Brian Conrad: Last Lecture

Addendum #1 $E(\mathbb{Q}_p)_{tors} \xrightarrow{\sim} E(\mathbb{F}_p)$

orders prime to p

e.g. $E_n(\mathbb{Q}_p)_{tors} \xrightarrow{\sim} E(\mathbb{F}_p)$ $\}$ order $= p+1$

$\cup$

$E_n(\mathbb{Q})_{tors} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$

Hensel's lemma ~ P-adic Newton's Method

Addendum 2. For number fields K, $\mathcal{O}_K^\times$ = cyclic

For $E/\mathbb{Q}$ What can we say about $E(\mathbb{Q})_{tors}$?

↳ Google "Mazur, Morel"

Structure of $E(\mathbb{Q})$.

(also works over number fields)

§ 1. Mordell-Weil Theorem

$E(\mathbb{Q})$ is finitely-generated

↳ $E(\mathbb{Q}) \cong$ finite part $\times \mathbb{Z}^r$, $r = \text{rank}(E(\mathbb{Q}))$

Consequences. (i) $|E(\mathbb{Q})_{tors}| < \infty$

(ii) $|E(\mathbb{Q})| = \infty \Rightarrow$ $P \in E(\mathbb{Q})$ with $|P| = \infty$

- The proof itself uses much alg. number theory & alg. geometry
- The method of the proof is a proof by contradiction in the spirit of Fermat's method of infinite descent.
- We cannot yet effectively compute $E(\mathbb{Q})$ (to find generators) using the proof.

Application of M-W Thm.

Can interpret Fermat's pf. of exponent 4 Case of FLT using MW .... see exercises

No a priori bound on the search for generators of $E(\mathbb{Q})$

Ex. (Bremner–Cassels)
E given by $y^2 = x^3 - 877x$
$E(\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}$
$\langle (0,0) \rangle \times \langle P_0 \rangle$ / $P_0 = (x_0, y_0)$, $x_0 = \left(\frac{a}{b}\right)^2$

$a =$ 612 776 683 187 947 368 101
$b =$ 7 884 153 586 063 900 210 } !

Given $\{P_1, \ldots, P_n\} \subset E(\mathbb{Q})$ there is a $\det \in \mathbb{R}$ whose non-vanishing implies linear independence mod $E(\mathbb{Q})_{tors}$

§2 Siegel's Thm.

$E = \{y^2 = f(x)\}$, $f \in \mathbb{Z}[x]$ monic $\Rightarrow |E(\mathbb{Z})| < \infty$

Ex. $y^2 = x^3 - 2 \Rightarrow E(\mathbb{Z}) = \{(3, \pm 5)\}$

There are bounds on the maximum co-ordinate
max. $(|x_0|, |y_0|)$ $(x_0, y_0) \in E(\mathbb{Z})$
Bound $\sim e^{B^{10^6}}$

* We cannot use congruence methods alone to show that $E(\mathbb{Z}) \neq \emptyset$

Remark. MW thm for $E/\mathbb{Q}$ is analogous to Unit theorem for number fields

$$\begin{array}{ccc} E(\mathbb{Q}) & \longleftarrow & \mathcal{O}_K^\times \\ \cup & & \\ E(\mathbb{Q})_{tors} & \longleftarrow & \{\text{roots of unity in } K\} \\ & \sim & \end{array}$$

§ 3. Rank and many Conjectures

- It is conjectured that the rank of of $E(\mathbb{Q})$ can be arbitrarily large

[redacted]

- [redacted]

Tate-Shafarevich Group

$Ш(E/\mathbb{Q})$ = analogue of class group of # field

nontrivial elements corresponds to curves like Selmer's "$3x^3+4y^3+5z^2=0$"

↳ Conjectured to be finite

Know only in very special cases.

Experience shows "most" $E(\mathbb{Q})$ seem to have rank ≤ 1

Conjecture (Goldfeld): "average rank" $= 1/2$

Thm. (Bhargava-Shankar, 2010)

"average rank" < 2

↳ Method produces lots of $E/\mathbb{Q}$ of rank 1

How do we tell if rank > 0

the → BSD conjecture addresses this.
's ↳ relates $rk(E/\mathbb{Q})$ to $\#E(\mathbb{F}_p)$ for good p.

$$L^*(E/\mathbb{Q}, s) = \prod_{p \text{ good}} \left(1 - a_p(E) p^{-s} + p^{1-2s}\right)^{-1} \qquad \cdots\cdots\cdots (1)$$

where $a_p(E) = \#E(\mathbb{Q}) - (p+1) \in [-2\sqrt{p}, 2\sqrt{p}]$

(1) converges nicely for $Re(s) > 3/2$

Thm (Wiles, 1994). $L^*(E/\mathbb{Q}, s)$ can be analytically continued to the whole complex plane via a symmetry $s \leftrightarrow 2-s$

BSD Conjecture:

$$\text{ord}_{s=1} L^*(E/\mathbb{Q}, s) = rk(E).$$

Known Cases (Wiles, Coates, Gross-Zagier, ...):
↳ if $\text{ord}_{s=1} \leq 1$ then ~~conjecture is true~~ known to be ~~known to be true.~~ Conjecture is true

one-way