Construction of modular curves and computation of their cardinality over $\mathbb{F}_p$

Cdric Tavernier

Projet codes, Bâtiment 10, INRIA Rocquencourt 78150 Le Chesnay, France

Abstract. Following [3], and in using several results, we describe an algorithm which compute with a level N given the cardinality over $\mathbb{F}_p$ of the Jacobian of elliptic curves and hyperelliptic curves of genus 2 which come from $X_0(N)$. We will also sketch how to get a plane affine model for these curves.

1 Introduction

Elliptic curves are used for electronic signature. A required condition to have a secure cryptosystem is to have $\#Jac(C(\mathbb{F}_p))$ nearly prime. It is known that the computation over $\mathbb{F}_p$ of elliptic curves and hyperelliptique curves of genus two is a difficult problem. Several algorithms (Schoof (1985), Atkin, Elkies, Sato, Pila, Huang) exist with polynomial complexity in $Log(p)$. These methods consist in computing the Frobenius action on l-torsion points. This gives the cardinality modulo l (CRT construction). A new way : G. Frey and M.Mller (1998), used $X_0(N)$ and newforms to compute the cardinalities of jacobian of elliptic and hyperelliptic modular curves over $\mathbb{F}_p$.

In section two we will give some results and definitions about $X_0(N)$. The curves $X_0(N)$ has a structure of Riemann surface compact and it is a curve with rational coefficients, so we will study the space of holomorphic differentials $\Omega^1(X_0(N))$ of $X_0(N)$. In fact $\Omega^1(X_0(N))$ is isomorphic to the space of modular forms which are vanishing on cusps of $X_0(N)$ and this space is called space of cusp-forms.

In the third section we will introduce the Hecke algebra. The Hecke algebra is generated by some operators called the Hecke operators and the Atkin-Lehner operators. We will see how this algebra acts on the modular curves $X_0(N)$ and further more on its Jacobian and on its homology. In consequence, we will give some definitions and results about a sub-space of the cusp-forms which is called the space of new-forms.

In the fourth section we will study the first homology group $H_1(X_0(N), \mathbb{Z})$ and the relative homology $H_1(X_0(N), cusps, \mathbb{Z})$ and we will see that there is a correspondence between the homology group and cusp-forms. An important problem is to give a representation for the elements of the homology groups and we want a representation which can be easily computed. Thus we will study two methods, one using the theory of modular symbols and one using the Manin-symbols. We will present the algorithms which permit to convert

Modular-symbols into Manin-symbols and conversely. With these theories we will be able to restrict to new-forms.

In the fifth section we will summarize some results about modular Abelian varieties. We know that for a level N given the new-forms are in correspondence with Abelian varieties of conductor N^g where g is the dimension of these Abelian varieties. In particular we are interested in computing the cardinality over $\mathbb{F}_p$ of these Abelian varieties, so we will give some results about L-series and Abelian varieties.

In the sixth section we will describe the algorithm to compute the cardinality $\mathbb{F}_p$ of Abelian varieties coming from new-forms, and more specially we will give a method to restrict to Abelian varieties of dimension one, that is to say elliptic curves, and Abelian varieties of dimension two which are sometimes Jacobian of modular hyperelliptic curves of genus two.

In the seventh section we will sketch some possible algorithms to obtain an affine model of curve C such that the the Jacobian of C is isogeneous to A_f, we will apply some methods due to [1] for genus one and [10] for the genus two.

2 About modular curves $X_0(N)$

Here, we give some definitions and results about $X_0(N)$.

We know that $SL_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $R = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

For a positive integer N, we consider the group denoted by

$$\Gamma_0(N) = \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \ mod \ N \right\}.$$

which is the Hecke subgroup of $SL_2(\mathbb{Z})$ of level N. The groups $SL_2(\mathbb{Z})$ and $\Gamma_0(N)$ act on the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by homographic transformations given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z \longmapsto \frac{az+b}{cz+d}.$$

We denote the orbits of this action by $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$. The quotient $Y_0(N)$ is equipped with a complex analytic structure which comes from $\pi : \mathbb{H} \longrightarrow \Gamma_0(N)\backslash\mathbb{H}$. We compactify $Y_0(N)$ by adjoining the set of cusps $\mathbb{Q} \cup \{\infty\}$. We denote $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ and we denote

$$X_0(N) = \Gamma_0(N)\backslash\mathbb{H}^*,$$

the modular curve of $\Gamma_0(N)$. So $X_0(N)$ is a Riemann surface compact and it can be seen as a projective algebraic curve defined over $\mathbb{C}$.

Definition 1 *A modular form for $\Gamma_0(N)$ of weight 2 is a function $f : \mathbb{H} \longrightarrow \mathbb{C}$ such that*

1. *f is holomorphic on $\mathbb{H}$;*
2. *for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $f(\gamma z) = (cz+d)^2 f(z)$;*
3. *f is holomorphic at the cusps.*

We denote this space by $M_2(N)$. If a modular form f vanishes at the cusps, then f is called a cusp-form and we denote the space of cusp-forms of weight two, $S_2(N)$.

Proposition 1 *Let π be the quotient map $\mathbb{H}^* \longrightarrow \Gamma_0(N)\backslash\mathbb{H}^*$, and for any holomorphic differential ω on $\Gamma_0(N)\backslash\mathbb{H}^*$, set $\pi^*\omega = f dz$. Then $\omega \longmapsto f$ is an isomorphism from the space of holomorphic differentials $\Omega^1(X_0(N))$ on $\Gamma_0(N)\backslash\mathbb{H}^*$ to $S_2(N)$. The dimension of $S_2(N)$ as a complex vector space is equal to the genus of the curve $X_0(N)$.*

3 The Hecke algebra $\mathbb{T}_N$

Let $\tau \in \mathbb{H}$. We denote by E the elliptic curve $\mathbb{C}/L$ where $L = \mathbb{Z} + \mathbb{Z}\tau$. Let C_N be a cyclic subgroup of order N of $E[N]$, the group of N-torsion points. Then, by $P = (E, C_N)_\sim$ we denote the isomorphism class of a pair (E, C_N). Using the modular interpretation of the points on $X_0(N)_\mathbb{Z}$ we can define the Atkin-Lehner operators which are also called Atkin-Lehner involutions [2] and are denoted W_n . Let n be a positive divisor of N such that $\gcd(n, N/n) = 1$, then the action of the n-th Atkin-Lehner operator is given by

$$W_n(P) = (E/C_n, (C[n] \times C_{N/n})/C_n)_\sim.$$

Also using the modular interpretation we define the Hecke operator [2]. Let n not dividing N, then the n-th Hecke operator is denoted T_n and its action is given by

$$T_n(P) = \sum_G (E/G, (C[n] \times C_{N/n})/C_n)_\sim,$$

where G runs thought the set of subgroups of order n of E that have trivial intersection with $(C[n] \times C_{N/n})$. As a consequence, W_n and T_n act on

1. the Jacobian variety $J_0(N)$ of $X_0(N)$;
2. the space of cusp forms $S_2(N)(\mathbb{Z})$;
3. the homology group $H_1(X_0(N), \mathbb{Z})$.

Definition 2 *The Hecke algebra $\mathbb{T}_N$ of level N is the $\mathbb{Z}$-sub-algebra of the endomorphism ring $End_\mathbb{Z}(\Omega^1(X_0(N))_\mathbb{Z})$ generated by*

$$W_n \text{ with } n|N,\ \gcd(n, N/n) = 1 \text{ and } T_k \text{ with } \gcd(k, N) = 1.$$

The Hecke algebra is commutative.

Theorem 1 *The operators T_n and W_n have the following properties:*

1. $T_{nm} = T_n T_m$ *if* $\gcd(m,n) = 1$;
2. $T_p T_{p^r} = T_{p^{r+1}} + pT_{p^{r-1}}$ *if p prime doesn't divide N;*
3. $T_p T_{p^r} = T_p^r,\ r \geq 1$, *if p divides N.*

Definition 3 *A cusp-form $f \in S_2(N)$ is a Hecke-eigenform, if f satisfies*

$$T(f) = \lambda_T \cdot f \text{ for all } T \in \mathbb{T}_N;$$

where λ_T is the Hecke-eigenvalues with respect to T. We denote

$$E_{\lambda_T} = \{f \in S_2(N) \mid T(f) = \lambda_T \cdot f\},$$

the λ_T-eigenspace where $T \in \mathbb{T}_N$ is fixed. Now we define the space of old forms of $S_2(N)$ as

$$S_2^{old} = \left\langle g(dz) \mid g(z) \in S_2(M) \text{ with } M|N; M \neq N; d|\frac{N}{M} \right\rangle.$$

Definition 4 *The orthogonal complement of S_2^{old} with respect to the Petersson inner product:*

$$\langle f, g \rangle = \int_{X_0(N)} f(z)\overline{g(z)}dxdy \quad \text{with } f, g \in S_2(N),\ z = x + iy,$$

is denoted by $S_2^{new}(N)$ and is called space of new-forms. a cusp-form f is a new-form if and only if $f(z) = q + \sum_{n\geq 2} a_n q^n$ and f is a Hecke-eigenform.

Theorem 2 ***(Atkin-Lehner (1970))***. *$S_2^{new}(N)$ is stable under all operators T_n, and so $S_2^{new}(N)$ decomposes into a direct sum of orthogonal subspaces X_i,*

$$S_2^{new}(N) = \oplus X_i$$

each of which is a simultaneous eigenspace for all T_n with $\gcd(n, N) = 1$. *The T_p for $p|N$ stabilize each X_i over $\mathbb{C}$. The spaces X_i in the above decomposition all have dimension* 1 *over $\mathbb{C}$.*

It is known that $Hom(S_2(N), \mathbb{C})$ is a free $\mathbb{T}_N \otimes \mathbb{C}$-module of rank one and $\mathbb{T}_N$ is a free $\mathbb{Z}$-module of rank equal to the genus of $X_0(N)$.

Proposition 2 ***(Merel (1994))***. *Let R be a commutative ring and let $\psi \in Hom(\mathbb{T}_N, R)$, then*

$$\sum_{n=1}^{\infty} \psi(T_n) q^n \in S_2(N)(R).$$

We will use this property to compute the Fourier expansion of cusp-forms. Since $\mathbb{T}_N$ is a free $\mathbb{Z}$-module of finite rank acting on $S_2(N)$ we get

Lemma 1 *Let $f = q + \sum_{n=2}^{\infty} a_n q^n \in S_2^{new}(N)$ be a Hecke eigenform and $T \in \mathbb{T}_N$. Then the eigenvalue λ_T is a totally real integral algebraic integer and the field*

$$K_f = \mathbb{Q}(\lambda_T \mid T \in \mathbb{T}_N)$$

is a finite extension of $\mathbb{Q}$.

4 Hecke theory on modular symbols

Let us consider $H_1(X_0(N), \mathbb{Z}) = \mathrm{AB}(\Pi^1(X_0(N), z))$ which is the Abelian group obtained by taking as generators all closed paths on $X_0(N)$, and by factoring out by the relation that two clothed paths are equivalent if one can be continuously deformed into the other. Let $\alpha,\ \beta \in \mathbb{H}^*$ be points equivalent under the action of $\Gamma_0(N)$, so that $\beta = M(\alpha)$ for some $M \in \Gamma_0(N)$, then any smooth path from α to β determines an integral homology class in $H_1(X_0(N), \mathbb{Z})$ which only depends only on α and β ($\mathbb{H}^*$ is simply connected). We denote this homology class by the modular symbol $\{\alpha, \beta\}$. Conversely every integral homology class $\gamma \in H_1(X_0(N), \mathbb{Z})$ can be represented by such a modular symbol $\{\alpha, \beta\}$.

Proposition 3 *Let $\alpha, \beta, \gamma \in \mathbb{H}^*$, and let $M \in \Gamma_0(N)$. Then*

1. $\{\alpha, \alpha\} = 0$;
2. $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\}$;
3. $\{M\alpha, M\beta\} = \{\alpha, \beta\}$;

Corollary 1 *The map $M \mapsto \{\alpha, M\alpha\}$ is a surjective group morphism $\Gamma_0(N) \longrightarrow H_1(X_0(N), \mathbb{Z})$, which is independent of $\alpha \in \mathbb{H}^*$.*

One considers $H_1(X_0(N), cusp, \mathbb{Z})$, the relative homology of $X_0(N)$ with respect to the set of the cusps. In particular we can see that $H_1(X_0(N), \mathbb{Z})$ is a subgroup of $H_1(X_0(N), cusp, \mathbb{Z})$ because we can take as an element of $H_1(X_0(N), \mathbb{Z})$, a linear combination of elements $\{\alpha, M\alpha\}$ with $\alpha \in \mathbb{Q} \cup \{\infty\}$. We denote by $\mathbb{Z}^{\nu_\infty}$ the set of the cusps $\Gamma_0(N)\backslash\mathbb{Q} \cup \{\infty\}$. A modular symbol $\{\alpha, \beta\}$ is an element of $H_1(X_0(N), cusp, \mathbb{Z})$, where $\alpha,\ \beta$ are cusps. For $\alpha \in \mathbb{Q} \cup \{\infty\}$, we denote by $[\alpha]$ its image in $\Gamma_0(N)\backslash\mathbb{Q} \cup \{\infty\}$. Later we will study more precisely the correspondence.

Proposition 4 ***(Eichler and Shimura)*** *One has the exact sequence*

$$\begin{array}{ccccccccc} & & & & & \overset{\delta}{} & & \overset{\theta}{} & \\ 0 \to & H_1(X_0(N), \mathbb{Z}) & \to & H_1(X_0(N), cusp, \mathbb{Z}) & \to & \mathbb{Z}^{\nu_\infty} & \to & \mathbb{Z} \to 0 & \\ & \{\alpha, M\alpha\} & \mapsto & \{\alpha, M\alpha\} & & & & & \\ & & & \{\alpha, \beta\} & \mapsto & [\alpha] - [\beta] & & & \\ & & & & & \lambda[\alpha] & \mapsto \lambda & & \end{array} \tag{1}$$

Now we give some recalls: the projective line over $\mathbb{Z}/N\mathbb{Z}$ is defined by

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \{(c,d) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid \gcd(c,d,N) = 1\}/\sim,$$

where $(c,d) \sim (c',d')$ iff $cd' \equiv c'd \mod N$. We can show that the map

$$\Gamma_0(N)\backslash SL_2(\mathbb{Z}) \longrightarrow \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}),\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto (c:d) \mod N$$

is a bijection between the right coset $\Gamma_0(N)\backslash SL_2(\mathbb{Z})$ and the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. The elements of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ are called Manin-symbols.

Theorem 3 ***(Manin 1972)*** *$H_1(X_0(N), cusp, \mathbb{Z})$ is a free $\mathbb{Z}$-module and it rank is equal to $2g(X_0(N)) + \nu_\infty(N) - 1$. It is generated by the modular symbols*

$$\{\{M(0), M(\infty)\} | M \in \Gamma_0(N)\backslash SL_2(\mathbb{Z})\};$$

and we have the isomorphism

$$\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})]/\langle u + uS, u + uR + uR^2 | u \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\rangle \cong H_1(X_0(N), cusp, \mathbb{Z}).$$

Let i be the following involution which acts on $\mathbb{H}^*$, on the Manin-symbols and the modular symbols by the following relations:

$$i(z) = -\overline{z}, \quad i((c,d)) = (c,d)\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i(\{\alpha,\beta\}) = \{-\alpha,-\beta\}.$$

Restricting (1) to invariant elements under the involution, we get:

$$0 \longrightarrow H_1(X_0(N),\mathbb{Z})_+ \longrightarrow H_1(X_0(N), cusp, \mathbb{Z})_+ \overset{\delta_+}{\longrightarrow} \mathbb{Z}_+^{\nu_\infty}$$

If we want to construct a basis of $H_1(X_0(N),\mathbb{Z})_+$, we have to construct the matrix of δ_+, thus a basis of $H_1(X_0(N), cusp, \mathbb{Z})_+$ and of $\mathbb{Z}_+^{\nu_\infty}$. The construction is similar if we want to construct a basis of $H_1(X_0(N),\mathbb{Z})$, we just have to omit the involution action.

To find a basis of $H_1(X_0(N),\mathbb{Z})_+$, we use the following relations:

1. $(c:d) + (c:d)S = (c:d) + (-d:c) = 0$;
2. $(c:d) + (c:d)R + (c:d)R^2 = (c:d) + (c+d:-c) + (d:-c-d) = 0$;
3. $(c:d) - i((c:d)) = (c:d) - (-c:d) = 0$.

These formulas give us the relations between the elements of the representative system of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, then we just have to index-link the elements of this representative system in a canonic basis, then we can construct our $\mathbb{Z}$-module quotient. It is similarly to obtain a $\mathbb{Z}$-module basis of $\mathbb{Z}_+^{\nu_\infty}$. We have the following equivalence:

1. $i([\alpha]) = [\alpha]$ et $[\alpha] \equiv [\beta] \Longleftrightarrow \alpha = \pm\beta \mod \Gamma_0(N)$;
2. For $j = 1, 2$, let $\alpha_j = p_j/q_j$, be equivalent cusps written in lowest terms. Then $s_1 q_2 \equiv \pm s_2 q_1 \ mod\ gcd(q_1 q_2, N)$ where s_j satisfies $p_j s_j \equiv 1 \mod q_j$.

Now we present some results about the correspondence between homology and cusp-forms.

Proposition 5 ***(Merel 1994)*** *We have isomorphisms*

1. $H_1(X_0(N), cusp, \mathbb{Z}) \cong \varepsilon is(\Gamma_0(N)) \oplus S_2(N) \oplus \overline{S_2(N)}$;
2. $H_1(X_0(N), \mathbb{Z}) \cong S_2(N) \oplus \overline{S_2(N)}$ *and* $H_1(X_0(N), \mathbb{Z})_+ \cong S_2(N)$;
3. $\dim H_1(X_0(N), \mathbb{Z})_+ = \dim H_1(X_0(N), \mathbb{Z})_- = g(X_0(N))$;

where $\overline{S_2(N)}$ *is the anti-holomorphic space of cusp-forms,* $\varepsilon is(\Gamma_0(N))$ *is a space of modular forms which is called space of Eisenstein series, and we noted* $g(X_0(N))$ *as the genus of* $X_0(N)$.

We are going to describe the action of Hecke algebra on Manin-symbols and modular symbols:

Proposition 6 *For* p *prime and* $p \not| N$, *if* $\alpha,\ \beta$ *are cusps, we have:*

$$T_p(\{\alpha, \beta\}) = \{p\alpha, p\beta\} + \sum_{k=0}^{p-1} \left\{ \frac{\alpha + k}{p}, \frac{\beta + k}{p} \right\}.$$

If $p^a || N$, *then let* $W_p = \begin{pmatrix} p^a x & y \\ Nz & p^a t \end{pmatrix}$, *with* $x,\ y,\ z,\ t \in \mathbb{Z}$, $\det(W_p) = p^a$. *Then*

$$T_{p^a}(\{\alpha, \beta\}) = \left\{ \frac{p^a x\alpha + y}{Nz\alpha + p^a t}, \frac{p^a x\beta + y}{Nz\beta + p^a t} \right\}.$$

To compute the matrix of Hecke operators acting on cusp-forms we need to be able to convert the modular symbols into Manin symbols [1].

If $(c : d) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, with the Bezout lemma we can find $a, b \in \mathbb{Z}$ such that $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = 1$, so we are be able to convert a Manin symbol into modular symbol:

$$(c : d) \longrightarrow M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \{M(0), M(\infty)\} = \left\{ \frac{a}{c}, \frac{b}{d} \right\}.$$

If we give us a modular symbol $\left\{\frac{a}{c}, \frac{b}{d}\right\}$, we have the following algorithm:

$$\left\{ \frac{a}{c}, \frac{b}{d} \right\} = \left\{ \frac{a}{c}, 0 \right\} + \left\{ 0, \frac{b}{d} \right\} \text{ and we note } \left\{ 0, \frac{b}{d} \right\} = \{0, t\}$$

Let $[a_1, \ldots, a_n]$ be the simple continued fraction expansion of t, i.e.

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}$$

If we note $C_k = [a_1, \ldots, a_k]$ then the numerator p_k and the denominator q_k of C_k satisfy the equations (For $i = 3, 4, \ldots, k$)

$$p_i = a_i p_{i-1} + p_{i-2},\ p_{-1} = 0,\ p_0 = 1,\ p_1 = a_1,\ p_2 = a_1 a_2 + 1,$$
$$q_i = a_i q_{i-1} + q_{i-2},\ q_{-1} = 1,\ q_0 = 0,\ q_1 = 1,\ \ q_2 = a_2.$$

where $t = \frac{p_n}{q_n}$ and we know that $p_i q_{i-1} - p_{i-1} q_i = (-1)^i$, where $i \geq 0$. So we obtain that

$$\{0, t\} = \sum_{i=0}^{i=n} \{M_i(0), M_i(\infty)\} \text{ with } M_i = \begin{pmatrix} (-1)^{i-1} p_i & p_{i-1} \\ (-1)^{i-1} q_i & q_{i-1} \end{pmatrix}.$$

We present another method: the Hecke algebra can act directly on Manin symbols, in such manner continued fractions are not needed.

Definition 5 *Let* $M_n = \{v \in M^{2\times 2}(\mathbb{Z}) \mid \det(v) = n\}$ *and*

$$(c:d)M = \begin{cases} 0 & \text{if } (c:d)M \notin \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \\ (c:d)M & \text{if } (c:d)M \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}). \end{cases}$$

For any integer $n \in \mathbb{Z}$ *we will say that the element* $\Theta_n = \sum_{M \in M_n} u_M M \in \mathbb{Z}[M_n]$ *satisfies the condition* C_n *if*

$$\sum_{M \in M_n} u_M (M(\infty) - M(0)) = (\infty) - (0).$$

Theorem 4 ***(Merel 1994)*** *If* Θ_n *satisfies the condition* C_n *then we have the following formula for the action of Hecke and Atkin-Lehner operators on Manin symbols:*

$$T_n((c:d)) = \sum_{M \in M_n} u_M (c:d)M \text{ for } \gcd(n, N) = 1,$$

$$W_n((c:d)) = \sum_{M \in M_n,\ (c:d)M \equiv (0,0) \mod n} u_M \epsilon_n(gM) \text{ for } n|N,$$

where $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *and* $\epsilon_n(gM)$ *is the unique element of* $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ *congruent to* $(1,0)gM \mod n$ *and to* $(0,1)gM \equiv (c:d)M \mod N/n$.

Theorem 5 ***(Merel 1994)*** *The element*

$$\sum_{a>b\geq 0,\ d>c\geq 0,\ ad-bc=n} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}[M_n] \tag{2}$$

satisfies the condition C_n.

Now we give a very useful result which gives us an algorithm to restrict to new-forms which are in correspondence with elliptic curves and hyperelliptic curves of genus two.

Theorem 6 ***(Merel 1994)*** *Let $x \in \mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})]$ and $\Theta = \sum_{M \in M_1} u_M M$ which satisfies the condition C_1 and let*

$$\epsilon_1 : S_2(N) \longrightarrow S_2(N/n), \quad \epsilon_1(x) = \sum u_M x M \tag{3}$$

for n dividing N and where the sum is restricted to the matrices M such that $xM \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Then x belongs to $S_2^{new}(N)$ if and only if x and $W_N(x)$ belong to the kernel of ϵ_1 for all divisors n of N.

Using (2), (3), it is easy to see that the sum Θ is restricted to the matrix identity. With these results we now are able to construct a basis of new-forms which are in correspondence with Abelian varieties of genus one or two. We are going to see this correspondence in the following section.

5 New-forms and Abelian varieties

Theorem 7 *Let $f = q + \sum_{n=2}^{\infty} a_n q^n$ be a Hecke eigenform and let $K_f = \mathbb{Q}(a_n \mid n \in \mathbb{N})$ be the field generated by the Fourier coefficients of f. Then there exists an Abelian sub-variety A_f of $J_0(N)$ and an isomorphism θ from K_f to $End(J_0(N)) \otimes \mathbb{Q}$ with the properties:*

1. $\dim(A_f) = [K_f : \mathbb{Q}] = d$;
2. *If* $\gcd(n, N) = 1$, *then $\theta(a_n)$ coincides with the restriction of T_n to A_f;*
3. *The conductor $N(A_f)$ is equal to N^d, where* $d = \dim(A_f)$.

Moreover the pair (A_f, θ) is unique and A_f is a simple Abelian variety defined over $\mathbb{Q}$.

5.1 L-series and applications

Case of elliptic curves Recall that for an elliptic curves E over $\mathbb{Q}$, we define

$$L(E, s) = \prod_{p \ good} \frac{1}{1 - a_p p^{-s} + p^{1-s}} \cdot \prod_{p \ bad} \frac{1}{1 - a_p p^{-s}} = \sum a_n n^{-s}$$

where

$$a_p = \begin{cases} p + 1 - N_p & \text{if } p \text{ good;} \\ 1 & \text{if } p \text{ split nodal;} \\ -1 & \text{if } p \text{ nonsplit nodal;} \\ 0 & \text{if } p \text{ cuspidal.} \end{cases} \qquad \text{and } N_p = \#E(\mathbb{F}_p).$$

Recall that to a new-form f we can associate a Dirichlet series which admits an Euler product [7]

$$L(f,s) = \prod_{\gcd(p,N)=1} \frac{1}{1 - a_p p^{-s} + p^{1-s}} \cdot \prod_{p|N} \frac{1}{1 - a_p p^{-s}} = \sum a_n n^{-s}$$

Theorem 8 ***(Eichler-Shimura)*** *Let $f = q + \sum_{n=2}^{\infty} a_n q^n$ a new-form with $a_n \in \mathbb{Z}$ for all $n \geq 0$. Then there exists an elliptic curve E_f of conductor N such that $L(f,s) = L(E,s)$.*

In fact we know now that all elliptic curves are modular, that is to say that all elliptic curves of conductor N are simple factors of the Jacobian $J_0(N)$.

Case of Abelian variety of genus 2 Let $f = q + \sum_{n=2}^{\infty} a_n q^n$ be a Hecke eigenform, with $K_f(a_n \mid n \in \mathbb{Z})$ being a quadratic extension of $\mathbb{Q}$. Let $I_f = \{Id, \sigma\}$ be the set of distinct embedding of K_f into $\mathbb{C}$, then we define the L-series of f in p by

$$L_p(f,s) = \begin{cases} 1 - a_p s + p s^2 & \text{if } p \text{ doesn't divide } N, \\ 1 - a_p s & \text{if } p \text{ divide } N. \end{cases}$$

Theorem 9 *Let $L_p(A_f, s)$ be the L-series of A_f in p. Then, for a p prime not dividing N, we have the following properties:*

1. $L_p(A_f, s) = \prod_{\sigma \in I_f} L_p(f^\sigma, s)$;
2. $L_p(A_f, 1) = \#(A_f \otimes \mathbb{F}_p)$.

In particular we have the following formula

$$L_p(A_f, 1) = (1 + p + a_p)(1 + p + \sigma(a_p)) = \chi_p^f(p+1),$$

where χ_p^f is the minimal polynomial of T_p acting on f.

Remark 1 *The same properties hold if $K_f(a_n \mid n \in \mathbb{Z})$ is an extension of $\mathbb{Q}$ of greater degree but we are just interested by elliptic curves and hyperelliptic curves of genus 2.*

6 Steps to compute the cardinality over $\mathbb{F}_p$

We are going to summarize by the following points how to compute the cardinality of elliptic curves or Abelian variety over $\mathbb{F}_p$:

- First we construct a representative system of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, one can take all elements (d,i) with d dividing N and $\gcd(d,i) = 1$, then we have to choose a representant in the coset (d,i) where d is fixed because two elements (d,i) and (d,j) are equivalent if and only if $i - j \equiv 0 \mod N/d$;

- Secondly we find a Manin-symbol basis of $H_1(X_0(N), cusp, \mathbb{Z})_+$, for this, the relations that we have seen before are essential:
  1. $(c:d) + (-d:c) = 0$;
  2. $(c:d) + (c+d:-c) + (d:-c-d) = 0$;
  3. $(c:d) - (-c:d) = 0$.

  We just index-link the representative system of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ by the elements of a canonical basis, then we just recognize the relations seen above in this canonical basis. After we quotient a free $\mathbb{Z}$-module of rank $\#(\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}))$ index-linked by the canonical basis by the relation seen above. We obtain in fact a morphism $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to H_1(X_0(N), cusp, \mathbb{Z})_+$
- Similarly, we construct a $\mathbb{Z}$-module basis of $\mathbb{Z}_+^{\nu_\infty}$. To do this:
  1. First we extract a representative system of cusps which come from $H_1(X_0(N), cusp, \mathbb{Z})_+$, we saw that it is possible because we can convert a Manin-symbol into modular symbol. So we will obtain two cusps for each modular symbol.
  2. Then we use the equivalent properties of cusps: [1]
     (a) $i([\alpha]) = [\alpha]$ et $[\alpha] \equiv [\beta] \iff \alpha = \pm\beta \bmod \Gamma_0(N)$;
     (b) For $j = 1, 2$, let $\alpha_j = p_j/q_j$, be equivalent cusps written in lowest terms. Then $s_1 q_2 \equiv \pm s_2 q_1 \bmod gcd(q_1 q_2, N)$ where s_j satisfies $p_j s_j \equiv 1 \bmod q_j$.

  We also obtain a morphism cusps $\longrightarrow \mathbb{Z}_+^{\nu_\infty}$
- Now we are able to construct the matrix of δ_+ because we have a basis of $\mathbb{Z}_+^{\nu_\infty}$ and $H_1(X_0(N), cusp, \mathbb{Z})_+$, with the extended Euclidean algorithm we just convert some Manin-symbols into modular symbols and extract the two cusps of each modular symbol.
- To obtain a Manin-symbol basis of $S_2(N)$, we just compute the kernel of δ_+. Thus we obtain the vector basis. We get the Manin-symbol basis in looking the index-linking that we choose for the representative system of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.
- Our goal now is to restrict to basis of new-forms which are in correspondence with Abelian varieties of genus one or two. Thus we choose the smaller prime p not dividing N, and we compute the matrix of the p-th Hecke operator T_p acting on $S_2(N)$. Then we compute the characteristic polynomial of T_p and we extract a basis of eigenvectors which corresponds to irreducible factors of degree one or two of the characteristic polynomial of T_p.
- For each eigenvector we verify if it is an element of $S_2^{new}(N)$ with the map (3) $\epsilon_1 : S_2(N) \longrightarrow S_2(N/n)$ with $n \mid N$. We keep only the elements which belong to $S_2^{new}(N)$. So we get a Manin-symbol basis of $S_2^{new}(N)$ which are in correspondence with these Abelian varieties of genus one or two. Of course sometimes there doesn't exist modular Abelian varieties with level N given. We are just interested by the best cases, where there is at least an Abelian variety of genus one or two.
- Now we would like compute the Fourier coefficients of these new-forms in order to get the cardinality of these varieties over $\mathbb{F}_p$. In fact the

eigenvalues of the p-th Hecke operator acting on a element of the basis of $S_2^{new}(N)$ is equal to the p-th coefficient of the new-form which is in bijection with this element. So to compute the series of a new-form we just compute the eigenvalues of the Hecke algebra acting on the element of the basis of $S_2^{new}(N)$.

In this example we programmed this algorithm with Magma:

Here is a representative system of $\mathbb{P}^1(\mathbb{Z}/33\mathbb{Z})$. We choose this natural order given by magma as index-linking for the canonic basis:

```
>RepresSyst(33);

[
    [ 1, 0 ],[ 1, 1 ],[ 1, 2 ],[ 1, 3 ],[ 1, 4 ],[ 1, 5 ],..
    ,[ 1, 32 ],[ 3, 14 ],[ 3, 11 ],[ 3, 20 ],..,[ 3, 1 ],
    [ 11, 3 ],[ 11, 2 ],[ 11, 1 ],[ 0, 1 ]
]
```

Now here is a Manin-symbol basis of $S_2(33)$. We know that the genus of $X_0(N)$ is equal to 3, thus we get 3 vectors. We also take this natural order to index-link the basis of $S_2(33)$.

```
>S2base(33);

  [              [               [
    -[ 3, 5 ]        [ 3, 5 ]      -[ 3, 4 ]
    -[ 11, 3 ]     +[ 3, 4 ]       -[ 11, 3 ]
    +[ 11, 1 ]     -[ 3, 1 ]       +[ 11, 1 ]
  ],               +[ 11, 3 ]    ]
                   -[ 11, 1 ]
                 ],
```

The smaller prime p not dividing N is 2. Thus we compute the action of the 2-th Hecke operator on $S_2(33)$, because we want to extract the new-forms which interest us.

```
> HeckeAction(2,33);

      [ 0  2  1]
A := [ 0 -2  0]
      [ 2  2 -1]
```

```
> CharcPolyHecke(2,33);

[
  <x - 1, 1>,
  <x + 2, 2>
]
```

We see that there are two eigenspaces, one is associated to the eigenvalue 1 and the other is associated to the eigenvalue -2. We need the eigenvectors of this eigenspaces:

```
> Eigenspace(A,-2);          > Eigenspace(A,1);
Echelonized basis:           Echelonized basis:
( 1  0 -1)                   (2 2 1)
( 0  1  0)
```

We search now the elements of $S_2^{new}(N)$. The degree of the irreducible factors of the characteristic polynomial of T_2 is one. Thus if $S_2^{new}(N) \neq 0$, the new-forms are in correspondence with elliptic curves (up to isogeny) of conductor equal to 33. We verify that the 1-eigenvector satisfies the condition of the theorem 6 (3), that is to say that Eigenspace(A,1) has to belong to the kernel of the map ϵ_1 for the divisors 3 and 11 of 33.

```
> Epsilon1(A,1,3);           > Epsilon1(A,1,11);
(0)                          (0)

> Epsilon1(W33(A,1),3);      > Epsilon1(W33(A,1),11);
(0)                          (0)
```

Epsilon1(A,i,3), for $i = 1, -2$ is always equal to 0 because $\dim(S_2(3)) = 0$ whereas $\dim(S_2(11)) = 1$. We verify that the other eigenvectors which are associated to the eigenvalue -2 do not belong to $S_2^{new}(N)$:

```
> Epsilon1(A,-2,3);          > Epsilon1(A,-2,11);
(0)                           (-4)
(0)                           (1)
```

Therefore, the eigenvector which is associated to the eigenvalue 1 of the Hecke operator T_2 belongs to $S_2^{new}(N)$. So the 1-eigenspace is in fact a new-form for which we can compute its Fourier coefficients. We see that the elements which is in correspondence with the eigenvalues -2 belong to because $\dim(E_{-2}) = 2$.

We have two ways to compute the Fourier coefficients, we can apply the p-th Hecke operator directly on the 1-eigenvector of Manin-symbols, using the Manin and Merel results, or we can transform these Manin-symbols into modular symbols and then we use the continued fraction method. In practice the continued fraction method is more easier to implement.

$N = 33$: genus$(X_0(33)) = 3$, we can get a new-form associated to a elliptic curve:[9]

$$f(z) = q + q^2 - q^3 - q^4 - 2q^5 - q^6 + 4q^7 - 3q^8 + q^9 - 2q^{10} + q^{11} + q^{12} - 2q^{13} \ldots$$

This elliptic curve admits for minimal model $E : y^2 + xy = x^3 + x^2 - 11x$ [1].

7 Construction of modular curves from new-forms

First we summarize the results of Shimura [4]. Let $f(z)$ a new-form of weight two and $\omega(f) = 2\pi i f(z)dz$ be the associated differential.

Let $I_f = \{\sigma_1, \dots, \sigma_d\}$ be all the distinct embeddings of $K_f = \mathbb{Q}(a_1, \dots)$ into $\mathbb{C}$ which is the field generated by the coefficients of f. Let $\{f^{\sigma_1}, \dots f^{\sigma_d}\}$ be the complete set of new-forms conjugate to f over $\mathbb{Q}$. There exists an Abelian variety A_f rational over $\mathbb{Q}$ (see section 4 theorem 7) such that the space of differential 1-forms $\Omega^1(A_f)$ is isomorphic to $\sum_{\sigma \in I_f} \mathbb{C}\omega(f^\sigma)$. Let $\mathbf{f} = (f^{\sigma_1}, \dots, f^{\sigma_d})^t$ and $\omega(\mathbf{f}) = (\omega(f^{\sigma_1}), \dots, \omega(f^{\sigma_d}))^t$. Then the image of $H_1(X_0(N), \mathbb{Z})$ by the map

$$H_1(X_0(N), \mathbb{Z}) \longrightarrow \mathbb{C}^d;\ \gamma \longmapsto \int_\gamma \omega(\mathbf{f}) = \left(\int_\gamma \omega(f^{\sigma_1}), \dots, \int_\gamma \omega(f^{\sigma_d}) \right)^t$$

q is a free $\mathbb{Z}$-module of rank $2d$. It is a lattice Λ_f in $\mathbb{C}^d$ and we get

$$A_f \cong \mathbb{C}^d / \Lambda_f.$$

When $d = 1$ we have an elliptic curve and in this case it is possible to get a minimal model of elliptic curve C such that $C \cong A_f$. See [1].

When $d = 2$, sometimes we can get a model of hyperelliptic curve of genus two C such that $Jac(C) \cong A_f$. This model can be obtained if the period matrix of A_f satisfies certain conditions. See [10].

8 Conclusion

With this method it is possible to construct a general family of elliptic curves because we know that all elliptic curves are modular. In fact for a level N given we are able to construct up to isogeny all the elliptic curves and in fact, without constructing these elliptic curves, we can give the number of elliptic curves over $\mathbb{Q}$ (up to isogeny) with given conductor N. The complexity of this algorithm is polynomial in N, so if the level N is not too large we can get a great number of Abelian varieties. We have the Shimura-Taniyama conjecture which asserts that any Abelian variety A with real multiplication, both defined over $\mathbb{Q}$, is isogenous to a factor of $J_0(N)$ for a suitable N. So we just can say that with this algorithm we can compute the number of modular Abelian varieties of genus two and conductor N^2 with level N given. We just interested by Abelian varieties of genus one or two because the hyperelliptic curves of genus two and elliptic curves may give good cryptosystems. An important problem in cryptography is to compute of the cardinality of the Jacobian of these curves over $\mathbb{F}_p$.

Computing the cardinality over $\mathbb{F}_p$ with this algorithm is not possible if p is too large: we see that if we choose the method using continued fraction we need to compute p continued fractions on fractions of number very closed to p. This computing need about $\mathcal{O}(p \log(p))$ arithmetic operations. The method which uses the matrices sum acting on the Manin-symbols is not better because we know (see [5], [3]) that these families have a cardinal very closed to

$p \log(p)$ and it is not easy in practice to construct this sum. So we can't use these methods in cryptography.

A possible improvement would be to find the matrix of the p-th Hecke operator with p large. It would be interesting if we find for example a method to compute the p-th Hecke operator action modulo some small prime numbers l_i with a polynomial complexity who depends of l_i. (CRT)

References

1. John Cremona. *Arithmetic of modular elliptique curves*. Cambridge University Press, 1992.
2. Bas Edixhoven. The modular curves $X_0(N)$. In *Trieste, ICTP, Summer school on elliptic curves*, 1997.
3. Gerhard Frey and Michael Müller. Arithmetic of modular curves and application. In G.-M.; Hiss G. Matzat, B.H.; Greuel, editor, *Algorithmic Algebra and Number Theory, Springer-Verlag*, 1999.
4. G.Shimura. *Introduction to the arithmetic theory of automorphic Functions*. Princeton university press, 1971.
5. Loïc Merel. Universal fourier expansions of modular forms. *Lecture Notes in Mathematics*, 1994.
6. Jean-Francois Mestre. Construction de courbes de genre 2 à partir de leur modules. *Effective Methods in Algebraic Geometry*, 1991.
7. Joseph Milne. Elliptic curves. Available on `http://www.jmilne.org/math/CourseNotes/math679.html`, 1996.
8. Jean-Pierre Serre. *Cours d'arithmétique*. Presses Univ. France, 1970.
9. William A. Stein. The modular forms database. Available on `http://modular.fas.harvard.edu/Tables/index.html`, 1999.
10. Xiangdong Wang. 2-dimensional simple factors of $J_0(N)$. *Manuscripta Mathematica*, 1995.
11. Xiangdong Wang. The Hecke operators on the cusp-forms of $\Gamma_0(N)$. In G. Frey, editor, *On Artin's Conjecture for Odd 2-dimensional Representations*, number 1585 in Lecture notes in Mathematics, pages 59–94. Spriger-Verlag, 1995.