Special values of L-functions 2

——— p-adic analysis on $\mathbb{Z}_p$

Recall: For a primitive Dirichlet character $\eta: (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$

Consider $f_\eta(t) := \dfrac{\sum_{n=1}^{N-1} \eta(n) e^{-nt}}{1-e^{-Nt}} = \dfrac{1}{t} \sum_{n=0}^{+\infty} B_{n,\eta} \dfrac{t^n}{n!}$ ← η-Bernoulli polynomial.

Then a useful lemma from last time

$$\Rightarrow L(\eta, -n) = (-1)^n f_\eta^{(n)}(0) = (-1)^n \frac{B_{n+1,\eta}}{n+1}$$

Fix a prime p today. (For simplicity, $p \geq 3 \Rightarrow \mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)^\times$.)

Magical words: fix an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}}_p$

True meaning: let $\mathbb{Q}^{alg}$ be alg. closure of $\mathbb{Q}$ in $\mathbb{C}$ & pick a p-adic place of $\mathbb{Q}^{alg}$.

Generalized Kummer's congruence. Assume $p \nmid N$. Given $k \in \mathbb{Z}_{\geq 1}$ and two integers $n_1, n_2 \geq k$

s.t. $n_1 \equiv n_2 \bmod (p-1)p^{k-1}$ and $p-1 \nmid n_1$ if η is trivial,

Then $\dfrac{B_{n_1+1,\eta}}{n_1+1} \equiv \dfrac{B_{n_2+1,\eta}}{n_2+1} \bmod p^k$, or equivalently, $L(\eta, -n_1) \equiv L(\eta, -n_2) \bmod p^k$.

These two lectures: Prove this by constructing the corresponding p-adic L-function.

§1 Reinterpretation of Dirichlet characters

There are two ways to reinterprete Dirichlet characters, we will discuss the other one later.

(Galois) $\eta: \mathrm{Gal}_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\eta} \mathbb{C}^\times$

⇝ In general, one can associate L-functions to a "nice" Galois representation

(for a number field F) $\rho: \mathrm{Gal}_F \to GL_n(\mathbb{C})$ or $GL_n(\overline{\mathbb{Q}}_p)$ (later)

* We will decompose η as $\eta^{(p)}: (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ with $p \nmid N$. Will fix $\eta^{(p)}$ today

$\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow \bar{\mathbb{Q}}^\times$ where we also allow η_p nontrivial.

p-adic L-function = a p-adic "function" that interpolates

$L(\eta^{(p)}\eta_p, -n)$ for a fixed $\eta^{(p)}$ and for all η_p and all $n \in \mathbb{Z}_{\geq 1}$.

$\eta^{(p)} \longleftrightarrow$ character of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$

η_p and n together give a p-adic character of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$

$$\mathbb{Z}_p^\times \longrightarrow \bar{\mathbb{Q}}_p^\times$$
$$a \longmapsto \eta_p(a \bmod p^r) \cdot a^n$$

or rather, we will view (η_p, n) as a p-adic continuous function $f_{\eta_p,n}(x)$ on $\mathbb{Z}_p^\times$

Also needs to modify the L-functions : p-deprived L-function

$$L^{(p)}(\eta, s) := \prod_{\substack{q \neq p \\ q \nmid N}} \frac{1}{1-\eta(q)q^{-s}} = \begin{cases} L(\eta^{(p)}\eta_p, s) & \text{when } \eta_p \text{ is nontriv} \\ L(\eta^{(p)}, s)\cdot(1-\eta^{(p)}(p)p^{-s}) & \text{when } \eta_p = \mathbb{1} \end{cases}$$

Theorem When $\eta^{(p)}$ is nontrivial, there exists a "measure" $d\mu_{\eta^{(p)}}$ on $\mathbb{Z}_p^\times$ such that for any character $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow \bar{\mathbb{Q}}_p^\times$ and any $n \in \mathbb{Z}_{\geq 0}$,

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

Version 1: The "correct" object for p-adic L-function is a p-adic measure

(but not really a function) ↖ may give a different viewpoint later

Remark: In general, the correct formulation may not to "deprive" all L-factors at p.

for Dirichlet L-function, yes, but not for more general L-functions

§2 Continuous p-adic functions on $\mathbb{Z}_p$

We need to make sense of "p-adic integrations" of p-adic functions

Definition. Let K be a completely valued field/$\mathbb{Q}_p$ (e.g. $\mathbb{Q}_p$) with valuation ring $\mathcal{O}_K$. ($|\cdot|: K \to \mathbb{R}_{\geq 0}$)

A (p-adic) Banach space over K is a K-vector space V completed w.r.t. a norm

$$\|\cdot\| : V \longrightarrow \mathbb{R}_{\geq 0}$$

s.t. (1) $\|av\| = |a| \cdot \|v\| \quad \forall a \in K, v \in V$

(2) $\|v+w\| \leq \max\{\|v\|, \|w\|\} \quad \forall v, w \in V$

(3) $\|v\| = 0 \iff v = 0$.

Example: $\ell^\infty := \{(a_n)_{n \in \mathbb{Z}_{\geq 1}} ; a_n \in K, \text{ s.t. } a_n \to 0 \text{ when } n \to +\infty\} = \left(\widehat{\bigoplus_{n \in \mathbb{Z}_{\geq 1}}} \mathcal{O}_K\right) \otimes_{\mathcal{O}_K} K$

"dual" to L^∞-space.

with norm $\|(a_n)\| := \max_n \{|a_n|\}$.

Example: For X a compact space, $C^\infty(X, \mathcal{O}_K) = \{f : X \to \mathcal{O}_K \text{ continuous}\}$

$$C^\infty(X, K) = C^\infty(X, \mathcal{O}_K) \otimes_{\mathcal{O}_K} K, \quad \|f\|_{\sup} := \sup_x |f(x)|.$$

Definition For a Banach space V, an orthonormal basis $\{e_i\}_{i \in I}$ is a family of elements

s.t. ⓪ $\|e_i\| = 1$ for any $i \in I$.

① Every $v \in V$ can be written as $x = \sum_{i \in I} x_i e_i$ for $x_i \in K$ and

$x_i \to 0$ in the sense that for any $\varepsilon > 0$, $\#\{x_i ; |x_i| \geq \varepsilon\}$ is finite

② $\|x\| = \max_{i \in I} \{|a_i|\}$

Such V is called ONable.

- $C^0(\mathbb{Z}_p, \mathbb{Z}_p) := \{\text{continuous functions } f : \mathbb{Z}_p \to \mathbb{Z}_p\}, \quad \|f\| := \sup_{x \in \mathbb{Z}_p} |f(x)|$

For a completely valued field K, define $C^0(\mathbb{Z}_p, -) := C^0(\mathbb{Z}_p, \mathbb{Z}_p) \hat{\otimes} -$ for $- \in \{\mathcal{O}_K, K\}$.

* For $n \in \mathbb{Z}_{\geq 0}$, define $\binom{x}{n} := \begin{cases} 1 & \text{when } n = 0 \\ \frac{x(x-1)\cdots(x-n+1)}{n!} & n \geq 1. \end{cases}$

Lemma. $\binom{x}{n} \in C^0(\mathbb{Z}_p, \mathbb{Z}_p)$ and $\|\binom{x}{n}\| = 1$

Proof: It is clear that for $x \in \mathbb{Z}$, $\binom{x}{n} \in \mathbb{Z}$.

By density of $\mathbb{Z}$ in $\mathbb{Z}_p$ $\Rightarrow$ for $x \in \mathbb{Z}_p$, $\binom{x}{n} \in \mathbb{Z}_p$, so $\left\|\binom{x}{n}\right\| \leq 1$.

Yet $\binom{n}{n} = 1 \Rightarrow \left\|\binom{x}{n}\right\| = 1$.

Theorem (Mahler) Every $f \in C^0(\mathbb{Z}_p, \mathbb{Q}_p)$ admits a unique expansion (called Mahler expansion)

$$f(x) = \sum_{n \geq 0} a_n(f) \cdot \binom{x}{n} \quad \text{with } a_n(f) \to 0 \text{ as } n \to +\infty. \qquad (*)$$

Moreover, $\|f\| = \sup_n |a_n(f)|$

i.e. $\left\{\binom{x}{n}\right\}_{n \in \mathbb{Z}_{\geq 0}}$ is an orthonormal basis of $C^0(\mathbb{Z}_p, \mathbb{Q}_p)$

* Alternatively, we have an isomorphism $C^0(\mathbb{Z}_p, \mathbb{Q}_p) \xrightarrow{\simeq} \ell_\infty$

$$f(x) \longmapsto (a_n(f))_{n \in \mathbb{Z}_{\geq 0}}.$$

Proof: For $f \in C^0(\mathbb{Z}_p, \mathbb{Q}_p)$, define

$$f^{[0]} = f, \quad f^{[k+1]}(x) := f^{[k]}(x+1) - f^{[k]}(x). \quad \forall k \in \mathbb{Z}_{\geq 0}$$

Put $a_n(f) := f^{[n]}(0)$. $\forall n \in \mathbb{Z}_{\geq 0}$ $\rightsquigarrow (f^{[k]})^{[l]}(x) = f^{[k+l]}(x)$

(The rationale is the following: $a_0(f) = f(0)$ by setting $x=0$ in $(*)$

If $f(x) = \sum a_n(f) \cdot \binom{x}{n}$, then $f^{[1]}(x) = \sum a_n(f) \binom{x}{n-1}$

and inductively $f^{[k]}(x) = \sum a_n(f) \binom{x}{n-k}$. Thus $a_k(f) = f^{[k]}(0)$.)

Explicit formula: $$f^{[n]}(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(x+n-k) \qquad (*)$$

$$a_n(f) = f^{[n]}(0) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k). \qquad (**)$$

From now on, we may assume $\|f\| = 1$.

$\Rightarrow f \in C^0(\mathbb{Z}_p, \mathbb{Z}_p)$ and $\exists\, m \in \mathbb{Z}_{\geq 0}$ s.t. $|f(m)| = 1$. (take the smallest such m)

By explicit formula $(**)$, $|a_n(f)| \leq 1$ for all $n \in \mathbb{Z}_{\geq 0}$, and $|a_m(f)| = 1$.

So we have $\sup_n |a_n(f)| = 1$.

Now, we prove that (1) $a_n(f) \to 0$ as $n \to +\infty$

(2) $f(x) = \sum_{n \geq 0} a_n(f) \binom{x}{n}$.

(1) We need a lemma: For every $f \in C^0(\mathbb{Z}_p, \mathbb{Z}_p)$, $\exists\, k \in \mathbb{Z}_{\geq 1}$ s.t. $f^{[p^k]} \in p \cdot C^0(\mathbb{Z}_p, \mathbb{Z}_p)$

Proof: Consider $\bar{f}: \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_p \xrightarrow{\bmod p} \mathbb{F}_p$ continuous

$\Rightarrow \exists\, k = k(m)$, s.t. $\bar{f}$ is locally constant on each $a + p^k\mathbb{Z}_p$

Then $f^{[p^k]}(x) = \sum_{j=0}^{p^k} (-1)^j \binom{p^k}{j} f(x + p^k - j)$

$= f(x+p^k) - f(x) + p \cdot \boxed{////} \quad \in p \cdot C^0(\mathbb{Z}_p, \mathbb{Z}_p)$. □

From this, we deduce that $a_n(f) \to 0$ as $n \to +\infty$

(2) As $a_n(f) \to 0$ when $n \to +\infty$, $\sum_{n\geq 0} a_n(f)\binom{x}{n} \in C^0(\mathbb{Z}_p, \mathbb{Z}_p)$.

$\Rightarrow f(x) - \sum_{n\geq 0} a_n(f)\binom{x}{n} \in C^0(\mathbb{Z}_p, \mathbb{Z}_p)$ and is zero at $x \in \mathbb{Z}$

$\Rightarrow f(x) = \sum_{n\geq 0} a_n(f)\binom{x}{n}$. □

§3 Distribution on $\mathbb{Z}_p$.

Definition. Define the space of distribution on $\mathbb{Z}_p$ to be

$$\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) := \mathrm{Hom}_{\mathrm{cont}}(C^0(\mathbb{Z}_p, \mathbb{Z}_p), \mathbb{Z}_p)$$

We may "naïvely" identify $\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$

$$A_\mu(T) := \sum_{n\geq 0} b_n T^n \longmapsto \left(f(x) = \sum_{n\geq 0} a_n \binom{x}{n} \mapsto \sum_{n\geq 0} a_n b_n \right)$$

(The condition $a_n \to 0$ implies that $a_n b_n \to 0$, so the sum converges.)

Amice transform: For $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, the corresponding power series $A_\mu(T) = \sum_{n\geq 0} b_n T^n \in \mathbb{Z}_p[\![T]\!]$ admits a formula

$$\int_{\mathbb{Z}_p} (1+T)^x \, d\mu(x) = \int_{\mathbb{Z}_p} \sum_{n\geq 0} \binom{x}{n} T^n \cdot d\mu(x) = \sum_{n\geq 0} T^n \cdot \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) = \sum_{n\geq 0} b_n T^n = A_\mu(T).$$

Theorem $\mu \longmapsto A_\mu(T) := \int_{\mathbb{Z}_p} (1+T)^x \, d\mu(x)$ gives an isomorphism $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \simeq \mathbb{Z}_p[\![T]\!]$.

A better formulation of Amice transform (A good-looking formula must have a canonical explanation)

Definition For a profinite group $G = \varprojlim_{\substack{H \lhd G \\ \text{finite}}} G/H$, define the associate **Iwasawa algebra** for G to be $\mathbb{Z}_p[\![G]\!] = \varprojlim_{\substack{H \lhd G \\ \text{finite}}} \mathbb{Z}_p[G/H]$.

Each $g \in G$ defines an element $[g] \in \mathbb{Z}_p[\![G]\!]$; $\mathbb{Z}_p[G] \subseteq \mathbb{Z}_p[\![G]\!]$ is dense.

Upshot: For G discrete group, there is an equivalence of categories

$$\{\text{representations of } G \text{ on } \mathbb{Z}\text{-modules } M\} \xleftrightarrow{\sim} \{\mathbb{Z}[G]\text{-modules } M\}$$

$$\rightsquigarrow \{\text{continuous representations of } G \text{ on } \mathbb{Z}_p\text{-modules } M\} \xleftrightarrow{\sim} \{\text{continuous } \mathbb{Z}_p[\![G]\!]\text{-modules } M\}$$

In particular, $\{\text{cont. homom. } \eta : G \to \bar{\mathbb{Z}}_p^\times\} \xleftrightarrow{\sim} \{\text{cont. ring homom. } \mathbb{Z}_p[\![G]\!] \to \bar{\mathbb{Z}}_p\}$

$$\tilde{\eta}\left(\sum a_g [g]\right) := \sum a_g \eta(g).$$

Example: $\mathbb{Z}_p[\![\mathbb{Z}_p]\!] \cong \varprojlim_{m\to\infty} \mathbb{Z}_p[\mathbb{Z}_p/p^m\mathbb{Z}_p] \cong \varprojlim_{m\to\infty} \mathbb{Z}_p[x]/(x^{p^m}-1)$ $\qquad x \leftrightarrow [1],\ 1 \leftrightarrow [0]$

$\cong \varprojlim_{m\to\infty} \mathbb{Z}_p[T]/((T+1)^{p^m}-1) \cong \varprojlim_{m\to\infty} \mathbb{Z}_p[T]/(p,T)^m$ $\qquad T \leftrightarrow [1]-1$

$\cong \mathbb{Z}_p[\![T]\!]$

If $\eta : \mathbb{Z}_p \to \bar{\mathbb{Q}}_p^\times$ is a continuous character, it corresponds to

$\tilde{\eta} : \mathbb{Z}_p[\![T]\!] \to \bar{\mathbb{Q}}_p$ $\qquad$ i.e. $\tilde{\eta} \leftrightarrow$ point $T = \eta(1)-1$ on $\operatorname{Spec} \mathbb{Z}_p[\![T]\!]$

$f(T) \mapsto f(\eta(1)-1)$ $\qquad$ viewed as a disc.

Theorem. For any profinite group G, $\mathbb{Z}_p[\![G]\!]$ can be naturally identified with

$$\operatorname{Hom}_{\text{cont}}(C^0(G,\mathbb{Z}_p), \mathbb{Z}_p) = \mathcal{D}_0(G).$$

When $G = \mathbb{Z}_p$, this identification is precisely the Amice transform.

Proof: $\operatorname{Hom}_{\text{cont}}(C^0(G,\mathbb{Z}_p), \mathbb{Z}_p) = \operatorname{Hom}_{\text{cont}}\left(\left(\varinjlim_H C^0(G/H,\mathbb{Z}_p)\right)^\wedge, \mathbb{Z}_p\right)$

$$= \varprojlim_H C^0(G/H,\mathbb{Z}_p)^\vee = \varprojlim_H \mathbb{Z}_p[G/H] \simeq \mathbb{Z}_p[\![G]\!].$$

We need to show $\mathrm{Hom}_{\mathrm{cont}}\left(C^0(\mathbb{Z}_p,\mathbb{Z}_p),\mathbb{Z}_p\right) \xrightarrow{\sim} \mathbb{Z}_p[[\mathbb{Z}_p]] \xrightarrow{\sim} \mathbb{Z}_p[[T]]$

Amice transform

$$\mu \longmapsto A_\mu(T)$$

$$\mathcal{D}_0(\mathbb{Z}_p) = \varprojlim_{m\to\infty} \mathcal{D}_0\left(\mathbb{Z}_p/p^m\mathbb{Z}_p\right) \cong \varprojlim_m \mathbb{Z}_p\left[\mathbb{Z}_p/p^m\mathbb{Z}_p\right] \cong \varprojlim_m \mathbb{Z}_p[T]\Big/(1+T)^{p^m}-1$$

$$\mu \longmapsto \lim_{m\to+\infty} \sum_{a\in\mathbb{Z}_p/p^m\mathbb{Z}_p} \mu\left(a+p^m\mathbb{Z}_p\right)\cdot[a] \longmapsto \lim_{m\to+\infty} \sum_{a\in\mathbb{Z}_p/p^m\mathbb{Z}_p} \mu\left(a+p^m\mathbb{Z}_p\right)(1+T)^a$$

$$\| $$

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

This is indeed a proof....