Regular primes and Bernoulli numbers

Murilo Corato Zanarella

October 18, 2019

Algebraic number theory

A *number field* K is a finite field extension of $\mathbb{Q}$. Its *ring of integers* $\mathcal{O}_K$ is the subring of algebraic integers.

$\mathcal{O}_K$ usually does not have unique factorization like $\mathbb{Z}$, but it has unique factorization in prime ideals.

Example

In $K = \mathbb{Q}[\sqrt{-5}]$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and

$$(2) = (2, 1 + \sqrt{-5})^2,$$

but $(2, 1 + \sqrt{-5})$ is not principal.

Class group

Definition

The *class group* $\mathrm{Cl}(K)$ of K is the set of nonzero ideals of $\mathcal{O}_K$ modulo the relation

$$\mathfrak{a} \sim \mathfrak{b} \quad \text{when} \quad (\alpha)\mathfrak{a} = (\beta)\mathfrak{b} \text{ for some } \alpha, \beta \in \mathcal{O}_K,$$

and the group operation is multiplication of ideals.

It measures the failure of $\mathcal{O}_K$ being a UFD, and is always finite.

We denote $h_K = \#\mathrm{Cl}(K)$.

Regular primes

Definition

A prime p is *regular* if $p \nmid h_{\mathbb{Q}[\xi_p]}$.

Why do we care?

Theorem (Kummer 1849)

If $p > 2$ is regular, then $x^p + y^p = z^p$ has no nontrivial solution.

Sketch of proof of case $p \nmid xyz$.

Factor $(x^p + y^p) = (x + y)(x + \xi_p y) \cdots (x + \xi_p^{p-1} y)$. Analize gcd of the terms, and prove each one is a p-power. Use that $\mathfrak{a}^p$ is principal $\implies$ $\mathfrak{a}$ is principal to conclude each term is a principal p-power. $\square$

Bernoulli numbers

Definition

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

Theorem

$$\zeta(1-n) = -\frac{B_n}{n} \quad \textit{for } n \geq 1.$$

So really, Bernoulli numbers $\longleftrightarrow$ special values of ζ.

Goal

Theorem (Kummer 1850)

A prime p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers $B_2, \dots, B_{p-3}$.

Can be seen as an instance of a more general philosophy:

$$\text{special values of L-functions} \longleftrightarrow \text{arithmetic objects}$$

First ingredient: class number formula

Definition

The Dedekind zeta function of a number field K is

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \text{ prime}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1},$$

where $N(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$.

It is analytic in $\mathbb{C} - \{1\}$, with a simple pole at 1, exactly like $\zeta(s) = \zeta_{\mathbb{Q}}(s)$.

First ingredient: class number formula

Theorem (Analytic class number formula)

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{\omega_K\sqrt{|D_K|}}, \text{ where}$$

- $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^r \oplus \mathbb{C}^s$ *as* $\mathbb{R}$*-algebras,*
- $\sqrt{|D_K|}$ *is the volume of the fundamental domain of* $\mathcal{O}_K \subseteq K \otimes_{\mathbb{Q}} \mathbb{R}$,
- ω_K *is the number of roots of unity in* K,
- Reg_K *is the regulator of* K*:* $\mathcal{O}_K^\times \simeq \mathbb{Z}^{r+s-1} \times \{$*roots of unity*$\}$, *and the regulator is a measure of how "big" the generators of* $\mathbb{Z}^{r+s-1}$ *are.*

First ingredient: class number formula

Theorem (Analytic class number formula)

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{\omega_K\sqrt{|D_K|}}$$

All terms except h_K and Reg_K are easy.

For $K = \mathbb{Q}[\xi_p]$, we have $K^+ = \mathbb{Q}[\xi_p + \xi_p^{-1}] = K \cap \mathbb{R}$ its totally real subfield, and $r = 0,\ s = (p-1)/2$ while $r^+ = (p-1)/2,\ s^+ = 0$, and so $r + s - 1 = r^+ + s^+ - 1$. Hence

$$\frac{\mathrm{Reg}_K \omega_K}{\mathrm{Reg}_{K^+}\omega_{K^+}} = \#\mathcal{O}_K^\times/\mathcal{O}_{K^+}^\times = p \cdot 2^{(p-3)/2}.$$

First ingredient: class number formula

Corollary

$$\frac{\zeta_K}{\zeta_{K^+}}(1) = \frac{h_K}{h_{K^+}} \cdot \frac{\pi^{(p-1)/2}}{p^{(p+3)/4}}.$$

Using the factorizations

$$\zeta_K(s) = \prod_{\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}} L(s,\chi), \quad \zeta_{K^+}(s) = \prod_{\substack{\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C} \\ \chi(-1)=1}} L(s,\chi),$$

we get

$$\frac{\zeta_K}{\zeta_{K^+}}(s) = \prod_{\chi \text{ odd}} L(s,\chi).$$

First ingredient: class number formula

Theorem

$$\frac{h_K}{h_{K^+}} = \prod_{\chi \ odd} L(1,\chi) \cdot \frac{p^{(p+3)/4}}{\pi^{(p-1)/2}} = 2p \prod_{\chi \ odd} -\frac{1}{2} L(0,\chi).$$

$L(0,\chi) \in \{$Special values of L-functions$\} \longrightarrow$ Bernoulli numbers?

More on that later.

Second ingredient: cyclotomic units

To analyze h_{K^+}, we need to understand Reg_{K^+}. This amounts to understanding $\mathcal{O}_{K^+}^\times$.

Definition

The *cyclotomic units* are the units of the form

$$c(a) = \xi_p^{(1-a)/2} \frac{\xi_p^a - 1}{\xi_p - 1} \in \mathcal{O}_{K^+}^\times, \quad p \nmid a.$$

Proposition

The cyclotomic units generate $\mathcal{O}_{K^+}^\times \otimes \mathbb{Q}$.

Second ingredient: cyclotomic units

Corollary

If C is the subgroup generated by ± 1 and the cyclotomic units, then $\mathrm{Reg}_{K^+} = \mathrm{Reg}\left(C\right)/\#(\mathcal{O}_{K^+}^{\times}/C)$.

Together with the class number formula:

Theorem

$$h_{K^+} = \frac{\mathrm{res}_{s=1}\zeta_{K^+}(s)\omega_{K^+}\sqrt{|D_{K^+}|}}{2^r(2\pi)^s\mathrm{Reg}(C)} \cdot \#(\mathcal{O}_{K^+}^{\times}/C) = \#(\mathcal{O}_{K^+}^{\times}/C).$$

Recap

Theorem

If C is the subgroup of cyclotomic units, then

$$h_K = 2p \prod_{\chi \text{ odd}} -\frac{1}{2} L(0, \chi) \cdot \#(\mathcal{O}_{K^+}^\times / C).$$

We need to relate these to Bernoulli numbers.

Generalized Bernoulli numbers

Recall that $\frac{t}{e^t-1} = \sum_{n\geq 0} B_n \frac{t^n}{n!}$ satisfy $\zeta(1-n) = -\frac{B_n}{n}$.

Definition

For a character $\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}$, define

$$\sum_{a=1}^{p-1} \frac{\chi(a)te^{at}}{e^{pt}-1} = \sum_{n\geq 0} B_{n,\chi} \frac{t^n}{n!}.$$

Proposition

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}.$$

Generalized Bernoulli numbers

Corollary

$$h_K = 2p \prod_{\chi\ odd} \frac{1}{2} B_{1,\chi} \cdot \#(\mathcal{O}_{K^+}/C).$$

And by definition, $B_{1,\chi} = \frac{1}{p}\sum_{a=1}^{p-1} a\chi(a)$.

And we want to relate $B_{1,\chi}$ with B_n in terms of their divisibilities by p.

p-adic L-functions

Kummer noticed that the Bernoulli numbers satisfy some p-adic properties: If $2m \equiv 2n \mod (p-1)p^{k-1}$ and $2n \not\equiv 0 \mod (p-1)$, then

$$(1-p^{2m-1})\frac{B_{2m}}{2m} \equiv (1-p^{2n-1})\frac{B_{2n}}{2n} \mod p^k.$$

We can rephrase this as

$$\zeta^*(1-2m) \equiv \zeta^*(1-2n) \mod p^k$$

where $\zeta^*(s)$ is obtained by removing the Euler factor at p of $\zeta(s)$.

p-adic L-functions

Turns out that we have this p-adic "continuity" in much more generality.

Choose an embedding $\mathbb{C} \hookrightarrow \mathbb{C}_p$ and consider the character

$\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p$ where $\omega(a)$ is the unique $(p-1)$ root of unity in $\mathbb{Z}_p$

congruent to a modulo p.

Theorem

There is a meromorphic (analytic if $\omega^j \neq 1$) p-adic L-function $L(s, \omega^j)$ in a p-adic disk around $s = 1$ such that

$$L_p(1-n, \omega^j) = -(1-\omega^{j-n}(p)p^{n-1})\frac{B_{n,\omega^{j-n}}}{n} = L^*(1-n, \omega^{j-n}).$$

Moreover, $L_p(s, \omega^j) = a_0 + a_1(s-1) + \dots$ *with* $p \mid a_i$ *for* $i > 0$ *if* $\omega^j \neq 1$.

We can recover the Kummer congruences:

$$(1-p^{2n-1})\frac{B_{2n}}{2n} = -L_p(1-2n,\omega^{2n}) \equiv -L_p(1-2m,\omega^{2m}) = (1-p^{2m-1})\frac{B_{2m}}{2m}$$

but we also get

Corollary

$$\textit{If } p-1 \nmid j+1, \textit{ then } \quad B_{1,\omega^j} \equiv \frac{B_{j+1}}{j+1} \mod p.$$

Proof.

$$-B_{1,\omega^j} = L_p(1-1,\omega^{j+1}) \equiv_p L_p(1-(j+1),\omega^{j+1}) = -(1-p^j)\frac{B_{j+1}}{j+1}. \qquad \square$$

p-adic L-functions

Corollary

$$2p \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi} \equiv \prod_{j=1}^{(p-3)/2} -\frac{1}{2} \frac{B_{2j}}{2j}.$$

Proof.

The odd characters are $\omega, \omega^3, \ldots, \omega^{p-2}$. We have

$\omega^{p-2} = \omega^{-1} = \frac{1}{p} \sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv \frac{p-1}{p} \mod p$, and have $B_{1,\omega^j} \equiv \frac{B_{j+1}}{j+1}$ for $j = 1, 3, \ldots, p-4$. $\square$

Corollary

$p \mid \frac{h_K}{h_{K^+}}$ *if and only if* $p \mid B_{2j}$ *for some* $1 \leq j \leq (p-3)/2$.

What about the cyclotomic units?

Let $E = \mathcal{O}_{K^+}^\times$. Recall that $h_{K^+} = \# E/C$ where C is generated by the units

$$c(a) = \xi_p^{(1-a)/2} \frac{\xi_p^a - 1}{\xi_p - 1}.$$

Looking at the p-component $(E/C)[p^\infty]$ of E/C, we have projectors

$\epsilon_j \in \mathbb{Z}_p(\mathrm{Gal}\,(K/\mathbb{Q}))$

$$\epsilon_j = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^j(a) \sigma_a^{-1}$$

that separates the problem into eigenspaces $\epsilon_j(E/C)[p^\infty]$.

What about the cyclotomic units?

Proposition

$\epsilon_j(C/p^N C)$ is generated by

$$\kappa_j = \prod_{a=1}^{p-1} c(g)^{\omega_N(a)^j \sigma_a^{-1}}$$

where g is a primitive root modulo p and $\omega_N(a) \equiv \omega(a) \mod p^N$ with $\omega_N(a) \in \mathbb{Z}$.

In the same way that the regulator of C was related to special values of L-functions, one may compute

$$\log_p(\kappa_j) \equiv -(\omega^j(g) - 1)\tau(\omega^{-j})L_p(1, \omega^j) \mod p^N.$$

What about the cyclotomic units?

And so, if N is large enough,

Proposition

$$\nu_p(\log_p(\kappa_j)) = \frac{j}{p-1} + \nu_p(L_p(1,\omega^j)).$$

But note $\epsilon_j(E/C)[p^\infty] \neq 0$ if and only if κ_j is a $p-$power. If this is the case, then $\nu_p(\log_p(\kappa_j)) \geq 1$, and so $\nu_p(L_p(1,\omega^j)) > 0$, which means that $p \mid B_{1,\omega^j}$. We conclude that

Theorem

$$p \mid h_{K^+} \implies p \mid \frac{h_K}{h_{K^+}}.$$

Recap

Theorem

$p \mid h_{K^+} \implies p \mid \frac{h_K}{h_{K^+}}$ *and* $\frac{h_K}{h_{K^+}} \equiv (-2)^{-(p-3)/2} \frac{B_2}{2} \frac{B_4}{4} \cdots \frac{B_{p-3}}{p-3} \mod p.$

Corollary (Kummer)

$p \mid h_k \iff p \mid B_2 B_4 \cdots B_{p-3}.$

Beyond class groups

The cyclotomic units form an example of what's called an Euler system, and the relations

$$h_{K^+} = \#(\mathcal{O}_{K^+}^{\times}/C) \quad \text{and} \quad \begin{cases} \log_p(\kappa_j) = (*) \cdot L_p(1, \omega^j) \\ Reg(C) = (*) \cdot \mathrm{res}_{s=1}\zeta_{K^+}(s) \end{cases}$$

are an example of the more general philosophy that there should be certain relations

arithmetic objects $\longleftrightarrow$ Euler systems $\longleftrightarrow$ special values of L-functions

Beyond class groups

While we obtained $h_{K^+} = \#(\mathcal{O}_{K^+}^\times/C)$ using the class number formula, one can use methods pioneered by Kolyvagin to obtain it without the class number formula.

For instance, in the case of elliptic curves E/K the analog of the class number formula is the BSD formula

Conjecture (BSD formula)

$$\mathrm{res}_{s=1} L(E/K, s) = \frac{\Omega_{E/K} \#\text{Ш}(E/K) \mathrm{Reg}(E/K) \prod_{v|N} c_v(E/K)}{(\#E(K)_{\mathrm{tor}})^2}.$$

Beyond class groups

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{\omega_K\sqrt{|D_K|}}$$

$$\longleftrightarrow \mathrm{res}_{s=1}L(E/K,s) = \frac{\Omega_{E/K}\#\text{Ш}(E/K)\mathrm{Reg}(E/K)\prod_{v|N}c_v(E/K)}{(\#E(K)_{\mathrm{tor}})^2}$$

where $\mathcal{O}_K^\times \longleftrightarrow E(K)$, in a way that

$$2^r(2\pi)^s \longleftrightarrow \Omega_E, \quad h_k \longleftrightarrow \#\text{Ш}(E/K),$$

$$\mathrm{Reg}_K \longleftrightarrow \mathrm{Reg}(E/K), \quad \omega_k \longleftrightarrow (\#E(K)_{\mathrm{tor}})^2,$$

$$\frac{1}{\sqrt{|D_K|}} \longleftrightarrow \prod_{v|N} c_v(E/K).$$

Beyond class groups

In the case $K = \mathbb{Q}[\sqrt{-D}]$ for certain D, one can construct an Euler system of Heegner points $\kappa = \{\kappa_n\}$, and when $\mathrm{ord}_{s=1} L(E/K, s) = 1$, one have:

Theorem (Kolyvagin)

$\#\text{Ш}(E/K) = p^{2(\mathcal{M}_0 - \mathcal{M}_\infty)}$ *where* $\mathcal{M}_0, \mathcal{M}_\infty$ *are certain parameters of* κ.

Theorem (Gross–Zagier)

$L'(E, 1) = (*) \cdot \langle \kappa_1, \kappa_1 \rangle_{\mathrm{NT}}$

which in certain cases can be combined to give the BSD formula for $r = 1$.