Are ζ-functions able to solve Diophantine equations?

An introduction to (non-commutative) Iwasawa theory

Otmar Venjakob

Mathematical Institute
University of Heidelberg

CMS Winter 2007 Meeting

Leibniz (1673)

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \frac{\pi}{4}$$

(already known to GREGORY and MADHAVA)

Special values of L-functions

$N \geq 1, \qquad (\mathbb{Z}/N\mathbb{Z})^\times \qquad$ units of ring $\qquad \mathbb{Z}/N\mathbb{Z}.$

Dirichlet Character (modulo N) :

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

extends to $\mathbb{N}$

$$\chi(n) := \begin{cases} \chi(n \bmod N), & (n, N) = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Dirichlet L-function w.r.t. χ :

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad s \in \mathbb{C}, \quad \Re(s) > 1.$$

satisfies:

- Euler product

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}},$$

- meromorphic continuation to $\mathbb{C}$,
- functional equation.

Examples

$\chi \equiv 1$: Riemann ζ-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}},$$

Examples

$\chi \equiv 1$: Riemann ζ-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}},$$

$$\chi_1 : (\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} \to \mathbb{C}^\times, \quad \chi_1(\overline{1}) = 1, \quad \chi_1(\overline{3}) = -1$$

$$L(1,\chi_1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \frac{\pi}{4}$$

Diophantine Equations

Conjectures of Catalan and Fermat

p, q prime numbers

Catalan(1844), Theorem(MIHĂILESCU, 2002):

$$x^p - y^q = 1,$$

has unique solution

$$3^2 - 2^3 = 1$$

in $\mathbb{Z}$ with $x, y > 0$.

Conjectures of Catalan and Fermat

p, q prime numbers

Catalan(1844), Theorem(MIHĂILESCU, 2002):

$$x^p - y^q = 1,$$

has unique solution

$$3^2 - 2^3 = 1$$

in $\mathbb{Z}$ with $x, y > 0$.

Fermat(1665), Theorem(WILES et al., 1994):

$$x^p + y^p = z^p, \quad p > 2,$$

has no solution in $\mathbb{Z}$ with $xyz \neq 0$.

Factorisation over larger ring of integers

ζ_m primitive mth root of unity

$\mathbb{Z}[\zeta_m]$ the ring of integers of $\mathbb{Q}(\zeta_m)$,

e.g. for $m = 4$ with $i^2 = -1$ we have in $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$:

$$x^3 - y^2 = 1 \Leftrightarrow x^3 = (y + i)(y - i)$$

and for $m = p^n$ we have in $\mathbb{Z}[\zeta_{p^n}]$:

$$x^{p^n} + y^{p^n} = (x + y)(x + \zeta_{p^n} y)(x + \zeta_{p^n}^2 y) \cdot \ldots \cdot (x + \zeta_{p^n}^{p^n - 1} y) = z^{p^n}.$$

The strategy

Hope: Use *unique prime factorisation* to conclude a contradiction from the assumption that the Catalan or Fermat equation has a non-trivial solution.

The strategy

Hope: Use *unique prime factorisation* to conclude a contradiction from the assumption that the Catalan or Fermat equation has a non-trivial solution.

Problem: In general, $\mathbb{Z}[\zeta_m]$ is *not* a unique factorisation domain (UFD), e.g. $\mathbb{Z}[\zeta_{23}]$!

Ideals

Kummer: Replace numbers by ‘ideal numbers’:

For ideals(=$\mathbb{Z}[\zeta_m]$-submodules) $0 \neq \mathfrak{a} \subseteq \mathbb{Z}[\zeta_m]$ we have unique factorisation into prime ideals $\mathfrak{P}_i \neq 0$:

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{P}_i^{n_i}$$

Principal ideals: $(a) = \mathbb{Z}[\zeta_m]a$

Ideal class group

$$\begin{aligned} Cl(\mathbb{Q}(\zeta_m)) : &= \{ \text{ ideals of } \mathbb{Z}[\zeta_m]\}/\{ \text{ principal ideals of } \mathbb{Z}[\zeta_m]\} \\ &\cong Pic(\mathbb{Z}[\zeta_m]) \end{aligned}$$

Fundamental Theorem of algebraic number theory:

$$\# Cl(\mathbb{Q}(\zeta_m)) < \infty$$

and

$$h_{\mathbb{Q}(\zeta_m)} := \# Cl(\mathbb{Q}(\zeta_m)) = 1 \Leftrightarrow \mathbb{Z}[\zeta_m] \text{ is a UFD}$$

Nevertheless, $Cl(\mathbb{Q}(\zeta_m))$ is difficult to determine, too many relations!

The L-function solves the problem

How can we compute

$$h_{\mathbb{Q}(i)}?$$

The L-function solves the problem

How can we compute

$$h_{\mathbb{Q}(i)}?$$

It is a mystery that

$$L(s, \chi_1)$$

knows the answer!

The cyclotomic character

Gauß:

$$G(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow[\cong]{\kappa_N} (\mathbb{Z}/N\mathbb{Z})^\times$$

with $g(\zeta_N) = \zeta_N^{\kappa_N(g)}$ for all $g \in G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$

$N = 4$:

$\Rightarrow \chi_1$ is character of Galois group $G(\mathbb{Q}(i)/\mathbb{Q})$

$\Rightarrow L(s, \chi_1)$ (analytic) invariant of $\mathbb{Q}(i)$.

Analytic class number formula for imaginary quadratic number fields:

$$h_{\mathbb{Q}(i)} \quad = \quad \frac{\#\mu(\mathbb{Q}(i))\sqrt{N}}{2\pi} L(1, \chi_1)$$

Analytic class number formula for imaginary quadratic number fields:

$$
\begin{aligned}
h_{\mathbb{Q}(i)} &= \frac{\#\mu(\mathbb{Q}(i))\sqrt{N}}{2\pi} L(1,\chi_1) \\
&= \frac{4\cdot 2}{2\pi} L(1,\chi_1) \\
&= \frac{4}{\pi} L(1,\chi_1) = 1 \quad \text{(by Leibniz' formula)}
\end{aligned}
$$

Analytic class number formula for imaginary quadratic number fields:

$$\begin{aligned} h_{\mathbb{Q}(i)} &= \frac{\#\mu(\mathbb{Q}(i))\sqrt{N}}{2\pi} L(1,\chi_1) \\ &= \frac{4\cdot 2}{2\pi} L(1,\chi_1) \\ &= \frac{4}{\pi} L(1,\chi_1) = 1 \quad \text{(by Leibniz' formula)} \end{aligned}$$

$\Rightarrow \mathbb{Z}[i]$ is a UFD.

A special case of the Catalan equation

Since '$L(s, \chi_1)$ knows the arithmetic' of $\mathbb{Q}(i)$, it is able to solve our problem:

Claim: $x^3 - y^2 = 1$ has no solution in $\mathbb{Z}$.

In the decomposition $x^3 = (y+i)(y-i)$ the factors $(y+i)$ and $(y-i)$ are coprime (easy!)

$\Rightarrow y + i = (a + bi)^3$ for some $a, b \in \mathbb{Z}$

taking $\mathrm{Re}(-)$ and $\mathrm{Im}(-)$ gives: $y = 0$, contradiction!

Regular primes

Similarly $\zeta(s)$ 'knows' for which p

$$Cl(\mathbb{Q}(\zeta_p))(p) = 1$$

holds! Then the Fermat equation does not have any non-trivial solution. But $37 | h_{Cl(\mathbb{Q}(\zeta_{37}))}$!

Iwasawa:

$$Cl(\mathbb{Q}(\zeta_{p^n}))(p) =? \quad \text{for} \quad n \geq 1.$$

The function field case

Number fields versus function fields

$$\mathbb{Q} \longleftrightarrow \mathbb{F}_l(X) = K(\mathbb{P}^1_{\mathbb{F}_l})$$

$$K/\mathbb{Q} \text{ number field } \longleftrightarrow K(C)/\mathbb{F}_l(X) \text{ function field}$$

$C \subseteq \mathbb{P}^n_{\mathbb{F}_l}$ smooth, projective curve, i.e.

$K(C)/\mathbb{F}_l(X)$ finite extension

Counting points on C

$N_r := \#C(\mathbb{F}_{l^r})$ cardinality of $\mathbb{F}_{l^r}$-rational points

$$\begin{aligned} \phi : C &\to C \\ x_i &\mapsto x_i^l \end{aligned}$$

Frobenius-automorphism

Lefschetz-Trace-Formula

$$\begin{aligned} N_r &= \#\{\text{Fix points of } C(\overline{\mathbb{F}_l}) \text{ under } \phi^r\} \\ &= \sum_{n=0}^{2} (-1)^n \mathrm{Tr}\big(\phi^r | \mathbb{H}^n(C)\big) \end{aligned}$$

ζ-function of C, WEIL (1948)

$$\begin{aligned}
\zeta_C(s) := & \prod_{x \,\epsilon\, |C|} \frac{1}{1-(\#k(x))^{-s}}, \quad s \,\epsilon\, \mathbb{C}, \ \Re(s) > 1, \\
= & \exp\Big(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\Big), \qquad t = l^{-s} \\
= & \prod_{n=0}^{2} \det(1-\phi t | \mathbb{H}^n(C))^{(-1)^{n+1}} \\
= & \frac{\det(1-\phi t| \text{“}Pic^0(\overline{C})\text{”})}{(1-t)(1-lt)} \quad \epsilon\, \mathbb{Q}(t)
\end{aligned}$$

Riemann hypothesis for C

ζ_C is a rational function in t and has

poles at: $s = 0, \ s = 1$

zeroes at certain $s = \alpha$ satisfying $\Re(\alpha) = \frac{1}{2}$.

Can the Riemann ζ-function also be expressed as rational function?

Classical Iwasawa theory

Tower of number fields

Studying the class number formula in a whole tower of number fields simultaneously:

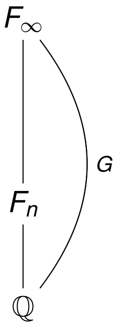
$$\mathbb{Q} \subseteq F_1 \subseteq \ldots \subseteq F_n \subseteq F_{n+1} \subseteq \ldots \subseteq F_\infty := \bigcup_{n \geq 0} F_n.$$

with $F_n := \mathbb{Q}(\zeta_{p^n}),\ 1 \leq n \leq \infty$,

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \ \subseteq\ \mathbb{Q}_p := \mathrm{Quot}(\mathbb{Z}_p),$$

$$\kappa : G := G(F_\infty/\mathbb{Q}) \xrightarrow{\cong} \mathbb{Z}_p^\times,$$

$$g(\zeta_{p^n}) = \zeta_{p^n}^{\kappa(g)} \text{ for all } g \in G, n \geq 0$$



$\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, i.e. $G = \Delta \times \Gamma$ with

$\Delta = G(F_1/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ and

$\Gamma = G(F_\infty/F_1) = \overline{<\gamma>} \cong \mathbb{Z}_p$.

Iwasawa-Algebra

$$\Lambda(G) := \varprojlim_{G' \trianglelefteq G \text{ open}} \mathbb{Z}_p[G/G'] \cong \mathbb{Z}_p[\Delta][[T]]$$

with $T := \gamma - 1$.

p-adic functions

Maximal ring of quotients of $\Lambda(G)$: $\quad Q(G) \cong \prod_{i=1}^{p-1} Q(\mathbb{Z}_p[[T]]).$

$Z = (Z_1(T), \ldots, Z_{p-1}(T)) \in Q(G)$ are functions on $\mathbb{Z}_p$: for $n \in \mathbb{N}$

$$Z(n) := Z_{i(n)}(\kappa(\gamma)^n - 1) \in \mathbb{Q}_p \cup \{\infty\}, \quad i(n) \equiv n \bmod (p-1)$$

Analytic p-adic ζ-function

KUBOTA, LEOPOLDT and IWASAWA:

$\zeta_p \in Q(G)$ such that for $k < 0$

$$\zeta_p(k) = (1 - p^{-k})\zeta(k),$$

i.e. ζ_p interpolates - up to the Euler-factor at p - the Riemann ζ-function p-adically.

Ideal class group over F_∞

IWASAWA: $\#Cl(F_n)(p) = p^{n\,\mathrm{rk}_{\mathbb{Z}_p}(X)+\mathrm{const}}$ where

$$X := X(F_\infty) = \varprojlim_n Cl(F_n)(p) \quad \text{with } G\text{-action},$$

$$\mathbb{Z}_p(1) := \varprojlim_n \mu_{p^n} \quad \text{with } G\text{-action},$$

$$X^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \qquad \mathbb{Q}_p(1) := \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

finite-dimensional $\mathbb{Q}_p$-vector spaces with operation by γ.

Iwasawa Main Conjecture

MAZUR and WILES (1986):

$$\zeta_p \equiv \frac{\det(1-\gamma T | X^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)}{\det(1-\gamma T|\mathbb{Q}_p(1))} \mod \Lambda(G)^\times$$

$$\equiv \prod_i \det(1-\gamma T|\mathbb{H}^i)^{(-1)^{i+1}} \mod \Lambda(G)^\times$$

analytic *algebraic* p-adic ζ-function

'Trace formula'

The analogy

function field	number field
$\overline{\mathbb{F}_l} = \mathbb{F}_l(\mu)$	$F_\infty = \mathbb{Q}(\mu(p))$
ϕ	γ
C	$\mathbb{G}_m$
ζ_C	ζ_p
$Pic^0(\overline{C})$	X'=' $Pic(F_\infty)$

Non-commutative Iwasawa Theory

From $\mathbb{G}_m$ to arbitrary representations

up to now:

coefficients in cohomology: $\mathbb{Z}_p(1)$

$\mathbb{G}_m,\ \mu(p)$

tower of number fields: $F_\infty = \mathbb{Q}(\mu(p))$

Generalisations

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$$

(continuous) representation with $V \cong \mathbb{Q}_p^n$
and Galois-stable lattice $T \cong \mathbb{Z}_p^n$.

ρ → coefficients in cohomology: T

ρ → tower of fields: $K_\infty = \overline{\mathbb{Q}}^{\ker(\rho)}$

Example: E elliptic curve over $\mathbb{Q}$,
$T = T_pE = \varprojlim_n E[p^n] \cong \mathbb{Z}_p^2, \quad V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$

p-adic Lie extensions

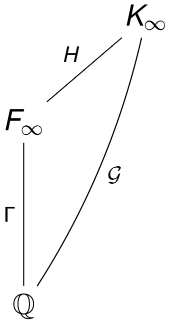
$F_\infty \subseteq K_\infty$ such that

$\mathcal{G} := G(K_\infty/\mathbb{Q}) \subseteq \mathrm{GL}_n(\mathbb{Z}_p)$

is a p-adic Lie group

with subgroup H such that

$$\Gamma := \mathcal{G}/H \cong \mathbb{Z}_p$$



Philosophy

Attach to (ρ, V)

- *analytic* p-adic L-function $\mathcal{L}(V, K_\infty)$ with interpolation property
$$\mathcal{L}(V, K_\infty) \sim L(1, V \otimes \chi)$$
for $\chi : \mathcal{G} \to GL_n(\mathbb{Z}_p)$ with finite image.
- *algebraic* p-adic L-function $F(V, K_\infty)$.

Problem: $\Lambda(\mathcal{G})$ in general not commutative! Non-commutative determinants?

Non-commutative Iwasawa Main Conjecture

COATES, FUKAYA, KATO, SUJATHA, V.:

There exists a canonical localisation $\Lambda(\mathcal{G})_S$ of $\Lambda(\mathcal{G})$, such that $F(V, K_\infty)$ exists in

$$K_1(\Lambda(\mathcal{G})_S).$$

Also $\mathcal{L}(V, K_\infty)$ should live in this K-group.

Main Conjecture:

$$\mathcal{L}(V, K_\infty) \equiv F(V, K_\infty) \mod K_1(\Lambda(\mathcal{G})).$$

Non-commutative characteristic polynomials

$M \quad \Lambda(\mathcal{G})$-module, which is finitely generated $\Lambda(H)$-module

BURNS, SCHNEIDER, V.:

$$\Lambda(\mathcal{G})_S \otimes_{\Lambda(H)} M \xrightarrow[\cong]{\text{“}1-\gamma\text{”}} \Lambda(\mathcal{G})_S \otimes_{\Lambda(H)} M$$

induces “$\det(1-\gamma T|M)$” $\in K_1(\Lambda(\mathcal{G})_S)$.

Main Conjecture over K_∞ :

“Trace formula" in $K_1(\Lambda(\mathcal{G})_S)$ mod $K_1(\Lambda(\mathcal{G}))$:

$$\mathcal{L}(K_\infty, \mathbb{Z}_p(1)) \equiv \det(1-\gamma T|\mathbb{H}^\bullet(K_\infty, \mathbb{Z}_p(1)))$$

New Congruences

If $\mathcal{G} \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$ and coefficients: $\mathbb{Z}_p(1)$

KATO:
$$\begin{array}{ccc} K_1(\Lambda(\mathcal{G})) & \hookrightarrow & \prod_{\chi_i} \mathcal{O}_i[[T]]^\times \\ \downarrow & & \downarrow \\ K_1(\Lambda(\mathcal{G})_S) & \longrightarrow & \prod_{\chi_i} \mathrm{Quot}(\mathcal{O}_i[[T]])^\times \end{array}$$

$$\mathcal{L}(K_\infty/\mathbb{Q}) \longmapsto (L_p(\chi_i, F_\infty))_i$$

Existence of $\mathcal{L}(K_\infty/\mathbb{Q}) \iff$ congruences between $L_p(\chi_i, F_\infty)$
Main Conjecture $/K_\infty \iff$ Main Conjecture $/F_\infty$ for all χ_i

Similar results by RITTER, WEISS for finite H.

A theorem for totally real fields

F totally real, $F_{cyc} \subseteq K_\infty$ totally real,

$\mathcal{G} \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$

MAHESH KAKDE, a student of Coates, recently announced:

Theorem (Kakde)

Assume Leopoldt's conjecture for F. Then the non-commutative Main Conjecture for the Tate motive (i.e. for $= \mathbb{G}_m$) holds over K_∞/F.