An Introduction to Iwasawa Theory

Jordan Schettler

University of California, Santa Barbara

?/?/2012

Outline

Cyclotomic Fields

Notation

Unless noted otherwise, p is an odd prime: 3, 5, 7, 11, 13, 17, 19 . . .

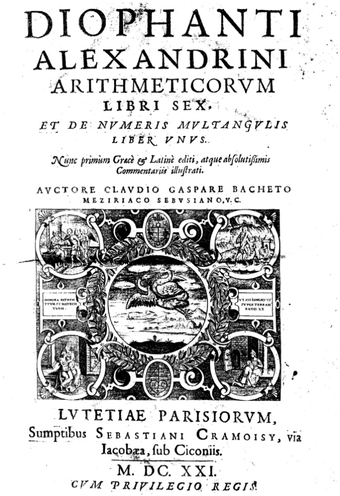
Notation

Unless noted otherwise, p is an odd prime: 3, 5, 7, 11, 13, 17, 19 . . .

Throughout m, n are positive integers.

Diophantus of Alexandria (≈ AD 207–291)

Arithmetica: integer or rational solutions to polynomial equations w/ integer coeff.s



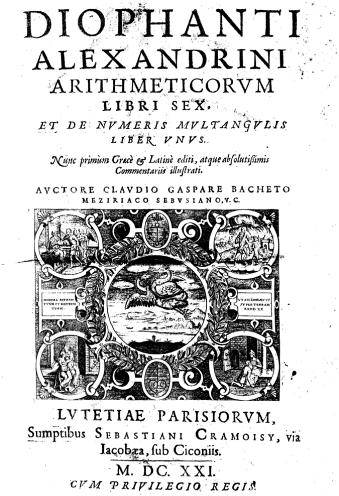
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diophantus of Alexandria (≈ AD 207–291)

Arithmetica: integer or rational solutions to polynomial equations w/ integer coeff.s

E.g., Diophantus noticed there are no tuples of integers (x, y, z) s.t. $x^2 + y^2 = 4z + 3$

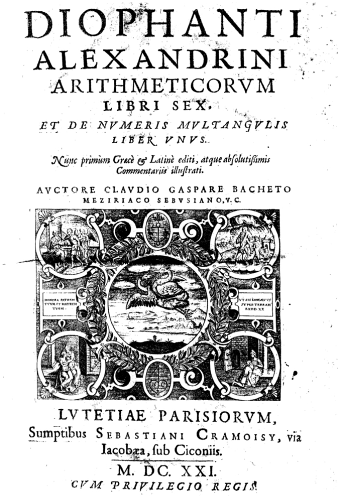


Diophantus of Alexandria ($\approx$ AD 207–291)

Arithmetica: integer or rational solutions to polynomial equations w/ integer coeff.s

E.g., Diophantus noticed there are no tuples of integers (x, y, z) s.t. $x^2 + y^2 = 4z + 3$

We know $\exists\infty$ly many tuples of relatively prime positive integers (x, y, z) s.t. $x^2 + y^2 = z^2$


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Pierre de Fermat (1601–1665)

Fermat claimed that if $n \geq 3$, there are no tuples of positive integers (x, y, z) s.t. $x^n + y^n = z^n$

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat (1601–1665)

Fermat claimed that if $n \geq 3$, there are no tuples of positive integers (x, y, z) s.t. $x^n + y^n = z^n$

OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Fermat proved this conjecture in the case $n = 4$ by the method of infinite descent.

Pierre de Fermat (1601–1665)

Fermat claimed that if $n \geq 3$, there are no tuples of positive integers (x, y, z) s.t. $x^n + y^n = z^n$

OBSERVATIO DOMINI PETRI DE FERMAT.

Cvbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

Fermat proved this conjecture in the case $n = 4$ by the method of infinite descent.

Thus the conjecture boils down to the case $n = p$.

Ernst Kummer (1810–1893)

Suppose (x, y, z) is a tuple of pairwise relatively prime integers s.t. $x^p + y^p = z^p$.

Suppose (x, y, z) is a tuple of pairwise relatively prime integers s.t. $x^p + y^p = z^p$.

As ideals in $\mathbb{Z}[\zeta_p]$:

$$(z)^p = (x^p + y^p) = \prod_{j=0}^{p-1} (x + \zeta_p^j y)$$

Ernst Kummer (1810–1893)

Suppose (x, y, z) is a tuple of pairwise relatively prime integers s.t. $x^p + y^p = z^p$.

As ideals in $\mathbb{Z}[\zeta_p]$:

$$(z)^p = (x^p + y^p) = \prod_{j=0}^{p-1}(x + \zeta_p^j y)$$

Note: $\mathbb{Z}[\zeta_p]$ is a Dedekind domain but not necessarily a PID.

Kummer Continued

If $p \nmid xyz$, the ideals $(x + \zeta_p^j y)$ are pairwise relatively prime.

Kummer Continued

If $p \nmid xyz$, the ideals $(x + \zeta_p^j y)$ are pairwise relatively prime.

Thus $(x + \zeta_p y) = J^p$ is the pth power of an ideal J in $\mathbb{Z}[\zeta_p]$.

Kummer Continued

If $p \nmid xyz$, the ideals $(x + \zeta_p^j y)$ are pairwise relatively prime.

Thus $(x + \zeta_p y) = J^p$ is the pth power of an ideal J in $\mathbb{Z}[\zeta_p]$.

If $p \nmid$ class number of $\mathbb{Q}(\zeta_p)$, then $J = (\alpha)$ is principal,

Kummer Continued

If $p \nmid xyz$, the ideals $(x + \zeta_p^j y)$ are pairwise relatively prime.

Thus $(x + \zeta_p y) = J^p$ is the pth power of an ideal J in $\mathbb{Z}[\zeta_p]$.

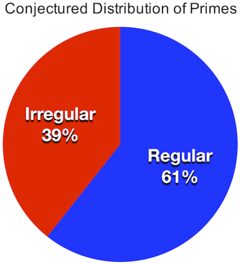
If $p \nmid$ class number of $\mathbb{Q}(\zeta_p)$, then $J = (\alpha)$ is principal,

but $x + \zeta_p y = \varepsilon \alpha^p$ (some unit ε) leads to a contradiction.

Regular versus Irregular Primes

We say a prime p is regular if $p \nmid$ class number of $\mathbb{Q}(\zeta_p)$.

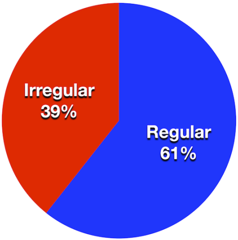
We say a prime p is regular if $p \nmid$ class number of $\mathbb{Q}(\zeta_p)$.



There are ∞ly many irregular primes: $37, 59, 67, 101, \ldots$

but it's unknown if there are ∞ly many regular primes

We say a prime p is regular if $p \nmid$ class number of $\mathbb{Q}(\zeta_p)$.



There are ∞ly many irregular primes: $37, 59, 67, 101, \ldots$

but it's unknown if there are ∞ly many regular primes

Theorem (Kummer's Criterion)

An odd prime p is regular if and only if $p \nmid$ *numerator of* B_j *for all* $j = 2, 4, \ldots, p-3$ *where* $\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$.

Bernoulli Numbers: $\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$

$B_0 = 1, B_1 = -\frac{1}{2}$ while $B_{2n+1} = 0$ for all n and

$$B_2 = \frac{1}{6}, \qquad B_4 = -\frac{1}{30}, \qquad B_6 = \frac{1}{42},$$

$$B_8 = -\frac{1}{30}, \qquad B_{10} = \frac{5}{66}, \qquad B_{12} = -\frac{691}{2730}$$

Bernoulli Numbers: $\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$

$B_0 = 1, B_1 = -\frac{1}{2}$ while $B_{2n+1} = 0$ for all n and

$$B_2 = \frac{1}{6}, \qquad B_4 = -\frac{1}{30}, \qquad B_6 = \frac{1}{42},$$

$$B_8 = -\frac{1}{30}, \qquad B_{10} = \frac{5}{66}, \qquad B_{12} = -\frac{691}{2730}$$

Theorem (Bernoulli's/Faulhaber's Formula)

$$1^n + 2^n + 3^n + \cdots + m^n = \frac{m^{n+1}}{n+1} \sum_{j=0}^{n} \binom{n+1}{j} \frac{B_j}{(-m)^j}$$

In lowest terms,

$$B_{2n} \text{ has denominator} = \prod_{p-1|2n} p$$

More About Bernoulli Numbers

In lowest terms,

$$B_{2n} \text{ has denominator} = \prod_{p-1|2n} p$$

$$B_{2n} \text{ has numerator} = ???$$

In lowest terms,

$$B_{2n} \text{ has denominator} = \prod_{p-1|2n} p$$

$$B_{2n} \text{ has numerator} = ???$$

Theorem (Kummer Congruences)

If $n \equiv m \not\equiv -1 \pmod{p-1}$,

$$\frac{B_{n+1}}{n+1} \equiv \frac{B_{m+1}}{m+1} \pmod{p}$$

Zeta Values

In 1735, Euler showed

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

In general,

$$\frac{1}{1^{2n}} + \frac{1}{2^{2n}} + \cdots = \frac{|B_{2n}|(2\pi)^{2n}}{2(2n)!}$$

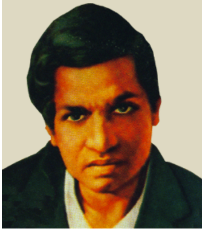
Zeta Values

In 1735, Euler showed

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$$

In general,

$$\frac{1}{1^{2n}} + \frac{1}{2^{2n}} + \cdots = \frac{|B_{2n}|(2\pi)^{2n}}{2(2n)!}$$



In 1913, Ramanujan suggested

$$1 + 2 + 3 + \cdots = -\frac{1}{12}$$

In general,

$$1^n + 2^n + 3^n + \cdots = -\frac{B_{n+1}}{n+1}$$

Bernhard Riemann (1826–1866)

For $\Re(s) > 1$,

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

Bernhard Riemann (1826–1866)

For $\Re(s) > 1$,

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

$\exists!$meromorphic continuation of ζ s.t.

$$\frac{\zeta(s)}{(-s)!} = (2\pi)^{s-1} 2 \sin(s\pi/2) \zeta(1-s)$$

Restatement of Kummer Criterion

Let A denote the p-primary part of the class group of $\mathbb{Q}(\zeta_p)$.

Restatement of Kummer Criterion

Let A denote the p-primary part of the class group of $\mathbb{Q}(\zeta_p)$.

Theorem (Kummer Criterion)

Then $A \neq 0$ if and only if $p | \zeta(-n)$ for some odd n.

Restatement of Kummer Criterion

Let A denote the p-primary part of the class group of $\mathbb{Q}(\zeta_p)$.

Theorem (Kummer Criterion)

Then $A \neq 0$ if and only if $p | \zeta(-n)$ for some odd n.

E.g., we have $691 | \zeta(-11)$. What does the -11 mean here?

$\exists$isomorphism $\phi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/(p))^\times$ given by

$$\sigma(\zeta_p) = \zeta_p^{\phi(\sigma)}$$

The Teichmüller Character

$\exists$isomorphism $\phi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/(p))^\times$ given by

$$\sigma(\zeta_p) = \zeta_p^{\phi(\sigma)}$$

Define $\omega\colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{Z}_p$ via

$$\omega(\sigma) \equiv \phi(\sigma) \pmod{p} \quad \text{and} \quad \omega(\sigma)^{p-1} = 1$$

$G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $A =$ p-primary part of class grp.

‘Eigenespace’ Decomposition

$G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $A = p$-primary part of class grp.

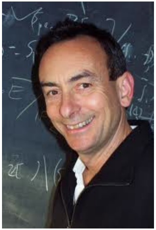
Regard A as a $\mathbb{Z}_p G$-module (written additively):

$$A = \bigoplus_{n=1}^{p-1} A^{\omega^{-n}}$$

where

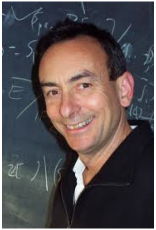
$$\alpha \in A^{\omega^{-n}} \Leftrightarrow \sigma\alpha = \omega(\sigma)^{-n}\alpha \quad \forall \sigma \in G$$

J. Herbrand (1908–1931), K. Ribet (1948–)



Theorem (Herbrand showed $\Rightarrow$, Ribet showed $\Leftarrow$)

Let n be odd. Then $A^{\omega^{-n}} \neq 0 \Leftrightarrow p | \zeta(-n)$.

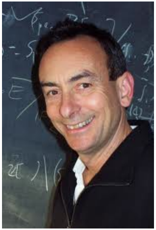


Theorem (Herbrand showed $\Rightarrow$, Ribet showed $\Leftarrow$)

Let n be odd. Then $A^{\omega^{-n}} \neq 0 \Leftrightarrow p | \zeta(-n)$.

E.g., we have $A^{\omega^{-11}} \neq 0$ for $p = 691$.

J. Herbrand (1908–1931), K. Ribet (1948–)



Theorem (Herbrand showed $\Rightarrow$, Ribet showed $\Leftarrow$)

Let n be odd. Then $A^{\omega^{-n}} \neq 0 \Leftrightarrow p | \zeta(-n)$.

E.g., we have $A^{\omega^{-11}} \neq 0$ for $p = 691$.

Conjecturally, $A^{\omega^{-n}} = 0$ for all p and all even n.

Theorem (Higher Kummer Congruences)

If $n \equiv m \not\equiv -1 \pmod{p-1}$ *and* $n \neq m$

$$\left| \frac{\zeta(-n)}{(1-p^n)^{-1}} - \frac{\zeta(-m)}{(1-p^m)^{-1}} \right|_p < |n-m|_p$$

where $|\cdot|_p$ *is the normalized* p*-adic absolute value.*

Theorem (Higher Kummer Congruences)

If $n \equiv m \not\equiv -1 \pmod{p-1}$ *and* $n \neq m$

$$\left| \frac{\zeta(-n)}{(1-p^n)^{-1}} - \frac{\zeta(-m)}{(1-p^m)^{-1}} \right|_p < |n-m|_p$$

where $|\cdot|_p$ *is the normalized p-adic absolute value.*

Theorem (Kubota and Leopoldt, 1964)

$\exists!$*continuous function* $L_p(s, \omega^j)$ *from* $\mathbb{Z}_p$ *to* $\mathbb{Q}_p$ *s.t.*

$$L_p(-n, \omega^j) = \frac{\zeta(-n)}{(1-p^n)^{-1}}$$

whenever $n \equiv j-1 \pmod{p-1}$*.*

Summary So Far

Fermat's Last Theorem for exponent p (an odd prime)

Summary So Far

Fermat's Last Theorem for exponent p (an odd prime)

$\rightsquigarrow$ Study $A = p$-primary part of the class group of $\mathbb{Q}(\zeta_p)$

Summary So Far

Fermat's Last Theorem for exponent p (an odd prime)

$\rightsquigarrow$ Study $A =$ p-primary part of the class group of $\mathbb{Q}(\zeta_p)$

$\rightsquigarrow$ 'Eigenspace' decomposition $A = \bigoplus_{n=1}^{p-1} A^{\omega^{-n}}$

Summary So Far

Fermat's Last Theorem for exponent p (an odd prime)

$\rightsquigarrow$ Study $A =$ p-primary part of the class group of $\mathbb{Q}(\zeta_p)$

$\rightsquigarrow$ 'Eigenspace' decomposition $A = \bigoplus_{n=1}^{p-1} A^{\omega^{-n}}$

$\rightsquigarrow$ For n odd, $L_p(s, \omega^{n+1})$ contains information about $A^{\omega^{-n}}$

$\mathbb{Z}_p$-Extensions

First Examples of $\mathbb{Z}_p$-Extensions

We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/(p^n))^\times$$

We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/(p^n))^\times$$

so (for p odd)

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \ldots)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/(p^n))^\times$$

First Examples of $\mathbb{Z}_p$-Extensions

We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/(p^n))^\times$$

so (for p odd)

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \ldots)/\mathbb{Q}) &\cong \varprojlim_n (\mathbb{Z}/(p^n))^\times \\ &\cong \mathbb{Z}_p^\times\end{aligned}$$

First Examples of $\mathbb{Z}_p$-Extensions

We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/(p^n))^\times$$

so (for p odd)

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \ldots)/\mathbb{Q}) &\cong \varprojlim_n (\mathbb{Z}/(p^n))^\times \\
&\cong \mathbb{Z}_p^\times \\
&= (\text{roots of unity}) \times (1 + p\mathbb{Z}_p)
\end{aligned}$$

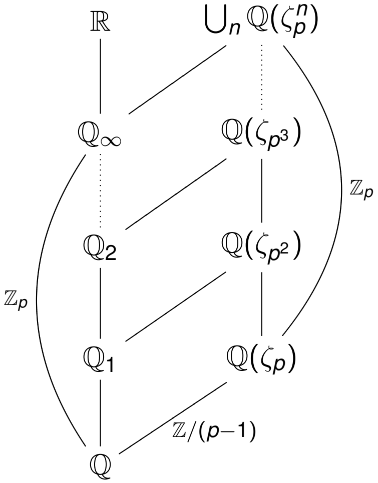
We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/(p^n))^\times$$

so (for p odd)

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \ldots)/\mathbb{Q}) &\cong \varprojlim_n (\mathbb{Z}/(p^n))^\times \\ &\cong \mathbb{Z}_p^\times \\ &= (\text{roots of unity}) \times (1 + p\mathbb{Z}_p) \\ &\cong \frac{\mathbb{Z}}{(p-1)} \oplus \mathbb{Z}_p\end{aligned}$$

First Examples of $\mathbb{Z}_p$-Extensions



The field $\mathbb{Q}_\infty$ above is the *only* $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

The field $\mathbb{Q}_\infty$ above is the *only* $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

There is at least one $\mathbb{Z}_p$-extension of any number field F.

The field $\mathbb{Q}_\infty$ above is the *only* $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

There is at least one $\mathbb{Z}_p$-extension of any number field F.

Namely, there is the cyclotomic $\mathbb{Z}_p$-extension $F\mathbb{Q}_\infty/F$.

The field $\mathbb{Q}_\infty$ above is the *only* $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

There is at least one $\mathbb{Z}_p$-extension of any number field F.

Namely, there is the cyclotomic $\mathbb{Z}_p$-extension $F\mathbb{Q}_\infty/F$.

Note: If $\zeta_p \in F$, then $F\mathbb{Q}_\infty = F(\zeta_p, \zeta_{p^2}, \ldots)$.

General $\mathbb{Z}_p$-Extensions

Now let p be any prime, and suppose F is a number field s.t.

$$\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$$

Now let p be any prime, and suppose F is a number field s.t.

$$\text{Gal}(F_\infty/F) \cong \mathbb{Z}_p$$

The subfields of F_∞ which contain F lie in a tower

$$F \subset F_1 \subset F_2 \subset \ldots \subset F_\infty$$

s.t. for all n

$$\text{Gal}(F_n/F) \cong \mathbb{Z}/(p^n)$$

Kenkichi Iwasawa (1917–1998)

Iwasawa spoke about the next result in his talk *A theorem on Abelian groups and its application to algebraic number theory* at the 1956 summer meeting of the AMS.

Kenkichi Iwasawa (1917–1998)

Iwasawa spoke about the next result in his talk *A theorem on Abelian groups and its application to algebraic number theory* at the 1956 summer meeting of the AMS.

Theorem (Iwasawa's Growth Formula)

Suppose $F \subset F_1 \subset F_2 \dots$ is a $\mathbb{Z}_p$-extension of number fields. Let A_n denote the p-primary part of the class group of F_n. Then $\exists$ integers λ, μ, ν s.t.

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

for all sufficiently large n.

Trivial Iwasawa Invariants λ, μ, ν

Theorem

Let F be a number field with exactly one prime above p. If $p \nmid$ class number of F, then $\lambda = \mu = \nu = 0$ for any $\mathbb{Z}_p$-extension F_∞/F.

Trivial Iwasawa Invariants λ, μ, ν

Theorem

Let F be a number field with exactly one prime above p. If $p \nmid$ class number of F, then $\lambda = \mu = \nu = 0$ for any $\mathbb{Z}_p$-extension F_∞/F.

In fact, $p \nmid$ class number of F_n for all n in this case.

Trivial Iwasawa Invariants λ, μ, ν

Theorem

Let F be a number field with exactly one prime above p. If $p \nmid$ class number of F, then $\lambda = \mu = \nu = 0$ for any $\mathbb{Z}_p$-extension F_∞/F.

In fact, $p \nmid$ class number of F_n for all n in this case.

E.g., consider $F = \mathbb{Q}$, or $F = \mathbb{Q}(\zeta_p)$ for a regular prime p.

Theorem

Suppose F is a number field in which p splits completely. Then $\lambda \geq r_2$ for the cyclotomic $\mathbb{Z}_p$-extension $F\mathbb{Q}_\infty/F$ where $r_2 = \#$ complex primes of F.

Theorem

Suppose F is a number field in which p splits completely. Then $\lambda \geq r_2$ for the cyclotomic $\mathbb{Z}_p$-extension $F\mathbb{Q}_\infty/F$ where $r_2 = \#$ complex primes of F.

E.g., consider $F = \mathbb{Q}(\sqrt{-1})$. If $p \equiv 1 \pmod 4$, then p splits in $F/\mathbb{Q}$, so here $\lambda \geq 1$ for $\mathbb{Q}_\infty(i)/\mathbb{Q}(i)$.

Nontrivial Iwasawa Invariants λ, μ, ν

Theorem

Suppose F is a number field in which p splits completely. Then $\lambda \geq r_2$ for the cyclotomic $\mathbb{Z}_p$-extension $F\mathbb{Q}_\infty/F$ where $r_2 = \#$ complex primes of F.

E.g., consider $F = \mathbb{Q}(\sqrt{-1})$. If $p \equiv 1 \pmod 4$, then p splits in $F/\mathbb{Q}$, so here $\lambda \geq 1$ for $\mathbb{Q}_\infty(i)/\mathbb{Q}(i)$.

What about $r_2 = 0$ (F is totally real)? Can we have $\lambda > 0$?

Iwasawa Modules

Iwasawa's Idea to Derive Growth Formula

Let $L_n = p$-Hilbert class field of F_n. Take $L_\infty = \bigcup_n L_n$.

Iwasawa's Idea to Derive Growth Formula

Let $L_n = p$-Hilbert class field of F_n. Take $L_\infty = \bigcup_n L_n$.

We have $\mathrm{Gal}(L_n/F_n) \cong A_n$ by class field theory.

Let $L_n = p$-Hilbert class field of F_n. Take $L_\infty = \bigcup_n L_n$.

We have $\mathrm{Gal}(L_n/F_n) \cong A_n$ by class field theory.

$g \in \Gamma := \mathrm{Gal}(F_\infty/F)$ acts on $x \in X := \mathrm{Gal}(L_\infty/F_\infty)$ as

$$g \cdot x = \tilde{g} x \tilde{g}^{-1} \text{ where } \tilde{g} \text{ extends } g \text{ to } L_\infty$$

Let $L_n = p$-Hilbert class field of F_n. Take $L_\infty = \bigcup_n L_n$.

We have $\mathrm{Gal}(L_n/F_n) \cong A_n$ by class field theory.

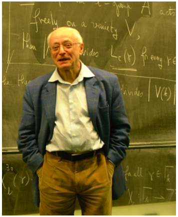
$g \in \Gamma := \mathrm{Gal}(F_\infty/F)$ acts on $x \in X := \mathrm{Gal}(L_\infty/F_\infty)$ as

$$g \cdot x = \tilde{g} x \tilde{g}^{-1} \text{ where } \tilde{g} \text{ extends } g \text{ to } L_\infty$$

If F has only one prime above p, and this prime is totally ramified in F_∞/F, then

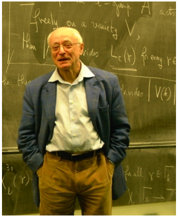
$$X/(\gamma^{p^n} - 1)X \cong A_n \text{ where } \overline{\langle\gamma\rangle} = \Gamma$$

Jean-Pierre Serre (1926–)



Serre's 1959 Seminaire Bourbaki: let T act on X as $\gamma - 1$. Then X becomes a finitely generated, torsion Λ-module where $\Lambda = \mathbb{Z}_p[[T]]$.

Jean-Pierre Serre (1926–)



Serre's 1959 Seminaire Bourbaki: let T act on X as $\gamma - 1$. Then X becomes a finitely generated, torsion Λ-module where $\Lambda = \mathbb{Z}_p[[T]]$.

Then use the structure theory for Λ-modules to compute

$$|X/((T+1)^{p_n} - 1)X|$$

Structure Theorem for Λ-Modules

$\Lambda = \mathbb{Z}_p[[T]]$ is a local Noetherian UFD, but *not* a PID.

Structure Theorem for Λ-Modules

$\Lambda = \mathbb{Z}_p[[T]]$ is a local Noetherian UFD, but *not* a PID.

The prime ideals of Λ are $(0), (p), (p, T)$ and $(f(T))$ where $f(T) \equiv x^{\deg(f)} \pmod{p}$ is an irreducible polynomial.

Structure Theorem for Λ-Modules

$\Lambda = \mathbb{Z}_p[[T]]$ is a local Noetherian UFD, but *not* a PID.

The prime ideals of Λ are $(0), (p), (p, T)$ and $(f(T))$ where $f(T) \equiv x^{\deg(f)} \pmod{p}$ is an irreducible polynomial.

Theorem

Suppose M is a finitely gen'd Λ-module. Then $\exists$homomorphism with finite kernel and cokernel

$$M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \frac{\Lambda}{(p^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(f_i(T)^{n_j})}$$

where each $f_j(T) \equiv x^{\deg(f_j)} \pmod{p}$ is an irred. poly.

Cyclotomic Fields
$\mathbb{Z}_p$-Extensions
Iwasawa Modules
The Main Conjecture

In particular, ∃homom. with finite kernel and cokernel

$$X \longrightarrow \bigoplus_{i=1}^{s} \frac{\Lambda}{(p^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(f_i(T)^{n_j})}$$

where each $f_j(T) \equiv x^{\deg(f_j)} \pmod{p}$ is an irred. poly.

In particular, ∃homom. with finite kernel and cokernel

$$X \longrightarrow \bigoplus_{i=1}^{s} \frac{\Lambda}{(p^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(f_j(T)^{n_j})}$$

where each $f_j(T) \equiv x^{\deg(f_j)} \pmod{p}$ is an irred. poly.

We have a well-defined 'characteristic polynomial'

$$\text{char}(X) = \prod_{i=1}^{s} p^{m_i} \prod_{j=1}^{t} f_j(T)^{n_j}$$

In fact, if λ, μ, ν are as in the growth formula for F_∞/F,

$$\mu = \mathrm{ord}_p(\mathrm{char}(X)) = m_1 + \cdots + m_s$$

$$\lambda = \deg(\mathrm{char}(X)) = n_1 \deg(f_1) + \cdots + n_t \deg(f_t)$$

The Main Conjecture

'Eigenspaces' of X

If $F = \mathbb{Q}(\zeta_p)$, then $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on X.

‘Eigenspaces’ of X

If $F = \mathbb{Q}(\zeta_p)$, then $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on X.

Again, we have a decomposition

$$X = \bigoplus_{n=1}^{p-1} X^{\omega^{-n}}$$

and each $X^{\omega^{-n}}$ is a finitely gen’d torsion Λ-module.

‘Eigenspaces’ of X

If $F = \mathbb{Q}(\zeta_p)$, then $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on X.

Again, we have a decomposition

$$X = \bigoplus_{n=1}^{p-1} X^{\omega^{-n}}$$

and each $X^{\omega^{-n}}$ is a finitely gen’d torsion Λ-module.

Again, $L_p(s, \omega^{n+1})$ contains info about $X^{\omega^{-n}}$.

Main Conjecture

There is a power series $\tilde{L}_p(T, \omega^{n+1}) \in \Lambda = \mathbb{Z}_p[[T]]$ s.t.

$$\tilde{L}_p((1+p)^s - 1, \omega^{n+1}) = L_p(s, \omega^{n+1})$$

for all $s \in \mathbb{Z}_p$.

There is a power series $\tilde{L}_p(T, \omega^{n+1}) \in \Lambda = \mathbb{Z}_p[[T]]$ s.t.

$$\tilde{L}_p((1+p)^s - 1, \omega^{n+1}) = L_p(s, \omega^{n+1})$$

for all $s \in \mathbb{Z}_p$.

Theorem (Mazur and Wiles, 1984)

Suppose n is odd and $n \not\equiv 1 \pmod{p-1}$. Then

$$(\mathrm{char}(X^{\omega^{-n}})) = (\tilde{L}_p(T, \omega^{n+1}))$$

as ideals in Λ.

Thank You!