Some Conjectures of Elliptic Curves

(Notes from Tim Dokchitser)

Ranks

Conjecture
There exists elliptic curves over $\mathbb{Q}$ of arbitrarily large rank.

Current record: Rank = 28 (Elkies)
For over $\mathbb{Q}(t)$, also unbounded?
For over $\mathbb{F}_p(t)$, known to be unbounded. (Shafarevich-Tate)
For a fixed $E/\mathbb{Q} : y^2 = f(x)$, look at the family of its "quadratic twists".

$$E_d : dy^2 = f(x), \qquad d \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$$

In such a family,

Conjecture 1 (Honda)
Rank is bounded.

Conjecture 2
Rank is unbounded.

Conjecture 3 (Goldfield)

$$\begin{aligned} \mathrm{rk}(E_d) &= 0 \qquad \text{for } 50\% \ d\text{'s} \\ &= 1 \qquad \text{for } 50\% \ d\text{'s} \\ &> 1 \qquad \text{for } 0\% \ d\text{'s} \qquad \text{(still infinitely many)} \end{aligned}$$

Selmer and Ш

Recall the Kummer sequence

$$0 \longrightarrow \tfrac{E(\mathbb{Q})}{mE(\mathbb{Q})} \longrightarrow \underset{\text{(not hard)}}{H^1(G_\mathbb{Q}, E[m])} \longrightarrow \underset{\text{(very hard)}}{H^1(G_\mathbb{Q}, E(\overline{\mathbb{Q}}))[m]} \longrightarrow 0$$

where we do not need the $E[m] \subseteq E(\mathbb{Q})$ for the last term.
Restrict to "everywhere locally trivial classes".

Definition
The m-Selmer Group

$$\mathrm{Sel}^{(m)}(E/\mathbb{Q}) := \bigcap_{v \text{ places of } \mathbb{Q}} \ker\left(H^1(G_\mathbb{Q}, E[m]) \to H^1(G_{\mathbb{Q}_v}, E(\overline{\mathbb{Q}_v}))\right)$$

The Tate-Shafaravich Group

$$Ш(E/\mathbb{Q}) = \bigcap_{v \text{ places of } \mathbb{Q}} \ker\left(H^1(G_\mathbb{Q}, E(\overline{\mathbb{Q}})) \to H^1(G_{\mathbb{Q}_v}, E(\overline{\mathbb{Q}_v}))\right)$$

We get an exact sequence

$$0 \to \frac{E(\mathbb{Q})}{mE(\mathbb{Q})} \to \underset{\substack{\text{finite group} \\ \text{(we proved this)} \\ \text{"computable"}}}{\mathrm{Sel}^{(m)}(E/\mathbb{Q})} \to \underset{\substack{\text{obstruction} \\ \text{to } m\text{-descent}}}{Ш(E/\mathbb{Q})[m]} \to 0$$

If $Ш(E/K)[m] = 0$, one can find $E(\mathbb{Q})/mE(\mathbb{Q})$ and therefore $E(\mathbb{Q})$. $(*)$.

Example
For $E/\mathbb{Q} : y^2 = x(x+3)(x-6)$, we found $\mathrm{Sel}^{(2)}$

Conjecture ("Shafarevich-Tate")
$Ш(E/\mathbb{Q})$ is finite.
($\implies$ $(*)$ is okay for all but finitely many $m = p$ primes.)
Known that if Ш is finite, then $|Ш|$ is a square. (Cassels)

The Birch and Swinnerton-Dyer Conjecture

$E/\mathbb{Q}$ elliptic curve is global minimal model.

Definition Zeta Function

$$\begin{aligned} Z_{E/\mathbb{Q}}(s) &= \prod_p \zeta_{\tilde{E}/\mathbb{F}_p}(p^{-s}) \\ &= \prod_p \frac{F_p(p^{-s})}{(1-p^{-s})(1-p^{1-s})} \\ &= \frac{\zeta(s)\zeta(1-s)}{L(E,s)} \end{aligned}$$

with

$$L(E,s) = \prod_p \frac{1}{F_p(p^{-s})} \qquad [L - \text{function of }]$$

with

$$F_p(T) = \begin{cases} 1 - a_pT + pT^2 & p \nmid \Delta_E, a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p) \\ 1 - T & p \text{ split multiplicative} \\ 1 + T & p \text{ non-split multiplicative} \\ 1 & p \text{ additive} \end{cases}$$

with the first case being the most difficult case.
Alternatively,

$$F_p(T) = \det(1 - \mathrm{Frob}^{-1}T(V^{I_p}))$$
$$V = (T_lE \otimes \mathbb{Q}_l)^* \qquad [= H^1_{\text{ét}}(E, \mathbb{Q}_l) \text{ for any } l \neq p]$$

Remark

$$\begin{aligned} L(E,s) &= \prod_{p \nmid \Delta_E} \frac{1}{1 - a_pp^{-s} + p^{1-2s}} \cdot \prod_{p|\Delta_E} \frac{1}{1 - a_pp^{-s}}, \qquad a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p) \text{ in all cases} \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \end{aligned}$$

(i) $a_n \in \mathbb{Z}$, depend on E

(ii) same a_p as above for $n = p$ prime

(iii) $|a_n| \leqslant 2\sqrt{n}$ by Hasse

So this Dirichlet series converges for $\Re(s) > 3/2$.

Definition

$$L^*(E,s) = \Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)\left(\frac{\sqrt{n}}{\pi}\right)^s L(E,s)$$

where N is the conductor of E. (from $G_{\mathbb{Q}} \hookrightarrow T_l E$)

Theorem (Wiles; Taylor-Wiles; Breuil-Conrad-Diamond-Taylor)(1996)
$L(E,s)$ analytic on $\mathbb{C}$ satisfies

$$L^*(E,s) = \pm\, L^*(E, 2-s)$$
$$\hookrightarrow \text{ root number of } E/\mathbb{Q}$$

[Also true over totally real number fields with 'analytic' replaced by 'meromorphic' (Taylor)]

Conjecture (BSD-I)
For $E/\mathbb{Q}$,

$$\underset{\substack{\text{arithmetic}\\ \text{rank}}}{\text{rk}E/\mathbb{Q}} = \underset{\substack{\text{analytic}\\ \text{rank}}}{\text{ord}_{s=1}L(E,s)} = r$$

Conjecture (BSD-II)

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\Omega \cdot R \cdot \prod c_p |Ш|}{|\#E(\mathbb{Q})_{\text{tors}}|^2}$$

R = regulator = $\det(<,>)$ on $E(\mathbb{Q})/\text{torsion}$
$c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ Tamagawa number
$\Omega = \begin{cases} \text{real period if } E(\mathbb{R}) \text{ connected} \\ 2\times \text{ real period otherwise} \end{cases}$ $\left[\int_{-\infty}^{\infty} \frac{dx}{2y+a_1x+a_3}\right]$

Some Known Facts

- If $E \sim E'$ isogenous, then $T_l E \cong T_l E'$ for almost all l, so as expected,
  - $\text{rk}E/\mathbb{Q} = \text{rk}E'/\mathbb{Q}$
  - $\text{BSD}_{E/\mathbb{Q}} = \text{BSD}_{E'/\mathbb{Q}}$ (Cassels) [none of the individual terms have to be equal]
- If $\text{ord}_{s=1}L(E,s) \leqslant 1$, then BSD-I is true, Ш is finite,, BSD-II is true "upto a few primes" (Coates-Wiles, Kolyragin, Gross-Zagier,Rubin,...)
- (Parity Conjecture) If $Ш \supsetneq \mathbb{Q}/\mathbb{Z}$ (- an enormous infinite group), then $\text{rk}E/\mathbb{Q} \equiv \text{ord}_{s=1}L(E,s) \mod 2$
- True, numerically, for millions of curves
- BSD I not known for a single elliptic curve of rank $\geqslant 4$
- BSD II not known for a single elliptic curve of rank $\geqslant 2$
- Analogue (BSD-Tate) for abelian varieties over number fields