Math 726: L-functions and modular forms — Fall 2011

Lectures 32-33 : Values of zeta functions

Instructor: Henri Darmon — *Notes written by: Clement Gomez*

Recall from last lectures

$$\forall n \in \mathbb{N}, \zeta(-n) \in \mathbb{Q}$$

The proof is to consider the Mellin transform:
$L(f, s) := \frac{1}{\Gamma(s)} \int_0^\infty f(t) t^s \frac{dt}{t}$.
Then one can show that $L(f, -n) = (-1)^n f^{(n)}(0)$.
On the other hand, by a direct computation, $\zeta(s) = \frac{1}{s-1} L(f, s)$ where $f(t) = \frac{t}{e^t - 1}$
Since $\frac{t}{e^t-1}$ has rational Taylor expansion, we conclude that $\forall n \in \mathbb{N}, \zeta(-n) \in \mathbb{Q}$.

Problem 1. Understand the $p-$adic properties of $\zeta(-n)$:

Idea: Express $\zeta(-n)$ as a $p-$adic Mellin transform of $\frac{t}{e^t-1}$.

Rudiments of $p-$adic integration theory:

Definition 1. A **p-adic Banach** space B is a $\mathbb{Q}_p$-vector space, such that there exists a $\mathbb{Z}_p$-submodule B_0 with the following properties:
$(i) B_0 \to lim_{\leftarrow} B_0/p^n B_0$ is an isomorphism
$(ii) \forall x \in B, \exists n \in \mathbb{Z}$ such that $p^n.x \in B_0$
We can define the valuation for any element of B, by $\mathrm{v}_p(x) := min\{n \in \mathbb{Z} | p^n.x \in B_0\}$.
The norm is then defined by $||x|| := p^{-\mathrm{v}_p(x)}$.

Remark 1. The Banach space is complete relative to this norm and $B_0 =$ unit ball in B.

Example 2. $B = \overline{\mathbb{Q}_p}$ is NOT a Banach space.
Indeed, $B_0 = \mathcal{O}_{\overline{Z_p}} \to lim_{\leftarrow} B_0/p^n B_0$ is NOT an isomorphism
Proof: Considering elements of the form $\sum_{i=1}^\infty b_i p^i$ with $deg(b_i) \to \infty$. Theses elements are in $lim_{\leftarrow} B_0/p^n B_0$ but one can show that some of thoses elements can NOT have finite degree over Q_p.
Let's give an example of this fact. Consider $\alpha := \sum_{k=0}^\infty p^{\frac{1}{2^{k^2}}}.p^k$.

By definition, α belongs to $lim_{\leftarrow} B_0/p^n B_0$.

Suppose that α has degree N over $\mathbb{Q}_p$. Choose n such that $\frac{2^{n^2}N}{2^{(n+1)^2}} < 1$ then $\sum_{k=n+1}^{\infty} p^{\frac{1}{2^{k^2}}}.p^k$ belongs to $\mathbb{Q}_p(p^{\frac{1}{2^{n^2}}}, x)$ which is an extension of degree $\leq 2^{n^2}.N$.

So, $\mathrm{v}_p(\sum_{k=n+1}^{\infty} p^{\frac{1}{2^{k^2}}}.p^k).2^{n^2}.N \in \mathbb{Z}$.

But on the other hand:

$$\mathrm{v}_p(\sum_{k=n+1}^{\infty} p^{\frac{1}{2^{k^2}}}.p^k).2^{n^2}.N = \mathrm{v}_p(p^{\frac{1}{2^{(n+1)^2}}}.p^{n+1})).2^{n^2}.N$$

$$= (n+1).2^{n^2}.N + \frac{2^{n^2}.N}{2^{(n+1)^2}} \text{ is not an element of } \mathbb{Z} \text{ , a contradiction.} \square$$

EXAMPLE 3. We can complete the first example to get a $p-$adic Banach space:

$B = \mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$

$B_0 = \mathcal{O}_{\mathbb{C}_p} = \widehat{\mathcal{O}_{\overline{\mathbb{Q}_p}}}$

EXAMPLE 4. $B = \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) = \{$continuous $\mathbb{Q}_p$-valued functions on $\mathbb{Z}_p\}$

$B_0 = \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$

The property (ii) for a Banach space, follows from the compactness of $\mathbb{Z}_p$. ($f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ has bounded valuation)

EXAMPLE 5. $B = \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$

$B_0 = \mathcal{C}(\mathbb{Z}_p, \mathcal{O}_{\mathbb{C}_p})$

EXAMPLE 6. Let I be an index set:

$B = \ell_\infty(I, \mathbb{Q}_p) := \{(X_i)_{i \in I} \text{ bounded } ||X_i|| \leq C, \forall i \in I\}$

$B_0 = \ell_\infty(I, \mathbb{Z}_p)$

EXAMPLE 7. Let I be an index set:

$B = \ell_1(I, \mathbb{Q}_p) := \{(X_i)_{i \in I}, (X_i) \text{ is "summable" }\}$

$:= \{(X_i) | \sharp\{i \in I | \mathrm{v}_p(X_i) \leq C\} < \infty, \forall C > 0\}$.

$B_0 = \ell_1(I, \mathbb{Z}_p)$

In particular, if (X_i) belongs to $\ell_1(I, \mathbb{Q}_p)$, then $\sum_{i \in I} X_i \in \mathbb{Q}_p$ makes sense.

Definition 8. A **Banach basis** of B is a family of elements $(e_i)_{i\in I}$ in $B_0 \setminus pB_0$, such that $\forall x \in B$ there exists a unique $(x_i)_{i\in I} \in \ell_1(I, \mathbb{Q}_p)$ such that:

$$x = \sum_{i\in I} x_i e_i$$

Theorem 9. *$(e_i)_{i\in I}$ is a Banach basis for B if and only if $(\overline{e_i})_{i\in I}$ is a $\mathbb{F}_p$-basis for B_0/p^nB_0*

Sketch of the proof:

$(\Rightarrow)$

Let $\overline{x} \in B_0/p^nB_0$ and choose x lifting $\overline{x}$. Then, $x = \sum_{i\in I} x_i e_i$. So, $\overline{x} = \sum_{i\in I} \overline{x_i}.\overline{e_i}$ and the sum is finite since $(x_i)_{i\in I}$ belongs to $\ell_1(I, \mathbb{Z}_p)$

$(\Leftarrow)$

Let φ: $\ell_1(I, \mathbb{Q}_p) \to B$

$(x_i)_{i\in I} \to \sum x_i e_i$

φ is injective:

By multiplying $(x_i)_{i\in I}$ by $\mathrm{v}_p((x_i)_{i\in I})$ and by reducting modulo p gives:

$\varphi(x) = 0 \Leftrightarrow \mathrm{v}_p(x) = \infty$.

φ is surjective:

Let $x \in B$. Without a loss of generality, we can assume that $x \in B_0$. By hypothesis, $\overline{x} = \sum_i \overline{x_{1,i}}\ \overline{e_i}$. Take $x^{(0)} := \sum x_{1,i} e_i$ (Recall that the sum is finite).

$x - x^{(0)} \in pB_0$.

By recurrence, $x = x^{(0)} + p.x^{(1)} + ... + p^n.x^{(n)} + ...$ with $x^{(i)}$ linear combination of e_i with coefficients in $\mathbb{Z}_p$.

$\square$

Corollary 1. *Every Banach space has a Banach basis*

Proof:

Consider B_0/pB_0. Let $\overline{e}_{i\in I}$ be a basis for B_0/pB_0. Then, just take e_i lift for $\overline{e_i}$.$\square$

Sometimes, we can easily find an explicit expression of the basis:

Example 10. $B = \ell_1(I, \mathbb{Q}_p)$.

A basis is given by $(e_i)_{i\in I}$ such that $e_i = \delta_i$ ($\delta_i(i) = 1$, $\delta_i(j) = 0$ if $i \neq j$).

But, sometimes, the explicit expression is not that clear.

Example 11. $B = \ell_\infty(I, \mathbb{Q}_p)$

$B_0/pB_0 = functions(I, \mathbb{F}_p)$

We know that there exists a basis. Its existence relies on the full strenght of the axiom of choice but this basis is not countable.

LEMMA 1. *The functions* $\binom{x}{n} := \frac{x(x-1)\dots(x-n+1)}{n!}$ *belong to* $B_0 \setminus pB_0$

Proof: (i) $f_n(x) := \binom{x}{n}$ sends $\mathbb{Z}$ to $\mathbb{Z}$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, it maps $\mathbb{Z}_p$ to $\mathbb{Z}_p \Rightarrow f_n \in B_0$.
(ii) $f_n(n) = 1 \Rightarrow f_n \in B_0 \setminus pB_0$.$\square$

THEOREM 12. ***(Mahler)***
The functions $(f_n)_{n \in \mathbb{N}}$ *are a Banach basis of* $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$

Proof: Define the "discrete derivative" $(\delta f)(x) := f(x+1) - f(x)$ and the Mahler coefficients of f by $a_n(f) := (\delta^n f)(0)$

The proof follows from the lemma

LEMMA 2. *If* f *belongs to* $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ *then:*
$(i)(a_n(f))_{n \geq 0}$ *belongs to* $\ell_1(I, \mathbb{Q}_p)$.
$(ii) f(x) = \sum_0^\infty a_n(f) \binom{x}{n}$, $\forall x \in \mathbb{Z}_p$
$(iii) \mathrm{v}_p(f) = \mathrm{v}_p((a_n(f))_{n \in \mathbb{N}}$, $\forall f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$

Proof of the lemma:

(i) Let's assume without a loss of generality that $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p) \setminus p\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$.
$a_n(f) = (\delta^n f)(0)$
$\mathrm{v}_p(a_n(f)) \geq \mathrm{v}_p(\delta^n f)$ by definition.

The sequence $\mathrm{v}_p(\delta^n f)$ is clearly increasing, since δ preserves $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ so it is enough to show that $\mathrm{v}_p(\delta^n f)$ is unbounded as $n \to \infty$.

f is continuous on $\mathbb{Z}_p$ which is compact, hence f is uniformly continuous.

Hence, for all M, $\exists p^k$ satisfying: $\mathrm{v}_p(f(x+p^k) - f(x)) > M, \forall x \in \mathbb{Z}_p$.

Let $(sf)(x) := f(x+1)$, $\delta = s - 1$.
$(\delta^{p^k} f) = (s-1)^{p^k}(f) = \sum_{j=0}^{p^k} (-1)^j \binom{p^k}{j} s^j.f$
$(\delta^{p^k} f)(x) = f(x) - f(x+p^k) + \sum_{j=1}^{p^k-1} (-1)^j \binom{p^k}{j} f(x+j)$
which means:
$\mathrm{v}_p(\delta^{p^k} f) \geq min(M, 1 + \mathrm{v}_p(f))$

So choosing M such that $M \geq 1 + \mathrm{v}_p(f)$, we get $\mathrm{v}_p(\delta^{p^k} f) \geq 1 + \mathrm{v}_p(f)$.

Then taking $\delta^{p^k} f$ instead of f proves by recurrence that the sequence $\mathrm{v}_p(\delta^n f)$ is unbounded.

(ii) Let $\tilde{f} := \sum_0^\infty a_n(f) \binom{x}{n}$.
$\delta(\binom{x}{n}) = \binom{x+1}{n} - \binom{x}{n} = \frac{(x+1)\dots(x-n+2)}{n!} - \frac{x\dots(x-n+1)}{n!} = \frac{(x+1-(x-n+1))x\dots(x-n+2)}{n!} = \binom{x}{n-1}$
$a_n(\tilde{f}) = (\delta^n \tilde{f})(0) = (\delta^n. \sum_0^\infty a_n(f) \binom{x}{n})(0) = a_n(f)$

The assignement $f \to (a_n(f))_{n \in \mathbb{N}}$ is injective. This is because, if $\delta^n(f)(0) = 0, \forall n \in \mathbb{N}$ then $f(j) = 0, \forall j \in \mathbb{N}$.

(Indeed, $f(0)=0$ so $f(1)-f(0)=0 \Rightarrow f(1)=0$, so $f(2)-2f(1)+f(0)=0 \Rightarrow f(2)=0$ ...)

Hence $f=0$ since $\mathbb{N}$ is dense in $\mathbb{Z}_p$.

Finally, by injectivity, $\tilde{f}=f$.

(iii) Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, we know $f(x)=\sum_0^\infty a_n(f)\binom{x}{n}$

Since $\mathrm{v}_p(\delta^n f) \to \infty$, then $\exists N$ such that $\mathrm{v}_p(f)=\mathrm{v}_p(\sum_{n=0}^N a_n(f)\binom{x}{n})$.

But $\mathrm{v}_p(\sum_0^N a_n(f)\binom{x}{n}) \geq min(\mathrm{v}_p(a_n(f)\binom{x}{n})) \geq min(\mathrm{v}_p(a_n(f))$ since $\binom{x}{n}$ $(n \geq 0)$ belongs to $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$.

So, $\mathrm{v}_p(f) \geq \mathrm{v}_p((a_n(f))_{n\in\mathbb{N}})$.

Reciprocally, if $p^k f \in B_0$, then $\sum_{n=0}^\infty p^k a_n(f)\binom{x}{n} \in B_0$ and we want to show that $\mathrm{v}_p(p^k(a_n(f))_{n\in\mathbb{N}}) \geq 0$.

Let $j=min_{n\in\mathbb{N}}\{n|\mathrm{v}_p(p^k(a_n(f))<0\}$. Then, $\mathrm{v}_p(p^k f(j)) \geq 0$ by hypothesis, but on the other hand $\mathrm{v}_p(\sum_0^\infty p^k a_n(f)\binom{j}{n}) = \mathrm{v}_p(\sum_{n=0}^{j-1} p^k a_n(f)\binom{j}{n} + p^k a_j(f)) = \mathrm{v}_p(p^k a_j(f)) < 0$ which is absurd. So $\{n|\mathrm{v}_p(p^k(a_n(f))<0\}$ is empty and $\mathrm{v}_p((a_n(f))_{n\in N}) \geq \mathrm{v}_p(f)$ which finishes the proof. □

In conclusion, we understand $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) \to \ell_1(\mathbb{N}, \mathbb{Q}_p)$. Now, we would like to understand its dual.

Dual spaces, measures, and integration:

For all this section ,let B be a Banach space.

Definition 13. A **B-valued measure** on $\mathbb{Z}_p$ is a continuous linear map from $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ to B.

Notations: 1/ $D(\mathbb{Z}_p, \mathbb{Q}_p)$ = space of $\mathbb{Q}_p$-valued measures on $\mathbb{Z}_p$.
$D(\mathbb{Z}_p, B)$ = space of B-valued measures on $\mathbb{Z}_p$.
2/ If $\mu \in D(\mathbb{Z}_p, \mathbb{Q}_p)$, we write $\mu(f)=\int_{\mathbb{Z}_p} f(x)d\mu(x)$

Concrete description of $D(\mathbb{Z}_p, \mathbb{Q}_p)$

Theorem 14. *The map* $D(\mathbb{Z}_p, \mathbb{Q}_p) \to \ell_\infty(\mathbb{N}, \mathbb{Q}_p)$

$$\mu \to \mu(\binom{x}{n})$$

is an isomorphism of $p-$*adic Banach spaces, which identifies:*

$$D(\mathbb{Z}_p, \mathbb{Z}_p) := \{\mu|\mu(f) \in \mathbb{Z}_p, \forall f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)\} \textit{ with } \ell_\infty(\mathbb{N}, \mathbb{Z}_p)$$

.

Sketch of the proof: If $\mu \in D(\mathbb{Z}_p, \mathbb{Q}_p)$, $\mu(\binom{x}{n}) \in \mathbb{Q}_p$ have to be bounded. (indeed $\binom{x}{n} \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$, and $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ is a compact so $\mu(\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ is compact).

Conversely, given a sequence $(b_n)_{n\in\mathbb{N}}$ which is bounded, we can define:

$$\mu_b(f) := \sum_{n\in\mathbb{N}} a_n(f) b_n \in \mathbb{Q}_p$$

. □

DEFINITION 15. Given $\mu \in D(\mathbb{Z}_p, \mathbb{Q}_p)$, the **Amice transform** of μ is the power serie;

$$\begin{aligned} A_\mu(T) &:= \sum_{n=0}^{\infty} \mu \binom{x}{n} T^n \\ &= \sum_{n=0}^{\infty} \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) T^n \\ &= \int_{\mathbb{Z}_p} \sum_{n=0}^{\infty} \binom{x}{n} d\mu(x) T^n \\ &= \int_{\mathbb{Z}_p} (1+T)^x d\mu(x) \end{aligned}$$

REMARK 2. $\mu \to A_\mu(T)$ gives an isomorphism $D(\mathbb{Z}_p, \mathbb{Q}_p) \to \mathbb{Q}_p \otimes \mathbb{Z}_p[[T]]$

Let's give some examples (or counterexamples) of measures

EXAMPLE 16. **Haar measure**

We would like to have a measure invariant by translation (1) and with value 1 for the constant function 1 (2):

It should satisfy $\mu(x+a) = \mu(x)$ by (1), but $\mu(x+a) = \mu(x) + a$ by 2/. That's absurd, so there exits NO Haar measure on $\mathbb{Z}_p$.

EXAMPLE 17. **Dirac measure**

Let $a \in \mathbb{Z}_p$. The dirac measure associated to a is defined by the evaluation at a:
$\delta_a(f) := f(a)$
$A_{\delta_a}(T) = \sum_{n=0}^{\infty} \delta_a \binom{x}{n} T^n = \sum_{n=0}^{\infty} \binom{a}{n} T^n = (1+T)^a$