# An Introduction to $p$-adic $L$-functions – Bonus Exercises

*The following longer series of exercises go through aspects of the theory we didn't have time to cover in the lectures.*

### Generalising to $p$-adic $L$-functions over number fields

In this series of exercises, we see why the interpretation of $p$-adic $L$-functions as measures on Galois groups provides the most natural generalisation of these ideas to other number fields.

***Exercise 1.*** — Show that $F_\infty = \mathbf{Q}(\mu_{p^\infty})$ is the maximal abelian extension of $\mathbf{Q}$ unramified outside $p$.

Hence the $p$-adic zeta function can be seen as a measure on the Galois group of the maximal abelian extension of $\mathbf{Q}$ unramified outside $p$. The same is true of other arithmetic objects over $\mathbf{Q}$; for example, the $p$-adic $L$-function of a rational elliptic curve will also be a measure on this Galois group.

Suppose now we have an arithmetic object defined over a number field $K$ (for example, the Dedekind zeta function of $K$ or an elliptic curve over $K$). The $p$-adic $L$-function of this object should be a measure on the Galois group $\mathrm{Gal}(K^{\mathrm{ab},p}/K)$, where $K^{\mathrm{ab},p}$ is the maximal abelian extension of $K$ unramified outside primes above $p$. In this series of exercises, we examine the structure of this space. First, we interpret the rational case in terms of ideles.

***Exercise 2.*** — Prove directly that there is an isomorphism

$$\mathcal{G} := \mathrm{Gal}(F_\infty/\mathbf{Q}) \cong \mathbf{Q}^\times\mathbf{R}_{>0}\backslash\mathbf{A}_{\mathbf{Q}}^\times/U(p^\infty),$$

where $\mathbf{A}_{\mathbf{Q}}^\times$ is the ring of ideles defined in the introduction of the lecture notes and $U(p^\infty)$ is the open compact subgroup

$$U(p^\infty) := \big\{(x_2, x_3, x_5, ...) \in \prod_{\ell \text{ prime}} \mathbf{Z}_\ell^\times : x_p = 1\big\}.$$

The double quotient on the right hand side is called the *narrow ray class group of* $\mathbf{Q}$ *of conductor* $p^\infty$. This isomorphism is a special case of a general fact of class field theory; more generally, if $K$ is a number field, the Artin symbol induces an isomorphism

$$\mathrm{Gal}(K^{\mathrm{ab},p}/K) \cong K^\times K_\infty^+\backslash\mathbf{A}_K^\times/U(p^\infty),$$

where now:

– $\mathbf{A}_K^\times$ is the idele ring of $K$ from the introduction to the lecture notes.

– $K_\infty^+$ is the connected component of 1 in $(K\otimes\mathbf{R})^\times$. It is isomorphic to $\mathbf{R}_{>0}^{r_1}\times(\mathbf{C}^\times)^{r_2}$, where $r_1$ is the number of real places and $r_2$ the number of complex places of $K$.

– We define

$$U(p^\infty) = \big\{(x_v)_{v \text{ finite}} : x_{\mathfrak{p}} = 1 \text{ for all } \mathfrak{p}|p\big\}$$
$$\subset \widehat{\mathscr{O}}_K^\times := \prod_{v \text{ finite}} \mathscr{O}_{K,v}^\times.$$

Naturally, the double quotient in this isomorphism is the *narrow ray class group of* $K$ *of conductor* $p^\infty$, denoted $\mathrm{Cl}_K^+(p^\infty)$.

We've proved that when $K = \mathbf{Q}$, this all collapses to just give $\mathbf{Z}_p^\times$. We get this simple description because

(a) The class group of $\mathbf{Q}$ is trivial, and
(b) The totally positive units of $\mathbf{Q}$ are trivial.

We'll first look at the class group.

***Exercise 3.*** — To an idele $x = (x_v)_v \in \mathbf{A}_K^\times$, we associate a fractional ideal

$$I(x) = \prod_{\mathfrak{p} \text{ prime of } K} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})},$$

noting that this is a finite product. Show that this identification induces an isomorphism

$$\mathrm{Cl}_K^+ \cong K^\times K_\infty^+ \backslash \mathbf{A}_K^\times / \widehat{\mathscr{O}}_K^\times,$$

where $\mathrm{Cl}_K^+$ is the narrow class group of $K$, that is, the group of fractional ideals modulo principal ideals with a totally positive generator. (It is conceptually easier to replace $K_\infty^+$ with $K_\infty = (K \otimes \mathbf{R})^\times$, and we then get the regular class group).

***Exercise 4.*** — Using the above, deduce that there is a decomposition

$$\mathbf{A}_K = \bigsqcup_{i \in \mathrm{Cl}_K^+} K^\times \cdot K_\infty^+ \cdot a_i \widehat{\mathscr{O}}_K^\times,$$

where $a_i$ is an idele which is trivial at infinite places and where $I(a_i)$ is a representative of the $i$th class of $\mathrm{Cl}_K^+$. This formula is the analogue of strong approximation for $K$ (Proposition 1.11 in the notes).

***Exercise 5.*** — Let $n \geq 0$, and define

$$\begin{aligned} U(p^n) &= \{(x_v)_{v \text{ finite}} : x_p \equiv 1 \pmod{p^n}\} \\ &\subset \widehat{\mathscr{O}}_K^\times, \end{aligned}$$

where $x_p = (x_\mathfrak{p})_{\mathfrak{p}|p} \in (\mathscr{O}_K \otimes \mathbf{Z}_p)^\times$ is the component at $p$. Define

$$\mathrm{Cl}_K^+(p^n) := K^\times K_\infty^+ \backslash \mathbf{A}_K^\times / U(p^n).$$

Show that there is an exact sequence

$$0 \to \mathscr{O}_{K,+}^\times \longrightarrow (\mathscr{O}_K \otimes_\mathbf{Z} \mathbf{Z}_p)^\times \longrightarrow \mathrm{Cl}_K^+(p^n) \longrightarrow \mathrm{Cl}_K^+ \to 0,$$

where $\mathscr{O}_{K,+}^\times$ denotes the totally positive global units of $K$.

***Exercise 6.*** — Hence deduce that there is an exact sequence

$$0 \to \overline{\mathscr{O}_{K,+}^\times} \longrightarrow (\mathscr{O}_K \otimes_\mathbf{Z} \mathbf{Z}_p)^\times \longrightarrow \mathrm{Cl}_K^+(p^\infty) \longrightarrow \mathrm{Cl}_K^+ \to 0,$$

where the overline on the first term denotes $p$-adic completion.

Thus we can decompose $\mathrm{Gal}(K^{\mathrm{ab},p}/K)$ as a disjoint union of $h^+$ copies of the quotient $(\mathscr{O}_K \otimes \mathbf{Z}_p)^\times / \overline{\mathscr{O}_{K,+}^\times}$, where $h^+$ is the narrow class number of $K$.

***Remark 0.1.*** — The point of this exercise is to illustrate the difficulty in generalising the notion of $p$-adic $L$-functions without using Galois theory and class field theory. In particular, suppose we have an arithmetic object defined over $K$. Its $p$-adic $L$-function should be a measure on $\mathrm{Gal}(K^{\mathrm{ab},p}/K)$, which we can view as a collection of measures on $(\mathscr{O}_K \otimes \mathbf{Z}_p)^\times$ modulo global units, or as a collection of analytic functions on $\mathscr{O}_K \otimes \mathbf{Z}_p$, each indexed by a class group. It turns out to be much nicer to work adelically and sidestep the issue of breaking things up over class groups.

***Remark 0.2.*** — To get a flavour of the above, it might be easier to take $K$ an imaginary quadratic field, and then the 'totally positive' parts disappear. In this case, we are dealing with regular class groups and regular unit groups.

## Constructing the Kubota–Leopoldt $p$-adic $L$-function using Bernoulli polynomials

The aim of this series of exercises is to prove a theorem of Washington, giving a formula (and an alternative construction) for the $p$-adic zeta function in terms of Bernoulli polynomials. Recall that the Bernoulli numbers $B_n$ are defined by the identity

$$\frac{t}{e^t-1}=\sum_{n=0}^{+\infty}B_n\frac{t^n}{n!}$$

and, more generally, for any Dirichlet character $\chi\colon(\mathbf{Z}/D\mathbf{Z})^\times\to\mathbf{C}^\times$ of conductor $D$, the generalized Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{D}\chi(a)\frac{te^{at}}{e^{Dt}-1}=\sum_{n=0}^{+\infty}B_{n,\chi}\frac{t^n}{n!}.$$

In the same spirit, define the Bernoulli polynomials $B_n(X)$ by

$$\frac{te^{Xt}}{e^t-1}=\sum_{n=0}^{+\infty}B_n(X)\frac{t^n}{n!}.$$

***Exercise 7.*** — (1) Show that $B_n(1-X)=(-1)^nB_n(X)$.

(2) Show that

$$B_n(X)=\sum_{k=0}^{n}\binom{n}{k}B_kX^{n-k}.$$

(3) Show that, for any $F$ such that $D|F$,

$$B_{n,\chi}=F^{n-1}\sum_{a=1}^{F}\chi(a)B_n(\frac{a}{F}),$$

and deduce that $B_{1,\chi}=D^{-1}\sum_{a=1}^{D}\chi(a)a$ for any $\chi\neq 1$.

(4) Show that $B_{n,\chi}=0$ whenever $\chi$ is odd (i.e. $\chi(-1)=-1$) (resp. even) and $n$ is even (resp. odd).

For any integers $F\geq 1$, $0\leq a<F$ and $s$ a complex variable, let

$$\zeta_{a,F}(s):=\sum_{n=0}^{+\infty}(a+Fn)^{-s}.$$

***Exercise 8.*** —
Show that, for all $n\geq 1$,

$$\zeta_{a,F}(1-n)=-F^{n-1}\frac{B_n(\frac{a}{F})}{n}.$$

Let

$$\zeta_{p,a,F}(s)=\frac{1}{s-1}F^{-1}\langle a\rangle^{1-s}\sum_{k=0}^{+\infty}\binom{1-s}{k}\cdot B_k\cdot(F/a)^k. \tag{1}$$

(note that the $B_k$ appearing here is a Bernoulli number and not a polynomial!).

***Exercise 9.*** — Show that, for all $k\geq 2$ even and every prime $\ell$, $\ell B_k$ is $\ell$-integral (hint: use points (2) and (3) of Exercise 7 with $\chi=1$ and $F=p$).

***Exercise 10.*** — (1) Suppose that $p|F$ and that $(a,p)=1$. Show that the series (1) above converges and defines a meromorphic function on $\{s\in\mathbf{C}_p\,|\,v_p(s)\geq 0\}$ with a single simple pole at $s=1$ with residue $1/F$.

(2) Show that the $p$-adic function $\zeta_{p,a,F}(s)$ satisfies the interpolation property

$$\zeta_{p,a,F}(1-n) = \omega^{-n}(a)\zeta_{a,F}(1-n) \text{ for every } n \geq 1.$$

Deduce that $\zeta_{p,a,F}(1-n) = \zeta_{a,F}(1-n)$ for every $n \geq 1$ such that $p-1|n$.

We are going to use the functions $\zeta_{p,a,F}(s)$ to recover the $p$-adic zeta function. Let $F$ be divisible by $p$ and $D$ and define

$$L'_p(\chi, s) := \frac{1}{s-1} F^{-1} \sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a)\langle a \rangle^{1-s} \sum_{k=0}^{+\infty} \binom{1-s}{k} \cdot B_k \cdot (F/a)^k.$$

***Exercise 11.*** — (1) Show that the series converges in $\{s \in \mathbf{C}_p \mid v_p(s) \geq 0\}$ and defines analytic function except when $\chi = 1$ and $s = 1$, where it has a simple pole.

(2) Show that, for every $n \geq 1$, we have the following interpolation property:

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

Deduce that $L'_p(\chi, s) = L_p(\chi\omega^{-1}, s)$, where the right hand term denotes the Mellin transform of the measure $\mu_\chi$ defined in the lecture notes.

## Constructing the Kubota–Leopoldt $p$-adic $L$-function using Bernoulli distributions

***Exercise 12.*** — Recall the definition of the Bernoulli polynomials given above.

(1) Show that, if $k \geq 1$, then $B_k(X)$ is the unique polynomial of degree $k$ verifying the following identities

$$B_k(X+1) - B_k(X) = kX^{k-1} \quad ; \quad \sum_{i=0}^{d-1} B_k(X + i/d) = d^{1-k} B_k(dX) \text{ for any } d \geq 1.$$

(2) If $x \in \mathbf{Q}_p$, define $\{x\} \in \mathbf{Z}[\frac{1}{p}] \cap [0,1)$ as the unique element such that $x - \{x\} \in \mathbf{Z}$. Show that, for any $a \in \mathbf{Z}_p^\times$, the formula

$$\lambda_a(i + p^n\mathbf{Z}_p) := B_1\big(\{\frac{i}{p^n}\}\big) - aB_1\big(\{\frac{a^{-1}i}{p^n}\}\big), \quad i \in \mathbf{Z}_p, n \in \mathbf{N}$$

defines a measure on $\mathbf{Z}_p$.

(3) Show that, for every $k, n \in \mathbf{N}$ and $i \in \mathbf{Z}_p$, we have

$$\int_{i+p^n\mathbf{Z}_p} x^k \cdot \mu_a = \frac{p^{nk}}{k+1}\Big(B_{k+1}\big(\{\frac{i}{p^n}\}\big) - a^{k+1}B_{k+1}\big(\{\frac{a^{-1}i}{p^n}\}\big)\Big).$$

(4) Let $\mu \in \mathscr{M}(\mathbf{Z}_p, \mathscr{O}_L)$ be any $\mathscr{O}_L$-valued measure. Show that, for any integers $k \geq 1$ and $n_1, n_2 \geq k$ such that $n_1 \equiv n_2 \pmod{(p-1)p^{k-1}}$, we have

$$v_p\left(\int_{\mathbf{Z}_p} x^{n_1} \cdot \mu - \int_{\mathbf{Z}_p} x^{n_2} \cdot \mu\right) \geq k.$$

(5) Write $\int_{\mathbf{Z}_p^\times} x^k \cdot \lambda_a$ in terms of $B_k(0)$ and deduce Kummer's congruences between Bernoulli numbers. Conclude also that $\lambda_a = \mu_a$, where $\mu_a$ is the measure, whose Amice transform is $\frac{1}{T} - \frac{a}{(1+T)^a - 1}$, used to define the $p$-adic zeta function.

Joaquín Rodrigues Jacinto, University College of London • *E-mail :* ucahrod@ucl.ac.uk
Chris Williams, Imperial College • *E-mail :* christopher.williams@imperial.ac.uk