Università degli Studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Magistrale in Matematica

From the Pell's equation to Gross–Stark units

Relatore:
Prof. Marco Andrea Garuti

Laureanda: **Giuditta Bellosi**
Matricola: **1239287**

Anno Accademico 2020/2021

21 Luglio 2021

Introduction

This thesis is a mathematical journey from the Pell's equation to Gross–Stark units, centered around the theme of the relationship between leading terms of L-series, and algebraic units.

Our story begins with Pell's equation, and two methods to solve it. In particular, we will focus on the study the fundamental solution of a real quadratic number field k. Then we will move to a general abelian extension of number fields K/k by stating the Stark conjecture. To conclude we will discuss the p-adic analogue of the Stark conjecture, namely the Gross–Stark conjecture. We will state the conjecture for k a real quadratic number field and K its narrow Hilbert class field. We will define the Gross–Stark unit, and compute an explicit example.

In the first chapter, we will focus on the Pell's equation which is a diophantine equation of the form $x^2 = dy^2 + 1$ where d is positive integer. This equation is of great interest in the history of mathematics; one of the oldest examples is the *cattle problem* of Archimedes (287-212 B.C.). This equation mistakenly takes is name after the English mathematician John Pell (1611-1685), since Euler (1707-1783) attributed to him a solution method that had been found instead by the English mathematician William Brouncker (1620-1684) in response to a challenge by Fermat (1601-1665). The solution of this equation has been the subject of many studies. Finding the fundamental solution to Pell's equation comes down to finding the fundamental unit ε of norm 1 of the number ring $\mathbb{Z}[\sqrt{d}]$, by using Dirichlet's unit theorem. We will present the continued fraction method and Dirichlet's method using L-functions. The first method is based on the continued fraction expansion of $\sqrt{d}$. We will first define continued fractions and the associated N-convergent C_N and use it to solve some examples of Pell equations. From these examples we will also observe that the size of the fundamental unit is quite unpredictable. The second method was found by Dirichlet and involves special values of L-functions. Specifically, we will consider the L-function

$$L(t, \chi_D) = \sum_{n=1}^{\infty} \chi_D(n) n^{-t}$$

where $D > 0$ is the discriminant of $\mathbb{Q}[\sqrt{d}]$; which converges for $\Re(t) > 0$. We will see that the logarithm of the fundamental unit is closely related to the value of $L(1, \chi_D)$, which leads to the expression:

$$\varepsilon^{2h} = \prod_{m=1}^{D} (1 - e^{2i\pi m/D})^{\chi(m)}.$$

The continued fraction method is much more efficient in practice, while the approach via L-functions leads to the generalization found in the Stark and the Gross–Stark conjecture, which are the other two chapters of this thesis.

The second chapter will be focused on the rank one abelian Stark conjecture. In general the rank of the unit group can be arbitrarily large and the unit group is not easily reconstructed from the regulator. To remedy this, Stark refined the Dirichlet class number formula, by breaking up the unit group $\mathcal{O}_K^\times$ into 'pieces'. We will first present the Stark conjecture which says that if K/k is an abelian Galois extension and the partial zeta function $\zeta_{K,\mathcal{S}}(s, \sigma)$ vanishes to order 1 then there is a unit ε, the so-called "Stark unit", in K such that:

$$\zeta'_{K,\mathcal{S}}(0, \sigma) \sim \log |\sigma(\varepsilon)|_w.$$

This conjecture is also connected to Hilbert's twelfth problem. Hilbert asked for a systematic construction of algebraic numbers that generate all finite abelian extensions of k, where k is a general number field A.1 . We will define the objects which play a role in this conjecture, namely the partial zeta function $\zeta_{K,\mathcal{S}}$, the characteristics of the set $\mathcal{S}$ and the related L-function $L_S(s,\chi)$. To conclude, we will state the rank one abelian Stark conjecture both in the general case and in the case where K is the narrow Hilbert class field of k. We recall that the Stark conjecture has been proved only for $k = \mathbb{Q}$ and for k an imaginary quadratic field, and it is still an open problem in general. On the other hand, the p-adic counterpart, which is the Gross–Stark conjecture, was proved by Darmon, Dasgupta and Pollack in 2011.

The last chapter will be focused on the Gross–Stark conjecture. We will first recall some of the basics of p-adic analysis by defining continuous and analytic functions on $\mathbb{Z}_p$ and by recalling Hensel's lemma. We will focus then on the p-adic L-function associated to an odd character:

$$\chi : \mathfrak{Cl}_k^+ \longrightarrow \overline{\mathbb{Q}}_p^\times$$

where k is a real quadratic field. Deligne and Ribet proved the existence of a p-adic L-function $L_p(s,\chi)$ in $\mathbb{Z}_p[[s]]$, satisfying the interpolation property:

$$L_p(n,\chi) = (1-p^{-2n})L(n,\chi) \quad \forall n \in \mathbb{Z},\ n \leq 0 \text{ and } (p-1)|n.$$

We assume that $L(0,\chi) \neq 0$, hence $\operatorname{ord}_{s=0} L_p(s,\chi) = 1$. There are two different methods in order to compute the quantity $L_p'(s,\chi)$. The first method uses the approach of T. Shintani and was developed by Roblot. The second method uses the diagonal restriction of Hilbert Eisenstein series and it was developed by J.Vonk and A. Lauder. We will discuss this last one and we will compute some examples. Then we discuss the p-adic Gross–Stark conjecture, applied to the case where K is the narrow Hilbert class field of k, which predicts that

$$L_p'(0,\chi) \sim \log_p(u)$$

for a p-unit u in K. We will compute a concrete example.

Contents

Chapter 1

Two approaches to Pell's equation

In this chapter we introduce Pell's equation $x^2 = dy^2 + 1$ where d is a positive integer. We dedicate a section to a brief historical treatment since this equation has an incredibly rich history and it seems that it first appeared in poem of Archimedes (287-212 B.C.). We will show subsequently that finding a fundamental solution to the Pell's equation comes down to find a fundamental unit ε of norm 1 of the number ring $\mathbb{Z}[\sqrt{d}]$. After that, we will focus on two methods to find and compute the fundamental unit. The first method uses the continued fraction expansion of $\sqrt{d}$, and we will compute some examples. The second method is due to Dirichlet and it involves special values of L-functions. We will prove that given the L-function $L(t, \chi_D)$ where χ_D is the quadratic Dirichlet character associated to $\mathbb{Z}[\sqrt{d}]$ and h is its class number, we obtain the following relation with the logarithm of the fundamental unit: $\log(\varepsilon) = L(1, \chi_D)\sqrt{D}/2h$. Dirichlet computed the value of $L(1, \chi_D)$ and found that

$$\varepsilon^{2h} = \prod_{m=1}^{D} (1 - e^{2i\pi m/D})^{\chi(m)}.$$

We will end this section with a proof of this result. To conclude, we will observe that this method hinges on the fact that the rank of the unit group is equal to one, so that we can recover a fundamental unit from the regulator. This is not possible in general number fields. A conjectural refinement of Dirichlet's method will be the main aim of the second chapter.

1.1 Pell's equation

Definition 1.1. A *Pell's equation* is a diophantine equation of the form:

$$x^2 = dy^2 + 1$$

where d is a positive non-square integer and the solutions are taken to be two positive integers.

The case where d is a square may be excluded, since the only squares which differ by 1 are 0 and 1. We find that $d = 1, x^2 = 1$ and $y^2 = 0$, and so, the only possible solutions are $(x, y) = (\pm 1, 0)$.

Definition 1.2. A *negative Pell's equation* is a diophantine equation of the form:

$$x^2 = dy^2 - 1$$

where d is a positive non-square integer and the solutions are taken to be two positive integers.

1.1.1 History of Pell's equation

This equation is named after the English mathematician John Pell (1611-1685) since Euler (1707-1783) mistakenly attributed to him a solution method that had been found by the English mathematician, William Brouncker (1620-1684), in response to a challenge by Fermat (1601-1665).

The history of Pell's equation is very interesting. It seems that the method of Brouncker is very similar to a method that was known to Indian mathematicians at least six centuries earlier, while the existence of the equation was already known to Greek mathematicians, even if there is no evidence that they could solve it. A thorough discussion can be found in *"Number theory: an approach through history"* of A. Weil [AWe84] and an explanation of the method can be found in Euler's *Algebra* [Eul70]. The only certainty is that if there was a solution then the method would have found it, however, Euler took for granted that the method always found a solution. One of the earliest proofs of the method for every d was probably found by Fermat, and Lagrange was the first who published it in his paper [Gra73].

One of the oldest examples of Pell's equation is given by the *cattle problem* of Archimedes (287-212 B.C.). The famous Greek mathematician issued a challenge to the Alexandrian mathematicians, headed by Eratosthenes. The problem was written in elegiac distichs and may be summarised as follows:

"The sun god had a herd of cattle consisting of bulls and cows, one part of which was white, a second black, a third spotted, and a fourth brown. Among the bulls, the number of white ones was one half plus one third the number of the black greater than the brown; the number of the black, one quarter plus one fifth the number of the spotted greater than the brown; the number of the spotted, one sixth and one seventh the number of the white greater than the brown. Among the cows, the number of white ones was one third plus one quarter of the total black cattle; the number of the black, one quarter plus one fifth the total of the spotted cattle; the number of spotted, one fifth plus one sixth the total of the brown cattle; the number of the brown, one sixth plus one seventh the total of the white cattle. What was the composition of the herd?"

In addition, the last 14 lines of the poem impose the additional constraints that:

"[...]the white and black bulls together form a square and that the brown and spotted bulls together form a triangle."

We can observe that if we indicate with x, y, z, t the numbers of white, black, spotted, and brown bulls we obtain the following relations from the text.

$$x = \left(\frac{1}{2} + \frac{1}{3}\right) y + t, \quad y = \left(\frac{1}{4} + \frac{1}{5}\right) z + t \quad z = \left(\frac{1}{6} + \frac{1}{7}\right) x + t.$$

While if we indicate with x', y', z', t' the number of cows of the same respective colors, we obtain that:

$$x' = \left(\frac{1}{3} + \frac{1}{4}\right)(y + y'), \quad y' = \left(\frac{1}{4} + \frac{1}{5}\right)(z + z'), \quad z' = \left(\frac{1}{5} + \frac{1}{6}\right)(t + t'), \quad z' = \left(\frac{1}{6} + \frac{1}{7}\right)(x + x'),$$

In addition, $x + y$ must be a square and $z + t$ must be a triangular number. One the one hand the general solution of the equations of the bulls is given by:

$$(x, y, z, t) = m \cdot (2226; 1602; 1580; 891)$$

and the equations of the cows are solvable if and only if m is divisible by 4657. As a consequence, if we write $m = 4657 \cdot k$ we obtain that

$$(x', y', z', t') = k \cdot (7206360; 4893246; 3515820; 5439213).$$

What it is challenging now is to find a k s.t.

$$x + y = 4657 \cdot 3828 \cdot k$$

is a square and

$$z + t = 4657 \cdot 2471 \cdot k$$

is a triangular number. From the prime decomposition we obtain that

$$k = \alpha l^2,$$

where α, l are integers and $\alpha = 3{\cdot}11{\cdot}29{\cdot}4657$. From the triangular condition we obtain the following equation:

$$h^2 = 8(z+t)+1 = 8\cdot 4657\cdot 2471\cdot \alpha l^2 + 1$$

Observe that this is a Pell equation. Throughout the 19th century, many mathematicians attempted to obtain reasonable solutions. The first to solve the cattle problem satisfactorily was A. Amthor in 1880 [KA80] even if he didn't apply the continued fraction method that we will present in the next section. He showed that, in the smallest solution to the cattle problem, the total number of cattle is given by a number of 206545 digits. Written out in full, this huge number would occupy forty-seven pages of computer printout!

1.1.2 Initial properties

Let us consider the following Pell's equation with d non-square positive integer:

$$x^2 = dy^2 + 1.$$

We can rewrite the equation in the following way:

$$(x+\sqrt{d}y)(x-\sqrt{d}y) = 1.$$

We can observe that $x+\sqrt{d}y$ and $x-\sqrt{d}y$ are units of $\mathbb{Z}[\sqrt{d}]$. As a consequence, we can see that finding a solution of Pell's equation comes down to finding a non-trivial unit of the ring $\mathbb{Z}[\sqrt{d}]$ of norm one. This implies that once we have found a solution to Pell's equation we can actually find infinitely many solutions to it. If we write $x_1+\sqrt{d}y_1$ for the smallest possible solution (x_1,y_1) and call it the *fundamental solution* of Pell's equation, we obtain more solutions (x_n,y_n) by:

$$x_n+\sqrt{d}y_n = (x_1+\sqrt{d}y_1)^n.$$

Remark 1.1.1. This result could be seen as an application of *Dirichlet's unit theorem* A.2.2 if we set $K=\mathbb{Q}[\sqrt{d}]$. For a real quadratic field we have that $\mu_K = \pm 1$ and there are only two embedding σ_1,σ_2 of $\mathbb{Q}[\sqrt{d}]$ in $\mathbb{C}$ and they are both real:

$$\begin{aligned} id = \sigma_1 : \sqrt{d} &\longmapsto \sqrt{d}, \\ \sigma_2 : \sqrt{d} &\longmapsto -\sqrt{d}. \end{aligned}$$

Therefore $r=2, s=0$ and $r+s-1=1$. This means that:

$$\mathcal{O}_K^\times = \{\pm1\}\times\langle\varepsilon_k\rangle$$

We call ε_k the *fundamental unit of* K.

We will study step by step all the possible cases for d.

First of all, let us suppose that $d\equiv 2,3 \pmod 4$, $K=\mathbb{Q}[\sqrt{d}]$ and then $\mathcal{O}_K=\mathbb{Z}[\sqrt{d}]$. From *Dirichlet's unit theorem* A.2.2 applied to real quadratic case we have that there is, up to sign, a unique fundamental unit, which we indicate with ε_K, which generates the group of units of $\mathbb{Z}[\sqrt{d}]$. As a consequence, once we have found ε_K, we have found the fundamental solution of the associated Pell's equation. Moreover, since ε_K is the generator of the unit group, we can obtain all the other solutions by raising it to all positive powers.

Let us suppose now that $d\equiv 1 \pmod 4$, $K=\mathbb{Q}[\sqrt{d}]$ and then $\mathcal{O}_K=\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. There exists a unique fundamental unit ε_K but $\varepsilon_K\in\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and not $\mathbb{Z}[\sqrt{d}]$. This will lead us to some observations.

First of all, we have that:

$$\varepsilon_K = \frac{1}{2}x+\frac{\sqrt{d}}{2}y, \quad x,y\in\mathbb{Z}.$$

Since ε_k is a unit, it has to have unitary norm. This means:

$$\varepsilon_K\overline{\varepsilon_K} = (\frac{1}{2}x+\frac{\sqrt{d}}{2}y)(\frac{1}{2}x-\frac{\sqrt{d}}{2}y) = \frac{1}{4}(x^2-dy^2) = \pm1.$$

Which implies that:

$$x^2 - dy^2 = 4, \quad or \quad x^2 - dy^2 = -4$$

We can refer to the first equation by calling it the 4-Pell's equation and to the second by calling it the negative 4-Pell's equation.

Remark 1.1.2. We can observe that if we find a solution to a usual Pell's equation, we can always obtain a solution to the 4-Pell's equation by multiplying by 2 the two components of the first solution.

Let us $x, y \in \mathbb{Z}$ be such that $x + \sqrt{d}y$ is a solution of the Pell's equation:

$$x^2 + dy^2 = 1.$$

Then if we multiply both x, y by 2, we obtain:

$$(2x)^2 + d(2y)^2 = 4x^2 + 4dy^2 = 4(x^2 + dy^2) = 4,$$

therefore, $2x + 2\sqrt{d}y$ is a solution of the 4-Pell equation.

On the other hand, the converse is not true, since the components of ε_K may be half-integers. Firstly, we define $R := \mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{d+\sqrt{d}}{2}]$. In this case, in order to find the integer solutions to the Pell's equation, we have to raise ε_K to the minimal integer power j such that $\varepsilon_K^j \in \mathbb{Z}[\sqrt{d}]$.

We can see that $\varepsilon_R := \varepsilon_K^j$ is a unit since it is a power of a unit; it belongs to $\mathbb{Z}[\sqrt{d}]$ by construction and it is the smallest possible unit since we have taken the smallest power of ε_K. As a consequence, ε_R is the fundamental unit of $\mathbb{Z}[\sqrt{d}]$.

Example 1.1. Let us consider the case where $d = 5$. We have $K = \mathbb{Q}[\sqrt{5}]$ and $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

First of all, we can observe that $\alpha := \frac{1+\sqrt{5}}{2}$ is a unit, since:

$$\alpha\overline{\alpha} = \frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = -1.$$

Observe that the component of α: $x = 1, y = 1$, they satisfy the *Negative* 4*-Pell's equation*:

$$(1 + \sqrt{5})(1 - \sqrt{5}) = -4.$$

However, $\alpha \notin R := \mathbb{Z}[\sqrt{5}]$. To find the solutions of the *Negative Pell's equation* we raise α to the minimal power such that it will belongs to $\mathbb{Z}[\sqrt{5}]$.

$$\alpha^2 = \frac{1}{2}(3 + \sqrt{5}) \notin \mathbb{Z}[\sqrt{5}]$$
$$\alpha^3 = 2 + \sqrt{5} \in \mathbb{Z}[\sqrt{d}].$$

Therefore, the components of $\alpha^3 = 2 + \sqrt{5}$ are solutions of the Negative Pell's equation. As a matter of facts:

$$2^2 - 5 \cdot 1 = 4 - 5 = -1.$$

Now we want to find the fundamental unit of $\mathcal{O}_K^\times$. With a method that we will describe later, we will obtain that:

$$\varepsilon_K = \frac{3}{2} + \frac{1}{2}\sqrt{5}.$$

On one hand, we can observe that the components of ε_K, $x = 3, y = 1$ satisfy the 4-Pell's equation:

$$x^2 - 5y^2 = 9 - 5 = 4.$$

On the other hand, in order to find the fundamental unit of R, we raise ε_K to powers until we find an element of R. We can see that:

$$\varepsilon_K^2 = \frac{1}{2}(7 + 3\sqrt{5}) \notin \mathbb{Z}[\sqrt{5}]$$
$$\varepsilon_K^3 = 9 + 4\sqrt{5} \in \mathbb{Z}[\sqrt{5}].$$

As a consequence, we have found that $\varepsilon_R = \varepsilon_K^3$ is the fundamental unit of the group of units of $\mathbb{Z}[\sqrt{5}]$.

The last case that we have to study is when d is not squarefree. In this case, we can write

$$d = f^2 d',$$

where d' is square free. Hence if x, y solve the Pell's equation for d, then $x, f \cdot y$ solve the Pell's equation for d' and $x + fy\sqrt{d'}$ will be equal for some n to the n-th solution x'_n, y'_n of the Pell's equation for d':

$$x + fy\sqrt{d'} = (x'_1 + y'_1\sqrt{d'})^n.$$

Therefore, in order to find the fundamental solution to the Pell's equation for d, we have to compute two steps. First of all, we have to solve the Pell's equation for d', then we have to find the least value of n for which y'_n is divisible by f. The n-th power of the fundamental solution of the Pell's equation for d' is the fundamental solution of the Pell's equation for d, and we can find infinitely many solutions by raising it to the powers.

Example 1.2. Let us consider the case where $d = 45$. We can write $d = 3^2 \cdot 5$. First of all, we solve the Pell's equation for 5. We already know that the fundamental solution of this equation is $9 + 4\sqrt{5}$. Since, $3 \nmid 4$, we have to find the least value of n such that y'_n is divisible by 3.
We compute:

$$(9 + 4\sqrt{4})^2 = 161 + 72\sqrt{5},$$

and observe that $3 \mid 72$. As a consequence, we find the least value of n, and we have that $161+72\sqrt{5}$ is the fundamental solution of the Pell's equation for $d = 45$.

Ultimately, in this section, we have seen an important result namely once we find the fundamental unit of norm 1 of the ring of integer $\mathbb{Z}[\sqrt{d}]$ we have found the fundamental solution to the Pell's equation for d and we can obtain infinitely many other solutions of it by raising the fundamental solution to powers.

1.2 Continued fraction method

In this section, we will introduce the continued fraction expression and the associated method to solve the Pell's equation. We will show that, given a certain d, which refers to the Pell's equation $x^2 = dy^2 + 1$, we can obtain important information by looking at the continued fraction expression of $\sqrt{d}$. As a matter of fact, if the period length of its continued fraction expression is even, we will truncate the continued fraction at the end of the first period. We will calculate the N-convergent C_N and $C_N = \frac{x_1}{y_1}$ where x_1 and y_1 are such that $x_1 + \sqrt{d}y_1$ is the fundamental unit. On the other hand, if the period length of the continued fraction expression of $\sqrt{d}$ is odd, we will truncate the continued fraction at the end of the second period. We will calculate the $2N$-convergent C_{2N} and $C_{2N} = \frac{x_1}{y_1}$. To conclude, we will compute some examples.

1.2.1 Continued fraction expression

A *continued fraction* is an expression obtained through an iterative process of representing a number as the sum of its integer part and the reciprocal of another number, then writing this other number as the sum of its integer part and another reciprocal, and so on.

Definition 1.3 (Continued fraction expansion)**.** An expression of the form:

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \cfrac{b_3}{\cdots}}}}.$$

is said to be a *continued fraction.* The values of $a_1, a_2, a_3, \ldots$ and $b_1, b_2, b_3, \ldots$ can be either real or complex values. There can be either an infinite or a finite number of terms.

A continued fraction can be created from any number n by using the following recursive algorithm:

$$a_i = \lfloor n_i \rfloor$$
$$n_i = \frac{1}{n_i - a_i}.$$

where $n_0 = n$. The sequence of a_i's are the terms of the continued fraction.

The continued fraction expressions which we will use are called *simple continued fractions.*

Definition 1.4 (Simple continued fraction)**.** A *simple continued fraction* is a continued fraction in which the value of $b_n = 1$ for all n.

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\cdots}}}}.$$

The value of a_n is a positive integer for all $n \geq 1$, while a_0 can be any integer value, including 0. We will represent the fraction in this way:

$$[a_0; a_1, a_2, a_3, \dots].$$

The *terms* of a simple continued fraction refer to the values of $a_i, i \geq 0$ and we can also call them *partial quotients*. For example, a_4 is the *fifth* term, since we are starting from a_0.

Definition 1.5 (Finite and infinite simple continued fraction)**.** A *finite simple continued fraction* is a simple continued fraction with only a finite number of terms. An *infinite simple continued fraction* is a simple continued fraction with an infinite number of terms.

Definition 1.6 (k-Convergent)**.** The continued fraction $[a_0; a_1, a_2, \dots, a_{k-1}]$ where k is a non-negative integer less than or equal to n is called the k-th convergent of the continued fraction $[a_0; a_1, a_2, \dots, a_n]$. The k-th convergent is denoted by C_k.

Example 1.3. Given the continued fraction:

$$1 + \frac{1}{2 + \frac{1}{3}}.$$

We can write it as: $[1; 2, 3]$.
Then:

$$C_1 = 1;$$
$$C_2 = 1 + \frac{1}{2} = \frac{3}{2}$$
$$C_3 = 1 + \frac{1}{\frac{7}{3}} = 1 + \frac{3}{7} = \frac{10}{7}.$$

Definition 1.7 (Periodic continued fraction)**.** The infinite simple continued fraction $[a_0; a_1, a_2, \dots]$ is said to be *periodic* if there is a positive integer N such that $a_n = a_{n+N}$ for all sufficiently large n. We represent this continued fraction in this way:

$$[a_0; (a_1, a_2, \dots, a_N)^*].$$

We say that this continued fraction has *period length* equal to N.

Proposition 1.2.1. *We have the following properties:*

1. *The continued fraction representation for a rational number is finite and only rational numbers have finite representations.*

2. *The continued fraction representation of an irrational number is unique.*

1.2.2 Resolution of Pell's equation

In this section, we will show how to use the continued fraction expression to solve Pell's equation for a given d.

Let us suppose that the period length N of the continued fraction expression of $\sqrt{d}$ is even. In this case, we truncate the continued fraction expression of $\sqrt{d}$ at the end of the first period. Then we calculate the corresponding convergent C_N. The numerator of C_N is x_1 while the denominator of C_N is y_1. Hence we have found the fundamental solution of the Pell's equation for d.

Example 1.4. Let us consider $d = 14$. The continued fraction expansion of $\sqrt{14}$ is $[3;(1,2,1,6)^*]$. The period is $(1,2,1,6)$ and has length 4, which is even. We compute C_4 which is the computation of $[3;1,2,1]$:

$$3 + \cfrac{1}{1 + \frac{1}{2+\frac{1}{\frac{1}{1}}}} = \frac{15}{4}.$$

Therefore, the fundamental solution of Pell's equation for $d = 14$ is $15 + 4\sqrt{14}$.

Example 1.5. Let us consider $d = 28$. The continued fraction expansion of $\sqrt{28}$ is $[5;(3,2,3,10)^*]$. The period is $(3,2,3,10)$ and has length 4, which is even. We compute C_4 which is the computation of $[5;3,2,3]$:

$$5 + \cfrac{1}{3 + \frac{1}{2+\frac{1}{\frac{3}{1}}}} = \frac{127}{24}.$$

Therefore, the fundamental solution of Pell's equation for $d = 28$ is $127 + 24\sqrt{28} = 127 + 48\sqrt{28}$.

Example 1.6. Let us consider $d = 71$. The continued fraction expansion of $\sqrt{71}$ is $[8;(2,2,1,7,1,2,2,16)^*]$. The period is $(2,2,1,7,1,2,2,16)$ and has length 8, which is even. We compute C_8 which is the computation of $[8;2,2,1,7,1,2,2]$:

$$8 + \cfrac{1}{2 + \frac{1}{2+\frac{1}{1+\frac{1}{7+\frac{1}{1+\frac{1}{2+\frac{1}{\frac{2}{1}}}}}}}} = \frac{3480}{413}.$$

Therefore, the fundamental solution of Pell's equation for $d = 71$ is $3480 + 413\sqrt{71}$.

Let us suppose now that the period length N is odd. In this case, we truncate the continued fraction expression of $\sqrt{d}$ at the end of the second period. Then we calculate the correspondent convergent C_{2N}. The numerator of C_{2N} is x_1 while the denominator of C_{2N} is y_1. Hence we have found the fundamental solution of the Pell's equation for d.

Example 1.7. Let us consider $d = 5$. The continued fraction expansion of $\sqrt{5}$ is $[2;(4)^*]$. The period is (4) and has length 1, which is odd. We compute C_2 which is the computation of $[2;4]$:

$$2 + \frac{1}{\frac{4}{1}} = \frac{9}{4}.$$

Therefore, the fundamental solution of the Pell's equation for 5 is $9+4\sqrt{5}$. This is the same solution that we have obtained in the Example 1.1.

Example 1.8. Let us consider $d = 13$. The continued fraction expansion of $\sqrt{13}$ is $[3;(1,1,1,1,6)^*]$. The period is $(1,1,1,1,6)$ and has length 5, which is odd. We compute C_{10} which is the computation of $[3;1,1,1,1,6,1,1,1,1]$:

$$3 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{6+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}}}}}} = \frac{649}{180}.$$

Therefore, the fundamental solution of the Pell's equation for 13 is $649 + 180\sqrt{13}$.

Example 1.9. Let us consider $d = 313$. The continued fraction expansion of $\sqrt{313}$ is

$$[17; (1, 2, 4, 11, 1, 1, 3, 2, 2, 3, 1, 1, 11, 4, 2, 1, 34)^*].$$

The period is $(1, 2, 4, 11, 1, 1, 3, 2, 2, 3, 1, 1, 11, 4, 2, 1, 34)$ and has length 17, which is odd. We compute C_{34} and we obtain:

$$\frac{32188120829134849}{1819380158564160}.$$

Therefore, the fundamental solution of the Pell's equation for 313 is:

$$32188120829134849 + 1819380158564160\sqrt{313}.$$

Remark 1.2.2. Observe that the size of the fundamental unit is quite unpredictable. We can see, indeed, that the fundamental unit of the Pell's equation for $d = 14$ which is $15 + 4\sqrt{14}$ is much smaller than the fundamental unit of the Pell's equation for $d = 13$ which is $649 + 180\sqrt{13}$.

To conclude in this section we have shown the first method which we can use in order to solve the Pell's equation. This method uses basic concepts of algebraic number theory and it is the most common and efficient method used so far to compute solutions of the Pell's equation. We will see another method, which will involve more analytic number theory, in the next section.

1.3 Dirichlet's method using L-functions

A different method was discovered by Dirichlet, and involves special values of L-functions. Specifically, we will consider the L-function

$$L(t, \chi_D) = \sum_{n=1}^{\infty} \chi_D(n) n^{-t}$$

which converges for $\Re(t) > 0$. As we will see, $\log(\varepsilon_K)$ is very closely related to $L(1, \chi_D)$, so that the fundamental unit ε_K may be recovered by exponentiation. Dirichlet furthermore made this special value explicit, which leads to the expression

$$\varepsilon_K^{2h} = \prod_{m=1}^{D} (1 - e^{2i\pi m/D})^{\chi(m)},$$

in terms of so-called *circular units*. We observe that this method is less efficient in practice than the continued fraction method, but it lends itself more easily to generalization, as we will explore in our discussion of the Stark and Gross–Stark conjectures.

1.3.1 The class number formula

As before, we let K be a number field. We define its Dedekind zeta function by

$$\zeta_K(t) = \sum_{I \neq 0} \mathrm{Norm}(I)^{-t} \qquad \text{where } \Re(t) > 1,$$

where the sum ranges over non-zero integral ideals I in $\mathcal{O}_K$. For quadratic number fields K, the Dedekind zeta function relates to the Dirichlet L-function of the quadratic character χ_D according to the following theorem.

Theorem 1.3.1. *Let $K/\mathbb{Q}$ be a quadratic number field, then*

$$\zeta_K(t) = \zeta(t) \cdot L(t, \chi_D), \tag{1.1}$$

where $\zeta(t)$ is the Riemann zeta function, and χ_D is the quadratic Dirichlet character of conductor D, the discriminant of K.

In order to prove this theorem, we make a study of prime decomposition in $\mathcal{O}_K$. The basics are reviewed in Appendix A.3. We begin by determining how many ideals have norm equal to a given prime p. Note that the value $\chi_D(p)$ depends on the behaviour of the ideal (p) in the ring of integers $\mathcal{O}_K$:

$$\chi_D(p) = \begin{cases} 0, & \text{if } p \text{ is ramified} \\ 1, & \text{if } p \text{ split} \\ -1. & \text{if } p \text{ is inert} \end{cases} \tag{1.2}$$

Any ideal of $\mathcal{O}_K$ of norm p is a prime above p. We observe that if p is inert in K then there are no ideals $\mathfrak{q}$ in $\mathcal{O}_K$ which have norm p, since $p\mathcal{O}_K$ is prime also in $\mathcal{O}_K$, hence it has norm p^2. If p splits in K, we have two ideals in $\mathcal{O}_K$ of norm p, and these are the two prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ that lie over p. Finally, if p is ramified in K, we have just one ideal of $\mathcal{O}_K$ which has norm p since $\mathrm{Norm}(\mathfrak{p}^2) = \mathrm{Norm}(p) = p^2$. In summary, we proved the following proposition:

Proposition 1.3.2. *The number of ideals of $\mathcal{O}_K$ of norm p, with p prime, is given by:*

$$\#\{\mathfrak{q} \lhd \mathcal{O}_K | \ \mathrm{Norm}(\mathfrak{q}) = p\} = 1 + \chi_D(p), \tag{1.3}$$

In order to prove Theorem 1.3.1, observe that

$$\begin{aligned} \zeta_K(t) &= \sum_{I \neq 0} \mathrm{Norm}(I)^{-t} && (1.4) \\ &= \prod_{\mathfrak{p} \ prime \ in \ K} (1 - \mathrm{Norm}(\mathfrak{p})^{-t})^{-1} = && (1.5) \\ &= \prod_{p \ prime \ in \ \mathbb{Q}} \left(\prod_{\substack{\mathfrak{p} \ prime \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} (1 - \mathrm{Norm}(\mathfrak{p})^{-t})^{-1} \right) && (1.6) \end{aligned}$$

On the other hand,

$$\begin{aligned} \zeta(t) L(t, \chi_D) &= \prod_{p \ prime \ in \ \mathbb{Q}} (1 - p^{-t})^{-1} (1 - \chi_D(p) p^{-t})^{-1} = && (1.7) \\ &= \prod_{p \ prime \ in \ \mathbb{Q}} (1 - (1 + \chi_D(p)) p^{-t} + \chi_D(p) p^{-2t})^{-1}. && (1.8) \end{aligned}$$

To prove the identity (1.1), it now suffices to prove that for each prime p, the corresponding factors in (1.6) and (1.8) are equal, which can be checked case by case:

1. Suppose first that p is inert, then its corresponding factor in (1.6) is equal to $(1 - p^{2t})^{-1}$. On the other hand, using (1.2), we have that $\chi_D(p) = -1$ and the factor in (1.8) is equal to:

$$(1 - (1 + \chi_D(p)) p^{-t} + \chi_D(p) p^{-2t})^{-1} = (1 - (1 - 1) p^{-t} - 1 p^{-2t})^{-1} = (1 - p^{-2t})^{-1}.$$

2. When p is split, its factor in (1.6) is equal to $(1 - p^{-t})^{-1}(1 - p^{-t})^{-1}$. On the other hand, we have that $\chi_D(p) = 1$ and the factor in (1.8) is equal to:

$$\begin{aligned} (1 - (1 + \chi_D(p)) p^{-t} + \chi_D(p) p^{-2t})^{-1} &= (1 - (1 + 1) p^{-t} + 1 p^{-2t})^{-1} \\ &= (1 - 2p^{-t} + p^{-2t})^{-1} \\ &= (1 - p^{-t})^{-1} (1 - p^{-t})^{-1}. \end{aligned}$$

3. Finally, when p is ramified, it factor in (1.6) is equal to $(1 - p^{-t})^{-1}$. On the other hand, we have that $\chi_D(p) = 0$ and (1.8) is equal to:

$$(1 - (1 + \chi_D(p)) p^{-t} + \chi_D(p) p^{-2t})^{-1} = (1 - (1 + 0) p^{-t} + 0 \cdot p^{-2t})^{-1} = (1 - p^{-t})^{-1}.$$

The Dedekind zeta function of a number field K encodes several arithmetic invariants of K in its residue at $t = 1$, as described by the *Class number formula*:

$$\mathrm{res}_{t=1} \zeta_K(t) = \frac{2^r (2\pi)^s h_K R_K}{w_K \sqrt{D}}. \tag{1.9}$$

When $K = \mathbb{Q}[\sqrt{d}]$ is a real quadratic field, we have $r + s - 1 = 1$ and the regulator is:

$$R_K = \det(\log|\sigma_j(\varepsilon_i)|)_{1\le i,j\le 1} = \det(\log|\sigma_1(\varepsilon_1)|) = \log(\varepsilon_K),$$

where ε_K is a fundamental unit of $\mathcal{O}_K^\times$. In addition, the number w_K of roots of unity in K is equal to 2, since the roots of unity in $\mathbb{Q}[\sqrt{d}]$ are $\{\pm 1\}$. Therefore (1.9) simplifies to:

$$\operatorname{res}_{t=1}\zeta_K(t) = \frac{2h_K\log(\varepsilon_K)}{\sqrt{D}}. \tag{1.10}$$

We apply the identity (1.1) and we obtain:

$$\lim_{t\to 1}(t-1)(\zeta(t)L(t,\chi_D)) = \frac{2h_K\log(\varepsilon_K)}{\sqrt{D}} \tag{1.11}$$

Since the Riemann zeta function has a simple pole with residue 1 at $t = 1$ by (1.9), and the function $L(t,\chi_D)$ is analytic $t = 1$, we obtain

$$L(1,\chi_D) = \frac{2h_K\log(\varepsilon_K)}{\sqrt{D}}. \tag{1.12}$$

Hence:

$$\log(\varepsilon_K) = \frac{L(1,\chi_D)\sqrt{D}}{2h_K}. \tag{1.13}$$

Therefore, we can recover ε_K by exponentiating the right hand side. As a consequence, we can find the fundamental solution of the Pell's equation for d.

1.3.2 The functional equation for ζ_K

Alternatively, we may use the functional equation for ζ_K to obtain a similar analytic method for computing a fundamental unit, using instead the first derivative of ζ_K at $t = 0$. This leads to simpler expressions, and paves the way for the formulation of the Stark and Gross–Stark conjectures, discussed in subsequent chapters.

The Dedekind zeta function satisfies the following functional equation:

Theorem 1.3.3. *Let K be a number field of degree n with r real and $2s$ complex embeddings. Then ζ_K can be extended to a holomorphic function on $\mathbb{C}\setminus\{1\}$. The completed zeta function:*

$$Z_K(t) = \sqrt{|D_K|}^{\,t}(\Gamma(t/2)\pi^{-t/2})^r(\Gamma(t)(2\pi)^{-t})^s\zeta_K(t). \tag{1.14}$$

satisfies the functional equation $Z_K(t) = Z_K(1-t)$, where

$$\Gamma(t) = \int_0^\infty x^{t-1}e^{-x}dx. \tag{1.15}$$

We observe that we can rewrite the class number formula in terms of the behaviour of $\zeta_K(t)$ at $t = 0$ by applying the functional equation. We obtain that $\operatorname{ord}_{t=0}\zeta_K(t) = r + s - 1$ and

$$\lim_{t\to 0} t^{-(r+s-1)}\zeta_K(t) = -\frac{h_K R_K}{w_K}, \tag{1.16}$$

For real quadratic fields K, we have $\operatorname{ord}_{t=0}\zeta_K(t) = 1$ and the equation (1.16) becomes:

$$\begin{aligned}
\zeta_K'(0) &= \zeta'(0)L(0,\chi_D) + \zeta(0)L'(0,\chi_D)\\
&= -\frac{1}{2}L'(0,\chi_D)\\
&= -\frac{h_K\log(\varepsilon_K)}{2}.
\end{aligned}$$

Therefore, we can obtain the fundamental unit ε_K by exponentiating the quantity $L'(0,\chi_D)/h_K$.

1.3.3 Circular units method

We can make (1.13) more explicit, since the value of $L(1,\chi_D)$ can be made explicit. Dirichlet, in his paper *"Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires"* [Dir80], obtained the following identity.

$$\varepsilon_K^{2h} = \prod_{m=1}^{D} (1 - e^{2i\pi m/D})^{\chi_D(m)}. \tag{1.17}$$

Remark 1.3.4. The expressions on the right hand side of (1.17) are the simplest examples of *circular units*. These in general give rise to a systematic collection of units in abelian extensions of $\mathbb{Q}$ and are of fundamental importance in the classical theory of cyclotomic fields.

The primitive D-th root of unity $e^{2i\pi/D}$ will henceforth be denoted by $\zeta_D := e^{2i\pi/D}$. We will now describe the Dirichlet character in (1.17) more precisely. We recall the definition of the *Kronecker symbol*.

Definition 1.8 (Kronecker symbol)**.** Let n be a non-zero integer, with prime factorization:

$$n = u \cdot p_1^{h_1} \cdots p_r^{h_r},$$

where u is a unit and the p_i are primes. Let a be an integer.

The *Kronecker symbol* $\left(\frac{a}{n}\right)$ is defined as:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{h_i}.$$

Where for odd primes p_i, the number $\left(\frac{a}{p_i}\right)$ is the *Legendre symbol*, defined by

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

When $p_i = 2$, we define:

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

The quantity $\left(\frac{a}{u}\right) = 1$ when $u = 1$, while:

$$\left(\frac{a}{-1}\right) = \begin{cases} -1 & \text{if } a < 0, \\ 1 & \text{if } a \geq 0. \end{cases}$$

Finally we put:

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & \text{if } a = \pm 1, \\ 0 & \text{otherwise}. \end{cases}$$

Proposition 1.3.5. *Let χ be a primitive real Dirichlet character. Then $\chi(m)$ equals the Kronecker symbol $\left(\frac{D}{m}\right)$, where D is the discriminant of the quadratic field K corresponding to χ.*

The last thing to prove in this section is the equality (1.17). The following theorem is proved in [Was97, Theorem 4.9].

Theorem 1.3.6. *Let χ be a Dirichlet's character with conductor f_χ, then:*

$$L(1,\chi) = \pi i \frac{\tau(\chi)}{f_\chi} \sum_{a=1}^{f_\chi} \overline{\chi}(a) a \quad if\ \chi(-1) = -1. \tag{1.18}$$

$$L(1,\chi) = -\frac{\tau(\chi)}{f_\chi} \sum_{a=1}^{f_\chi} \overline{\chi}(a) \log|1-\zeta_{f_\chi}^a| \quad if\ \chi(-1) = 1. \tag{1.19}$$

where $\tau(\chi)$ is the Gauss sum defined by

$$\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a) e^{2\pi i a/f_\chi}.$$

Since we are working with an even character, we will focus on (1.19). Our character is real, therefore $\chi = \overline{\chi}$ and its conductor is the discriminant D of the corresponding number field K. As a consequence, (1.19) becomes:

$$L(1,\chi_D) = -\frac{\tau(\chi_D)}{D} \sum_{a=1}^{D} \chi_D(a) \log|1-\zeta_D^a|. \tag{1.20}$$

Since $\log(1-\zeta_D^a) + \log(1-\zeta_D^{-a}) = 2\log|1-\zeta_D^a|$ and χ_D is even, we can rewrite (1.20) as:

$$L(1,\chi_D) = -\frac{\tau(\chi_D)}{D} \sum_{a=1}^{D} \chi_D(a) \log(1-\zeta_D^a). \tag{1.21}$$

Let us focus now on $\tau(\chi_D)$. It is proved in [Was97, Lemma 4.8] that

$$|\tau(\chi_D)| = \sqrt{D}. \tag{1.22}$$

We observe that, in our case, $\tau(\chi_D)$ is real. Indeed, we calculate its conjugate $\overline{\tau}(\chi_D)$:

$$\overline{\tau}(\chi_D) = \sum_{a=1}^{D} \overline{\chi_D}(a) e^{-2\pi i a/D} = \sum_{a=1}^{D} \chi_D(a) e^{-2\pi i a/D} = \sum_{a=1}^{D} \chi_D(-a) e^{2\pi i(-a)/D} = \tau(\chi_d).$$

Therefore, $\tau(\chi_D) = \pm\sqrt{D}$, and (1.21) becomes:

$$L(1,\chi_D) = \frac{\pm 1}{\sqrt{D}} \sum_{a=1}^{D} \chi_D(a) \log(1-\zeta_D^a) \tag{1.23}$$

Now, we susbstitute it in 1.13 and we obtain that:

$$\begin{aligned} \log(\varepsilon_K) &= \frac{\pm 1}{2h_K} \sum_{a=1}^{D} \chi_D(a) \log(1-\zeta_D^a), & (1.24)\\ &= \frac{\pm 1}{2h_K} \log\left(\prod_{a=1}^{D} (1-\zeta_D^a)^{\chi_D(a)} \right) & (1.25) \end{aligned}$$

and therefore (1.17) holds, up to a root of unity contained in K. Since ± 1 are the only roots of unity in K, the right hand side of (1.17) is equal to the $2h_K$-th power of a fundamental unit.

1.4 Conclusion

We discussed two methods to compute the fundamental unit of a real quadratic number field:

- The continued fraction method;
- Dirichlet's method using L-functions.

It is important to note that the continued fraction method is vastly superior in practice. On the other hand, we showed how equation (1.13) is the simplest non-trivial instance of the analytic class number formula, valid for general number fields. The analytic approach via L-functions therefore suggests the possibility of generalisation, and as we will see, it leads to deep conjectures in number theory like the Stark conjecture and the Gross–Stark conjecture, which we discuss in the remainder of this thesis.

Chapter 2

The rank one abelian Stark conjecture

In this chapter, we will present the rank one abelian Stark conjecture. First of all, we will recall the definitions of the objects which appear in the conjecture and we will state the conjecture in a general way. Secondly, we will focus on a specific case that involve the narrow Hilbert class field.

2.1 Stark's conjectures

In the previous chapter, we have seen how we can obtain a fundamental unit in the case where the ground field is $\mathbb{Q}$ with two different methods.

In particular, we discussed the *Dirichlet class number formula* (1.9) for number fields K, which by the functional equation implies that

$$\zeta_K(t) = -\frac{h_K R_K}{w_K} t^{r+s-1} + O(t^{r+s}),$$

where we recall that h_K and R_K denote the class number and regulator of K respectively, and w_K denotes the number of roots of unity in K.

Remark 2.1.1. We have seen that if $r + s - 1 = 1$, we can replace the regulator R_K with $\log(\varepsilon_K)$ and we can obtain a fundamental unit as we have discussed in the previous chapter. However, for general number fields, we have no possibility of easily recovering the unit group from the regulator whenever the unit rank is greater than one.

To remedy this, Harold Mead Stark formulated a conjecture which gives a refinement of the Dirichlet class number formula, by breaking up the unit group $\mathcal{O}_K$ into 'pieces'. The Stark conjectures, introduced by Stark [Sta71; Sta75a; Sta76; Sta80] and later expanded by Tate [Tat84], give conjectural information about the coefficient of the leading term in the Taylor expansion of an Artin L-function associated with a Galois extension K/k of algebraic number fields.

Moreover, in the case where K/k is an abelian extension, Stark has given a refined conjecture which essentially states there exists a unit of K such that specific linear combinations of its archimedean valuations give the values of the derivatives $L'(0,\chi)$, where χ is a character of $\mathrm{Gal}(K/k)$. In certain cases, this *"Stark unit"* can be seen to generate K over k, and hence the refined conjecture implies that K can be obtained from k by adjoining the value of a certain analytic function at zero. This is reminiscent of the celebrated Hilbert's twelfth problem, which asks whether one can generate all abelian extensions of a given algebraic number field in a way that would generalize the so-called theorem of Kronecker and Weber to any base number field.

Theorem 2.1.2 (Kronecker-Weber theorem)**.** *Every finite abelian extension of the rational numbers $\mathbb{Q}$ is a subfield of a cyclotomic field. Hence, whenever an algebraic number field has a Galois group over $\mathbb{Q}$ that is an abelian group, the field is a subfield of a field obtained by adjoining a root of unity to the rational numbers.*

In particular, Hilbert asked what are the algebraic numbers necessary to construct all abelian extensions of k, where k is a general number field. As Stark observed himself *"a reference to Hilbert's 12th problem may not be completely inappropriate."* [Sta75b]. In fact, in cases where a solution to Hilbert's 12th problem is known, namely when k is either $\mathbb{Q}$ or a quadratic imaginary field, Stark was able to prove his abelian conjecture. For these reasons, Stark's conjectures remain among the central open problems in number theory.

The case that we are going to study in this chapter is the abelian rank one Stark conjecture in which the extension is abelian and the L-function vanishes to order one and this case leads to the notion of a "Stark unit". Namely, under certain technical assumptions, Stark predicts that there is a unit ε in K such that:

$$\zeta'_{\mathcal{S}}(0,\sigma) \sim \log|\sigma(\varepsilon)|_{\omega},$$

where $\zeta_{\mathcal{S}}(0,\sigma)$ is a the partial zeta function that we will introduce in the next section.

2.2 The partial zeta function

In this section, we will present the *partial zeta function* which will be a fundamental ingredient for the rank one Stark conjecture that we will state in the next section. Firstly, we will give the definition in the simplest case, and then we will move to a more general version which will be used in the statement of the conjecture.

Let K/k be a finite abelian Galois extension and $G = \mathrm{Gal}(K/k)$. We can construct a map α from the integral ideals of $\mathcal{O}_k$ and G defined in the following way:

$$\begin{array}{rccc} \alpha: & \{\text{Ideals of } \mathcal{O}_k\} & \longrightarrow & G \\ & \mathfrak{a} & \longmapsto & [\mathfrak{a}] \end{array}$$

by sending a prime ideal $\mathfrak{p}$ to the Frobenius element $[\mathfrak{p}]$, which is the unique element of G in the decomposition group $D_{\mathfrak{p}}$ defined in A.5 which reduces to the Frobenius morphism $x \mapsto x^p$ in the Galois group of the residue field extension at $\mathfrak{p}$. For a general ideal $\mathfrak{a}$, we factor it into prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

and sent it to the corresponding product of Frobenius elements:

$$\mathfrak{a} \mapsto [\mathfrak{a}] = [\mathfrak{p}_1]^{e_1} \dots [\mathfrak{p}_r]^{e_r}.$$

Now we can define the *partial zeta function.*

Definition 2.1 (The partial zeta function)**.** Let K/k be a finite abelian Galois extension and $G = \mathrm{Gal}(K/k)$. Then for every $\sigma \in G$ we can define the *partial zeta function* for complex number s with $\mathfrak{R}(s) > 1$:

$$\zeta_{\mathcal{S}}(s,\sigma) = \sum_{\substack{\mathfrak{a} \triangleleft \mathcal{O}_k \\ [\mathfrak{a}] = \sigma}} \mathrm{Norm}(\mathfrak{a})^{-s}. \tag{2.1}$$

namely we sum only over ideals of K whose class $[\mathfrak{a}]$ is equal to σ.

More generally, we can define a version of the partial zeta function relative to a finite set of places $\mathcal{S}$ in k, which we assume to minimally contain:

1. all Archimedean places
2. all places which ramify in K/k.

Definition 2.2 ($\mathcal{S}$-Partial zeta function)**.** To any element $\sigma \in \mathrm{Gal}(K/k)$, with K/k and $\mathcal{S}$ as above, we associates the *partial zeta function* defined for a complex number s with $\mathfrak{R}(s) > 1$ by the Dirichlet series:

$$\zeta_{\mathcal{S}}(s,\sigma) = \sum_{\substack{(\mathfrak{a},\mathcal{S})=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \mathrm{Norm}(\mathfrak{a})^{-s}. \tag{2.2}$$

where $\mathfrak{a}$ runs through the integral ideals of k not divisible by any finite prime ideal contained in $\mathcal{S}$ and such that the Artin symbol $\sigma_{\mathfrak{a}}$ is equal to σ.

Moreover, with the same setup, we can also define an L- function.

Definition 2.3. Let K/k and $\mathcal{S}$ as above, we can associates an L-function to a character χ over G defined for a complex number s with $\Re(s) > 1$ by the Euler product:

$$L_{\mathcal{S}}(s,\chi) = \prod_{\mathfrak{p}\notin\mathcal{S}} (1 - \chi(\mathfrak{p})\operatorname{Norm}(\mathfrak{p})^{-s})^{-1}. \tag{2.3}$$

where $\mathfrak{p}$ runs through the finite prime ideals of k not contained in $\mathcal{S}$.

Remark 2.2.1. Since $G = \operatorname{Gal}(K/k)$ is abelian, all of its irreducible representations are 1-dimensional, so the character χ is a multiplicative homomorphism $\chi : G \longrightarrow \mathbb{C}^{\times}$.

In order to have some information about the order of vanishing of this L-function we need the following definition. If χ_0 is the trivial character we set $r(\chi_0) = |\mathcal{S}| - 1$. Otherwise

$$r(\chi) = |\{v \in \mathcal{S} : \chi(D_v) = 1\}| \tag{2.4}$$

where D_v is the decomposition group for v. The following theorem is proved in [Das99].

Theorem 2.2.2. *The order of vanishing at $s = 0$ of the L-function $L_{\mathcal{S}}(s,\chi)$ is equal to $r(\chi)$.*

In addition, we have the following relation between the partial zeta function and the L-function:

Proposition 2.2.3.

$$L_{\mathcal{S}}(s,\chi) = \sum_{\sigma\in G} \zeta_{\mathcal{S}}(s,\sigma)\chi(\sigma). \tag{2.5}$$

$$\zeta_{\mathcal{S}}(s,\sigma) = \frac{1}{|G|}\sum_{\chi\in\hat{G}} L_{\mathcal{S}}(s,\chi)\overline{\chi}(\sigma). \tag{2.6}$$

We can observe that both of these functions can be analytically continued to meromorphic functions on the whole complex plane.

2.3 The rank one abelian Stark conjecture

In this section, we will state the rank one abelian Stark conjecture with a specific focus for K the Hilbert Narrow class field of k. In addition, we will present an important remark which is connected to the *Hilbert 12^{th} problem.*

Let us consider K/k a finite abelian extension of number fields, with $G = \operatorname{Gal}(K/k)$ and let us consider a finite set of places $\mathcal{S}$ in k, which minimally contains all Archimedean places and all places which ramify in K, as before. We define the group of $\mathcal{S}$-units in the following way.

Definition 2.4 ($\mathcal{S}$-unit)**.** An element $x \in K$ is an $\mathcal{S}$-unit if the fractional ideal (x) is a product of primes that lie above primes of $\mathcal{S}$.

Remark 2.3.1. We can observe that asking that the fractional ideal (x) is a product of primes lying above primes in $\mathcal{S}$ is the same as asking that the valuation of x is equal to 1 for all finite primes of K not above $\mathcal{S}$, i.e. $|x|_w = 1$ for all places $w \notin \mathcal{S}_K$ with w in K and where $\mathcal{S}_K$ is the set of places of K which lie above $\mathcal{S}$.

Let us choose the set $\mathcal{S}$ such that it satisfies the following conditions:

1. $\mathcal{S}$ is finite set of places containing all Archimedean places and all places ramifying in K/k.
2. $\mathcal{S}$ contains at least one place v which splits completely in K.

3. $L_{\mathcal{S}}(s;\chi)$ vanishes to order 1 at $s=0$.

4. $|\mathcal{S}| \geq 2$.

With these conditions on $\mathcal{S}$, the rank one abelian conjecture takes the following form:

Conjecture 2.3.2 (Rank one abelian Stark conjecture)**.** Choose a place w of K lying above the place v of k that splits completely in K. Then there exists an $\mathcal{S}$-unit ε such that:

1. If $|S| \geq 3$ then $|\varepsilon|_w' = 1$ for all places w' of K s.t. w' doesn't divide v in k.

2. If $S = \{v,\ v'\}$ then $|\varepsilon|_{\sigma(w)} = |\varepsilon|_{w'}$ for all $\sigma \in G$ and all places w' of K dividing v'.

3. For every $\sigma \in G$ we have:
$$\log|\sigma(\varepsilon)|_w = -e\zeta_{\mathcal{S}}'(0,\sigma) \tag{2.7}$$
where e is the number of roots of unity in K;
or equivalently:
$$L_{\mathcal{S}}'(0,\chi) = -\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma)\log|\sigma(\varepsilon)|_w \tag{2.8}$$
for any character χ over G.

4. The extension $K(\varepsilon^{1/e})/k$ is an abelian extension of k.

Any unit satisfying the conditions of this conjecture will be referred to as a *Stark unit.*

Remark 2.3.3. Condition 1 requires that ε is a v-unit, which is stronger than just asking that ε is an $\mathcal{S}$-unit. Indeed, the absolute value of ε is trivial not only in the places outside $\mathcal{S}$ but also in the places of $\mathcal{S}$ which do not divide v, hence the only important information resides in the valuations at the prime divisors of v.

Remark 2.3.4. In addition, since the conditions on ε specify its absolute value at every place of K, we have that ε is uniquely determined up to multiplication by a root of unity in K.

Henceforth, k will be a real quadratic field, and we will focus on the case where K is the narrow Hilbert class field of k. Since k is a real quadratic field, we have two embeddings in $\mathbb{C}$ namely $\sigma_1 : k \longrightarrow \mathbb{C}$ and $\sigma_2 : k \longrightarrow \mathbb{C}$ and they are both real. In particular, if $k = \mathbb{Q}[\sqrt{d}]$ we have that $\sigma_1(\sqrt{d}) = \sqrt{d}$ and $\sigma_2(\sqrt{d}) = -\sqrt{d}$. We recall the Ostrowski's theorem.

Theorem 2.3.5 (Ostrowski's theorem)**.** *Let k be a number field. Then for every embedding $\sigma : k \longrightarrow \mathbb{C}$ there will be an archimedian place denoted by $|\cdot|_\sigma : k \longrightarrow \mathbb{R}_{\geq 0}$.*

Therefore, there are exactly two archimedean places of k namely $\infty_1 := |\cdot|_{\sigma_1}$ and $\infty_2 := |\cdot|_{\sigma_2}$.

We recall the definition of a class group.

Definition 2.5 (Class group)**.** The *ideal class group* of a number field k is the quotient group $\mathfrak{Cl}_k := \mathcal{I}(k)/\mathcal{P}(k)$ where $\mathcal{I}(k)$ is the group of fractional ideals of $\mathcal{O}_k$, and $\mathcal{P}(k)$ is its subgroup of principal ideals.

Definition 2.6 (Hilbert class field)**.** The *Hilbert class field* $\mathcal{H}$ of a number field k is the maximal finite abelian extension that is unramified at all places of k. It is finite Galois extension of k, and $\mathrm{Gal}(\mathcal{H}/k)$ is isomorphic to the class group of k via the Artin map.

We can define also the narrow class group.

Definition 2.7 (Narrow class group)**.** The *narrow class group* of a number field k is the quotient group $\mathfrak{Cl}_k^+ := \mathcal{I}(k)/\mathcal{P}(k)^+$, where $\mathcal{I}(k)$ is the group of fractional ideals of $\mathcal{O}_k$, and $\mathcal{P}(k)^+$ is its subgroup of principal ideals generated by totally positive elements of k, that is an element $a \in k$ such that $\sigma(a) > 0$ for every real embedding $\sigma :\ k \hookrightarrow \mathbb{R}$.

We have the following proposition.

Proposition 2.3.6. *Let k be a real quadratic field. Then:*

1. $\mathfrak{Cl}_k = \mathfrak{Cl}_k^+$ *if and only if there exists a unit in $\mathcal{O}_k$ of norm equal to -1.*
2. *otherwise* $\mathfrak{Cl}_k^+$ *is twice as big as* $\mathfrak{Cl}_k$*, namely* $[\mathfrak{Cl}_k^+ : \mathfrak{Cl}_k] = 2$.

Example 2.1. Let us consider $k = \mathbb{Q}(\sqrt{3})$. We know that k is a PID, namely every ideal is principal, hence $\mathfrak{Cl}_k$ is trivial and $h_k = 1$. On the other hand, we can observe that the equation:

$$\mathrm{Norm}(u) = x^2 - 3y^2 = -1,$$

has no solution. This means, by the proposition, that $[\mathfrak{Cl}_k^+ : \mathfrak{Cl}_K] = 2$, hence $\mathfrak{Cl}_k^+ \cong \mathbb{Z}/2\mathbb{Z}$.

We recall the definition of the narrow Hilbert class field.

Definition 2.8 (Narrow Hilbert Class field)**.** The *narrow Hilbert Class field* $\mathcal{H}^+$ of a number field k is the maximal finite abelian extension of k that is unramified at all finite primes of k.

Remark 2.3.7. It is easy to prove that the narrow Hilbert class field of $\mathbb{Q}(\sqrt{3})$ in example 2.1 is $\mathcal{H}^+ := \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ since it satisfies the previous conditions.

To conclude, we have the following relation.

Proposition 2.3.8. *Let k be a number field and $\mathcal{H}^+$ its narrow Hilbert class field, then:*

$$\mathrm{Gal}(\mathcal{H}^+/k) \cong \mathfrak{Cl}_k^+. \tag{2.9}$$

As a consequence we have the following diagram:

$$\begin{tikzcd} \mathcal{H}^+ \arrow[d, dash, "2\ or\ 1"'] \\ \mathcal{H} \arrow[d, dash, "h_k"'] \\ k \end{tikzcd}$$

Let us consider K as the *narrow Hilbert Class field* $\mathcal{H}^+$ of k.

Observe that if we consider $K = \mathcal{H}^+$, we do not have any information about the behaviour of the two infinite places ∞_1 and ∞_2; they could be either real or complex. As a consequence, if we want the set $\mathcal{S}$ to satisfy the conditions necessary for Stark's conjecture, we may need to include finite primes. Consider the set $\mathcal{S} = \{\infty_1, \infty_2, \mathfrak{p}\}$ where $\mathfrak{p}$ is a finite prime of k which splits completely in $\mathcal{H}^+/k$. Note that the set $\mathcal{S}$ now satisfies $|\mathcal{S}| = 3$; it contains all the archimedean places of k, there are no finite places which ramify in $\mathcal{H}/k$, andthere is at least one place which splits completely in $\mathcal{H}^+$ which is $\mathfrak{p}$. When $L_S(s;\chi)$ vanishes to order 1 at $s = 0$, Stark's conjecture then predicts:

Conjecture 2.3.9. Choose w a prime of $\mathcal{H}^+$ above $\mathfrak{p}$. Then there exists an $\mathcal{S}$-unit ε such that:

1. $|\varepsilon|_{w'} = 1$ for all places w' of $\mathcal{H}^+$ not dividing $\mathfrak{p}$.
2. For every $\sigma \in G$ we have:
$$\log|\sigma(\varepsilon)|_w = -e\zeta'_{\mathcal{S}}(0,\sigma) \tag{2.10}$$
where e is the number of roots of unity in $\mathcal{H}^+$; or equivalently:
$$L'_{\mathcal{S}}(0,\chi) = -\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma)\log|\sigma(\varepsilon)|_w \tag{2.11}$$
for any character χ of G.
3. The extension $H^+(\varepsilon^{1/e})/k$ is an abelian extension of k.

Remark 2.3.10. In order to choose the possible $\mathfrak{p}$ which splits completely in $\mathcal{H}^+/k$ we can apply the following theorem. Let consider p inert in $k/\mathbb{Q}$, then $\mathfrak{p} := (p)$ is generated by a totally positive element of k, and therefore it splits completely in the narrow Hilbert class field $\mathcal{H}^+/k$.

The relation between Stark's conjecture and *Hilbert's twelfth problem* comes from the following proposition:

Proposition 2.3.11. *Let K/k be an extension of number fields, and assume that $G = \mathrm{Gal}(K/k)$ is cyclic. For any set $\mathcal{S}$ as before, containing only one place which splits completely in K, and any faitful character χ of G (i.e. χ has trivial kernel), the Stark conjecture implies that $K = k(\varepsilon)$.*

Note that, since χ has trivial kernel, equation (2.4) implies that $r(\chi) = |\{v \in S : \chi(D_v) = 1\}| = 1$, and therefore the L-function $L_{\mathcal{S}}(s,\chi)$ indeed has rank one. If we consider K and k such that any $\tau \in G$ satisfies $\tau(\varepsilon) = \varepsilon$, then we can rewrite (2.11) in the following way:

$$L'_{\mathcal{S}}(0,\chi) = -\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma)\log|\sigma(\varepsilon)|_w \tag{2.12}$$

$$= -\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma\tau)\log|\sigma(\tau(\varepsilon))|_w \tag{2.13}$$

$$= -\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma)\chi(\tau)\log|\sigma(\varepsilon)|_w \tag{2.14}$$

$$= -\chi(\tau)\frac{1}{e}\sum_{\sigma\in G}\chi(\sigma)\log|\sigma(\varepsilon)|_w \tag{2.15}$$

$$= \chi(\tau)L'_{\mathcal{S}}(0,\chi). \tag{2.16}$$

As a consequence $\chi(\tau) = 1$ and since χ is faithful it follows that $\tau = 1$, hence ε is fixed only by the trivial element of G. Therefore, $k(\varepsilon)$ is fixed only by the trivial subgroup of G. This means that $K = k(\varepsilon)$, since otherwise $k(\varepsilon)$ would be a proper subfield of K, hence it should be fixed by a non-trivial subgroup of G by Galois theory.

Dasgupta underlined another interesting case, namely when k is also totally real and the only place v which splits completely is real. Suppose that ε is a positive *Stark* unit and fix an embedding $k \subset K \subset K_w$, corresponding to a real place w above v. We are still in the conditions of the Stark conjecture and in this specific case we have that $e = 2$. Applying (2.7) to $\sigma = 1$ we obtain:

$$\varepsilon = \exp(-2\zeta'_{\mathcal{S}}(0,1)) \tag{2.17}$$

From the previous observations, this implies that $K = k(\exp(-2\zeta'_{\mathcal{S}}(0,1))$.

Remark 2.3.12. On one hand, this result is relevant to Hilbert's twelfth problem, since the extension K can be obtained (condintionally on Stark's conjecture) by adjoining a unit, which can be computed as the special value of an analytic function. On the other hand, however, this function $\zeta'_{\mathcal{S}}(s,1)$ still depends on the extension K/k.

Remark 2.3.13. In general, the Stark conjecture remains an open problem. On the other hand, the p-adic counterpart (the *Gross–Stark conjecture*) was proved by Darmon, Dasgupta and Pollack in 2011.

Chapter 3

The Gross–Stark conjecture

In this chapter, we state a p-adic analogue of the Stark conjecture for real quadratic fields. It has several advantages over the complex version. On the one hand, the p-adic analogue of the Stark conjecture is actually a theorem, proved by Samit Dasgupta, Henri Darmon, and Robert Pollack in [SP11]. On the other hand, it is also possible to compute the first order derivatives of the relevant p-adic L-series, leading to practical algorithms to determine Gross–Stark units, which are contained in abelian extensions of real quadratic fields.

In the first section we present some of the basics of p-adic analysis. We study continuous functions on $\mathbb{Z}_p$ and *Mahler's theorem*, which allows us to write a continuous function on $\mathbb{Z}_p$ as a formal combination of binomial polynomials, called its Mahler expansion. After that, we will focus on Hensel's lemma and we underline some of its main consequences. We conclude this section by studying analytic functions on $\mathbb{Z}_p$, and we define the p-adic logarithm

$$\log_p : \mathbb{C}_p^\times \longrightarrow \mathbb{C}_p.$$

The second section introduces p-adic L-functions of real quadratic fields. After a brief historical introduction, we recall some properties of these p-adic L-functions, notably the interpolation property.In the context of the Gross–Stark conjecture, we choose the prime p such that p is inert in $k/\mathbb{Q}$, and consider the p-adic L-function associated to an *odd* character

$$\chi : \mathfrak{Cl}_k^+ \longrightarrow \overline{\mathbb{Q}}^\times,$$

of the narrow class group $\mathfrak{Cl}_k^+$ of k, which means that $\chi([(\sqrt{D_k})]) = -1$, where D_k is the discriminant of k. For such a character to exist, k must have a fundamental unit of positive norm. Finally, we discuss an algorithm to compute these p-adic L-functions, and we illustrate this with some examples of p-adic L-functions and Gross–Stark units.

3.1 p-adic analytic functions

In this section we introduce some of the basics of the p-adic analysis that will be useful. We will discuss continuous and analytic functions on $\mathbb{Z}_p$, and define the p-adic logarithm. To conclude, we will define p-adic L-functions of real quadratic fields, and discuss some of their principal properties. The proofs of the results of this section could be found in [Ste21; Von21]

3.1.1 Continuous functions on $\mathbb{Z}_p$

In this section we will make a small presentation of the continuous functions on $\mathbb{Z}_p$ which take values in a finite extension of $\mathbb{Q}_p$. We will also present the Mahler's theorem. The definitions of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ and their basic properties can be found in A.4 and the basic properties of non-archimedean analysis can be found the paper [Von21].

Definition 3.1 (Continuous function on $\mathbb{Z}_p$)**.** Let L be a finite extension of $\mathbb{Q}_p$ and $f : \mathbb{Z}_p \longrightarrow L$. We say that f is continuous on $\mathbb{Z}_p$ if for every $x_0 \in \mathbb{Z}_p$ we have that:

$$\forall \varepsilon \in \mathbb{R}^+, \exists \delta_{\varepsilon,x_0} \in \mathbb{R}^+ : \forall x \in B(x_0, \delta_{\varepsilon,x_0}) = \{x \in \mathbb{Z}_p \ : \ |x - x_0|_p < \delta_{\varepsilon,x_0}\} \Rightarrow |f(x_0) - f(x)|_L < \varepsilon$$

Essentially the same definition may be given for any metric space. Since many of the properties we will use can be stated and proved in much more generality, we make abstraction of the specifics of $\mathbb{Z}_p$, and focus on two of its crucial properties that go into consequent results. First of all, $\mathbb{Z}_p$ is a compact space, hence we can apply the theorem of Heine-Cantor.

Theorem 3.1.1 (Heine-Cantor)**.** *Let $(X, \phi_X), (Y, \phi_Y)$ two metric spaces and $f : X \longrightarrow Y$ a continuous function on X. If X is a compact space, then f is also uniformly continuous.*

This statement immediately implies that every continuous function $f : \mathbb{Z}_p \longrightarrow L$ is also uniformly continuous. A second important important property of $\mathbb{Z}_p$ is that the set of natural numbers $\mathbb{N}$ is dense in it. This implies that if we can define a continuous function on $\mathbb{N}$, it uniquely extends to a continuous function on $\mathbb{Z}_p$. This mechanism is reffered to as *interpolation*.

Proposition 3.1.2. *Let $g : \mathbb{N} \longrightarrow L$ be a uniformly continuous function, with respect to the subspace topology on $\mathbb{N} \subset \mathbb{Z}_p$. Then g uniquely extends to a continuous function $f : \mathbb{Z}_p \longrightarrow L$.*

We now define binomial polynomials, which will be our prototypical example of a continuous function $\mathbb{Z}_p \to \mathbb{Z}_p$. We will see that these are in some sense the only examples, as is made precise by Mahler's theorem stated below.

Definition 3.2. For every $n \in \mathbb{N}$ we define the binomial polynomial

$$\binom{x}{n} := \begin{cases} 1 & \text{if } n = 0, \\ \dfrac{x(x-1)\cdots(x-n+1)}{n!} & \text{if } n \geq 1. \end{cases} \tag{3.1}$$

Firstly, we prove that it defines a continuous function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.

Lemma 3.1.3. *If $x \in \mathbb{Z}_p$, then $\binom{x}{n} \in \mathbb{Z}_p$ for all $n \in \mathbb{N}$.*

Proof. The polynomial function $f(x) = \binom{x}{n}$ is continuous and $f(m)$ is an integer for all $m \in \mathbb{N}$. The previous proposition then implies that this function maps the closure of $\mathbb{N}$, which is $\mathbb{Z}_p$, to $\mathbb{Z}_p$ [Alp85]. □

We are now ready to state the Mahler's theorem.

Theorem 3.1.4 (Mahler's theorem)**.** *Let $f : \mathbb{Z}_p \longrightarrow L$ be a continuous function. Then there exist a unique sequence of elements $a_n \in L$ with $\lim_{n\to\infty} a_n = 0$ such that:*

$$f(x) = \sum_{n\geq 0} a_n \binom{x}{n}. \tag{3.2}$$

This expression is called the *Mahler expansion* of the continuous function f and the a_n are called its *Mahler coefficients*. A similar result was proved by Dieudonné in [Die44] for compact subsets of $\mathbb{Q}_p$.

We now define a norm on the space of continuous functions on $\mathbb{Z}_p$.

Definition 3.3 (Supremum norm)**.** Let $f : \mathbb{Z}_p \longrightarrow L$ be a continuous function, then we can define:

$$||f|| := \sup_{x\in\mathbb{Z}_p} |f(x)|. \tag{3.3}$$

Remark 3.1.5. We can observe that, since $\mathbb{Z}_p$ is a compact space, any continuous function on $\mathbb{Z}_p$ has to be bounded in it, hence this norm is always finite.

In addition, we can give an equivalent definition of this norm, based on the Mahler's theorem.

Definition 3.4. Let $f : \mathbb{Z}_p \longrightarrow L$ be a continuous function, and $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$, then we can define:

$$\|f\| := \sup_{n \to \infty} |a_n|. \tag{3.4}$$

To conclude, we underline that the space of continuous function from $\mathbb{Z}_p$ to L, denoted by $\mathcal{C}(\mathbb{Z}_p, L)$ is a Banach space with respect to the supremum norm, i.e. a complete normed vector space, and this norms endows it with a topology.

3.1.2 Hensel's lemma

In this section we state Hensel's Lemma both in general, and in the p-adic case. Then we will prove that the roots of unity of $\mathbb{Z}_p$ are exactly the $p-1$ roots of $X^{p-1} - 1 \in \mathbb{Z}_p[X]$. To conclude, we will recall the Teichmüller representatives and the Teichmüller character.

The main aim of Hensel's lemma is to lift approximate factors of a polynomial f, defined over a complete non-archimedean valued field, to actual factors.

Theorem 3.1.6 (Hensel's lemma)**.** *Let K be complete with respect to a non-archimedean valuation and A the valuation ring of K. Suppose that $f \in A[X]$ is a polynomial that factors over the residue class field $k = A/\mathfrak{m}$ as:*

$$\overline{f} = \overline{g} \cdot \overline{h} \in k[X]$$

with $\overline{g}, \overline{h} \in k[X]$ non-zero and coprime. Then there exist $g, h \in A[X]$ with $deg(g) = deg(\overline{g})$, such that

$$f = g \cdot h \in A[X].$$

Observe that if $\overline{g}$ is a linear factor of $\overline{f}$, namely if $\overline{g} = X - \overline{\alpha}$, then asking that $\overline{g}$ and $\overline{f}/\overline{g}$ are coprime is equivalent to requiring that $\overline{\alpha}$ is a simple root of $\overline{f} \in k[X]$. As a consequence, we obtain the following useful corollary, which will be used repeatedly in what follows.

Corollary 3.1.7. *Let $f \in A[X]$ be a polynomial. Then every simple zero $\overline{\alpha} \in k = A/\mathfrak{m}$ of $\overline{f} \in k[X]$ can uniquely be lifted to a zero $\alpha \in A$ of f satisfying:*

$$\overline{\alpha} \equiv \alpha \pmod{\mathfrak{m}}.$$

Let us consider the case where $K = \mathbb{Q}_p$, so that $A = \mathbb{Z}_p$ and $k = \mathbb{F}_p$. We will be able to determine all roots of unity in $\mathbb{Z}_p$ using Hensel's lemma. First, we consider the polynomial $X^p - X \in \mathbb{F}_p[X]$. By Fermat's little theorem we know that this polynomial splits completely into linear factors over $\mathbb{F}_p[X]$. More precisely, we have

$$X^p - X = \prod_{i=0}^{p} (X - i) \in \mathbb{F}_p[X].$$

Since all of these roots are simple, we apply Hensel's lemma and obtain that the polynomial $X^{p-1} - 1$ has $p-1$ distinct roots in $\mathbb{Z}_p$. It can be shown that the number of roots of unity in $\mathbb{Z}_p^\times$ equals

$$\mathcal{U}(\mathbb{Z}_p^\times) = \begin{cases} 2 & if\ p = 2 \\ p-1 & if\ p > 2 \end{cases}. \tag{3.5}$$

We assume henceforth that p is an odd prime. We now define the *Teichmüller representative* and the *Teichmüller character.*

Definition 3.5 (Teichmüller lift)**.** The *Teichmüller representative* $\overline{\omega}(a)$ of an element a in $\mathbb{F}_p^\times$ is the unique root of unity in $\mathbb{Z}_p^\times$ that reduces to a. This defines a morphism

$$\begin{aligned} \overline{\omega} : \mathbb{F}_p^\times &\longrightarrow \mathbb{Z}_p^\times \\ a &\longmapsto \overline{\omega}(a). \end{aligned}$$

Remark 3.1.8. In general we have no information on the p-adic expansion of the Teichmüller representative $\overline{\omega}(a)$ besides its first digit, which must be a. However, since $\overline{\omega}$ is a group homomorphism, we do know that

$$\begin{aligned}\overline{\omega}(1) &= 1\\ \overline{\omega}(-1) &= (p-1)+(p-1)p+\cdots+(p-1)p^n+\ldots.\end{aligned}$$

Definition 3.6 (Teichmüller character)**.** The *Teichmüller character* is the homomorphism:

$$\begin{aligned}\omega : \mathbb{Z}_p^\times &\longrightarrow \mathbb{Z}_p^\times\\ a &\longmapsto \omega(a)\end{aligned}$$

obtained by first reducing modulo p, then sending an element to its Teichmüller representative. Moreover, we can define the following projection:

$$\begin{aligned}\langle\cdot\rangle : \mathbb{Z}_p^\times &\longrightarrow 1+p\mathbb{Z}_p\\ x &\longmapsto \langle x\rangle := \frac{x}{\omega(x)}\end{aligned}$$

Hence the Teichmüller representatives give us an isomorphism $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p)$ with the following identification:

$$x \in \mathbb{Z}_p^\times = (\omega(x), \langle x\rangle).$$

3.1.3 Analytic functions on $\mathbb{Z}_p$

In this section we discuss analytic functions on $\mathbb{Z}_p$. We study their radius convergence, and define the p-adic logarithm and the p-adic exponential.

In the previous section we have studied the space of continuous functions $\mathcal{C}(\mathbb{Z}_p, L)$ where L is a finite extension of $\mathbb{Q}_p$. We now consider only a particular kind of continuous functions, namely the analytic functions. We give a definition of analytic functions using the Mahler expansion.

Definition 3.7 (Analytic function)**.** Let $f : \mathbb{Z}_p \longrightarrow L$ be a continuous function with Mahler expansion:

$$f(x) = \sum_{n\geq 0} a_n \binom{x}{n}.$$

We say this function is analytic if

$$\lim_{n\to\infty} \frac{a_n}{n!} = 0. \tag{3.6}$$

All analytic functions are continuous but the converse is not true. Indeed, the condition (3.6) is stronger than the condition that $a_n \to 0$ given by Mahler's theorem. An equivalent definition is that analytic functions are those functions defined by a power series $f(x) \in L[\![x]\!]$.

Remark 3.1.9. One of the main properties of analytic functions, which distinguish them from mere continuous functions, is that they can be evaluated at arguments x in extensions of $\mathbb{Q}_p$.

In order to do that, consider an analytic function $f(x) \in \mathbb{C}_p[\![x]\!]$. We recall that $\mathbb{C}_p$ is algebraically closed from Proposition A.4.4. We are now ready to define the *radius of convergence* of the analytic function f on $\mathbb{Z}_p$.

Definition 3.8 (Radius of convergence)**.** Let

$$f(x) = \sum_{n\geq 0} a_n x^n \;\in\; \mathbb{C}_p[\![x]\!]$$

be an analytic function. Then its radius of convergence R is defined as:

$$\frac{1}{R} = \limsup_n |a_n|^{\frac{1}{n}}. \tag{3.7}$$

We can see that $0 \leq R \leq \infty$ and study the convergence.

Proposition 3.1.10. *An analytic function $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{C}_p[\![x]\!]$ converges for a given value $x \in \mathbb{C}_p$ if and only if we have:*

$$\begin{cases} |x| \leq R & \text{if } \lim_{n\to\infty} |a_n| R^n \to 0 \\ |x| < R & \text{otherwise.} \end{cases} \tag{3.8}$$

Remark 3.1.11. We observe that in p-adic analysis any power series either converges on the entire boundary $|x| = R$ or nowhere at all on the boundary. In contrast, we can have different behaviours on the boundary in real and complex analysis. This is one of the many advantages of studying objects in the p-adic setting.

We are now ready to introduce the p-adic logarithm which will be fundamental for the p-adic Gross–Stark conjecture.

Definition 3.9 (p-adic logarithm)**.** We define the p-adic logarithm as the following analytic function:

$$\log_p(1+x) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \tag{3.9}$$

The radius of convergence of this analytic function is $R = 1$ and this function does not converge anywhere on the boundary. This function may be extended to the domain $\mathbb{C}_p^\times$ by choosing the *Iwasawa branch* of the p-adic logarithm, which we now describe.

Proposition 3.1.12. *There exists an unique function $\log_p : \mathbb{C}_p^\times \longrightarrow \mathbb{C}_p$ such that:*

1. $\log_p(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$ *for all $x \in \mathbb{C}_p^\times$ s.t. $|x| < 1$;*
2. $\log_p(xy) = \log_p(x) + \log_p(y)$ *for all $x, y \in \mathbb{C}_p^\times$;*
3. $\log_p(p) = 0$.

Proof. First of all, we choose an element p^r for any $r \in \mathbb{Q}$, s.t. $p^{r+s} = p^r \cdot p^s$ for all $r, s \in \mathbb{Q}$. We can write any element $a \in \mathbb{C}_p$ as $a = p^r \cdot a_0$, with $r \in \mathbb{Q}$ and $|a_0| = 1$, because of the fact that $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$, hence it has value group equal to $p^{\mathbb{Q}}$. In addition, since $|a_0| = 1$ we can write it uniquely as $a_0 = \omega \cdot a_1$ s.t. ω is a root of unity of order coprime with p, and $|a_1 - 1| < 1$. This comes from the fact that any sequence of elements in $\overline{\mathbb{Q}}_p$ which approximate a_0, determines a sequence of elements also in the residue field of $\overline{\mathbb{Q}}_p$, which is eventually constant, since $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$. As a consequence, we can lift this element in the residue class of $\overline{\mathbb{Q}}_p$ to a root of unity ω by the Hensel's lemma and we can define the p-adic logarithm in the following way:

$$\log_p(a) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(a_1 - 1)^n}{n} = \log_p(a_1).$$

This object satisfies the previous properties. □

In a similar way we can define the p-adic exponential.

Definition 3.10 (p-adic exponential)**.** We define the p-adic exponential as the following analytic function:

$$\exp_p(1+x) := \sum_{n=1}^{\infty} \frac{x^n}{n!} \tag{3.10}$$

With some computations we obtain that its radius of convergence is $R = p^{-1/(p-1)} < 1$.

Remark 3.1.13. We can observe that its radius of convergence depends on the prime p while the radius of of convergence of the p-adic logarithm is always 1.

Remark 3.1.14. Unlike the p-adic logarithm, there is no possibility to extend the p-adic exponential to a larger set. As a matter of facts, if we want to have better possibilities we could for instance consider the *Artin-Hasse exponential*, which is similar to the p-adic exponential but has better convergence properties. It is defined by

$$E(x) := \exp(\sum_{i=0}^{\infty} \frac{x^{p^i}}{p^i}) \tag{3.11}$$

and one can show that $E(x) \in 1 + x \cdot \mathbb{Z}_p[\![x]\!]$.

To conclude, we can see that under certain circumstances the p-adic logarithm and the p-adic exponential are mutual inverses.

Proposition 3.1.15. *If* $|x| < p^{-1/(p-1)}$ *then*

$$\log_p \exp_p(x) = x$$

$$\exp_p \log_p(x+1) = x+1.$$

3.2 p-adic L-functions

In this section we introduce the p-adic L-functions of characters of totally real fields with some historical hints and some of their fundamental properties. We will refer to the paper of Dasgupta, Darmon and Pollack [SP11] for more details. In the second section we present a method to compute the special values of these p-adic functions, following A. Lauder and J. Vonk in [LV21]. To conclude, we will compute some examples to illustrate the algorithm.

3.2.1 Historical hints

The concept of p-adic L-functions was first introduced by T. Kubota and H. W. Leopoldt in 1964 with their paper *Eine p-adische Theorie der Zetawerte I* [KL64]. Their main aim was to p-adically interpolate special values of the Riemann zeta function at negative odd integers. After this influential development, the subject of p-adic L-functions garnered tremendous successes through its arithmetic applications. Iwasawa discovered that the invariants of p-adic L-functions are closely related to the arithmetic of towers of cyclotomic fields $\mathbb{Q}(\zeta_{p^n})$. This subject continues to flourish today, and is called *Iwasawa theory.* Its main conjecture, which is now a theorem, is the statement that the Kubota-Leopoldt p-adic L-function are essentially the same as the arithmetic analogue constructed by Iwasawa theory from unit groups in cyclotomic towers.

A more contemporary view on p-adic L-functions was introduced in 1972 by B.Mazur [B72] who systematically developped the theory of p-adic L-functions through the language of p-adic measures. For an excellent treatment on this viewpoint, we refer to the notes of J. Rodrigues and C. Williams in [RW21]. Since we will consider p-adic L-functions of totally real fields other than $\mathbb{Q}$, even this theory does not suffice for the construction, which requires additional deep tools that go far beyond the scope of this thesis, originally developped by Deligne and Ribet [DR80]. We will therefore assume their existence, and focus on their explicit computation, for which it suffices to know their interpolation properties.

3.2.2 Main properties of $L_p(s,\chi)$

In this section we introduce the p-adic L-functions that feature in the statement of the rank one abelian Gross–Stark conjecture.

We start by considering a totally real field F of degree n over $\mathbb{Q}$. Let us consider a character of conductor $\mathfrak{n}$:

$$\chi : \mathrm{Gal}(\overline{F}/F) \to \overline{\mathbb{Q}}^{\times},$$

where $\overline{F}$ is an algebraic closure of F.Since $\mathrm{Gal}(\overline{F}/F)$ is a finite group, the image of χ is a finite group of roots of unity. Since we are about to discuss both p-adic and complex L-series, and we wish to compare their special values at negative integers with each other, we fix a pair of embeddings:

$$\begin{array}{rcl}\overline{\mathbb{Q}} & \hookrightarrow & \mathbb{C}_p, \\ \overline{\mathbb{Q}} & \hookrightarrow & \mathbb{C}.\end{array}$$

Henceforth, algebraic numbers will be considered freely as elements of $\mathbb{C}_p$ or $\mathbb{C}$ according to these embeddings, without further explicit reference.

Remark 3.2.1. We recall that

$$\mathrm{Ker}(\chi) := \{\sigma \in \mathrm{Gal}(\overline{F}/F) |\ \chi(\sigma) = 1\}$$

is a subgroup of $\mathrm{Gal}(\overline{F}/F)$, since χ is a group homomorphism. Consider H, the fixed field of $\mathrm{Ker}(\chi)$ by the Galois correspondence. We note that H is a Galois extension of F and its Galois group is finite and abelian. By class field theory, we may see χ as a function of the ideals of F, by sending $\chi(\mathfrak{c}) = 0$ if $\mathfrak{c}$ is not prime to $\mathfrak{n}$.

We associate a complex L-function to our character χ as we have done in the previous chapter. Consider a finite set of places $\mathcal{S}$ of F containing all the archimedean places. Then we define

$$L_{\mathcal{S}}(s,\chi) := \prod_{\mathfrak{p}\notin\mathcal{S}} (1 - \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s})^{-1}.$$

This series converges for $\Re(s) > 1$ and has a meromorphic continuation to all of $\mathbb{C}$. In addition, Siegel proved in [Sie70] that the value $L_{\mathcal{S}}(n,\chi)$ is algebraic whenever $n \le 0$ is an integer.

To simplify things as much as possible, let us now specialize to the main case of interest. Henceforth, F will denote a real quadratic number field and $\mathcal{H}^+$ its narrow Hilbert class field. Furthermore, we choose a character

$$\chi : \mathfrak{Cl}_F^+ \longrightarrow \overline{\mathbb{Q}}^\times. \tag{3.12}$$

Since we are considering an unramified case, the conductor of χ is $\mathfrak{n} = 1$. In addition, the rational prime p which we will choose for our p-adic studies is a prime p that is inert in F. Since $\mathfrak{p} = (p)$ is principal and it is generated by p, which is a totally positive element of F, we have that $\mathfrak{p}$ is trivial in $\mathfrak{Cl}_F^+$, hence $\chi(\mathfrak{p}) = 1$ due to the fact that χ is a group homomorphism. Consequently, the ideal $\mathfrak{p}$ splits completely in the extension $\mathcal{H}^+/F$. Moreover, $\mathrm{Norm}(\mathfrak{p}) = p^2$.

Now consider a finite extension E of $\mathbb{Q}_p$ containing the values of the character χ, and we let ω be the p-adic Teichmüller character defined in 3.6. Suppose $\mathcal{S}$ contains $\mathfrak{p}$. Deligne and Ribet in [DR80] proved that there exists a unique continuous function E-valued function $L_{\mathcal{S},p}(s,\chi)$ for $s \in \mathbb{Z}_p$ which satisfies the following interpolation property:

$$L_{\mathcal{S},p}(n,\chi) = L_{\mathcal{S}}(n,\chi\omega^n) \tag{3.13}$$

for all integers $n \le 0$.

Remark 3.2.2. The function $L_{\mathcal{S},p}(s,\chi)$ is in fact analytic on $\mathbb{Z}_p$ when χ is nontrivial.

Consider the finite set $\mathcal{R} := \mathcal{S} - \{\mathfrak{p}\}$. By definition of $L_{\mathcal{S}}(s,\chi)$ we obtain:

$$\begin{aligned} L_{\mathcal{S}}(s,\chi) &= \prod_{\mathfrak{p}\notin\mathcal{S}} (1 - \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s})^{-1} \\ &= (1 - \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}) \prod_{\mathfrak{p}\notin\mathcal{R}} (1 - \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s})^{-1} \\ &= (1 - \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}) L_{\mathcal{R}}(s,\chi). \end{aligned}$$

Hence:

$$L_{\mathcal{S}}(s,\chi) = (1 - \chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}) L_{\mathcal{R}}(s,\chi). \tag{3.14}$$

We evaluate this function in $s = 0$ and we obtain that:

$$L_{\mathcal{S}}(0,\chi) = (1-\chi(\mathfrak{p}))L_{\mathcal{R}}(0,\chi). \tag{3.15}$$

This implies that $L_{\mathcal{S}}(0,\chi) = 0$ when $\chi(\mathfrak{p}) = 1$, which is always satisfied under our assumptions. In addition, since $s = 0$ is in our interval of interpolation we can apply the interpolation property 3.13 and we obtain that the p-adic L- function $L_{\mathcal{S},p}(s,\chi)$ vanishes in $s = 0$. This zero, which is caused by a vanishing Euler factor at p, is called an *exceptional zero*.

3.2.3 Computing $L_p(s,\chi)$

In this section we discuss the computation of p-adic L-functions. Two methods exist: one was developped by X.Roblot in [Rob15], and the other by J.Vonk and A.Lauder in [LV21]. While each of these methods has its merits, we will focus on the second one, which relies on an idea of Hecke and Siegel–Klingen and uses the diagonal restriction of Eisenstein series. We do not go into the details, since the theory behind these results goes beyond the scope of this thesis. Finally, we provide a concrete example to illustrate the algorithm.

Recall that we are considering the special case where F is a real quadratic field, and χ is an odd narrow class group character. Consider a prime p which is inert in $F/\mathbb{Q}$ and set $\mathfrak{p} := (p)$. We choose the set

$$\mathcal{S} = \{\infty_1, \infty_2, \mathfrak{p}\}$$

and consider its associated p-adic L-function $L_p(s,\chi) \in \mathbb{Z}_p[\![s]\!]$. We saw that $\mathfrak{p}$ splits completely in $\mathcal{H}^+/F$; this means both that $\mathrm{Norm}(\mathfrak{p}) = p^2$ and that $\chi(\mathfrak{p}) = 1$. Therefore we obtain from the interpolation property of 3.13 that:

$$L_{\mathcal{S},p}(n,\chi) = (1-p^{-2n})L_{\mathcal{R}}(n,\chi) \quad \forall n \le 0,\ (p-1)|n. \tag{3.16}$$

In addition, we saw that $L_p(0,\chi) = 0$ because the Euler factor at p vanishes. As a consequence $\mathrm{ord}_{s=0} L_p(s,\chi) \ge 1$. To investigate the order of vanishing at $s = 0$, we may look at the right side of (3.16) and recall that from Theorem 2.2.2

$$\mathrm{ord}_{s=0} L_{\mathcal{R}}(s,\chi) = r(\chi) = |\{v \in \mathcal{R} : \chi(D_v) = 1\}|,$$

The order of vanishing of the p-adic L-function is one more than the number of infinite places whose decomposition group is in the kernel of χ, and since χ is *odd*, it follows that the complex L-function does not vanish i.e. $\mathrm{ord}_{s=0} L(s,\chi) = 0$. Therefore, $L_p(s,\chi)$ has order of vanishing precisely equal to 1. As a consequence, the quantity $L_p'(0,\chi)$ will be of interest to us.

Remark 3.2.3. We will see in the next section that the quantity $L_p'(0,\chi)$ is related to the p-adic analogue of the Gross–Stark conjecture and to the p-adic logarithm of what will be defined as the Gross–Stark unit.

There are two different methods to compute this quantity. The first method uses the approach of T. Shintani presented in his paper *An evaluation of zeta-functions of totally real algebraic fields at non-positive integers* in 1976 [Shi76]. This method was found by X. Roblot in his paper *Computing p-adic L-functions of totally real number fields* in 2015 [Rob15]. His procedure relies on the so-called *cone decompositions* and on an explicit formula. The second method uses the diagonal restriction of Hilbert modular forms and it was presented by J.Vonk and A. Lauder in their paper *Computing p-adic L-functions of totally real fields* in 2021 [LV21]. This approach uses an old idea of E. Hecke appearing in his 1924 paper [Hec24] and was developed by C.L. Siegel in 1968 [Sie68]; later on, an application to the construction of p-adic L-functions was found by J.-P. Serre in 1972 [Ser73]. On the one hand, this method relies on important and sometimes difficult prerequisites like modular forms and diagonal restrictions. On the other hand, however, the basic idea of this method is quite simple.

Let us briefly explain the second method. The key idea is the construction for any $k \geq 1$ of a formal power series in one variable:

$$f_k(q) = a_0 + a_1 q + \cdots \in \mathbb{Q}_p[\![q]\!],$$

which satisfies the following properties:

- The constant term a_0 equals $L(1-k,\chi)$, whereas the a_n with $n > 0$ are elementary quantities, resembling those appearing in the computations with continuous fractions.
- The power series $f_k(q)$ is the q-expansion of a modular form of weight $2k$ and level one.

This allows one to compute the special value $L(1-k,\chi)$ by computing the coefficients a_n for $n > 0$, and computing the q-expansions of a $\mathbb{Q}$-basis of the space of modular forms of weight $2k$. By expressing $f_k(q)$ as a finite $\mathbb{Q}$-linear combination of these basis elements (which can be done using only the coefficients a_n for $n > 0$) one obtains numerically the value of a_0.

More specifically, the power series $f_k(q)$ are obtained as the diagonal restrictions of Hilbert Eisenstein series, and they have the form

$$f_k(q) = L(1-k,\chi) + 2^2 \sum_{n\geq 1} \left(\sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{Tr}(\nu)=n}} \sum_{\mathfrak{a}|(\nu)\mathfrak{d}} \chi(\mathfrak{a}) \,\mathrm{Norm}(\mathfrak{a})^{k-1} \right) q^n, \tag{3.17}$$

where $\mathfrak{d}$ is the different ideal of $\mathcal{O}_F$ and with $\mathfrak{d}_+$ we indicate the set of totally positive elements contained in $\mathfrak{d}$. The exponent of 2 is equal to $[F : \mathbb{Q}] = 2$. The n-Fourier coefficient a_n of this diagonal restriction may be rewritten as:

$$a_n = 2^2 \sum_{\mathcal{C}\in \mathfrak{Cl}_F^+} \psi(\mathcal{C}) \sum_{(\mathfrak{a},\nu)\in \mathbb{I}(n,\mathcal{C})} \mathrm{Norm}(\mathfrak{a})^{k-1}, \tag{3.18}$$

where we define the index set in the following way:

$$\mathbb{I}(n,\mathcal{C}) := \left\{ (\mathfrak{a},\nu) \in \mathscr{I}_F \times \mathfrak{d}_+^{-1} : \ \mathrm{Tr}(\nu) = n, \quad \mathfrak{a}|(\nu)\mathfrak{d}, \quad [\mathfrak{a}] = \mathcal{C} \right\}, \tag{3.19}$$

where $\mathscr{I}_F$ is the set of integral ideals of F. This index set is still not very easy to compute efficiently. A crucial idea in the algorithm is to find an explicit bijection between $\mathbb{I}(n,\mathcal{C})$ and a certain set $\mathbb{RM}(n,\tau)$ of so-called *augmented* RM points of discriminant $n^2 D$, which can be computed efficiently using continued fractions and reduction theory of indefinite quadratic forms.

Remark 3.2.4. We can observe that this index set is independent of k, and the only thing in $f_k(q)$ which depends on k is the exponent of the norm, hence is very elementary. This will help us in the efficiency of the computation since we have to compute the index set just one time.

Finally, from a large set of special values $L(1-k,\chi)$ for $k \geq 1$ and $(p-1)|(k-1)$, we then compute the power series $L_p(s,\chi)$ by interpolation, modulo some power of p. In summary, the main steps of the algorithm are:

1. Compute the Fourier coefficients a_n with $n > 0$ of the diagonal restriction $f_k(q)$ up to a large enough bound $n < N$.
2. Compute the q-expansions of a $\mathbb{Q}$-rational basis for $M_{2k,1}$, the space of modular forms of weight $2k$ level 1.
3. Recognize the power series $f_k(q)$ as an element of $M_{2k,1}$, and determine the value of its constant term $a_0 = L(1-k,\chi)$.

Then use finite differences to interpolate these special values (multiplied by the corresponding Euler factor at p), to compute $L_p(\chi,s)$ as a power series in $\mathcal{O}[\![s]\!]/(p^m)$ for any p-adic precision m.

3.2.4 Example

We will illustrate this method with an example.

Example 3.1. Let us consider the real quadratic field $F = \mathbb{Q}(\sqrt{3})$. We saw in 2.3.7 that the narrow Hilbert class field of F is $\mathcal{H}^+ = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ and that $\mathfrak{Cl}_F^+ = \mathbb{Z}/2\mathbb{Z}$ and we consider the prime $\mathfrak{p} := (5)$ which splits completely in $\mathcal{H}^+/F$ since 5 is inert in $F/\mathbb{Q}$.

As a consequence, we have only two possibilities for a character defined on $\mathfrak{Cl}_F^+$. On the one hand, we have the trivial character which sends everything to 1, however this character is not odd, hence we can't take it into consideration. The only other possibility is the following character:

$$\begin{array}{rccc} \psi : & \mathfrak{Cl}_F^+ & \longrightarrow & \overline{\mathbb{Q}}^\times \\ & [(\sqrt{3})] & \longmapsto & -1. \end{array}$$

We can observe that $D_F = 12$ and $\psi((\sqrt{12})) = \psi((2\sqrt{3})) = -1$, hence it is odd and it is the character that we will use. We use the algorithm of Lauder–Vonk to compute the diagonal restrictions $f_k(q)$ for the first few values of k:

1. When $k = 1$ we compute to order of precision equal to 20 that:

$$f_1(q) = \mathcal{O}(q^{20}),$$

which was to be expected, since it is a modular form of weight 2 and level 1, and $M_{2,1} = \{0\}$.

2. When $k = 5$, we obtain

$$f_5(q) = L(-4, \psi) - 440q - 225720q^2 - 8660960q^3 + \dots$$

We look at $f_5(q)$ in the space of classical modular forms $M_{10,1}$, which has dimension 1, and we obtain that the constant term is 5/3, hence $L(-4, \psi) = 5/3$.

3. When $k = 9$, we obtain

$$f_9(q) = L(-8, \psi) - 28280q - 3561592440q^2 + \dots$$

We look at $f_9(q)$ in the space of classical modular forms $M_{18,1}$, which has dimension 2. A basis for $M_{18,1}$ is given by:

$$\begin{cases} F_1 & = 1 - 86184q^2 - 84575232q^3 + \dots \\ F_2 & = q - 528q^2 - 4284q^3 + \dots \end{cases} \tag{3.20}$$

Since F_1 does not have q term, we must have that

$$f_9(q) = -28280F_2 + aF_1,$$

for some $a \in \mathbb{Q}$, which we can in turn determine by looking at the coefficient of q^2:

$$f_9(q) + 28280F_2 = L(-8, \psi) - 3576524280q^2 + \dots = aF_1$$

hence $a = 1120465/27$ this means that the constant term of $f_9(q)$ is 1120465/27, hence

$$L(-8, \psi) = \frac{1120465}{27}.$$

Remark 3.2.5. Observe that we used only the coefficients of q and q^2 of $f_k(q)$.In the actual code, the number of coefficients that is computed is equal to the so-called *Sturm bound* which is the minimal number of coefficients needed to determine f_k uniquely in $M_{2k,1}$.

At this point, the chosen prime $\mathfrak{p}$ enters the computation. The Euler factor which appears in the interpolation property is equal to $(1 - p^{-2s}) = (1 - 25^{-s})$ where $s = 1 - k$, and we have that:

$$L_5(1-k,\psi) = (1 - 25^{-1+k})L(1-k,\psi), \quad 4|(k-1)$$

In order to use the interpolation we compute a high number of $L(1-k,\psi)$ values in the same way as before. Therefore, we obtain an high number of $L_5(1-k,\psi)$. We compute a power series, with order of precision equal to 10, which interpolates the values $L_5(1-k,\psi)$. We obtain the following first coefficients of an s-power series $\mathscr{F}(s)$:

$$\begin{aligned}\mathscr{F}(s) = &-(2\cdot 5^9 + \mathcal{O}(5^{10}))s^{11} + \mathcal{O}(5^{10})s^{10} + (2\cdot 5^8 + \mathcal{O}(5^{10}))s^9 + (52\cdot 5^7 + \mathcal{O}(5^{10}))s^8 \\ &- (143\cdot 5^6 + \mathcal{O}(5^{10}))s^7 - (189\cdot 5^6 + \mathcal{O}(5^{10}))s^6 - (6182\cdot 5^4 + \mathcal{O}(5^{10}))s^5 \\ &- (6218\cdot 5^4 + \mathcal{O}(5^{10}))s^4 - (7134\cdot 5^3 + \mathcal{O}(5^{10}))s^3 + (30489\cdot 5^3 + \mathcal{O}(5^{10}))s^2 \\ &- (728698\cdot 5 + \mathcal{O}(5^{10}))s + \mathcal{O}(5^{10}).\end{aligned}$$

This power series is the 5-adic L-function $L_5(s,\psi)$. In addition, we can see that $\mathscr{F}(0) = \mathcal{O}(5^{10})$, hence it is 5-adically very close to 0, which agrees with the fact that $L_5(0,\psi) = 0$. The quantity $L_5'(0,\psi)$ will be connected to a Gross–Stark unit by the p-adic Gross–Stark conjecture presented in the next section.

Remark 3.2.6. We can observe that the coefficients of s are divisible by 5, and the number of time a coefficient is divisible by 5 grow with the growth of the exponent of s. This is positive since we are in the case where the radius of convergence is $\frac{p-2}{p-1} = 3/4$. Hence the coefficient of s^n should be divisible by $\frac{3}{4}n$ power of 5. As a matter of facts, if we look at the coefficient of s^8 we have that it should be divided by $\frac{3}{4}\cdot 8 = 6$ power of 5 and it is indeed divided by 5^7 hence by 5^6.

3.3 The Gross–Stark conjecture

In this section, we will state the p-adic Gross–Stark conjecture with the assumptions that we took in the previous section. There are many advantages of the p-adic Gross–Stark conjecture. On the one hand, as we said in the introduction, this conjecture is an actual theorem. On the other hand, the first derivative of the p-adic L-function is directly computable, using the methods we described above. In addition, we will have more specific information about the Gross–Stark unit, unlike the complex case.

In a nutshell, the Gross–Stark conjecture in our setup predicts that we have:

$$L'_{\mathcal{S},p}(0,\chi) = \mathscr{L}(\chi)L(0,\chi). \tag{3.21}$$

where $\mathcal{S} = \{\infty_1, \infty_2, \mathfrak{p}\}$, and $\mathscr{L}(\chi)$ is a certain invariant attached to χ, which is essentially the p-adic logarithm of a p-unit in the narrow Hilbert class field. This unit is called a *Gross–Stark unit*, and we will define it more precisely now.

Since χ is an odd character, the real quadratic field F cannot have a fundamental unit of norm -1, and therefore all the infinite places of F ramify in the narrow Hilbert class field $\mathcal{H}^+$. Therefore, the field $\mathcal{H}^+$ has no real embeddings, and has $2h_F$ pairs of complex conjugate embeddings, where h_F is the class number of F. Dirichlet's unit theorem now implies that

$$\mathrm{rk}_{\mathbb{Z}}\ \mathcal{O}^\times_{\mathcal{H}^+} = 2h_F - 1.$$

Therefore, the rank of the group of p-units in $\mathcal{H}^+$ is equal to

$$\mathrm{rk}_{\mathbb{Z}}\ \mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}} = 4h_F - 1.$$

Now we extend scalars to E, which we recall is a finite extension of $\mathbb{Q}_p$. Thus we consider $\mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}}\otimes E$, which is a finite E-vector space with the same dimension of $\mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}}$.

Since $\mathrm{Gal}(\mathcal{H}^+/F)$ acts on F, it will acts also on $\mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}}$. In particular we consider the following subspace of $\mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}} \otimes E$:

$$\mathcal{U}_\chi := (\mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}} \otimes E)^{\chi^{-1}} := \{u \in \mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}} \otimes E \mid \sigma u = \chi^{-1}(\sigma)u\}. \tag{3.22}$$

Remark 3.3.1. We can observe that $\mathcal{U}_\chi$ is the subspace characterized by the fact that each element is mapped to a multiple of itself by σ, and the coefficient is exactly $\chi^{-1}(\sigma)$.

In addition, there is a stronger version of the Dirichlet's unit theorem which allow us to predict the dimension of this sub-space. In particular:

$$\dim_E \mathcal{U}_\chi = \#\{v \in \mathcal{S} \mid \chi(v) = 1\}.$$

We have seen in 2.2.2 that $\#\{v \in \mathcal{S} \mid \chi(v) = 1\} = \mathrm{ord}_{s=0} L_{\mathcal{S}}(s,\chi)$. Moreover, since $\mathcal{S}$ and $\mathcal{R}$ differs from each other by a $\mathfrak{p}$ and $\chi(\mathfrak{p}) = 1$, then:

$$\mathrm{ord}_{s=0} L_{\mathcal{S}}(s,\chi) = \mathrm{ord}_{s=0} L_{\mathcal{R}}(s,\chi) + 1,$$

hence:

$$\dim_E \mathcal{U}_\chi = \mathrm{ord}_{s=0} L_{\mathcal{S}}(s,\chi) = \mathrm{ord}_{s=0} L_{\mathcal{R}}(s,\chi) + 1. \tag{3.23}$$

Therefore, we can observe that $\mathcal{U}_\chi$ has dimension one, namely it is a line, if and only if $\mathrm{ord}_{s=0} L_{\mathcal{R}}(s,\chi) = 0 \Rightarrow L_{\mathcal{R}}(0,\chi) \neq 0$. In our study this is the case. On the other hand, if $L_{\mathcal{R}}(0,\chi) \neq 0$ then $\mathcal{U}_\chi$ is a line and we can consider a general nonzero vector u_χ in $\mathcal{U}_\chi$. This element will be our Gross–Stark unit. To normalise it properly and to define $\mathscr{L}(\chi)$, we use the p-adic valuation.

Remark 3.3.2. We know that $\mathfrak{p}$ splits completely in $\mathcal{H}^+/F$, hence $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_{[\mathcal{H}^+:F]}$.

Let us choose a prime $\mathfrak{P}$ of $\mathcal{H}^+$ which lies above $\mathfrak{p}$. This prime $\mathfrak{P}$ induces the following homomorphisms of $\mathbb{Z}$-modules.

$$\mathrm{ord}_{\mathfrak{P}} : \mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}} \longrightarrow \mathbb{Z} \tag{3.24}$$

and

$$\begin{array}{rccc} \mathbf{L}_{\mathfrak{P}} : & \mathcal{O}^\times_{\mathcal{H}^+,\mathcal{S}} & \longrightarrow & \mathbb{Z}_p \\ & u & \longmapsto & \log_p(\mathrm{Norm}_{\mathcal{H}^+_{\mathfrak{P}}/\mathbb{Q}_p}(u)). \end{array}$$

where with $\log_p$ we indicate the p-adic logarithm. With the extension of the scalars to E, we can obtain the same homomorphisms but from $\mathcal{U}_\chi$ to E; we will indicate these homomorphisms in the same way: $\mathrm{ord}_{\mathfrak{P}}$, $\mathbf{L}_{\mathfrak{P}}$. Now we can define the $\mathscr{L}(\chi)$ invariant attached to χ by following R. Greenberg [Gre94] in the following way:

$$\mathscr{L}(\chi) := -\frac{\mathbf{L}_{\mathfrak{P}}(u_\chi)}{\mathrm{ord}_{\mathfrak{P}}(u_\chi)} \in E. \tag{3.25}$$

Remark 3.3.3. This invariant is independent of the choice of u_χ in $\mathcal{U}_\chi$, and of the choice of the prime $\mathfrak{P}$ above $\mathfrak{p}$.

To conclude, we considered the space of $\mathcal{S}$-units of H units, which has a big rank, and the character χ which is acting on it. We saw that there is a specific "line" in that space where the character χ acts in a very specific way, specified equation 3.22. Then, we saw that the p-adic analogue of the Gross–Stark conjecture says that we can find a unit, and it will be precisely a specific unit on that line. Firstly, we said that this unit belongs to that line, but we are not sure where, then we normalized it, so we have a specific generator.

Remark 3.3.4. In conclusion, given the values of $L'_{\mathcal{S},p}(0,\chi\omega)$ and $L_{\mathcal{R}}(0,\chi\omega)$, we can compute a Gross–Stark unit u_χ. We can observe that this pattern is similar to the pattern followed for solving the Pell's equations in Dirichlet's analytic way. As a matter of facts, we studied a special value of complex L-functions and we found that it was related to a logarithm of a unit in a real quadratic field, because the character that we chose there was a quadratic character for $\mathbb{Q}$. Now we upgrade the study, we changed the base field from $\mathbb{Q}$ to a more interesting field such as a real quadratic field and we considered a character of this real quadratic field. Now the first order derivative of the p-adic L-function gives access to the logarithm of a p-unit in the narrow Hilbert class field.

To conclude, we show an explicit computation of a Gross–Stark unit.

Example 3.2. Let $F = \mathbb{Q}(\sqrt{321})$. We have that $D_F = 321$ and $\mathfrak{Cl}_F^+ = \mathbb{Z}/6\mathbb{Z}$. We choose $\mathfrak{p} := (7)$ since 7 is inert in $F/\mathbb{Q}$. The space of odd functions on the $\mathfrak{Cl}_F^+$ is spanned by the three following functions χ_1, χ_2, χ_3.

$$\begin{aligned} \chi_1 &= 1_{[\mathcal{O}_F]} - 1_{[\mathfrak{d}]} \\ \chi_2 &= 1_{[\mathfrak{a}]} - 1_{[\mathfrak{a}\mathfrak{d}]} \\ \chi_3 &= 1_{[\mathfrak{b}]} - 1_{[\mathfrak{b}\mathfrak{d}]} \end{aligned}$$

where $\mathfrak{a} = (4, (-15 + \sqrt{321})/2)$ and $\mathfrak{b} = (2, (-15 + \sqrt{321})/2)$.

To obtain a 7-unit in the narrow Hilbert class field $\mathcal{H}^+$ of F we do the following steps.

1. We compute $L_7(T, \chi_1)$ where $T = (1 + 7)^s - 1$ with the algorithm of Lauder–Vonk of section 3.2.3 to find:

$$L_7(T, \chi_1) \equiv (3 + \mathcal{O}(7^2))T^3 - (10 + \mathcal{O}(7^3))T^2 + (913 + \mathcal{O}(7^4))T \pmod{T^4}$$

2. We obtain a power series which exhibits $L_7(0, \chi_1) = 0$ with variable s.

3. We obtain $L_7'(0, \chi_1)$.

In reality we did the above computation to precision $O(7^{50})$. We found that $L_7'(0, \chi_1)$ is equal up to the computed precision to $\log_7(u)$, where u satisfies:

$$7^{16}u^6 - 20976 \cdot 7^8 u^5 - 270624 \cdot 7^4 u^4 + 526859689u^3 + 270624u^2 - 20976u^2 + 7^4 = 0.$$

To conclude, u is a 7-unit in $\mathcal{H}^+$ of F and $u \in \mathcal{O}_{\mathcal{H}^+}[1/7]^\times$.

Remark 3.3.5. Observe that in the first section we start from an equation, the Pell's equation, and we end up in finding a unit, which was the fundamental unit of $\mathbb{Z}[\sqrt{d}]$ of norm 1. At the end of this thesis with this last example, instead, we start from a unit, which is a Gross–Stark unit, and we find an equation satisfied by it. We reversed the process.

Appendix A

Background in algebraic number theory

In this section, we will recall some basic concepts of algebraic number theory. The proofs of these results could be found in [Mar18; Ste21].

A.1 Number Fields

Definition A.1 (Number field)**.** A number field is a subfield of $\mathbb{C}$ having a finite degree over $\mathbb{Q}$.

In addition to that, we know that every such field has the form $\mathbb{Q}[\alpha]$ for some algebraic number $\alpha \in \mathbb{C}$, from the Galois Theory on the subfield of $\mathbb{C}$.

Definition A.2 (Algebraic integer)**.** A complex number is an algebraic integer if and only if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Theorem A.1.1. *The only algebraic integers in $\mathbb{Q}$ are the ordinary integers.*

In particular, we will work with a specific class of number fields consisting in the quadratic fields.

Definition A.3 (Quadratic field)**.** A quadratic field K is a number field of degree two over $\mathbb{Q}$.

As a consequence, K is in the form $K = \mathbb{Q}[\sqrt{m}]$ for some $m \in \mathbb{Z}$ with m not a perfect square.

Definition A.4. We call *real quadratic field* the $\mathbb{Q}[\sqrt{m}]$ for $m > 0$ and *imaginary quadratic field* the $\mathbb{Q}[\sqrt{m}]$ for $m < 0$.

We recall some basics results for quadratic number fields.

Corollary A.1.2. *Let m be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$ is:*

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \ if \ m \equiv 2, 3 \pmod 4.$$
$$\{\frac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\} \ if \ m \equiv 1 \pmod 4.$$

We will study now the ring of integers of a number field K; let us denote by $\mathbb{A}$ the set of algebraic integers in $\mathbb{C}$.

Definition A.5 (Ring of integral elements of K)**.** We call $\mathcal{O}_K := \mathbb{A} \cap K$ the *number ring* corresponding to K. It is the ring of all integral elements contained in K.

We recall the definition of *norm*.

Definition A.6 (Norm)**.** Let K be a number field and let $\sigma_1, \dots, \sigma_n$ be the embeddings of K in $\mathbb{C}$, where $n = [K : \mathbb{Q}]$. For each $\alpha \in K$ we define the *norm* of *alpha* as:

$$\mathrm{Norm}(\alpha) = \sigma_1(\alpha)\dots\sigma_n(\alpha).$$

In particular, for the real quadratic field $K = \mathbb{Q}[\sqrt{m}]$ we have that:

$$\mathrm{Norm}(a + b\sqrt{m}) = a^2 - mb^2,$$

for $a, b \in \mathbb{Q}$.
We recall also the definition of the discriminant.

Definition A.7 (Discriminant)**.** Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \dots, \sigma_n$ denote the n embeddings of K in $\mathbb{C}$. For any n-tuple of elements $\alpha_1, \dots, \alpha_n \in K$, we define the *discriminant* of $\alpha_1, \dots, \alpha_n$ to be:

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = |\sigma_i(\alpha_j)|^2,$$

i.e. the square of the determinant of the matrix having $\sigma_i(\alpha_j)$ in the i^{th} row, j^{th} column.

We underline that the discriminant is independent from the ordering of the σ_i and the ordering of the α_j.
In addition, by using the discriminant we can determine the additive structure of $\mathcal{O}_K$.

Theorem A.1.3. *$\mathcal{O}_K$ is a free abelian group of rank n.*

This means that $\mathcal{O}_K$ has a basis over $\mathbb{Z}$, namely, there exist $\beta_1, \dots, \beta_n \in \mathcal{O}_K$ s.t. every $\alpha \in \mathcal{O}_K$ is uniquely representable in the form:

$$a_1\beta_1 + \dots + a_n\beta_n, \quad a_i \in \mathbb{Z}.$$

Definition A.8 (Integral basis)**.** We call $\{\beta_1, \dots, \beta_n\}$ an *integral basis* for $\mathcal{O}_K$.

Remark A.1.4. We can observe that $\{\beta_1, \dots, \beta_n\}$ is a basis for K over $\mathbb{Q}$ too.

Theorem A.1.5. *In the quadratic number field $K = \mathbb{Q}[\sqrt{m}]$, with m squarefree, an integral basis for $\mathcal{O}_K = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$ consist of:*

$$\{1, m\} \quad if\ m \equiv 2, 3 \pmod 4, \tag{A.1}$$

$$\{1, \frac{1+\sqrt{m}}{2}\} \quad if\ m \equiv 1 \pmod 4. \tag{A.2}$$

hence:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & if\ m \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & if\ m \equiv 1 \pmod 4. \end{cases}$$

We recall that the discriminant of an integral basis can be regarded as an invariant of the ring $\mathcal{O}_K$, and we can denote it as $\mathrm{disc}(\mathcal{O}_K)$.
:

Theorem A.1.6. *Let $K = \mathbb{Q}[\sqrt{m}]$, with m squarefree we have:*

$$\mathrm{disc}(\mathcal{O}_K) = \begin{cases} \mathrm{disc}(\sqrt{m}) = 4m & if\ m \equiv 2,3 \pmod 4, \\ \mathrm{disc}(\frac{1+\sqrt{m}}{2}) = m & if\ m \equiv 1 \pmod 4. \end{cases}$$

A.2 Dirichlet's unit theorem

In this section we will study the units $\mathcal{O}_K$ of a number ring K.

Definition A.9 (Unit)**.** A *unit* of a ring R is any element u which has a multiplicative inverse in R.

Theorem A.2.1. *The units in $\mathcal{O}_K$ are all the elements having norm ± 1.*

Proof. Since the norm is multiplicative, we can conclude that every unit has norm ± 1. On the other hand, if α is an algebraic integer having norm ± 1 and every conjugate of α is an algebraic integer, then $\frac{1}{\alpha}$ is also an algebraic integer, hence α is a unit. □

Definition A.10 (Multiplicative group of units of K)**.** Let us denote by $\mathcal{O}_K^\times$ the multiplicative group of units of the number ring $\mathcal{O}_K$.

We state the *Dirichlet's unit theorem.*

Theorem A.2.2 (Dirichlet's unit theorem)**.** *Let $\mathcal{O}_K^\times$ be the group of units of the number ring $\mathcal{O}_K = \mathbb{A} \cap K$. Let r and $2s$ denote the number of real and non-real embedding of K in $\mathbb{C}$. Then $\mathcal{O}_K^\times$ is the direct product $W \times V$ where W is a finite cyclic group consisting of the roots of 1 in K, and V is a free abelian group of rank $r + s - 1$.*

More explicitly, the theorem states that there exists a finite set $\{\eta_1, \dots, \eta_{r+s-1}\}$ whose elements are called *fundamental units* such that we have:

$$\mathcal{O}_K^\times = \mu_K \times \langle \eta_1 \rangle \times \cdots \times \langle \eta_{r+s-1} \rangle$$

Where μ_k is the group of roots of unit of K. Such system of fundamental units, which forms a $\mathbb{Z}$-basis for $\mathcal{O}_K^\times / \mu_k$, is unique up to coordinate transformations and multiplication by roots of unity.

Remark A.2.3. We have that $r + 2s = [K : \mathbb{Q}]$.

A.3 Prime decomposition in a number ring

We consider the number field K with $\mathbb{Q} \subset K$, and $\mathcal{O}_K = \mathbb{A} \cap K$. We recall that the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$ and the prime ideals of $\mathbb{Z}$ are the ideals of the form $p\mathbb{Z}$ where p is prime.

Definition A.11. Let p be a prime in $\mathbb{Z}$ and $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. If

$$\mathfrak{p} \cap \mathbb{Z} = (p),$$

we will say that $\mathfrak{p}$ *lies over* p, or p *lies under* $\mathfrak{p}$.

Theorem A.3.1. *Every prime $\mathfrak{p}$ of $\mathcal{O}_K$ lies over a unique prime p of $\mathbb{Z}$; every prime p of $\mathbb{Z}$ lies under at least one prime $\mathfrak{p}$ of $\mathcal{O}_K$.*

Definition A.12. The primes lying over a given p are the ones that occur in the prime decomposition of $p\mathcal{O}_K$. The exponents with which they occur are called the *ramification indices.* Thus, if $\mathfrak{p}^e$ is the exact power of $\mathfrak{p}$ dividing $p\mathcal{O}_K$, then e is the ramification index of $\mathfrak{p}$ over p denoted by $e(\mathfrak{p}|p)$.

Definition A.13. We call $\mathbb{Z}/p$ and $\mathcal{O}_K/\mathfrak{p}$ the residue fields associated with p and $\mathfrak{p}$. We know that $\mathcal{O}_K/\mathfrak{p}$ is an extension of finite degree over $\mathbb{Z}/p$: let f be the degree of this extension. Then f is called the *inertial degree* of $\mathfrak{p}$ over p and is denoted by $f(\mathfrak{p}|p)$.

Proposition A.3.2. *The ramification index e and the inertial degree f are multiplicative in towers.*

Let us state the following theorem in the generic case, where M and L are number fields with $M \subset L$, and let $O_M = \mathbb{A} \cap M$, $O_L = \mathbb{A} \cap L$.

Theorem A.3.3. *Let n be the degree of L over M and let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the primes of O_L lying over a prime P of O_M. Denote by $e_1, \dots, e_r$ and $f_1, \dots, f_r$ the corresponding ramification indices and inertial degrees. Then:*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Corollary A.3.4. *If $M = \mathbb{Q}$, then, $O_M = \mathbb{Z}$ and we have that:*

$$pO_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

hence:

$$\mathrm{Norm}(pO_L) = \prod_{i=1}^{r} \mathrm{Norm}(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{r} p_i^{e_i f_i}$$

and we know that $\mathrm{Norm}(pS) = p^2$

Let $L = \mathbb{Q}[\sqrt{d}]$ be a real quadratic extension of $\mathbb{Q}$, while $M = \mathbb{Q}$. As a consequence $[L : M] = 2$. This means that given a certain p in $\mathbb{Z}$ we have only three possibilities for the primes lying over it in $K := \mathbb{Q}[\sqrt{d}]$.

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2, & f(\mathfrak{p}|p) = 1 \\ \mathfrak{p}, & f(\mathfrak{p}|p) = 2 \\ \mathfrak{p}_1\mathfrak{p}_2. & f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1 \end{cases} \tag{A.3}$$

Definition A.14. In the first case we say that p is *ramified* in $\mathcal{O}_K$. In the second case we say that p is *inert* in $\mathcal{O}_K$. In the third case, we say that p is *split* in $\mathcal{O}_K$.

A.4 Valuations

In this chapter we study the valuations.

Definition A.15 (Valuation)**.** A valuation on a field K is a function $\phi : K \longrightarrow \mathbb{R}_{\geq 0}$ satisfying:

1. $\phi(x) = 0$ if and only if $x = 0$;
2. $\phi(xy) = \phi(x)\phi(y)$ for $x, y \in K$;
3. there exists $C \in \mathbb{R}> 0$ such that $\phi(x + y) \leq C \max\{\phi(x), \phi(y)\}$ for all $x, y \in K$.

Theorem A.4.1. *A non-trivial valuation on $\mathbb{Q}$ is either equivalent to the p-adic valuation ϕ_p : $\mathbb{Q} \longrightarrow \mathbb{R}$ given by $\phi_p(x) = p^{-\mathrm{ord}_p(x)}$ for a prime number p, or to the ordinary absolute value on $\mathbb{Q}$ given by $\phi_\infty(x) = |x|$.*

In addition, for every non-archimedean valuation ϕ on a field K we can define the *valuation ring.*

Definition A.16 (Valuation ring)**.** Let K be a field and ϕ a non-archimedean valuation on it. The valuation ring of ϕ is the ring:

$$A = \{x \in K \mid \phi(x) \leq 1\}. \tag{A.4}$$

Proposition A.4.2. *The valuation ring of a non-archimedean valuation ϕ on a field K has the following properties:*

1. *K=Frac(A);*
2. *for every $x \in K^\times$ we have that $x \in A$ or $x^{-1} \in A$;*
3. *A is an integrally closed subring of K*
4. *A is a local ring with unit group $A^\times = \{x \in K \mid \phi(x) = 1\}$ and maximal ideal $\mathfrak{m} = \{x \in K \mid \phi(x) < 1\}$.*

Definition A.17 (Resideu class field)**.** We call the residue class field of ϕ the quotient $k = A/\mathfrak{m}$.

We can complete a valued field in order to obtain a complete field, namely a field where every Cauchy sequence in it has a limit in it.

Theorem A.4.3. *Let K be a valued field and let ϕ be its valuation. There exists a field extension $K \subset K_\phi$ and an extension of ϕ to a valuation on K_ϕ such that K_ϕ is a complete valued field containing K as a dense subfield.*

Therefore, we can define $\mathbb{Q}_p$.

Definition A.18 ($\mathbb{Q}_p$)**.** We define the p-adic number field $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ under the p-adic valuation ϕ_p. Its valuation ring is called $\mathbb{Z}_p$ and its residue class field is the finite field $\mathbb{F}_p$.

We recall that every p-adic number have a unique p-adic expansion. As a matter of facts, if we set $\pi_i = p^i$ and $S = \{0, 1, \ldots, p-1\}$ for $K = \mathbb{Q}_p$ in the theorem (vedere se citare il teorema) then:

$$x = \sum_{i \gg -\infty}^{\infty} a_i p^i, \tag{A.5}$$

with $a_i \in S$, where with $i \gg \infty$ we indicate that there are only finitely many $i < 0$ with $a_i \neq 0$.
In order to define $\mathbb{C}_p$ we have to consider the algebraic closure of $\mathbb{Q}_p$ and we refer to it as $\overline{\mathbb{Q}}_p$. First of all, we observe that $[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \infty$. In addition, it can be shown that $\overline{\mathbb{Q}}_p$ is not complete with respect to the unique extension of the p-adic valuation.

Definition A.19 ($\mathbb{C}_p$)**.** We define $\mathbb{C}_p$ as the completion of $\overline{\mathbb{Q}}_p$ with respect to the valuation mentioned before.

Proposition A.4.4. *The field $\mathbb{C}_p$ is algebraically closed.*

Proof. We will prove it by contradictions. Let us consider the following polynomial $f(x) : \prod_{i=1}^n (x - \alpha_i) \in \mathbb{C}_p[x]$ and let us suppose that $\alpha = \alpha_1$ is one of its roots in the algebraic closure of $\mathbb{C}_p$. Since $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$, if we consider the polynomial $g(x) = \prod_{i=1}^n (x - \beta_i) \in \overline{\mathbb{Q}}_p[x]$ of degree n whose coefficients are p-adically very close to those of $f(x)$, then $g(\alpha)$has to be very small, hence $|\alpha - \beta_i|$ has to be very small for every $i \leq n$. As a consequence, if we choose $g(x)$ very close to $f(x)$ we will obtain that $|\alpha - \beta_i| < |\alpha - \alpha_i|$ for all $1 \leq i \leq n$. This implies from the Krasner's lemma that $\mathbb{C}_p(\alpha) \subseteq \mathbb{C}_p(\beta_i)$ for all $1 \leq i \leq n$. However, $\beta_i \in \overline{\mathbb{Q}_p}$ since the polynomial $g(x)$ is necessarily defined over a finite extension of $\mathbb{Q}_p$. This implies that $\mathbb{C}_p(\alpha) = \mathbb{C}$, hence $\alpha \in \mathbb{C}_p$, but this is absurd. Therefore, $\mathbb{C}_p$ is agebraically closed. □

A.5 Decomposition group

Let us consider a valuation ϕ on a field K and ψ an extension of ϕ to a finite Galois extension L of K.

We recall that the completion L_ψ is the compositum of its subfields L and K_ϕ and L_ψ/K_ϕ is a finite Galois extension from Galois theory.

Definition A.20 (Decomposition group)**.** $D_\psi := \mathrm{Gal}(L_\psi/K_\phi)$ is the *decomposition group* of ψ in L/K and it can be seen as a subgroup of $\mathrm{Gal}(L/K)$ in the following way:

$$D_\psi = \{\sigma \in \mathrm{Gal}(L/K) |\ \psi(\sigma(x)) = \psi(x)\ \forall x \in L\}. \tag{A.6}$$

One of the most interesting things is that under certain conditions all the decomposition groups are conjugate in $\mathrm{Gal}(L/K)$.

Proposition A.5.1. *Let L/K be a finite Galois extension with group G and X the set of extensions of a valuation ϕ on K to L. Then G acts transitively on X, and the stabilizer $D_\phi \subset G$ of $\psi \in X$ is the decomposition group of ψ in L/K. All decomposition groups D_ψ of $\psi \in X$ are conjugate in G.*

In particular we have the following proposition.

Proposition A.5.2. *If the extension L/K is a finite abelian Galois extension, all decomposition groups D_ψ for $\psi \in X$ coincide.*

In that case, we can speak of the decomposition group D_ϕ of ϕ in L/K.

Appendix B

Background in analytic number theory

In this section we will recall some basic concepts of analytic number theory. The proofs of these results could be found in [Von21; Jan21].

B.1 Dirichlet Characters

In this section we will present the Dirichlet Characters.

Definition B.1 (Dirichel character)**.** A *Dirichlet character* is a multiplicative homomorphism:

$$\chi : (\mathbb{Z}/n\mathbb{Z})^{\times} \to \mathbb{C}^{\times}.$$

where $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\overline{a} \mid gcd(a, n) = 1\}$.

Remark B.1.1. We can observe that if $n|m$, then χ induces a homomorphism $(\mathbb{Z}/m\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ by composition with the natural map $(\mathbb{Z}/m\mathbb{Z})^{\times} \to (\mathbb{Z}/n\mathbb{Z})^{\times}$. Therefore, we could regard χ as being defined *mod m* or *mod n*, since both are essentially the same map.

Definition B.2 (Trivial character)**.** Let χ be a Dirichlet character. If $\chi(a) = 1$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then we call it the *trivial character* modulo n.

Let χ be a character mod n and d a positive divisor of n.

Definition B.3. We say that χ is induced by a character χ' mod d if

$$\chi(a) = \chi'(a) \quad for\ every\ a \in (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

Definition B.4 (Conductor of a character)**.** We define the *conductor* of χ as the smallest positive divisor d of n such that χ is induced by a character mod d. We indicate this conductor with f_{χ}.

Definition B.5 (Primitive character)**.** A character χ is called *primitive* if there is no divisor $d < n$ of n such that χ is induced by a character mod d. In other words, χ has conductor n i.e. it is defined modulo its conductor.

We define the product of two Dirichlet characters.

Definition B.6 (Product of characters)**.** Let χ and ψ be Dirichlet characters of conductors f_{χ} and f_{ψ}. We define $\chi\psi$ as follows. Considered the homomorphism:

$$\varphi : (\mathbb{Z}/lcm(f_{\chi}, f_{\psi})\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$$

defined by $\varphi(a) = \chi(a)\psi(a)$. Then $\chi\psi$ is the primitive character associated to φ.

Remark B.1.2. Observe that if $gdc(f_{\chi}, f_{\psi}) = 1$ then $f_{\chi\psi} = f_{\chi} f_{\psi}$.

We define an odd character and an even character.

Definition B.7. We define a Dirichlet character χ to be *even* if $\chi(-1) = 1$.
We define a Dirichlet character χ to be *odd* if $\chi(-1) = -1$.

We conclude this section with the following theorem.

Theorem B.1.3. *The number of Dirichlet characters mod n are $\varphi(n)$.*

B.2 Dedekind zeta function

The Dedekind zeta-function ζ_K of a number field K is a complex analytic function that encodes a lot of fundamental information on the number field.

First of all, if $K = \mathbb{Q}$ the Dedekind zeta-function is the *Riemann zeta function.*

Definition B.8 (Riemann zeta function)**.** The *Riemann zeta function* is a complex analytic function which is defined on the complex right half-plane $\Re(t) > 1$ by the formula:

$$\zeta(t) = \sum_{n=1}^{\infty} n^{-t}.$$

If we consider the generic case where K is a number field, we have the following definition.

Definition B.9 (Dedekind zeta-function)**.** The *Dedekind zeta-function* ζ_K of a number field K is a complex analytic function defined as:

$$\zeta_K(t) = \sum_{I \neq 0} (\text{Norm}(I))^{-t}.$$

where the sum ranges over all non-zero ideals $I \subset \mathcal{O}_K$ of the ring of integers $\mathcal{O}_K$ of K.

We indicate with $\text{Norm}(I)$ the absolute norm of I, which is the index $[\mathcal{O}_K : I]$, i.e. the cardinality of $\mathcal{O}_K/I$.

We recall that:

Theorem B.2.1. *Every number ring is a Dedekind domain.*

Corollary B.2.2. *The ideal classes in a Dedekind domain form a group.*

Theorem B.2.3. *Every ideal in a Dedekind domain R is uniquely representable as a product of prime ideals.*

Corollary B.2.4. *The ideals in a number ring factor uniquely into prime ideals.*

We recall that the convergence properties of the sum are just as for the Riemann zeta function, and it has a representation as an Euler product over prime ideals, as follows.

Theorem B.2.5. *Let $t \in \mathbb{C}$ be a complex number with $\Re(t) > 1$. Then we have an identity:*

$$\zeta_K(t) = \sum_{I \neq 0} (\text{Norm}(I))^{-t} = \prod_{\mathfrak{p}} (1 - \text{Norm}(\mathfrak{p})^{-t})^{-1}.$$

in which the sum over $I \neq 0$ and the Euler product over $\mathfrak{p}$ are absolutely convergent. The function ζ_K is a holomorphic function without zeroes in the half plane $\Re(t) > 1$.

B.3 Class number formula

We recall that the sum in the definition of the Dedekind zeta function B.9 diverges for $t = 1$ it does have a meromorphic continuation to the left of the half space $\Re(t) > 1$ such that $t = 1$ becomes a simple pole for this extended function.

Theorem B.3.1 (Class number formula)**.** *Let K be a number field of degree n with r real and $2s$ complex embeddings. Then the zeta-function ζ_K of K admits a meromorphic extension to the half-plane $\Re(t) > 1 - 1/n$. It is holomorphic except for a single pole at $t = 1$ with residue:*

$$\mathrm{res}_{t=1}\,\zeta_K(t) = \frac{2^r(2\pi)^s h_K R_K}{w_K\sqrt{D_K}}. \tag{B.1}$$

Where h_K is the class number of K, R_K is the regulator of K, w_K is the number of roots of unit in K and D_K is the discriminant of K.

We recall two invariant of K.

Definition B.10 (Class number)**.** The *class number* h_K of a number field K is the order of the ideal class group of its ring of integers $\mathcal{O}_K$.

Remark B.3.2. A number field K has class number 1 if and only if $\mathcal{O}_K$ is a principal ideal domain and thus a unique factorization domain.

Definition B.11 (Regulator of K)**.** The *regulator* of K is obtained by choosing a system $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ of generators for the units of K modulo torsion and by taking the determinant of an $(r+s-1)\times(r+s-1)$ matrix of logarithms of these units relative to any set $\sigma_1, \dots, \sigma_{r+s-1}$ of distinct embeddings of K into $\mathbb{R}$ or $\mathbb{C}$:

$$R_K := \det(\log|\sigma_j(\varepsilon_i)|)_{1\le i,j\le r+s-1}.$$

B.4 Dirichlet L-series

In this section, we will present the Dirichlet L-functions.

Definition B.12 (Dirichlet series)**.** Let f be an arithmetic function i.e. a function $f : \mathbb{Z}_{>0} \to \mathbb{C}$. The *Dirichlet series* associated to f is:

$$L_f(t) = \sum_{n=1}^{\infty} f(n)n^{-t},$$

where t is a complex variable.

Theorem B.4.1. *There exists a number $\sigma_0(f)$ with $-\infty \le \sigma_0(f) \le \infty$ such that $L_f(t)$ converges for all $t \in \mathbb{C}$ with $\Re(t) > \sigma_0(f)$ and diverges for all $t \in \mathbb{C}$ with $\Re(t) < \sigma_0(f)$.*
Moreover, if $\sigma_0(f) < \infty$, then for $t \in \mathbb{C}$ with $\Re(t) > \sigma_0(f)$ the function L_f is analytic, and:

$$L_f^{(k)}(t) = \sum_{n=1}^{\infty} f(n)(-\log n)^k n^{-t} \quad for\ k \ge 1.$$

Definition B.13 (Abscissa of convergence)**.** The number $\sigma_0(f)$ is called the *abscissa of convergence* of L_f.

We recall two important kinds of arithmetic functions.

Definition B.14 (Multiplicative function)**.** A *multiplicative* function is an arithmetic function f s.t. $f \not\equiv 0$ and $f(nm) = f(m)f(n)$ for all positive integers with $\gcd(m,n) = 1$.

A *strongly multiplicative* function is an arithmetic function f with the property that $f \not\equiv 0$ and $f(nm) = f(m)f(n)$ for all integers m, n.

Theorem B.4.2. *Let f be a multiplicative function. Let $t \in \mathbb{C}$ be such that $L_f(t) = \sum_{n=1}^{\infty} f(n)n^{-t}$ converges absolutely. Then:*

$$L_f(t) = \prod_p \left(\sum_{j=0}^{\infty} f(p^j)p^{-jt} \right).$$

Further, $L_f(t) \neq 0$ as soon as $\sum_{j=0}^{\infty} f(p^j)p^{-jt} \neq 0$ for every prime p.

Corollary B.4.3. *Let f be a strongly multiplicative function. Let $t \in \mathbb{C}$ be such that $L_f(t)$ converges absolutely. Then*

$$L_f(t) = \prod_p \frac{1}{1 - f(p)p^{-s}}.$$

Further $L_f(t) \neq 0$.

Remark B.4.4. For $t \in \mathbb{C}$ with $\Re(t) > 1$ we have:

$$\zeta(t) = \sum_{n=1}^{\infty} n^{-t} = \prod_p (1 - p^{-t})^{-1}.$$

Now, we will be focusing on the Dirichlet characters. We recall that a Dirichlet character can be seen as an arithmetic function.

Definition B.15. The *L-series* of a Dirichlet character χ modulo n is defined by:

$$L(t, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-t}, \quad \Re(t) > 1.$$

Remark B.4.5. We can view $\zeta(t) = \sum_{n=1}^{\infty} n^{-t}$ as the L-series of the principal character modulo 1.

Since χ is a strongly multiplicative arithmetic function, we have the following theorem.

Theorem B.4.6. *The L-series of a Dirichlet character χ modulo n has the following convergent Euler product expansion:*

$$L(t, \chi) = \prod_p (1 - \chi(p) p^{-t})^{-1}.$$

Bibliography

[AWe84] A.Weil. *Number theory: an approach through history.* Birkhauser, Boston, 1984.

[Alp85] Roger C. Alperin. "Sur les fonctions continues p-adic". In: *The American Mathematical Monthly* 92.8 (1985), pp. 576–578.

[B72] Masur B. "Analyse p-adique". In: *Bourbaki report (unpublished)* (1972).

[Bre13] Paul T. Young Brett A. Tangedal. "Explicit computation of Gross–Stark units over real quadratic fields". In: *Journal of Number Theory* 133 (2013), pp. 1045–1061.

[DR11] H. Darmon and V. Rotger. *Algebraic cycles and Stark-Heegner points.* Notes, 2011, pp. 7–10.

[Das99] Samit Dasgupta. "Stark's Conjectures". In: *Harvard University Cambridge, Massachusetts* (1999), p. 32.

[DR80] P. Deligne and K. A. Ribet. "Values of abelian L-functions at negative integers over totally real fields". In: *Invent. Math* 59 (1980), pp. 227–286.

[Die44] J. Dieudonné. "Sur les fonctions continues p-adic". In: *Bull. Sci. Math.* 68 (1944), pp. 79–95.

[Dir80] G. Lejeune Dirichlet. "Sur la maniére de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires." In: *HJournal für die reine und angewandte Mathematik* 1837 (1880), pp. 286–290.

[Eul70] L. Euler. "Vollständige Anleitung zur Algebra". In: *Zweyter Theil, Kays. Acad. der Wissenschaften, St. Petersburg* (1770). Reprinted in Opera mathematica, ser. I, vol. 1, Teubner, Leipzig, 1911; translated as Elements of algebra, Springer, New York, 1984.

[Gra73] J.-L. de la Grange. "Solution d'un problème d'arithmétique". In: *Mélanges de philosophie et de math. de la Société Royale de Turin 4* (1773). This paper was written and submitted for publication in 1768, and it appeared in 1773. Reprinted in Lagrange's *OEuvres*, vol. I, Gauthier-Villars, Paris, 1867, 669–731.

[Gre94] R. Greenberg. "Trivial zeros of p-adic L-functions, in p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991)". In: *Contemp. Math.* 165 (1994), pp. 149–174.

[Hec24] E. Hecke. "Analytische Funktionen und Algebraische Zahlen". In: *Abhandlungen aus dem Mathematischen Universitat Bd.* 3 (1924), pp. 213–236.

[Jan21] Evertse Jan-Hendrik. "Notes of the course: Analytic Number Theory". In: (2021).

[JR08] H.W. Lenstra JR. "Solving the Pell equation". In: *Algorithmic Number Theory MSRI Publications* 44 (2008).

[KA80] B. Krumbiegel and A. Amthor. ""Das Problema Bovinum des Archimedes"". In: *Historisch-literarische Abteilung der Zeitschrift für Mathematik und Physik* 25 (1880), pp. 121–136, 153–171.

[KL64] P. Kubota and H.W. Leopoldt. "Eine p-adische Theorie der Zetawerte I". In: *J. Reine Angew. Math* 214/215 (1964), pp. 328–339.

[LV21] A. Lauder and J. Vonk. "Computing p-adic L-functions of totally real fields". In: (2021).

[Mar18] Daniel A. Marcus. *Number Fields. Second edition.* Springer, 2018.

[Rob15] X.-F. Roblot. "Computing p-adic L-functions of totally real number fields". In: *Math. Comp.* 84.292 (2015), pp. 831–874.

[RW21] J. Rodrigues and C. Williams. "An introduction to p-adic l-functions". In: *Notes from a TCC Course* (2021).

[SP11] Henri Darmon Samit Dasgupta and Robert Pollack. "Hilbert modular forms and the Gross-Stark conjecture". In: *Annals of Mathematics* 174 (2011), pp. 439–484.

[Ser73] J.-P. Serre. "Formes modulaires et fonctions zeta p-adiques". In: *Lecture Notes in Math.Springer, Berlin* 350 (1973).

[Shi76] T. Shintani. "An evaluation of zeta-functions of totally real algebraic fields at non-positive integers". In: *J. Fac. Sci., Univ. Tokyo, Sect. IA* 23 (1976), pp. 393–417.

[Sie70] C. L. Siegel. "Uber die Fourierschen Koeffizienten von Modulformen," in: *Nachr. Akad. Wiss. Gottingen Math.-Phys. Kl. Ill* 1970 (1970), pp. 15–56.

[Sie68] C.L. Siegel. "Berechnung von Zetafunktionen an ganzzahlingen Stellen". In: *Nachr. Akad. Wiss. Göttingen, Math.-Phys. Klasse* 2 (1968), pp. 7–38.

[Sta71] H.M. Stark. "Values of L-functions at $s = 1$. I. L-functions for quadratic forms." In: *Advances in Mathematics* 7.3 (1971), pp. 301–343.

[Sta75a] H.M. Stark. "L-functions at $s = 1$. II. Artin L-functions with rational characters." In: *Advances in Mathematics* 17.1 (1975), pp. 60–92.

[Sta75b] H.M. Stark. "L-Functions at s = 1. II. Artin L-functions with Rational Characters". In: *Adv. Math* 22 (1975), pp. 60–92.

[Sta76] H.M. Stark. "L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem." In: *Advances in Mathematics* 22.1 (1976), pp. 64–84.

[Sta80] H.M. Stark. "L-functions at $s = 1$. IV. First derivatives at $s = 0$". In: *Advances in Mathematics* 35.3 (1980), pp. 197–235.

[Ste21] P. Stevenhagen. "VOORTGEZETTE GETALTHEORIE". In: *Notes of the course: Topics in Number Theory* (2021).

[Tat84] J. T. Tate. "Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$". In: *Birkhäuse,Boston* (1984).

[Von21] Jan Vonk. "Topics in Number Theory: p-Adic L-functions". In: *Notes of the course: Topics in Number Theory* (2021).

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics.* Springer-Verlag, New York, 1997.