On the Computation of p-adic Theta Functions arising from the Hurwitz Quaternions

Isabella Negrini

A Thesis
In the Department
of
Mathematics and Statitstics

Presented in Partial Fulfillment of the Requirements
For the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada

July 2017

Concordia University

School of Graduate Studies

This is to certify that the thesis prepared

By: **Isabella Negrini**

Entitled: **On the Computation of p-adic Theta Functions arising from the Hurwitz Quaternions**

and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair
Dr. P. Stevenhagen

_____ Examiner
Dr. V. Paskunas

_____ Examiner
Dr. C. Mazza

_____ Supervisor
Dr. A. Iovita

Approved by _____
Chair of Department or Graduate Program Director

_____
Dean of Faculty

ABSTRACT

On the computation of p-adic theta functions
arising from the Hurwitz quaternions

Isabella Negrini

The aim of this thesis is to give an efficient method to compute a certain theta function $\Theta(a, b; z)$, up to a given p-adic precision n. The function $\Theta(a, b; z)$ arises from the Hurwitz quaternions and is meromorphic on the upper-half plane. We will first discuss a "naïve" method to compute $\Theta(a, b; z)$ and, by counting Hurwitz quaternions of a given norm, we will show that this method is not efficient. We will then develop some recursive relations for the Hurwitz quaterions, which will be the fundamental tool to describe a more efficient way to compute $\Theta(a, b; z)$.

Acknowledgements

First and foremost, I wish to thank my thesis supervisor, Professor Henri Darmon, for his patience and for all the time he devoted to me. I am also grateful to Professor Darmon for giving me this thesis problem and for introducing me to this fascinating topic.

Secondly, I wish to thank Professor Adrian Iovita for the discussions about this thesis and for his help and support during this year in Montréal.

I am also very grateful to Professor Fabrizio Andreatta for encouraging me last year in Milano.

I wish to thank all the post-docs and graduate students from Concordia University and McGill University number theory group, in particular thanks to Jan Vonk, David Lilienfeldt, Peter Gräf and Nicolas Simard. I also have to thank my fellow students from Milano, in particular Lorenzo Pagani.

I thank the ISM, Concordia University and Milano University for the financial support. Finally, I thank my family for their support through my studies.

Contents

1 Introduction

Theta functions have been studied in general by Gerritzen and van der Put in [GvdP80] and [vdP92]. In this thesis, we are interested in a particular Theta function $\Theta(a, b; z)$ on the p-adic upper-half plane $\mathcal{H}_p$. This function is defined as a certain infinite product whose factors depend on Möbius transformations given by Hurwitz quaternions on $\mathcal{H}_p$. To define $\Theta(a, b; z)$, it will be necessary to study the structure of $\mathcal{H}_p$. In particular, the correspondence between the Bruhat-Tits tree $\mathcal{T}$ and $\mathcal{H}_p$ will be fundamental to prove the convergence and meromorphicity of $\Theta(a, b; z)$, because knowing how the elements of $\mathrm{PGL}_2(\mathbb{Q}_p)$ (and hence the quaternions) act on $\mathcal{T}$ will give us information on how Möbius transformations move the points of $\mathcal{H}_p$.

Our final goal is to compute $\Theta(a, b; z)$ to a given number of p-adic digits. The most intuitive method to approximate $\Theta(a, b; z)$ is probably to multiply as many factors of the infinite product as possible. To do this, we will need to define a filtration of the group Γ on which the infinite product is indexed. Then we will be able to approximate $\Theta(a, b; z)$ by finite products $\Theta_n(a, b; z)$ with an increasing number of factors. However, this method is not efficient, because the number of operations to do grows exponentially in the desired precision. To see this, we will need to count the Hurwitz quaternions of a given norm. This will be done using the Theta function θ_R associated to the lattice of Hurwitz quaternions (using the same techniques that are used to prove Jacobi's four-square theorem with modular forms).

To overcome this problem, we will find a recursive formula for $\Theta_n(a, b; z)$. In this case, the number of operations involved grows polynomially in the desired precision, so applying this formula is better than multiplying all the factors defining $\Theta_n(a, b; z)$. To write the formula, we will first need to understand how to write recursively the Hurwitz quaternions of norm p^n, which will be done by studying the factorizations of such quaternions.

This thesis represents a preparatory study for the author's PhD work, during which the function $\Theta(a, b; z)$ should be actually computed (implementing the algorithms in `Sage`) and these topics will be studied in more depth.

The thesis is organized as follows:

In Chapter 2, we will study the Hurwitz quaternions and find the recursive relations needed to compute $\Theta(a, b; z)$ efficiently. These relations have been checked for some small primes p and n using `Sage`. (The function `_find_ elements_in_order` of the `Sage` package `BTQuotients` by Franc and Masdeu is used in our code).

In Chapter 3, we recall some properties of Theta functions associated to lattices, we show that the function θ_R is a weight two modular form of level $\Gamma_0(4)$ and we use its Fourier expansion to count the Hurwitz quaternions of given norm.

In Chapter 4 we study the p-adic upper-half plane, with particular emphasis on its cover by affinoids. We also introduce the Bruhat-Tits tree and sketch the construction of the reduction map from $\mathcal{H}_p$ to the tree.

In Chapter 5, we finally define the function $\Theta(a, b; z)$, we show its convergence and meromorphicity, and we compare the two methods to compute it.

2 Hurwitz Quaternions

In this chapter we study the Hurwitz quaternions, which will be used in Chapter 5 to define the theta function $\Theta(a, b; z)$. In particular, our aim is to state some recursive relations for the Hurwitz quaternions. This relations will be used at the end of Chapter 5 in order to find an efficient method of computing $\Theta(a, b; z)$.

2.1 Factorization

Every Hurwitz quaternion can be written as product of irreducible quaternions, but the factorization is not unique. In this section we show how different factorizations of the same quaternion are related to each other. Knowing when two factorizations give the same quaternion will be a fundamental tool in the next two sections. The main references for this section are [CP12] and [CS05].

Definition 2.1.1. *Let $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ be the algebra of Hamilton quaternions. The conjugate $\bar{q}$ of a quaternion $q = a + bi + cj + dk$ is defined as $\bar{q} = a - bi - cj - dk$. The norm and the trace of q are*

$$Nm(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2 \quad \textit{and} \quad Tr(q) = q + \bar{q} = 2a.$$

Moreover, if $A \subseteq R$, we write $\bar{A} = \{\, \bar{a} \mid a \in A \,\}$.

It is easy to see that $\overline{q_1 q_2} = \bar{q_2}\bar{q_1}$ and $Nm(q_1 q_2) = Nm(q_1)Nm(q_2)$.

From now on, we will work in the ring R of Hurwitz quaternions, that is:

$$R = \mathbb{Z}\left[i, j, k, \frac{1+i+j+k}{2}\right].$$

Proposition 2.1.1. *R is the ring of all Hamilton quaternions whose coordinates are either all integers or all half-integers, that is:*

$$R = \left\{ a + bi + cj + dk \;\middle|\; a, b, c, d \in \mathbb{Z} \quad \textit{or} \quad a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}.$$

Proof. An element of R is of the form

$$a + bi + cj + d\left(\frac{1+i+j+k}{2}\right) = \frac{d}{2} + \left(a + \frac{d}{2}\right) i + \left(c + \frac{d}{2}\right) j + \left(b + \frac{d}{2}\right) k,$$

so we see that its coordinates in the basis $\{\, 1, i, j, k \,\}$ are all integers if d is even, while they are all half-integers if d is odd.

□

Proposition 2.1.2. *The units of R are given by*

$$R^\times = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}.$$

As a group, $R^\times$ is isomorphic to the tetrahedral binary group, that is a central extension of A_4 by a group of order 2

Proof. It is easy to see that if $q \in R$ then $Nm(q) \in \mathbb{Z}_{\geq 0}$. Indeed, if we let $q = a + bi + cj + d\left(\frac{1+i+j+k}{2}\right)$, then:

$$\begin{aligned} Nm(q) &= \frac{d^2}{4} + \frac{(2a+d)^2}{4} + \frac{(2b+d)^2}{4} + \frac{(2c+d)^2}{4} \\ &= \frac{4(a^2+b^2+c^2+d^2+ab+ac+ad)}{4}. \end{aligned}$$

From this and the fact that the norm is multiplicative we have that $q \in R$ is a unit if and only if $Nm(q) = 1$. Clearly, the only $q \in R$ with $Nm(q) = 1$ and integer coordinates in the basis $\{ 1, i, j, k \}$ are $\pm 1, \pm i, \pm j, \pm k$. Then, since the only way to write 1 as a sum of squares of four half-integers is $1 = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$, we have that the only $q \in R$ with $Nm(q) = 1$ and integer coordinates in the basis $\{ 1, i, j, k \}$ are $\frac{\pm 1 \pm i \pm j \pm k}{2}$. Now, the center of $R^\times$ is the group $C = \{ \pm 1 \}$. If we denote by G the quotient

$$G = \frac{R^\times}{C},$$

then the sequence

$$1 \to C \to R^\times \to G \to 1$$

is exact, so $R^\times$ is a central extension of G by C. We want to show that G is isomorphic to A_4. By Sylow theorems, G has either one or four Sylow 3-subgroups. Moreover, it's easy to see that G has eight elements of order three, so we see that G has four Sylow 3-subgroups. Then, G acts on the set of its Sylow 3-subgroups by conjugation, so we have a map

$$f :\to S_4.$$

For any Sylow 3-subgroup P, we have

$$\mathrm{Stab}_G(P) = P,$$

so the kernel of f is the intersection of all Sylow 3-subgroups, hence f is injective and G is isomorphic to a subgroup of S_4. But the only subgroup of order 12 of S_4 is A_4, so G is isomorphic to A_4. □

We now introduce the notion of *primitive* quaternion, which will be used repeatedly in Section 2.2.

Definition 2.1.2. *If a Hurwitz quaternion q is of the form $q = nq'$ for some $n \in \mathbb{Z}$, we write $n|q$. We say that q is* primitive *if it cannot be written as $q = nq'$ with $n \in \mathbb{Z}$.*

The following lemma will be used to prove results about the factorization of quaternions.

Lemma 2.1.1. *Let $Q, P, B \in R$ with $Nm(P) = p$ and $p|QPB$ but $p \nmid QP$, then $p|PB$.*

Proof. Consider the right ideal $I = \bar{P}R + BR$. Then it must be $I = \alpha R$ for some $\alpha \in R$ and we see that α cannot be a unit, because otherwise we would have

$$1 = \bar{P}a + Bb \quad \text{for some } a, b \in R,$$

but this implies

$$QP = QP\bar{P}a + QPBb,$$

so $p|QP$, which is not possible. But then, since $\bar{P} \in I$ and $Nm(\bar{P}) = p$, we have $Nm(\alpha) = p$ (by the multiplicativity of the norm) and so $\alpha = \bar{P}\epsilon$ for some unit ϵ. This tells us that $B = \bar{P}w$ for some $w \in R$, hence $pw = P\bar{P}w = PB$, so $p|PB$. □

Remark 2.1.1. In the same way, we can prove that if $p|QPB$ but $p \nmid PB$, then $p|QP$. To prove it we use the same argument used in the proof of Lemma 2.1.1, but we consider the *left* ideal $I = R\bar{P} + RQ = R\alpha$, and we multiply by PB on the right the equation $1 = a\bar{P} + bQ$ to show that α is not a unit. The rest of the proof is analogous to what we have seen above.

Theorem 2.1.1. *If q is a primitive Hurwitz quaternion and $Nm(q) = p_1 \dots p_n$ is a* fixed *factorization of $Nm(q)$ as product of prime numbers, then q can be written as $q = P_1 \dots P_n$, where $P_i \in R$ are such that $Nm(P_i) = p_i$ for $i = 1, \dots n$.*

Proof. We proceed by induction on n. The case $n = 1$ is clear. Now we assume that the statement holds for $n - 1$ and show it holds also for n. Consider $Nm(q) = p_1 \dots p_n$ and the left ideal $I = Rq + Rp_n$. Then I must be principal $I = RP$, and since $p_n \in I$, we have $Nm(P)|p_n^2$. But $Nm(P) \neq p_n^2$, otherwise we would have $P = p_n\epsilon$ for some unit ϵ, but then $p_n|q$, which is not possible because q is primitive. Moreover, $Nm(P) \neq 1$, otherwise it would be $1 = aq + bp_n$ for some $a, b \in R$, so by $aq = 1 - bp_n$ we would have that $p_n \nmid Nm(q)$, a contradiction. So we see that $Nm(P) = p_n$. Now let $P_n := P$, clearly we have $q = q'P_n$ for some $q' \in R$ (because $q \in I$). But q' is primitive and, by induction hypothesis, it has a factorization $q' = P_1 \dots P_{n-1}$, where $P_i \in R$ are such that $Nm(P_i) = p_i$. So we see that $q = P_1 \dots P_n$ and the proof is complete. □

Theorem 2.1.2. *The factors in Theorem 2.1.1 are unique up to multiplication by units, i.e. if $q = P_1 \dots P_n$ and $q = P'_1 \dots P'_n$ are two factorizations of the same quaternion q, then there are some units $\epsilon_1 \dots \epsilon_{n-1}$ such that:*

$$\begin{array}{rcl} P'_1 & = & P_1\epsilon_1^{-1} \\ P'_2 & = & \epsilon_1 P_2 \epsilon_2^{-1} \\ & \dots & \\ P'_{n-1} & = & \epsilon_{n-2} P_{n-1} \epsilon_{n-1}^{-1} \\ P'_n & = & \epsilon_{n-1} P_n. \end{array}$$

Proof. We proceed by induction on n. The case $n = 1$ is trivial. Now we assume that the statement holds for $n-1$ and prove it for n. If $q = P_1 \dots P_n$ and $q = P'_1 \dots P'_n$ are two factorizations of q where $Nm(P_i) = p_i$, then:

$$P_1 \dots P_n \bar{P}_n = P'_1 \dots P'_n \bar{P}_n,$$

so:

$$p_n | (P'_1 ... P'_{n-1}) P'_n \bar{P}_n,$$

which implies $p_n | P'_n \bar{P}_n$ (by Lemma 2.1.1 and the fact that q is primitive). Hence, since $Nm(P_n) = Nm(P'_n) = p_n$, we have:

$$P'_n \bar{P}_n = \epsilon p_n = \epsilon P_n \bar{P}_n$$

for some unit ϵ, so $P'_n = \epsilon P_n$ and $P_1 \dots P_{n-1} P_n = P'_1 \dots P'_{n-1} \epsilon P_n$. Now we can use the induction hypothesis on $P_1 \dots P_{n-1} = P'_1 \dots P'_{n-1} \epsilon$ to see that :

$$\begin{array}{rcl} P'_1 & = & P_1\epsilon_1^{-1} \\ P'_2 & = & \epsilon_1 P_2 \epsilon_2^{-1} \\ & \dots & \\ P'_{n-1}\epsilon & = & \epsilon_{n-2} P_{n-1}. \end{array}$$

So it suffices to let $\epsilon_{n-1} := \epsilon$ to have $P'_{n-1} = \epsilon_{n-2} P_{n-1} \epsilon_{n-1}^{-1}$ and $P'_n = \epsilon_{n-1} P_n$. This completes the proof. □

Now we study the factorization of a non-primitive quaternion q. For our purposes, we can restrict aur attention to the case where the norm of q is the power of a prime number.

Definition 2.1.3. *A quaternion q is said to be p-pure if $q = p^n$ fore some prime number p and some integer $n \geq 1$.*

Proposition 2.1.3. *If q is a non-primitive, p-pure quaternion and a factorization for q is $q = P_1 \dots P_n$, then $p | P_{i-1} P_i$ for some i with $2 \leq i \leq n$.*

Proof. If $p | P_{n-1} Pn$ the statement holds. Otherwise, let i be an integer such that $p \nmid P_i \dots P_n$ but $i | P_{i-1} P_i \dots P_n$. Clearly, $i \geq 2$ since q is non-primitive. Then by Remark 2.1.1 we can conclude that $p | P_{i-1} P_i$. □

The next lemma will be used in the following section.

Lemma 2.1.2. *If q is a non-primitive, p-pure quaternion of norm p^n, then there is a factorization $q = P_1 \dots P_n$ such that $p | P_{n-1}P_n$.*

Proof. We proceed by induction on n. If n=1, then q must be primitive, so we start with $n = 2$, in which case the statement is clear. So now we assume that the statement holds for $n-1$ and prove it for n. We can assume $p \nmid P_2 \dots P_n$ (otherwise the thesis would immediately follow by induction hypothesis). So by Lemma 2.1.1 we have $p | P_1P_2$ (because $p|q$). This means that $P_1P_2 = p\epsilon = P_1\bar{P}_1\epsilon$ for some unit ϵ, thus $P_2 = P_1\epsilon$. So we have:

$$\begin{aligned} q &= P_1P_2P_3 \dots P_n \\ &= P_1\bar{P}_1\epsilon P_3 \dots P_n \\ &= P_1\bar{P}_1P'_3 \dots P_n \quad (where\ P'_3 = \epsilon P_3) \\ &= P'_3\bar{P}_3{}'P'_3 \dots P_n. \end{aligned}$$

But $p | \bar{P}_3{}'P'_3 \dots P_n$, so the thesis follows by induction hypothesis. □

Corollary 2.1.1. *In the same hypothesis of lemma 2.1.2, we can assume $P_{n-1}P_n = p$ if $n > 2$.*

Proof. Since $Nm(P_i) = p$ and $p | P_{n-1}P_n$, we have $P_{n-1}P_n = \epsilon p$ for some unit ϵ, so by letting $P'_{n-2} = P_{n-2}\epsilon$, we get a new factorization $q = P'_1 \dots P'_n$ with $P_{n-1}P_n = p$. □

Remark 2.1.2. In the same hypothesis of Lemma 2.1.2, we can prove that there is a factorization $q = P_1 \dots P_n$ with $p | P_1P_2$ and furthermore we can assume $P_1P_2 = p$ if $n > 2$. The proofs are analogous to the ones of Lemma 2.1.2 and Corollary 2.1.1.

We saw that the factorization of a primitive quaternion q is unique up to multiplication by units. Things are a bit more complicated if q is not primitive, i.e. if $q = p^k q'$ with q' primitive, because we have also to take into account the fact that p can be factored in many ways. For example $p = P_1\bar{P}_1 = P_2\bar{P}_2$. Following [CP12] and [CS05], we call this process *recombination*.

Definition 2.1.4. *If p is a prime number such that $p|q$ and P_1, P_2 are quaternions such that $Nm(P_1) = Nm(P_2) = p$, then we call **recombination** the process of substituting $p = P_1\bar{P}_1$ with $p = P_2\bar{P}_2$ in the factorization of q.*

Theorem 2.1.3. *The factorization of a non-primitive quaternion q with $Nm(q) = p^n$ is unique up to recombinations and multiplication by units (in the sense of Theorem 2.1.2).*

Proof. We proceed by induction on n. We start from $n = 2$ (if $n = 1$ then q is primitive). If $Nm(q) = p^2$, then $q = p\epsilon$ for some unit ϵ. Let $q = P_1P_2$ and $q = P_1'P_2'$ be two different factorizations of q. Then:

$$\begin{aligned} q &= P_1P_2 = P_1\bar{P}_1\epsilon \\ &= P_1P_2 = P_1'\bar{P}_1{}'\epsilon, \end{aligned}$$

so $P_2 = \bar{P}_1\epsilon$ and $P_2' = \bar{P}_1{}'\epsilon$. But then

$$q = P_1\bar{P}_1\epsilon = P_1'\bar{P}_1{}'\epsilon$$

is a recombination. Now let $n > 2$ and $q = P_1 \dots P_{n-1}P_n = P_1' \dots P_{n-1}'P_n'$ be two factorizations of q. By Corollary 2.1.1 we can assume $P_{n-1}P_n = p$ and $P_{n-1}'P_n' = p$ (because passing to this form requires only multiplication by units and recombinations). So $P_1 \dots P_{n-2} = P_1' \dots P_{n-2}'$ and these two factorizations differ only by multiplication by units and recombinations (by induction hypothesis). Then, since $p = P_{n-1}P_n = P_{n-1}'P_n'$ is a recombination, the thesis follows. □

2.2 Counting quaternions

In this section we count the primitive and non-primitive quaternions of norm p^n and their factorizations. Knowing how many of these quaternions there are is useful to test the recursive relations that we will find in the next section. Moreover, the counting methods we use are in the same spirit of the proofs of these relations. From the rest of the section, p will denote an odd prime number and we will use the notation: $Q_i = \{\, q \in R \mid Nm(q) = p^i \,\}$.

Definition 2.2.1. *Let q, $q' \in Q_1$ and let ϵ be a unit. Then we write $q \sim q'$ if $q = \epsilon q'$ and $q \dot{\sim} q'$ if $q = q'\epsilon$.*

Lemma 2.2.1. *There are $24(1 + p + \dots + p^n)$ Hurwitz quaternions of norm p^n and $p + 1$ representatives for $\sim$ (and $\dot{\sim}$). So Q_1 is the disjoint union of $p + 1$ equivalence classes with 24 elements each.*

Proof. The quaternions of norm m are as many as all the ways to write m as a sum of four squares of integers or half-integers. We will see in Chapter 3 that there are $\sum_{d|m, 2\nmid d} d$ ways of doing this (where the sum is taken over positive d). So the quaternions of norm p^n are $24(1 + p + \dots + p^n)$. To prove the second statement, we see that Q_1 has $24(p + 1)$ elements, divided in equivalence classes of $\sim$ (or $\dot{\sim}$). But each class of $\sim$ is given by $\{\, \epsilon q \mid \epsilon \text{ is a unit} \,\}$, where q is a representative for the class. So clearly we have 24 elements in each class. We proceed in the same way for $\dot{\sim}$. □

From now on, we will use the notation $T = \{\, r_i,\ i = 1 \dots p + 1 \,\}$ to denote the set of repreentatives for $\sim$ and $\dot{T}$ to denote the set of representatives of $\dot{\sim}$. Moreover, C_q and $\dot{C}_q$ will denote the equivalence classes of q with respect to $\sim$ and $\dot{\sim}$, respectively.

Remark 2.2.1. We have that $\dot{T} = \{ \bar{r_i} \mid r_i \in T \}$. Indeed

$$C_{r_i} = \{ \epsilon r_i \mid \epsilon \text{ is a unit} \}, \quad \text{and} \quad \dot{C_{\bar{r}_i}} = \{ \bar{r_i}\mu \mid \mu \text{ is a unit} \}.$$

Furthermore:

$$\begin{aligned} \bar{C_{r_i}} &= \{ \bar{r_i}\bar{\epsilon} \mid \epsilon \text{ is a unit} \} \\ &= \left\{ \bar{r_i}\epsilon^{-1} \;\middle|\; \epsilon \text{ is a unit} \right\} \\ &= \{ \bar{r_i}\mu \mid \mu \text{ is a unit} \} \\ &= \dot{C_{\bar{r}_i}}, \end{aligned}$$

and different equivalence classes remain disjoint when we take the conjugate.

We start by counting the primitive and non-primitive elements in Q_2 before doing it for Q_n. We know that Q_2 has $24(1 + p + p^2)$ elements q with factorization $q = q_1q_2$ where $Nm(q_1) = Nm(q_2) = p$. Clearly, there are $(24(1 + p))^2$ of these factorizations. Since $(24(1 + p))^2 > 24(1 + p + p^2)$, we see that the factorization is not unique.

Proposition 2.2.1. *There are $24p(1 + p)$ primitive elements in Q_2 , each of which has 24 factorizations. There are 24 non-primitive elements in Q_2, each of which has $24(1 + p)$ factorizations.*

Proof. A non-primitive quaternion q of norm p^2 is necessarily of the form $q = p\epsilon = \epsilon p$ for some unit ϵ. So we see that the non-primitive quaternions of norm p^2 are 24. Then, p can be written as $p = r\bar{r}$ in $24(1 + p)$ ways (as many as the quaternions $r \in R$).

We now count the factorizations $q = q_1q_2$ giving distinct primitive quaternions. A priori, q_1 should be chosen in Q_1, but it is enough to choose it in $\dot{T}$. Indeed, if $q_1' = q_1\epsilon$, then the factorizations q_1q_2 and $q_1'(\epsilon^{-1}q_2)$ give the same quaternion. Moreover, if q_1 and q_1' are not equivalent with respect to $\dot{\sim}$, it will be $q_1q_2 \neq q_1'q_2'$ for every q_2, q_2'. So we have $p+1$ choices for q_1. Once that q_1 is fixed, we see that q_2 can be any element of $Q_1 \setminus \dot{C_{\bar{q}_1}}$ (it cannot be in $\dot{C_{\bar{q}_1}}$ because otherwise q would not be primitive). So there are $24p$ choices for q_2, hence there are $24p(p + 1)$ choices for q_1q_2.

Finally, given a primitive quaternion $q \in Q_2$, we see that it has 24 factorizations, by Theorem 2.1.2 and the fact that we can write

$$q = q_1q_2 = (q_1\epsilon)(\epsilon^{-1}q_2)$$

in 24 ways (as many as the units of R).

□

Remark 2.2.2. The second part of the proof above is useful to understand the factorization and the same argument will be used below. Anyway, we could have proven the statement also in the following way: we know that there are $24(1 + p + p^2)$ elements in Q_2, 24 of which are

non-primitive. So the primitive ones must be $24(1+p+p^2)-24 = 24p(1+p)$. Furthermore, the number of *all* factorizations of the form q_1q_2 is $24^2(1+p)^2$, while the number of the factorizations giving non-primitive quaternions is $24^2(1+p)$. So the number of factorizations giving primitive quaternions must be

$$24^2(1+p)^2 - 24^2(1+p) = 24^2p(1+p).$$

(We are counting also factorizations giving the same quaternion). But, since the non-primitive quaternions are $24p(1+p)$, each of them must have $(24^2p(1+p))/(24p(1+p)) = 24$ factorizations.

Proposition 2.2.2. *If $n \geq 1$, there are $24(p+1)p^{n-1}$ primitive quaternions of norm p^n and each of them has 24^{n-1} factorizations.*

Proof. As in the proof of Proposition 2.2.1, we count the factorizations $q_1 \dots q_n$ giving dinstinct primitive quaternions q. We proceed by induction on n. The case $n = 1$ is clear and the case $n = 2$ has been done above. We assume that the statement holds for $n-1$, so we have $24(p+1)p^{n-2}$ choices for $q_1 \dots q_{n-1}$ in $q = (q_1 \dots q_{n-1})q_n$. Once that $q_1 \dots q_{n-1}$ is fixed, q_n can be any element of T, except for the representative of $C_{\bar{q}_{n-1}}$ (otherwise q is not primitive). This means that there are p ways of choosing q_n, so there are $24(p+1)p^{n-1}$ factorizations $q = q_1 \dots q_n$ giving dinstinct quaternions. The second part of the statement follows from Theorem 2.1.2, in particular from the equality

$$q_1q_2 \dots q_{n-1}q_n = (q_1\epsilon_1)(\epsilon_1^{-1}q_2\epsilon_2) \dots (\epsilon_{n-2}^{-1}q_{n-1}\epsilon_{n-1})(\epsilon_{n-1}^{-1}q_n).$$

□

Proposition 2.2.3. *If $n \geq 2$, there are $24(1+p+\dots p^{n-2})$ non-primitive quaternions. The total number of factorizations giving non-primitive quaternions of norm p^n is*

$$24^n\left((n-1)p^{n-1} + \binom{n}{2}p^{n-2} + \dots + 1\right).$$

Proof. We showed that there are $24(1+p+\dots+p^n)$ quaternions of norm p^n, of which $24(p^n+p^{n-1})$ are primitive, so the number of non-primitive ones is

$$24(1+p+\dots+p^n) - 24(p^n+p^{n-1}) = 24(1+p+\dots p^{n-2}).$$

There are $24^n(p+1)^n$ factorizations of the form $q = (q_1 \dots q_{n-1})q_n$. From Proposition 2.2.2, we have that $24^{n-1}24(p+1)p^{n-1}$ of them give primitive quaternions. So we have

$$24^n(p+1)^n - 24^n(p+1)p^{n-1} = 24^n\left((n-1)p^{n-1} + \binom{n}{2}p^{n-2} + \dots + 1\right)$$

factorizations left. (We are counting also factorizations giving the same quaternion). □

Remark 2.2.3. The folowing reasoning provides an extra check for the formula giving the number of non-primitive factorizations and is also useful to understand the structure of quaternion factorization. We can obtain a factorization $q_1 \dots q_{n-1} q_n$ from $q_1 \dots q_{n-1}$ multiplying by q_n. Proceeding by induction, we assume the statement holds for $n-1$ (We have already done the case $n = 2$). We have two cases.

1. $q_1 \dots q_{n-1}$ *is primitive.*

   There are $24^{n-1}(p+1)p^{n-2}$ primitive factorizations $q = q_1 \dots q_{n-1}$ and, since it must be $q_n = \bar{q}_{n-1}\epsilon$ for some unit ϵ, we have 24 choices for q_n. So finally the number of factorizations $q = q_1 \dots q_{n-1} q_n$ where $q = q_1 \dots q_{n-1}$ is non-primitive is $24^n(p+1)p^{n-2}$.

2. $q_1 \dots q_{n-1}$ *is non-primitive.*

   By induction hypothesis, we have $24^{n-1}((n-2)p^{n-2} + \binom{n-1}{2}p^{n-3} + \dots + 1)$ factorizations giving a non-primitive quaternion $q = q_1 \dots q_n$. Since q is non-primitive, q_n can be any of the $24(p+1)$ elements of Q_1. So the number of factorizations $q = q_1 \dots q_{n-1} q_n$ where $q = q_1 \dots q_{n-1}$ is non-primitive is

   $$24^n \left[(n-2)p^{n-1} + \left(\binom{n-1}{2} + (n-2) \right) p^{n-2} + \binom{n}{3} p^{n-3} + \dots + 1 \right],$$

   since $\left(\binom{n-1}{2} + \binom{n-1}{3} \right) = \binom{n}{3}$.

Adding the numbers we get in these two cases, we have:

$$\begin{aligned}
&= 24^n \left[(n-1)p^{n-1} + \left(\binom{n-1}{2} + (n-1) \right) p^{n-2} + \binom{n}{3} p^{n-3} + \dots + 1 \right] \\
&= 24^n \left[\binom{n-1}{1} p^{n-1} + \left(\binom{n-1}{2} + \binom{n-1}{1} \right) p^{n-2} + \dots + 1 \right] \\
&= 24^n \left[(n-1)p^{n-1} + \binom{n}{2} p^{n-2} + \binom{n}{3} p^{n-3} + \dots + 1 \right],
\end{aligned}$$

which is the right number.

2.3 Recursive relations

In this section, we describe how to obtain Q_n recursively. In particular, let Q_n^{pr} and Q_n^{non-pr} be respectively the set of primitive and non-primitive quaternions in Q_n. We will see how to derive Q_n^{pr} and Q_n^{non-pr} from Q_{n-1}^{pr} and Q_{n-1}^{non-pr}.

We start with the non-primitive quaternions. Clearly we have

$$Q_0^{non-pr} = Q_1^{non-pr} = \emptyset.$$

The elements of Q_2^{non-pr} are necessarily of the form $q = p\epsilon$ where ϵ is a unit; the elements of Q_3^{non-pr} are necessarily of the form $q = pq_1$ where $Nm(q_1) = p$; the elements of Q_4^{non-pr} can be of the form $q = p^2\epsilon$ where ϵ is a unit, or of the form $q = pq_2$ where $Nm(q_2) = p^2$, and so on. We can summarize this in the table below (we use the notation $Nm(q_i) = p^1$ in the table).

$Nm = p^n$	Elements of Q_n^{non-pr}			
p^2	$p\epsilon$			
p^3	pq_1			
p^4	$p^2\epsilon$	pq_2		
p^5	p^2q_1	pq_3		
p^6	$p^3\epsilon$	p^2q_2	pq_4	
p^7	p^3q_1	p^2q_3	pq_5	
p^8	$p^4\epsilon$	p^3q_2	p^2q_4	pq_6

From the table we see that, if $n \geq 4$, then

$$Q_n^{non-pr} = \left\{ pq \;\middle|\; q \in Q_{n-2}^{non-pr} \right\} \cup \left\{ pq \;\middle|\; q \in Q_{n-2}^{pr} \right\}.$$

So if we compute Q_2^{non-pr} and Q_3^{non-pr}, then we can find Q_n^{non-pr} recursively.

We now consider the primitive quaternions; if $n = 0, 1$, then all quaternions of norm p^n are primitive. The cases $n = 2$ and $n > 2$ are treated in the propositions below.

Proposition 2.3.1. *We have*

$$Q_2^{pr} = \{ qr \mid q \in Q_1, r \in T \} \setminus (p+1) \{ p\epsilon \mid \epsilon \textit{ is a unit} \},$$

where $\{ qr \mid q \in Q_1, r \in T \}$ *and* $(p+1)\{ p\epsilon \mid \epsilon \textit{ is a unit} \}$ *are multisets.*

Proof. Let $A = \{ qr \mid q \in Q_1, r \in R \}$, then we have:

$$\begin{aligned} A &= \bigcup_{i=1}^{p+1} \{ qr_i \mid q \in Q_1 \} \\ &= \bigcup_{i=1}^{p+1} \bigcup_{j=1}^{p+1} \left\{ qr_i \;\middle|\; q \in C_{r_j} \right\} \\ &= \bigcup_{i=1}^{p+1} \bigcup_{j=1}^{p+1} \{ \epsilon r_j r_i \mid \epsilon \textit{ is a unit} \}. \end{aligned}$$

Call $A_{ij} = \{ \epsilon r_j r_i \mid \epsilon \textit{ is a unit} \}$ and call $r_{\bar{\imath}}$ the representative of the class of $\bar{r_i}$. Moreover, let $A_i = \{ qr_i \mid q \in Q_1 \}$.

Then, $j \neq \bar{\imath}$ if and only if all the elements in A_{ij} are primitive. Furthermore, all the elements in $A_{i,j}$ are dinstinct and $A_{i,j} \cap A_{i',j'} = \emptyset$ if $A_{i,j}$ and $A_{i',j'}$ have primitive elements. (This follows by Theorem 2.1.2 if $i \neq i'$, and it is clear otherwise). We also have that each primitive quaternion q_1q_2 of Q_2 belongs to A, because $q_1q_2 = q_1(\epsilon r_i) = (q_1\epsilon)(r_i)$ if $q_2 \in C_{r_i}$. All this means that A contains each primitive quaternion of norm p^2, without repetitions.

We now show that A contains also the set $\{ p\epsilon \mid \epsilon \textit{ is a unit} \}$ with $p+1$ repetitions. Indeed, if $j = \bar{\imath}$, then $A_{ij} = \{ p\epsilon \mid \epsilon \textit{ is a unit} \}$ and, since T has $p+1$ elements, A contains $p+1$ repetitions of this set. □

Remark 2.3.1. We have

$$|\{\, qr \mid q \in Q_1, r \in T \,\}| = (p+1)24(p+1),$$

and

$$|(p+1)\{\, p\epsilon \mid \epsilon \textit{ is a unit} \,\}| = 24(p+1),$$

so

$$|\{\, qr \mid q \in Q_1, r \in T \,\} \setminus (p+1)\{\, p\epsilon \mid \epsilon \textit{ is a unit} \,\}| = |Q_2^{pr}|.$$

Proposition 2.3.2. *If $n \geq 3$, then Q_n^{pr} is given by*

$$Q_n^{pr} = \left\{\, qr \;\middle|\; q \in Q_{n-1}^{pr}, r \in T \,\right\} \setminus p\left\{\, pq \;\middle|\; q \in Q_{n-2}^{pr} \,\right\},$$

where $\left\{\, qr \;\middle|\; q \in Q_{n-1}^{pr}, r \in T \,\right\}$ and $p\left\{\, pq \;\middle|\; q \in Q_{n-2}^{pr} \,\right\}$ are multisets.

Proof. Let $A = \left\{\, qr \;\middle|\; q \in Q_{n-1}^{pr}, r \in R \,\right\}$, then we have:

$$\begin{aligned} A &= \bigcup_{i=1}^{p+1} \left\{\, qr_i \;\middle|\; q \in Q_{n-1}^{pr} \,\right\} \\ &= \bigcup_{i=1}^{p+1}\bigcup_{j=1}^{p+1} \left\{\, qr_i \;\middle|\; q = q_1 \dots q_{n-1},\ q \in Q_{n-1}^{pr},\ q_{n-1} \in C_{r_j} \,\right\}. \end{aligned}$$

Let $A_{ij} = \left\{\, qr_i \;\middle|\; q = q_1 \dots q_{n-1},\ q \in Q_{n-1}^{pr},\ q_{n-1} \in C_{r_j} \,\right\}$ and call $r_{\bar{\imath}}$ the representative of the class of $\bar{r}_i$. Then:

$$A_{ij} = \left\{\, q_1 \dots q_{n-2}\epsilon r_j r_i \;\middle|\; q_1 \dots q_{n-2}\epsilon r_j \in Q_{n-1}^{pr},\ \epsilon \textit{ is a unit} \,\right\}.$$

If $j = \bar{\imath}$ we see that $A_{ij} = \left\{\, pz \;\middle|\; z \in Q_{n-2}^{pr},\ z = q_1 \dots q_{n-2},\ q_{n-2} \notin \dot{C}_{r_i} \,\right\}$. Indeed, $q_1 \dots q_{n-1}$ is primitive, so it must be $q_{n-2} \neq \bar{q}_{n-1} = r_i\epsilon^{-1}$. Since $|T| = p+1$, we have that A contains p times the set $\left\{\, pq \;\middle|\; q \in Q_{n-2}^{pr} \,\right\}$.

If $j \neq \bar{\imath}$ all the elements in A_{ij} are primitive. Using exactly the same argument as in the prof of Proposition 2.3.1, we see that A contains all the elements in Q_n^{pr}, with no repetitions. □

Remark 2.3.2. We have

$$|\left\{\, qr \;\middle|\; q \in Q_{n-1}^{pr}, r \in T \,\right\}| = (p+1)24(p+1)p^{n-2},$$

and

$$|p\left\{\, pq \;\middle|\; q \in Q_{n-2}^{pr} \,\right\}| = p24(p+1)p^{n-3},$$

so

$$\left|\left\{\, qr \;\middle|\; q \in Q_{n-1}^{pr}, r \in T \,\right\} \setminus p\left\{\, pq \;\middle|\; q \in Q_{n-2}^{pr} \,\right\}\right| = |Q_n^{pr}|.$$

3 Theta functions associated to lattices

The aim of this chapter is to find the number of Hurwitz quaternions with norm m, for any positive integer m. This is exactly the number of ways in which m can be written as a sum of four squares of integers or half-integers. This number is the m-th Fourier coefficient of the theta function Θ_R associated to the ring of Hurwitz Quaternions R, seen as a $\mathbb{Z}$-lattice in B. We will prove that this function is an element of the space of weight two modular forms of level $\Gamma_0(4)$, denoted by $\mathcal{M}_2(\Gamma_0(4))$, and we will find its coefficients by giving a basis for $\mathcal{M}_2(\Gamma_0(4))$.

3.1 The function Θ_R

In this section, we define and study the function Θ_R, after recalling some properties about lattices. In particular, our goal for this section is to show that Θ_R is an element of $\mathcal{M}_2(\Gamma_0(4))$.

Definition 3.1.1. *Let $\mathcal{L} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ be a lattice in $\mathbb{R}^n$. Then the dual of $\mathcal{L}$ is $\mathcal{L}^* = \{\, v \in \mathbb{R}^n \mid \langle v, w\rangle \in \mathbb{Z},\ \forall w \in \mathcal{L} \,\}$, where $\langle\ ,\rangle$ denotes the inner product in $\mathbb{R}^n$.*

Remark 3.1.1. This definition can be applied to our case. Indeed we have $B \cong \mathbb{Q}^4$ as $\mathbb{Q}$-module and $R \cong \mathbb{Z}^4$ as $\mathbb{Z}$-module via the identification

$$\begin{aligned} &\iota : B \to \mathbb{Q}^4 \hookrightarrow \mathbb{R}^4 \\ &1 \mapsto (1,0,0,0) \\ &i \mapsto (0,1,0,0) \\ &j \mapsto (0,0,1,0) \\ &k \mapsto (0,0,0,1). \end{aligned}$$

Moreover R, being an order, is a lattice in B, so $\iota(R)$ is a lattice in $\mathbb{R}^4$. We can also define an inner product on B as:

$$\begin{gathered} \langle\ ,\rangle_B : B \times B \to \mathbb{Q} \\ \langle a + bi + cj + dk, \alpha + \beta i + \gamma j + \delta k\rangle_B = a\alpha + b\beta + c\gamma + d\delta, \end{gathered}$$

and clearly $\langle q_1, q_2\rangle = \langle \iota(q_1), \iota(q_2)\rangle$.

Proposition 3.1.1. *Let $\mathcal{L} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ be a lattice in $\mathbb{R}^n$. Then $\mathcal{L}^*$ is a lattice in $\mathbb{R}^n$. In particular we have $\mathcal{L}^* = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$, where $w_1 \dots w_n$ is the dual basis of $v_1 \dots v_n$, i.e. $\langle w_i, v_j\rangle = \delta_{ij} \quad \forall i, j = 1 \dots n$.*

Proof. We first prove $\mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n \subseteq \mathcal{L}^*$. Let

$$\sum_{i=1}^{n} a_i w_i \quad \textit{and} \quad \sum_{j=1}^{n} b_i v_i,$$

be respectively in $\mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$ and $\mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$. Then,

$$\langle \sum_{i=1}^{n} a_i w_i, \sum_{j=1}^{n} b_i v_i \rangle = \sum_{i,j=1}^{n} a_i b_j \delta_{ij} \ \in \mathbb{Z},$$

so $\mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n \subseteq \mathcal{L}^*$. Now, let u be an element of $\mathcal{L}^*$. Then we can write:

$$u = \sum_{i=1}^{n} c_i w_i, \quad c_i \in \mathbb{R}.$$

Hence

$$\langle u, v_j \rangle = \sum_{i,j=1}^{n} c_i \delta_{ij} = c_j \ \in \ \mathbb{Z},$$

and so $\mathcal{L}^* \subseteq \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$. □

Proposition 3.1.2. *The dual lattice of R is*

$$R^* = 2\mathbb{Z} + (-1+i)\mathbb{Z} + (-1+j)\mathbb{Z} + (-1+k)\mathbb{Z}.$$

Proof. Via the identification in Remark 3.1.1, the basis $\{\, i, j, k, \frac{1+i+j+k}{2} \,\}$ in B corresponds to the basis in $\mathbb{R}^4$ given my the columns of the matrix

$$M = \begin{pmatrix} 0 & 0 & 0 & 1/2 \\ 1 & 0 & 0 & 1/2 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1 & 1/2 \end{pmatrix}.$$

So the dual basis is given by the columns of

$$(M^T)^{-1} = \begin{pmatrix} -1 & -1 & -1 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

which give the basis $\{\, 2,\ -1+i,\ -1+j,\ -1+k \,\}$ in B. □

Definition 3.1.2. *A lattice $\mathcal{L}$ in $\mathbb{R}^n$ is integral if $\mathcal{L} \subseteq \mathcal{L}^*$.*

We see that the lattice R^* is integral because its elements have integer coordinates.

Definition 3.1.3. *Let $\mathcal{L} = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ be a lattice in $\mathbb{R}^n$ and let M be the matrix whose columns are given by the vectors $v_1 \dots v_n$. The determinant of $\mathcal{L}$ is $det(\mathcal{L}) = |det(M)|$.*

Remark 3.1.2. We have that $det(\mathcal{L})$ is equal to the volume of the region $\mathbb{R}^n/\mathcal{L}$. Moreover, $det(\mathcal{L}^*) = 1/det(\mathcal{L})$. Indeed with the notation of the above definition, a basis for $\mathcal{L}^*$ is given by the columns of $(M^T)^{-1}$, so

$$det(\mathcal{L}^*) = |det((M^T)^{-1})| = 1/det(\mathcal{L}).$$

Lemma 3.1.1. *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$, m a positive integer and*

$$r_{\mathcal{L}}(m) = \#\left\{ v \in \mathcal{L} \mid \langle v, v\rangle = m \right\}.$$

Then the series

$$\sum_{m=0}^{\infty} r_{\mathcal{L}}(m) q^m$$

converges absolutely if $|q| < 1$.

Proof. We will show that $r_{\mathcal{L}}(m) < Cm^{n/2}$ for a positive constant C. The thesis then follows from the ratio test. Indeed, there is a finite number of elements of $\mathcal{L}$ with norm less then 1, so we can write

$$\#(\mathcal{L} \cap \left\{ v \in \mathbb{R}^n \mid \langle v, v\rangle \leq 1 \right\}) < C$$

for some $C > 0$. But then

$$r_{\mathcal{L}}(m) < \#(\mathcal{L} \cap \left\{ v \in \mathbb{R}^n \;\middle|\; \langle v, v\rangle^{1/2} \leq m^{1/2} \right\}) < Cm^{n/2},$$

because $r_{\mathcal{L}}(m) = \#(\mathcal{L} \cap \left\{ v \in \mathbb{R}^n \;\middle|\; \langle v, v\rangle^{1/2} = m^{1/2} \right\})$. □

Lemma 3.1.2. *The series*

$$\sum_{m=0}^{\infty} r_{\mathcal{L}}(m) e^{2\pi i \tau m} \quad \text{and} \quad \sum_{m=0}^{\infty} r_{\mathcal{L}}(m) e^{-\pi i m/2\tau}$$

converge uniformly on compact subsets of $\mathcal{H} = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{Q})$, the complex upper-half plane.

Proof. For the first series we have

$$\left| \sum_{m=0}^{\infty} r_{\mathcal{L}}(m) e^{2\pi i \tau m} - \sum_{m=0}^{N} r_{\mathcal{L}}(m) e^{2\pi i \tau m} \right| \leq \sum_{m=N+1}^{\infty} r_{\mathcal{L}}(m) e^{-2\pi Im(\tau) m},$$

which, if $N \to \infty$, goes to zero uniformly in τ on compact subsets of $\mathcal{H}$. (Because, on a compact, $Im(\tau) \geq \epsilon$ for some $\epsilon > 0$). For the second series, we have

$$\left| \sum_{m=0}^{\infty} r_{\mathcal{L}}(m) e^{-\pi i m/2\tau} - \sum_{m=0}^{N} r_{\mathcal{L}}(m) e^{-\pi i m/2\tau} \right| \leq \sum_{m=N+1}^{\infty} r_{\mathcal{L}}(m) e^{\pi m Im(\bar{\tau})/2|\tau|^2},$$

and this goes to zero if $N \to \infty$, because on compacts $Im(\bar{\tau}) = -Im(\tau) \leq -\epsilon$ for some $\epsilon > 0$. □

We are now ready to define the theta function of a lattice.

Definition 3.1.4. *The theta function associated to a lattice $\mathcal{L}$ in $\mathbb{R}^n$ is defined as*

$$\theta_{\mathcal{L}}(\tau) = \sum_{m=0}^{\infty} r_{\mathcal{L}}(m) q^m, \quad q = e^{2\pi i \tau}$$

where τ is an element of the complex upper-half plane $\mathcal{H}$.

The above definition makes sense because $|q| < 1$ if $Im(\tau) > 0$, so if $\tau \in \mathcal{H}$. We now consider the theta function associated to the lattice R. Our goal is to find $r_R(m)$. We now show that $\theta_R(\tau)$ is a weight two modular form of level $\Gamma_0(4)$. For this purpose, it will be useful to know that we can write our function in the form

$$\theta_R(\tau) = \sum_{v \in R} e^{2\pi i \tau \langle v, v \rangle}.$$

since $\langle v, v \rangle \in \mathbb{Z}$ for each $v \in R$.

Proposition 3.1.3. *Let f be a rapidly decreasing smooth function on $\mathbb{R}^n$ and let $\widetilde{f}$ be its Fourier transform. Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$. Then*

$$\sum_{x \in \mathcal{L}} f(x) = \frac{1}{v} \sum_{y \in \mathcal{L}^*} \widetilde{f}(y),$$

where v is the volume of $\mathbb{R}^n / \mathcal{L}$.

Proof. See [Ser12]. □

Lemma 3.1.3. *Let $c > 0$ be a constant and let $f(x) = e^{-c\langle x, x \rangle}$. Then*

$$\widetilde{f}(y) = (\pi/c)^{n/2} e^{-\pi^2 \langle y, y \rangle / c},$$

where x, $y \in \mathbb{R}^n$.

Proof. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then we have

$$\begin{aligned}
\widetilde{f}(y) &= \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle x, y \rangle} d^n x \\
&= \int_{\mathbb{R}^n} e^{-(c \sum_{j=1}^n x_j^2 + 2\pi i x_j y_j)} d^n x \\
&= \prod_{j=1}^n \int_{\mathbb{R}} e^{-(c x_j^2 + 2\pi i x_j y_j)} dx \\
&= \prod_{j=1}^n e^{-\pi^2 y_j^2 / c} \int_{\mathbb{R}} e^{(\sqrt{c} x_j + \pi i y_j / \sqrt{c})^2} dx \\
&= e^{-\pi^2 \langle y, y \rangle / c} \prod_{j=1}^n \frac{1}{\sqrt{c}} \int_{\mathbb{R}} e^{-t_j^2} dt_j \\
&= (\pi/c)^{n/2} e^{-\pi^2 \langle y, y \rangle / c}.
\end{aligned}$$

□

Lemma 3.1.4. *Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$ such that $\langle x,\, x\rangle \in \mathbb{Z}$ and $\langle y,\, y\rangle \in \mathbb{Z}$ for each $x \in \mathcal{L}$ and $y \in \mathcal{L}^*$. Then*

$$\theta_{\mathcal{L}}(\tau) = (i/2\tau)^{n/2} det\mathcal{L}^* \theta_{\mathcal{L}^*}(-1/4\tau).$$

Proof. Let $c = -2\pi i\tau$. If $\tau = \alpha i$ with $\alpha > 0$, we can apply Lemma 3.1.3 to the function $f = e^{2\pi i\tau\langle x,\, x\rangle}$ and we get

$$\widetilde{f}(y) = (-1/2i\tau)^{n/2} e^{\pi\langle y,\, y\rangle/2i\tau} = (i/2\tau)^{n/2} e^{-i\pi\langle y,\, y\rangle/2\tau}.$$

By Proposition 3.1.3, we have

$$\sum_{x\in\mathcal{L}} e^{2\pi i\tau\langle x,\, x\rangle} = det\mathcal{L}^* \sum_{x\in\mathcal{L}^*} (i/2\tau)^{n/2} e^{-i\pi\langle y,\, y\rangle/2\tau},$$

that is

$$\theta_{\mathcal{L}}(\tau) = (i/2\tau)^{n/2} det\mathcal{L}^* \theta_{\mathcal{L}^*}(-1/4\tau) \quad if\ \tau = \alpha i,\ \alpha > 0.$$

So we only need to show that

$$\sum_{x\in\mathcal{L}} e^{2\pi i\tau\langle x,\, x\rangle} \quad and \quad \sum_{x\in\mathcal{L}^*} e^{-i\pi\langle y,\, y\rangle/2\tau}$$

are analytic in τ and the statement will follow by analytic continuation. But by hypothesis $\langle y,\, y\rangle$ and $\langle x,\, x\rangle$ are integers, so

$$\sum_{x\in\mathcal{L}} e^{2\pi i\tau\langle x,\, x\rangle} = \sum_{m=0}^{\infty} r_{\mathcal{L}}(m) e^{2\pi i\tau},$$

and

$$\sum_{x\in\mathcal{L}^*} e^{-i\pi\langle y,\, y\rangle/2\tau} = \sum_{m=0}^{\infty} r_{\mathcal{L}^*}(m) e^{-\pi im/2\tau},$$

which are analytic in $\tau \in \mathcal{H}$ by Lemma 3.1.2. □

Lemma 3.1.5. *Let h be a positive integer such that $h^{1/2}\mathcal{L}^*$ is integral, then*

$$\theta_{\mathcal{L}^*}(\tau + h) = \theta_{\mathcal{L}^*}(\tau).$$

Proof. We have

$$\theta_{\mathcal{L}^*}(\tau + h) = \sum_{w\in\mathcal{L}^*} e^{2\pi i(\tau+h)|w|^2} = \sum_{w\in\mathcal{L}^*} e^{2\pi i(\tau)|w|^2} = \theta_{\mathcal{L}^*}(\tau)$$

since $|h^{1/2}w| = h|w|^2$ and $h^{1/2}\mathcal{L}^*$ is integral. □

Lemma 3.1.6. *Let h be a positive integer such that $h^{1/2}\mathcal{L}^*$ is integral, then*

$$\theta_{\mathcal{L}}(\tau/(4h\tau+1)) = (4h\tau+1)^{n/2}\theta_{\mathcal{L}}(\tau).$$

Proof. Let $t = -(4h\tau+1)/4\tau = -h - 1/4\tau$. Then

$$\begin{aligned}
\theta_{\mathcal{L}}(\tau/(4h\tau+1)) &= \theta_{\mathcal{L}}(-1/4t) \\
&= (2t/i)^{n/2} det\mathcal{L}^* \theta_{\mathcal{L}^*}(t) \\
&= (2t/i)^{n/2} det\mathcal{L}^* \theta_{\mathcal{L}^*}(-1/4\tau) \\
&= (2t/i)^{n/2} det\mathcal{L}^* (2\tau/i)^{n/2} (det\mathcal{L}^*)^{-1} \theta_{\mathcal{L}}(\tau) \\
&= (-4t\tau)^{n/2}\theta_{\mathcal{L}}(\tau) \\
&= (4h\tau+1)^{n/2}\theta_{\mathcal{L}}(\tau).
\end{aligned}$$

□

We will need the following theorem, taken from [DS05]

Theorem 3.1.1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ of level N, and let $q_N = e^{2\pi i\tau/N}$ for $\tau \in \mathcal{H}$. Suppose that the function $f : \mathcal{H} \to \mathbb{C}$ is holomorphic and weight-k invariant under Γ. Suppose also that, in the Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} a_n q_N^n$, we have*

$$|a_n| \leq Cn^r \quad \textit{for some positive constants } C \textit{ and } r.$$

Then $f \in \mathcal{M}_k(\Gamma)$.

Theorem 3.1.2. *The function $\theta_R(\tau)$ is an element of $\mathcal{M}_2(\Gamma_0(4))$, the space of weight two modular forms of level $\Gamma_0(4)$.*

Proof. All the above lemmas can be applied to $\theta_R(\tau)$ because R^* is integral and $\langle x,\, x\rangle \in \mathbb{Z}$ for each $x \in R$. We see that $\theta_R(\tau)$ is holomorphic by Lemma 3.1.2 and it is bounded at $+i\infty$. Moreover,

$$\theta_R(\tau+1) = \theta_R(\tau) \quad \text{and} \quad \theta_R(\tau/(4\tau+1)) = (4\tau+1)^2\theta_R(\tau),$$

where we have applied Lemma 3.1.6 with $h = 1$ and $n = 4$. This means that $\theta_R(\tau)$ is weakly modular of weight two for the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix},$$

hence it is weakly modular of weight two for every matrix in $\Gamma_0(4)$. (Indeed, these two matrices generate $\Gamma_0(4)$, see [DS05]). Then, we can apply Theorem 3.1.1 because

$$\theta_R(\tau) = \sum_{k=0}^{\infty} c_k r_R(k/4) q^{k/4}, \quad q = e^{2\pi i\tau},$$

where $c_k = 1$ if $k \equiv 0 \,(mod\, 4)$ and $c_k = 0$ otherwise. □

3.2 Computing the numbers $r_R(m)$

The aim of this section is to get the m-th Fourier coefficient of $\theta_R(\tau)$. We will use several facts, mainly from [DS05], to find the Fourier expansion of the elements of a basis for $\mathcal{M}_2(\Gamma_0(4))$. Finally, we will find the coordinates of $\theta_R(\tau)$ in this basis.

Definition 3.2.1. *Let k be an even positive integer. We denote by $G_k(\tau)$ the weight k Eisenstein series*

$$G_k(\tau) = \sum_{c\in\mathbb{Z}} \sum_{d\in\mathbb{Z}'_c} \frac{1}{(c\tau+d)^k}$$

where $\mathbb{Z}'_c = \mathbb{Z} - \{0\}$ and $\mathbb{Z}'_c = \mathbb{Z}$ otherwise.

One can show that $G_k(\tau)$ converges absolutely if $k > 2$ and $G_2(\tau)$ converges conditionally (See [Ser12] or [DS05]). Moreover,

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n, \quad \sigma_{k-1}(n) = \sum_{\substack{d|n\\ d>0}} d, \quad \zeta(k) = \sum_{n=1}^{\infty}\frac{1}{n^k},$$

where $q = e^{2\pi i\tau}$. (For the proof, see [Ser12] or [DS05]).

Definition 3.2.2. *Let $N > 0$ be an integer. We denote by $G_{2,N}(\tau)$ the function*

$$G_{2,N}(\tau) = G_2(\tau) - NG_2(N\tau).$$

Proposition 3.2.1. *The functions $G_{2,2}(\tau)$ and $G_{2,4}(\tau)$ have the following Fourier expansions:*

$$G_{2,2}(\tau) = \frac{-\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{d|n,\, 2\nmid d} d\right)q^n\right)$$

and

$$G_{2,4}(\tau) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{d|n,\, 4\nmid d} d\right)q^n\right),$$

where $d > 0$ and $q = e^{2\pi i\tau}$.

Proof. We have seen above that

$$G_2(\tau) = \frac{\pi^2}{3} - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

so

$$\begin{aligned} G_{2,2}(\tau) &= \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n - 2\left(\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^{2n}\right) \\ &= -\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} (\sigma_1(n) q^n - 2\sigma_1(n) q^{2n}) \\ &= -\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \left(\sigma_1(n) - \left(\sum_{d|n,\, 2|d} d\right)\right) q^n \\ &= -\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \left(\sum_{d|n,\, 2\nmid d} d\right) q^n \\ &= \frac{-\pi^2}{3}\left(1 + 24 \sum_{n=1}^{\infty} \left(\sum_{d|n,\, 2\nmid d} d\right) q^n\right). \end{aligned}$$

The other statement is proved analogously. □

Theorem 3.2.1. *The functions $G_{2,2}(\tau)$ and $G_{2,4}(\tau)$ are in $\mathcal{M}_2(\Gamma_0(4))$ and they are also linearly independent.*

Proof. We have $\sigma_1(n) < n^2$, so $G_{2,2}(\tau)$ and $G_{2,4}(\tau)$ converge uniformly on compact subsets of $\mathcal{H}$. (The proof is analogous to what we did for $\theta_R(\tau)$). One can also prove that $G_{2,2}(\tau)$ and $G_{2,4}(\tau)$ are weight-2 invariant under $\Gamma_0(4)$ (See [DS05]). So we can apply Theorem 3.1.1 as we did for $\theta_R(\tau)$. We now show that the two functions are linearly independent. If they were dependent, we see by looking at the first Fourier coefficients that it would be $G_{2,4}(\tau) = 3G_{2,2}(\tau)$. But then, by looking at the Fourier coefficients for $n = 1$, we would have $24 = 8$, so they are independent. □

In the following theorem and lemmas, Γ will denote a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, g will be the genus of $X(\Gamma)$, ϵ_∞ the number of cusps, ϵ_2 the number of elliptic points with period 2, ϵ_3 the number of elliptic points with period 3.

Theorem 3.2.2. *If k is an even integer, then*

$$dim(\mathcal{M}_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k}{2}\epsilon_\infty & if\ k \geq 2, \\ 1 & if\ k = 0, \\ 0 & if\ k < 0. \end{cases}$$

Proof. See [DS05]. □

The following two lemmas are taken from [DS05].

Lemma 3.2.1. *The number of elliptic points for* $\Gamma_0(N)$ *is*

$$\epsilon_2(\Gamma_0(N)) = \begin{cases} \prod_{p|N}(1+\left(\frac{-1}{p}\right)) & if\ 4 \nmid N, \\ 0 & if\ 4|N, \end{cases}$$

where $(-1/p)$ *is* ± 1 *if* $p \equiv \pm 1\ (mod\ 4)$ *and is* 0 *if* $p = 2$ *and*

$$\epsilon_3(\Gamma_0(N)) = \begin{cases} \prod_{p|N}(1+\left(\frac{-3}{p}\right)) & if\ 9 \nmid N, \\ 0 & if\ 9|N, \end{cases}$$

where $(-3/p)$ *is* ± 1 *if* $p \equiv \pm 1\ (mod\ 3)$ *and is* 0 *if* $p = 3$.

Lemma 3.2.2. *The number of cusps of* $\Gamma_0(N)$ *is*

$$\epsilon_\infty(\Gamma_0(N)) = \sum_{d|N} \phi(\gcd(d, N/d)),$$

where $d > 0$ *and* ϕ *is the Euler totient function.*

The following proposition can be found in [Shi71].

Lemma 3.2.3. *Let* Γ' *be a subgroup of* $SL_2(\mathbb{Z})$ *of index d, and let* ϵ_2 *and* ϵ_3 *be the numbers of* Γ'*-inequivalent elliptic points of order 2,3, respectively. Furthermore, let* ϵ_∞ *be the number of* Γ'*-inequivalent cusps. Then the genus* g *of* $X(\Gamma)$ *is given by*

$$g = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}.$$

We are now ready to find the cardinality of Γ_m.

Proposition 3.2.2. *We have*

$$r_R(m) = 24 \sum_{d|n,\ 2\nmid d} d,$$

where $d > 0$.

Proof. We have

$$[\mathrm{SL}_2(\mathbb{Z}) :\ \Gamma_0(N)] = N \prod_{p|N}(1 + 1/p),$$

hence we see from the above lemmas and from Theorem 3.2.2 that

$$dim(\mathcal{M}_2(\Gamma_0(4))) = 2,$$

so $G_{2,2}(\tau)$ and $G_{2,4}(\tau)$ are a basis for $\mathcal{M}_k(\Gamma_0(4))$. Then, it is easy to check that $r_R(0) = 1$ and $r_R(1) = 24$. So we have

$$\theta_R\tau = \alpha G_{2,2}(\tau) + \beta G_{2,4}(\tau),$$

where

$$\begin{cases} \alpha(\frac{-\pi^2}{3}) + \beta(-\pi^2) = 1 \\ \alpha(-24\frac{\pi}{3}) + \beta(-8\pi^2) = 24. \end{cases}$$

The solutions for the system are $\alpha = -3/\pi^2$, $\beta = 0$. Hence

$$\theta_R\tau = (-3/\pi^2)G_{2,2}(\tau),$$

and the statement follows. □

4 The p-adic upper half plane and the Bruhat-Tits tree

Let p be a prime, we will denote by $\mathcal{H}_p$ the *p-adic upper half plane*, which (as a set) is defined as

$$\mathcal{H}_p = \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p),$$

where $\mathbb{C}_p$ is the p-adic completion of an algebraic closure of $\mathbb{Q}_p$. In this chapter we will study a covering of $\mathcal{H}_p$ by affinoids subsets, we will introduce the Bruhat-Tits tree and study its relation to $\mathcal{H}_p$.

4.1 Affinoids and annuli

In Chapter 5 we will introduce the notion of rigid-analytic function on $\mathcal{H}_p$, which will somehow be analougous to the notion of holomorphic function and, to define it, we need to cover $\mathcal{H}_p$ with suitable subsets. At first, we could think about the p-adic balls (as an analogue of the usual balls in $\mathbb{C}$). However, this would not be a good choice, because the p-adic balls are either disjoint or contained in one another (so, defining the notion of holomorphic function on the p-adic balls, we would not be able to use the analytic continuation principle, because the identity theorem for holomorphic functions would fail). In this section we will find a suitable covering of $\mathcal{H}_p$ by *affinoids*. Our main references are [DT08] and [Dar04].

Let v_p and $|\ |_p$ be the p-adic valuation and the p-adic absolute value (normalized so that $|p|_p = 1/p$). We will use the notation

$$\tau = [\tau_0, \tau_1],$$

to denote points of $\mathcal{H}_p$. We can always choose τ_0, τ_1 such that they are both integral and at least one of them is a unit (this choice is unique up to multiplication by units). Such homogeneous coordinates are called *unimodular* coordinates. From now on, we will always assume that the points of $\mathcal{H}_p$ are written in unimodular coordinates.

Definition 4.1.1. *We write*

$$[\tau_0, \tau_1] \equiv [\tau_0', \tau_1'] \quad (mod\, p^n)$$

if $\tau_0 \equiv \tau_0'\ (mod\, p^n)$ *and* $\tau_1 \equiv \tau_1'\ (mod\, p^n)$.

Let

$$red:\ \mathbb{P}^1(\mathbb{C}_p) \to \mathbb{P}^1(\bar{\mathbb{F}}_p)$$

be the reduction modulo the maximal ideal of the ring of integers of $\mathbb{C}_p$. Defining

$$\mathcal{A} := red^{-1}(\mathbb{P}^1(\bar{\mathbb{F}}_p) - \mathbb{P}^1(\mathbb{F}_p)),$$

we have $\mathcal{A} \subset \mathcal{H}_p$ because $red(\mathbb{P}^1(\mathbb{Q}_p)) \subset \mathbb{P}^1(\mathbb{F}_p)$. So

$$\begin{aligned}\mathcal{A} &= \mathcal{H}_p - \{\, \tau \in \mathcal{H}_p \mid |\tau|_p \geq 1, \text{ and } |\tau - s|_p \leq 1 \text{ for } s = 0, \ldots, p-1 \,\} \\ &= \{\, \tau \in \mathcal{H}_p \mid |\tau|_p \leq 1, \text{ and } |\tau - s|_p \geq 1 \text{ for } s = 0, \ldots, p-1 \,\}.\end{aligned}$$

The set $\mathcal{A}$, which can be imagined as a sphere with $p+1$ holes, is called *standard affinoid*. Now, consider the sets

$$\begin{aligned}\mathcal{W}_s &= \left\{ \tau \in \mathbb{P}^1(\mathbb{C}_p) \;\middle|\; \frac{1}{p} < |\tau - s| < 1 \right\} \quad s = 0, \ldots, p-1, \\ \mathcal{W}_\infty &= \{\, \tau \in \mathbb{P}^1(\mathbb{C}_p) \mid 1 < |\tau| < p \,\}.\end{aligned}$$

These sets are all contained in $\mathcal{H}_p$ because $|\tau| \in p^{\mathbb{Z}}$ if $\tau \in \mathbb{Q}_p$ and $\tau \neq 0$. They are called *annuli* and $\mathcal{W}_0$ is called *standard annulus*. We will now construct general affinoids.

Definition 4.1.2. *Let $r > 0$ and $c = [c_0, c_1]$ in $\mathbb{P}^1(\mathbb{C}_p)$. We define the closed ball of center c and radius r as*

$$B(c, r) = \{\, \tau = [\tau_0, \tau_1] \in \mathbb{P}^1(\mathbb{C}_p) \mid v_p(\tau_0 c_1 - \tau_1 c_0) \geq r \,\},$$

and the open ball of center c and radius r as

$$B^-(c, r) = \{\, \tau = [\tau_0, \tau_1] \in \mathbb{P}^1(\mathbb{C}_p) \mid v_p(\tau_0 c_1 - \tau_1 c_0) > r \,\}.$$

Lemma 4.1.1. *Let $r > 0$. If $c = [a, 1]$ with $v_p(a) \geq 0$, then*

$$B(c, r) = \left\{ \tau = [\tau_0, \tau_1] \in \mathbb{P}^1(\mathbb{C}_p) \;\middle|\; v_p\left(\frac{\tau_0}{\tau_1} - a\right) \geq r \right\}.$$

If $c = [1, b]$ with $v_p(b) \geq 0$, then

$$B(c, r) = \left\{ \tau = [\tau_0, \tau_1] \in \mathbb{P}^1(\mathbb{C}_p) \;\middle|\; v_p\left(\frac{\tau_1}{\tau_0} - b\right) \geq r \right\}.$$

Proof. If τ_1 is an unit, then $v_p\left(\frac{\tau_0}{\tau_1} - a\right) = v_p(\tau_0 - \tau_1 a)$, so in this case the first statement is clear. Otherwise, if $v_p(\tau_1) > 0$, we have

$$v_p\left(\frac{\tau_0}{\tau_1} - a\right) = -v_p(\tau) < 0 \quad \text{and} \quad v_p(\tau_0 - \tau_1 a) = v_p(\tau_0) = 0,$$

so the conditions

$$v_p\left(\frac{\tau_0}{\tau_1} - a\right) \geq r \quad \text{and} \quad v_p(\tau_0 - \tau_1 a) \geq r$$

are both false. Thse second statement is proven analogously. □

Remark 4.1.1. The result of the previous lemma holds also if we consider $B^-(c,r)$ insetad of $B(c,r)$.

Lemma 4.1.2. *Let $c = [c_0, c_1]$, $c' = [c'_0, c'_1]$ and let n be a positive integer. The following statements are equivalent:*

1. $B(c,n) \cap B(c',r) \neq \emptyset$
2. $[c_0, c_1] \equiv \mu[c'_0, c'_1] \pmod{p^n}$,

where μ is a unit in $\mathbb{Z}_p$.

Proof. Let $\tau = [\tau_0, \tau_1] \in B(c,n) \cap B(c',r)$. Without loss of generality, we can assume $v_p(\tau_0) = 0$. Then we have

$$v_p(c'_0 c_1 \tau_0 - c'_0 c_0 \tau_1) \geq v_p(c_1\tau_0 - c_0\tau_1) \geq n,$$

and

$$v_p(c_0 c'_1 \tau_0 - c_0 c'_0 \tau_1) \geq v_p(c'_1\tau_0 - c'_0\tau_1) \geq n.$$

So, using the fact that $v_p(\alpha + \beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$, we have

$$v_p(c'_0 c_1 - c_0 c'_1) \geq n.$$

(Where we substituted $\alpha = c'_0 c_1 \tau_0 - c'_0 c_0 \tau_1$, $\beta = c_0 c'_1 \tau_0 - c_0 c'_0 \tau_1$ and then we divided byτ_0). So we see that the matrix

$$\begin{pmatrix} c_0 & c_1 \\ c'_0 & c'_1 \end{pmatrix}$$

is singular modulo p^n and the second statement holds. Now assume that $[c_0, c_1]$ and $[c'_0, c'_1]$ are multiples modulo p^n. This means that there is a non-zero vector $[\tau_0, \tau_1]$ such that

$$\begin{pmatrix} c_0 & c_1 \\ c'_0 & c'_1 \end{pmatrix} \begin{pmatrix} \tau_0 \\ \tau_1 \end{pmatrix} = \begin{pmatrix} c_0\tau_0 + c_1\tau_1 \\ c'_0\tau_0 + c'_1\tau_1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^n}.$$

Then $[-\tau_1, \tau_0]$ is in $B(c,n) \cap B(c',r)$. □

Definition 4.1.3. *Let n be a positive integer and $\mathcal{R}_n$ a set of representatives for $\mathbb{P}^1(\mathbb{Q}_p)$ modulo p^n. We define the sets Ω_n and Ω_n^- as*

$$\Omega_n := \mathbb{P}^1(\mathbb{C}_p) - \bigcup_{c \in \mathcal{R}_n} B(c,n),$$

and

$$\Omega_n^- := \mathbb{P}^1(\mathbb{C}_p) - \bigcup_{c \in \mathcal{R}_n} B^-(c, n-1).$$

The sets Ω_n^- are called affinoids.

From the above definition and from Lemma 4.1.2, we see that $\Omega_n \subset \Omega_{n+1}$ and that $\bigcup_{n\geq 1} \Omega_n = \mathcal{H}_p$. Moreover, we notice that the interior of the regions

$$\Omega_n - \Omega_n^-$$

is given by

$$\bigcup_{c\in\mathcal{R}_n} (B^-(c, n-1) - B(c, n)),$$

which is the union of open annuli.

Lemma 4.1.3. *Let $[\tau_0, \tau_1] \in \mathbb{P}^1(\mathbb{C}_p)$ and let $b \in \mathbb{C}_p$ such that $v_p(b) > 0$. Assume that $v_p(b) < n$, where n is a positive integer. Then the following conditions are equivalent.*

1. $v_p(\frac{\tau_1}{\tau_0} - b) < n$
2. $v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b}) < n - 2v_p(b)$

Proof. If $v_p(\tau_0) \geq 0$ and $v_p(\tau_1) = 0$, then

$$v_p(\frac{\tau_1}{\tau_0} - b) = v_p(\frac{\tau_1}{\tau_0}) < 0, \text{ and}$$
$$v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b}) = -v_p(b) < 0,$$

so conditions *1.* and *2.* are both satisfied. Assume now that $v_p(\tau_1) \geq 0$ and $v_p(\tau_0) = 0$. If $v_p(b) < v_p(\tau_1)$ then

$$v_p(\frac{\tau_1}{\tau_0} - b) = v_p(b) < n,$$

so *1.* holds. Moreover

$$v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b}) = -v_p(\tau_1) < -v_p(b) < -v_p(b) + n - v_p(b),$$

so also *2.* holds. If $v_p(b) > v_p(\tau_1)$ then

$$v_p(\frac{\tau_1}{\tau_0} - b) = v_p(\tau_1) < v_p(b) < n, \text{ and}$$
$$v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b}) = -v_p(b) < n - 2v_p(b),$$

so both conditions *1.* and *2.* hold. Finally, if $v_p(b) = v_p(\tau_1)$, then

$$v_p(\frac{\tau_1}{\tau_0} - b) = v_p(\tau_1) + v_p(b) + v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b}) = 2v_p(b) + v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b}),$$

so *1.* holds if and only if *2.* holds. □

Proposition 4.1.1. *Let $\{a_i\}_{i=0}^{p^n-1}$ be a set of representatives for $\mathbb{Z}_p/p^n\mathbb{Z}_p$ and $\{b_i\}_{j=0}^{p^{n-1}-1}$ be a set of representatives for $p\mathbb{Z}_p/p^n\mathbb{Z}_p$ where we choose $b_0 = 0$. Then Ω_n is defined by the inequalities*

$$v_p(\frac{\tau_0}{\tau_1} - a_i) < n, \quad v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b_j}) < n - 2v_p(b_j), \quad v_p(\frac{\tau_0}{\tau_1}) > -n,$$

and Ω_n^- is defined by the inequalities

$$v_p(\frac{\tau_0}{\tau_1} - a_i) \leq n - 1, \quad v_p(\frac{\tau_0}{\tau_1} - \frac{1}{b_j}) \leq n - 1 - 2v_p(b_j), \quad v_p(\frac{\tau_0}{\tau_1}) \geq 1 - n,$$

where $\tau \in \mathbb{P}^1(\mathbb{C}_p)$.

Proof. The statements follow from the definitions of Ω_n and Ω_n^- and from Lemma 4.1.3. □

From the above construction we see that Ω_1^- is the standard affinoid and $\Omega_1 - \Omega_1^-$ is the union of the annuli $\mathcal{W}_\infty$ and $\mathcal{W}_s$ with $s = 0, \ldots, p-1$. So affinoids are constructed by cutting off open balls centered at points of $\mathbb{P}^1(\mathbb{Q}_p)$. We also see that two affinoids Ω_n^- and Ω_{n+1}^- are "glued" through the annuli

$$B^-(c, n-1) - B(c, n), \text{ where } c \in \mathcal{R}_n.$$

Indeed, given an affinoid Ω_n^-, we "shrink" its holes (including the hole at infinity) by "thickening" it with the open region $\Omega_n - \Omega_n^-$. Then, we construct Ω_{n+1}^- by filling all the holes centered in points of $\mathcal{R}_n$ and cutting off open balls centered at the points of $\mathcal{R}_{n+1}$. In the next section, we will se another way to think this construction.

4.2 The Bruhat-Tits tree

In this section we will introduce the Bruhat-Tits tree, which can be viewed as the skeleton of the p-adic upper half plane. The main references for this section are [DT08] and [Ser80].

Definition 4.2.1. *A lattice L in $\mathbb{Q}_p^2$ is a free, rank two $\mathbb{Z}_p$-module given by $L = \langle e_1, e_2 \rangle$, where $\{ e_1, e_2 \}$ is a basis for $\mathbb{Q}_p^2$. Two such lattices L and L' are called homothetic if $L' = zL$ for some constant $z \in \mathbb{Q}_p$.*

Clearly, being homothetic is an equivalence relation; we will denote by $[L]$ the class of all lattices which are homothetic to L. Given two lattices L and L', we want to define the notion of distance between $[L]$ and $[L']$. By the invariant factor theorem, we can find a basis $\{ e_1, e_2 \}$ for L and integers a, b such that $\{ p^a e_1, p^b e_2 \}$ is a basis for L'. The distance between $[L]$ and $[L']$ is then defined as

$$d([L], [L']) = |a - b|.$$

This definition does not depend on the choice of the representatives for the homothety classes. Indeed, if z, z' are elemnts of $\mathbb{Q}_p$, then

$$zL = \langle ze_1, ze_2 \rangle,$$

and

$$z'L' = \langle p^a z' e_1, p^b z' e_2 \rangle = \langle p^{a+v_p(\frac{z'}{z})} z e_1, p^{b+v_p(\frac{z'}{z})} z e_2 \rangle.$$

So we have

$$d([zL], [z'L']) = |a + c - (b + c)| = |a - b|,$$

where $c = v_p(\frac{z'}{z})$.

Remark 4.2.1. We have

$$d([L], [L']) = 1 \Leftrightarrow \text{ there are representatives } L' \subset L \text{ such that } l(L/L') = 1,$$

where $l(L/L')$ denotes the lenght of a Jordan-Hölder sequence for L/L'.

Lemma 4.2.1. *If L and L' are two lattices in $\mathbb{Q}_p$, the following conditions are equivalent:*

1. *$L' \subset L$ and L' is maximal in $[L']$ with this property,*
2. *$L' \subset L$ and $L' \not\subset pL$,*
3. *$L' \subset L$ and L/L' has only one generator.*

Proof. If we assume *1* then *2* follows. Indeed, if it was $L' \subset pL$, then $\frac{1}{p}L' \subset L$,which contradicts the maximality of L'.

We now show that *2* implies *1*.Let $\{ e_1, e_2 \}$ and $\{ p^a e_1, p^b e_2 \}$ be bases for L and L', respectively. Then a and b are positive because L' is contained in L. Moreover, since $L' \not\subset pL$, either $a = 0$ or $b = 0$. We can assume without loss of generality that $a = 0$. Then, if there was a L'' in $[L']$ such that $L' \subset L'' \subset L$, it would be

$$L'' = \langle p^c e_1, p^{b+c} e_2 \rangle.$$

But then $c \geq 0$ (because $L'' \subset L$), and it cannot be $c > 0$ (because otherwise $L' \subset pL$). So $c = 0$ and $L'' = L'$.

Then, condition *3* also follows fron *2*, because we have just seen that *2* implies that L' is of the form $\{ p^b e_1, e_2 \}$, where $b > 0$ and $\{ e_1, e_2 \}$ is a basis for L. So $L/L' = \mathbb{Z}_p/p^b\mathbb{Z}_p$.

Finally, if we assume that condition *3* holds we will have $L' = \langle p^a e_1, p^b e_2 \rangle$ with $a, b \geq 0$. So

$$L/L' = (\mathbb{Z}_p/p^a\mathbb{Z}_p) \oplus (Z_p/p^b\mathbb{Z}_p).$$

But L/L' has only one generator, so either $a = 0$ or $b = 0$, so $L' \not\subset pL$ and condition *2* is also satisfied. □

Remark 4.2.2. If L is given, then for each class $[L']$ we have an unique representative L'' satisfying the conditions of Lemma 4.2.1. Indeed, if $\{ e_1, e_2 \}$ and $\{ p^a e_1, p^b e_2 \}$ are bases for L and L', we take $L'' = p^{-\min\{a,b\}} L'$.

Definition 4.2.2. *The Bruhat-Tits tree for* $\mathrm{PGL}(\mathbb{Q}_p)$ *is the graph* $\mathcal{T}$ *whose vertices are the homotethy classes of lattices in* $\mathbb{Q}_p^2$*, where two vertices are joined by an edge if they correspond to classes* $[L]$ *and* $[L']$ *with*

$$pL \subset L' \subset L.$$

We denote by $V(\mathcal{T})$ *and* $E(\mathcal{T})$ *the vertices and edges of* $\mathcal{T}$*, respectively.*

We see that the relation above is symmetrical, so $\mathcal{T}$ is an unordered graph.

Theorem 4.2.1. *The Bruhat-Tits tree* $\mathcal{T}$ *for* $\mathrm{PGL}(\mathbb{Q}_p)$ *is a tree.*

Proof. To show that $\mathcal{T}$ is connected, consider two vertices $[L]$ and $[L']$, where L and L' are representatives satisfying $L' \subset L$ and $L' \not\subset pL$ (it is possible to pick such representatives because of Remark 4.2.2). Consider a Jordan-Hölder sequence for L/L'

$$L' = L_n \subset L_{n-1} \subset \cdots \subset L_0 = L.$$

Then $d(L_{i-1}, L_i) = 1$ by Remark 4.2.1, so we have a path connecting $[L]$ and $[L']$. So $\mathcal{T}$ is connected. We now prove that $\mathcal{T}$ is a tree. For this purpose, we consider a sequence without backtracking $[L_0], \ldots, [L_n]$ and we show that $[L_0] \neq [L_n]$. We can assume that the representatives are such that $L_{i+1} \subset L_i$ and $l(L_i/L_{i+1}) = 1$. If we show that $L_n \not\subset L_0$, then we will have $[L_0] \neq [L_n]$. We proceed by induction on n. The case $n = 0$ is clear. Assume now that $L_{n-1} \not\subset pL_0$. Since $pL_{n-2} \neq L_n$ (because we are assuming we have no backtracking), we have

$$L_{n-1} = L_n + pL_{n-2},$$

so $L_{n-1} \equiv L_n \pmod{pL_0}$ and the thesis follows by induction hypothesis. □

Proposition 4.2.1. *Let* L_0 *be a lattice in* $\mathbb{Q}_p^2$*. The vertices of* $\mathcal{T}$ *at distance* n *from a vertex* $[L_0]$ *are in bijection with points of* $\mathbb{P}^1(\mathbb{Z}_p/p^n\mathbb{Z}_p)$*.*

Proof. By Remark 4.2.2 each vertex of $\mathcal{T}$ has a unique representative L such that $L \subset L_0$ and $L_0/L \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$, where $n = d([L], [L_0])$. Moreover, L/p^nL_0 is a direct factor of rank one for the free $\mathbb{Z}_p/p^n\mathbb{Z}_p$-module of rank two L_0/p^nL_0. Viceversa, if

$$L_0/p^nL_0 = M_1 \oplus M_2 = (\mathbb{Z}_p/p^n\mathbb{Z}_p)^2,$$

then for each direct factor M_i we have

$$M_i \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \quad \text{and} \quad M_i = L/p^nL_0,$$

with $p^nL_0 \subset L \subset L_0$. So we see that the vertices of $\mathcal{T}$ at distance n from $[L_0]$ are in bijection with direct factors of L_0/p^nL_0 of rank one, but these are in bijection with points of $\mathbb{P}^1(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. □

Corollary 4.2.1. *The Bruhat-Tits tree is $p+1$-regular.*

Proof. Let $[L_0]$ be a vertex of $\mathcal{T}$. Then, by proposition 4.2.1, the vertices at distance one from $[L_0]$ are in bijection with points of $\mathbb{P}^1(\mathbb{Z}_p/p\mathbb{Z}_p)$, so there are $p+1$ of them. □

If e is an oriented edge running from the vertex v to the vertex w, we write

$$s(e) = v, \quad t(e) = w,$$

and we denote by $\bar{e}$ the oriented edge such that

$$s(\bar{e}) = v, \quad t(\bar{e}) = w.$$

If we see $\mathbb{Q}_p^2$ as space of column vectors, then we can associate to each lattice L the matrix M_L whose columns are the vectors of a basis for L. Then we can define an action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{T}$ by $g[L] = [gL]$, where $g \in \mathrm{PGL}_2(\mathbb{Q}_p)$. This action is well defined and preserves adjacency, so it gives an action on $\mathcal{T}$ by graph automorphisms. From now on, we will use the notation $v_0 = [\mathbb{Z}_p^2]$ and $v_1 = \left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right) v_0$. We will refer to v_0 as *privileged vertex*. Moreover, we will denote by e_0 the edge running from v_0 to v_1 and we will call it *the privileged edge*.

Definition 4.2.3. *We will denote*

$$G_0 = \mathrm{PGL}_2(\mathbb{Z}_p),$$

and

$$G_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Q}_p) \;\middle|\; p|c \right\}.$$

Proposition 4.2.2. *The stabilizers in* $\mathrm{PGL}_2(\mathbb{Q}_p)$ *for* v_0 *and* e_0 *are*

$$\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(v_0) = G_0$$

and

$$\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(e_0) = G_1.$$

As a consequence, we have the $\mathrm{PGL}_2(\mathbb{Q}_p)$*-equivariant bijections*

$$\phi : \mathrm{GL}_2(\mathbb{Q}_p)/G_0 \to V(\mathcal{T})$$

and

$$\psi : \mathrm{GL}_2(\mathbb{Q}_p)/G_1 \to E(\mathcal{T})$$

Proof. If $\gamma \in \mathrm{GL}_2(\mathbb{Q}_p)$, then γ fixes v_0 if and only if $\gamma[\mathbb{Z}_p^2] = [\mathbb{Z}_p^2]$, i. e., if and only if $\gamma \in \mathrm{GL}_2(\mathbb{Z}_p)$. Since we are considering homothety classes of lattices, this tells us that

$$\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(v_0) = \mathrm{PGL}_2(\mathbb{Z}_p).$$

Then,

$$\begin{aligned} \mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(e_0) &= \mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(v_0) \cap \mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Q}_p)}(v_1) \\ &= G_0 \cap \left(\left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right) G_0 \left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)^{-1} \right) \\ &= G_1. \end{aligned}$$

Defining $\phi(\gamma) = \gamma v_0$ and $\psi(\gamma) = \gamma e_0$, the second statement follows. □

Definition 4.2.4. *Let $P = ([L_0], [L_1], \dots)$ and $P'([L_0'], [L_1'], \dots)$ be infinite paths without backtracking in $\mathcal{T}$. If P and P' differ only by a finite number of vertices, we say that they are equivalent and we write*

$$P \sim P'.$$

*An equivalence class for $\sim$ of such sequences is called an **end** of $\mathcal{T}$. The set of all ends is denoted by* $\mathrm{Ends}(\mathcal{T})$.

We can put a topology on $\mathrm{Ends}(\mathcal{T})$ by taking as a basis the sets

$$U(e) = \{\, [P] \in \mathrm{Ends}(\mathcal{T}) \mid P = ([L_0], [L_1] \dots) \,\},$$

where e is an oriented edge running from $[L_0]$ to $[L_1]$. Moreover, the group $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts on $\mathbb{P}^1(\mathbb{C}_p)$ by Möbius transformations (see Section 5.1 for the definition of the action).

Proposition 4.2.3. *There is a $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivariant homeomorphism from $\mathrm{Ends}(\mathcal{T})$ to $\mathbb{P}^1(\mathbb{Q}_p)$.*

Proof. We can identify $\mathrm{Ends}(\mathcal{T})$ with the set of all infinite paths starting from the vertex v_0. Then, by Proposition 4.2.1 we have that the vertices at distance n from v_0 are identified with the lines of $\mathbb{Z}_p^2/p^n\mathbb{Z}_p^2$. By reducing modulo p one of these lines (which correspond to a vertex v), we get a line in $\mathbb{Z}_p^2/p^{n-1}\mathbb{Z}_p^2$ (which corresponds to a vertex w adjacent to v). Thus we see that the points of $\mathcal{T}$ give us an inverse system and, as sets

$$\mathrm{Ends}(\mathcal{T}) = \varprojlim \mathbb{P}^1(\mathbb{Z}_p/p^n\mathbb{Z}_p) = \mathbb{P}^1(\mathbb{Z}_p) = \mathbb{P}^1(\mathbb{Q}_p).$$

For the rest of the proof see [DT08]. □

4.3 The reduction map

It can be proved that there is a $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivariant map from the p-adic upper half plane to the Bruhat-Tits tree such that the affinoids Ω_n^- constructed in Section 4.1 are the inverse image of subtrees of $\mathcal{T}$ made up of edges and vertices at distance at most $n-1$ from the standard vertex v_0. In this section we will sketch the construction of such a map, mainly following [DT08].

Definition 4.3.1. *A norm on $\mathbb{Q}_p^2$ is a function $n : \mathbb{Q}_p^2 \to \mathbb{R} \cup \{\infty\}$ such that, for any $x, y \in \mathbb{Q}_p^2$ and $a \in \mathbb{Q}_p$, we have:*

1. *$n(x) = \infty$ iff $x = 0$,*
2. *$n(ax) = v_p(a) + n(x)$,*
3. *$n(x+y) \geq min\{n(x), n(y)\}$, where equality holds if $v_p(x) \neq v_p(y)$.*

Two such norms n and n' are said to be equivalent if $n - n' = c$ for some $c \in \mathbb{R}$.

To every point of the tree $\mathcal{T}$ we can associate an equivalence class of norms. In particular, if $v = [L]$ is a vertice and $\{ e_1, e_2 \}$ is a basis forthe lattice L, we construct a norm in the following way: given an an element x of $\mathbb{Q}_p^2$, we can write it in the basis $\{ e_1, e_2 \}$ as $x = ae_1 + be_2$. Then we define a norm $n_{[L]}$ as:

$$n_{[L]}(x) = \min \{ v_p(a), v_p(b) \}.$$

This definition does not depend on the basis that we choose for the lattice L, indeed:

$$\min \{ v_p(a), v_p(b) \} = - \min \left\{ h \in \mathbb{Z} \;\middle|\; p^h x \in L \right\}.$$

If $z = (1-t)[L] + t[L']$ is a point of an edge between the vertices $[L]$ and $[L']$, then we can find a basis $\{ e_1, e_2 \}$ for $[L]$ such that $\{ e_1, pe_2 \}$ is a basis for $[L']$. Writing $x = ae_1 + be_2$, we can define a norm n_z by:

$$n_z(x) = \min \{ v_p(a), v_p(b) - t \}.$$

If $n_{[L]}(x) = n_{[L']}(x)$, then $n_z = n_{[L]}(x)$, otherwise $n_z = n_{[L]} - t$, so n_z does not depend on the bases for L and L'. One can also check that if we choose different representatives for the homothethy classes of $[L]$ and $[L']$, we get norms equivalent to $n_{[L]}$ and n_z.

Proposition 4.3.1. *There is a bijection between the points of the Bruhat-Tits tree and the equivalence classes of norms on $\mathbb{Q}_p^2$.*

Proof. (Sketch). We have seen above that we can associate classes of equivalences of norms to points of $\mathcal{T}$. We show how to get a point of $\mathcal{T}$ from an equivalence class of norms C. One

can check that these two constructions give a bijection. We can take a representative $n \in C$ such that $n(x) = 0$ for some $x \in \mathbb{Q}_p^2$. Let

$$L' = \left\{ x \in \mathbb{Q}_p^2 \;\middle|\; n(x) \geq 0 \right\}.$$

L' is a lattice in $\mathbb{Q}_p^2$. Indeed if l is an element of L', by condition 2. in Definition 4.3.1 we can find another element $l' \in L'$ such that l and l' are not multiples, so the $\mathbb{Z}_p$-module L' has at least two generators. By Nakayama's lemma we conclude then that the generators are two. Moreover, they are clearly independent over $\mathbb{Z}_p$, and so also over $\mathbb{Q}_p$. Now, let $\mathcal{R}$ be a set of representatives for $\mathbb{P}^1(L'/pL')$; then $n(\mathcal{R}) \subseteq [0, 1)$. Moreover if $x \in \mathbb{Q}_p^2$ we can write

$$\begin{aligned} x &= p^m x' \quad \text{for some } m \in \mathbb{Z} \text{ and } x' \in L', \\ &= p^m(ur + pw), \end{aligned}$$

where $r \in \mathcal{R}, u \in \mathbb{Z}_p^*$ and $w \in L'$. So $n(x) = m + n(r)$ and, if $n(r) = 0$ for each element of $\mathcal{R}$, then we see that n is the norm $n_{[L']}$ associated to the vertex $[L']$ of $\mathcal{T}$. It can be shown that this is still true if one takes a different representative for C. Now we consider the case in which $n(r) > 0$ for some $r \in \mathcal{R}$. If there is another element r' in $\mathcal{R}$, then r and r' are not multiples, because if for example $r' = yr$ for some $y \in \mathbb{Z}_p$, then xy cannot have positive valuation (otherwise $n(r') > 1$), but y cannot be a unit either (because otherwise r and r' would not be dinstinct representatives). So r and r' span L', but this implies that every element of L' has strictly positive norm, a contradiction (because we are assuning that there is an element x of norm zero). We conclude that there is an unique r in $\mathcal{R}$ such that $n(r) > 0$. Let $L = L' + r/p$ and let $t = 1 - n(r)$. One can check that in this case the norm n is the same as the norm n_z associated to the point $z = (1-t)[L] + t[L']$ of the edge between $[L]$ and $[L']$ and that this is true regardless of of the choice of the lattices representing the homothety classes. □

Given a point $z = [x, y]$ in $\mathcal{H}_p$, we can define a norm on $\mathbb{Q}_p^2$ as

$$n_z\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = v_p(ax + by).$$

Clearly, n_z satisfies conditions 2. and 3. in the definition of norm. Moreover, we have

$$v_p(ax + by) = 0 \Leftrightarrow ax + by = 0 \Leftrightarrow a = b = 0,$$

where the last implication follows from the fact that $[x, y]$ is in $\mathcal{H}_p = \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$. Indeed, if for example $a \neq 0$, then

$$x = -(b/a)y,$$

so $[x, y] = [-(b/a), 1] \in \mathbb{P}^1(\mathbb{Q}_p)$, a contradiction. So n_z is a norm. We see that if we take a different representative for the point z, we will obtain a norm which is equivalent to n_z. By Proposition 4.3.1 we see that there is a map

$$\text{red} : \mathcal{H}_p \to \mathcal{T},$$

called *reduction map*.

Proposition 4.3.2. *The reduction map is* $\mathrm{PGL}_2(\mathbb{Q}_p)$*-equivariant and the inverse images of the privileged vertex and edge are*

$$red^{-1}(v_0) = \mathcal{A},$$

and

$$red^{-1}(e_0) = \mathcal{W}_0,$$

where $\mathcal{A}$ *and* $\mathcal{W}_0$ *are the standard affinoid and annulus defined in section 4.1.*

Proof. See [DT08]. □

Let $\mathcal{T}_n$ be the subset of $\mathcal{T}$ made up of all the vertices and edges at distance at most $n-1$ from the standard vertex v_0. It can be shown that the affinoids Ω_n^- constructed in Section 4.1 are given by

$$\Omega_n^- = \mathrm{red}^{-1}(\mathcal{T}_n).$$

So we see that we can imagine the p-adic upper-half plane as a "tubular neighbourhood" containing the Bruhat-Tits tree and the affinoids Ω_n^- as "tubular neighbourhoods" of $\mathcal{T}_n$. With this image in mind, we have another way to see that the ends of the tree correspond to $\mathbb{P}^1(\mathbb{Q}_p)$. Indeed, we can label the vertices at distance n from v_0 with representatives for $\mathbb{P}^1(\mathbb{Q}_p)$ modulo p^n, so we see that each end gives us a p-adic number (or ∞), written as a series. Alternatively, we can also label vertices at distance n from v_0 with representatives of $\mathbb{Z}/p^n\mathbb{Z}$ and see each end as a sequence in the inverse limit we used in the proof of Proposition 4.2.3.

Now that we have the reduction map we can also see that, given an edge e, the sets $U(e)$ defined at the end of Section 4.2 are in correspondence with balls of $\mathbb{P}^1(\mathbb{Q}_p)$. Indeed, if $\Sigma_e = \mathrm{red}^{-1}(U(e))$ and $\bar{\Sigma}_e$ is the closure of Σ_e in $\mathbb{P}^1(\mathbb{C}_p)$, then

$$U_e = \bar{\Sigma}_e \cap \mathbb{P}^1(\mathbb{Q}_p)$$

is a ball in $\mathbb{P}^1(\mathbb{Q}_p)$. Moreover, note that

$$U_e \bigsqcup U_{\bar{e}} = \mathbb{P}^1(\mathbb{Q}_p), \qquad \bigsqcup_{s(e)=v} U_e = \mathbb{P}^1(\mathbb{Q}_p),$$

where v is any vertex of $\mathcal{T}$.

We conclude this chapter with the definition of *standard affinoid* and *standard annulus* attached to an edge of the Bruhat-Tits tree.

Definition 4.3.2. *Let* e *be an edge of* $\mathcal{T}$ *between the vertices* v_1 *and* v_2*. The sets*

$$]e[= \{\, e \,\}$$

and

$$[e] = \{\, e, v_1, v_2 \,\}$$

are called respectively ***open edge*** *and* ***closed edge*** *attached to* e*. The sets*

$$\mathcal{A}_{[e]} := \mathrm{red}^{-1}([e])$$

and

$$\mathcal{W}_{]e[} := \mathrm{red}^{-1}(]e[)$$

are called the ***standard affinoid*** *and the****standard annulus*** *attached to* e *respectively.*

We note that $\mathcal{A}_{[e]}$ is given by two $\mathrm{PGL}_2(\mathbb{Q}_p)$-translates of the standard affinoid $\mathcal{A}$, "glued" along the annulus $\mathcal{W}_{]e[}$.

5 The theta function $\Theta(a, b; z)$

In this chapter we will define the theta function $\Theta(a, b; z)$ and we will prove that it is convergent and meromorphic on $\mathcal{H}_p$. We end the chapter with a discussion of a possible method to compute this function.

5.1 The definition

In this section we recall some notions about Hurwitz quaternions and define the theta function. We conclude the section with a useful lemma about distance between vertices in the Bruhat-Tits tree.

Recall that in Chapter 2 we denoted by B the algebra of Hamilton quaternions and by R the ring of Hurwitz quaternions, in particular

$$B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k \quad \text{and} \quad R = \mathbb{Z}\left[i, j, k, \frac{1+i+j+k}{2}\right].$$

Definition 5.1.1. *We will denote by $R[1/p]_1^\times$ the ring*

$$R[1/p]_1^\times = \{\, \gamma \in R[1/p] \mid \ Nm(\gamma) = 1 \,\}.$$

Lemma 5.1.1. *Let $p \neq 2$ be a prime number. Then -1 is a square in $\mathbb{Q}_p$ if and only if $p \equiv 1$ (modulo 4).*

Proof. First of all we note that if there is an $\alpha \in \mathbb{Q}_p$ such that $\alpha^2 = 1$, then $2v_p(\alpha) = 0$, so $\alpha \in \mathbb{Z}_p$. If such an α exists, then we have a solution of the equation $x^2 + 1 = 0$ in $\mathbb{F}_p$. Viceversa, if there is a $\beta \in \mathbb{F}_p$ such that $\beta^2 + 1 = 0$, then $2\beta \neq 0$ in $\mathbb{F}_p$, so by Hensel's lemma we have a solution of $x^2 + 1 = 0$ in $\mathbb{Z}_p$. So -1 is a square in $\mathbb{Q}_p$ if and only if the equation $x^2 + 1 = 0$ has solution in $\mathbb{F}_p$, which is equivalent to

$$\left(\frac{-1}{p}\right) = 1,$$

and this is equivalent to $p \equiv 1$ (modulo 4). □

Let p be a prime such that $p \equiv 1$ (modulo 4). Then we can define a map $\iota : B \to \mathrm{M}_2(\mathbb{Q}_p)$ by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \alpha \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & -\alpha \\ -\alpha & 0 \end{pmatrix},$$

where α denotes the square root of -1 in $\mathbb{Q}_p$. The matrices above satisfy the same multiplication table as $1, i, j, k$. Moreover, they form a basis for $\mathrm{M}_2(\mathbb{Q}_p)$, so we can conclude that $B \otimes \mathbb{Q}_p \cong \mathrm{M}_2(\mathbb{Q}_p)$. In general, our map will be given by

$$a + bi + cj + dk \mapsto \begin{pmatrix} a + b\alpha & -c - d\alpha \\ c - d\alpha & a - b\alpha \end{pmatrix},$$

and it is easy to check that the norm of quaternions maps to the determinant of matrices, so $R[1/p]_1^\times$ is mapped into a subset of $\mathrm{SL}_2(\mathbb{Q}_p)$. From now on, we will use the notation

$$\Gamma := \iota(R[1/p]_1^\times) \subseteq \mathrm{SL}_2(\mathbb{Q}_p).$$

We can define an action of the group Γ on $\mathcal{H}_p$. Let $\tau = [x, y] \in \mathcal{H}_p$ and $\gamma = \left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right) \in \Gamma$, then we set

$$\gamma\tau = [qx + ry, sx + ty].$$

Equivalently, if we identify $[x, y]$ with x/y, then γ gives us the Möbius transformation

$$\gamma\tau = \frac{q\tau + r}{s\tau + t}.$$

Definition 5.1.2. *Let a and b be points of $\mathcal{H}_p$. The theta function $\Theta(a, b; z)$ is defined as*

$$\Theta(a, b; z) = \prod_{\gamma \in \Gamma} \frac{z - \gamma a}{z - \gamma b},$$

where $z \in \mathcal{H}_p$.

The following lemma will be useful to prove that theta converges and is meromorphic.

Lemma 5.1.2. *Let $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$. Then the distance between the standard vertex v_0 and the vertex $\gamma v_0 = [L]$ of the Bruhat-Tits tree is*

$$d(v_0, \gamma v_0) = 2m,$$

where L is the lattice spanned by the columns of γ and m is the minimum integer such that $p^m L \subset \mathbb{Z}_p^2$.

Proof. By the elementary divisor theorem we can find a basis $\{ e_1, e_2 \}$ for $\mathbb{Z}_p^2$ and integers a, b such that $\{ p^a e_1, p^b e_2 \}$ is a basis for $p^m L$. Moreover, by the minimality of m, $p^m L$ is the unique representative of the class $[L]$ such that $p^m L \subset L$ and $p^m L$ is maximal with this property. But this means that the distance $d(v_0, \gamma v_0)$ is the size of the quotient $\mathbb{Z}_p^2 / p^m L$, so

$$\begin{aligned} d(v_0, \gamma v_0) &= |\mathbb{Z}_p^2 / p^m L| \\ &= a + b \\ &= v_p(p^a p^b) \\ &= v_p(\det(M_{p^m L})), \end{aligned}$$

where $M_{p^m L}$ is the matrix whose columns are $p^a e_1$ and $p^b e_2$. The last equality holds because the standard basis of $\mathbb{Q}_p^2$ is also a basis for $\mathbb{Z}_p^2$ and the matrix associated to this basis is the identity matrix, which has determinat one, and so also the matrix whose columns are e_1, e_2 has determinant one (because a base change does not affect the determinant). Now the thesis follows because

$$\begin{aligned} v_p(\det(M_{p^m L})) &= 2m + v_p(\det(\gamma)) \\ &= 2m. \end{aligned}$$

□

5.2 Convergence and meromorphicity

In order to prove that $\Theta(a, b; z)$ is convergent and meromrphic, we will introduce a filtration

$$\Gamma_0 \subset \Gamma_1 \subset \cdots \subset \Gamma_n \subset \ldots$$

for the group Γ. This is useful because it allows us to index the infinite product defining $\Theta(a, b; z)$. To prove the meromorphicity of $\Theta(a, b; z)$, we will adapt for our purposes the methods in [GvdP80]. Note that a possible filtration for the group Γ is defined in [GvdP80]. However, we will define the sets Γ_n following [FM14], because such a choice for the filtration of Γ will allow us to use Lemma 5.1.2, which will be useful to prove the convergence and meromorphicity of $\Theta(a, b; z)$.

Definition 5.2.1. *Let $n \geq 0$ and recall that we defined ι as the map such that $\iota(R[1/p]_1^\times) = \Gamma$. Then we set*

$$\Gamma_n := \left\{ \iota\left(\frac{x}{p^n}\right) \;\middle|\; x \in R \text{ and } Nm(x) = p^{2n} \right\}.$$

We have $\Gamma_n \subseteq \Gamma_{n+1}$ because we can write $x/p^n = (px)/p^{n+1}$. Moreover, given a $\gamma \in \Gamma$, we can always "clear the denominators" of its coefficients by multiplying by a suitable power of p, hence

$$\Gamma = \bigcup_{n \geq 0} \Gamma_n,$$

and the minimum n such that $\gamma \in \Gamma_n$ is the exponent of the smallest power of p such that $p^n \gamma$ has integer coefficients.

Definition 5.2.2. *Let $n \geq 0$, we set*

$$\Theta_n(a, b; z) = \prod_{\gamma \in \Gamma_n} \frac{z - \gamma a}{z - \gamma b}.$$

If $n \geq 1$, we set

$$\Phi_0(a, b; z) = \prod_{\gamma \in \Gamma_0} \frac{z - \gamma a}{z - \gamma b} \quad \textit{and} \quad \Phi_n(a, b; z) = \prod_{\gamma \in \Gamma_n - \Gamma_{n-1}} \frac{z - \gamma a}{z - \gamma b}.$$

Proposition 5.2.1. *The function $\Theta(a,b;z)$ converges for any a,b,z in the standard affinoid $\mathcal{A}$.*

Proof. We have that

$$\Theta(a,b;z) = \prod_{n\geq 1} \Phi_n(a,b;z).$$

We will show that each factor of the product defining $\Phi_n(a,b;z)$ tends to one as n tends to infinity. Let γ be an element of Γ and let n be the minimum integer such that

$$\gamma = \iota\left(\frac{x}{p^n}\right), \text{ with } Nm(x) = p^{2n}.$$

Then, by Lemma 5.1.2, the distance between the standard vertex v_0 and the vertex gv_0 is $d(v_0, gv_0) = 2n$. Moreover

$$\frac{z-\gamma a}{z-\gamma b} = \frac{z-ga}{z-gb},$$

because γ and g give the same Möbius transformation. Since a,b,z are all in the standard affinoid $\mathcal{A}$, we have

$$ga, gb \in (\Omega^-_{2n-1})^c = \bigcup_{y\in\mathcal{R}_{2n-1}} B^-(y, 2n-1),$$

where $\mathcal{R}_{2n-1}$ is a set of representatives for $\mathbb{P}^1(\mathbb{Q}_p)$ modulo p^{2n-1}. In particular there is a representative $\bar{y} \in \mathcal{R}_{2n-1}$ such that

$$ga, gb \in B^-(\bar{y}, 2n-1),$$

that is, both ga and gb lie in the "hole" corresponding to the vertex gv_0, because both a and b are in $\mathcal{A}$. But then

$$|ga - gb|_p < (1/p)^{2n-1}.$$

Now if we assume $|z-gb|_p \geq 1$ the thesis follows, because

$$\frac{z-ga}{z-gb} = 1 + \frac{gb-ga}{z-gb}$$

and

$$\left|\frac{gb-ga}{z-gb}\right|_p \leq |ga-gb|_p < (1/p)^{2n-1}.$$

So it remains to prove that $|z-gb|_p \geq 1$. This follows from the fact that $z \in \mathcal{A}$ but $gb \notin \mathcal{A}$, so either $|gb-t|_p < 1$ for $t = 0 \ldots p-1$ or $|gb|_p > 1$. In the first case we have

$$\begin{aligned} |z-gb|_p &= \max\{|z-t|_p, |t-gb|_p\} \\ &= |z-t|_p \geq 1, \end{aligned}$$

while in the second case

$$\begin{aligned} |z-gb|_p &= \max\{|z|_p, |gb|_p\} \\ &= |gb|_p > 1. \end{aligned}$$

□

Proposition 5.2.2. *The function $\Theta(a,b;z)$ converges for any a,b,z in $\mathcal{H}_p$.*

Proof. In the general case, a,b and z could lie on the preimage of any closed edge via the reduction map. If e_a and e_b are edges such that $a \in \mathrm{red}^{-1}(e_a)$ and $b \in \mathrm{red}^{-1}(e_b)$, let v and w be vertices such that $v \in [e_a]$ and $w \in [e_b]$. Given a matrix $\gamma \in \Gamma$, throughout this proof we will denote by g the matrix $\iota(x)$, where

$$\gamma = \iota\left(\frac{x}{p^n}\right), \text{ with } Nm(x) = p^{2n},$$

and n is minimum with this property. The action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{T}$ preserves the distance between vertices, so we see that we can always find a suitable n such that the distances $d(v_0, gv)$ and $d(v_0, gw)$ are as big as we want (because $d(v_0, v)$ and $d(v_0, w)$ are fixed by the action of g, while $d(v_0, gv_0) = 2n$ can be as big as we need). This, together with the fact that $d(v,w) = d(gv, gw)$, tells us that for any integer k we can find n such that, if $\gamma \in \Gamma_n$, then gv and gw are far enough from the standard vertex v_0 and we have

$$ga, gb \notin \Omega^-_{2k-1} \quad \text{and} \quad ga, gb \in B^-(y, 2k-1),$$

for some $y \in \mathcal{R}_{2k-1}$. So for almost all $\gamma \in \Gamma$ we have

$$|ga - gb|_p < (1/p)^{2k-1}.$$

Now note that z lies at a fixed distance from v_0, while we said above that $d(v_0, gw)$ can be as big as we want. So we conclude that there is an integer m such that, if $\gamma \in \Gamma_n$ for n big enough, then

$$gb \in B^-(y, 2m-1) \quad \text{and} \quad z \notin B^-(y, 2m-1),$$

for some $y \in \mathcal{R}_{2m-1}$. Let m_0 be the minimum m with this property, then

$$|z - gb|_p \geq (1/p)^{2m_0 - 1}.$$

We conclude that given an integer k we have

$$\left|\frac{gb - ga}{z - gb}\right|_p \leq (1/p)^{2(k-m_0)},$$

for almost all $\gamma \in \Gamma$. Consequently

$$\left|\frac{z - ga}{z - gb}\right|_p \to 1 \quad \text{if } k \to \infty.$$

□

Definition 5.2.3. *A $\mathbb{C}_p$-valued function f on $\mathcal{H}_p$ is said to be **rigid-analytic** if, for each edge e of $\mathcal{T}$, the restriction of f to the affinoid $\mathcal{A}_{[e]}$ is a uniform limit, with respect to the* sup *norm, of rational functions on $\mathbb{P}^1(\mathbb{C}_p)$ having poles outside $\mathcal{A}_{[e]}$.*

Definition 5.2.4. *A $\mathbb{C}_p$-valued function f on $\mathcal{H}_p$ is said to be meromorphic if its restriction to any affinoid $\mathcal{A}_{[e]}$ is the quotient $\frac{g(z)}{h(z)}$ of two analytic functions $g(z), h(z)$ where the denominator is non-trivial.*

Proposition 5.2.3. *The function $\Theta(a, b; z)$ is meromorphic on $\mathcal{H}_p$, with zeroes at the points $\{ \gamma a \mid \gamma \in \Gamma \}$ and poles at the points $\{ \gamma b \mid \gamma \in \Gamma \}$.*

Proof. Fix an integer n. Then there is an integer N such that $\gamma a, \gamma b \notin \Omega_n$ if $\gamma \in \Gamma_i$, for $i \geq N$. Let

$$f_k(z) := \prod_{i=N}^{k} \Phi_i(a, b; z).$$

Then f_k is analytic on Ω_n and

$$f_{k+1} - f_k = (\Phi_{k+1} - 1) f_k.$$

Recall that

$$\Phi_k(a, b; z) = \prod_{\gamma \in \Gamma_k - \Gamma_{k-1}} \frac{z - \gamma a}{z - \gamma b}$$

and

$$\frac{z - \gamma a}{z - \gamma b} = 1 + \frac{gb - ga}{z - gb},$$

where, for each $\gamma \in \Gamma_k - \Gamma_{k-1}$, the matrix g is defined as $\iota(x)$ if

$$\gamma = \iota \left(\frac{x}{p^k} \right), \text{ with } Nm(x) = p^{2k}.$$

For any point $z \in \Omega_n$ we have

$$|z - gb|_p \geq (1/p)^n,$$

because $\gamma b \notin \Omega_n$ if $\gamma \in \Gamma_i$, for $i \geq N$. Then, since $|gb - ga|_p$ tends to zero if $v_p(\det(g))$ tends to infinity, we have

$$\|\Phi_{k+1} - 1\|_{\Omega_n} \to 0.$$

This means that the sequence $\{f_k\}$ converges uniformly on Ω_n towards an analytic function $f^*(z)$. But since

$$\Theta(a, b; z) = \prod_{i=1}^{\infty} \Phi_i(a, b; z)$$

we have

$$\Theta(a, b; z) = f^*(z) \prod_{i=1}^{N-1} \Phi_i(a, b; z).$$

As this converges independently of n, we get a meromorphic function on $\mathcal{H}_p$. Moreover, the function $\Theta(a, b; z)$ can have no poles outside of $\{ \gamma b \mid \gamma \in \Gamma \}$, because $f^*(z)$ has no pole on Ω_n. As

$$\prod_{\gamma \in \Gamma} \frac{z - \gamma a}{z - \gamma b} \cdot \prod_{\gamma \in \Gamma} \frac{z - \gamma b}{z - \gamma a} \equiv 1$$

we conclude that $\Theta(a, b; z)$ has no zeroes outside $\{ \gamma a \mid \gamma \in \Gamma \}$, because $\Theta(b, a; z)$ has no poles outside $\{ \gamma a \mid \gamma \in \Gamma \}$. □

5.3 On the computation of $\Theta(a, b; z)$

The most "naïve" way of computing $\Theta(a, b; z)$ is probably to approximate it with

$$\Theta_n = \prod_{i=0}^{n} \Phi_i(a, b; z)$$

for growing values of n. However, this method is not efficient. Indeed, to compute $\Phi_n(a, b; z)$ we need to compute the set $\Gamma_n - \Gamma_{n-1}$, and this is like computing the set

$$\left\{ x \in R \;\middle|\; Nm(x) = p^{2n} \right\}.$$

From Chapter 3, we know that the cardinality of this set is

$$24(1 + p + \cdots + p^{2n}).$$

As this cardinality grows exponentially in p, computing $\Phi_n(a, b; z)$ by multiplying all its factors is not efficient. In this section we want to show how the recursive relations for Hurwitz quaternions that we found in Chapter 2 could lead to a more efficient way of computing $\Theta(a, b; z)$.

Lemma 5.3.1. *Let $n \geq 1$. Then*

$$\Phi_n(a, b; z) = c \prod_{\gamma \in \Gamma_n - \Gamma_{n-1}} \frac{\gamma^{-1} z - a}{\gamma^{-1} z - b},$$

where c is a constant in $\mathbb{C}_p$.

Proof. If $\gamma = \left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right)$, then

$$\frac{z - \gamma a}{z - \gamma b} = \frac{sb + t}{sa + t} \cdot \frac{zsa + zt - qa - r}{zsb + zt - qb - r},$$

while

$$\frac{\gamma^{-1} z - a}{\gamma^{-1} z - b} = \frac{tz - r + asz - aq}{tz - r + bsz - bq}.$$

So if we take

$$c = \prod_{\gamma \in \Gamma_n - \Gamma_{n-1}} \frac{sb + t}{sa + t}$$

the thesis follows. □

Definition 5.3.1. *If $n \geq 0$ we set*

$$\Gamma_n^{pr} = \left\{ \iota\left(\frac{x}{p^n}\right) \;\middle|\; x \in Q_{2n}^{pr} \right\}$$

and

$$\Gamma_n^{non-pr} = \left\{ \iota\left(\frac{x}{p^n}\right) \;\middle|\; x \in Q_{2n}^{non-pr} \right\},$$

where Q_n^{pr} and Q_n^{non-pr} are respectively the sets of primitive and non-primitive quaternions of norm p^n that we defined in Section 2.3. Moreover, we set

$$\Phi_n^{pr}(a,b;z) = \prod_{\gamma\in\Gamma_n^{pr}} \frac{z-\gamma a}{z-\gamma b},$$

and, if $n \geq 1$,

$$\Phi_0^{non-pr}(a,b;z) = 1, \quad \Phi_n^{non-pr}(a,b;z) = \prod_{\gamma\in\Gamma_n^{non-pr}} \frac{z-\gamma a}{z-\gamma b}.$$

We want to use the relations that we found in Section 2.3 to write Φ_n^{pr} and Φ_n^{non-pr} recursively. This will give us Φ_n, because of course

$$\Phi_n = \Phi_n^{pr} \cdot \Phi_n^{non-pr}.$$

Proposition 5.3.1. *If $n \geq 2$, then*

$$\Phi_n^{non-pr} = \Phi_{n-1}^{non-pr} \cdot \Phi_{n-1}^{pr}.$$

Proof. We saw in Section 2.3 that, if $n \geq 2$, then

$$Q_{2n}^{non-pr} = \left\{ pq \;\middle|\; q \in Q_{2n-2}^{non-pr} \right\} \cup \left\{ pq \;\middle|\; q \in Q_{2n-2}^{pr} \right\}.$$

Let $A = \left\{ \iota(pq) \;\middle|\; q \in Q_{2n-2}^{non-pr} \right\}$ and $B = \left\{ \iota(pq) \;\middle|\; q \in Q_{2n-2}^{pr} \right\}$, then

$$\begin{aligned} \Phi_n^{non-pr}(a,b;z) &= \prod_{\gamma\in A} \frac{z-\gamma a}{z-\gamma b} \cdot \prod_{\gamma\in B} \frac{z-\gamma a}{z-\gamma b} \\ &= \Phi_{n-1}^{non-pr}(a,b;z) \cdot \Phi_{n-1}^{pr}(a,b;z), \end{aligned}$$

because the matrices $\iota(q)$ and $\iota(pq)$ give the same Möbius transformation. □

The above proposition enables us to calculate Φ_n^{non-pr} recursively. The following lemma will be used to prove a similar relation for Φ_n^{pr}.

Lemma 5.3.2. *If $n \geq 2$, then the multiset*

$$\left\{ qr_ir_j \;\middle|\; r_i, r_j \in T, q \in Q_{2n-2}^{pr} \right\}$$

is equal to the multiset

$$p^2 \left\{ p^2 q \mid q \in Q_{2n-4}^{pr} \right\} \cup (p+1) \left\{ pq \;\middle|\; q \in Q_{2n-2}^{pr} \right\} \cup Q_{2n}^{pr},$$

where T is a set of representatives for the equivalence relation $\sim$ defined in Section 2.2.

Proof. The statement is proven using repeatedly Proposition 2.3.2, in particular

$$\left\{ qr_ir_j \;\middle|\; r_i, r_j \in T, q \in Q^{pr}_{2n-2} \right\} = A \cup B,$$

where $A = \left\{ qr_j \;\middle|\; r_j \in T, q \in Q^{pr}_{2n-1} \right\}$ and $B = p\left\{ pqr_j \;\middle|\; r_j \in T, q \in Q^{pr}_{2n-3} \right\}$. But now

$$A = Q^{pr}_{2n} \cup \left\{ pq \;\middle|\; q \in Q^{pr}_{2n-2} \right\},$$

while

$$B = p\left\{ pq \;\middle|\; q \in Q^{pr}_{2n-2} \right\} \cup p^2 \left\{ p^2q \;\middle|\; q \in Q^{pr}_{2n-4} \right\}.$$

□

Remark 5.3.1. The same result would follow if, instead of multiplying on the right by elements of T, we multiplied on the left by elements of $\dot{T}$.

We are now ready to write Φ^{pr}_n recursively.

Proposition 5.3.2. *If $n \geq 2$, we have*

$$\Phi^{pr}_n(a, b; z) = c \cdot \frac{\prod_{i,j} \Phi^{pr}_{n-1}(a, b; g_i^{-1} g_j^{-1} z)}{(\Phi^{pr}_{n-1}(a, b; z))^{p+1} (\Phi^{pr}_{n-2}(a, b; z))^{p^2}},$$

where c is a constant in $\mathbb{C}_p$ and the matrices g_i (or g_j) are defined as

$$g_i = \iota(r_i), \quad r_i \in \dot{T}.$$

Proof. Let us denote by A, B and C the multisets

$$A = \iota\left(\{ p^2q \mid q \in Q^{pr}_{2n-4} \}\right), \quad B = \iota\left((p+1)\left\{ pq \;\middle|\; q \in Q^{pr}_{2n-2} \right\}\right)$$

and $C = \iota\left(Q^{pr}_{2n}\right)$. Then, by Lemma 5.3.1 and Remark 5.3.1 we have

$$\prod_{i,j} \Phi^{pr}_{n-1}(g_i^{-1} g_j^{-1} z) \;=\; c \prod_{\gamma \in A} \frac{\gamma^{-1}z - a}{\gamma^{-1}z - b} \cdot \prod_{\gamma \in B} \frac{\gamma^{-1}z - a}{\gamma^{-1}z - b} \cdot \prod_{\gamma \in C} \frac{\gamma^{-1}z - a}{\gamma^{-1}z - b},$$

for some constant c in $\mathbb{C}_p$. But this is like saying

$$\prod_{i,j} \Phi^{pr}_{n-1}(a, b; g_i^{-1} g_j^{-1} z) = c(\Phi^{pr}_{n-2}(a, b; z))^{p^2} (\Phi^{pr}_{n-1}(a, b; z))^{p+1} \Phi^{pr}_n(a, b; z),$$

so the thesis follows. □

From the propositions above we see that, if $n \geq 2$, up to a multiplicative constant $\Phi_n(a, b; z)$ is equal to

$$\frac{\prod_{i,j} \Phi_{n-1}^{pr}(a, b; g_i^{-1} g_j^{-1} z)}{(\Phi_{n-1}^{pr}(a, b; z))^p (\Phi_{n-2}^{pr}(a, b; z))^{p^2}} \cdot \Phi_{n-1}^{non-pr}(a, b; z),$$

where g_i, g_j are the images via ι of representatives for the relation $\dot{\sim}$. So we see that in order to compute Θ_n up to a multiplicative constant we only need to compute $\Phi_0^{pr}(a, b; z)$, $\Phi_1^{pr}(a, b; z)$ and the set of representatives $\dot{T}$ (which has cardinality $p + 1$). To compute $\Phi_0^{pr}(a, b; z)$ and $\Phi_1^{pr}(a, b; z)$, we need the sets Γ_0 and Γ_1, which have cardinality 24 and $24(1 + p + p^2)$, respectively. Finding the sets Γ_0 and Γ_1 requires finding the Hurwitz quaternions of norm 1 and p^2. One way to do this is looking for all the ways to write 1 and p^2 as sum of four squares of integers or half integers; otherwise, we can also use the function `_find_elements_in_order` written by Franc and Masdeu in the `Sage` package `BTQuotients` (see [S+15]). If we have Γ_0 and Γ_1, we can compute $\Phi_0^{pr}(a, b; z)$ and $\Phi_1^{pr}(a, b; z)$ as functions of z for fixed a and b. Then we can compose by the Möbius transformations given by the matrices $g_i^{-1} g_j^{-1}$ and use the formula above to calculate $\Phi_n(a, b; z)$ (as a function of z) up to a multiplicative constant. Applying the formula involves just multiplying and dividing rational fractions, or raising them to the power p or p^2. Thus we see that this method of computing $\Theta_n(a, b; z)$ is much more efficient than the one described at the beginning of this section. Indeed, with the first method the number of operations at every step grew exponentially in n, while with this second method the number of operations grows polynomially in n.

References

[CP12] Coan, B., Perng, C. T.: *Factorization of Hurwitz quaternions.* Int. Math. Forum Vol. 7, No. 41-44 (2012), pp. 2143-2156.

[CS05] Conway, J. H., Smith D. A.: *On quaternions and octonions: their geometry, arithmetic, and symmetry.* A K Peters (2003).

[Dar04] Darmon, H.: *Rational points on modular elliptic curves.* CBMS Regional Conference Series in Mathematics **101**(2004).

[DT08] Dasgupta, S., Teitelbaum, J.T.: *The p-adic upper-half plane.* Amer. Math. Soc. Univ. Lecture Ser **45** (2008), pp. 65-121.

[DS05] Diamond, F., Shurman, J. M.: *A first course in modular forms.* Springer Graduate Texts in Mathematics (2005).

[FM14] Franc, C., Masdeu, M.: *Computing fundamental domains for the Bruhat-Tits tree for $GL_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura Curves.* LMS Journal of Computation and Mathematics **17** (2014), pp. 1-23.

[GvdP80] Gerritzen, L., van der Put, M.: *Schottky groups and Mumford curves.* Springer Lecture Notes in Mathematics **817** (1980).

[vdP92] van der Put, M.: *Discrete groups, Mumford curves and Theta functions.* Annales de la faculté des sciences de Toulouse, Vol. 1 No. 3, (1992), pp. 399 438.

[Ser80] Serre, J. P.: *Trees.* Springer Monographs in Mathematics (1980).

[Ser12] Serre, J. P.: *A course in arithmetic.* Springer Graduate Texts in Mathematics **7** (1973).

[Shi71] Shimura, G.: *Introduction to the arithmetic theory of automorphic functions.* Iwanami Shoten and Princeton University Press (1971).

[S+15] Stein, W. et al.: *Sage Mathematics Software.* The Sage Development Team (2015), `http://www.sagemath.org`.