Agashe
PANTS 8
9-19-09

The Birch and Swinnerton-Dyer Conjecture:

§1 Elliptic curves

§2 BSD conjecture

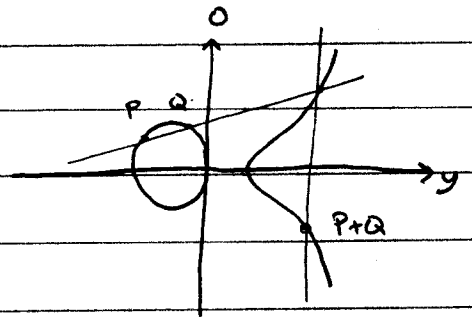
§3 Visibility

§1 Elliptic curves:

F a field, $\mathrm{char}(F) \neq 2, 3$.

Def: An elliptic curve over F is a curve given by $y^2 = x^3 + ax + b$ w/ $a, b \in F$, $4a^3 + 27b^2 \neq 0$ along with a special point O.

Example: $F = \mathbb{Q}$, $E: y^2 = x^3 - x$



Def: If L is a field containing F, then

$$E(L) = \{(x,y) : y^2 = x^3 + ax + b,\ x, y \in L\}$$

Thm: $E/\mathbb{Q}$, then $E(\mathbb{Q})$ is a f.g. abelian group. So $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$.

The goal is to find generators.

The group $E(\mathbb{Q})_{tors}$ is well understood. However, $r = rk(E(\mathbb{Q}))$ is not well-understood. There is a conjecture r can be arbitrarily large, but the largest known r is 28.

Example: $y^2 = x^3 - 673$

$r = 2$ generators $(29, 154)$

$$\left(\frac{33989232357}{617612^2}, \cdots \right)$$

§2 BSD conjecture:

Idea: Consider the number of solutions to E modulo various primes.

Let N_p = number of solutions to "E modulo p."

Example: $y^2 = x^3 - 673$

Only has solutions $(3,2), (3,3), 0$ modulo 5.

$N_5 = 3$.

Hasse: $|N_p - (p+1)| \leq 2\sqrt{p}$.

Idea: If r is large, iff. N_p/p should be large,

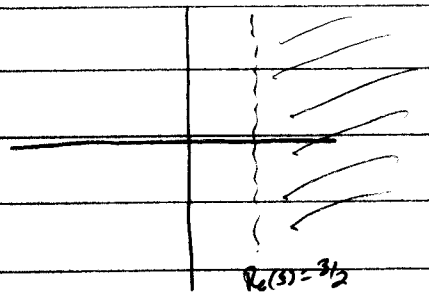
ie,

"$\prod_{p \le X} \frac{N_p}{p}$ should be large".

$$L_E(s) = \prod_{\substack{p \nmid 4a^3-27b^2 \\ p \neq 2}} \left(1 + (N_p - (p+1))p^{-s} + p^{1-2s}\right)^{-1} \prod \text{other factors for } p \text{ of bad reduction}$$

Write $$L_E^*(s) = \prod_{p \nmid 2(4a^3-27b^2)} \left(1 + (N_p - (p+1))p^{-s} + p^{1-2s}\right)^{-1}$$

Converges for $\mathrm{Re}(s) > 3/2$.



There is analytic continuation to $\mathbb{C}$.

$$L_E(1) = \text{"} \prod \frac{1}{1 + (N_p - (p+1))p^{-1} + p^{-1}} = \prod \frac{1}{(N_p/p)}$$

$$L_E(s) = C_t(s-1)^t + C_{t+1}(s-1)^{t+1} + \cdots$$

Conjecture (BSD1): $t = r$, i.e.

$$\operatorname{ord}_{s=1} L_E(s) = \text{rk of } E(\mathbb{Q}).$$

Known: If $\operatorname{ord}_{s=1} L_E(s) = 0, 1$, then $\mathrm{rk}\, E(\mathbb{Q}) = \operatorname{ord}_{s=1} L_E(s)$.

(Due to Gross-Zagier and Kolyvagin)

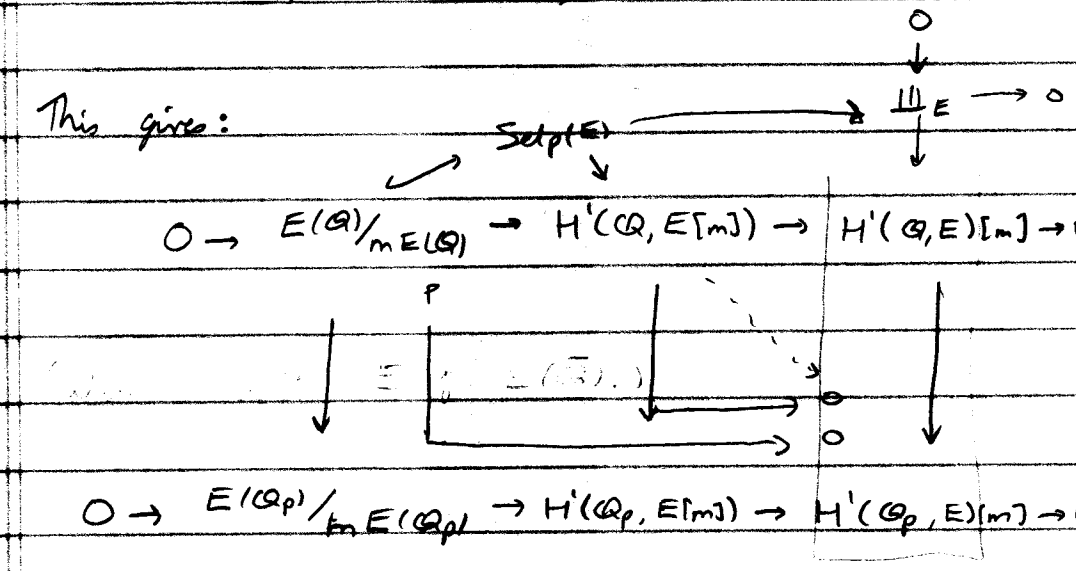
BSD II gives a formula for C_E.

$$0 \to E(\bar{\mathbb{Q}})[m] \to E(\bar{\mathbb{Q}}) \xrightarrow{m} E(\bar{\mathbb{Q}}) \to 0$$

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then $E(\bar{\mathbb{Q}})^{G_{\mathbb{Q}}} = E(\mathbb{Q})$. So we obtain

$$0 \to E(\mathbb{Q})[m] \to E(\mathbb{Q}) \xrightarrow{m} E(\mathbb{Q}) \to H^1(\mathbb{Q}, E(\bar{\mathbb{Q}})[m]) \to H^1(\mathbb{Q}, E(\bar{\mathbb{Q}})) \xrightarrow{\cdot m} H^1(\mathbb{Q}, E(\bar{\mathbb{Q}})) \to \cdots$$

This gives:



$Ш_E$ = Shafarevich-Tate group.

So $Ш_E[m] = \ker\left(H^1(\mathbb{Q}, E)[m] \to H^1(\mathbb{Q}_p, E)[m]\right)$

Real period $= \Omega_E = \int_{E(\mathbb{R})} \frac{dx}{y}$ (Think of as analogue of volume or arc length. measure length wrt the differential dx/y).

$\Phi_p(E)$ = # of components in "E mod p".

= arithmetic component group.

For simplicity, suppose $t=0$.

Conj. (BSD II): $\dfrac{C_t}{\Omega_E} = \dfrac{|Ш_E| \prod_p |\Phi_p(E)|}{|E(\mathbb{Q})_{tors}|^2} \in \mathbb{Q}$.

Ω_E: analytic and contains information modulo p

$|E(\mathbb{Q})_{tors}|^2$: arithmetic

§ Theory of visibility:

Suppose E is contained in some abelian variety $J = J_0(N_E)$.

Suppose there is another elliptic curve $F \subseteq J$, s.t.

$E[m] = F[m]$.

$Ш_E[m]$

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to H^1(\mathbb{Q}, E[m]) \to H^1(\mathbb{Q}, E)[m] \to 0$$

$$\uparrow \quad \uparrow \wr$$

$$0 \to F(\mathbb{Q})/mF(\mathbb{Q}) \to H^1(\mathbb{Q}, F[m]) \to H^1(\mathbb{Q}, F)[m] \to 0.$$

$0 \mapsto 0$, $\bullet \mapsto \bullet$

$\S$ $E(\mathbb{Q})/mE(\mathbb{Q}) = 0$. and $\operatorname{rk} F(\mathbb{Q}) > 0$, i.e.

$F(\mathbb{Q})/mF(\mathbb{Q}) \neq 0$. Go back to picture.

One hopes the element $\bullet$ maps to something in $Ш_E[m]$.

This idea is due to Mazur

Thm: (Dummigan-Stein-Watkins): Suppose N_E = conductor of E is prime and m is a prime that does not divide $N_E(N_E-1)$ Then in the situation above, $m \mid |Ш_E|$.

There exist (explicit) groups G_1, G_2, G_3 s.t.

"Thm": $$\frac{L_E(1)}{\Omega_E} = \frac{|G_1||G_2|}{|G_2|} \stackrel{?}{=} \frac{|Ш_E| \prod |\Phi_p(E)|}{|E(\mathbb{Q})_{tors}||E(\mathbb{Q})_{tors}|}$$

w/ $G_3 \subseteq E(\mathbb{Q})_{tors}$.

Assuming BSD + other hypotheses a prime p divides $|G_1|$ iff "visibility holds w/ $m=p$" and $\therefore$ if $p \mid |G_1|$ Then $p \mid |Ш_E|$.