A p-adic analogue of the class number formula

A master thesis in Mathematics for the ALGANT program.

Academic year 2017-2018

Student: *Alessandro Danelon*

Advisor: *Massimo Bertolini*

Leiden University
Wiskunde en Natuurwetenschappen

Duisburg-Essen University
Fakultät für Matematik

Contents

Notation

- Let $a, b \in \mathbb{Z}$ we write (a, b) for $\gcd\{a, b\}$.
- We denote by ζ_N with N a positive integer a primitive N-th root of one.
- The symbol $\sqcup$ denotes the disjoint union.
- Let K be a number field, then we denote with K^+ the maximal totally real subfield, namely, the maximal subfield admitting only real embeddings. In addition we denote with $\mathcal{O}_K$ its ring of integers and with $\mathcal{O}_K^\times$ the subset of invertible elements of $\mathcal{O}_K$.
- We denote by $\mathcal{H}$ the Poincaré upper half plane, namely:

  $$\mathcal{H} = \{z \in \mathbb{C} \text{ such that } \operatorname{Im}(z) > 0\}.$$

  Moreover, we denote by $\mathcal{H}^*$ the set $\mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q})$, where $\mathbb{P}^1(\mathbb{Q})$ denotes the projective line over $\mathbb{Q}$.
- We denote by $\zeta(s)$ the Riemann zeta function whose associated series on $\operatorname{Re}(s) > 1$ is $\sum_{n \geqslant 1} n^{-s}$.
- Let L/K be a finite extension of number fields and $\alpha \in L$. We denote by $\operatorname{Norm}_K^L(\alpha)$ the norm of α in K/L.

Introduction

Let K be an abelian extension of $\mathbb{Q}$ and let G_K be the Galois group of $K/\mathbb{Q}$. We consider the Dedekind zeta function associated to K:

$$\zeta_K(s) = \sum_{\mathcal{I} \subset \mathcal{O}_K} \frac{1}{\mathrm{Norm}_{\mathbb{Q}}^{K}(\mathcal{I})^s},$$

where $\mathcal{I}$ runs over the ideals of $\mathcal{O}_K$ and s is a complex number. As it is explained in the book of Daniel A. Marcus [Mar77], this function can be exploited in the computation of the class number of K. The formula relating the Dedekind zeta function with some invariants of the number field K is:

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_K \cdot h_K}{w_K \cdot \sqrt{|D_K|}},$$

where $[K : \mathbb{Q}] = r_1 + 2r_2$ with r_1 being the number of real embeddings and r_2 of complex embeddings up to conjugation, Reg_K is the regulator of K, h_K the class number, D_K the discriminant and w_K the number of roots of unity contained in K. The formula appears to be rather explicit, nevertheless it might be cumbersome to compute. First of all, it is still obscure how to handle with the Dedekind zeta function and, for example, the computation of the class number (which is also essential for the computation of the unit group) is usually feasible only for number rings of small degree. Fortunately, we have another way to compute the class number involving the so called L-functions. Naively, an L-function is a *generating series for arithmetic data* ([Dar11]) as the following definition suggests:

Definition 0.0.1. Let χ be a Dirichlet character, the associate L-function is:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

defined where the series converges.

Remark. If $\chi \neq 1$ then $L(s, \chi)$ converges for $\mathrm{Re}(s) > 0$.

To make a long story short, the Dedekind zeta function has also an expression as:

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\mathcal{I}(n)}{n^s},$$

where $\mathcal{I}(n)$ denotes the number of ideals in $\mathcal{O}_K$ having norm n. This expression is flexible enough to be divided into two parts:

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\mathcal{I}(n) - h_K \cdot k}{n^s} + h_K \cdot k \cdot \zeta(s),$$

where k is given by $\frac{2^{r+s}\pi^s \mathrm{reg}(\mathcal{O}_K)}{w\sqrt{|\mathrm{disc}(\mathcal{O}_K)|}}$ (see theorem 40 of [Mar77]), and $\zeta(s)$ represents the well known Riemann zeta function. Since ζ_K is holomorphic for $s \in \mathbb{C}$ such that $\mathrm{Re}(s) > 1 - 1/[K : \mathbb{Q}]$ (a result of chapter 7 in [Mar77]) and $\zeta(s)$ has a simple pole at $s = 1$, we can isolate the class number considering the following limit:

$$\rho = \lim_{s \to 1} \frac{\zeta_K(s)}{\zeta(s)} = h_K \cdot k.$$

In other words, $\rho/k = h_K$ and, as we know the value of k, it is enough to determine the value of ρ in order to give an expression for h_K. After some computations and complex analysis we discover a new expression for the quotient of the two zeta functions, namely:

$$\frac{\zeta_K(s)}{\zeta(s)} = \prod_{p \nmid N} \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p} \prod_{\substack{\chi \in \widehat{G}_K \\ \chi \neq 1}} L(s, \chi).$$

Here $\widehat{G}_K$ denotes the set of all the Dirichlet characters defined over G_K while f_p and r_p are two suitable integers. Theory about L-functions guarantees that for $\chi \neq 1$ the L-functions associated to χ are holomorphic on $\mathrm{Re}(s) > 0$. We are therefore allowed to compute ρ just by evaluating the L-functions in 1. Our life is made even easier since we can rewrite the L-function associated to a non-primitive character in terms of primitive characters inducing it (roughly speaking, primitive characters are the fundamental bricks to construct all the other characters). Our problem is finally reduced to compute the value in one of an L-function associated to a primitive Dirichlet character. Classical theory shows that the formula is given by the following expression:

$$L(1, \chi) = -\frac{\chi(-1)\mathfrak{g}(\chi)}{N} \sum_{a=1}^{N-1} \chi^{-1}(a) \log(1 - \zeta_N^a), \tag{1}$$

where $\mathfrak{g}(\chi) = \sum_{k=1}^{N-1} \chi(k)\zeta_N^k$ and it is called the Gauss sum attached to χ. We started looking for a concrete way to compute the class number and we ended up with a very interesting formula. First of all, the previous formula states that a specific value of an L-function gives information about arithmetic objects to which the L-function is attached. In fact, the L-function is attached to a character $\chi \in \widehat{G}_K$ and its evaluation at $s = 1$ is a key ingredient for determining the class number of K. In addition to this, the formula above outlines a relation between two objects of a rather different nature. In fact, for N compose, the terms $1 - \zeta_N^a$ inside the logarithm are the so-called cyclotomic (or circular) units of the number field $\mathbb{Q}(\zeta_N)$. Thus, on one side we have an analytic object, the L-function evaluated at a special point, on the other side the circular units, with a more arithmetic flavour, appear in the form of their logarithm. One may wonder whether or not the connection between L-functions and logarithm of cyclotomic units might be extended to the p-adic world. In other words, we can ask ourselves if we can relate the p-adic L-function with the circular units in the form of their p-adic logarithm. It turns out that the answer is positive and we have little to change in our classical formula (1). The result, discovered in 1964, is due to two mathematicians: the Japanese Tomio Kubota and the German Heinrick-Wolfgang Leopoldt. It is explained in their article *"Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen"*. As the title suggests, they introduced the concept of p-adic L-function.

Classical results, in fact, guarantee that for $k \geqslant 2$ the holomorphic Eisenstein series of weight k attached to a character χ has expression:

$$\begin{aligned} E_{k,\chi}(\tau) &= N^k \mathfrak{g}(\overline{\chi})^{-1} \frac{(k-1)!}{(2\pi i)^k} \sum_{\substack{(m,n)\in N\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{\overline{\chi}(n)}{(m\tau+n)^k} \\ &= L(1-k,\chi) + 2\sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n) q^n, \end{aligned} \tag{2}$$

where $q = e^{2\pi i \tau}$, $\sigma_{k-1,\chi}(n) = \sum_{d|n} \chi(d) d^{k-1}$ and $\overline{\chi}$ denotes the complex conjugation of the character χ. Clearly, the L-function appears as the constant term of the q-expansion of the Eisenstein series. It seems we are already stuck. We want to consider the value at 1 of the L-function and thus we need $k = 0$ in the expression (2). Unfortunately, for $k = 0$ the second equality of the previous formula doesn't hold any longer. On the other side, as we will formalize later, the p-adic world allows the p-adic Eisenstein series of weight 0 to have a q-expansion similar to (2). Therefore, in a totally rigorous setting we can interpret a p-adic analogue of $L(1,\chi)$ as the constant term of the p-adic Eisenstein series of weight zero associated to the character χ. Eisenstein series constitute the *trait d'union* with the theory of p-adic modular forms. In the complex context, a weight zero modular form respect to the group $\Gamma_1(N)$ is a function on the modular curve $X_1(N) = \Gamma_1(N)\backslash\mathcal{H}^*$, i.e. on a Riemann surface. Analogously, a p-adic Eisenstein series of weight zero is defined over the *ordinary locus*, a particular subset of the modular curve $X_1(N)$ over $\mathbb{C}_p$ (which we denote by $X_1(N)(\mathbb{C}_p)$). We will see that the p-adic Eisenstein series of weight zero associated to a certain character χ is in some sense holomorphic around the cusp ∞ of $X_1(N)(\mathbb{C}_p)$ (the right notion is to say it is rigid analytic). On the same disc the previous Eisenstein series admits also an interpretation as another p-adic modular form which is still rigid analytic around the cusp ∞. This new expression of the Eisenstein series involves the p-adic logarithm of the p-adic Siegel units. In the classical context, the Siegel units are invertible modular forms whose values at the cusp ∞ are, under certain conditions, cyclotomic units. All this characters will play a role in the proof of the so called Leopoldt formula:

$$L_p(1,\chi) = -\frac{(1-\chi(p)p^{-1})}{\mathfrak{g}(\chi^{-1})} \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^a),$$

which clearly has a non-trivial overlap with the classical formula (1).

In the first chapter we give the classical background, so we recap the notion of modular form and modular curve and we present in detail the cyclotomic units. In the second chapter we give an analytic definition of p-adic modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$ and we outline the most important results. In addition, we give a definition of p-adic modular forms attached to a character χ for more general congruence subgroups. The third and last chapter concerns a modular proof of the p-adic Leopoldt formula and we present there a result of Katz generalizing this discussion. Usually, we introduce notations and definitions when they are needed. If the meaning of a symbol doesn't appear, refer to the section Notation just before this introduction.

I chose to present facts and arguments in the way I understood them trying to be clear and specific. Moreover, I tried to introduce all the concepts which are not supposed to be the background of any mathematician. Even though my references are wisely chosen and they present the material in a rigorous and accurate setting, I might be superficial, sloppy or wrong. In that case, all the mistakes are to be addressed to me.

Acknowledgements

First of all, I thank Prof. Giuseppe Molteni, for his endless (and sometimes blind) support and enthusiasm. I thank my advisor Prof. Massimo Bertolini for introducing me to what research is and for working with me. I thanks Prof. Peter Stevenhagen for countless things. I thank the ALGANT consortium for the opportunities and the support it gives. I thank Andrea Agostini and Matteo Tamiozzo for the wise suggestions and corrections about this text. I thank the people of the mathematical institute of Leiden (classmates, PhD and professors), the members of my OWL group, the people of CREA Orkest: they all made amazing my time in Leiden. I thank the people who supported me, mathematically and personally, in Essen during a gray period of my life. Nothing would have happened without the friendship with Francesca Bergamaschi. A special thanks to my closest friends living far away on whom I can always rely. I thank my sometime wise sometime ciuch parents. I thank, finally, my beloved *Meisje*.

1

Preliminaries

1.1 Modular forms

The notion of modular form is a milestone in contemporary mathematics and it is extensively used in arithmetic geometry and number theory. Endless is the number of books and notes about this subject. One important classical text for finding exhaustive explanations about modular forms is [DS05]. I report in this section the most common facts and my intention is essentially to fix notation. Certainly, I am giving here an outline of the subject according to my taste. The mature reader will pardon me when the point of view is too naive and primitive but I thought it would be a better idea to present concepts in the way I understand and use them.

1.1.1 Complex tori and elliptic curves

Elliptic curves are one of the most studied objects in modern and contemporary mathematics. They are a versatile object able to connect different fields of mathematics. Elliptic curves may be defined over any field or even over rings but for treating complex modular forms the most meaningful definition is that over the complex numbers.

Definition 1.1.1. An elliptic curve is a smooth projective curve of genus one over $\mathbb{C}$.

Elliptic curves may be more concretely defined in terms of the projective Weierstrass equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

with $a_i \in \mathbb{Q}$. We have also a third way to look at elliptic curves which will be predominant in this text. First of all we need to introduce another object.

Definition 1.1.2. A torus over $\mathbb{C}$ is given by the quotient:

$$\mathbb{C}/\Lambda,$$

where Λ is a full lattice in $\mathbb{C}$, namely, is a subgroup of $\mathbb{C}$ of the shape:

$$\Lambda = \omega_1\mathbb{Z} \bigoplus \omega_2\mathbb{Z}, \tag{1.2}$$

with $\frac{\omega_1}{\omega_2} \in \mathbb{C}\backslash\mathbb{R}$.

Notation. We denote by $\mathcal{L}$ the set of all the lattices of $\mathbb{C}$ and with $[0] \in \mathbb{C}/\Lambda$ the equivalence class of $0 \in \mathbb{C}$.

Complex tori admit an interpretation as Riemann surfaces as it is clearly explained in [For99]. The interesting fact is that understanding holomorphic functions among complex tori sending $[0]$ to $[0]$ reduces to understand properties and relations among lattices defining them. So, any holomorphic map ϕ between two complex tori E_1 and E_2 of lattices respectively Λ_1 and Λ_2 sending the zero point $[0_1] \in E_1$ to the zero point $[0_2] \in E_2$ is given by multiplication by a complex scalar $\alpha \in \mathbb{C}^\times$ with the property that $\alpha\Lambda_1 \subset \Lambda_2$. More explicitly,

$$\phi : \mathbb{C}/\Lambda_1 \xrightarrow{\cdot\alpha} \mathbb{C}/\Lambda_2$$

sends the point $[P] \in E_1$ to the point $[\alpha \cdot P] \in E_2$. Straightforwardly, it follows that two complex tori are isomorphic if there exists $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$. We can now group together complex tori under the equivalence relation of being isomorphic. Equivalently, we can just divide $\mathcal{L}$, the set of all full lattices in $\mathbb{C}$, in equivalence relation given by $\Lambda_1 \sim \Lambda_2$ if there exists an $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$. Thereby, we have the following bijection of sets:

$$\mathcal{L}/\sim \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Isomorphism classes of}\\ \text{complex tori}\end{matrix}\right\}.$$

In addition to this, common theory about elliptic curves (like chapter VI: "Elliptic curves over $\mathbb{C}$" in [Sil86]) states a bijection between algebraic isomorphisms classes of elliptic curves and isomorphism classes of complex tori as we described before. The bijection

$$\left\{\begin{matrix}\text{Isomorphism classes of}\\ \text{elliptic curves over } \mathbb{C}\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{matrix}\text{Isomorphism classes of}\\ \text{complex tori}\end{matrix}\right\}$$

is given in terms of the so called j-fucntion. From now on, speaking of elliptic curves and of complex tori will be the same thing and therefore speaking of lattices and speaking of elliptic curves turns out to be the same thing as well. In particular, we are now motivated to find a connection between functions on lattices (in a sense which will be formalized later) and functions of elliptic curves. Now we turn to another way to look at the set $\mathcal{L}$. In the definition we described a lattice as the $\mathbb{Z}$-span of two $\mathbb{R}$-linearly independent complex vectors. It is easy to see that different choices of ω_1 and ω_2 may give birth to the same lattice. We want now to determine the relation linking bases defining the same lattice. First of all, we begin by putting an order on the set of all the basis.

Definition 1.1.3. A basis of a lattice Λ is given by the couple (ω_1, ω_2) of (1.2). A basis is called ordered if

$$\operatorname{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0.$$

Notation. We denote by $\mathcal{B}$ the set of ordered basis of the lattices of $\mathbb{C}$.

Clearly, if two basis, let's say (ω_1, ω_2) and $(\omega_1^{'}, \omega_2^{'})$, generate the same lattice, we can find an integral relation, like:

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

where $a, b, c, d \in \mathbb{Z}$. It is not hard to prove that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has determinant one, i.e. it belongs to the following group.

Definition 1.1.4. We call the special linear group of degree 2 over $\mathbb{Z}$ ($\mathrm{SL}_2(\mathbb{Z})$) the group of 2×2 invertible matrices with coefficients in $\mathbb{Z}$, namely;

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ such that } a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}.$$

We can summarize the previous fact just by describing the following action of $\mathrm{SL}_2(\mathbb{Z})$ on the set $\mathcal{B}$. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, and let $(\omega_1, \omega_2) \in \mathcal{B}$, then:

$$\gamma \cdot (\omega_1, \omega_2) = (a\,\omega_1 + b\,\omega_2, c\,\omega_1 + d\,\omega_2). \tag{1.3}$$

The right hand side of (1.3) is indeed an element of $\mathcal{B}$ since $\operatorname{Im}\left(\frac{a\,\omega_1 + b\,\omega_2}{c\,\omega_1 + d\,\omega_2}\right) > 0$ and it describes an ordered basis which spans the same lattice of (ω_1, ω_2). Actually, we have just found a way to describe all the bases generating the same lattice: it is the set $\{\gamma \cdot (\omega_1, \omega_1) \in \mathcal{B} \text{ such that } \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$ and therefore clearly we have the following correspondence:

$$\mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{B} = \mathcal{L}.$$

The condition $\operatorname{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$ of all the elements of $\mathcal{B}$ prompts us to consider another action on $\mathcal{B}$. In fact, we have a map

$$\mathcal{B} \to \mathbb{C}$$

sending (ω_1, ω_2) to ω_1/ω_2. A suitable inverse for this map is given by sending $\tau \in \mathcal{H}$ to the couple $(\tau, 1) \in \mathcal{B}$. From the definition of ordered basis, ω_1/ω_2 belongs to the upper part of $\mathbb{C}$. It is an obvious observation that (ω_1, ω_2) and $(\alpha \cdot \omega_1, \alpha \cdot \omega_2)$ are mapped to the same element by the previous map. This means the previous map factors through the right action of $\mathbb{C}^\times$ on $\mathcal{B}$ given by $\alpha \cdot (\omega_1, \omega_2) = (\alpha \cdot \omega_1, \alpha \cdot \omega_2)$. We shall give a name to the image of the previous map.

Definition 1.1.5. We define the (Poincaré) upper half plane to be the set:

$$\mathcal{H} = \{z \in \mathbb{C} \text{ such that } \operatorname{Im}(z) > 0\}.$$

Therefore the map

$$\mathcal{B}/\mathbb{C}^\times \overset{1:1}{\longleftrightarrow} \mathcal{H}$$

is a bijection and the inverse is given by sending $\tau \in \mathcal{H}$ to the couple $(\tau, 1) \in \mathcal{B}$. So far we got two actions on $\mathcal{B}$, one left and the other a right action. It is easy to prove that these action commute with each other and we have the following correspondences:

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{B} = \mathcal{L} \quad \text{and} \quad \mathcal{B}/\mathbb{C}^\times = \mathcal{H}.$$

So, we can now describe the actions on these quotients. It is clear that $\mathbb{C}^\times$ acts also on $\mathcal{L}$ by multiplication of the lattice by the complex scalar. In addition, $\mathrm{SL}_2(\mathbb{Z})$ has a left action on $\mathcal{H}$. In fact, if we consider a matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then the action of γ on $\tau \in \mathcal{H}$ is given by:

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Now it is clear that the following bijections hold:

$$\mathcal{L}/\mathbb{C}^\times \overset{1:1}{\longleftrightarrow} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{B}/\mathbb{C}^\times \overset{1:1}{\longleftrightarrow} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}.$$

In the light of all this argument we may conjecture that giving a function on $\mathcal{H}$ with some properties involving $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to give a function on $\mathcal{L}$ taking care of the action of $\mathbb{C}^\times$. In case of a positive answer, we would have found a function defined over $\mathcal{H}$ giving complex values to isomorphism classes of elliptic curves. The next section shows how this is indeed possible.

1.1.2 Modular forms for $\mathrm{SL}_2(\mathbb{Z})$

We start out with giving a proper definition of what we mean for a function of lattices.

Definition 1.1.6. A function of lattices of weight k is a function

$$F : \mathcal{L} \to \mathbb{C}$$

such that for any $\lambda \in \mathbb{C}^\times$ we have that $F(\lambda\Lambda) = \lambda^{-k}F(\Lambda)$.

Before proceeding further we just remark that if $\tau \in \mathcal{H}$ we can associate to it $(\tau, 1) \in \mathcal{B}$. This element gives birth to the lattice $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$.
Let F be a function of lattices according to our Definition 1.1.6:

$$F : \mathcal{L} \to \mathbb{C}.$$

We can then associate to F a function f on $\mathcal{H}$:

$$f : \mathcal{H} \to \mathbb{C}$$

given by $f(\tau) = F(\Lambda_\tau) = F(\tau\mathbb{Z} \oplus \mathbb{Z})$. We notice that this new function f satisfies the following rule. For any matrix $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have:

$$\begin{aligned} f\left(\frac{a\tau + b}{c\tau + d}\right) = F\left(\frac{a\tau + b}{c\tau + d}\mathbb{Z} \oplus \mathbb{Z}\right) &= (c\tau + d)^k F\left((a\tau + b)\mathbb{Z} \oplus (c\tau + d)\mathbb{Z}\right) \\ &= (c\tau + d)^k F(\Lambda_\tau) \\ &= (c\tau + d)^k f(\tau). \end{aligned}$$

As hoped, the converse also holds, namely, if we have a function on $\mathcal{H}$ satisfying the rule:

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \tag{1.4}$$

for any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ then we can recover a function of lattices F just by letting $F(\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}) = \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right)$. On account of the property (1.4) F is well defined, in fact:

$$F\left(\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}\right) = F\left((a\omega_1 + b\omega_2)\mathbb{Z} \oplus (c\omega_1 + d\omega_2)\mathbb{Z}\right).$$

Thus F is a function of lattices according to Definition 1.1.6. Having this mirror between functions on lattices and functions on the upper half plane is rather a fundamental fact because we may now look at functions of lattices from a complex point of view. When we were working with functions on $\mathcal{L}$ we didn't have any well known topology on it (except the trivial topologies). Now we just discovered we can consider functions of lattices as functions on $\mathcal{H}$ on which we can apply all the means of complex analysis. Not surprisingly, the next step is to select only the functions on the upper half plane we are comfortable working with, i.e. the holomorphic functions. Indeed, these functions will be sufficient for developing the theory and discovering new results.

Remark. It is a common exercise to show that all the holomorphic automorphisms of $\mathcal{H}$ are given by $\mathrm{SL}_2(\mathbb{R})$, namely, any automorphism of $\mathcal{H}$ is given by sending $\tau \in \mathcal{H}$ to $\frac{a\tau+b}{c\tau+d}$ where $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R})$.

Notation. We denote by $D^\times$ the unit punctured disc namely: $D^\times = \{s \in \mathbb{C}$ such that $0 < |s| < 1\}$.

There exists a map

$$\phi : \mathcal{H} \to D^\times$$

sending τ to $e^{2\pi i\tau}$ which actually maps the upper half plane on the punctured disc in a holomorphic way. This observation allows us to consider *growth condition* at infinity for the map in the upper half plane in a sense which will be made clear soon. We have now enough motivation for what follows. Let's consider a holomorphic function

$$f : \mathcal{H} \to \mathbb{C}$$

such that $f(\gamma \cdot \tau) = f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This implies that $f(\tau+1) = f(\tau)$ and therefore we can define a map

$$f^* : D^\times \to \mathbb{C}$$

sending $\phi(\tau) = [\tau] \in D^\times$ to $f(\tau)$.

Definition 1.1.7. We say that the f above is a modular function of weight k with respect to the group $\mathrm{SL}_2(\mathbb{Z})$ if f^*, as defined above, is meromorphic on the all unit disc, namely if f^* might be extended meromorphically also in the center of the disc. If the extension is also holomorphic we call f a modular form. If, in addition, the value of f^* is zero at the center of the disc, we call f a cusp form.

We conclude this section by underlying that modular forms show up as a natural object when we want to work on spaces of elliptic curves. In fact, we can rely on the bijections between points on the upper half plane and lattices. The formalization of this process will end up with the definition of modular curve.

1.1.3 Congruence subgroups

In the study of modular forms, there are other groups playing an important role. All these groups are subgroups of $\mathrm{SL}_2(\mathbb{Z})$. They appear naturally in the study of the structure of the so-called modular curve $X_0(1)$ which is the quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. Even though we are about to construct this object, we just advise that the details of this construction may be found in [DS05]. For our purposes it is enough to know these subgroups exist and are meaningful. We start out with introducing some subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

(i) $\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1) \text{ such that } c \equiv 0 \bmod N \right\}$,

(ii) $\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1) \text{ such that } a, b \equiv 1 \text{ and } c \equiv 0 \bmod N \right\}$,

(iii) $\Gamma(N) = \{\alpha \in \mathrm{SL}_2(\mathbb{Z}) \text{ such that } \alpha \equiv 1 \bmod N\}$.

Definition 1.1.8. We define a congruence subgroup to be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which contains $\Gamma(N)$ for some N.

Remark. The subgroups (i), (ii), (iii) are level groups, moreover, notice that:

$$\Gamma_0(N) \supset \Gamma_1(N) \supset \Gamma(N).$$

Our intention is to consider the quotient of $\mathcal{H}$ by any of these groups in order to get a wider definition of modular curve. Then we would like to construct some functions suitable for these smaller groups. We are not surprised that the definition of these functions will be just a wise reformulation of the concept of modular functions. Let $f : \mathcal{H} \to \mathbb{C}$ be a function, $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$, then we define:

$$\left(f_{|_k}\gamma\right)(\tau) = (c\tau + d)^{-k} f(\gamma \cdot \tau).$$

Definition 1.1.9. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and suppose that $\Gamma(N) \subset \Gamma$, then a modular form of weight $k \geqslant 0$ for Γ is a function $f : \mathcal{H} \to \mathbb{C}$ such that:

(1) f is holomorphic,

(2) $f_{|_k}\gamma = f$, namely, $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for any $\gamma \in \Gamma$,

(3) for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ we have that:

$$(f_{|_k}\gamma)(\tau) = \sum_{k \geqslant 0} a_n^\sigma q_N^n,$$

where $q_N = e^{2\pi i \tau/N}$ and $a_n^\sigma \in \mathbb{C}$ for any n.

In the case $a_0^\sigma = 0$ for any $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ we say that f is a cusp form.

Remark. The property (3) is called holomorphicity of f at the cusps.

The following definition will play an important role in the proof of the p-adic Leopoldt formula. We can in fact attach to a modular form also a so called Dirichlet character whose definition is the following.

Definition 1.1.10. A Dirichlet character of conductor N is a group homomorphism:

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

Clearly, any character can be extended to a function over $\mathbb{Z}$ sending $a \in \mathbb{Z}$ to $\chi([a])$ (where $[a]$ denotes the class of a in $\mathbb{Z}/N\mathbb{Z}$) and by letting $\chi([0]) = 0$. With an abuse of notation we will denote with χ also this extension.

Remark. (i) We say that the character χ is even if $\chi(-1) = 1$, odd otherwise.

(ii) Let χ and $\tilde{\chi}$ be two Dirichlet characters of conductor N and M respectively such that $N \mid M$. We say that χ induces $\tilde{\chi}$ if $\tilde{\chi}(a) = \chi(a)$ for any $a \in \mathbb{Z}$ coprime with M.

(iii) We say that a character is primitive if it is not induced by any other character.

Definition 1.1.11. Let χ be a Dirichlet character. A modular form of weight k, group level $\Gamma_1(N)$ and nebentypus χ is a holomorphic function f defined on $\mathcal{H}$ with values in $\mathbb{C}$ such that:

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = \chi(d)(c\tau + d)^k f(\tau)$$

for any $\tau \in \mathcal{H}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N)$.

1.1.4 Modular curves

So far we have spoken only about functions. In this section we want to turn our attention to the construction of a curve which will be used to parametrize isomorphism classes of elliptic curves.

Naively, once we have a curve consisting in a quotient of $\mathcal{H}$, then we have a way to treat general properties of elliptic curves on account of the well known correspondence of between $\mathcal{H}$ and $\mathcal{L}$. As we will clarify later, modular curves are an example of *moduli spaces*. First of all, let $\mathbb{P}^1(\mathbb{Q})$ be the projective line over the field $\mathbb{Q}$; we denote its elements by $(\alpha : \beta)$. Let Γ be one of the congruence subgroups defined in Section 1.1.3. We consider the action of Γ over $\mathbb{P}^1(\mathbb{Q})$ given by:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot (\alpha : \beta) = (a\alpha + b\beta : c\alpha + d\beta),$$

where $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$.

Remark. Notice that the point at infinity $(1 : 0)$ is sent to $(a : c)$.

Definition 1.1.12. We define a cusp to be an equivalence class of the quotient:

$$\Gamma \backslash \mathbb{P}^1(\mathbb{Q}).$$

The whole set is called the set of the cusps with respect to Γ.

Remark. The set of cusps is always finite since the action of $\mathrm{SL}_2(\mathbb{Z})$ is transitive on $\mathbb{P}^1(\mathbb{Q})$ and any subgroup Γ has, by definition, finite index in $\mathrm{SL}_2(\mathbb{Z})$. In fact, it is enough to consider the sequence:

$$\Gamma(N) \hookrightarrow \mathrm{SL}_2(N) \xrightarrow{\text{mod } N} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

where the first map denotes the inclusion and the second map is given by reducing the coefficients modulo N. $\Gamma(N)$ is the kernel of the second map therefore it is normal in $\mathrm{SL}_2(\mathbb{Z})$ and since $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is a finite group the index of $\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is finite as well. Finally, it is just enough to notice that $\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$.

Definition 1.1.13. Let $\mathcal{H}^* = \mathcal{H} \sqcup \mathbb{P}^1_{\mathbb{Q}}$ and Γ as before, namely, one among $\Gamma(1) \supset \Gamma_0(N) \supset \Gamma_1(N) \supset \Gamma(N)$. We call the modular curve associated to Γ the following quotient:

$$\Gamma \backslash \mathcal{H}^* = \Gamma \backslash \mathcal{H} \sqcup \Gamma \backslash \mathbb{P}^1_{\mathbb{Q}}$$

We will call $\Gamma \backslash \mathcal{H}$ the open (or affine) part of the modular curve.

Remark. The introduction of the cusps is motivated by the fact that we will interpret the modular curve as a Riemann surface. In order to get an interpretation as a compact Riemann surface we need to add to $\Gamma \backslash \mathcal{H}$ the set of cusps.

Remark. We use the following notations:

$$X_0(1) = \Gamma(1)\backslash\mathcal{H}^* = Y_0(1) \sqcup \{\infty\}, \quad X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^* = Y_0(N) \sqcup C_0(N),$$

$$X_1(N) = /\Gamma_1(N)\backslash\mathcal{H}^* = Y_1(N) \sqcup C_1(N),$$

where $Y_{-}(-)$ and $C_{-}(-)$ denote, respectively, the open part and the set of cusp of the modular curve. In case of $X_0(1)$, we find only one cusp which correspond to ∞. Moreover, notice that we have the natural projection:

$$X_1(N) \to X_0(N) \to X_0(1).$$

Theorem 1.1.14. *Any of the previous modular curves admits a structure of a compact Riemann surface.*

Proof. See Chapter 2: Modular curves as Riemann surfaces in [DS05]. □

Remark. $X_0(1)$ is isomorphic to $\mathbb{P}^1(\mathbb{C})$ therefore it is a smooth projective curve of genus zero.

The open part of a modular curve classifies isomorphism classes of complex tori, namely, of elliptic curves. For a detailed approach we invite the reader to see in chapter VI: “Elliptic curves over $\mathbb{C}$” of [Sil86] proposition 3.6 part (b). As we said before, modular curves admit an interpretation as moduli spaces which in a colloquial way might be defined as follows.

Definition 1.1.15. A moduli space is a geometric object, for example a topological space or a curve (in our case a Riemann surface) which parametrizes a family of geometric objects (in our case, elliptic curves).

As we have just seen, the open part of the affine curve admits an interpretation as an open Riemann surface and the following proposition clarifies the exact correspondence with classes of elliptic curves.

Proposition 1.1.16. *We have the following bijections:*

$$\begin{aligned}
Y_0(1) &\overset{1:1}{\longleftrightarrow} \left\{ \begin{matrix} \textit{Isomorpism classes} \\ \textit{of elliptic curves} \end{matrix} \right\}, \\
Y_0(N) &\overset{1:1}{\longleftrightarrow} \left\{ \begin{matrix} \textit{Iso classes of couples } (E,P) \textit{ where } E \textit{ is an elliptic curve} \\ \textit{and } P \in E \textit{ is a point of exact order } N \end{matrix} \right\}, \\
Y_1(N) &\overset{1:1}{\longleftrightarrow} \left\{ \begin{matrix} \textit{Iso classes of couples } (E,\mathcal{C}) \textit{ where } E \textit{ is an elliptic curve} \\ \textit{and } \mathcal{C} \subset E \textit{ is a cyclic subgroup of order } N \end{matrix} \right\}.
\end{aligned}$$

We started by considering a quotient of the upper half plane and we got a curve which also admits an interpretation as a Riemann surface. A natural question to pose is whether or not we can extend these objects to different fields of definition. In other words, it would be nice to find a modular curve defined over different fields or rings able to parametrize isomorphism classes of elliptic curves defined over different fields or rings. We will give an answer to this question in Section 3.2. For now we just recall the results needed for developing the theory later.

Theorem 1.1.17. *Any compact Riemann surface admits a structure of a smooth projective complex algebraic variety over $\mathbb{C}$ of dimension one.*

Proof. See in chapter VII: applications of Riemann-Roch of [Mir95] proposition 1.1. □

Theorem 1.1.18. *The modular curves $X_0(N)$ and $X_1(N)$ admit a model over $\mathbb{Q}$, i.e. they are given by equations with coefficients in $\mathbb{Q}$.*

Proof. See Theorem 7.7.1 in [DS05]. □

On account of these facts, we realize we can now define the previous modular curves over any fields extension of $\mathbb{Q}$. In fact, we can look for solutions of the equations guaranteed by Theorem 1.1.18 in any other fields extension of $\mathbb{Q}$, in particular we can consider solutions in $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$. Anyway, this will concern us later in this text.

1.2 Circular units

In this section we introduce circular units, also called cyclotomic units. Our main reference is [Was97]. Moreover, we looked also at [KL81] and [Lan90].

The determination of the group of units of a general algebraic number field is not easy. Nevertheless, the cyclotomic fields admit a subgroup (the group of cyclotomic units) which has finite index in the full group of unity. The index is strongly related to the class number and therefore with the p-adic L-functions. In fact, this relation is essential to prove Leopoldt's formula about the class number as it is proved in [Was97].

1.2.1 Setting and definitions

We consider the number field $\mathbb{Q}_{\zeta_p}$ where ζ_p denote a primitive p-th root of unity. Let $\zeta = \zeta_p$. Thanks to Theorem A.3.3, we know that the ring of integers for this field is $\mathbb{Z}[\zeta]$. We consider its group of units and we denote it by $\mathbb{Z}[\zeta]^\times$. In order to have a better understanding of this group we state and prove the following lemma:

Lemma 1.2.1. *Let $r, s \in \mathbb{Z}$ and ζ as before and assume that $(p, rs) = 1$ then:*

$$\frac{\zeta^r - 1}{\zeta^s - 1} \in \mathbb{Z}[\zeta]^\times.$$

Proof. Since r and s are invertible in $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ we can find an integer t such that $r = st \bmod p$ so:

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^{st} - 1}{\zeta^s - 1} = 1 + \zeta^s + \cdots + \zeta^{(t-1)s} \in \mathbb{Z}[\zeta].$$

Analogously, we find that $\left(\frac{\zeta^r-1}{\zeta^s-1}\right)^{-1} \in \mathbb{Z}[\zeta]$ concluding that $\frac{\zeta^r-1}{\zeta^s-1} \in \mathbb{Z}[\zeta]^\times$. □

We now consider the number field $\mathbb{Q}_{\zeta_N}$ where N is a positive integer. Again, the ring of integers is $\mathbb{Z}[\zeta]$ and we want to characterize some particular elements of $\mathbb{Z}[\zeta]^\times$. We first notice that when $N = p^n$, $\zeta_{p^n} - 1$ is not a unit (it suffices to compute its norm). On the other hand, a reasoning similar to that of the previous lemma shows that for any N $\frac{\zeta^a-1}{\zeta^b-1}$ with $(ab, N) = 1$ are units. We notice we have also the following fact.

Proposition 1.2.2. *If N has at least two distinct prime factors then*

$$1 - \zeta_N \in \mathbb{Z}[\zeta_N]^\times,$$

and moreover:

$$\prod_{(j,N)=1} (1 - \zeta_N^j) = 1.$$

Proof. We recall we have $x^N - 1 = \prod_{j=0}^{N-1}(x - \zeta_N^j)$, therefore, dividing by $x - 1$:

$$x^{N-1} + x^{N-2} + \cdots + x + 1 = \prod_{j=1}^{N-1}(x - \zeta_N^j).$$

We now evaluate at $x = 1$ getting $N = \prod_{j=1}^{N-1}(1 - \zeta_N^j)$. Suppose now p^a divides exactly N, namely, $p^a \mid N$ but $p^{a+1} \nmid N$. We assume $p^a k = N$ with $k \in \mathbb{Z}$. Thanks to the previous reasoning we can write $p^a = \prod_{i=1}^{p^a-1}(1 - \zeta_{p^a}^i) = \prod_{i=1}^{p^a-1}(1 - \zeta_N^{ki})$. We can now quotient N by p^a getting

$$k = \prod_{\substack{j=1 \\ k \nmid j}}^{N-1}(1 - \zeta_N^j).$$

With the same reasoning we now quotient the previous expression by another prime factor of N dividing exactly N. Once we have done this process for all the primes dividing N we get:

$$1 = \prod_j (1 - \zeta_N^j),$$

where the j runs among the divisor of N which haven't been considered in the process before. We notice that $(1 - \zeta_N)$ is still a factor in this product implying that $1 - \zeta_N \in \mathbb{Z}[\zeta_N]^\times$. For the second part of the proposition we consider the norm of $1 - \zeta_N$ which is:

$$\mathrm{Norm}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_N)}(1 - \zeta_N) = \prod_{(j,N)=1} (1 - \zeta_N^j) = \pm 1.$$

Since complex conjugation is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, the norm of any element may be written as $\alpha\overline{\alpha}$ and therefore it is positive. We deduce that $\prod_{(j,N)=1}(1-\zeta_N) = 1$. □

All the preceding units are called cyclotomic units. The name comes from the clear connection they have with the cyclotomic fields.
We want now to give a more general definition of cyclotomic units. We consider the number field $\mathbb{Q}(\zeta_N)$. Since $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{N/2})$ when $N = 2 \bmod 4$ ($\zeta_N = \pm\zeta_{N/2}$), we can assume N to be a integer different from 2 mod 4. We define V_N to be the multiplicative group generated by:

$$\{\pm\zeta_N, 1-\zeta_N^a \text{ such that } 1 < a \leqslant N-1\}.$$

Let E_N be the group of units of $\mathbb{Q}(\zeta_n)$. Then we can state:

Definition 1.2.3. We define the group of cyclotomic units to be:

$$C_N := V_N \cap E_N.$$

Remark. When the context is clear enough we write C instead of C_N.

1.2.2 Properties of the cyclotomic units group

We recall that if K is a number field we then denote by K^+ the maximal totally real subfield of K. In order to understand how the subgroup of cyclotomic units behaves in the full group of units of $\mathbb{Q}(\zeta)$ we start out with understanding which are the generators of these cyclotomic units. Before proceeding further we just remark that for any N all the elements of the shape:

$$\frac{1-\zeta_N^a}{1-\zeta_N},$$

with $(a, N) = 1$ can be written as a real unit times a root of one. In fact:

$$\frac{1-\zeta_N^a}{1-\zeta_N} = \zeta_N^{\frac{a-1}{2}} \frac{\zeta_N^a - \zeta_N^{-a}}{\zeta_N^{\frac{1}{2}} - \zeta_N^{-\frac{1}{2}}}$$

and clearly $\frac{\zeta_N^a - \zeta_N^{-a}}{\zeta_N^{\frac{1}{2}} - \zeta_N^{-\frac{1}{2}}}$ is a real unit. This remark is used in the proof of the following lemma. Notice that we now specialize in the case $N = p^m$ with m a positive integer.

Lemma 1.2.4. *1. The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$ are generated by -1 and by the units:*

$$\xi_a = \zeta_{p^m}^{\frac{1-a}{2}} \frac{1-\zeta_{p^m}^a}{1-\zeta_{p^m}},$$

with $1 < a < \frac{1}{2}p^m$ and $(a, p) = 1$.

2. The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})$ are generated by ζ_{p^m} and the cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$.

Proof. We first start with understanding why the restrictions $1 < a < \frac{1}{2}p^m$ and $(a, p) = 1$ are reasonable. We know, thanks to Lemma A.3.2, that for any positive integer $k < m$ the following relation holds:

$$1 - x^{p^k} = \prod_{j=0}^{p^k-1} (1 - \zeta_{p^m}^{jp^{m-k}} x).$$

Let $b \in \mathbb{Z}$ be coprime with p, then:

$$1 - \zeta_{p^m}^{bp^k} = \prod_{j=0}^{p^k-1} (1 - \zeta_{p^m}^{b+jp^{m-k}}).$$

Therefore we can reduce to look at $1 - \zeta_{p^m}^a$ only when a is prime to p. Moreover we notice that $(1 - \zeta^a) = -\zeta^a(1 - \zeta^{-a})$ and therefore we can reduce to consider only $1 < a < \frac{1}{2}p^m$. Now we proceed with proving part *2*: we suppose that

$$\xi = \zeta_{p^m}^d \prod_a (1 - \zeta^a)^{c_a}$$

with $c_a \in \mathbb{Z}$ is a unit in $\mathbb{Q}(\zeta_{p^m})$.
Since $(1 - \zeta^a)$ and $(1 - \zeta^b)$ differ only by a unit (thanks to Lemma 1.2.1), all the factors generate the same ideal and thus $\sum_a c_a = 0$. Eventually we can write:

$$\begin{aligned} \xi &= \zeta^d \prod_a \left(\frac{1 - \zeta_{p^m}^a}{1 - \zeta_{p^m}} \right)^{c_a} \\ &= \zeta^e \prod_a \xi_a^{c_a}, \end{aligned}$$

where $e = d + \sum_a c_a(a-1)/2$. This proves part *2*. Notice moreover that if ξ is real we have also that $\zeta_{p^m}^e$ is real since ξ_a are real. This concludes the proof of *1*. □

Remark. When N is not a power of a prime then not all the cyclotomic units are a product of roots of one and

$$\frac{1 - \zeta_N^a}{1 - \zeta_N},$$

with $(a, N) = 1$. In fact, in light of Proposition 1.2.2 we notice that $1 - \zeta_N$ does not have this shape.

We stick to the case $N = p^m$ and our aim is to show that the group of cyclotomic units has finite index in the full group of units. Before proceeding further we notice that the real units multiplied by a root of one have index one or two in the full units group.

Proposition 1.2.5. *Let E be the full unit group of $\mathbb{Q}(\zeta_N)$, then the subgroup generated by the roots of unity and the real units of $\mathbb{Q}(\zeta_N)$ have index one or two in E.*

Proof. See Theorem 4.12 in [Was97]. □

On account of this fact, it suffices to work only with real units.

Theorem 1.2.6. *Let C_N^+ and E_N^+ be, respectively, the group of cyclotomic units and the full group of units in $\mathbb{Q}(\zeta_N)^+$, then $C_{p^m}^+ \subset \mathbb{Q}(\zeta_{p^m})^+$ has finite index in $E_{p^m}^+$ and moreover:*

$$h_{p^m}^+ = [E_{p^m}^+ : C_{p^m}^+],$$

where $h_{p^m}^+$ denotes the class number of $\mathbb{Q}_{p^m}^+$.

Proof. We prove this statement with a wise use of the regulator. We denote with σ_a the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$ sending ζ_{p^m} to $\zeta_{p^m}^a$. If $(a,p) = 1$ and $1 \leqslant a < \frac{1}{2}p^m$ then $\{\sigma_a\}$ generate $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})^+/\mathbb{Q})$. We notice we can write:

$$\xi_a = \frac{\sigma_a\left(\zeta^{-\frac{1}{2}}(1-\zeta)\right)}{\zeta^{-\frac{1}{2}}(1-\zeta)}.$$

In order to be consistent with the notation of Lemma A.2.2, we define:

$$f(\sigma_a) = \log\left|\sigma_a\left(\zeta^{-\frac{1}{2}}(1-\zeta)\right)\right| = \log\left|\sigma_a\left(1-\zeta\right)\right|.$$

By computing the regulator we get:

$$\begin{aligned}\mathrm{Reg}\left\{\xi_a\right\}_a &= \left|\det\left(n_b \log|\sigma_b(\xi_a)|\right)_{a,b\neq 1}\right| \\ &= \left|\det\left(\log|\sigma_b\sigma_a(\zeta^{-\frac{1}{2}}(1-\zeta))| - \log|\sigma_b(\zeta^{\frac{1}{2}}(1-\zeta))|\right)_{a,b\neq 1}\right| \\ &= \left|\det\left(f(\sigma_b\sigma_{-a}^{-1}) - f(\sigma_b)\right)_{a,b\neq 1}\right|.\end{aligned}$$

We now apply Lemma A.2.2:

$$\left|\prod_{\chi\in\widehat{G}\setminus\{\mathbb{I}\}}\sum_{\sigma_a\in G} f(\sigma_a)\chi(\sigma_a)\right| = \left|\prod_{\chi\in\widehat{G}\setminus\{\mathbb{I}\}}\sum_{\sigma_a\in G}\chi(\sigma_a)\log|1-\zeta^a|\right| = \left|\prod\sum_{1\leqslant a<\frac{1}{2}p^m}\chi(a)\log|1-\zeta^a|\right|.$$

Since $|1-\zeta^{-a}| = |-\zeta^{-a}(1-\zeta^a)| = |1-\zeta^a|$, and since $\chi(-a) = \chi(a)$ we can rewrite the previous expression as follows:

$$\left|\prod\frac{1}{2}\sum_{a=1}^{p^m}\chi(a)\log|1-\zeta^a|\right|.$$

Thank to Lemma A.3.2 we have for any $0 < k < m$:

$$1 - \zeta_{p^k}^b = \prod_{\substack{a=1 \\ a \equiv b \bmod p^k}}^{p^m} (1 - \zeta_{p^m}^a).$$

Therefore if the conductor of χ is p^k:

$$\sum_{a}^{p^m} \chi(a) \log|1 - \zeta_{p^m}^a| = \sum_{b=1}^{p^k} \chi(b) \log|1 - \zeta_{p^k}^b| = -\frac{p^k}{\tau(\overline{\chi})} L(1, \overline{\chi}) = -\tau(\chi) L(1, \overline{\chi}).$$

In conclusion:

$$\text{Reg}\{\xi_a\}_a = \prod_{\chi \neq 1} -\tau(\chi) L(1, \overline{\chi}) = h^+ R^+,$$

where R^+ is the regulator of $\mathbb{Q}(\zeta_{p^m})^+$. By Lemma A.3.1 we conclude:

$$[E_{p^m}^+ : C_{p^m}^+] = \frac{\text{Reg}\{\xi_a\}}{R^+} = h^+,$$

as we wanted to show. □

In 1966 the Indian mathematician Kanakanahalli Ramarchandra determined in his article [Ram66] the generating units for a general N and proved they are independent allowing us to state:

Theorem 1.2.7. *Let $N \neq 2$ mod 4 and let $N = \prod_{i=1}^{s} p_i^{e_i}$ be its prime factorization. Let I run through all subsets of $\{1, \cdots, s\}$ except $\{1, \cdots, s\}$ and let $N_I = \prod_{i \in I} p_i^{e_i}$. For $1 < a < \frac{1}{2}N$, $(a, N) = 1$, define:*

$$\xi_a = \zeta_n^{d_a} \prod_{I} \frac{1 - \zeta_N^{aN_I}}{1 - \zeta_N^{N_I}},$$

where, $d_a = \frac{1}{2}(1 - a) \sum_I N_I$.
Then the set $\{\xi_a\}$ forms a set of multiplicatively independent units for $\mathbb{Q}(\zeta_N)^+$. If $C_N^{'}$ denotes the group generted by -1 and the ξ_a's, and E_N^+ denotes the group of units of $\mathbb{Q}(\zeta_N)^+$, then:

$$[E_N^+ : C_N^{'}] = h_N \prod_{\chi \neq 1} \prod_{p_i \nmid f_\chi} (\phi(p^{e_i}) + 1 - \chi(p_i)) \neq 0,$$

where h_N^+ is the class number of $\mathbb{Q}(\zeta_N)^+$ and χ runs through the nontrivial even characters of $\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^\times$.

Proof. See Theorem 8.3 in [Was97]. □

Remark. The proof is more technical than the proof of Theorem 1.2.6 but it follows the same line.

In addition, [Was97] reports that Sinnott also showed that there exist a $b \in \mathbb{Z}$ coprime with p such that:

$$[E_N^+ : C_N^+] = 2^b h_N^+.$$

As an immediate consequence of Theorem 1.2.7 we have the following result:

Corollary 1.2.8. *Let C_N'' be the group generated by -1 and*

$$\zeta_N^{\frac{1-a}{2}} \frac{1-\zeta_N^a}{1-\zeta_N} \quad \textit{with} \quad 1 < a < \frac{1}{2}N \quad \textit{and} \quad (a, N) = 1,$$

then:

$$[E_N^+ : C_N''] = h_N^+ \prod_{\chi \neq 1} \prod_{p \mid N} (1 - \chi(p)).$$

Proof. See Corollary 8.8 in [Was97]. □

We end this section by pointing out that if N is compose then the subgroup of cyclotomic units might not have finite index.

1.3 Siegel units

In this section we introduce a particular modular function whose specialization at certain points will produce units in the ring of integers of $\mathbb{Q}(\zeta_N)$. We are particularly interested in the q-expansion of this modular function. We follow closely [KL81] and [Lan87] (which appears to be a summary of [KL81]) omitting the most technical parts and aiming to present the q-expansion as soon as possible. Moreover, as a remark, we point out that [KL81] relies on chapters 18 and 19 of [Lan87].

1.3.1 Siegel functions and Siegel units

For an complete exposition of this paragraph, see Chapter 18 and 19 of [Lan87]. We report in a telegraphic way the essential steps for defining the Siegel functions. As before $\mathcal{H}$ denotes the Poincaré upper half plane and let $\tau \in \mathcal{H}$ so that $\tau\mathbb{Z} \oplus \mathbb{Z}$ is a full lattice in $\mathbb{C}$. Then for any $z \in \mathbb{C}$ we can write:

$$z = a_1\tau + a_2 \quad \text{with} \quad a_i \in \mathbb{R} \quad \text{for} \quad i = 1, 2.$$

Moreover, we denote by q_τ the value $e^{2\pi i \tau}$.

Definition 1.3.1. We define the Dedekind eta function to be:

$$\eta(\tau) = q_\tau^{1/24} \prod_{n=1}^{\infty} (1 - q_\tau^n).$$

Definition 1.3.2. We define the sigma Weierstrass function to be:

$$\sigma(z,\tau) = z \prod_{(a_1,a_2)\in\mathbb{Z}^2\setminus(0,0)} \left(1 - \frac{1}{a_1\tau + a_2} e^{z/(a_1\tau+a_2)+\frac{1}{2}\cdot\left(\frac{z}{(a_1\tau+a_2)}\right)^2}\right).$$

Remark. We report as a fact that the sigma function admits a q_τ-expansion.

Definition 1.3.3. We define the zeta Weierstrass function to be:

$$\zeta(z,\tau) = \frac{\sigma'}{\sigma}(z,\tau).$$

Definition 1.3.4. We define a Klein form to be:

$$\mathfrak{I}(z,\tau) = e^{\frac{-\eta(z,\tau)z}{2}}\sigma(z,\tau).$$

Remark. If $a \in \mathbb{R}^2$ denotes the couple (a_1, a_2) where $a_1\tau + a_2 = z$ then we write $\mathfrak{I}_a(\tau)$ for $\mathfrak{I}(z,\tau)$.

Definition 1.3.5. We define a Siegel function to be:

$$g_a(\tau) = \mathfrak{I}_a(\tau)\Delta(\tau)^{\frac{1}{12}},$$

where $\Delta(\tau)$ denotes the square of the Dedekind eta function.

Following [Lan87] this function admits q_τ-expansion:

$$g_a(\tau) = -q_\tau^{\frac{1}{2}B_2(a_1)} e^{\frac{2\pi i a_2(a_1)-1}{2}}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^{nq_z})(1-q_\tau^n/q_z),$$

where $B_2(x) = x^2 - x + \frac{1}{6}$ denotes the second Bernoulli polynomial and $q_z = e^{2\pi i z/N}$. Moreover the following theorem holds:

Theorem 1.3.6. *Assume that $a \in \mathbb{Q}^2$ has a denominator dividing N, then the Siegel functions are modular functions and they have no zeroes or poles on $\mathcal{H}$.*

Proof. See Theorem 2 of Chapter 19 in [Lan87]. It is a consequence of the formalism of the Klein forms which we didn't investigate. □

Now, if we specialize this function for $z = a$ with $1 < a \leqslant N - 1$ we call these special Siegel functions Siegel units. They have q_τ-expansion:

$$g_a(\tau) = q_\tau^{\frac{1}{12}}(1-\zeta^a)\prod_{n>0}(1-q_\tau^n\zeta^a)(1-q_\tau^n\zeta^{-a}).$$

Remark. Needless to say, in the case of $X_0(1)$, these are cusps forms.

Remark. Let S be a Riemann surface, we denote by $\mathcal{O}_S$ the ring of holomorphic functions. In light of Theorem 1.3.6 we notice that the Siegel function g_a belongs to $\mathcal{O}^\times_{Y_1(N)}$.

It is clear that Siegel units are units in the ring of holomorphic functions of $\mathcal{H}$, i.e. they are in $\mathcal{O}^\times_{\mathcal{H}}$. Moreover, they deserve the name "units" because when we evaluate these functions we get units for certain rings as the following paragraph will show.

1.3.2 Cyclotomic units revisited

Now we simply write q for q_τ and we consider the quotient of Siegel units:

$$\frac{g_a}{g_b} = \frac{(1-\zeta^a)\prod_{n>0}(1-q^n\zeta^a)(1-q^n\zeta^{-a})}{(1-\zeta^b)\prod_{n>0}(1-q^n\zeta^b)(1-q^n\zeta^{-b})}.$$

By evaluating the previous expression at $q = 0$, namely at one of the cusps, we get $\frac{(1-\zeta^a)}{(1-\zeta^b)}$ which on account of Lemma 1.2.1 is a unit in $\mathbb{Z}[\zeta]$. By considering $g_a(0)$ we get $1 - \zeta^a$ which, in case of N compose (Proposition 1.2.2), is still a unit in $\mathbb{Z}[\zeta]$. As defined in Section 1.2, those are cyclotomic units. Notice that since the Siegel units are modular functions the previous fact means that their evaluation at the cusp ∞ of $X_1(N)$ gives units in the ring of integer of the cyclotomic field $\mathbb{Q}(\zeta_N)$.

Remark. Siegel units don't just give birth to cyclotomic units but they are fundamental in the definition of elliptic units as we will see in Section 3.6.1.

2

Review of p-adic modular forms

2.1 Serre's theory

We now introduce what needed from the theory of the French mathematician Jean-Pierre Serre about p-adic modular forms. A full, crystalline and beautiful explanation can be found in his article ([Ser72]). We also stole a lot of inspiration from the oral lectures of M. Bertolini about *"Modular Forms"*. The main idea is to see p-adic modular forms as limits (in a suitable sense) of classical modular forms with respect to the group $\mathrm{SL}_2(\mathbb{Z})$. All these modular forms may be written as power series in $\mathbb{C}[[q]]$ with $q = e^{2\pi i\tau}$ for $\tau \in \mathcal{H}$. Since we are working with p-adic valuation we restrict our interest to modular forms admitting a representation in power series in $\mathbb{Q}[[q]]$. We will be working only with modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$. An idea about how to extend the concept of p-adic modular forms to different congruence subgroups will be given at the end of this section.

Definition 2.1.1. We denote with M_k the $\mathbb{Q}$-vector space of modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$ of weigh k admitting power series in $\mathbb{Q}[[q]]$.

Notation. From now on p denotes a positive prime integer even when not specified.

2.1.1 p-adic valuation of classical modular forms

As we said, we want to give a meaning to the notion of limit of classical modular forms, therefore we need to find an appropriate definition of distance between classical modular forms. We quickly recap the general meaning of p-adic valuation. Any rational number $\alpha \in \mathbb{Q}$ may be written as $p^n \alpha^{'}$ with p not appearing in the prime factorization of neither the numerator nor the denominator of $\alpha^{'}$.

Definition 2.1.2. In the previous setting we define the order at p of α as:

$$v_p(\alpha) = n.$$

Definition 2.1.3. In the previous setting we define the valuation at p of α as:

$$|\alpha|_p = p^{-v_p(\alpha)}.$$

Example. Let $\alpha_1 = \frac{1}{2}$, $\alpha_2 = \frac{2}{9}$, $\alpha_3 = \frac{36}{7}$ and $p = 3$ then:

$$v_3(\alpha_1) = 0, \quad v_3(\alpha_2) = -2, \quad v_3(\alpha_3) = 2,$$

and therefore:

$$|\alpha_1|_3 = 1, \quad |\alpha_2|_3 = 3^2, \quad |\alpha_3|_3 = \frac{1}{3^2}.$$

Proposition 2.1.4. *Let $p \in \mathbb{Z}$ be a prime number, then $|\cdot|_p$ is a norm on $\mathbb{Q}$.*

Remark. For the pleasure of the reader, we recall that a norm on $\mathbb{Q}$ (and more generally on any field K) is a function

$$|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geqslant 0}$$

satisfying:

1. $|\alpha| \geqslant 0 \ \forall \alpha \in \mathbb{Q}$ and it is zero if and only if $\alpha = 0$,

2. $|\alpha \cdot \beta| = |\alpha||\beta| \ \forall \alpha, \beta \in \mathbb{Q}$,

3. $|\alpha + \beta| \leqslant |\alpha| + |\beta| \ \forall \alpha, \beta \in \mathbb{Q}$.

Definition 2.1.5. In the case a norm on K satisfies the stronger condition $|\alpha + \beta| \leqslant \max\{|\alpha|, |\beta|\}$ $\forall \alpha, \beta \in K$ the norm is called non-Archimedean.

Remark. If we consider two numbers and we say that their p-adic distance is “small”, we are saying that a “big” power of p is dividing their difference.

We wish to work in $\mathbb{Q}$ with the p-adic norm, unfortunately $\mathbb{Q}$ is not complete with respect to this norm. In fact, the sequence $\{\alpha_n\}_n$ with $\alpha_n = 1 + p + \cdots + p^{n-1} + p^n$ is Cauchy but it doesn't admit a limit in $\mathbb{Q}$.

Definition 2.1.6. We denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

It can be proven that $\mathbb{Q}_p$ is not algebraically closed. One may think that analogously to the Archimedean case, once we consider the algebraic closure of $\mathbb{Q}_p$ (which we denote by $\overline{\mathbb{Q}}_p$), then we end up with a complete and algebraically closed field. Alas! The trap is just around the corner: this won't be the case since $\overline{\mathbb{Q}}_p$ is not complete. Fortunately, this is not a infinite loop and we will land to well known shores when we consider the completion of $\overline{\mathbb{Q}}_p$. The new born $\mathbb{C}_p$ is complete and algebraically closed. A full explanation of all this p-adic business is outside the purpose of this text and we redirect the reader to the very instructive and constructive book of Koblitz ([Kob84]). Now it is time to turn again our attention to modular forms. Let's pick $f \in M_k$. We recall that by definition we can write:

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n \quad a_n \in \mathbb{Q} \quad \text{and where} \quad q = e^{2\pi i \tau}. \tag{2.1}$$

In order to define a distance we look at the coefficients of the series defined in (2.1) one by one and consider their p-adic norm. Then, two power series will be close if the n-th coefficient of the power series are p-adically close for any n.

Definition 2.1.7. We define the order of f with respect to p to be:

$$v_p(f) = \inf_n\{v_p(a_n)\}.$$

Definition 2.1.8. We define the valuation at p of f to be:

$$|f|_p = p^{-v_p(f)} = \sup_n\{|a_n|_p\}.$$

Remark. If $g \in M_k$ and $g(\tau) = \sum_{n=0}^{\infty} b_n q^n$ the fact that $|f-g|_p$ is "small" means that the coefficients are p-adically close, namely, a "big" power of p divides $f - g$.

We would like to be sure that if $f \in M_k$ then $v_p(f) \in \mathbb{Z}$. This is indeed guaranteed by a result on the structure of the space of modular forms which we will not investigate. This result claims that any modular form is a finite $\mathbb{C}$-linear combination of two specific modular forms whose q-expansions have coefficients in $\mathbb{Z}$ after the multiplication by a sufficiently big integer.

2.1.2 p-adic modular forms

We start out with giving the following definition of p-adic modular form due to Serre.

Definition 2.1.9. A formal power series $f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Q}_p[[q]]$ is called a p-adic modular form if there exist a sequence $\{f_i\}_i$ of classical modular forms with $f_i \in M_{k_i}$ ($k_i \in \mathbb{Z}$ for $i = 1, 2, \cdots$) such that:

$$\lim_i |f - f_i|_p = 0.$$

Remark. We are requiring that the coefficients of f_i's tend uniformly to the coefficients of f.

Arguably, the previous is a problematic definition since we are left with the problem to associate weights to the new-born p-adic modular forms. In fact, we don't pose any condition on the behavior of the weights of the classical modular forms involved in the limit and therefore they might behave wildly. In the definition we just required the n-th coefficient of the classical sequence to tend p-adically to a_n for any n. Thus, first of all, we need to define a good space where the p-adic weights can live and afterwards we need also to check whether or not Definition 2.1.9 is well posed. In fact, two different sequences of classical modular forms may tend to the same p-adic modular form but the limits of their weights may differ one from the other. Thanks to a theorem of Swinnerton-Dyer about the structure of the algebra of modular forms mod p we can solve the problem of associating a weight to a p-adic modular form. We just report the result and a property of classical modular forms. For all the details, refer to [Ser72].

Theorem 2.1.10 (Swinnerton-Dyer)**.** *Assume $p \geqslant 5$ then the following equality holds:*

$$\widetilde{M}_\infty = \bigoplus_{\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}} \widetilde{M}^\alpha.$$

Instead, if $p = 2, 3$ we have:

$$\widetilde{M}_\infty = \widetilde{M}^0,$$

where $\widetilde{M}_\infty = +_{k \geqslant 0} \widetilde{M}_k$ and $\widetilde{M}^\alpha = \bigcup_{\substack{k \geqslant 0 \\ k \equiv \alpha \\ mod\ (p-1)}} \widetilde{M}_k$ and $\widetilde{M}_k$ is the $\mathbb{F}_p$-vector space of modular forms modulo p (when this makes sense).

Proof. See the original article in [SD72]. □

Remark. In the previous proof it is essential to work with modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$ and on account of this it is not straightforward how to extend this theory to more general congruence subgroups.

Theorem 2.1.11. *Let $m \in \mathbb{Z}_{\geqslant 1}$ and let f and g be two classical modular forms belonging to M_k and M_l respectively. Suppose $f \neq 0$ and assume that:*

$$v_p(f-g) \geqslant v_p(f) + m,$$

then:

(i) $k \equiv l$ *mod* $(p-1)p^{m-1}$ *if* $p \geqslant 3$,

(ii) $k \equiv l$ *mod* 2^{m-2} *if* $p = 2$.

Proof. See Théorème 1 in [Ser72]. □

On account of these facts we are suggested that the right set where to consider weights won't be $\mathbb{Z}$ any longer but it is defined as follows.

Definition 2.1.12. Let p be a prime integer and let n be a positive non-zero integer if $p \neq 2$ or $n \in \mathbb{Z}_{\geqslant 2}$ if $p = 2$, then we define:

$$W_n = \begin{cases} \frac{\mathbb{Z}}{(p-1)p^n\mathbb{Z}} = \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{p^n\mathbb{Z}} & \text{if} \quad p \neq 2 \\ \frac{\mathbb{Z}}{p^{n-2}\mathbb{Z}} & \text{if} \quad p = 2 \end{cases}.$$

We denote by W the space of weights for p-adic modular forms. W is defined to be the projective limit of W_n, namely:

$$W = \varprojlim W_n = \begin{cases} \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p & \text{if} \quad p \neq 2 \\ \mathbb{Z}_2 & \text{if} \quad p = 2 \end{cases}.$$

Once we found the right place of definition of weights, we are given peace with the following result.

Theorem 2.1.13. *Let f be a non zero p-adic modular form and $\{f_i\}_i$ a sequence of modular forms with rational coefficients having f as limit. Let k_i be the weight of f_i for any i. Then, the sequence $\{k_i\}_i$ has a limit k in W which depends on f but not on the sequence $\{f_i\}_i$ chosen.*

Proof. See Théorème 2 in [Ser72]. □

Definition 2.1.14. In the setting of the previous theorem we define $k \in W$ to be the weight of f.

Notation. We denote by $M_k^{(p)}$ the space of p-adic modular forms of weight k for the group $\mathrm{SL}_2(\mathbb{Z})$.

2.1.3 Properties of p-adic modular forms

We introduce here the necessary tools for handling with a good definition of p-adic Eisenstein series which will be studied in the next paragraph. We start out with noticing some analogues of the classical results about modular forms.

Theorem 2.1.15. *Let $f_k \in M_k^{(p)}$ and $f_l \in M_l^{(p)}$ with $k, l \in W$. Assume moreover that:*

(i) $f_k \neq 0$,

(ii) $v_p(f_k - f_l) \geqslant v_p(f_k) + m$ *for* $m \in \mathbb{Z}_{\geqslant 0}$,

then the images of k and l in W are the same.

Proof. First of all, we reduce ourselves to the case of classical modular forms and then exploit Theorem 2.1.11. We notice that *(ii)* implies $f_l \neq 0$. Then we consider two sequences of classical modular forms $\{f_i^k\}_i$ and $\{f_i^l\}_i$ of weights respectively k_i and l_i, tending respectively to f_k and f_l. For i big enough we have that:

$$v_p(f_k) = v_p(f_i^k) \quad \text{and} \quad v_p(f_l) = v_p(f_i^l) \quad \text{and} \quad v_p(f_k - f_l) = v_p(f_k^i - f_l^i),$$

with f_i^k and f_i^l both non-zero. Then *(ii)* can be rephrased as:

$$v_p(f_i^k - f_i^l) \geqslant v_p(f_k) + m,$$

and thanks to Theorem 2.1.11 we conclude k_i and l_i have the same image in W_i and the result follows. □

Corollary 2.1.16. *Let $f = \sum_{n=0}^{\infty} a_n q^n \in M_k^{(p)}$ and assume that there exists a positive integer m such that k is non zero in W_{m+1}, then we have:*

$$v_p(a_0) + m \geqslant inf_{n \geqslant 1} v_p(a_n).$$

Proof. See Corollaire 1 in [Ser72]. □

Remark. Suppose that k is not divisible by $p-1$ then it is not zero in W_1 and $m = 0$. This implies that:

$$v_p(a_0) \geqslant \inf_{n \geqslant 1}(v_p(a_n)).$$

If moreover $v_p(a_n) \geqslant 0$ for any $n \geqslant 1$ we infer $v_p(a_0) \in \mathbb{Z}_p$. In the nutshell, we derived an integral property of the constant term from integral properties of all the other coefficients.

The following corollary will play a central role in the definition of p-adic Eisenstein series.

Corollary 2.1.17. *Let*

$$f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n$$

be a sequence of p-adic modular forms of weights $k^{(i)}$. Assume that:

(i) $a_n^{(i)} \to a_n \in \mathbb{Q}_p$ *uniformly in* $n \geqslant 1$,

(ii) $k^{(i)} \to k \neq 0$ *in* W,

then the $a_0^{(i)}$ *admit a limit* $a_0 \in \mathbb{Q}_p$ *and the series* $f = \sum_{n=0}^{\infty} a_n q^n$ *is a p-adic modular form of weight* k.

Proof. See Corollaire 2 in [Ser72]. □

2.1.4 Example of p-adic modular forms: p-adic Eisenstein series

We start out with recalling the classical definition of Eisenstein series and few facts connected to it. Consider $k \in 2\mathbb{Z}$ bigger than 4 and $\tau \in \mathcal{H}$.

Definition 2.1.18. We define the weight k Eisenstein series to be:

$$E_k(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{(m\tau + n)^k}.$$

We want to underline that $k = 2$ is not admissible since the series in the previous definition doesn't converge. Moreover, we notice that if k is odd then the Eisenstein series would be zero. The restriction to $k \in 2\mathbb{Z}_{\geqslant 4}$ is now clear. Eisenstein series are the most easy example of modular forms and at least in the classical context, the only one. In fact, common theory on modular forms ([DS05]) states that the space of all modular forms is spanned only by two Eisenstein series. More explicitly, the space of modular forms coincides with:

$$\mathbb{C}[E_4, E_6]. \tag{2.2}$$

In other words a modular form of any weight is a $\mathbb{C}$-linear combination of powers and products of the Eisenstein series E_4 and E_6 of weights, respectively, 4 and 6. From the computations below we see that, up to a multiplicative factor, both E_4 and E_6 admit a q-expansion in $\mathbb{Z}[[q]]$. These are the modular forms we addressed at the end of section 2.1.1. Classical theory also shows that $E_k(\tau)$ is a weight k modular form for the group $\mathrm{SL}_2(\mathbb{Z})$ whose q-expansion is:

$$E_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \quad \text{where} \quad \sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1}.$$

We underline the fact that the value of the previous Eisenstein series at 0 (i.e. at the cusp ∞ of the modular curve $X_0(1)$) is connected with the zeta function. The zeta function admits moreover an expression in terms of the so called Bernoulli numbers:

$$\zeta(k) = \sum_{n=1}^{\infty} n^{-k} = (-1)^{\frac{k}{2}-1}\pi^k \frac{2^{k-1}}{k!} B_k,$$

where B_k denotes the k-th Bernoulli number defined as the k-coefficient of the Tailor expansion of $\frac{1}{1-e^t}$, namely:

$$\frac{1}{1-e^t} = \sum_{k=0}^{\infty} \frac{B_k}{k!} t^k.$$

One can moreover show that these numbers are rational so it might seem a good idea to isolate the rational part of the previous formula getting:

$$E_k(\tau) = \frac{(-1)^{\frac{k}{2}}\pi^k 2^{k+1}}{(k-1)!} \left(-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right).$$

The part in the parenthesis is a power series in q with rational coefficients which we will denote by

$$G_k(\tau) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

The idea behind the definition of a p-adic Eisenstein series is to use Corollary 2.1.17 for an appropriate sequence of classical Eisenstein series whose limit will genuinely give birth to a p-adic modular form. The appropriate sequence is given by choosing wisely the weights, as the following lemma suggests.

Lemma 2.1.19. *Pose* $\sigma_{k-1}^{(p)}(n) = \sum_{p \nmid d \mid n} d^{k-1}$ *and consider* $k \in 2W$ *and* $\{k_i\}_{i=1}^{\infty}$ *a sequence with terms in* $2\mathbb{N}$ *satisfying:*

(i) $k_i \geqslant 4$ *for any* $i = 1, \cdots, \infty$*,*

(ii) $k_i \to \infty$ *in the archimedean metric on* $\mathbb{R}$*,*

(iii) $k_i \to k \in W$ *p-adically,*

then $\lim_{i\to\infty} \sigma_{k_i-1}(n) = \sigma_{k-1}^{(p)}(n)$ *uniformly in* $n \geqslant 1$.

Proof. This lemma easily follows from the continuity of the p-adic exponential. It is possible to find more details about this function in chapter IV: p-adic power series of [Kob84] looking at the proposition at page 81. □

Remark. We can actually find such a sequence, for example: $\left\{k_i = 2\sum_{n=1}^{i} p^i\right\}_{i=1}^{\infty}$.

Theorem 2.1.20. *The following expression:*

$$G_k^{(p)} = a_0 + \sum_{n=1}^{\infty} \sigma_{k-1}^{(p)}(n) q^n \quad \textit{where} \quad a_0 = \lim_{i \to \infty} -\frac{B_{k_i}}{2k_i},$$

is a p-adic modular form for any sequence $\{k_i\}_{i=1}^{\infty}$ satisfying the hypothesis of Lemma 2.1.19. Moreover, a_0 is independent of the choice of such a sequence.

Proof. We consider the Eisenstein series G_{k_i} of weight k_i as defined above. Using Lemma 2.1.19 and Corollary 2.1.17 we get that

$$G_k^{(p)} = \lim_{i \to \infty} G_{k_i}$$

is a p-adic modular form of weight k, i.e. $G_k^{(p)} \in M_k^{(p)}$. One can check that it is independent from the sequence chosen. □

Definition 2.1.21. $G_k^{(p)}$ is called the p-adic Eisenstein series of weight k.

Remark. As we were previously pointing out, due to a convergence problem the classical Eisenstein series $E_2(\tau)$ is not a modular form. On the other hand, we see that by taking a sequence $\left\{k_i = 2\sum_{n=0}^{i} p^i\right\}_{i=1}^{\infty}$ for $p \geqslant 3$ the p-adic Eisenstein series $G_2^{(p)}$ is a p-adic modular form of weight 2.

2.2 p-adic modular forms for more general congruence subgroups

The p-adic theory of Serre relies heavily on the theorem of Swinnerton-Dyer about the structure algebra of the space of modular forms modulo p whose proof counts on the fact that only modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$ are considered. The American mathematician Nicholas Michael Katz developed a geometric theory of p-adic modular forms which generalizes the theory of Serre and enables us to construct p-adic modular forms *à la Serre*, namely as p-adic limits, for more general congruence subgroups. We won't investigate this theory and we just need the following definition. It is a good definition in light of theorem 4.5.1 of [Kat72].

Definition 2.2.1. A p-adic modular form of weight k and level group $\Gamma_1(N)$ with nebentypus χ, a Dirichlet character of conductor N, is a p-adic limit of certain classical modular forms $\{f_{k_i}\}$ of weight k_i converging p-adically to k, of level group $\Gamma_1(N)$ and nebentypus χ.

3

About the p-adic Leopoldt formula

The aim of this chapter is to give a modular proof of the p-adic Leopoldt formula. We will here combine all the tools we introduced so far. First of all, we state properly the result we are after.

Theorem 3.0.1 (Leopoldt)**.** *Let χ be a non trivial even primitive Dirichlet character of conductor N, then:*

$$L_p(1,\chi) = -\frac{(1-\chi(p)p^{-1})}{\mathfrak{g}(\chi^{-1})}\sum_{a=1}^{N-1}\chi^{-1}(a)\log_p(1-\zeta^a).$$

Remark. It is also possible to prove this result in a more computational way. For details see theorem 5.18 in [Was97].

Before starting let's have a quick overview at the hypotheses of this theorem. We know that we can rewrite a classical L-function associated to a non-primitive character as a product of L-functions associated to primitive characters inducing it. Therefore, it makes sense to restrict our interest to the case of primitive characters. Moreover, the character is assumed to be even because the p-adic L-function associated to a odd character is always zero as it is clarified in the Appendix A.1.

In this chapter we follow the approach of [BCD$^+$14] and we also took some material from [Iwa72]. We are looking for a p-adic equivalent of the class number formula and we are about to work with functions defined on $\mathbb{C}_p$. We then need a theory to handle with these new functions. First of all, in the next paragraph we give some intuition about the right approach to cope with this new setting.

3.1 Rigid geometry

The so called rigid geometry is a natural way to work in this new environment. For a complete overview on this subject we redirect the reader to the formal and exhaustive book of Bosch: [Bos14]. We accept to work with as little rigid geometry as possible and we just try to motivate why it is possible to treat rigid analytic functions as we would do with holomorphic complex functions. At the beginning, one might be tempted to introduce the following notion of "$\mathbb{C}_p$-holomorphiticity" considering on $\mathbb{C}_p$ the topology induced by the p-adic metric.

Definition 3.1.1 (first attempt: locally rigid analytic functions)**.** Let U be a subset of $\mathbb{C}_p$. We say that the function f is rigid analytic in $x \in U$ if there is a open neighbourhood of x inside U where f can be expressed as a power series, namely:

$$f(q) = \sum_{n=1}^{\infty} a_n q^n,$$

where a_n are coefficients in $\mathbb{C}_p$. A function is rigid analytic on U if it is rigid analytic at all the points of U.

This definition is inspired from the complex theory but, unfortunately, has to be revised because of the different topological properties connected to a non-Archimedean distance. Firstly, we notice that the analogous of this definition for the complex case works properly because $\mathbb{C}$ is connected. Suppose we are considering a function defined on a connected area of $\mathbb{C}$, and suppose we have an expression in power series of f on each open set of our covering. The condition about connection guarantees all the opens will overlap and therefore we can extend the power series on the whole connected area. This is not the case for $\mathbb{C}_p$ when we consider on it the topology induced by a non-Archimedean distance. It will turn out that $\mathbb{C}_p$ is totally disconnected, i.e. any subset of $\mathbb{C}_p$ consisting in more than one point is not connected. Since the topology of $\mathbb{C}_p$ we are working with is induced by the p-adic distance a basis for the open sets is given by the open balls:

$$B(x, r) = \{s \in \mathbb{C}_p \text{ such that } |x - s|_p < r\}. \tag{3.1}$$

Analogously, a basis of closed sets is given by the closed balls:

$$\overline{B(x, r)} = \{s \in \mathbb{C}_p \text{ such that } |x - s|_p \leqslant r\}. \tag{3.2}$$

Eventually, both these kinds of balls are open and close. This is a direct consequence of the non-Archimedean nature of the p-adic norm. In fact, in a p-adic setting we need to take care of the following different behaviour of the norm.

Proposition 3.1.2. *Let a, b be two numbers in $\mathbb{C}_p$ such that $|a|_p < |b|_p$ then:*

$$|a - b|_p = \max\{|a|_p, |b|_p\}.$$

This proposition implies that if we consider any triangle in $\mathbb{C}_p$ then it is always isosceles. Moreover, when we consider a ball in $\mathbb{C}_p$, any of its points might be taken as the center of it. As we were saying, another important consequence for the topology is that $B(x,r)$ and $\overline{B(x,r)}$ are both open and closed. In fact we easily see that $\overline{B(x,r)} = \bigcup_{y \in \overline{B(x,r)}} B(y,r)$ and if we consider an accumulation point of $B(x,r)$ then it belongs to $B(x,r)$. The most critical side effect of Proposition 3.1.2 is the following result.

Proposition 3.1.3. *$\mathbb{C}_p$ is totally disconnected, i.e. any subset with more than two points is not connected.*

Proof. Let $A \subset \mathbb{C}_p$ be a set with more than two elements, and assume $x, y \in A$ and $x \neq y$. We then define $r = \frac{1}{2}|x - y|_p$ and we consider $A_1 = A \cap B(x,r)$ and $A_2 = A \backslash A_1$. Then $A_1 \sqcup A_2 = A$ (namely, A is a disjoint union) and both A_1 and A_2 are open and closed. □

This proposition is rather astonishing. Just to give an idea we notice that we cannot now define any longer a function from the connected interval $[0,1]$ to $\mathbb{C}_p$ wishing it is non constant (the image, in fact, should be connected). In particular, a theory of integration in a classical sense is not feasible any longer. This means we cannot directly p-adically rephrase a Cauchy theory relating functions defined by differentiation and functions defined in terms of power series. The problem related to Definition 3.1.1 is now clear: we consider the open disc $B(0,1)$ and we extract a partition in disjoint discs of $B(0,1)$ from the following union where $r \in (0,1) \subset \mathbb{R}$:

$$B(0,1) = \bigcup_{\substack{x \in B(0,1) \\ r \in (0,1)}} B(x,r).$$

We call the disc of the disjoint partition D_i. Then we define on each D_i a constant function getting the value $f_i \in \mathbb{C}_p$. We take care that $f_i \neq f_j$ if $i \neq j$. Eventually we consider the function f on $B(0,1)$ such that $f_{|_{D_i}} = f_i$. This function is locally rigid analytic according to Definition 3.1.1 but its behavior is totally wild; in fact, it doesn't admit an expression in power series on the whole $B(0,1)$. This unpredictable behavior is due to the fact that the open of the covering we considered do not overlap. One way to avoid this issue is to consider the following definition.

Definition 3.1.4. A function f is said to be p-adic analytic on $B(0,r)$ if it is represented by a power series converging on $B(0,r)$.

This definition is indeed a good p-adic equivalent of the complex one. The downside is that we are working with only an open and therefore no much flexibility is allowed in this context. Nevertheless, definition 3.1.4 will be sufficient for our purposes since it is enough to work just in a neighbourhood of the cusp ∞ as we will see later. Therefore, in this text, being rigid analytic means to be p-adic analytic.

Anyway, we think we have enough motivated the need of a different theory in the investigation of spaces with non-Archimedean norm. As we were saying before the right setting to study these objects is rigid geometry, a theory so wide and charming that even a quick overview of the main concepts would require some pages. Again, we redirect the reader to [Bos14], and, as we said, we handle with rigid analytic functions as function admitting an expression in power series just in some areas and such that they behave as holomorphic functions. The domain of definition of these rigid analytic function won't be $\mathbb{C}_p$ with the topology induced by the p-adic norm as in our first attempt but rigid spaces (whose invention is due to Tate) equipped with the so-called *Grothendieck topology.*

3.2 The ordinary locus

The rigid analytic space we will be working with is the so called *ordinary locus.* It is a subset of the modular curve $X_1(N)$ over $\mathbb{C}_p$ as we defined it in Section 1.1.4. We denote this curve $X_1(N)(\mathbb{C}_p)$. We didn't clarify at that time if any type of correspondence of isomorphism classes of elliptic curves is still reasonable in this p-adic context. The following theorem gives some lights about this question at least for some N but, before stating it, we need to give a meaning to the concept of an elliptic curve defined over any $\mathbb{Q}$-algebra R.

Definition 3.2.1. An elliptic curve over R is a smooth projective curve of genus one over R.

In the case R is a field we can consider the Weierstrass equation (1.1) we gave in the first chapter:

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

with coefficients in $\mathbb{Q}$ and we just consider its solutions in the chosen $\mathbb{Q}$-algebra R.

Theorem 3.2.2. *Let $N \geqslant 5$, then the functor:*

$$\mathbb{Q}\text{-}\mathit{Alg} \longrightarrow \mathit{Set}$$

between $\mathbb{Q}$-algebras and sets, sending R to the set given by isomorphism classes of elliptic curves over R together with a point of exact order N, is a representable functor and it is represented by the algebraic variety $Y_1(N)/\mathbb{Q}$.

This allow us to attach to any point of our affine curve $Y_1(N)(\mathbb{C}_p)$ an isomorphism class of elliptic curves defined over $\mathbb{C}_p$ and a point of exact order N. In addition, we notice that $X_1(N)(\mathbb{C}_p) = X_1(N)(\mathcal{O}_{\mathbb{C}_p})$ where $\mathcal{O}_{\mathbb{C}_p} = \{s \in \mathbb{C}_p \text{ such that } |s|_p \leqslant 1\}$. In fact, the curve is projective and therefore we can multiply by a non-zero factor the coordinates of the points. Now we consider the following reduction map:

$$X_1(N)(\mathbb{C}_p) = X_1(N)(\mathcal{O}_{\mathbb{C}_p}) \longrightarrow X_1(N)(\overline{\mathbb{F}}_p),$$

where $X_1(N)(\overline{\mathbb{F}}_p)$ has the obvious meaning. The map is given by reducing suitable coordinates of points by the maximal ideal $\mathfrak{M} = \{s \in \mathbb{C}_p \text{ such that } |s|_p < 1\}$ of $\mathcal{O}_{\mathbb{C}_p}$. Now any point of $X_1(N)(\overline{\mathbb{F}}_p)$ is associated to an elliptic curve over $\overline{\mathbb{F}}_p$ which is just the reduction of an elliptic curve over $\mathbb{C}_p$. Now we pull back the points corresponding to supersingular elliptic curves defined as those elliptic curve with zero p^n-torsion for all the n. The number of these points is finite since up to isomorphism the number of supersingular elliptic curves is finite as showed in chapter V: elliptic curves over finite fields of [Sil86], theorem 4.1. The preimage is made of residue discs (namely, discs of radius one) since $\mathfrak{M}$ is the residue disc. We baptize these discs D_i with $i = 1, \cdots, m$ where m is the number of isomorphism classes of supersingular elliptic curves.

Definition 3.2.3 (ordinary locus)**.** The ordinary locus $\mathcal{A}$ is the subset of $X_1(N)(\mathbb{C}_p)$ given by erasing D_i for all i, more explicitly:

$$\mathcal{A} = X_1(N)(\mathbb{C}_p) \backslash \bigcup_{i=1}^{n} D_i.$$

Remark. We state without proving that $\mathcal{A}$ is an example of an affinoid subspace of $X_1(N)(\mathbb{C}_p)$ with a good reduction, i.e. it is a rigid space.

Therefore we will use the following unofficial definition of rigid analytic function.

Definition 3.2.4 (second attempt: rigid analytic function)**.** A rigid analytic function is a function defined over a neighbourhood of the cusp ∞ of the ordinary locus $\mathcal{A}$ and there it admits a representation as a q-expansion, namely, it can be represented in by:

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

For some $a_n \in \mathbb{C}_p$ and $|q|_p < 1$.

3.3 Eisenstein series associated to a Dirichlet character

In this section we elaborate a way to look at Eisenstein series defined together with a Dirichlet character. We will see we can find a p-adic equivalent even in this case and eventually it turns out that p-adic cousins of these functions are rigid analytic. First of all we recall the definition of Dirichlet character we gave in Section 1.1.3 and we clear the setting up.

Definition 3.3.1. A Dirichlet character of conductor N is a group homomorphism:

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

Clearly, any character can be extended to a function over $\mathbb{Z}$ sending $a \in \mathbb{Z}$ to $\chi([a])$ (where $[a]$ denotes the class of a in $\mathbb{Z}/N\mathbb{Z}$) and by letting $\chi([0]) = 0$. With an abuse of notation we will denote with χ also this extension.

Remark. (i) We say that the character χ is even if $\chi(-1) = 1$, odd otherwise.

(ii) Let χ and $\tilde{\chi}$ be two Dirichlet characters of conductor N and M respectively such that $N \mid M$. We say that χ induces $\tilde{\chi}$ if $\tilde{\chi}(a) = \chi(a)$ for any $a \in \mathbb{Z}$ coprime with M.

(iii) We say that a character is primitive if it is not induced by any other character.

Now we consider $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a primitive, non-trivial and even Dirichlet character of conductor N. Then we can associate to it the following Eisenstein series.

Definition 3.3.2. We define the Eisenstein series attached to the Dirichlet character χ to be the following holomorphic Eisenstein series:

$$E_{\chi,k}(\tau) := N^k \mathfrak{g}^{-1}(\overline{\chi}) \frac{(k-1)!}{(2\pi i)^k} \sum_{\substack{(m,n)\in N\mathbb{Z}\times\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{\overline{\chi}(n)}{(m\tau+n)^k},$$

where $\overline{\chi}$ denotes the complex conjugation of the character χ.

This Eisenstein series is a classical modular form of weight k, group level $\Gamma_1(N)$ and nebentype χ according to our Definition 1.1.11. As it happens for the trivial character, if we define $q = e^{2\pi i\tau}$, common analytic theory states we can rewrite this Eisenstein series as the following q-expansion:

$$E_{k,\chi}(q) = L(1-k,\chi) + 2\sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n) q^n,$$

where $\sigma_{k-1,\chi}(n) = \sum_{d\mid n} d^{k-1}$ and $L(1-k,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{1-k}}$.

Remark. The constant term of the previous series inherits the rationality properties of the coefficients $\sigma_{k-1,\chi}(n)$ which belong to $\mathbb{Q}_\chi$ defined as the extension of $\mathbb{Q}$ generated by the values of χ.

Remark. We will need the q-expansion only in a neighbourhood of ∞ therefore, throughout this chapter we always assume $|q|_p < 1$.

Now we are after a good definition for the p-adic equivalent of these Eisenstein series. We saw how to approach this issue for the special case when χ is the trivial character. Leaded by that, we consider the following strict analogous of the trivial case.

Definition 3.3.3. For any prime p, possibly dividing N, we define the ordinary p-stabilisation:

$$E^{(p)}_{k,\chi}(q) = E_{k,\chi}(q) - \chi(p)p^{k-1}E_{k,\chi}(q^p).$$

In this case we decided to directly define the p-adic analogue since the procedure in this case is the same of what we described in Section 2.1.4, namely we can see it as the p-adic limit of classical Eisenstein series $E_{k_i,\chi}$ for an appropriate sequence of weight $\{k_i\}$. Now we have a p-adic modular form and we want to rewrite it in a working way.

Proposition 3.3.4. *The ordinary p-stabilization has the following Fourier expansion:*

$$E^{(p)}_{k,\chi} = L_p\left(1-k,\chi\right) + 2\sum_{n=1}^{\infty}\sigma^{(p)}_{k-1,\chi}(n)q^n,$$

where $L_p(1-k,\chi) = (1-\chi(p)p^{k-1})L(1-k,\chi)$ *and* $\sigma^{(p)}_{k-1,\chi}(n) = \sum_{p\nmid d\mid n}\chi(d)d^{k-1}$.

Proof. Here it suffices to write down the expressions for $E_{k,\chi}(q)$ and $E_{k,\chi}(q^p)$. The only part to focus on is:

$$\sum_{n=1}^{\infty}\sigma_{k-1,\chi}(n)q^n - \sum_{n=1}^{\infty}\chi(p)p^{k-1}\sigma_{k-1,\chi}(n)q^{pn}.$$

We look a the q^m-th coefficient which can be:

1. $\sigma_{k-1,\chi}(m)$ if p doesn't divide m

2. $\sigma_{k-1,\chi}(m) - \chi(p)p^{k-1}\sigma_{k-1,\chi}(m')$ if p divides m (let $m = pm'$).

Writing down the second case explicitly we get that:

$$\sum_{d\mid m}\chi(d)d^{k-1} - \sum_{d'\mid m'}\chi(pd')(pd')^{k-1} = \sum_{p\nmid d\mid m}\chi(d)d^{k-1}.$$

Therefore we conclude:

$$\sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n)q^n - \sum_{n=1}^{\infty} \chi(p)p^{k-1}\sigma_{k-1,\chi}(n)q^{pn} = \sum_{n=1}^{\infty} \sigma_{k-1,\chi}^{(p)}(n)q^n,$$

and the formula holds. □

Remark. According to our Definition 3.2.4 the ordinary p-stabilization is rigid analytic.

As we said, Definition 3.3.3 presents a family of functions which have still an interpretation of p-adic modular forms of weight k and level N_0 the prime to p part of N. Now, if we consider the special case $k = 0$, thanks to the existence of the power series we can say they are rigid analytic functions. In total analogue with the non p-adic case, this point of view allows us to interpret $L_p(1, \chi)$ as the value at the cusp ∞ of the weight 0 Eisenstein series:

$$E_{0,\chi}^{(p)}(q) = L_p(1, \chi) + 2\sum_{n=1}^{\infty} \left(\sum_{p \nmid d \mid n} \chi(d)d^{-1} \right) q^n. \tag{3.3}$$

Our strategy now proceeds as follows: we have a rigid analytic function and in its q-series expression the constant term corresponds to the left hand side of the formula 3.0.1. We want to describe the same function in a different way, namely, with a different q-expression and different constant term which corresponds to the right hand side of formula in Theorem 3.0.1.

3.4 Another way to look at $E_{0,\chi}^{(p)}(q)$

We can find an independent expression for $E_{0,\chi}^{(p)}$ in term of Siegel units, described in Section 1.3. We recall that the Siegel units admit q-expansion:

$$g_a(q) = q^{\frac{1}{12}}(1 - q^n\zeta^a)\prod_{n>0}(1 - q^n\zeta^a)(1 - q^n\zeta^{-a}), \tag{3.4}$$

where ζ denotes a N-th root of unity. We won't go through the details and we just define the p-adic analogue of the Siegel units to be:

$$g_a^{(p)} = g_{pa}(q^p)g_a(q)^{-p}.$$

The expression (3.4) admits a representation in power series in q, therefore so do $g_{pa}(q^p)$ and $g_a(q)$. Since $g_a(q)$ is never zero except at $q = 0$ and since $g_{pa}(q^p)$ is also zero for $q = 0$ with the same order of $g_a(q)^p$, we state without proof that $g_a^{(p)}$ admits a q-expansion and therefore it is rigid analytic. In the classical formula about the class number, Siegel units appear in the form of their logarithm. On account of that, we try to understand if there is any hope that the p-adic logarithm of the Siegel units keeps making sense.

Proposition 3.4.1. *The p-adic logarithm of $g_a^{(p)}$, $\log_p(g_a^{(p)})$, admits the following q-expansion:*

$$\log_p g_a^{(p)} = \log_p\left(\frac{1-\zeta^{ap}}{(1-\zeta^a)^p}\right) + p\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\,|\,n}\frac{\zeta^{ad}+\zeta^{-ad}}{d}\right)q^n,$$

and therefore it is rigid analytic.

Proof. We begin with proving that the q-expansion holds. Writing down explicitly the expression we obtain:

$$\log_p g_a^{(p)} = \log_p\left(\frac{q^{\frac{p}{12}}(1-\zeta^{pa})\prod_{n>0}(1-q^{pn}\zeta^{pa})(1-q^{pn}\zeta^{-pa})}{q^{\frac{p}{12}}(1-\zeta^{a})^p\prod_{n>0}(1-q^{n}\zeta^{a})^p(1-q^{n}\zeta^{-a})^p}\right).$$

Since $n>0$ and by the additivity of the p-adic logarithm we can rewrite the previous expression as follows:

$$\log_p\left(\frac{(1-\zeta^{pa})}{(1-\zeta^a)^p}\right) + \sum_{n=1}^{\infty}\log_p(1-q^{pn}\zeta^{pa}) + \log_p(1-q^{pn}\zeta^{-pa}) - p\log_p(1-q^n\zeta^a) - p\log_p(1-q^n\zeta^{-a}).$$

We recall that even though p-adic logarithm admits an extension to $\mathbb{C}_p^\times$ we can express it in power series only on $D(1+s) := \{1+s\in\mathbb{C}_p : |s|_p<1\}$. Since we assumed that the p-adic norm of q is less than one we can write the summand in the following way:

$$\sum_{n=1}^{\infty}\left(-\sum_{m=1}^{\infty}\frac{q^{pnm}\zeta^{pam}}{m} - \sum_{m=1}^{\infty}\frac{q^{pnm}\zeta^{-pam}}{m} + p\sum_{m=1}^{\infty}\frac{q^{nm}\zeta^{am}}{m} + p\sum_{m=1}^{\infty}\frac{q^{nm}\zeta^{-am}}{m}\right).$$

Now, we want to rewrite the previous expression in the shape:

$$\sum_{k=1}^{\infty}a_kq^k.$$

It is convenient to consider two cases:

- If $p\nmid k$ then we have $a_k = p\sum_{d\,|\,k}\frac{\zeta^{ad}-\zeta^{-ad}}{d}$
- If $p\mid k$, write $k=pk'$ then $a_k = -\sum_{m\,|\,k'}\frac{\zeta^{pam}+\zeta^{-pam}}{m} + p\sum_{d\,|\,k}\frac{\zeta^{ad}+\zeta^{-ad}}{d}$. We notice that if $p\mid d$ there exist unique m such that $pm=d$, so $m=\frac{d}{p}$. Thanks to the minus sign we get:

$$a_k = p\sum_{p\nmid d\,|\,k}\frac{\zeta^{ad}+\zeta^{-ad}}{d}.$$

Therefore, we conclude that we have:

$$\sum_{n=1}^{\infty}\left(-\sum_{m=1}^{\infty}\frac{q^{pnm}\zeta^{pam}}{m} - \sum_{m=1}^{\infty}\frac{q^{pnm}\zeta^{-pam}}{m} + p\sum_{m=1}^{\infty}\frac{q^{nm}\zeta^{am}}{m} + p\sum_{m=1}^{\infty}\frac{q^{nm}\zeta^{-am}}{m}\right) =$$

$$p\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\,|\,n}\frac{\zeta^{ad}+\zeta^{-ad}}{d}\right)q^n,$$

and the formula holds. □

The previous proposition gave a meaning to the p-adic logarithm of Siegel units paving the way to the definition of the following function:

$$h_\chi^{(p)} := \frac{1}{p\mathfrak{g}(\chi^{-1})} \times \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p g_a^{(p)},$$

where $\mathfrak{g}(\chi) := \sum_{a=1}^{N-1} \chi(a)\zeta^a$.

Playing in anticipation, we constructed a function inspired by the classical class number formula result. Our first hope is that it is rigid analytic.

Proposition 3.4.2. $h_\chi^{(p)}$ *admits the following q-expansion:*

$$h_\chi^{(p)} = -\frac{(1-\chi(p)p^{-1})}{\mathfrak{g}(\chi^{-1})} \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^a) + 2\sum_{n=1}^{\infty} \left(\sum_{p\nmid d \mid n} \chi(d) d^{-1} \right) q^n. \tag{3.5}$$

Proof. We start out with writing down $h_\chi^{(p)}$ and with substituting the expression for $\log_p g_a^{(p)}$:

$$\frac{1}{p\mathfrak{g}(\chi^{-1})} \times \sum_{a=1}^{N-1} \chi^{-1}(a) \left(\log_p \left(\frac{1-\zeta^{ap}}{(1-\zeta^a)^p} \right) + p \sum_{n=1}^{\infty} \left(\sum_{p\nmid d \mid n} \frac{\zeta^{ad}+\zeta^{-ad}}{d} \right) q^n \right).$$

We divide the computation in two pieces. The first is:

$$\frac{1}{p\mathfrak{g}(\chi^{-1})} \left(\sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^{pa}) - p \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^a) \right), \tag{3.6}$$

and we want to prove it is equal to:

$$-\frac{(1-\chi(p)p^{-1})}{\mathfrak{g}(\chi^{-1})} \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^a).$$

Assume that $p \nmid N$ so that $\chi(p) \neq 0$ and ζ^p is still a primitive N-th root of unity. Then we can rewrite the expression (3.6) as follows:

$$\frac{1}{p\mathfrak{g}(\chi^{-1})} \left(\chi(p) \sum_{a=1}^{N-1} \chi^{-1}(ap) \log_p(1-\zeta^{pa}) - p \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^a) \right),$$

and therefore, by putting $pa = a$ (we can do this because p and N are coprime) and by gluing together we get:

$$-\frac{(1-\chi(p)p^{-1})}{\mathfrak{g}(\chi^{-1})} \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^a).$$

Now assume $p \mid N$ so that $\chi(p) = 0$. We want to show that:

$$\sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(1-\zeta^{ap}) = 0.$$

We expand the $\log_p$ as a power series and we notice we can exchange the two summands since one is finite, namely:

$$-\sum_{a=1}^{N-1}\chi^{-1}(a)\sum_{n=1}^{\infty}\frac{\zeta^{apn}}{n}=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{a=1}^{N-1}\chi^{-1}(a)\zeta^{apn}.$$

Now we just want to prove that:

$$\sum_{a=1}^{N-1}\chi^{-1}(a)\zeta^{apn}=0.$$

This is indeed a general fact as Lemma A.2.1 shows.

For the second part, we analyze:

$$\frac{1}{p\mathfrak{g}(\chi^{-1})}\sum_{a=1}^{N-1}\chi^{-1}(a)p\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\mid n}\frac{\zeta^{ad}+\zeta^{-ad}}{d}\right)q^n.$$

Again, since the first summand is finite we exchanges order of summation getting:

$$\frac{1}{\mathfrak{g}(\chi^{-1})}\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\mid n}\sum_{a=1}^{N-1}\chi^{-1}(a)\frac{\zeta^{ad}+\zeta^{-ad}}{d}\right)q^n.$$

If $(d,N)\neq 1$ we can apply Lemma A.2.1 which implies:

$$\sum_{a=1}^{N-1}\chi^{-1}(a)\zeta^{ad}=0.$$

Therefore we can consider only cases when d is coprime with N getting:

$$\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\mid n}\chi(d)d^{-1}\frac{1}{\mathfrak{g}(\chi^{-1})}\sum_{a=1}^{N-1}\chi^{-1}(ad)(\zeta^{ad}+\zeta^{-ad})\right)q^n.$$

Under the assumption $(d,N)=1$ and thanks to the fact that χ is even (so $\chi^{-1}(a)\zeta^{-a}=\chi^{-1}(-a)\zeta^{-a}$) we have

$$\sum_{a=1}^{N-1}\chi^{-1}(ad)(\zeta^{ad}+\zeta^{-ad})=\sum_{a=1}^{N-1}\chi^{-1}(a)(\zeta^{a}+\zeta^{-a})=2\sum_{a=1}^{N-1}\chi^{-1}(a)\zeta^{a}=2\mathfrak{g}(\chi^{-1}),$$

and finally we obtain:

$$\frac{1}{p\mathfrak{g}(\chi^{-1})}\sum_{a=1}^{N-1}\chi^{-1}(a)p\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\mid n}\frac{\zeta^{ad}+\zeta^{-ad}}{d}\right)q^n=2\sum_{n=1}^{\infty}\left(\sum_{p\nmid d\mid n}\chi(d)d^{-1}\right)q^n,$$

as we wanted to show. □

Remark. We just proved $h_\chi^{(p)}$ admits a q-expansion around the cusp ∞, therefore it is rigid analytic.

We finally have all the ingredients to face the last step and to give a modular proof of the Leopoldt formula.

3.5 The Leopoldt formula

In this section we prove the Leopoldt formula as it is stated in Theorem 3.0.1. We defined two p-adic modular forms of weight 0, group level $\Gamma_1(N_0)$ and nebentype χ: $E_{0,\chi}^{(p)}$ and $h_\chi^{(p)}$. We proved they are rigid analytic on the residue disc of the cusp ∞, namely, they admit a q-expansion for $|q|_p < 1$. The q-expansion of (3.3) and (3.5) are rather similar: the only difference is in the constant term. So, let's denote $g = E_{0,\chi}^{(p)} - h_\chi^{(p)}$ which is constant at the residue disc of the cusp ∞. As both $h_\chi^{(p)}$ and $E_{0,\chi}^{(p)}$ are p-adic modular forms of nebentypus character $\chi \neq 1$ we infer that also their difference g must have nebentype character $\chi \neq 1$. Since g is constant this clearly implies that $g = 0$ and therefore:

$$E_{0,\chi}^{(p)} = h_\chi^{(p)}.$$

By equating the constant term of (3.3) and (3.5) we find:

$$L_p(1,\chi) = -\frac{(1-\chi(p)p^{-1})}{\mathfrak{g}(\chi^{-1})}\sum_{a=1}^{N-1}\chi^{-1}(a)\log_p(1-\zeta^a),$$

and Theorem 3.0.1 is proved.

□

3.6 Conclusion

As we pointed out this formula has a strict relationship with the classical one. The most interesting phenomenon is the relation between the p-adic logarithm of certain units and the L-functions. The question raising naturally is whether or not we can reach an even more general level of generality and in which contest. The answer turns out to be positive and the next aspect to investigate is an analogous of this formula due to Katz. This new path starts with a different and more general definition of p-adic modular forms respect to the approach of Serre and it induces also a different definition of p-adic L-function. We won't introduce this new theory but we have a quick overview of the result of Katz. We first need to introduce an analogous of the cyclotomic units.

3.6.1 Elliptic units

It is easy to see that the ring of the endomorphisms of an elliptic curve can be either isomorphic to $\mathbb{Z}$ or to an order in the ring of integers of a quadratic imaginary field. This fact suggests the following definition.

Definition 3.6.1. We say that an elliptic curve has complex multiplication when its endomorphisms ring is isomorphic to an order in the ring of integers of an imaginary quadratic field. Moreover, we say that an elliptic curve E has complex multiplication by $\mathcal{O}$ with $\mathcal{O}$ an order in the ring of integers of an imaginary quadratic field if $\mathrm{End}(E) \cong \mathcal{O}$.

Example. Let's consider the elliptic curves:

$$\mathbb{C}/(\mathbb{Z} \oplus i\mathbb{Z}) \quad \text{and} \quad \mathbb{C}/(\mathbb{Z} \oplus \sqrt[3]{-3}\mathbb{Z}),$$

then the endomorphism group of the first elliptic curve is $\mathbb{Z}[i]$ which corresponds to the ring of integers of $\mathbb{Q}(i)$ while it is easy to check that the endomorphisms ring of the second elliptic curve is $\mathbb{Z}$. Therefore, the first is an elliptic curve with complex multiplication by $\mathbb{Z}[i]$ while the second is an elliptic curve without complex multiplication.

It is also clear that having complex multiplication is invariant under isomorphism of elliptic curves. Even more: the endomorphism ring is the same. In fact, two elliptic curves of lattices respectively Λ_1 and Λ_2 are isomorphic if there exists a $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$. Suppose $\mathcal{O}_1$ and $\mathcal{O}_2$ are the corresponding homomorphism rings and let $\beta \in \mathcal{O}_1$, then
$\beta\Lambda_2 = \beta\alpha\Lambda_1 = \alpha\beta\Lambda_1 \subset \alpha\Lambda_1 = \Lambda_2$, therefore, $\beta \in \mathcal{O}_2$. We infer that $\mathcal{O}_1 \subset \mathcal{O}_2$. An analogous reasoning shows that $\mathcal{O}_2 \subset \mathcal{O}_1$ implying that $\mathcal{O}_1 = \mathcal{O}_2$.
Modular curves have another type of special points besides the cusps: the CM-points. Those points correspond under the maps defined in the Introduction to elliptic curves having complex multiplication (from which the name CM comes). The surprising fact is that by computing special modular functions (in our case we will consider modular units) at these points we get units (elliptic units) for the ray class field of K as we will soon see. These units play the same role of the circular units for cyclotomic fields.

Definition 3.6.2. We define the Eisenstein series attached to a character χ of conductor N to be:

$$E_{\chi,k}(\tau) := N^k \mathfrak{g}^{-1}(\overline{\chi}) \frac{(k-1)!}{(2\pi i)^k} \sum_{\substack{(m,n) \in N\mathbb{Z}\times\mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{\overline{\chi}(n)}{(m\tau + n)^k},$$

where $\tau \in \mathcal{H}$ the Poincaré upper half plane. Notice that in the sum we are not taking the zero element.

Moreover, we define $q = e^{2\pi i\tau}$.
We then assume:

- K has class number one.

- $\mathcal{O}_K^* = \pm 1$.
- $\Delta_K := D$, the discriminant of the field K, is odd and negative.
- There exists an integral ideal $\mathfrak{n} \subset \mathcal{O}_K$ such that:

$$\frac{\mathcal{O}_K}{\mathfrak{n}} = \frac{\mathbb{Z}}{N\mathbb{Z}}.$$

In addition we baptize:

- $\tau_{\mathfrak{n}} := \frac{b+\sqrt{D}}{2N}$,
- $\mathfrak{n} := \mathbb{Z}N + \mathbb{Z}\frac{b+\sqrt{D}}{2}$.

Suppose we have a Dirichlet character, we can then define from an even character χ a character of finite order $\chi_{\mathfrak{n}}$ over the ideals of K (which are all principal since its class number is one) out of the rule:

$$\chi_{\mathfrak{n}}(\alpha) := \chi(\alpha \bmod \mathfrak{n}),$$

where $\alpha \in K$ and notice that $(\alpha \bmod \mathfrak{n}) \in \frac{\mathbb{Z}}{N\mathbb{Z}}$. Moreover, we notice that, thanks to the shape of $\mathfrak{n}$, we infer:

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{b+\sqrt{D}}{2}.$$

Definition 3.6.3. We define a CM-point to be:

$$\tau_{\mathfrak{n}} := \frac{b+\sqrt{D}}{2N}.$$

Remark. We notice that the element $\tau_{\mathfrak{n}}$ in $\mathcal{H}$ corresponds to the isomorphism class of the elliptic curve $E = \mathbb{C}/\mathbb{Z} \oplus \frac{b+\sqrt{D}}{2N}\mathbb{Z}$. The endomorphism ring of E is not $\mathbb{Z}$ since, for instance, $2N\sqrt{D} \in \mathrm{End}(E)$, and therefore, according to our Definition 3.6.1, it is an elliptic curve with complex multiplication. We also infer that any element of the class $\left[\mathbb{C}/\mathbb{Z} \oplus \frac{b+\sqrt{D}}{2N}\mathbb{Z}\right]$ has complex multiplication.

In order to get some confidence with these new objects we are working with we prove the following result.

Proposition 3.6.4. *The following equality holds:*

$$E_{k,\chi}(\tau_{\mathfrak{n}}) = N^k \mathfrak{g}^{-1}(\overline{\chi}) \frac{(k-1)!}{(2\pi i)^k} L(K, \chi_{\mathfrak{n}}, k, 0),$$

where $L(K, \chi_{\mathfrak{n}}, k_1, k_2) := \sum_{0 \neq \alpha \in \mathcal{O}_K} \chi_{\mathfrak{n}}(\alpha) \alpha^{-k_1} \alpha^{-k_2}$.

Proof. In order to get the formula we need to prove that:

$$\sum_{0 \neq \alpha \in \mathcal{O}_K} \chi_{\mathfrak{n}}(\alpha)\alpha^{-k} = \sum_{\substack{(m,n) \in N\mathbb{Z} \times \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{\chi(n)}{(m\tau_{\mathfrak{n}} + n)^k}.$$

We notice that $m\tau_{\mathfrak{n}} + n \in \mathcal{O}_K$ $\forall (m,n) \in N\mathbb{Z} \times \mathbb{Z}$ and $m\tau_{\mathfrak{n}} + n \bmod \mathfrak{n} = n \bmod \mathfrak{n}$, so:

$$\sum_{\substack{(m,n) \in N\mathbb{Z} \times \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{\chi(n)}{(m\tau_{\mathfrak{n}} + n)^k} = \sum_{\substack{(m,n) \in N\mathbb{Z} \times \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{\chi_{\mathfrak{n}}(m\tau_{\mathfrak{n}} + n)}{(m\tau_{\mathfrak{n}} + n)^k} = \sum_{0 \neq \alpha \in \mathcal{O}_K} \chi_{\mathfrak{n}(\alpha)}\alpha^{-k},$$

where the last equality is due to the fact that, by definition we have:

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{b + \sqrt{D}}{2}.$$

□

We now proceed to the definition of elliptic units.

Definition 3.6.5. We define the elliptic units to be the evaluation of the Siegel functions g_a at the CM points, namely:

$$u_{a,\mathfrak{n}} = g_a(\tau_{\mathfrak{n}})$$

Remark. The name unit in the previous definition is not meaningless in fact the elliptic units lie in $\mathcal{O}^{\times}_{K_{\mathfrak{n}}(\mu_N)}$ where $K_{\mathfrak{n}}$ denotes the ray class field of K.

3.6.2 Katz formula

We have already seen the Katz p-adic L-function in the context of Section 3.6.1, precisely in Proposition 3.6.4. It is:

$$L(K, \chi_{\mathfrak{n}}, k_1, k_2) = \sum_{\substack{\alpha \in \mathcal{O}_K \\ \alpha \neq 0}} \chi_{\mathfrak{n}}(\alpha)\alpha^{-k_1}\alpha^{-k_2}.$$

The fundamental article where this theory is shaped is due to Katz ([Kat72]). We just state the result which relates the values of the p-adic L-function with the p-adic logarithm of elliptic units. The setting of the theorem is outlined in Section 3.6.1.

Theorem 3.6.6 (Katz)**.** *Let χ be a non-trivial even primitive Dirichlet character of conductor N and let K be a quadratic imaginary field equipped with an ideal $\mathfrak{n}$ satisfying $\mathcal{O}_K/\mathfrak{n} = \mathbb{Z}/N\mathbb{Z}$. Let $\chi_{\mathfrak{n}}$ be the ideal character of K associated to the pair $(\chi, \mathfrak{n})$, then*

$$L_p(K, \chi_{\mathfrak{n}}, 0) = -\frac{(1 - \chi_{\mathfrak{n}}(\mathfrak{p})p^{-1})}{\mathfrak{g}(\overline{\chi})^{-1}} \times \sum_{a=1}^{N-1} \chi^{-1}(a) \log_p(u_{a,\mathfrak{n}}).$$

The important fact is that the techniques required in the proof of this theorem are analogous and a generalization of the techniques used in the proof of the Leopoldt formula.

A

Some results

A.1 About the p-adic L-function

Here we refer to the definition of analyticity in $\mathbb{C}_p$ as stated in Definition 3.1.4. Our way to define the p-adic L- function is to interpolate the classical L-function at the values it assumes on the integers. The following result realizes this idea of p-adic L-function.

Theorem A.1.1. *Let χ be a primitive Dirichlet character of conductor $f \geqslant 1$ then there exists a p-adic analytic function $L_p(\chi, s)$ on $B(R) = \{s \in \mathbb{C}_p$ such that $|s|_p < R\}$ with $R > 1$ except for a simple pole at $s = 1$ with residue $1 - \frac{1}{p}$ when the character is trivial, satisfying:*

$$L_p(\chi, n) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}.$$

Here the $B_{n,\chi\omega^{-n}}$ denotes the generalized Bernoulli numbers and the character $\chi\omega^{-n}$ is defined as the primitive character associated to:

$$\left(\frac{\mathbb{Z}}{\operatorname{lcm}(\text{conductor of } \chi, \text{conductor of } \omega^{-n})\mathbb{Z}}\right)^{\times} \to \mathbb{C}^{\times},$$

sending a to $\chi(a)\omega^{-n}(a)$ (here ω denotes the Teichmüller character). We want to show that in case χ is an odd character the p-adic L-function as defined above is equally zero. One can compute that the generalized Bernoulli numbers are zero for χ odd therefore L_p is zero on $\mathbb{Z}$ and, since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ we infer by continuity that L_p is zero $\mathbb{Z}_p$ as well. From our definition of analyticity, the power series representing L_p must be equally zero in $B(1)$ and therefore on the all $B(R)$.

A.2 Characters theory

Lemma A.2.1. *Define $\tau(b,\chi) := \sum_{a=1}^{N-1}\chi(a)\zeta^{ab}$ with χ a Dirichlet primitive character of conductor N and ζ a N-th root of unity. If $(b,N) \neq 1$ and χ is primitive, then $\tau(b,\chi) = 0$.*

Proof. First of all we claim that if χ is primitive than for any $N^{'} \mid N$ there exists a $c \in \mathbb{Z}$ such that $c \equiv 1 \bmod N^{'}$, $(c,N) = 1$ and $\chi(c) \neq 1$. In fact, if we consider the sequence $\{c_n\}$ with $c_n := 1 + nN^{'}$ then $c_n \equiv 1 \bmod N^{'}$. Moreover, we notice that there exists a c_i which is coprime with N, for instance we can consider c_d with $d := (b,N)$. Now, suppose that for any c such that $c \equiv 1 \bmod N^{'}$ and $(c,N) = 1$ we have $\chi(c) = 1$, this implies that χ is induced by a character modulo $N^{'}$ against the assumption that χ is primitive. In fact, if we consider $a, b \in \mathbb{Z}$ such that $a \equiv b \bmod N^{'}$ but $a \not\equiv b \bmod N$ then we can infer that $\chi(ab^{-1}) = 1$ since $ab^{-1} \equiv 1 \bmod N^{'}$. Thus $\chi(a) = \chi(b)$. So χ is induced by that character $\chi^{'}$ of conductor $N^{'}$ defined as $\chi^{'}(a) := \chi(a)$. As this is against the hypothesis that χ is primitive, we conclude that there exists a $c \in \mathbb{Z}$ satisfying:

- $c \equiv 1 \bmod N^{'}$
- $(c,N) = 1$
- $\chi(c) \neq 1$

Now we notice that if $\zeta \in \mathbb{C}_p$ is a primitive N-th root of one, $N = dN^{'}$ and $b = db^{'}$ (where $d = (b,N)$), then ζ^b is a primitive $N^{'}$-th root of one. In fact, clearly it is a $N^{'}$-th root of one and it is primitive because if $\zeta^{bs} = 1$ with $s \leqslant N^{'}$ then $N \mid bs$ so $s \geqslant N^{'}$ and we conclude $s = N^{'}$. Under the assumption that $c \equiv 1 \bmod N^{'}$ then $\zeta^{bc} = \zeta^{(1+kN^{'})b} = \zeta^b$ with $k \in \mathbb{Z}$.
So:

$$\tau(b,\chi) = \chi^{-1}(c)\sum_{a=1}^{N-1}\chi(ac)\zeta^{ab} = \chi^{-1}(c)\sum_{a=1}^{N-1}\chi(ac)\zeta^{acb} = \chi^{-1}(c)\tau(b,\chi)$$

Implying $\tau(b,\chi) = 0$ since $\chi^{-1}(c) \neq 1$. □

Lemma A.2.2. *Let G be a finite abelian group and f a function from G to any field of characteristic zero, then the following holds:*

$$det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau\neq 1} = \prod_{\chi\in\widehat{G}\backslash\{1\}}\sum_{\sigma\in G} f(\sigma)\chi(\sigma).$$

Proof. See Lemma 5.26 part (b) in [Was97]. □

A.3 Algebraic number theory

Lemma A.3.1. *We consider a field K. Let A be a subgroup generated by $\{\epsilon_1, \cdots, \epsilon_s\}$ with ϵ_i independent elements of the units group of K and by the roots of unity in K. Let B be a subgroup generated by $\{\eta_1, \cdots, \eta_s\}$ with η_j independent and in the group of unity of K. Suppose $A \subset B$ has finite index then:*

$$[B : A] = \frac{Reg(\{\epsilon_i\}_{i=1}^s)}{Reg(\{\eta_j\}_{j=1}^s)}.$$

Proof. We choose $\{\sigma_k\}_{k=1}^s$ a complete set of endomorphism of K into $\mathbb{C}$ distinct and pairwise not conjugate. Then by definition we have:

$$\mathrm{Reg}(\{\epsilon_i\}_{i=1}^s) = |\det(n_k \log|\sigma_k(\epsilon_i)|)_{i,k=1}^s|.$$

We notice that we can write:

$$\epsilon_i = \left(\prod_{j=1}^s \eta_j^{a_{i,j}}\right) \cdot (\text{root of unity}).$$

Therefore:

$$n_k \log|\sigma_k(\epsilon_i)| = \sum_{j=1}^s n_k a_{i,j} \log|\sigma_k(\eta_j)|,$$

and:

$$(n_k \log|\sigma_k(\epsilon_i)|)_{i,k=1}^s = (a_{i,j})_{i,j=1}^s (n_k \log|\sigma_k(\eta_j)|)_{j,k=1}^s.$$

So we conclude:

$$\frac{\mathrm{Reg}\{\epsilon_i\}_{i=1}^s}{\mathrm{Reg}\{\eta_j\}_{j=1}^s} = |\det(a_{i,j})_{i,j=1}^s|.$$

From the theory of elementary divisor we know we can find two integral matrices M, N such that $M(a_{i,j})N = \mathrm{diag}(d_1, \cdots, d_s)$ such that their determinant is ± 1. These matrices correspond to the change basis of A and B so there exist basis $\{x_1, \cdots, x_s\}$ for A and $\{y_1, \cdots, y_s\}$ for B such that $x_i = d_i y_i$. Thus $B/A \cong \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}$ and $[B : A] = |\prod_i d_i|$ proving the lemma. □

Lemma A.3.2. *Let m, k be positive integers such that $k < m$ and p an odd prime, then following formula holds:*

$$1 - x^{p^k} = \prod_{j=0}^{p^k-1} (1 - x\zeta_{p^m}^{jp^{m-k}}).$$

Proof. We have the following expressions:

$$x^{p^k} - 1 = \prod_{j=0}^{p^k-1} (x - \zeta_{p^k}^j) = \prod_{j=0}^{p^k-1} \zeta_{p^k}^j (x\zeta_{p^k}^{-j} - 1).$$

So:

$$1 - x^{p^k} = \prod_{j=0}^{p^k-1}(1 - \zeta_{p^k}^j x) = \prod_{j=0}^{p^k-1}(1 - \zeta_{p^m}^{jp^{m-k}} x).$$

□

Remark. We just notice that for p a prime integer and $k < m$ two positive integers this lemma implies:

$$1 - \zeta_{p^k}^b = 1 - \zeta_{p^m}^{bp^k} = \prod_{j=0}^{p^k-1}(1 - \zeta_{p^m}^{b+jp^{m-k}}) = \prod_{\substack{j=1 \\ j \equiv b \bmod p^k}}^{p^m} (1 - \zeta_{p^m}^j).$$

In this section we relied on [Was97] and [Ste17].

Theorem A.3.3. $\mathbb{Z}[\zeta_N]$ *is the ring of integers of* $\mathbb{Q}(\zeta_N)$.

Proof. See Theorem 2.6 in [Was97]. □

Definition A.3.4. Let K be a number field which has degree $r + 2s$ over $\mathbb{Q}$ with r real and $2s$ complex embeddings into $\mathbb{C}$. We consider a set $\{\sigma_i\}_{i=1}^{r+s}$ of distinct, pairwise non-conjugate embeddings of K into $\mathbb{C}$. We define the regulator of the set $\{\epsilon_1, \cdots, \epsilon_{r+s-1}\}$ where $\epsilon_i \in K^\times$ are elements of norm ± 1 as follows:

$$\mathrm{Reg}(\epsilon_1, \cdots, \epsilon_{r+s-1}) = |(n_i \log(\sigma_i(\epsilon_j)))_{i,j=1}^{r+s-1}|.$$

Where $n_i = 1$ if σ_i is a real embedding and $n_i = 2$ otherwise. If $\{\epsilon_1, \cdots, \epsilon_{r+s-1}\}$ is a set of fundamental unit for the ring of integer of K, then its regulator is called the regulator of K. In case the ring of integers has finite unit group we pose the regulator of K to be 1.

Bibliography

[BCD^{+}14] M. Bertolini, F. Castella, H. Darmon, S. Dasgupta, K. Prasanna, and V. Rotger, *p-adic L-functions and Euler systems: a tale in two trilogies*, Lecture note series 414, vol. I, Cambridge University Press, 2014.

[Bos14] S. Bosch, *Lectures on formal and rigid geometry*, Lecture Notes in Mathematics 2105, Springer International Publishing, 2014.

[Dar11] H. Darmon, *L-functions and modular forms*, 2011, http://www.math.mcgill.ca/darmon/courses/11-12/nt/notes/lecture1.pdf.

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics 228, Springer-Verlag, New York, 2005.

[For99] O. Forster, *Lectures on riemann surfaces*, Spinger-Verlag, 1999.

[Iwa72] K. Iwasawa, *Lecture on p-adic l-functions*, Annals of Mathematics Studies, Princeton University Press, 1972.

[Kat72] N. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III, Springer, Berlin, 1972, pp. 73–190.

[KL81] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, New York, 1981.

[Kob84] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Spinger-Verlag, 1984.

[Lan87] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics 112, Springer-Verlag, New York, 1987.

[Lan90] ———, *Cyclotomic fields i and ii*, Graduate Texts in Mathematics 121, Springer-Verlag, New York, 1990.

[Mar77] D. A. Marcus, *Number fields*, Springer-Verla, New York, 1977.

[Mir95] R. Miranda, *Algebraic curves and riemann surfaces*, Graduate Studies in Mathematics, American Mathematical Society, 1995.

[Ram66] K. Ramarchandra, *On the units of cyclotomic fields*, Acta Arithmetica **12** (1966), 165–173.

[SD72] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, Modular functions of one variable, III, Springer, Berlin, 1972, pp. 1–56.

[Ser72] J-P. Serre, *Formes modulaires et functions zeta p-adiques*, Modular functions of one variable, III, Springer, Berlin, 1972, pp. 191–268.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[Ste17] P. Stevenagen, *Number fields*, 2017, http://websites.math.leidenuniv.nl/algebra/ant.pdf.

[Was97] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1997.

Versicherung an Eides Statt

Ich, Alessandro Danelon; Via Celestino IV, 11, 20123 Milano, Italy, Matrikelnummer: 3071706, versichere an Eides Statt durch meine Unterschrift, dass ich die vorstehende Arbeit selbstständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annäh- ernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe, mich auch keiner anderen als der angegebenen Literatur oder sonstiger Hilfsmittel bedient habe. Ich versichere an Eides Statt, dass ich die vorgenannten Angaben nach bestemWissen und Gewissen gemacht habe und dass die Angaben der Wahrheit entsprechen und ich nichts verschwiegen habe. Die Strafbarkeit einer falschen eidesstattlichen Versicherung ist mir bekannt, namentlich die Strafandrohung gemäss §156 StGB bis zu drei Jahren Freiheitsstrafe oder Geldstrafe bei vorsätzlicher Begehung der Tat bzw. gemäss §163 Abs. 1 StGB bis zu einem Jahr Freiheitsstrafe oder Geldstrafe bei fahrlässiger Begehung.

Ort, Datum Unterschreift (Alessandro Danelon)