UNIVERSITÀ DEGLI STUDI DI PADOVA

Universiteit Leiden

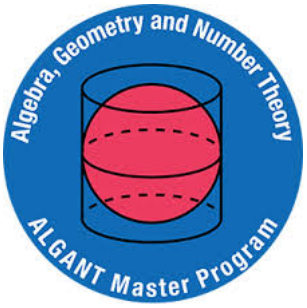
Dipartimento di Matematica "Tullio-Levi Civita"

Mathematisch Instituut

Mathematics Master course

ALGANT Master Thesis

Modular functions obtained from modular polynomials



Supervisors:
Dr. Marco Streng
Prof. Marco Garuti

Author:
Martina Fruttidoro
Student number:
1161737

---

2 July 2019
Academic Year 2018/2019

Introduction

A *modular function* is a meromorphic function on the upper half complex plane $\mathbb{H}$ which is also "meromorphic at the cusps" and invariant under the action on $\mathbb{H}$ of some matrix group Γ, called a "*congruence subgroup*". Modular functions play an essential role in number theory, for example modular forms are extensively used in the proof of Fermat's Last Theorem.

The quotient of the upper half complex plane $\mathbb{H}$ by the action of a congruence subgroup Γ gives rise to a Riemann surface $Y(\Gamma)$. We call its compactification $X(\Gamma)$ a "*modular curve*", which is obtained by adjoining to $Y(\Gamma)$ the Γ-orbits of the projective line $\mathbb{P}^1(\mathbb{Q})$: the *cusps*. The main reason of interest for the study of the modular curves is their *moduli interpretation*: the points of these curves can be used to classify elliptic curves together with some torsion data.

In 2014 Maarten Derickx and Mark van Hoeij gave upper bounds for the gonality of the modular curve $X_1(N)$ for each $N \leq 250$ using some particular functions obtained from the equation of $X_1(M)$, with M a positive integer different from N (for more details look at [3]). These functions have zeros and poles just on the cusps, therefore (as there are finitely many cusps) Derickx and van Hoeij used these special functions to make the zeros and poles cancel each other out and obtain lower degree functions on the modular curve $X_1(N)$, which they used to study its gonality. They furthermore conjectured that this kind of functions freely generate the modular units of $\mathbb{Q}(X_1(N))$, which are elements of $\mathbb{Q}(X_1(N))$ whose poles and zeros are cusps. This conjecture was proved by Marco Streng in 2015 (for reference look at [9]).

In this thesis we study the analogue of this issue for the modular curve $X_0(N)$. Given two distinct positive integers M and N, we will prove that the function on $X_0(N)$ obtained from the equation of $X_0(M)$ has zeros at complex multiplication points of the modular curve $X_0(N)$ and poles at its cusps. This disproves the analogue of the conjecture of Derickx and van Hoeij for $X_0(N)$. In particular for all positive distinct integers M and N, we study

the function f_M on the modular curve $Y_0(N)$ defined as follows:

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)), \end{aligned}$$

where $\Phi_M(X, Y) \in \mathbb{Z}[X, Y]$ is the *M-th modular polynomial*, which describes the modular curve $X_0(M)$ and j is the j-invariant. We will prove the following formula for the divisor of zeros of the function f_M:

Theorem. *Let M and N be two positive coprime integers not both squares and let*

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)). \end{aligned}$$

We have that

$$\mathrm{Div}_0(f_M) = \sum_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O})} \sum_{\{\alpha\in\mathcal{O} \,:\, \mathcal{O}/\alpha\mathcal{O}\cong\mathbb{Z}/MN\mathbb{Z}\}/\mathcal{O}^*} \left(\left[\left(\mathfrak{a}, \mathfrak{a} + \frac{\alpha}{N}\mathfrak{a}\right)\right]\right).$$

Here $\left[\left(\mathfrak{a}, \mathfrak{a} + \frac{\alpha}{N}\mathfrak{a}\right)\right]$ denotes the equivalence class under scalar complex multiplication of the pair of $\mathbb{C}$-lattices $\left(\mathfrak{a}, \mathfrak{a} + \frac{\alpha}{N}\mathfrak{a}\right)$, which corresponds to a precise point of the modular curve $Y_0(N)$ through the bijection given in Theorem 1.59.

From the theorem stated above we will derive in Chapter 3 that no non-constant product of powers of this type of functions will give rise to a modular unit of $\mathbb{Q}(X_0(N))$, since it will always have at least one zero or pole at a complex multiplication point. Finally we will give a lower bound for the degree of functions that we get multiplying and dividing by functions obtained from the modular polynomials.

Contents

Chapter 1

Prerequisites

1.1 The Riemann surface structure of the modular curve $Y(\Gamma)$

In this section we will give the basic definitions and we will show that the modular curve $Y(\Gamma)$ with the complex atlas that we will define is a Riemann surface. A reference for this section is [4, Chapter 2].

Definition 1.1. The *general linear group of degree 2*, denoted by $GL_2(\mathbb{C})$ is the group of 2×2 invertible matrices with coefficients in the complex numbers. The *modular group*, denoted by $SL_2(\mathbb{Z})$, is the subgroup of $GL_2(\mathbb{C})$ given by matrices with integer coefficients and determinant 1:

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

The group $GL_2(\mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$ by matrix-vector multiplication. Let us identify $\mathbb{C} \cup \{\infty\}$ to $\mathbb{P}^1(\mathbb{C})$ through the map

$$\begin{aligned} \mathbb{C} \cup \{\infty\} &\to \mathbb{P}^1(\mathbb{C}) \\ \tau &\mapsto \left[\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right] \\ \infty &\mapsto \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]. \end{aligned}$$

This gives the following action on $\mathbb{C} \cup \{\infty\}$:

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

for every $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{C})$ and $\tau \in \mathbb{C} \cup \{\infty\}$.

An easy computation shows that

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

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R})$ and for all $\tau \in \mathbb{C}$ (where if $|c\tau + d| = 0$, we take by convention $\frac{\mathrm{Im}(\tau)}{|c\tau+d|} = \infty$ and $\mathrm{Im}(\infty) = \infty$).

In particular, if $\gamma \in SL_2(\mathbb{Z})$, then

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

This allows us to restrict to the upper half complex plane

$$\mathbb{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\},$$

since the modular group maps $\mathbb{H}$ to itself.

Lemma 1.2. *Let $\tau \in \mathbb{H}$ and*

$$\mathcal{D} := \left\{\tau \in \mathbb{H} : |\mathrm{Re}(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\right\}.$$

Then there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma(\tau) \in \mathcal{D}$. Moreover let $\tau_1, \tau_2 \in \mathcal{D}$ with $Im(\tau_1) \leq Im(\tau_2)$ and suppose that $\gamma\tau_1 = \tau_2$ for some $\gamma \in SL_2(\mathbb{Z})$, then one of the following is true:

1. *$\tau_1 = \tau_2$ and $\gamma = \pm I$,*
2. *$Re(\tau_1) = \frac{1}{2}$, $\tau_2 = \tau_1 - 1$ and $\gamma = \pm \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$,*
3. *$Re(\tau_1) = -\frac{1}{2}$, $\tau_2 = \tau_1 + 1$ and $\gamma = \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$,*
4. *$|\tau_1| = 1$, $\tau_2 = -\frac{1}{\tau_1}$ and $\gamma = \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$,*
5. *$\tau_1 = \zeta_3 = \tau_2$ and $\gamma \in \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \right\rangle$ or $\tau_1 = \zeta_3$, $\tau_2 = \zeta_6$ and $\gamma = \pm \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$,*
6. *$\tau_1 = \zeta_6 = \tau_2$ and $\gamma \in \left\langle \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right) \right\rangle$ or $\tau_1 = \zeta_6$, $\tau_2 = \zeta_3$ and $\gamma = \pm \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$,*

where $\zeta_3 = e^{2\pi i/3}$ and $\zeta_6 = e^{2\pi i/6}$.

Proof. For a proof of the fact that for every $\tau \in \mathbb{H}$ there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma(\tau) \in \mathcal{D}$ look at [4, Lemma 2.3.1.]. Let $\tau_1, \tau_2 \in \mathcal{D}$ with $\mathrm{Im}(\tau_1) \leq \mathrm{Im}(\tau_2)$ such that $\gamma\tau_1 = \tau_2$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Then $\mathrm{Im}(\tau_2) = \frac{\mathrm{Im}(\tau_1)}{|c\tau_1+d|^2} \geq \mathrm{Im}(\tau_1)$, which means that $|c\tau_1 + d|^2 \leq 1$. Consider the following two cases:

$c = 0$: If $c = 0$, then $d = \pm 1 = a$. Thus $\gamma = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$ with $b \in \mathbb{Z}$ and $\tau_2 = \tau_1 \pm b$. On the other hand, $|\mathrm{Re}(\tau_1)| \leq 1/2 \geq |\mathrm{Re}(\tau_2)|$; as a consequence $b = 0$ and $\gamma = \pm I$ or $|\mathrm{Re}(\tau_1)| = 1/2$. If $\mathrm{Re}(\tau_1) = 1/2$, then $\tau_2 = \tau_1 - 1$, so $\gamma = \pm \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$; if $\mathrm{Re}(\tau_1) = -1/2$, then $\tau_2 = \tau_1 + 1$, so $\gamma = \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

$c \neq 0$: From $|c\tau_1 + d|^2 \leq 1$ we deduce that $c^2 \mathrm{Im}(\tau_1)^2 + \mathrm{Re}(c\tau_1 + d)^2 \leq 1$. In particular $c^2 \mathrm{Im}(\tau_1)^2 \leq 1$ and $c^2 \leq 4/3$ (because $\mathrm{Im}(\tau_1) \geq \sqrt{3}/2$), therefore $c = \pm 1$. As a consequence

$$\mathrm{Re}(c\tau_1 + d)^2 = (c\mathrm{Re}(\tau_1) + d)^2 \leq 1 - c^2 \mathrm{Im}(\tau_1)^2 \leq 1/4$$

Hence $|c\mathrm{Re}(\tau_1) + d| \leq 1/2 \Rightarrow |d| \leq 1/2 + |\mathrm{Re}(\tau_1)| \leq 1$. Consider the following two possibilities for d:

$d = 0$: In this case $|c\tau_1 + d| = |\tau_1| \leq 1$, but $\tau_1 \in \mathcal{D}$, hence $|\tau_1| = 1$. Moreover $\gamma = \pm \left(\begin{smallmatrix} a & -1 \\ 1 & 0 \end{smallmatrix}\right)$ for some $a \in \mathbb{Z}$, so $\tau_2 = -\frac{1}{\tau_1} + a$. As the transformation $\tau \mapsto -\frac{1}{\tau}$ acts like the symmetry respect to the imaginary axis on the circumference $\{\tau \in \mathbb{C} : |\tau| = 1\}$, this leads to other three possibilities for a:

- $a = 0$, $\gamma = \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $|\tau_1| = 1$ and $\tau_2 = -1/\tau_1$;
- $a = 1, \gamma = \pm \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\tau_1 = \zeta_6 = \tau_2$;
- $a = -1, \gamma = \pm \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\tau_1 = \zeta_3 = \tau_2$.

$d = \pm 1$: Now we have $|\mathrm{Re}(\tau_1)| = 1/2$ and $\mathrm{Im}(\tau_1) = \sqrt{3}/2$. We have now two possible cases:

$cd = 1$: $\gamma = \pm \left(\begin{smallmatrix} a & a-1 \\ 1 & 1 \end{smallmatrix}\right)$ and $\tau_2 = -\frac{1}{\tau_1 + 1} + a$ with $a \in \mathbb{Z}$. Therefore $\tau_1 = \zeta_3, \tau_2 = \zeta_6$ and $\gamma = \pm \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ or $\tau_1 = \zeta_3 = \tau_2$ and $\gamma = \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$.

$cd = -1$: $\gamma = \pm \left(\begin{smallmatrix} a & -a-1 \\ 1 & -1 \end{smallmatrix}\right)$ and $\tau_2 = -\frac{1}{\tau_1 - 1} + a$ for some $a \in \mathbb{Z}$. Thus $\tau_1 = \zeta_6, \tau_2 = \zeta_3$ and $\gamma = \pm \left(\begin{smallmatrix} -1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ or $\tau_1 = \zeta_6 = \tau_2$ and $\gamma = \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.

□

The action of the modular group gives rise to an equivalence relation on $\mathbb{H}$: if $\tau_1, \tau_2 \in \mathbb{H}$, then $\tau_1 \sim \tau_2$ if and only if there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\gamma(\tau_1) = \tau_2$. As a consequence, the set $\mathcal{D}$ with the suitable boundary identification is a set of representatives of the equivalence classes of $\mathbb{H}$ under the action of $SL_2(\mathbb{Z})$ and $\mathcal{D}$ is called the *standard fundamental domain* for $SL_2(\mathbb{Z})$.

Definition 1.3. Let N be a positive integer. The *principal congruence subgroup of level N* is the subgroup of $SL_2(\mathbb{Z})$ formed by the matrices congruent

to the identity modulo N:

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition 1.4. A subgroup Γ of $SL_2(\mathbb{Z})$ is a *congruence subgroup* if there exists some positive integer N such that $\Gamma(N) \subseteq \Gamma$.

One of the most important congruence subgroups is

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

Definition 1.5. For every congruence subgroup Γ of $SL_2(\mathbb{Z})$, we define the *modular curve*

$$Y(\Gamma) := \Gamma \backslash \mathbb{H} = \{\Gamma\tau : \tau \in \mathbb{H}\}.$$

The modular curves for $\Gamma(N)$ and $\Gamma_0(N)$ are denoted respectively $Y(N)$ and $Y_0(N)$.

For every congruence subgroup we define the quotient map

$$\begin{aligned} \pi : \mathbb{H} &\to Y(\Gamma) \\ \tau &\mapsto \Gamma\tau. \end{aligned}$$

The modular curve $Y(\Gamma)$ inherits the quotient topology, so a subset $U \subset Y(\Gamma)$ is open in the modular curve if and only if its preimage under π is open in $\mathbb{H}$. Furthermore π is an open map, but in order to show this we need the following result from complex analysis, which can be found in [6, Theorem 10.32.].

Theorem 1.6 (Open mapping theorem)**.** *Let U be a connected subset of $\mathbb{C}$ and $f : U \to \mathbb{C}$ a non-constant holomorphic function. Then f is an open map.*

Let $U \subset \mathbb{H}$ be an open subset. Then for every $\gamma \in SL_2(\mathbb{Z})$ we get that $\gamma(U)$ is open by the open mapping theorem. As a consequence $\pi(U) = \Gamma U$ is open in $Y(\Gamma)$ because $\pi^{-1}(\Gamma U) = \bigcup_{\gamma \in \Gamma} \gamma U$, which is open. Consequently π is open.

Definition 1.7. Let X be a topological space. A *complex chart* on X is a homeomorphism $\phi : U \to V$ of an open subset $U \subset X$ onto an open subset $V \subset \mathbb{C}$. Two complex charts $\phi_{1,2} : U_{1,2} \to V_{1,2}$ are *holomorphically compatible* if the maps

$$\phi_2 \circ \phi_1^{-1} : \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$$

and

$$\phi_1 \circ \phi_2^{-1} : \phi_2(U_1 \cap U_2) \to \phi_1(U_1 \cap U_2)$$

are holomorphic. A *complex atlas* on X is a system $\mathcal{U} = \{\phi_i : U_i \to V_i, i \in I\}$ of charts which are holomorphically compatible and such that $\bigcup_{i\in I} U_i = X$. Two complex atlases $\mathcal{U}$ and $\mathcal{U}'$ on X are *analytically equivalent* if every chart of $\mathcal{U}$ is holomorphically compatible with every chart of $\mathcal{U}'$.

Definition 1.8. A *complex structure* on a Hausdorff topological space X is a class of analytically equivalent atlases on X.

Definition 1.9. A *Riemann surface* is a pair (X, Σ) where X is a connected Hausdorff topological space and Σ is a complex structure on X.

Notice first of all that since π is continuous and $\mathbb{H}$ is connected, we have that also $Y(\Gamma)$ is connected.

We start by showing that the modular curve is Hausdorff, but first we need some preliminary results.

Lemma 1.10. *Let $U_1, U_2 \subset \mathbb{H}$, then*

$$\pi(U_1) \cap \pi(U_2) = \emptyset \text{ in } Y(\Gamma) \Leftrightarrow \Gamma(U_1) \cap U_2 = \emptyset \text{ in } \mathbb{H}.$$

The proof of this lemma is straightforward. □

Proposition 1.11. *Let $\tau_1, \tau_2 \in \mathbb{H}$, then there exist neighbourhoods U_1 of τ_1 and U_2 of τ_2 such that for all $\gamma \in SL_2(\mathbb{Z})$,*

$$\gamma(U_1) \cap U_2 \neq \emptyset \Rightarrow \gamma(\tau_1) = \tau_2.$$

Proof. For a proof of this proposition look at [4, Proposition 2.1.1.]. □

Corollary 1.12. *The modular curve $Y(\Gamma)$ is Hausdorff.*

Proof. Let $\Gamma\tau_1$ and $\Gamma\tau_2$ be distinct points of $Y(\Gamma)$. By Proposition 1.11 we know that there exist a neighbourhood U_1 of τ_1 and a neighbourhood U_2 of τ_2 such that for every $\gamma \in SL_2(\mathbb{Z})$, if $\gamma(U_1) \cap U_2 \neq \emptyset$ then $\gamma(\tau_1) = \tau_2$. Since $\gamma(\tau_1) \neq \tau_2$ for all $\gamma \in \Gamma$, we have that $\Gamma(U_1) \cap U_2 = \emptyset$ and by Lemma 1.10 we get that $\pi(U_1) \cap \pi(U_2) = \emptyset$. Since π is an open map, $\pi(U_1)$ and $\pi(U_2)$ are disjoint neighbourhoods of $\Gamma\tau_1$ and $\Gamma\tau_2$ respectively. □

In order to make $Y(\Gamma)$ into a Riemann surface, we still need to define a complex atlas on it. To do this, we have to distinguish two types of points on the modular curve.

Definition 1.13. Let $\tau \in \mathbb{H}$ and let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. We define the *isotropy subgroup* of τ in Γ as the τ-fixing subgroup of Γ and we denote it by Γ_τ:

$$\Gamma_\tau = \{\gamma \in \Gamma : \gamma(\tau) = \tau\}.$$

Definition 1.14. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A point $\tau \in \mathbb{H}$ is an *elliptic point for* Γ if the inclusion $\{\pm I\} \subseteq \{\pm I\}\Gamma_\tau$ is proper. In this case, also the point $\pi(\tau) \in Y(\Gamma)$ is called elliptic.

First of all we define local charts for $Y(\Gamma)$ on neighbourhoods of points which are not elliptic. Let $\tau \in \mathbb{H}$ be a point such that $\Gamma_\tau = \{\pm I\}$. By Proposition 1.11 there exist neighbourhoods $U_1, U_2 \subset \mathbb{H}$ of τ such that for every $\gamma \in SL_2(\mathbb{Z})$, if $\gamma(U_1) \cap U_2 \neq \emptyset$, then $\gamma(\tau) = \tau$. Hence if $\pm I \neq \gamma \in \Gamma$, we have that $\gamma(U_1) \cap U_2 = \emptyset$ and in particular $\gamma(U_1 \cap U_2) \cap U_1 \cap U_2 = \emptyset$. Thus $U := U_1 \cap U_2$ is a neighbourhood of τ with no Γ-equivalent points. We then take the local inverse of π:

$$\phi : \pi(U) \to U,$$

which is a homeomorphism. Therefore we use ϕ as a complex chart. Notice that for every $\gamma \in \Gamma$ we have the local chart

$$\phi_\gamma : \pi(U) \to \gamma(U).$$

All these complex charts are holomorphically compatible, in fact for every $\gamma, \gamma' \in \Gamma$ the transition map

$$\begin{aligned} \phi_\gamma \circ \phi_{\gamma'}^{-1} : \gamma'(U) &\to \gamma(U) \\ \tau &\mapsto (\gamma\gamma'^{-1})(\tau) \end{aligned}$$

is holomorphic because every element of $SL_2(\mathbb{Z})$ gives a holomorphic map on $\mathbb{H}$.

In order to proceed showing that the modular curve $Y(\Gamma)$ is a Riemann surface, we need to study the points that have non-trivial isotropy subgroup in Γ.

Corollary 1.15. *The elliptic points for $SL_2(\mathbb{Z})$ are the points in the $SL_2(\mathbb{Z})$-orbit of i and ζ_3 where $\zeta_3 = e^{2\pi i/3}$. Thus the modular curve $Y(1)$ has two elliptic points ($SL_2(\mathbb{Z})i$ and $SL_2(\mathbb{Z})\zeta_3$) and the isotropy subgroups of i and ζ_3 in $SL_2(\mathbb{Z})$ are*

$$SL_2(\mathbb{Z})_i = \pm\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \text{ and } SL_2(\mathbb{Z})_{\zeta_3} = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

Finally for each elliptic point τ of $SL_2(\mathbb{Z})$, its isotropy subgroup $SL_2(\mathbb{Z})_\tau$ is finite cyclic.

Proof. Isotropy subgroups of elements of the same orbit are conjuate, so it suffices to prove the corollary for elliptic points $\tau \in \mathcal{D}$. By Lemma 1.2 the elliptic points in $\mathcal{D}$ are just i, ζ_3 and ζ_6, since $\tau = -1/\tau$ if and only if $\tau = i$. From Lemma 1.2 we also deduce that $\zeta_6 \in SL_2(\mathbb{Z})\zeta_3$ and that the isotropy subgroup of i is $\pm\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\rangle$ and the isotropy subgroup of ζ_3 is $\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)\rangle$. As a consequence, the elliptic points for $SL_2(\mathbb{Z})$ lie in $SL_2(\mathbb{Z})i$ and $SL_2(\mathbb{Z})\zeta_3$ and their isotropy subgroups are finite cyclic. □

Corollary 1.16. *For every congruence subgroup Γ the modular curve $Y(\Gamma)$ has finitely many elliptic points τ and their isotropy subgroups Γ_τ are finite cyclic.*

Proof. Let N be a positive integer. First of all notice that the homomorphism

$$\begin{aligned} SL_2(\mathbb{Z}) &\to SL_2(\mathbb{Z}/N\mathbb{Z}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod N \right) \end{aligned}$$

has kernel $\Gamma(N)$, thus $[SL_2(\mathbb{Z}) : \Gamma(N)]$ is finite. As a consequence, every congruence subgroup Γ has finite index in $SL_2(\mathbb{Z})$. Hence we have $SL_2(\mathbb{Z}) = \bigcup_{j=i}^{d} \Gamma\gamma_j$ for some suitable $\gamma_1, \ldots, \gamma_d \in SL_2(\mathbb{Z})$. Then the elliptic points of $Y(\Gamma)$ are a subset of $\{\Gamma\gamma_j(i), \Gamma\gamma_j(\zeta_3) : j = 1, \ldots, d\}$, so they are finitely many. Besides Γ_τ is a subgroup of $SL_2(\mathbb{Z})_\tau$ for every elliptic point τ, so Γ_τ is finite cyclic by Corollary 1.15. □

Definition 1.17. Let Γ be a congruence subgroup and $\tau \in \mathbb{H}$. We define the *period* of τ to be

$$h_\tau = |\{\pm I\}\Gamma_\tau / \{\pm I\}| = \begin{cases} |\Gamma_\tau|/2 \text{ if } -I \in \Gamma \\ |\Gamma_\tau| \text{ if } -I \notin \Gamma \end{cases} .$$

Notice that $h_\tau > 1$ if and only if τ is an elliptic point. Moreover if $\tau \in \mathbb{H}$ and $\gamma \in SL_2(\mathbb{Z})$, then the period of $\gamma\tau$ under $\gamma\Gamma\gamma^{-1}$ is equal to the period of τ under Γ. This tells us that the period of a point τ is Γ-invariant and it is therefore well-defined in $Y(\Gamma)$. We also observe that, since γ and $-\gamma$ give the same fractional linear transformation for every $\gamma \in SL_2(\mathbb{Z})$, the period h_τ correctly counts the fractional linear transformation fixing the point τ.

Now we continue the study of finding complex charts for elliptic points. Let $\tau \in \mathbb{H}$ and $\pi(\tau)$ the corresponding point in $Y(\Gamma)$. We begin taking the point τ to the origin and its conjugate $\bar{\tau}$ to ∞ thanks to the map $\delta_\tau := \left(\begin{smallmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{smallmatrix}\right) \in GL_2(\mathbb{C})$. As we have already seen, the isotropy subgroup of 0 in

the conjugated congruence subgroup is the conjugate of the isotropy group of τ, in other words $(\delta_\tau \Gamma \delta_\tau^{-1})_0 = \delta_\tau \Gamma_\tau \delta_\tau^{-1}$. Observe that if a linear fractional transformation $\gamma \in SL_2(\mathbb{Z})$ fixes $\tau \in \mathbb{H}$, then it also fixes $\bar{\tau}$ and so the group $(\delta_\tau \{\pm I\} \Gamma \delta_\tau^{-1})_0 / \{\pm I\}$ is cyclic of order h_τ and consists of linear fractional transformations fixing 0 and ∞. Thus these maps must be of the form $z \mapsto \alpha z$ for some $\alpha \in \mathbb{C}$ and since they form a cyclic group of order h_τ, they must be rotations of angle $k\frac{2\pi}{h_\tau}$ about the origin for some $k \in \{0, \dots, h_\tau - 1\}$.

Proposition 1.18. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. For every point $\tau \in \mathbb{H}$ there exists a neighbourhood U of τ in $\mathbb{H}$ such that*

$$\text{for all } \gamma \in \Gamma, \text{ if } \gamma(U) \cap U \neq \emptyset \text{ then } \gamma \in \Gamma_\tau.$$

Moreover U does not contain any elliptic point for Γ except possibly τ.

Proof. By Proposition 1.11 there exists a neighbourhood U of τ such that for all $\gamma \in SL_2(\mathbb{Z})$, $\gamma(U) \cap U \neq \emptyset \Rightarrow \gamma(\tau) = \tau$. Thus in particular, if $\gamma \in \Gamma$ and $\gamma(U) \cap U \neq \emptyset$, then $\gamma \in \Gamma_\tau$. For every point $\tau' \in U$ that is elliptic for Γ there exists $\pm I \neq \gamma' \in \Gamma_{\tau'}$. Then $\gamma'(U) \cap U \neq \emptyset$ because $\tau' \in \gamma'(U) \cap U$, but this means that $\gamma' \in \Gamma_\tau$. Since every $\pm I \neq \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ fixes at most one point in $\mathbb{H}$ (the root of the polynomial $cz^2 + (d-a)z - b$ with positive imaginary part), we have that $\tau = \tau'$ and the proof is concluded. □

We are now ready to define the local charts on neighbourhoods of elliptic points of the modular curve. Consider $\tau \in \mathbb{H}$ and a neighbourhood U of τ as in Proposition 1.18; let us define

$$\tilde{\psi} := \rho_\tau \circ \delta_\tau : \mathbb{H} \to \mathbb{C},$$

where $\rho_\tau(z) = z^{h_\tau}$. Let $V := \rho_\tau \circ \delta_\tau(U)$. By the open mapping theorem, V is an open subset of $\mathbb{C}$.

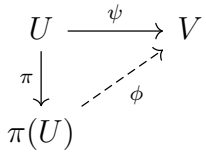
Consider now the quotient map $\pi : U \to \pi(U) \subset Y_0(N)$ and the restriction of $\tilde{\psi}$ to U and V:

$$\psi : U \to V \subset \mathbb{C}.$$

Let $\tau_1, \tau_2 \in U$. We prove that τ_1 and τ_2 have the same image under π if and only if they have the same image under ψ: we have that $\pi(\tau_1) = \pi(\tau_2)$ if and only if there exists $\gamma \in \Gamma$ such that $\tau_1 = \gamma\tau_2$. Hence $\tau_1 \in \gamma(U) \cap U$. By Proposition 1.18, this implies that $\gamma \in \Gamma_\tau$. Thus $\tau_1 \in \Gamma_\tau \tau_2$, so $\delta_\tau(\tau_1) \in (\delta_\tau \Gamma_\tau \delta_\tau^{-1})(\delta_\tau \tau_2)$. This means that $\Leftrightarrow \delta_\tau(\tau_1) = \zeta_{h_\tau}^k \delta_\tau(\tau_2)$ where $\zeta_{h_\tau} = e^{2\pi i/h_\tau}$ and $k \in \{0, \dots, h_\tau - 1\}$, as we have already observed that the group $\delta_\tau \Gamma_\tau \delta_\tau^{-1}$ consists of all the rotations of angle $2\pi k/h_\tau$. Therefore

$$\pi(\tau_1) = \pi(\tau_2) \Leftrightarrow (\delta_\tau(\tau_1))^{h_\tau} = (\delta_\tau(\tau_2))^{h_\tau} \Leftrightarrow \psi(\tau_1) = \psi(\tau_2).$$

Hence there exists an injective map $\phi : \pi(U) \to V$ such that the diagram



commutes. Notice that ϕ is also a surjection, since ψ surjects by definition of V. Moreover ϕ is bicontinuous because ψ is open by the open mapping theorem and we know that π is open. Concluding, ϕ is a homeomorphism, so it is the local chart we were looking for.

To show that these local charts give a complex structure on $Y(\Gamma)$, we still need to verify that the transition maps are holomorphic and a proof of this can be found in [4, Chapter 2].

We have therefore showed the following:

Theorem 1.19. *The modular curve $Y(\Gamma)$ with the complex structure constructed above is a Riemann surface.*

Since we will study some special functions on the modular curve $Y_0(N)$, we give some notions about functions on Riemann surfaces.

Definition 1.20. Let X be a Riemann surface and $\mathbb{C}(X)$ the field of meromorphic functions on X:

$$\mathbb{C}(X) = \{f : X \to \mathbb{C} \cup \{\infty\} : f \text{ is meromorphic}\}.$$

Let $x \in X$ and let $\phi : U \to V \subset \mathbb{C}, x \mapsto 0$ be a coordinate chart on a neighbourhood U of x. Then every $f \in \mathbb{C}(X)^*$ can be uniquely written as $\phi^n g$ where $n \in \mathbb{Z}$ and $g \in \mathbb{C}(X)$ such that $g(x) \neq 0$. Thus we define a valuation

$$\begin{aligned} \text{ord}_x : \mathbb{C}(X)^* &\to \mathbb{Z} \\ f = \phi^n g &\mapsto n. \end{aligned}$$

The number $\text{ord}_x(f)$ is called *order of f at x* and it does not depend on the choice of ϕ.

Definition 1.21. Let X,Y be two Riemann surfaces, $x \in X$ and $F : X \to Y$ be a non-constant holomorphic map. Then the *ramification index of F at x* is

$$e_F(x) := \text{ord}_x(\eta \circ F)$$

where $\eta : U \to V \subset \mathbb{C}, F(x) \mapsto 0$ is a coordinate chart on a neighbourhood U of $F(x)$. The ramification index is independent of the coordinate chart chosen.

Consider now a positive integer N and the quotient map

$$\begin{aligned} \pi_N : \mathbb{H} &\to Y_0(N) \\ \tau &\mapsto \Gamma_0(N)\tau. \end{aligned}$$

Its ramification index at a point of $\mathbb{H}$ will be useful in later computations, so we are now going to study it.

Lemma 1.22. *Let $\tau \in \mathbb{H}$. We have that*

$$e_{\pi_N}(\tau) = h_\tau.$$

Proof. Let $\tau \in \mathbb{H}$ and let U be an open neighbourhood of τ in $\mathbb{H}$; consider the coordinate chart $\phi : \pi_N(U) \to V \subset \mathbb{C}$ as previously defined and observe that $\phi(\pi_N(\tau)) = \psi(\tau) = 0$ where ψ is defined as before to be $\rho_\tau \circ \delta_\tau : U \to V \subset \mathbb{C}$. Furthermore notice that $\delta_\tau : U \to V \subset \mathbb{C}$ is a coordinate chart on the neighbourhood U of τ such that $\delta_\tau(\tau) = 0$. Consequently

$$e_{\pi_N}(\tau) = \mathrm{ord}_\tau(\phi \circ \pi_N) = \mathrm{ord}_\tau(\psi) = \mathrm{ord}_\tau(\rho_\tau\delta_\tau) = \mathrm{ord}_\tau(\delta_\tau^{h_\tau}) = h_\tau.$$

Thus the ramification index of π_N in a point τ is its period h_τ. □

1.2 Modular functions

In this section we introduce some notions on modular functions, but first we define the j-invariant, which is the most important modular function.

Definition 1.23. For every $\tau \in \mathbb{H}$, we define

$$g_2(\tau) = 60 \sum_{\substack{(m,n)\in\mathbb{Z}^2,\\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4}$$

and

$$g_3(\tau) = 140 \sum_{\substack{(m,n)\in\mathbb{Z}^2,\\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^6}.$$

The *j-function* or *j-invariant* $j : \mathbb{H} \to \mathbb{C}$ is defined as

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

Theorem 1.24.

1. *The j-function is holomorphic on $\mathbb{H}$;*
2. *if $\tau, \tau' \in \mathbb{H}$, then $j(\tau) = j(\tau') \Leftrightarrow \tau' = \gamma\tau$ for some $\gamma \in SL_2(\mathbb{Z})$;*
3. *the j-function $j : \mathbb{H} \to \mathbb{C}$ is surjective.*

For a proof of this theorem we refer to [2, Theorem 11.2.]. □

Observe that $j(\tau + 1) = j\left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\tau\right) = j(\tau)$, so j is $\mathbb{Z}$-periodic. Consider now $D' := \{q \in \mathbb{C} : |q| < 1\} \setminus \{0\}$ and the $\mathbb{Z}$-periodic holomorphic function $\tau \mapsto e^{2\pi i\tau} = q(\tau)$ taking $\mathbb{H}$ to D'. Let $g : D' \to \mathbb{C}$ be the map $g(q) := j(\log(q)/2\pi i))$, so that $j(\tau) = g(e^{2\pi i\tau})$. Since j is holomorphic on $\mathbb{H}$, the function g is holomorphic on D', thus j is a holomorphic function in $q = e^{2\pi i\tau} \in D'$ and it has a Laurent expansion

$$j(\tau) = \sum_{n=-\infty}^{\infty} c_n q(\tau)^n,$$

which converges absolutely on every compact subset of $\mathbb{H}$ and that we will call the *q-expansion of j*.

Theorem 1.25. *The q-expansion of $j(\tau)$ is of the form*

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

where $c_n \in \mathbb{Z}$ for every $n \geq 0$.

The reader can find in [2, Theorem 11.8.] a proof of this theorem. □

Let Γ be a congruence subgroup and let $f : \mathbb{H} \to \mathbb{C}$ be a meromorphic function on $\mathbb{H}$ that is invariant under Γ, so $f(\gamma'\tau) = f(\tau)$ for all $\gamma' \in \Gamma$ and $\tau \in \mathbb{H}$. Let $N \in \mathbb{Z}_{\geq 1}$ such that $\Gamma(N) \subseteq \Gamma$. Let $U := \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ and observe that $\tau + N = U\tau$. If $\gamma \in SL_2(\mathbb{Z})$, then $\gamma U\gamma^{-1} \in \Gamma$, thus we have

$$f(\gamma(\tau + N)) = f(\gamma U\tau) = f(\gamma U\gamma^{-1}\gamma\tau) = f(\gamma\tau).$$

Hence $f \circ \gamma$ is $N\mathbb{Z}$-periodic. Consider the $N\mathbb{Z}$-periodic holomorphic function $\tau \mapsto e^{2\pi i\tau/N} =: q(\tau)^{1/N}$ taking $\mathbb{H}$ to D'. Let $g : D' \to \mathbb{C}$ be the map $g(q) := f(\gamma(N\log(q)/2\pi i))$, so that $f(\gamma\tau) = g(e^{2\pi i\tau/N}) = g(q(\tau)^{1/N})$. Since

$f\gamma$ is meromorphic on $\mathbb{H}$, the function g is meromorphic on D', thus $f\gamma$ admits a Fourier expansion

$$f(\gamma\tau) = \sum_{n=-\infty}^{\infty} a_n q(\tau)^{n/N},$$

which we will call the *q-expansion of* $f(\gamma\tau)$.

Definition 1.26. Let Γ be a congruence subgroup and let $f : \mathbb{H} \to \mathbb{C}$ be a meromorphic function on $\mathbb{H}$ that is Γ-invariant. Then we say that f is *meromorphic at the cusps* if for all $\gamma \in SL_2(\mathbb{Z})$, the q-expansion of $f(\gamma\tau)$ has only finitely many non-zero coefficients for negative exponents.

Definition 1.27. Let Γ be a congruence subgroup and let $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ be a complex-valued function on $\mathbb{H}$ such that

1. f is meromorphic on $\mathbb{H}$;
2. $f(\tau)$ is Γ-invariant;
3. $f(\tau)$ is meromorphic at the cusps.

Then we say that f is a *modular function for* Γ.

The j-function is a modular function for $SL_2(\mathbb{Z})$ because it is holomorphic on $\mathbb{H}$, it is $SL_2(\mathbb{Z})$-invariant and by Theorem 1.25 it is also meromorphic at cusps.

Definition 1.28. We say that a modular function for $SL_2(\mathbb{Z})$ is *holomorphic at* ∞ if its q-expansion involves only non-negative powers of q.

Observe that if we consider ∞ as lying in the imaginary direction, then $\tau \to \infty$ if and only if $q = e^{2\pi i\tau} \to 0$, since $|q| = e^{-2\pi \mathrm{Im}(\tau)}$. Hence proving that a modular function is holomorphic at ∞ is equivalent to proving that the limit of the q-expansion of f for $q \to 0$ exists and it is a complex number, which is the same as showing that $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)$ exists as a complex number.

Lemma 1.29.

1. *Every holomorphic modular function for* $SL_2(\mathbb{Z})$ *that is also holomorphic at* ∞ *is constant.*
2. *Every holomorphic modular function for* $SL_2(\mathbb{Z})$ *is a polynomial in* $j(\tau)$.

Proof. For a proof of this lemma look at [2, Lemma 11.10.] □

Theorem 1.30.

1. *The j-function is a modular function for $SL_2(\mathbb{Z})$ and every modular function for $SL_2(\mathbb{Z})$ is a rational function in $j(\tau)$.*
2. *Let N be a positive integer; the functions $j(\tau)$ and $j(N\tau)$ are modular functions for $\Gamma_0(N)$ and every modular function for $\Gamma_0(N)$ is a rational function in $j(\tau)$ and $j(N\tau)$.*

Proof. The reader may find the proof in [2, Theorem 11.9.] □

1.3 The modular polynomial $\Phi_N(X,Y)$

First of all we prove the following result, which will be useful later:

Lemma 1.31. *Let N be a positive integer and consider*

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

Let $\sigma_0 := \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) \in C(N)$. For every $\sigma \in C(N)$ the set

$$(\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$$

is a right coset of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. This induces a one-to-one correspondence between elements of $C(N)$ and the right cosets of $\Gamma_0(N)$.

Lemma 1.31 is a result from [2] left to the reader as an exercise, so we are now going to give a proof of it.

Proof. First of all we show that $\Gamma_0(N) = (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z})$:

- ($\subseteq$) let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, then $A = \sigma_0^{-1} \left(\begin{smallmatrix} a & bN \\ c/N & d \end{smallmatrix}\right) \sigma_0$ and $\left(\begin{smallmatrix} a & bN \\ c/N & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, so $A \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z})$;
- ($\supseteq$) now let $B \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z})$, so there exists $B' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ such that $B = \sigma_0^{-1} B' \sigma_0 = \left(\begin{smallmatrix} a' & b'/N \\ c'N & d' \end{smallmatrix}\right)$, which is of course in $\Gamma_0(N)$.

Now we want to prove that for every $\sigma \in C(N)$, the set $(\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$ is a right coset of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$, so we have to prove that it is a non-empty stable set under the left multiplication by $\Gamma_0(N)$ and that this action is transitive. Notice that for every $\gamma \in \Gamma_0(N)$ we have that $\sigma_0 \gamma \sigma_0^{-1} \in SL_2(\mathbb{Z})$, so for every $\sigma_0^{-1} M \sigma \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$

and $\gamma \in \Gamma_0(N)$, we have $\gamma\sigma_0^{-1}M\sigma = \sigma_0^{-1}\sigma_0\gamma\sigma_0^{-1}M\sigma = \sigma_0^{-1}M'\sigma$ where $M' = \sigma_0\gamma\sigma_0^{-1}M \in SL_2(\mathbb{Z})$. This means that the set $(\sigma_0^{-1}SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$ is $\Gamma_0(N)$-stable. We now show that the set $(\sigma_0^{-1}SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$ is non-empty. Let $\sigma := \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ and let $k \in \mathbb{Z}$ such that $\gcd(dk, a - kb) = 1$. As a consequence there exist $x, y \in \mathbb{Z}$ such that $xdk - y(a - kb) = 1$. Then $\sigma_0^{-1}\left(\begin{smallmatrix} dk & a-kb \\ y & x \end{smallmatrix}\right)\sigma = \left(\begin{smallmatrix} k & 1 \\ ya & yb+xd \end{smallmatrix}\right) \in (\sigma_0^{-1}SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$. As for transitivity, let $\sigma_0^{-1}M\sigma, \sigma_0^{-1}M'\sigma \in (\sigma_0^{-1}SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$ with $M, M' \in SL_2(\mathbb{Z})$. It is sufficient to show that there is $\gamma \in \Gamma_0(N)$ such that $\sigma_0^{-1}M\sigma = \gamma\sigma_0^{-1}M'\sigma$, i.e. $(\sigma_0^{-1}M\sigma)(\sigma_0^{-1}M'\sigma)^{-1} \in \Gamma_0(N)$. Since

$$\begin{aligned}(\sigma_0^{-1}M\sigma)(\sigma_0^{-1}M'\sigma)^{-1} &= \sigma_0^{-1}M(M')^{-1}\sigma_0 \\ &\in (\sigma_0^{-1}SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z}) = \Gamma_0(N),\end{aligned}$$

we have that $(\sigma_0^{-1}SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$ is a right coset of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. In order to prove that there is a bijection between $C(N)$ and the right cosets of $\Gamma_0(N)$, we finally need to show that different σ's give rise to different cosets and that all cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$ arise in this way. Suppose there exist $\sigma_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ 0 & d_1 \end{smallmatrix}\right), \sigma_2 = \left(\begin{smallmatrix} a_2 & b_2 \\ 0 & d_2 \end{smallmatrix}\right) \in C(N)$ such that $\sigma_0^{-1}M\sigma_1 = \sigma_0^{-1}M'\sigma_2 = A \in SL_2(\mathbb{Z})$ for some $M, M' \in SL_2(\mathbb{Z})$. As a consequence $\sigma_1\sigma_2^{-1} = M^{-1}M' \in SL_2(\mathbb{Z})$. On the other hand an easy computation shows that

$$\sigma_1\sigma_2^{-1} = \begin{pmatrix} a_1d_2/N & (-a_1b_2 + a_2b_1)/N \\ 0 & d_1a_2/N \end{pmatrix},$$

so $\sigma_1\sigma_2^{-1} \in SL_2(\mathbb{Z})$ if and only if $a_1 = a_2$, $d_1 = d_2$ and $d_1 \mid b_1 - b_2$. Since $0 \leq b_1$ and $b_2 < d_1$, we get that $\sigma_1\sigma_2^{-1} \in SL_2(\mathbb{Z})$ if and only if $\sigma_1 = \sigma_2$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. We now show that there exists $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right) \in C(N)$ such that $A \in \sigma_0^{-1}SL_2(\mathbb{Z})\sigma$. Therefore we have to prove that $\sigma_0 A\sigma^{-1} = \left(\begin{smallmatrix} a\delta & \alpha b - a\beta \\ c\delta/N & (\alpha d - \beta c)/N \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Define α to be $\gcd(N, c)$ and $\delta := N/\alpha$. Notice that δ and c/α are coprime, thus c/α is an invertible element of $\mathbb{Z}/\delta\mathbb{Z}$. Let β be the unique number such that $0 \leq \beta < \delta$ and $\beta \equiv d(c/\alpha)^{-1} \pmod{\delta}$. To prove that the matrix $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right)$ is an element of $C(N)$ we just have to prove that $\gcd(\alpha, \beta, \delta) = 1$. Let $n := \gcd(\alpha, \beta, \delta)$. We have that $n \mid \alpha \mid c$, $n \mid \delta$ and $n \mid \beta$, so $n \mid d$. On the other hand $ad - bc = 1$, which means that c and d are coprime, consequently $n = 1$. Hence $\sigma := \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right) \in C(N)$. Now we just have to show that $N \mid c\delta$ and $N \mid \alpha d - \beta c$: $N = \alpha\delta \mid c\delta$ if and only if $\alpha \mid c$, which is true by definition of α. Finally $N = \alpha\delta \mid \alpha d - \beta c$ if and only if $\delta \mid d - \beta(c/\alpha)$, which is satisfied thanks to the way we defined β. Therefore $A \in (\sigma_0^{-1}SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$, which proves that all the right cosets of $\Gamma_0(N)$ are of this type. □

As a consequence, for every right coset representative $\Gamma_0(N)\gamma$ there exists a unique $\sigma \in C(N)$ such that $\gamma = \sigma_0^{-1} A \sigma$ for some $A \in SL_2(\mathbb{Z})$. Therefore

$$j(N\gamma\tau) = j(\sigma_0\gamma\tau) = j(A\sigma\tau) = j(\sigma\tau) \tag{1.1}$$

for every $\tau \in \mathbb{H}$.

Lemma 1.32. *Let N be a positive integer and let $\mathbb{C}(\mathbb{H})$ be the set of meromorphic functions on $\mathbb{H}$. We define the following polynomial:*

$$\Phi_N(\tau, Y) := \prod_{\gamma \in \Gamma_0(N)\backslash SL_2(\mathbb{Z})} (Y - j(N\gamma_i\tau)) \in \mathbb{C}(\mathbb{H})[Y].$$

Then $\Phi_N(\tau, Y)$ is a polynomial in Y and $j(\tau)$.

Proof. We want to prove that the coefficients of $\Phi_N(\tau, Y)$ are polynomials in $j(\tau)$. Therefore we show that they are holomorphic modular functions for $SL_2(\mathbb{Z})$ so that we conclude by Lemma 1.29. Consider $\{\gamma_1, \ldots, \gamma_{|C(N)|}\}$ a set of representatives of right cosets of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. Notice first of all that the coefficients of $\Phi_N(\tau, Y)$ are symmetric polynomials in the $j(N\gamma_i\tau)$'s and they are thus holomorphic. We now show the $SL_2(\mathbb{Z})$-invariance: let $\gamma \in SL_2(\mathbb{Z})$, then the cosets $\Gamma_0(N)\gamma_i\gamma$ are just a permutation of the $\Gamma_0(N)\gamma_i$'s. Furthermore, since $j(N\tau)$ is $\Gamma_0(N)$-invariant, we get that the $j(N\gamma_i\gamma\tau)$'s are a permutation of the $j(N\gamma_i\tau)$'s; as the coefficients are symmetric polynomials in the $j(N\gamma_i\tau)$'s, they stay the same if we replace $j(N\gamma_i\tau)$ by $j(N\gamma_i\gamma\tau)$. Finally we need to show that the coefficients are meromorphic at the cusps. By (1.1), we have that $j(N\gamma_i\tau) = j(\sigma\tau)$ for some $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in C(N)$. Then we have that the q-expansion of $j(N\gamma_i\tau)$ is

$$j(N\gamma_i\tau) = \frac{\zeta_N^{-ab}}{(q^{1/N})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_N^{abn} (q^{1/N})^{a^2 n} \tag{1.2}$$

(a proof of this can be found in [2, Chapter 11, Section B]). We have thus proved that the coefficients of $\Phi_N(\tau, Y)$ are modular functions for $SL_2(\mathbb{Z})$ that are holomorphic on $\mathbb{H}$ and we conclude the proof thanks to Lemma 1.29. □

As a consequence of Lemma 1.32, there exists a polynomial $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$ of degree $|C(N)|$ in Y such that the coefficient of $Y^{|C(N)|}$ is 1 and

$$\Phi_N(j(\tau), Y) = \prod_{i=1}^{|C(N)|} (Y - j(N\gamma_i\tau)) \tag{1.3}$$

for every $\tau \in \mathbb{H}$. Observe that

$$\Phi_N(j(\tau), j(N\tau)) = 0, \tag{1.4}$$

for every $\tau \in \mathbb{H}$, since $j(N\tau)$ is equal to $j(N\gamma\tau)$ when $\gamma \in \Gamma_0(N)$.

Lemma 1.33. *The polynomial $\Phi_N(X, Y)$ is irreducible over $\mathbb{C}$.*

Proof. Let γ_i with $i = 1, \dots, |C(N)|$ be coset representatives for $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. Let also $\mathcal{F}$ be the field of meromorphic functions on $\mathbb{H}$ and $\mathcal{F}_N := \mathbb{C}(j, j \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right))$ be the smallest subfield of $\mathcal{F}$ containing the functions j and $j \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$. As we have previously seen,

$$\Phi_N(j(\tau), Y) = \prod_{i=1}^{|C(N)|} (Y - j(N\gamma_i\tau)).$$

Moreover $\Phi_N(j, Y)$ has coefficients in $\mathbb{C}(j)$ and $\Phi_N(j, j \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)) = 0$, hence $[\mathcal{F}_N : \mathbb{C}(j)] \leq |C(N)|$. We now want to prove that $[\mathcal{F}_N : \mathbb{C}(j)] = |C(N)|$, so that $\Phi_N(j, Y)$ is the minimal polynomial of $j \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ over $\mathbb{C}(j)$ and it is therefore irreducible. For every $\gamma \in SL_2(\mathbb{Z})$, consider the map

$$\begin{aligned} \iota_\gamma : \mathcal{F}_N &\to \mathcal{F} \\ f &\mapsto f \circ \gamma, \end{aligned}$$

which is an embedding of $\mathcal{F}_N$ in $\mathcal{F}$ fixing the subfield $\mathbb{C}(j)$. Let $\gamma \in SL_2(\mathbb{Z})$; by Lemma 1.31 there exists $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in C(N)$ such that $\gamma \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z})$. We have already seen in (1.2) that the q-expansion of $j(N\gamma\tau)$ is

$$j(N\gamma\tau) = \frac{\zeta_N^{-ab}}{(q^{1/N})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_N^{abn} (q^{1/N})^{a^2 n}.$$

From (1.2) we notice that if $i \neq j$, then $(\tau \mapsto j(N\gamma_i\tau)) \neq (\tau \mapsto j(N\gamma_j\tau))$, because the two Laurent series are different: let $\sigma_i = \left(\begin{smallmatrix} a_i & b_i \\ 0 & d_i \end{smallmatrix}\right), \sigma_j = \left(\begin{smallmatrix} a_j & b_j \\ 0 & d_j \end{smallmatrix}\right) \in C(N)$ such that $\gamma_i \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_i) \cap SL_2(\mathbb{Z})$ and $\gamma_j \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_j) \cap SL_2(\mathbb{Z})$, then the first terms of the two q-expansions $\frac{\zeta_N^{-a_i b_i}}{(q^{1/N})^{a_i^2}}$ and $\frac{\zeta_N^{-a_j b_j}}{(q^{1/N})^{a_j^2}}$ are the same if and only if $a_i = a_j$ and $b_i = b_j$, which implies that $\sigma_i = \sigma_j$ and thus $\gamma_i = \gamma_j$. As a consequence $\iota_{\gamma_1}, \dots, \iota_{\gamma_{|C(N)|}}$ are $|C(N)|$ different embeddings of $\mathcal{F}_N$ in $\mathcal{F}$ fixing $\mathbb{C}(j)$, so $[\mathcal{F}_N : \mathbb{C}(j)] \geq |C(N)|$. This proves that $\Phi_N(X, Y)$ is irreducible over $\mathbb{C}$. □

Proposition 1.34. *Let $N > 1$ be a positive integer. Then $\Phi_N(X, Y) = \Phi_N(Y, X)$.*

Proof. As seen in (1.1), for every coset representative $\Gamma_0(N)\gamma$ there exists a unique $\sigma \in C(N)$ such that $j(N\gamma\tau) = j(\sigma\tau)$. Hence we get

$$\Phi_N(j(\tau), Y) = \prod_{\sigma \in C(N)} (Y - j(\sigma\tau)). \tag{1.5}$$

Consider the matrix $\sigma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right) \in C(N)$. By (1.5) we have

$$0 = \Phi_N(j(\tau), j(\sigma\tau)) = \Phi_N(j(\tau), j(\tau/N))$$

for every $\tau \in \mathbb{H}$. Hence $\Phi_N(j(N\tau), j(\tau)) = 0$ for every $\tau \in \mathbb{H}$. On the other hand we also have that $\Phi_N(j(\tau), j(N\tau)) = 0$. Thus $j \circ \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is a root of both $\Phi_N(Y, j)$ and $\Phi_N(j, Y)$. By the irreducibility of $\Phi_N(j, Y)$, we get that

$$\Phi_N(Y, j) = g(Y, j)\Phi_N(j, Y) = g(Y, j)g(j, Y)\Phi_N(Y, j)$$

for some polynomial $g(Y, j) \in \mathbb{C}[Y, j]$. This means that $g(Y, j)g(j, Y) = 1$, therfore the function g is a constant. From this we deduce that $g(Y, j) = g(j, Y)$, so $g(Y, j) = \pm 1$. If $g(Y, j) = -1$, then $\Phi_N(j, j) = -\Phi_N(j, j)$ and as a consequence j is a root of $\Phi_N(j, Y)$, which is irreducible over $\mathbb{C}(j)$. Hence $Y - j = \Phi_N(j, Y)$, which implies that $N = 1$, leading to a contradiction. Therefore we have $\Phi_N(Y, j) = \Phi_N(j, Y)$. □

Thanks to the irreducibility of the polynomial $\Phi_N(X, Y)$ we now state its uniqueness:

Definition 1.35. From Lemma 1.33 and Proposition 1.34 there exists a unique polynomial $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$ of degree $|C(N)|$ in X and Y such that the coefficients of $Y^{|C(N)|}$ and $X^{|C(N)|}$ are 1 and

$$\Phi_N(j(\tau), Y) = \prod_{i=1}^{|C(N)|} (Y - j(N\gamma_i\tau)).$$

The equation $\Phi_N(X, Y) = 0$ is called *modular equation* and the polynomial $\Phi_N(X, Y)$ is called *modular polynomial.*

We now show that the modular equations describes the curve $(j(\tau), j(N\tau)) \subset \mathbb{A}^2(\mathbb{C})$ with $\tau \in \mathbb{H}$, which we will denote by $\mathcal{C}_N$: let $(u, v) \in \mathbb{A}^2_{\mathbb{C}}$ such that $\Phi_N(u, v) = 0$. Since j is surjective, $u = j(\tau)$ for some $\tau \in \mathbb{H}$. Consequently

$$0 = \Phi_N(j(\tau), v) = \prod_{\gamma \in \Gamma_0(N)\backslash SL_2(\mathbb{Z})} (v - j(N\gamma_i\tau)),$$

which means that $v = j(N\gamma\tau)$ for some $\gamma \in SL_2(\mathbb{Z})$. Finally $u = j(\tau) = j(\gamma\tau)$, so $(u, v) = (j(\gamma\tau), j(N\gamma\tau))$ for some $\tau \in \mathbb{H}$ and $\gamma \in SL_2(\mathbb{Z})$.

Theorem 1.36. *Let N be a positive integer. Then $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.*

A proof of this result can be found in [2, Theorem 11.18.] □

1.4 $\mathbb{C}$-lattices

We will show later the connection between modular curves and $\mathbb{C}$-lattices, so we now give some basic knowledge on lattices in $\mathbb{C}$.

Definition 1.37. A *lattice* in $\mathbb{C}$ is a set $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with $\{\omega_1, \omega_2\}$ a basis for $\mathbb{C}$ over $\mathbb{R}$. Two lattices L and L' are *homothetic* if there exists $m \in \mathbb{C}^*$ such that $mL = L'$.

Definition 1.38. Let n be a positive integer, L a lattice of $\mathbb{C}$ and L' a sublattice of L such that

- $[L : L'] = n$;
- the quotient L/L' is a cyclic group.

Then we say that L' is a *cyclic sublattice* of L of index n.

Lemma 1.39. *Consider two lattices $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ and $L' = \omega_1'\mathbb{Z} + \omega_2'\mathbb{Z}$ with $\frac{\omega_1}{\omega_2}$, $\frac{\omega_1'}{\omega_2'} \in \mathbb{H}$. Then $L = L'$ if and only if*

$$\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \text{ for some } \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(\mathbb{Z}).$$

Proof. ($\Rightarrow$) Let $\{e_1, e_2\}$ be a basis for $\mathbb{Z}^2$ and consider the homomorphisms of $\mathbb{Z}$-modules:

$$\phi : \mathbb{Z}^2 \to L$$
and
$$\phi' : \mathbb{Z}^2 \to L'$$

of matrices respectively $\left(\begin{smallmatrix}\omega_1 & \omega_2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\omega_1' & \omega_2'\end{smallmatrix}\right)$. If $L = L'$, then $\phi^{-1}\phi' \in \mathrm{Aut}(\mathbb{Z}^2) = GL_2(\mathbb{Z})$. Hence $\left(\begin{smallmatrix}\omega_1 & \omega_2\end{smallmatrix}\right) A = \left(\begin{smallmatrix}\omega_1' & \omega_2'\end{smallmatrix}\right)$ for some $A = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. From this we obtain $\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = A^t\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$. Finally $\det(A^t) > 0$ because

$$0 < \mathrm{Im}(\omega_1'/\omega_2') = \frac{1}{\det(A^t)}\frac{\mathrm{Im}(\omega_1/\omega_2)}{|c(\omega_1/\omega_2) + d|^2}.$$

Hence $A^t \in SL_2(\mathbb{Z})$.

($\Leftarrow$) Suppose there exists $A \in SL_2(\mathbb{Z})$ such that $\begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} = A\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$. We have that

$$L' = \begin{pmatrix}\omega_1' & \omega_2'\end{pmatrix}\mathbb{Z}^2 = \begin{pmatrix}\omega_1 & \omega_2\end{pmatrix}A^t\mathbb{Z}^2 = \begin{pmatrix}\omega_1 & \omega_2\end{pmatrix}\mathbb{Z}^2 = L.$$

□

Theorem 1.40. ***(Elementary Divisor Theorem)*** *Let L' be a $\mathbb{Z}$-submodule of a free module L of the same rank. Then there exist positive integers $d_1, \ldots, d_n$ (called the elementary divisors of L' in L) satisfying the following conditions:*

1. *For every i such that $1 \leq i < n$ we have $d_{i+1} \mid d_i$.*
2. *As $\mathbb{Z}$-modules, we have the isomorphism*

$$L/L' \cong \bigoplus_{1 \leq i \leq n} (\mathbb{Z}/d_i\mathbb{Z})$$

   and in particular $[L : L'] = d_1 \cdots d_n$.

3. *There exists a $\mathbb{Z}$-basis $(v_1, \ldots, v_n)$ of L such that $(d_1 v_1, \ldots, d_n v_n)$ is a $\mathbb{Z}$-basis of L'.*

Moreover the d_i's are uniquely determined by L and L'.

This theorem can be found in [5, Theorem 7.8.].

Definition 1.41. Let L be a lattice of $\mathbb{C}$, so $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ and suppose $\omega_1/\omega_2 \in \mathbb{H}$. Then we define $j(L)$ to be $j(\omega_1/\omega_2)$. From Lemma 1.39 we have that $j(L)$ is independent of the chosen basis.

For simplifying the notation from now on we will refer to the lattice $\tau\mathbb{Z}+\mathbb{Z}$ as Λ_τ.

1.5 The multiplier ring

Definition 1.42. Let L be a lattice. We define its *multiplier ring* as

$$\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}.$$

Theorem 1.43. *Let L be a lattice. The multiplier ring $\mathcal{O}(L)$ is $\mathbb{Z}$ unless L is homothetic to a lattice of the form Λ_τ for some $\tau \in \mathbb{C} \setminus \mathbb{R}$ such that τ is a zero of an irreducible quadratic polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$ with negative discriminant D. In this case $\mathcal{O}(L) = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$.*

Proof. Obviously $\mathbb{Z} \subseteq \mathcal{O}(L)$ for every lattice L. Notice that every lattice L is homothetic to a lattice Λ_τ for some $\tau \in \mathbb{H}$. Moreover $\mathcal{O}(L) = \mathcal{O}(\Lambda_\tau)$. Suppose now that there exists $\alpha \in \mathcal{O}(L) \setminus \mathbb{Z}$. This means that $\alpha \in \Lambda_\tau$ and $\alpha \cdot \tau \in \Lambda_\tau$, hence there exist $z_1, z_2, z_3, z_4 \in \mathbb{Z}$ such that $\alpha = z_1\tau + z_2$ and $\alpha\tau =$

$z_3\tau+z_4$. From this we deduce that $z_3\tau+z_4=\alpha\tau=(z_1\tau+z_2)\tau$ and τ is a root of the polynomial $z_1x^2+(z_2-z_3)x-z_4=0\in\mathbb{Z}[x]$. Consider the polynomial ax^2+bx+c obtained dividing the coefficients of $z_1x^2+(z_2-z_3)x-z_4$ by their greatest common divisor. Thus τ is a root of $ax^2+bx+c\in\mathbb{Z}[x]$, which is irreducible over $\mathbb{Z}$ and with negative discriminant D because $\tau\in\mathbb{H}$. Consider now $\tau\in\mathbb{H}$ be a root of an irreducible polynomial $ax^2+bx+c\in\mathbb{Z}[x]$ with discriminant $D:=b^2-4ac<0$ and we show that $\mathcal{O}(\Lambda_\tau)=\mathbb{Z}[\frac{D+\sqrt{D}}{2}]$. Notice that $\tau=\frac{-b+\sqrt{D}}{2a}$, therefore $\mathbb{Z}[\frac{D+\sqrt{D}}{2}]=\mathbb{Z}[a\tau]$. From this, it easy to verify through simple computations that $\mathbb{Z}[a\tau]=\mathcal{O}(\Lambda_\tau)$: of course $\mathbb{Z}[a\tau]\subseteq\mathcal{O}(\Lambda_\tau)$ because $a\tau^2=-b\tau-c\in\Lambda_\tau$. On the other hand if $\alpha\in\mathcal{O}(\Lambda_\tau)$, then $\alpha=z_1\tau+z_2$ and $\alpha\tau=z_3\tau+z_4$ for some $z_1,z_2,z_3,z_4\in\mathbb{Z}$. Hence $z_3\tau+z_4=\alpha\tau=z_1\tau^2+z_2\tau=z_1(-\frac{b}{a}\tau-\frac{c}{a})+z_2\tau=(z_2-\frac{z_1b}{a})\tau-\frac{z_1c}{a}$, from which we deduce that $a\mid z_1b$ and $a\mid z_1c$. Since the polynomial ax^2+bx+c is an irreducible polynomial, we have that $\gcd(a,b,c)=1$. As a consequence $a\mid z_1$, implying that $\alpha\in\mathbb{Z}[a\tau]$. □

Notice that if $\tau,\tau'\in\mathbb{H}$ are such that $\tau=\gamma\tau'$ for some $\gamma\in SL_2(\mathbb{Z})$, then $\Lambda_{\tau'}=z\Lambda_\tau$ for some $z\in\mathbb{C}^*$, consequently $\mathcal{O}(\Lambda_\tau)=\mathcal{O}(\Lambda_{\tau'})$.

Definition 1.44. Let $\tau\in\mathbb{H}$. We say that τ is a *complex multiplication point* if $\mathcal{O}(\Lambda_\tau)\neq\mathbb{Z}$.

We now define a special kind of homomorphisms between $\mathbb{C}$-lattices.

Definition 1.45. We say that a map $\phi:L_1\to L_2$ between two $\mathbb{C}$-lattices is an *isogeny* if there exists $m\in\mathbb{C}^*$ such that $mL_1\subseteq L_2$ and $\phi(x)=mx$ for every $x\in L_1$.

Notice that there exists an invertible isogeny between two $\mathbb{C}$-lattices if and only if they are homothetic. Moreover a homomorphism $\phi:L\to L$ is an isogeny if and only if $\phi(x)=\alpha x$ for some $\alpha\in\mathcal{O}(L)^*$.

We will now prove that $\mathbb{C}$-lattices are homothetic to invertible fractional ideals of their multiplier rings, which will be very useful later, since ideals are easier then lattices to study.

Definition 1.46. Let R be an integral domain. We define the following equivalence relation on $R\times(R\setminus\{0\})$:

$$(m_1,n_1)\sim(m_2,n_2)\Leftrightarrow m_1n_2=m_2n_1.$$

The *field of fractions* of R is the set

$$\mathrm{Frac}(R):=\left\{\frac{m}{n}\mid m,n\in R,n\neq0\right\}$$

where $\frac{m}{n}$ denotes the equivalence class of the pair $(m,n) \in R \times (R \setminus \{0\})$ under $\sim$.

Corollary 1.47. *Let L be a lattice in $\mathbb{C}$ and $\mathcal{O}(L)$ its multiplier ring. If $\mathcal{O}(L) \neq \mathbb{Z}$, then $L = z\mathfrak{a}$ for some $z \in \mathbb{C}^*$ and $\mathfrak{a}$ an invertible fractional $\mathcal{O}(L)$-ideal.*

Proof. Consider a $\mathbb{C}$-lattice L such that $\mathcal{O}(L) \neq \mathbb{Z}$. By Theorem 1.43 we know that $L = z\Lambda_\tau$ for some $z \in \mathbb{C}^*$ and some $\tau \in \mathbb{H}$ root of an irreducible polynomial $ax^2+bx+c \in \mathbb{Z}[x]$. Moreover $\mathcal{O}(L) = \mathcal{O}(\Lambda_\tau) = \mathbb{Z}[a\tau]$, as showed in the proof of Theorem 1.43. Thus if we prove that Λ_τ is an invertible fractional ideal of $\mathbb{Z}[a\tau]$ we are done. Of course Λ_τ is a fractional ideal of $\mathbb{Z}[a\tau]$ because $a\Lambda_\tau = a\tau\mathbb{Z} + a\mathbb{Z}$, which is an ideal of $\mathbb{Z}[a\tau]$. Now to show that Λ_τ is invertible, we have to find another fractional ideal $\mathfrak{b}$ such that $\Lambda_\tau\mathfrak{b} = \mathbb{Z}[a\tau]$. Notice that, since $a\Lambda_\tau$ is an ideal of $\mathbb{Z}[a\tau]$, we have that $\overline{a\Lambda_\tau} = a\Lambda_{\bar\tau}$ is an ideal of $\overline{\mathbb{Z}[a\tau]} = \mathbb{Z}[a\tau]$. Keeping in mind that $\tau + \bar\tau = -b/a$ and $\tau\bar\tau = c/a$, we are able to conclude that Λ_τ is an invertible fractional $\mathbb{Z}[a\tau]$-ideal:

$$\begin{aligned} a\Lambda_{\bar\tau}\Lambda_\tau &= a(\tau\bar\tau\mathbb{Z} + \tau\mathbb{Z} + \bar\tau\mathbb{Z} + \mathbb{Z}) = a\left(\tau\mathbb{Z} + \frac{b}{a}\mathbb{Z} + \frac{c}{a}\mathbb{Z} + \mathbb{Z}\right) \\ &= a\tau\mathbb{Z} + a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} = \mathbb{Z}[a\tau], \end{aligned}$$

since $\gcd(a,b,c) = 1$. □

Given an integral domain R, we will denote by $\mathcal{I}(R)$ the set of invertible fractional R-ideals.

At this point we define a notion of index between $\mathbb{C}$-lattices and we study its properties.

Definition 1.48. Let L and L' be two $\mathbb{C}$-lattices such that $L \cap L'$ is a $\mathbb{C}$-lattice. We define the *index of L over L'* to be

$$[L : L'] = \frac{[L : L \cap L']}{[L' : L \cap L']}.$$

Lemma 1.49. *Given three $\mathbb{C}$-lattices L, L' and L'' such that $L \cap L \cap L'''$ is a $\mathbb{C}$-lattice, we have*

$$[L : L'][L' : L''] = [L : L''].$$

Proof. We have that $L \cap L'$ is a $\mathbb{Z}$-submodule of L and it is free because L is a free $\mathbb{Z}$-module. Therefore we just have to show that the rank of $L \cap L'$ is 2. Since $L \cap L' \cap L''$ is a $\mathbb{C}$-lattice, it is a $\mathbb{Z}$-submodule of $L \cap L'$ of rank 2, so:

$$2 = \mathrm{rk}(L \cap L' \cap L'') \leq \mathrm{rk}(L \cap L') \leq \mathrm{rk}(L) = 2.$$

Therefore $L \cap L'$ is a $\mathbb{C}$-lattice and analogously we deduce that also $L \cap L''$ and $L' \cap L''$ are $\mathbb{C}$-lattices. Hence

$$\begin{aligned}
[L : L'][L' : L''] &= \frac{[L : L \cap L']}{[L' : L \cap L']} \cdot \frac{[L' : L' \cap L'']}{[L'' : L' \cap L'']} \\
&= \frac{[L : L \cap L' \cap L'']}{[L' : L \cap L' \cap L'']} \cdot \frac{[L' : L \cap L' \cap L'']}{[L'' : L \cap L' \cap L'']} \\
&= \frac{[L : L \cap L''][L \cap L'' : L \cap L' \cap L'']}{[L'' : L \cap L''][L \cap L'' : L \cap L' \cap L'']} \\
&= \frac{[L : L \cap L'']}{[L'' : L \cap L'']} = [L : L''].
\end{aligned}$$

□

Definition 1.50. Let $\mathcal{O}(L)$ be the multiplier ring of some $\mathbb{C}$-lattice L and let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}(L)$-ideal. We define the *norm* of $\mathfrak{a}$ to be

$$N(\mathfrak{a}) := [\mathcal{O}(L) : \mathfrak{a}].$$

Lemma 1.51. *Let $\mathcal{O} = \mathbb{Z}[u]$ be an order in an imaginary quadratic number field. Consider $0 \neq \alpha \in \mathcal{O}$, so $u\alpha = au + b$ and $\alpha = cu + d$ for some $a, b, c, d \in \mathbb{Z}$. Then $N(\alpha) = \alpha\bar{\alpha} = ad - bc$.*

Proof. Consider $\mathcal{O}$ as a vector space over $\mathbb{Z}$ with basis $\{u, 1\}$ and let λ be the linear transformation

$$\begin{aligned}
\lambda : \mathcal{O} &\to \mathcal{O} \\
x &\mapsto \alpha x,
\end{aligned}$$

which is described by the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$. If $\alpha \in \mathbb{Z}$, then the matrix that we obtain is simply $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right)$, so $ad - bc = \alpha^2 = N(\alpha)$. If instead $0 \neq \alpha \in \mathcal{O} \setminus \mathbb{Z}$, consider the characteristic polynomial of the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$, which is $x^2 - (a + d)x + ad - bc$. Since λ is the multiplication by α, we have that $\alpha^2 - (a + d)\alpha + ad - bc = 0$, therefore $ad - bc = N(\alpha) = \alpha\bar{\alpha}$. □

Proposition 1.52. *Let $\mathcal{O}$ be the multiplier ring of some $\mathbb{C}$-lattice L and let $0 \neq \alpha$ be an element of the field of fractions of $\mathcal{O}$. Then*

$$\alpha\bar{\alpha} = [\mathcal{O} : \alpha\mathcal{O}] = [L : \alpha L].$$

Proof. Write $\mathcal{O} = \mathbb{Z}[u]$ and for now let $0 \neq \alpha \in \mathcal{O}$, so $\alpha = au + b$ and $u\alpha = cu + d$ for some $a, b, c, d \in \mathbb{Z}$. Using the Elementary Divisor Theorem we know

$$|\mathcal{O}/\alpha\mathcal{O}| = \left|\det \begin{pmatrix} a & c \\ b & d \end{pmatrix}\right|.$$

By Lemma 1.51 we conclude that $[\mathcal{O} : \alpha\mathcal{O}] = N(\alpha)$. Moreover by Lemma 1.49

$$[L : \alpha L] = [L : \mathcal{O}][\mathcal{O} : \alpha\mathcal{O}][\alpha\mathcal{O} : \alpha L] = [L : \mathcal{O}][\mathcal{O} : \alpha\mathcal{O}][\mathcal{O} : L] = [\mathcal{O} : \alpha\mathcal{O}].$$

Consider now an element $\alpha \in \mathrm{Frac}(\mathcal{O})^*$, hence $\alpha = \frac{\alpha_1}{\alpha_2}$ for some $\alpha_1, \alpha_2 \in \mathcal{O}$. Notice that $\alpha\mathcal{O}/\alpha_1\mathcal{O} \cong \mathcal{O}/\alpha_2\mathcal{O}$ and that $\mathcal{O} \cap \alpha_1\mathcal{O} \cap \alpha\mathcal{O} = \alpha_1\mathcal{O}$ so we can apply Lemma 1.49. Therefore we obtain

$$\begin{aligned}[\mathcal{O} : \alpha\mathcal{O}] &= [\mathcal{O} : \alpha_1\mathcal{O}][\alpha_1\mathcal{O} : \alpha\mathcal{O}] = \frac{[\mathcal{O} : \alpha_1\mathcal{O}]}{[\mathcal{O} : \alpha_2\mathcal{O}]} \\ &= \frac{\alpha_1\bar{\alpha_1}}{\alpha_2\bar{\alpha_2}} = \alpha\bar{\alpha}.\end{aligned}$$

Finally since $\alpha L/\alpha_1 L \cong L/\alpha_2 L$ and $L \cap \alpha_1 L \cap \alpha L = \alpha_1 L$, we have

$$\begin{aligned}[\mathcal{O} : \alpha\mathcal{O}] &= \frac{[\mathcal{O} : \alpha_1\mathcal{O}]}{[\mathcal{O} : \alpha_2\mathcal{O}]} = \frac{[L : \alpha_1 L]}{[L : \alpha_2 L]} \\ &= \frac{[L : \alpha_1 L]}{[\alpha L : \alpha_1 L]} = [L : \alpha_1 L][\alpha_1 L : \alpha L] \\ &= [L : \alpha L].\end{aligned}$$

□

1.6 Orders in imaginary quadratic fields

Since we have shown that the multiplier ring of some $\mathbb{C}$-lattices is of the form $\mathbb{Z}[\frac{D+\sqrt{D}}{2}]$ where D is a negative integer, it is useful to introduce some notions about imaginary quadratic orders.

Definition 1.53. An *order* in a quadratic field K is a subset $\mathcal{O} \subset K$ such that

1. $\mathcal{O}$ is a subring of K;
2. $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module;
3. $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

Notice that this means that $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2 in K and K is the field of fractions of $\mathcal{O}$. Recall that, given a quadratic field $K = \mathbb{Q}(\sqrt{N})$ with $N \neq 0, 1$ a squarefree integer, one of its invaraints is the *discriminant* d_K, defined as

$$d_K = \begin{cases} N \text{ if } N \equiv 1 \pmod 4 \\ 4N \text{ otherwise} \end{cases}$$

and the ring of integers $\mathcal{O}_K$ of K is $\mathbb{Z}[\frac{d_K+\sqrt{d_K}}{2}]$. Therefore $\mathcal{O}_K$ is an order of K and in particular it is the *maximal order* of K. In fact all the elements of an order are algebraic integers (we derive this from [8, Lemma 3.16.]).

Lemma 1.54. *Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. We have that $\mathcal{O}$ has finite index in $\mathcal{O}_K$ and if we set $f := [\mathcal{O}_K : \mathcal{O}]$, then*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K.$$

Moreover let $D := f^2 d_K$; we get that

$$\mathcal{O} = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right].$$

A proof of this lemma can be found in [2, Lemma 7.2.] □

Definition 1.55. Given an order $\mathcal{O}$ in a quadratic field K of discriminant d_K, the index $f := [\mathcal{O}_K : \mathcal{O}]$ is called the *conductor* of $\mathcal{O}$ and the integer $D := f^2 d_K$ is called its *discriminant*.

Proposition 1.56. *If $\mathcal{O}$ is an order in an imaginary quadratic field $K \subset \mathbb{C}$, then either*

- $\mathcal{O} = \mathbb{Z}[i]$ *and* $|\mathcal{O}^*| = 4$, *or*
- $\mathcal{O} = \mathbb{Z}[\zeta_3]$ *and* $|\mathcal{O}^*| = 6$, *or*
- $\mathcal{O}^* = \{1, -1\}$.

Proof. Of course $|\mathbb{Z}[i]^*| = 4$ and $|\mathbb{Z}[\zeta_3]^*| = 6$. Consider $\mathcal{O}$ an order in an imaginary quadratic field K. Let ζ_m be a primitive m-th root of unity for every $m \in \mathbb{Z}_{\geq 1}$. Suppose that $\zeta_m \in \mathcal{O}^*$ for some $m \in \mathbb{Z}_{\geq 3}$. Thus $2 = [K : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$. As a consequence $\phi(m) \leq 2$, so $m \mid 4$ or $m \mid 6$. Therefore if $\mathcal{O} \neq \mathbb{Z}[i], \mathbb{Z}[\zeta_3]$, we have that $\mathcal{O}^* = \{1, -1\}$. □

Proposition 1.57. *Let $\mathcal{O}$ be an order in an imaginary quadratic number field and let D be the discriminant of $\mathcal{O}$. For every element $\alpha \in \mathcal{O} \setminus \mathbb{Z}$, we have that $N(\alpha) \geq \frac{|D|}{4}$.*

Proof. Let $\alpha \in \mathcal{O} \setminus \mathbb{Z}$. Consider $\mathbb{Z}[\alpha] \subseteq \mathcal{O}$ and let D be the discriminant of $\mathcal{O}$ and D' the discriminant of $\mathbb{Z}[\alpha]$. Of course we have $|D| \leq |D'|$. The discriminant D' of $\mathbb{Z}[\alpha]$ is the square of the discriminant of the minimal polynomial of α over $\mathbb{Q}$, so

$$|D| \leq |D'| = |(\alpha - \bar{\alpha})^2| \leq |(2\sqrt{\alpha\bar{\alpha}})^2| = 4N(\alpha).$$

□

Lemma 1.58. *Let $\mathcal{O}$ be an order in a number field, let $\mathfrak{b}$ be an invertible fractional ideal of $\mathcal{O}$ and let $\mathfrak{c}$ be an ideal of $\mathcal{O}$. Then*

$$\mathfrak{b}/\mathfrak{bc} \cong \mathcal{O}/\mathfrak{c}$$

as $\mathcal{O}$-modules.

Proof. Let $\mathfrak{b}$ be an invertible fractional ideal of $\mathcal{O}$, so there exists $r \in \mathcal{O}$ such that $r\mathfrak{b} \subseteq \mathcal{O}$. Since $\mathfrak{b}/\mathfrak{bc} \cong (r\mathfrak{b})/(r\mathfrak{bc})$, we assume without loss of generality that $\mathfrak{b}$ is an ideal of $\mathcal{O}$. Our goal is to find an isomorphism of $\mathcal{O}$-modules

$$\mathcal{O}/\mathfrak{c} \to \mathfrak{b}/\mathfrak{bc},$$

so we just have to find the image of the element $1 + \mathfrak{c} \in \mathcal{O}/\mathfrak{c}$, which must be an element $x \in \mathfrak{b}$ such that $x\mathfrak{b}^{-1}$ is coprime to $\mathfrak{c}$. In order to find such an element x we first prove that for every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ there exists an element $x_\mathfrak{p} \in \mathfrak{b}$ such that the $\mathcal{O}$-ideal $x_\mathfrak{p}\mathfrak{b}^{-1}$ is coprime to $\mathfrak{p}$. First of all notice that $\mathcal{O}$ is a number ring and has therefore Krull dimension 1. This implies that prime ideals are also maximal ideals. Therefore an ideal is coprime to a prime ideal $\mathfrak{p}$ if and only if it is not contained in $\mathfrak{p}$. Suppose that for every element $x \in \mathfrak{b}$, we have $x\mathfrak{b}^{-1} \subseteq \mathfrak{p}$. As a consequence $\mathcal{O} = \mathfrak{b}\mathfrak{b}^{-1} = \{x_1y_1 + \cdots + x_ny_n : x_1, \ldots, x_n \in \mathfrak{b}, y_1, \ldots, y_n \in \mathfrak{b}^{-1}, n \in \mathbb{N}_{\geq 1}\} \subseteq \mathfrak{p}$, which is a contradiction. For every prime ideal $\mathfrak{p}$ we have thus proved the existence of an element $x_\mathfrak{p} \in \mathfrak{b}$ such that $x_\mathfrak{p}\mathfrak{b}^{-1}$ is coprime to $\mathfrak{p}$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be all the prime ideals containing $\mathfrak{c}$ and define $I_k := \prod_{i \leq k} \mathfrak{p}_i$ for every $k \leq n$. We claim that for every $k \leq n$ there exists $x_k \in \mathfrak{b}$ such that for every $i \leq k$ we have that $x_k\mathfrak{b}^{-1}$ is coprime to $\mathfrak{p}_i$. We proceed by induction on k.

k=0: It is sufficient to choose an arbitrary $x \in \mathfrak{b}$.

$k \geq 1$: Since $\mathfrak{p}_k$ and I_{k-1} are coprime ideals, there exist $y_1 \in \mathfrak{p}_k$ and $y_2 \in I_{k-1}$ such that $y_1 + y_2 = 1$. We define x_k to be $y_1x_{k-1} + y_2x_{\mathfrak{p}_k} \in \mathfrak{b}$, where the element $x_{\mathfrak{p}_k} \in \mathfrak{b}$ is such that $x_{\mathfrak{p}_k}\mathfrak{b}^{-1}$ is coprime to $\mathfrak{p}_k$. We now show that $x_k\mathfrak{b}^{-1}$ is coprime to $\mathfrak{p}_i$ for every $i \leq k$. Notice that $x_k - x_{\mathfrak{p}_k} = (x_k - y_2x_{\mathfrak{p}_k}) + (y_2 - 1)x_{\mathfrak{p}_k} = y_1x_{k-1} - y_1x_{\mathfrak{p}_k} \in \mathfrak{p}_k\mathfrak{b}$, therefore $x_k\mathfrak{b}^{-1} + \mathfrak{p}_k = x_{\mathfrak{p}_k}\mathfrak{b}^{-1} + \mathfrak{p}_k = \mathcal{O}$. On the other hand $x_k - x_{k-1} = (x_k - y_1x_{k-1}) + (y_1 - 1)x_{k-1} = y_2x_{\mathfrak{p}_k} - y_2x_{k-1} \in I_{k-1}\mathfrak{b}$, so $x_k\mathfrak{b}^{-1} + \mathfrak{p}_i = x_{k-1}\mathfrak{b}^{-1} + \mathfrak{p}_i = \mathcal{O}$ for every $i \leq k$.

Let $x := x_n \in \mathfrak{b}$. We prove that $x\mathfrak{b}^{-1}$ is coprime to $\mathfrak{c}$. Suppose by contradiction that $x\mathfrak{b}^{-1}$ is not coprime to $\mathfrak{c}$. This means that there exists a prime ideal $\mathfrak{p}$ dividing $x\mathfrak{b}^{-1} + \mathfrak{c}$, so $x\mathfrak{b}^{-1} + \mathfrak{c} \subseteq \mathfrak{p}$. As a consequence $\mathfrak{c} \subseteq \mathfrak{p}$ and $x\mathfrak{b}^{-1} \subseteq \mathfrak{p}$,

leading to a contradiction by the way we defined x. We are now ready to define the isomorphism we were looking for:

$$\begin{aligned}\phi : \mathcal{O}/\mathfrak{c} &\to \mathfrak{b}/\mathfrak{bc} \\ r + \mathfrak{c} &\mapsto xr + \mathfrak{bc}.\end{aligned}$$

The multiplication by an element is a morphism of $\mathcal{O}$-modules, so we just have to show that ϕ is a bijection. For the injectivity, let $y \in \ker(\phi)$. Then $xy \in \mathfrak{bc}$, so $(x\mathfrak{b}^{-1})y \subseteq \mathfrak{c}$. Moreover $1 = qx + r$ for some $q \in \mathfrak{b}^{-1}$ and $r \in \mathfrak{c}$. Thus $y = yqx + yr \in \mathfrak{c}$ because $yqx \in (x\mathfrak{b}^{-1})y \subseteq \mathfrak{c}$. For the surjectivity let $z \in \mathfrak{b}$. Then $z = qxz + rz \equiv x(qz) \pmod{\mathfrak{bc}}$, so $z = \phi(qz)$. □

1.7 The modular curve $Y_0(N)$ and lattices

Theorem 1.59. *Let N be a positive integer and define*

$$\mathcal{L}_{\mathcal{N}} := \{[(L, L')] : L \subseteq L' \text{ are } \mathbb{C}\text{-lattices}, L'/L \cong \mathbb{Z}/N\mathbb{Z}\}_{/\mathbb{C}^*}.$$

Then we have the following bijection

$$\begin{aligned}Y_0(N) &\to \mathcal{L}_{\mathcal{N}} \\ \Gamma_0(N)\tau &\mapsto \left[\left(\Lambda_\tau, \frac{1}{N}\Lambda_{N\tau}\right)\right],\end{aligned}$$

where $\left[\left(\Lambda_\tau, \frac{1}{N}\Lambda_{N\tau}\right)\right]$ denotes the equivalence class of the pair $\left(\Lambda_\tau, \frac{1}{N}\Lambda_{N\tau}\right)$ under complex scalar multiplication.

Proof. First of all we prove that we have a well-defined map. Let $\tau_1, \tau_2 \in \mathbb{H}$ such that $\Gamma_0(N)\tau_1 = \Gamma_0(N)\tau_2$, so there is $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ such that $\tau_1 = \gamma\tau_2$. Consider $\gamma' := \left(\begin{smallmatrix} a & bN \\ c/N & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and notice that $\gamma'(N\tau_2) = N\tau_1$. Therefore by Lemma 1.39, $(c\tau_2 + d)\Lambda_{\tau_1} = \Lambda_{\tau_2}$ and $(c\tau_2 + d)\Lambda_{N\tau_1} = (c/N \cdot N\tau_2 + d)\Lambda_{N\tau_1} = \Lambda_{N\tau_2}$. We now prove that the map is injective. Consider $\Gamma_0(N)\tau_1, \Gamma_0(N)\tau_2 \in Y_0(N)$ such that $[(\Lambda_{\tau_1}, \frac{1}{N}\Lambda_{N\tau_1})] = [(\Lambda_{\tau_2}, \frac{1}{N}\Lambda_{N\tau_2})]$. This means that there exists $m \in \mathbb{C}^*$ such that $\frac{m}{N}\Lambda_{N\tau_1} = \frac{1}{N}\Lambda_{N\tau_2}$ and $m\Lambda_{\tau_1} = \Lambda_{\tau_2}$. Thus $m\tau_1 = a\tau_2 + b$ and $m = c\tau_2 + d$ for some $a, b, c, d \in \mathbb{Z}$ such that $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Moreover, since $\frac{m}{N} = \frac{c\tau_2 + d}{N} \in \tau_2\mathbb{Z} + \frac{1}{N}\mathbb{Z}$, we have that $N \mid c$ and $\gamma \in \Gamma_0(N)$. As a consequence $\Gamma_0(N)\tau_1 = \Gamma_0(N)\tau_2$, because $\tau_1 = \gamma\tau_2$. Finally, let $[(L, L')] \in \mathcal{L}_N$, we show that there exists $\tau \in \mathbb{H}$ such that $[(L, L')] = [(\Lambda_\tau, \tau\mathbb{Z} + \frac{1}{N}\mathbb{Z})]$. By the Elementary Divisor Theorem, we know that there exists a $\mathbb{Z}$-basis $\{v_1, v_2\}$ of L' such that $\{Nv_1, v_2\}$ is a $\mathbb{Z}$-basis for L, therefore $L' = Nv_1(\frac{v_2}{Nv_1}\mathbb{Z} + \frac{1}{N}\mathbb{Z}), L = Nv_1(\frac{v_2}{Nv_1}\mathbb{Z} + \mathbb{Z})$ and $\tau = v_2/Nv_1$. □

In particular the special case $N = 1$ gives that $Y(1)$ is in bijection with the set

$$\{\mathbb{C}\text{-lattices}\}_{/\mathbb{C}^*}.$$

Chapter 2

The zeros of modular functions obtained from modular polynomials

Let M and N be two positive distinct integers. Recall the following maps:

$$\begin{aligned} \pi_N : \mathbb{H} &\to Y_0(N) \\ \tau &\mapsto \Gamma_0(N)\tau \end{aligned}$$

and

$$\begin{aligned} \phi_N : Y_0(N) &\to \mathcal{C}_N \\ \Gamma_0(N)\tau &\mapsto (j(\tau), j(N\tau)). \end{aligned}$$

Let f_M be the holomorphic function on the modular curve $Y_0(N)$ defined as follows:

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau \mapsto (\Phi_M \circ \phi_N)(\Gamma_0(N)\tau) &= ((\Phi_M \bmod \Phi_N) \circ \ \phi_N)(\Gamma_0(N)\tau) \\ &= \Phi_M(j(\tau), j(N\tau)). \end{aligned}$$

Our goal is to find the divisor of zeros of f_M. Thus we want to compute

$$\mathrm{Div}_0(f_M) = \sum_{\Gamma_0(N)\tau \in Y_0(N)} \mathrm{ord}_{\Gamma_0(N)\tau}(f_M) \cdot (\Gamma_0(N)\tau).$$

In this chapter we will prove the following theorem:

Theorem 2.1. *Let M and N be two positive coprime integers not both squares and let*

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)). \end{aligned}$$

We have that

$$\mathrm{Div}_0(f_M) = \sum_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O})} \sum_{\{\alpha\in\mathcal{O} \,:\, \mathcal{O}/\alpha\mathcal{O}\cong\mathbb{Z}/MN\mathbb{Z}\}_{/\mathcal{O}^*}} \left(\left[\left(\mathfrak{a}, \mathfrak{a}+\frac{\alpha}{N}\mathfrak{a}\right)\right]\right).$$

By definition of divisor of zeros we get

$$\mathrm{Div}_0(f_M) = \sum_{\Gamma_0(N)\tau\in Y_0(N)} \mathrm{ord}_{\Gamma_0(N)\tau}(f_M)\cdot(\Gamma_0(N)\tau).$$

Therefore we want to compute $\mathrm{ord}_{\Gamma_0(N)\tau_0}(f_M)$ for every $\Gamma_0(N)\tau_0 \in Y_0(N)$.

Recall that

$$\Phi_M(j(\tau), Y) = \prod_{\gamma\in\Gamma_0(M)\backslash SL_2(\mathbb{Z})} (Y - j(M\gamma\tau)),$$

therefore

$$f_M(\pi_N(\tau)) = \prod_{\gamma\in\Gamma_0(M)\backslash SL_2(\mathbb{Z})} (j(N\tau) - j(M\gamma\tau)). \tag{2.1}$$

The function $f_M \circ \pi_N$ is a holomorphic function on $\mathbb{H}$, which is also meromorphic at the cusps and $\Gamma_0(N)$-invariant. Thus $f_M \circ \pi_N$ is a modular function for $\Gamma_0(N)$.

Before proceeding we need the following result:

Proposition 2.2. *Let $\phi : X \to Y$ be a non-constant morphism of Riemann surfaces, let $g \in \mathbb{C}(Y)$ be a meromorphic function on Y and $P \in X$. Then*

$$\mathrm{ord}_P(g\circ\phi) = e_\phi(P)\mathrm{ord}_{\phi(P)}(g).$$

We deduce that for every $\tau_0 \in \mathbb{H}$, we have

$$\mathrm{ord}_{\tau_0}(f_M\circ\pi_N) = e_{\pi_N}(\tau_0)\mathrm{ord}_{\pi_N(\tau_0)}(f_M)$$

by Proposition 2.2. Our aim is to determine

$$\mathrm{ord}_{\pi_N(\tau_0)}(f_M) = \frac{\mathrm{ord}_{\tau_0}(f_M\circ\pi_N)}{e_{\pi_N}(\tau_0)} \tag{2.2}$$

for every $\tau_0 \in \mathbb{H}$.

2.1 The ramification index $e_{\pi_N}(\tau_0)$

Our goal in this section is to compute the ramification index $e_{\pi_N}(\tau_0)$ for every $\tau_0 \in \mathbb{H}$, which is needed to compute the order of the function f_M at the point $\Gamma_0(N)\tau_0$.

Theorem 2.3. *Let $\tau \in \mathbb{H}$. We have that*

$$e_{\pi_N}(\tau) = \frac{|\mathcal{O}(\Lambda_\tau)^* \cap \mathcal{O}(\Lambda_{N\tau})^*|}{2}. \tag{2.3}$$

Proof. We already know that $e_{\pi_N}(\tau) = h_\tau = \frac{|\Gamma_0(N)_\tau|}{2}$ for all $\tau \in \mathbb{H}$. Thus we want to prove that

$$\begin{aligned} \chi : \Gamma_0(N)_\tau &\to \mathcal{O}(\Lambda_\tau)^* \cap \mathcal{O}(\Lambda_{N\tau})^* \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto c\tau + d \end{aligned}$$

is a bijection. First of all we show that χ is well-defined. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)_\tau$. Then $c\tau+d \in \Lambda_\tau$ and $(c\tau+d)\tau = a\tau+b \in \Lambda_\tau$, hence $c\tau+d \in \mathcal{O}(\Lambda_\tau)$; in the same way $c\tau + d \in \Lambda_{N\tau}$ because $N \mid c$ and $(c\tau + d)N\tau = aN\tau + bN \in \Lambda_{N\tau}$. To prove that $c\tau + d$ is a unit, consider the characteristic polynomial of the matrix γ, which is $x^2-(a+d)x+1$. Noticing that $c\tau+d$ is the eigenvalue of the eigenvector $\left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right)$ for the matrix γ, we deduce that

$$(c\tau + d)^2 - (a + d)(c\tau + d) + 1 = 0.$$

Consequently $(c\tau + d)(c\tau - a) = -1$. Furthermore it is easy to verify that $c\tau - a \in \mathcal{O}(\Lambda_\tau) \cap \mathcal{O}(\Lambda_{N\tau})$, so $c\tau + d$ is a unit in $\mathcal{O}(\Lambda_\tau)$ and in $\mathcal{O}(\Lambda_{N\tau})$. In order to see that the above map is a bijection, we consider

$$\begin{aligned} \psi : \mathcal{O}(\Lambda_\tau)^* \cap \mathcal{O}(\Lambda_{N\tau})^* &\to \Gamma_0(N)_\tau \\ c\tau + d &\mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

where $a, b \in \mathbb{Z}$ are such that $(c\tau+d)\tau = a\tau+b$. Now we prove that ψ is well-defined: let $c\tau + d \in \mathcal{O}(\Lambda_\tau)^* \cap \mathcal{O}(\Lambda_{N\tau})^*$ and $\gamma := \psi(c\tau + d)$. Then $c\tau + d \in \Lambda_{N\tau} \Rightarrow N \mid c$ and $\frac{a\tau+b}{c\tau+d} = \tau$, hence we just have to show that $\gamma \in SL_2(\mathbb{Z})$. Since $c\tau + d \in \mathcal{O}(\Lambda_\tau)^*$, the multiplication by $c\tau + d$ is an automorphism of Λ_τ. Therefore $\tau\mathbb{Z} + \mathbb{Z} = \Lambda_\tau = (c\tau + d)\Lambda_\tau = (a\tau + b)\mathbb{Z} + (c\tau + d)\mathbb{Z}$. This implies that $\gamma \in SL_2(\mathbb{Z})$ thanks to Lemma 1.39. It is now sufficient to show that the compositions of the two maps $\chi \circ \psi$ and $\psi \circ \chi$ give the identity map, which is simply straightforward computation. □

Taking $N = 1$, we obtain the following special case:

Corollary 2.4. *Let $\tau \in \mathbb{H}$ and let $\pi : \mathbb{H} \to Y(1)$ be the quotient map. Then*

$$e_\pi(\tau) = \frac{|\mathcal{O}(\Lambda_\tau)^*|}{2}.$$

2.2 The order $\mathbf{ord}_{\tau_0}(f_M \circ \pi_N)$

By (2.1) we have that for every $\tau_0 \in \mathbb{H}$

$$\mathrm{ord}_{\tau_0}(f_M \circ \pi_N) = \sum_{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z})} \mathrm{ord}_{\tau_0}(j(N\tau) - j(M\gamma\tau)), \tag{2.4}$$

thus we now try to find $\mathrm{ord}_{\tau_0}(j(N\tau) - j(M\gamma\tau))$ with $\gamma \in SL_2(\mathbb{Z})$.

Before proceeding we need the following:

Lemma 2.5. *Let U be an open connected subset of $\mathbb{C}$, $z_0 \in U$ and $g : U \to \mathbb{C}$ a holomorphic non-constant map. Then*

$$\mathrm{ord}_{z_0}(g(z) - g(z_0)) = \max\{k \in \mathbb{N}_{>0} : g'(z_0) = g''(z_0) = \cdots = g^{(k-1)}(z_0) = 0\}.$$

Proof. The proof is obvious recalling the definition of the order and that holomorphic functions are analytic. □

From this lemma we deduce:

Proposition 2.6. *Let U, V be two open connected subsets of $\mathbb{C}$ and let $z_0 \in U$. Consider two holomorphic non-constant maps $g : U \to V$ and $h : V \to \mathbb{C}$. Let $r \leq \mathrm{ord}_{g(z_0)}(h)$ be a positive integer. We have that*

$$\left(\frac{d}{dz}\right)^r (h \circ g)(z_0) = h^{(r)}(g(z_0)) \cdot (g'(z_0))^r.$$

Proof. We proceed by induction on r.

$r = 0$: The formula is obviously true.

$r = 1$: We have $\left(\frac{d}{dz}\right)(h \circ g)(z_0) = h'(g(z_0))g'(z_0)$.

$r > 1$: If $1 < r \leq \mathrm{ord}_{g(z_0)}(h)$, then $h(g(z_0)) = 0$. Hence

$$\begin{aligned} r &\leq \mathrm{ord}_{g(z_0)}(h(w) - h(g(z_0))) \\ &= \max\{k \in \mathbb{N}_{>0} : h'(g(z_0)) = h''(g(z_0)) = \cdots = h^{(k-1)}(g(z_0)) = 0\} \end{aligned}$$

by Lemma 2.5. In particular $h'(g(z_0)) = 0$ because $r > 1$, hence $\mathrm{ord}_{g(z_0)}(h') = \mathrm{ord}_{g(z_0)}(h'(w) - h'(g(z_0))) = \mathrm{ord}_{g(z_0)}(h) - 1$. Using the fact that $(h')^{(k)}(g(z_0)) = 0$ for every $k < r-1$, we have

$$\begin{aligned}\left(\frac{d}{dz}\right)^r (h \circ g)(z_0) &= \left(\frac{d}{dz}\right)^{r-1} \left((h' \circ g) \cdot g'\right)(z_0) \\ &= \sum_{k=0}^{r-1} \binom{r-1}{k} \left[\left(\frac{d}{dz}\right)^k (h' \circ g)\right] \cdot \left[\left(\frac{d}{dz}\right)^{r-1-k} (g')\right](z_0) \\ &= \left(\frac{d}{dz}\right)^{r-1} (h' \circ g)(z_0) g'(z_0).\end{aligned}$$

Finally by the inductive hypothesis,

$$\begin{aligned}\left(\frac{d}{dz}\right)^r (h \circ g)(z_0) &= \left(\frac{d}{dz}\right)^{r-1} (h' \circ g)(z_0) g'(z_0) \\ &= (h')^{(r-1)}(g(z_0)) \cdot (g'(z_0))^{r-1} g'(z_0) \\ &= h^{(r)}(g(z_0)) \cdot (g'(z_0))^r.\end{aligned}$$

□

Given two positive coprime integers M and N that are not both squares and given $\tau_0 \in \mathbb{H}$ such that $j(N\tau_0) = j(M\gamma\tau_0)$ for some $\gamma \in SL_2(\mathbb{Z})$, we want to compute the order $\mathrm{ord}_{\tau_0}(j(N\tau) - j(M\gamma\tau))$. But first we need to study the order $\mathrm{ord}_{\tau_0}(j(\tau) - j(\tau_0))$.

Let us define the map

$$\begin{aligned}\tilde{j} : Y(1) &\to \mathbb{C} \\ SL_2(\mathbb{Z})\tau &\mapsto j(\tau),\end{aligned}$$

which is well-defined because j is $SL_2(\mathbb{Z})$-invariant and it is an isomorphism of Riemann surfaces.

Lemma 2.7. *Let $\tau_0 \in \mathbb{H}$. We have*

$$\mathrm{ord}_{\tau_0}(j(\tau) - j(\tau_0)) = \frac{|\mathcal{O}(\Lambda_{\tau_0})^*|}{2}.$$

Proof. Notice that $j = \tilde{j} \circ \pi$. Let $\tau_0 \in \mathbb{H}$ and let η be a coordinate chart on a neighbourhood of $j(\tau_0)$. Since $\tilde{j}$ is an isomorphism, we have that $\mathrm{ord}_{\pi(\tau_0)}(\eta \circ \tilde{j}) = 1$. Recalling Proposition 2.2 we compute

$$e_j(\tau_0) = e_{\tilde{j} \circ \pi}(\tau_0) = \mathrm{ord}_{\tau_0}(\eta \circ \tilde{j} \circ \pi) = e_\pi(\tau_0) \mathrm{ord}_{\pi(\tau_0)}(\eta \circ \tilde{j}) = e_\pi(\tau_0).$$

We therefore conclude that

$$\mathrm{ord}_{\tau_0}(j(\tau)-j(\tau_0))=e_j(\tau_0)=e_\pi(\tau_0)=\frac{|\mathcal{O}(\Lambda_{\tau_0})^*|}{2}.$$

□

From now on we will call $\tilde{j}$ just j for simplicity.

Lemma 2.8. *Let M and N be two positive coprime integers not both squares. Let $\tau_0 \in \mathbb{H}$ such that $j(N\tau_0)=j(M\gamma\tau_0)$ for some $\gamma \in SL_2(\mathbb{Z})$. Then*

$$\mathrm{ord}_{\tau_0}(j(N\tau)-j(M\gamma\tau))=\frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}.$$

Proof. Let $\tau_0 \in \mathbb{H}$ and consider $\gamma \in SL_2(\mathbb{Z})$ such that $j(N\tau_0)=j(M\gamma\tau_0)$; this happens if and only if there exists $A \in SL_2(\mathbb{Z})$ such that $N\tau_0=AM\gamma\tau_0$. Fix such an A and we now indicate with B the matrix $A\left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma=\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with determinant M. Define two maps $g_1, g_2 : \mathbb{H} \to \mathbb{C}$, $g_1(\tau):=N\tau$ and $g_2(\tau):=B\tau=\frac{a\tau+b}{c\tau+d}$. Notice that $g_1(\tau_0)=g_2(\tau_0)$. Moreover $j(N\tau)=(j\circ g_1)(\tau)$ and $j(M\gamma\tau)=(j\circ g_2)(\tau)$. Using Lemma 2.5, we know

$$\begin{aligned}&\mathrm{ord}_{\tau_0}(j(N\tau)-j(M\gamma\tau))=\\ &=\max\{k\in\mathbb{N}_{>0}:(j\circ g_1)^{(i)}(\tau_0)-(j\circ g_2)^{(i)}(\tau_0)=0 \text{ for } i=1,\dots,k-1\}\\ &=\max\{k\in\mathbb{N}_{>0}:(j\circ g_1)^{(i)}(\tau_0)=(j\circ g_2)^{(i)}(\tau_0) \text{ for } i=1,\dots,k-1\}.\end{aligned} \tag{2.5}$$

Let $r:=\frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}=\mathrm{ord}_{g_1(\tau_0)}(j(\tau)-j(g_1(\tau_0)))=\mathrm{ord}_{g_2(\tau_0)}(j(\tau)-j(g_2(\tau_0)))$ by Lemma 2.7. From Lemma 2.5 we have that $j^{(k)}(g_1(\tau_0))=j^{(k)}(g_2(\tau_0))=0$ for every $k<r$. Then $(j\circ g_1)^{(k)}(\tau_0)=0=(j\circ g_2)^{(k)}(\tau_0)$ for every $k<r$. Now our goal is to show that $(j\circ g_1)^{(r)}(\tau_0)\neq(j\circ g_2)^{(r)}(\tau_0)$, implying that $\mathrm{ord}_{\tau_0}(j(N\tau)-j(M\gamma\tau))=\frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}$. By Proposition 2.6,

$$\left(\frac{d}{dz}\right)^r(j\circ g_1)(\tau_0)=j^{(r)}(g_1(\tau_0))\cdot(g_1'(\tau_0))^r=j^{(r)}(g_1(\tau_0))N^r$$

and

$$\left(\frac{d}{dz}\right)^r(j\circ g_2)(\tau_0)=j^{(r)}(g_2(\tau_0))\cdot(g_2'(\tau_0))^r=j^{(r)}(g_2(\tau_0))\left(\frac{M}{(c\tau_0+d)^2}\right)^r.$$

Thus we have

$$\left(\frac{d}{dz}\right)^r(j\circ g_1)(\tau_0)=\left(\frac{d}{dz}\right)^r(j\circ g_2)(\tau_0)\Leftrightarrow(c\tau_0+d)^{2r}=(M/N)^r,$$

or equivalently there exists a primitive s-th root of unity ζ_s such that

$$(c\tau_0 + d)^2 = \zeta_s \frac{M}{N}$$

for some $s \mid r$. Remember that $r = \mathrm{ord}_{N\tau_0}(j(\tau) - j(N\tau_0)) = \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}$ thanks to Lemma 2.7. Hence by Proposition 1.56 we just have three possibilities for r and consequently for s: 1, 2 or 3. Define K to be the field of fractions of $\mathcal{O}(\Lambda_{N\tau_0})$ and let us consider separately all the three cases.

$s = 1$: Suppose that $(c\tau_0 + d)^2 = M/N \in \mathbb{R}$, so $c = 0$; consequently $d^2 N = M$, hence $N = 1$ because $\gcd(N, M) = 1$. On the other hand, N is a square thus $M = d^2$ leads to a contradiction since we assumed M and N to be not both squares.

$s = 2$: Consider now the case in which $(c\tau_0 + d)^2 = -M/N$, so $c\tau_0 + d = \pm i\sqrt{M/N}$. Of course $c\tau_0 + d \in K$ and $i \in K$ because $i \in \mathcal{O}(\Lambda_{N\tau_0})^*$, thus $\pm\sqrt{M/N} = \frac{c\tau_0 + d}{i} \in K \cap \mathbb{R} = \mathbb{Q}$ (remember that the multiplier ring of a lattice L is either $\mathbb{Z}$ or an order in some imaginary quadratic field $\mathbb{Q}(\alpha)$ and that $\mathcal{O}(L)$ has field of fractions exactly $\mathbb{Q}$ or $\mathbb{Q}(\alpha)$). This results in a contradiction because we assumed M and N to be coprime and not both squares.

$s = 3$: Suppose that $(c\tau_0 + d)^2 = \zeta_3 \frac{M}{N} \Rightarrow \zeta_3(c\tau_0 + d) = \pm\sqrt{M/N}$. As before, $\pm\sqrt{M/N} \in K \cap \mathbb{R} = \mathbb{Q}$, which gives a contradiction again.

This allows us to conclude that the two derivatives are different, therefore

$$\mathrm{ord}_{\tau_0}(j(N\tau) - j(M\gamma\tau)) = \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}.$$

□

Finally we deduce a formula for the order $\mathrm{ord}_{\tau_0}(f_M \circ \pi_N)$, as wanted.

Theorem 2.9. *Let M and N be two positive coprime integers not both squares. Let $\tau_0 \in \mathbb{H}$ and let f_M be the map on the modular curve $Y_0(N)$ defined as follows:*

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)). \end{aligned}$$

Then

$$\mathrm{ord}_{\tau_0}(f_M \circ \pi_N) = \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2} \cdot \#\{\gamma \in \Gamma_0(M) \backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}. \tag{2.6}$$

Proof. Thanks to Lemma 2.8 we are now able to compute

$$\begin{aligned}\mathrm{ord}_{\tau_0}(f_M \circ \pi_N) &\overset{(2.4)}{=} \sum_{\gamma\in\Gamma_0(M)\backslash SL_2(\mathbb{Z})} \mathrm{ord}_{\tau_0}(j(N\tau) - j(M\gamma\tau)) \\ &= \sum_{\substack{\gamma\in\Gamma_0(M)\backslash SL_2(\mathbb{Z}) \\ \text{s.t } j(N\tau_0)=j(M\gamma\tau_0)}} \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2} \\ &= \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2} \cdot \#\{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}.\end{aligned}$$

□

2.3 The order $\mathrm{ord}_{\pi_N(\tau_0)}(f_M)$

In order to find a formula for the divisor of zeros of the function

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)) \end{aligned}$$

where M and N are two positive coprime integers not both squares, we need to compute the order of the function at a arbitrary point $\Gamma_0(N)\tau_0 \in Y_0(N)$.

Using

$$\mathrm{ord}_{\pi_N(\tau_0)}(f_M) \overset{(2.2)}{=} \frac{\mathrm{ord}_{\tau_0}(f_M \circ \pi_N)}{e_{\pi_N}(\tau_0)},$$

$$\mathrm{ord}_{\tau_0}(f_M \circ \pi_N) \overset{(2.6)}{=} \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2} \cdot |\{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}|,$$

and

$$e_{\pi_N}(\tau_0) \overset{(2.3)}{=} \frac{|\mathcal{O}(\Lambda_{\tau_0})^* \cap \mathcal{O}(\Lambda_{N\tau_0})^*|}{2},$$

we know that

$$\mathrm{ord}_{\pi_N(\tau_0)}(f) = \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{|\mathcal{O}(\Lambda_{\tau_0})^* \cap \mathcal{O}(\Lambda_{N\tau_0})^*|} \cdot |\{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}|. \tag{2.7}$$

For this reason we now try to understand better for which $\tau \in \mathbb{H}$ there exists $\gamma \in SL_2(\mathbb{Z})$ such that $j(N\tau) = j(M\gamma\tau)$. Recall the map

$$\begin{aligned} \phi_N : Y_0(N) &\to \mathbb{C}^2 \\ \Gamma_0(N)\tau &\mapsto (j(\tau), j(N\tau)). \end{aligned}$$

Before continuing with the computation of $\mathrm{ord}_{\pi_N(\tau_0)}(f)$, it is useful to translate our study in terms of lattices. Consider the map

$$\begin{aligned}\psi_N : Y_0(N) &\to Y(1) \times Y(1)\\ \Gamma_0(N)\tau &\mapsto (SL_2(\mathbb{Z})\tau, SL_2(\mathbb{Z})N\tau)\end{aligned}$$

and notice that $\phi_N = (j, j) \circ \psi_N$. We can also describe the map ψ_N in terms of lattices thanks to Theorem 1.59:

$$\begin{aligned}\psi_N : \mathcal{L}_N &\to \mathcal{L}_1 \times \mathcal{L}_1\\ [(L, L')] &\mapsto ([L], [L'])\end{aligned}$$

and observe that for all $\tau \in \mathbb{H}$

$$\begin{aligned}\phi_N(\Gamma_0(N)\tau) = (j(\tau), j(N\tau)) &= \left(j(\Lambda_\tau), j\left(\tau\mathbb{Z} + \frac{1}{N}\mathbb{Z}\right)\right)\\ &= ((j, j) \circ \psi_N)\left(\left[\left(\Lambda_\tau, \tau\mathbb{Z} + \frac{1}{N}\mathbb{Z}\right)\right]\right).\end{aligned}$$

We then define the corresponding map ϕ_N on $\mathcal{L}_N$:

$$\begin{aligned}\phi_N : \mathcal{L}_N &\to \mathbb{C}^2\\ [(L, L')] &\mapsto (j(L), j(L')).\end{aligned}$$

Consider now $[(L, L_N)] \in \mathcal{L}_N$ and $[(L', L'_M)] \in \mathcal{L}_M$ with N and M two positive distinct integers. Then

$$\begin{aligned}\phi_N([(L, L_N)] = \phi_M([(L', L'_M)]) &\Leftrightarrow j(L) = j(L') \text{ and } j(L_N) = j(L'_M)\\ &\Leftrightarrow \psi_N([(L, L_N)]) = \psi_M([(L', L'_M)]).\end{aligned}$$

This means that $\phi_N([(L, L_N)] = \phi_M([(L', L'_M)])$ if and only if the lattice L is homothetic to L' and L_N is homothetic to L'_M.

We are now going to prove that the zeros of the function f_M are complex multiplication points.

Lemma 2.10. *Let M and N be two positive different integers, let τ be a point of $\mathbb{H}$ and let $\gamma \in SL_2(\mathbb{Z})$. Then*

$$j(N\tau) = j(M\gamma\tau) \Leftrightarrow \phi_N(\Gamma_0(N)\tau) = \phi_M(\Gamma_0(M)\gamma\tau).$$

Proof. Let $\gamma \in SL_2(\mathbb{Z})$. Recalling the definition of the maps ϕ_N and ϕ_M, we have that $\phi_N(\Gamma_0(N)\tau) = (j(\tau), j(N\tau))$ and $\phi_M(\Gamma_0(M)\gamma\tau) = (j(\gamma\tau), j(M\gamma\tau))$. Thus $\phi_N(\Gamma_0(N)\tau) = \phi_M(\Gamma_0(M)\gamma\tau)$ if and only if $j(N\tau) = j(M\gamma\tau)$. □

If $f_M(\Gamma_0(N)\tau) = 0$, then there exists $\gamma \in SL_2(\mathbb{Z})$ such that $j(N\tau) = j(M\gamma\tau)$, which means that $N\tau = AM\gamma\tau$ for some $A \in SL_2(\mathbb{Z})$. As a consequence the lattice Λ_τ is homothetic to the lattice $\Lambda_{\gamma\tau}$ and $\Lambda_{N\tau}$ is homothetic to the lattice $\Lambda_{M\gamma\tau}$ by Lemma 1.39. Hence we have the following isogenies between $\mathbb{C}$-lattices:

$$\Lambda_\tau \overset{\times N}{\to} \Lambda_{N\tau} \overset{\cong}{\to} \Lambda_{M\gamma\tau} \hookrightarrow \Lambda_{\gamma\tau} \overset{\cong}{\to} \Lambda_\tau.$$

If we call α the composition of these isogenies, we have that $\alpha\Lambda_\tau \subseteq \Lambda_\tau$. Therefore $\alpha \in \mathcal{O}(\Lambda_\tau)$. We have thus found a special element of the multiplier ring of the lattice Λ_τ which is likely not an integer. We now prove it rigorously.

Proposition 2.11. *Let M and N be two positive distinct integers. Consider $[(L, L_N)] \in \mathcal{L}_N$ such that $[(L, L_N)] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$. Then $\mathcal{O}(L) \neq \mathbb{Z} \neq \mathcal{O}(L_N)$.*

Proof. Suppose that $[(L, L_N)] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$; consequently there exists $[(L', L'_M)] \in \mathcal{L}_M$ such that $\phi_N([(L, L_N)]) = \phi_M([(L', L'_M)])$. Therefore there exist $z, z' \in \mathbb{C}^*$ such that $L' = zL$ and $L'_M = z'L_N$. Notice that $[(L', L'_M)] = [(zL', zL'_M)] = [(L, zL'_M)]$, so we assume without loss of generality that $z = 1$ and we get that $\phi_N([(L, L_N)]) = \phi_M([(L, L_M)])$ for some $[(L, L_M)] \in \mathcal{L}_M$ such that there exists $\beta \in \mathbb{C}^*$ with $\beta L_N = L_M$. Consider $\alpha := M\beta$ and we see that $\alpha \in \mathcal{O}(L)$: $\alpha L = M\beta L \subseteq M\beta L_N = ML_M \subseteq L$. Moreover $\alpha L_N = M\beta L_N = ML_M \subseteq L \subseteq L_N$, thus $\alpha \in \mathcal{O}(L_N)$ and $\beta = \frac{\alpha}{M}$ is an element of the field of fractions of $\mathcal{O}(L_N)$. We therefore use Proposition 1.52 and compute

$$\begin{aligned} \alpha\bar{\alpha} &= M^2\beta\bar{\beta} = M^2[L_N : \beta L_N] = M^2[L_N : L_M] \\ &= M^2\frac{[L_N : L_M \cap L_N]}{[L_M : L_M \cap L_N]} = M^2\frac{[L_N : L_M \cap L_N]}{[L_M : L_M \cap L_N]}\frac{[L_N \cap L_M : L]}{[L_N \cap L_M : L]} \\ &= M^2\frac{[L_N : L]}{[L_M : L]} = M^2\frac{N}{M} = MN. \end{aligned} \tag{2.8}$$

Suppose now that $\alpha \in \mathbb{Z}$. Hence $L/\alpha L \cong (\mathbb{Z}/\alpha\mathbb{Z})^2$ and $\alpha\bar{\alpha} = \alpha^2 = MN$, so $\alpha = \pm\sqrt{MN} \in \mathbb{Z}$. Consider now

$$\alpha L \subseteq \alpha L_N = ML_M \subseteq L;$$

this shows that $\alpha L_N/\alpha L \subseteq L/\alpha L$. Therefore

$$\mathbb{Z}/N\mathbb{Z} \cong \alpha L_N/\alpha L \subseteq L/\alpha L \cong (\mathbb{Z}/\alpha\mathbb{Z})^2.$$

From this we deduce that there is an element of order N in the group $(\mathbb{Z}/\alpha\mathbb{Z})^2$; but all the elements of this group have order dividing α, thus $N \mid \alpha$. In the same way we notice that

$$\alpha L = \bar{\alpha} L \subseteq \bar{\alpha} L_M = \alpha^{-1} M N L_M = \beta^{-1} N L_M = N L_N \subseteq L.$$

Consequently

$$\mathbb{Z}/M\mathbb{Z} \cong \alpha L_M/\alpha L \subseteq L/\alpha L \cong (\mathbb{Z}/\alpha\mathbb{Z})^2.$$

As before we conclude that M divides α. On the other hand, $MN = \alpha^2$, so $M = N = \alpha$, which contradicts the hypothesis that M and N are different. We have therefore found an element α such that $\alpha \in \mathcal{O}(L) \setminus \mathbb{Z}$ and $\alpha \in \mathcal{O}(L_N) \setminus \mathbb{Z}$, which concludes the proof. □

Theorem 2.12. *Let M and N be two positive different integers and let $\tau \in \mathbb{H}$ such that $f_M(\Gamma_0(N)\tau) = 0$. Then τ is a complex multiplication point.*

Proof. The fact that $f_M(\Gamma_0(N)\tau) = 0$ implies that $j(N\tau) = j(M\gamma\tau)$ for some $\gamma \in SL_2(\mathbb{Z})$, which means that $\Gamma_0(N)\tau \in \phi_N^{-1}(\phi_M(Y_0(M)))$ by Lemma 2.10. Using the correspondence between $Y_0(N)$ and $\mathcal{L}_N$ given in Theorem 1.59, we have that $[(\Lambda_\tau, \tau\mathbb{Z} + \frac{1}{N}\mathbb{Z})] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$. By Proposition 2.11 we know that $\mathcal{O}(\Lambda_\tau) \neq \mathbb{Z}$ and as a consequence τ is a complex multiplication point. □

Recall that

$$\mathrm{ord}_{\pi_N(\tau_0)}(f_M) \overset{(2.7)}{=} \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{|\mathcal{O}(\Lambda_{\tau_0})^* \cap \mathcal{O}(\Lambda_{N\tau_0})^*|} \cdot |\{\gamma \in \Gamma_0(M) \backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}|.$$

Now we show that if $f_M(\pi_N(\tau)) = 0$, then $\mathcal{O}(\Lambda_\tau) = \mathcal{O}(\Lambda_{N\tau})$.

Lemma 2.13. *Let M and N be two positive coprime integers and consider $[(L, L_N)] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$. Then $\mathcal{O}(L) = \mathcal{O}(L_N)$.*

Proof. By Proposition 2.11 we deduce that $\mathcal{O}(L) \neq \mathbb{Z} \neq \mathcal{O}(L_N)$. Let $[(L', L'_M)] \in \mathcal{L}_M$ such that $\phi_N([(L, L_N)]) = \phi_M([(L', L'_M)])$ and as in the proof of Proposition 2.11 we have that $[(L', L'_M)] = [(L, L_M)]$. The lattices L_N and L_M are homothetic, therefore they have the same multiplier ring. We want to show that $\mathcal{O}(L) = \mathcal{O}(L_N)$.

($\subseteq$) Observe that

$$\begin{aligned} M\mathcal{O}(L) &= \{M\alpha \in \mathbb{C} : \alpha L \subseteq L\} = \{\alpha \in \mathbb{C} : \alpha \frac{1}{M} L \subseteq L\} \\ &\subseteq \{\alpha \in \mathbb{C} : \alpha L_M \subseteq L_M\} = \mathcal{O}(L_M) = \mathcal{O}(L_N). \end{aligned}$$

Analogously $N\mathcal{O}(L) \subseteq \mathcal{O}(L_N)$. Since M and N are coprime, we have that $N\mathbb{Z} + M\mathbb{Z} = \mathbb{Z}$, hence

$$\mathcal{O}(L) = M\mathcal{O}(L) + N\mathcal{O}(L) \subseteq \mathcal{O}(L_N).$$

($\supseteq$) Notice that

$$M\mathcal{O}(L_N) = M\mathcal{O}(L_M) = \{\alpha \in \mathbb{C} : \alpha L_M \subseteq ML_M\}$$
$$\subseteq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} \subseteq \mathcal{O}(L).$$

Similarly $N\mathcal{O}(L_N) \subseteq \mathcal{O}(L)$. Therefore

$$\mathcal{O}(L_N) = M\mathcal{O}(L_N) + N\mathcal{O}(L_N) \subseteq \mathcal{O}(L).$$

□

Lemma 2.14. *Let M and N be two positive coprime integers and let $\tau_0 \in \mathbb{H}$ such that $f_M(\Gamma_0(N)\tau_0) = 0$. Then*

$$e_{\pi_N}(\tau_0) = \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}. \tag{2.9}$$

Proof. Let $\tau_0 \in \mathbb{H}$ such that $f_M(\Gamma_0(N)\tau_0) = 0$. Then there exists $\gamma \in SL_2(\mathbb{Z})$ such that $j(N\tau_0) = j(M\gamma\tau_0)$, so $[(\Lambda_{\tau_0}, \frac{1}{N}\Lambda_{N\tau_0})] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$ by Lemma 2.10. Thus from Lemma 2.13 we deduce that $\mathcal{O}(\Lambda_{\tau_0}) = \mathcal{O}(\Lambda_{N\tau_0})$. As a consequence $e_{\pi_N}(\tau_0) = \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}$ by Theorem 2.3. □

Recall that the function

$$f_M : Y_0(N) \to \mathbb{C}$$
$$\Gamma_0(N)\tau \mapsto \Phi_M(j(\tau), j(N\tau)).$$

Theorem 2.15. *Let M and N two positive coprime integers not both squares. Let $\tau_0 \in \mathbb{H}$. Then*

$$ord_{\pi_N(\tau_0)}(f_M) = \#\{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}.$$

Proof. Recall that

$$\mathrm{ord}_{\pi_N(\tau_0)}(f_M) \overset{(2.2)}{=} \frac{\mathrm{ord}_{\tau_0}(f_M \circ \pi_N)}{e_{\pi_N}(\tau_0)},$$
$$\mathrm{ord}_{\tau_0}(f_M \circ \pi_N) \overset{(2.6)}{=} \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2} \cdot \#\{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}$$

and

$$e_{\pi_N}(\tau_0) \overset{(2.9)}{=} \frac{|\mathcal{O}(\Lambda_{N\tau_0})^*|}{2}.$$

We are thus able to conclude that

$$\mathrm{ord}_{\pi_N(\tau_0)}(f_M) = \#\{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau_0) = j(M\gamma\tau_0)\}.$$

□

From Theorem 2.15 we obtain

$$\mathrm{Div}_0(f_M) = \sum_{\Gamma_0(N)\tau \in Y_0(N)} \sum_{\substack{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) \\ \text{s.t. } j(N\tau)=j(M\gamma\tau)}} (\Gamma_0(N)\tau). \tag{2.10}$$

Therefore for every $\tau \in \mathbb{H}$ we want to give a better description of the set

$$G_\tau := \{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) : j(N\tau) = j(M\gamma\tau)\}.$$

Theorem 2.16. *Let M and N be two positive coprime integers and $\tau \in \mathbb{H}$. Recall the definition of the maps ϕ_N and ϕ_M:*

$$\begin{aligned} \phi_N : Y_0(N) &\to \mathbb{C} & \qquad \phi_M : Y_0(M) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto (j(\tau), j(N\tau)) & \qquad \Gamma_0(M)\tau &\mapsto (j(\tau), j(M\tau)). \end{aligned}$$

Let H_τ be the set

$$H_\tau := \{\Gamma_0(M)\tau' \in Y_0(M) : \phi_N(\Gamma_0(N)\tau) = \phi_M(\Gamma_0(M)\tau')\}.$$

Then there is a bijection

$$\begin{aligned} B : G_\tau &\to H_\tau \\ \Gamma_0(M)\gamma &\mapsto \Gamma_0(M)\gamma\tau. \end{aligned}$$

Proof. First of all B is well-defined as a map $\Gamma_0(M)\backslash SL_2(\mathbb{Z}) \to Y_0(M)$. Second the image of G_τ under this map is exactly H_τ by Lemma 2.10, thus B is surjective. To prove injectivity we claim that for all $\gamma \in SL_2(\mathbb{Z})$ such that $\Gamma_0(M)\gamma \in G_\tau$, we have

$$\Gamma_0(M)_{\gamma\tau} = SL_2(\mathbb{Z})_{\gamma\tau}.$$

Assuming the claim for now, we get that if $\Gamma_0(M)\gamma\tau = \Gamma_0(M)\gamma'\tau$ for some $\Gamma_0(M)\gamma, \Gamma_0(M)\gamma' \in G_\tau$, then there is an element $\delta \in \Gamma_0(M)$ such that $\delta\gamma\tau = \gamma'\tau$. Hence $\gamma\gamma'^{-1}\delta \in SL_2(\mathbb{Z})_{\gamma\tau} \subseteq \Gamma_0(M)$. As a consequence $\gamma\gamma'^{-1} \in \Gamma_0(M)$, so $\Gamma_0(M)\gamma = \Gamma_0(M)\gamma'$. It now suffices to prove the claim. Of course $\Gamma_0(M)_{\gamma\tau} \subseteq SL_2(\mathbb{Z})_{\gamma\tau}$ for every $\gamma \in SL_2(\mathbb{Z})$, thus we just need to show that these two groups have the same order if $\Gamma_0(M)\gamma \in G_\tau$. In the proof of Theorem 2.3 we have shown that for every $\tau \in \mathbb{H}$ and $N \in \mathbb{Z}_{\geq 1}$ we have $|\Gamma_0(N)_\tau| = |\mathcal{O}(\Lambda_\tau)^* \cap \mathcal{O}(\Lambda^*_{N\tau}|$. Recall that $j(N\tau) = j(M\gamma\tau)$ and thus the two lattices $\Lambda_{N\tau}$ and $\Lambda_{M\gamma\tau}$ are homothetic. In particular they have the same multiplier ring. Moreover we have that $[(\Lambda_\tau, \frac{1}{N}\Lambda_{N\tau})] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$, so we can apply Lemma 2.13 to conclude that

$$\mathcal{O}(\Lambda_{\gamma\tau}) = \mathcal{O}(\Lambda_\tau) = \mathcal{O}(\Lambda_{N\tau}) = \mathcal{O}(\Lambda_{M\gamma\tau}).$$

We thus have that $\mathcal{O}(\Lambda_{\gamma\tau})^* \cap \mathcal{O}(\Lambda_{M\gamma\tau})^* = \mathcal{O}(\Lambda_{\gamma\tau})^*$ and that

$$|\Gamma_0(M)_{\gamma\tau}| = |\mathcal{O}(\Lambda_{\gamma\tau})^* \cap \mathcal{O}(\Lambda_{M\gamma\tau})^*| = |\mathcal{O}(\Lambda_{\gamma\tau})^*| = |SL_2(\mathbb{Z})_{\gamma\tau}|.$$

Thus we have proved the claim and the proof is concluded. □

For every pair of positive integers M and N we define the set

$$Z_{N,M} := \{(x, y) \in Y_0(N) \times Y_0(M) : \phi_N(x) = \phi_M(y)\}.$$

From Theorem 2.16 we obtain

$$\begin{aligned} \mathrm{Div}_0(f_M) &= \sum_{\Gamma_0(N)\tau \in Y_0(N)} \sum_{\substack{\gamma \in \Gamma_0(M)\backslash SL_2(\mathbb{Z}) \text{ s.t.} \\ j(N\tau)=j(M\gamma\tau)}} (\Gamma_0(N)\tau) \\ &= \sum_{\Gamma_0(N)\tau \in Y_0(N)} \sum_{\substack{\Gamma_0(M)\tau' \in Y_0(M) \text{ s.t.} \\ \phi_N(\Gamma_0(N)\tau)=\phi_M(\Gamma_0(M)\tau')}} (\Gamma_0(N)\tau) \\ &= \sum_{(x,y)\in Z_{N,M}} (x). \end{aligned} \tag{2.11}$$

Hence to be able to understand the order of the zeros of f_M better, we now focus on the study of the set $Z_{N,M}$.

2.4 The zeros of f_M

Let M and N be two positive coprime integers not both squares. Keeping in mind Theorem 1.59, which describes the bijection between the modular curve $Y_0(N)$ and the set $\mathcal{L}_N$, we have:

$$\begin{aligned} Z_{N,M} \leftrightarrow \{([(L, L_N)], [(L', L'_M)]) \in \mathcal{L}_N \times \mathcal{L}_M : \phi_N([(L, L_N)]) = \phi_M([(L', L'_M)])\} \\ = \{([(L, L_N)], [(L', L'_M)]) \in \mathcal{L}_N \times \mathcal{L}_M : \exists z, z' \in \mathbb{C}^* \text{ s.t. } L = zL', L_N = z'L'_M\} \end{aligned}$$

and noticing as before that $[(L', L'_M)] = [(zL', zL'_M)] = [(L, zL'_M)]$, we get

$$Z_{N,M} \leftrightarrow \{([(L, L_N)], [(L, L_M)]) \in \mathcal{L}_N \times \mathcal{L}_M : \exists \beta \in \mathbb{C}^* \text{ s.t. } \beta L_N = L_M\}. \tag{2.12}$$

For simplicity we call U the set in (2.12).

Before continuing it is useful to translate the study our $\mathbb{C}$-lattices in terms of invertible fractional ideals, which are easier to work with.

Lemma 2.17. *Let $[(L, L_N)] \in \mathcal{L}_N$ such that $\mathcal{O}(L) = \mathcal{O}(L_N) \neq \mathbb{Z}$ and let K be the field of fractions of $\mathcal{O}(L)$. Then $[(L, L_N)] = [(\mathfrak{a}, \mathfrak{b}_N)] \in \mathcal{L}_N$ where $\mathfrak{a}$ and $\mathfrak{b}_N$ are invertible fractional $\mathcal{O}(L)$-ideals.*

Proof. We have shown in the proof of Theorem 1.59 that for some $\tau \in \mathbb{H}$ we have $[(L, L_N)] = [(\Lambda_\tau, \frac{1}{N}\Lambda_{N\tau})] = [(N\Lambda_\tau, \Lambda_{N\tau})]$. We have moreover seen in the proof of Theorem 1.43 that Λ_τ is an invertible fractional $\mathcal{O}(\Lambda_\tau)$-ideal. Since Λ_τ is homothetic to L and $\Lambda_{N\tau}$ is homothetic to L_N, they have the same multiplier rings. As Λ_τ is an invertible fractional $\mathcal{O}(L)$-ideal, also $N\Lambda_\tau$ is, so the proof is concluded. □

Recall that, given an integral domain R, we denote by $\mathcal{I}(R)$ the set of invertible fractional R-ideals. For every imaginary quadratic order $\mathcal{O}$, let us define the set

$$\mathcal{J}_N(\mathcal{O}) := \{(\mathfrak{a}, \mathfrak{b}) \in \mathcal{I}(\mathcal{O}) \times \mathcal{I}(\mathcal{O}) : \mathfrak{a} \subseteq \mathfrak{b} \text{ and } \mathfrak{b}/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}\}_{/\sim}$$

where $(\mathfrak{a}, \mathfrak{b}) \sim (\mathfrak{a}', \mathfrak{b}')$ if there exists $x \in \mathrm{Frac}(\mathcal{O})^*$ such that $(\mathfrak{a}, \mathfrak{b}) = x(\mathfrak{a}', \mathfrak{b}')$. We denote by $[(\mathfrak{a}, \mathfrak{b})]_\sim$ the equivalence class of the pair $(\mathfrak{a}, \mathfrak{b})$.

Lemma 2.18. *The set U in (2.12) is in bijection with the set*

$$\bigcup_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \{([(\mathfrak{a}, \mathfrak{b}_N)]_\sim, [(\mathfrak{a}, \mathfrak{b}_M)]_\sim) \in \mathcal{J}_N(\mathcal{O}) \times \mathcal{J}_M(\mathcal{O}) : \exists \beta \in \mathrm{Frac}(\mathcal{O})^* \text{ s.t. } \beta\mathfrak{b}_N = \mathfrak{b}_M\}, \tag{2.13}$$

that we call V. More specifically, the bijection is

$$\begin{aligned} R : U &\longrightarrow V \\ ([(L, L_N)], [(L, L_M)]) &\mapsto ([(zL, zL_N)]_\sim, [(zL, zL_M)]_\sim), \end{aligned}$$

where $z \in \mathbb{C}^*$ is such that $zL, zL_N \in \mathcal{I}(\mathcal{O}(L))$.

Proof. Our goal is to prove that

$$\begin{aligned} R : U &\longrightarrow V \\ ([(L, L_N)], [(L, L_M)]) &\mapsto ([(zL, zL_N)]_\sim, [(zL, zL_M)]_\sim) \end{aligned}$$

is a bijection, where $z \in \mathbb{C}^*$ is such that $zL, zL_N \in \mathcal{I}(\mathcal{O}(L))$. We prove that R is well-defined. We prove that $[(zL, zL_M)]_\sim \in \mathcal{J}_M(\mathcal{O})$. By Lemma 2.17 we have that there exists $z' in \mathbb{C}^*$ such that $[(z'L, z'L_M)]_\sim \in \mathcal{J}_M(\mathcal{O})$. Thus both zL and $z'L$ are invertible fractional $\mathcal{O}$-ideals and $zL = \frac{z}{z'}(z'L)$, so $\frac{z}{z'} \in \mathrm{Frac}(\mathcal{O})^*$. As a consequence $[(z'L, z'L_M)]_\sim = [(zL, zL_M)]_\sim \in \mathcal{J}_M(\mathcal{O})$. Let now $([(L, L_N)], [(L, L_M)]) \in U$ and $z \in \mathbb{C}^*$ such that $zL_N \in \mathcal{I}(\mathcal{O}(L))$. If $z' \in \mathbb{C}^*$, then $\frac{z}{z'}z'L_N \in \mathcal{I}(\mathcal{O}(L))$, thus we get $R([(z'L, z'L_N)], [(z'L, z'L_M)]) = ([(zL, zL_N)]_\sim, [(zL, zL_M)]_\sim)$. Moreover let $z, z' \in \mathbb{C}^*$ such that $zL_N, z'L_N \in \mathcal{I}(\mathcal{O}(L))$. We get that $z'L_N = \frac{z'}{z}zL_N$, hence $\frac{z'}{z} \in \mathrm{Frac}(\mathcal{O}(L))^*$. Therefore

we have $([(zL, zL_N)]_\sim, [(zL, zL_M)]_\sim) = ([(z'L, z'L_N)]_\sim, [(z'L, z'L_M)]_\sim)$. Obviously $\beta \in \mathrm{Frac}(\mathcal{O})^*$, since $\mathfrak{b}_N, \mathfrak{b}_M \in \mathcal{I}(\mathcal{O})$. In order to prove that the map R is a bijection we consider its inverse

$$S : V \to U$$
$$([(\mathfrak{a}, \mathfrak{b}_N)]_\sim, [(\mathfrak{a}, \mathfrak{b}_M)]_\sim) \mapsto ([(\mathfrak{a}, \mathfrak{b}_N)], [(\mathfrak{a}, \mathfrak{b}_M)]).$$

It is straightforward that S is well-defined and that the compositions with the map R give the identity. □

Now instead of pairs $(\mathfrak{a}, \mathfrak{b}) \in \mathcal{I}(\mathcal{O}) \times \mathcal{I}(\mathcal{O})$ with $\mathcal{O}$ an imaginary quadratic order and $\mathfrak{b}$ related to $\mathfrak{a}$, we look at pairs $(\mathfrak{a}, \mathfrak{c})$, where $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$ and $\mathfrak{c}$ is an ideal of $\mathcal{O}$ independent of $\mathfrak{a}$, which helps for getting a nice formula. The relation between the two types of pairs is $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a}$. In particular we have:

Theorem 2.19. *The set V as in (2.13) is in bijection with the set*

$$W := \bigcup_{\substack{\mathcal{O} \subset \mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \mathrm{Pic}(\mathcal{O}) \times \left\{ (\mathfrak{c}_N, \mathfrak{c}_M) : \begin{array}{c} \mathcal{O}/\mathfrak{c}_N \cong \mathbb{Z}/N\mathbb{Z}, \mathcal{O}/\mathfrak{c}_M \cong \mathbb{Z}/M\mathbb{Z} \\ \text{and } \exists \beta \in K^* \text{ s.t. } \beta\mathfrak{c}_M = \mathfrak{c}_N \end{array} \right\}. \tag{2.14}$$

In particular the bijection is

$$T : V \to W$$
$$([(\mathfrak{a}, \mathfrak{b}_N)]_\sim, [(\mathfrak{a}, \mathfrak{b}_M)]_\sim) \mapsto ([\mathfrak{a}], (\mathfrak{b}_N^{-1}\mathfrak{a}, \mathfrak{b}_M^{-1}\mathfrak{a})).$$

Proof. We show that T is a bijection. First of all we prove that T is well-defined. Therefore let $([(\mathfrak{a}, \mathfrak{b}_N)]_\sim, [(\mathfrak{a}, \mathfrak{b}_M)]_\sim) \in V$ with $\mathfrak{a}, \mathfrak{b}_N, \mathfrak{b}_M \in \mathcal{I}(\mathcal{O})$ and let $z \in \mathrm{Frac}(\mathcal{O})^*$ for some imaginary quadratic order $\mathcal{O}$. Then $[z\mathfrak{a}] = [\mathfrak{a}]$, $(z\mathfrak{b}_N)^{-1}z\mathfrak{a} = \mathfrak{b}_N^{-1}\mathfrak{a}$ and $(z\mathfrak{b}_M)^{-1}z\mathfrak{a} = \mathfrak{b}_M^{-1}\mathfrak{a}$. Let $\mathfrak{c}_N := \mathfrak{b}_N^{-1}\mathfrak{a}$ and $\mathfrak{c}_M := \mathfrak{b}_M^{-1}\mathfrak{a}$. Notice that $\mathfrak{c}_N, \mathfrak{c}_M \subseteq \mathcal{O}$, since $\mathfrak{a} \subseteq \mathfrak{b}_M, \mathfrak{b}_N$; in addition $\beta\mathfrak{c}_M = \beta(\mathfrak{b}_M^{-1}\mathfrak{a}) = \mathfrak{b}_N^{-1}\mathfrak{a} = \mathfrak{c}_N$. Using Lemma 1.58, we obtain

$$\mathcal{O}/\mathfrak{c}_N = \mathcal{O}/\mathfrak{b}_N^{-1}\mathfrak{a} \cong \mathfrak{b}_N/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$$

and

$$\mathcal{O}/\mathfrak{c}_M = \mathcal{O}/\mathfrak{b}_M^{-1}\mathfrak{a} \cong \mathfrak{b}_M/\mathfrak{a} \cong \mathbb{Z}/M\mathbb{Z}.$$

Therefore T is well-defined. In order to prove that T is a bijection it is sufficient to see that the compositions with its inverse

$$T' : W \to U$$
$$([\mathfrak{a}], (\mathfrak{c}_N, \mathfrak{c}_M)) \mapsto ([(\mathfrak{a}, \mathfrak{c}_N^{-1}\mathfrak{a})]_\sim, [(\mathfrak{a}, \mathfrak{c}_M^{-1}\mathfrak{a})]_\sim)$$

are the identity. We first need to show that T' is well-defined. Hence let $([\mathfrak{a}], (\mathfrak{c}_N, \mathfrak{c}_M)) \in W$ with $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$ for some imaginary quadratic order $\mathcal{O}$. Since M and N are coprime, $\mathcal{O} = M\mathcal{O} + N\mathcal{O} \subseteq \mathfrak{c}_M + \mathfrak{c}_N \subseteq \mathcal{O}$. Therefore $\mathcal{O} = (\beta^{-1}, 1)\mathfrak{c}_N = (\beta, 1)\mathfrak{c}_M$. As a consequence, $\mathfrak{c}_N$ and $\mathfrak{c}_M$ are invertible ideals of $\mathcal{O}$. Of course we have that $\mathfrak{a} \subseteq \mathfrak{c}_N^{-1}\mathfrak{a} \cap \mathfrak{c}_M^{-1}\mathfrak{a}$ and $\beta\mathfrak{c}_N^{-1}\mathfrak{a} = \mathfrak{c}_M^{-1}\mathfrak{a}$. By Lemma 1.58 we have again

$$\mathfrak{c}_N^{-1}\mathfrak{a}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{c}_N \cong \mathbb{Z}/N\mathbb{Z}$$

and

$$\mathfrak{c}_M^{-1}\mathfrak{a}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{c}_M \cong \mathbb{Z}/M\mathbb{Z}.$$

It is clear that $T \circ T'$ is the identity of W and that $T' \circ T$ is the identity of V. □

We prove that, given an imaginary quadratic order $\mathcal{O}$, the pairs of $\mathcal{O}$-ideals $(\mathfrak{c}_N, \mathfrak{c}_M)$ such that $\mathcal{O}/\mathfrak{c}_N \cong \mathbb{Z}/N\mathbb{Z}, \mathcal{O}/\mathfrak{c}_M \cong \mathbb{Z}/M\mathbb{Z}$ and there exists $\beta \in \mathrm{Frac}(\mathcal{O})^*$ such that $\beta\mathfrak{c}_M = \mathfrak{c}_N$ are determined by some elements $\alpha \in \mathcal{O}$ such that $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}$. This allows us to have an explicit description of these ideals. More precisely we have:

Theorem 2.20. *Let $\mathcal{O} \subset \mathbb{C}$ be an order in an imaginary quadratic number field K. We have the following bijection*

$$\begin{aligned} \{\alpha \in \mathcal{O} : \mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}\}_{/\mathcal{O}^*} &\leftrightarrow \left\{(\mathfrak{c}_N, \mathfrak{c}_M) : \begin{array}{c} \mathcal{O}/\mathfrak{c}_N \cong \mathbb{Z}/N\mathbb{Z}, \mathcal{O}/\mathfrak{c}_M \cong \mathbb{Z}/M\mathbb{Z} \\ \text{and } \exists \beta \in K^* \text{ s.t. } \beta\mathfrak{c}_M = \mathfrak{c}_N \end{array}\right\} \\ \alpha &\longmapsto ((\alpha, N), (\bar{\alpha}, M)) \\ M\beta &\longmapsfrom (\mathfrak{c}_N, \mathfrak{c}_M). \end{aligned}$$

Proof. Suppose that $\alpha \in \mathcal{O}$ is such that $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}$. Define $\mathfrak{c}_M := (\bar{\alpha}, M)$ and $\mathfrak{c}_N := (\alpha, N)$. Of course we have $\mathcal{O}/\mathfrak{c}_M \cong \mathbb{Z}/M\mathbb{Z}$ and $\mathcal{O}/\mathfrak{c}_N \cong \mathbb{Z}/N\mathbb{Z}$ because $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}$. Finally define β to be $\frac{\alpha}{M}$. Then by Proposition 1.52 we have

$$\beta\mathfrak{c}_M = \frac{\alpha}{M}(\bar{\alpha}, M) = (\frac{\alpha\bar{\alpha}}{M}, \alpha) = (N, \alpha) = \mathfrak{c}_N.$$

Assume now that $\mathfrak{c}_M$ and $\mathfrak{c}_N$ are two $\mathcal{O}$-ideals such that $\mathcal{O}/\mathfrak{c}_M \cong \mathbb{Z}/M\mathbb{Z}$, $\mathcal{O}/\mathfrak{c}_N \cong \mathbb{Z}/N\mathbb{Z}$ and there exists $\beta \in K^*$ such that $\beta\mathfrak{c}_M = \mathfrak{c}_N$. Let $\alpha := M\beta$. Then $N = N(\mathfrak{c}_N) = N(\beta\mathfrak{c}_M) = \beta\bar{\beta}N(\mathfrak{c}_M) = \beta\bar{\beta}M$. This implies that $\alpha\bar{\alpha} = M^2\beta\bar{\beta} = M^2\frac{N}{M} = MN$. Moreover $\alpha\mathcal{O} = M\beta\mathcal{O} \subseteq \beta\mathfrak{c}_M = \mathfrak{c}_N \subseteq \mathcal{O}$, so $\alpha \in \mathcal{O}$. Now we prove that $\mathfrak{c}_M = (\bar{\alpha}, M)$ and $\mathfrak{c}_N = (\alpha, N)$: we have seen that $\alpha\mathcal{O} \subseteq \mathfrak{c}_N$, thus $(\alpha, N) \subseteq \mathfrak{c}_N$. As a consequence $|\mathcal{O}/(\alpha, N)| \geq |\mathcal{O}/\mathfrak{c}_N| = N$; on the other hand $N\mathcal{O} \subseteq (\alpha, N)$, consequently $\mathfrak{c}_N = (\alpha, N)$. Furthermore

$\bar{\alpha}\mathcal{O} = \frac{MN}{\alpha}\mathcal{O} = \frac{N}{\beta}\mathcal{O} \subseteq \beta^{-1}\mathfrak{c}_N = \mathfrak{c}_M$. Hence $(\bar{\alpha}, M) \subseteq \mathfrak{c}_M$ and reasoning with the indexes in the same way as before we find that $(\bar{\alpha}, M) = \mathfrak{c}_M$. Finally $(\alpha, M)(\alpha, N) = (\alpha^2, M\alpha, N\alpha, MN) = \alpha\mathcal{O}$. As $\mathcal{O}/(\alpha, M) \cong \mathcal{O}/(\bar{\alpha}, M)$ and $(\alpha, N) + (\alpha, M) = \mathcal{O}$, we have by the Chinese Remainder Theorem that

$$\mathcal{O}/\alpha\mathcal{O} \cong \mathcal{O}/(\alpha, N) \times \mathcal{O}/(\alpha, M) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \cong \mathbb{Z}/MN\mathbb{Z}.$$

We have thus proved that we have two well-defined maps. It is now straightforward to see that the compositions of the two maps are the identity. □

By Theorem 2.20, we finally have

$$Z_{N,M} \leftrightarrow \bigcup_{\substack{\mathcal{O} \text{ imaginary} \\ \text{quadratic order}}} \mathrm{Pic}(\mathcal{O}) \times \{\alpha \in \mathcal{O} : \mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}\}_{/\mathcal{O}^*}, \tag{2.15}$$

where we have that

$$\begin{aligned}(\Gamma_0(N)\tau, \Gamma_0(M)\tau') &\leftrightarrow ([(\Lambda_\tau, \frac{1}{N}\Lambda_{N\tau})], [(\Lambda_\tau, L_M)]) \\ &\overset{R}{\mapsto} ([N\Lambda_\tau, \Lambda_{N\tau})]_\sim, [(N\Lambda_\tau, NL_M)]_\sim) \\ &\overset{T}{\mapsto} ([\Lambda_\tau], (N\Lambda_{N\tau}^{-1}\Lambda_\tau, L_M^{-1}\Lambda_\tau)) \\ &\leftrightarrow ([\Lambda_\tau], \alpha^*)\end{aligned}$$

where $\alpha \in \mathcal{O}(\Lambda_\tau)$ such that $\Lambda_{N\tau} = \Lambda_\tau(\alpha, N)^{-1}$ and $\mathcal{O}(\Lambda_\tau)/\alpha\mathcal{O}(\Lambda_\tau) \cong \mathbb{Z}/MN\mathbb{Z}$ and α^* denotes the equivalence class of α under scalar multiplication by the units of $\mathcal{O}(\Lambda_\tau)$.

Thanks to (2.11) and (2.15) we obtain that

$$\mathrm{Div}_0(f_M) = \sum_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathcal{O})} \sum_{\{\alpha\in\mathcal{O}\,:\,\mathcal{O}/\alpha\mathcal{O}\cong\mathbb{Z}/MN\mathbb{Z}\}_{/\mathcal{O}^*}} \left(\left[\left(\mathfrak{a}, \mathfrak{a}(\alpha, N)^{-1}\right)\right]\right).$$

We have that $(\alpha, N)^{-1}$ is $(\frac{\bar{\alpha}}{N}, 1)$:

$$(\alpha, N)(\bar{\alpha}/N, 1) = (M, \bar{\alpha}, \alpha, N) = \mathcal{O}.$$

This proves the following theorem:

Theorem 2.1. *Let M and N be two positive coprime integers not both squares and let*

$$\begin{aligned}f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)).\end{aligned}$$

We have that

$$\mathrm{Div}_0(f_M) = \sum_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathcal{O})} \sum_{\{\alpha\in\mathcal{O}\,:\,\mathcal{O}/\alpha\mathcal{O}\cong\mathbb{Z}/MN\mathbb{Z}\}_{/\mathcal{O}^*}} \left(\left[\left(\mathfrak{a}, \mathfrak{a} + \frac{\alpha}{N}\mathfrak{a}\right)\right]\right).$$

It is important to underline that all these summations are finite. First of all the Picard group of an order in a number field is always a finite abelian group (a reference for this result is [8, Theorem 5.4.]). Furthermore there are finitely many elements α in an imaginary quadratic order $\mathcal{O}$ such that $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}$. In fact by Proposition 1.52 this means that $N(\alpha) = MN$ and there are finitely many elements of $\mathcal{O}$ with norm MN. Finally there are finitely many orders $\mathcal{O}$ containing elements α with the property that $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}$: let $\mathcal{O}$ be an imaginary quadratic order with an element α such that $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/MN\mathbb{Z}$. Notice that $\alpha \notin \mathbb{Z}$, otherwise $\alpha^2 = MN$ and

$$\mathcal{O}/\alpha\mathcal{O} \cong (\mathbb{Z}/\alpha\mathbb{Z})^2 \ncong \mathbb{Z}/\alpha^2\mathbb{Z}.$$

Thus we conclude by Proposition 1.57 that the discriminant D of $\mathcal{O}$ is such that $|D| \leq 4MN$.

2.5 An example

In order to illustrate the formula we show an example. For simplicity of notation we will denote the imaginary quadratic orders of discriminant D by $\mathcal{O}_D$.

Let $N = 1$ and $M = 2$. We now compute the divisor of zeros of the function

$$\begin{aligned} f_2 : Y(1) &\to \mathbb{C} \\ SL_2(\mathbb{Z})\tau &\mapsto \Phi_2(j(\tau), j(\tau)). \end{aligned}$$

By Theorem 2.1, we know that

$$\begin{aligned} \mathrm{Div}_0(f_2) &= \sum_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O})} \sum_{\{\alpha\in\mathcal{O}\,:\, \mathcal{O}/\alpha\mathcal{O}\cong\mathbb{Z}/2\mathbb{Z}\}_{/\mathcal{O}^*}} ([(\mathfrak{a}, \mathfrak{a} + \alpha\mathfrak{a})]) \\ &= \sum_{\substack{\mathcal{O}\subset\mathbb{C} \text{ imaginary} \\ \text{quadratic order}}} \sum_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O})} \sum_{\{\alpha\in\mathcal{O}\,:\, \mathcal{O}/\alpha\mathcal{O}\cong\mathbb{Z}/2\mathbb{Z}\}_{/\mathcal{O}^*}} ([\mathfrak{a}])\,. \end{aligned} \tag{2.16}$$

We have seen that the elements α in an imaginary quadratic order $\mathcal{O}$ satisfying $\mathcal{O}/\alpha\mathcal{O} \cong \mathbb{Z}/2\mathbb{Z}$ are not rational integers and satisfy $N(\alpha) = 2$ by Proposition 1.52. Now let α be such an element. Then we deduce that α is a root of a quadratic polynomial of the form

$$x^2 + bx + 2$$

with $b \in \mathbb{Z}$ such that the discriminant of the polynomial is negative. This means that $b^2 - 8 < 0$, so we have $|b| \leq 2$. Thus we distinguish three different cases:

b=0 : The roots of the polynomial x^2+2 in $\mathbb{C}$ are $\alpha_1 = \sqrt{-2}$ and $\alpha_2 = -\sqrt{-2}$. The only imaginary quadratic order containing α_1 and α_2 is $\mathcal{O}_{-2}$, which is a principal ideal domain. As a consequence $\mathrm{Pic}(\mathcal{O}_{-2}) = 0$. Notice moreover that $\alpha_2 = -\alpha_1$, so

$$\#\{\alpha \in \mathcal{O}_{-2} : \mathcal{O}_{-2}/\alpha\mathcal{O}_{-2} \cong \mathbb{Z}/2\mathbb{Z}\}_{/\mathcal{O}_{-2}^*} = 1.$$

As a consequence $[\mathcal{O}_{-2}]$ (or equivalently $SL_2(\mathbb{Z})\sqrt{-2} \in Y(1)$) is a zero of the function f_2 with order 1.

$|b|$=1: The zeros of the polynomials $x^2 \pm x + 2$ in $\mathbb{C}$ are $\alpha_1 = \frac{1+\sqrt{-7}}{2}$, $\alpha_2 = \frac{-1-\sqrt{-7}}{2}$, $\alpha_3 = \frac{1-\sqrt{-7}}{2}$ and $\alpha_4 = \frac{-1+\sqrt{-7}}{2}$. The unique imaginary quadratic order containing $\alpha_1, \alpha_2, \alpha_3$ or α_4 is $\mathcal{O}_{-7}$ and we have $\mathrm{Pic}(\mathcal{O}_{-7}) = 0$. Furthermore $\alpha_2 = -\alpha_1$ and $\alpha_4 = -\alpha_3$. Consequently

$$\#\left\{\alpha \in \mathcal{O}_{-7} : \mathcal{O}_{-7}/\alpha\mathcal{O}_{-7} \cong \mathbb{Z}/2\mathbb{Z}\right\}_{/\mathcal{O}_{-7}^*} = 2.$$

This allows us to conclude that $[\mathcal{O}_{-7}]$ (or equivalently $SL_2(\mathbb{Z})\frac{1+\sqrt{-7}}{2} \in Y(1)$) is a zero of the function f_2 of order 2.

$|b|$=2: Finally the zeros of the polynomials $x^2 \pm 2x + 2$ in $\mathbb{C}$ are $\alpha_1 = 1+i$, $\alpha_2 = 1-i$, $\alpha_3 = -1-i$ and $\alpha_4 = -1+i$. The only imaginary quadratic order containing $\alpha_1, \alpha_2, \alpha_3$ or α_4 is $\mathcal{O}_{-1}$. We have that $\mathrm{Pic}(\mathcal{O}_{-1}) = 0$ and that $\alpha_1 = i\alpha_2 = -\alpha_3 = -i\alpha_4$. The units of the order $\mathcal{O}_{-1}$ are $\{\pm 1, \pm i\}$, so

$$\#\{\alpha \in \mathcal{O}_{-1} : \mathcal{O}_{-1}/\alpha\mathcal{O}_{-1} \cong \mathbb{Z}/2\mathbb{Z}\}_{/\mathcal{O}_{-1}^*} = 1.$$

Hence $[\mathcal{O}_{-1}]$ (or equivalently $SL_2(\mathbb{Z})i \in Y(1)$) is a zero of the function f_2 of order 1.

We conclude by (2.16) that

$$\begin{aligned}\mathrm{Div}_0(f_2) &= ([\mathcal{O}_{-2}]) + 2\,([\mathcal{O}_{-7}]) + ([\mathcal{O}_{-1}]) \\ &= (SL_2(\mathbb{Z})\sqrt{-2}) + 2\left(SL_2(\mathbb{Z})\frac{1+\sqrt{-7}}{2}\right) + (SL_2(\mathbb{Z})i).\end{aligned}$$

In order to check the correctness of the formula we computed the factoriztion of the polynomial $\Phi_2(X, X)$ thanks to [10]. In this way we find the roots of the polynomial $\Phi_2(X, X)$, which are exactly the points $j(\tau) \in \mathbb{C}$ such that $f_2(SL_2(\mathbb{Z})\tau) = 0$.

First of all we compute the modular polynomial $\Phi_2(X, Y)$ in [10] through the function "polmodular":

$$\begin{aligned}\Phi_2(X,Y) =& X^3 - X^2Y^2 + 1488X^2Y - 162000X^2 + 1488XY^2 \\ &+ 40773375XY + 8748000000X + Y^3 - 162000Y^2 \\ &+ 8748000000Y - 157464000000000.\end{aligned}$$

Hence we compute the factorization of the polynomial $\Phi_2(X, X)$ and obtain

$$\Phi_2(X,X) = -(X - 8000)(X - 1728)(X + 3375)^2.$$

Therefore the zeros of the function f_2 are the points $SL_2(\mathbb{Z})\tau \in Y(1)$ such that $j(\tau)$ is a root of $\Phi_2(X, X)$. We have that $j(\sqrt{-2}) = 8000$, $j(i) = 1728$ and $j(\frac{1+\sqrt{-7}}{2}) = -3375$. Thus we showed that Theorem 2.1 gave us the right divisor of zeros of the function f_2 on the modular curve $Y(1)$.

Chapter 3

The modular curve $X_0(N)$ and combination of functions obtained from modular polynomials

In this chapter we will show that the modular curve $X(\Gamma)$ with Γ a congruence subgroup is a compact Riemann surface. Moreover we will prove that every non-constant finite product of powers of functions of the form

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)) \end{aligned}$$

is not a modular unit and we will give a lower bound for the degree of this kind of functions on the modular curve $X_0(N)$.

3.1 The Riemann surface structure of the modular curve $X(\Gamma)$

The goal of this section is to show the Riemann surface structure of the modular curve $X(\Gamma)$, which is already a well-known result. A reference for this section is [4, Chapter 2].

Recall the action of the modular group $SL_2(\mathbb{Z})$ on the set $\mathbb{C}\cup\{\infty\}$ defined in the first chapter. The modular group $SL_2(\mathbb{Z})$ acts transitively on $\mathbb{Q}\cup\{\infty\}$: given a rational number $\frac{a}{c}$ with $a, c \in \mathbb{Z}$ and $\gcd(a, c) = 1$, there exists a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ with a and c in the first column and we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c}.$$

Notice that the isotropy subgroup of ∞ is

$$SL_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}.$$

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and recall that the modular curve $Y(\Gamma)$ is defined as the quotient $\Gamma\backslash\mathbb{H}$ where $\mathbb{H}$ is the upper half complex plane. In order to compactify $Y(\Gamma)$ we consider $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

Definition 3.1. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. The set underlying the *modular curve* $X(\Gamma)$ is the quotient

$$X(\Gamma) := \Gamma\backslash\mathbb{H}^* = Y(\Gamma) \cup (\Gamma\backslash(\mathbb{Q} \cup \{\infty\})).$$

The points Γs with $s \in \mathbb{Q} \cup \{\infty\}$ are called the *cusps* of the modular curve $X(\Gamma)$.

The modular curves for the congruence subgroups $\Gamma(N)$ and $\Gamma_0(N)$ are denoted respectively $X(N)$ and $X_0(N)$.

Since the modular group acts transitively on $\mathbb{Q}\cup\{\infty\}$, the modular curve $X(1)$ has only one cusp. Moreover for every congruence subgroup Γ, the modular curve $X(\Gamma)$ has at most $[SL_2(\mathbb{Z}) : \Gamma]$ cusps, so there are finitely many.

We now define the modular curve $X(\Gamma)$ as a (compact) Riemann surface. First of all we define a basis for the topology on $\mathbb{H}^*$ adjoining to the usual open subsets of $\mathbb{H}$ the sets of the form

$$\alpha(\mathcal{N}_M \cup \{\infty\})$$

where $\alpha \in SL_2(\mathbb{Z})$ and $\mathcal{N}_M := \{\tau \in \mathbb{H} : \mathrm{Im}(\tau) > M\}$ for every $M > 0$. Let

$$\begin{aligned} \pi : \mathbb{H}^* &\to X(\Gamma) \\ s &\mapsto \Gamma s \end{aligned}$$

be the quotient map and endow $X(\Gamma)$ with the quotient topology, making π a continuous map. Moreover π is open: we have already shown that if U is an open subset of $\mathbb{H}$, then $\pi(U)$ is open, so let us consider an open subset of $\mathbb{H}^*$ of the form $\alpha(\mathcal{N}_M \cup \{\infty\})$. We have that $\pi(\alpha(\mathcal{N}_M \cup \{\infty\})) = \Gamma(\alpha(\mathcal{N}_M \cup \{\infty\}))$ is open because its preimage through π is $\bigcup_{\gamma\in\Gamma} \gamma\alpha(\mathcal{N}_M \cup \{\infty\})$, which is open in $\mathbb{H}^*$.

Proposition 3.2. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. The modular curve $X(\Gamma)$ is Hausdorff, connected and compact.*

A proof of this statement can be found in [4, Proposition 2.4.2.]. □

Now we just need to define local charts for the modular curve $X(\Gamma)$ and check that the transition maps are holomorphic. We already defined local charts for a neighbourhood $U \subset \mathbb{H}$ in Chapter 1, so now we study what happens at the cusps.

Definition 3.3. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let $s \in \mathbb{Q} \cup \{\infty\}$. The *width* of s is the number

$$h_s := |SL_2(\mathbb{Z})_s / \{\pm I\}\Gamma_s|.$$

Lemma 3.4. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let $s \in \mathbb{Q} \cup \{\infty\}$. The width h_s is finite. Moreover if $\gamma \in SL_2(\mathbb{Z})$, then the width of $\gamma(s)$ under $\gamma\Gamma\gamma^{-1}$ is the same as the width of s under Γ.*

This lemma is an exercise in [4], so we show the proof.

Proof. We know that there exists $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}_{\geq 1}$. Let $\delta \in SL_2(\mathbb{Z})$ such that $\delta(s) = \infty$; thus $\delta\Gamma(N)\delta^{-1} = \Gamma(N)$. Consequently

$$\begin{aligned} h_s &= |SL_2(\mathbb{Z})_s / \{\pm I\}\Gamma_s| \leq |SL_2(\mathbb{Z})_s / \{\pm I\}\Gamma(N)_s| \\ &= |\delta^{-1} SL_2(\mathbb{Z})_\infty \delta / \{\pm I\}\delta^{-1}\Gamma(N)_\infty \delta| = |SL_2(\mathbb{Z})_\infty / (\{\pm I\}\Gamma(N))_\infty| = N \end{aligned}$$

because $(\{\pm I\}\Gamma(N))_\infty = \{\pm \left(\begin{smallmatrix} 1 & kN \\ 0 & 1 \end{smallmatrix}\right) : k \in \mathbb{Z}\}$. Moreover we have that $(\delta\Gamma\delta^{-1})_\infty \subseteq \pm\langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle$ where h is the width of s under Γ. Consider now $\gamma \in SL_2(\mathbb{Z})$ and we compute the width of $\gamma(s)$ under $\gamma\Gamma\gamma^{-1}$:

$$\begin{aligned} h_{\gamma(s)} &= |SL_2(\mathbb{Z})_{\gamma(s)} / (\{\pm I\}\gamma\Gamma\gamma^{-1})_{\gamma(s)}| = |\gamma SL_2(\mathbb{Z})_s \gamma^{-1} / \gamma(\{\pm I\}\Gamma)_s \gamma^{-1}| \\ &= |SL_2(\mathbb{Z})_s / (\{\pm I\}\Gamma)_s|, \end{aligned}$$

which is the width of s under Γ. □

From Lemma 3.4 we deduce in particular that the width is well-defined on $X(\Gamma)$.

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. Let $s \in \mathbb{Q} \cup \{\infty\}$ and let $\delta \in SL_2(\mathbb{Z})$ such that $\delta(s) = \infty$. Define the open neighbourhood $U := \delta^{-1}(\mathcal{N}_2 \cup \{\infty\})$ of s and $\rho : \mathbb{H}^* \to \mathbb{C}, z \mapsto e^{2\pi i z/h}, \infty \mapsto 0$, where h is the width of s under Γ. As in Chapter 1 we now define

$$\begin{aligned} \psi := \rho \circ \delta : U &\to V \subset \mathbb{C} \\ \tau &\mapsto e^{2\pi i \delta(\tau)/h}, \end{aligned}$$

where $V = (\rho \circ \delta)(U)$. Let $\tau_1, \tau_2 \in U$ and observe that $\pi(\tau_1) = \pi(\tau_2)$ if and only if there exists $\gamma \in \Gamma$ such that $\tau_1 = \gamma(\tau_2)$. Of course this is equivalent to $\delta(\tau_1) = (\delta\gamma\delta^{-1})(\delta(\tau_2))$. We know that $\mathrm{Im}(\delta(\tau_1)) > 2$ and $\mathrm{Im}(\delta(\tau_2)) > 2$. Let $\delta\gamma\delta^{-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. If $c \neq 0$, then

$$2 < \mathrm{Im}(\delta(\tau_1)) = \frac{\mathrm{Im}(\delta(\tau_2))}{|c\delta(\tau_2) + d|^2} < \frac{\mathrm{Im}(\delta(\tau_2))}{c^2 \mathrm{Im}(\delta(\tau_2))^2} < 1/2.$$

We have thus proved that $\delta\gamma\delta^{-1}$ is a translation. Thus $\delta\gamma\delta^{-1} \in \delta\Gamma\delta^{-1} \cap SL_2(\mathbb{Z})_\infty = (\delta\Gamma\delta^{-1})_\infty \subseteq \pm\langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle$ where h is the width of s under Γ.

We conclude that that for all $\tau_1, \tau_2 \in U$, we have

$$\pi(\tau_1) = \pi(\tau_2) \Leftrightarrow \delta(\tau_1) = \delta(\tau_2) + mh \text{ for some } m \in \mathbb{Z} \Leftrightarrow \psi(\tau_1) = \psi(\tau_2).$$

We hence conclude that there exists a bijection

$$\phi : \pi(U) \to V \subset \mathbb{C}$$

such that $\phi \circ \pi = \psi$. By the open mapping theorem ψ is an open map. As also π is open, we get that ϕ is a homeomorphism. We have in this way defined the local charts of $X(\Gamma)$.

It remains to show that the transition maps are holomorphic and this is explained in Diamond and Shurman [4, Chapter 2].

We have thus shown that:

Theorem 3.5. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. The modular curve $X(\Gamma)$ with the complex atlas given above is a compact Riemann surface.*

Proposition 3.6. *Let X be a compact Riemann surface and $f \in \mathbb{C}(X)$ be a meromorphic function on X. Then* $\deg(\mathrm{Div}(f)) = 0$, *where* $\mathrm{Div}(f) = \sum_{x \in X} \mathrm{ord}_x(f) \cdot (x)$ *is the divisor of f.*

Proof. This result is in Bobenko and Klein [1, Corollary 2, Section 2, Chapter1]. □

Let N and M be two positive distinct integers. The function $f_M := \Phi_M(j(\tau), j(N\tau))$ is a meromorphic function on the modular curve $X_0(N)$ and it is holomorphic on $Y_0(N)$. As a consequence all the poles of f_M are at the cusps of $X_0(N)$. Moreover, as $X_0(N)$ is a compact Riemann surface, we have that

$$\deg(\mathrm{Div}_0(f_M)) = \deg(\mathrm{Div}_\infty(f_M))$$

thanks to Proposition 3.6.

3.2 Modular units of $\mathbb{Q}(X_0(N))$

Definition 3.7. A non-zero element of $\mathbb{Q}(X_0(N))$ is called a *modular unit* if all its poles and zeros are cusps.

For every positive natural number M different from N we define the following function on the modular curve $Y_0(N)$:

$$\begin{aligned} f_M : Y_0(N) &\to \mathbb{C} \\ \Gamma_0(N)\tau &\mapsto \Phi_M(j(\tau), j(N\tau)). \end{aligned}$$

In this section we will show that every non-constant product of powers of functions of this form is not a modular unit of $\mathbb{Q}(X_0(N))$.

Proposition 3.8. *Let M be a positive natural number different from N. Then there exists a point $\Gamma_0(N)\tau \in Y_0(N)$ such that $f_M(\Gamma_0(N)\tau) = 0$ and $\mathcal{O}(\Lambda_\tau) = \mathbb{Z}[\sqrt{-MN}]$.*

Proof. Let $L := \mathbb{Z}[\sqrt{-MN}]$ and $L_N := \sqrt{-M/N}\mathbb{Z} + \mathbb{Z}$. Notice that $L \subset L_N$ and $L_N/L \cong \mathbb{Z}/N\mathbb{Z}$, so $[(L, L_N)] \in \mathcal{L}_N$. Let $\Gamma_0(N)\tau \in Y_0(N)$ be the point on the modular curve corresponding to $[(L, L_N)] \in \mathcal{L}_N$ through the bijection in Theorem 1.59. Notice that $\mathcal{O}(L) = \mathbb{Z}[\sqrt{-MN}]$. Thus we are now going to prove that $f_M(\Gamma_0(N)\tau) = 0$: this is equivalent to $[(L, L_N)] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$ by Lemma 2.10. Let $L_M := \sqrt{-N/M}\mathbb{Z} + \mathbb{Z}$. We have that $[(L, L_M)] \in \mathcal{L}_M$ and

$$\sqrt{\frac{-N}{M}} L_N = \sqrt{\frac{-N}{M}} \left(\sqrt{\frac{-M}{N}}\mathbb{Z} + \mathbb{Z} \right) = \sqrt{\frac{-N}{M}}\mathbb{Z} + \mathbb{Z} = L_M.$$

Therefore $\phi_N([(L, L_N)]) = \phi_M([(L, L_M)])$, so $f_M(\Gamma_0(N)\tau) = 0$. □

From Proposition 3.8 we have that f_M is not a modular unit of $\mathbb{Q}(X_0(N))$ for any positive integer M different from N.

We want to prove that also any non-constant product of powers of functions f_M is not a modular unit of $\mathbb{Q}(X_0(N))$. Thus now we want to prove that every function of this form always has a zero or a pole that is not a cusp. To do this we study the properties of the zeros of the functions f_M better:

Lemma 3.9. *Let M be a positive integer different from N and let $\Gamma_0(N)\tau \in Y_0(N)$ be a zero of f_M. The discriminant D of the order $\mathcal{O}(\Lambda_\tau)$ is such that $|D| \leq 4MN$.*

Proof. If $\Gamma_0(N)\tau \in Y_0(N)$ is such that $f_M(\Gamma_0(N)\tau) = 0$, then $[(\Lambda_\tau, \tau\mathbb{Z} + \frac{1}{N}\mathbb{Z})] \in \phi_N^{-1}(\phi_M(\mathcal{L}_M))$ by Lemma 2.10. Thanks to Proposition 2.11 we deduce that $\mathcal{O}(\Lambda_\tau) \neq \mathbb{Z}$ and we have showed in the proof of Proposition 2.11 that there exists $\alpha \in \mathcal{O}(\Lambda_\tau) \setminus \mathbb{Z}$ such that $N(\alpha) = MN$. From the proof of Proposition 1.57 we have then that $|D| \leq 4N(\alpha) = 4MN$. □

Consider a positive integer M different from N. From what we have previously shown we know that

$$\max\big\{|D| \in \mathbb{N} : \exists\ \Gamma_0(N)\tau \in Y_0(N) \text{ s.t. } \mathrm{ord}_{\Gamma_0(N)\tau}(f_M) > 0, \mathcal{O}(\Lambda_\tau) = \mathbb{Z}\,[\tfrac{D+\sqrt{D}}{2}]\big\} \leq 4MN.$$

On the other hand, by Proposition 3.8 we know that there exists a point $\Gamma_0(N)\tau \in Y_0(N)$ such that $f_M(\Gamma_0(N)\tau) = 0$ and the absolute value of the discriminant of $\mathcal{O}(\Lambda_\tau)$ is $4MN$. As a consequence we have

$$\max\big\{|D| \in \mathbb{N} : \exists\ \Gamma_0(N)\tau \in Y_0(N) \text{ s.t. } \mathrm{ord}_{\Gamma_0(N)\tau}(f_M) > 0, \mathcal{O}(\Lambda_\tau) = \mathbb{Z}\,[\tfrac{D+\sqrt{D}}{2}]\big\} = 4MN. \tag{3.1}$$

Consider a function $F \in \mathbb{Q}(X_0(N))$ that is a combination of the f_M's:

$$F = \prod_{\substack{M \in \mathbb{Z}_{\geq 1} \\ M \neq N}} f_M^{e_M} \tag{3.2}$$

such that F is non-constant, $e_M \in \mathbb{Z}$ and just finitely many of the exponents e_M are different from 0.

Theorem 3.10. *Let $F \in \mathbb{Q}(X_0(N))$ as in (3.2). Then F is not a modular unit.*

Proof. Let $P := \max\{M \in \mathbb{Z}_{\geq 1}, M \neq N : e_M \neq 0\}$. Thanks to Proposition 3.8 we know that there exists $\tau \in \mathbb{H}$ such that $\mathrm{ord}_{\Gamma_0(N)\tau}(f_P) > 0$ and $\mathcal{O}(\Lambda_\tau) = \mathbb{Z}[\sqrt{-NP}]$. As a consequence $\mathrm{ord}_{\Gamma_0(N)\tau}(f_M) = 0$ for all $M \in \mathbb{Z}_{\geq 1}$ with $M < P$ and $M \neq N$ by Lemma 3.9. This means that

$$\mathrm{ord}_{\Gamma_0(N)\tau}(F) = \mathrm{ord}_{\Gamma_0(N)\tau}\Big(\prod_{\substack{M \in \mathbb{Z}_{\geq 1} \\ M \neq N}} f_M^{e_M}\Big) = e_P \cdot \mathrm{ord}_{\Gamma_0(N)\tau}(f_P) \neq 0. \tag{3.3}$$

Therefore we have proved that F has a complex multiplication point as zero or pole and therefore it is not a modular unit of $\mathbb{Q}(X_0(N))$. □

3.3 The degree of the function F

The main result of this section is to give a lower bound of the degree of a function F as in (3.2). We start defining the degree of a function.

Definition 3.11. Let k be a field, C/k a curve and $k(C)$ the function field of C over k. Given a function $f \in k(C)$, the *degree* of f is the integer

$$\deg(f) = \deg(\mathrm{Div}_0(f)) = \deg(\mathrm{Div}_\infty(f)).$$

Now consider again a function $F \in \mathbb{Q}(X_0(N))$ that is a multiplicative combination of the functions f_M constructed as before:

$$F = \prod_{\substack{M \in \mathbb{Z}_{\geq 1} \\ M \neq N}} f_M^{e_M} \tag{3.4}$$

where F is non-constant, $e_M \in \mathbb{Z}$ and just finitely many of the e_M's are different from 0. Take $P := \max\{M \in \mathbb{Z}_{\geq 1}, m \neq N : e_M \neq 0\}$. We now notice that

$$\begin{aligned}&\deg(F)\\ &\geq \left|\left\{\Gamma_0(N)\tau \in Y_0(N) : \mathrm{ord}_{\Gamma_0(N)\tau}(f_P) > 0 \text{ and } \mathrm{ord}_{\Gamma_0(N)\tau}(f_M) = 0 \text{ for all } M < P\right\}\right|.\end{aligned}$$

We have previously showed that all the zeros $\Gamma_0(N)\tau$ of f_P such that $\mathcal{O}(\Lambda_\tau) = \mathbb{Z}[\sqrt{-NP}]$ are such that $\mathrm{ord}_{\Gamma_0(N)\tau}(f_P) > 0$ and moreover $\mathrm{ord}_{\Gamma_0(N)\tau}(f_M) = 0$ for all $M < P$, thus

$$\deg(F) \geq |\{\Gamma_0(N)\tau \in Y_0(N) : \mathrm{ord}_{\Gamma_0(N)\tau}(f_P) > 0 \text{ and } \mathcal{O}(\Lambda_\tau) = \mathbb{Z}[\sqrt{-NP}]\}|. \tag{3.5}$$

Proposition 3.12. *Let M and N be two different positive integers and let f_M be the function $\Phi_M(j(\tau), j(N\tau))$ on the modular curve $X_0(N)$. Then we have*

$$\begin{aligned}&|\{\Gamma_0(N)\tau \in Y_0(N) : \mathrm{ord}_{\Gamma_0(N)\tau}(f_M) > 0, \mathcal{O}(\Lambda_\tau) = \mathbb{Z}[\sqrt{-MN}]\}|\\ &\geq |\mathrm{Pic}(\mathbb{Z}[\sqrt{-MN}])|.\end{aligned}$$

The case where M and N are coprime and not both squares is immediate from Theorem 2.1 and (3.3). We will now check that the proof holds in general.

Proof. Let $\mathcal{O} := \mathbb{Z}[\sqrt{-MN}]$ to simplify the notation. Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}$-ideal; first of all we prove that $[(L_1, L)]$ is an element of $\mathcal{L}_N$, where $L := \mathfrak{a}$ and $L_1 := N\mathfrak{a} + \sqrt{-MN}\mathfrak{a}$:

$$\begin{aligned}\mathfrak{a}/(N\mathfrak{a} + \sqrt{-MN}\mathfrak{a}) &\cong \mathfrak{a}/(N\mathcal{O} + \sqrt{-MN}\mathcal{O})\mathfrak{a}\\ &\cong \mathcal{O}/(N\mathcal{O} + \sqrt{-MN}\mathcal{O}) \cong \mathbb{Z}/N\mathbb{Z},\end{aligned}$$

where the second isomorphism derives from Lemma 1.58. Consider now the point $\Gamma_0(N)\tau \in Y_0(N)$ corresponding to the element $[(L_1, L)] \in \mathcal{L}_N$. We prove that it is a zero of the function f_M. For this we just have to prove that $\phi_N([(L_1, L)]) \in \phi_M(\mathcal{L}_M)$. The element $[(L_2, L)] := [(M\mathfrak{a} + \sqrt{-MN}\mathfrak{a}, \mathfrak{a})] \in \mathcal{L}_M$ is such that

$$\sqrt{\frac{-M}{N}}L_1 = \sqrt{\frac{-M}{N}}(N\mathfrak{a} + \sqrt{-MN}\mathfrak{a}) = M\mathfrak{a} + \sqrt{-MN}\mathfrak{a} = L_2.$$

Thus $\phi_N([(L_1, L)]) \in \phi_M([(L_2, L)])$. We have showed that every element $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ gives rise to a different zero $\Gamma_0(N)\tau$ of the function f_M such that $\mathcal{O}(\Lambda_\tau) = \mathcal{O}$ and this concludes the proof. □

From (3.5) and from Proposition 3.12 we deduce that

$$\deg(F) \geq |\mathrm{Pic}(\mathbb{Z}[\sqrt{-NP}])|. \tag{3.6}$$

We now try to give an estimate of this order.

Theorem 3.13 (Siegel's Theorem)**.** *Given any imaginary quadratic number field K, let d_K be its discriminant and let h_K be its class number. Then as $|d_K| \to \infty$ we have*

$$\log(h(\mathcal{O}_K)) \sim \log(\sqrt{|d_K|}).$$

A reference for this result is [7].

Thus we have

$$\lim_{|d_K|\to\infty} \frac{\log(|\mathrm{Pic}(\mathcal{O}_K)|)}{\log(\sqrt{|d_K|})} = 1.$$

In particular, for every $\epsilon > 0$ there exists $J \in \mathbb{Z}_{>0}$ such that for all $|d_K| > J$, we have

$$\frac{\log(|\mathrm{Pic}(\mathcal{O}_K)|)}{\log(\sqrt{|d_K|})} > 1 - \epsilon.$$

This means that for every $\epsilon > 0$ there exists $J \in \mathbb{Z}_{>0}$ such that for all $|d_K| > J$

$$|\mathrm{Pic}(\mathcal{O}_K)| > (\sqrt{|d_K|})^{1-\epsilon}.$$

In our case it could happen that $\mathbb{Z}[\sqrt{-NP}]$ is not the ring of integers $\mathcal{O}_K$, but the following theorem shows that the same asymptoties hold. First we give the following definitions:

Definition 3.14. Let p be an odd prime. An integer n is a *quadratic residue modulo p* if it is congruent to a perfect square modulo p.

Definition 3.15. Let p be an odd number and $n \in \mathbb{Z}_{>0}$. The *Legendre symbol* is a function of n and p defined as follows:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 \text{ if } n \text{ is a quadrtaic residue modulo } p \text{ and } n \not\equiv 0 \pmod{p} \\ -1 \text{ if } n \text{ is not a quadratic residue modulo } p \\ 0 \text{ if } n \equiv 0 \pmod{p}. \end{cases}$$

Definition 3.16. Let n be a positive integer. The *Kronecker symbol* is

$$\left(\frac{n}{2}\right) = \begin{cases} 0 \text{ if } n \text{ is even} \\ 1 \text{ if } n \equiv \pm 1 \pmod{8} \\ -1 \text{ if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

Theorem 3.17 (Theorem 7.24 of [2])**.** *Let $\mathcal{O}$ be the order of conductor f in an imaginary quadratic number field K with discriminant d_K. Then*

$$|\mathrm{Pic}(\mathcal{O})| = \frac{|\mathrm{Pic}(\mathcal{O}_K)| \cdot f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \cdot \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

Theorem 3.18. *For every $\epsilon > 0$ there exists $J \in \mathbb{Z}_{>0}$ such that for all $P > J$ and $F \in \mathbb{Q}(X_0(N))$ as in (3.4) such that $P = \max\{M \in \mathbb{Z}_{\geq 1}, M \neq N : e_M \neq 0\}$, we have*

$$\deg(F) \geq (\sqrt{4NP})^{1-\epsilon} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right),$$

where f is the conductor of the order $\mathbb{Z}[\sqrt{-NP}]$ and d_K is the discriminant of its field of fractions.

Proof. From Theorem 3.17, for every $\epsilon > 0$ there exists $J \in \mathbb{Z}_{>0}$ such that for all $P > J$ we have

$$\begin{aligned} |\mathrm{Pic}(\mathbb{Z}[\sqrt{-NP}])| &\geq (\sqrt{|d_K|})^{1-\epsilon} f \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \\ &= (\sqrt{|d_K|f^2})^{1-\epsilon} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right) \\ &= (\sqrt{4NP})^{1-\epsilon} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right). \end{aligned}$$

Let $F \in \mathbb{Q}(X_0(N))$ as in (3.4) such that $P = \max\{M \in \mathbb{Z}_{\geq 1}, M \neq N : e_M \neq 0\}$. By (3.6) we conclude that

$$\deg(F) \geq (\sqrt{4NP})^{1-\epsilon} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

□

Bibliography

[1] Bobenko Alexander I., Klein Christian, Computational Approach to Riemann Surfaces, Springer,Verlag Berlin Heidelberg, 2011.

[2] Cox, David A, Primes of the form $x^2 + ny^2$, Fermat, class field theory, and complex multiplication, John Wiley & Sons, Hoboken, New Jersey, 2013.

[3] Derickx Maarten, van Hoeij Mark, Gonality of the modular curve $X_1(N)$, Journal of Algebra 417 (2014) 52-71, `https://www.sciencedirect.com/science/article/pii/S0021869314003585`.

[4] Diamond Fred, Shurman Jerry, A First Course in Modular Forms, Springer, New York, 2005.

[5] Lang Serge, Algebra, Springer New York, New York, 2002.

[6] Rudin Walter, Real and Complex Analysis, Tata McGraw-Hill, New Delhi, 1974.

[7] Siegel Carl Ludwig, Über die Classenzahl quadratischer Zahlkörper, Acta Arithmetica (1935), vol. 1, issue 1 83-86.

[8] Stevenhagen Peter, Number rings, Lecture notes of the course Algebraic Number Theory in Leiden, 2017, `http://websites.math.leidenuniv.nl/algebra/ant.pdf`.

[9] Streng Marco, Generators of the group of modular units for $\Gamma_1(N)$ over $\mathbb{Q}$, 2015, `https://arxiv.org/abs/1503.08127v2`.

[10] The PARI Group, PARI/GP version `2.11.0`, Univ. Bordeaux, 2018, `http://pari.math.u-bordeaux.fr/`.