Arithmetic properties of the p-adic logarithm

Cédric Dion[1]
Université Laval

In number theory, many important problems require a good understanding of the arithmetic properties of prime numbers. Let p be a fixed prime. It is then possible to define a metric on the rational numbers by looking at the divisibility of the numerator and denominator of a rational number by p. This metric is called the p-adic metric. Continuous functions behave very differently with this metric compared to the euclidean metric. For example, the p-adic logarithm factors into an infinite product of polynomials, which is not the case for the standard logarithm.

In this paper, many properties of p-adic functions will be studied. In particular, the factorization of the p-adic logarithm makes it possible to define new p-adic functions that can be used to solve problems in Iwasawa theory. Our main result gives a new description of Pollack's plus and minus p-adic logarithms in terms of distributions. We then generalize our results to p-adic logarithms in two variables.

Contents

1 Introduction **2**
1.1 p-adic numbers 2
1.2 p-adic continuous functions 5
1.3 Locally analytic functions on $\mathbf{Z}_p$ 7
1.4 p-adic distributions and the Amice transform 7
1.5 Cyclotomic polynomials and roots of unity 9
1.6 The characteristic function as a sum of roots 11

2 Pollack's plus and minus logarithm $\log_p^{\pm}$ **12**
2.1 Definitions 12
2.2 Interpolation formulae 14

3 $\log_p^{\pm}$ and the Amice transform **14**
3.1 Main result 14
3.2 Generalization for two-variable logarithms 16

[1]Supported by the ISM undergraduate summer scholarships.

1 Introduction

The goal of this section is to introduce background knowledge required for the rest of the document. We follow closely the structure of Koblitz [1].

1.1 p-adic numbers

For completeness, we state the familiar definition of a norm on a field.

Definition 1.1.1. A *norm* on a field F is a map $\|\cdot\|$ from F to the non-negative real numbers such that for all $x, y \in F$

1. $\|x\| = 0$ if and only if $x = 0$,
2. $\|xy\| = \|x\| \, \|y\|$,
3. $\|x + y\| \leq \|x\| + \|y\|$.

Proposition 1.1.1. $\|\cdot\|$ is a continuous function.

Proof. Let $\varepsilon > 0$. By the reverse triangle inequality, $| \, \|x\| - \|y\| \, | \leq \|x - y\|$. Hence, it suffices to take $\delta = \varepsilon$. So we have $\|x - y\| < \delta \implies | \, \|x\| - \|y\| \, | < \varepsilon$. □

To analyse convergence of sequences in a set, we need the notion of distance between elements of the set.

Definition 1.1.2. If X is a nonempty set, a *distance*, or *metric*, on X is a function d from pairs of elements (x, y) of X to the nonnegative real numbers such that

1. $d(x, y) = 0$ if and only if $x = y$,
2. $d(x, y) = d(y, x)$,
3. $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.

It is easy to check that a norm $\|\cdot\|$ induces a metric by letting $d(x, y) = \|x - y\|$. In real analysis, the metric is induced by the absolute value on $\mathbf{Q}$. It is possible to define another norm on $\mathbf{Q}$ to get a different metric.

Definition 1.1.3 (Koblitz)**.** Let p be a fixed prime number. For any non-zero integer a, let the *p-adic valuation* of a, denoted $v_p(a)$, be the highest power of p which divides a, i.e., the greatest m such that $a \equiv 0 \mod p^m$. By convention, let $v_p(0) = \infty$. Further extend the definition of v_p on rational numbers by letting $v_p(a/b) = v_p(a) - v_p(b)$.

Proposition 1.1.2. v_p behave a little like the logarithm would: $v_p(ab) = v_p(a) + v_p(b)$.

Proof. Write $a = p^v r$ where $p \nmid r$ and $b = p^u s$ where $p \nmid s$. Then, $v_p(ab) = v_p(p^{v+u}rs) = v + u = v_p(a) + v_p(b)$. □

Note that v_p is well defined for $x = a/b \in \mathbf{Q}$. If we take a different representative for x, let's say $x = ac/bc$, we get $v_p(ac/bc) = v_p(a) + v_p(c) - v_p(b) - v_p(c) = v_p(a/b)$.

Definition 1.1.4. Define a map $|\ |_p$ on $\mathbf{Q}$ as follows:

$$|x|_p = \begin{cases} \frac{1}{p^{v_p(x)}} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

Proposition 1.1.3. $|\ |_p$ is a norm on $\mathbf{Q}$.

Proof. Since $\frac{1}{p^{v_p(x)}} \neq 0$ for all $x \neq 0$, we have $|x|_p = 0$ if and only if $x = 0$. For the second property of norms, let $x, y \in \mathbf{Q}^\times$. By using the previous proposition we obtain $|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$. For the triangular inequality, the result is trivial if $x = 0$, $y = 0$ or $x+y = 0$, so we assume that x, y and $x+y$ are all non-zero. Let $x = a/b$ and $y = c/d$ be written in lowest terms. Then $v_p(x + y) = v_p((ad + bc)/bd) = v_p(ad + bc) - v_p(bd)$. Because the highest power of p dividing the sum of two number is at least the minimum of the highest power dividing the first and the highest power dividing the second, we have

$$\begin{aligned} v_p(x + y) &\geq \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d) \\ &= \min(v_p(a) + v_p(d), v_p(b) + v_p(c)) - v_p(b) - v_p(d) \\ &= \min(v_p(a) - v_p(b), v_p(c) - v_p(d)) \\ &= \min(v_p(x), v_p(y)) \end{aligned}$$

This implies $v_p(x + y) \geq v_p(x) + v_p(y)$ which in turn implies $|x + y|_p \leq |x|_p + |y|_p$. □

We have in fact proven a much stronger inequality, $|x+y|_p \leq \max(|x|_p, |y|_p)$ with equality if $|x|_p \neq |y|_p$. Norms with this property are called *non-archimedean norms* in contrast with *archimedean norms* like the absolute value. Non-archimedean norms induce non-archemidean metrics, that is, metrics with the property that $d(x, y) \leq \max(d(x, z), d(z, y))$. To construct the real numbers from $\mathbf{Q}$, we consider the completion of $\mathbf{Q}$ with respect to the metric $d(x, y) = |x - y|$. We now fix a prime number p. We can complete $\mathbf{Q}$ with the metric induced by $|\ |_p$ to get a field with different properties than $\mathbf{R}$. Let S be the set of Cauchy sequences with respect to $|\ |_p$. That is, for $\{a_i\} \in S$, given an $\varepsilon > 0$, there exist an N such that $|a_i - a_j|_p < \varepsilon$ if both $j, i > N$. We say that two Cauchy sequences $\{a_i\}$ and $\{b_i\}$ are equivalent if $|a_i - b_i|_p \to 0$ as $i \to \infty$. We define the set of p-adic numbers $\mathbf{Q}_p$ to be the set of equivalence classes of Cauchy sequences. We identify $\mathbf{Q}$ with the subset of constant

Cauchy sequences in $\mathbf{Q}_p$.

We say that a set X equipped with a metric is *complete* if every Cauchy sequence in X converge in X.

Definition 1.1.5. We define the norm $|\ |_p$ of an equivalence class $a \in \mathbf{Q}_p$ to be $\lim_{i\to\infty} |a_i|_p$ where $\{a_i\}$ is any representative of a.

Proposition 1.1.4. The limit $|a|_p$ exists and does not depend on the choice of representative.

Proof. If $a = 0$, the constant Cauchy sequence whose all terms are zero, then by definition of a norm $|a|_p = 0$. Suppose $a \neq 0$. Because a is Cauchy and $|\ |_p$ on $\mathbf{Q}$ is a continuous function, $|a_i|_p$ forms a Cauchy sequence in $\mathbf{R}$. This limit exists by the completeness of $\mathbf{R}$. If $\{a_i\} \sim \{b_i\}$, then

$$|a_i|_p = |a_i - b_i + b_i|_p \leq |a_i - b_i|_p + |b_i|_p$$

and the same way,

$$|b_i|_p \leq |a_i - b_i|_p + |a_i|_p,$$

hence, $\lim_{i\to\infty} |a_i|_p = \lim_{i\to\infty} |b_i|_p$. □

Definition 1.1.6. Let a and b be two equivalence classes of Cauchy sequences. We choose any representatives $\{a_i\} \in a$ and $\{b_i\} \in b$ and define

- $a + b = \{a_i + b_i\}$.
- $ab = \{a_i b_i\}$.

Proposition 1.1.5. Addition and multiplication on equivalence classes are well defined.

Proof. Let $\{a_i\} \sim \{a_i'\}$ and $\{b_i\} \sim \{b_i'\}$ be two representatives of a and b respectively. For the multiplication, we have

$$\begin{aligned} |a_i b_i - a_i' b_i'|_p &= |a_i'(b_i' - b_i) + b_i(a_i' - a_i)|_p \\ &\leq \max\left(|a_i'(b_i' - b_i)|_p, |b_i(a_i' - a_i)|_p\right). \end{aligned}$$

As $i \to \infty$, the first expression approaches $|a|_p \lim |b_i' - b_i|_p = 0$, and the second expression approaches $|b|_p \lim |a_i' - a_i|_p = 0$. Hence $\{a_i' b_i'\} \sim \{a_i b_i\}$. For addition, we have

$$|(a_i' + b_i') - (a_i + b_i)|_p \leq \max\left(|a_i' - a_i|_p, |b_i' - b_i|_p\right).$$

As $i \to \infty$, both expression approaches 0. Hence $\{a_i' + b_i'\} \sim \{a_i + b_i\}$. □

We also define additive inverse and multiplicative inverse in the obvious way. Though a bit tedious, it can be shown that $\mathbf{Q}_p$ is a field with these operations and that $\mathbf{Q}_p$ is a complete metric space. Interested readers may refer to Koblitz for more details on this subject.

Like a real number can be viewed as a decimal expansion, an element of $\mathbf{Q}_p$ can be written as a p-adic expansion in this way:

Theorem 1.1.1. Let $a \in \mathbf{Q}_p$, then a can be expressed in the form $a = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots$ where $a_i \in \{0, 1, \ldots, p-1\}$.

In other words, a can be written as an infinite expansion in base p with only finitely many negative power of p. The a_i are called the digits of a. We accept this result without demonstration. It is more useful to think of $\mathbf{Q}_p$ this way because it gives us a more concrete sense of elements in $\mathbf{Q}_p$. With this notation, the valuation of $a \in \mathbf{Q}_p$ is given by the power of p corresponding to the first nonzero digit of a. For example, the valuation of $4 \cdot 5^3 + 1 \cdot 5^4 + 2 \cdot 5^7 + \cdots$ in $\mathbf{Q}_5$ is 3. We write $a \equiv b \mod p^n$ if $|a - b|_p \leq p^{-n}$. If a and b are in $\mathbf{Z}$, then this definition agrees with the usual definition of modulo.

Definition 1.1.7. We denote $\mathbf{Z}_p = \{a \in \mathbf{Q}_p : |a|_p \leq 1\}$ and we call $\mathbf{Z}_p$ the set of *p-adic integers*.

$\mathbf{Z}_p$ consists of all the p-adic numbers whose p-adic expansion only contains positive power of p. The p-adic integers form a subring of $\mathbf{Q}_p$.

Proposition 1.1.6. $\mathbf{Z}_p$ is sequentially compact, hence compact.

Proof. See [2][lemma 4]. □

We shall sometime need to consider a bigger field than $\mathbf{Q}_p$, the algebraic closure of $\mathbf{Q}_p$, the field $\overline{\mathbf{Q}_p}$. The only thing for us to know about $\overline{\mathbf{Q}_p}$ is that it contains all roots of polynomials with coefficients in $\mathbf{Q}_p$. We extend the definition of v_p on $\overline{\mathbf{Q}_p}$ by letting $v_p(z) = \min_{\mathbf{Q}_p,z}(0)^{1/d}$ where $\min_{\mathbf{Q}_p,z}$ is the minimal polynomial of z over $\mathbf{Q}_p$ and d is the degree of that polynomial. $\overline{\mathbf{Q}_p}$ is not complete. We denote $\mathbf{C}_p$ the completion of $\overline{\mathbf{Q}_p}$. It is a complete, algebraically closed field.

1.2 p-adic continuous functions

In analysis, one often uses the concept of a *ball* centred at a of radius n. In $\mathbf{Q}_p$, a ball centred at a of radius n is of the form $a + p^n\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x - a|_p \leq p^{-n}\}$. Interestingly, this set is both open and closed at the same time. Let $b \in a + p^n\mathbf{Z}_p$ where the nth digit of b is b_n. Then, b is included in the smaller ball $a + b_n + p^{n+1}\mathbf{Z}_p$ and we have $a + b_n + p^{n+1}\mathbf{Z}_p \subset a + p^n\mathbf{Z}_p$.

This shows that $a + p^n\mathbf{Z}_p$ is an open set. The complement of $a + p^n\mathbf{Z}_p$ is the union over all $a' \in \mathbf{Q}_p$ such that $a' \notin a + p^n\mathbf{Z}_p$ of the open sets $a' + p^n\mathbf{Z}_p$. Thus, $a + p^n\mathbf{Z}_p$ is also a closed set. Those balls form a basis of open sets, meaning that every open subset of $\mathbf{Q}_p$ is an union of open subsets of this type.

The rest of this section and the next one are important results from [3].

Definition 1.2.1. Let $\mathcal{C}^0(\mathbf{Z}_p, \mathbf{Q}_p)$ be the space of continuous functions on $\mathbf{Z}_p$ with values in $\mathbf{Q}_p$. The valuation of this space is $v_{\mathcal{C}^0}(f) = \inf_{x\in\mathbf{Z}_p}(v_p(f(x)))$.

$\mathcal{C}^0$ endowed with this valuation has the structure of a normed complete metric space. A function f on $\mathbf{Z}_p$ is continuous if $f(x) - f(y)$ is divisible by a high power of p ($f(x)$ and $f(y)$ are p-adically close), then $x - y$ is also divisible by a high power of p.

For $x \in \mathbf{Z}_p$, we define the binomial function

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

We now state a result due to Mahler that characterize continuous functions on $\mathbf{Z}_p$.

Theorem 1.2.1 (Mahler)**.** $f \in \mathcal{C}^0(\mathbf{Z}_p, \mathbf{Q}_p)$ if and only if

1. for all $x \in \mathbf{Z}_p$, $f(x) = \sum_{n=0}^{\infty} a_n(f)\binom{x}{n}$,
2. $\lim_{n\to\infty} v_p(a_n(f)) = \infty$,

where $a_n(f)$ are the Mahler coefficients given by $a_n(f) = \sum_{i=0}^{n}(-1)^i\binom{n}{i}f(n-i)$.

Proof. The proof of the theorem can be found in [3] page 8. □

Definition 1.2.2. For $z \in \overline{\mathbf{Q}_p}$ such that $v_p(z-1) > 0$ we define $z^x = \sum_{n=0}^{\infty}\binom{x}{n}(z-1)^n$.

By Mahler's theorem, $z^x \in \mathcal{C}^0(\mathbf{Z}_p, \mathbf{Q}_p)$ and by properties of binomial coefficients, $z^{x+y} = z^x z^y$.

Definition 1.2.3. Let X and Y be two metric spaces. A map $f : X \to Y$ is called *locally constant* if every point $x \in X$ is included in a ball U such that $f(U)$ is a single element of Y.

It is immediate that locally constant functions are continuous. We shall see that these special type of functions play the same role as step functions in p-adic integration.

Definition 1.2.4. For $n \geq 0$, let the characteristic function of $a + p^n\mathbf{Z}_p$ be

$$\chi_{a+p^n\mathbf{Z}_p} : \mathbf{Z}_p \to \{0,1\}$$
$$x \mapsto \begin{cases} 0 & \text{if } x \notin a + p^n\mathbf{Z}_p \\ 1 & \text{if } x \in a + p^n\mathbf{Z}_p. \end{cases}$$

Proposition 1.2.1. Let $f : \mathbf{Z}_p \to \mathbf{Q}_p$ be a locally constant function. Then, f is a finite $\mathbf{Q}_p$-linear combination of characteristic functions.

Proof. Let $x \in \mathbf{Z}_p$. Then, because f is locally constant, there exist a neighbourhood $a+p^n\mathbf{Z}_p$ of x such that for all $y \in a + p^n\mathbf{Z}_p$, $f(y) = 1 \cdot c = \chi_{a+p^n\mathbf{Z}_p}(y) \cdot c$ where $c \in \mathbf{Q}_p$. Now, let's consider the open covering $\{V_i\} = a_i + p^{n_i}\mathbf{Z}_p$ where, for all $x_i \in \mathbf{Z}_p$, V_i is a neighbourhood of x_i where f is locally constant. Since $\mathbf{Z}_p$ is compact, there is only a finite number of such neighbourhood, let's say $\{V_i\}_{j=1}^N$. Hence, $f(x) = c_1\chi_{V_1}(x) + c_2\chi_{V_2}(x) + \cdots + c_N\chi_{V_N}(x)$ with $c_1, c_2, \ldots, c_N \in \mathbf{Q}_p$. □

1.3 Locally analytic functions on $\mathbf{Z}_p$

Just like in the real case, the p-adic derivative is defined to be the limit of the quotient $\frac{f(x+h)-f(x)}{h}$ as $|h|_p \to 0$. For $x_0 \in \mathbf{C}_p$ and $r \in \mathbf{R}$, we define

$$D(x_0, r) = \{x \in \mathbf{C}_p : v_p(x - x_0) \geq r\}.$$

Definition 1.3.1. A function $f : D(x_0, r) \to \mathbf{C}_p$ is *analytic* if it can be expressed as a Taylor expansion at x_0. In other words,

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n$$

for $x \in D(x_0, r)$.

We denote $LA(\mathbf{Z}_p, \mathbf{Q}_p)$ the set of locally analytic functions on $\mathbf{Z}_p$.

Remark. Analytic functions are infinitely differentiable, and so, continuous. This implies the inclusion $LA \subset \mathcal{C}^0$.

1.4 p-adic distributions and the Amice transform

Definition 1.4.1. A *distribution* μ on $\mathbf{Z}_p$ with values in $\mathbf{Q}_p$ is a continuous $\mathbf{Q}_p$-linear map $f \mapsto \int_{\mathbf{Z}_p} f\mu$ from $LA(\mathbf{Z}_p, \mathbf{Q}_p)$ to $\mathbf{Q}_p$. We denote the set of distributions from LA to $\mathbf{Q}_p$ by $\mathcal{D}(\mathbf{Z}_p, \mathbf{Q}_p)$.

In other words, a distribution is an element of the dual space of $LA(\mathbf{Z}_p, \mathbf{Q}_p)$.

Definition 1.4.2. Let $\mathbf{Q}_p[\![T]\!]$ be the set of formal power series with coefficients in $\mathbf{Q}_p$.

Definition 1.4.3. The *Amice transform* of a distribution μ is the function:

$$A_\mu(T) = \sum_{n=0}^{\infty} T^n \int_{\mathbf{Z}_p} \binom{x}{n} \mu = \int_{\mathbf{Z}_p} (1+T)^x \mu.$$

Since $\binom{x}{n}$ is just a polynomial, $\binom{x}{n}$ is clearly analytic and so $\int_{\mathbf{Z}_p} \binom{x}{n}\mu$ is well defined. The second equality comes from the fact that if $v_p(T) > 0$, then $\sum_{n=0}^{\infty} T^n \binom{x}{n}$ converges to $(1+T)^x$. We can see that the Amice transform maps a distribution μ to an element of $\mathbf{Q}_p[\![T]\!]$. The converse is also true for convergent power series on the unit disc.

Theorem 1.4.1. The map $\mu \mapsto A_\mu$ is an isomorphism of complete metric spaces from $\mathcal{D}(\mathbf{Z}_p, \mathbf{Q}_p)$ to convergent series on the unit circle in $\mathbf{Q}_p[\![T]\!]$ under the appropriate valuation for each spaces.

We will give a sketch of the proof. Giving the complete proof would require definning valuations on both spaces and showing that A_μ is continuous wich is a bit tedious. The details can be found in [3]. However, we will show how one can go from $\mathcal{D}$ to $\mathbf{Q}_p[\![T]\!]$ and from $\mathbf{Q}_p[\![T]\!]$ to $\mathcal{D}$. Let $\mu \in \mathcal{D}(\mathbf{Z}_p, \mathbf{Q}_p)$. Then, the associated power series is given by $F(T) = \sum_{n=0}^{\infty} b_n(\mu) T^n$ where $b_n(\mu) = \int_{\mathbf{Z}_p} \binom{x}{n}\mu$. On the converse, let $F(T) = \sum_{n=0}^{\infty} b_n T^n$ such that $F(T)$ converges on the unit circle. Then, for $f \in LA$ we let $\mu : f \mapsto \sum_{n=0}^{\infty} b_n a_n(f)$. It can be shown that $\sum_{n=0}^{\infty} b_n a_n(f)$ is indeed convergent and that $\mu \in \mathcal{D}$.

Proposition 1.4.1. The space of locally constant function is dense in $LA(\mathbf{Z}_p, \mathbf{Q}_p)$.

Proof. Let $f \in LA(\mathbf{Z}_p, \mathbf{Q}_p)$ and write $f_n = \sum_{j=0}^{p^n-1} f(j)\chi_{j+p^n\mathbf{Z}_p}$. It is clear that $f_n \to f$ in $\mathcal{C}^0$ and particularly in LA. □

Hence, for $f \in LA(\mathbf{Z}_p, \mathbf{Q}_p)$, $\int_{\mathbf{Z}_p} f\mu$ is given by the following "Riemann sums"

$$\int_{\mathbf{Z}_p} f\mu = \lim_{n\to\infty} \sum_{i=0}^{p^n-1} f(i) \int_{\mathbf{Z}_p} \chi_{i+p^n\mathbf{Z}_p}\mu.$$

From this result, it follows that a distribution μ is uniquely determined by its values at characteristic functions.

1.5 Cyclotomic polynomials and roots of unity

For this section, we use $\mathbf{Z}/n$ to denote the set of integers modulo n.

Most of this section except theorem 1.5.2 comes from [4].

Definition 1.5.1. An nth root of unity is a solution to the polynomial equation $x^n - 1 = 0$. We denote μ_n the set of nth roots of unity.

By the fundamental theorem of algebra, the cardinality of μ_n is exactly n in characteristic 0.

Proposition 1.5.1. The set μ_n together with usual multiplication forms an abelian group.

Proof. Let $z_1, z_2 \in \mu_n$. $(z_1 z_2)^n - 1 = z_1^n z_2^n - 1 = 0$ implies that $z_1 z_2 \in \mu_n$ and that $(\mu_n, \cdot)$ is closed. $1 \in \mu_n$ is the identity. If z is a root of unity with order k, then z^{n-k} is the multiplicative inverse of z. □

Definition 1.5.2. For a positive integer n, if $z^n = 1$ and $z^t \neq 1$ for all positive integers $t < n$, we say that z is a *primitive* nth root of unity.

Proposition 1.5.2. In addition, μ_n is also a cyclic group.

Proof. Let z be a primitive nth root of unity. This means that z as order n in the group μ_n. Hence, $\langle z \rangle$ is a group of order n inside μ_n. Thus, $\langle z \rangle = \mu_n$ and μ_n is cyclic. □

Since μ_n is cyclic of order n, it is isomorphic to $\mathbf{Z}/n$, the integers modulo n.

We now define polynomials whose roots are the primitive nth roots of unity.

Definition 1.5.3. For any positive integer n the *nth cyclotomic polynomial*, $\phi_n(x)$, is given by

$$\phi_n(x) = (x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_s),$$

where $\zeta_1, \zeta_2, \ldots, \zeta_s$ are the primitive nth roots of unity.

Theorem 1.5.1. Let n be a positive integer, then

$$x^n - 1 = \prod_{d|n} \phi_d(x).$$

Proof. This proof comes from [4][Theorem 3.9]. Suppose that ζ is a root of $\phi_d(x)$, where $d|n$. It follows that ζ is a dth root of unity. Let q be the integer such that $n = dq$, then

$$\zeta^n = (\zeta^d)^q = 1^q = 1.$$

It follows that ζ is a root of $x^n - 1$. Now suppose that ζ is a root of $x^n - 1$. It follows that ζ is an nth root unity. Say that the order of ζ is d, and note that ζ will be a primitive dth root of unity. Therefore, ζ is a root of $\phi_d(x)$. Since μ_d forms a subgroup of μ_n because $d \leq n$, it follows that $d|n$ by Lagrange theorem. So ζ is a root of $\Phi_d(x)$ for some d that divides n. We have shown that $x^n - 1$ and $\prod_{d|n} \phi_d(x)$ share all their roots. Since $\prod_{d|n} \phi_d(x)$ is a product of monic polynomials, it will also be monic. Hence, $x^n - 1$ and $\prod_{d|n} \phi_d(x)$ are both monic, which means that they must be equal. □

Corollary 1.5.1. The p^nth cyclotomic polynomial is given by $\phi_{p^n}(x) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1$.

Proof. We use the previous theorem twice to get

$$\begin{aligned} x^{p^n} - 1 &= \prod_{d|p^n} \phi_d(x) \\ &= \phi_{p^n}(x) \prod_{d|p^{n-1}} \phi_d(x) \\ &= \phi_{p^n}(x)(x^{p^{n-1}} - 1). \end{aligned}$$

Dividing both sides by $(x^{p^{n-1}} - 1)$ gives $\phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1$. □

Remark. This also shows that the degree of $\phi_{p^n}(x)$ is $(p-1)p^{n-1}$.

The next theorem will be of importance later on.

Theorem 1.5.2. Let us write $\Phi_n(x)$ for $\phi_{p^n}(x)$ to abbreviate the notation. Let $n \geq 1$, $m \geq 0$ be integers and let $\lambda_n^+(m) = \sum_{l=0}^{n-1} p^{2l+1} \lfloor m/p^l \rfloor \mod p^{2(l+1)}$, then

$$\prod_{j=1}^{n} \Phi_{2j}(x) = \sum_{m=0}^{p^n-1} x^{\lambda_n^+(m)}$$

with $\lambda_n^+(m)$ all distinct.

Proof. To appear in [5]. □

To give an idea, here is an example for the case $p = 3$ and $n = 5$.

$$\begin{aligned} \prod_{j=1}^{2} \Phi_{2j}(x) &= \sum_{m=0}^{3^2-1} x^{\sum_{l=0}^{1} 3^{2l+1} \lfloor m/3^l \rfloor \mod 3^{2(l+1)}} \\ &= \sum_{m=0}^{3^2-1} x^{3\lfloor m \rfloor \mod 3^2 + 3^3 \lfloor m/3 \rfloor \mod 3^4} \\ &= 1 + x^3 + x^6 + x^{27} + x^{30} + x^{33} + x^{54} + x^{57} + x^{60} \end{aligned}$$

Like mentioned above, the power of x are all integers whose expansion in base 3 contains only odd power of 3.

Here is the analogous result for the product of odd prime power cyclotomic polynomials. Again, we write $\Phi_n(x)$ for $\phi_{p^n}(x)$.

Theorem 1.5.3. Let n be an integer greater than 0 and let $\lambda_n^-(m) = \sum_{l=0}^{n-1} p^{2l}\lfloor m/p^l \rfloor \mod p^{2l+1}$, then

$$\prod_{j=1}^{n} \Phi_{2j-1}(x) = \sum_{m=0}^{p^n-1} x^{\lambda_n^-(m)}.$$

Proof. Similar to the case of even prime power cyclotomic polynomials. □

1.6 The characteristic function as a sum of roots

Definition 1.6.1. Let $\zeta \in \mu_{p^n}$ be a p^nth root of unity. We define the function $\zeta^x : \mathbf{Z}_p \to \overline{\mathbf{Q}_p}$ given by $x \mapsto \zeta^x$. There are p^n such function for a given $n \geq 1$.

The function ζ^x is locally constant mod p^n i.e. $\zeta^{(x+p^n)} = \zeta^x$ as shown by the next proposition.

Proposition 1.6.1. If $x \in p^n\mathbf{Z}_p$, then $\zeta^x = 1$.

Proof. Suppose $x \in p^n\mathbf{Z}_p$. Then, x can be written as $x = a_n p^n + a_{n+1}p^{n+1} + \cdots$. Now,

$$\begin{aligned}\zeta^x &= \zeta^{a_n p^n + a_{n+1}p^{n+1} + \cdots} \\ &= (\zeta^{p^n})^{a_n}(\zeta^{p^{n+1}})^{a_{n+1}} \cdots \\ &= 1\end{aligned}$$

because the multiplicative order of ζ is less or equal to p^n. □

Proposition 1.6.2. $\zeta^x : (\mathbf{Z}_p, +) \to (\overline{\mathbf{Q}_p}^\times, \cdot)$ is a group homomorphism.

Proof. Let $x, y \in \mathbf{Z}_p$, we have $\zeta^{(x+y)} = \zeta^x\zeta^y$. □

Corollary 1.6.1. We have the injection $\zeta^x : \mathbf{Z}_p/p^n\mathbf{Z}_p \to \overline{\mathbf{Q}_p}^\times$.

Proof. This follow from the fact that $\ker \zeta^x = p^n\mathbf{Z}_p$. □

Lemma 1.6.1. $\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$ as additive groups.

Proof. A straightforward application of the first isomorphism theorem gives the result. □

So we can see the function ζ^x as an injection from the integers modulo p^n to the p^nth roots of unity. Surjectivity depends on whether or not ζ is a primitive p^nth root.

Proposition 1.6.3. For $n \geq 1$, the characteristic function of $a+p^n\mathbf{Z}_p$ is given by the formula

$$\chi_{a+p^n\mathbf{Z}_p}(x) = \frac{1}{p^n}\sum_{\zeta\in\mu_{p^n}} \zeta^{x-a}.$$

Proof. If $x \in p^n\mathbf{Z}_p$, then $\sum_{z\in\mu_{p^n}} \zeta^x = p^n$. If $x \notin p^n\mathbf{Z}_p$, then by choosing ζ_n a generator of μ_{p^n}, we have that

$$\begin{aligned}\sum_{\zeta\in\mu_{p^n}} \zeta^x &= 1 + \zeta_n^x + (\zeta_n^2)^x + \cdots + (\zeta_n^{p^n-1})^x \\ &= 1 + \zeta_n^x + (\zeta_n^x)^2 + \cdots + (\zeta_n^x)^{p^n-1} \\ &= \frac{1-(\zeta_n^x)^{p^n}}{1-\zeta_n^x} \\ &= 0\end{aligned}$$

We can use the formula for geometric sums because ζ_n is primitive, thus $\zeta_n^x \neq 1$. Hence, $\sum_{\zeta\in\mu_{p^n}} \zeta^{x-a}$ will be equal to p^n if $x \in a + p^n\mathbf{Z}_p$ and equal to 0 if not. □

2 Pollack's plus and minus logarithm $\log_p^{\pm}$

In this section we will give the definition and some properties of the plus and minus logarithms defined by Pollack in [6].

2.1 Definitions

Like in theorem 1.5.2, let $\Phi_n(T) = \sum_{t=0}^{p-1} T^{p^{n-1}t}$ be the p^nth cyclotomic polynomial. We also write ζ_n for a primitive p^nth root of unity.

Definition 2.1.1. The p-adic logarithm is defined by the following formula

$$\log_p(1+T) = \prod_{k=1}^{\infty} \frac{\Phi_k(T)}{p}.$$

It is also possible to define the p-adic logarithm in the more standard way $\log_p(1+T) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$. Both are equivalent.

Definition 2.1.2. We say that γ is a topological generator of a group G if the closure of $\langle\gamma\rangle$ is dense in G.

Definition 2.1.3. For any integer j and γ a topological generator of $1 + p\mathbf{Z}_p$, we define

$$\log_{p,j}^{+}(T) := \frac{1}{p}\prod_{n=1}^{\infty} \frac{\Phi_{2n}(\gamma^{-j}(1+T))}{p},$$

$$\log_{p,j}^{-}(T) := \frac{1}{p}\prod_{n=1}^{\infty} \frac{\Phi_{2n-1}(\gamma^{-j}(1+T))}{p}.$$

Lemma 2.1.1. $\log_{p,j}^{+}(T)$ and $\log_{p,j}^{-}(T)$ converge and define power series in $\mathbf{Q}_p[\![T]\!]$ which are convergent on the open unit disc.

Proof. We prove convergence for the first product, the proof for the second is similar. To see that the product converges, it suffices to see that

$$\frac{\Phi_{2n}\left(\gamma^{-j}(1+T)\right)}{p} \to 1 \quad \text{as } n \to \infty.$$

Let $f_n(T) = (1/p)\Phi_{2n}(\gamma^{-j}(1+T)) - 1$. We must show that $f_n \to 0$ as $n \to \infty$. We have for $k < 2n$,

$$f_n(\gamma^j \cdot \zeta_k - 1) = \frac{\Phi_{2n}(\zeta_k)}{p} - 1 = \frac{1}{p}\left(\sum_{t=0}^{p-1} \zeta_k^{p^{n-1}t}\right) - 1 = \frac{1}{p}(p) - 1 = 0.$$

So if $\omega_{n,j} = (\gamma^{-j}(1+T))^{p^{2n-1}} - 1$, then $\omega_{n,j} | f_n$ because $\omega_{n,j}$ shares its roots with f_n and $\deg(\omega_{n,j}) = p^{2n-1} < (p-1)p^{2n-1} = \deg(f_n)$. Because $\gamma \in 1 + p\mathbf{Z}_p$, it follows that γ^{-j} is also in $1 + p\mathbf{Z}_p$, let's say $\gamma^{-j} = 1 + p \cdot a$ where $a \in \mathbf{Z}_p$. We can now apply the binomial theorem to get

$$\begin{aligned}\omega_{n,j}(T) &= \left((1+p\cdot a)^{p^{2n-1}}\right)\left((1+T)^{p^{2n-1}}\right) - 1 \\ &= \sum_{m=1}^{p^{2n-1}} \sum_{k=1}^{p^{2n-1}} \binom{p^{2n-1}}{m}\binom{p^{2n-1}}{k}(pa)^m T^k\end{aligned}$$

and deduce that each term has a valuation of at least $2n$. Hence, $v_p(\omega_{n,j}) \to \infty$ when $n \to \infty$. This imply that $\omega_{n,j} \to 0$ and our original product converges. □

Corollary 2.1.1. The power series

$$\log_p^{+}(T) := \prod_{j=0}^{k-2} \log_{p,j}^{+}(T),$$
$$\log_p^{-}(T) := \prod_{j=0}^{k-2} \log_{p,j}^{-}(T),$$

in $\mathbf{Q}_p[\![T]\!]$ are convergent on the open unit disc.

Proof. This follows from lemma 2.1.1. □

Those functions were given that name because we have the relation

$$\log_p^{+}(T)\log_p^{-}(T) = \prod_{j=0}^{k-2} \frac{\log_p(\gamma^{-j}(1+T))}{p^2(\gamma^{-j}(1+T)-1)}.$$

2.2 Interpolation formulae

To simplify, we will work in the case $k = 2$. We have $\log_p^+(T) = \frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n}(1+T)}{p}$ and $\log_p^-(T) = \frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n-1}(1+T)}{p}$. Pollack found the following interpolation property of $\log_p^{\pm}$:

Lemma 2.2.1. In the case where $k = 2$, $\log_p^{\pm}$ take special values at $\zeta_n - 1$. These values are

$$\log_p^+(\zeta_n - 1) = \begin{cases} 0 & 2|n, \\ p^{-(n+1)/2}\prod_{j=1}^{(n-1)/2}\Phi_{2j}(\zeta_n) & 2\nmid n, \end{cases}$$

$$\log_p^-(\zeta_n - 1) = \begin{cases} p^{-n/2-1}\prod_{j=1}^{n/2}\Phi_{2j-1}(\zeta_n) & 2|n, \\ 0 & 2\nmid n. \end{cases}$$

Proof. For $m > n$,

$$\Phi_m(\zeta_n) = 1 + (\zeta_n)^{p^{m-1}} + \cdots + (\zeta_n)^{p^{m-1}(p-1)} = p.$$

Hence the terms in the tail-end of the product describing $\log_p^{\pm}$ are all 1, and the beginning of the product is what appears in the above formula. □

Remark. If we have a primitive p^kth roots of unity where $k < n$, then

$$p^{-(k+1)/2}\prod_{j=1}^{(k-1)/2}\Phi_{2j}(\zeta_k) = p^{-(n+1)/2}\prod_{j=1}^{(n-1)/2}\Phi_{2j}(\zeta_k).$$

This is because, as stated above, every term with index greater than $(k-1)/2$ is p and does not change the product as it gets cancelled by the added factor of $p^{-(n+1)/2}$. A similar argument also works for the formula interpolating $\log_p^-$.

3 $\log_p^{\pm}$ and the Amice transform

Proofs of this section won't be given as they will appear in a article to be published [5].

3.1 Main result

We have just seen that $\log_p^{\pm}$ are power series on the open unit disc, though defined as products, and we have also seen that for each power series in $\mathbf{Q}_p[\![T]\!]$, there is an associated distribution in $\mathcal{D}(\mathbf{Z}_p, \mathbf{Q}_p)$. Here, we will give explicit formulae for the distributions associated to $\log_p^+$ and $\log_p^-$.

Definition 3.1.1. For a distribution $\mu \in \mathcal{D}(\mathbf{Z}_p, \mathbf{Q}_p)$, we let $\mu(a + p^n\mathbf{Z}_p) = \int_{a+p^n\mathbf{Z}_p} \mu = \int_{\mathbf{Z}_p} \chi_{a+p^n\mathbf{Z}_p}(x)\mu(x)$.

We now recall the definition of the Amice transform.

Definition 3.1.2. The Amice transform of a distribution μ is defined to be

$$A_\mu(T) = \int_{\mathbf{Z}_p} (1+T)^x \mu(x).$$

Definition 3.1.3. Let μ_+ be the distribution associated to $\log_p^+$ and μ_- be the distribution associated to $\log_p^-$.

Lemma 3.1.1. For $\zeta \in \mu_{p^n}$, $\log_p^\pm$ can be expressed in terms of an integral

$$\int_{\mathbf{Z}_p} \zeta^x \mu_\pm(x) = \log_p^\pm(\zeta - 1).$$

Proof. First remark that because μ_+ is the distribution associated to $\log_p^+$, we have that $A_{\mu_+}(T) = \log_p^+(T)$. Furthermore, $A_{\mu_+}(\zeta - 1) = \int_{\mathbf{Z}_p} \zeta^x \mu_+(x)$. □

We can now give fairly explicit formulae describing the values that $\mu_\pm$ takes on characteristic functions. For μ_+, the case where n is odd is natural, while the case n even requires some adjustment. The same goes for μ_- where the role of n is inversed. In order to better understand where the results come from, the reader may find it useful to first assume that n is odd when looking at results about $\log_p^+$. In doing so, floor functions can be ignored.

Proposition 3.1.1. The distribution μ_+ is given by

$$\int_{a+p^n\mathbf{Z}_p} \mu_+(x) = \frac{1}{p^{\lfloor (3n+2)/2 \rfloor}} \sum_{\zeta \in \mu_{p^n}} \zeta^{-a} \prod_{j=1}^{\lfloor n/2 \rfloor} \Phi_{2j}(\zeta)$$

and the distribution μ_- is given by

$$\int_{a+p^n\mathbf{Z}_p} \mu_-(x) = \frac{1}{p^{\lfloor (3n+1)/2 \rfloor + 1}} \sum_{\zeta \in \mu_{p^n}} \zeta^{-a} \prod_{j=1}^{\lfloor (n+1)/2 \rfloor} \Phi_{2j-1}(\zeta).$$

The product on the right hand side is still a bit complex so we would want to find a more simple expression for $\prod \Phi_{2j}(x)$ and $\prod \Phi_{2j-1}(x)$ in the form $\sum a_n x^n$. We use theorem 1.5.2 to do so. Because we have floor functions in our summation bounds, the λ are given by $\lambda^+_{\lfloor n/2 \rfloor}(m) = \sum_{l=0}^{\lfloor (n-2)/2 \rfloor} p^{2l+1} \lfloor m/p^l \rfloor \mod p^{2(l+1)}$ and $\lambda^-_{\lfloor (n+1)/2 \rfloor}(m) = \sum_{l=0}^{\lfloor (n-1)/2 \rfloor} p^{2l} \lfloor m/p^l \rfloor \mod p^{2l+1}$.

Corollary 3.1.1.

$$\int_{a+p^n\mathbf{Z}_p} \mu_+ = \frac{1}{p^{\lfloor (3n+2)/2 \rfloor}} \sum_{m=0}^{p^{\lfloor n/2 \rfloor}-1} \sum_{\zeta \in \mu_{p^n}} \zeta^{\lambda^+_{\lfloor n/2 \rfloor}(m)-a},$$

$$\int_{a+p^n\mathbf{Z}_p} \mu_- = \frac{1}{p^{\lfloor (3n+1)/2 \rfloor+1}} \sum_{m=0}^{p^{\lfloor (n+1)/2 \rfloor}-1} \sum_{\zeta \in \mu_{p^n}} \zeta^{\lambda^-_{\lfloor (n+1)/2 \rfloor}(m)-a}.$$

We now define two subsets of $\mathbf{Z}_p$ that will allow us to express $\mu_\pm$ in terms of those sets. Let

$$\mathcal{S}_n^+ := \{a \in \mathbf{Z}_p : \text{even powers of } p \text{ vanish in the expansion of } a \text{ modulo } p^n\};$$
$$\mathcal{S}_n^- := \{a \in \mathbf{Z}_p : \text{odd powers of } p \text{ vanish in the expansion of } a \text{ modulo } p^n\}.$$

Theorem 3.1.2. The values of $\mu_\pm$ are given by

$$\int_{a+p^n\mathbf{Z}_p} \mu_+ = \begin{cases} p^{-\lfloor (n+2)/2 \rfloor} & \text{if } a \in \mathcal{S}_n^+, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{a+p^n\mathbf{Z}_p} \mu_- = \begin{cases} p^{-\lfloor (n+3)/2 \rfloor} & \text{if } a \in \mathcal{S}_n^-, \\ 0 & \text{otherwise.} \end{cases}$$

3.2 Generalization for two-variable logarithms

In this section, we apply our result on one-variable logarithms to two-variable logarithms such as those defined by Loeffler in [7].

Definition 3.2.1. For $*, \circ \in \{+, -\}$, we define four new two-variable logarithms by using $\log_p^+$ and $\log_p^-$:

$$\log_p^{*,\circ}(T_1, T_2) = \log_p^*(T_1) \cdot \log_p^\circ(T_2).$$

Definition 3.2.2. We define $\mathbf{a} = (a, b)$ and $\mathbf{n} = (n, m)$. We write $\mathbf{a} + p^{\mathbf{n}}\mathbf{Z}_p$ for $(a + p^n\mathbf{Z}_p, b + p^m\mathbf{Z}_p)$ in $\mathbf{Z}_p^2$. Let $\chi_{\mathbf{a}+p^{\mathbf{n}}\mathbf{Z}_p}$ be the characteristic function of $(a + p^n\mathbf{Z}_p, b + p^m\mathbf{Z}_p)$ on $\mathbf{Z}_p^2$.

$$\chi_{\mathbf{a}+p^{\mathbf{n}}\mathbf{Z}_p} : \mathbf{Z}_p^2 \to \{0, 1\}$$
$$(x, y) \mapsto \begin{cases} 1 & \text{if } x \in a + p^n\mathbf{Z}_p \text{ and } y \in b + p^m\mathbf{Z}_p, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.2.1. For $n, m \geq 1$, the characteristic function χ is given by

$$\chi_{\mathbf{a}+p^{\mathbf{n}}\mathbf{Z}_p}(x, y) = \frac{1}{p^{n+m}} \left(\sum_{\zeta \in \mu_{p^n}} \zeta^{x-a} \right) \left(\sum_{\zeta \in \mu_{p^m}} \zeta^{y-b} \right).$$

Proof. The RHS will be nonzero only if both $x \in a+p^n\mathbf{Z}_p$ and $y \in b+p^m\mathbf{Z}_p$. In this case, by the same argument as in 1 dimension, the product of the two sums will be equal to p^{n+m}. $\square$

Definition 3.2.3. For $\mu \in \mathcal{D}(\mathbf{Z}_p^2, \mathbf{Q}_p)$, we define the *two-dimensional Amice transform* by the formula

$$A_\mu(T_1, T_2) = \int_{\mathbf{Z}_p^2} (1+T_1)^x (1+T_2)^y \mu(x,y).$$

Remark. As shown by Kim in [8], not all distribution on $\mathbf{Z}_p^2$ can be expressed as power series. The following condition must holds : For any $F(T_1,T_2) = \sum_{i,j\geq 0} b_{i,j} T_1^i T_2^j$, $|b_{i,j}|_p \leq O(\frac{1}{|a_p^{r+s}|_p})$ for $i < p^r$ and $j < p^s$. Since $\mu_{*,\circ}$, $*, \circ \in \{+,-\}$, is in $\mathcal{D}^{(1/2,1/2)}(\mathbf{Z}_p^2, \mathbf{Q}_p)$, the condition is satisfied. Kim's construction also shows that μ is completely determined by its values on characteristic functions.

Just like in the one-dimensional case, the two-dimensional Amice transform gives a correspondence between convergent power series in $\mathbf{Q}_p[\![T_1, T_2]\!]$ and distributions in $\mathcal{D}(\mathbf{Z}_p^2, \mathbf{Q}_p)$ as long as the condition stated by Kim holds.

Corollary 3.2.1. It is immediate from the definition that $\log_p^{*,\circ}(\zeta_n - 1, \zeta_m - 1) = \int_{\mathbf{Z}_p^2} \zeta_n^x \zeta_m^y \mu_{*,\circ}(x,y)$.

Theorem 3.2.1. The problem of finding values of $\mu_{*,\circ}(x,y)$ can be reduced to the one-dimensional case:

$$\int_{\substack{a+p^n\mathbf{Z}_p \\ b+p^m\mathbf{Z}_p}} \mu_{*,\circ}(x,y) = \int_{a+p^n\mathbf{Z}_p} \mu_*(x) \int_{b+p^m\mathbf{Z}_p} \mu_\circ(y).$$

Using results already proven for the one-dimensional case, we deduce the next corollary.

Corollary 3.2.2. The values of $\mu_{*,\circ}$ are given by

$$\int_{\substack{a+p^n\mathbf{Z}_p \\ b+p^m\mathbf{Z}_p}} \mu_{+,+}(x,y) = \begin{cases} p^{-\lfloor (n+2)/2 \rfloor - \lfloor (m+2)/2 \rfloor} & \text{if } a \in \mathcal{S}_n^+ \text{ and } b \in \mathcal{S}_m^+, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{a+p^n\mathbf{Z}_p \\ b+p^m\mathbf{Z}_p}} \mu_{+,-}(x,y) = \begin{cases} p^{-\lfloor (n+2)/2 \rfloor - \lfloor (m+3)/2 \rfloor} & \text{if } a \in \mathcal{S}_n^+ \text{ and } b \in \mathcal{S}_m^-, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{a+p^n\mathbf{Z}_p \\ b+p^m\mathbf{Z}_p}} \mu_{-,+}(x,y) = \begin{cases} p^{-\lfloor (n+3)/2 \rfloor - \lfloor (m+2)/2 \rfloor} & \text{if } a \in \mathcal{S}_n^- \text{ and } b \in \mathcal{S}_m^+, \\ 0 & \text{otherwise,} \end{cases}$$

$$\int_{\substack{a+p^n\mathbf{Z}_p \\ b+p^m\mathbf{Z}_p}} \mu_{-,-}(x,y) = \begin{cases} p^{\lfloor (n+3)/2 \rfloor - \lfloor (m+3)/2 \rfloor} & \text{if } a \in \mathcal{S}_n^- \text{ and } b \in \mathcal{S}_m^-, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This follows directly from theorem 3.1.2. $\square$

Acknowledgment I'd like to thank L'Institut des Sciences Mathématiques for giving me the opportunity to do this summer project. I also deeply appreciate the help and advices given by my supervisor Antonio Lei without whom this paper could not have been completed.

References

[1] Neil Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions Second Edition.* Springer, New-York, 1984.

[2] Scott Zinzer. Euclidean models of the p-adic integers. `https://math.la.asu.edu/~paupert/Zinzerproject.pdf`, 2012.

[3] Pierre Colmez. Fontaine's rings and p-adic L-functions. `http://staff.ustc.edu.cn/~yiouyang/colmez.pdf`, 2004.

[4] Brett Porter. Cyclotomic polynomials. `https://www.whitman.edu/Documents/Academics/Mathematics/2015/Final%20Project%20-%20Porter,%20Brett.pdf`, 2015.

[5] Cédric Dion and Antonio Lei. Plus and minus logarithms and Amice transform. To appear.

[6] Robert Pollack. On the p-adic L-function of a modular form at a supersingular prime. *Duke Math. J.*, 118(3):523–558, 2003.

[7] David Loeffler. p-adic integration on ray class groups and non-ordinary p-adic L-functions. In *Iwasawa theory 2012*, volume 7 of *Contrib. Math. Comput. Sci.*, pages 357–378. Springer, Heidelberg, 2014.

[8] Byoung Du Kim. Two-variable p-adic L-functions of modular forms for non-ordinary primes. *J. Number Theory*, 144:188–218, 2014.