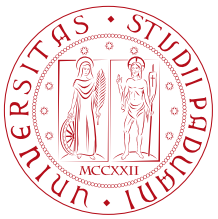
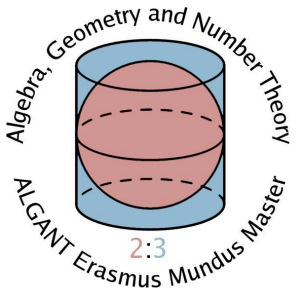




ERASMUS MUNDUS MASTER ALGANT

UNIVERSITÀ DEGLI STUDI DI PADOVA

UNIVERSITÉ BORDEAUX 1 SCIENCES ET TECHNOLOGIES

MASTER THESIS

COMPUTING MODULAR POLYNOMIALS WITH THETA FUNCTIONS

ILARIA LOVATO

ADVISOR: PROF. ANDREAS ENGE
CO-ADVISOR: DAMIEN ROBERT

ACADEMIC YEAR 2011/2012

Contents

Introduction

The purpose of this work is to understand how to use ϑ functions to build modular polynomials.

Both of these topics have been intensively studied; in particular, we date back to Gauss the first studies about ϑ functions, and to the 19th century the first studies about modularity.

Modular polynomials, in particular, have been studied from last century on with an eye on their possible exploitation in the cryptographic field. As we will see, these are polynomials in two variables which have important applications when studying elliptic curves: if we evaluate one variable in an invariant which characterises a given elliptic curve, the zeros in the other variable are invariants of curves linked to our original one by means of isogenies. We will prove this theorem over $\mathbb{C}$, but it remains true also when considering the reduction of curves and polynomials over a finite field.

There is a whole family of cryptographic systems based on elliptic curves defined over finite fields; their strength relies on the difficulties of solving the discrete logarithm problem. If we know isogenies linking a given curve to others, we can make our problem shift from one curve to another, and this may possibly reduce difficulties, as S. Galbraith explains in [Gal99]. So, computing isogenous curves is a nowadays well-studied topic.

Our interest, however, will not be in computing isogenies. Classical modular polynomials, that are modular polynomials built by means of the classical j invariant defined over elliptic curves, are easy to define but not always comfortable to use. As a matter of fact, they turn out to have coefficients that dramatically increase even when considering relatively low isogeny levels; we suggest the reader to have a look at pages 32-33 to have an idea about that. So our aim here is to define and compute modular polynomials by means of the so-called ϑ functions, which could be in some sense considered as a particular kind of invariants over elliptic curves, and whose values allow in any case to retrieve the value of the classical j invariant.

We have done this by performing all the computations with PARI/GP version 2.5.1; we display all the codes we wrote and the results we finally ob-

tained.
The main advantage of ϑ functions is that they could be defined without any regard to the dimension of the space we are working in; so, this point of view could be generalised to look for modular polynomials linking invariants for higher genus objects. We will try to explain how to develop this kind of considerations with respect to genus 2 objects.
This is the detailed plan of the work.

Chapter 1. To justify the computations and the considerations of the following chapters, we will give basic definitions about elliptic curves and we will prove the isomorphism between an elliptic curve and a quotient of the form $\frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}}$, with $\tau \in \mathbb{C}$; we will give an operative definition of isogeny, so to have all the tools for doing computations in the following chapters.

Chapter 2. We will introduce classical modular polynomials, and prove some properties about them; we will see their shape for low levels, and we will try to understand how to build modular polynomials different from the classical ones.

Chapter 3. We will study ϑ functions in dimension 1; we will introduce the definitions and various properties connected to ϑ constants, and we will see how to build a modular polynomial by means of them.

Chapter 4. Here we explain how we performed the computations: we analyse our way of proceeding and we display all the codes we used and the results we got for low degrees.

Chapter 5. Once we set up the situation for elliptic curves, we ask ourselves if it would be possible to extend this analysis to higher genus objects. We try to give a sketch about the situation in genus 2, giving basic definitions in order to try to adapt our code to this environment.

All along this work, we choose to adopt an explicit computational point of view. We started by performing computations, and as we proceeded with them we developed and study the theory we needed to fully understand what was going on.
This reflects immediately in the structure of this work; the aim of the first three chapters is to explain and understand the results we display at Chapter 4. The contents of Chapter 5 are meant to be a sort of introduction to what can be done by adapting to genus 2 what we did in genus 1.
The results we display at Chapter 4 are original; we explain in that chapter how we obtained them and we present as well all the preliminary work we did before computing them. Their interest lies, as we said, in the possibility to

adapt the same kind of computations to higher genus; we tried in Chapter 5 to proceed in this direction, but due to a lack of time and of powerful computer we got no significant results.
However, the nice shape of the polynomials we computed for genus 1 is an encouragement to proceed in this direction.

Chapter 1

Basic facts about elliptic curves

We start our work by recalling the notions we will need about elliptic curves; mainly, we will sketch how to prove the isomorphism between an elliptic curve and a torus and give some basic notions about isogenies. The purpose of this chapter is utilitarian: we simply want to define tools and correspondences we will massively use in the rest of the work, without any pretence about doing a complete discussion on the topic, which is in fact an immense and really intriguing one.

1.1 From tori to elliptic curves

Definition 1.1.1. *An **elliptic curve** over a field k can be defined as a nonsingular projective plane curve of the form*

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

From now on, we will set $k = \mathbb{C}$. This assumption allows us to write elliptic curves in a simpler form, as a simple change of variables gives us an equation which is the more familiar one:

Definition 1.1.2. *If char(k) is different from 2 or 3 an elliptic curve is isomorphic to a curve of equation*

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

*This equation is commonly known as **short Weierstrass equation**.*

These kind of curves have a lot of very interesting properties; the most important of them is perhaps the possibility to define a group law over it. For more informations about this construction, we address the reader to [Sil09, Chapter 3.2].

As we are going to consider only curves over the complex numbers, the thing which is more interesting for us is to see the curve as a torus, so that to have a uniquely defined elliptic curve it would be enough to specify the generators of the lattice defining the torus. In our computations, we will denote a curve simply by a complex quantity which will allow us to retrieve the lattice.
We are going now to justify briefly why we can proceed this way; we recall some very basic definitions, just to fix notations:

Definition 1.1.3. *Let $\omega_1, \omega_2 \in \mathbb{C}$ be complex numbers which are linearly independent over $\mathbb{R}$. They define the* ***lattice***

$$L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}.$$

The set

$$F = \{a_1\omega_1 + a_2\omega_2 : 0 \leq a_1, a_2 < 1\}$$

is called a ***fundamental parallelogram*** *for L.*

We can define the torus $\frac{\mathbb{C}}{L}$, and we would like to define functions on it; a function on $\frac{\mathbb{C}}{L}$ can be seen as a function f on $\mathbb{C}$ such that $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in L$. We are only interested in meromorphic functions, so we define a **doubly periodic function** to be a meromorphic function $f : \mathbb{C} \to \mathbb{C} \cup \infty$ such that $f(z + \omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in L$, that means $f(\omega_i + z) = f(z)$ for $i = 1, 2$. The values ω_i are the **periods** for the function f.
Actually, we have a well known characterisation for those functions:

Theorem 1.1.4. *Given a lattice L, we define the* ***Weierstrass $\wp$-function*** *by*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Then:

1. *The sum defining $\wp(z)$ converges absolutely and uniformly on compact sets not containing elements of L;*
2. *$\wp$ is meromorphic in $\mathbb{C}$ and has a double pole at each $\omega \in L$;*
3. *$\wp(z) = \wp(-z)$ for all $z \in \mathbb{C}$;*
4. *$\wp(z + \omega) = \wp(z)$ for all $\omega \in L$;*
5. *The set of doubly periodic functions for L is $\mathbb{C}(\wp, \wp')$. This means that every doubly periodic function is a rational function of $\wp$ and its derivative $\wp'$.*

Proof. See for example [Was08, Theorem 9.3]. □

We introduce now the so-called Eisenstein series:

Definition 1.1.5. *For any integer $k \geq 3$, the corresponding **Eisenstein series** is*

$$G_k = G_k(L) = \sum_{\omega \in L, \omega \neq 0} \omega^{-k}$$

A straightforward calculation (done explicitly for example in [Was08, page 262]) shows that the series converges. When k is odd, the terms for ω and $-\omega$ cancel, so $G_k = 0$.

Lemma 1.1.6. *For $0 < |z| < \min_{\omega \in L, \omega \neq 0}(|\omega|)$,*

$$\wp(z) = \frac{1}{z^2} + \sum_{j=1}^{\infty} (2j+1) G_{2j+2} z^{2j}.$$

Proof. When $|z| < |\omega|$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2} \left(\frac{1}{(1-(z/\omega))^2} - 1 \right) = \omega^{-2} \left(\sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^n} \right).$$

Therefore

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\omega^{n+2}}$$

Thanks to absolute and locally uniform convergence, we can exchange the summations, as [Was08, page 268] says; this yields the desired result. □

Theorem 1.1.7. *Let $\wp(z)$ be the Weierstrass $\wp$-function for a lattice L. Then*

$$\wp'(z)^2 = 4\wp(z)^3 - 60 G_4 \wp(z) - 140 G_6.$$

Proof. From Lemma 1.1.6,

$$\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \dots$$

$$\wp'(z) = -2z^{-3} + 6G_4 z + 20 G_6 z^3 + \dots$$

Cubing and squaring these relations we get

$$\wp(z)^3 = z^{-6} + 9G_4 z^{-2} + 15 G_6 + \dots$$

$$\wp'(z)^2 = 4z^{-6} - 24 G_4 z^{-2} - 80 G_6 + \dots$$

Therefore,

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$$

is a power series with no constant term and without negative powers of z. The only possible poles of $f(z)$ are at the poles of $\wp(z)$ and $\wp'(z)$, so at the elements of L. Since $f(z)$ is doubly periodic and, having no negative powers of z in its expansion, has no pole at 0, $f(z)$ has no poles. We know that doubly periodic functions without poles should be constant; and from the fact we have no constant term, we have $f(0) = 0$. Therefore, $f(z)$ is identically 0. □

To simplify the above expression, it is customary to set

$$g_2 = 60G_4,\ g_3 = 140G_6.$$

The theorem then says that $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$. If we consider the affine space $[x : y : 1]$, we see that this in an equation on the same shape as those of Definition 1.1.1. We can say that the points $(\wp(z), \wp'(z))$ lie on the curve $y^2 = 4x^3 - g_2x - g_3$.
This equation defines a non-degenerate elliptic curve; we can see it by computing the discriminant of the cubic polynomial defining the equation, namely:

Lemma 1.1.8. $\Delta = g_2^3 - 27g_3^2 \neq 0$.

Proof. See [Was08, page 269]. □

So we have that $E : y^2 = 4x^3 - g_2x - g_3$ is an elliptic curve, and we have a map from $z \in \mathbb{C}$ to the point with complex coordinates $(\wp(z), \wp'(z))$ on E. Since $\wp(z)$ and $\wp'(z)$ depend only on $z (\text{mod } L)$, we have a map $\frac{\mathbb{C}}{L} \to E(\mathbb{C})$. In fact, we have more:

Theorem 1.1.9. *Let L be a lattice and E be the elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$. The map*

$$\begin{array}{rccc} \Phi : & \frac{\mathbb{C}}{L} & \to & E(\mathbb{C}) \\ & z & \mapsto & (\wp(z), \wp'(z)) \\ & 0 & \mapsto & \infty \end{array}$$

is an isomorphism of groups.

Proof. For a proof of it, see for example [Sil09, Proposition 3.6]. □

What we state here says that the natural group law defined by the addition on the torus $\frac{\mathbb{C}}{L}$ matches the well-known group law (again, see [Sil09, Chapter 3.2]) defined on the elliptic curve.

1.2 From elliptic curves to tori

In the previous section, we showed that a torus gives an elliptic curve; we have now to show the converse, namely that every elliptic curve over $\mathbb{C}$ comes from a torus. Before doing it, in the following section we introduce some notions about the modular group, a topic which will be extensively developed in the next chapter.

1.2.1 The modular group

Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice and let $\tau = \frac{\omega_1}{\omega_2}$. Since ω_1 and ω_2 are independent over $\mathbb{R}$, τ cannot be real. By switching ω_1 and ω_2 if necessary, we may assume that the imaginary part of τ is positive, in other words that τ lies in the upper half plane

$$\mathcal{H} = \{x + \imath y \in \mathbb{C} : y > 0\},$$

which is called **Poincaré half-plane**. The lattice $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$ is said to be **homothetic** to L, as there exist a nonzero complex number λ such that $L = \lambda L_\tau$ (in this case, $\lambda = \omega_2$).
We set[1] $q = e^{2\pi\imath\tau}$; note that, if $\tau = x + \imath y \in \mathcal{H}$, then $|q| = e^{-2\pi y} < 1$. We define $g_2(\tau) = g_2(L_\tau)$, $g_3(\tau) = g_3(L_\tau)$. If we express these quantities in terms of q, we obtain

$$g_2(\tau) = \frac{4\pi^4}{3}(1 + 240q + \dots) = \frac{4\pi^4}{3}\left(1 + 240\sum_{t=1}^{\infty}\frac{t^3q^t}{1-q^t}\right)$$

$$g_3(\tau) = \frac{8\pi^6}{27}(1 - 504q + \dots) = \frac{8\pi^6}{27}\left(1 - 504\sum_{t=1}^{\infty}\frac{t^5q^t}{1-q^t}\right).$$

A straightforward calculation shows that

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2 = (2\pi)^{12}(q + \dots).$$

Define

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta}$$

Then

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \dots = \tag{1.1}$$

[1] This definition is not the unique one which is used; we can also find $q = e^{\pi\imath\tau}$.

$$= 1728\frac{(1+240\sum_{t=1}^{\infty}\frac{t^3q^t}{1-q^t})^3}{(1+240\sum_{t=1}^{\infty}\frac{t^3q^t}{1-q^t})^3-(1-504\sum_{t=1}^{\infty}\frac{t^5q^t}{1-q^t})^2}.$$

It can be shown (see [Lan87, page 249]) that $\Delta = (2\pi)^{12}q^2\prod_{k=1}^{\infty}(1-q^k)^{24}$, and this gives the expression

$$j = \frac{(1+240\sum_{t=1}^{\infty}\frac{t^3q^t}{1-q^t})^3}{q\prod_{k=1}^{\infty}(1-q^k)^{24}}.$$

More generally (and more traditionally), if L is a lattice we set

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3-27g_3(L)^2}.$$

If $\lambda \in \mathbb{C}^\times$, then the definitions of G_4 and G_6 easily imply

$$g_2(\lambda L) = \lambda^{-4}g_2(L),\ g_3(\lambda L) = \lambda^{-6}g_3(L);$$

therefore

$$j(L) = j(\lambda L).$$

So, letting $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $\lambda = \omega_2^{-1}$, we have $j(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = j(\tau)$, where $\tau = \frac{\omega_1}{\omega_2}$. We set an action of

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

on the upper half plane $\mathcal{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau = \frac{a\tau+b}{c\tau+d}$$

for all $\tau \in \mathcal{H}$.

Proposition 1.2.1. *Let $\tau \in \mathcal{H}$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $j(\frac{a\tau+b}{c\tau+d}) = j(\tau)$.*

Proof. We first compute which is the result of the action on G_k:

$$G_k(\frac{a\tau+b}{c\tau+d}) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\frac{a\tau+b}{c\tau+d}+n)^k} =$$

$$= (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{(m(a\tau+b)+n(c\tau+d))^k} =$$

$$= (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{((ma+nc)\tau+(mb+nd))^k}.$$

Since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant 1, we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. Let now

$$(m', n') = (m, n)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (ma + nc, mb + nd);$$

then $(m, n) = (m', n')\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, so there is a 1-1 correspondence between pairs of integers (m, n) and (m', n'). Therefore

$$G_k(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k \sum_{(m',n')\neq(0,0)} \frac{1}{(m'\tau + n')^k} = (c\tau + d)^k G_k(\tau).$$

Now it is easy to deduce from here the behaviour of g_2 and g_3, as they are multiples of G_4 and G_6; so we have

$$g_2(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^4 g_2(\tau), g_3(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^6 g_3(\tau)$$

Therefore, when we substitute these expressions into the definition of j, all the factors $(c\tau + d)$ cancel. □

Let $\mathcal{F}$ be the subset of $z \in \mathcal{H}$ such that

$$\mathcal{F} = \left\{ |z| \geq 1, -\frac{1}{2} \leq \operatorname{Re} z < \frac{1}{2}, z \neq e^{i\theta} \text{ for } \frac{\pi}{3} < \theta < \frac{\pi}{2} \right\}$$

This is what is called a **fundamental domain** for the action of $\mathrm{SL}_2(\mathbb{Z})$ over $\mathcal{H}$, that is:

Definition 1.2.2. *Let G be a group acting on a set X endowed with a topology. A set $Y \subset X$ is a **fundamental domain** for the action of G over X if:*

1. *for any $x \in X$ there exist $g \in G$ and $y \in Y$ such that $y = g \cdot x$;*
2. *for any y_1, $y_2 \in Y$ and $g \in G \setminus \{1\}$ such that $y_1 = g \cdot y_2$, we have y_1,$y_2 \in \partial(Y)$.*

Proposition 1.2.3. *Given $\tau \in \mathcal{H}$, there exists $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that*

$$\frac{a\tau + b}{c\tau + d} = z \in \mathcal{F}.$$

Moreover, $z \in \mathcal{F}$ is uniquely determined by τ.

This proposition is useful as it enables us to prove the following:

Corollary 1.2.4. *Let $L \in \mathbb{C}$ be a lattice; then there exists a unique basis $\{\omega_1, \omega_2\}$ of L with $\frac{\omega_1}{\omega_2} \in \mathcal{F}$. In other words, $L = \lambda(\mathbb{Z}\tau + \mathbb{Z})$ for some $\lambda \in \mathbb{C}^\times$ and some uniquely determined $\tau \in \mathcal{F}$*

Proof. Let $\{\alpha, \beta\}$ be a basis for L and let $\tau_0 = \frac{\alpha}{\beta}$. We may assume that $\tau_0 \in \mathcal{H}$, by changing the sign of α if needed. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\frac{a\tau_0+b}{c\tau_0+d} = \tau \in \mathcal{F}$. Let $\omega_1 = a\alpha + b\beta$, $\omega_2 = c\alpha + d\beta$. Since the matrix is in $SL_2(\mathbb{Z})$, $L = \alpha + \mathbb{Z}\beta = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \omega_2(\mathbb{Z}\tau + \mathbb{Z})$, which proves the corollary. □

Instead of proving directly Proposition 1.2.3 (a prove of which can be found, for example, in [Ser96]), we are going now to give and to prove a slightly different statement, which will be more useful for our purposes.
In fact, we can easily verify the identity $\mathrm{Im}(g\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$. This shows that $\mathcal{H}$ is stable for the action of $\mathrm{SL}_2(\mathbb{Z})$. Moreover, we notice that the element $-\mathbb{1} \in \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $\mathcal{H}$ and we set:

Definition 1.2.5. *The group*

$$\Gamma = \frac{\mathrm{SL}_2(\mathbb{Z})}{\{\pm\mathbb{1}\}}$$

is called the ***modular group****.*

Remark: Let us denote by M the set of all lattices in $\mathbb{C}$. We make $\mathbb{C}^\times$ act on it by the action $(\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2)$ for every $\lambda \in \mathbb{C}^\times$. The quotient $\frac{M}{\mathbb{C}^\times}$ is identified with $\mathcal{H}$ by $(\omega_1, \omega_2) \mapsto \tau = \frac{\omega_1}{\omega_2}$, and this identification transforms the action of $\mathrm{SL}_2(\mathbb{Z})$ on M into the action of Γ on $\mathcal{H}$. So, from now on, we will identify the two actions; sometimes, to better highlight the nature of the elements we are working with, we will take elements in $\mathrm{SL}_2(\mathbb{Z})$, but considered as elements of Γ.

Let now

$$S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),\ T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right).$$

We have

$$S\tau = -\frac{1}{\tau},\ S^2 = \mathbb{1},\ T\tau = \tau + 1,\ (ST)^3 = \mathbb{1}.$$

Namely, we have then:

Theorem 1.2.6. *1. For every $\tau \in \mathcal{H}$, there exists an element $g \in \Gamma$ such that $g \cdot \tau \in \mathcal{F}$.*

2. *If two distinct points $\tau, \tau' \in \mathcal{F}$ are equivalent modulo Γ, then either* $\mathrm{Re}(\tau) = \frac{1}{2}$, $\tau = \tau' \pm 1$ *or* $|\tau| = 1$ *and* $\tau' = -\frac{1}{\tau}$.

3. *Let $\tau \in \mathcal{F}$, and let* $\mathrm{Stab}(\tau) = \{g \in \Gamma : g\tau = \tau\}$ *be the stabiliser of τ in Γ. Then* $\mathrm{Stab}(\tau) = \{\mathbb{1}\}$, *except in the following cases:*

   (a) $\tau = \imath$ *whose stabiliser is the cyclic group of order 2 generated by S;*

   (b) $\tau = \rho = e^{\frac{2\pi\imath}{3}}$, *whose stabiliser is the cyclic group of order 3 generated by ST;*

   (c) $\tau = -\bar{\rho} = e^{\frac{\imath\pi}{3}}$, *whose stabiliser is the cyclic group of order 3 generated by TS;*

4. *Γ is generated by S and T.*

Remark: We notice here that the derivative $j'(\tau)$ is non-zero for every τ having trivial stabiliser; in the other cases, $j'(\tau) = 0$ but $j''(\tau) \neq 0$ if the stabiliser is cyclic of order 2 and $j''(\tau) = 0$, $j'''(\tau) \neq 0$ if the stabiliser is cyclic of order 3.

Proof. Let G be the subgroup of Γ generated by S and T, and $\tau \in \mathcal{H}$. We will show that there exist $g' \in G$ such that $g' \cdot \tau \in \mathcal{F}$, which will prove assertion 1 of the theorem.
If $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, we have $\mathrm{Im}(g \cdot \tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$; since c, $d \in \mathbb{Z}$ the number of pairs (c, d) such that $|c\tau + d|$ is less than a given quantity is finite. We deduce that there exists $g \in G$ such that $\mathrm{Im}(g \cdot \tau)$ is maximal. We can find, on the other hand, $n \in \mathbb{Z}$ such that $|\mathrm{Re}(T^n g \cdot \tau)| < \frac{1}{2}$; this is because T acts simply as a translation of unitary modulus, so we can make it act until the real part lands in the interval we want it to be.
Such an element $\tau' = T^n g\tau \in \mathcal{F}$; we should only verify that $|\tau'| \geq 1$. The point is that if we had $|\tau'| < 1$, $-\frac{1}{\tau'}$ would have imaginary part bigger than $\mathrm{Im}(\tau')$, which contradicts our maximal choice. So the element $g' = T^n g$ is the element that proves the first assertion.
Let now $\tau \in \mathcal{F}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ such that $g \cdot \tau \in \mathcal{F}$. By possibly replacing (τ, g) by $(g \cdot \tau, g^{-1})$, we can assume that $\mathrm{Im}(g \cdot \tau) \geq \mathrm{Im}(\tau)$, that is $|c\tau + d| \leq 1$. This is obviously impossible if $|c| \geq 2$; so we are left with the cases $c = 0, \pm 1$.
If $c = 0$, we have $d = \pm 1$ and g is a translation of $\pm b$. Since $\mathrm{Re}(\tau)$ and $\mathrm{Re}(g \cdot \tau)$ are both between $-\frac{1}{2}$ and $\frac{1}{2}$, we are forced to have either $b = 0$, which means $g = 1$, or $b = \pm 1$, in which case one value among $\mathrm{Re}(\tau)$ and $\mathrm{Re}(g \cdot \tau)$ should be equal to $-\frac{1}{2}$, the other one to $\frac{1}{2}$.

If $c = 1$, $|\tau + d| \leq 1$ implies $d = 0$, except if $\tau = \rho$ (respectively, $-\bar{\rho}$), in which case we can have $d = 0, 1$ (respectively, $d = 0, -1$). The case $d = 0$ gives $g \cdot \tau = a - \frac{1}{\tau}$ and the first part of this discussion shows that $a = 0$, except if $\mathrm{Re}(\tau) = \pm\frac{1}{2}$, id est if $\tau = \rho, -\bar{\rho}$, in which case we could take $a = 0, -1$ or $a = 0, 1$.
The case $\tau = \rho$, $d = 1$ gives $g \cdot \tau = a - \frac{1}{1+\rho} = a + \rho$, that is, $a = 0, 1$; in the same vein we solve the case $\tau = -\bar{\rho}$, $d = -1$.
Finally, the case $c = -1$ can be solved in the same way just by changing the signs of a, b, c, d, which does not change the sign of $g \in \Gamma$. This concludes the second and the third points of the theorem.
We are left to prove that $G = \Gamma$; let $g \in \Gamma$. We choose a point τ_0 in the interior of $\mathcal{F}$, and let $\tau = g \cdot \tau_0$. We showed that there exists $g' \in G$ such that $g' \cdot \tau \in \mathcal{F}$. The points τ_0, $g' \cdot \tau = g'g \cdot \tau_0 \in \mathcal{F}$ are congruent modulo Γ, and one of them is in the interior of $\mathcal{F}$. So, from the previous assertions we deduce that these two points are the same, and that $g'g = \mathbb{1}$. Finally, we have $g \in G$, which ends our proof. □

1.2.2 Proving the isomorphism

In the previous section, we introduced the j-invariant and the action induced on it by the modular group. We can state here a proposition, whose proof is rather technical:

Proposition 1.2.7. *If $z \in \mathbb{C}$, then there is exactly one $\tau \in \mathcal{F}$ such that $j(\tau) = z$.*

Proof. See, for example, [Was08, Proposition 9.18]. □

This enables us to prove the following:

Theorem 1.2.8. *Let $y^2 = 4x^3 - Ax - B$ define an elliptic curve E over $\mathbb{C}$. Then there is a lattice L such that $g_2(L) = A$ and $g_3(L) = B$. There is an isomorphism of groups $\frac{\mathbb{C}}{L} \simeq E(\mathbb{C})$.*

Proof. Let $j = 1728\frac{A^3}{A^3 - 27B^2}$. From the previous proposition, we have that there exists a lattice $L = \mathbb{Z}\tau + \mathbb{Z}$ such that $j(\tau) = j(L) = j$.
Assume first that $g_2(L) \neq 0$; then $j = j(L) \neq 0$, so $A \neq 0$. Choose $\lambda \in \mathbb{C}^\times$ such that $g_2(\lambda L) = \lambda^{-4} g_2(L) = A$. The equality $j = j(L)$ implies that $g_3(\lambda L)^2 = B^2$, so $g_3(\lambda L) = \pm B$. If $g_3(\lambda L) = B$, we are done; if $g_3(\lambda L) = -B$, then $g_3(\imath\lambda L) = \imath^{-6} g_3(\lambda L) = B$ and $g_2(\imath\lambda L) = \imath^{-4} g_2(\lambda L) = A$. Therefore, either λL or $\imath\lambda L$ is the desired lattice.
If $g_2(L) = 0$, then $j = j(L) = 0$, so $A = 0$. Since $A^3 - 27B^2 \neq 0$ by assumption and since $g_2(L)^3 - 27 g_3(L)^2 \neq 0$ by Lemma 1.1.8, we have $B \neq 0$

and $g_3(L) \neq 0$. Choose $\mu \in \mathbb{C}^\times$ such that $g_3(\mu L) = \mu^{-6} g_3(L) = B$; then $g_2(\mu L) = \mu^{-2} g_2(L) = 0 = A$, so μL is the desired lattice. By Theorem 1.1.9, the map $\frac{\mathbb{C}}{L} \to E(\mathbb{C})$ is an isomorphism. □

This proves the correspondence between tori and elliptic curves. In the following chapters, we will deal with elliptic curves simply by taking into account the quantities $\tau = \frac{\omega_1}{\omega_2}$ relative to their associated lattices.

1.3 Isogenies

In this section, we are going to briefly introduce isogenies, morphisms between elliptic curves. In general, we define an isogeny to be a morphism between abelian varieties that has finite kernel and it is surjective; more, it is automatically a group homomorphism between the group of the k-valued points, over any field k over which the isogeny is defined. In particular, for elliptic curves, an isogeny is a surjective morphism of varieties that preserves the basepoint. We limit ourselves to presenting basic properties linked to the strict computational side (for a more complete discussion on this topic, see for example [Sil09, Chapter 3.4]).
In the rest of this work, we will be concerned with relations between invariants of a given elliptic curve and invariants of the images that are obtained from it by an isogeny; we start here by considering the effect of these functions over lattices (which, as we saw, is just a different way of carrying on our analysis of elliptic curves).

Definition 1.3.1. *Let $E_1 = \frac{\mathbb{C}}{L_1}$ and $E_2 = \frac{\mathbb{C}}{L_2}$ be elliptic curves over $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be such that $\alpha L_1 \subseteq L_2$. Then*

$$\begin{array}{rccc} [\alpha]: & E_1 & \to & E_2 \\ & z & \mapsto & \alpha z \end{array}$$

*gives a homomorphism from E_1 to E_2; the fact $\alpha L_1 \subseteq L_2$ tells us that the map is well defined. For any $\alpha \neq 0$, a map of this form is called an **isogeny** from E_1 to E_2. If there exists an isogeny from E_1 to E_2 we say that the curves are **isogenous**.*

Lemma 1.3.2. *If $\alpha \neq 0$, then αL_1 is of finite index in L_2.*

Proof. Let $\left\{\omega_1^{(k)}, \omega_2^{(k)}\right\}$ be a basis for L_k, $k = 1, 2$. Write

$$\alpha \omega_i^{(1)} = a_{i,1}\omega_1^{(2)} + a_{i,2}\omega_2^{(2)}$$

with $a_{i,j} \in \mathbb{Z}$. If $\det(a_{i,j}) = 0$, then $(a_{1,1}, a_{1,2})$ is a rational multiple of $(a_{2,1}, a_{2,2})$, which implies that $\alpha\omega_1^{(1)}$ is a rational multiple of $\alpha\omega_2^{(1)}$, and this is impossible since $\omega_1^{(1)}$ and $\omega_2^{(1)}$ are linearly independent over $\mathbb{R}$.
We consider now each $\omega_i^{(k)}$ as a two-dimensional vector over $\mathbb{R}$. Then the area of the fundamental parallelogram of L_k is $|\det(\omega_1^{(k)}, \omega_2^{(k)})|$. Since

$$\det(\alpha\omega_1^{(1)}, \alpha\omega_2^{(2)}) = \det(a_{i,j}) \det(\omega_1^{(2)}, \omega_2^{(2)}),$$

the index of αL_1 in L_2, which can be seen as the ratio of the areas of the fundamental parallelograms, is $|\det(a_{i,j})|$. □

We define the **degree** of $[\alpha]$ to be the index $[L_2 : \alpha L_1]$. If $\alpha = 0$, we define the degree to be 0. If N is the degree, we say that $\frac{\mathbb{C}}{L_1}$ and $\frac{\mathbb{C}}{L_2}$ are N-isogenous. In practice, we can always find the so-called **dual isogeny**, that means a map ensuring us that if E_1 and E_2 are N-isogenous, E_2 and E_1 are N-isogenous; the relation of being isogenous is then symmetric.

Proposition 1.3.3. *If $\alpha \neq 0$, then* $\mathrm{card}(\ker([\alpha])) = \deg([\alpha])$.

Proof. Let $z \in \mathbb{C}$. Then $[\alpha](z) = 0$ if and only if $\alpha z \in L_2$, so

$$\ker([\alpha]) = \frac{\alpha^{-1}L_2}{L_1} \simeq \frac{L_2}{\alpha L_1},$$

where the isomorphism is given by the multiplication by α. Therefore, the order of the kernel is the index, which is in fact the degree. □

If $\ker([\alpha]) = \frac{\alpha^{-1}L_2}{L_1}$ is cyclic, we say that $[\alpha]$ is a **cyclic isogeny**. In general, $\ker([\alpha])$ is a finite abelian group with at most two generators (coming from the generators of L_2), so it can be written in the form $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, with $n_1 | n_2$; therefore, the isogeny equals multiplication by n_1 on E_1 composed with a cyclic isogeny whose kernel has order $\frac{n_2}{n_1}$.
Let now $\alpha \neq 0$ and let $N = \deg([\alpha])$. Define the **dual isogeny** $\hat{[\alpha]} : \frac{\mathbb{C}}{L_2} \to \frac{\mathbb{C}}{L_1}$ to be the map given by multiplication by $\frac{N}{\alpha}$. We need to show that this is well defined: since $N = [L_2 : \alpha L_1]$, we have $NL_2 \subseteq \alpha L_1$. Therefore, $\frac{N}{\alpha} L_2 \subseteq L_1$, as desired. We have the fundamental relation $\hat{[\alpha]} \circ [\alpha] = [\deg([\alpha])]$, where $[\deg([\alpha])]$ stands here for the integer multiplication on $\frac{\mathbb{C}}{L_2}$. It is immediate to show that $\hat{\hat{[\alpha]}} = [\alpha]$, and that $[\alpha] \circ \hat{[\alpha]} = [\deg(\hat{[\alpha]})] = [\deg([\alpha])]$.
A particular mention is deserved to the case $\alpha = 1$. This means we have $L_1 \subseteq L_2$ and that the isogeny is simply the map $z (\mathrm{mod}\ L_1) \mapsto z (\mathrm{mod}\ L_2)$. In this case, the kernel is $\frac{L_2}{L_1}$. In fact, any arbitrary isogeny can be reduced to this situation by composing with the isomorphism $\frac{\mathbb{C}}{L_2} \to \frac{\mathbb{C}}{\alpha^{-1}L_2}$ given by multiplication by α^{-1}.

Proposition 1.3.4. *Let $C \subset E_1 = \frac{\mathbb{C}}{L_1}$ be a finite subgroup. Then there exist an elliptic curve $E_2 = \frac{\mathbb{C}}{L_2}$ and an isogeny from E_1 to E_2 whose kernel is C.*

Proof. C can be written as $\frac{L_2}{L_1}$ for some subgroup L_2 of $\mathbb{C}$ containing L_1. If N is the order of C, then $NL_2 \subseteq L_1$, so $L_1 \subseteq L_2 \subseteq \frac{1}{N}L_1$. So, as both L_1 and $\frac{1}{N}L_1$ are lattices, they are both isomorphic to $\mathbb{Z}^2$. More, we have that L_2 is isomorphic to $\mathbb{Z}^2$, hence it is a lattice; therefore, $\frac{\mathbb{C}}{L_1} \to \frac{\mathbb{C}}{L_2}$ is the isogeny we were looking for. □

To end with, we now prove that all nonconstant maps between elliptic curves over $\mathbb{C}$ are linear. This has the interesting consequence that a nonconstant map taking 0 to 0 is of the form $[\alpha]$, hence it is an homomorphism.

Theorem 1.3.5. *Let $E_1 = \frac{\mathbb{C}}{L_1}$ and $E_2 = \frac{\mathbb{C}}{L_2}$ be elliptic curves over $\mathbb{C}$. Suppose that $f : E_1 \to E_2$ is an analytic map (that means, it can be developed as a power series in a neighbourhood of any point of E_1); then there exist $\alpha, \beta \in \mathbb{C}$ such that $f(z \pmod{L_1}) = \alpha z + \beta \pmod{L_2}$ for all $z \in \mathbb{C}$. In particular, if $f(0 \pmod{L_1}) = 0 \pmod{L_2}$ and f is not the 0-map, then f is an isogeny.*

Proof. We can lift f to a continuous map $\tilde{f} : \mathbb{C} \to \mathbb{C}$ satisfying

$$f(z(\text{mod } L_1) = \tilde{f}(z)(\text{mod } L_2)$$

for all $z \in \mathbb{C}$. Moreover, $\tilde{f}$ can be expressed as a power series in the neighbourhood of each point in $\mathbb{C}$; then the function $\tilde{f}(z+\omega) - \tilde{f}(z)$ reduces to 0 mod L_2. Since it is continuous and takes values in the discrete set L_2, it is constant; therefore its derivative is 0, so $\tilde{f}'(z+\omega) = \tilde{f}'(z)$ for all z. This means that $\tilde{f}'$ is a holomorphic doubly periodic function, hence constant, as an immediate consequence of the maximum modulus principle for holomorphic functions. Therefore, $\tilde{f}(z) = \alpha z + \beta$, as we wanted to show. □

Let us try to write down the explicit correspondence between an elliptic curve and the image of it by an ℓ-isogeny, that is to say an isogeny of degree ℓ. If the departing curve is $\frac{\mathbb{C}}{\omega_1\mathbb{Z}+\omega_2\mathbb{Z}}$, the target curve will be $\frac{\mathbb{C}}{\frac{\omega_1}{\ell}\mathbb{Z}+\omega_2\mathbb{Z}}$, and the correspondence is simply expressed by writing

$$\begin{array}{ccc} \frac{\mathbb{C}}{\omega_1\mathbb{Z}+\omega_2\mathbb{Z}} & \to & \frac{\mathbb{C}}{\frac{\omega_1}{\ell}\mathbb{Z}+\omega_2\mathbb{Z}} \\ z & \mapsto & z \end{array}$$

which means that, if we normalise the lattice by writing it as generated by $\{1, \tau\}$ with $\tau = \frac{\omega_1}{\omega_2}$, the image of the corresponding curve by an ℓ-isogeny would be the curve associated to the lattice $\left\{1, \frac{\tau}{\ell}\right\}$. From now on, we will adopt this notation to denote isogenies.

Chapter 2

Modular polynomials

In this chapter, we will give some general definitions about modular functions and modular polynomials; we will try to understand what a modular polynomial is, and we will give some examples of modular polynomials computed by means of j-invariants over an elliptic curve.

2.1 Modular functions for $\Gamma^0(m)$

We are going here to focus on modular functions for the subgroup

$$\Gamma^0(m) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma : b \equiv 0 (\text{mod } m) \right\} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right)^{-1} \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & m \end{smallmatrix}\right) \cap \Gamma \subset \Gamma,$$

defined for any positive integer m.
The formulation we chose for giving definitions is not the most generic one; most of the definitions can be adapted to any subgroup of Γ, and are not specific for subgroups in the shape of $\Gamma^0(m)$. Anyway, our interest is really to focus on the polynomials defined by means of $\Gamma^0(m)$, and this is the reason why we chose to stick from the beginning to these subgroups; this will allow us to work with concrete properties that a ampler generality would have prevented.

Definition 2.1.1. *A **modular function** for $\Gamma^0(m)$ is a complex valued function $f(\tau)$ defined on the upper half plane $\mathcal{H}$, except for isolated singularities, which satisfies the following conditions:*

- *$f(\tau)$ is meromorphic on $\mathcal{H}$;*
- *$f(\tau)$ is invariant under $\Gamma^0(m)$, that is to say $f(\gamma\tau) = f(\tau)$ for all $\tau \in \mathcal{H}$ and $\gamma \in \Gamma^0(m)$;*
- *$f(\tau)$ is meromorphic at the cusps.*

We try now to understand the last condition. Suppose that $f(\tau)$ satisfies the first two conditions, and that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$; we claim that $f(\gamma\tau)$ has period m.
To see this, we recall that $\tau + m = U\tau$, where $U = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$. An easy computation shows that $\gamma U \gamma^{-1} \in \Gamma^0(m)$, and then we obtain

$$f(\gamma(\tau + m)) = f(\gamma U\tau) = f(\gamma U\gamma^{-1}\gamma\tau) = f(\gamma\tau),$$

since $f(\tau)$ is $\Gamma^0(m)$-invariant.
It follows that, if we set $q = q(\tau) = e^{2\pi\imath\tau}$ as usual, then $f(\gamma\tau)$ is a holomorphic function in $q^{\frac{1}{m}} = q^{2\pi\imath\frac{\tau}{m}}$, for $0 < |q^{\frac{1}{m}}| < 1$. Thus $f(\gamma\tau)$ has a Laurent expansion $f(\gamma\tau) = \sum_{n=-\infty}^{+\infty} a_n q^{\frac{n}{m}}$, which by abuse of notation will be called the q-expansion of $f(\gamma\tau)$. Then $f(\tau)$ is said to be **meromorphic at the cusps** if for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the q-expansion of $f(\gamma\tau)$ has only finitely many non-zero coefficients for negative exponents.
It is straightforward to verify that $j(\tau)$ fits these requirements: it is holomorphic in $\mathcal{H}$, invariant under Γ and meromorphic at the cusps by (1.1); thus $j(\tau)$ is a modular function for $\Gamma = \Gamma^0(1)$.
The interest of this description lies in the fact that functions which are modular for Γ can be easily expressed in terms of the j function:

Theorem 2.1.2. *Let m be a positive integer. Then:*

1. *$j(\tau)$ is a modular function for Γ and every modular function for Γ is a rational function in $j(\tau)$;*

2. *$j(\tau)$ and $j(m\tau)$ are modular functions for $\Gamma^0(m)$, and every modular function for $\Gamma^0(m)$ is a rational function of $j(\tau)$ and $j(m\tau)$.*

Remark: Note that the first point is just a special case of the second one; here we distinguish the two as they are both important properties to notice, and in any case we are going to use the proof of the first assertion to prove the second.
Notice also that the function which are modular for Γ are modular also for $\Gamma^0(m)$, as $\Gamma^0(m) \subseteq \Gamma$.

Before starting with the proof, we state a lemma that will be useful, and that characterises modular functions:

Lemma 2.1.3. • *A holomorphic modular function for Γ which is holomorphic at ∞ is constant.*

- *A holomorphic modular function for Γ is a polynomial in $j(\tau)$.*

Proof. To prove the first point, let $f(\tau)$ be our modular function. Since $f(\tau)$ is holomorphic at ∞, we know that $f(\infty) = \lim_{\mathrm{Im}(\tau)\to\infty}$ exists as a complex number. We will show that $f(\mathcal{H} \cup \{\infty\})$ is compact; by maximum modulus principle for holomorphic functions, this would imply that $f(\tau)$ is constant. Let $f(\tau_k)$ be a sequence of points in this image. We need to find a subsequence that converges to a point of the form $f(\tau)$ for some $\tau \in \mathcal{H}$. Since $f(\tau)$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant, we can assume that the τ_k lies in the fundamental domain $\mathcal{F}$ (see Proposition 1.2.3). If the imaginary parts of τ_k are unbounded, then by the above limit a subsequence of them converges to $f(\infty)$; if the imaginary parts are bounded, then the τ_k lie in a compact subset of $\mathcal{H}$, and this implies we have a subsequence converging to the limit. In both cases, we can find our subsequence and prove the first point.
To prove the second point, let again $f(\tau)$ be our holomorphic modular function for Γ; we know from Definition 2.1.1 that its q-expansion has only finitely many terms with negative powers of q. Since the q-expansion of $j(\tau)$ begins with $\frac{1}{q}$, one can find a polynomial $A(x)$ such that $f(\tau) - A(j(\tau))$ is holomorphic at ∞. Since by our hypothesis it is holomorphic on $\mathcal{H}$, it is a constant function; thus, $f(\tau)$ is a polynomial in $j(\tau)$. □

Proof of the theorem: To prove modularity, our definition requires to check the q-expansion of $f(\gamma\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since $f(\tau)$ is $\Gamma^0(m)$-invariant, we actually need only to consider the q-expansions of $f(\gamma_i\tau)$, where the γ_i are the coset representatives of $\Gamma^0(m) \subset \Gamma$, so there are only a finite number of q-expansions to check. The nicest case is when $f(\tau)$ is a modular function for Γ, because in this case we only need to consider the q-expansion of $f(\tau)$ itself.
For the first point, we already know that $j(\tau)$ is a modular function for Γ, so we just need to show that every modular function $f(\tau)$ for Γ is a rational function in $j(\tau)$. The previous lemma studies some particular cases; to set ourselves in the general case, let $f(\tau)$ be an arbitrary modular function for Γ, possibly with poles on $\mathcal{H}$. If we can find a polynomial $B(x)$ such that $B(j(\tau))f(\tau)$ is holomorphic on $\mathcal{H}$, then the lemma will imply that $f(\tau)$ is a rational function in $j(\tau)$.
Since $f(\tau)$ has a meromorphic q-expansion, it follows that $f(\tau)$ has only finitely many poles in $\mathcal{F}$ and since $f(\tau)$ is Γ-invariant, Proposition 1.2.3 implies that every pole of $f(\tau)$ is Γ-equivalent to one in $\mathcal{F}$; thus, if $B(j(\tau))f(\tau)$ has no poles in $\mathcal{F}$, then it is holomorphic on $\mathcal{H}$.
So suppose now that $f(\tau)$ has a pole of order m at $\tau_0 \in \mathcal{F}$; if $j'(\tau_0) \neq 0$, then $(j(\tau) - j(\tau_0))^m f(\tau)$ is holomorphic at τ_0. Proceeding this way, one can find

a polynomial $B(x)$ such that $B(j(\tau))f(\tau)$ has no poles, except possibly for those where $j'(\tau_0) = 0$. When this happens, the last statement of Theorem 1.2.6 (the remark, in particular) says that we can assume $\tau_0 = \imath$ or $\tau_0 = e^{\pm 2\frac{\pi\imath}{3}}$. As an example, we see here how to deal with the case $\tau_0 = \imath$; in this case, we claim that m is even. To see this, we notice that, in a neighbourhood of $\imath$, $f(\tau)$ can be written in the form

$$f(\tau) = \frac{g(\tau)}{(\tau - \imath)^m},$$

where $g(\tau)$ is holomorphic and $g(\imath) \neq 0$. Now $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ fixes $\imath$, so that

$$f(\tau) = f(-\frac{1}{\tau}) = \frac{g(\frac{-1}{\tau})}{(\frac{-1}{\tau} - \imath)^m}.$$

Comparing these two expressions for $f(\tau)$, we see that $g(\frac{1}{\tau}) = \frac{1}{(\imath\tau)^m} g(\tau)$. Evaluating this at $\tau = \imath$ implies that $g(\imath) = (-1)^m g(\imath)$, and since $g(\imath) \neq 0$, it follows that m is even. By the Remark to Theorem 1.2.6, we know that $j(\tau) - 1728$ has a zero of order 2 at $\imath$, hence $(j(\tau) - 1728)^{\frac{m}{2}} f(\tau)$ is holomorphic at $\imath$. A similar argument allows us to conclude when $\tau = e^{\pm 2\frac{\pi\imath}{3}}$, and this solves all the possible cases.

To prove the second assertion, as we already pointed out before, we have automatically that $j(\tau)$ is a modular function for $\Gamma^0(m)$. As far as $j(m\tau)$ is concerned, it is certainly holomorphic; we have to check its invariance properties.

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma^0(m)$; then $j(m\gamma\tau) = j(\frac{m(a\tau+b)}{c\tau+d}) = j(\frac{am\tau+bm}{\frac{c}{m}m\tau+d})$. Since $\gamma \in \Gamma^0(m)$, it follows that $\gamma' = \left(\begin{smallmatrix} a & bm \\ \frac{c}{m} & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$; thus

$$j(m\gamma\tau) = j(\gamma' m\tau) = j(m\tau),$$

which proves that $j(m\tau)$ is $\Gamma^0(m)$-invariant. In order to show that $j(m\tau)$ is meromorphic at the cusps, we introduce the set of matrices

$$C(m) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) : ad = m, a > 0, 0 \leq b < d, \gcd(a, b, d) = 1 \right\}.$$

Consider the matrix $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(m)$; this is such that $\sigma_0\tau = m\tau$, and $\Gamma^0(m) = (\sigma_0^{-1}\Gamma\sigma_0) \cap \Gamma$. More generally, it can be proved (see [Cox89, page 228]) that for $\sigma \in C(m)$, the set $(\sigma_0^{-1}\Gamma\sigma) \cap \Gamma$ is a right coset of $\Gamma^0(m)$ in Γ. This induces a one-to-one correspondence between right cosets of $\Gamma^0(m)$ and elements of $C(m)$.

We compute now some q-expansions. Fix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and choose $\sigma \in C(m)$ so that γ lies in the right coset corresponding to σ. This means that $\sigma_0\gamma = \tilde{\gamma}\sigma$ for some $\tilde{\gamma} \in SL_2(\mathbb{Z})$, and hence

$$j(m\gamma\tau) = j(\sigma_0\gamma\tau) = j(\tilde{\gamma}\sigma\tau) = j(\sigma\tau),$$

since $j(\tau)$ is Γ-invariant; so

$$j(m\gamma\tau) = j(\sigma\tau). \tag{2.1}$$

Suppose that $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$; we know that the q-expansion of $j(\tau)$ is

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n,\ c_n \in \mathbb{Z}, \tag{2.2}$$

and since $\sigma\tau = \frac{a\tau+b}{d}$ it follows that $q(\sigma\tau) = e^{2\pi\imath\frac{a\tau+b}{d}} = e^{2\pi\imath\frac{b}{d}} q^{\frac{a}{d}}$. If we set $\zeta_m = e^{2\frac{\pi\imath}{m}}$, we can write it as $q(\sigma\tau) = \zeta_m^{ab}(q^{\frac{1}{m}})^{a^2}$, since $ad = m$. This gives us the q-expansion

$$j(m\gamma\tau) = j(\sigma\tau) = \frac{\zeta_m^{-ab}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abn} (q^{\frac{1}{m}})^{a^2 n}, \tag{2.3}$$

$c_n \in \mathbb{Z}$. As we can see, there is only one negative exponent, which shows that $j(m\tau)$ is meromorphic at the cusps, and thus $j(m\tau)$ is a modular function for $\Gamma^0(m)$.

The following step is to introduce the modular equation $\Phi_m(X, Y)$; this will be used here to complete the proof, but it will be one of the major objects of interest of all the following discussion. Let the right cosets of $\Gamma^0(m)$ in $\mathrm{SL}_2(\mathbb{Z})$ be $\Gamma^0(m)\gamma_i$, $i = 1, \ldots, |C(m)|$. Then consider the polynomial in X:

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)).$$

We will prove that this expression is a polynomial in X and in $j(\tau)$. To see it, consider the coefficients of it as polynomial in X: being symmetric polynomials in the $j(m\gamma_i\tau)$, they are certainly holomorphic. To check invariance under Γ, pick $\gamma \in \Gamma$; then the cosets $\Gamma^0(m)\gamma_i\gamma$ are a permutation of the cosets $\Gamma^0(m)\gamma_i$, and since $j(m\tau)$ is invariant under $\Gamma^0(m)$, the $j(m\gamma_i\gamma\tau)$ are a permutation of the $j(m\gamma_i\tau)$. This shows that the coefficients are invariant under Γ.

We then have to show that the coefficients are meromorphic at infinity. Rather than expanding in powers of q, it suffices to expand in terms of $q^{\frac{1}{m}} = e^{2\pi\imath\frac{\tau}{m}}$ and show that only finitely many negative exponents appears. From (2.1), we know that $j(m\gamma_i\tau) = j(\sigma\tau)$ for some $\sigma \in C(m)$, and then the q-expansion (2.3) we computed shows that the q-expansion for $j(m\gamma_i\tau)$ has only finitely many negative exponents. Since the coefficients are polynomials in the $j(m\gamma_i\tau)$, they are clearly meromorphic at the cusps. This proves that

the coefficients of $\Phi_m(X,\tau)$ are holomorphic modular functions; thus they are polynomials in $j(\tau)$, as shown in the Lemma 2.1.3.
This means that there exists a polynomial $\Phi_m(X,Y) \in \mathbb{C}[X,Y]$ such that $\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|}(X - j(m\gamma_i\tau))$. The equation $\Phi_m(X,Y) = 0$ is called the **classical modular equation**, and we will call the polynomial $\Phi_m(X,Y)$ the **classical modular polynomial**.
It is easy to prove that $\Phi_m(X,Y)$ is irreducible as a polynomial in X (an explicit proof can be found for example in [Cox89, page 230]). By (2.1), each $j(m\gamma_i\tau)$ can be written as $j(\sigma\tau)$ for a unique $\sigma \in C(m)$; thus we can also express the modular polynomial in the form

$$\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau)). \tag{2.4}$$

Note that $j(m\tau)$ is always one of the $j(\sigma\tau)$ since $\left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(m)$; hence

$$\Phi_m(j(m\tau), j(\tau)) = 0,$$

which is one of the important properties we will exploit about this polynomial.
We compute now the degree in X of $\Phi_m(X,Y)$: we can see immediately that it is equal to $|C(m)|$, and counting the number of elements there we get $|C(m)| = m\prod_{p|m}(1 + \frac{1}{p}) = \deg_X(\Phi_m(X,Y))$ (again, for the explicit computation we refer to [Cox89, page 228]).
Now let $f(\tau)$ be an arbitrary modular function for $\Gamma^0(m)$. To prove that $f(\tau)$ is a rational function in $j(\tau)$ and in $j(m\tau)$, consider the function

$$G(X,\tau) = \Phi_m(X, j(\tau)) \sum_{i=1}^{|C(m)|} \frac{f(\gamma_i\tau)}{X - j(m\gamma_i\tau)} = \tag{2.5}$$

$$= \sum_{i=1}^{|C(m)|} f(\gamma_i\tau) \prod_{i \neq j} (X - j(m\gamma_i\tau)).$$

This is a polynomial in X, and one can check that the coefficients are modular functions for Γ (to verify it, we have to do computations analogous to what we did above for classical modular polynomials); but once we know that the coefficients are modular functions for Γ, by Theorem 2.1.2 they are rational functions of $j(\tau)$. Hence $G(X,\tau)$ is a polynomial in $\mathbb{C}(j(\tau))[X]$.
We assume now that $\gamma_1 = \mathbb{1}$; by the product rule, we obtain

$$\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)) = \prod_{i \neq 1} (j(m\tau) - j(m\gamma_i\tau)).$$

The substitution $X = j(m\tau)$ in (2.5) gives

$$G(j(m\tau), j(\tau)) = f(\tau)\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)).$$

Now, we know that $\Phi_m(X, j(\tau))$ is irreducible, hence it has all distinct roots, so that $\frac{\partial \Phi_m}{\partial X}(j(m\tau), j(\tau)) \neq 0$; so we can write $f(\tau) = \frac{G(j(m\tau),j(\tau))}{\frac{\partial \Phi_m}{\partial X}(j(m\tau),j(\tau))}$, which proves that $f(\tau)$ is in fact a rational function in $j(\tau)$ and $j(m\tau)$. □

The polynomial will be one of the objects of study for all the rest of this work; so, we recall here the definition in order to set it in a better evidence:

Definition 2.1.4. *We call **classical modular polynomial** the polynomial*

$$\Phi_m(X, Y) \in \mathbb{C}[X, Y]$$

such that

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)).$$

We end this chapter by a last remark, which will be massively exploited during computations. We said that the set $|C(m)|$ is in bijection with the right cosets of $\Gamma^0(m)$ into Γ; actually, there is a very easy and useful way to represent these cosets by means of the matrices S and T we introduced in the preceding chapter, when working with a prime m. Namely:

Proposition 2.1.5. *For any prime integer m, $\Gamma^0(m)$ has index $m+1$ in Γ, and $\left\{\left(\begin{smallmatrix}1 & k\\ 0 & 1\end{smallmatrix}\right) : k \in [0, m-1]\right\} \cup \left\{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\right\} = \left\{T^k : k \in [0, m-1]\right\} \cup \{S\}$ is a set of representatives for the cosets ${}_{\Gamma^0(m)}\backslash^{\Gamma}$.*

Proof. We set $\mathcal{R}_m = \left\{\left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right) : k \in [0, m-1]\right\} \cup \left\{\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)\right\}$, defined for every prime m. To prove our assertion, we have to show that different elements in $\mathcal{R}_m$ are not equivalent modulo the action of $\Gamma^0(m)$, and that on the other side every element of Γ is equivalent to an element of $\mathcal{R}_m$ modulo this action. Let us take $k, t \in [0, m-1]$; then $\left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & k\\ 0 & 1\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}1 & k-t\\ 0 & 1\end{smallmatrix}\right)$, and this matrix is in $\Gamma^0(m)$ if and only if $t = k$.
Moreover, we have $S\left(\begin{smallmatrix}1 & k\\ 0 & 1\end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix}0 & -1\\ 1 & -k\end{smallmatrix}\right) \notin \Gamma^0(m)$, and this proves that different elements are not equivalent modulo the action of the group. On the other hand, we know that Γ is generated by T and S; since ${}^tT = ST^{-1}S$, we can say as well that Γ is generated by S and ${}^tT$. Since ${}^tT \in \Gamma^0(m)$, for any $k \in [0, m-1]$ we have that ${}^tT\left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right)$ is in the same class as $\left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right)$ and that ${}^tTS$ is in the same class as S; a direct check tells us that $S\left(\begin{smallmatrix}1 & k\\ 0 & 1\end{smallmatrix}\right)$ is in the same class as S, and we have $SS = \mathbb{1}$. So, we cannot have classes different from the $m+1$ that we have already considered. □

This description will turn out to be really useful when doing computations, as it will enable us to characterise in a precise and simple way the elements of the group ${}_{\Gamma^0(m)}\backslash^{\Gamma}$, when we will use them to build the classical modular polynomial and other modular polynomials.

2.2 Properties of the classical modular polynomial

In this section, we will prove some of the fundamental properties of the modular polynomial Φ_m, which will be massively used in the last part of this work, doing computations.

Theorem 2.2.1. *Let $m \in \mathbb{N}$.*

1. *$\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$;*
2. *$\Phi_m(X,Y)$ is irreducible when regarded as a polynomial in X;*
3. *if $m > 1$, $\Phi_m(X,Y) = \Phi_m(Y,X)$;*
4. *if m is not a perfect square, then $\Phi_m(X,X)$ is a polynomial of degree > 1 whose leading coefficient is ± 1;*
5. *if m is a prime p, then $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p)(mod\ p\mathbb{Z}[X,Y])$.*

Remark: Here we state the theorem in this form for sake of completeness, but we are not going to prove the last point, as it boils down to be just technical computations, which can be found for example in [Cox89, Theorem 11.18] or in [Lan87, pages 57-60].

Proof. To prove the first assertion, it suffices to prove that an elementary symmetric function $f(\tau)$ in the $j(\sigma\tau)$, $\sigma \in C(m)$, is a polynomial in $j(\tau)$ with integer coefficients.
We begin by studying the q-expansion of a generic $f(\tau)$ more in detail. Let $\zeta_m = e^{2\frac{\pi\imath}{m}}$. By (2.3), each $j(\sigma\tau)$ lies in the field of formal meromorphic Laurent series $\mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$, and since $f(\tau)$ is an integer polynomial in the $j(\sigma\tau)$s, $f(\tau)$ also lies in $\mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$. We will prove, by using Galois theory, that $f(\tau)$ is contained in the smaller field $\mathbb{Q}((q^{\frac{1}{m}}))$.
An automorphism $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta_m) \setminus \mathbb{Q})$ induces, by acting on the coefficients, an automorphism of $\mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$. Given $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$, let us see how ψ

affects $j(\sigma\tau)$. We know that $\psi(\zeta_m) = \zeta_m^k$ for some integer k relatively prime to m, and from (2.3) it follows that

$$\psi(j(\sigma\tau)) = \frac{\zeta_m^{-abk}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abkn} (q^{\frac{1}{m}})^{a^2 n},$$

since all the c_n are integers.
Let b' be the integer $0 \leq b' < d$ such that $b' \equiv bk (\text{mod } d)$. Since $ad = m$, we have $\zeta_m^{abk} = \zeta_m^{ab'}$, and consequently the formula can be written

$$\psi(j(\sigma\tau)) = \frac{\zeta_m^{-ab'}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{ab'n} (q^{\frac{1}{m}})^{a^2 n}.$$

If we let $\sigma' = \left(\begin{smallmatrix} a & b' \\ 0 & d \end{smallmatrix}\right) \in C(m)$, (2.3) implies that $\psi(j(\sigma\tau)) = j(\sigma'\tau)$, thus the elements of $\text{Gal}(\mathbb{Q}(\zeta_m)|\mathbb{Q})$ permute the $j(\sigma\tau)$s. Since $f(\tau)$ is symmetric in the $j(\sigma\tau)$, it follows that $f(\tau) \in \mathbb{Q}((q^{\frac{1}{m}}))$. We conclude that $f(\tau) \in \mathbb{Z}((q))$ since the q-expansion of $f(\tau)$ involves only integral powers of q and the coefficients of the q-expansion are algebraic integers.
It remains now to show that $f(\tau)$ is an integer polynomial in $j(\tau)$. By Lemma 2.1.3, we can find $A(X) \in \mathbb{C}[X]$ such that $f(\tau) = A(j(\tau))$. In the proof of the Lemma, we had that $A(X)$ was chosen so that the q-expansion of $f(\tau) - A(j(\tau))$ has only terms of degree > 0. Since the expansions of $f(\tau)$ and $j(\tau)$ have integer coefficients and $j(\tau)$ has only -1 as negative exponent, it follows that $A(X) \in \mathbb{Z}[X]$. Thus $f(\tau) = A(j(\tau))$ is an integer polynomial in $j(\tau)$, and the first point is proven.

Remark: This way of proving, that is to say the passage from the coefficients of the q-expansion to the coefficients of the polynomial $A(X)$ is a special case of the **Hasse q-expansion principle**, which we will not explain here (one can find more about it for example on [Lan87]).

Then the second point comes from the fact that Γ permutes the functions $j \circ \sigma_i$, where $\sigma_i = \left(\begin{smallmatrix} a_i & b_i \\ 0 & d_i \end{smallmatrix}\right)$ and

$$j \circ \sigma(\tau) = j(\sigma\tau)$$

(from now on, we will use the right-hand short notation to express this composition); moreover, the elements in Γ act as automorphisms on the field $\mathbb{C}(j, j \circ \sigma_1, \ldots, j \circ \sigma_{|C(m)|})$, as we have seen before.

Now we prove the symmetry of that polynomial. One of the matrices σ_i can be seen as $\left(\begin{smallmatrix}1 & 0\\ 0 & m\end{smallmatrix}\right)$; hence, if we denote by $\hat{n}$ the multiplication for a generic quantity n, $j \circ \frac{\hat{1}}{m}$ is a root of $\Phi_m(X, j)$, id est

$$\Phi_m(j(\frac{\tau}{m}), j(\tau)) = 0$$

for all τ, that is to say,

$$\Phi_m(j(\tau), j(m\tau)) = 0;$$

using the new notation we introduced, we can say $\Phi_m(j, j \circ \hat{m}) = 0$. So, $j \circ \hat{m}$ is a root of $\Phi_m(j, X)$, but it is also a root of $\Phi_m(X, j)$, corresponding to the matrix $\left(\begin{smallmatrix}m & 0\\ 0 & 1\end{smallmatrix}\right)$; since $\Phi_m(X, j)$ is irreducible, we conclude that $\Phi_m(X, j)$ divides $\Phi_m(j, X)$, that is to say $\Phi_m(j, X) = g(X, j)\Phi_m(X, j)$ for some polynomial $g(t, j) \in \mathbb{Z}[t, j]$ from the Gauss Lemma. From the properties above this would mean $\Phi_m(j, X) = g(X, j)g(j, X)\Phi_m(j, X)$, whence $g(X, j)g(j, X) = 1$ and so $g(X, j)$ should be constant, $= \pm 1$. If $g(X, j) = -1$, then $\Phi_m(j, j) = -\Phi_m(j, j)$, and hence j is a root of $\Phi_m(X) \in \mathbb{Z}[j]$; but this is impossible, since we know $\Phi_m(X)$ to be irreducible over $\mathbb{Q}(j)$.
Lastly, assume that m is not a square, so that if $\sigma = \left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$ is a primitive element and $ad = m$, then $a \neq d$. We have the q-expansion

$$j - j \circ \sigma = \frac{1}{q} + \cdots - \frac{1}{\zeta_d^b q^{\frac{a}{d}}} - \ldots.$$

Since $a \neq d$, there is no cancellation in the fractional summand, and the leading coefficient of this q-expansion is a root of unity.
We know that $\Phi_m(j, j) \in \mathbb{Z}[j]$; taking the product of the $j - j \circ \sigma_i$, we see that the q-expansion for $\Phi_m(j, j)$ starts with $\frac{c_n}{q^n}$ for a certain integer n (the maximal degree of the polynomial), where $c_n = \pm 1$, because it has to be an integer but also a root of unity. Hence $\Phi_m(j, j) = c_m j^m + \ldots$ is a polynomial in j with leading coefficient $c_n = \pm 1$, as was to be shown. □

As we have seen, the properties of the modular polynomial are straightforward consequences of the properties of the j-function, which makes the modular polynomial seem a reasonable object to deal with. This is true only on an abstract level, but if one asks for concrete examples the situation gets surprisingly complicated; in particular, the point is that we find ourselves to deal with polynomials that, though nicely shaped, turn out to have very big coefficients. Here we give some examples:

$$\begin{aligned} l = 2 : {} & X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 + 40773375XY + \\ & + 8748000000X + Y^3 - 162000Y^2 + 8748000000Y - \\ & - 157464000000000; \end{aligned}$$

$$
\begin{aligned}
l = 3 : {} & X^4 - X^3Y^3 + 2232X^3Y^2 - 1069956X^3Y + 36864000X^3 + \\
& + 2232X^2Y^3 + 2587918086X^2Y^2 + 8900222976000X^2Y + \\
& + 452984832000000X^2 - 1069956XY^3 + 8900222976000XY^2 - \\
& - 770845966336000000XY + 1855425871872000000000X + Y^4 + \\
& + 36864000Y^3 + 452984832000000Y^2 + \\
& + 18554258718720000000000Y;
\end{aligned}
$$

$$
\begin{aligned}
l = 5 : {} & X^6 - X^5Y^5 + 3720X^5Y^4 - 4550940X^5Y^3 + 2028551200X^5Y^2 - \\
& - 246683410950X^5Y + 1963211489280X^5 + 3720X^4Y^5 + \\
& + 1665999364600X^4Y^4 + 107878928185336800X^4Y^3 + \\
& + 383083609779811215375X^4Y^2 + \\
& + 1285417989068288163840000X^4Y + \\
& + 1284733132841424456253440X^4 - 4550940X^3Y^5 + \\
& + 107878928185336800X^3Y^4 - \\
& - 4412069655129148352461000X^3Y^3 + \\
& + 2689848885838073157741772800 0X^3Y^2 - \\
& - 1924579346189282996551082311680000X^3Y + \\
& + 2802447778284395278043215652978688 00X^3 + \\
& + 2028551200X^2Y^5 + 383083609779811215375X^2Y^4 + \\
& + 2689848885838073157741772800 0X^2Y^3 + \\
& + 5110941777552418083110765199360000X^2Y^2 + \\
& + 3655473658394962929570647233265664 0000X^2Y + \\
& + 6692500042627997708487149415015068467200X^2 - \\
& - 246683410950XY^5 + 1285417989068288163840000XY^4 - \\
& - 1924579346189282996551082311680000XY^3 + \\
& + 3655473658394962929570647233265664 0000XY^2 - \\
& - 2640734570766205962597157902479787829493 76XY + \\
& + 5327433080342442545042016027335650915123 2000X + Y^6 + \\
& + 1963211489280Y^5 + 1284733132841424456253440Y^4 + \\
& + 2802447778284395278043215652978688 00Y^3 + \\
& + 6692500042627997708487149415015068467200Y^2 + \\
& + 5327433080342442545042016027335650915123 2000Y + \\
& + 1413599471547213586977534746910713627510046720 00.
\end{aligned}
$$

As we see, they are not very handle to deal with; by increasing the degree,

we increase the size of the coefficients as well, and they grow dramatically fast. We have bounds limiting the size of coefficients; if we set h to be the (logarithmic) **height** of a given polynomial as the logarithm of the maximum of the absolute value of its coefficients, R. Bröker and A. Sutherland proved in 2010 ([BS10]) that for any integer $m \geq 1$ we have

$$h(\Phi_m) \leq 6m\log(m) + 16m + 14\sqrt{m}\log(m); \tag{2.6}$$

in practice, we may use the more convenient bound

$$h(\Phi_m) \leq 6m\log(m) + 18m.$$

(the same article provides also a table for values of $h(\Phi_m)$ for $m \leq 3307$). This justifies our assertion about coefficients growing with the level of the modular polynomial we have. The difficulties in handling such big coefficients motivate to think about different approaches to the problem: the strategy could be looking for new tools that would allow us to carry the same kind of analysis we could do by means of modular polynomials. But in fact, what are these modular polynomial important for? We will explain it in the next section.

2.3 Relations with isogenies

In this section, we want to understand the modular polynomials in term of j-invariants of lattices. The basic idea is that if L is a lattice, then the roots of $\Phi_m(X, j(L)) = 0$ are given by the j-invariants of particular sublattices, namely those $L' \subset L$ which are sublattices of index m in L, with $[L : L'] = m$ and such that the quotient $\frac{L}{L'}$ is a cyclic group. We call those L' **cyclic sublattices** of index m. Our aim is to prove the following:

Theorem 2.3.1. *Let m be a positive integer. If $u, v \in \mathbb{C}$, then $\Phi_m(u, v) = 0$ if and only if there is a lattice L and a cyclic sublattice $L' \subset L$ of index m such that $u = j(L')$ and $v = j(L)$.*

Before proving it, we are going to study in more detail cyclic sublattices of the lattice $[1, \tau]$, $\tau \in \mathcal{H}$:

Lemma 2.3.2. *Let $\tau \in \mathcal{H}$, and consider the lattice $[1, \tau]$.*

- *Given a cyclic sublattice $L' \subset [1, \tau]$ of index m, there exists a unique $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$ such that $L' = d[1, \sigma\tau]$;*
- *conversely, if we have $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(m)$, then $d[1, \sigma\tau]$ is a cyclic sublattice of $[1, \tau]$ of index m.*

Proof. We know from the previous chapter that a sublattice $L' \in L = [1, \tau]$ can be written $L' = [a\tau + b, c\tau + d]$ and we know that $[L : L'] = |ad - bc| = m$. Furthermore, a very easy argument shows that

$$\frac{L}{L'} \text{ is cyclic } \Leftrightarrow \gcd(a, b, c, d) = 1. \tag{2.7}$$

In fact, we see immediately that a necessary condition for $\frac{L}{L'}$ to be cyclic is $\gcd(a, b, c, d) = 1$; now suppose $\gcd(a, b, c, d) = 1$.
By the elementary divisor Theorem, we know that we can find bases $\{\omega_1, \omega_2\}$ for L and $\{\omega_1', \omega_2'\}$ for L' such that $\omega_1' = e_1\omega_1$ and $\omega_2' = e_2\omega_2$, $e_1 | e_2$. Since $\gcd(a, b, c, d) = 1$, we are forced to set $e_1 = 1$, so $\frac{L}{L'}\langle\omega_2\rangle$ is cyclic.
Now suppose that $L' \subset [1, \tau]$ is cyclic of index m. If d is the smallest positive integer contained in L', then it follows easily that L' is of the form $L' = [d, a\tau + b]$ for some integers a and b. We may assume that $a > 0$, and then $ad = m$. However, if k is any integer, then

$$L' = [d, (a\tau + b) + kd] = [d, a\tau + (b + kd)];$$

this means that, if we choose k in a proper way, we can assume $0 \leq b < d$. We also know by (2.7) that $\gcd(a, b, d) = 1$, thus the matrix $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ lies in $C(m)$. Then $L' = [d, a\tau + b] = d[1, \frac{a\tau+b}{d}] = d[1, \sigma\tau]$, showing that L' has the desired form. These computations also show that $\sigma \in C(m)$ is uniquely determined by L', thus we proved the first point.
The proof of the second one follows immediately from (2.7), and we are done. □

We can now prove Theorem 2.3.1:

Proof of the theorem: We know from the lemma that the j-invariants of cyclic sublattices L' of $[1, \tau]$ of index m are given by

$$j(L') = j(d[1, \sigma\tau]) = j([1, \sigma\tau]) = j(\sigma\tau).$$

By 2.4, it follows that the roots of $\Phi_m(X, j(\tau))$ are exactly the j-invariants of the cyclic sublattices of index m of $[1, \tau]$. We conclude then thanks to the surjectivity of the j function. □

What is the advantage of this point of view? We know that the function j itself parametrises isomorphism classes of elliptic curves; for any possible $\Gamma^0(\ell)$, the correspondent modular polynomial parametrises isomorphism classes of elliptic curves together with an isogeny of degree ℓ.
The real point of interest of this application is that the theorem still holds true when considering curves defined over finite fields.

Consider for example E, E' defined over $\bar{\mathbb{F}}_q$ of characteristic p, with invariants j_E, $j_{E'}$ respectively; moreover, we denote by $\bar{\Phi_m}$ the reduction modulo q of a generic classical modular polynomial. If we take $\ell \in \mathbb{N}$, coprime with p and such that $\bar{\Phi}_\ell(j_E, j_{E'}) = 0$, then there exist an isogeny of degree ℓ mapping E to E'.
If we descend over $\mathbb{F}_q$, the situation is more delicate. Given two curves E, E' defined over $\mathbb{F}_q$ such that $\bar{\Phi}_\ell(j_E, j_{E'}) = 0$, with $(\ell, p) = 1$ as above, they are not necessarily isomorphic; in fact, we have the following result:[1]

Proposition 2.3.3. *Let E, E' be two ordinary elliptic curves defined over $\mathbb{F}_q$, $q = p^r$, such that $j_E \neq 0, 1728$. If $\ell \in \mathbb{N}$ is such that $(\ell, p) = 1$ and $\bar{\Phi}_\ell(j_E, j_{E'}) = 0$, then there exists a degree ℓ rational isogeny $E \to \tilde{E}'$, where $\tilde{E}'$ is a twist of E'.*

Essentially, this proposition presents two different kinds of problems. One sees immediately, in fact, that the hypothesis of the curve not being supersingular and the j invariant not being equal to 0 or 1728 is essential; as soon as we try to weaken the hypothesis, we find counterexamples (see [Sch95]).
Moreover, we have a priori no difference between the existence of an isogeny landing on a curve or on its twist in terms of roots of the modular polynomial. So, once the roots are computed, we need some way to detect what is the target of the isogeny they define; a way for doing it is very well explained in [Ler97].
In any case, we see that it is only over $\mathbb{C}$ that we have the clear situation we described above.

2.4 Other modular polynomials

From Lemma 2.1.3, we know that for any modular function f we can find a rational function $F(X) \in \mathbb{C}(X)$ such that for any $\tau \in \mathcal{H}$ we have

$$f(\tau) = F(j(\tau))$$

(this comes really from the second point of the Lemma, it is enough to treat denominator and numerator separately and we get a polynomial as numerator and a polynomial as denominator, so a rational function). Here we show a result which allows us to generalise all the discussion we did up to now:

Proposition 2.4.1. *Let Γ' be a finite index subgroup of Γ and f a modular function for Γ'. Then there exists a polynomial $P(X, Y) \in \mathbb{C}[X, Y]$ of degree*

[1] For a proof of all these assertions, see [Sch95] and [Sil09].

$[\Gamma : \Gamma']$ *in* X *such that, for all* $\tau \in \mathcal{H}$,

$$P(f(\tau), j(\tau)) = 0.$$

Proof. Let Γ' be a subgroup of Γ of finite index n, and let $\{\gamma_i\}_{i\in\{1,\dots n\}}$ be a set of representatives of the cosets of ${}_{\Gamma'}\backslash^{\Gamma}$. We consider f a modular function for Γ', and the functions $(c_j)_{j\in\{0,\dots,n-1\}} : \mathcal{H} \to \mathbb{C}$ defined by writing $\prod_{j\in\{1,\dots,n\}}(X - f(\gamma_j\tau)) = X^n + \sum_{j=0}^{n-1} c_j(\tau)X^j$, for every $\tau \in \mathcal{H}$. These functions are symmetric with respect to the map $\tau \mapsto f(\gamma_j(\tau))$, and since f is a modular function for Γ' and we chose γ_j as representatives of the cosets for ${}_{\Gamma'}\backslash^{\Gamma}$, the functions c_j are invariant under the action of Γ; moreover, they are meromorphic on $\mathcal{H}$ and at ∞, so they are modular functions for Γ. As an immediate consequence of Lemma 2.1.3, there exist some rational functions $(F_j)_{j\in\{0,\dots,n-1\}}$ such that, for any $\tau \in \mathcal{H}$, $c_j(\tau) = F_j(j(\tau))$; from this we deduce the desired result. □

We can now extend the definition of modular polynomial:

Definition 2.4.2. *Let* Γ_x *and* Γ_y *be subgroups of finite index for* Γ*, and* f_x*,* f_y *be modular functions respectively for* Γ_x*,* Γ_y*. We call* ***modular polynomial*** *the irreducible polynomial* $\Phi_{f_x,f_y}(X, Y) \in \mathbb{C}[X, Y]$ *the non zero polynomial such that, for any* $\tau \in \mathcal{H}$*,* $\Phi(f_x(\tau), f_y(\tau)) = 0$*.*

Remark: We know that such a polynomial exists in case $f_x = j$, or $f_y = j$ (it is the content of Lemma 2.1.3). To show the existence in the general case, it is enough to consider the resultant of two such polynomials to make j vanish.

A modular polynomial is then nothing else than an algebraic relation between two generic modular functions.
We saw that the principal inconvenient about working with classical modular polynomials lies in the size of their coefficients, which a priori can grow really fast. The idea of looking for modular polynomials different from the classical one is not a new one; in [Ler97], we can find a brief presentation of the main ideas that have been developed in this direction. All the different polynomials presented there have smaller coefficients, and carry with them the same kind of information about isogenies, even if their construction is done by means of functions that could be more complicated than the j invariant.
Now, one could ask oneself how to generalise this framework to a higher genus situation. Of course we have classical invariants characterising surfaces built by means of a quotient by a lattice, and we can build polynomials by means

of them; the point is that, if we had some size problems in genus 1, the situation precipitates dramatically already in genus 2 (see [Dup06] to have an idea of the situation). We need in this case to think about a function that could be easily generalised to higher genus (which is not the case for all the functions built starting explicitly for j, as for example η, see [Dup06]). This is the case of ϑ functions: in the following chapter, we will introduce them in genus 1, and we will see how to use them to build modular polynomials; then, we will try to discuss as an example the case of genus 2, and we will see that again using ϑ functions we can still hope to find some polynomials which should be better than the classical ones.

Chapter 3

Theta functions

In this chapter we introduce the function $\vartheta(z,\tau)$ that enables us to define some invariants linked to each elliptic curve different from the j-invariant we already presented.

3.1 Definitions and basic properties

Definition 3.1.1. *We define the* ***theta function*** *as the analytic function in two variables defined by*

$$\vartheta(z,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi\imath n^2\tau + 2\pi\imath nz}$$

where $z \in \mathbb{C}$ *and* $\tau \in \mathcal{H}$.

The series converges absolutely and uniformly on every compact set; in fact, if $|\operatorname{Im}(z)| < c$ and $\operatorname{Im}(\tau) > \epsilon$, then $|e^{\pi\imath n^2\tau+2\pi\imath nz}| < (e^{-\pi\epsilon})^{n^2}(e^{2\pi c})^n$. Hence, if n_0 is chosen so that $(e^{-\pi\epsilon})^{n_0}(e^{2\pi c}) < 1$, then the inequality

$$|e^{\pi\imath n^2\tau+2\pi\imath nz}| < (e^{-\pi\epsilon})^{n(n-n_0)}$$

shows that the series converges, and in fact that it converges very rapidly. We may think about this series as the Fourier series for a function in z, periodic with respect to the transformation $z \mapsto z+1$:

$$\vartheta(z,\tau) = \sum_{n\in\mathbb{Z}} a_n(\tau)e^{2\pi\imath nz},\ a_n(\tau) = e^{\pi\imath n^2\tau}$$

which highlights the fact that $\vartheta(z+1,\tau) = \vartheta(z,\tau)$.

Moreover, we can remark a peculiar behaviour of ϑ with respect to $z \mapsto z+\tau$; we have:

$$\vartheta(z+\tau,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi\imath n^2\tau + 2\pi\imath n(z+\tau)} =$$

$$= \sum_{n\in\mathbb{Z}} e^{\pi\imath(n+1)^2\tau - \pi\imath\tau + 2\pi\imath nz} = \sum_{m=n+1\in\mathbb{Z}} e^{\pi\imath m^2\tau - \pi\imath\tau + 2\pi\imath mz - 2\pi\imath z} = e^{-\pi\imath\tau - 2\pi\imath z}\vartheta(z,\tau).$$

We can say that ϑ has a kind of periodic behaviour with respect to the lattice $L_\tau \subset \mathbb{C}$ generated by 1 and τ. If we put the two periodicities together we get

$$\vartheta(z+a\tau+b,\tau) = e^{-\pi\imath a^2\tau - 2\pi\imath az}\vartheta(z,\tau).$$

We will show that this function is in fact the simplest possible having this behaviour. Suppose we are looking for entire functions $f(z)$ with the simplest possible quasi-periodic behaviour with respect to L_τ; we know by Liouville's Theorem that f cannot actually be periodic both in 1 and in τ, so we may try the simplest more general possibilities:

$$f(z+1) = f(z) \text{ and } f(z+\tau) = e^{az+b}f(z). \tag{3.1}$$

From the first periodicity, we can write f as a Fourier series:

$$f(z) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi\imath nz},$$

$a_n \in \mathbb{C}$. By combinining the preceding functional equations, we get

$$f(z+\tau+1) = f(z+\tau) = e^{az+b}f(z),$$

and

$$f(z+\tau+1) = e^{a(z+1)+b}f(z+1) = e^a e^{az+b}f(z),$$

hence $a = 2\pi\imath k$ for some $k \in \mathbb{Z}$. Now, substituting the Fourier series into the second equation of (3.1), we find that

$$\sum_{n\in\mathbb{Z}} a_n e^{2\pi\imath n\tau} e^{2\pi\imath nz} = f(z+\tau) = e^{2\pi\imath kz+b}f(z) =$$

$$= \sum_{n\in\mathbb{Z}} a_n e^{2\pi\imath(n+k)z} e^b = \sum_{n\in\mathbb{Z}} a_{n-k} e^b e^{2\pi\imath nz}.$$

So, we can also express the Fourier coefficients as

$$a_n = a_{n-k} e^{b-2\pi\imath n\tau} \tag{3.2}$$

for all $n \in \mathbb{Z}$. By setting $k = 0$, we get the trivial possibility $f(z) = e^{2\pi\imath z}$; for $k \neq 0$, we get a recursive formula for expressing a_{n+kp} in terms of a_n for all $p \in \mathbb{Z}$. For instance, if $k = -1$, we find easily that $a_n = a_0 e^{-nb+\pi\imath n(n-1)\tau}$ for all $n \in \mathbb{Z}$.
This means that

$$f(z) = a_0 \sum_{n\in\mathbb{Z}} e^{-nb-\pi\imath n\tau} e^{\pi\imath n^2\tau+2\pi\imath nz} = a_0\vartheta(-z - \frac{1}{2}\tau - \frac{b}{2}\pi\imath, \tau).$$

If $k > 0$, the recursive relation 3.2 leads to rapidly growing coefficients a_n and hence to no entire functions $f(z)$. On the other hand, if $k < -1$, we will find a $|k|$-dimensional vector space of possibilities for f, depending essentially on b, that is studied in detail below.
Now we are going to introduce the **theta functions with characteristic**, which play a very important role in the application of ϑ to the study of elliptic curves. To better explain this, we are going to reintroduce elements and groups we already know, and we will see how they act not on elliptic curves, but on theta functions. We will actually see that the actions are compatible and this allow us to make very useful observations about elements which are invariant under these actions.
Let us fix τ and introduce the transformations as follows: for every holomorphic function $f(z)$ and a, $b \in \mathbb{C}$ let

$$S_b f(z) = f(z + b),\ T_a f(z) = e^{\pi\imath a^2\tau+2\pi\imath az} f(z + a\tau).$$

Note then that

$$S_{b_1}(S_{b_2})f = S_{b_1+b_2}f \text{ and } T_{a_1}(T_{a_2}f) = T_{a_1+a_2}f$$

These are called the **one-parameter groups**. They do not commute, but we can find an easy relation between them; namely, we have

$$S_b(T_a f)(z) = T_a(f)(z + b) = e^{\pi\imath a^2\tau+2\pi\imath a(z+b)} f(z + b + a\tau),$$

and

$$T_a(S_b f)(z) = e^{\pi\imath a^2\tau+2\pi\imath az} S_b f(z + a\tau) = e^{\pi\imath a^2\tau+2\pi\imath az} f(z + a\tau + b),$$

hence

$$S_b \circ T_a = e^{2\pi\imath ab} T_a \circ S_b.$$

The group of transformations generated by the T_a and the S_b is the 3-dimensional group

$$\mathcal{G} = \mathbb{C}_1^* \times \mathbb{C} \times \mathbb{C},$$

with the convention $\mathbb{C}_1^* = \{z \in \mathbb{C} : |z| = 1\}$; the element $(\lambda, a, b) \in \mathcal{G}$ stands for the transformation

$$U_{(\lambda,a,b)} f(z) = \lambda(T_a \circ S_b) f(z) = \lambda e^{\pi \imath a^2 \tau + 2\pi \imath a z} f(z + a\tau + b).$$

We see immediately that with this notation, for any $a, b \in \mathbb{R}$, we identify T_a with $(1, a, 0)$ and S_b with $(1, 0, b) \in \mathcal{G}$.
The group law on $\mathcal{G}$ is given by

$$(\lambda, a, b)(\lambda', a', b') = (\lambda\lambda' e^{2\pi \imath b a'}, a + a', b + b').$$

We note that the subset

$$\Gamma = \{(1, a, b) \in \mathcal{G} : a, b \in \mathbb{Z}\}$$

is a subgroup of $\mathcal{G}$. Our characterisation immediately shows that ϑ is the unique entire function invariant under the action of Γ. Suppose now that l is a positive integer; set $l\Gamma = \{(1, la, lb)\} \subseteq \Gamma$ and

$$V_l = \{\text{entire functions invariant under } l\Gamma\}.$$

Then we have the following:

Lemma 3.1.2. *An entire function $f(z)$ is in V_l if and only if*

$$f(z) = \sum_{n \in \frac{1}{l}\mathbb{Z}} c_n e^{\pi \imath n^2 \tau + 2\pi \imath n z}$$

such that $c_n = c_m$ if $n - m \in l\mathbb{Z}$. In particular, $\dim(V_l) = l^2$.

Proof. If $f \in V_l$, then by invariance of f under $S_l \in l\Gamma$ it follows that

$$f(z) = \sum_{n \in \frac{1}{l}\mathbb{Z}} c'_n e^{2\pi \imath n z}.$$

On the other hand, if we write the coefficients as $c'_n = c_n e^{\pi \imath n^2 \tau}$ and we impose the invariance of $f(z)$ under T_l, a short computation shows that $c_{n+l} = c_n$ for all $n \in \mathbb{Z}$, as required.
The converse is obvious: if $c_n = c_m$ any time that $n - m \in l\mathbb{Z}$, then the action of $l\Gamma$ on f, which does nothing different than a translating any coefficient of l positions, sends any coefficient on another which is equal; so f is obviously invariant under this action. □

For $m \in \mathbb{N}$, let $\boldsymbol{\mu}_m \subseteq \mathbb{C}_1^*$ be the group of m-th roots of unity. For $l \in \mathbb{N}$, let $\mathcal{G}_l$ be the finite group defined as

$$\mathcal{G}_l = \left\{ (\lambda, a, b) : \lambda \in \boldsymbol{\mu}_{l^2}, a, b \in \frac{1}{l}\mathbb{Z} \right\} (\text{mod } l\Gamma) = \mu_{l^2} \times \frac{\frac{1}{l}\mathbb{Z}}{l\mathbb{Z}} \times \frac{\frac{1}{l}\mathbb{Z}}{l\mathbb{Z}}$$

with group law given by $(\lambda, a, b)(\lambda', a', b') = (\lambda\lambda' e^{2\pi\imath ba'}, a + a', b + b')$. Now the elements $S_{\frac{1}{l}}, T_{\frac{1}{l}} \in \mathcal{G}$ commute with $l\Gamma$ because of (3.2) and hence act on V_l. This induces an action of $\mathcal{G}_l$ on V_l; in fact, the generators of $\mathcal{G}_l$ act on V_l as follows:

$$S_{\frac{1}{l}}(\sum_{n\in\frac{1}{l}\mathbb{Z}} c_n e^{\pi\imath n^2\tau+2\pi\imath nz}) = \sum_{n\in\frac{1}{l}\mathbb{Z}} c_n e^{2\pi\imath\frac{n}{l}} e^{\pi\imath n^2\tau+2\pi\imath nz},$$

$$T_{\frac{1}{l}}(\sum_{n\in\frac{1}{l}\mathbb{Z}} c_n e^{\pi\imath n^2\tau+2\pi\imath nz}) = \sum_{n\in\frac{1}{l}\mathbb{Z}} c_{n-\frac{1}{l}} e^{\pi\imath n^2\tau+2\pi\imath nz}.$$

This gives us the following:

Lemma 3.1.3. *The finite group $\mathcal{G}_l$ acts irreducibly on V_l.*

Proof. Let $W \subseteq V_l$ be a $\mathcal{G}_l$-stable subspace. Take a non-zero element $f \in W$, say $f(z) = \sum_{n\in\frac{1}{l}\mathbb{Z}} c_n e^{\pi\imath n^2\tau+2\pi\imath nz}$, $c_{n_0} \neq 0$; operating by powers of $S_{\frac{1}{l}}$ on $f(z)$, we find in W:

$$\sum_{0\le p\le l^2-1} e^{-2\pi\imath n_0\frac{p}{l}}(S_{\frac{p}{l}}f)(z) =$$

$$= \sum_{n\in\frac{1}{l}\mathbb{Z}} c_n(\sum_p e^{2\pi\imath(n-n_0)\frac{p}{l}} e^{\pi\imath n^2\tau+2\pi\imath nz}) = l^2 c_{n_0}(\sum_{n\in n_0+l\mathbb{Z}} e^{\pi\imath n^2\tau+2\pi\imath nz}).$$

Since $c_{n_0} \neq 0$, we see that W contains the function $\sum_{n\in n_0+l\mathbb{Z}} e^{\pi\imath n^2\tau+2\pi\imath nz}$. Now, working with $T_{\frac{1}{l}}$ and doing a similar procedure, we find that W contains similar functions for every $n_0 \in \frac{\frac{1}{l}\mathbb{Z}}{l\mathbb{Z}}$; hence, $W = V_l$. □

So, thanks to the irreducibility, the action of $\mathcal{G}_l$ on V_l determines, up to a constant, a canonical basis for V_l (which, from all the previous considerations, is clear to have dimansion l^2).[1] The standard basis for V_l is given by the **theta functions with rational characteristic** $\vartheta_{a,b}$:

[1] Usually, to specify a basis in this way we will need to specify the element we start from and consider all the elements we get letting $\mathcal{G}$ act on it; depending from the element we start with, we may obtain different representations.

The point here is that the group $\mathcal{G}$ is a very well-known and well-studied group, called the **Heisenberg group**, which is known to have a single irreducible representation. In this specific case, the choice of the initial element does not affect the basis we obtain making the element of the group act on it; the basis that we obtain will be always the same, up to a constant.

Definition 3.1.4. *Take $a,\ b \in \frac{1}{l}\mathbb{Z}$; then the* ***theta function with rational characteristic*** (a,b) *is* $\vartheta_{a,b} = S_b T_a \vartheta = e^{2\pi\imath ab} T_a S_b \vartheta$, *that is*

$$\vartheta_{a,b}(z,\tau) = e^{\pi\imath a^2\tau + 2\pi\imath a(z+b)}\vartheta(z + a\tau + b, \tau) =$$

$$= \sum_{n\in\mathbb{Z}} e^{\pi\imath(a^2+n^2)\tau + 2\pi\imath n(z+a\tau+b) + 2\pi\imath a(z+b)} = \sum_{n\in\mathbb{Z}} e^{\pi\imath(a+n)^2\tau + 2\pi\imath(n+a)(z+b)}.$$

These functions, when considered as a basis for V_l, are also called ***theta constants****.*

Straightforward properties of this definition are:

1. $\vartheta_{0,0} = \vartheta$;
2. $S_{b_1}(\vartheta_{a,b}) = \vartheta_{a,b+b_1}$ for $a, b, b_1 \in \frac{1}{l}\mathbb{Z}$;
3. $T_{a_1}(\vartheta_{a,b}) = e^{-2\pi\imath a_1 b}\vartheta_{a_1+a,b}$, $\forall a, a_1, b \in \mathbb{Z}$;
4. $\vartheta_{a+p,b+q} = e^{2\pi\imath aq}\vartheta_{a,b}$, $\forall p, q \in \mathbb{Z}$, $a, b \in \frac{1}{l}\mathbb{Z}$.

From 4, we have that $\vartheta_{a,b}$, up to a constant, depends only on $a, b \in \frac{\frac{1}{l}\mathbb{Z}}{\mathbb{Z}}$. Moreover, from Lemma 3.1.2 and from the Fourier expansion given for $\vartheta_{a,b}$, it is clear that as a, b run through coset representatives of $\frac{\frac{1}{l}\mathbb{Z}}{\mathbb{Z}}$, we get a basis of V_l.
We notice that in fact $\vartheta_{a,b}$ is just a translate of ϑ, except for a trivial exponential factor.
Relations between ϑ constants for a fixed τ depending on the values of z have been an important object of study. This quest has produced a lot of formulae, as for example addition and multiplication formulae and other general formulae which are known under the name of Riemann Theta formulae (see [Mum83, page 14]); these are relations exploiting the symmetry in the expressions of the different ϑ constants.
We focus now on the case $l = 2$; in this case, we have just four elements generating our space V_2. To simplify notations, we are going to call them ϑ_{00}, $\vartheta_{01} = \vartheta_{0,\frac{1}{2}}$, $\vartheta_{10} = \vartheta_{\frac{1}{2},0}$, $\vartheta_{11} = \vartheta_{\frac{1}{2},\frac{1}{2}}$, and to consider them just as functions of z, keeping τ fixed. Here we display the results of the formulae mentioned above; notably these are formulae linking ϑ computed in $z = 0$ and in a generic z, for a fixed value of τ:

$$\vartheta_{00}(z)^2\vartheta_{00}(0)^2 = \vartheta_{01}(z)^2\vartheta_{01}(0)^2 + \vartheta_{10}(z)^2\vartheta_{10}(0)^2; \tag{3.3}$$

$$\vartheta_{11}(z)^2\vartheta_{00}(0)^2 = \vartheta_{01}(z)^2\vartheta_{10}(0)^2 - \vartheta_{10}(z)^2\vartheta_{01}(0)^2. \tag{3.4}$$

In particular, if we specify the first one for the value $z = 0$, we get the so-called **Jacobi identity**:

$$\vartheta_{00}(0)^4 = \vartheta_{01}(0)^4 + \vartheta_{10}(0)^4. \tag{3.5}$$

3.2 Embeddings by theta functions

We are going here to see the geometric applications of the theta functions we introduced above.
Take any $l \geq 2$. Let E_τ be the complex torus $\frac{\mathbb{C}}{L_\tau}$, where $L_\tau = \mathbb{Z} + \mathbb{Z}\tau$, and let (a_i, b_i), $0 \leq i < l^2$ be a set of coset representatives for $(\frac{\frac{1}{l}\mathbb{Z}}{\mathbb{Z}})^2$ in $(\frac{1}{l}\mathbb{Z})^2$. Write $\vartheta_i = \vartheta_{a_i,b_i}$.
For all $z \in \mathbb{C}$, consider the l^2-tuple $(\vartheta_0(lz,\tau), \dots, \vartheta_{l^2-1}(lz,\tau))$ modulo scalars, id est the homogeneous coordinates of a point in the projective space $\mathbb{P}^{l^2-1}(\mathbb{C})$ (we should check, and we will do it soon, that there is no z, τ for which all the coordinates are 0).
Since

$$(\vartheta_0(z+l,\tau), \dots, \vartheta_{l^2-1}(z+l,\tau)) = (\vartheta_0(z,\tau), \dots, \vartheta_{l^2-1}(z,\tau))$$

and

$$(\vartheta_0(z+l\tau,\tau), \dots, \vartheta_{l^2-1}(z+l\tau,\tau)) = \lambda(\vartheta_0(z,\tau,\dots, \vartheta_{l^2-1}(z,\tau))$$

where $\lambda = e^{-\pi i l^2 \tau - 2\pi i l z}$, it follows that

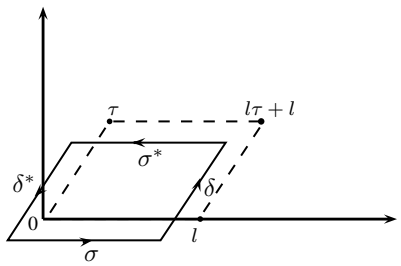
$$\begin{array}{rccc} \phi_l : & E_\tau & \to & \mathbb{P}^{l^2-1} \\ & z & \mapsto & [\cdots : \vartheta_i(lz,\tau) : \dots] \end{array} \tag{3.6}$$

defines a holomorphic map. To better study it, we prove the following

Lemma 3.2.1. *Every $f \in V_l$, $f \neq 0$ has exactly l^2 zeros (counted with multiplicities) in a fundamental domain for $\frac{\mathbb{C}}{lL_\tau}$; the zeros of $\vartheta_{a,b}$ are the points $(a+p+\frac{1}{2})\tau + (b+q+\frac{1}{2})$, $p, q, \in \mathbb{Z}$.*

Remark: This means, in particular, that ϕ_l is well defined, as ϑ_i, ϑ_j have no common zeros for $i \neq j$.

Proof. The first part comes from the argument principle, in a very standard way. We choose a parallelogram built on the fundamental parallelogram of the lattice lL_τ, and we translate it in order not to have zeros of f on the border, for any $f \in V_l$; let it be $P = \sigma + \delta + \sigma^* + \delta^*$, where σ, σ^* run parallel to the x axis, and δ, δ^* are parallel to the vector $l\tau$ (see the graphic below).



From the argument principle and the fact of f being without poles we have

$$\text{card}\,\{\text{zeros of } f\} = \frac{1}{2\pi\imath}\int_{\sigma+\delta+\sigma^*+\delta^*}\frac{f'}{f}dz.$$

Since $f(z+l) = f(z)$ and $f(z+l\tau) = ke^{-2\pi\imath lz}f(z)$ where k is a constant term, we get that

$$\int_\delta + \int_{\delta^*} = 0 \text{ and } \int_\sigma + \int_{\sigma^*} = 2\pi\imath l^2.$$

To compute exactly the zeros in the case of ϑ constants, we notice that $\vartheta(z,\tau)$ is even and it has a single zero in $\frac{\mathbb{C}}{L_\tau}$; when looking at ϑ constants, so at translated of ϑ, we have:[2]

$$\vartheta_{\frac{1}{2},\frac{1}{2}}(-z,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi\imath(n+\frac{1}{2})^2\tau+2\pi\imath(n+\frac{1}{2})(-z+\frac{1}{2})} =$$

$$= \sum_{m=-1-n\in\mathbb{Z}} e^{\pi\imath(-m-\frac{1}{2})^2\tau+2\pi\imath(-m-\frac{1}{2})(-z+\frac{1}{2})} =$$

$$= \sum_{m\in\mathbb{Z}} e^{\pi\imath(m+\frac{1}{2})^2\tau+2\pi\imath(m+\frac{1}{2})(z+\frac{1}{2})-2\pi\imath(m+\frac{1}{2})} = -\vartheta_{\frac{1}{2},\frac{1}{2}}(z,\tau),$$

hence $\vartheta_{\frac{1}{2},\frac{1}{2}}$ is zero at $z=0$.
A direct computations for all the values stated above tells us that they are all zeros for the correspondent ϑ constants, and they are distinct modulo $\frac{\frac{1}{l}\mathbb{Z}}{\mathbb{Z}}$; they are exactly l^2 in each case, and from the discussion above we know that they can not be more. □

Next, we observe that the group $\mathcal{G}_l$ modulo its center, that is the group $(\frac{\frac{1}{l}\mathbb{Z}}{\mathbb{Z}})^2$ naturally acts on both E_τ and $\mathbb{P}^{l^2-1}$, and the map ϕ_l is equivariant. To see this, we let $a,b \in (\frac{1}{l}\mathbb{Z})^2$; this element acts on E_τ by

$$z \mapsto z + \frac{a\tau+b}{l},$$

[2]Here we keep the complete notation as we are considering the function in itself, not as element of the basis for the space generated by ϑ constants when $l=2$, as above.

and the action is free.
On the other hand, if $U_{(1,a,b)}\vartheta_i = \sum_{0\leq j\leq l^2-1} c_{ij}\vartheta_j$, the action on $\mathbb{P}^{l^2-1}$ is given by

$$[z_0 : \cdots : z_{l^2-1}] \mapsto [\sum_j c_{0,j}z_j : \cdots : \sum_j c_{l^2-1,j}z_j].$$

Now we see that

$$\phi_l\left(z + \frac{a\tau+b}{l}\right) = [\cdots : \vartheta_i(lz + a\tau + b, \tau) : \dots] =$$

$$= [\cdots : U_{(1,a,b)}\vartheta_i(lz,\tau) : \dots] = [\cdots : \sum_j c_{i,j}\vartheta_j(lz,\tau) : \dots]$$

so the group action is preserved and ϕ_l is equivariant.
We prove now that ϕ_l is an embedding; suppose we have $\phi_l(z_1) = \phi_l(z_2)$, $z_1 \neq z_2$ in E_τ, or that $\mathrm{d}\phi_l(z_1) = 0$ (the limit case, when $z_2 \to z_1$). Translating by some $\frac{a\tau+b}{l}$, $a, b \in \frac{1}{l}\mathbb{Z}$, we find a second pair z_1', z_2' such that $\phi_l(z_1') = \phi_l(z_2')$, or $\mathrm{d}\phi_l(z_1') = 0$.
We choose $l^2 - 3$ further points $w_1, \dots, w_{l^2-3}$ such that all our points are distinct modulo lL_τ. Now, we can find an $f \in V_l$, $f \neq 0$ such that

$$f(z_1) = f(z_1') = f(w_1) = \cdots = f(w_{l^2-3}) = 0;$$

this is possible because, writing $f = \sum \lambda_i\vartheta_i$, $\lambda_i \in \mathbb{C}$, we get $l^2 - 1$ linear equations in the l^2 variables $\lambda_0, \dots, \lambda_{l^2-1}$ and so they have a non-zero solution. Since $\phi_l(z_1) = \phi_l(z_2)$, it follows that $f(z_2) = 0$ or, if $\mathrm{d}\phi_l(z_1) = 0$, f has a double zero at z_1.
Similarly, we get that $f(z_2') = 0$ or f has a double zero at z_1'. Therefore, f would have at least $l^2 + 1$ zeros in $\frac{\mathbb{C}}{lL_\tau}$, contradicting Lemma 3.2.1.
Thus $\phi_l(E_\tau)$ is a complex analytic submanifold isomorphic to the torus E_τ; moreover, we have the following result:

Theorem 3.2.2 (Chow)**.** *Every closed projective analytic subspace is an algebraic subspace.*

Proof. See [Ser56]. □

This tells us that $\phi_l(E_\tau)$ is even an algebraic variety, id est it is defined by some homogeneous polynomials; we know already that these polynomials are the polynomials giving the equation of the elliptic curve related to our torus. We can make explicit these considerations considering, as above, the example $l = 2$; in this case, we have that $\phi_2(E_\tau)$ is indeed the curve C in $\mathbb{P}^3$ defined by the equations

$$\begin{cases} \vartheta_{00}(0)^2x_0^2 = \vartheta_{01}(0)^2x_1^2 + \vartheta_{10}(0)^2x_2^2 \\ \vartheta_{00}(0)^2x_3^2 = \vartheta_{10}(0)^2x_1^2 - \vartheta_{01}(0)^2x_2^2 \end{cases} \tag{3.7}$$

By Bézout's Theorem, we know that a generic hyperplane in $\mathbb{P}^3$ meets C in at most four points. The generic hyperplane $\sum a_i x_i = 0$ meets $\phi_2(E_\tau)$ at the points where $a_0\vartheta_{00}(2x) + a_1\vartheta_{01}(2x) + a_2\vartheta_{10}(2x) + a_3\vartheta_{11}(2x) = 0$, and we can find exactly four points on this kind mod $2L_\tau$. These are really the points which satisfy the equations (3.7) by means of (3.3), (3.4). We definitely have that $\phi_2(E_\tau)$ should coincide with C, and this gives explicit formulae linking ϑ constants with elliptic curves.
The case $l = 2$ gives us, from what we saw above, an explicit description of an elliptic curve in terms of ϑ constants. We will see in the remaining part of this chapter how to exploit this description to build convenient modular polynomials, which will profit from the properties of the ϑ functions.

3.3 The functional equation of theta

In the previous sections we focused on the behaviour of $\vartheta(z, \tau)$ as a function of z. It behaves nicely also as a function of τ, but in a more subtle way.
Just as ϑ is periodic up to an elementary factor for a group of transformations acting on z, it is also periodic up to a factor for a group acting on z and τ. In fact, if we consider $\vartheta(z, \tau)$ for a fixed τ, the definition involves the generators 1 and τ of the lattice L_τ quite asymmetrically; still, when considering the application to E_λ this asymmetry disappears.
In other words, if we had picked any two other $a\tau + b$, $c\tau + d$ generating the lattice L_τ, $a, b, c, d \in \mathbb{Z}$, $ad - bc = \pm 1$, we could have constructed different theta functions, which would have been periodic with respect to $z \mapsto z+c\tau+d$ and periodic up to an exponential factor with respect to $z \mapsto z + a\tau + b$, and these theta functions would have been equally useful for the study of E_τ; the different choice for the generators should not make any difference.
If we try to make this point precise, we obtain a relation which is known as the **functional equation for** ϑ in τ.
Fix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, id est $a, b, c, d \in \mathbb{Z}$, $ab - bc = 1$; we determine the sign of this element by setting $c \geq 0$ and we assume that ab, cd are even. Consider the function $\vartheta((c\tau + d)y, \tau)$; clearly, when y is replaced by $y + 1$, the function is unchanged except for an exponential factor.
We want to make this factor explicit and convert the function $\vartheta((c\tau+d)y, \tau)$ to a periodic function $y \mapsto y + 1$. If we set

$$\psi(y, \tau) = e^{\pi\imath c(c\tau+d)y^2}\vartheta((c\tau + d)y, \tau),$$

a simple calculation shows that $\psi(y+1, \tau) = \psi(y, \tau)$ (the fact that cd is even helps in the verification, as a factor $e^{\pi\imath cd}$ comes out). The periodic behaviour of ϑ with respect to $z \mapsto z + \tau$ gives another quasi-period for ψ, namely

$\psi(y+\frac{a\tau+b}{c\tau+d},\tau) = e^{-\pi\imath\frac{a\tau+b}{c\tau+d}-2\pi\imath y}\psi(y,\tau)$. We do some computations in order to show this; formally writing we have by definition

$$\frac{\psi(y+\frac{a\tau+b}{c\tau+d},\tau)}{\vartheta((c\tau+d)y+a\tau+b,\tau)} = e^{\pi\imath c(c\tau+d)y^2+2\pi\imath cy(a\tau+b)+\pi\imath c\frac{(a\tau+b)^2}{c\tau+d}},$$

and

$$\frac{\vartheta((c\tau+d)y+a\tau+b,\tau)}{\psi(y,\tau)} = \frac{e^{-\pi\imath a^2\tau-2\pi\imath ay(c\tau+d)}\vartheta((c\tau+d)y,\tau)}{e^{\pi\imath c(c\tau+d)y^2}\vartheta((c\tau+d)y,\tau)} =$$

$$= e^{-\pi\imath a^2\tau-2\pi\imath ay(c\tau+d)-\pi\imath c(c\tau+d)y^2}.$$

So, multiplying these equations and exploiting the fact $ad-bc=1$, we get

$$\frac{\psi(y+\frac{a\tau+b}{c\tau+d},y)}{\psi(y,\tau)} = e^{-2\pi\imath y(ad-bc)+\pi\imath c\frac{(a\tau+b)^2}{c\tau+d}-\pi\imath a^2\tau} =$$

$$= e^{-2\pi\imath-\frac{\pi\imath y}{c\tau+d}(a^2\tau(c\tau+d)-c(a\tau+b)^2)} = e^{-2\pi\imath y-\frac{\pi\imath}{c\tau+d}(a^2\tau d-2abc\tau-b^2c)},$$

but

$$a^2\tau d-2abc\tau-b^2c = a(ad-bc)\tau-ab(c\tau+d)+b(ad-bc) = (a\tau+b)-ab(c\tau+d)$$

Now what we want comes from the simple observation that ab is even.
By the characterisation we gave, $\vartheta(y,\tau')$ is the unique function (up to scalars) invariant[3] under $L_{\tau'}$, where $\tau' = \frac{a\tau+b}{c\tau+d}$; since we showed that $\psi(y,\tau)$ shares this property, it must be a function of that kind, so we get

$$\psi(y,\tau) = \phi(\tau)\vartheta\left(y,\frac{a\tau+b}{c\tau+d}\right)$$

for some function $\phi(\tau)$. In other words, if $y=\frac{z}{c\tau+d}$, then

$$\vartheta(z,\tau) = \phi(\tau)e^{-\pi\imath c\frac{z^2}{c\tau+d}}\vartheta\left(\frac{z}{c\tau+d},\frac{a\tau+b}{c\tau+d}\right).$$

We would like to evaluate $\phi(\tau)$; note that $\vartheta(z,\tau)$ is normalised thanks to the property that the constant term of the Fourier series is just 1, that means

$$\int_0^1 \vartheta(y,\tau)dy = 1.$$

[3]We saw the sense of this invariance with respect to the second variable; it is invariant up to an exponential factor, which is exactly what we want here.

Hence

$$\phi(\tau) = \int_0^1 \psi(y,\tau)dy = \int_0^1 e^{\pi\imath c(c\tau+d)y^2}\vartheta((c\tau+d)y,\tau)dy$$

From a computational point of view, this integral is not too hard to evaluate; first we notice that $\phi(\tau) = d = \pm 1$ if $c = 0$, so we can assume $c > 0$. Now we substitute the defining series for ϑ and we get:

$$\phi(\tau) = \int_0^1 \sum_{n\in\mathbb{Z}} e^{\pi\imath(cy+n)^2(\tau+\frac{d}{c})-\pi\imath n^2\frac{d}{c}}dy = \sum_{n\in\mathbb{Z}} e^{-\pi\imath n^2\frac{d}{c}} \int_0^1 e^{\pi\imath(cy+n)^2(\tau+\frac{d}{c})}dy.$$

But, since cd is even, we have $e^{-\pi\imath d\frac{(n+c)^2}{c}} = e^{-\pi\imath n^2\frac{d}{c}}$ and so we get

$$\phi(\tau) = \sum_{1\le n\le c} e^{-\pi\imath n^2\frac{d}{c}} \int_{-\infty}^{+\infty} e^{\pi\imath c^2y^2(\tau+\frac{d}{c})}dy.$$

We evaluate the integral by supposing at first that $\tau = \imath t - \frac{d}{c}$; in this case we get

$$\int_{-\infty}^{+\infty} e^{\pi\imath c^2y^2(\tau+\frac{d}{c})}dy = \int_{-\infty}^{+\infty} e^{-\pi c^2y^2t}dy$$

and if we set by a change of variables $u = ct^{\frac{1}{2}}y$, we obtain that the same integral becomes

$$\frac{1}{ct^{\frac{1}{2}}}\int_{-\infty}^{+\infty} e^{-\pi u^2}du = \frac{1}{ct^{\frac{1}{2}}}$$

using the well-known value $\int_{-\infty}^{+\infty} e^{-\pi u^2}du = 1$.
It follows then by analytic continuation that for any τ with $\mathrm{Im}(\tau) > 0$ we have

$$\int_{-\infty}^{+\infty} e^{\pi\imath c^2y^2(\tau+\frac{d}{c})}\,\mathrm{d}\,y = \frac{1}{c(\frac{\tau+\frac{d}{c}}{\imath})^{\frac{1}{2}}}$$

where the denominator is chosen in such a way to have strictly positive real part. The sum $\sum_{1\le n\le c} e^{-\pi\imath n^2\frac{d}{c}}$ is a very well known Gauss sum, which gives just $c^{\frac{1}{2}}$ times some 8-th root of unity. In fact, what we get is the following:

Theorem 3.3.1. *Given $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$, ab and dc even, there exists ζ a 8^{th} root of 1 such that*

$$\vartheta(\frac{z}{c\tau+d}, \frac{a\tau+b}{c\tau+d}) = \zeta(c\tau+d)^{\frac{1}{2}}e^{\frac{\pi\imath cz^2}{c\tau+d}}\vartheta(z,\tau). \tag{3.8}$$

In some particular situations, we are even able to compute ζ exactly:

1. *if c is even and d is odd, then $\zeta = \imath^{\frac{1}{2}(d-1)}\left(\frac{c}{|d|}\right)$, where $\left(\frac{c}{|d|}\right)$ is the Legendre symbol (to take care of all the possible cases, we set $\left(\frac{0}{1}\right) = 1$);*
2. *if c is odd and d is even, then $\zeta = e^{-\pi\imath\frac{c}{4}}\left(\frac{d}{c}\right)$.*

Proof. See [Mum83, Theorem 7.1]. □

3.4 Theta as a modular form

In this section we are going to recall some definitions and results we gave previously and to put them together in order to study some properties characterising the theta functions.
We saw in the previous sections that the matrices corresponding to substitutions in the variables z, τ for which ϑ is a quasi-periodic function form a group; in fact, $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{C}\times\mathcal{H}$ by $(z,\tau)\mapsto(\frac{z}{c\tau+d},\frac{a\tau+b}{c\tau+d})$, because $\left(\frac{\frac{z}{c\tau+d}}{c'\frac{a\tau+b}{c\tau+d}+d'},\frac{a'\frac{a\tau+b}{c\tau+d}+b'}{c'\frac{a\tau+b}{c\tau+d}+d'}\right)=\left(\frac{z}{(c'a+d'c)\tau+(c'b+dd')},\frac{(aa'+b'c)\tau+(a'b+b'd)}{(c'a+d'c)\tau+c'b+d'd}\right)$.
Moreover, this action normalises the lattice action on z, id est we have the action of a semidirect product $\mathrm{SL}_2(\mathbb{Z})\rtimes\mathbb{Z}^2$ on $\mathbb{C}\times\mathcal{H}$, where the element $(\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right),(m,n))$ acts by $(z,\tau)\mapsto(\frac{z+m\tau+n}{c\tau+d},\frac{a\tau+b}{c\tau+d})$.
Actually, not all of these transformations carry ϑ exactly to itself; this is the reason for adding the conditions ab, cd even. To understand this condition theoretically, we recall here some properties and definitions we already presented in the previous chapters; we will state them under a more computational point of view, in order to apply them to computations for ϑ.
We have a natural homomorphism $\gamma_N:\Gamma\to\frac{\mathrm{SL}_2(\frac{\mathbb{Z}}{N\mathbb{Z}})}{\pm\mathbb{1}}$ for every N. Its kernel Γ_N, the so called **principal congruence subgroup of level** N is given by $\Gamma_n=\left\{\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\Gamma : b,c\equiv 0(\mathrm{mod}\ N), a,d\equiv 1(\mathrm{mod}\ N)\right\}$.
As an example, we examine here the case $l=2$. We start by defining $\Gamma_{1,2}\subset\Gamma$ to be γ_2^{-1} of the subgroup of $\frac{\mathrm{SL}_2(\frac{\mathbb{Z}}{2\mathbb{Z}})}{\pm\mathbb{1}}$ consisting of $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$; this is the subset of Γ such that ab and cd are even.
Γ_N is a normal subgroup, whereas $\Gamma_{1,2}$ is not; in fact, it has two conjugates, $\gamma_2^{-1}(\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right),\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right))\Gamma_0(2)$ and $\gamma_2^{-1}(\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right),\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right))=\Gamma^0(2)$ respectively, described by the condition c even and b even (so, respectively, c and $b\equiv 0(\mathrm{mod}\ 2)$, notation which allows us to extend immediately this definition to any case $\neq 2$. We already saw the second of these groups in the previous chapter).
These are the groups for which ϑ_{01} and ϑ_{10} have functional equations; this means that we can express $\vartheta(\frac{z}{c\tau+d},\frac{a\tau+b}{c\tau+d})$, for $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\notin\Gamma_{1,2}$ as a multiple of $\vartheta_{01}(z,\tau)$ or $\vartheta_{10}(z,\tau)$ by means of an elementary factor.

Rather than trying to express the transformation that a completely generic $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ produces over an arbitrary $\vartheta_{i,j}$ we will consider the action of the generators $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. This is what we get:

$$\begin{array}{ll} \vartheta_{00}(z,\tau+1)=\vartheta_{01}(z,\tau), & \vartheta_{00}(\frac{z}{\tau},-\frac{1}{\tau})=(-\imath\tau)^{\frac{1}{2}}e^{\pi\imath\frac{z^2}{\tau}}\vartheta_{00}(z,\tau) \\ \vartheta_{01}(z,\tau+1)=\vartheta_{00}(z,\tau), & \vartheta_{01}(\frac{z}{\tau},-\frac{1}{\tau})=(-\imath\tau)^{\frac{1}{2}}e^{\pi\imath\frac{z^2}{\tau}}\vartheta_{10}(z,\tau) \\ \vartheta_{10}(z,\tau+1)=e^{\frac{\pi\imath}{4}}\vartheta_{10}(z,\tau), & \vartheta_{10}(\frac{z}{\tau},-\frac{1}{\tau})=(-\imath\tau)^{\frac{1}{2}}e^{\frac{\pi\imath z^2}{4}}\vartheta_{01}(z,\tau) \\ \vartheta_{11}(z,\tau+1)=e^{\frac{\pi\imath}{4}}\vartheta_{11}(z,\tau), & \vartheta_{11}(\frac{z}{\tau},-\frac{1}{\tau})=-(-\imath\tau)^{\frac{1}{2}}e^{\frac{\pi\imath z^2}{\tau}}\vartheta_{11}(z,\tau) \end{array} \tag{3.9}$$

Geometrically, the reason why the subgroup $\Gamma_{1,2}$ appears is that $\vartheta(z,\tau)$ vanishes at $\frac{1}{2}(\tau+1) \in \frac{\frac{1}{2}L_\tau}{L_\tau}$, and it is easy to check that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_{1,2}$ if and only if the transformation $z \mapsto \frac{z}{c\tau+d}$ carries $\frac{1}{2}(\tau+1)$ to $\frac{1}{2}(\tau'+1)\text{mod } L_{\tau'}$, where $\tau' = \frac{a\tau+b}{c\tau+d}$.
We shall pose from now on $z=0$, and we will study the behaviour of the ϑ functions as functions in the single variable τ. In this case, the functional equation of $\vartheta(0,\tau)$ reduces to

$$\vartheta\left(0,\frac{a\tau+b}{c\tau+d}\right)=\zeta(c\tau+d)^{\frac{1}{2}}\vartheta(0,\tau),$$

where ζ is an 8-th root of unity as given from Theorem 3.3.1.
This expression will lead us to show that $\vartheta(0,\tau)^2$ is a **modular form**, that is that it fits this definition:

Definition 3.4.1. *Let $k \in \mathbb{N}\cup\{0\}$ and $N \in \mathbb{N}$. A **modular form of weight k and level N** is a holomorphic function $f(\tau)$ on the upper half-plane $\mathcal{H}$ such that:*

1. *for all $\tau \in \mathcal{H}$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_N$, $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$;*
2. *f is bounded as follows:*
   (a) *$\exists t, s$ constants such that $|f(\tau)| \leq t$ if $\operatorname{Im}\tau > s$;*
   (b) *$\forall \frac{p}{q} \in \mathbb{Q}$, $\exists$ positive real $t_{p,q}$, $s_{p,q}$ such that $|f(\tau)| \leq t_{p,q}|\tau-\frac{p}{q}|^{-k}$ if $|\tau-\frac{p}{q}-\imath s_{p,q}| < s_{p,q}$.*

The set of modular forms of weight k and level N is a vector space and it is denoted by $\mathbf{Mod}_k^{(N)}$. Condition 2a of the previous definition gives the bound at ∞ for modular forms defined on $\mathcal{H}$; the action of Γ is defined on the points of $\mathbb{Q}\cup\{\infty\}$ and since $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$, then the bound at $\frac{p}{q} \in \mathbb{Q}\cup\{\infty\}$ is equivalent to the bound at $\frac{a\frac{p}{q}+b}{c\frac{p}{q}+d}$.

The definition above relies on the fact that the factor $(c\tau + d)^k$ satisfies the 1-cocycle condition, that is to say, if we write $e_\gamma(\tau) = (c\tau + d)^k$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, for all γ_1, $\gamma_2 \in \Gamma_N$ we can write $e_{\gamma_1\gamma_2}(\tau) = e_{\gamma_1}(\gamma_2\tau)e_{\gamma_2}(\tau)$.
This condition, together with the fact that Γ_N is normal in Γ, gives an action of $\frac{\Gamma}{\Gamma_N}$ on the vector space $\mathbf{Mod}_k^{(N)}$: if f is a modular form and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, define $f^\gamma(\tau) = e_\gamma(\tau)^{-1} f(\gamma\tau)$. This is a modular form of the same kind as f, as it follows directly by checking the definition.
More, we notice that if $f \in \mathbf{Mod}_k^{(N)}$ and $g \in \mathbf{Mod}_h^{(N)}$, then the product $fg \in \mathbf{Mod}_{k+h}^{(N)}$. Thus $\mathbf{Mod}^{(N)} = \oplus_{k\in\mathbb{N}\cup\{0\}} \mathbf{Mod}_k^{(N)}$ is a graded ring, namely the **ring of modular forms of level** N.
We can now state the following:

Proposition 3.4.2. *$\vartheta_{00}^2(0,\tau)$, $\vartheta_{01}^2(0,\tau)$ and $\vartheta_{10}^2(0,\tau)$ are modular forms of weight 1 and level 4.*

Proof. To start with, verifying condition 1 of the definition amounts to saying that ζ, the 8-th root of unity that appears in the functional equation (3.8) is ± 1 when $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_4$; this comes directly from the description of ζ we gave in Theorem 3.3.1(1), as we only need c even and $d \equiv 1 (\mathrm{mod}\ 4)$. We can also verify immediately the bound 2a at ∞ for $\vartheta_{00}^2(0,\tau)$. In fact, the Fourier expansion

$$\vartheta_{00}(0,\tau) = \sum_{n\in\mathbb{Z}} e^{\pi\imath n^2\tau}$$

shows that, as $\mathrm{Im}(\tau) \to \infty$ we have $\vartheta_{00}(0,\tau) = 1 + O(e^{-\pi\,\mathrm{Im}(\tau)})$, hence $\vartheta_{00}^2(0,\tau)$ is close to 1 when $\mathrm{Im}(\tau) \gg 0$. Before checking the last condition of the definition, we consider the action of Γ on $\vartheta_{00}^2(0,\tau)$. We can check the following equalities, by means of (3.9):

$$\begin{aligned} T(\vartheta_{00}^2(0,\tau)) &= \vartheta_{01}^2(0,\tau), \quad & S(\vartheta_{00}^2(0,\tau)) &= -\imath\vartheta_{00}^2(0,\tau) \\ T(\vartheta_{01}^2(0,\tau)) &= \vartheta_{00}^2(0,\tau), \quad & S(\vartheta_{01}^2(0,\tau)) &= -\imath\vartheta_{10}^2(0,\tau) \\ T(\vartheta_{10}^2(0,\tau)) &= \imath\vartheta_{10}^2(0,\tau), \quad & S(\vartheta_{10}^2(0,\tau)) &= -\imath\vartheta_{01}^2(0,\tau). \end{aligned}$$

This shows that the three elements span an Γ-invariant subspace of $\mathbf{Mod}_1^{(4)}$.
We have now to check the last point, which boils down to verifying condition 2a for the three functions, because a suitable element $\gamma \in \Gamma$ carries any cusp to ∞.
Proceeding in the same way we did for $\vartheta_{00}(0,\tau)$, with Fourier expansions, we have, for $\mathrm{Im}(\tau) \to \infty$,

$$\vartheta_{01}(0,\tau) = 1 + O(e^{-\pi\,\mathrm{Im}(\tau)})$$

and

$$\vartheta_{10}(0,\tau) = O(e^{-\pi\,\mathrm{Im}(\frac{\tau}{4})});$$

this completes the proof of the proposition. □

3.5 Building modular polynomials

We saw in Chapter 2 the inconvenience of working with classical modular polynomials.
From what we know, we can say that ϑ constants could carry information about elliptic curves, since they are invariants when computed on the element defining the lattice; in fact, they are even more precise than the j invariants, as they identify a single curve, not a class of curves modulo isomorphisms (for example, the values of the ϑ functions enable us to distinguish a curve from a twist of it). We can think about building modular polynomials by means of *vartheta* functions; Proposition 3.4.2 tells us that we have a modular structure if we consider their squares. The existence of a modular polynomial having them as variables is then ensured by the analysis we did in the previous chapter (see the Remark at Definition 2.4.2).
We have to consider a priori four different values, the values of the ϑ constants evaluated in $z = 0$ and in the value of τ characterising the lattice of the elliptic curve we are working on. We know from Lemma 3.2.1 that in fact we need only three of them, as $\vartheta_{11} = 0$ in this case. In fact, we can even pass from a projective environment to an affine one, by means of one of the non-zero constants; again, Lemma 3.2.1 ensures that this process is well defined (we already have a constant which is 0, we could not have another one). This make us work with only two variables; but now, thanks to (3.5), we can express the fourth power of one by means of the fourth power of the other, and determine the squares up to a sign.
By doing this, we can already retrieve the information we had when considering j invariants; in fact, we have even a formula expressing the j invariant by means of ϑ constants, namely

$$j(\tau) = 432\frac{(\vartheta_{00}(\tau)^8 + \vartheta_{10}(\tau)^8 + \vartheta_{01}(\tau)^8)^3}{(\vartheta_{00}(\tau)\vartheta_{01}(\tau)\vartheta_{10}(\tau))^8}. \tag{3.10}$$

We give a sketch for the proof of this. Let us set $f = 432\frac{(\vartheta_{00}(\tau)^8+\vartheta_{10}(\tau)^8+\vartheta_{01}(\tau)^8)^3}{(\vartheta_{00}(\tau)\vartheta_{01}(\tau)\vartheta_{10}(\tau))^8}$.
To show (3.10), we have to show that f has a unique simple pole at ∞; if this is the case, after multiplying by a constant c we have that $j - cf$ has no poles at ∞, so it is holomorphic; then it is constant by Liouville's Theorem, since it is continuous over a compact space, so it is bounded (this is more or less the same kind of reasoning we had in Lemma 2.1.3). To prove that in fact this constant is 0, and that our $c = 1$, it is enough to evaluate the functions at two distinct points; so we have proven the equality.
Formula (3.10) tells us in particular that we do not have to worry about the sign; any ϑ constant is considered to a power 8, the sign ambiguity mentioned above that occurs while determining ϑ^2 does not emerge.

The polynomials we obtain this way are already smaller than the classical ones; one can find some examples on [BB87, Chapter 4.5], where the authors compute them explicitly. Our project was in fact a more ambitious one: we wanted polynomials taking into account just the single variables ϑ, not their squares. This is possible if we consider not the functions evaluated in τ, but in $\frac{\tau}{2}$; in practice, this allows us to eliminate the squares.
To summarize, we take into account a ratio of two different ϑ constants and we compute the modular polynomial with respect to it. Our departing function was, in particular, $f = \frac{\vartheta_{00}}{\vartheta_{10}}$; for any $\ell \in \mathbb{N}$, our ℓ-polynomial, once we evaluate in $f(\frac{\tau}{2})$ for a given $\tau \in \mathbb{C}$, the variable X, have as zeros in Y the values of $f(\frac{\tau}{2\ell})$, so the same function evaluated on ℓ-isogenous curves. Once we have the ratio for isogenous curves, we can retrieve the value of the third constant up to a sign, and this is enough to retrieve the correct value of j by means of (3.10).
In practice, we see immediately that we can forget that we are dealing with $\frac{\tau}{2}$, as we are free to choose our element on the whole $\mathcal{H}$; the division by 2 it is just a formal remark we have to consider, but in practice it does not pose any constraint on our τ. We are then free to choose a generic $\tau \in \mathbb{C}$.
We remark also that formula (3.10) is useful to forecast some heuristic informations about the coefficients of the polynomial we are looking for; naively, it says that relations between ϑ constants could possibly be expressed by polynomials whose coefficients are twenty-four times smaller than the coefficients of the classical modular polynomials. We say this simply by looking at exponent appearing in the expression; both the denominator and the numerator present ϑ function with 24 as maximal exponent. We could guess that an expression involving directly the modular structure of ϑ without any direct regard to j could possibly have coefficients whose size is of the order of a 24-th root of the coefficients of a classical modular polynomial.
We will see in the next chapter that this is actually the case: these polynomial relations exist, can be computed by means of two independent ϑ constants which we choose between all of them, and have coefficients which are significantly smaller.
As we already said, we did all this work not only to compute polynomials with smaller coefficients, but also in view of a generalisation to a higher genus case. In fact, genus 1 curves are peculiar from the characterisation point of view: the single j invariant is enough to characterise all the isomorphism classes.
In genus 2, for example, we have the Igusa invariants which do the same kind of characterisation, but to identify a single class we need the value of three distinct invariants. This means also that, if we look for a polynomial linking between them the invariant of a given curve and all the invariants of curves

which are l-isogenous to it, we cannot rely on a single polynomial any more; we will need three of them, and the computations of them for low isogeny degrees reveal that they will have very huge coefficients. The computations of modular polynomials by means of ϑ constants would mean an important advantage in terms of polynomial size, so in terms of computational time. More generally, we could extend this way of proceeding in any genus, without knowing a priori invariants classifying curves up to isogenies.

Chapter 4

Algorithms and computations

In this section we are going to explain different algorithms for computing modular polynomials and to present our implementation of them.

The program we used is PARI/GP version 2.5.1, and we used quite a lot of pre-implemented functions, whose detailed behaviour we are not going to specify; we are going to explain more extensively what we did when writing original parts of code.

We will compare different strategies that can be followed in computations of classical modular polynomials or of modular polynomials by means of ϑ functions, a comparison that will be carried on both on the practical side and on the side of complexity; we will see that the new modular polynomials we will obtain by means of ϑ functions are indeed smaller, and that the fact of having smaller coefficients asymptotically cuts the computational cost.

The structure of this chapter reflects the way of proceeding we adopted while programming and doing computations: in the first section we present the different algorithms, as well as their computation of complexity, and we test them over j invariants. The advantage of this method consists on the fact that we already knew the final results we should get, so this was a good way to check the correctness of our codes.

In the second section we explain the work we did with ϑ functions. We explain the difficulties we faced in adapting the algorithms to this case; we did not know a priori the final shape of the results, so sometimes we had to pay attention to some details that were not dangerous when working with j invariants. We display and comment then the results we got, always specifying which method carried which results, and how much time did it take; we will see that already for low isogenies levels there are significant differences between the algorithms, not only in terms of time but also in terms of results.

4.1 Modular polynomials for j-invariants

First of all, we tried to compute the modular polynomials linking the usual j-invariant of a given elliptic curve with the j-invariant of the curves obtained from it by applying an isogeny of a given degree l. We tried essentially two methods, which were tested here in order to be applied to the analogous study with theta constants. All these methods, together with a computation of complexity, are presented in [Eng09].
The case of j-invariants was simpler since we already know the shape of the desired result and we could therefore simplify some computations when performing them; moreover, the value of the j-invariant for a given a value of τ defining the lattice is already implemented in the PARI system, so we did not have to program a separate function for doing it.

4.1.1 Substitution in q-expansion

The first method one can think about, from what we saw in the preceding chapters of this work, is to find a linear relation between q-expansions for $j(\tau)$ and for $j(\frac{\tau}{l})$. This is a very naive method: one compares the two expressions (2.2) and (2.3) (this last taken for the identity matrix), and tries to cancel all the appearing terms, starting from the lowest ones. We know the polynomial we are looking for is symmetric, we know that it is monic and we know its degree; these are important clues that enable us to spare time and to proceed in a more assured way.
The strategy is to proceed by cancellations; one compares the q-expansions relative to $j(\tau)$ and to $j(\frac{\tau}{l})$, and tries to find a combination that cancels all the terms, starting from the lowest degrees. The information we know about the final shape of the polynomial helps us in this procedure: every time we add a monomial to the polynomial we have to add its symmetric as well, and we know at lest a coefficient, which is the coefficient of the leading term.
This method works, but it is not really efficient; finding the right term could be not immediate, and the fact of dealing with infinite sums is not making things simpler; though, it is a very intuitive strategy, easy to understand and not requiring particular mathematical tools (the only tool that is needed is in fact a performing machine to compute coefficients, as the calculations can turn out to be really hard and memory-demanding!).
Actually, we could even proceed in a smarter way, using some properties we know of the polynomial we are looking for, and in particular the characterisation we gave for the representatives of the classes in ${}_{\Gamma^0(l)}\backslash^{\Gamma}$ (we took this idea from [Mor95]). If we set $f(z) = j(\frac{z}{l})$, we can in fact express the polynomial

as

$$\prod_{b=0}^{l-1}(X - f_b)(X - f_S), \tag{4.1}$$

where $f_b(z) = f(T_b z)$ and $f_S(z) = f(Sz)$, by means of q-expansions.
To do so, we have to study the changes produced on q-expansions by the actions of the representatives of ${}_{\Gamma^0(l)}\backslash^{\Gamma}$; if the q-expansion of f is

$$f(z) = \sum_{k=vl}^{\infty} a_k q^{\frac{k}{l}} \in \mathbb{C}((q^{\frac{1}{l}})),$$

with $q^{\frac{1}{l}} = e^{2\pi\imath\frac{z}{l}}$, with a_k rational integers, the q-expansion of the conjugates $f_b(z)$ are of the same form, with the coefficients a_k being multiplied by the root of unity $\zeta_l^b = e^{2\frac{\pi\imath b}{l}}$.
This is not the case for the last conjugate, $f(Sz)$, which requires separate computations to be expressed; anyway, as it is the only case that should be dealt with separately, this does not affect too much the total complexity. The reason for this difference is that in this case $f(Sz) = j(lz)$, so it express an isogeny which does not fit the notation we employ for all the others.

4.1.1.1 Computation of complexity

Even if we did not implement this algorithm directly, we present here a brief analysis of its computation of complexity, in order to compare it with the methods we present above. According to [Mor95], the second method we illustrate above is the fastest between all the methods exploiting q-expansions. This is easily understandable, as this method boils down to computing a fixed product of terms really close one to the other (coefficients differ only by multiplication by an l-th root of unity) and a single different term. We know we have a bound on the size of the coefficients of the polynomial; so, as Enge explicitly computes, the final complexity is $O(l^3 \log(l) M(n)) \subset O(l^4 \log(l)^{3+\epsilon})$, where $M(n) \in O(n \log(n)^{1+\epsilon})$ is the complexity of performing a multiplication between integers of size n by means of the fast multiplication methods (we will keep this notation fixed from now on), and n is the bound (2.6) we have on coefficients size.
This estimate does not come from direct computations as we presented them above, but from performing them modulo a big prime of bit size $n \in O(l \log(l))$, which prevents coefficients in the product from growing too much, or from performing all the computations modulo small primes and then retrieving the desired result by means of the Chinese Remainder Theorem.

4.1.2 Looking for linear relations

4.1.2.1 Computing kernels...

One can think about another very intuitive method: to build a matrix with all the possible monomials evaluated in the j invariant of a curve and of the image of it by an l-isogeny, and to look for a linear dependency relation by looking at its kernel. In practice, we look at the coefficients of the modular polynomial as solutions of a big linear system whose equations are given by the rows of the matrix, so the evaluated monomials are considered as coefficients.
It was very straightforward to implement this method, as we already knew that the final result should be a polynomial of degree $l + 1$, so for a given l we had a fixed number of monomials to consider, $(l + 2)^2$ a priori. The situation was even better as we knew that the polynomial has a single term of degree $l+1$ in each variable, monic, and this allows us to reduce even more the number of monomials we should consider.
We built a square matrix whose columns are given by the evaluation of the different monomials and whose rows are given by different values of τ we chose randomly; then we applied to the matrix the methods for computing kernels.
In practice, though, when using the pre-implemented command in PARI, this gave no results. This is due to the fact that, even if we are dealing with matrices whose determinant is very close to zero, it is not exactly zero due to the errors of the floating point representation. So we decided to make computations more explicit, in order to see better how things developed.

4.1.2.2 ...or solving an affine linear system

To make computations simpler (in order to deal with smaller matrices) and we can specify the leading terms and solve an affine linear system having the leading terms evaluated in $j(\tau)$ and in its image[1] via the l-isogeny as column of solution; this gives the desired result.
This method is indeed more stable than the previous one. In fact, while computing kernels, computations may give rise to very small values in place of zeros; the problems is that these values are really difficult to deal with, as when performing divisions they make the result explode. So, even if we

[1]Usually, when we speak about the image via an isogeny we are referring to the action of the map on the curve, so to the map sending one point of the domain curve to a point in the target one. Here we use the word image to denote the action of this ma on the j invariants; in other words, if we start from $j(\tau)$, we say that its image via an l-isogeny is $j(\frac{\tau}{l})$, or $j(l\tau)$.

start from little approximation errors due to the floating point notation, they progressively increase all along the computations giving us at the end a result which could be very far from the correct one. The advantage of solving an affine linear system is that this make us deal with an invertible matrix; in general, we are not suppose to deal with very small values and so even if we start from a matrix of perturbed data, this perturbations do not dramatically amplify.

What we got by those computations was a symmetric 2-variables modular polynomial; we knew that we were looking for integer coefficients, and the coefficients we got were indeed very close to integer ones. We wrote some lines of codes in order to erase the not integer part; we could not use the rounding pre-implemented function as a priori we had to deal with complex coefficients (even if the imaginary part was always negligible). Essentially, we rounded separately the imaginary and the real part of each coefficient. Our code takes as input a parameter p: for the imaginary part, it checks whether it is less than $10^{\frac{p}{2}}$, and if this is the case, it rounds it to 0; for the real part, it checks if the difference with an integer is less than $10^{\frac{p}{2}}$, and again, if this is the case, it sets this integer as the new real part of the coefficient. If those verifications are negative, it leaves the coefficient unvaried.

Here is the code we used for $l = 2$, preceded by the function we used to detect integer values:

```
reductionc(t, p)=

/* Given a complex number t, and the precision p at
which we are performing computations, this function
gives as output a reasonable rounding of t, allowing
us to see that in our case the modular polynomial
has all integer coefficients.*/

{
my(r, i);
i=imag(t);
if(i<10^(-p/2), i=0);
t=t-imag(t)*I+i*I;
r=round(real(t));
if(abs(r-t)<10^(-p/2), t=r+i*I);
t
}


/*With this procedure, we should have in p the modular
polynomial we were looking for, with 1 as coefficient
```

```
22 for X^(l+1).
23 Knowing this, we can directly isolate the
24 values of X^(l+1):*/
25
26
27
28 l=2;
29 d=(l+2)*(l+1);
30
31 V=vector(d,k,
32 (random(1000)-500)/1000.0 + I*(1 + random(1000)/1000.0))
      ;
33 lV=vector(d, k, V[k]*l );
34 jV=vector(d, k, ellj(V[k]));
35 jlV=vector(d, k, ellj(lV[k]));
36 ex=vector(d, k, (k-1) % (l+2));
37 ey=vector(d, k, (k-1-ex[k])/(l+2));
38 M=matrix(d, d, k, i, jlV[k]^ex[i] * jV[k]^ey[i]);
39 s=vectorv(d, k, -jV[k]^(l+1));
40 b=matsolve(M, s);
41 p=0;
42
43 for(k=1,d,
44         p=p+reductionc(b[k], 100) * Y^ex[k] * X^ey[k]);
45 p=p+X^(l+1)
```

At row 31, in the vector V we put all the $\tau \in \mathbb{C}$ we randomly generate. We see that the choice of the values is not a completely random one; this choice avoids the generation of very big values or of values too close to 0, still remaining inside $\mathcal{H}$.

4.1.2.3 Computation of complexity

First of all, we have to build the big initial matrix. For doing so, for any τ we choose we have to evaluate j in τ and $\frac{\tau}{l}$, and then to create all the possible monomial combinations up to degree $l+1$. In the Phd Thesis of R. Dupont, [Dup06], we have the description of an algorithm that requires $O(M(n)\log(n))$ bit operations for any evaluation performed at precision n; this algorithm can be adapted to a wide class of modular functions, and its complexity (as we can see) does not depend on the value of τ we choose.
Basically, our code performs $2t$ evaluations for different values of τ, where in any case $t \geq l+1$; we have $(l+2)(l+1)$ possible monomial combinations, and computing each of them costs $O(\log(l+1)^2 M(n))$ bits operations. Definitely,

we can say that building our matrix costs $O((l\log(n) + log(l)^2)M(n))$ bits operations.
We apply then to it well-known algorithms; we know, following for example [VzGG03, Chapter 12], that the cost for performing the Gauss reduction of a matrix of size l^2 (or of the same order) takes $O(l^3)$ arithmetic operations; this means that computing kernels and solving linear systems has the same complexity (in both cases, we need to provide ourselves with a reduced matrix). This makes, in terms of bit operations, $O(l^3M(n))$. Finally, the total cost is $O((l^3 + l\log(n) + \log(l)^2)M(n))$.

4.1.3 Evaluation-interpolation

This method is more subtle than the previous one, and it is proven to have a better complexity; the main difference is that here we are going to exploit the properties of our functions j, instead of simply considering them as unknown generic objects linked by a polynomial relation. We do this by treating the two variable separately, dealing at first only with $j(\tau)$ and then considering $j(\frac{\tau}{l})$ only in a second moment.
The idea is simple: basically, we would like to use the fact that we are dealing with a modular polynomial, and that we are able to specify all the roots in a single variable. In fact, what we are looking for is a polynomial $\Phi_l(X, Y)$ such that $\Phi_l(j(\tau), j(\frac{\tau}{l})) = 0$. The fact of being a modular polynomial tells us that if we consider $\tau' = M \circ \tau$, $M \in_{\Gamma^0(l)} \backslash^{\Gamma}$, we have $\Phi_l(j(\tau'), j(\frac{\tau}{l})) = 0$ for any τ' we can define in this way. More, we know that the polynomial should be monic; if we define the function $j_l(\tau) = j(\frac{\tau}{l})$ for any $\tau \in \mathbb{C}$, we can set:

$$\tilde{\Phi}_l(Y) = \Phi_l(j(\tau), Y) = \prod_{\sigma \in \mathrm{Aut}(\mathbb{C}(j,j_l)|\mathbb{C}(j))} (Y - j_l^{\sigma}(\tau)) =$$

$$= \prod_{M \in_{\Gamma^0(l)} \backslash^{\Gamma}} (Y - j(M \circ \tau)) =$$

$$Y^{l+1} + \sum_{i=0}^{l} a_i Y^i, \tag{4.2}$$

and of course we have

$$\tilde{\Phi}_l(j(\frac{\tau}{l})) = \Phi(j(\tau), j(\frac{\tau}{l}) = 0. \tag{4.3}$$

We have already seen this construction before, and precisely in the equation (4.1); that equation shows explicitly the action of each element of the group $\Gamma^0(l)\backslash^{\Gamma}$, by means of the characterisation we gave in Proposition 2.1.5.

Up to now, we have considered our polynomial $\tilde{\Phi}$ in just a single variable; in fact, what we are looking for is intimately linked to it, it is now enough for us to analyse the behaviour with respect to the other variable. If we take into account the expression (4.2), that is to say, if we write $\tilde{\Phi}$ as sum, we can say that all the coefficients a_i are nothing more than polynomials $\tilde{a}_i(X)$ evaluated in $j(\tau)$, that can be recovered by interpolation if we consider different values for τ; that means, we just have to explicit the property (4.3) with respect to $j(\tau)$.
We know exactly the number of different τ we need to perform interpolation; in fact, as our result Φ should be a symmetric polynomial, each polynomial $\tilde{a}_i$ cannot have degree more than $l+1$, $l+2$ values for τ would be enough. We need indeed even less: as the polynomial is symmetrical, and it is monic in its leading terms, we can say that to compute each of the polynomials $\tilde{a}_i$ we should need $l+1$ values for τ; we have that all the polynomials $\tilde{a}_i$ have degree X^l except for $\tilde{a}_0$, whose leading term is X^{l+1} (and we are sure that the coefficient is 1).
This procedure is faster, and again, gives the desired result; as before, we have to cope with some little errors due to computer calculus, but we recognise easily the result. Here is the code:

```
{

W=vector(l+1, k,
(random(1000)-500)/1000.0+I*(1+random(1000))/1000.0);
GW=matrix(l+1, l+1);
for(i=1, l+1,
   GW[1,i]=ellj(W[i]*l);
   for(kt=1, l,
      GW[kt+1,i]=ellj((W[i]+kt-1)/l)
  )
);
sist=vector(l+1, k, prod(i=1,l+1, Y-GW[i, k]));
val=matrix(l+1, l+1, x, y, polcoeff(sist[x],y-1));

tn=vector(l+1, k, ellj(W[k])^(l+1));/*This is
because I already know that my polynomials here
are symmetric, so I just put the right coefficient
for the highest degree term at the end, without
needing interpolation*/

jW=vector(l+1, k, ellj(W[k]));
P=polinterpolate(jW, val[ ,1]~-tn, X);

```

```
24 P=P+X^(l+1)+Y^(l+1)+sum(i=1, l,
25         polinterpolate(jW, val[ ,i+1]~, X)*Y^i);
26 p=0;
27
28 for(i=0, poldegree(P, Y),
29 for(j=0, poldegree(polcoeff(P, i, Y), X),
30 p=p+
31 reductionc(polcoeff(polcoeff(P, i, Y), j), 100)
32 *X^j*Y^i));
33 p
34 }
```

4.1.3.1 Computation of complexity

From our discussion above, we can decompose the method in various steps: first, we need an evaluation phase, which requires $(l+1)(\deg_j(\Phi_l)+1)$ evaluations of $f = j(\frac{\tau}{l})$, that is to say $(l+1)(l+2)$ evaluations whose cost is $O(\log(n)M(n))$ each, which gives a complexity $O(l^2E(n))$. Then, we need to build $l+2$ degree $l+1$ polynomials starting from their roots. This step takes $O((l+1)l\log^2(l)M(n))$, plus an eventually negligible term of order $O(\log(n)M(n))$ coming from the features of the FFT (we need to know a primitive root of unity of sufficiently high order to perform the computations; for more informations about FFT, we refer again to [VzGG03, Chapter 8]). Then we pass to the interpolation phase; again, using fast algorithms, we can say that this can be done in $O(l(l+1)\log^2(l+1)M(n))$ (we already have a suitable root of unity from the previous step). So we reach a total cost of $O(l^2(\log^2(l)+\log(n))M(n))$.

4.2 Modular polynomials via theta functions

This section is devoted to the computation of modular polynomials by means of theta functions. As we explained in the previous chapter, we can choose to compute these polynomials by means of a ratio of theta constants; we simplify the notations by writing

$$\vartheta_{00}(\tau) = \vartheta_0(\tau) = \sum_{n\in\mathbb{Z}} e^{\imath\pi\tau n^2} = 1 + 2\sum_{n\in\mathbb{N}^*} (e^{\imath\pi\tau})^{n^2},$$

$$\vartheta_{10}(\tau) = \vartheta_1(\tau) = \sum_{n\in\mathbb{Z}} e^{\imath\pi\tau n^2+\imath\pi n} = \sum_{n\in\mathbb{Z}} (-1)^n e^{\imath\pi\tau n^2} = 1 + 2\sum_{n\in\mathbb{N}^*} (-1)^n (e^{\imath\pi\tau})^{n^2},$$

and we will compute our polynomials by means of $\frac{\vartheta_0}{\vartheta_1}(\tau)$ and $\frac{\vartheta_0}{\vartheta_1}(\frac{\tau}{l})$.

We need first of all to program the function ϑ, as in this case it is not a pre-implemented function; we have to be particularly careful as it is defined as a series, so we have to fix an exponent at which it is reasonable to cut off computations. Then we exploit the very same methods as before, adapting them to the particular situation in which we are now.

4.2.1 Computation of theta constants

We define once for all a quantity that we will use all along the computations: $q_0 = e^{i\pi\tau}$, which depends only on the τ at which we are evaluating our function[2]. Actually, as we can see from the formulae above, both ϑ_0 and ϑ_1 present the same summands; in the second function we are just taking them with alternating signs.
A smart way to proceed here is to compute at each step the new term and then to add it to the partial sum of all the previous other (in the case of ϑ_1, we just pay attention to the sign we put before it). To compute the new term, we just exploit the formula for the binomial square, that is to say $(n+1)^2 = n^2 + 2n + 1$; we define 2 sequences, $A_n = q_0^{n^2}$ and $B_n = q_0^{2n}$, as follows: $A_1 = q_0$, $B_1 = q^2$; $A_{n+1} = A_n \cdot B_n \cdot q_0$, $B_{n+1} = B_n \cdot B_1^2$ (in [Coh96, Chapter 7.6] it is describe a similar method for the computation of η). Then the sequence $(A_n)_{n\in\mathbb{N}}$ provides us with the terms we have to add at each step.
As we said, we need a termination rule for the sum. Actually we can easily see that at each step the terms we are adding become smaller and smaller, and we can guess that at a certain point they should be so little that they will no more change the result we see as output from the computer.
If we decide a priori to work with k digits of precision, this happens when $|A_n| \leq 10^{-k}$, that is to say when

$$n^2 \ln(|q_0|) = n^2 \pi \operatorname{Im}(\tau) \geq k \ln 10, \tag{4.4}$$

so the resulting bound is $n \geq \sqrt{\frac{k \ln 10}{\pi \operatorname{Im}(\tau)}}$. Alternatively, we can just set a desired precision and keep on adding new terms until the terms we are adding are smaller than the bound we decided. Here is the code:

```
1 thetaconstants(tau)=
2
3 { /*Given a complex value tau as imput, gives as output
4 a vector containing the two values of the desired theta
5 constants and their quotient:*/
```

[2]Beware of the difference between this quantity and $q = q_0^2$, the values we employed all along the preceding chapters.

```
6
7  my(k,q0,theta0,theta1,N,i,A,B);
8  k=600;
9  q0=exp(Pi*I*tau);
10 theta0=1;
11 theta1=1;
12 /*N=round(sqrt(k*log(10)/Pi*imag(tau)));*/
13 A=q0;
14 B=q0^2;
15 q2=B;
16 i=1;
17 while(2*abs(A)>10^(-2*k),
18         theta0=theta0+2*A;
19         theta1=theta1+2*(-1)^i*A;
20         A=A*B*q0;
21         B=B*q2;
22         i++
23         );
24 [theta0, theta1, theta0/theta1 ]
25 }
```

Notice that at row 8 we fix a value for the parameter k; this choice depends on the precision we finally want to reach. Here, we chose to keep it fixed as we only used this code to computations for low l; in fact, as l increases, we should decrease k if we want to get some output. Maybe it would have been better to define a variable to have some control on it; anyway, this value works for all the computations we chose to perform.

4.2.1.1 Computation of complexity

The algorithm we used for evaluating ϑ constants is simple to evaluate in terms of complexity: at each step we have to perform two sums, three multiplications, a square and two multiplications by 2 (which can be seen as addictions); so the only thing we have to take into account is the number of iterations we perform.
If we keep the bound we set at Section 4.2.1, that is to say (4.4), the resulting cost is $O(M(n)\sqrt{\frac{n}{\mathrm{Im}(\tau)}})$, where n is the precision at which we want to evaluate our function.
We see that the bound depends here on the choice of τ; in the next section, we will briefly describe a method to pass from a generic τ to a value in the fundamental domain $\mathcal{F}$, which with this method would lower the computation of complexity.

How to reduce an element to the fundamental domain

We have seen from the analysis above that the computational complexity depends on the imaginary part of the value τ we choose. We know that in the fundamental domain we have the values with the smaller imaginary part allowed; more, we know that transformations via elements of $\Gamma(l)$ do not affect the value of the ϑ constants. Definitely, if we find a way to reduce our values in the fundamental domain we can reduce remarkably the computational costs; we know from Proposition 1.2.3 the existence of such a transformation for any choice of $\tau \in \mathcal{H}$. So, the strategy was to apply recursively elements of $\Gamma(l)$ to our random τ until we land in the fundamental domain, and only then compute our ϑ constant.
The elements we apply are elements which are meant to reduce the norm; thanks to the action of the elements of $\Gamma(l)$, we make perform a sort of Gauss reduction on the associated quadratic form, until we land in $\mathcal{F}$.
This is the code; a similar algorithm is performed internally by the PARI system when computing j.

```
1  t=tau;
2  S=[0,-1;1,0];
3  T=[1,1; 0,1];
4  G=[1,0;0,1];
5  n=round(real(t));
6  t=t-n;
7  G=T^(-n);
8  while(norm(t)<1, t=-1/t; G=S*G; n=round(real(t)); t=t-n;
       G=T^(-n)*G)
9
10 /*At each step, we keep track in the matrix G of the
     elements of Gamma that are acting on our initial
     value tau. At the end, in t we will find the element
     act(G, tau), where act is the action defined by the
     elements of Gamma on the upper complex half-plane.
11 Of course, this procedure can easily be adapted when
     working, as above, in Gamma(1), simply by taking the
     correspondent class of our matrix G.*/
```

Actually, the algorithm we presented is not the fastest way to evaluate ϑ functions; as we already said above, in his Phd thesis ([Dup06]), R. Dupont explains how to exploit in this sense the AGM method, an idea that may date back to Gauss' times (for a discussion on this topic, see [Cox84]).
In his work, Dupont presents an algorithm which costs $O(M(n)\log(n))$ and can be adapted to compute ϑ functions; in this case, the cost does not depend

any more on the element τ we are considering. However, we did not take into account this method, which is hard to implement and at our level would not have produced an appreciable advantage in terms of computing time.

4.2.2 Looking for linear relations

As in the previous case, we tried to obtain some relations linking monomials evaluated in the ratios of ϑ constants. We applied exactly the same method as before, so we built a matrix having as columns the different monomials evaluated in different choices of τ, choices ranging on the rows.

```
1
2
3  relatq(l, L, t)=
4
5  /*Here we define big matrices and we compute their
6  kernels, in order to get a relation with integer
7  coefficients between the elements involved. L is
8  the final degree of the polynomial we want to obtain
9  as output; our aim is, via computing the kernel of
10 the matrix of relations of a given degree, to decide
11 if such a polynomial exists or not. The parameter t
12 gives us the dimension of the matrix, that is to say
13 the number of values we consider when building it:*/
14 {
15 my(W, thet, i, j, M, k);
16 W=vector(t, j, I*(10000+random(20*10000))/100000.0);
17 thet=matrix(t, 2);
18 for(i=1, t, thet[i, 1]=thetaconstants(W[i])[3];
19                  thet[i,2]=thetaconstants(W[i]/l)[3]
20                           );
21 M=matrix(t, (L+1)^2);
22 for(k=1, t,
23               for(i=0, L,
24                  for(j=0, L,
25         M[k,(L+1)*i+j+1]=thet[k, 1]^(i)*thet[k, 2]^(j)
26 )));
27 [M,W]
28 }
```

4.2.2.1 Computing kernels...

In this case, we did not know in advance the shape of the result; what we knew was simply that the evaluated monomials should be linearly dependent. We took a big number of different τ and we tried to compute the kernel of that matrix. Actually, we could not use the pre-implemented function to build the kernel; we wrote a code performing Gauss reduction and putting the matrix in a triangular form. We know that there exists a dependency relation involving columns of that matrix, and the Gauss algorithm should highlight it by the presence of 0 as an eigenvalue on the diagonal of the triangular matrix (as we are dealing with floating points quantities, this is not an exact value, but just an approximate one).

To summarize, the Gauss algorithm made us find R and C unitary matrices and a triangular matrix $\tilde{M}$ such that $R \circ M \circ C = \tilde{M}$; any time we find 0 as an eigenvalue on the diagonal of $\tilde{M}$, say in the k-th position, it means that the k-th column of C belongs to the kernel of M.

```
1  gaussker(M, eps)=
2
3  /*Here we try to implement the Gauss reduction,
4  stopping when we find an element of the kernel
5  (we in fact need just a single vector). Our
6  inputs are the matrix we want to reduce, and a
7  value epsilon that gives the bound under which
8  we will consider the values to be 0. */
9  {
10 my(l, R, C, i, j, m, k,v, h , kernel);
11 l=length(M);
12 c=length(M~);
13 h=vector(l);
14 R=matid(c);
15 C=matid(l);
16 i=1;
17 kernel=[;];
18 while(i<=l, m=M[i, i];
19         k=i;
20         for(j=i+1,c, if(abs(M[j,i])>abs(m), k=j;
21                                             m=M[j,i]));
22                 if(abs(m)<eps,
23 kernel=concat(kernel, C[ ,i]),
24  v=M[i, ];
25         M[i, ]=M[k, ];
26         M[k, ]=v;
```

```
27          M[ ,i]=M[ ,i]/m;
28          for(j=i+1, l, h[j]=M[i,j];
29                  M[ ,j]=M[ ,j]-h[j]*M[ ,i]);
30          v=R[i, ];
31          R[i, ]=R[k, ];
32          R[k, ]=v;
33          C[ ,i]=C[ ,i]/m;
34          for(j=i+1, l, C[ ,j]=C[ ,j]-h[j]*C[ ,i]);
35          );
36          i++);
37
38  /*If the loop ends because of the break, it
39  means we have found a zero column, which means
40  we have a non-zero element in the kernel of
41  the matrix we are considering. If this is not
42  the case, we have an invertible matrix, and so
43  we can not find any element in its kernel.
44  Actually, what we do want is an element whose
45  coefficients are integer values; we have kept
46  track of all the operations we performed on
47  the matrix M by means of the matrix G, that
48  enables us to recover the element of the kernel
49  we are looking for. In fact, its k-th column
50  will belong to the kernel of M*/
51  kernel
52  }
```

We expected to find a one-dimensional kernel with integer coordinates; and in fact, that was the final result, that we display here for low isogenies levels:

$$l = 3 : Y^4 - 4XY + 6X^2Y^2 - 4X^3Y^3 + X^4$$

$$l = 5 : Y^6 - 16XY + 10XY^5 + 15X^2Y^4 - 20X^3Y^3 + 15X^4Y^2 + 10X^5Y - \\ - 16X^5Y^5 + X^6$$

$$l = 7 : Y^8 - 64XY + 56XY^5 - 112X^2Y^2 + 140X^2Y^6 - 112X^3Y^5 + 56X^3Y^7 + \\ + 70X^4Y^4 + 56X^5Y - 112X^5Y^3 + 140X^6Y^2 - 112X^6Y^6 + \\ + 56X^7Y^3 - 64X^7Y^7 + X^8$$

Remark:From what we see here, we have already something encouraging. As in the case of j, we have symmetric polynomials, but here even in a broader sense than before: the variable X is symmetric to the variable Y,

but they are symmetric also with respect to the substitutions $X \mapsto \frac{1}{X}$, $Y \mapsto \frac{1}{Y}$.
Another surprising feature is the low degree. After the Remark to Definition 2.4.2, we base the existence of such polynomials on the computation resultants; but we see from (3.10) that this degree could be very high, $24^2(l+1)$ a priori. When computing the relation matrix we did not fix a priori the degree of the monomials inside it; from these concrete examples we see that in fact a degree $l+1$ is enough. The degree is the same as for classical modular polynomials; this, together with the fact of the coefficients being so small, makes these polynomials really suitable for practical computations. Some considerations about the precise rate of decreasing for the coefficients' size will be performed in the final section of this chapter.

This method works, but it is not very stable. Even for $l = 7$, for example, we needed a precision of 500 digits.
So, trying to optimize the computations, we used the algorithm LLL. This algorithm builds a basis for the lattice we create with the columns of the matrix filled with evaluated monomials by taking the smaller integer combinations of vectors that give a basis (see [LLL82] for a complete description of the algorithm). In our case, as we have to reduce ourselves to work only with real quantities, so we consider separately real and imaginary parts, doubling the numbers of the row we consider. From this algorithm, we can easily deduce an algorithm for computing integer kernels, as it is explained in [Coh96, Chapter 2.7.1]. Here we are working with complex values, so we have to use the adapted LLL algorithm as presented in [BK93], which has a cost of $O(l^6(n)^3 M(n))$. We see that this is more demanding from a computational point of view, but it turns out to be more stable.
When doing it, with the pre-implemented function for computing LLL in PARI/GP, we obtained the same results as before but less precision was needed for computations; for example, we passed from 500 to 200 digits needed for $l = 7$.

4.2.2.2 ...or solving an affine linear system

Exactly as in the previous case, we could think about isolating a column and deal with it as column of solutions.
Here we don't know a priori the shape of the result, so we can't assume, for example, that the leading coefficient is 1 as we did in the j-invariants case; still, we can impose this condition, and then look for rational coefficients

instead of looking for integer ones. As a matter of facts, we see from the examples above that the leading coefficient is indeed 1, so this condition does not make any difference for the computations; a priori, though, this could have been dangerous, because if we have chosen a term whose coefficient is 0 in the polynomial this may have caused a bug.
The other problem here is that we need to deal with a square matrix, that means that there is no point in taking a big number of different τ, which was the strategy we adopted before; in this case, we consider only $(l+1)^2 - 1$ values of τ at each time.
We already explain why this method is stabler than the computations of a kernel, even with a LLL algorithm. However, it needs a quite good precision to work; to find the result for $l = 7$, we needed again a precision of 200 digits.

```
1  affinesist(M, l)={
2  /*Here we want to deal with the matrix as with an affine
       system; that means, we need to separate a single
     column from the matrix and to deal with it as column
     of solutions. The strategy here is, even if we don't
     know the coefficient concerning that particular
     column, we set it to be one, and we look for the
     other coefficients that could possibly be rational
     quantities, and not integers any more. We have to be
     very careful in choosing the column we want to
     specify, as we have to choose a column whose
     coefficient should not be 0; to be sure of it, we
     choose the term of highest degree in just one
     variable. We compute then the correspondent column,
     we extract it from the matrix and we fill the
     correspondent column with 0s; this gives us an affine
       system, whose solution is the column of coefficients
       we are looking for. */
3  my(A, x, s,d, L,m);
4  d=length(M);/*We need this information, as we want to
     extract a square submatrix in order to solve the
     system */
5  L=l+1;/*this is the complexive degree of the polynomial
     we are looking for*/
6  m=2^((L+1)*L);
7  s=vecextract(M, m);
8  A=vecextract(M, 2^(d-1)-1, 2^d-1-m);
9  s=vecextract(s~, 2^(d-1)-1)~;
10 x=matsolve(A, -s);
11 x}
```

4.2.3 Evaluation-interpolation

We wanted here to exploit the same technique of evaluation-interpolation to get the modular polynomials for the theta functions; in the computations of the ϑ functions polynomials the computation time is consistent, so it could be worth approaching the computations this way in order to spare time.
We tried to adapt the same code we had for j-invariants; the difference here is in the choice of the group for the matrices M which have to act on our ϑ functions. The modular group now it is not any more ${}_{\Gamma^0(l)}\backslash^{\Gamma}$ but the group ${}_{\Gamma^0(l)\cap\Gamma(8)}\backslash^{\Gamma(8)}$, as we saw in the preceding chapter. So we have to think about a method to produce the representatives of this group.
We consider left cosets; we have to compute the coset correspondent to any element of the group ${}_{\Gamma^0(l)}\backslash^{\Gamma}$, so elements $G \circ M \in \Gamma(8)$, for $M \in \Gamma^0(l)$ and G in ${}_{\Gamma^0(l)}\backslash^{\Gamma}$.
We compute first the element coming form the action of S; we need a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $S \circ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} -b & a \\ -d & c \end{smallmatrix}\right) \in \Gamma(8)$ and acting like S, that means $ad - bc = 1$ and $-b \equiv 1 (\mathrm{mod}\ 8)$, $c \equiv 1 (\mathrm{mod}\ 8)$, $8 \mid a$, $8 \mid -d$. More, we have that $M \in \Gamma^0(l)$, so $l \mid b$. We can express our elements as $a = 8a'$, $d = 8d'$, $b = -1 + 8b' = kl$, $c = 1 + 8c'$.
Thanks to the Chinese Remainder Theorem we can compute the values of b, b'; the relation we have on the determinant becomes

$$16a'd' - (-1 - 8c' + 8b' + 16c'b') = 1,$$

that means $8(a'd' - c'b') = b' - c'$; so $c' - 8c'b' \equiv b' (\mathrm{mod}\ 8)$, that is to say $c' \equiv \frac{b'}{1-8b'} (\mathrm{mod}\ 8)$, that allows us to choose a suitable c' and to compute a', d' from it, obtaining the exact values for the entries of M. Here is the complete code:

```
1  inverse(l)=
2  {
3  /* Creates the modular correspondent for the matrix S in
       the group Gamma, that is to say our analogue to the
     operation of taking the inverse with opposite sign */
4  my(d, c, A, L, s);
5  A=[-1,0;1,0];
6  L=[8,1]~;
7  s=[1,0]~;
8  b=component(lift(matsolvemod(A, L,s)), 1);
9  c=(b+1)+1;
10 a=c-1;
11 d=c-1;
12 [c, d; -a, -b]
```

```
13 }
```

In the code above, we see that at the line 8 we do not use the simplest formulation possible; indeed, we could have used an extended Euclidean algorithm to obtain the same result.
By performing the same kind of computations over the power of T we get that they simply act as translations. In fact, we need matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $T^n \circ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(8)$. By imposing as above that our starting matrix should belong to $\Gamma^0(l)$ and that its determinant should be 1, we obtain the relations[3]

$$\begin{cases} a + nc \equiv 1 \pmod 8 \\ b + nd \equiv 0 \pmod 8 \\ c \equiv 0 \pmod 8 \\ d \equiv 1 \pmod 8. \end{cases}$$

We see that a possible solution is $a = 1 = d$, $c = 0$, $b = nl + 8l$, which correspond to translations; this is the corresponding code:

```
1  translation(l, n)={
2  /*creates the modular correspondent for the matrix T^n
       in the group Gamma(8), that is to say the analogue to
        the operation of taking the translation*/
3  my(d, c,b, a, A, L, s);
4  A=[1,0;1,0];
5  L=[8,1]~;
6  s=[n,0]~;
7  b=component(lift(matsolvemod(A, L,s)), 1);
8
9  c=0;
10 a=1;
11 d=1;
12 [a+n*c, b+n*d; c, d]
13 }
```

As we are looking for representatives for cosets, all computations are easier if we consider as representatives translations whose module is a multiple of 8. Analogous results for the group ${}_{\Gamma(l)\cap\Gamma(48)}\backslash^{\Gamma(48)}$ are presented in [Eng09]. Exploiting these results in the final code we have:

```
1  polinter1q(W, l)={
```

[3]Remember that $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & \alpha+\beta \\ 0 & 1 \end{smallmatrix}\right)$, that is equivalent to say that the composition of two translations gives as result the translation whose module is the sum of the module of the two; in our case, we simply denote $T^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$.

```
2  /*Here we try to adapt the same procedure we used for
       modular polynomials for j-invariants: */
3  my(GW, d, kt, i, sist, val, tW, P);
4  d=length(W);
5  /*W=vecextract(W, 2^(d+1)-1);*/
6  GW=matrix(l+1,d);
7  for(i=1, d,
8     GW[1,i]=thetaconstants(act(inverse(l), W[i])/l)[3];
9     for(kt=1, l,
10       GW[kt+1,i]=thetaconstants((W[i]+(kt-1)*8)/l)[3]
11    )
12 );
13 sist=vector(d, k, prod(i=1, l+1, Z-GW[i, k]));
14 val=matrix(d, l+1  , x, y, polcoeff(sist[x],y-1));
15
16 tW=vector(d, k, thetaconstants(W[k])[3]);
17 P=Z^(l+1)+sum(i=0, l, polinterpolate(tW, val[ ,i+1]~, X)
       *Z^i);
18 P
19 }
```

This method, being more stable, enabled us to compute relatively fast polynomials for higher degree of isogeny:

$$\begin{aligned} l = 11 : {} & Y^{12} + (-1024X^{11} + 140X^7 - 396X^3)Y^{11} + (-5632X^{10} + \\ & + 4400X^6 + 1298X^2)Y^{10} + (-16192X^9 + 16368X^5 - 396X)Y^9 + \\ & + (-18656X^8 + 19151X^4)Y^8 + (1408X^{11} - 18568X^7 + \\ & + 16368X^3)Y^7 + (4400X^{10} - 7876X^6 + 4400X^2)Y^6 + \\ & + (16368X^9 - 18568X^5 + 1408X)Y^5 + (19151X^8 - 18656X^4)Y^4 + \\ & + (-396X^{11} + 16368X^7 - 16192X^3)Y^3 + (1298X^{10} + 4400X^6 - \\ & - 5632X^2)Y^2 + (-396X^9 + 1408X^5 - 1024X)Y + X^{12}; \end{aligned}$$

$$\begin{aligned} l = 13 : {} & Y^{14} + (-4096X^{13} + 6656X^9 - 2704X^5 + 130X)Y^{13} + \\ & + (-26624X^{10} + 21632X^6 + 5083X^2)Z^{12} + (-66560X^{11} + \\ & + 4160X^7 + 62036X^3)Y^{11} + (-26624X^{12} - 168064X^8 + \\ & + 195689X^4)Y^{10} + (6656X^{13} - 295776X^9 + 289822X^5 - \\ & - 2704X)Y^9 + (-168064X^{10} + 149435X^6 + 21632X^2)Y^8 + \\ & + (4160X^{11} - 11752X^7 + 4160X^3)Y^7 + (21632X^{12} + \\ & + 149435X^8 - 168064X^4)Y^6 + (-2704X^{13} + 289822X^9 - \end{aligned}$$

$$
\begin{aligned}
&- 295776X^5 + 6656X)^5 + (195689X^{10} - 168064X^6 - \\
&- 26624X^2)Y^4 + (62036X^{11} + 4160X^7 - 66560X^3)Y^3 + \\
&+ (5083X^12 + 21632X^8 - 26624X^4)Y^2 + (130X^{13} - 2704X^9 + \\
&+ 6656X^5 - 4096X)Y + X^{14}
\end{aligned}
$$

$$
\begin{aligned}
l = 17 : \; & Y^{18} + (-65536X^{17} + 139264X^{13} - 91392X^9 + 17952X^5 - \\
&- 306X)Y^{17} + (835584X^{14} - 2067200X^{10} + 1203328X^6 + \\
&+ 28441X^2)Y^{16} + (2506752X^{15} - 10000896X^{11} + 8287296X^7 - \\
&- 793968X^3)Y^{15} + (835584X^{16} - 15131904X^{12} + 12179072X^8 + \\
&+ 2120308X^4)Y^{14} + (139264X^{17} - 21176832X^{13} + 8712160X^9 + \\
&+ 12298888X^5 + 17952X)Y^{13} + (-15131904X^{14} - 19510016X^{10} + \\
&+ 33457156X^6 + 1203328X^2)Y^{12} + (-10000896X^{15} - \\
&- 26236032X^{11} + 27917808X^7 + 8287296X^3)Y^{11} + \\
&+ (-2067200X^{16} - 19510016X^{12} + 9441902X^8 + \\
&+ 12179072X^4)Y^{10} + (-91392X^{17} + 8712160X^{13} - 17290156X^9 + \\
&+ 8712160X^5 - 91392X)Y^9 + (12179072X^{14} + 9441902X^{10} - \\
&- 19510016X^6 - 2067200X^2)Y^8 + (8287296X^{15} + 27917808X^{11} - \\
&- 26236032X^7 - 10000896X^3)Y^7 + (1203328X^{16} + 33457156X^{12} - \\
&- 19510016X^8 - 15131904X^4)Y^6 + (17952X^{17} + 12298888X^{13} + \\
&+ 8712160X^9 - 21176832X^5 + 139264X)Y^5 + (2120308X^{14} \\
&+ 12179072X^{10} - 15131904X^6 + 835584X^2)Y^4 + (-793968X^{15} + \\
&+ 8287296X^{11} - 10000896X^7 + 2506752X^3)Y^3 + (28441X^{16} + \\
&+ 1203328X^{12} - 2067200X^8 + 835584X^4)Y^2 + (-306X^{17} + \\
&+ 17952X^{13} - 91392X^9 + 139264X^5 - 65536X)Y + X^{18}
\end{aligned}
$$

4.3 Considerations

By looking at the polynomials above, we can immediately see that our remark about the ϑ polynomials for $l = 3, 5, 7$ are confirmed by the further examples displayed here. Indeed, they are symmetric both in X, Y and in $X \mapsto \frac{1}{X}$, $Y \mapsto \frac{1}{Y}$, they are monic and they have degree $l + 1$.
Moreover, it is self-evident that the polynomials we obtain by means of ϑ functions are more practical to deal with, as their coefficients are significantly smaller. We would like to estimate the rate of their size decrease, and in particular to show that they fit the bound of being twenty-four times smaller that we set in the last chapter.

The following table allows us to better visualise the situation: we display here the number of bits occupied by the biggest coefficient for classical and theta functions modular polynomials respectively; in the last column we put an approximate value for the ratio between these quantities, expressing the gain we have in terms of size. We see immediately that this quantity is never less than 24, on the contrary tends apparently to be even bigger.

	Classical polynomials	Theta polynomials	Ratio
$l = 3$	71	3	24
$l = 5$	157	5	31
$l = 7$	220	8	27
$l = 11$	421	15	28
$l = 13$	496	19	26
$l = 17$	705	25	28

It is immediate the advantage of having smaller coefficients when performing the algorithms above; the parameter n, so the number of binary digits considered when performing computations, is twenty-four times smaller. In any case, it is clear that for any application the fact of dealing with smaller polynomials is a big advantage, and a factor 24 is not a negligible one when considering high isogeny levels.
Moreover, this way of building modular polynomials can be easily generalised to higher genus computations; modular polynomials are in fact really hard to retrieve when considering traditional invariants over higher genus varieties.
We would like to point out a last consideration about the precision we used doing computations. Indeed, to get some results with all the kernel methods we need a relatively high precision, as we already mentioned all along this chapter.
If we choose to proceed by the evaluation-interpolation method, instead, we can gain something in terms of precision. In this case, indeed, we do not need a big number of values for τ any more; it is enough to consider just the values that allow us to interpolate (that is to say, $l + 2$ values as we know that the maximal degree is $l + 1$), retrieving the polynomials a_i from the coefficients.
In this case, the number of values τ we need increases as l increases; so, when l is relatively small we do not need a high precision, because we are performing interpolation on a low number of values. It is self-evident that, as l increases, we have to interpolate on a higher number of τ, so we need a higher precision. This in principle allow us to predict which is the precision at which we have to perform the computations; heuristically, a function linear in l gives good values for the precision.

This simplifies remarkably computations for high isogenies levels, as we could work at a relatively low precision and get the right result all the same, which is no more true when using the kernel method. So, the evaluation-interpolation method reveals itself to be better not only on the side of the computation of complexity, but also on the precision side.

Chapter 5

Perspectives: genus 2

In this section, we will try to give a short overview of the situation in genus 2. We will try to explain how to extend the notions we presented for genus 1 such as modular polynomials and ϑ functions, and we will present the computations we did.
Our discussion here does not want to be more than a general overview; we will not give proofs for theorems and propositions we will state here. We suggest to refer to [Mum83] for a complete discussion about ϑ functions in general variables, and to [BGL11] or to [BL04] for a discussion about invariants for complex surfaces in genus 2.

5.1 Theta functions

We seek a generalisation of the function $\vartheta(z, \tau)$ in dimension 2, where $z \in \mathbb{C}$ should be replaced by a pair $\bar{z} = \binom{z_1}{z_2} \in \mathbb{C}^2$ and which should be quasi-periodic with respect to a lattice L where $L \in \mathbb{C}^2$. It is not obvious what should be the analogue of τ in an higher dimension, but it turns out to be a 2×2 symmetric complex matrix Ω whose imaginary part is positive definite. Let $\mathcal{H}_2$ be the set of such matrices; it is then a subset in $\mathbb{C}^3$, called the **Siegel upper half-space**. We define our ϑ function to be

$$\vartheta(\bar{z}, \Omega) = \sum_{\bar{n} \in \mathbb{Z}^2} e^{\pi \imath^t \bar{n} \Omega \bar{n} + 2\pi \imath^t \bar{n} \cdot \bar{z}}.$$

This definition gives a convergent series provided we choose Ω to be in $\mathcal{H}_2$.

5.1.1 Theta constants with rational characteristic

As in genus 1, to any Ω we can associate a lattice $L_\Omega = \mathbb{Z}^2 + \Omega\mathbb{Z}^2 \subset \mathbb{C}^2$, id est the lattice generated by the unit vectors and the columns of Ω. The

basic property of ϑ is to be quasi-periodic for the transformation $z \mapsto z + a$, $a \in L_\Omega$, that is to say, periodic up to a multiplicative factor; what we have is $\vartheta(\bar{z} + \bar{m}, \Omega) = \vartheta(\bar{z}, \Omega)$, $\vartheta(\bar{z} + \Omega\bar{m}, \Omega) = e^{-\pi\imath^t\bar{m}\Omega\bar{m} - 2\pi\imath^t\bar{m}z}\vartheta(\bar{z}, \Omega)$ for any $\bar{m} \in \mathbb{Z}^2$. As in genus 1, ϑ is the simplest function we can find enjoying this property: if $f(\bar{z})$ is an entire function such that $f(\bar{z} + \bar{m}) = f(\bar{z})$, $f(\bar{z} + \Omega\bar{m}) = e^{-\pi\imath^t\bar{m}\Omega\bar{m} - 2\pi\imath^t\bar{m}\bar{z}}f(z)$, then $f(\bar{z}) = k \cdot \vartheta(\bar{z}, \Omega)$, where k is a constant term.
We can slightly generalise this concept:

Definition 5.1.1. *Fix $\Omega \in \mathcal{H}_2$. Then an entire function $f(\bar{z})$ on $\mathbb{C}^2$ is L_Ω-**quasi-periodic** of weight l if*

$$f(\bar{z} + \bar{m}) = f(\bar{z})$$

and

$$f(\bar{z} + \Omega\bar{m}) = e^{-\pi\imath l\cdot^t\bar{m}\Omega\bar{m} - 2\pi\imath l\cdot^t\bar{z}\bar{m}}f(\bar{z})$$

for all $\bar{m} \in \mathbb{Z}^2$. We call $\mathcal{R}_l^\Omega$ the space of such functions.

As in genus 1, one of the applications of such functions is to define holomorphic maps from the torus $\frac{\mathbb{C}^2}{L_\Omega}$ to the projective space. In fact, if we consider L_Ω-quasi-periodic functions $f_0, \ldots, f_n$ of the same weight l with the property that at every $\bar{a} \in \mathbb{C}^2$, $f_i(\bar{a}) \neq 0$ for at least one i, then we have a well defined holomorphic map

$$\begin{array}{ccc} \frac{\mathbb{C}^2}{L_\Omega} & \to & \mathbb{P}^n \\ \bar{z} & \mapsto & [f_0(\bar{z}) : \cdots : f_n(\bar{z})]. \end{array}$$

A basis for the space $\mathcal{R}_l^\Omega$ can be found by means of a slight generalisation of **theta functions with characteristic**, which are in fact nothing more than translated of ϑ multiplied by an elementary exponential factor:

$$\vartheta_{a,b}(z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{i\pi^t(n+a)\Omega(n+a) + 2i\pi^t(z+b)(n+a)},$$

that is to say

$$\vartheta_{a,b}(z, \Omega) = e^{\pi\imath^t\bar{a}\Omega\bar{a} + 2\pi\imath^t\bar{a}(\bar{z}+\bar{b})}\vartheta(\bar{z} + \Omega\bar{a} + \bar{b}, \Omega)$$

for any $\bar{a}, \bar{b} \in \mathbb{Q}^2$.
We can easily see that $\vartheta = \vartheta_{0,0}$, and that integral vectors hardly modify our original function: $\vartheta_{\bar{a}+\bar{n},\bar{b}+\bar{m}}(\bar{z}, \Omega) = e^{2\pi\imath^t\bar{a}\bar{m}}\vartheta_{\bar{a},\bar{b}}$ for any $\bar{m}, \bar{n} \in \mathbb{Z}^2$. Finally, the quasi-periodicity of $\vartheta_{\bar{a},\bar{b}}$ is given by $\vartheta_{\bar{a},\bar{b}}(\bar{z} + \bar{m}, \Omega) = e^{2\pi\imath^t\bar{a}\bar{m}}\vartheta_{\bar{a},\bar{b}}(\bar{z}, \Omega)$, $\vartheta_{\bar{a},\bar{b}}(\bar{z} + \Omega\bar{m}, \Omega) = e^{-2\pi\imath^t\bar{b}\bar{m} - \pi\imath^t\bar{m}\Omega\bar{m} - 2\pi\imath^t\bar{m}\bar{z}}\vartheta_{\bar{a},\bar{b}}(\bar{z}, \Omega)$, that means, the quasi-periodicity is ruled by the same law that holds for $\vartheta_{0,0}$, except for a root of unity. We then have:

Proposition 5.1.2. *Fix $\Omega \in \mathcal{H}_2$. Then a basis of $\mathcal{R}_l^\Omega$ is given by either*

- $f_{\bar{a}}(\bar{z}) = \vartheta_{\frac{\bar{a}}{l},0}(l\bar{z}, l\Omega)$, *for* $0 \leq a_i < l$;
- $g_{\bar{b}}(\bar{z}) = \vartheta_{0,\frac{\bar{b}}{l}}(\overrightarrow{z}, \frac{1}{l}\Omega)$, *for* $0 \leq b_i < l$.
- *If $l = k^2$, then we have also*

$$h_{\bar{a},\bar{b}}(\bar{z}) = \vartheta_{\frac{\bar{a}}{k},\frac{\bar{b}}{k}}(l\bar{z}, \Omega),$$

for $0 \leq a_i, b_i < k$.

These bases are related by

$$g_{\bar{b}} = \sum_{\bar{a}} e^{2\pi\imath \frac{1}{l}{}^t \bar{a}\bar{b}} f_{\bar{a}},\ h_{\bar{a},\bar{b}} = \sum_{\bar{c}\equiv\bar{a} mod\ k} e^{2\pi\imath \frac{1}{k}{}^t \bar{c}\bar{b}} f_{\bar{c}}.$$

We can then describe the embeddings we have from this construction, not only for standard tori in the form $\frac{\mathbb{C}^2}{L_\Omega}$ but also isogenous tori $\frac{\mathbb{C}^2}{L}$, L a generic lattice in $L_\Omega\mathbb{Q}$. The result we have is the following:

Proposition 5.1.3. *A complex torus $\frac{C^2}{L}$ can be embedded into some projective space if and only if $A(L) \subset \Omega\mathbb{Q}^2 + \mathbb{Q}^2$ for some 2×2 complex matrix A and some $\Omega \in \mathcal{H}_2$.*

Proves for all these assertions, as well as a complete discussion on the topic, can be found in [Mum70].

5.1.2 Theta as a modular form

We want now to consider the dependence of the function $\vartheta(\bar{z}, \Omega)$ on Ω. We have in fact, as in the 1-dimensional case, a functional equation for ϑ for the action of a subgroup $\mathrm{Sp}(4, \mathbb{Z})$ (which is to say the set of the elements γ that, modulo 2, preserve the classical scalar product, that is to say the orthogonal form

$$Q(n_1, n_2) = {}^t n_1 \cdot n_2 \in \frac{\mathbb{Z}}{2\mathbb{Z}}$$

as well as the alternating form

$$A((x_1, x_2), (y_1, y_2) = {}^t x_1 \cdot y_2 - {}^t x_2 \cdot y_1,$$

and this second condition turns in fact out to be a particular case of the first one) on both variables $\bar{z}$ and Ω, that is

$$\vartheta({}^t(C\Omega + D)^{-1}\bar{z}, (A\Omega + B)(C\Omega + D)^{-1}) = \tag{5.1}$$

$$= \zeta_\gamma \det(C\Omega + D)^{\frac{1}{2}} e^{\pi\imath {}^t\bar{z}(C\Omega+D)^{-1}C\bar{z}} \vartheta(\bar{z}, \Omega)$$

where $\zeta_\gamma^8 = 1$, $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(4, \mathbb{Z})$ satisfies the condition that the products of the diagonal elements for ${}^tAC$ and for ${}^tBD$ are even. This set form a subgroup of $\mathrm{Sp}(4, \mathbb{Z})$; we call it $\Gamma_{1,2}$. If we set

$$\Gamma_n = \{\gamma \in \mathrm{Sp}(4, \mathbb{Z}) : \gamma \equiv \mathbb{1}_4 \mathrm{mod}\ n\},$$

$\Gamma_{1,2}$ is an intermediate subgroup between Γ_2 and $\Gamma_1 = \mathrm{Sp}(4, \mathbb{Z})$, that is to say $\Gamma_2 \subset \Gamma_{1,2} \subset \Gamma_1$.
We would like now to recover some of the invariance properties we had in genus 1; for doing this, we work directly on the functional equation above, and we set $\vartheta^\alpha_{n_1,n_2}(\Omega) = e^{\pi\imath {}^t n_1 \Omega n_1 + \pi\imath {}^t n_1 n_2} \vartheta(\Omega n_1 + n_2, \Omega)$. Then we have the following

Proposition 5.1.4. *Let* $\mathrm{Sp}(4, \mathbb{Z})$ *act as follows:*

- *On* $\mathbb{Z}^4$ *by* $(n_1, n_2) \mapsto (Dn_1 - Cn_2, -B_1 + An_2)$*;*
- *On* $\mathcal{H}_2$ *by* $\Omega \mapsto (A\Omega + B)(C\Omega + D)^{-1}$*;*
- *On* $\mathbb{C}^2$ *by* $\overrightarrow{z} \mapsto^t (C\Omega + D)^{-1}\overrightarrow{z}$*.*

Then the functional equation for ϑ (5.1) *asserts that, up to an 8-th root of unity,* $\vartheta^\alpha_{n_1,n_2}(\Omega)\sqrt{dz_1 \wedge \cdots \wedge dz_4}$ *is invariant under* $\Gamma_{1,2} \subset \mathrm{Sp}(4, \mathbb{Z})$*.*

A useful corollary is the following:

Corollary 5.1.5. *If* $\gamma \in \Gamma_4$*, id est* $\gamma \equiv \mathbb{1}_4 (mod\ 4)$*, then in the functional equation* (5.1) $\zeta = \pm 1$*.*

We can generalise to a higher dimension the concept of modular form we already introduced in genus 1:

Definition 5.1.6. *Let* $\Gamma \subset \mathrm{Sp}(4, \mathbb{Z})$ *be a subgroup of finite index. Then a* ***modular form*** *of weight* k *and level* Γ *is a holomorphic function* f *defined on the Siegel upper half-plane* $\mathcal{H}_2$ *such that, for all* $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ *we have* $f((A\Omega + B)(C\Omega + D)^{-1}) = \det(C\Omega + D)^k f(\Omega)$*.*

Note that here the hypothesis we needed in genus 1 to set the behaviour at the cusps is no more needed. In fact, the boundedness is ensured by the Koecher principle (see [Mum83, page 198]).
If $\Gamma = \Gamma_n$, then f is said to be a **modular form of level** n. In fact, it can be shown that any Γ contains some subgroup Γ_n for some n, so a modular form of level Γ is a modular form of level n for some n. The functional equation for ϑ states that $\vartheta(0, \Omega)^2$ is a modular form of level 1 and weight 4.

More precisely, we can introduce the so-called **intermediate levels** $(n, 2n)$ by setting

$$\Gamma_{2n} \subset \Gamma_{n,2n} \subset \Gamma_n$$

where n is assumed to be even and $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_{n,2n}$ if $\gamma \equiv \mathbb{1}_4 (\text{mod } n)$ and $2n$ divides the diagonals of B and C; then we prove:

Proposition 5.1.7. *Let n be even. Then for all $n_1, n_2, m_1, m_2 \in \frac{1}{n}\mathbb{Z}^2$,*

$$\vartheta_{n_1,n_2}(0,\Omega)\vartheta_{m_1,m_2}(0,\Omega)$$

is a modular form of weight 1 and level $(n^2, 2n^2)$.

Geometrically, we can proceed as in genus 1, and define a holomorphic map:

$$\begin{array}{ccc} \frac{\mathcal{H}_2}{\Gamma_{n^2,2n^2}} & \to & \mathbb{P}^{N-1} \\ \Omega & \mapsto & [\cdots : \vartheta_{n_1^i,n_2^i}(0,\Omega)\vartheta_{m_1^i,m_2^i}(0,\Omega) : \dots] \end{array}$$

where N is given by the number of pairs $\left[\begin{smallmatrix} n_1^i \\ n_2^i \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} m_1^i \\ m_2^i \end{smallmatrix}\right]$ we have to consider in a system of coset representatives of $\frac{\frac{1}{n}\mathbb{Z}^2}{\mathbb{Z}^2}$. This gives an isomorphism of the analytic space $\frac{\mathcal{H}_2}{\Gamma_{n^2,2n^2}}$ with a quasi-projective variety, that means a subset of $\mathbb{P}^{N-1}$ defined by a polynomial variety minus a smaller set of the same type (that is to say, the algebraic set that makes the ϑ functions vanish).
We can do even better; if we extend the definition of modular forms to half-integral weights we can express modularity in terms of a single ϑ function. Namely:

Definition 5.1.8. *Let $\Gamma \subset \Gamma_{1,2}$ be a subgroup of finite index. Then a modular form f of weight $k \in \frac{1}{2}\mathbb{Z}$ and level Γ is a holomorphic function f on $\mathcal{H}_2$ such that $\frac{f((A\Omega+B)(C\Omega+D)^{-1}}{\vartheta_{0,0}((A\Omega+B)(C\Omega+D)^{-1})^{2k}} = \frac{f(\Omega}{\vartheta_{0,0}(\Omega)}$ for all $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$.*

With this definition, we can extend Proposition 5.1.7 as follows:

Proposition 5.1.9. *For all $n_1, n_2 \in \mathbb{Q}^2$, $l \in \mathbb{N}$, $\vartheta_{n_1^i,n_2^i}(0, l\Omega)$ is a modular form of weight $\frac{1}{2}$ for a suitable level Γ.*

All these tools will enable us to extend computations we did in genus 1 to the case of genus 2; that will be our aim in the final part of this chapter.
The following section will be devoted to an analysis of the Igusa invariants, which could be considered the analogue of the j-invariant for genus 2; we will see that in the genus 2 case the considerations we had in genus 1 about the polynomial size are even more important than before.

5.2 Igusa invariants

Before starting computations with ϑ functions by applying the strategies we presented in the past chapter, we would like to try to understand why in genus 2 computations by means of ϑ functions turn out to be even more convenient than in case of genus 1.
The immediate generalisation of the case we dealt with in the previous chapters is a surface on the form

$$A_\Omega = \frac{\mathbb{C}^2}{\mathbb{Z}^2 + \Omega\mathbb{Z}^2},$$

$\Omega \in \mathcal{H}_2$;[1] these are the so-called **principally polarised abelian surfaces**, whose moduli space is denoted by $\mathcal{A}_2$.
In fact here we consider the subspace $\mathcal{M}_2 \subset \mathcal{A}_2$, the space of Jacobians of curves. We can describe the elements of this space by means of equations of the form $Y^2 = a_6X^6 + \cdots + a_0 = f(X)$, which are in fact equations which describe genus 2 curves; if $\alpha_1, \ldots, \alpha_6$ are the roots of f, we denote $(ij) = (\alpha_{k_i} - \alpha_{k_j})$ for a given ordering of the roots. Then, following [Igu60], we define the **Igusa-Clebsch invariants** by

$$\begin{aligned}
I_2 =& a_6^2 \sum_{15} (12)^2(34)^2(56)^2 \\
I_4 =& a_6^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \\
I_6 =& a_6^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \\
I_{10} =& a_6^{10} \sum_{i<j} (ij) = a_6^{10} \operatorname{disc}(f)
\end{aligned}$$

where we sum over all root orderings $\{\alpha_{k_i}\}$ that give distinct summands (in the definition of I_2, I_4 and I_6 we specify the number of terms we take into account in that sum). This definition gives rise to a subspace of the weighted projective space $\mathbb{P}^3_w(\mathbb{C})$ with weights 2, 4, 6, 10

$$\left\{[I_2 : I_4 : I_6 : I_{10}] \in \mathbb{P}^3_w(\mathbb{C}) : I_{10} \neq 0\right\}$$

which is isomorphic to $\mathcal{M}_2$ (see [Igu60] for a proof of this). We remark that the condition $I_{10} \neq 0$ ensures that the polynomial f defining the genus 2 curve is separable.

[1] Which is in fact the case we had also in the previous chapter, and by means of what we learned how to compute ϑ functions.

The most common convention is to work not with this weighted projective space, but with a non-weighted affine subspace of it, namely

$$(j_1, j_2, j_3) = \left(\frac{I_2^5}{I_{10}}, \frac{I_4 I_2^3}{I_{10}}, \frac{I_6 I_2^2}{I_{10}} \right);$$

these are the so-called **Igusa invariants**. They are frequently compared to the classical j invariant in dimension 1, as they have the property that for Ω, Ω' corresponding to Jacobians of curves, the equalities $j_i(\tau) = j_i(\tau') \neq 0$ for $i = 1, 2, 3$ imply that our objects are isomorphic.
In [Dup06] we can find detailed computations about these invariants and some examples of the modular polynomials they give. They are not at all practice to deal with; they have been computed only for $l = 2$, they are rational functions and, simply by stocking the numerators for $l = 2$, they fill 26.8 Mo of space!
Again, as in case of genus 1, we have formulae similar to (3.10) linking Igusa invariants to ϑ functions (see [Igu67, pag. 848] for a proof of this). Again, we look for some polynomial relations built by means of ϑ functions, hoping to find relations with smaller coefficients.

5.3 Computations

In this section, we will try to explain how to proceed to generalise the computations of the previous chapter relative to ϑ functions to the case of genus 2. First of all, we notice that here computations become far more difficult than before; we are working in a dimension 3 space, so we need at least three invariants to identify the object we are working with. In fact, if we think about it, even when considering Igusa invariants we consider the value of three distinct functions to determine a single object; we would like to reduce to this case even when working with ϑ.
The problem here is that we do not have anything similar to Lemma 3.2.1; we start with the usual four ϑ constants built as in case of genus 1, but now none of them is constantly 0 when evaluated in $z = 0$. This could be dangerous if one wants to restrict to the affine case; we do not have any way to check if a function gets the value 0, a thing that can very well happen here. So we have no way to be sure that the process of passing from the projective to the affine space is well defined; we have no way to check if we are dividing out by 0. So, we have to carry the four ϑ functions all along the computations.
Moreover, from a strict computational point of view, we have problems even when evaluating ϑ constants, as even the simple evaluation requires around a minute to be performed at a relatively low precision (ten digits computed).

In the rest of this chapter, we are going to detail our computations and to explain the methods we follow.

5.3.1 Computation of ϑ constants

We apply the same reasoning as before; we need here four different theta constants, that is to say $\vartheta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (0, \Omega)$, $\vartheta \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix} (0, \Omega)$, $\vartheta \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} (0, \Omega)$, $\vartheta \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} (0, \Omega)$, where here Ω is a square matrix of dimension 2, and we interpret a and b as row vectors. In fact, with this choice, we have that the vector a is always the 0-vector; what we definitely have to compute is

$$\vartheta_{0,b}(0, \Omega) = \sum_{n \in \mathbb{Z}^2} e^{i\pi {}^t n \Omega n + 2i\pi {}^t b n}.$$

Again, as in the case of genus 1, we can simplify this expression by remarking that $e^{i\pi} = -1$, so we are dealing with alternating sums involving always the same terms, where the sign for each term depends only on the value of b. If we consider $\Omega = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix}$, matrix with complex entries, we have

$${}^t n \Omega n = \tau_1 n_1^2 + 2\tau_2 n_1 n_2 + \tau_3 n_2^2,$$

where $n = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$. So if we compute $q_j = e^{i\pi\tau_j}$, our sum turns out to be

$$\sum_{n \in \mathbb{Z}^2} q_1^{n_1^2} q_2^{2n_1 n_2} q_3^{n_2^2} ((-1)^{{}^t(2b)n}).$$

Here we cannot proceed as before, reducing our sum over natural numbers; what we can do is to implement the sum over half the values of the lattice instead of taking the whole lattice $\mathbb{Z}^2$, by remarking that vectors with the same values and opposite signs actually give the same value to add (so we can pair them, and just add twice each value coming from an element taken in the half lattice).

```
1 theta2(M, k)=
2 /*Given a matrix and a given precision, this function
     computes the theta constants in genus 2 evaluated at
     that matrix */
3 {
4 my(Theta, q1, q2, q3, n, p, n1, n2, s, t1, t2, t3, a, b,
      e, m, v);
```

```
5  t1=M[1,1];
6  t2=M[1,2];
7  t3=M[2,2];
8  Theta=vector(4, k,1);
9  q1=exp(Pi*I*t1);
10 q2=exp(Pi*I*t2);
11 q3=exp(Pi*I*t3);
12 n=1;
13 p=0;
14 v=vector(10^k, i, i^2);
15 m=matrix(10^k, 10^k, i, j, 2*i*j);
16 while(abs(Theta[1]-p)>10^(-k),
17                          p=Theta[1];
18                          n1=n;
19                          for(n2 = -n, n,
20                                  a=abs(n1); b=abs(n2); if
                                       (n1*n2>0, e=1;e=-1);
21                                  s=q1^(v[a])*q2^(e*m[a, b
                                       ])*q3^(v[b]);
22                                  Theta[1]=Theta[1]+s;
23                                  Theta[2]=Theta[2]+(-1)^
                                       n1*s;
24                                  Theta[3]=Theta[3]+(-1)^
                                       n2*s;
25                                  Theta[4]=Theta[4]+(-1)^(
                                       n1+n2)*s;
26                                  );
27                          n1=-n;
28                          for(n2 = -n, n,
29                                  a=abs(n1);b=abs(n2);if(
                                       n1*n2>0, e=1;e=-1);
30                                  s=q1^(v[a])*q2^(e*m[a,b
                                       ])*q3^(v[b]);
31                                  Theta[1]=Theta[1]+s;
32                                  Theta[2]=Theta[2]+(-1)^
                                       n1*s;
33                                  Theta[3]=Theta[3]+(-1)^
                                       n2*s;
34                                  Theta[4]=Theta[4]+(-1)^(
                                       n1+n2)*s;
35                                  );
36                          n2=n;
37                          for(n1 = -n+1, n-1,
```

```
38                                  a=abs(n1);b=abs(n2); if(
                                       n1*n2>0, e=1;e=-1);
39                                  s=q1^(v[a])*q2^(e*m[a,b
                                       ])*q3^(v[b]);
40                                  Theta[1]=Theta[1]+s;
41                                  Theta[2]=Theta[2]+(-1)^
                                       n1*s;
42                                  Theta[3]=Theta[3]+(-1)^
                                       n2*s;
43                                  Theta[4]=Theta[4]+(-1)^(
                                       n1+n2)*s;
44                                  );
45                          n2=-n;
46                          for(n1 = -n+1, n-1,
47                                  a=abs(n1);b=abs(n2); if(
                                       n1*n2>0, e=1;e=-1);

                                       s=q1^(v[a])*q2^(e*m[a
                                       ,b])*q3^(v[b]);
48                                  Theta[1]=Theta[1]+s;
49                                  Theta[2]=Theta[2]+(-1)^
                                       n1*s;
50                                  Theta[3]=Theta[3]+(-1)^
                                       n2*s;
51                                  Theta[4]=Theta[4]+(-1)^(
                                       n1+n2)*s;
52                                  );
53                                          n=n+1);
54  Theta
55  }
56  /*At the end, Theta is a vector containing the 4 values
       for the theta functions at that matrix. To be well
       defined , the theta functions must be invoked on
       matrixes whose imaginary part should be positive. */
```

5.3.2 Looking for modular polynomials

After having defined our new ϑ functions, we try to compute now polynomial relations. As we said, we had a priori four ϑ constants to consider, that reduced to three variables when passing from a projective perspective to an affine one. In genus 2, though, the landscape is more complicated than in genus 1; we may have abelian varieties defined not only as Jacobians of

hyperelliptic curves, but also as product of elliptic curves, so of two curves of genus 1.
This is the dangerous case, the case at which the ϑ functions may vanish. In fact, this is a critical case even when considering Igusa invariants; in this case, in fact, the I_{10} defined above vanish, making the definitions of Igusa invariants fail. Coming back to ϑ functions, we can solve this problem by means of quotients. In fact, once we choose the ϑ constant which we want to divide out to get an affine space from the projective one, we start by subtracting from the domain all the values of Ω that make this constant vanish; but still, this is not enough. The same problem may in fact arise when considering isogenous curves; we have to be sure that the ϑ constant does not vanish on them. So what we need is to quotient our domain by the equation describing the locus of Ω linked by an isogeny to a matrix that makes our ϑ constant vanish.
This prevents us from looking for a single polynomial; we have to look for rational functions, that is to look for a denominator and a numerator separately. Moreover, in this case we have no conditions on the coefficients; a priori we are looking for coefficients in $\mathbb{C}$.
We see immediately that the evaluation-interpolation method becomes really hard to apply; we need to compute a set of representatives for the modular group, which cannot be described in an easy way as in genus 1. After having computed them, though, we have to cope with another problem: we are not dealing with polynomials any more, but with rational functions, so the interpolation phase we have to perform on coefficients obtained from the evaluation phase cannot be carried on in a simple way any more.
We tried to perform the other method, that is to build the big matrix containing all the evaluated monomials and to work with it in order to compute its kernel; a priori, we have to consider eight variables, which makes a considerable number of monomials to take into account even for low degrees.
Just to start with and to test complexity and time of calculus, we build a matrix involving only five different variables instead of eight; luckily, we could hope to find a relation involving just the five of them, and in any case it was a good test to understand if our generalisation could really be performed in that simple way. Our worries revealed themselves to be justified: the computations gave no result, as the calculator stacked overflow.
This is not surprising, if we consider the size of the matrix we are building and the cost of every single evaluation for a ϑ function computed in genus 2: by a rapid glance at the code above, we see that we have four cycles to repeat at each step, each of them consisting in five lines of computations; in general, the number of steps depends on the growth of the terms we add, so depends again on the particular element Ω we consider. So a good choice for

the starting elements could be a significant point in sparing some time; we can easily see, in any case, that the evaluation step is really heavy to perform in terms of computational cost.
Then we have to build the matrix, so to consider all the possible monomials; if we think for a while about it, we realise that the number of columns of this matrix is really high. Taking the most simple case, the case in which we look for relations between only five different variables, and taking a very low level for the isogeny, for example $l = 3$, we see that the number of columns we have to build is l^5, that is to say $3^5 = 243$ different columns, so we have to deal with matrices of size 243, and this could even not be enough to find something interesting!

Bibliography

[BB87] Jonathan Borwein and Peter Borwein. *Pi and the AGM, A study in Analytic Nuber Theory and Computational Complexity.* John Wiley and Sons, 1987.

[BGL11] Reiner Bröker, Davis Gruenewald, and Kristin Lauter. Explicit CM-theory for level 2-structures on abelian surfaces. *Algebra and Numbery Theory*, 5(4):495–528, 2011.

[BK93] Joseph Buchmann and Volker Kessler. Computing a reduced lattic basis from a generating system. *Preprint*, 1993.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BS10] Reiner Bröker and Andrew Sutherland. An explicit height bound for classical modular polynomials. *Ramanujan Journal*, (22):293–313, 2010.

[Coh84] Paula Cohen. On the coefficients for transformations polynomials for the elliptic modular function. *Mathematical Preecedings of the Cambridge Philosophical Society*, 95:389–402, 1984.

[Coh96] Henri Cohen. *A course in Computational Algebraic Number Theory.* Graduate Texts in Mathematics. Springer-Verlag, 1996.

[Cox84] David Cox. The arithmetic-geometric mean of Gauss. *L'Enseignement Mathématique*, 30:275–330, 1984.

[Cox89] David Cox. *Primes of the form $x^2 + ny^2$.* John Wiley and Sons, Inc., 1989.

[Dup06] Régis Dupont. *Moyenne Arithmético-géométrique, suites de Borchardt et applications.* PhD thesis, École Polythécnique, 2006.

[Elk97] Noam Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory*, 1997.

[Eng99] Andreas Enge. *Elliptic curves and their applications to cryptography, An introduction*. Kluver Academic Publishers, 1999.

[Eng09] Andreas Enge. Computing modular polynomials in quasi-linear time. *Mathematics of Computations*, 78(267):1809–1824, 2009.

[FLR11] Jean-Charles Faugère, David Lubicz, and Damien Robert. Computing modular correspondence for abelian varieties. *Journal of Algebra*, 243:248–277, 2011.

[Gal99] Steven Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999.

[Gre92] Alphred George Greenhill. *The applications of elliptic functions*. MacMillan and Co., 1892.

[Han28] M. Hanna. The modular equation. *Proc. London Math. Soc. (2) 28 (1928) 46–52.*, 2(28):46–52, 1928.

[Igu60] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72:612–649, 1960.

[Igu67] Jun-Ichi Igusa. Modular forms and projective invariants. *American Journal of Mathematics*, 89(3):817–855, 1967.

[Igu68] Jun-Ichi Igusa. On the algebraic theory of elliptic modular functions. *Journal of Mathematical Society, Japan*, 20, 1968.

[Lan76] Serge Lang. *Introduction to Modular Forms*. Graduate Texts in Mathematics. Springer-Verlag, 1976.

[Lan87] Serge Lang. *Elliptic Functions*. Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 1987.

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. PhD thesis, École Polythecnique, 1997.

[LLL82] Arjen Lenstra, Hendrik Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Matematische Annalen*, 261:515–534, 1982.

[Mah72] Kurt Mahler. On the coefficients of the 2^n-th transformation polynomial for $j(\omega)$. *Acta Arithmetica*, 21, 1972.

[Mah74] Kurt Mahler. On the coefficients for transformation polynomials for the modular functions. *Bulletin Australian Mathematical Society*, 10:197–218, 1974.

[Mil06] James Stuart Milne. *Elliptic curves*. BookSurge Publishers, 2006.

[Mil12] James Stuart Milne. Modular functions and modular forms (v1.30), 2012. Available at www.jmilne.org/math/.

[Mor95] François Morain. Calcul du nombre de points sur une curbe elliptique dans un corps fini: aspects algorithmiques. *Journal de Théorie des Nombres de Bordeaux*, pages 255–282, 1995.

[Mum66] David Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum67a] David Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[Mum67b] David Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3:215–244, 1967.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum83] David Mumford. *Tata lectures on theta I*. Birkhauser, 1983.

[Rob10] Damien Robert. *Fonctions thêta et applications à la cryptographie*. PhD thesis, Université Henri Poincaré - Nancy 1, 2010.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995.

[Ser56] Jean-Pierre Serre. Géométrie algébrique et géometrie analytique. *Annales de l'institut Fourier*, 6:1–42, 1956.

[Ser96] Jean-Pierre Serre. *A cours in arithmetic*. Graduate Texts in Mathematics. Springer-Verlag, 5th edition, 1996.

[Sho08] Victor Shoup. *A computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2nd edition, 2008.

[Sil94] Joseph Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, 1994.

[Sil09] Joseph Silverman. *The Arithmetic of Elliptic curves*. Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 2009.

[VzGG03] Joachim Von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2003.

[Was08] Lawrence Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and its applications. Chapman and Hall/CRC, 2008.