The BSD conjecture

David, transcribed by Soham

August 2016

Theorem 1 (Mordell-Weil)**.** $E(\mathbb{Q})$ is a finitely generated abelian group.

This gives us that

$$E(\mathbb{Q}) = T \oplus \mathbb{Z}^r$$

where T is torsion, and we know about its structure due to a (very cool) theorem of Mazur.

Theorem 2 (Hasse)**.** If $E/\mathbb{F}_p$ is an elliptic curve, define

$$a_p = p + 1 - \#E(\mathbb{F}_p).$$

Then $|a_p| \leq 2\sqrt{p}$.

One expects half ....
Recall that

$$\Delta = -16(4a^3 + 27b^2)$$

is the discriminant.
If E has bad reduction mod p, there are three cases:

1. A triple point, then the group of points (leaving out the singular point) is isomorphic to the additive group $\mathbb{F}_p$. "Additive". $a_p = 0$.
2. A double point, with tangent lines having slope in $\mathbb{F}_p$. "Split multiplicative." $a_p = 1$.
3. A double point, with tangent lines having slope in $\mathbb{F}_{p^2}$
$\mathbb{F}_p$. "Nonsplit multiplicative". $a_p = -1$.

Algorithms that decide which of these is the case do exist.

1 L-functions

Definition 1. The L-function of E is

$$L(E, s) := \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s} + p \cdot p^{-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

This "degree-2 L-function" converges for $\mathrm{Re}(s) > \frac{3}{2}$. Analytically continue?
We want a "completed" L-function that has a nice functional equation. Recall that

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} \, \mathrm{d}t$$

Define the *conductor* of E to be

$$N = \prod_{p|\Delta} p^{e_p}$$

where $e_p = 1$ if multiplicative reduction, 2 if additive reduction (these are for $p \geq 5$).
$\varepsilon = \pm 1$ is the "root number".
Define

$$\Lambda(E, s) = N^{s/2} 2\pi^{-s} \Gamma(s) L(E, s)$$

Theorem 3. $\Lambda(E,s)$ analytically continues to all of $\mathbb{C}$, and

$$\Lambda(E, 2-s) = \varepsilon\Lambda(E,s).$$

Proof. $f_E = \sum a_n q^n$, $q = \exp(2\pi i n z) \in S_0(\Gamma_0(N))$. Now a result of Hecke shows that $L(f_E, s) = \sum a_n n^{-s}$, the L-function of the modular form, has an analytic continuation and satisfies a functional equation. □

Conjecture 1 (BSD)**.** If $L(E,s) = \alpha_m(s-1)^m + \cdots$ is the Taylor series around $s=1$, then

$$\text{(analytic rank) } m = r \text{ (algebraic rank)}$$

and

$$\alpha = \frac{\Omega_E \operatorname{Reg}(E) \#(E/\mathbb{Q}) \cdot \prod_p c_p}{(T)^2}$$

where

$$\Omega_E = \int_{E(\mathbb{R})} \frac{\mathrm{d}x}{2y + a_1 x + a_3}$$

is a *period* (somehow related to de Rham!), writing $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. ("Minimal model", minimal discriminant.)

1.1 Heights

2 Moar cohomology, because why not

We have a short exact sequence over $\bar{\mathbb{Q}}$:

$$0 \to E[n] \to E \xrightarrow{n} E \to 0$$