Algebraic number theory

Sarah Zerbes

December 18th, 2010

Number theory produces, without effort, innumerable problems which have a sweet, innocent air about them, tempting flowers; and yet... number theory swarms with bugs, waiting to bite the tempted flower-lovers who, once bitten, are inspired to excesses of effort!

Outline

Definition

- Upper half-plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$
- j is a complex-valued function on $\mathcal{H}$
- $j(z) = 1726\frac{g_2^3(z)}{\Delta(z)}$, where
  - $\Delta = g_2^3 - 27g_3^2$,
  - $g_2 = 60\sum_{(m,n)\neq(0,0)}(m+nz)^{-4}$,
  - $g_3 = 140\sum_{(m,n)\neq(0,0)}(m+nz)^{-6}$.
- put $q = e^{2\pi iz}$:

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

Importance

Modular forms

- j is invariant under $z \to -\frac{1}{z}$ and $z \to z+1$
- $\Rightarrow$ j is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

- $\Rightarrow$ j is determined by its values on a *fundamental domain*
- modular form = holomorphic function $\mathcal{H} \to \mathbb{C}$ with certain transformation properties under $\mathrm{SL}_2(\mathbb{Z})$
- j is 'almost' a modular form (*almost* because it has the term q^{-1})

Elliptic curves

- Elliptic curves = algebraic curves defined by a cubic in 2 variables with no singular points
- For $\tau \in \mathcal{H}$, consider the cubic curve

$$E(\tau) : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

- isomorphism class of $E(\tau)$ unchanged by action of $\mathrm{SL}_2(\mathbb{Z})$ on τ
- hence determined by $j(\tau)$
- $\Rightarrow j$ classifies isomorphism classes of elliptic curves $/\mathbb{C}$

Class field theory

- j generates certain class of algebraic number fields

Finite group theory

coefficients of q-expansion of j

$$\Leftrightarrow$$

dimensions of linear representations of the Monster

(moonshine conjecture)

Outline

Definition

- elliptic curve $/\mathbb{Q}$ = nonsingular algebraic plane curve

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q}$$

Theorem (Mordell-Weil): For $K/\mathbb{Q}$ finite, $E(K)$ is a finitely generated abelian group.

$\Rightarrow E(K) \cong \Delta_K \times \mathbb{Z}^{r_K}$, where

- Δ_K is finite;
- $r_K \geq 0$ is the rank of E over K.

The L-function

- one can associate to E a complex analytic function $L(E, s)$ *(analogue of Riemann zeta function)*

Birch-Swinnerton-Dyer conjecture:

$$\mathrm{order}_{s=1} L(E, s) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$$

BSD-conjecture

Parity conjecture ($=$ BSD-conjecture mod 2):

$$\mathrm{order}_{s=1} L(E,s) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \mod 2$$

- generalisation to number fields
- construction of elliptic curves with fast-growing ranks over Iwasawa towers
- *People: Dokchitser brothers (Cambridge)*

Iwasawa theory

- Idea: study asymptotic growth of $r_E(F)$ as F varies over a tower of number fields
- let p prime, $F_n = \mathbb{Q}(\mu_{p^n})$, $F_\infty = \bigcup F_n$ and $\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q})$
- *Strategy:* study natural Γ-modules associated to E (Selmer groups)

Main Conjecture: relate Selmer groups to values of $L(E, s)$

$\Rightarrow$ via BSD, get information about the growth of the rank

- *People: Coates (Cambridge), Burns (Kings College)*

Explicit methods

- numercial examples supporting BSD-conjecture and Main Conjecture of Iwasawa theory
- algorithms for determining the rank of elliptic curves
- explicit determination of generators of $E(K)$

- *People: Cremona (Warwick), Fisher (Cambridge)*

Outline

Definition

- a modular form of weight k is an analytic function $f : \mathcal{H} \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

- Examples: Eisenstein series

$$g_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^{2k}}$$

- q-expansion: put $q = e^{2\pi i z}$

$$\Rightarrow f(q) = \sum_{i\geq 0} c_i q^i$$

Basic properties

- the $\mathbb{C}$-vector space of modular forms of weight k is finite-dimensional
- the vector space has a basis consisting of *eigenforms* (simultaneous eigenvector for a collection of linear operators)

mod p modular forms

- if f is an *eigenform*, the q-expansion has algebraic integer coefficients
  $\Rightarrow$ study $f(q) \mod p$ for p prime

Questions:
(1) Which eigenforms are congruent mod p?
(2) Which $\sum_{i \geq 0} c_i q^i \in \overline{\mathbb{F}}_p[[q]]$ arise from a modular form?

- *People: Diamond (Kings' College)*

p-adic families of modular forms

- Basic question: Which eigenforms are congruent mod p^i for $i \geq 1$?
- $\Rightarrow$ construct families of modular forms depending on a p-adic variable
- *People: Buzzard (Imperial), Hill (UCL), Kassaei (Kings)*

Modularity lifting

- any modular form f gives rise to a 2-dimensional p-adic representation V_f of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- **Main question:** given a representation V, is it modular (i.e. equal to V_f for some modular form f)?
- Idea: show V is congruent mod p to a modular representation, then “lift” this to show V is modular
- Known in many cases (e.g. Taniyama-Shimura conjecture: every elliptic curve $/\mathbb{Q}$ is modular)
- *People: Diamond (Kings), Jarvis, Berger, Manoharmayum (Sheffield)*

p-adic representations

- Idea: restrict the representation associated to f to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$
- study this local representation using p-adic analysis (p-adic differential equations)
- $\Rightarrow$ new results in Iwasawa theory about Selmer groups of elliptic curves and modular forms
- *People: Loeffler (Warwick), Zerbes (Exeter)*

Outline

1. The j-invariant
2. Elliptic curves
3. Modular forms
4. Other areas of research

- points on higher-dimensional varieties (Skorobogatov, Siksek,...)
- ramification in number fields (Byott)
- p-adic geometry (Langer, Saidi)
- ...