Topics in Number theory: Special values of L-functions
Exercise 1 (due on September 26)

Choose 4 out of 8 problems to submit, must including Exercise 1.5 (The problems are chronically ordered by the materials, not necessarily by difficulties. I do recommend to at least read all problems.)

Exercise 1.1 (Gauss sums)**.** Let $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a (not necessarilty primitive) Dirichlet character of conductor $N \geq 2$, we define the Gauss sum of η as follows:

$$G(\eta) := \sum_{a=1}^{N-1} \eta(a) e^{2\pi \mathtt{i} \cdot a/N} \in \mathbb{C}. \tag{1.1.1}$$

Prove the following properties of the Gauss sum.

(1) If η' is another Dirichlet character of conductor N' with $(N, N') = 1$, then $\eta\eta'$ may be viewed as a Dirichlet character of conductor NN'. Show that in this case

$$G(\eta\eta') = \eta(N')\eta'(N)G(\eta)G(\eta').$$

(2) If η is primitive, then $|G(\eta)| = \sqrt{N}$.

(3) When η and η' are both Dirichlet characters of same conductor N such that $\eta\eta'$ is a primitive Dirichlet character of conductor N, show that

$$G(\eta)G(\eta') = G(\eta\eta') \cdot J(\eta, \eta'), \tag{1.1.2}$$

where $J(\eta, \eta')$ is the *Jacobi sum*

$$J(\eta, \eta') := \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \eta(a)\eta'(1 - a),$$

where we use the convention that $\eta(a) = 0$ if $(a, N) \neq 1$.

Remark 1. It would be interesting to compare the Gauss sums with the Gamma functions. In some sense, the definition of (1.1.1) may be viewed as an integral of the product of an additive character $e^{2\pi \mathtt{i}(\cdot)/N}$ of $\mathbb{Z}/N\mathbb{Z}$ and a multiplicative character η of $(\mathbb{Z}/N\mathbb{Z})^\times$. Similarly, the definition of Gamma function

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$$

can also be viewed as an integral of the product of the additive character e^{-t} and the multiplicative character t^s.

Analogous to the relation (1.1.2) between the Gauss sums and the (finite) Jacobi sums, Gamma functions satisfy a similar property: for $s, s' \in \mathbb{C}$

$$B(s, s') = \frac{\Gamma(s)\Gamma(s')}{\Gamma(s + s')},$$

where $B(s, s')$ is a beta function

$$B(s, s') = \int_0^1 t^{s-1}(1 - t)^{s'-1} dt, \qquad (\Re(s) > 0, \Re(s') > 0).$$

Solution. (1) We need to be careful about the precise isomorphism $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N'\mathbb{Z} \cong \mathbb{Z}/NN'\mathbb{Z}$. Then

$$\begin{aligned} G(\eta)G(\eta') &= \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{a' \in (\mathbb{Z}/N'\mathbb{Z})^\times} \eta(a)\eta'(a') e^{2\pi \mathtt{i} \cdot a/N} e^{2\pi \mathtt{i} \cdot a'/N'} \\ &= \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{a' \in (\mathbb{Z}/N'\mathbb{Z})^\times} \eta(a)\eta'(a') e^{2\pi \mathtt{i} \cdot (aN' + a'N)/NN'} \end{aligned}$$

Note that $\eta\eta'(aN' + a'N) = \eta(aN')\eta'(a'N) = \eta(N')\eta'(N)\eta(a)\eta'(a')$. From this, we see that

$$G(\eta)G(\eta')\eta(N')\eta'(N) = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{a' \in (\mathbb{Z}/N'\mathbb{Z})^\times} \eta\eta'(aN' + a'N) e^{2\pi \mathtt{i} \cdot (aN' + a'N)/NN'} = G(\eta\eta').$$

(2) Using (1), we may immediately reduce to the case when $N = p^r$ is a power of a prime p. Now we compute

$$\begin{aligned} G(\eta)\overline{G(\eta)} &= \sum_{a,b \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \eta(a) e^{2\pi \mathtt{i} \cdot a/p^r} \bar{\eta}(b) e^{-2\pi \mathtt{i} \cdot b/p^r} \\ &= \sum_{a,b \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \eta(ab^{-1}) e^{2\pi \mathtt{i} \cdot (a-b)/p^r} \\ &\overset{a=bc}{=} \sum_{b,c \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \eta(c) e^{2\pi \mathtt{i} \cdot b(c-1)/p^r}. \end{aligned} \tag{1.1.3}$$

Now the valuation $v_p(c-1) = s$ matters.

- When $s < r-1$,

$$\sum_{b \in (\mathbb{Z}/p^r\mathbb{Z})^\times} e^{2\pi \mathtt{i} \cdot (c-1)b/p^r} = \sum_{b \in (\mathbb{Z}/p^r\mathbb{Z})^\times} e^{2\pi \mathtt{i} \cdot b/p^{r-s}} = -\sum_{b \in p\mathbb{Z}/p^r\mathbb{Z}} e^{2\pi \mathtt{i} \cdot b/p^{r-s}} = -\sum_{b \in \mathbb{Z}/p^{r-1}\mathbb{Z}} e^{2\pi \mathtt{i} \cdot b/p^{r-s-1}} = 0, \tag{1.1.4}$$

  because the sums of all powers of $e^{2\pi \mathtt{i}/p^{r-s+1}}$ and all powers of $e^{2\pi \mathtt{i}/p^{r-s+1}}$ are both zero.
- When $s = r-1$, the same discussion above shows that the sum (1.1.4) is equal to $-p^{r-1}$. Thus, the contribution of these terms to (1.1.3) is

$$\sum_{\substack{c = 1 + dp^{r-1} \\ d = 1, \dots, p-1}} \eta(c) p^{r-1} = (-1) \cdot (-p^{r-1}) = p^{r-1}.$$

- When $c = 1$, the contribution to (1.1.3) is $\#\{b \in (\mathbb{Z}/p^r\mathbb{Z})^\times\} = (p-1)p^{r-1}$.

To sum up, we see that $G(\eta)\overline{G(\eta)} = p^{r-1} + (p-1)p^{r-1} = p^r$.

(3) We first observe that for Dirichlet characters η_1, η_1' of conductor N_1 and η_2, η_2' of conductor N_2 with $(N_1, N_2) = 1$, we have

$$J(\eta_1\eta_2, \eta_1'\eta_2') = J(\eta_1, \eta_1')J(\eta_2, \eta_2').$$

It then follows that we need only to prove (1.1.2) when $N = p^r$ is a power of a prime.

In this case, we compute this directly.

$$G(\eta)G(\eta') = \sum_{a,b\in\mathbb{Z}/p^r\mathbb{Z}} \eta(a)\eta'(b)e^{2\pi\mathrm{i}\cdot(a+b)/p^r} \overset{c=a+b}{=} \sum_{a,c\in\mathbb{Z}/p^r\mathbb{Z}} \eta(a)\eta'(c-a)e^{2\pi\mathrm{i}\cdot c/p^r}$$

$$= \sum_{a\in\mathbb{Z}/p^r\mathbb{Z}} \sum_{c\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \eta(c\cdot \tfrac{a}{c})\eta'(c(1-\tfrac{a}{c}))e^{2\pi\mathrm{i}\cdot c/p^r} + \sum_{a\in\mathbb{Z}/p^r\mathbb{Z}} \sum_{c\in p\mathbb{Z}/p^r\mathbb{Z}} \eta(a)\eta'(c-a)e^{2\pi\mathrm{i}\cdot c/p^r}.$$

The first sum is equal to $G(\eta\eta')J(\eta,\eta')$, whereas for the second sum, we may rewrite it as

$$\sum_{a\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \sum_{c\in p\mathbb{Z}/p^r\mathbb{Z}} \eta\eta'(a)\cdot\eta(\tfrac{c}{a}-1)e^{2\pi\mathrm{i}c/p^r}.$$

If we change a into $a\cdot(1+dp^{r-1})$ for some $d\in\mathbb{Z}$, the second term does not change as $p|c$. But $\eta\eta'$ is a primitive character, so the sum is zero. □

Exercise 1.2 (Modified Mahler basis)**.** In this problem, we give a different orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Z}_p)$. Consider the function $f(z)=\frac{z^p-z}{p}$ on $\mathbb{Z}_p$.

(1) Show that $f\in\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Z}_p)$.

Consider the following inductively defined functions:

$$f^{\langle 0\rangle}(z)=z,\quad f^{\langle 1\rangle}(z)=f(z)=\frac{z^p-z}{p},\quad f^{\langle 2\rangle}(z)=f^{\langle 1\rangle}\Big(\frac{z^p-z}{p}\Big)=\frac{\big(\frac{z^p-z}{p}\big)^p-\frac{z^p-z}{p}}{p},$$

$$f^{\langle k+1\rangle}(z)=f\big(f^{\langle k\rangle}(z)\big),\qquad \text{for } k\geq 1.$$

For $n\geq 0$, write $n=n_0+n_1p+n_2p^2+\cdots$ for the p-adic expansion of n, i.e. each $a_i\in\{0,1,\dots,p-1\}$, put

$$\mathsf{e}_n(z)=\big(f^{\langle 0\rangle}(z)\big)^{n_0}\big(f^{\langle 1\rangle}(z)\big)^{n_1}\big(f^{\langle 2\rangle}(z)\big)^{n_2}\cdots$$

We call $\{\mathsf{e}_n(z)\}$ a *modified Mahler basis.*

(2) Prove that $\mathsf{e}_p(z)+\binom{z}{p}\in\mathbb{Z}_p[z]$.
(3) Prove that each $\mathsf{e}_n(z)$ may be written as a $\mathbb{Z}_p$-linear combination of binomial functions $\binom{z}{m}$'s, and show that the change of basis matrix from the Mahler basis to $\mathsf{e}_n(z)$ is upper triangular with all entries in $\mathbb{Z}_p$ and diagonal entries in $\mathbb{Z}_p^\times$.
(4) Deduce that $\{\mathsf{e}_n(z)\,|\,n\geq 0\}$ form an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Z}_p)$.
(5) Assume that $p\geq 3$. Recall that $\mathbb{Z}_p^\times\cong\mu_{p-1}\times(1+p\mathbb{Z}_p)^\times$, where μ_{p-1} is the subgroup of $(p-1)$th roots of unity in $\mathbb{Q}_p$. The group μ_{p-1} acts naturally on $\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Z}_p)$ such that for $\zeta\in\mu_{p-1}$, it sends $h(z)$ to $h(\zeta z)$. Show that each of $\mathsf{e}_n(z)$ is an eigenfunction for this action.

Remark 2. We call $\mathsf{e}_n(z)$'s the *modified Mahler basis.* As (2) suggested, $\mathsf{e}_n(z)$ is essentially the "leading terms" of $\binom{z}{n}$ up to a constant multiple.

The disadvantage of modified Mahler basis is that it is not compatible with the Amice transform. However, part (5) shows that the modified Mahler basis is formed by μ_{p-1}-eigenfunctions, which is useful in some applications.

Solution. (1) The Fermat's Little Theorem shows that $z^p\equiv z \bmod p$ for $z\in\mathbb{Z}$. Then $f(z)\in\mathbb{Z}_p$ for every $z\in\mathbb{Z}_p$.

(2) We expand $\binom{z}{p}$ as follows.

$$\binom{z}{p} = \frac{z(z-1)\cdots(z-(p-1))}{p!} \in \frac{z^p}{p!} + \frac{z}{p} + \mathbb{Z}_p[z] = -\frac{z^p - z}{p} + \mathbb{Z}_p[z].$$

(3) Since $f(z)$ defines a continuous function $f(z): \mathbb{Z}_p \to \mathbb{Z}_p$, its iteration $f^{\langle k\rangle}$ is also a $\mathbb{Z}_p$-valued continuous function on $\mathbb{Z}_p$, so is each $\mathsf{e}_n(z)$ as a product of these $f^{\langle k\rangle}$'s. In particular, each $\mathsf{e}_n(z)$ is a $\mathbb{Z}_p$-linear combination of $1, z, \dots, \binom{z}{n}$, as its Mahler expansion:

$$\mathsf{e}_n(z) = \sum_{i=0}^{n} m_{ni}\binom{z}{i}, \qquad \text{with } m_{ni} \in \mathbb{Z}_p,$$

where we only need to add up to $\binom{z}{n}$ because $1, z, \dots, \binom{z}{n}$ form a $\mathbb{Q}_p$-basis of $\mathbb{Q}_p[z]^{\deg \le n}$. This way, we have $(\mathsf{e}_0, \mathsf{e}_1, \dots) = (1, z, \binom{z}{2}, \dots)M$ for the change of basis matrix $M = (m_{ij})_{i,j\ge 0}$. Clearly, M has entries in $\mathbb{Z}_p$, and is upper triangular.

To see the diagonal entry of M, it suffices to compare the leading coefficients of $\mathsf{e}_n(z)$ with $\binom{z}{n}$. If $n = n_0 + pn_1 + p^2n_2 + \cdots$, we have

$$\mathsf{e}_n(z) = p^{-(n_1 + (p+1)n_2 + (p^2+p+1)n_3 + \cdots)} z^n + \cdots, \quad \text{and} \quad \binom{z}{n} = \frac{1}{n!}z^n + \cdots$$

It is clear that the two leading coefficients differ by some element of $\mathbb{Z}_p^\times$. Part (3) is proved.

(4) Since M is upper triangular, with all entries in $\mathbb{Z}_p$ and diagonal entries in $\mathbb{Z}_p^\times$, it is integrally invertible, i.e. M^{-1} is also upper triangular, with all entries in $\mathbb{Z}_p$ and diagonal entries in $\mathbb{Z}_p^\times$. This implies that the modified Mahler basis is indeed an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$.

(5) We note that by the inductive definition of $f^{\langle k\rangle}(z)$, the monomials in every $f^{\langle k\rangle}(z)$ have degree $\equiv 1 \bmod p-1$. It then follows that every monomials in $\mathsf{e}_n(z)$ has exponent congruent to $n_0 + n_1 + \cdots$ modulo $p-1$, which is further congruent to n modulo $p-1$. It then follows that for every $\zeta \in \mu_{p-1}$, $\mathsf{e}_n(\zeta z) = \zeta^n \mathsf{e}_n(z)$ for every $n \in \mathbb{Z}_{\ge 0}$, i.e. each modified Mahler basis element is an eigenfunction for the μ_{p-1}-action. □

Exercise 1.3 (Orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$)**.** Let $\mathbb{Q}_{p^r}$ be the unramified extension of $\mathbb{Q}_p$ of degree r, and $\mathbb{Z}_{p^r}$ be its ring of integers. In this exercise, we will produce an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$ similar to the modified Mahler basis defined in the previous exercise.

Let σ denote the (arithmetic) Frobenius on $\mathbb{Z}_{p^r}$, i.e. the automorphism of $\mathbb{Z}_{p^r}$ whose reduction modulo p sends $\bar{x}$ to $\bar{x}^p$. Write $z_0 : \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^r}$ for the identify function, i.e. $z_0(a) = a$. We then inductively define

$$z_{j+1}(a) = \sigma(z_j(a)) \qquad \text{for } j \ge 0.$$

Clearly, $z_{j+r} = z_j$ for $j \ge 0$. It is also clear that $\mathbb{Q}_{p^r}[z_0, \dots, z_{r-1}]$ is a dense subring of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Q}_{p^r})$ (but $\mathbb{Z}_p[z_0, \dots, z_{r-1}]$ is not dense in $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$).

We define inductively

$$f_0 := 1, \quad f_1 := z_0, \quad f_p := \frac{z_0^p - z_1}{p}, \quad f_{p^{i+1}} = f_p \circ f_{p^r} = \frac{f_{p^i}^p - \sigma(f_{p^i})}{p}, \text{ with } i = 1, 2, \dots$$

For example, $f_{p^2} = \dfrac{\left(\frac{z_0^p - z_1}{p}\right)^p - \frac{z_1^p - z_2}{p}}{p}$.

If $m = m_0 + pm_1 + p^2m_2 + \cdots$ is the p-adic expansion of a positive integer (with $s_i \in \{0, \dots, p-1\}$), we set

$$f_m := f_1^{m_0} f_p^{m_1} f_{p^2}^{m_2} \cdots$$

Finally, if $\mathbf{n} = (n_0, \dots, n_{r-1}) \in \mathbb{Z}_{\geq 0}^r$ is an r-tuple of index, we set

$$\mathbf{f_n} := f_{n_0} \cdot \sigma(f_{n_1}) \cdots \sigma^{r-1}(f_{n_{r-1}}). \tag{1.3.1}$$

(1) Show that each function $\mathbf{f_n}$ is a continuous function in $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$, and compute its leading coefficients, as a polynomial in $z_0, \dots, z_{r-1}$.

(2) Show that $\mathbf{f_n}$'s form an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$.

(Hint: it might be helpful to compare this to a "known" (noncanonical) Mahler basis: choose a $\mathbb{Z}_p$-linear isomorphism

$$\begin{aligned} c : \mathbb{Z}_{p^r} &\xrightarrow{\quad\cong\quad} (\mathbb{Z}_p)^r \\ a &\longmapsto (\mathsf{c}_0^*(a), \dots, \mathsf{c}_{r-1}^*(a)). \end{aligned}$$

Here we may view each c_j^* as a function $\mathbb{Z}_{p^r}$ with values in $\mathbb{Z}_p$. Then the functions $\mathbf{u_n} : a \mapsto \binom{\mathsf{c}_0^*(a)}{n_0} \cdots \binom{\mathsf{c}_{r-1}^*(a)}{n_{r-1}}$ for $\mathbf{n} \in \mathbb{Z}_{\geq 0}^r$ form an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$ with respect to the maximal norm $||\cdot||$. It is then a question to compare the two bases $\mathbf{f_n}$ and $\mathbf{u_n}$.)

Solution. (1) We note that for every $a \in \mathbb{Z}_{p^r}$, $a^p \equiv \sigma(a) \bmod p$, so $f_p = \frac{z_0^p - z_1}{p}$ defines a continuous function from $\mathbb{Z}_{p^r}$ to $\mathbb{Z}_{p^r}$. Iteration and multiplication of continuous functions in $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$ still gives continuous function in $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$. It then follows that all $\mathbf{f_n} \in \mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$. Note that for $m = m_0 + pm_1 + p^2m_2 + \cdots$ written in its p-adic expansion, the leading term of f_m is

$$z_0^m \cdot p^{-m_1 - (p+1)m_2 - (p^2+p+1)m_3 - \cdots} = z_0^m \cdot p^{-v_p(m!)}.$$

So for $\mathbf{n} = (n_0, \dots, n_{r-1}) \in \mathbb{Z}_{\geq 0}^r$, the leading term of $\mathbf{f_n}$ is

$$\frac{z_0^{n_0} z_1^{n_1} \cdots z_{r-1}^{n_{r-1}}}{p^{v_p(n_0!) + v_p(n_1!) + \cdots + v_p(n_{r-1}!)}}.$$

(2) In what follows, for $\mathbf{n} = (n_0, \dots, n_{r-1}) \in \mathbb{Z}_{\geq 0}^r$, we write $\mathbf{z^n} = z_0^{n_0} z_1^{n_1} \cdots z_{r-1}^{n_{r-1}}$, and $|\mathbf{n}| = n_0 + n_1 + \cdots + n_{r-1}$.

Keep the notation of c_j and $\mathbf{u_n}$ as given in the hint. Consider the subspace $F_n := \mathbb{Q}_{p^r}[\mathbf{z}]^{\deg \leq n} \subset \mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Q}_{p^r})$ of polynomial functions of total degree $\leq n$ (with $n \in \mathbb{N}$), which has a natural $\mathbb{Q}_{p^r}$-basis given by $\{\mathbf{z^n}\}_{|\mathbf{n}| \leq n}$ and a $\mathbb{Q}_{p^r}$-basis given by $\{\mathbf{f_n}\}_{|\mathbf{n}| \leq n}$. On the other hand, every element in $\{\mathbf{u_n} \mid |\mathbf{n}| \leq n\}$ belongs to F_n and the set is $\mathbb{Z}_{p^r}$-linearly independent; so $\{\mathbf{u_n}\}_{|\mathbf{n}| \leq n}$ also forms a $\mathbb{Q}_{p^r}$-basis of F_n. It then follows that each $\mathbf{f_n}$ with $|\mathbf{n}| \leq n$ is a $\mathbb{Q}_{p^r}$-linear combination and hence also a $\mathbb{Z}_{p^r}$-linear combination of $\{\mathbf{u_n}\}_{|\mathbf{n}| \leq n}$. As this works for all n, the change of basis matrix from $\{\mathbf{f_n}\}$ to $\{\mathbf{u_n}\}$ is a matrix with coefficients in $\mathbb{Z}_{p^r}$ and is block-upper-triangular with blocks labeled by total degree n.

It remains to show that each block component is invertible in $\mathbb{Z}_{p^r}$, or equivalently the change of basis matrix $\mathrm{M}_{\mathbf{f},\mathbf{u}}^{(n)}$ on F_n/F_{n-1} from the basis $\{\mathbf{f_n}\}_{|\mathbf{n}|=n}$ to the basis $\{\mathbf{u_n}\}_{|\mathbf{n}|=n}$ has determinant in $\mathbb{Z}_{p^r}^\times$ (as opposed to just in $\mathbb{Z}_{p^r}$). We have already shown that $\mathrm{M}_{\mathbf{f},\mathbf{u}}^{(n)}$ has entries in $\mathbb{Z}_p$; so it is enough to show that $\det \mathrm{M}_{\mathbf{f},\mathbf{u}}^{(n)} \in \mathbb{Z}_{p^r}^\times$.

The change of basis matrix $\mathrm{M}_{\mathbf{f},\mathbf{z}}^{(n)}$ from $\{\mathbf{f}_{\mathbf{n}}\}_{|\mathbf{n}|=n}$ to $\{\mathbf{z}^{\mathbf{n}}\}_{|\mathbf{n}|=n}$ is the diagonal matrix with $\frac{1}{p^{v_p(\mathbf{n}!)}}$ on the diagonal. On the other hand, the change of basis matrix $\mathrm{M}_{\mathbf{u},\mathbf{z}}^{(n)}$ from $\{\mathbf{u}_{\mathbf{n}}\}_{|\mathbf{n}|=n}$ to $\{\mathbf{z}^{\mathbf{n}}\}_{|\mathbf{n}|=n}$ has its $\mathbf{n}$th column in $\frac{1}{\mathbf{n}!}\mathbb{Z}_{p^r}^{\times}$. As $\mathrm{M}_{\mathbf{f},\mathbf{z}}^{(n)} = \mathrm{M}_{\mathbf{u},\mathbf{z}}^{(n)}\mathrm{M}_{\mathbf{f},\mathbf{u}}^{(n)}$, we deduce that $\det \mathrm{M}_{\mathbf{f},\mathbf{u}}^{(n)} \in \mathbb{Z}_{p^r}^{\times}$. From this, we see that $\mathrm{M}_{\mathbf{f},\mathbf{u}}^{(n)}$ is integrally invertible over $\mathbb{Z}_{p^r}$. Part (2) of the exercise is proved. $\square$

Exercise 1.4 (An explicit formula for ψ-operator)**.** Let p be a prime number. Recall that on $\mathbb{Z}_p[\![T]\!]$, we have defined an operator φ such that $\varphi(T) = (1+T)^p - 1$. There is a left inverse to φ, given as follows: each $F \in \mathbb{Z}_p[\![T]\!]$ can be written uniquely as $F = \sum_{i=0}^{p-1}(1+T)^i\varphi(F_i)$; then $\psi(F) = F_0$.

(1) Let ζ_p denote a primitive p-th root of unity. Prove that the ψ-operator admits the following characterization: for $F \in \mathbb{Z}_p[\![T]\!]$, $\psi(F)$ is the unique power series in $\mathbb{Z}_p[\![T]\!]$ such that

$$\psi(F)((1+T)^p - 1) = \frac{1}{p}\sum_{i=0}^{p-1} F((1+T)\zeta_p^i - 1). \tag{1.4.1}$$

(2) Show that φ and ψ can be naturally extended to the p-adic completion of $\mathbb{Z}_p((T))$, denoted by $\mathbb{A}_{\mathbb{Q}_p}$.

(3) Show that $\psi\Big(\dfrac{1}{T}\Big) = \dfrac{1}{T}$. (One might find (1.4.1) useful, but there is a "better" proof without using it.)

Remark 3. (1) Without going into details, let us simply remark that the actions of φ, ψ, and $\Gamma \cong \mathbb{Z}_p^{\times}$ on $\mathbb{Z}_p[\![T]\!]$ and their extensions to $\mathbb{A}_{\mathbb{Q}_p}$ defines the most important ground ring for (φ,Γ)-modules; this is a very useful tool in studying p-adic Hodge theory of local fields. We will further discuss this in future lectures.

(2) The right hand side of formula (1.4.1) may be viewed as taking the trace from $\mathbb{Z}_p[\![T]\!]$ to $\varphi(\mathbb{Z}_p[\![T]\!])$; it is a (non-étale) Galois extension, and the conjugates of $T+1$ are $\zeta_p^i(T+1)$ for $i = 0, 1, \dots, p-1$.

Solution. (1) (Continued with the discussion in Remark 3, we may view the extension $\mathbb{Z}_p[\![T]\!]$ over $\varphi(\mathbb{Z}_p[\![T]\!])$ as a (non-étale) Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$ and $1 \in \mathbb{Z}/p\mathbb{Z}$ sends $f(T)$ to $f(\zeta_p(1+T)-1)$.) For the proof of (1), we compare the two formulas. Write $F \in \mathbb{Z}_p[\![T]\!]$ as $F = \sum_{j=0}^{p-1}(1+T)^j\varphi(F_j)$ for $F_0, F_1, \dots, F_{p-1} \in \mathbb{Z}_p[\![T]\!]$, then $\psi(F) = F_0$. We compute

$$\begin{aligned}
\frac{1}{p}\sum_{i=0}^{p-1} F\big((1+T)\zeta_p^i - 1\big) &= \frac{1}{p}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(1+T)^j\zeta_p^{ij}\cdot\varphi(F_j)\big((1+T)\zeta_p^i - 1\big)\\
&= \frac{1}{p}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(1+T)^j\zeta_p^{ij}\cdot F_j\big((1+T)^p - 1\big)\\
&= F_0\big((1+T)^p - 1\big),
\end{aligned}$$

where the last equality uses the equality $\frac{1}{p}\sum_{i=0}^{p-1}\zeta_p^{ij} = \begin{cases} 1 & \text{when } j \neq 0, \\ 0 & \text{when } j = 0. \end{cases}$ Part (1) is proved.

(2) First consider the φ-action: $\varphi(T) = (1+T)^p - 1 = T^p + pQ(T)$, for a polynomial $Q(T) \in \mathbb{Z}_p[T]$. From this, we see that

$$\varphi\Big(\frac{1}{T}\Big) = \frac{1}{T^p + pQ(T)} = T^{-p} + pT^{-2p}Q(T) + p^2T^{-3p}Q(T) + \cdots$$

This converges p-adically. From this, we see that if an expression $f = \sum_{n=0}^{\infty} a_n(T)p^n \in \mathbb{A}_{\mathbb{Q}_p}$ with $a_n(T) \in T^{-r_n}\mathbb{Z}_p[\![T]\!]$ for some $r_n \in \mathbb{Z}$, then

$$\varphi(f) = \sum_{n=0}^{\infty} \varphi(T)^{-r_n} \cdot \varphi(T^{r_n}a_n(T))p^n.$$

It converges well in $\mathbb{A}_{\mathbb{Q}_p}$.

The definition of ψ is similar as we may write each $F \in \mathbb{A}_{\mathbb{Q}_p}$ uniquely as a linear combination $F = \sum_{i=0}^{p-1}(1+T)^i\varphi(F_i)$, and then define $\psi(F) = F_0$.

(3) (Direct calculation) Using the formula (1.4.1), it suffices to show that

$$\frac{1}{(1+T)^p - 1} = \frac{1}{p}\sum_{i=0}^{p-1}\frac{1}{(1+T)\zeta_p^i - 1},$$

or equivalently,

$$\sum_{i=0}^{p-1}\frac{(1+T)^p - 1}{(1+T)\zeta_p^i - 1} = p.$$

The left hand side is a polynomial in T of degree $\leq p-1$. We need only to check this equality when $T = \zeta_p^i - 1$ for every $i = 0, \dots, p-1$. Plugging in $T = \zeta_p^{-j} - 1$ (for some $j = 0, \dots, p-1$), the left hand side is nonzero only when $i = j$, in which case, the term is equal to

$$\prod_{i=0,\ i\neq j}^{p-1}\big(\zeta_p^{-j}\cdot\zeta_p^i - 1\big) = \prod_{k=1}^{p-1}\big(\zeta_p^k - 1\big) = p.$$

Part (3) is proved.

(3) (“Better” proof) Note that the φ-action preserves the subring $\mathbb{Z}_p[T]$ and the subfield $\mathbb{Z}_p(T)$ (without taking any completion); and the map ψ can be defined similarly via the same recipe. Now we may make change of variable $S := 1 + T$ and it is clear that $\varphi(S) = S^p$, and $\mathbb{Z}_p(T) = \mathbb{Z}_p(S)$. This φ-action extends to a “different completion of $\mathbb{Z}_p(S)$”, namely $\mathbb{Z}_p((S))$. (Note that one cannot compare $\mathbb{Z}_p((S))$ directly with $\mathbb{Z}_p((T))$.) Over $\mathbb{Z}_p((S))$, the ψ-operator can be made explicit: every $F(S) \in \mathbb{Z}_p((S))$ can be written as $F(S) = \sum_{i=0}^{p-1} S^i\varphi(F_i)$, then $\psi(F) = F_0$.

Now it suffices to check $\psi(\frac{1}{S-1}) = \frac{1}{S-1}$ in $\mathbb{Z}_p((S))$. But this is easy:

$$\frac{1}{1-S} = 1 + S + S^2 + \cdots = \sum_{i=0}^{p-1} S^i\varphi(1 + S + S^2 + \cdots) = \sum_{i=0}^{p-1} S^i\varphi\Big(\frac{1}{1-S}\Big).$$

It then follows that $\psi(\frac{1}{1-S}) = \frac{1}{1-S}$. Part (3) is proved. $\square$

Exercise 1.5 ("Miraculous congruence" encoded in p-adic L-functions)**.** Assume $p \geq 3$ for simplicity. We have constructed p-adic Dirichlet L-functions as p-adic measures on $\mathbb{Z}_p^\times$ that interpolate special values of (p-modified) Dirichlet L-functions. It is natural to ask: is the p-adic Dirichlet L-function uniquely determined by these interpolation values? In fact, the answer is that these values "overdetermine" the p-adic L-functions. (We will discuss this in lectures at a later stage.) Assume that $p \geq 3$ is an odd prime number.

(1) Let G be a general profinite group and let $\chi : G \to R^\times$ be a continuous p-adic character with values in a p-adically complete ring R, then it induces a continuous ring homomorphism $\tilde{\chi} : \mathbb{Z}_p\llbracket G\rrbracket \to R$. Alternatively, χ can be viewed as a R-valued function on G, so one can integrate against a p-adic measure on G.

Prove that we have the following commutative diagram

$$\begin{tikzcd} \mathbb{Z}_p\llbracket G\rrbracket \arrow[rr, "\cong"] \arrow[dr, "\tilde{\eta}"'] & & \mathcal{D}_0(G, \mathbb{Z}_p) \arrow[dl, "\mu \mapsto \int_G \eta(g) d\mu(g)"] \\ & R & \end{tikzcd}$$

(2) Write $\Delta := \mathbb{F}_p^\times$, which may be viewed as a subgroup of $\mathbb{Z}_p^\times$ via Teichmüller character ω. Give an canonical isomorphism $\Phi : \mathbb{Z}_p\llbracket\mathbb{Z}_p^\times\rrbracket \cong \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\llbracket X\rrbracket$, so that $X = [\exp(p)] - 1$, where $\exp(p) = 1 + p + \frac{p^2}{2!} + \cdots$ is the formal expansion.

(3) Prove that $\mathbb{Z}_p\llbracket\mathbb{Z}_p^\times\rrbracket$ is canonical isomorphic to a product of $p-1$ rings:

$$\begin{aligned} \mathbb{Z}_p\llbracket\mathbb{Z}_p^\times\rrbracket \;\cong\; \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\llbracket X\rrbracket \quad &\cong \quad \prod_{i=0}^{p-2} \mathbb{Z}_p\llbracket X\rrbracket \\ (a, f(X)) &\longmapsto (\omega^i(a) f(X))_{i=0,\dots,p-2}. \end{aligned} \tag{1.5.1}$$

(4) Let $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ be a finite character and let $n \in \mathbb{Z}_{\geq 0}$; we may form the p-adic character

$$\begin{aligned} \chi_{\eta,n} : \mathbb{Z}_p^\times &\longrightarrow \overline{\mathbb{Q}}_p^\times \\ a &\longmapsto \eta(a) a^n. \end{aligned}$$

If we denote by $\bar{\chi}_{\eta,n}$ the restriction of $\chi_{\eta,n}$ to Δ, then for any $\mu \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$,

$$\int_{\mathbb{Z}_p^\times} \eta(x) x^n d\mu(x) = \Phi(\mu)|_{\Delta = \bar{\chi}_{\eta,n},\, T = \chi_{\eta,n}(\exp(p)) - 1}.$$

(5) Prove that two p-adic measures $\mu_1, \mu_2 \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$ are equal if for any $n \in \mathbb{Z}_{\geq 0}$,

$$\int_{\mathbb{Z}_p^\times} x^n d\mu_1(x) = \int_{\mathbb{Z}_p^\times} x^n d\mu_2(x).$$

(Hint: Show that the difference $\mu_1 - \mu_2$ is divisible by some infinite product.)

(6) Prove that two p-adic measures $\mu_1, \mu_2 \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$ are equal if for a *fixed* $n \in \mathbb{Z}_{\geq 0}$ but for all finite characters $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ for all r, we have

$$\int_{\mathbb{Z}_p^\times} \eta(x) x^n d\mu_1(x) = \int_{\mathbb{Z}_p^\times} \eta(x) x^n d\mu_2(x).$$

Hint: For (4) and (5), you may find the following Weierstrass preparation theorem useful: for a complete noetherian local ring $(A, \mathfrak{m})$, if $f(x) \in A[\![x]\!]$ is a power series that does not lie in $\mathfrak{m}[\![x]\!]$, then we may factor $f(x) = g(x)u(x)$, with $g(x)$ a monic polynomial (of finite degree) and $u(x) \in A[\![x]\!]^\times$ is a unit. In the case of $A = \mathbb{Z}_p$, the Weierstrass preparation theorem has the following version: every nonzero power series $f(x) \in \mathbb{Z}_p[\![x]\!]$ can be factored as $f(x) = p^r g(x)u(x)$, with $r \in \mathbb{Z}_{\geq 0}$, $g(x)$ a monic polynomial, and $u(x) \in A[\![x]\!]^\times$ a unit.

Solution. (1) Suppose that R is I-adically complete for an ideal I of R. We may replace R by R/I^n and thus reduce to the case when G is finite. In this case, write $\Psi : R[G] \xrightarrow{\cong} \mathcal{D}_0(G, R)$ for the isomorphism. We have, for any $\mu \in R[G]$,

$$\tilde{\eta}(\mu) = \sum_{g \in G} \eta(g)\mu(g) = \int_G \eta(g) d\Psi(\mu)(g).$$

Part (1) is proved.

(2) Take the isomorphism $\mathbb{Z}_p^\times \cong \Delta \times (1 + p\mathbb{Z}_p)^\times$, where we embed Δ into $\mathbb{Z}_p^\times$ via the Teichmüller character ω. We may identify $(1 + p\mathbb{Z}_p)^\times$ with $\mathbb{Z}_p$ via p-adic logarithm and thus we deduce that

$$\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![(1 + p\mathbb{Z}_p)^\times]\!] \cong \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!],$$

where X stands for $[\exp(p)] - 1$.

(3) is clear.

(4) follows from combining (1) an (2).

(5) Write $\mu := \mu_1 - \mu_2$, we have by (3) that

$$\Phi(\mu)\big|_{\Delta = \bar{x}^n,\, T = \exp(np) - 1} = 0.$$

For the element $\Phi(\mu) \in \mathbb{Z}_p[\Delta] \otimes \mathbb{Z}_p[\![X]\!]$, write $(h_0, h_1, \ldots, h_{p-2}) \in \prod_{i=0}^{p-2} \mathbb{Z}_p[\![X]\!]$ for its image under the isomorphism (1.5.1). The condition implies that $h_a(\exp(np) - 1) = 0$ for $n \equiv a \bmod p-1$. But no function in $\mathbb{Z}_p[\![X]\!]$ has infinitely many zeros, except for the zero function, by Weierstrass preparation theorem. It follows that $h_0 = \cdots = h_{p-2} = 0$. Thus $\mu_1 = \mu_2$.

(6) The argument is similar to (5), except that the zeros of h_a for each $a = 0, \ldots, p-2$ are precisely $\eta(\exp(p)) - 1$ for those η for which $\eta|_\Delta = \omega^i$. There are infinitely many such η's. By Weierstrass preparation theorem, we have $\mu_1 = \mu_2$. $\square$

Exercise 1.6. (Kubota–Leopoldt p-adic L-function) In the second and the third lectures, we have constructed the p-adic Dirichlet L-function when the (tame) Dirichlet character η is nontrivial. For the case when $\eta = \mathbf{1}$, we should also construct the corresponding p-adic zeta-function, traditionally called the *Kubota–Leopoldt p-adic L-function*. Unfortunately, this will not be a p-adic measure on $\mathbb{Z}_p^\times$, but only a "quasi-measure", which is philosophically reflects the fact that the Riemann zeta function has a pole at $s = 1$ (so should the p-adic zeta have). For this reason, we need some technical maneuver for its construction.

Assume $p \geq 3$ for simplicity. Pick $a \in \mathbb{Z}_{>1}$ relatively prime to p. Consider

$$\zeta_a(s) := (1 - a^{1-s}) \cdot \zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} - a \cdot \sum_{\substack{n \geq 1 \\ a \mid n}} \frac{1}{n^s},$$

$$A_a(T) = (1 - a\gamma_a)\Big(\frac{1+T}{1-(1+T)}\Big) = \frac{1+T}{1-(1+T)} - a \cdot \frac{(1+T)^a}{1-(1+T)^a},$$

where $\gamma_a \in \Gamma = \mathbb{Z}_p^\times$ is the element corresponding to $a \in \mathbb{Z}_p^\times$, which acts on $\mathbb{Z}_p[\![T]\!]$ by sending T to $(1+T)^a - 1$.

(1) Show that $A_a(T) \in \mathbb{Z}_p[\![T]\!]$ defines a p-adic measure; so does $A_a^{\{p\}}(T) := (1-\varphi\psi)(A_a(T))$.

Define $\mu_a^{\{p\}}$ to be the p-adic measure associated to $A_a^{\{p\}}(T)$ via Amice transform. For any primitive character $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$, define

$$L^{\{p\}}(\eta_p, s) = \begin{cases} (1-p^{-s}) \cdot \zeta(s) & \text{if } \eta_p = \mathbf{1}, \\ L(\eta_p, s) & \text{if } \eta_p \neq \mathbf{1}, \end{cases}$$

$$L_a^{\{p\}}(\eta_p, s) = (1-a^{1-s}) \cdot L^{\{p\}}(\eta_p, s) = \sum_{\substack{n\geq 1 \\ (n,p)=1}} \frac{\eta_p(n)}{n^s} - a \cdot \sum_{\substack{n\geq 1 \\ (n,p)=1}} \frac{\eta_p(an)}{(an)^s}$$

(2) Show that for any character $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$ and any $n \in \mathbb{Z}_{\geq 0}$, we have

$$\int_{\mathbb{Z}_p^\times} \eta_p(x) x^n d\mu_a^{\{p\}}(x) = L_a^{\{p\}}(\eta_p, -n).$$

(3) Recall the identification $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]$. We may define the *Kubota–Leopoldt p-adic L-function* to be the element

$$\mu_{\mathrm{KL}} := \frac{\mu_a^{\{p\}}}{(1-a[\gamma_a])} \in \mathbb{Z}_p[\Delta] \otimes \frac{1}{X - \exp(-p) + 1} \mathbb{Z}_p[\![X]\!].$$

Sometimes, this is called a *pseudo-measure*; show that μ_{KL} is independent of the choice of $a \in \mathbb{Z}_p^\times$. (Hint: We need only to prove that $(1-b\gamma_b)(\mu_a^{\{p\}}) = (1-a\gamma_a)(\mu_b^{\{p\}})$ for two different $a, b \in \mathbb{Z}_{>1}$ relatively prime to p. One can make use of Exercise 1.5(4)(5).)

Remark 4. Our definition of pseudo-measure slightly differs from that of Jacinto–Williams' note, who shifted the p-adic Kubota–Leopolds L-function so that the pole is at $s = 0$.

Solution. (1) To see that $A_a(T) \in \mathbb{Z}_p[\![T]\!]$, it suffices to show that it has no pole at $T = 0$, or equivalently

$$\mathrm{res}_{T=0}\Big(\frac{1+T}{1-(1+T)}\Big) = \mathrm{res}_{T=0}\Big(a \cdot \frac{(1+T)^a}{1-(1+T)^a}\Big)$$

But this is clear. From this, it is clear that $A_a^{\{p\}}(T) \in \mathbb{Z}_p[\![T]\!]$.

(2) This construction is essentially the same as the construction of the p-adic Dirichlet L-functions presented in the lecture. In accordance with the definition of $L_a^{\{p\}}(\eta_p, s)$, we define for $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$ (primitive if $\eta_p \neq \mathbf{1}$ and put $r = 1$ if $\eta_p = \mathbf{1}$),

$$\begin{aligned} A_{\eta_p,a}^{\{p\}}(T) &:= \frac{\displaystyle\sum_{\substack{n=1 \\ (n,ap)=1}}^{ap^r-1} \eta_p(n)(1+T)^n - a \cdot \sum_{n=1}^{p^r-1} \eta(an)(1+T)^{an}}{1-(1+T)^{ap^r}} \\ &= \sum_{\substack{n\geq 1 \\ (n,ap)=1}} \eta(n)(1+T)^n - a \cdot \sum_{\substack{n\geq 1 \\ (n,p)=1}} \eta(an)(1+T)^{an}, \end{aligned}$$

and $f^{\{p\}}_{\eta_p,a}(t) := A^{\{p\}}_{\eta_p,a}(e^{-t}-1)$. Then $L^{\{p\}}(\eta_p, s) = \dfrac{1}{\Gamma(s)}\displaystyle\int_0^\infty f^{\{p\}}_{\eta_p,a}(t)t^s \cdot \frac{dt}{t}$ and

$$L^{\{p\}}(\eta_p, -n) = \Big(-\frac{d}{dt}\Big)^n \big(f^{\{p\}}_{\eta_p,a}\big)\Big|_{t=0} = \Big((1+T)\frac{d}{dT}\Big)^n \big(A^{\{p\}}_{\eta_p,a}\big)\Big|_{T=0} = \int_{\mathbb{Z}_p^\times} x^n d\mu^{\{p\}}_{\eta_p,a}(x),$$

where $\mu^{\{p\}}_{\eta_p,a}$ is the p-adic measure associated to $A^{\{p\}}_{\eta_p,a}$ via the Amice transform. It remains to prove that

$$\mu^{\{p\}}_{\eta_p,a} = \sum_{i\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \eta_p(i)\cdot \mathrm{Res}_{i+p^r\mathbb{Z}_p}(\mu^{\{p\}}_a).$$

But this is clear by checking the corresponding $(1+T)$-expansion of the Amice transforms. Indeed, the Amice transform of the right hand side is equal to

$$\begin{aligned}&\sum_{i\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \eta_p(i)\cdot\Bigg(\sum_{\substack{n\geq 1\\ n\equiv i \bmod p^r}}(1+T)^n - a\cdot \sum_{\substack{n\geq 1\\ an\equiv i \bmod p^r}}(1+T)^{an}\Bigg)\\ &= \sum_{\substack{n\geq 1\\ (n,ap)=1}} \eta_p(n)(1+T)^n - a\cdot\sum_{\substack{n\geq 1\\ (n,p)=1}}\eta_p(an)(1+T)^{an} = A^{\{p\}}_{\eta_p,a}(T).\end{aligned}$$

This completes the proof of the interpolation formula for p-adic L-functions.

(3) We first check that $\mu_{\mathrm{KL}} \in \mathbb{Z}_p[\Delta]\otimes\frac{1}{X-\exp(-p)+1}\mathbb{Z}_p[\![X]\!]$. For this, we may take a so that $\bar{a}$ is a generator of $\mathbb{F}_p^\times$. Write $a = \omega(\bar{a})\cdot\langle a\rangle$ with $\bar{a}\in\Delta$ and $\langle a\rangle\in(1+p\mathbb{Z}_p)^\times$. We consider the image of $1-a\gamma_a$ under the isomorphism $\mathbb{Z}_p[\mathbb{Z}_p]\cong\prod_{i=0}^{p-2}\mathbb{Z}_p[\![X]\!]$ using the characters $\omega^i:\Delta\to\mathbb{Z}_p^\times$ with $i\in\{0,\dots,p-2\}$. When $i\neq p-2$,

$$\omega^i(1-a\gamma_a) = 1 - a\omega^i(a)(1+X)^{\langle a\rangle}\in\mathbb{Z}_p[\![X]\!]^\times.$$

When $i = p-2$, we have

$$\omega^{p-2}(1-a\gamma_a) = 1-\langle a\rangle(1+X)^{(\log_p\langle a\rangle)/p} = 1-\langle a\rangle\cdot\langle a\rangle^{(\log_p(1+X))/p}.$$

This function has as simple pole at $X=\exp(-p)-1$. From this, we deduce that

$$\mu_{\mathrm{KL}}\in\mathbb{Z}_p[\Delta]\otimes\frac{1}{X-\exp(-p)+1}\mathbb{Z}_p[\![X]\!].$$

It suffices to compare for $a,b\in\mathbb{Z}_{>1}$, that $(1-b\gamma_b)\big(\mu_a^{\{p\}}\big) = (1-a\gamma_a)\big(\mu_b^{\{p\}}\big)$. By Exercise 1.5(4), it suffices to verify that

$$\int_{\mathbb{Z}_p^\times} x^n d\big((1-b\gamma_b)\big(\mu_a^{\{p\}}\big)\big)(x) = \int_{\mathbb{Z}_p^\times} x^n d\big((1-a\gamma_a)\big(\mu_b^{\{p\}}\big)\big)(x).$$

But the action on the measures can be turned into an action on the functions, i.e.

$$\int_{\mathbb{Z}_p^\times}(x^n - b\cdot b^n x^n)d\mu_a^{\{p\}}(x) = (1-b^{n+1})\int_{\mathbb{Z}_p^\times} x^n d\mu_a^{\{p\}}(x) = (1-b^{n+1})(1-a^{n+1})\zeta(-n).$$

This expression is clearly symmetric in a,b. Part (3) is proved. □

Exercise 1.7 (A more classical version of p-adic L-function)**.** Historically, there is also an old version of p-adic L-function which is really just p-adic functions. In this exercise, we recover the classical p-adic L-function from the p-adic measures, and we will see that the p-adic measures contains stronger congruence relations than classical p-adic L-functions.

(To avoid talking about pseudo-measures, we again work with p-adic Dirichlet L-functions.) Let η be a primitive Dirichlet character of conductor N (with $p \nmid N$). We have constructed a p-adic measure $\mu_\eta^{\{p\}}$ such that

$$\int_{\mathbb{Z}_p^\times} x^n d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta, -n).$$

(This measure also interpolates Dirichlet L-functions for varying the character at p; we will not use it here.)

We are interested in understanding the p-adic function $\zeta_{p,i}$ on $\mathbb{Z}_p$ for $i = 0, 1, \ldots, p-2$, defined by for $s \in \mathbb{Z}$ such that $s \equiv i \bmod p-1$,

$$\zeta_{p,i}(s) := \int_{\mathbb{Z}_p^\times} x^s d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta, -s).$$

(1) Show that $\zeta_{p,i}(s)$ extends naturally to a continuous function on $s \in \mathbb{Z}_p$. (So far, this is weaker than a function on $s \in \mathcal{O}_{\mathbb{C}_p}$.)

Now we study these functions $\zeta_{p,i}$ more carefully. Abstractly by Exercise 1.5, we may view $\mu_\eta^{\{p\}}$ as an element in $\mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]$, where $X = [\exp(p)] - 1$. (Here we view $\Delta = \mathbb{F}_p^\times$ as a subgroup of $\mathbb{Z}_p^\times$ via the Teichmüller character ω.) For $i = 0, \ldots, p-2$, write $\mu_{\eta,i}(X) \in \mathcal{O}[\![X]\!]$ for the image of $\mu_\eta^{\{p\}}$ under the map $\Delta \to \mathbb{Z}_p^\times$ sending x to $\omega(x)^i$.

(2) Show that (formally)

$$\zeta_{p,i}(s) = \mu_{\eta,i}(\exp(ps)). \tag{1.7.1}$$

(3) From (2), deduce that $\zeta_{p,i}(s)$ extends to a p-adic analytic function for $s \in p^{-\frac{p-2}{p-1}}\mathfrak{m}_{\mathbb{C}_p}$.

Remark 5. One sees from this exercise that the classical p-adic L-function only captures part of the information provided. Even knowing the convergence of $\zeta_{p,i}(s)$ for $s \in p^{-\frac{p-2}{p-1}}\mathfrak{m}_{\mathbb{C}_p}$, it is far from enough to deduce the integrality of $\mu_\eta^{\{p\}}$. For more discussion in this direction, see the post

`https://mathoverflow.net/questions/435265/why-p-adic-measures`.

Solution. (1) This is obvious, because whenever $s_1 \equiv s_2 \bmod p^{k-1}(p-1)$ for some $k \in \mathbb{Z}_{\geq 1}$, we have $x^{s_1} \equiv x^{s_2} \bmod p^k$, then $\zeta_{p,i}(s_1) \equiv \zeta_{p,i}(s_2) \bmod p^k$. So each $\zeta_{p,i}(s)$ extends to a continuous function in $s \in \mathbb{Z}_p$.

(2) By Exercise 1.5(1), integration against a character x^s is the same as evaluating the measure μ_η at the ring homomorphism $\mathcal{O}[\![\mathbb{Z}_p^\times]\!] \to \mathcal{O}$ defined by x^s. In particular, this means that when $s \equiv i \bmod p-1$, $\int_{\mathbb{Z}_p^\times} x^i d\mu_\eta^{\{p\}}(x) = \mu_{\eta,i}(\exp(ps))$. (The condition $s \equiv i \bmod p-1$ ensures that we use the factor $\eta_{p,i}$.) The equality (1.7.1) follows from the interpolation properties of p-adic Dirichlet L-functions.

(3) As $\mu_{\eta,i} \in \mathbb{Z}_p[\![X]\!]$, for $\mu_{\eta,i}(\exp(ps))$ to make sense, we need $|\exp(ps)| < 1$, which forces that $ps \in p^{\frac{1}{p-1}}\mathfrak{m}_{\mathbb{C}_p}$ or equivalently, $s \in p^{-\frac{p-2}{p-1}}\mathfrak{m}_{\mathbb{C}_p}$. $\square$

Exercise 1.8 (Volume of ideles class group versus residue of Dedekind zeta values)**.** Let F be a number field with r_1 real embeddings and r_2 pairs of complex embeddings. Let $\mathbb{A}_F^\times$ be the group of ideles and $\mathbb{A}_F^{\times,1} := \{x \in \mathbb{A}_F^\times \,|\, |x| = 1\}$ be the subgroup of norm one elements. We have stated (and proved in the quadratic case) of the analytic class number formula, for the Dedekind zeta function $\zeta_F(s)$ at $s = 1$:

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\cdot h_F \mathrm{Reg}_F}{w_F\sqrt{|\Delta_F|}}, \tag{1.8.1}$$

where h_F is the class number, Reg_F is the regulator for units of F, w_F is the number of roots of unity contained in F, and Δ_F is the discriminant of F.

(1) Using the functional equation of Dedekind zeta function to deduce from (1.8.1) the following analytic class number formula at $s = 0$:

$$\lim_{s\to 0} s^{-r_1-r_2+1}\zeta_F(s) = -\frac{h_F\cdot \mathrm{Reg}_F}{w_F}.$$

(2) Show that the right hand side of (1.8.1) can be interpreted as $\mathrm{Vol}(\mathbb{A}_F^{\times,1}/F^\times)$, if we provide the Haar measure on $\mathbb{A}_F^{\times,1}$ so that under the product decomposition $\mathbb{A}_F^\times = \mathbb{A}_F^{\times,1} \times \mathbb{R}^\times$ (where $\mathbb{R}^\times$ is provided with the measure $\frac{dx}{x}$) admits the following Haar measure:
- at a real place v of F, the Haar measure on $F_v^\times$ is $\frac{dx}{|x|}$,
- at a complex place v of F, the Haar measure on $F_v^\times \simeq \mathbb{C}^\times$ is $\frac{2dx\wedge dy}{|x^2+y^2|} = \frac{2drd\theta}{r}$,
- at a p-adic place v of F with different ideal $\mathfrak{d}_v \subseteq F_v$, the Haar measure on $F_v^\times$ is so that volume of $\mathcal{O}_{F_v}^\times$ is $||\mathfrak{d}_v||^{-\frac{1}{2}}$, where $||\mathfrak{d}_v|| = \#(\mathcal{O}_{F_v}/\mathfrak{d}_v)$.

Solution. (1) Recall the functional equation for Dedekind zeta function. Let

$$\Lambda_F(s) = \Gamma_{\mathbb{R}}(s)^{r_1}\cdot\Gamma_{\mathbb{C}}(s)^{r_2}\cdot\zeta_F(s)$$

denote the complete Dedekind zeta function. Then the functional equation is given by

$$\Lambda_F(s) = |\Delta_F|^{\frac{1}{2}-s}\Lambda_F(1-s).$$

Considering this equality near $s = 0$, we have

$$\zeta_F(s)\underbrace{\Big(\pi^{-\frac{s}{2}}\Gamma\Big(\frac{s}{2}\Big)\Big)^{r_1}}_{\approx(\frac{2}{s})^{r_1}}\underbrace{\Big(2(2\pi)^{-s}\Gamma(s)\Big)^{r_2}}_{\approx(\frac{2}{s})^{r_2}} = \underbrace{|\Delta_F|^{\frac{1}{2}-s}}_{|\Delta_F|^{\frac{1}{2}}}\cdot\zeta_F(1-s)\cdot\underbrace{\Big(\pi^{-\frac{1-s}{2}}\Gamma\Big(\frac{1-s}{2}\Big)\Big)^{r_1}}_{\approx\pi^{-\frac{1}{2}}\cdot\sqrt{\pi})^{r_1}}\underbrace{\Big(2(2\pi)^{s-1}\Gamma(1-s)\Big)^{r_2}}_{\approx(\frac{2}{2\pi})^{r_2}}.$$

$$\begin{aligned}\zeta_F(s) &\approx \Big(\frac{s}{2}\Big)^{r_1+r_2}\pi^{-r_2}|\Delta_F|^{\frac{1}{2}}\cdot\zeta_F(1-s)\\ &\approx \Big(\frac{s}{2}\Big)^{r_1+r_2}\pi^{-r_2}|\Delta_F|^{\frac{1}{2}}\cdot\Big(-\frac{1}{s}\Big)\frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}_F\cdot h_F}{w_F|\Delta_F|^{\frac{1}{2}}}.\end{aligned}$$

From this, we deduce that

$$\lim_{s\to 0} s^{r_1+r_2-1}\zeta_F(s) = -\frac{\mathrm{Reg}_F h_F}{w_F}.$$

(2) Let M_F denote the the set of places of F, and $\mathsf{M}_{F,f}$ the subset of finite places. We consider the following exact sequence:

$$0 \to \prod_{v \in \mathsf{M}_{F,f}} \mathcal{O}_{F_v}^{\times} \to \mathrm{Cl}(\mathcal{O}_F) \to 0$$

□