MAZUR'S CONSTRUCTION OF THE KUBOTA–LEPOLDT p-ADIC L-FUNCTION

XEVI GUITART

Abstract. We give an overview of Mazur's construction of the Kubota–Leopoldt p-adic L-function as the p-adic Mellin transform of a Bernoulli measure. We follow (or rather just copy in many occasions) Lang [Lan78] (§2 of Chapter 2 and §3 of Chapter 4) and Koblitz [Kob84, Chapter II].

1. Introduction

Let $\zeta(s)$ be the zeta function, defined for $\mathrm{Re}(s) > 1$ as

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1}. \tag{1.1}$$

We aim to give a construction of the Kubota–Leopoldt p-adic zeta function ζ_p, which is a function of a p-adic variable that interpolates values of ζ at negative integers. One might think, on first thought, that the interpolation property of ζ_p should be

$$\zeta_p(1-k) = \zeta(1-k), \text{ for all } \ k \in \mathbb{Z}_{>0}. \tag{1.2}$$

However, as we will see, this is not exactly the interpolation property that ζ_p satisfies. The actual one differs from (1.2) in two aspects:

(1) it interpolates ζ "with the p-th Euler factor removed", and
(2) only at those integers $k \equiv 0 \pmod{p-1}$.

That is to say, ζ_p satisfies the interpolation property

$$\zeta_p(1-k) = (1-p^{k-1})\zeta(1-k) \text{ for all } \ k \equiv 0 \pmod{p-1}. \tag{1.3}$$

Recall the following properties of $\zeta(s)$:

(1) Integral representation:
$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} x^{s-1} \frac{dx}{e^x - 1}.$$
In other words, $\zeta(s)$ is essentially (i.e., except for the term $\Gamma(s)$) the *Mellin transform* of the measure $dx/(e^x-1)$.
(2) Special values: They can be given in terms of Bernoulli numbers. For any $k \in \mathbb{Z}_{>0}$ we have that

$$\zeta(1-k) = -\frac{B_k}{k}, \tag{1.4}$$

Date: November 17, 2013.
2010 *Mathematics Subject Classification.* 11G40 (11F41, 11Y99).

where the *Bernoulli numbers* B_k are defined by

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

The strategy for proving (1.4) is to explicitly compute by a direct calculation using (1.1) $\zeta(k)$ for k positive and even. Then one uses the functional equation relating $\zeta(s)$ and $\zeta(1-s)$ to derive (1.4) for all $k\in\mathbb{Z}_{>0}$.

We will present Mazur's construction of ζ_p, in which ζ_p is defined as a "p-adic Mellin transform" of a so-called Bernoulli distribution.

Actually, we will treat a more general case. Let

$$\chi\colon\ (\mathbb{Z}/p^m\mathbb{Z})^\times\longrightarrow\overline{\mathbb{Q}}^\times$$

be a Dirichlet character, which we lift to a function $\chi\colon\mathbb{Z}\to\overline{\mathbb{Q}}$ extending by 0 to the non prime to p integers. We fix an embedding $\overline{\mathbb{Q}}\subset\mathbb{C}_p=\widehat{\overline{\mathbb{Q}}}_p$, and we regard the values of χ either as algebraic numbers or as elements of $\mathbb{C}_p$ via this fixed embedding.

The L-function of χ is given for $\mathrm{Re}(s)>1$ by

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_{\ell}\left(1-\frac{\chi(\ell)}{\ell^s}\right).$$

It can be extended by analytic continuation to $\mathbb{C}$ and it turns out that for positive integers k its special values are

$$L(1-k,\chi)=-\frac{B_{k,\chi}}{k},$$

where the $B_{k,\chi}$ are the so-called generalized Bernoulli numbers (see Definition 3.5 below for the definition).

The goal of this notes is to give a proof of the following result.

Theorem 1.1 (Kubota–Leopoldt, Iwasawa)**.** *There exists a unique p-adic meromorphic (analytic if $\chi\neq\chi_{triv}$) function $L_p(s,\chi)$, $s\in\mathbb{Z}_p$, such that for $k\in\mathbb{Z}_{>0}$*

$$L_p(1-k,\chi)=L(1-k,\chi\omega^{-k}),$$

where $\omega\colon\ (\mathbb{Z}/p\mathbb{Z})^\times\to\overline{\mathbb{Q}}^\times$ denotes the Teichmüller character.

Remark 1.2. If we take $\chi=\chi_{\mathrm{triv}}\colon\ (\mathbb{Z}/p\mathbb{Z})^\times\to\overline{\mathbb{Q}}^\times$ the trivial character modulo p and $k\equiv 0 \pmod p$ we see that

$$L_p(1-k,\chi)=L(1-k,\chi)=(1-p^{k-1})\zeta(1-k),$$

so that we obtain the p-adic zeta function $\zeta_p(s)$ as a particular case.

2. p-adic distributions

Let $\{X_n\}$ be a collection of finite sets and

$$\pi_{n+1}\colon X_{n+1}\longrightarrow X_n$$

a collection of surjective maps. Thus we can consider the projective limit $X=\varprojlim X_n$ and the projections $r_n\colon X\to X_n$. We endow X with the limit topology, meaning that a basis of opens is

$\{r_n^{-1}(x) \colon x \in X_n\}_n$. Let also K be a complete local field with respect to a non-Archimedean norm $|\cdot|$, and let $\varphi_n \colon X_n \to K$ be a collection of maps.

Definition 2.1. $\{\varphi_n\}_n$ is said to be *compatible* if for each $x \in X_n$

$$\sum_{y \in \pi_{n+1}^{-1}(x)} \varphi_{n+1}(y) = \varphi(x).$$

Definition 2.2. A function $f \colon X \to K$ is *locally constant* if it factors through X_n for some n. We denote by $\mathrm{LC}(X, K)$ the set of locally constant functions.

Observe that if f factors through X_n it also factors through X_m for any $m \geq n$. Then the compatibility of $\{\varphi_n\}$ implies that

$$\sum_{x \in X_n} f(x)\varphi_n(x) = \sum_{x \in X_m} f(x)\varphi_m(x),$$

so that there is a well defined K-linear functional

$$\begin{array}{cccc} d\varphi \colon & \mathrm{LC}(X,K) & \longrightarrow & K \\ & f & \longmapsto & \int f d\varphi := \sum_{x \in X_n} f(x)\varphi_n(x). \end{array}$$

Then $\{\varphi_n\}$ (or the functional $d\varphi$) is called a *distribution* on X. Observe that

$$\left| \int f d\varphi \right| = \left| \sum_{x \in X_n} f(x)\varphi_n(x) \right| \leq \max_{x \in X_n} |f(x)| \cdot |\varphi_n(x)| \leq ||f|| \cdot ||\varphi||, \tag{2.1}$$

where $||\cdot||$ denotes the sup norm and $||\varphi|| = \sup_n ||\varphi_n||$.

Proposition 2.3. *Every continuous function $f \in C(X, K)$ is a uniform limit of locally constant functions. That is to say, there exist functions $f_n \in LC(X, K)$ such that $||f_n - f|| \to 0$.*

Proof. One can define $\tilde{f}_n \colon X_n \to K$ by $f_n(x) = f(s)$ for any s such that $r_n(s) = x$, and then take $f_n = \tilde{f}_n \circ r_n$. □

We also have that $||f_n - f_m|| \to 0$, and by (2.1) we see that

$$\left| \int (f_n - f_m) d\varphi \right| \leq ||f_n - f_m|| \cdot ||\varphi||,$$

so that the sequence $\int f_n d\varphi$ converges if $||\varphi|| < \infty$.

Definition 2.4. A *measure* is a bounded distribution.

By the discussion above, a measure φ defines a functional

$$\begin{array}{cccc} d\varphi \colon & \mathrm{C}(X,K) & \longrightarrow & K \\ & f & \longmapsto & \int f d\varphi := \lim_n \int f_n d\varphi(x). \end{array}$$

We end this section with a reformulation of the above formalism, also particularized to the case of interest to us, which is when $X = \mathbb{Z}_p$. In this case a distribution is a collection of maps $\varphi_n \colon \mathbb{Z}/p^n\mathbb{Z} \to K$ satisfying the compatibility condition

$$\varphi_n(a) = \sum_{b=0}^{p-1} \varphi_{n+1}(a + bp^n).$$

Let us denote by $\mathcal{U}$ the set of open compacts in $\mathbb{Z}_p$. Any $U \in \mathcal{U}$ is a disjoint union of balls of the form $a + p^n\mathbb{Z}_p$. In particular, we have that

$$a + p^n\mathbb{Z}_p = \bigsqcup_{b=0}^{p-1} a + bp^n + p^{n+1}\mathbb{Z}_p.$$

Then we can define a map

$$\begin{array}{rccc} \varphi\colon & \mathcal{U} & \longrightarrow & K \\ & a + p^n\mathbb{Z}_p & \longmapsto & \varphi(a + p^n\mathbb{Z}_p) := \varphi_n(a), \end{array}$$

and the compatibility condition is equivalent to

$$\varphi(a + p^n\mathbb{Z}_p) = \sum_{b=0}^{p-1} \varphi(a + bp^n + p^{n+1}\mathbb{Z}_p).$$

If we let $\mathcal{U}_n = \{a + p^n\mathbb{Z}_p\}_{a=0,\dots,p^n-1}$ denote the set of balls of radius p^{-n} we can rewrite the integral of a continuous function f as

$$\int_{\mathbb{Z}_p} f d\varphi = \lim_{n\to\infty} \sum_{U\in\mathcal{U}_n} f(t_U)\varphi(U),$$

where $t_U \in U$ is any sample point.

Finally, if $Y \subset \mathbb{Z}_p$ we will use the notation

$$\int_Y f d\varphi = \int_{\mathbb{Z}_p} \mathbb{1}_Y f d\varphi.$$

3. Bernoulli distributions

Recall the definition of the Bernoulli numbers B_k:

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

The *Bernoulli polynomials* $B_k(X)$ are defined by:

$$\frac{te^{tX}}{e^t - 1} = \sum_{k=0}^{\infty} B_k(X) \frac{t^k}{k!}.$$

Observe that $B_k = B_k(0)$. The first Bernoulli polynomials are

$$B_0(X) = 1,\ B_1(X) = X - \frac{1}{2},\ B_2(X) = X^2 - X - \frac{1}{6}.$$

Proposition 3.1. *The Bernoulli polynomials satisfy the relation*

$$B_k(X) = p^{k-1} \sum_{a=0}^{p-1} B_k\left(\frac{X+a}{p}\right). \tag{3.1}$$

Proof. We have that

$$\begin{aligned}\sum_{a=0}^{p-1}\frac{te^{(X+a)t}}{e^{pt}-1} =&\frac{1}{p}\sum_{a=0}^{p-1}\frac{pte^{\frac{X+a}{p}pt}}{e^{pt}-1} = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{k=0}^{\infty}B_k\left(\frac{X+a}{p}\right)\frac{(pt)^k}{k!}\\ =&\frac{1}{p}\sum_{a=0}^{p-1}\sum_{k=0}^{\infty}p^{k-1}B_k\left(\frac{X+a}{p}\right)\frac{t^k}{k!}.\end{aligned}$$

On the other hand, by summing the geometric series we find that:

$$\sum_{a=0}^{p-1}\frac{te^{(X+a)t}}{e^{pt}-1} = \frac{te^{Xt}}{e^{pt}-1}\cdot\frac{1-e^{pt}}{1-e^{t}} = \frac{te^{Xt}}{e^{t}-1} = \sum_{k=0}^{\infty}B_k(X)\frac{t^k}{k!},$$

and the result follows by comparing the terms of $\frac{t^k}{k!}$ in the two expressions. □

Definition 3.2. The k-th *Bernoulli distribution* is defined by the maps

$$\begin{array}{ccc}\mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Q}\subset\mathbb{Q}_p\\ x & \longmapsto & p^{n(k-1)}B_k\left(\frac{x}{p^n}\right),\end{array}$$

where in this expression we take x to be an integer between 0 and p^n-1.

If t is a rational number let $\langle t\rangle$ denote the least nonnegative in the same class of t modulo $\mathbb{Z}$. Sometimes we will use also a notation like $B_k(\langle\frac{x}{p^n}\rangle)$ if we don't want to specify that x has to be taken between 0 and p^n-1.

Remark 3.3. The maps of Definition 3.2 do specify a distribution. Indeed, the compatibility property follows from (3.1).

It is convenient to work with a normalized version of the Bernoulli distribution.

Definition 3.4. We denote by E_k the distribution given by the maps

$$E_k^{(n)}(x) = \frac{1}{k}p^{n(k-1)}B_k(\langle\frac{x}{p^n}\rangle)\quad\text{for } x\in\mathbb{Z}/p^n\mathbb{Z}.$$

Observe that since the function 1 factorizes through $\mathbb{Z}/p\mathbb{Z}$ we have

$$\int_{\mathbb{Z}_p}dE_k = \frac{1}{k}\cdot\sum_{a=0}^{p-1}B_k(\frac{a}{p}) = \frac{B_k(0)}{k} = \frac{B_k}{k}. \tag{3.2}$$

Generalized Bernoulli numbers. Let $f\colon\mathbb{Z}/p^n\mathbb{Z}\to K$ be a function.

Definition 3.5. The *generalized Bernoulli polynomials* $B_{k,f}$ are defined by

$$\sum_{a=0}^{p^n-1}f(a)\frac{te^{(X+a)}t}{e^{p^nt}-1} = \sum_{k=0}^{\infty}B_{k,f}(X)\frac{t^k}{k!}.$$

The constant terms $B_{k,f} := B_{k,f}(0)$ are the *generalized Bernoulli numbers* (relative to f).

The following identity is an immediate consequence of the definitions:

$$B_{k,f} = p^{n(k-1)}\sum_{a=0}^{p^n-1}f(a)B_k(\frac{a}{p^n}).$$

Interpreting f as a locally constant function on $\mathbb{Z}_p$ we can rewrite this as

$$\frac{1}{k}B_{k,f} = \int_{\mathbb{Z}_p} f dE_k. \tag{3.3}$$

From distributions to measures. Returning to the Bernoulli distributions, we remark the fact that they are not measures. For instance

$$E_1^{(n)}(x) = B_1(\frac{x}{p^n}) = \frac{x}{p^n} - \frac{1}{2} = \frac{2x-p^n}{p^n},$$

which is not p-adically bounded. They can be turned into measures by a standard process, called *regularization*. For this let $c \neq 1$ be a rational integer such that $p \nmid c$. Then we define distributions $E_{k,c}$ by means of the maps

$$E_{k,c}^{(n)}(x) = E_k^{(n)}(x) - c^k \cdot E_k^{(n)}(c^{-1} \cdot x), \quad \text{for } x \in \mathbb{Z}/p^n\mathbb{Z}.$$

Here $c^{-1} \cdot x$ denotes multiplication in $\mathbb{Z}/p^n\mathbb{Z}$. It is easy to see that $E_{k,c}$ is a distribution (for a linear combination of distributions is a distribution). Passing to the limit the above maps we can write

$$E_{k,c}(x) = E_k(x) - c^k E_k(c^{-1} \cdot x) \tag{3.4}$$

The following two properties are really key in the construction of the p-adic L-function.

Proposition 3.6. (1) *The values of $E_{k,c}^{(n)}$ are p-integral (i.e., they belong to $\mathbb{Z}_p$).*

(2) $E_{k,c}^{(n)}(x) \equiv x^{k-1}E_{1,c}^{(n)}(x) \pmod{p^{n-d_k}\mathbb{Z}_p}$*, where d_k is*[1] *the p-adic valuation of the least common multiple of the denominators of the coefficients of $B_k(X)$.*

Proof. We will first prove the second assertion. To begin with, let's assume that $d_k = 0$, so that the coefficients of B_k lie in $\mathbb{Z}_p$. It is easily checked that $B_k(X)$ is of the form

$$X^k + \frac{k}{2}X + \text{ higher order terms.}$$

Now let $x \in \mathbb{Z}/p^n\mathbb{Z}$, which we also view as an integer $0 \leq x \leq p^n - 1$. Denote by $\{c^{-1}x\}$ the representative of $c^{-1}x$ in $\mathbb{Z}/p^n\mathbb{Z}$ that lies in the range $0, \ldots, p^n - 1$. Then we can write $c\{c^{-1}x\} = x + ap^n$ for some $a \in \mathbb{Z}$. The following congruences are modulo $p^n\mathbb{Z}_p$:

$$\begin{aligned}
E_{k,c}^{(n)}(x) &= \frac{1}{k}p^{n(k-1)}\left[B_k\left(\frac{x}{p^n}\right) - c^k B_k\left(\frac{\{c^{-1}x\}}{p^n}\right)\right] \equiv \\
&\equiv \frac{1}{k}p^{n(k-1)}\left[\left(\frac{x}{p^n}\right)^k - \frac{k}{2}\left(\frac{x}{p^n}\right)^{k-1}\right] - \frac{1}{k}p^{n(k-1)}\left[c^k\left(\frac{\{c^{-1}x\}}{p^n}\right)^k - c^k\frac{k}{2}\left(\frac{\{c^{-1}x\}}{p^n}\right)^{k-1}\right] \\
&\equiv \frac{1}{k}p^{n(k-1)}\left[\left(\frac{x}{p^n}\right)^k - \frac{k}{2}\left(\frac{x}{p^n}\right)^{k-1}\right] - \frac{1}{k}p^{n(k-1)}\left[\left(c\frac{\{c^{-1}x\}}{p^n}\right)^k - c\frac{k}{2}\left(c\frac{\{c^{-1}x\}}{p^n}\right)^{k-1}\right] \\
&\equiv \frac{1}{k}p^{n(k-1)}\left[\left(\frac{x}{p^n}\right)^k - \frac{k}{2}\left(\frac{x}{p^n}\right)^{k-1}\right] - \frac{1}{k}p^{n(k-1)}\left[\left(\frac{x}{p^n}+a\right)^k - c\frac{k}{2}\left(\frac{x}{p^n}+a\right)^{k-1}\right] \\
&\equiv x^{k-1}\left(\frac{c-1}{2} - a\right).
\end{aligned}$$

[1] actually this d_k is missing in Lang's statement, but I believe it should be there (cf. [Kob84], Chapter 4, §5, Theorem 5). In any case, it does not make any difference for large n, since d_k is independent of n.

On the other hand:

$$E_{1,c}^{(n)}(x) = B_1\left(\frac{x}{p^n}\right) - cB_1\left(\frac{\{c^{-1}x\}}{p^n}\right) = \frac{x}{p^n} - \frac{1}{2} - c\left[\frac{\{c^{-1}x\}}{p^n} - \frac{1}{2}\right]$$
$$= \frac{x}{p^n} - \frac{1}{2} - \frac{x+ap^n}{p^n} - \frac{c}{2} = \frac{c-1}{2} - a. \tag{3.5}$$

If $d_k > 0$, one considers $D_k B_k$ where D_k is the least common multiple of the denominators of $B_k(X)$. Since $D_k B_k$ has coefficients in $\mathbb{Z}_p$, the above calculations go through and give the result in general.

Now we prove the first statement. First of all observe that $E_{1,c}^{(n)}$ takes values in $\mathbb{Z}_p$ because of (3.5) (recall that $a \in \mathbb{Z}$). Now for n big enough $n - d_k \geq 0$, and that $E_{k,c}^{(n)}(x)$ belongs to $\mathbb{Z}_p$ follows from part (2) of the proposition. If n is such that $n - d_k < 0$, we just take m such that $m - d_k > 0$ and use the distribution relation:

$$E_{k,c}^{(n)}(x) = \sum_{y \equiv x \pmod{p^n}} E_{k,c}^{(m)}(y) \in \mathbb{Z}_p.$$

□

Remark 3.7. Passing to the limit the second statement in the proposition it can be rewritten as

$$E_{k,c}(x) = x^{k-1} \cdot E_{1,c}(x). \tag{3.6}$$

Combining this with the formula (3.2) for B_k we obtain the following important expression of B_k in terms of $E_{1,c}$.

Proposition 3.8. *For any $k \in \mathbb{Z}_{>0}$*

$$\frac{B_k}{k} = \frac{1}{1-c^k}\int_{\mathbb{Z}_p} x^{k-1} dE_{1,c}(x) \tag{3.7}$$

Proof. It follows from the following computation:

$$\frac{B_k}{k} \overset{(3.2)}{=} \int_{\mathbb{Z}_p} dE_k \overset{(3.4)}{=} \int_{\mathbb{Z}_p} dE_{k,c} + \int_{\mathbb{Z}_p} c^k dE_k(c^{-1}\cdot x)$$
$$\overset{(*)}{=} \int_{\mathbb{Z}_p} dE_{k,c} + \int_{\mathbb{Z}_p} c^k \cdot dE_k(x) \overset{(3.6)}{=} \int_{\mathbb{Z}_p} x^{k-1} dE_{1,c} + c^k \frac{B_k}{k},$$

where in $(*)$ we used the change of variables $x \mapsto cx$ (observe that this transforms $\mathbb{Z}_p$ in $\mathbb{Z}_p$ because by assumption $c \in \mathbb{Z}_p^\times$). □

Observe that the left term in (3.7) is (the negative of) $\zeta(1-k)$. Therefore, if the right hand side of (3.7) was still meaningful when we replace the integer $k-1$ by an arbitrary $s \in \mathbb{Z}_p$, we could use this expression on the right to define a p-adic function that interpolates ζ at the integers.

However, in the right hand side of (3.7) we have the function x^{k-1} for x ranging over the domain of integration, which is $\mathbb{Z}_p$. The problem is that if $x \in \mathbb{Z}_p$ and $s \in \mathbb{Z}_p$, we can not always consider something like x^s. For instance, if $x \in p\mathbb{Z}_p$ then it is clear that we can not give a meaning to x^s for arbitrary $s \in \mathbb{Z}_p$. A first step in order to fix this problem would be to express the Bernoulli numbers as integrals over $\mathbb{Z}_p^\times$, rather than over $\mathbb{Z}_p$. The following proposition tells us that this is also possible, and the cost is the appearance of an Euler factor term.

Proposition 3.9. *For any $k \in \mathbb{Z}_{>0}$*

$$(1-p^{k-1}) \cdot \frac{B_k}{k} = \frac{1}{1-c^k} \int_{\mathbb{Z}_p^\times} x^{k-1} dE_{1,c}(x). \tag{3.8}$$

Proof. Since $\mathbb{Z}_p = \mathbb{Z}_p^\times \sqcup p\mathbb{Z}_p$ we have:

$$\int_{\mathbb{Z}_p} x^{k-1} dE_{1,c}(x) = \int_{\mathbb{Z}_p^\times} x^{k-1} dE_{1,c}(x) + \int_{p\mathbb{Z}_p} x^{k-1} dE_{1,c}(x).$$

Now the result follows immediately from the following claim:

Claim. $\displaystyle\int_{p\mathbb{Z}_p} x^{k-1} dE_{1,c} = p^{k-1} \int_{\mathbb{Z}_p} x^{k-1} dE_{1,c}.$

In order to prove the claim, we consider the decomposition of $\mathbb{Z}_p$

$$\mathbb{Z}_p = \bigsqcup_{x=0}^{p^n-1} x + p^n \mathbb{Z}_p,$$

which induces the following decomposition of $p\mathbb{Z}_p$:

$$p\mathbb{Z}_p = \bigsqcup_{x=0}^{p^n-1} px + p^{n+1} \mathbb{Z}_p.$$

Then, by definition of the integral we have

$$\begin{aligned}\int_{p\mathbb{Z}_p} x^{k-1} dE_{1,c} &= \lim_{n\to\infty} \sum_{x=0}^{p^n-1} (px)^{k-1} E_{1,c}^{n+1}(px) \\ &\overset{(*)}{=} p^{k-1} \lim_{n\to\infty} \sum_{x=0}^{p^n-1} x^{k-1} E_{1,c}^{n}(x) \\ &= p^{k-1} \int_{\mathbb{Z}_p} x^{k-1} dE_{1,c}(x),\end{aligned}$$

where in $(*)$ we have used that $E_{1,c}^{(n+1)}(px) = E_{1,c}^{(n)}(x)$. This follows directly from the shape of the Bernoulli polynomial $B_1(X) = X - \frac{1}{2}$. Indeed,

$$B_1^{(n)}(x) = \frac{x}{p^n} = \frac{px}{p^{n+1}} - \frac{1}{2} = B_1^{(n+1)}(px).$$

□

Remark 3.10. The expression on the right hand side of (3.8) still does not make sense when replacing $k-1$ by an arbitrary $s \in \mathbb{Z}_p$. Indeed, the expression x^s is well defined in general only when x belongs $1 + p\mathbb{Z}_p$. But at least now $x \in \mathbb{Z}_p^\times$ in (3.8), so that $\langle x \rangle := x\omega(x)^{-1}$ lies in $1 + p\mathbb{Z}_p$ and $\langle x \rangle^s$ makes sense for all $s \in \mathbb{Z}_p$. This is is how we will obtain the desired p-adic L-function, but we postpone the details until the next section.

From the expressions of the Bernoulli numbers in terms of p-adic integrals of Proposition 3.9 one recovers, as a consequence of rather elementary properties of the integrals, the following classical congruences.

Corollary 3.11 (Congruences of Kummer and von Staudt)**.** *Let k be a positive integer.*

(1) *If* $p-1\nmid k$ *then* $\left|\frac{B_k}{k}\right|_p\leq 1$.
(2) *If* $p-1\nmid k$ *and* $k\equiv k' \pmod{(p-1)p^n}$ *then*

$$(1-p^{k-1})\frac{B_k}{k}\equiv(1-p^{k'-1})\frac{B_{k'}}{k'}\pmod{p^{n+1}}.$$

(3) *If* $k\equiv 0 \pmod{(p-1)}$ *and* k *is even then*

$$B_k\equiv-\frac{1}{p}\pmod{\mathbb{Z}_p}.$$

Proof. We just prove the second statement, the others are proved similarly. First of all, observe that the congruence is equivalent to

$$\frac{1}{1-c^k}\int_{\mathbb{Z}_p^\times}x^{k-1}dE_{1,c}(x)\equiv\frac{1}{1-c^{k'}}\int_{\mathbb{Z}_p^\times}x^{k'-1}dE_{1,c}(x)\pmod{p^{n+1}}. \tag{3.9}$$

It is enough to prove that:

$$\frac{1}{1-c^k}\equiv\frac{1}{1-c^{k'}}\pmod{p^{n+1}\mathbb{Z}_p},\quad\text{and}$$

$$\int_{\mathbb{Z}_p^\times}x^{k-1}dE_{1,c}(x)\pmod{p^{n+1}}\equiv\int_{\mathbb{Z}_p^\times}x^{k'-1}dE_{1,c}(x)\pmod{p^{n+1}\mathbb{Z}_p}. \tag{3.10}$$

For this choose c a primitive root modulo p, so that $c^k\not\equiv 1\pmod{p}$. This implies that $1-c^k$ and $1-c^{k'}$ are p-adic units. In addition, if we write $k=k'+ap^n(p-1)$ for some a we find that

$$c^k-c^{k'}=c^k(1-c^{(p-1)p^na}).$$

But $c^{p-1}\equiv 1\pmod{p}$, and an easy exercise using the binomial expansion shows that $c^{(p-1)p^n}\equiv 1 \pmod{p^{n+1}}$. Equivalently,

$$|c^k-c^{k'}|_p\leq p^{-(n+1)},$$

and from this it also follows that

$$\left|\frac{1}{1-c^k}-\frac{1}{1-c^{k'}}\right|_p\leq p^{-(n+1)}.$$

Applying the same argument to x^k and $x^{k'}$ (which we can since $x\in\mathbb{Z}_p^\times$) we also find that

$$|x^k-x^{k'}|_p\leq p^{-(n+1)}.$$

Now (3.10) follows from the basic property of the integrals (2.1), together with the fact that $E_{1,c}$ takes values in $\mathbb{Z}_p$. $\square$

Now let $\chi\colon\mathbb{Z}/p^n\mathbb{Z}\longrightarrow\overline{\mathbb{Q}}\subset\mathbb{C}_p$ be an Dirichlet character (we assume $n>0$, and we extend by 0 on the non-invertible elements). By (3.3) and the fact that χ is zero on $p\mathbb{Z}_p$ we see that

$$\frac{B_k}{k}=\int_{\mathbb{Z}_p^\times}\chi dE_k.$$

Proposition 3.12. *For* $k\in\mathbb{Z}_{>0}$ *we have that*

$$\frac{B_{k,\chi}}{k}=\frac{1}{1-\chi(c)c^k}\int_{\mathbb{Z}_p^\times}\chi(x)x^{k-1}dE_{1,c}(x) \tag{3.11}$$

Proof. It is computation, similar to that of Proposition 3.7:

$$\begin{aligned}\frac{B_{k,\chi}}{k} &= \int_{\mathbb{Z}_p^\times} \chi dE_k = \int_{\mathbb{Z}_p^\times} \chi dE_{k,c} + \int_{\mathbb{Z}_p^\times} \chi(x) c^k dE_k(c^{-1}\cdot x) \\ &= \int_{\mathbb{Z}_p^\times} x^{k-1}\chi(x) dE_{1,c}(x) + \int_{\mathbb{Z}_p^\times} \chi(c)\chi(x)c^k dE_k(x) \\ &= \int_{\mathbb{Z}_p^\times} x^{k-1}\chi(x)dE_{1,c}(x) + c^k\chi(c)\frac{B_{k,\chi}}{k}.\end{aligned}$$

□

4. Definition of the p-adic L-function

Let $\omega\colon \mathbb{Z}_p^\times \to \mu_{p-1} \subset \mathbb{Z}_p^\times$ denote the Teichmüller character (we assume $p \neq 2$ for simplicity here), characterized by the property that $\omega(a) \equiv a \pmod{p}$. Then any $a \in \mathbb{Z}_p^\times$ can be written uniquely as

$$a = \langle a\rangle \cdot \omega(a), \quad \text{with } \langle a\rangle \equiv 1 \pmod{p}.$$

Definition 4.1. The Mellin transform of a measure μ is the function on the p-adic variable s defined by

$$\mathbb{M}_p\mu(s) = \int_{\mathbb{Z}_p^\times} \langle a\rangle^s \cdot a^{-1} d\mu(a).$$

The Mellin transform is analytic on $\mathbb{Z}_p$. This follows from the following lemma.

Lemma 4.2. *Let μ be a measure on $\mathbb{Z}_p^\times$. Then there exist $b_n \in \mathbb{Z}_p$ with $b_n \longrightarrow 0$ such that*

$$\int_{\mathbb{Z}_p^\times} \langle a\rangle^s d\mu = \sum_n b_n s^n, \text{ for } s \in \mathbb{Z}_p.$$

Proof. We can decompose the integral as

$$\int_{\mathbb{Z}_p^\times} \langle a\rangle^s d\mu = \sum_{b=1}^{p-1} \int_{\omega(b)\cdot(1+p\mathbb{Z}_p)} \langle a\rangle^s d\mu(a).$$

In each integral we can make the change of variables $a = \omega(b)x$ (and replace μ by another measure), so that we are reduced to prove the proposition for integrals of the form

$$\int_{1+p\mathbb{Z}_p} \langle x\rangle^s d\mu(x).$$

Now we have that

$$\begin{aligned}\int_{1+p\mathbb{Z}_p} \langle x\rangle^s d\mu &= \int_{1+p\mathbb{Z}_p} x^s d\mu = \int_{1+p\mathbb{Z}_p} \sum_{n=0}^{\infty} \binom{n}{s}(x-1)^n d\mu(x) = \\ &= \int_{1+p\mathbb{Z}_p} \sum_{n=0}^{\infty} s(s-1)\cdots(s-n+1)\frac{(x-1)^n}{n!} d\mu(x).\end{aligned}$$

Now x runs over $1+p\mathbb{Z}_p$, so that $x \equiv 1 \pmod{p\mathbb{Z}_p}$. This implies that $\frac{(x-1)^n}{n!}$ is p-integral and tends to 0 p-adically. Thus we can interchange the sum and the integral:

$$\int_{1+p\mathbb{Z}_p} \langle x \rangle^s d\mu = \sum_{n=0}^{\infty} s(s-1)\cdots(s-n+1)c_n, \tag{4.1}$$

where the $c_n = \int_{1+p\mathbb{Z}_p} \frac{(x-1)^n}{n!} d\mu(x)$ are p-integral and tend to 0 as $n \to \infty$. Now it is clear that we can reorder (4.1) and write it as a power series of the shape stated in the proposition. □

Fix a c such that $\chi(c)\langle c \rangle^s$ is not identically 1.

Definition 4.3. The p-adic L-function $L_p(1-s,\chi)$ is defined as

$$L_p(1-s,\chi) = \frac{-1}{1-\chi(c)\langle c \rangle^s} \int_{\mathbb{Z}_p^\times} \langle x \rangle^s \chi(x) x^{-1} dE_{1,c}(x).$$

Observe that the integral is an analytic function of s by the lemma. The term in front is analytic except when $\chi(c)\langle c \rangle^s = 1$. If χ is non trivial then one can choose c such that $\chi(c) \neq 1$ and therefore it is analytic also at $s = 0$.

Finally we see that this function satisfies the desired interpolation properties.

Theorem 4.4. *For any $k \in \mathbb{Z}_{>0}$ we have that*

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

Proof. It follows from this simple computation:

$$\begin{aligned}
\int_{\mathbb{Z}_p^\times} \langle x \rangle^{k-1} \chi(x)\omega(x)^{-1} dE_{1,c}(x) &= \int_{\mathbb{Z}_p^\times} x^{k-1}\chi(x)\omega(x)^{-(k-1)}\omega(x)^{-1} dE_{1,c}(x) \\
&= \int_{\mathbb{Z}_p^\times} x^{k-1}\chi(x)\omega(x)^{-k} dE_{1,c}(x) \\
&\overset{(3.11)}{=} \frac{1}{k}\left(1 - \chi\omega^{-k}(c)c^k\right) B_{k,\chi\omega^{-k}}.
\end{aligned}$$

□

Corollary 4.5. *If $k \equiv 0 \pmod{(p-1)}$ and p is odd then*

$$L_p(1-k,\chi) = \frac{-1}{k} B_{k,\chi}.$$

References

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR 754003 (86c:11086)

[Lan78] Serge Lang, *Cyclotomic fields*, Springer-Verlag, New York, 1978, Graduate Texts in Mathematics, Vol. 59. MR 0485768 (58 #5578)

E-mail address: xevi.guitart@gmail.com