ P_y &= \frac{x_1x_5 - x_2x_3 + x_3x_4}{x_1x_2} \end{aligned}$$

Mordell-Weil generator $P_0 = (-1, 0)$.
Bound $\delta = 10^{10000}$.
$k_\delta = 187$.

Level $p = 271$.
Genus $g = 6$.
Equations

$$\begin{cases} x_1^2 + 2x_1x_2 + x_1x_5 - x_1x_6 - x_2x_4 - 2x_2x_5 - x_2x_6 + x_3x_5 = 0 \\ x_1^2 + x_1x_2 - x_1x_4 - x_1x_6 - x_2x_3 - x_2x_4 - x_2x_5 - x_2x_6 + x_4^2 = 0 \\ -x_1^2 - 2x_1x_2 - x_1x_5 + x_1x_6 + x_2x_3 + x_2x_4 + x_2x_5 + x_4x_5 = 0 \\ x_1x_2 - x_1x_4 - x_1x_6 - x_2x_3 + x_2x_6 + x_3^2 + x_4x_6 = 0 \\ x_1^2 + 3x_1x_2 + 2x_1x_3 + x_1x_5 - 3x_1x_6 - 2x_2x_4 - x_2x_5 + x_5^2 = 0 \\ -x_1x_2 - x_1x_3 - x_1x_4 - x_1x_5 + x_1x_6 - x_2x_3 + x_2x_4 + x_2x_5 + x_2x_6 + x_3x_4 + x_5x_6 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(1 : 0 : 1 : 1 : 0 : 1)$	-43
$(0 : 1 : 1 : 1 : -1 : 0)$	-27
$(0 : 1 : 0 : 0 : 0 : 0)$	-19
$(1 : 0 : 1 : 0 : 0 : 1)$	-12
$(3 : -2 : -5 : 4 : -4 : -3)$	-4

Level $p = 281$.
Genus $g = 7$.
Equations

$$\begin{cases} -x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 - x_3x_4 + x_3x_6 = 0 \\ -x_1x_6 - x_2x_3 - x_2x_4 - x_2x_5 + x_3^2 + x_3x_5 + x_3x_7 = 0 \\ x_1x_2 + x_1x_7 + 2x_3x_4 - x_3x_5 + x_4^2 = 0 \\ -x_1x_2 - 2x_1x_3 - x_1x_4 - x_1x_5 - x_1x_7 - x_2x_3 + 2x_3x_5 + x_4x_5 = 0 \\ x_1x_2 - x_1x_3 + x_2x_5 + 2x_3x_4 + x_4x_6 = 0 \\ 2x_1x_3 + 2x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 - x_2^2 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 - 2x_3x_5 + x_4x_7 = 0 \\ x_1x_2 + 2x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 + x_2x_3 - x_2x_4 - x_3x_5 + x_5^2 = 0 \\ x_1x_2 - x_1x_3 + x_2^2 - x_2x_3 - x_2x_4 - x_2x_5 + x_3x_5 + x_5x_6 = 0 \\ x_1x_2 - x_1x_3 - x_1x_4 - x_1x_7 + x_2^2 + x_2x_6 + x_3x_5 + x_5x_7 = 0 \\ x_1x_2 - x_1x_3 + x_1x_6 - x_2x_3 - x_2x_4 - x_2x_7 + 2x_3x_4 + x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0 : 0 : 0 : 0 : 0 : 0 : 1)$	cusp
$(2 : -5 : -5 : -1 : 1 : 5 : -3)$	-163
$(0 : 1 : -1 : 1 : 1 : 1 : -1)$	-43
$(0 : 0 : 1 : -2 : 0 : -2 : -1)$	-28
$(1 : 0 : 0 : 0 : 0 : 0 : 0)$	-16
$(1 : 0 : 0 : 1 : 0 : 0 : -1)$	-8
$(0 : 0 : 1 : 0 : 0 : 0 : -1)$	-7
$(1 : 2 : -2 : 2 : 2 : 0 : -2)$	-4

Level $p = 283$.
Genus $g = 9$.
Equations

$$\begin{cases}
x_1x_2 + x_1x_3 + x_1x_4 - x_1x_5 + x_1x_7 + x_3x_5 = 0\\
-x_1x_2 - x_1x_3 - 2x_1x_7 - x_1x_8 - x_1x_9 - x_3^2 + x_3x_6 = 0\\
x_1x_3 - x_1x_5 - x_1x_6 + x_1x_7 - x_2^2 - x_2x_3 + x_2x_5 + x_3^2 + x_3x_4 + x_3x_7 = 0\\
x_1x_2 + 3x_1x_3 - x_1x_5 - x_1x_6 + 3x_1x_7 + x_1x_8 + x_1x_9 - x_2^2 - x_2x_3 + x_2x_5 + x_2x_6 - x_2x_7 +\\
\quad +2x_3^2 + 2x_3x_4 + x_3x_8 = 0\\
2x_1x_2 + 2x_1x_3 + x_1x_4 + x_1x_6 + 2x_1x_7 + 2x_1x_8 + 2x_1x_9 + x_2x_3 - x_2x_7 - x_2x_8 + x_3^2 + x_3x_4 + x_3x_9 = 0\\
-x_1x_2 - x_1x_5 - x_1x_6 - x_1x_8 - x_2x_3 + x_2x_5 + x_2x_6 + x_3x_4 + x_4^2 = 0\\
-x_1x_2 - 2x_1x_3 - 2x_1x_7 - 2x_1x_8 - x_1x_9 - x_2x_4 - x_3^2 - x_3x_4 + x_4x_5 = 0\\
2x_1x_2 + x_1x_3 + x_1x_4 + x_1x_6 + x_1x_7 + x_1x_8 - x_3x_4 + x_4x_6 = 0\\
2x_1x_2 + x_1x_3 + x_1x_4 + x_1x_6 + x_1x_7 + x_1x_8 + x_1x_9 + x_2x_3 + x_4x_7 = 0\\
-x_1^2 - x_1x_2 - 3x_1x_3 - x_1x_4 + x_1x_5 - 2x_1x_7 - 2x_1x_8 - x_1x_9 + x_2^2 + x_2x_3 - x_2x_5 - x_3^2 - x_3x_4 + x_4x_8 = 0\\
x_1^2 - 3x_1x_2 - 2x_1x_3 - x_1x_4 + x_1x_5 - 2x_1x_7 - x_1x_9 + x_2^2 + x_2x_3 + x_2x_4 - x_2x_5 - x_2x_6 + x_2x_7 + x_4x_9 = 0\\
x_1x_9 - x_5x_6 + x_5x_7 = 0\\
-x_1^2 - x_1x_2 - x_1x_3 - 2x_1x_4 + x_1x_5 - x_1x_6 - x_1x_8 - x_2x_3 + x_2x_6 + x_5x_8 = 0\\
x_1^2 - x_1x_2 + x_1x_3 + x_1x_7 + 2x_1x_8 + x_1x_9 + x_2x_5 + x_3^2 + x_3x_4 + x_5x_9 = 0\\
-2x_1x_2 - 3x_1x_3 - x_1x_4 + x_1x_5 - 4x_1x_7 - 2x_1x_8 - 2x_1x_9 - x_3^2 + x_5x_6 + x_6^2 = 0\\
-x_1x_2 - x_1x_3 - x_1x_4 - x_1x_6 - x_1x_7 - x_1x_8 - 2x_1x_9 - x_2^2 - x_2x_3 + x_2x_5 + x_5x_6 + x_6x_7 = 0\\
x_1^2 + x_1x_2 + 4x_1x_3 + x_1x_4 - x_1x_5 + 4x_1x_7 + 3x_1x_8 + 2x_1x_9 - x_2^2 - x_2x_3 + x_2x_5 - x_2x_7 +\\
\quad +2x_3^2 + 2x_3x_4 + x_6x_8 = 0\\
-x_1^2 + 4x_1x_2 + 4x_1x_3 + x_1x_4 - x_1x_5 + 4x_1x_7 + 2x_1x_8 + 3x_1x_9 - x_2^2 - x_2x_3 + x_2x_5 +\\
\quad +x_2x_6 - x_2x_7 - x_2x_8 + x_3^2 + x_3x_4 + x_6x_9 = 0\\
-x_1x_3 + x_1x_5 + x_1x_6 - 2x_1x_7 - x_1x_9 - x_2x_6 - x_2x_8 - x_3^2 - x_3x_4 + x_5x_6 + x_7^2 = 0\\
-x_1x_3 + x_1x_5 + x_1x_6 - x_1x_7 - x_2x_5 - x_2x_6 - x_2x_9 - x_3^2 - x_3x_4 + x_7x_8 = 0\\
-x_1^2 - x_1x_2 - 5x_1x_3 - x_1x_4 + x_1x_5 + x_1x_6 - 5x_1x_7 - 3x_1x_8 - 2x_1x_9 + x_2^2 +\\
\quad +x_2x_3 - x_2x_5 - x_2x_6 + x_2x_7 - 3x_3^2 - 3x_3x_4 - x_7x_9 + x_8^2 = 0
\end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(0:0:0:0:0:0:0:0:0:1)$	cusp
$(1:0:2:-1:0:1:-1:-2:0)$	-67
$(0:1:0:0:1:-1:-1:1:-1)$	-43
$(0:0:0:0:1:-1:-1:0:0)$	-27
$(0:0:0:0:1:0:0:0:0)$	-19
$(1:0:1:-1:0:1:0:-1:0)$	-12
$(0:0:1:-1:0:1:0:0:0)$	-8
$(3:0:-3:3:2:-5:4:3:-6)$	-3

List of explicit equations for a projective model of $X_{ns}^{+}(p)$ where

$$p = 17.$$

We list the level, the genus and the rational points associated to Heegner points.

Level $p = 17$.
Genus $g = 6$.
Equations

$$\begin{cases} -3x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + 2x_2x_4 + x_2x_5 - x_2x_6 - 2x_3^2 + \\ \quad +2x_3x_4 + 2x_3x_5 + x_3x_6 + x_4x_5 - x_4x_6 + x_5^2 - x_5x_6 = 0 \\ \\ x_1x_2 - 2x_1x_3 - 2x_1x_4 + x_1x_6 + x_2x_5 + 2x_2x_6 - x_3x_4 - 2x_3x_5 + \\ \quad +x_4^2 - x_4x_5 + x_4x_6 - 2x_5^2 + x_6^2 = 0 \\ \\ 3x_1^2 + 3x_1x_2 + x_1x_3 - x_1x_4 + x_1x_6 + x_2x_3 - x_2x_4 + x_2x_5 + 2x_2x_6 + \\ \quad +x_3^2 - x_3x_4 - x_4^2 - x_4x_5 - x_4x_6 + x_5^2 + 2x_5x_6 = 0 \\ \\ 2x_1^2 + 2x_1x_2 - 2x_1x_3 + x_1x_4 - 2x_1x_5 + x_1x_6 - x_2x_3 - x_2x_5 + \\ \quad +3x_2x_6 - x_3^2 + 3x_3x_4 - 3x_3x_5 - x_4^2 - x_4x_5 + 2x_5^2 - x_5x_6 + x_6^2 = 0 \\ \\ x_1x_2 + 5x_1x_3 + 2x_1x_4 - x_1x_5 + x_2^2 + 3x_2x_3 + 2x_2x_4 - x_2x_5 - x_3^2 + \\ \quad +2x_3x_4 - 3x_3x_5 + x_4^2 + 3x_4x_6 - x_5^2 - 2x_5x_6 - x_6^2 = 0 \\ \\ -3x_1x_2 + x_1x_3 - 2x_1x_4 + 4x_1x_5 - 3x_1x_6 - 3x_2^2 - 2x_2x_3 - 5x_2x_4 + \\ \quad +x_2x_5 - x_2x_6 + x_3^2 + x_3x_4 - 3x_3x_5 + x_4^2 - 2x_4x_5 - 2x_4x_6 + x_5^2 + 3x_5x_6 - x_6^2 = 0. \end{cases}$$

Rational points and corresponding discriminants

Rational point	Discriminant
$(-7 : 9 : 35 : 21 : 5 : 1)$	-163
$(0 : 0 : 0 : 1 : 1 : 1)$	-28
$(2 : -5 : -10 : -6 : 1 : 7)$	-27
$(-4 : 10 : 3 : -5 : -2 : 3)$	-12
$(3 : 1 : 2 : -9 : -7 : 2)$	-11
$(-6 : -2 : -4 : 1 : -3 : 13)$	-7
$(2 : -2 : -1 : 3 : -2 : 1)$	-3

Bibliography

[1] T.M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Springer-Verlag, New York (1976).

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

[3] A.O.L. Atkin and W.C.W. Li, *Twists of Newforms and Pseudo-Eigenvalues of W-Operators*, Inv. Math. **48** (1978), 221-234.

[4] A. Bajolet and Y. Bilu, *Computing Integral Points on $X_{ns}^+(p)$*, http://arxiv.org/pdf/1212.0665v1.pdf (2012).

[5] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204-216.

[6] B. Baran, *A Modular Curve of Level 9 and the Class Number One Problem*, http://arxiv.org/pdf/0801.4693v2.pdf (2009).

[7] B. Baran, *An Exceptional Isomorphism Between Modular Curves of Level 13*, to appear (2012).

[8] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves and the class number one problem*, Journal of Number Theory **130** issue 12 (2010), 2753-2772.

[9] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi sums*, John Wiley & Sons, Inc., New York (1998).

[10] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Annals of Mathematics **173** (2011), 569-584.

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

[12] B.J. Birch and W. Kuyk, [eds.] *Modular Functions of One Variable IV* (Proc. Internat. Summer School, Univ. of Antwerp, RUCA, 1972), Lecture Notes in Math. **476**, Springer-Verlag, Berlin, Heidelberg, New York (1975), Table 5, 135-141.

[13] A. Brumer and K. Kramer, *The Rank of Elliptic curves*, Duke Mathematical Journal Vol. **44** No. 4 (1977), 715-743.

[14] I. Chen, *The jacobian of the modular curve* $X^{+}_{non\text{-}split}(p)$, Oxford (1994).

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

[16] B. de Smit and B. Edixhoven, *Sur un résultat d'Imin Chen*, Math. Res. Lett. (7) **2-3** (2000), 147-153.

[17] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular Functions of One Variable II (Proc. Internat. Summer School, Univ. of Antwerp, RUCA, 1972), Lecture Notes in Math. **349**, Springer-Verlag, Berlin, Heidelberg, New York (1973), 143-316.

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

[19] B. Edixhoven, *Modular parametrizations at primes of bad reduction*, unpublished (2001).

[20] B. Edixhoven, *On a result of Imin Chen*, http://arxiv.org/pdf/alg-geom/9604008v1.pdf (2013).

[21] E. Freitag and R. Busam, *Complex Analysis*, Springer-Verlag, Berlin, Heidelberg (2005).

[22] W. Fulton and J. Harris, *Representation Theory. A First Course*, Springer-Verlag, New York (1991).

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

[24] S.D. Galbraith, *Rational Points on* $X^{+}_{0}(p)$, Experimental Mathematics Vol. **8** No. 4 (1999).

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

[26] R. Gunning, *Lectures on Modular Forms*, Princeton University Press: Princeton, New Jersey (1962).

[27] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York (1977).

[28] K. Heegner, *Diophantische analysis und modulfunktionen*, Math. Zeit. (1952), 227-253.

[29] N.M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press: Princeton, New Jersey (1985).

[30] A.W. Knapp, *Elliptic Curves*, Princeton University Press: Princeton, New Jersey (1992).

[31] S. Lang, *Algebra* (3rd ed.), Graduate Texts in Mathematics **211**, Springer-Verlag, New York (2002).

[32] S. Lang, *Introduction to Modular Forms*, Springer-Verlag, Berlin Heidelberg (1976).

[33] G. Ligozat, *Courbes modulaires de niveau 11*, Modular Functions of One Variable V (Proc. Internat. Conference, Univ. Bonn, Bonn, 1977), Lecture Notes in Math. **601**, Springer-Verlag, Berlin (1977), 149-238.

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

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

[36] B. Mazur, *Rational Isogenies of Prime Degree*, Inv. Math. **44** (1978), 129-162.

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

[38] T. Miyake, *Modular Forms*, Springer-Verlag, Berlin Heidelberg (2006).

[39] A.P. Ogg, *Rationals points on certain elliptic modular curves*, Analytic number theory (St. Louis, MO, 1972), Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence (1973), 221-231.

[40] I. Piatetski-Shapiro, *Complex Representations of* GL(2, *K*) *for Finite Fields K*, Contemp. Math. **16**, AMS, New York (1983).

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

[42] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics **7**, Springer-Verlag, New York (1973).

[43] J.-P. Serre, *Lectures on the Mordell-Weil Theorem* (3rd ed.), Aspects of Mathematics **E 15**, Vieweg, Braunschweig/Wiesbaden (1989).

[44] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. **15** (1972), 259-331.

[45] G. Shimura, *Introduction To The Arithmetic Theory Of Automorphic Functions*, Iwanami Shoten and Princeton University Press (1971).

[46] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* (2^{nd} ed.), Graduate Texts in Mathematics **151**, Springer-Verlag, New York (1999).

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

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

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

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