Universidad de Guanajuato

Trabajo de tesis para la obtención de título de

Licenciatura en Matemáticas

Applications of the Arithmetic Theory of Elliptic Curves

Autor
José Ibrahim
Villanueva Gutiérrez

Director de Tesis
Dr. Xavier
Gómez-Mont Ávalos

18 de Agosto del 2012

A mis padres Verónica y Manuel,
a mis abuelos Margarita y José,
y a mi familia.

Contents

Chapter 1

Elliptic Functions

A *Complex Torus* is a compact Riemann surface of genus 1. It is the set of equivalence classes of the quotient $\mathbb{C}/L$, where $L = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ is a *lattice*, i.e. a discrete subgroup of $\mathbb{C}$ generated by two complex numbers ω_1 and ω_2 linearly independent over $\mathbb{R}$. The projection

$$\pi : \mathbb{C} \to \mathbb{C}/L$$

$$z \mapsto z \bmod(L),$$

is continuous and open, this makes $\mathbb{C}/L$ a Haussdorf, connected and compact topological space. Its complex structure can be defined by the set of triples (π^{-1}, U, V), where

$$\pi^{-1} : U \subset \mathbb{C}/L \to V \subset \mathbb{C}$$

and such that $\pi : V \to U$ is a homeomorphism. In this way $\mathbb{C}/L$ is a Riemann surface.

Algebraically a complex torus is an abelian group, the addition of points is the usual addition on $\mathbb{C}$ modulus L.

Topologically, $\mathbb{C}/L$ is homeomorphic to the torus $S^1 \times S^1$ via the map

$$x\omega_1 + y\omega_2 \mapsto (e^{2\pi ix}, e^{2\pi iy}), \text{ with } x, y \in \mathbb{R},$$

then geometrically one can figure out the complex torus as a doughnut shaped bubble (Fig 1.1).

We say that a function f is meromorphic in W an open subset of $\mathbb{C}/L$ if and only if $f \circ \pi$ is meromorphic on $\pi^{-1}(W)$. It turns out that the function $f \circ \pi$ is L-periodic, that is

$$f(z + \omega) = f(z) \text{ for all } z \in \mathbb{C} \text{ and } \omega \in L;$$

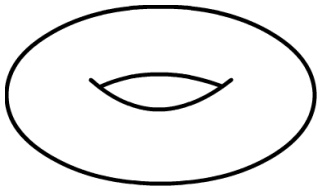

Figure 1.1: Torus

thus there is a correspondence between functions on $\mathbb{C}/L$ and L-periodic functions on $\mathbb{C}$. A meromorphic L-periodic function on $\mathbb{C}$ is called an *elliptic function*, then the next one-to-one correspondence holds

$$\left\{ \begin{array}{c} \text{Elliptic functions} \\ \text{on } \mathbb{C} \end{array} \right\} \overset{1-1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{Meromorphic functions} \\ \text{on } \mathbb{C}/L \end{array} \right\}.$$

Trough all this chapter we will work with elliptic functions. We will see that the set of basis for L is invariant under the action of the special linear group $SL_2(\mathbb{Z})$ and that we can find a positive ordered basis (ω_1, ω_2) for L such that the quotient $\tau = \omega_2/\omega_1$ lies in a fundamental domain $\mathcal{B} \subset \mathbb{H}$.

L-periodicity implies that elliptic functions are totally defined in a representant of $\mathbb{C}/L$, this fundamental domain turns out to be a domain shaped parallelogram. This allows us to restrict our study of elliptic functions into a fundamental parallelogram and prove the next facts about elliptic functions.

Holomorphic elliptic functions must be constants because of Liouville's Theorem. The number of poles and zeros inside a fundamental parallelogram must be the same counting multiplicities and its location on the plane is not random at all.

The residue of any elliptic function on a fundamental domain is zero, thus the simplest kinds of non-constant elliptic functions are those which have two simple poles with residues equal in absolute value but opposite sign or elliptic functions with a double pole with residue zero, these elliptic functions are called Weierstrass-$\wp$ functions. Due to their importance we will study them in great detail in this chapter and the beginning of the next chapter.

The map

$$\varphi : \mathbb{C}/\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} \to \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z},$$

is an holomorphic isomorphism between complex tori.

The set of all meromorphic functions on $\mathbb{C}/L$, denoted $\mathcal{M}(\mathbb{C}/L)$ forms a field denoted $\mathcal{E}_L$. We show that this field is generated by two elliptic functions: the Weierstrass $\wp-$function and its derivative, moreover we study a differential equation that relates both functions.

In this chapter, we will expose all these results with some detail, from a basic complex analysis aproach, we study important examples of elliptic and quasi-elliptic functions which turn out to be related with Number Theory.

1.1 Periods of meromorphic functions

The meromorphic functions defined on an open connected set in the complex plane form a field. In what follows, a meromorphic function is supposed to mean a function meromorphic in the whole complex plane denoted $\mathbb{C}$.

A meromorphic function f is said to be *periodic*, if there exists a complex constant $\omega \neq 0$, such that

$$f(z+\omega) = f(z)$$

for all $z \in \mathbb{C}$. The number ω is said to be a *period* of f. The number zero is called the *trivial period*. Every constant function f is periodic, and every complex number is a period of f; conversely if every complex number is a period of a meromorphic function f, then f must be constant. If ω is a period, so are all integral multiples $n\omega$. Let $\mathrm{per}(f)$ be the set of all the periods, if ω_1 and ω_2 belong to $\mathrm{per}(f)$, so does any linear combination $m\omega_1 + n\omega_2$ with $m, n \in \mathbb{Z}$. Thus the set $\mathrm{per}(f)$ is a $\mathbb{Z}$-module $\subset \mathbb{C}$ and we call it the *period module* of f.

Lemma. *Let f be a non-constant meromorphic function, then all the points of* $\mathrm{per}(f)$ *are isolated.*

Proof. Suppose ω_0 is a finite accumulation point of $\mathrm{per}(f)$. Let ε be an arbitrarily small positive number. We can find two different periods ω_1, ω_2 inside the open disk $|z - \omega_0| < \varepsilon$, evidently $\omega_1 - \omega_2$ is a period. Then there exists a sequence of periods say $\{\omega_n\}$ such that $\lim_{n\to\infty} \omega_n = 0$. If z_0 is

a point at which f is holomorphic then $f(z_0) = f(z_0 + \omega_n)$, $n = 1, 2, ...$, so that $f(z) - f(z_0)$ has an infinity of zeros $z_0 + \omega_n$, $n = 1, 2, ...$, which have z_0 as a finite accumulation point. Hence $f(z)$ is a constant, contradicting our assumption.

■

Then if f is non-constant, $\mathrm{per}(f)$ is an abelian discrete closed group and it contains a period ω of minimal absolute value.

Theorem 1. *The period module* $\mathrm{per}(f)$ *of a non-constant meromorphic function consists either of zero alone, of the integral multiples* $n\omega$ *of a single period or of all linear combinations* $n\omega_1 + m\omega_2$ *with integral coefficients of two periods* ω_1, ω_2 *with* $\mathrm{Im}(\omega_2/\omega_1) \neq 0$.

Proof. Suppose $\mathrm{per}(f) \neq \{0\}$, let ω_1 be a period of minimal absolute value and suppose that for every $\omega \in \mathrm{per}(f)$ the quotient ω/ω_1 is real, then for every ω there exists an integer k such that

$$0 \leq \frac{\omega}{\omega_1} - k < 1.$$

Then the difference, $\omega - k\omega_1 = \omega_0$ is a period with $|\omega_0| < |\omega_1|$, thus $\omega_0 = 0$ and $\omega = k\omega_1$. It follows that every period ω whose quotient is real is of the form $k\omega_1$, $k \in \mathbb{Z}$.

Now, let $\omega \in \mathrm{per}(f)$ such that the quotient ω/ω_1 is not real, let ω_2 denote one such period whose absolute value is smallest. Let $\tau = \omega_2/\omega_1$, so $|\tau| \geq 1$.

Every complex number z can be written uniquely in the form

$$z = (m + \alpha)\omega_1 + (n + \beta)\omega_2,$$

where $m, n \in \mathbb{Z}$ and $-1/2 \leq \alpha < 1/2$, $-1/2 \leq \beta < 1/2$. Then, we can write $\omega = (m + \alpha)\omega_1 + (n + \beta)\omega_2$, it follows that

$$\omega_0 = \omega - m\omega_1 - n\omega_2 = \alpha\omega_1 + \beta\omega_2$$

is a period. If α or β are zero, then $\omega_0 = 0$ and this immediately proves our assertion. Suppose both are non-zero, thus

$$\left|\frac{\omega_0}{\omega_2}\right| = \left|\frac{\alpha}{\tau} + \beta\right| \leq \frac{|\alpha|}{|\tau|} + |\beta| \leq 1$$

since $|\tau| \geq 1$.

The right inequality holds if and only if $\alpha = \beta = -1/2$ and $|\tau| = 1$. Then $|1+\tau| < 2$ since $\mathrm{Im}(\tau) > 0$ (see Figure 1.2), that is the first inequality is strict.

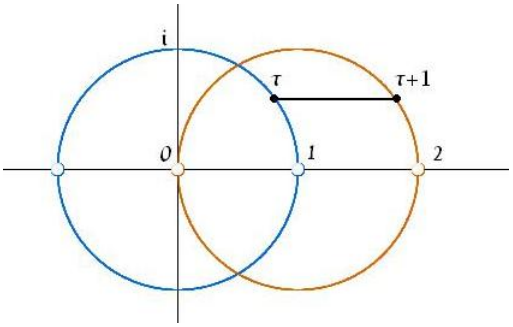

Figure 1.2: The orange circle is the image of the map $\tau \mapsto \tau+1$ when $|\tau| = 1$ and $\mathrm{Im}(\tau) > 0$.

Then, at least one of the inequalities is strict, that is $|\omega_0| < |\omega_2|$. It follows that ω_0/ω_1 is real and $\beta = 0$, hence also that $\alpha = 0$. Therefore $\omega_0 = 0$, we conclude that every period ω of f is a linear combination $\omega = m\omega_1 + n\omega_2$, with $m, n \in \mathbb{Z}$.

■

If $\mathrm{per}(f)$ is generated by a single period $\omega_1 \neq 0$, f is said to be *simply periodic*. In case that $\mathrm{per}(f)$ is generated by a pair of periods ω_1 and ω_2 which are linearly independent over $\mathbb{R}$, f is said to be *doubly periodic*. Let $\tau = \omega_2/\omega_1$, if ω_1 is a period of minimal absolute value, $|\omega_2|$ is small as possible, and $\mathrm{Im}(\tau) > 0$, we say such pair is *primitive* or *reduced*, i.e. such pair of periods form an ordered positive oriented basis for $\mathrm{per}(f)$. Geometrically, $\mathrm{per}(f)$ forms a *lattice* in the complex plane.

Example 1. The integral domain of the *Gaussian integers*

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

forms a square lattice, see Figure 1.3.

★

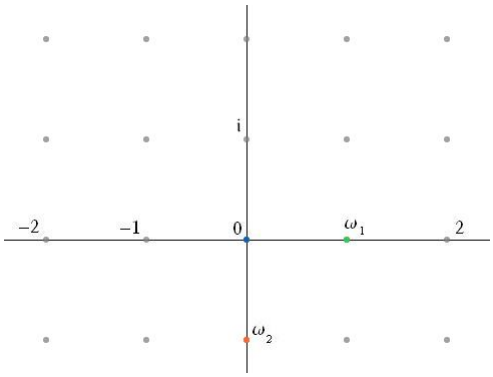

Figure 1.3: The lattice of the Gaussian integers generated by two non-reduced periods.

Example 2. Let ω be a primitive cube root of the unity, say $e^{2\pi i/3}$. Then the set of Eisenstein integers

$$\{a + b\omega \mid a, b \in \mathbb{Z}\}$$

forms a triangular lattice which periods are ω and 1, see Figure 1.4.

★

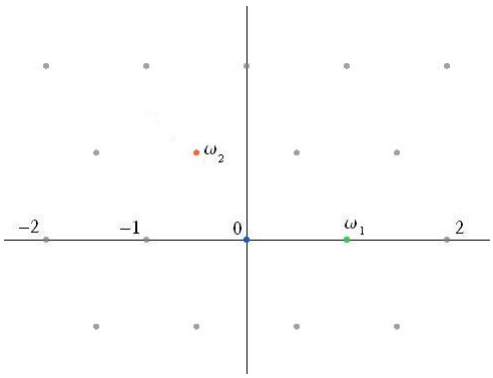

Figure 1.4: The lattice of the Eisenstein integers generated by two reduced periods.

Definition. A doubly periodic meromorphic function in the complex plane is called an *elliptic function*.

We have seen in the previous examples, that the period module of an elliptic function may have several associated bases. Now we exhibit the relation between two such bases.

Theorem 2. *The complex numbers ω_1^*, ω_2^* form a pair of basic periods of an elliptic function $f(z)$, if and only if they are related to a pair of basic periods ω_1, ω_2 of $f(z)$ by a transformation of the type*

$$\omega_1^* = a\omega_1 + b\omega_2$$

$$\omega_2^* = c\omega_1 + d\omega_2$$

where a, b, c, d are integers, with the property $ad - bc = \pm 1$.

Such transformation of (ω_1, ω_2) into (ω_1^*, ω_2^*) is called a unimodular transformation. *A unimodular transformation is said to be a* proper unimodular transformation *if $ad - bc = 1$.*

Proof. $\Rightarrow$) Since (ω_1, ω_2) is a basis there exist integers a, b, c, d such that

$$\begin{pmatrix} \omega_1^* \\ \omega_2^* \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

Similarly, since (ω_1^*, ω_2^*) is a basis there exists integers a', b', c', d' such that

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \omega_1^* \\ \omega_2^* \end{pmatrix},$$

then we obtain

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

then the matrices are inverses of each other, so they must satisfy

$$\det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1,$$

since the entries are integers, the determinants have value ± 1.

$\Leftarrow$) Let $\omega = m\omega_1 + n\omega_2 \in \mathrm{per}(f)$, and

$$\omega_1^* = a\omega_1 + b\omega_2$$

$$\omega_2^* = c\omega_1 + d\omega_2,$$

with $ad - bc = \pm 1$, then there exists an inverse unimodular transformation such that

$$\omega_1 = d\omega_1^* - b\omega_2^*$$
$$\omega_2 = a\omega_2^* - c\omega_1^*$$

therefore every $\omega \in \mathrm{per}(f)$ can be written uniquely as $\omega = m'\omega_1^* + n'\omega_2^*$, with m', n' integers.

■

Two bases of reduced periods for an elliptic function f are related via a proper unimodular transformation, for let (ω_1, ω_2) and (ω_1^*, ω_2^*) be such bases, where $\omega_1^* = m\omega_1 + n\omega_2$ and $\omega_2^* = p\omega_1 + q\omega_2$ with $m, n, p, q \in \mathbb{Z}$ and let $\tau = \omega_2/\omega_1$ and $\tau^* = \omega_2^*/\omega_1^*$. Then

$$\mathrm{Im}(\tau^*) = \frac{mq - np}{|n\tau + m|^2}\mathrm{Im}(\tau),$$

this implies $mq - np = 1$. Moreover, this transformations induce a *modular transformation*

$$M : \mathbb{H} \to \mathbb{H},$$

such that

$$\tau \mapsto \tau^* = \frac{m\tau + n}{p\tau + q},\ m, n, p, q \in \mathbb{Z},\ \tau \in \mathbb{H},$$

with $mq - np = 1$, and $p\tau + q \neq 0$. These transformations form a group, called the *modular group*, which we denote Γ, it is generated by the two transformations

$$A : \tau \to \tau + 1, \quad \text{and} \quad B : \tau \to -\frac{1}{\tau}. \tag{1.1}$$

Where A is a translation and B is an inversion followed by a reflection. The set

$$\mathrm{SL}(2, \mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1\}$$

is a *discrete* subgroup of the *complex special linear group* $SL(2, \mathbb{C})$ with identity I. There is a natural inclusion of the modular group into the Möbius transformations. Both facts yield the group isomorphism

$$SL(2, \mathbb{Z})/\{I, -I\} \cong \Gamma,$$

thus Γ acts *properly discontinuously* on the upper-half plane $\mathbb{H}$.

Theorem 3. *A pair of basic periods ω_1, ω_2 is reduced if and only if the point $\tau = \omega_2/\omega_1 = \xi + i\eta$ lies in the region of the upper half of the complex plane defined by the three inequalities*

$$\xi^2 + \eta^2 \geq 1, \qquad -\frac{1}{2} \leq \xi \leq \frac{1}{2}. \tag{1.2}$$

Proof. $\Rightarrow$) Suppose the pair (ω_1, ω_2) is reduced, then we have

$$|\omega_2 \pm \omega_1| \geq |\omega_2| \geq |\omega_1|,$$

since the quotient $\operatorname{Im}\left(\frac{\omega_2 \pm \omega_1}{\omega_1}\right) > 0$, so dividing by $|\omega_1|$ we have

$$(\xi \pm 1)^2 + \eta^2 = |\tau + 1|^2 \geq \xi^2 + \eta^2 = |\tau|^2 \geq 1,$$

and $\pm 2\xi + 1 \geq 0$, from which follow (1.2).

$\Leftarrow$) Let ω_2, ω_1 be two periods such that $\tau = \omega_2/\omega_1 = \xi + i\eta$ lies in the region defined by (1.2). By hypothesis, $|\tau| \geq 1$ and $\operatorname{Im}(\tau) > 0$, that is $|\omega_2| \geq |\omega_1|$ and τ is non-real. Then it suffices to show that ω_1 and ω_2 have minimal absolute value, for this consider any non-trivial period $\omega = m\omega_1 + n\omega_2$, $m, n \in \mathbb{Z}$.

If $n = 0$, then $\omega/\omega_1 = m$, where $m \in \mathbb{Z}^*$ since ω is non-trivial, hence $|\omega| \geq |\omega_1|$.

If $n \neq 0$, then ω/ω_1 is not real, since ω_2/ω_1 is not. Then

$$|\omega| \geq |\omega_2| \Leftrightarrow |m + n\tau|^2 - |\tau|^2 \geq 0,$$

thus set

$$D = |m + n\tau|^2 - |\tau|^2 = (m + n\xi)^2 - \xi^2 + (n^2 - 1)\eta^2.$$

If $n \neq \pm 1$, and m any integer, then we have $n^2 \geq 4$, $\xi^2 \leq 1/4$ and $\eta^2 = (\xi^2 + \eta^2) - \xi^2 \geq 3/4$, so

$$D \geq (m + n\xi)^2 - \xi^2 + \frac{9}{4} \geq 2.$$

If $n = \pm 1$, then

$$D = (m \pm \xi)^2 - \xi^2 = m^2 \pm 2m\xi \geq 0$$

since $|\xi| \leq 1/2$. Thus if $n \neq 0$, $|\omega| \geq |\omega_2|$.

We conclude that the pair ω_1, ω_2 is reduced.

■

In order to find a region where the action of the modular group Γ is *non-transitive*, we sharpen the previous theorem somewhat.

The boundary of the region defined by the inequalities (1.2), consists of the rays $\xi = \pm 1/2$, $\eta \geq \sqrt{3}/2$ and the arc $\xi^2 + \eta^2 = 1$ with $|\xi| \leq 1/2$, see Figure 1.5.

If τ belongs to the right ray, then $\tau^* = \tau - 1$ belongs to the left ray. Similarly if τ belongs to the right half arc, then $\tau^* = -\tau^{-1}$ belongs to the left half arc.

Then given a non-constant elliptic function, there exists a pair of reduced periods (ω_1, ω_2) such that $\tau = \omega_2/\omega_1 = \xi + i\eta$ satisfies

$$\begin{aligned} \xi^2 + \eta^2 \geq 1 \text{ and } -\frac{1}{2} \leq \xi < \frac{1}{2}; \text{ with} \\ -1/2 \leq \xi \leq 0, \text{ if } |\tau| = 1, \end{aligned} \tag{1.3}$$

Now we prove that a pair (ω_1, ω_2) of reduced periods which quotient τ satisfies (1.3) is uniquely determined.

Suppose (ω_1, ω_2) and (ω_1^*, ω_2^*) are two pairs of such reduced periods, thus they are related by a proper unimodular transformation, say $\omega_1^* = a\omega_1 + b\omega_2$, $\omega_2^* = c\omega_1 + d\omega_2$, with $ad - bc = 1$. Also we have

$$|\omega_2| \geq |\omega_1| = |\omega_1^*| \leq |\omega_2^*| \text{ and } \operatorname{Im}(\tau) = \operatorname{Im}(\tau^*).$$

If $b = 0$, then $a = d = \pm 1$. So that $\tau^* = \tau \pm c$ implies $c = 0$, therefore $\tau = \tau^*$.

If $b \neq 0$, ω_1^*/ω_1 is not real, then as in the previous theorem $b = \pm 1$, $|\omega_1| = |\omega_1^*| = |\omega_2|$, $|\tau| = 1$, $-1/2 \leq \xi \leq 0$, and $a = 0$ or $a = \pm 1$.

In case $a = 0$, $\tau^* = \pm d \mp \tau^{-1}$, $-1 \leq \operatorname{Re}(\tau) + \operatorname{Re}(\tau^*) = \pm d < 1$ since $|\tau| = 1$, thus $d = 0$ or $d = -1$. If $d = 0$, then $\tau^* = -\tau^{-1}$, so $\tau^* = \tau = i$. If $d = -1$, then $\operatorname{Re}(\tau) = \operatorname{Re}(\tau^*) = -1/2$, so $\tau^* = \tau = e^{2\pi i/3}$.

In case $a = \pm 1$, we have $|\tau + 1| = 1 = |\tau|$, and therefore $\tau = e^{2\pi i/3}$, and since $\operatorname{Im}(\tau) = \operatorname{Im}(\tau^*)$, we must have $\tau = \tau^* = e^{2\pi i/3}$.

Therefore the conditions (1.3) determine τ uniquely.

We denote $\mathcal{B}$ the set defined by (1.3), it is *a fundamental domain* for the modular group Γ, see Figure 1.5. That is, the fundamental domain $\mathcal{B}$

contains all the representatives of the different equivalence classes given by the action of Γ in $\mathbb{H}$, for $\tau_1, \tau_2 \in \mathbb{H}$ we define the equivalence relation

$$\tau_1 \sim \tau_2 \Leftrightarrow \exists M \in \Gamma \text{ such that } \tau_2 = M\tau_1.$$

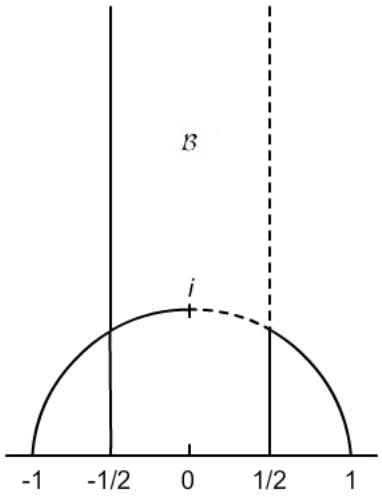

Figure 1.5: Fundamental domain

Definition. A complex-valued function $f(z)$ of one complex variable z is said to be a *modular function*, if it is meromorphic in $\mathbb{H}$, and $f(Mz) = f(z)$ for all transformations M belonging to the modular group Γ, or for all M belonging to a subgroup of the modular group of finite index.

1.2 General properties of elliptic functions

Given an elliptic function f, let (ω_1, ω_2) be a pair of reduced periods for its period-lattice $L = \{m\omega_1 + n\omega_2 | m, n \in \mathbb{Z}\}$. Let $\Pi_{m,n}$, be the set defined by

$$\Pi_{m,n} = \{z \in \mathbb{C} | z = x\omega_1 + y\omega_2, m \leq x < m+1, n \leq y < n+1,\ m, n \in \mathbb{Z}\}.$$

Then every lattice element defines a parallelogram $\Pi_{m,n}$, which we call a *period-parallelogram*. Since f is elliptic, it suffices to consider $\Pi_{0,0} = \Pi$ a

fundamental period-parallelogram, see Figure 1.6. We consider the passage from 0 to ω_1, $\omega_1 + \omega_2$, ω_2, and back to 0, in that order, defines a positive orientation of the curve $\partial\Pi$, we denote each of those segments c_1, c_2, c_3 and c_4, respectively.

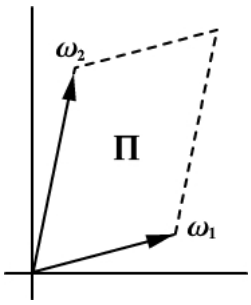

Figure 1.6: Fundamental parallelogram

Let $\mathcal{E}_L$ denote the set of the elliptic functions for a lattice L. Every constant is, trivially an elliptic function. If $f, g \in \mathcal{E}_L$, then their sum $f + g$, their difference $f - g$, their product $f * g$ and, if g is not identically zero, their quotient f/g are all elliptic functions. Thus the set $\mathcal{E}_L$ forms a field. In addition, $\mathcal{E}_L$ is closed under differentiation.

We now prove a sequence of propositions giving some very special properties which any elliptic function must have.

Theorem 4. *A function $f \in \mathcal{E}_L$ without poles in the fundamental parallelogram Π must be constant.*

Proof. Any such function must be entire and bounded on $\overline{\Pi}$, since $\overline{\Pi}$ is compact. Hence by Liouville's theorem, is a constant.

■

Notice that, since a meromorphic function f can only have finitely many poles in a bounded region, it is always possible to choose an α such that the boundary of $\alpha + \Pi$ misses the poles of f, so let $\alpha + \Pi = \{\alpha + z | z \in \Pi\}$ denote the translate of Π by the complex number α.

Theorem 5. *Suppose that $f \in \mathcal{E}_L$ has no poles on the boundary C of $\alpha + \Pi$, for some α. Then the sum of the residues of f in $\alpha + \Pi$ is zero.*

Proof. By the residue theorem, this sum is equal to

$$\frac{1}{2\pi i}\int_C f(z)dz.$$

Let $C = c_1 + c_2 + c_3 + c_4$, where the c_i's are the sides of $\alpha + \Pi$ (choosing a positive orientation), then we have

$$\int_{c_1} f(z)dz + \int_{c_3} f(z)dz = 0 \text{ and } \int_{c_2} f(z)dz + \int_{c_4} f(z)dz = 0$$

because of the periodicity of f. Thus the integral is zero, and so the sum of residues is zero.

■

The preceding theorems immediately imply that a non-constant elliptic function cannot have just one simple pole in a period-parallelogram. It must have therefore at least two simple poles, or at least one pole which is not simple, in any period-parallelogram.

Theorem 6. *Suppose that $f \in \mathcal{E}_L$ is not constant and has no poles on the boundary C of $\alpha + \Pi$, for some α. Then, the number of zeros of f in $\alpha + \Pi$ is equal to the number of poles in $\alpha + \Pi$, being counted according to their multiplicity.*

Proof. Let $\{m_i\}$ be the order of the various zeros and $\{n_j\}$ be the orders of the various poles of f in $\alpha + \Pi$. Consider the elliptic function f'/f, which residue is zero by Theorem 5. On the other hand, by the argument principle we have

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}dz = \sum m_i - \sum n_j = 0.$$

■

It is convenient to say that z_1 is congruent to z_2, $z_1 \equiv z_2 \bmod(L)$, if $z_1 - z_2 \in L$. Then the function f takes the same values at congruent points, and may thus be regarded as a function on the congruence classes. If c is any constant and $f \in \mathcal{E}_L$, $f(z) - c$ has the same poles as $f(z)$. Therefore, all values are assumed equally many times. The number of incongruent roots of the equations $f(z) = c$ is called the *order* of the elliptic function, each root being counted according to its multiplicity.

Theorem 7. *Suppose that $f \in \mathcal{E}_L$ is not constant and has no poles on the boundary C of $\alpha + \Pi$, for some α. Let $a_1, ..., a_h$ be the zeros and $b_1, ..., b_h$ be the poles, each of them repeated according to its multiplicity, of an elliptic function $f \in \mathcal{E}_L$. Then*

$$a_1 + \cdots + a_h \equiv b_1 + \cdots + b_h \bmod(L).$$

Proof. Let α be such that the function $z\frac{f'(z)}{f(z)}$ is holomorphic and non-zero on $C = \partial(\alpha + \Pi)$. Consider the integral

$$\frac{1}{2\pi i}\int_C z\frac{f'(z)}{f(z)}dz = \sum_{i=1}^{h} a_i - \sum_{i=1}^{h} b_i,$$

since the argument principle and the residue theorem, call this sum Ω. Let c_1, c_2, c_3 and c_4 be the sides of C, under some changes of variable, we have

$$2\pi i\Omega = -\omega_2 \int_{c_1} \frac{f'(z)}{f(z)}dz - \omega_1 \int_{c_4} \frac{f'(z)}{f(z)}dz,$$

since f is periodic. Now, $\omega \in L$ implies $\log f(\alpha + \omega) = \log f(\alpha) + 2k\pi i$ for $k \in \mathbb{Z}$. Therefore

$$\begin{aligned} 2\pi i\Omega &= -\omega_2 \log f(z)|_{\alpha}^{\alpha+\omega_1} - \omega_1 \log f(z)|_{\alpha+\omega_2}^{\alpha} \\ &= 2\pi i(\omega_2 k + \omega_1 l) \text{ with } k, l \in \mathbb{Z}, \end{aligned}$$

thus $\Omega \in L$.

■

1.3 Non-constant elliptic and quasi-elliptic functions

We proceed now to construct non-constant elliptic functions. In seeking to do so, after the results of the preceeding section, there are two simplest types of elliptic functions; the *Weierstrassian elliptic functions* which have a double pole, with residue zero, in a period-parallelogram, and the *Jacobian elliptic functions* which have two simple poles, each of them being the negative of the other.

1.3.1 Weierstrass's $\wp$-function

Let (ω_1, ω_2) be a pair of reduced periods and $L = \{m\omega_1 + n\omega_2\}$ its period-lattice, let $L^* = L - \{0\}$. We define, for $z \in \mathbb{C}$,

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \tag{1.4}$$

this function is called the *Weierstrass $\wp$-function*. It is denoted $\wp(z; \omega_1, \omega_2)$, $\wp(z; L)$ or simply $\wp(z)$. Indeed, this is the partial fraction decomposition of the $\wp$-function, for more information on obtaining this, see the Appendix **??**. We shall prove that the series on (1.4) converges absolutely and uniformly on any compact subset of the complex plane, for this, we prove the next lemma.

Lemma. *The series $\sum_{\omega \in L^*} |\omega|^{-\rho}$ converges for $\rho > 2$.*

Proof. Let P_k be the set of periods lying in the sides of the parallelogram with corners in $\pm k\omega_1 \pm k\omega_2$, with $k \geq 1$, there are $8k$ such periods. Denote $T_k = \sum_{\omega \in P_k} |\omega|^{-\rho}$ the partial sums. The series $\sum_{\omega \in L^*} |\omega|^{-\rho}$ converges if and only if $\sum_{k=1}^{\infty} T_k$ does. Furthermore, there exists $a, b > 0$ for all $k \geq 1$ such that $ak < |\omega| < bk$ for all $\omega \in P_k$. Now, for all $w \in P_k$, $(ak)^\rho < |\omega|^\rho < (bk)^\rho$, then

$$\sum_{k=1}^{\infty} 8b^\rho k^{1-\rho} < \sum_{k=1}^{\infty} T_k < \sum_{k=1}^{\infty} 8a^\rho k^{1-\rho},$$

the series on the left side does not converge for $\rho \leq 2$, and note that for the series on the right side we have

$$8a^\rho \sum_{k=1}^{\infty} k^{1-\rho} < 8a^\rho \left(1 + \int_1^{\infty} \frac{1}{x^2} dx \right) = 16a^\rho,$$

for $\rho > 2$.

■

Theorem 8. *The sum*

$$\sum_{\omega \in L^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

converges absolutely and uniformly for z in any compact subset of $\mathbb{C} - L$.

Proof. We prove this theorem for every circle of finite radius discarding a sufficient number of terms. Given $R > 0$, let $|z| \leq R$ be the circle of radius R. In order to produce convergence we consider the periods such that $|\omega| > 2R$, then we have

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| = \left|\frac{\omega z(2 - z/\omega)}{\omega^4(z/\omega - 1)^2}\right| \leq \frac{10|z|}{|\omega|^3} \leq \frac{10R}{|\omega|^3}$$

since $|2 - z/\omega| \leq 2 + |-z/\omega| \leq 5/2$ and $|z/\omega - 1|^2 \geq 1/4$. The theorem follows after comparison of the series of the preceding lemma.

■

In order to prove some properties of the $\wp$-function and its derivatives we shall prove the next lemma.

Lemma. *The series*

$$\sum_{\omega \in L^*} |\omega - z|^{-\rho}$$

converges uniformly in every circle of finite radius for $\rho > 2$, if we discard a sufficient number of terms at the beginning.

Proof. Let $|z| \leq R$ and $|\omega| > 2R$, for $R > 0$, so that $|\omega| < 2(|\omega| - |z|) < 2|\omega - z|$, then

$$\frac{1}{|z-\omega|} \leq \frac{2}{|\omega|},$$

hence

$$\frac{1}{|z-\omega|^\rho} < \frac{2^\rho}{|\omega|^\rho} \text{ for } \rho > 0,$$

this proves the lemma, since the sum of the second part of inequality converges for $\rho > 2$.

■

Let $\mathcal{E}_L^+$ be the subfield of the *even elliptic functions* for a given lattice L, and let $\mathcal{E}_L^-$ be the subset of the *odd elliptic functions*.

Theorem 9. *For a given lattice L, the following properties hold*

(i) $\wp' \in \mathcal{E}_L^-$;

(ii) $\wp^{(n)} \in \mathcal{E}_L$ *for* $n \geq 2$, *where* $\wp^{(n)}$ *is the* n*-derivative;*

(iii) $\wp \in \mathcal{E}_L^+$.

Proof. By Theorem 8 and the uniform convergence theorem for holomorphic functions, $\wp$ is a meromorphic function with double poles at all $\omega \in L$. Also, Theorem 8 permits differentiation term by term, then

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3},$$

by the former lemma the series converges absolutely for $z \notin L$, and defines a meromorphic function with triple poles at all $\omega \in L$. Now, a rearrangement of the series of $\wp'(z+\omega)$ yields $\wp'(z+\omega) = \wp'(z)$, therefore $\wp'$ is an elliptic function. The same argument as above gives

$$\wp^{(n)}(z) = (-1)^n (n+1)! \sum_{\omega \in L} \frac{1}{(z-\omega)^{n+2}},$$

this proves (ii).

Note that $\wp(-z) = \frac{1}{z^2} + \sum_{\omega \in L^*} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right)$, and that $\{-\omega\} = \{\omega\}$, so that $\wp(-z) = \wp(z)$, differentiating we have $-\wp'(z) = \wp'(-z)$, thus $\wp$ is an even function and $\wp'$ is an odd function, then (i) holds.

Finally, integrating $\wp'(z+\omega) = \wp'(z)$ we obtain $\wp(z+\omega) = \wp(z) + c$. Setting $z = -\omega/2$, we get $\wp(\omega/2) = \wp(-\omega/2) + c$, since $\wp$ is even, it follows $c = 0$, then (iii) holds.

■

Inside a fundamental parallelogram Π, there is exactly one pole for $\wp$, which is one of the $\omega \in L$. By Theorem 7 there exists two zeros, say u and v, such that $u + v \equiv 0 \bmod(L)$. $\wp$ is an elliptic function of order two, that is, for $c \in \mathbb{C}$ there exists two points u and v in a fundamental parallelogram such that $\wp(u) = \wp(v) = c$, and since the poles of $\wp(z) - c$ coincide with those of $\wp(z)$, then $u + v \equiv 0 \bmod(L)$. If $u \equiv -u \bmod(L)$, then $u = v$, that is the points coincide. There are exactly four points in a fundamental parallelogram Π such that $u \equiv -u \bmod(L)$,

$$0, \ \frac{\omega_1}{2}, \ \frac{\omega_2}{2} \text{ and } \frac{\omega_1 + \omega_2}{2}.$$

The first of these points is the pole of $\wp$ in Π. Now let $\omega_3 = \omega_1 + \omega_2$. The elliptic function $\wp'$ is of order 3, by Theorem 9 $\wp'(-z) = -\wp'(z)$, moreover the periodicity of $\wp$ yields $\wp'(\omega_i/2) = \wp'(-\omega_i/2)$ for $i = 1, 2, 3$, then $\wp'(\omega_i/2) = -\wp'(\omega_i/2)$. Thus $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$ are the three zeros of $\wp'(z)$ in Π. Additionally, the values of $\wp$ at these points, call them

$$e_1 = \wp\left(\frac{\omega_1}{2}\right),\ e_2 = \wp\left(\frac{\omega_2}{2}\right) \text{ and } e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right),$$

are all of multiplicity 2 and distinct.

The field of elliptic functions

The Weierstrass function not only gives an example of an elliptic function but enable one to describe the structure of all elliptic functions. We first prove the next lemma which enable us to demonstrate the next important theorem.

Lemma. *The subfield $\mathcal{E}_L^+ \subset \mathcal{E}_L$ of even elliptic functions for a lattice L is generated by $\wp$, i.e., $\mathcal{E}_L^+ = \mathbb{C}(\wp)$.*

Proof. Let $f \in \mathcal{E}_L^+$. The idea of the proof is to build a function which has the same zeros and poles as $f(z)$ using only functions of the form $\wp(z) - u$ for $u \in \mathbb{C}$, recalling that for every u there exists two points in a fundamental parallelogram Π, counting multiplicity. Then the ratio of $f(z)$ to such constructed function must be constant.

We list the zeros and poles inside a fundamental parallelogram Π, ommiting 0 from our list, and counting only *half* of them since $\wp$ is of order 2. We describe the method of listing the poles; the method of listing the zeros is analogous, but first let's show some properties on the zeros and poles of an even elliptic function.

Suppose that $b \in \Pi - \{0\}$ is a pole of order m which is not a half of a lattice point. Let b^* be point inside Π such that $b + b^* \equiv 0 \bmod(L)$. If b is a pole of order m, because of the periodicity and the evenness of $f(z)$ we have $f(b^* - z) = f(b + z)$. Thus if $f(b + z) = b_m z^{-m} + \cdots$ then $f(b^* + z) = b_m(-z)^{-m} + \cdots$, then b^* is also a pole of order m.

Now suppose that $b \neq 0$ is a pole of f with $b \equiv -b \bmod(L)$. We have $f(b + z) = b_m z^{-m} + \cdots$ and $f(b + z) = f(-b + z) = f(b - z)$ because of the periodicity and the evenness of $f(z)$, then $f(b - z) = b_m(-z)^{-m} + \cdots$, that is the order m of the pole b must be even.

Now we list the zeros and poles of f. Let $\{b_j\}$ be a list of the poles of f in Π which are not half-lattice points, each taken as many times as the multiplicity of the pole there, but only one taken from each pair of symmetrical poles b, b^*; if one of the three nonzero half-lattice points in Π is a pole of f, include it in the list half as many times as its multiplicity. Let $\{a_i\}$ the list of nonzero zeros, counted in the same way as the poles.

Since $a_i \neq 0$ and $b_j \neq 0$ for all i, j, the values $\wp(a_i)$ and $\wp(b_j)$ are finite, and it makes sense to define the elliptic function

$$g(z) = \frac{\Pi_i(\wp(z) - \wp(a_i))}{\Pi_j(\wp(z) - \wp(b_j))},$$

where the nonzero zeros of g come from the zeros of $\wp(z) - \wp(a_i)$ and the nonzero poles of g come from the zeros of $\wp(z) - \wp(b_j)$, since $\wp$ has order 2, then it has one double zero $u \in \Pi$ such that $u \equiv -u \bmod(L)$ or two symmetric points u and v in Π such that $u + v \equiv 0 \bmod(L)$. Then g and f have the same nonzero zeros and poles in Π, with the possible exception of the point 0. Theorem 6 tell us that when we know that two elliptic functions have the same order of zero or pole everywhere but possibly at one point in $\Pi + \alpha$, then that one point is carried along automatically, this implies that g has the same zeros and poles as f, from wich it follow that $f(z) = cg(z)$ for some constant c and $g \in \mathbb{C}(\wp)$.

■

Theorem 10. *Let f and $\wp \in \mathcal{E}_L$. Then there exist rational functions R and T such that*

$$f = R(\wp) + T(\wp)\wp',$$

that is $\mathcal{E}_L = \mathbb{C}(\wp, \wp')$ the field of elliptic functions for a lattice L equals the rational functions field generated by $\wp$ and $\wp'$.

Proof. Let $f \in \mathcal{E}_L$, then we can write f as follows

$$f(z) = \underbrace{\frac{f(z) + f(-z)}{2}}_{\in \mathcal{E}_L^+} + \underbrace{\frac{f(-z) - f(z)}{2\wp'(z)}}_{\in \mathcal{E}_L^+} \wp'(z),$$

the Theorem follows from the former Lemma.

■

A certain differential equation

The Theorem 10 has many implications, one of the most important is that the Weierstrass function satisfies certain differential equation, we explain this result below. Later we give another independent derivation of the differential equation for $\wp$.

Since $\wp'(z)^2$ is an even elliptic function, it can be expressed as a rational function of $\wp(z)$, furthermore it can be expressed as a polynomial of $\wp(z)$ since its poles lie at the nodes of the period lattice. The zeros of $\wp'(z)$ turn out to be double zeros of $\wp'(z)^2$. Hence we have

$$\wp'(z)^2 = c(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3),$$

where c is some constant. In order to find this constant let's compare the coefficients of the leading term on each side of the equation; the leading term on the left side is $(-2z^{-3})^2 = 4z^{-6}$, while on the right it is $c(z^{-2})^3 = cz^{-6}$, we conclude that $c = 4$. That is, $\wp(z)$ satisfies the differential equation

$$\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3). \tag{1.5}$$

Notice that the cubic polynomial on the right side has distinct roots. Suppose, for example, $e_1 = e_2$, then the function $\wp(z) - e_1$ has zeros of multiplicity 2 at the points $\omega_1/2$ and $\omega_2/2$, then there are inside Π at least 4 zeros of this function, which is impossible.

Example 3. The even function $\wp''(z)$ which has a pole of order 4 at the nodes of L can be expressed as $f(\wp(z))$, where $f(x)$ is a second degree polynomial. We exhibit this polynomial using the technique explained below. ★

So as to give another independent derivation of the differential equation for $\wp(z)$, we seek find a cubic polynomial

$$f(x) = ax^3 + bx^2 + cx + d,$$

such that the Laurent expansion of the elliptic function $f(\wp(z))$ agrees with the Laurent expansion of $\wp'(z)^2$ through the negative powers of z. Then by Theorem 4, the function $\wp'(z)^2 - f(\wp(z))$ would be constant, and we can

choose d in such a way that this constant is zero. Since $\wp(z)$ is an even function, its Laurent expansion at $z = 0$ is given by

$$\wp(z) = \frac{1}{z^2} + b_1 z^2 + b_2 z^4 + \cdots + b_n z^{2n} + \cdots ; \tag{1.6}$$

by Theorem 8 if $|\omega| > 2R \geq |z|$ we can expand each term of the series as follows

$$\left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\} = \frac{2}{\omega^3} z + \frac{3}{\omega^4} z^2 + \frac{4}{\omega^5} z^3 + \frac{5}{\omega^6} z^4 + \cdots ;$$

hence we have

$$b_1 = 3G_4,\ b_2 = 5G_6,\ b_n = (2n+1)G_{2n+2},$$

where for $k \geq 2$ we denote

$$G_{2k} = G_{2k}(L) = \sum_{\omega \in L^*} \frac{1}{\omega^{2k}}, \tag{1.7}$$

each of this series is called the *holomorphic Eisenstein series* G_{2k} of weight $2k$, we will go deeper on this later; and so (1.6) turns in

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \cdots + (2n+1)G_{2n+2} z^{2n} + \cdots , \tag{1.8}$$

and computing we have

$$\wp(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + (9G_4^2 + 14G_8) z^4 + (30G_4 G_6 + 18G_{10}) z^6 + \cdots \tag{1.9}$$

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + (27G_4^2 + 21G_8) z^2 + (90G_4 G_6 + 27G_{10}) z^4 + \cdots \tag{1.10}$$

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + 72G_{10} z^7 + 110G_{12} z^9 + \cdots ; \tag{1.11}$$

$$\wp'(z)^2 = \frac{4}{z^6} - 24G_4 \frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8) z^2 + \cdots . \tag{1.12}$$

Now, for find the coefficients a, b, c, d of a cubic $f(x) = ax^3 + bx^2 + cx + d$ such that

$$\wp'(z)^2 = a\wp(z)^3 + b\wp(z)^2 + c\wp(z) + d,$$

we multiply equation (1.10) by a, and comparing the principal parts of $\wp'(z)^2$ and $a\wp(z)^3$ we have that $a = 4$, that is

$$\wp'(z)^2 - 4\wp(z)^3 = -(24G_4 + 4(9G_4))\frac{1}{z^2} - (80G_6 + 4(15G_6)) + h(z),$$

where $h(z)$ is holomorphic and vanishes at $z = 0$. The preceding function does not have any pole of order 4, then $b = 0$. If we multiply the equation (1.8) by c and compare the principal part of $c\wp$ with the principal part of the previous function, we have that $c = -60G_4$, that is

$$\wp'(z)^2 - 4\wp(z)^3 - 60G_4\wp(z) = -(80G_6 + 4(15G_6)) + h_1(z),$$

where $h_1(z)$ is holomorphic and vanishes at $z = 0$. Finally, $d = -140G_6$. It is traditional to denote

$$g_2 = 60G_4 \text{ and } g_3 = 140G_6. \tag{1.13}$$

We have thereby derived a second form for (1.5):

$$\wp'(z)^2 = f(\wp(z)) \text{ where } f(x) = 4x^3 - g_2x - g_3 \in \mathbb{C}[x]. \tag{1.14}$$

Example 4. From Example 3 the even function $\wp''(z)$ can be expressed as $f(\wp(z))$, where $f(x)$ is a quadratic polynomial. Now differentiating (1.14) we have

$$\wp''(z) = 6\wp(z)^2 - \frac{g_2}{2},$$

then

$$\wp''(z) - 6\wp(z)^2 + \frac{g_2}{2} = (-54G_4^2 + 126G_8)z^4 + (-180G_4G_6 + 396G_{10})z^6 + \cdots; \tag{1.15}$$

by Theorem 4 this equation is identically zero for every z, thus $G_8 = \frac{3}{7}G_4^2$. ★

The former example exhibits relations among the Eisenstein series, actually developing the laurent expansion on each side of the equation $\wp''(z) = 6\wp(z)^2 - \frac{g_2}{2}$ we have

$$\frac{6}{z^4} + \sum_{n=1}^{\infty}(2n+1)(2n)(2n-1)G_{2n+2}z^{2n-2} = \frac{6}{z^4}\left(1 + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n+2}\right)^2 - \frac{g^2}{2}.$$

By comparing the coefficients of z^{2n-2} on each side of the equation, for $n \geq 3$, we obtain

$$(2n+1)(2n)(2n-1)G_{2n+2} = 6\left(2(2n+1)G_{2n+2} + \sum_{k=1}^{n-2}(2(n-k)-1)(2k+1)G_{2(n-k)}G_{2k+2}\right),$$

that is

$$G_{2n+2} = \frac{6}{2(2n+3)(2n+1)(n-2)}\sum_{k=1}^{n-2}(2(n-k)-1)(2k+1)G_{2(n-k)}G_{2k+2}.$$

This is a very remarkable fact that shows how Eisenstein series are related to each other, actually, $G_{2k} \in \mathbb{Q}[G_4, G_6]$, that is they are rational polynomials depending on G_4 and G_6.

Example 5. Let $L = \mathbb{Z}[i]$ be the lattice of Gaussian integers and consider the Einsenstein series $G_6(L)$ and $G_4(L)$, if we choose any pair of reduced periods then $\tau = i$, that is $\omega_2 = i\omega_1$, substituting in $G_6(L)$ we have

$$G_6(L) = \sum_{m,n\in\mathbb{Z}} \frac{1}{(m+ni)^6\omega_1^6},$$

note that $(m+ni)^6 + (-n+mi)^6 = 0$, thus $G_6(L) = 0$. While

$$(m+in)^4 = (n-im)^4 = (-m-in)^4 = (-n+im)^4,$$

that is

$$G_4(L) = \sum_{\omega\in L^*}\frac{1}{\omega^4} = 4\sum_{\substack{m\geq 0\\ n>0}}\frac{1}{(m+in)^4\omega_1^4},$$

which is a non-zero number.

★

Example 6. Now let L be the lattice of the Eisenstein integers, let $\xi = e^{2\pi i/3}$ and consider the Einsenstein series $G_6(L)$ and $G_4(L)$, if we choose any pair of reduced periods then $\tau = \xi$, that is $\omega_2 = \xi\omega_1$, substituting in

$G_4(L)$ we have

$$\begin{aligned} G_4(L) &= \sum_{m,n\in\mathbb{Z}} \frac{1}{(m+n\xi)^4\omega_1^4} \\ &= \sum_{\substack{m\geq 0\\ n>0}} \left\{ \frac{1}{(m+\xi n)^4\omega_1^4} + \frac{1}{(\xi(m+\xi n))^4\omega_1^4} + \frac{1}{(\xi^2(m+\xi n))^4\omega_1^4} \right\} \\ &= \sum_{\substack{m\geq 0\\ n>0}} \frac{1+\xi+\xi^2}{(m+\xi n)^4\omega_1^4} \\ &= 0. \end{aligned}$$

Similarly, for $G_6(L)$ we have

$$\begin{aligned} G_6(L) &= \sum_{\substack{m\geq 0\\ n>0}} \left\{ \frac{1}{(m+\xi n)^6\omega_1^6} + \frac{1}{(\xi(m+\xi n))^6\omega_1^6} + \frac{1}{(\xi^2(m+\xi n))^6\omega_1^6} \right\} \\ &= \sum_{\substack{m\geq 0\\ n>0}} \frac{3}{(m+\xi n)^6\omega_1^6}. \end{aligned}$$

Thus for the lattice L of the Einsenstein integers we have $G_4(L) = 0$ and $G_6(L) \neq 0$.

★

1.3.2 Weierstrass's ζ-function and σ-function

We have looked at the derivatives of the Weiestrass $\wp-$function so far, a similar process can be carried out integrating. The Weierstrass zeta function $\zeta(z)$ is the function defined by

$$\frac{d\zeta(z)}{dz} = -\wp(z) \text{ and } \lim_{z\to 0} \zeta(z) - z^{-1} = 0. \tag{1.16}$$

Then using the definition

$$\begin{aligned} \zeta(z) - z^{-1} &= -\int_0^z \wp(z) - z^{-2} dz \\ &= -\sum_{\omega\in L^*} \int_0^z (z-\omega)^{-2} - \omega^{-2} dz, \end{aligned}$$

that is

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \in L^*} \frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}. \tag{1.17}$$

The ζ-function is then a single-valued odd function which converges absolutely and uniformly in every compact subset of $\mathbb{C} - L$ and it has simple poles at the nodes of the lattice L. Now integrating the next equality $\wp(z + w_i) = \wp(z)$ for $i = 1, 2$, we have that ζ satisfies the relation

$$\zeta(z + w_i) = \zeta(z) + \eta_i, \tag{1.18}$$

with $\eta_i \neq 0$ since ζ is not elliptic. We can find the value of the η_i substituting $z = -\omega_i/2$ in (1.18) and using the fact that ζ is an odd function. We have

$$\eta_1 = 2\zeta\left(\frac{\omega_1}{2}\right) \text{ and } \eta_2 = 2\zeta\left(\frac{\omega_2}{2}\right). \tag{1.19}$$

Now we prove a theorem that relates the periods ω_1 and ω_2 with the the constants η_1 and η_2 known as the *Legendre's relation*.

Theorem 11. *Let $\wp(z; \omega_1, \omega_2)$ be the Weierstrass elliptic function for the periods ω_1 and ω_2 then*

$$\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i.$$

Proof. From one hand we have

$$\frac{1}{2\pi i}\int_{\partial(\Pi+\alpha)} \zeta(z)dz = 1,$$

with $\alpha \neq 0$, since ζ has a simple pole with residue 1. Now, in the other hand, if we choose $\alpha = -\frac{\omega_1+\omega_2}{2}$ (see Figure 1.7) we have

$$\frac{1}{2\pi i}\int_{\partial(\Pi+\alpha)} \zeta(z)dz = \frac{1}{2\pi i}\int_{c_1+c_2+c_3+c_4} \zeta(z)dz$$

where the c_i are the sides of the parallelogram. Then

$$\begin{aligned}
\int_{c_1} \zeta(z)dz &= -\int_{c_3} \zeta(z-\omega_2)dz \\
&= -\int_{c_3} \zeta(z)dz + \int_{c_3} \eta_2 dz \\
&= -\int_{c_3} \zeta(z)dz + \eta_2 z\Big|_{\frac{\omega_1+\omega_2}{2}}^{\frac{\omega_2-\omega_1}{2}} \\
&= -\int_{c_3} \zeta(z)dz - \eta_2\omega_1
\end{aligned}$$

thus

$$\int_{c_1} \zeta(z)dz + \int_{c_3} \zeta(z)dz = -\eta_2\omega_1.$$

Similarly we have

$$\begin{aligned}
\int_{c_2} \zeta(z)dz &= -\int_{c_4} \zeta(z+\omega_1)dz \\
&= -\int_{c_4} \zeta(z)dz - \int_{c_4} \eta_1 dz \\
&= -\int_{c_4} \zeta(z)dz - \eta_1 z\Big|_{\frac{\omega_2-\omega_1}{2}}^{\frac{-\omega_2-\omega_1}{2}} \\
&= -\int_{c_4} \zeta(z)dz + \eta_1\omega_2
\end{aligned}$$

thus

$$\int_{c_2} \zeta(z)dz + \int_{c_4} \zeta(z)dz = \eta_1\omega_2.$$

Therefore,

$$2\pi i = \eta_1\omega_2 - \eta_2\omega_1.$$

■

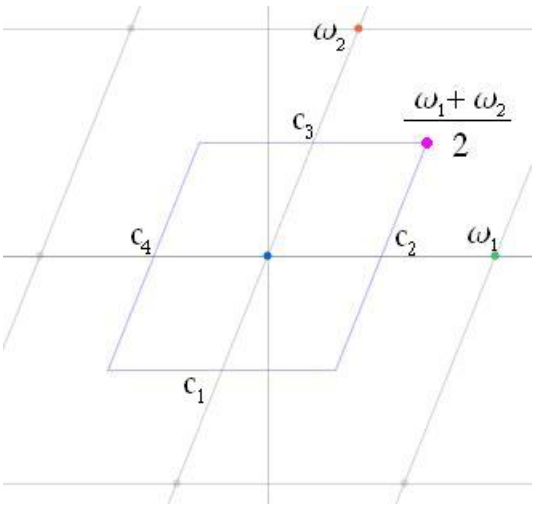

Figure 1.7: The fundamental parallelogram centered at 0.

The integration can be carried one step further. The Weierstrass sigma function $\sigma(z)$ is the function defined by

$$\frac{d}{dz}\log(\sigma(z)) = \frac{\sigma'(z)}{\sigma(z)} = \zeta(z) \text{ and } \lim_{z\to 0}\frac{\sigma(z)}{z} = 1. \tag{1.20}$$

Then using the definition

$$\begin{aligned}\zeta(z) - \frac{1}{z} &= \log'(\sigma(z)) - \frac{1}{z} \\ &= \log'(\sigma(z)) - \log'(z),\end{aligned}$$

integrating we have

$$\begin{aligned}\int_0^z \zeta(z) - \frac{1}{z}dz &= \int_0^z \log'(\sigma(z)) - \log'(z)dz \\ \int_0^z \sum_{\omega\in L^*} \frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}dz &= \log\left(\frac{\sigma(z)}{z}\right)\Bigg|_0^z \\ \sum_{\omega\in L^*} \log\left(1-\frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{z^2}{2\omega^2} &= \log\left(\frac{\sigma(z)}{z}\right),\end{aligned}$$

finally we use the exponential to eliminate the multiple-valuedness, and we have

$$\sigma(z) = z\prod_{\omega\in L^*}\left(1-\frac{z}{\omega}\right)e^{z/\omega+z^2/2\omega^2}. \tag{1.21}$$

The infinite product on the left side of (1.21) converges absolutely and uniformly in a suitable circle. Thus the Weierstrass's σ-function is an entire odd function with simple zeros at the lattice points. For a fixed lattice and any non-zero complex number λ we have

$$\sigma(\lambda z; \lambda\omega_1, \lambda\omega_2) = \lambda\sigma(z; \omega_1, \omega_2)$$

It is clear that the σ function is not elliptic, we are about to know its behaviour in values which differ by a period. By integrating the relations $\zeta(z+\omega_i) = \zeta(z) + 2\eta_i$ for $i = 1, 2$, where the η_i come from (1.19), we have

$$\log(\sigma(z+\omega_i)) - \log(\sigma(\omega_i)) = \log(\sigma(z)) - \log(\sigma(0)) + 2\eta_i z,$$

exponentiating we have

$$\sigma(z+\omega_i) = C_i\sigma(z)e^{2\eta_i z},$$

where $C_i = \frac{\sigma(\omega_i)}{\sigma(0)}$ is a constant. Now, setting $z = -\frac{\omega_i}{2}$ we have

$$\sigma\left(\frac{\omega_i}{2}\right) = -C_i\sigma\left(\frac{\omega_i}{2}\right)e^{-\eta_i\omega_i},$$

since $\sigma(z)$ is an odd function. It results that

$$C_i = -e^{\eta_i\omega_i}.$$

Then we have proved that

$$\begin{aligned}\sigma(z+\omega_1) &= -e^{\eta_1(\omega_1+2z)}\sigma(z),\\ \sigma(z+\omega_2) &= -e^{\eta_2(\omega_2+2z)}\sigma(z).\end{aligned} \tag{1.22}$$

Example 7. Let f be a non-constant elliptic function with reduced periods ω_1 and ω_2. Let $\{a_i\}$ and $\{b_i\}$ the list of its zeros and poles, repetitions allowed according to their multiplicity. By Theorem 6, f has as many zeros as poles, say n. Let $\Omega = \sum_{i=1}^{n} b_i - a_i$. Theorem 7 implies $\Omega \in L$, then consider the ratio of sigma functions

$$g(z) = \frac{\prod_{i=1}^{n}\sigma(z-a_i)}{\sigma(z-b_n+\Omega)\prod_{i=1}^{n-1}\sigma(z-b_i)},$$

note that g is a meromorphic function with zeros at the a_i's and poles at the b_i's. Moreover, equations (1.22) show that g is doubly-periodic since

$$\begin{aligned} g(z+w_i) &= \frac{(-1)^n e^{2\eta_i(nz+n\frac{\omega_i}{2}-\sum_{i=1}^{n}a_k)}\prod_{i=1}^{n}\sigma(z-a_i)}{(-1)^n e^{2\eta_i(nz+n\frac{\omega_i}{2}-\sum_{i=1}^{n}b_k)+\Omega}\sigma(z-b_n+\Omega)\prod_{i=1}^{n-1}\sigma(z-b_i)} \qquad (1.23)\\ &= g(z), \qquad (1.24)\end{aligned}$$

for $i = 1, 2$. Then f/g is an elliptic function without poles, then it must be constant, that is $f(z) = cg(z)$ for some $c \in \mathbb{C}$. Therefore, we can express any non-constant elliptic function f as a ratio of sigma functions.

★

Example 8. Consider the function $g(z) = \wp(z) - \wp(u)$ for $u \in \mathbb{C} - L$. g is an elliptic function with zeros at $z = \{u, -u\}$ and a double pole at $z = 0$, then by the Example 7, we have that

$$\frac{\sigma(z-u)\sigma(z+u)}{\sigma^2(z)}$$

is an elliptic function with the same zeros and poles as $g(z)$, then they are equal up to multiplication by a constant c which not depends on z. If we compare the principal parts of the functions, we have that $c = -\frac{1}{\sigma^2(u)}$, that is

$$\wp(z) - \wp(u) = -\frac{\sigma(z-u)\sigma(z+u)}{\sigma^2(z)\sigma^2(u)}.$$

★

In the last examples we have seen how useful can be the sigma and the zeta functions in order to build elliptic functions. Next, we study other function which enable us to build elliptic functions too.

1.3.3 The theta-functions

In 1.3.1 we studied a method to construct elliptic functions, now we give a somewhat different method to do so with the help of *theta-functions*. Let (ω_1, ω_2) be a pair of reduced periods and $\tau = \omega_2/\omega_1$, we define

$$\theta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i[n^2\tau + 2nz]}.$$

This series converges absolutely and uniformly on compact subsets of $\mathbb{C}$, namely, let c be a real positive constant and let $|z| < c$, the map $e^{i\pi\tau}$ maps $\tau \in \mathbb{H}$ into the unit disk. Let $q = e^{i\pi\tau}$ then $|q| < 1$, the absolute value of the ratio of the consecutive terms of the series is equal to

$$|q^{2n+1}e^{2\pi iz}| \leq |q|^{2n+1}e^{2\pi|z|}.$$

Since $\lim_{n\to\infty} |q|^{2n+1} = 0$, thus the series of entire functions converge uniformly in the domain $|z| < c$. Hence the theta function is analytic on all of $\mathbb{C}$.

Note that

$$\theta(z+1) = \theta(z), \tag{1.25}$$

for every $z \in \mathbb{C}$, that is θ is periodic and we expect it to be well behaved respecting to τ, actually we have the next relation

$$\begin{aligned}\theta(z+\tau) &= \sum_{n-1=-\infty}^{\infty} e^{\pi i[(n-1)^2\tau+2(n-1)(z+\tau)]} \\ &= e^{-\pi i[2z+\tau]}\theta(z), \end{aligned} \tag{1.26}$$

for all $z \in \mathbb{C}$. Then we have

$$\theta(z-\tau) = e^{\pi i[2z-\tau]}\theta(z), \tag{1.27}$$

for all $z \in \mathbb{C}$.

Then theta functions are entire functions with one genuine period and one quasiperiod.

After equations (1.25) and (1.26) it follows that z_0 is a zero of θ if and only if $z_0 + L_\tau$ are zeros, where $L_\tau = \{m + n\tau | m, n \in \mathbb{Z}\}$.

Further consequences of (1.25), (1.26) and (1.27) are that

$$\frac{\theta'(z \pm \tau)}{\theta(z \pm \tau)} = \frac{\theta'(z)}{\theta(z)} \mp 2\pi i, \text{ and } \frac{\theta'(z+m)}{\theta(z+m)} = \frac{\theta'(z)}{\theta(z)} \text{ for every } m \in \mathbb{Z}.$$

Lemma. *The θ-function has a unique simple zero $z_0 = 1/2 + \tau/2$ in the fundamental parallelogram Π for the lattice L_τ.*

Proof. Consider the integral

$$\frac{1}{2\pi i}\int_{\partial\Pi} \frac{\theta'(z)}{\theta(z)} dz,$$

which counts the number of zeros inside the fundamental parallelogram of the entire functions. We have

$$\int_{\partial\Pi} \frac{\theta'(z)}{\theta(z)} dz = \int_0^1 \frac{\theta'(z)}{\theta(z)} dz + \int_1^{\tau+1} \frac{\theta'(z)}{\theta(z)} dz + \int_{\tau+1}^{\tau} \frac{\theta'(z)}{\theta(z)} dz + \int_\tau^0 \frac{\theta'(z)}{\theta(z)} dz,$$

now, making some substitutions we have

$$\begin{aligned}\int_1^{\tau+1} \frac{\theta'(z)}{\theta(z)} dz &= \int_0^\tau \frac{\theta'(z+1)}{\theta(z+1)} dz \\ &= -\int_\tau^0 \frac{\theta'(z)}{\theta(z)} dz, \end{aligned}$$

that is

$$\int_1^{\tau+1} \frac{\theta'(z)}{\theta(z)}dz + \int_\tau^0 \frac{\theta'(z)}{\theta(z)}dz = 0,$$

and

$$\begin{aligned}\int_{\tau+1}^{\tau} \frac{\theta'(z)}{\theta(z)}dz &= \int_1^0 \frac{\theta'(z+\tau)}{\theta(z+\tau)}dz,\\ &= -\int_0^1 \left(\frac{\theta'(z)}{\theta(z)} - 2\pi i\right)dz,\end{aligned}$$

that is

$$\int_0^1 \frac{\theta'(z)}{\theta(z)}dz + \int_{\tau+1}^{\tau} \frac{\theta'(z)}{\theta(z)}dz = 2\pi i,$$

therefore there is a unique simple zero inside the fundamental parallelogram.

Now, to know where is the zero located, we consider the integral

$$\frac{1}{2\pi i}\int_{\partial\Pi} z\frac{\theta'(z)}{\theta(z)}dz,$$

and we apply a similar reasoning. We have

$$\begin{aligned}\int_{\tau+1}^{\tau} z\frac{\theta'(z)}{\theta(z)} &= \int_1^0 (z+\tau)\frac{\theta'(z+\tau)}{\theta(z+\tau)},\\ &= -\int_0^1 z\frac{\theta'(z)}{\theta(z)}dz - \int_0^1 \tau\frac{\theta'(z)}{\theta(z)}dz + \int_0^1 (2\pi iz + 2\pi i\tau)dz,\\ &= \pi i + 2\pi i\tau - \int_0^1 z\frac{\theta'(z)}{\theta(z)}dz,\end{aligned}$$

similarly

$$\begin{aligned}\int_1^{\tau+1} z\frac{\theta'(z)}{\theta(z)}dz &= \int_0^{\tau} (z+1)\frac{\theta'(z+1)}{\theta(z+1)}dz,\\ &= -\int_\tau^0 z\frac{\theta'(z)}{\theta(z)}dz - \int_\tau^0 \frac{\theta'(z)}{\theta(z)}dz,\\ &= -\int_\tau^0 z\frac{\theta'(z)}{\theta(z)}dz + \log\left[e^{-\pi i\tau}\theta(0)\right] - \log[\theta(0)],\\ &= -\int_\tau^0 z\frac{\theta'(z)}{\theta(z)}dz - \pi i\tau,\end{aligned}$$

since $\theta(\tau) = e^{-\pi i \tau}\theta(0)$.
Therefore

$$\frac{1}{2\pi i}\int_{\partial\Pi} z\frac{\theta'(z)}{\theta(z)}dz = 1/2 + \tau/2,$$

this proves our lemma.

■

Consider the translation

$$\theta^{(x)}(z) = \theta(z - (1/2) - (\tau/2) - x), \tag{1.28}$$

which has simple zeros at the points $x + L_\tau$. The next relations are direct consequences of (1.25), (1.26) and (1.28). It is obvious that

$$\theta^{(x)}(z+1) = \theta^{(x)}(z), \tag{1.29}$$

now we find out how translates are behaved under the addition of τ,

$$\begin{aligned}
\theta^{(x)}(z+\tau) &= \theta(z+\tau-(1/2)-(\tau/2)-x), \\
&= \sum_{n-1=\infty}^{\infty} e^{\pi i[(n-1)^2\tau + 2(n-1)(z+\tau-(1/2)-(\tau/2)-x)]}, \\
&= \sum_{n-1=\infty}^{\infty} e^{\pi i[n^2\tau + 2n(z-(1/2)-(\tau/2)-x)-2z+2x+1]}, \\
&= -e^{-2\pi i[z-x]}\theta^{(x)}(z).
\end{aligned} \tag{1.30}$$

The next theorem is an important result which relates every elliptic function with theta functions, it can be seen as equivalent to Theorem 10, which relates $\wp$-function and its derivative with every elliptic function.

Theorem 12. *Let $N \in \mathbb{N}$ fixed, choose two disjoint multisets of N complex numbers $\{a_i\}$ and $\{b_j\}$ such that $\sum_{i=1}^{N} a_i - \sum_{j=1}^{N} b_j \in \mathbb{Z}$. Then the ratio of the translated theta functions*

$$R(z) = \frac{\prod_{i=1}^{N} \theta^{(a_i)}(z)}{\prod_{j=1}^{N} \theta^{(b_j)}(z)}$$

is an elliptic function. Furthermore, every elliptic function can be written in this way.

Proof. Let $N \in \mathbb{N}$ fixed, let $\{a_i\}$ and $\{b_j\}$ be two disjoint multisets of N complex numbers such that $\sum_{i=1}^{N} a_i - \sum_{j=1}^{N} b_j \in \mathbb{Z}$ and consider the function

$$R(z) = \frac{\prod_{i=1}^{N} \theta^{(a_i)}(z)}{\prod_{j=1}^{N} \theta^{(b_j)}(z)},$$

then R is a meromorphic function on $\mathbb{C}$ and $R(z+1) = R(z)$, thus it is periodic. Now, we want to show that R is L_τ-periodic, observe that

$$\begin{aligned}
R(z+\tau) &= \frac{\prod_{i=1}^{N} \theta^{(a_i)}(z+\tau)}{\prod_{j=1}^{N} \theta^{(b_j)}(z+\tau)}, \\
&= \frac{\prod_{i=1}^{N} -e^{-2\pi i[z-a_i]}\theta^{(a_i)}(z)}{\prod_{j=1}^{N} -e^{-2\pi i[z-b_j]}\theta^{(b_j)}(z)}, \\
&= \frac{(-1)^N e^{-2\pi i \sum_{i=1}^{N}[z-a_i]} \prod_{i=1}^{N} \theta^{(a_i)}(z)}{(-1)^N e^{-2\pi i \sum_{j=1}^{N}[z-b_j]} \prod_{j=1}^{N} \theta^{(b_j)}(z)}, \\
&= e^{2\pi i\left[\sum_{j=1}^{N}[z-b_j]-\sum_{i=1}^{N}[z-a_i]\right]} \frac{\prod_{i=1}^{N} \theta^{(a_i)}(z)}{\prod_{j=1}^{N} \theta^{(b_j)}(z)}, \\
&= e^{2\pi i\left[\sum_{i=1}^{N} a_i-\sum_{j=1}^{N} b_j\right]} \frac{\prod_{i=1}^{N} \theta^{(a_i)}(z)}{\prod_{j=1}^{N} \theta^{(b_j)}(z)}, \\
&= R(z),
\end{aligned}$$

since $\sum_{i=1}^{N} a_i - \sum_{j=1}^{N} b_j \in \mathbb{Z}$. Then the function R has zeros at the points $x_i + L_\tau$, poles at the points $y_i + L_\tau$ and it is L_τ-periodic, therefore R is an elliptic

function.

To prove the second part of the Theorem, let $f \in \mathcal{E}_{L_\tau}$. By Theorem 6, f has as many zeros as poles; let $\{a_i\}$ and $\{b_i\}$ with $i = 1, ..., n$ be the sets of the zeros and poles respectively, with repetitions allowed. And by Theorem 7 we have $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \bmod(L_\tau)$, then form the ratio of translated theta functions

$$R(z) = \frac{\prod_{i=1}^{n} \theta^{(a_i)}(z)}{\prod_{j=1}^{n} \theta^{(b_j)}(z)},$$

and consideer the elliptic function $g = R/f$, since R and f have the same zeros and poles g must be a nonzero constant. Then f can be written as a ratio of theta functions multiplied by a constant.

■

1.3.4 Remarks

Trough all this section, we have discussed some non trivial examples of elliptic and quasi-elliptic functions, namely the Weierstrass $\wp$-function, its derivative $\wp'$, its integral function ζ and its exponential double integral σ, all of them clearly related to the $\wp$ function; and the θ functions. We devote the last part of this section to explain which are the relations between theta functions and Weierstrass functions.

Given an elliptic function $f \in \mathcal{E}_L$, we can express it in terms of rational functions of $\wp$ and its derivative just making inspection over the zeros and poles of the two auxiliary even elliptic functions seen in Theorem 10. In a similar way, knowing the zeros and poles of f we can reconstruct it as a quotient of σ functions, see Example 7. The latter process can be applied in a similar fashion for translated θ functions as shown in Teorem 12.

Thus, both the quotient of σ and translated θ functions are similar, however notice that the σ function is defined as a product of functions and the θ function as a function series.

Let L be a lattice generated by a pair of reduced periods (ω_1, ω_2). Set

$q = e^{\pi i \tau}$ with $\tau = \omega_2/\omega_1$ and consider the function

$$\vartheta(z) = \frac{1}{i} \sum_{n=-\infty}^{\infty} (-1)^n q^{(n+\frac{1}{2})^2} e^{(2n+1)\pi i z}, \tag{1.31}$$

one can prove that

$$\begin{aligned} \vartheta(z) &= \theta(z + \frac{1}{2} + \frac{\tau}{2}) \left(q^{1/4} e^{\pi i z} \frac{1}{i} \right), \\ &= \theta^{(-1-\tau)}(z) \left(q^{1/4} e^{\pi i z} \frac{1}{i} \right); \end{aligned}$$

thus ϑ is the product of a translated theta function by a periodic function. Therefore it converges absolutely and it is an entire function with simple zeros at $L_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$. Moreover ϑ satisfies the relations

$$\vartheta(z+1) = -\vartheta(z), \quad \vartheta(z+\tau) = -\frac{1}{q} e^{2\pi i z} \theta(z) \quad \text{and} \quad \vartheta(z) = -\vartheta(-z). \tag{1.32}$$

These considerations allow us to state in a simple way the desired relation in the next theorem.

Theorem 13. *Let (ω_1, ω_2) be a pair of reduced periods, $\tau = \omega_2/\omega_1$, with $Im(\tau) > 0$, $\eta_1 = \zeta(\omega_1/2)$ and $\vartheta'(0)$ the derivative of ϑ with respect to z at $z = 0$. Then*

$$\sigma(z) = \vartheta\left(\frac{z}{\omega_1}\right) \frac{\omega_1}{\vartheta'(0)} e^{\eta_1 z^2/\omega_1}.$$

Finally, in Chapter 2, we will see applications of both kind of elliptic and quasi-elliptic functions. First, the study of the Weierstrass $\wp$ function will provide us a functional and deep isomorphism between elliptic curves and complex tori. Secondly, theta-like functions are of especial interest when computing the Hasse-Weil L function of an elliptic curve, since for an especial theta function, the Mellin transform of such theta function turns out to be the Riemann zeta-function.

Chapter 2

Arithmetic Theory of Elliptic Curves

The Weierstrass elliptic function is very special in its own right. The $\wp$-function gives an isomorphism between two mathematical objects: the Complex Elliptic Curves and the Complex Tori. This means, we can take profit from the geometrical structure of the complex torus, just as we defined in Chapter 1 and take this properties to the algebraic language.

In this chapter, we define what an elliptic curve is and we give the analytical isomorphism connecting them with the complex tori.

Complex tori are abelian groups with the addition of points modulo a lattice L, it turns out that complex elliptic curves are abelian groups as well, so given a pair of points in the elliptic curve the addition is well defined.

These results are generalized algebraically for every elliptic curve defined over a field K. Further we make some investigation in the torsion group of an elliptic curve, consisting in the points of finite order. We show that any elliptic curve has at most N^2 points of order N.

We shall make an inspection in the field extensions of the field K over which an elliptic curve is defined, looking for extra points, some of them being probably of finite order. So naturally, we study a couple of examples involving the Galois group of a field extension K' and its relation with the points on an elliptic curve defined over K.

Through all this chapter we discuss and show some examples concerning a special elliptic curve, which is a substantial part of the approach to the

problem exposed in Chapter 5.

2.1 Elliptic curves

Definition. An *elliptic curve* E is a smooth projective curve over a field K of genus 1 together with a point $O \in E$.

An elliptic curve E over a field K can be given by the projective completition of an equation of the form

$$E : y^2 = ax^3 + bx^2 + cx + d, \text{ with } a, b, c, d \in K; \tag{2.1}$$

from now on, we will use indistinctly both notations.

The smoothness assumption is equivalent to ask that the cubic polynomial in the right of (2.1)

$$f(x) = ax^3 + bx^2 + cx + d, \tag{2.2}$$

has different roots in some extension K' of K. In order to establish the point O, we look at the plane algebraic curve, that is, at the homogeneus equation

$$E : y^2z = ax^3 + bx^2z + cxz^2 + dz^3, \text{ with } a, b, c, d \in K, \tag{2.3}$$

which solutions are of the form

$$(x, y, 1) \text{ and } (x, y, 0) \in \mathbb{P}^2_K,$$

for the latter case there is only one solution, namely the point $(0, 1, 0) := O$ which is the point at infinity. We shall investigate the former case in more detail and we use the affine notation when referring to these points, namely $(x, y) := (x, y, 1)$.

Example 9. Let $n \in \mathbb{Z}^+$ and K a field of characteristic p. Consider the equation

$$E_n : y^2 = x^3 - n^2x;$$

let $F(x, y, z)$ be its projective completition

$$F(x, y, z) = y^2z - x^3 + n^2xz^2.$$

The points $P \in E_n(K)$ are of the form $(x, y, 1)$ and $(0, 1, 0)$. F is not singular at $(0, 1, 0)$ since

$$F(0,1,0) = \frac{\partial F}{\partial x}(0,1,0) = \frac{\partial F}{\partial y}(0,1,0) = 0,$$

but $\frac{\partial F}{\partial z}(0,1,0) \neq 0$.

Now, for the rest of the points we have

$$\frac{\partial F}{\partial y}(x,y,1) = 2y,$$

thus $\frac{\partial F}{\partial y}(x,y,1) = 0$ if $y = 0$ or K has characteristic 2.

Suppose that $\text{char}(K) = 2$, then reduction modulus 2 yields

$$E_n : y^2 = x(x+1)^2,$$

thus $(1, 0, 1)$ is always a singular point.

Now, suppose that $y = 0$, we have

$$F(x,0,1) = \frac{\partial F}{\partial z}(x,0,1) = \frac{\partial F}{\partial x}(x,0,1) = 0,$$

if and only if $n \equiv 0 \text{mod} p$ and $x = 0$.

Therefore E_n defines an elliptic curve for every field K of characteristic p, as long as p does not divide 2n.

★

Elliptic curves are abelian groups under addition of points, this is quite easy to see for Complex Elliptic Curves. Define $(0, 1, 0) \in \mathbb{P}^2_{\mathbb{C}}$ to be the identity of the Complex Elliptic Curve

$$E(\mathbb{C}) : y^2 = ax^3 + bx^2 + cx + d$$

and let l be a line in $\mathbb{P}^2_{\mathbb{C}}$ with no common factors with $E(\mathbb{C})$, say

$$l : y = mx + \beta z,$$

by Bezout's theorem l and E intersect in three points (multiplicities counted). Then we say that collinear points sum zero, that is

$$P_1 + P_2 + P_3 = 0 \leftrightarrow P_1, P_2, P_3 \in l \cap E,$$

and that two points of the curve which are on the same vertical line are inverses, namely for $P = (x, y)$ then $-P = (x, -y)$ (even in the special case when $y = 0$).

This geometric construction can be put in algebraic terms as well. let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be different points lying in $l \cap E$, then their x coordinates are roots of the cubic polynomial

$$(mx + \beta)^2 - f(x) = 0, \tag{2.4}$$

the x coordinate of the remaining point of intersection $P_3 = (x_3, y_3)$ must satisfy 2.4, so

$$(mx + \beta)^2 - f(x) = (x - x_1)(x - x_2)(x - x_3),$$

from which we deduce that

$$x_3 = -x_1 - x_2 - \frac{b - m^2}{a},$$

and substitution in l yields

$$y_3 = mx_3 + \beta,$$

where $\beta = y_1 - mx_1$. Now, we must take the negative value of P_3 in order to determine the point $P_1 + P_2$, thus

$$P_1 + P_2 = -P_3 = \left(-x_1 - x_2 - \frac{b - m^2}{a}, -y_1 + m(x_1 - x_3)\right), \tag{2.5}$$

where $m = \frac{y_2 - y_1}{x_2 - x_1}$, furthermore if we allow $P_1 = P_2$, we obtain m by implicity differentiating $y^2 = f(x)$ and we have $m = \frac{f'(x_1)}{2y_1}$.

If K is any field and if $f(x) \in K[x]$ is like (2.2), we define

$$f'(x) = 3ax^2 + 2bx + c,$$

and generalize the later construction. We summarize this in the next theorem, which can be verified algebraically.

Theorem 14. *Let E be an elliptic curve over a field K. For all P_1 and P_2 in E, we have*

$$P_1 + P_2 = -P_3 = \left(-x_1 - x_2 - \frac{b - m^2}{a}, -y_1 + m(x_1 - x_3)\right),$$

in other words, every elliptic curve is an abelian group under addition of points.

We will use the former theorem in the end of the next section, when we have all the tools to enounce the addition theorem for the $\wp$-function as corollary.

2.2 Complex elliptic curves as complex tori

Every Complex Elliptic Curve can be reduced by linear changes of homogeneous coordinates to the following normal form

$$y^2z = 4x^3 - Axz^2 - Bz^3 \text{ Weierstrass' Form;} \tag{2.6}$$

the polynomial on the right side having distinct roots, equivalently, its cubic discriminant

$$\Delta = A^3 - 27B^2 \tag{2.7}$$

is not zero.

We shall show that there exists a lattice L for which the invariants $g_2(L)$ and $g_3(L)$ as in (1.13) satisfy

$$g_2(L) = A;$$

$$g_3(L) = B.$$

First note that if $A = 0$ then $B \neq 0$, we deduce from Example 6 that $L = \omega_1 L(1, e^{2\pi i/3})$, that is, the lattice of the Eisenstein Integers multiplied by a non zero complex number ω_1. Similarly if $B = 0$ then $A \neq 0$, we deduce from Example 5 that $L = \omega_1\mathbb{Z}[i]$, the lattice of the Gaussian Integers multiplied by a non zero complex number ω_1. Finally it remains to study the case where A and B are both nonzero.

In the later case set $\Delta = A^3 - 27B^2$, we have that $\Delta \neq 0$ by hypothesis. Then $A = g_2(L)$ and $B = g_3(L)$ for some L if and only if

$$\frac{g_2(L)}{g_3(L)} = \frac{A}{B}, \text{ and } \frac{g_2^3(L)}{g_2^3(L) - 27g_3^2(L)} = \frac{A^3}{\Delta}. \tag{2.8}$$

If we replace $\tau = \omega_1/\omega_2$, i.e. normalize L to L_τ, the equation on the right of (2.8) can be written as

$$J(\tau) = \frac{g_2^3(L_\tau)}{g_2^3(L_\tau) - 27g_3^2(L_\tau)} = \frac{A^3}{\Delta},$$

but the equation $J(\tau) - a = 0$ has exactly one solution in the fundamental domain $\mathcal{B}$ showed in Figure 1.5, wether a is real or non-real. Then, in order to find ω_1 we rewrite the left side of (2.8) as follows

$$\omega_1^2 = \frac{Ag_3(L_\tau)}{Bg_2(L_\tau)},$$

and we have $\omega_2 = \tau\omega_1$.

Therefore, given an elliptic curve in Weierstrass form we can find a lattice L such that $g_2(L) = A$ and $g_3(L) = B$.

Now, let $\wp(z; L)$ the Weierstrass elliptic function for a lattice L. Recall that $\wp$ satisfies the differential equation (1.14), this enable us to state the following theorem.

Theorem 15. *The map*

$$\begin{aligned} F : \mathbb{C}/L \to E(\mathbb{C}) : y^2 &= 4x^3 - g_2x - g_3 \\ z &\mapsto (\wp(z), \wp'(z), 1) \\ 0 &\mapsto (0, 1, 0) \end{aligned} \tag{2.9}$$

is an analytic isomorphism between the Complex Torus $\mathbb{C}/L$ and the Complex Elliptic Curve E.

Proof. The image of any nonzero point z is well defined because $\wp$ satisfies the differential equation (1.14). Moreover, the map is analytic since it is given by a triple of analytic functions near of non-lattice points and near of the lattice points is given by

$$z \mapsto (\wp(z)/\wp'(z), 1, 1/\wp'(z)),$$

which is a triple of analytic functions as well.
Let $(x, y, 1) \in E(\mathbb{C})$, for every point x there are one or two preimages. In the first case x is a root of the cubic polynomial and therefore the corresponding y coordinate is $y = \wp'(z) = 0$. In the second case there are two two points in $\mathbb{C}/L$ say z and z' such that $z + z' \equiv 0 \mathrm{mod}\ L$ and the corresponding two y's coordinates are opposites in sign, leading different points in $E(\mathbb{C})$. Thus the correspondence is one-to-one.

Finally, the inverse map from the elliptic curve to the torus is done by

means of path integrals, this is explained in Appendix 1.

■

The former theorem together with the fact that every complex elliptic curve can be reduced to an elliptic curve in the Weierstrass form enable us to use the terms complex elliptic curve and complex torus indistinctly, in this way one may think elliptic curves over finite fields as discrete tori.

The next corollary is a consequence of Theorem 14 and Theorem 15.

Corollary 1. *Let L be a lattice and $\wp(z, L)$ its Weierstrass elliptic function. Then for u and v complex numbers we have*

$$\wp(u+v) = -\wp(u) - \wp(v) - \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2. \tag{2.10}$$

2.3 Points of finite order

Let $P = (x, y)$ be a point in an elliptic curve $E(K)$, let $N \geq 2$ be a positive integer and consider the map

$$[N] : E(K) \to E(K),$$

$$P \mapsto NP = \underbrace{P + \cdots + P}_{N \text{ times}};$$

we say that P is a *point of order* N if $P \in \mathrm{Ker}[N]$. The group $\bigcup_{N \geq 2} \mathrm{Ker}[N]$ is called the *torsion subgroup* of the elliptic curve. For $N > 2$ we mean by a nontrivial point of order N a point such that $P \neq 0$, $NP = 0$ and in the case of N even $2P \neq 0$.

It follows from Theorem 15 that $P_z = (x, y) \in E(\mathbb{C})$ is a point of order N if and only if $Nz \in L$.

Obviously, there may be points of infinite order. Complex elliptic curves are isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, from the analog case of the circle we know that the group of points of finite order of $\mathbb{R}/\mathbb{Z}$ is isomporphic to $\mathbb{Q}/\mathbb{Z}$, then the torsion subgroup of complex elliptic curves is isomorphic to $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$. Moreover, the group of points of order N on a complex elliptic curve is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

For any elliptic curve defined over the rationals, we have the following useful and special theorem due to Mordell.

Theorem 16. *The group $E(\mathbb{Q})$ of $\mathbb{Q}-$points on an elliptic curve E defined over $\mathbb{Q}$ is a finitely generated abelian group. That is*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

where the torsion subgroup $E(\mathbb{Q})_{tors}$ is finite and the nonnegative integer r is called the rank *of $E(\mathbb{Q})$.*

The group of points of order N of an elliptic curve $E(K')$ is invariant under the action of the Galois group of a field extension K' of K, we denote $\mathrm{Gal}(K'/K)$ the Galois group of the field extension K'/K.

Let K be a subfield of $\mathbb{C}$ and denote K_N the field obtained by adjoining both the x- and the y-coordinates and K_N^x the field obtained by adjoining just the x-coordinates, of all points of order N. Then K_N and K_N^x are finite Galois extensions of K, for in both cases we are adjoining a finite set of complex numbers which are permuted under the action of $\mathrm{Gal}(\mathbb{C}/K)$.

Compute the points of order 2 for every elliptic curve $E(K)$ is quite simple, these points are: the point at infinity 0 and the points $(e_i, 0)$ with $i = 1, 2, 3$, where the e_i's are the roots of the cubic polynomial which defines $E(K)$. The e_i's may be in some extension K' of K, this yields that $K_2 = K_2^x$ is the splitting field of the cubic polynomial which defines $E(K)$.

Since any $\sigma \in \mathrm{Gal}(K_N/K)$ permutes the points of order N and respects point addition, i.e. $\sigma(P_1+P_2) = \sigma(P_1)+\sigma(P_2)$, then σ is an automorphism of $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$, thus $\mathrm{Gal}(K_N/K)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the group of the 2×2 matrices with entries in $\mathbb{Z}/N\mathbb{Z}$ and determinant in the subgroup of units of $\mathbb{Z}/N\mathbb{Z}$.

Example 10. The group $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is isomporphic to S_3 the group of permutations of $\{1, 2, 3\}$, since $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ permutes the elements of $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ fixing $(0, 0)$.

Consider the following elliptic curves over the rational numbers $\mathbb{Q}$:

(a) $y^2 = x^3 - nx$

If n is a perfect square, then $x^3 - nx = x(x - a)(x + a)$ where $a \in \mathbb{Z}^+$, then the points of order 2 are the point at infinity 0, $(0, 0), (a, 0)$ and $(-a, 0)$, all of them having coordinates at $\mathbb{Q}$, thus for this case we have $\mathbb{Q} = \mathbb{Q}_2$ and $\mathrm{Gal}(\mathbb{Q}_2) = \{I_{\mathbb{Q}}\}$.

If n is not a perfect square, then $x^3 - nx = x(x - \sqrt{n})(x + \sqrt{n})$ and

the points of order 2 being the point at infinity 0, $(0,0)$, $(-\sqrt{n},0)$ and $(\sqrt{n},0)$. The field extension generated by the coordinates of the points of order 2, i.e. $\mathbb{Q}_2$ is simply $\mathbb{Q}(\sqrt{n})$, since $\mathrm{Gal}(\mathbb{Q}(\sqrt{n}))$ permutes $(\sqrt{n},0)$ and $(-\sqrt{n},0)$, we conclude that $\mathrm{Gal}(\mathbb{Q}(\sqrt{n}))$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ of order 2.

(b) $y^2 = x^3 - n$
If n is a perfect cube, the splitting field of $f(x) = x^3 - n = x^3 - a^3$, where $a \in \mathbb{Z}^+$, is $\mathbb{Q}(i\sqrt{3})$, since

$$f(x) = (x-a)\left(x - a\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right)\left(x - a\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right),$$

and therefore $i\sqrt{3}$ generates all the roots of f. We have two roots which coordinates do not belong to $\mathbb{Q}$, thus $\mathrm{Gal}(\mathbb{Q}(i\sqrt{3}))$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ of order 2.
If n is not a perfect cube, let α be the positive cubic root of n. The roots of $f(x) = x^3 - n$ are α, $\alpha\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$ and $\alpha\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)$. Now since α and $i\sqrt{3}$ generate all the roots of f, the splitting field of f is $\mathbb{Q}(\alpha, i\sqrt{3})$. In this case, the three points of order 2 different from infinity do not have coordinates in $\mathbb{Q}$, thus the resulting Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{3}))$ is isomorphic to the entire group $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

★

The process to find the x-coordinates of the points of order N is simple for elliptic curves in the Weierstrass form over some extension K of the rational numbers which includes g_2 and g_3, i.e. elliptic curves

$$E(K) = y^2 = f(x) = 4x^3 - g_2 x - g_3.$$

This process is carried out by means of a polynomial for which K_N^x will be the splitting field. The way we construct such a polynomial has been already studied in *The field of elliptic functions* 1.3.1 and it is a direct consequence of Theorem 15.

Consider a nontrivial point u of exact order N, then $\wp(u)$ corresponds to the x-coordinate of a point of exact order N in the elliptic curve metioned above. Since $\wp$ is an even function, $\wp(-u)$ is also a point of exact order N

and $u \neq -u$. So, we can form pairs of points $\{u, -u\}$ of exact order N. Define the function

$$f_N(z) = N \prod (\wp(z) - \wp(u)); \tag{2.11}$$

where the product is taken over a point u for each pair $\{u, -u\}$ of points of exact order N. Now consider the two following cases:

(a) Let N be odd. There are $N^2 - 1$ points of exact order N. Then $f_N(z) = F_N(\wp(z))$, $F_N(x) \in \mathbb{C}[x]$ is a polynomial of degree $\frac{N^2-1}{2}$. The even elliptic function $f_N(z)$ has $N^2 - 1$ simple zeros and a single pole of order $N^2 - 1$ at $z = 0$ with leading term $\frac{N}{z^{N^2-1}}$.

(b) Let N be even. There are $N^2 - 4$ points of exact order N. Then $F_N(x)$ is a polynomial of degree $\frac{N^2-4}{2}$. The even elliptic function $f_N(z)$ has $N^2 - 4$ simple zeros and a single pole of order $N^2 - 4$ at $z = 0$ with leading term $\frac{N}{z^{N^2-4}}$.

Therefore, a point $(x, y) = (\wp(u), \wp'(u))$ has odd order N if and only if $F_N(x) = 0$. It has even order if and only if either $y = 0$ or $F_N(x) = 0$, since the remaining nontrivial points of order N are the roots of $4x^3 - g_2x - g_3$, namely $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$ and $e_3 = \wp(\omega_1 + \omega_2/2)$.

Example 11. To find the $x-$coordinates of the points of order three of a complex elliptic curve in the Weierstrass form we can proceed in either of the two following ways

(i) We can simply apply the method just described below and we will have

$$f_3(z) = 3\left(\wp(z) - \wp\left(\frac{\omega_1}{3}\right)\right)\left(\wp(z) - \wp\left(\frac{\omega_2}{3}\right)\right)$$

$$\left(\wp(z) - \wp\left(\frac{\omega_1 + \omega_2}{3}\right)\right)\left(\wp(z) - \wp\left(\frac{2\omega_1 + \omega_2}{3}\right)\right),$$

rewriting it as a polynomial in $\wp(z) = x$ we have

$$F_N(x) = 3x^4 - ax^3 + bx^2 - cx + d,$$

where

$$\frac{a}{3} = \wp\left(\frac{\omega_1}{3}\right) + \wp\left(\frac{\omega_2}{3}\right) + \wp\left(\frac{\omega_1 + \omega_2}{3}\right) + \wp\left(\frac{2\omega_1 + \omega_2}{3}\right),$$

$$\vdots$$

$$\frac{d}{3} = \wp\left(\frac{\omega_1}{3}\right)\wp\left(\frac{\omega_2}{3}\right)\wp\left(\frac{\omega_1+\omega_2}{3}\right)\wp\left(\frac{2\omega_1+\omega_2}{3}\right);$$

and we can find explicity the values of each coefficient. Obviously this can be a hard long calculation without a computer.

(ii) It turns out that for a complex elliptic curve, the inflection points are precisely the points of order three. Then, consider an elliptic curve $E(\mathbb{C})$ in the Weierstrass form.
Implicity differentiating twice we have

$$y^2 = f(x),$$

$$2y\frac{dy}{dx} = f'(x),$$

$$2\left(\frac{dy}{dx}\right)^2 + 2y\frac{d^2y}{dx^2} = f''(x);$$

then if x is a point of order three the latter equation holds and $\frac{d^2y}{dx^2} = 0$, multiplying it by $2y^2$ we have

$$2f(x)f''(x) - f'(x)^2 = 0;$$

finally substituting $f(x) = 4x^3 - g_2x - g_3$ and dividing both sides by 16, we have

$$F_N(x) = 3x^4 - \frac{3}{2}g_2x^2 - 3g_3x - \frac{1}{16}g_2^2,$$

which is the polynomial whose roots are the $x-$coordinates of order three.

★

If we want to find the $x-$coordinates of the points of order N of an elliptic curve not necessarily in Weierstrass form over a field K, we can repeatedly apply the formulas viewed in Theorem 14 to compute a rational function depending on x and y which is the $x-$coordinate of NP. Thus $P = (x, y)$ is a point of order N if and only if x is a pole of such a function.
While in the case of a complex elliptic curve it contains all its points of

order N it could happen that for a general field K some of its points may lie in the algebraic closure of K, and even worse, if K has characteristic p the rational function which is the $x-$coordinate of NP may have less poles than expected.

Even in that cases, however, algebraically one can prove that the polynomial on the denominator of the rational function mentioned above will be of degree $\frac{N^2-1}{2}$ when N is odd, otherwise of the form $y \cdot p(x)$, where $p \in K[x]$ is of degree $\frac{N^2-4}{2}$.

This can be summarized in the following theorem.

Theorem 17. *Let E be an elliptic curve over a field K. Then the subgroup of points of order N has at most N^2 elements over any extension K' of K.*

As an example of applications of the latter theorem, we will calculate the number of points on certain kind of elliptic curves over some finite fields. Further, since elliptic curves over finite fields are finite abelian groups, then we will see what are the possible prime group decomposition of the $\mathbb{F}_q-$points on the elliptic curve.

Example 12. Let $q = p^r$, $p \nmid 2n$ and suppose that $q \equiv 3 \bmod(4)$. Consider the elliptic curve

$$E_n : y^2 = x^3 - n^2 x;$$

we want to calculate $|E_n(\mathbb{F}_q)|$.

The curve contains all its points of order 2, namely the point at infinity, $(0,0)$, $(n,0)$ and $(-n,0)$. Now consider the pairs $\{x,-x\}$ with $x \neq 0, \pm n$; there are $\frac{q-3}{2}$ such different pairs. Consider the function

$$f(x) = x^3 - n^2 x,$$

notice that $f(-x) = -x^3 + n^2 x = -f(x)$, thus f is an odd function. Thus for each pair of x's we have four possibilities

$$y = \pm\sqrt{\pm f(x)},$$

however if $f(x)$ is a square in $\mathbb{F}_q$ then $-f(x)$ is not a square and vice versa (Since -1 is not a square in $\mathbb{F}_q$ with $q \equiv 3 \bmod 4$, for $\frac{q-1}{2} \equiv 1 \bmod 2$). Thus for each pair $\{x,-x\}$ we have exactly two solutions. Therefore there are $q+1$

points in all.

Notice that the number of points does not depend on n.

Let $q = 3^{2r+1}$, $r \geq 1$, then $q \equiv 3 \bmod 4$. We have the following isomorphisms

$$E_n(\mathbb{F}_{3^3=27}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7,$$

$$E_n(\mathbb{F}_{3^5=243}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{61},$$

$$E_n(\mathbb{F}_{3^7=2187}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{547};$$

we see that there are not nontrivial points of order three, this agrees with the fact that the $x-$coordinates of the points of order three can obtained as in the Example 11, that is the $x-$coordinates are the solutions to the polynomial

$$-3x^4 + 6n^2x^2 + n^4,$$

and since $\mathbb{F}_{3^{2r+1}}$ is of characteristic 3, the nonconstant terms of the polynomial vanish, thus there are not nontrivial points of order 3 in the elliptic curves $E_n(\mathbb{F}_{3^{2r+1}})$ with $r \geq 1$.

★

Chapter 3

Number of points in hypersurfaces over finite fields

In this chapter we will investigate how to calculate the number of points in certain hypersurfaces in finite fields.

Historically there has been many mathematicians devoted to compute the number of solutions in certain equations defined over finite fields. Gauss, Jacobi, Hasse, Davenport and Weil among them, and their contributions are so remarkable that have been named after them.

Trough all this section we consider a field $\mathbb{F}_q$ of q elements, with q a prime power, and its extensions $\mathbb{F}_{q^r}/\mathbb{F}_q$ of degree r. We denote $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$.

Consider the equation

$$x^m = u,$$

for $u \in \mathbb{F}_q$.

If $u = 0$ then it has only one solution, namely $x = 0$.

If $u \in \mathbb{F}_q^*$, since $\mathbb{F}_q^*$ is a cyclic multiplicative group of order $q-1$, then x is a solution to $x^m = u$ if and only if u is a $d = \gcd(m, q-1)$ power. Notice that if $\gcd(m, q-1) = 1$ then the equation $x^m = u$ has only one solution.

A *character* is a group homomorphism from a group G to the multiplicative group of the complex numbers. A character is said to be *multiplicative* or *additive* if the group law is multiplicative or additive respectively. We

denote $\hat{G}$ the set of the characters defined in G.

For instance, consider the multiplicative group $\mathbb{F}_q^*$, every multiplicative character χ maps to a subset of the $q-1$ roots of the unity because $\mathbb{F}_q^*$ has finite order $q-1$. We denote χ_0 the trivial multiplicative character which takes every element in the field to 1, we can expand our definition and set $\chi_0(0)=1$, while for every nontrivial character $\chi(0)=0$. Nontrivial multiplicative characters are totally defined once whe chose the image of a generator w of $\mathbb{F}_q^*$.

Let $< w >= \mathbb{F}_q^*$, we denote χ_α the multiplicative character such that

$$\chi_\alpha(w) = e^{2\pi i\alpha},$$

where α is a rational number such that $\alpha(q-1)$ is an integer, that is $e^{2\pi i\alpha}$ is a $q-1$ root of the unity determined by α. This machinery motivates the next lemma.

Lemma. *The number of solutions* $N_m(u) = |\{x \in \mathbb{F}_q | x^m = u\}|$ *equals* $\sum_\alpha \chi_\alpha(u)$ *where* $\alpha \cdot m$ *is an integer, equivalently the sum over all the characters for which* $\chi^m = \chi_0$.

Proof. If $u=0$ then both sides equal 1. Now, if u is a m power there are $d = \gcd(m, q-1)$ solutions, then

$$\sum_\alpha \chi_\alpha(u) = \sum_\alpha \chi_\alpha^m(x) = d = N_m(u),$$

since there are d characters χ_α such that $\chi_\alpha^m = \chi_0$; while if u is not a m power both sides equal zero.

■

3.1 Jacobi sums

We have considered equations of the form $ax^m = u$ so far. Next, we want to compute the number of solutions of equations involving several varibles, we will see how Jacobi sums arise naturally in the way.

Let's first consider an easy example, let's compute the number of solutions of

$$x^m + y^m = 1.$$

From the above lemma we have that the number N of solutions is

$$\begin{aligned} N &= \sum_{u+v=1} N_m(u)N_m(v), \\ &= \sum_{u+v=1} \left(\sum_{\alpha} \chi_\alpha(u)\right)\left(\sum_{\beta} \chi_\beta(v)\right) \text{ with } \alpha\cdot m,\ \beta\cdot m \in \mathbb{Z}, \\ &= \sum_{\alpha,\beta} \left(\sum_{u+v=1} \chi_\alpha(u)\chi_\beta(v)\right) \text{ with } \alpha\cdot m,\ \beta\cdot m \in \mathbb{Z}. \end{aligned} \tag{3.1}$$

The sum between brackets motivates the following definition.

Definition. Let $\mathbb{F}_q$ be the field with q elements. For any $\alpha \in \mathbb{Q}^k$ such that $\alpha_i(q-1) \in \mathbb{Z}$. The *Jacobi sum* attached to α is defined by

$$J(\alpha) = J(\alpha_1, ..., \alpha_k) := \sum_{u_1+...+u_k=1} \chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k). \tag{3.2}$$

We also introduce the following sum

$$J_0(\alpha) := \sum_{u_1+...+u_k=0} \chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k). \tag{3.3}$$

Continuing with the equation $x^m + y^m = 1$, we express its number N of $\mathbb{F}_q$-points as follows

$$N = \sum_{\alpha,\beta} J(\alpha,\beta) \text{ with } \alpha\cdot m,\ \beta\cdot m \in \mathbb{Z}.$$

Now we shall prove some general properties of the Jacobi sums in the next proposition.

Proposition 1. *1. If $\alpha = 0 \in \mathbb{Q}^k$, then $J(\alpha) = J_0(\alpha) = q^k$;*

2. If $\alpha = (\alpha_1, ..., \alpha_l, 0, ..., 0) \in \mathbb{Q}^k$, $\alpha_i \neq 0$ for $i = 1, ..., l$, then $J(\alpha) = J_0(\alpha) = 0$;

3. If $\alpha \neq 0 \in \mathbb{Q}^k$, then

$$\begin{aligned} J_0(\alpha) &= \chi_{\alpha_1+\ldots+\alpha_{k-1}}(-1)J(\alpha_1,\ldots,\alpha_{k-1})\sum_{u\neq 0}\chi_{\alpha_1+\ldots+\alpha_k}(u) \\ &= \begin{cases} (q-1)\chi_{\alpha_k}(-1)J(\alpha_1,\ldots,\alpha_{k-1}) & \text{if } \sum_{i=1}^{k}\alpha_i \in \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Proof.

1. This follows immediatly because for $b \in \mathbb{F}_q$ the linear variety $u_1 + \ldots + u_k = b$ has q^{k-1} points.

2. We have

$$\begin{aligned} & \sum_{u_1+..+u_k=b}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_l}(u_l)\chi_0(u_{l+1})\cdots\chi_0(u_k) \\ = \quad & q^{k-l-1}\sum_{u_1,\ldots,u_l\in\mathbb{F}_q}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_l}(u_l) \\ = \quad & q^{k-l-1}\left(\sum_{u_1\in\mathbb{F}_q}\chi_{\alpha_1}(1)\right)\cdots\left(\sum_{u_l\in\mathbb{F}_q}\chi_{\alpha_l}(l)\right); \end{aligned}$$

notice that the first equality holds since the variety $\sum u_i = b$ has q^{k-1} points and we chose arbitrarily the points for which $\alpha = 0$. Also notice that the terms on the latter profuct is zero since the sum is taken over all the values in $\mathbb{F}_q$.

3. We have

$$\begin{aligned} J_0(\alpha_1,\ldots,\alpha_k) &= \sum_{u_1+\ldots+u_k=0}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k) \\ &= \sum_{u\neq 0}(\chi_{\alpha_k}(u))\left(\sum_{u_1+\ldots+u_{k-1}=-u}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_{k-1}}(u_{k-1})\right) \\ &= \sum_{u\neq 0}(\chi_{\alpha_k}(u))\left(\sum_{v_1+\ldots+v_{k-1}=1}\chi_{\alpha_1}(-u\cdot v_1)\cdots\chi_{\alpha_{k-1}}(-u\cdot v_{k-1})\right) \\ &= \sum_{u\neq 0}(\chi_{\alpha_k}(u))\left(\sum_{v_1+\ldots+v_{k-1}=1}\chi_{\alpha_1+\ldots+\alpha_{k-1}}(-u)\chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_{k-1}}(v_{k-1})\right) \\ &= \sum_{u\neq 0}\chi_{\alpha_1+\ldots+\alpha_k}(u)\chi_{\alpha_1+\ldots+\alpha_{k-1}}(-1)J(\alpha_1,\ldots,\alpha_{k-1}) \\ &= \chi_{\alpha_1+\ldots+\alpha_{k-1}}(-1)J(\alpha_1,\ldots,\alpha_{k-1})\sum_{u\neq 0}\chi_{\alpha_1+\ldots+\alpha_k}(u). \end{aligned}$$

■

3.2 Gauss sums

Now we investigate Gauss sums which are closely related to Jacobi sums. Both of these sums allow us to continue our exploration of the number of solutions of equations in finite fields. For this we show some properties involving both Gauss sums and Jacobi sums.

Let $\mathbb{F}_{q^r}/\mathbb{F}_q$ be a field extension of the finite field with $q = p^r$ elements, with p prime.

Definition. We define the *trace* and the *norm* by

$$\begin{gathered}\mathrm{Tr} : \mathbb{F}_{q^r} \to F_q,\\ x \mapsto x + x^q + ... + x^{q^{r-1}};\\ \mathrm{Nm} : \mathbb{F}_{q^r} \to F_q,\\ x \mapsto x \cdot x^q \cdots x^{q^{r-1}};\end{gathered}$$

respectively.

The trace is an onto $\mathbb{F}_q$-linear map and the norm is an onto multiplicative map.

Consider the following additive character given by

$$\begin{gathered}\psi : \mathbb{F}_{q^r} \to \mathbb{C};\\ x \mapsto e^{\frac{2\pi i}{q}\mathrm{Tr}(x)},\end{gathered}$$

since Tr is onto, we obtain in this way a non trivial additive character.

Definition. Let $\chi \in \hat{\mathbb{F}}_q^*$ and ψ the additive character defined above. We define the *Gauss sum* of χ depending on $t \in \mathbb{F}_q$ by the relation

$$g_t(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(tx).$$

We denote $g_1(\chi)$ simply as $g(\chi)$.

Lets denote χ_0 the trivial character and the χ denote a nontrivial character; and $\bar{\chi}$ denotes the complex conjugate character of χ, whose value at x is the complex conjugate of $\chi(x)$. We have the following proposition

Proposition 2. *1.* $g(\chi_0) = 0$;

2. $g(\bar{\chi}) = g(\chi^{-1}) = \chi(-1)\overline{g(\chi)}$;

3. $g(\chi) \cdot \overline{g(\chi)} = q$;

4. *Let* $\alpha \in \mathbb{Q}^k$. *If* $\alpha_1, ..., \alpha_k$ *and* $\sum \alpha_i \notin \mathbb{Z}$, *then*

$$J(\alpha_1, ..., \alpha_k) = \frac{g(\chi_{\alpha_1}) \cdots g(\chi_{\alpha_k})}{g(\chi_{\alpha_1} \cdots \chi_{\alpha_k})},$$

and therefore

$$|J(\alpha_1, ..., \alpha_k)| = q^{\frac{k-1}{2}}.$$

5. *Let* $\alpha \in \mathbb{Q}^k$. *If* $\alpha_1, ..., \alpha_k$ *are nonzero and* $\sum \alpha_i \in \mathbb{Z}$, *then*

$$\begin{aligned} J(\alpha_1, ..., \alpha_k) &= -\frac{g(\chi_{\alpha_1}) \cdots g(\chi_{\alpha_k})}{q} \\ &= -\chi_{\alpha_k}(-1) J(\alpha_1, ..., \alpha_{k-1}), \end{aligned} \tag{3.4}$$

and therefore

$$|J(\alpha_1, ..., \alpha_k)| = q^{\frac{k-2}{2}}.$$

Proof.

1. $g(\chi_0) = \sum_{x \in \mathbb{F}_q} \psi(x) = 0.$

2. The first equality holds since $|\bar{\chi}(x)| = 1$, thus $\bar{\chi}(x) = \chi^{-1}(x)$. The

second runs as follows

$$\begin{aligned}
\chi(-1)\sum_{x\in\mathbb{F}_q}\overline{\chi(x)\psi(x)} &= \chi(-1)\sum_{x\in\mathbb{F}_q}\overline{\chi(x)\psi(x)} \\
&= \chi(-1)\sum_{x\in\mathbb{F}_q}\chi^{-1}(x)\psi^{-1}(x) \\
&= \sum_{x\in\mathbb{F}_q}\chi(-1)\chi(x^{-1})\psi(-x) \\
&= \sum_{x\in\mathbb{F}_q}\chi^{-1}(-x)\psi(-x) \\
&= \sum_{-x\in\mathbb{F}_q}\overline{\chi(x)}\psi(x) \\
&= g(\overline{\chi}).
\end{aligned}$$

3. In the Gauss sums we will sum over the nonzero elements in $\mathbb{F}_q$ since the terms containing 0 are 0 as well. Then we have

$$\begin{aligned}
g(\chi)\cdot\overline{g(\chi)} &= \sum_{x\in\mathbb{F}_q^*}\chi(x)\psi(x)\sum_{y\in\mathbb{F}_q^*}\overline{\chi(y)\psi(y)} \\
&= \sum_{x,y\in\mathbb{F}_q^*}\chi(xy^{-1})\psi(x-y),
\end{aligned}$$

now making $x = xy$, we have

$$\begin{aligned}
&= \sum_{x,y\in\mathbb{F}_q^*}\chi(x)\psi(y(x-1)) \\
&= \sum_{x\in\mathbb{F}_q^*}\chi(x)\sum_{y\in\mathbb{F}_q^*}\psi(y(x-1)) \\
&= \chi(1)\sum_{y\in\mathbb{F}_q^*}\psi(0) - \sum_{x\neq 0,1}\chi(x) \\
&= q.
\end{aligned} \tag{3.5}$$

4. First notice that

$$\begin{aligned}
g(\chi_{\alpha_1})\cdots g(\chi_{\alpha_k}) &= \left(\sum_{u_1\in\mathbb{F}_q^*}\chi_{\alpha_1}(u_1)\psi(u_1)\right)\cdots\left(\sum_{u_k\in\mathbb{F}_q^*}\chi_{\alpha_k}(u_k)\psi(u_k)\right)\\
&= \sum_{u}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k)\psi(u_1+...+u_k)\\
&= \sum_{v}\left(\sum_{u_1+...+u_k=v}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k)\right)\psi(v)\\
&= J_0(\alpha_1,...,\alpha_k)+\sum_{v\neq 0}\left(\sum_{u_1+...+u_k=v}\chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k)\right)\psi(v)\\
&= J_0(\alpha_1,...,\alpha_k)+\sum_{v\neq 0}\left(\sum_{u_1'+...+u_k'=1}\chi_{\alpha_1}(u_1'v)\cdots\chi_{\alpha_k}(u_k'v)\right)\psi(v)\\
&= J_0(\alpha_1,...,\alpha_k)+J(\alpha_1,...,\alpha_k)\sum_{v\neq 0}\chi_{\alpha_1}(v)\cdots\chi_{\alpha_k}(v)\psi(v)\\
&= J_0(\alpha_1,...,\alpha_k)+J(\alpha_1,...,\alpha_k)g(\chi_{\alpha_1}\cdots\chi_{\alpha_k})\\
&= J(\alpha_1,...,\alpha_k)g(\chi_{\alpha_1}\cdots\chi_{\alpha_k}).
\end{aligned}$$

In the fifth equality we make $u_i = u_i'v$ for $i = 1,...,k$, since $v \neq 0$. We also have $J_0(\alpha_1,...,\alpha_k) = 0$ by property (3) of Proposition 1, since $\sum\alpha_i \notin \mathbb{Z}$. Finally the norm $|J(\alpha)| = q^{\frac{k-1}{2}}$ follows from property (3) of the current proposition.

5. From the past property we have

$$g(\chi_{\alpha_1})\cdots g(\chi_{\alpha_k}) = J_0(\alpha_1,...,\alpha_k)+J(\alpha_1,...,\alpha_k)\sum_{v\neq 0}\chi_{\alpha_1}(v)\cdots\chi_{\alpha_k}(v)\psi(v),$$

notice that

$$\sum_{v\neq 0}\chi_{\alpha_1}(v)\cdots\chi_{\alpha_k}(v)\psi(v) = -1,$$

because we are summing over all nonzero $v \in \mathbb{F}_q$ and $\chi_{\alpha_1}\cdots\chi_{\alpha_k}$ is the trivial character. So we have

$$J(\alpha_1,...,\alpha_k) = J_0(\alpha_1,...,\alpha_k) - g(\chi_{\alpha_1})\cdots g(\chi_{\alpha_k}),$$

from property (3) of Proposition 1 we have

$$J_0(\alpha) = (q-1)\chi_{\alpha_k}(-1)J(\alpha_1,...,\alpha_{k-1}), \tag{3.6}$$

using properties (2) and (3) of the current proposition we deduce

$$\chi_{\alpha_k}(-1) = \frac{g(\chi_{\alpha_k})g(\overline{\chi_{\alpha_k}})}{q},$$

substituting this last equation in (3.6) we get

$$J_0(\alpha) = (q-1)J(\alpha_1, ..., \alpha_{k-1})\frac{g(\chi_{\alpha_k})g(\overline{\chi_{\alpha_k}})}{q},$$

notice that since $\chi_{\alpha_1} \cdots \chi_{\alpha_k} = \chi_0$ then $\chi_{\alpha_1} \cdots \chi_{\alpha_{k-1}} = \overline{\chi_{\alpha_k}}$, that is

$$J(\alpha_1, ..., \alpha_k) = -\frac{g(\chi_{\alpha_1}) \cdots g(\chi_{\alpha_k})}{q}.$$

Finally the norm $|J(\alpha)| = q^{\frac{k-2}{2}}$ follows from property (3) of the current proposition.

■

3.3 Weil's Theorem

In this subsection we state and reproduce the proof of a result due to the french mathematician André Weil. The theorem gives a formula for the number of points in certains hypersurfaces in finite fields, an estimate will be given as well.

Theorem 18. *Consider the equation*

$$a_1 x_1^{n_1} + ... + a_k x_k^{n_k} = b, \tag{3.7}$$

with $a_i, b \in \mathbb{F}_q$ *and* $n_i | q-1$.

1. *If* $b = 0$, *then the number* N *of* $\mathbb{F}_q$*-points in (3.7) is given by*

$$N = q^{k-1} + \sum_{\alpha} \chi_{\alpha_1}(a_1^{-1}) \cdots \chi_{\alpha_k}(a_k^{-1}) J_0(\alpha_1, ..., \alpha_k),$$

with $\alpha \in \mathbb{Q}^k \cap (0,1)^k$ *and* $\alpha_i \cdot n_i \in \mathbb{Z}$ *for all* i. *If*

$$M_0 = |\{\alpha \in \mathbb{Q}^k \cap (0,1)^k | \alpha_i \cdot n_i \in \mathbb{Z} \text{ for all } i; \text{ and } \sum \alpha_i \in \mathbb{Z}\}|$$

then

$$|N - q^{k-1}| \leq M_0(q-1)q^{\frac{k-2}{2}}.$$

2. If $b \neq 0$, then the number N of $\mathbb{F}_q$-points in (3.7) is given by

$$N = q^{k-1} + \sum_{\alpha} \chi_{\alpha_1} \cdots \chi_{\alpha_k}(b)\chi_{\alpha_1}(a_1^{-1}) \cdots \chi_{\alpha_k}(a_k^{-1})J(\alpha_1, ..., \alpha_k),$$

with $\alpha \in \mathbb{Q}^k \cap (0,1)^k$, $\alpha_i \cdot n_i \in \mathbb{Z}$ for all i. If

$$M = |\{\alpha \in \mathbb{Q}^k \cap (0,1)^k | \alpha_i \cdot n_i \in \mathbb{Z} \text{ for all } i; \text{ and } \sum \alpha_i \notin \mathbb{Z}\}|$$

then

$$|N - q^{k-1}| \leq M_0 q^{\frac{k-2}{2}} + M q^{\frac{k-1}{2}}.$$

Proof.

1. If $b = 0$, let N the number of solutions to (3.7), thus

$$\begin{aligned}
N &= \sum_{a_1u_1+...+a_ku_k=0} N_{n_1}(u_1) \cdots N_{n_k}(u_k) \\
&= \sum_{a_1u_1+...+a_ku_k=0} \left(\sum_{\alpha_1} \chi_{\alpha_1}(u_1)\right) \cdots \left(\sum_{\alpha_k} \chi_{\alpha_k}(u_k)\right) \\
&= \sum_{\substack{a_1u_1+...+a_ku_k=0 \\ \alpha}} \chi_{\alpha_1}(u_1) \cdots \chi_{\alpha_k}(u_k) \\
&= q^{k-1} + \sum_{\substack{a_1u_1+...+a_ku_k=0 \\ \alpha \neq 0}} \chi_{\alpha_1}(u_1) \cdots \chi_{\alpha_k}(u_k) \\
&= q^{k-1} + \sum_{\substack{u_1+...+u_k=0 \\ \alpha \neq 0}} \chi_{\alpha_1}(a_1^{-1}) \cdots \chi_{\alpha_k}(a_k^{-1})\chi_{\alpha_1}(u_1) \cdots \chi_{\alpha_k}(u_k) \\
&= q^{k-1} + \sum_{\alpha \neq 0} \chi_{\alpha_1}(a_1^{-1}) \cdots \chi_{\alpha_k}(a_k^{-1})J_0(\alpha_1, ..., \alpha_k).
\end{aligned}$$

In the penultimate equation we replace u_i by $\frac{u_i}{a_i}$; by properties (2) and (3) of Proposition 1 we may ask $\alpha_i \neq 0$ and $\sum \alpha_i \in \mathbb{Z}$. This proves the first part.

In the next development we use properties (3) and (5) of Proposition 1 and 2 respectively,

$$\begin{aligned}
|N - q^{k-1}| &= \left| \sum_{\alpha \neq 0} \chi_{\alpha_1}(a_1^{-1}) \cdots \chi_{\alpha_k}(a_k^{-1})J_0(\alpha_1, ..., \alpha_k) \right| \\
&\leq M_0 \, |J_0(\alpha_1, ..., \alpha_k)| \\
&= M_0 \, |(q-1)\chi_{\alpha_k}(-1)J(\alpha_1, ..., \alpha_{k-1})| \\
&= M_0(q-1) \, |J(\alpha_1, ..., \alpha_k)| \\
&= M_0(q-1)q^{\frac{k-2}{2}}.
\end{aligned}$$

2. Similarly, if $b \neq 0$ we get

$$N = q^{k-1} + \sum_{\substack{a_1u_1+\ldots+a_ku_k=b \\ \alpha\neq 0}} \chi_{\alpha_1}(u_1)\cdots\chi_{\alpha_k}(u_k),$$

we replace u_i by $\frac{v_i b}{a_i}$ and we get

$$\begin{aligned} N &= q^{k-1} + \sum_{\substack{v_1+\ldots+v_k=1 \\ \alpha\neq 0}} \chi_{\alpha_1}\cdots\chi_{\alpha_k}(b)\chi_{\alpha_1}(a_1^{-1})\cdots\chi_{\alpha_k}(a_k^{-1})\chi_{\alpha_1}(v_1)\cdots\chi_{\alpha_k}(v_k) \\ &= q^{k-1} + \sum_{\alpha\neq 0} \chi_{\alpha_1}\cdots\chi_{\alpha_k}(b)\chi_{\alpha_1}(a_1^{-1})\cdots\chi_{\alpha_k}(a_k^{-1})J(\alpha_1,...,\alpha_k). \end{aligned}$$

Now the inequality follows from the properties (4) and (5) of Proposition 2, we get

$$\begin{aligned} |N - q^{k-1}| &= \left|\sum_{\alpha\neq 0} \chi_{\alpha_1}\cdots\chi_{\alpha_k}(b)\chi_{\alpha_1}(a_1^{-1})\cdots\chi_{\alpha_k}(a_k^{-1})J(\alpha_1,...,\alpha_k)\right| \\ &\leq \sum_{\alpha\neq 0} \left|\chi_{\alpha_1}\cdots\chi_{\alpha_k}(b)\chi_{\alpha_1}(a_1^{-1})\cdots\chi_{\alpha_k}(a_k^{-1})J(\alpha_1,...,\alpha_k)\right| \\ &= \sum_{\alpha\neq 0} |J(\alpha_1,...,\alpha_k)| \\ &= M_0 q^{\frac{k-2}{2}} + M q^{\frac{k-1}{2}}. \end{aligned}$$

This proves the theorem.

■

Now we compute the number of points in $\mathbb{F}_q$ of a particular equation.

Example 13. Let $q = p^r$ be a prime power and $p \nmid 2n$, consider the equation

$$x_1^2 - x_2^4 = 4n^2; \tag{3.8}$$

denote N the number of its $\mathbb{F}_q$-points. Let w be a generator of $\mathbb{F}_q^*$.

First suppose that $q \equiv 3 \bmod 4$. Then we have

$$N = \sum_{u_1-u_2=4n^2} N_2(u_1)N_4(u_2),$$

notice that $\gcd(2, q-1) = \gcd(4, q-1) = 2$, then

$$\begin{aligned} N &= \sum_{u_1-u_2=4n^2} \left(\sum_{i=0,1} \chi_{i/2}(u_1) \right) \left(\sum_{j=0,1} \chi_{j/2}(u_2) \right) \\ &= q + \sum_{u_1-u_2=4n^2} \chi_{1/2}(u_1)\chi_{1/2}(u_2) \\ &= q + \sum_{v_1+v_2=1} \chi_{1/2}(4n^2)\chi_{1/2}(v_1)\chi_{1/2}(-1)\chi_{1/2}(4n^2)\chi_{1/2}(v_2), \end{aligned} \tag{3.9}$$

where in the last equation we replaced $u_1 = 4n^2 v_1$ and $u_2 = -4n^2 v_2$. We get

$$N = q + \chi_{1/2}(-1) J(1/2, 1/2),$$

by property (5) of Proposition 2 we have that $J(1/2, 1/2) = -\chi_{1/2}(-1)$, thus

$$N = q - 1.$$

Now if $q \equiv 1 \bmod 4$ by Theorem 18 we have

$$\begin{aligned} N &= q + \sum_{j=1,2,3} \chi_{\frac{1}{2}}(4n^2)\chi_{\frac{j}{4}}(4n^2)\chi_{\frac{1}{2}}(1)\chi_{\frac{j}{4}}(-1) J\left(\frac{1}{2}, \frac{j}{4}\right) \\ &= q + \sum_{j=1,2,3} \chi_{\frac{j}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{j}{4}\right) \\ &= q + \chi_{\frac{1}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{1}{4}\right) + \chi_{\frac{2}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{2}{4}\right) + \chi_{\frac{3}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{3}{4}\right) \\ &= q + \chi_{\frac{1}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{1}{4}\right) + J\left(\frac{1}{2}, \frac{2}{4}\right) + \chi_{\frac{3}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{3}{4}\right), \end{aligned}$$

notice that $\chi_{\frac{2}{4}}(4n^2) = \chi_{\frac{1}{2}}(4n^2) = 1$; because of $\chi_{\frac{1}{2}}(w) = e^{\pi i} = -1$ we compute that $\chi_{\frac{1}{2}}(-1) = \chi_{\frac{1}{2}}(w^{\frac{q-1}{2}}) = (-1)^{\frac{q-1}{2}} = 1$ since $\frac{q-1}{2}$ is even; and $\chi_{\frac{3}{4}} = \chi_{\frac{2}{4}}\chi_{\frac{1}{4}}$. By property (5) of Proposition 2 we have that $J\left(\frac{1}{2}, \frac{1}{2}\right) = -\chi_{\frac{1}{2}}(-1) = -1$. Therefore

$$\begin{aligned} N &= q - 1 + \chi_{\frac{1}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{1}{4}\right) + \chi_{\frac{1}{4}}(-4n^2) J\left(\frac{1}{2}, \frac{3}{4}\right), \\ &= q - 1 + \chi_{\frac{1}{4}}(-4n^2) \left(J\left(\frac{1}{2}, \frac{1}{4}\right) + J\left(\frac{1}{2}, \frac{3}{4}\right) \right). \end{aligned}$$

If $q \equiv 1 \bmod 8$ choosing a generator w of $\mathbb{F}_q^*$ such that $\chi_{1/4}(w) = i$ we have

$$\chi_{1/4}(-1) = \chi_{1/4}(w^{\frac{q-1}{2}}) = i^{4k} = 1,$$

for some $k \in \mathbb{Z}$.

Similarly, if $q \equiv 5 \bmod 8$ we have that $\chi_{1/4}(-1) = -1$.

By quadratic reciprocity we have

$$\chi_{1/4}(4) = \chi_{1/2}(2) = \begin{cases} 1 & \text{if } q \equiv 1 \bmod 8 \\ -1 & \text{if } q \equiv 5 \bmod 8. \end{cases}$$

Therefore $\chi_{1/4}(-4n^2) = \chi_{1/2}(n)$ and we have

$$N = q - 1 + \chi_{1/2}(n)(J(1/2, 1/4) + J(1/2, 3/4)),$$

finally replacing $\mu = \mu_{n,q} = -\chi_{1/2}(n)J(1/2, 1/4)$ we have

$$N = q - 1 - \mu - \overline{\mu}.$$

In the next chapter we will pursue the investigations on this equations, especially on the nature of the variable μ.

3.4 The Hasse-Davenport Relation

We have investigated the number of solutions of equations in a fixed finite field so far, but we have not yet dealed with extensions of such a fixed field, we do not have any information about the behaviour of the number of points in such equations.

The next result is due to two mathematicians: Hasse and Davenport, whose result is of considerable interest, enabling us to compare the number of solutions of an equation in a given finite field and in all the extensions of finite degree of that field. We will prove the theorem of Hasse and Davenport and apply it to the equations we are considering.

Let χ_α be a multiplicative character of $\mathbb{F}_q$, such that $\chi_\alpha(w) = e^{2\pi i\alpha}$ for a generator w of $\mathbb{F}_q^*$. Consider a finite extension of $\mathbb{F}_q$, say $\mathbb{F}_{q^r}$, then there exists a generator z of $\mathbb{F}_{q^r}^*$ such that $\mathrm{Nm}(z) = w$. Then $\chi_{\alpha,r}(z) = \chi_\alpha(\mathrm{Nm}(z))$

defines a multiplicative character in $\mathbb{F}_{q^r}$, when the α is fixed we just write χ_r. Similarly $\psi_r(z) = \psi(\mathrm{Tr}(z))$ defines an additive character in $\mathbb{F}_{q^r}$. Let now define the next gauss sum in $\mathbb{F}_{q^r}$

$$g(\chi_r) = \sum_{x \in \mathbb{F}_{q^r}} \chi_r(x)\psi_r(x).$$

Theorem 19. *Let χ_r be a multiplicative character of $\mathbb{F}_{q^r}$, then we have*

$$-g(\chi_r) = (-g(\chi))^r. \tag{3.10}$$

Proof. Let $S \subset \mathbb{F}_q[x]$ be the set of all monic polynomials over F_q, and let $\tilde{S} \subset S$ be the set of all those irreducible polynomials (Subscrips will indicate the degree of the polynomials). $\mathbb{F}_{q^r}$ is the splitting field for the polynomial $x^{q^r} - x$ thus

$$x^{q^r} - x = \prod_{a \in \mathbb{F}_{q^r}} (x - a),$$

furthermore

$$x^{q^r} - x = \prod_{\substack{f \in \tilde{S} \\ \deg f | r}} f, \tag{3.11}$$

for if $g(x)$ is any monic irreducible factor of $F(x) = x^{q^r} - x$ over $\mathbb{F}_q$, all its roots lie in $\mathbb{F}_{q^r}$ and the extension $\mathbb{F}_q(a)/\mathbb{F}_q$ generated by one of its roots must have degree $m = \deg(g)$ with $m|r$. Conversely, let $g(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ with degree m that divides r. Then $\mathbb{F}_{q^r}$ has a subfield with q^m elements, and this field is isomorphic to $\mathbb{F}_q(a)$, with $a \in \mathbb{F}_{q^r}$. Then we have $g(a) = F(a) = 0$, and since $g(a)$ is the minimal polynomial of a over $\mathbb{F}_q$, $g(x)$ divides $F(x)$. The roots of $F(x)$ are all distinct, so no irreducible factor can appear more than once.

Now consider a multiplicative character χ and an additive character ψ of $\mathbb{F}_q$. We define the map

$$\begin{aligned} \lambda : S &\to \mathbb{C}, \\ f(x) = x^d - c_1 x^{d-1} + \ldots + (-1)^d c_d &\mapsto \chi(c_d)\psi(c_1); \end{aligned} \tag{3.12}$$

this map is multiplicative, since for

$$f(x) = x^d - c_1 x^{d-1} + \ldots + (-1)^d c_d \text{ and } g(x) = x^{d'} - c'_1 x^{d'-1} + \ldots + (-1)^{d'} c'_{d'}$$

we have

$$\begin{aligned}\lambda(fg) &= x^{d+d'} - (c_1 + c_1')x^{d+d'-1} + ... + (-1)^{d+d'}c_d c_{d'} \\ &= \chi(c_d c_{d'})\psi(c_1 + c_1') \\ &= \chi(c_d)\psi(c_1)\chi(c_{d'})\psi(c_1') \\ &= \lambda(f)\lambda(g).\end{aligned}$$

We can express the Gauss sum of a character χ in terms of $f \in S_1$ as follows

$$\sum_{f \in S_1} \lambda(f) = \sum_{f \in S_1} \chi(c)\psi(c) = \sum_{c \in \mathbb{F}_q} \chi(c)\psi(c) = g(\chi). \tag{3.13}$$

Next we prove some equalities that enable us to prove a similar assertion about Gauss sums of a character χ_r in terms of irreducible polynomials.

Suppose that $a \in \mathbb{F}_{q^r}$ is a root of $f \in \tilde{S}_d$ where d divides r. Then

$$\mathbb{F}_q(a) \simeq \mathbb{F}_q[x]/f(x) \simeq \mathbb{F}_{q^d},$$

that is a generates a field extension of degree d. Now if

$$f(x) = x^d - c_1 x^{d-1} + ... + (-1)^d c_d$$

then $\mathrm{Tr}(a) = c_1$ and $\mathrm{Nm}(a) = c_d$. So we have

$$\lambda(f) = \chi(\mathrm{Nm}(a))\psi(\mathrm{Tr}(a)),$$

where Tr and Nm denote the trace and the norm from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$ respectively.

On the other hand we have that

$$\mathbb{F}_{q^r} \simeq \mathbb{F}_{(q^d)^m} \simeq \mathbb{F}_{q^d}/g(x),$$

with $r = dm$ and $g(x) \in \mathbb{F}_{q^d}[x]$ is of degree m, that is $\mathbb{F}_{q^r}$ is an extension of $\mathbb{F}_{q^d}$ of degree m. Then if we consider the map

$$\lambda' : S' \to \mathbb{C};$$

where S' is the set of the monic polynomials over $\mathbb{F}_{q^r}$ we have that

$$\begin{aligned}\lambda'(x-a) &= \chi_r(a)\psi_r(a) \\ &= \chi(\mathrm{Nm}_{r,1}(a))\psi(\mathrm{Tr}_{r,1}(a)) \\ &= \chi(\mathrm{Nm}_{d,1} \circ \mathrm{Nm}_{r,d}(a))\psi(\mathrm{Tr}_{d,1} \circ \mathrm{Tr}_{r,d}(a)) \\ &= \chi(\mathrm{Nm}_{d,1}(a^m))\psi(\mathrm{Tr}_{d,1}(ma)) \\ &= \chi(\mathrm{Nm}_{d,1}(a)^m)\psi(m\mathrm{Tr}_{d,1}(a)) \\ &= \chi(\mathrm{Nm}_{d,1}(a))^m\psi(\mathrm{Tr}_{d,1}(a))^m,\end{aligned}$$

here $\mathrm{Nm}_{i,j}$ and $\mathrm{Tr}_{i,j}$ denote the norm and the trace from $\mathbb{F}_{q^i}$ to $\mathbb{F}_{q^j}$ for $j|i$; therefore

$$\lambda(f)^{r/d} = \chi_r(a)\psi_r(a). \tag{3.14}$$

A polynomial $f \in \tilde{S}_d$ with $d|r$ has d differet roots in $\mathbb{F}_{q^r}$ (each of them satisfying (3.14)) and the roots of all those polynomials coincide with the elements $\mathbb{F}_{q^r}$ by (3.11), thus

$$g(\chi_r) = \sum_{d|r} \sum_{f \in \tilde{S}_d} d\lambda(f)^{r/d}. \tag{3.15}$$

For an indeterminate T the power series identity

$$\sum_{f \in S} \lambda(f) T^{\deg f} = \prod_{f \in \tilde{S}} (1 - \lambda(f) T^{\deg f})^{-1}, \tag{3.16}$$

holds. For the right side we have

$$\begin{aligned}
\prod_{f \in \tilde{S}} (1 - \lambda(f) T^{\deg f})^{-1} &= \prod_{f \in \tilde{S}} \sum_{n \geq 0} \left(\lambda(f) T^{\deg f}\right)^n \\
&= \prod_{f \in \tilde{S}} \sum_{n \geq 0} \lambda(f)^n T^{n \deg f} \\
&= \prod_{f \in \tilde{S}} \sum_{n \geq 0} \lambda(f^n) T^{\deg f^n} \\
&= \sum_{f \in S} \lambda(f) T^{\deg f},
\end{aligned}$$

the last equation holds since every monic polynomial is the product of irreducible monic polynomials.

We can simplify the expression on the left of the equation (3.16) as follows

$$\begin{aligned}
\sum_{f \in S} \lambda(f) T^{\deg f} &= 1 + \sum_{f \in S_1} \lambda(f) T + \sum_{f \in S_2} \lambda(f) T^2 + \sum_{f \in S_3} \lambda(f) T^3 + \ldots \\
&= 1 + g(\chi) T + \sum_{n \geq 2} \left(q^{n-2} \left(\sum_{c_n \in \mathbb{F}_q} \chi(c_n) \right) \left(\sum_{c_1 \in \mathbb{F}_q} \chi(c_1) \right) T^n \right) \\
&= 1 + g(\chi) T.
\end{aligned}$$

Then the equation (3.16) becomes

$$1 + g(\chi) T = \prod_{f \in \tilde{S}} (1 - \lambda(f) T^{\deg f})^{-1}. \tag{3.17}$$

Taking the logarithmic derivative in both sides of (3.17) and multiplying by T we have

$$\frac{g(\chi)T}{1+g(\chi)T} = \sum_{f\in\tilde{S}} \frac{\deg(f)\lambda(f)T^{\deg(f)}}{1-\lambda(f)T^{\deg(f)}},$$

expanding the geometric series in both sides of the latter equation we get

$$\sum_{n\geq 0}(-1)^n g(\chi)^{n+1}T^{n+1} = \sum_{f\in\tilde{S}}\sum_{n'\geq 0}\deg(f)\lambda(f)^{n'+1}T^{(n'+1)\deg(f)},$$

then we equate the coefficients of T^r

$$(-1)^{r-1}g(\chi)^r = \sum_{d|r}\sum_{f\in\tilde{S}_d} d\lambda(f)^{r/d},$$

finally substituting the right side as in equation (3.15) and multiplying by -1 we have the desired result

$$(-g(\chi))^r = -g(\chi_r).$$

■

3.5 Remarks on Gauss sums

Until now we have considered characters over finite fields. Although we can expand our definition to some rings. We will see now how to do this and prove some properties about these characters, especially those which concern their Gauss sums.

Let R be the ring of integers in a number field K, and let I be a nonzero ideal of R. Then R/I is a finite ring.

Let

$$\psi : R/I \ \to \ \mathbb{C}^*$$

be an additive character which is nontrivial on any additive subgroup of R/I of the form J/I for any strictly larger ideal $J \supset I$, including the improper ideal R, which will be the only such J if I is a prime ideal.

Define the norm $\mathrm{Nm}(I) = |R/I|$ and let

$$\chi : (R/I)^* \ \to \ \mathbb{C}^*$$

be any multiplicative character, with $\chi(x) = 0$ for $x \in R/I$ not prime to I.

Finally define the Gauss sum of a multiplicative character χ of R/I as

$$g(\chi) \;=\; g(\chi, \psi) \;=\; \sum_{x \in R/I} \chi(x)\psi(x).$$

We say that a multiplicative character χ is *primitive* modulo I if for any strictly larger ideal $J \supset I$, χ is nontrivial on the subgroup of $(R/I)^*$ consisting of elements congruent to 1 modulo J.

Proposition 3. *Let R and I be as before, for any $a \in (R/I)^*$ we have*

$$\sum_{x \in R/I} \chi(x)\psi(ax) = \overline{\chi}(a) g(\chi, \psi).$$

Moreover if χ is primitive then the equation holds for any $a \in R/I$.

Proof. First let $x = x/a$, then

$$\begin{aligned} \sum_{x \in R/I} \chi(x)\psi(ax) &= \sum_{x \in R/I} \chi(x)\overline{\chi}(a)\psi(x) \\ &= \overline{\chi}(a) g(\chi, \psi). \end{aligned}$$

For the second part let $a \in R/I$ and let χ be primitive. Denote J the ideal of elements $x \in R$ such that $ax \in I$.

Suppose that a is not prime with I, then the right side of the equality vanishes since $\overline{\chi}(a) = 0$.

For instance if $a \in I$ then $J = R$ and $\psi(a) = 1$, we have

$$\sum_{x \in R/I} \chi(x)\psi(ax) = \sum_{x \in R/I} \chi(x) = 0,$$

therefore both sides equal zero.

Since $\chi(x) = 0$ if x is not prime to I then the left side becomes

$$\sum_{x \in R/I} \chi(x)\psi(ax) = \sum_{x \in (R/I)^*} \chi(x)\psi(ax),$$

now we can decompose the right side of the later equation as follows

$$\begin{aligned} \sum_{x \in (R/I)^*} \chi(x)\psi(ax) &= \psi(a) \sum_{\substack{x \in (R/I)^* \\ x \equiv 1 \mod J}} \chi(x) + \psi(-a) \sum_{\substack{x \in (R/I)^* \\ x \equiv -1 \mod J}} \chi(x) \\ &= \Big(\psi(a) + \overline{\psi}(a)\chi(-1)\Big) \sum_{\substack{x \in (R/I)^* \\ x \equiv 1 \mod J}} \chi(x); \end{aligned}$$

where the sum

$$\sum_{\substack{x\in(R/I)^* \\ x\equiv 1 \mod J}} \chi(x)$$

is taken over a multiplicative subgroup then it must be zero, this proves our assertion.

■

In the same fashion we did for Gauss sums of multiplicative characters of a finite field, we can calculate the norm of a Gauss sum of a primitive character of R/I. We resume this in the next proposition.

Proposition 4. *For any χ primitive*

$$g(\chi,\psi)g(\overline{\chi},\psi) = \chi(-1)Nm(I),$$

and

$$g(\chi,\psi)\overline{g(\chi,\psi)} = Nm(I).$$

Proof. First we have

$$\begin{aligned}\overline{g(\chi,\psi)} &= g(\overline{\chi},\overline{\psi}) \\ &= \sum_{x\in R/I} \overline{\chi}(x)\psi(-x) \\ &= \chi(-1)g(\overline{\chi},\psi).\end{aligned}$$

Then it suffices to prove one of the equalities. We shall prove the second one.

We have that

$$\begin{aligned}
|g(\chi,\psi)|^2 &= g(\chi,\psi)g(\overline{\chi},\overline{\psi}) \\
&= \sum_{x\in R/I}\chi(x)\psi(x)\sum_{y\in R/I}\overline{\chi}(y)\overline{\psi}(y) \\
&= \sum_{x,y\in R/I}\chi(x)\overline{\chi}(y)\psi(x-y) \\
&= \sum_{x,y\in R/I}\chi(x)\overline{\chi}(xy)\psi(x-(xy)) \\
&= \sum_{x,y\in R/I}\overline{\chi}(y)\psi(x(1-y)) \\
&= \sum_{x,y\neq 1\in R/I}\overline{\chi}(y)\psi(x(1-y))+\sum_{x\in R/I}\overline{\chi}(1) \\
&= \sum_{x,y\neq 1\in R/I}\overline{\chi}(y)\psi(x(1-y))+\mathrm{Nm}(I).
\end{aligned} \tag{3.18}$$

Finally notice that the following sum vanishes

$$\sum_{x,y\neq 1\in R/I}\overline{\chi}(y)\psi(x(1-y)) = \sum_{y\neq 1\in R/I}\overline{\chi}(y)\left(\sum_{x\in R/I}\psi(x(1-y))\right),$$

since ψ is not trivial and therefore $\sum_{x\in R/I}\psi(x(1-y))=0$. This proves our proposition.

■

Chapter 4

The Hasse-Weil L-Function

In this chapter we study two number theoretic functions which encode information about varieties via their reduction to finite fields.

Zeta functions are defined as a sort of generating function for the number of points in an algebraic variety over the finite extensions of a finite field $\mathbb{F}_q$. The Hasse-Weil L-function is defined as the inverse product of all the zeta functions over the extensions of the reduction of the variety modulo p, with p prime.

Such functions have given rise to many conjectures, some of them have been already proved and some of them are still waiting for a proof.

For instance, zeta functions were studied by André Weil, he stated his famous Weil Conjectures which would be proved some years later.

Nevertheless, the main conjecture in the frame of this work is the one made by Birch and Swinnerton-Dyer which relates the number of points in an elliptic curve defined over the rationals and the behavior of the L-function of the elliptic curve at one.

We compute the zeta function of the elliptic curve $E_n : y^2 = x^3 - n^2x$ for all primes p in a long example and we enunciate a theorem due to Coates and Wiles which could be seen as a weak proof of one side of the Birch and Swinnerton-Dyer conjecture.

4.1 Zeta Functions

A *zeta function* is a function whose logaritmic derivative is a generating function for the number of points of an algebraic variety V over the extensions of a finite field $\mathbb{F}_q$. In other words, given an algebraic variety V and a prime power q, we define a local zeta function with parameter T as

$$Z(V(\mathbb{F}_q);T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right), \tag{4.1}$$

where N_r is the number of points of $V(\mathbb{F}_{q^r})$.

Now we prove a couple of lemmas which will be useful to investigate zeta functions.

Lemma. *Suppose that* $N_r = \beta_1^r + ... + \beta_t^r - \alpha_1^r - ... - \alpha_s^r$ *for a fixed set* $\alpha_1, ..., \alpha_s, \beta_1, ..., \beta_t$, *then*

$$Z(T) = \frac{(1-\alpha_1 T)\cdots(1-\alpha_s T)}{(1-\beta_1 T)\cdots(1-\beta_t T)}.$$

Proof.

$$\begin{aligned} Z(T) &= \exp\left(\sum_{r=1}^{\infty}(\beta_1^r + ... + \beta_t^r - \alpha_1^r - ... - \alpha_s^r)\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty}\frac{(\beta_1 T)^r}{r} + ... + \frac{(\beta_t T)^r}{r} - \frac{(\alpha_1 T)^r}{r} - ... - \frac{(\alpha_s T)^r}{r}\right), \end{aligned}$$

the Taylor development of $\log(1-x)$ is

$$\log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - ...;$$

then substituting we have

$$\begin{aligned} Z(T) &= \exp\left(-\log(1-\beta_1 T) - ... - \log(1-\beta_t T) + \log(1-\alpha_1 T) + ... + \log(1-\alpha_s T)\right), \\ &= \frac{(1-\alpha_1 T)\cdots(1-\alpha_s T)}{(1-\beta_1 T)\cdots(1-\beta_t T)}. \end{aligned}$$

■

Lemma. *Suppose that $N_r < cA^r$ for c and A constants, then the power series $Z(T)$ converges in the open disc of radius $1/A$ in the complex plane.*

Proof.
$$\left|\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right| \leq \sum_{r=1}^{\infty} N_r \frac{|T|^r}{r} < c\sum_{r=1}^{\infty} \frac{(A|T|)^r}{r},$$
where the last sum converges to $-c\log(1-A|T|)$ if $|T| < 1/A$.

■

In the next example we compute the zeta function for the $m-$dimensional affine and projective space over the extensions of $\mathbb{F}_q$.

Example 14. Let $\mathbb{A}_K^m$ denote the $m-$dimensional affine space over the field K and $\mathbb{P}_K^m$ the projective space over the field K. We have
$$\begin{aligned} Z(\mathbb{A}^m_{\mathbb{F}_q}(\mathbb{F}_q);T) &= \exp\left(\sum_{r=1}^{\infty} (q^r)^m \frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty} \frac{(q^m T)^r}{r}\right) \\ &= \frac{1}{(1-q^m T)}. \end{aligned}$$

Similarly for the projective space we get
$$\begin{aligned} Z(\mathbb{P}^m_{\mathbb{F}_q}(\mathbb{F}_q);T) &= \exp\left(\sum_{r=1}^{\infty} \frac{(q^r)^{m+1}-1}{q-1}\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty} \left((q^r)^m + (q^r)^{m-1} + ... + (q^r)^2 + 1\right)\frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty} \left((q^m)^r + (q^{m-1})^r + ... + (q^2)^r + 1\right)\frac{T^r}{r}\right) \\ &= \frac{1}{(1-T)(1-qT)\cdots(1-q^m T)}. \end{aligned}$$

★

Zeta functions gave rise to Weil Conjectures. They say that zeta functions for an algebraic variety over finite field extensions of a finite field should

be rational functions, should satisfy a form of functional equation, and should have their zeros in restricted places. These conjectures were proved by Dwork (1960), Grothendieck (1965) and Deligne (1974). Next we state them in the case of smooth projective curves.

Theorem 20. *Let V be a smooth projective curve, then*

1. *The zeta function of V over the finite extensions of $\mathbb{F}_q$ have the form*

$$Z(V(\mathbb{F}_q);T) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) \in \mathbb{Z}[T]$ have constant term 1, and if V is the reduction modulo p of $\tilde{V}(\mathbb{Q})$ then $deg(P) = 2g$, where g is the genus of $\tilde{V}(\mathbb{C})$.

2. *If α is a reciprocal root of $P(T)$ so is $\frac{q}{\alpha}$. Thus if $deg(P) = 2g$ then*

$$P(T) = (1-\alpha_1 T)\left(1-\frac{q}{\alpha_1}T\right)\cdots(1-\alpha_g T)\left(1-\frac{q}{\alpha_g}T\right);$$

moreover all reciprocal roots of P have norm $\sqrt{q}$.

In particular, the zeta function of any elliptic curve E defined over $\mathbb{F}_q$ has the form

$$Z(E(\mathbb{F}_q);T) = \frac{1-2a_E T+qT^2}{(1-T)(1-qT)},$$

where the integer a_E depends on E.

In the next example, we compute the zeta function of the elliptic curve $E_n \subset \mathbb{P}^2_{\mathbb{F}_p}$, for every p prime.

Example 15. Let $E_n : y^2 = x^3 - n^2x$ with n a square free integer, and let $\mathbb{F}_p$ the finite field with p elements.

(i) First suppose that $p|2n$. Then the curve reduction becomes simply

$$y^2 = x^3.$$

If 2 and 3 (the powers of the equation) divide $p^r - 1$ we use Theorem 18 and get

$$N = p^r + \sum_{i=1,2} \chi_{1/2}(1)\chi_{i/3}(-1)J_0(1/2, i/3),$$

but $\frac{1}{2}+\frac{i}{3} \notin \mathbb{Z}$ for $i=1,2$. Then by property 3 of the Proposition 1 we have $J_0(1/2, i/3) = 0$ for $i = 1, 2$. Therefore $N = p^r$.

Now if 2 or 3 do not divide $p^r - 1$, there are p^r points again, corresponding to the solutions of the linear variety $u - v = 0$.

Once counted the affine points, it remains to count how many points there are in the whole projective space, but the projective completition of E_n when $p|2n$ is $zy^2 = x^3$, thus there is only one missing point $(0, 1, 0)$.

Then if p divides $2n$, we conclude that

$$\begin{aligned} Z(E(\mathbb{F}_p); T) &= \exp\left(\sum_{r=1}^{\infty}(1+p^r)\frac{T^r}{r}\right) \\ &= \frac{1}{(1-T)(1-pT)}. \end{aligned} \tag{4.2}$$

(ii) Suppose that $p \nmid 2n$. We construct a one-to-one correspondence between the elliptic curves E_n and $\tilde{E}_n : u^2 = v^4 + 4n^2$, the correspondence is

$$\begin{aligned} E_n &\rightarrow \tilde{E}_n, \\ (x, y) &\mapsto (2x - \frac{y^2}{x^2}, \frac{y}{x}); \end{aligned}$$

and

$$\begin{aligned} \tilde{E}_n &\rightarrow E_n, \\ (u, v) &\mapsto (\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)); \end{aligned}$$

the correspondence maps affine nonzero points in E_n to affine points in $\tilde{E}_n$.

Then the points of $\tilde{E}_n$ are the points in E_n minus 2, i.e. the point at infinity $(0, 1, 0)$ and $(0, 0)$.

The advantage of computing the points of $\tilde{E}_n$ instead of E_n, is that the equation $\tilde{E}_n$ is in the form of equation (3.7) and we can apply the

Theorem 18.

We have already done this in Example 13 for prime powers q congruent to 1 or 3 modulo 4, moreover for $q \equiv 3 \mod 4$ we have done it twice (see Example 12).

Therefore we have two cases, $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$.

Before computing the number of points for each kind of prime, we prove the next proposition.

Proposition 5. *Let* $q \equiv 1 \mod 4$. *Then*

$$1 + J(1/2, 1/4) \equiv 0 \mod 2 + 2i,$$

in the ring of the Gaussian integers $\mathbb{Z}[i]$.

Proof. First notice that

$$J(1/2, 1/4) = \chi_{1/2}(-1) J(1/4, 1/4),$$

by properties 2, 3 and 4 of Proposition 2. We rewrite the Jacobi sum in the right side as follows

$$\begin{aligned} J(1/4,1/4) &= \sum_{u+v=1} \chi_{1/4}(u)\chi_{1/4}(v) \\ &= \sum_{u\neq 0,1} \chi_{1/4}(u)\chi_{1/4}(1-u) \\ &= \chi_{1/4}\left(\frac{p+1}{2}\right)\chi_{1/4}\left(\frac{p+1}{2}\right) + \sum_{u\neq 1,0,\frac{p+1}{2}} \chi_{1/4}(u)\chi_{1/4}(1-u) \\ &= \chi_{1/4}^2\left(\frac{p+1}{2}\right) + 2\sum_{\substack{\{u,1-u\} \\ u\neq 0,\frac{p+1}{2}}} \chi_{1/4}(u)\chi_{1/4}(1-u). \end{aligned}$$

We have $\chi_{1/4}(x) \equiv 1 \mod (1+i)$ since $\chi_{1/4}(x)$ is a power of i, then

$2\chi_{1/4}(u)\chi_{1/4}(1-u) \equiv 2 \mod (2+2i)$, which implies that

$$\begin{aligned} J(1/4,1/4) &= \chi_{1/4}^2\left(\frac{p+1}{2}\right) + 2\sum_{\substack{\{u,1-u\}\\ u\neq 0,\frac{p+1}{2}}} \chi_{1/4}(u)\chi_{1/4}(1-u) \\ &\equiv \chi_{1/4}^2\left(\frac{p+1}{2}\right) + q - 3 \\ &\equiv 2 + \chi_{1/4}(4) \mod (2+2i), \end{aligned}$$

since $q-3 \equiv \pm 2 \mod (4)$ and $2+2i|4$. Having this on mind, we deduce that

$$\begin{aligned} 1 + J(1/2,1/4) &= 1 + \chi_{1/4}(-1)J(1/4,1/4) \\ &\equiv 1 + \chi_{1/4}(-1)(2+\chi_{1/4}(4)) \\ &\equiv 1 + 2\chi_{1/4}(-1) + \chi_{1/4}(-4) \\ &= 2 + 2\chi_{1/4}(-1) \mod (2+2i), \end{aligned}$$

where $\chi_{1/4}(-4) = 1$ by quadratic reciprocity. Then the last equation $2(1+\chi_{1/4}(-1))$ is either 0 or 4, both being multiples of $2+2i$. Therefore $1 + J(1/2,1/4) \equiv 0 \mod (2+2i)$.

■

1. Suppose $p \equiv 1 \mod 4$. Then $p^r \equiv 1 \mod 4$ for every $r \geq 1$.

   By Example 13, we have that $|\tilde{E}_n(\mathbb{F}_p)| = p - 1 - \mu_{n,p} - \overline{\mu}_{n,p}$ where $\mu_{n,p} = \mu_n = -\chi_{1/2}(n)J(1/2,1/4)$. Then

   $$N_1 = |E_n(\mathbb{F}_p)| = p + 1 - \mu_{n,p} - \overline{\mu}_{n,p}.$$

   Using a multiplicative character $\chi_{\alpha,r} = \chi_\alpha \circ \mathrm{Nm}$ of $\mathbb{F}_{p^r}$ we compute N_r for $r \geq 2$, we get

   $$N_r = |E_n(\mathbb{F}_{p^r})| = p^r + 1 - \mu_{n,p^r} - \overline{\mu}_{n,p^r},$$

   where

   $$\mu_{n,p^r} = -\chi_{1/2,r}(n)\frac{g(\chi_{1/2,r})g(\chi_{1/4,r})}{g(\chi_{3/4,r})},$$

notice that $\chi_{1/2,r}(n) = \chi_{1/2}(\mathrm{Nm}(n)) = \chi^r_{1/2}(n)$ and by Theorem 19 we have that

$$\begin{aligned}\mu_{n,p^r} &= (-1)^r \chi^r_{1/2}(n) \frac{g(\chi_{1/2})^r g(\chi_{1/4})^r}{g(\chi_{3/4})^r} \\ &= \mu^r_{n,p}.\end{aligned}$$

Therefore

$$N_r = |E_n(\mathbb{F}_{p^r})| = p^r + 1 - \mu^r_{n,p} - \overline{\mu}^r_{n,p};$$

finally from Lemma 4.1 we have that the zeta function when $p \equiv 1 \mod 4$ is

$$Z(E_n(\mathbb{F}_p); T) = \frac{(1-\mu_n T)(1-\overline{\mu_n} T)}{(1-T)(1-pT)}. \tag{4.3}$$

Now we determine the nature of the gaussian integer $\mu = a + ib$. Since Jacobi sums can be written in terms of gauss sums by property 4 of Proposition 2, we have that $|\mu|^2 = a^2 + b^2 = p$, this yields eight possibilities to μ, i.e. $\pm a \pm ib$ and $\pm b \pm ia$. From the Proposition 5 we have that

$$1+J(1/2,1/4) \equiv 0 \mod (2+2i) \Leftrightarrow 1 \equiv -J(1/2,1/4) \mod (2+2i)$$

$$\Leftrightarrow \chi_{1/2}(n) \equiv -\chi_{1/2}(n) J(1/2,1/4) \mod (2+2i),$$

where $\mu_n = -\chi_{1/2}(n) J(1/2,1/4)$, taking in count that $\chi_{1/2}(n)$ is simply the Dirichlet character $\left(\frac{n}{p}\right)$, we conclude that μ is a gaussian integer of norm $\sqrt{p}$ congruent to $\left(\frac{n}{p}\right)$ modulo $2+2i$.

2. Suppose $p \equiv 3 \mod 4$. In this case we have $p^{2r+2} \equiv 1 \mod 4$ and $p^{2r+1} \equiv 3 \mod 4$ for $r \geq 0$.

   In Example 12 we have seen that

   $$N_{2r+1} = p^{2r+1} + 1,$$

   for $r \geq 0$.

   As seen in the Example 13, explicitly for $\mathbb{F}_{p^2}$ we have

   $$N_2 = |E_n(\mathbb{F}_{p^2})| = |\tilde{E}_n(\mathbb{F}_{p^2})| + 2 = p^2 + 1 - \mu_{n,p^2} - \overline{\mu}_{n,p^2},$$

we can see that $\chi_{1/2}(n) = 1$ since $n \in \mathbb{F}_p$ and any polynomial $x^2 - a \in \mathbb{F}_p[x]$ has a root in $\mathbb{F}_{p^2}$. μ is a gaussian integer of norm p, there are four possibilities $\pm p$ or $\pm ip$, but by Proposition 5 we have

$$1 \equiv \mu \mod (2+2i) \Leftrightarrow 1 + i^k p \equiv 0 \mod (2+2i),$$

for some k satisfying $1 \leq k \leq 4$. It is easy to check that k can not be 1 or 3, then it remains to verify 2 and 4, but $p \equiv 3 \mod (4)$, this implies that $k = 4$. Therefore $\mu = -p$.

Finally we apply the Theorem 19 to

$$N_{2r+2} = |E_n(\mathbb{F}_{p^{2r+2}})| = p^{2r+2} + 1 - \mu_{n,p^{2r+2}} - \overline{\mu}_{n,p^{2r+2}},$$

for $r \geq 1$. We get

$$\begin{aligned} N_{2r+2} &= \left(p^2\right)^{r+1} + 1 - \mu_{n,(p^2)^{r+1}} - \overline{\mu}_{n,(p^2)^{r+1}} \\ &= \left(p^2\right)^{r+1} + 1 - \mu_{n,p^2}^{r+1} - \overline{\mu}_{n,p^2}^{r+1} \\ &= p^{2r+2} + 1 - (-p)^{r+1} - (-p)^{r+1}. \end{aligned}$$

We have for any $r \geq 1$

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r.$$

Finally from Lemma 4.1 we have that the zeta function when $p \equiv 3 \mod 4$ is

$$Z(E_n(\mathbb{F}_p); T) = \frac{(1 - i\sqrt{p}T)(1 + i\sqrt{p}T)}{(1-T)(1-pT)}. \tag{4.4}$$

★

4.2 The Hasse-Weil L-function

Let E be an elliptic curve, we will define a function which incorporates all the numbers of solutions of E over every finite extension $\mathbb{F}_{p^r}$ for almost[1]

[1]The word almost comes from the fact that the reduction modulo p of a curve could let to a singular curve.

every prime p.

The Theorem 20 establishes that the zeta function of an elliptic curve over $\mathbb{F}_p$, with p a good[2] prime, has the form

$$Z(E(\mathbb{F}_p);T) = \frac{1 - 2a_{E,p}T + pT^2}{(1-T)(1-pT)},$$

where the integer $a_{E,p}$ depends on E and p. Now, if we replace $T = p^{-s}$ where s is a complex variable, we have

$$Z(E(\mathbb{F}_p);p^{-s}) = \frac{1 - 2a_{E,p}p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}.$$

We define the Hasse-Weil L-function $L(E,s)$ as

$$L(E,s) = \frac{\zeta(s)\zeta(1-s)}{\prod\limits_{p \text{ prime}} Z(E(\mathbb{F}_p);p^{-s})}, \tag{4.5}$$

where

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

is the Riemann ζ-function. If

$$(1-p^{-s})(1-p^{1-s})Z(E(\mathbb{F}_p);p^{-s}) = 1$$

when the reduction modulo p is singular, we can simplify the function (4.5) obtaining

$$L(E,s) = \prod_{p \text{ prime}} \frac{1}{1 - 2a_{E,p}p^{-s} + p^{1-2s}}. \tag{4.6}$$

For every elliptic curve E the meromorphic function $L(E,s)$ is well defined on the right half plane $\mathrm{Re}(s) > \frac{3}{2}$, in some cases as we will see in the next chapter, it can be extended to the whole complex plane.

The value at $s = 1$ (even when it does not make sense to speak about it) is called the critical value, since the L functions of some curves satisfy a functional equation relating $L(E,s)$ to $L(E,2-s)$, i.e. the point $s = 1$ is the center of the functional equation.

Moreover L functions gave rise to a famous conjecture called the *Birch and Swinnerton-Dyer Conjecture* (usually denoted BSD Conjecture) which shows the importance of the critical value.

[2]We suppose that $E(\mathbb{F}_p)$ is a nonsingular projective curve.

Conjecture 1. *Let E be an elliptic curve defined over $\mathbb{Q}$.*

The order of the zero of $L(E, s)$ at $s = 1$ equals the rank of $E(\mathbb{Q})$.

A complex elliptic curve E is said to have *complex multiplication* if there is an automorphism of its lattice given by multiplication by some complex numbers others than integers.

It turns out that curves with complex multiplication behave well because their L functions can be extended to the whole complex plane and Coates and Wiles were able to make an advance in proving the BSD conjecture.

Theorem 21. *Let E be an elliptic curve defined over $\mathbb{Q}$ having complex multiplication. If E has infinitely many $\mathbb{Q}$-points, then $L(E, 1) = 0$.*

The scope of the proof goes beyond our investigation for the moment, since it is a rather difficult result to prove.

Chapter 5

Application

In this chapter we apply the tools studied trough all this work towards a solution to the ancient problem of the Congruent Number.

Some of the results were already showed as examples mainly through chapters 2, 3 and 4.

This is a very nice classical example, which illustrates the power of some of the most sophisticated tools developed in modern mathematics.

We start this chapter giving a couple of characterizations of the Congruent Number Problem which lead us to an elliptic curve. According to Mordell, the elliptic curve seen as a group over the rationals can be decomposed in its free part and its torsion part (see Theorem 16). It turns out that a $\mathbb{Q}$-point of infinite order on such a curve implies the existence of a congruent number. In fact, we show that the torsion subgroup of the curve consists of the points of order 2 only.

Therefore our main task will be to compute wether the curve has free part or not. For this we consider the reduction of the curve modulo every prime p and then count the number of points in the reductions and over all their finite extensions, this is made using mainly Weil's Theorem (18) and the Hasse-Davenport Relation (19).

Then we use this information and construct the zeta functions for the elliptic curve over the finite extensions of a finite field. We will give two equivalent forms of the zeta function, one considering a prime p in $\mathbb{Z}$ and the other one considered as a product of the prime ideals P in the ring $\mathbb{Z}[i]$ which divide the ideal generated by p, i.e. (p).

Finally we construct the Hasse-Weil L-function for this curve, we show some of its properties and we also give two equivalent forms to express it.

We state the so called weak Birch Swinnerton-Dyer conjecture and relate it to the Congruent Number Problem.

5.1 The Congruent Number Problem

Consider the next problem:

Given a fixed natural number n determine wether or not n is the area of some right triangle all of whose sides are rational numbers.

If there exists such a triangle we call n a *congruent number*. In other words, n is a congruent number if the two equations

$$\begin{aligned} X^2 + Y^2 &= Z^2 \\ XY &= 2n, \end{aligned}$$

have a simultaneous solution $X, Y, Z \in \mathbb{Q}$.

For example, 6 and 30 are congruent numbers since they are the areas of right triangles generated by the Pythagorean triples $(3, 4, 5)$ and $(5, 12, 13)$ respectively. Every Pythagorean triple gives rise to a congruent number. All the Pythagorean triples (X,Y,Z) can be generated by the relations

$$X = a^2 - b^2,\ Y = 2ab,\ Z = a^2 + b^2,\ \text{with } a > b \in \mathbb{N},$$

and therefore congruent numbers coming from Pythagorean triples are of the form

$$(a^2 - b^2)ab. \tag{5.1}$$

This gives us an idea of which kind of congruent numbers could come from right triangles generated by Pythagorean triples. For instance, at a first glance we do not know if a prime p could be a congruent number using (5.1) even if there exists a simple algorithm using Pythagorean triples that will eventually list all congruent numbers (of course not in increasing order).

It has been proved by Fermat that 1 is not a congruent number, neither 2, 3 and 4, but 5, 6, 7 are. 6 is the smallest congruent number coming from a Pythagorean triple, while 5 is the smallest congruent number since the right

triangle with sides $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$ has area 5; Euler was the first to show that 7 is a congruent number.

Our first step on trying to give a criterion is to reduce the set of search. Suppose that n is a congruent number for $(X, Y, Z) \in \mathbb{Q}^3$, then $k^2 n$ is a congruent number for $(kX, kY, kZ) \in \mathbb{Q}^3$ and $k \in \mathbb{Z}$. Therefore, from now on when speaking of congruent numbers, we shall always assume that the number is a square free positive integer.

We derive an alternate condition for n to be a congruent number. If $(X, Y, Z) \in \mathbb{Q}^3$ is a triple corresponding to a right triangle with hypotenuse Z, we fix an order of such triples requiring that $X < Y < Z$. The next proposition is due to the Arab scholars of the tenth century.

Proposition 6. *The maps*

$$\begin{aligned} (X, Y, Z) &\to \left(\left(\frac{X-Y}{2} \right)^2, \left(\frac{Z}{2} \right)^2, \left(\frac{X+Y}{2} \right)^2 \right) \\ (x-n, x, x+n) &\to \left(\sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x} \right) \end{aligned} \tag{5.2}$$

give rise to a one-to-one correspondence between rational triples of solutions (X, Y, Z) to (5.1) and triples of rational numbers $(x-n, x, x+n)$ all of their entries being the squares of rational numbers.

Thus, n is a congruent number if and only if there exists x such that x, $x-n$ and $x+n$ are squares of rational numbers.

Proof. Let n be a natural number. First suppose that (X, Y, Z) is a rational triple which solves

$$X^2 + Y^2 = Z^2$$

$$XY = 2n,$$

then $\pm 2XY = \pm 4n$, if we complete the quadratic binomials we have

$$\left(\frac{X \pm Y}{2} \right)^2 = \left(\frac{Z}{2} \right)^2 \pm n,$$

letting $x = \left(\frac{Z}{2} \right)^2$ we have that x, $x-n$ and $x+n$ are squares of rational numbers.

Now suppose that x, $x-n$ and $x+n$ are squares of rational numbers and let

$$X = \sqrt{x+n} - \sqrt{x-n},\ Y = \sqrt{x+n} + \sqrt{x-n} \text{ and } Z = 2\sqrt{x},$$

we have $X^2 + Y^2 = Z^2$ and $XY = 2n$.

Finally, let x and n be fixed, then Z is fixed as well since $Z = 2\sqrt{x}$. The equations

$$X^2 + Y^2 = 4x^2 \text{ and } XY = 2n,$$

are satisfied by the points $(\pm X, \pm Y)$ and $(\pm Y, \pm X)$, thus the triple (X, Y, Z) is the same in the four cases.

■

It is time to put our problem in the language we developed through all this work, that is, we will find another characterization of congruent numbers in terms of an elliptic curve.

The system of equations (5.1) is equivalent to the system of the completed squares

$$\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n,$$

multiplying both equations we get

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2,$$

if we replace $\left(\frac{Z}{2}\right)$ by u and $\left(\frac{X^2-Y^2}{4}\right)$ by v we get

$$v^2 = u^4 - n^2,$$

multiplying both sides by u^2, we get

$$(uv)^2 = u^6 - n^2u^2,$$

finally we make $x = u^2$ and $y = uv$

$$E_n :\ y^2 = x^3 - n^2x. \tag{5.3}$$

That is, given a right triangle with rational sides X, Y, Z and area n we obtain a point (x, y) having rational coordinates and lying on (5.3).

The next question to solve is wether a point (x, y) with rational coordinates which satisty (5.3) come from such a triangle. We answer this question with the following result.

Proposition 7. *Let (x, y) be a point with rational coordinates on the curve (5.3). If x is the square of a rational number and its denominator is even. Then there exists a right triangle with rational sides and area n.*

Proof. Let $x \in (\mathbb{Q}^+)^2$ and $u = \frac{r}{t} \in \mathbb{Q}^+$ with $\gcd(r, t) = 1$ and $r, t \in \mathbb{Z}$, such that $x = u^2 = \frac{r^2}{t^2}$. t is an even integer since t^2 is even by hyphotesis.

Now let $y = uv$ then $v^2 = \frac{y^2}{u^2} = \frac{x^3 - n^2 x}{x} = x^2 - n^2$, that is

$$x^2 = v^2 + n^2.$$

From the latter equation we deduce that $t^4 v^2 \in \mathbb{Z}$ since $n \in \mathbb{Z}$. Thus

$$t^4 x^2 = t^4 v^2 + t^4 n^2,$$

which implies that $(t^2 v, t^2 n, t^2 x)$ is a primitive Pythagorean triple, for we have that $t^2 v$ and $t^2 x$ are both odd integers and $t^2 n$ is an even integer. Therefore, there exist integers a and b such that

$$t^2 v = a^2 - b^2, \ t^2 n = 2ab, \text{ and } t^2 x = a^2 + b^2.$$

We obtain that $n = \frac{2ab}{t^2}$, making $X = \frac{2a}{t}$ and $Y = \frac{2b}{t}$ we get

$$X^2 + Y^2 = 4\frac{a^2 + b^2}{t^2} = 4x = 4u^2,$$

so $Z = 2u$. Then the right triangle with sides

$$X = \frac{2a}{t}, \ Y = \frac{2b}{t} \text{ and } Z = 2u,$$

has area n.

The image of the triangle under the correspondence in the Proposition 6 is $x = \left(\frac{Z}{2}\right)^2 = u^2$.

■

The Chapter 2 starts with the definition of an elliptic curve. According to Example 9 the cubic equation E_n (5.3) defines an elliptic curve over any

field K of characteristic p as long as $p \nmid 2n$. Then it make sens to talk about the addition of its points. It turns out that another chacarterization of the congruent numbers is obtained by means of the elliptic curve defined by E_n.

Consider the points $P = (x, y)$ not of order 2 with x and y rational, then the $x-$coordinate of the point $2P$ is a square in $\mathbb{Q}$ with even denominator, thus it gives rise to a congruent number n by Proposition 7.

For let $P = (x, y)$ be a point not of order 2 with rational coordinates on the curve E_n. By Theorem 14 the $x-$coordinate of $2P$ is given by

$$\left(\frac{x^2 + n^2}{2y}\right)^2,$$

clearly it belongs to $(\mathbb{Q}^+)^2$.

It remains to prove that the denominator of this $x-$coordinate is even. For this we define for every nonzero rational number r the function

$$\mathrm{Ord}_2 : \mathbb{Q}^* \to \mathbb{Z},$$

$$r \mapsto k;$$

where k is such that $r = 2^k s$ with $s \in \mathbb{Q}$ having both odd numerator and denominator, i.e. k is the exponent of the greatest power of 2 that factors r.

It follows that $\mathrm{Ord}_2(r_1 \pm r_2) = \min\{\mathrm{Ord}_2(r_1), \mathrm{Ord}_2(r_2)\}$, $\mathrm{Ord}_2(r_1 r_2) = \mathrm{Ord}_2(r_1) + \mathrm{Ord}_2(r_2)$ and that $\mathrm{Ord}_2(r_1/r_2) = \mathrm{Ord}_2(r_1) - \mathrm{Ord}_2(r_2)$.

Then we have

$$\begin{aligned}
\mathrm{Ord}_2\left(\left(\frac{x^2 + n^2}{2y}\right)^2\right) &= 2\mathrm{Ord}_2(x^2 + n^2) - \mathrm{Ord}_2(4y^2) \\
&= 2\min\{\mathrm{Ord}_2(x^2), \mathrm{Ord}_2(n^2)\} - 2 - \mathrm{Ord}_2(y^2) \\
&= \min\{\mathrm{Ord}_2(x^2), \mathrm{Ord}_2(n^2)\} - 2 - \mathrm{Ord}_2(x) \\
&= 2\min\{\mathrm{Ord}_2(x), \mathrm{Ord}_2(n)\} - 2 - \mathrm{Ord}_2(x),
\end{aligned}$$

notice that

$$\mathrm{Ord}_2(n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even,} \end{cases}$$

since n is square free. Consider the following three cases

1. Suppose $\mathrm{Ord}_2(x) = \mathrm{Ord}_2(n)$, then

$$\mathrm{Ord}_2\left(\left(\frac{x^2 + n^2}{2y}\right)^2\right) = \mathrm{Ord}_2(x) - 2 < 0.$$

2. Suppose $\mathrm{Ord}_2(x) > \mathrm{Ord}_2(n)$, then

$$\mathrm{Ord}_2\left(\left(\frac{x^2+n^2}{2y}\right)^2\right) = 2\mathrm{Ord}_2(n) - 2 - \mathrm{Ord}_2(x) < 2\mathrm{Ord}_2(n) - 3 < 0.$$

3. Finally suppose $\mathrm{Ord}_2(x) < \mathrm{Ord}_2(n)$, then

$$\mathrm{Ord}_2\left(\left(\frac{x^2+n^2}{2y}\right)^2\right) = \mathrm{Ord}_2(x) - 2 < \mathrm{Ord}_2(n) - 2 < 0.$$

This proves our assertion about the $x-$coordinates of the rational points not of order 2 in E_n.

According to the Theorem 16 of Chapter 2, the $\mathbb{Q}-$points of our special curve E_n form a finitely generated abelian group: $E_n(\mathbb{Q}) \simeq E_n(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^r$ where $r \geq 0$. It turns out that

$$E_n(\mathbb{Q})_{\mathrm{tors}} = \{(0,0), (\pm n, 0), 0_\infty\},$$

where 0_∞ is the point at infinity (which acts as zero in the addition of points in the curve). We prove this in the next proposition.

Proposition 8. $|E_n(\mathbb{Q})_{tors}| = 4$.

Proof. Let $P_1 = (x, y, z) \in E_{n(\mathbb{Q})} \subset \mathbb{P}^2_{\mathbb{Q}}$, without lose of generality we may assume that x, y, z are integeres with no common factor.
Consider the reduction map

$$\varphi : E_n(\mathbb{Q}) \ \rightarrow \ E_n(\mathbb{F}_p);$$

$$P_1 = (x, y, z) \in \mathbb{P}^2_{\mathbb{Q}} \mapsto \bar{P}_1 = (\bar{x}, \bar{y}, \bar{z}),$$

where the bar denotes reduction modulo p.
For two $\mathbb{Q}$-points P_1 and P_2 in E_n we have

$$\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2),$$

since algebraically the reduction modulo p of the addition formula in Theorem 14 concides with the addition of the $\mathbb{F}_p$-points defined by the same formula.

The map φ is thus a group homomorphism. We want to prove that it

is injective for most p.

Let P_1 and P_2 be considered as vectors in $\mathbb{R}^3$, then $\varphi(P_1) = \varphi(P_2)$ if and only if $\varphi(P_1 \times P_2) = 0$, i.e. the reduction modulo p of its cross product is zero.

First suppose that $\varphi(P_1) = \varphi(P_2)$, with out loss of generality suppose that $p \nmid x_1$, automatically $p \nmid x_2$, then

$$\varphi(P_1) = \bar{x}_2\bar{P}_1 = \bar{x}_1\bar{P}_2 = \varphi(P_2),$$

where the equality in the middle can be written as follows

$$\begin{aligned} x_2x_1 - x_1x_2 &\equiv 0 \mod p \\ x_2y_1 - x_1y_2 &\equiv 0 \mod p \\ x_2z_1 - x_1z_2 &\equiv 0 \mod p, \end{aligned}$$

that is $p|x_2z_1 - x_1z_2$ and $p|x_1y_2 - x_2y_1$ it remains to prove that $p|y_1z_2 - y_2z_1$.

If p divides both y_1 and z_1 it is over. With out loss of generality suppose that $p \nmid y_1$, then $p \nmid y_2$, then

$$\varphi(P_1) = \bar{y}_2\bar{P}_1 = \bar{y}_1\bar{P}_2 = \varphi(P_2),$$

and in the same fashion as before we write

$$\begin{aligned} y_2x_1 - y_1x_2 &\equiv 0 \mod p \\ y_2y_1 - y_1y_2 &\equiv 0 \mod p \\ y_2z_1 - y_1z_2 &\equiv 0 \mod p, \end{aligned}$$

therefore $p|y_1z_2 - y_2z_1$.

We conclude that $p|P_1 \times P_2$ and therefore $\varphi(P_1 \times P_2) = 0$.

Conversely, $\varphi(P_1 \times P_2) = 0$ if and only if p divides the entries of

$$(y_1z_2 - y_2z_1, z_1x_2 - x_1z_2, x_1y_2 - y_1x_2).$$

Suppose that $p|x_1$, then $p|x_2$ since p must divide $z_1x_2 - y_1x_2$ and we established that the entries of P_1 has no common factor. Then

$$\begin{aligned} \varphi(P_1) &= (0, \bar{y}_1, \bar{z}_1) \\ &= (0, \bar{y}_1\bar{y}_2, \bar{z}_1\bar{y}_2) \\ &= (0, \bar{y}_1\bar{y}_2, \bar{y}_1\bar{z}_2) \\ &= (\bar{y}_1\bar{x}_2, \bar{y}_1\bar{y}_2, \bar{y}_1\bar{z}_2) \\ &= \varphi(P_2). \end{aligned}$$

Now if $p \nmid x_1$ then $p|z_2$ and $p \nmid x_2$, therefore $\varphi(P_1) = \bar{x}_2\bar{P}_1 = \bar{x}_1\bar{P}_2 = \varphi(P_2)$.

Now suppose that $E_n(\mathbb{Q})$ has a subgroup of odd order or even order greater than 2. Let $H = \{P_1, P_2, ..., P_m\} \subset E_n(\mathbb{Q})_{\text{tors}}$ be such a subgroup. The points $P_i \in E_n(\mathbb{Q}) \subset \mathbb{P}^2_{\mathbb{Q}}$ are all distinct as vectors in $\mathbb{R}^3$ for $i = 1, .., m$; then the cross product $P_i \times P_j$ is nonzero for all $i \neq j$.

Let

$$d_{i,j} = \gcd(y_i z_j - y_j z_i, z_i x_j - x_i z_j, x_i y_j - y_i x_j),$$

then if $p|d_{i,j}$ we have that $\varphi(P_i) = \varphi(P_j)$. Then if $p \nmid 2n$ and $p \geq n_{i,j}$ for all $1 \leq i < j \leq m$, then $p \nmid d_{i,j}$, i.e. the map φ gives an injection from H to $E_n(\mathbb{F}_p)$. This implies that the order of $\varphi(H)$ which is the order of H divides the order of $E_n(\mathbb{F}_p)$.

Suppose that p is a prime with $p \equiv 3 \mod 4$. Then by Example 12 we have $p + 1$ points in $E_n(\mathbb{F}_p)$, then $|H| = m$ divides $p + 1$ or equivalently $p \equiv -1 \mod m$. But we have that if $\gcd(a, m) = 1$ for a, m positive integers, by Dirichlet's theorem on arithmetic progressions there are infinitely many primes p of the form $p \equiv a \mod m$, then there are infinitely many primes p such that $m \nmid p + 1$. Then there is not a subgroup of $E_n(\mathbb{Q})$ of odd order or even order greater than 2.

■

Then our elliptic curve $E_n(\mathbb{Q})$ over the rationals decomposes in four points which are the only points of finite order (the points of order two) and a free part which could not exist.

Proposition 9. *Let n be a square free integer. n is a congruent number if and only if $E_n(\mathbb{Q})$ has positive rank.*

Proof. If n is a congruent number, then there exists a $\mathbb{Q}$-point not of order two in $E_n(\mathbb{Q})$, by Mordell Theorem and Proposition 8 this point must have infinite order, that is $r \geq 1$.
Conversely if $E_n(\mathbb{Q})$ has positive rank, then there exists a point $P \in E_n(\mathbb{Q})$ of infinite order and the $x-$coordinate of $2P$ is the square of a rational number with even denominator.

■

Now, our main task abording the congruent number problem becomes in determine wether the group of $\mathbb{Q}$ points of an elliptic curve E_n for a fixed squarefree integer n has positive rank in its group decomposition.

To do this first we give the zeta function of E_n over the finite extensions of $\mathbb{F}_p$ for every prime p.

The following theorem is a direct consequence of the Example 15.

Theorem 22. *Let E_n be the elliptic curve given by $y^2 = x^3 - n^2x$ defined over $\mathbb{F}_p$, where $p \nmid 2n$. Then*

$$Z(E_n(\mathbb{F}_p); T) = \frac{1 - 2a_{E_n,p}T + pT^2}{(1-T)(1-pT)} = \frac{(1-\mu_p T)(1-\overline{\mu_p}T)}{(1-T)(1-pT)},$$

where $a = Re(\mu_p)$; $\mu_p = i\sqrt{p}$ if $p \equiv 3 \mod 4$; and if $p \equiv 1 \mod 4$, then μ_p is an element of $\mathbb{Z}[i]$ of norm $\sqrt{p}$ which is congruent to $\left(\frac{n}{p}\right)$ modulo $2 + 2i$. Moreover, if $p|2n$ then the zeta function is simply

$$Z(E_n(\mathbb{F}_p); T) = \frac{1}{(1-T)(1-pT)}.$$

We can express the zeta function of E_n as product of prime ideals of the Gaussian integers.

Let $\mathbb{Z}[i]$ be the ring of the Gaussian integers. There are two types of prime ideals, namely the ideals P generated by a prime congruent to 3 modulo 4; and the ideals P generated by a gaussian integer of norm $\sqrt{p}$, with p prime congruent to 1 modulo 4. That is, if a prime number $p \equiv 3 \mod (4)$ there is a unique prime ideal containing p and if $p \equiv 1 \mod (4)$ there are two prime ideals $P = (a + ib)$ and $\bar{P} = (a - ib)$ where $a^2 + b^2 = p$. Now if $p = 2$ then there is only one ideal containing 2, i.e. the ideal $P = (1 + i)$, for which $P^2 = (2)$.

We define the degree of a prime ideal P dividing the ideal (p) as the degree of the field extension $\mathbb{Z}[i]/P$ of $\mathbb{F}_p$, hence

$$\deg(P) = \begin{cases} 1 & \text{if } P|(p) \text{ for } p \equiv 1 \mod (4), \\ 2 & \text{if } P = (p) \text{ for } p \equiv 3 \mod (4). \end{cases}$$

We can rephrase the Theorem 22 as follows.

Theorem 23.

$$(1-T)(1-pT)Z(E_n(\mathbb{F}_p); T) = \prod_{P|(p)} (1 - (\mu_P T)^{\deg P}),$$

where the product is over the prime ideals of $\mathbb{Z}[i]$ *dividing* (p)*, and where* $\mu_P = i\sqrt{p}$ *if* $P = (p)$*; and* $\mu_P = a+ib$ *if* $(p) = P\bar{P}$*, where* $a+ib$ *is the unique generator of* P *which is congruent to* $\left(\frac{n}{p}\right)$ *modulo* $2+2i$*.*
Moreover if $p|2n$*, we take* $\mu_P = 0$*, thus the product on the right equals one.*

Once we know how the zeta functions of E_n look like for every prime p (actually we have two maners to express them), we want to multiply those functions in order to find the $L(E_n, s)$ function.

Let s be a complex variable. We substitute the $T = p^{-s}$, then we have according to Theorem 22 and to Theorem 23 the next equalities

$$L(E_n, s) = \prod_{p\nmid 2n} \frac{1}{1 - 2a_{E_n,p}p^{-s} + p^{1-2s}}, \tag{5.4}$$

$$= \prod_{\substack{P|(p)\\ p\nmid 2n}} \frac{1}{1 - \mu_P^{\deg P}(\mathrm{Nm}(P))^{-s}}. \tag{5.5}$$

In the equality (5.5) the function $\mathrm{Nm}(P) = |\mathbb{Z}[i]/P|$ is the norm of an ideal in a ring, it simply count the different cosets of P.

We have that $\mathrm{Nm}(P) = p$ if P is a prime ideal generated by a gaussian integer of squared norm p congruent to 1 mod (4). And $\mathrm{Nm}(P) = p^2$ if $P = (p)$ for p prime congruent to 3 mod (4).

Notice that this agrees with the substitution made for the equality (5.5).

We now prove the convergence of the series product for $L(E_n, s)$.

Proposition 10. *The series product for* $L(E_n, s)$ *converges in the right half of the s-plane for* $Re(s) > \frac{3}{2}$*.*

Proof. We have

$$L(E_n, s) = \prod_{P\nmid(2n)} \frac{1}{1 - \mu_P^{\deg P}(\mathrm{Nm}(P))^{-s}},$$

the product converges if and only if

$$\sum_P |\mu_P|^{\deg P}(\mathrm{Nm}(P))^{-s}$$

converges.

Now if $P = (a + ib)$ we have $\mathrm{Nm}(P) = p$, $\deg P = 1$ and $|\mu_P| = \sqrt{p}$,

then $|\mu_P|^{\deg P} = \sqrt{p} = \mathrm{Nm}(P)^{1/2}$. Similarly, if $P = (p)$ then $\mathrm{Nm}(P) = p^2$, $\deg P = 2$ and $|\mu_P| = \sqrt{p}$, then $|\mu_P|^{\deg P} = p = \mathrm{Nm}(P)^{1/2}$. Therefore in both cases we have $|\mu_P|^{\deg P} = \mathrm{Nm}(P)^{1/2}$, this yields

$$\sum_P |\mu_P|^{\deg P}(\mathrm{Nm}(P))^{-s} = \sum_P (\mathrm{Nm}(P))^{\frac{1}{2}-s},$$

furthermore $(\mathrm{Nm}(P))^{\frac{1}{2}-s} \leq p^{\frac{1}{2}-s}$ for $s \geq \frac{1}{2}$, then since there are at most two prime ideals P for each prime p, we have the bound

$$\sum_P |\mu_P|^{\deg P}(\mathrm{Nm}(P))^{-s} \leq 2 \sum_{p \text{ prime}} \frac{1}{p^{s-\frac{1}{2}}},$$

where the sum in the right converges for $s - \frac{1}{2} > 1$, thus in the s-plane for $\mathrm{Re}(s) > \frac{3}{2}$.

■

In the next theorem we state some properties concerning the $L(E_n, s)$ function. Those properties will be useful for the main result concerning the Congruent Number Problem.

Theorem 24. *The Hasse-Weil L-function $L(E_n, s)$ for the elliptic curve $E_n : y^2 = x^3 - n^2x$, which for $Re(s) > \frac{3}{2}$ is defined by (5.4), extends analitically to an entire function on the whole complex s-plane. In addition, let*

$$N = \begin{cases} 32n^2, & n \text{ odd}; \\ 16n^2, & n \text{ even}. \end{cases} \tag{5.6}$$

Let

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right)\Gamma(s)L(E_n, s), \tag{5.7}$$

where $\Gamma(s)$ is the usual Gamma function defined by

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt.$$

Then $L(E_n, s)$ satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(2 - s), \tag{5.8}$$

where the sign is plus if $n \equiv 1, 2, 3 \mod (8)$ and is minus if $n \equiv 5, 6, 7 \mod (8)$.

We will not prove the former theorem, since some of the contents go beyond the purpose of this work. Nevertheless we make some remarks involving the theorem.

Since the function $L(E_n, s)$ extends analytically to the whole complex plane, it make sense to speak about the behavior of the L-function at the critical value $s = 1$.

The curve E_n has complex multiplication because of its lattice, which is a multiple of the lattice of the gaussian integers $\mathbb{Z}[i]$, some of the preceding results are possible thanks to this fact.

The complex multiplication of E_n and the analitical continuation of the function $L(E_n, s)$ allow us to compute the critical value of $L(E_n, s)$ for some n, proving in some cases that $L(E_n, 1) \neq 0$, thus by Theorem 21, E_n has only finitely many points $\mathbb{Q}$-points.

The functional equation satisfied by the function $L(E_n, s)$ is of the same style as the functional equation for the Riemann ζ-function, that is, if

$$\Lambda_\zeta(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

then

$$\Lambda_\zeta(s) = \Lambda_\zeta(1 - s).$$

Both functions have certain symmetry with respect to vertical stripes in the complex plane.

The next conjecture is commonly called the weak Birch Swinnerton-Dyer conjecture, since it does not assert nothing about the order of the zero of the L-function.

Conjecture 2. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $L(E, 1) = 0$ if and only if E has infinitely many rational points.*

The following proposition reveals an application for which a proof of the BSD conjecture will end in good hands.

Proposition 11. *If $n \equiv 5, 6$ or $7 \mod (8)$, and if the weak Birch Swinnerton-Dyer conjecture holds for E_n, then n is a congruent number.*

Proof. From Theorem 24 we have that if $n \equiv 5, 6$ or $7 \mod (8)$ then $\Lambda(s) = -\Lambda(2 - s)$, now if $s = 1$ we get

$$2\Lambda(1) = 2\left(\frac{\sqrt{N}}{2\pi}\right)L(E_n, s) = 0$$

since $\Gamma(1) = 1$. Since $\left(\frac{\sqrt{N}}{2\pi}\right) \neq 0$, it follows that $L(E_n, s) = 0$, then the weak Birch Swinnerton-Dyer conjecture tell us that E_n has infinitely many $\mathbb{Q}$-points, thus n is a congruent number.

■

Some advances have been made in trying to prove either the weak or the whole BSD conjecture. Until now, efforts have not been totally successful, but significant advances have been made using the Modularity Theorems and in general the Theory of Automorphic Forms, from which Modular Forms are examples.

In this fashion, Tunnell used the theorems of Shimura, Waldspurger and himself, to give a nice characterization of the Congruent Number Problem. The statement is

Theorem 25. *If n is a congruent number then the number of integer solutions of the first equation is twice the number of solution of the second equation, for one of the next systems of equations depending if n is odd or even.*

n odd

$$n = 2x^2 + y^2 + 32z^2,$$
$$n = 2x^2 + y^2 + 8z^2.$$

n even

$$\frac{n}{2} = 4x^2 + y^2 + 32z^2,$$
$$\frac{n}{2} = 4x^2 + y^2 + 8z^2.$$

Conversely, if the weak Birch Swinnerton-Dyer conjecture is true for the elliptic curves E_n, then these equations imply that n is a congruent number.

More recently B. H. Gross, D. Zagier and R. Greenberg have made advances towards the proof of the BSD conjecture. The first two of them showed it for a family of elliptic curves E_n, Greenberg showed that if the conjecture were to fail for an elliptic curve of the kind of E_n, then it would imply a very improbable result for elliptic curves.

Bibliography

[1] L. V. Ahlfors, *Complex Analysis*. McGraw-Hill, 1966.

[2] K. Chandrasekharan, *Elliptic Functions*. A series of Comprehensive Studies in Mathematics, Springer-Verlag, 1980.

[3] F. Diamond and J. Shurman, *A First Course in Modular Forms*. Graduate Texts in Mathematics, Springer, 2005.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford University Press, 1975.

[5] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics, Springer-Verlag, 1984.

[6] C. L. Siegel, *Topics in Complex Function Theory*. Wiley-Interscience, 1969.

[7] R. Miranda, *Algebraic Curves and Riemann Surfaces*. Graduate Studies in Mathematics, AMS, 1991.

[8] H.L. Montgomery, I. Niven, H.S. Zuckerman, *An Introduction to the Theory of Numbers Fifth Edition*. John Wiley & Sons, Inc; 1991.

[9] V. Prasolov and Y. Solovyev, *Elliptic Functions and Elliptic Integrals*. Translations of Mathematical Monographs AMS, 1991.

[10] A. Weil, *Number of solutions of equations in finite fields*. Bulletin 55 of the AMS, 497-508; 1949.