TALK NOTES: p-ADIC MODULAR FORMS À LA SERRE

FRANCESCA BERGAMASCHI

1. Introduction

Goal: Defining p-adic modular forms so that they carry the p-adic topology, by following Serre's paper "Formes modulaires et fonctions zêta p-adiques" ([Ser1]). The subject of p-adic modular forms was introduced in the 70's through the following steps:

- Serre, Swinnerton-Dyer ([Ser1, Ser2, SD]): Understanding of modular forms mod p (This was explained during Giulio's talk).
- Serre ([Ser1]): Definition of p-adic modular forms as limits of regular modular forms.
- Katz ([Katz]): Generalization of Serre's definition to a geometric context (Serre's p-adic modular forms will be a particular case of a much wider class of objects).

1.1. **Motivation.** - Motivation for Serre (and for this seminar): defining p-adic L-functions through p-adic interpolation starting from the q-expansion of p-adic modular forms.

Given a number field K, we may define its zeta-function:

$$\zeta_K(s) := \sum_{\mathfrak{a} \triangleleft O_K} \frac{1}{Norm(\mathfrak{a})^s} = \prod_{\substack{\mathfrak{p} \triangleleft \mathscr{O}_K \\ \mathfrak{p} \text{ prime}}} \frac{1}{1 - Norm(\mathfrak{p})^{-s}}, \quad Re(s) > 1.$$

In order to find a p-adic analogue to regular L-functions, Kubota and Leopoldt, looked fot a p-adic meromorphic function which takes the same value as regular L-functions on negative integers. They relied on the following result:

Given K is an abelian extension of $\mathbb{Q}$:

$$\zeta_K(1-k) = \prod_{\chi} L(\chi, 1-k) = \prod_{\chi} (-b_k(\chi)/k), \qquad k \geq 1,$$

where χ runs through the set of rational characters attached to K. This identity allows us to deduce relations for $\zeta_K(1-k)$ for various values of k and hence to construct by interpolation a p-adic ζ-function for K.

Serre's aim is to extend this strategy to any totally real number field. His results are inspired by methods of Klingen and Siegel. They hold on the fact that $\zeta_K(1-k)$ appears as the constant term of a certain modular form whose higher coefficients are easy to compute. The method consists essentially in transferring the properties

Date: February 5^{th} 2012.

of coefficients of higher degree to the constant term. An example is the proof by Siegel of the following result:

$$\zeta_K(1-k) \in \mathbb{Q},$$

for k a positive integer.

Another motivation for Serre was to construct p-adic analytic families of modular forms. He had in mind connections to Galois representations and Iwasawa theory.

2. p-adic modular forms á la Serre

Fix a prime p.

Remark. *The exposition by Serre is done for modular forms over $\mathbb{Q}$ of level 1, but the theory can be developed more generally for modular forms over number fields of any level. We will hence denote by $\mathcal{M}_k$ the space of modular forms over $\mathbb{Q}$ of level 1 and weight k.*

Serre starts by defining a notion of p-adic valuation of a formal series with rational coefficients $f = \sum_n a_n q^n \in \mathbb{Q}[[q]]$:

$$v_p(f) := \inf_n v_p(a_n).$$

Definition 2.0.1 (Serre)**.** *A p-adic modular form is a formal power series*

$$f = \sum_n a_n q^n \in \mathbb{Z}_p[[q]] \otimes \mathbb{Q}$$

such that there exists a sequence $f_i \in \mathcal{M}_{k_i}$ such that $v_p(f - f_i) = \infty$, for $i \to \infty$ (that is, if $\{f_i\}$ converges uniformly with respect to the p-adic topology).

3. Is this a 'good' definition?

Remark. *It is not required that the f_i's have the same weight (in fact they need to be different in order to obtain a new, non-trivial notion). We will soon be able to define a notion of weight as the p-adic limit as the k_i's. In order to do so, we shall define a new environment by studying congruences of regular modular forms.*

3.1. Modular forms modulo p^m.

3.1.1. *Recall: the algebra of modular forms mod p.* I will briefly recall the results on congruences of modular forms modulo a prime p, which have been explained in detail during Giulio's talk. As already remarked by him, the following results are due to Swinnerton-Dyer ([SD]). We want to study the reduction modulo p of modular forms:

$$M_k \xrightarrow{\pi} \mathbb{F}_p[[q]],$$

we denote by $\tilde{M}_k := \pi(M_k)$. We want namely to study the following object:

$$\tilde{M} := \sum_{k \in \mathbb{Z}} \tilde{M}_k \subset \mathbb{F}_p[[q]],$$

the *algebra of modular forms modulo p*. Recall that $Q = E_4$ and $R = E_6$ generate the graded algebra of modular forms. We have various cases. For $p \geq 5$, for any element $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$, set

$$\tilde{M}^\alpha = \bigcup_{k \equiv_{p-1} \alpha} \tilde{M}_k.$$

Swinnerton-Dyer proved that $\tilde{M}$ is the graded algebra

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

One has moreover the following identification:

$$\tilde{M} = \mathbb{F}_p[Q, R]/(\tilde{A} - 1).$$

I would like to remark that this description allows us to interpret $\tilde{M}$ geometrically, as the affine algebra of a smooth algebraic curve, see [Ser2] for details.

Fof $p = 2, 3$, one has that

$$\tilde{M} = \mathbb{F}_p[\tilde{\Delta}].$$

(Where I recall $\Delta = 2^{-6}3^{-3}(Q^3 - R^2)$).

Theorem 3.1.1. *[Modulo p^m congruences] Let $m \geq 1$ be an integer. Let f and f' be two modular forms of weight k and k' respectively. Suppose that $f \neq 0$ and that*

$$v_p(f - f') \geq v_p(f) + m.$$

Then

$$\begin{array}{lll} k' \equiv k & \text{mod } (p-1)p^{m-1} & \text{if } p \geq 3 \\ k' \equiv k & \text{mod } 2^{m-2} & \text{if } p = 2 \end{array}$$

Proof. Suppose first $m = 1$. By (in case) multiplying f by a scalar, we may suppose $v_p(f) = 0$, so that the hypothesis of the theorem becomes:

$$f' \equiv f \qquad \text{mod } p^m.$$

In particular the coefficients of both f and f' will be p-integers, and $\tilde{f} = \tilde{f}' \neq 0 \in \tilde{M}$. If $p \geq 5$, it follows that f and f' belong to the same component $\tilde{M}^{\alpha}$ of $\tilde{M}$, that is $k \equiv k'$ mod $(p-1)$. Since k and k' are even, the same holds for $p = 2, 3$.
See Theorem 1, section 1.3 of [Ser1] for the general proof. □

Indeed, let $m \geq 1$ be an integer ($m \geq 2$ if $p = 2$). We define the following group

$$X_m = \begin{cases} \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z} = \mathbb{Z}/p^{m-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \neq 2 \\ \mathbb{Z}/2^{m-2}\mathbb{Z} & \text{if } p = 2 \end{cases}$$

Note that the X_m's form a projective system and hence we define

$$X := \varprojlim_m X_m = \begin{cases} \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \neq 2 \\ \mathbb{Z}_2 & \text{if } p = 2 \end{cases}$$

We remark that the natural map $\mathbb{Z} \to X$ is injective and through this we shall think of the integers as a *dense* subgroup of X

3.2. **Weights of a p-adic modular form.** Let f be a non-zero p-adic modular form and let $(f_i)_i$ be a sequence of rational modular forms of weights k_i, converging to f. Then the k_i's converge to a number in the group X. Such a limit depends on f, but not on the f_i's.

Proof. Since $v_p(f_i - f_j) \to \infty$, we may apply the theorem above, obtaining that for any $m \geq 1$, the image of (k_i) in X_m is stationary. Hence we may set $k = \varprojlim k_i$. □

Definition 3.2.1. *We call $k = \varprojlim k_i$ as above the* weight *of f. It is an even element (being the limit of even elements).*

The p-adic modular forms of a given weight form a $\mathbb{Q}_p$-vector space.

4. First properties

We expect p-adic modular forms to satisfy properties similar to those satisfied by regular modular forms.

Theorem 4.0.2. *Let $m \geq 1$ be an integer and let f and f' be two non-zero p-adic modular forms, of weight k and k' respectively. If*

$$v_p(f - f') \geq v_p(f) + m,$$

then $k = k'$ in X_m.

Proof. By definition f and f' can both be written as limits of regular modular forms f_i (resp f_i') of weight k_i (resp k_i'). For i big enough one has that

$$v_p(f_i - f_i') \geq v_p(f) + m,$$

and hence, by the theorem above, it follows that $k_i = k_i'$ in X_m and hence the conclusion. □

This theorem has a certain number of corollaries.

Corollary 4.0.3. *Let $f = \sum a_n q^n$ be a p-adic modular form of weight $k \in X$ and m is a positive integer such that the image of k in X_{m+1} is non-zero. Then*

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

Proof. Note that we may suppose $a_0 \neq 0$. Indeed if $a_0 = 0$ then $v_p(a_0) = \infty$ and the assertion holds obviously. Hence we define the constant modular form of weight 0: $f' = a_0$ and we have

$$v_p(f - f') = \inf_{n \geq 1} v_p(a_n).$$

Since the weights of f and f' have different images inside X_{m+1}, by Theorem (4.0.2)

$$v_p(f) + m + 1 > v_p(f - f'),$$

hence the conclusion since $v_p(a_0) \geq v_p(f)$. □

Remark. *In case $p - 1 \neq |k$ (i.e. it does not belong to $\mathbb{Z}_p \leq X$) we may choose $m = 0$ in the corollary above. Id est:*

Corollary 4.0.4. *Under the hypotheses in the Remark, if the coefficients a_i are integral for every $i \geq 1$, then a_0 is also integral.*

This result can be seen as an integral analog to the rationality theorem by Siegel, and it is an example of the *Klingen-Siegel* method I referred to in the beginning. There is a concrete example to have in mind. (In Serre's paper it is stated as a Theorem).

Corollary 4.0.5. *Let K be a totally real number field of degree g and let $k \geq 2$ be an integer.*

(1) *If $kg \not\equiv 0$ mod $p - 1$, we have that $\zeta_K(1 - k)$ is p-integral.*

(2) *If $kg \equiv 0 \mod p-1$, we have that $v_p(\zeta_K(1-k)) \geq -1 - v_p(gk)$.*

Proof. For every m there is a modular form of weight mg:

$$f_k = \frac{\zeta_K(1-k)}{2^g} + \sum_{n=1}^{\infty} a_k(n) q^n,$$

where

$$a_k(n) = \sum_{\substack{\nu \in (\mathcal{D}_K^{-1})^+ \\ Tr(\nu)=n}} \sum_{(\nu)\mathcal{D}_K \subseteq \mathfrak{a} \subseteq \mathscr{O}_K} Norm(\mathfrak{a})^{k-1},$$

(where $\mathcal{D}_K$ denotes the different of K, $Tr(\nu) \geq 1$). This modular form is related to the diagonal curve. The higher coefficients of f_k are p-integers (in fact they are really integers), and hence if $kg \not\equiv 0 \mod p-1$, then also the leading coefficient is p-integral. Suppose now $kg \equiv 0 \mod p-1$. Put $\tilde{k} = kg$ and $m = v_p(\tilde{k}) + 1$. By hypothesis $\tilde{k} \notin X_{m+1}$ and hence

$$v_p(\zeta_K(1-k)) + m \geq inf_l\{v_p(a_l)\} \geq 0.$$

□

This last corollary is the essence of the result by Serre.

Corollary 4.0.6. *Let*

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

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

(1) *the $a_n^{(i)}$ converge uniformly to a number $a_n \in \mathbb{Q}_p$ for $n \geq 1$,*
(2) *the $k^{(i)}$ converge in X to a limit k.*

Then the $a_0^{(i)}$ converge to a limit $a_0 \in \mathbb{Q}_p$ and the series

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

is a p-adic modular form of weight k.

4.1. **Examples.** Using this result we may construct the first example of p-adic modular form.

Recall the definition of the Eisenstein series of weight k:

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

Consider now a sequence $(k_i)_i$ of even numbers converging p-adically to a number $k \in X$ and such that $|k_i| \to \infty$, where $|\cdot|$ denotes the archimedean norm. Then we have that $d^{k_i-1} \to 0$ if $p|d$ and

$$d^{k_i-1} \to d^{k-1}, \qquad \text{if } (p,d) = 1.$$

Hence it follows that

$$\sigma(n)_{k_i-1} \to \sigma^*_{k-1}(n) := \sum_{\substack{d|n \\ (d,p)=1}} d^{k-1},$$

p-adically and *uniformly in* n. We have obtained the following: the $\sigma_{k_i-1}(n)$ are the coefficients of index $i \geq 1$ of the Eisenstein series

$$G_{k_i} = -\frac{b_{k_i}}{2k_i} + \sum_{n\geq 1}^{\infty} \sigma_{k_i-1}(n) q^n.$$

We apply hence Corollary (4.0.6) and obtain that the G_{k_i} converge to a p-adic modular form of weight k:

$$G_k^* = a_0 + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n) q^n,$$

(where a_0 is the limit of the Bernoulli number, which exists by Corollary (4.0.6)). Clearly this limit does not depend on the choice of (k_i). We call this the *p-adic Eisenstein series of weight k.*

I would like to underline another important consequence of this result. I recall that the Bernoulli numbers are related to the zeta function in the following way:

$$-\frac{b_{k_i}}{2k_i} = \frac{1}{2}\zeta(1-k_i).$$

The result above tells us that the series $\zeta(1-k_i)$ has p-adic limit. This defines a function ζ^* on the odd elements of $X - \{1\}$.

Theorem 4.1.1 (Serre)**.** *In fact ζ^* is the Kubota-Leopoldt p-adic zeta function ζ_p. More precisely*

(1) *If $p \neq 0$ and if (s,u) is an odd element of $X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ different from* 1*, we have*
$$\zeta^*(s,u) = L_p(s;\omega^{1-u}),$$
(2) *if $p = 2$ and s is an idd element of Z_2 different from* 1*, one has*
$$\zeta^*(s) = L_2(s,\chi^0).$$

This results holds on the principles on the base of p-adic interpolation of L-fuctions, found by Kubota and Leopoldt.

5. The Kubota-Leopoldt p-adic L-function

We followed mainly Iwasawa's book [Iwa].

5.1. **What does interpolation mean?** Suppose we have a function

$$f : \mathbb{Z} \to \mathbb{R},$$

find a *continuous* function $F : \mathbb{R} \to \mathbb{R}$ such that $F(n) = f(n)$ for every $n \in \mathbb{Z}$. There are of course many ways of doing that (it means essentially connecting the dots). This has to do with the fact that $\mathbb{Z}$ is discrete in the reals. Already with the rationals it's different.

It is easy to see that p-adic interpolation is a richer fenomenon: given $f : \mathbb{Z} \to \mathbb{Z}_p$ continuous we look for $F : \mathbb{Z}_p \to \mathbb{Z}_p$ extending f. F will have to satisfy some continuity properties:it has to do with the fact that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$(for instance it will have to map 1 and $1 + p^{1000000}$ very close together).

5.2. **The normed space P_K.** Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and for an elements $\xi \in \overline{\mathbb{Q}}_p$ denote by $|\xi|$ the absolute value normalized so that $|p| = p^{-1}$. The topology induced on $\mathbb{Q}_p$ is of course the p-adic topology. Consider $\mathbb{Q}_p \subset K \subset \overline{\mathbb{Q}}_p$ a finite extension and denote by $K[[x]]$ the algebra of formal power series with coefficients in K. Recall that $A = \sum_{n \geq 0} a_n x^n$ converges at ξ if and only if $|a_n \xi^n| \to 0$ as $n \to \infty$.

This is the general idea. We want to interpolate power series..

Lemma 5.2.1 (Unicity). *Let $A(x), B(x) \in K[[x]]$, convergent in a neighbourhood of $0 \in \overline{\mathbb{Q}}_p$. Suppose that there exists a sequence $\xi_n \neq 0, n \geq 0$ in $\overline{\mathbb{Q}}_p$, with $\lim_{n \to 0} \xi_n = 0$ such that*

$$A(\xi_n) = B(\xi_n).$$

Then

$$A(x) = B(x).$$

Proof. Let

$$A(x) - B(x) = \sum_n c_n \in K[[x]],$$

and suppose by absurd $A(x) \neq B(x)$. Denote by n_0 the smallest natural such that $c_{n_0} \neq 0$. Then one has

$$-c_{n_0} = \xi_i \sum_{n > n_0} c_n \xi_i^{n - n_0 - 1}$$

for every i. Since $\xi_i \to 0$ for $i \to \infty$, and since, by hp, the sum on the right is bounded, we get the contradiction

$$c_{n_0} = 0.$$

□

For any $A = \sum a_k x^k \in K[[x]]$, we set the sup-norm $\|A\| = \sup_k |a_k|$. Denote by P_K the K-subalgebra of power series $A(x)$ such that $\|A\| < \infty$. Note that $\| \cdot \|$ defines a norm on P_K, which is complete with respect to it.

Definition 5.2.2. *For $n \geq 0$ we define through the Newton Binomial a polynomial in $K[x]$:*

$$\binom{x}{n} = \frac{x!}{n!(x-n)!}.$$

One has (see [Iwa, Lemma 3, Chap. 3])

$$\left\|\binom{x}{n}\right\| \leq \left|\frac{1}{n!}\right| \leq |p|^{-\frac{n}{p-1}}.$$

Let (b_n) be a sequence K, and put

$$c_n = \sum_i^n (-1)^{n-i}\binom{n}{i} b_i.$$

Since $\frac{c_n}{n!} = \sum_{i=0}^n (-1)^{n-i} \frac{1}{i!(n-i)!} b_i$ one has

$$e^{-t}\sum_{n=0}^{\infty} b_n \frac{t^n}{n!} = \sum_{n=0}^{\infty} c_n \frac{t^n}{n!}.$$

Then it follows that $c_n \in K, n \geq 0$ and that

$$b_n = \sum_i^n \binom{n}{i} c_i.$$

With this notations we have

Lemma 5.2.3 (Interpolation)**.** *Let $0 < r < |p|^{\frac{1}{p-1}}$ and $|c_n| \leq Cr^n$, for some $C > 0$. Then there exists a unique $A \in P_K$ convergent for $\xi < \delta = \frac{|p|^{\frac{1}{p-1}}}{r}$ such that for all n*

$$A(n) = b_n.$$

Proof. Put $A_k(t) = \sum_{i=0}^k \binom{t}{i} c_i \in P_K$. Of course

$$A_k(n) = b_n, \forall n \geq 0.$$

Using the estimate on the Newton binomial:

$$\left|c_i\binom{t}{i}\right| \leq |c_i|\left|\frac{1}{i!}\ \right| \leq |c_i||p|^{\frac{-i}{p-1}} \leq Cr_i(|p|)^{\frac{-i}{p-1}} = C\delta^{-i}.$$

Hence

$$\|A_j - A_{k-1}\| \leq \max_{k\leq i\leq j} \left\|c_i\binom{t}{i}\right\| \leq C\delta^{-k}. \tag{5.1}$$

Since by hypothesis $\delta^{-1} < 1$, it follows that (A_k) is Cauchy and hence convergent to an $A \in P_K$ with respect to the sup-norm, since P_K is complete. We need to verify that such an A converges for ξ such that $|\xi| < \delta$. Put $A := \sum a_j t^j$ and $A_k := \sum a_{j,k} t^j$ with $a_{j,k} \to a_j$. By definition, A_k is a polynomial of degree k, and hence $a_{k,k-1} = 0$, whenever $j \geq k$, therefore

$$|a_{j,k}| = |a_{j,k} - a_{k,k-1}| \leq \|A_j - A_{k-1}\| \leq C\delta^{-1}.$$

Hence for $j \to \infty$ one has that

$$|a_k| \leq C\delta^{-k}.$$

Hence $A(\xi)$ converges for $|\xi| < \delta$.
If we show now that for a fixed ξ such that $|\xi| < \delta$ one has $A_k(\xi) \to A(\xi)$ we are done. For any k, put

$$A(\xi) - A_k(\xi) = \sum b_{j,k}\xi^j,$$

where of course $b_{j,k} = a_j - a_{j,k}$. To prove our claim it is enough to show that $\sup_j |b_{j,k}\xi^k| \to 0$. We will distinguish two cases.
If $j > k$, then $|b_{j,k}\xi^j| = |a_j\xi^j| \le C(\delta^{-1}|xi|)^j \le C(\delta^{-1}|\xi|)^k$. If on the other hand $j \le k$: $|b_{j,k}\xi^j| \le \|A - A_k\||\xi^j| \le C\delta^{-(k+1)}|\xi^j| \le C(\max\{\delta^{-1}, \delta^{-1}|\xi|\}^k$. Hence in any case

$$\sup_j |b_{j,k}\xi^j| \le C(\max\{\delta^{-1}, \delta^{-1}|\xi|\}^k.$$

□

5.2.1. *Generalized Bernoulli numbers.* Recalls on Dirichlet characters:

Definition 5.2.4. *Let n be a positive integer. A function*

$$\chi : \mathbb{N} \to \mathbb{C}$$

is called a Dirichlet character *of modulus n if*

(1) *$\chi(a)$ depends only on the class of a mod n,*
(2) *χ is completely multiplicative,*
(3) *$\chi(a) \neq 0$ if and only if $(a, n) = 1$.*

The notion of primitive character and conductor are particularly important.

Definition 5.2.5. *A Dirichlet character χ mod n is* primitive *if it is not induced by any Dirichlet character of modulus $m|n$. We say that χ is* induced *by $\tilde{\chi}$ modulus m if*

$$\chi(a) = \tilde{\chi}(a) \text{ if } (a, n) = 1, \chi(a) = 0 \text{ otherwise.}$$

Recall the definition of the classical Bernoulli numbers: we are given a function

$$F(t) = \frac{te^t}{e^t - 1},$$

and this can be expanded into a power series of t:

$$F(t) = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

One may generalize the above definition as follows: given a Dirichlet character χ of conductor $f = f_\chi$ we define

$$F_\chi(t) = \sum_{a=1}^{f} \frac{\chi(a)e^{at}}{e^{ft} - 1}, \qquad F_\chi(t, x) = F_\chi(t)e^{tx} = \sum_{a=1}^{f} \chi(a)\frac{te^{(a+x)t}}{e^{ft} - 1};$$

expanding these into power series of t one has

$$F_\chi(t) = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}, \qquad F_\chi(t, x) = \sum_{n=0}^{\infty} B_{n,\chi}(x)\frac{t^n}{n!}.$$

The generalized Bernoulli numbers satisfy the following relations

$$B_{n,\chi}(x) = \sum_{i=0}^{n} \binom{n}{i} B_{i,\chi} x^{n-i}, \qquad n \geq 0, \tag{5.2}$$

$$\sum_{a=1}^{kf} \chi(a) a^n = \frac{1}{n+1} \{B_{n+1,\chi}(kf) - B_{n+1,\chi}\}. \tag{5.3}$$

This gives us a somehow p-adic characterization of Bernoulli numbers: set

$$S_{n,\chi}(x) = \frac{1}{n+1}(B_{n+1,\chi}(x) - B_{n+1,\chi}).$$

We know that for $n \geq 0$, $B_{n,\chi}$ are algebraic numbers in $\mathbb{Q}(\chi)$. Fixed a prime p, we may consider them as elements in $\mathbb{Q}_p(\chi)$. One has the following result:

Lemma 5.2.6. *In* $\mathbb{Q}_p(\chi)$

$$B_{n,\chi} = \lim_{h \to \infty} \frac{1}{p^h f} S_{n,,\chi}(p^h f).$$

Proof. Note that we have

$$S_{n,\chi}(p^h f) = \frac{1}{n+1}(B_{n+1,\chi}(p^h f) - B_{n+1,\chi}) \equiv B_{n,\chi} \bmod p^{2h}.$$

Indeed, by the property shown above:

$$B_{n+1,\chi}(x) = B_{n+1,\chi} + (n+1) B_{n,\chi} x \bmod (x^2).$$

□

Why are these numbers important? Recall that we are interested in values of L-functions at negative integers.

Theorem 5.2.7. *For any Dirichlet character* χ *and for any* $n \geq 1$

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

For a proof, see [Iwa, Theorem 1, Chap. 2].

5.3. **Definition of the p-adic L-function.** Let χ be a Dirichlet character of conductor f and $K = \mathbb{Q}_p(\chi)$. Consider $\omega : \mathbb{Z} \to \mathbb{C}$ a fixed embedding of the Teichmueller character in $\mathbb{C}$.

Let U is the multiplicative group of all p-adic units. ($p \neq 2$) Topologically it is a direct product $U = V \times D$, where $D = \{1 + pa\}, a \in \mathbb{Z}_p$ and V is a finite cycliic group of order $(p-1)$ ($(p-1)$ roots of unity of $\mathbb{Q}_p$). Each $a \in U$ can be written uniquely i the form

$$a = \omega(a) < a >,$$

(they are the various projections). By putting $\omega(a) = 0$ when $(a,p) \neq 1$, we define a Dirichlet character of conductor p.

Recall that for any n we may define the twisted character

$$\chi_n(a) = \chi(a) \omega^{-n}(a).$$

Let

$$b_n = (1 - \chi_n(p) p^{n-1}) B_{n,\chi_n}$$

and

$$c_n = \sum_{i=0}^{n} \binom{n}{i} b_i (-1)^{n-i}.$$

Lemma 5.3.1. *For any $n \geq 0$ one has that with the notation above*

$$|c_n| \leq \frac{1}{|p^2 f|} |p|^n.$$

Proof. We will use the stated properties on generalized Bernoulli numbers.

$$\begin{aligned} B_{n\chi_n} = \lim_{h\to\infty} \frac{1}{p^h f_n} S_{n,\chi_n}(p^h f_n) &= \lim_{h\to\infty} \frac{1}{p^h f} S_{n,\chi_n}(p^h f) \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{a=1}^{p^h f} \chi_n(a) a^n. \end{aligned}$$

We obtain hence a description for b_n:

$$\begin{aligned} (1-\chi_n(p)p^{n-1})B_{n,\chi_n} &= B_{n,\chi_n} - \lim_{h\to\infty} \frac{\chi_n(p)p^{n-1}}{p^{h-1}f} \sum_{a=1}^{p^{h-1}f} \chi_n(a)a^n \\ &= \lim_{hto\infty} \frac{1}{p^h f} \sum_{c=1}^{p^h f} \chi(c)c^n - \lim_{h\to\infty} \frac{1}{p^h f} \sum_{a=1}^{p^{h-1}f} \chi_n(ap)(ap)^n \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \chi_n(a)a^n = \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \chi(a)\langle a\rangle^n. \end{aligned}$$

And hence, by definition of c_n

$$\begin{aligned} c_n &= \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \chi(a)\langle a\rangle^i = \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \chi(a) \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} \langle a\rangle^i \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \chi(a)(\langle a\rangle - 1)^n = \lim_{h\to\infty} \frac{1}{p^h f} c_n(h). \end{aligned}$$

<u>Claim</u>: $c_n(h) \equiv 0 \bmod p^{n+h-2}$. (See [Iwa, Lemma 4, Chap. 3] for a proof,)

Then $c_n(h) = p^{h+n-2}\theta_n(h)$, where $|\theta_n(h)| \leq 1$ and henve

$$|c_n| = \lim_{h\to\infty} \frac{1}{|p^h f|} |p^{h+n-2}\theta_n(h)| \leq \frac{1}{|p^2 f|} |p^n|.$$

□

From this we obtain the following

Corollary 5.3.2. *There exists $A_\chi \in K[[T]]$ convergent $\zeta < |p|^{-\frac{1}{p-1}}$ such that*

$$A_\chi(n) = (1-\chi_n(p)p^{n-1})B_{n,\chi_n}.$$

Proof. One needs to apply the Interpolation Lemma with $r = |p|, C = \frac{1}{|p^2 f|}$. □

Theorem 5.3.3 (Kubota-Leopoldt)**.** *There exists a p-adic meromorphic function $L_p(s,\chi)$ with the following properties:*

(1)
$$L_p(s,\chi) = \frac{a_{-1}}{s-1} + \sum_{n=0}^{\infty} a_n (s-1)^n, \qquad a_n \in \mathbb{Q}_p(\chi),$$
where
$$a_{-1} = 1 - \frac{1}{p}, \text{ if } \chi = \chi^0, \qquad a_{-1} = 0, \text{ if } \chi \neq \chi^0$$
and where the power series converges in the domain
$$\{s \in \Omega_p \mid |s-1| < r,\ r = |p|^{\frac{1}{p-1}} |q|^{-1} > 1\}.$$

(2) *For $n \geq 1$ one has*
$$\begin{aligned} L_p(1-n,\chi) &= -(1-\chi_n(p)p^{n-1})\frac{B_{n,\chi_n}}{n} \\ &= (1-\chi_n(p)p^{n-1})L(1-n,\chi_n). \end{aligned}$$

As a p-adic meromorphic function defined on the domain defined above, $L_p(s,\chi)$ is completely characterized by these two properties.

Proof. Let
$$L_p(s,\chi) = \frac{1}{s-1} A_\chi(1-s)$$
as above. The uniqueness follows from the unicity Lemma. The value of a_{-1} follows from [Iwa, Theorem 2, Chap. 2]. □

We call $L_p(s,\chi)$ the p-adic L-function for the Dirichlet character χ.

5.3.1. *Conclusion.* We want hence to prove the result by Serre.

Theorem 5.3.4 (Serre)**.** *In fact ζ^* is the Kubota-Leopoldt p-adic zeta function ζ_p. More precisely*

(1) *If $p \neq 0$ and if (s,u) is an odd element of $X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ different from* 1*, we have*
$$\zeta^*(s,u) = L_p(s;\omega^{1-u}),$$
(2) *if $p = 2$ and s is an idd element of Z_2 different from* 1*, one has*
$$\zeta^*(s) = L_2(s,\chi^0).$$

I recall that $L_p(s,\chi)$ is a p-adic meromorphic function such that for $n = 1,2,3,\dots$
$$L_p(1-n,\chi) = (1-\chi_n(p)p^{n-1})(-\frac{B_{n,\chi_n}}{n}).$$
Denote by ζ' the function
$$(s,u) \mapsto L_p(s,\omega^{1-u}).$$
By results of Iwasawa, ζ' is continuous and for k even, positive.
$$\zeta'(1-k) = (1-p^{k-1})\zeta(1-k).$$
Indeed: $\omega_k^k(p) = 1$ (primitive character..). Now, if $k \in 2X$, different from 0 and if (k_i) is a sequence converging to k it follows that
$$\zeta'(1-k) = \lim_{i\to\infty} \zeta'(1-k_i) = \lim_{i\to\infty}(1-p^{k_i-1})\zeta(1-k_i).$$

Now, since $|k_i| \to \infty$, we have that $(1 - p^{k_i - 1})$ tends p-adicaly to 1 and hence

$$\zeta'(1-k) = \zeta^*(1-k).$$

The results really holds on the *unicity result*.

References

[Iwa] K. Iwasawa, *Lectures on p-adic L-functions.* Annals of Mathematics Studies, No. 74, Princeton University Press, N.J., 1972

[Katz] N. Katz, *p-adic properties of modular schemes and modular forms.* Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 101-268. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[Ser1] J.P. Serre, *Formes modulaires et fonctions zêta p-adiques.* Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 101-268. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[Ser2] J.P. Serre, *Congruences et formes modulaires [d'après H.P.F. Swinnerton Dyer].* Séminaire Bourbaki, 24e année (1971/1072), Exp. No. 416, pp.319-338. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[SD] H.P.F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms.* Modular functions in one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1-55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.