Topics in ANT

Lecture 1

Meetings weekly 9:30 - 13:00

Final grade based on

Homework (weekly)	20 %
Final exam	80 %

Material:

Part I: Local fields.

Part II: p-Adic L-functions.

§1. The Basel problem.

Q: Evaluate

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots = \sum_{n \geq 1} n^{-2} \quad =: \zeta(2)$$

A: (Euler 1735) $\quad \pi^2/6$

Proof will also evaluate more general quantity

$$\zeta(2i) := \sum_{n \geq 1} \frac{1}{n^{2i}}, \qquad i \in \mathbb{Z}_{\geq 1}$$

Consider

$$\sin(\pi z) = \pi z \prod_{n \in \mathbb{Z} \setminus 0} (1 - z/n)$$

then its logarithmic derivative is

$$\pi \cot(\pi z) = \pi \cos(\pi z) / \sin(\pi z)$$

$$= \frac{1}{z} + \sum_{n \in \mathbb{Z} \setminus 0} \frac{1}{z-n}$$

(1) $$= \frac{1}{z} - 2 \sum_{n \geq 1} \zeta(2n) z^{2n-1}$$

On the other hand, using

$$e^{i\theta} = \cos\theta + i \sin\theta$$

we find that

$$\cot(z) = -i \cdot \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}}$$

$$= -i \cdot \frac{e^{2iz} + 1}{e^{2iz} - 1}$$

$$(2) = \frac{1}{z} - \sum \frac{(-1)^{n-1} \cdot 2^{2n} \cdot B_{2n}}{(2n)!} z^{2n-1}$$

where B_i is defined by

$$\frac{t}{e^t - 1} = \sum B_i \cdot \frac{t^i}{i!}$$

(Bernoulli numbers)

Comparing (1) and (2) gives

$$\zeta(2n) = \frac{(2\pi)^{2n} \cdot (-1)^{n+1} \cdot B_{2n}}{2 \cdot (2n)!}$$

$$\left(B_2 = \tfrac{1}{6} \, , \; B_4 = \tfrac{-1}{30} \, , \; B_6 = \tfrac{1}{42} \, , \ldots \right)$$

Later (1859) Riemann showed that

$$\zeta(s) = \sum_{n\geq 1} n^{-s} \qquad (\mathrm{Re}(s)>1)$$

may be analytically continued to all $s \neq 1$, and satisfies functional equation

$$\boxed{\xi(s) = \xi(1-s)},$$

where $\xi(s) = \pi^{-s/2} \cdot \Gamma\left(\frac{s}{2}\right) \cdot \zeta(s)$

It follows that we may rephrase Euler's result as

$$\zeta(1-2n) = \frac{-B_{2n}}{2n} \in \mathbb{Q}$$

§2. Kummer's work on Fermat's Last Theorem

Theorem (Kummer 1847)

Suppose $p > 2$ prime does not divide class number of $\mathbb{Q}(\zeta_p)$. Then

$$x^p + y^p = z^p$$

has no solutions in non-zero integers $x, y, z \in \mathbb{Z}$.

You'll be able to guess some steps of proof, and significance of the class assumption, based on your experience from ANT Mastermath course.

The full argument is difficult, and makes detailed study of unit group $\mathbb{Z}[\zeta_p]^\times$

Kummer's arguments are hugely influential!

We highlight two statements:

① $p > 3$ divides class no. of $\mathbb{Q}(\zeta_p)$

$\iff$ p divides the numerator of B_n for some $n = 2, 4, \ldots, p-3$.

② If $m, n > 0$ even integers,

* NOT divisible by $(p-1)$,

then if $m \equiv n \mod (p-1)p^i$, we have

$$(1 - p^{m-1}) \cdot \frac{B_m}{m} \equiv (1 - p^{n-1}) \cdot \frac{B_n}{n} \pmod{p^{i+1}}$$

Suggests that quantity $(1-p^{n-1}) \cdot \frac{B_n}{n}$ is "continuous" as a function of n, with respect to some strange notion of "distance"

depending on p.

§3. p-Adic numbers

Kummer's result is most naturally understood in terms of p-adic absolute value

$$\left|\tfrac{a}{b}\right|_p := p^{\mathrm{ord}_p(b) - \mathrm{ord}_p(a)} \quad \in \mathbb{R}_{\geq 0}$$

where $\begin{cases} a, b \in \mathbb{Z},\ b \neq 0,\ p \text{ prime} \\ \mathrm{ord}_p(n) = \text{largest integer } N \text{ s.t. } p^N \mid n \end{cases}$

Like the 'usual' absolute value $|x| = \mathrm{sgn}(x) \cdot x \in \mathbb{R}_{\geq 0}$ it satisfies certain abstract properties:

Def: A <u>valuation</u> on a field K is a function

$$\phi : K \longrightarrow \mathbb{R}_{\geq 0} \quad \text{s.t.}$$

① $\phi(x) = 0 \iff x = 0$

② $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in K$

③ $\exists\, C > 0$ such that

$$\phi(x+y) \leq C \cdot \max\{\phi(x), \phi(y)\}$$

The smallest possible C is called the 'norm' of ϕ.

$\phi = |\cdot|$ 'usual' absolute value, norm $= 2$

$\phi = |\cdot|_p$ 'p-adic' absolute value, norm $= 1$.

(non-Archimedean)

The completion (see later) of $\mathbb{Q}$ wrt $|\cdot|$ is $\mathbb{R}$ but can also complete $\mathbb{Q}$ wrt $|\cdot|_p$, obtain field of p-adic numbers $\mathbb{Q}_p$

$$\begin{tikzcd} & & \mathbb{Q} \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] & & \\ \mathbb{R} & \mathbb{Q}_2 & \mathbb{Q}_3 & \mathbb{Q}_5 & \cdots \end{tikzcd}$$

Will do analysis (continuity, convergence, integration, ...). over any of these completions.

Remark: p-Adic numbers are natural and inevitable

(E.g Ostrowski: $|\cdot|^c$ and $|\cdot|_p^c$ are the only non-trivial valuations on $\mathbb{Q}$)

In the 2^{nd} part of this course, we will define p-adic analogues $\zeta_p(s)$ of the Riemann zeta function, which have many deep applications to the study of unit groups & class groups of

$$\mathbb{Q}(\zeta_{p^n}).$$

<u>Theorem</u> (Iwasawa)

There exist integers $\lambda, \mu, \nu \geq 0$ such that for all n large enough, we have

$$\mathrm{ord}_p \left| Cl(\mathbb{Q}(\zeta_{p^n})) \right| = \mu p^n + \lambda n + \nu$$

§ 4. Valuation topology

The first piece of structure we will study on a valued field (k, ϕ) is its topology.

Big differences between

norm $= 1$ (non-archimedean)

norm > 1 (archimedean)

Non-archimedean valuations satisfy ultrametric inequality

$$\phi(x_1 + \cdots + x_n) \leq \max\{\phi(x_1), \ldots, \phi(x_n)\}$$

which is stronger than the triangle inequality

$$\phi(x_1 + \cdots + x_n) \leq \phi(x_1) + \cdots + \phi(x_n).$$

Lemma: A valuation satisfies the triangle inequality $\iff$ its norm is at most 2

Pf: $\Rightarrow$ Clear

$\Leftarrow$ Have $\phi(x_1+x_2) \leq 2 \max\{\phi(x_1), \phi(x_2)\}$

$$\phi(x_1+x_2+x_3+x_4) \leq 4 \max\{\phi(x_1) \cdots \phi(x_4)\}$$

$$\vdots$$

$$\phi(x_1+\cdots+x_{2^n}) \leq 2^n \max\{\phi(x_1) \cdots \phi(x_{2^n})\}$$

Now suppose that $2^{N-1} < k \leq 2^N$, then set

then set $x_{k+1} = \cdots = x_{2^N} = 0$, get

$$\phi(x_1+\cdots+x_k) \leq 2^N \max\{\phi(x_1) \cdots, \phi(x_k)\}$$
$$\leq 2k \max\{\phi(x_1), \ldots, \phi(x_k)\}$$

In particular, setting $x_1 = \ldots = x_k = 1$, get

$$\phi(k) \leq 2k \qquad \text{for all } k \in \mathbb{Z}_{\geq 1}.$$

We deduce that

$$\begin{aligned}\phi(x+y)^n &= \phi\left((x+y)^n\right) \\ &\leq 2(n+1)\max_i\left\{\phi\left(\underbrace{\binom{n}{i}x^i y^{n-i}}_{}\right)\right\} \qquad \in \mathbb{Z} \\ &\leq 4(n+1)\max_i\left\{\binom{n}{i}\phi(x)^i\phi(y)^{n-i}\right\} \\ &\leq 4(n+1)\left(\phi(x)+\phi(y)\right)^n.\end{aligned}$$

Since this holds for all $n \in \mathbb{Z}_{\geq 1}$, get

$$\phi(x+y) \leq \phi(x) + \phi(y). \qquad \square$$

Corollary: Let ϕ be a valuation.
There exists an $r \in \mathbb{R}_{>0}$ such that ϕ^r satisfies the triangle inequality.

The following proposition 'detects' non-archimedean valuations:

<u>Prop</u>: A valuation is non-archimedean $\iff$ $\{\phi(n) : n \in \mathbb{Z}\}$ is bounded.

<u>Pf</u>: $\Rightarrow$ We have $\phi(n) \leq \phi(1) = 1$ by ultrametric inequality.

$\Leftarrow$ Choose $\Phi = \phi^r$ for some $r > 0$ such that Φ satisfies triangle inequality.

Then

$$\Phi(x+y)^n \leq (n+1) \cdot M \cdot \max\{\phi(x), \phi(y)\}^n$$

for any M upper bound for $\{\phi(i) : i \in \mathbb{Z}\}$.

Taking n^{th} roots, get (as $n \to \infty$) that

$$\phi(x+y) \leq \left(\begin{matrix}\text{Goes to } 1\\ \text{as } n \to \infty\end{matrix}\right) \cdot \max\{\phi(x), \phi(y)\}$$

$\square$

<u>Corollary</u>: A valuation on a field of positive characteristic is non-archimedean.

Let ϕ be a valuation on a field K, then get induced topology $\mathcal{T}_\phi$ on K, defined by basis of open neighbourhoods around $x \in K$:

$$U_\varepsilon(x) := \{ y \in K : \phi(x-y) < \varepsilon \}$$

$\varepsilon \in \mathbb{R}_{>0}$

This makes K into a topological field, i.e

$$K \times K \longrightarrow K : (x,y) \longmapsto xy$$

$$K \times K \longrightarrow K : (x,y) \longmapsto x+y$$

$$K^\times \longrightarrow K^\times : x \longmapsto x^{-1}$$

are continuous.