BSD (part 1).

A/K ab. var

$L(E,s) = \sum a_n \cdot n^{-s}$

$f_E = \sum a_n q^n \in S_2(\Gamma_0(N))$

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

BSD rank: $\operatorname{ord}_{s=1} L(A,s) = r = \operatorname{rank}(A(K))$

Special case: $E/\mathbb{Q}$ Clay Millenium Problem.

BSD formula:

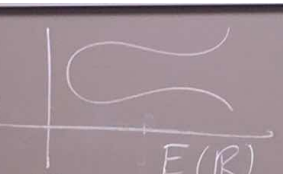
$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \prod c_p \cdot \mathrm{Reg}_E \cdot \#Ш_E}{\#E(\mathbb{Q})_{tor}^2}$$

$\Omega_E \in \mathbb{R}_{>0}$, $c_p \in \mathbb{Z}$, $\mathrm{Reg}_E \in \mathbb{R}_{>0}$, $Ш_E \in \mathbb{Z}_{>0} \cup \{\infty\}$

$\frac{L^{(r)}(E,1)}{r!} \in \mathbb{R}$

$\#E(\mathbb{Q})_{tor} \in \mathbb{Z}$

$\Omega_E = \int_{E(\mathbb{R})} \omega_E \in \mathbb{R}_{>0}$



(elliptic integral)

Gauss AGM.

$E(\mathbb{C}) = \mathbb{C}/\Lambda$

Néron

$c_p = \#\left(\mathcal{E}_{\mathbb{F}_p} / \mathcal{E}^0_{\mathbb{F}_p}\right)(\mathbb{F}_p)$

$c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$

c_p = "fudge factors"

Tamagawa numbers.

Exercise:

- 11a $c_{11} = 5$
- $c_p = 1 \ \forall p \nmid N_E$
- Find curve with $c_p = 37$

Tate's algorithm

- 1 for good primes
- ≤ 4 for additive primes or nonsplit multiplicative $\propto G_a$ twist G_m
- $\text{ord}_p(\Delta)$ split mult reduction $\propto G_m$

$= -\text{ord}_p(j(E))$

- Reg_E :

$h : E(\mathbb{Q}) \to \mathbb{R}$

$h(nP) = n^2 h(P)$

$h(\text{torsion}) = 0.$

$h(P) = \lim_{m \to \infty} \frac{H(2^m P)}{4^m}$

$H(P) = \max(\log(\text{numer}(x(P))), \log(\text{denom}(y(P))))$

"number of digits"

$H(nP) \not\approx n^2 P$

- $E(\mathbb{Q})_{tor} \hookrightarrow E(\mathbb{F}_p)$ for $p \gg 0$.

$P+P+P+P+P=O$

Ifti Burhanudin : ~~linear in input~~ quasi-

BSD formula:

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \prod c_p \cdot \mathrm{Reg}_E \cdot \#Ш_E}{\#E(\mathbb{Q})_{tor}^2}$$

$L^{(r)}(E,1) \in \mathbb{R}$, $r \in \mathbb{Z}_{\geq 0}$, $\Omega_E \in \mathbb{R}_{>0}$, $c_p \in \mathbb{Z}$, $\mathrm{Reg}_E \in \mathbb{R}_{>0}$, $Ш_E \in \mathbb{Z}_{>0} \cup \{\infty\}$, $\#E(\mathbb{Q})_{tor} \in \mathbb{Z}$

$Ш(E)$ = { genus 1 curves X equipped with $E \times X \to X$ / $\mathbb{Q}$ } / $\sim$ ⊆ { all the X's } $WC(E/\mathbb{Q})$ Weil-Chatelet

simply transitive group action

$P, Q \mapsto Q - P$ such that $X(\mathbb{Q}_v) \neq \emptyset$ for all $v = 2, 3, \ldots, \infty$

Ex.

E: $x^3 + y^3 + 60z^3 = 0$ (twist of $y^2 = x^3 + 1$)

$-(1:-1:0)$

X: $3x^3 + 4y^3 + 5z^3 = 0$ $\in Ш(E)$

$\ker\left(H^1(\mathbb{Q}, E) \to \prod_v H^1(\mathbb{Q}_v, E) \right)$

$g = \frac{(d-1)(d-2)}{2}$

(Barry Mazur in Bulletins) Similar for $\frac{L(\cdots)}{\cdots} \in \mathbb{Q}$

Open Problem: Show $Ш(E)$ is finite for at least one E with $r_{an}(E) \geq 2$.

Theorem (Gross-Zagier-Kolyvagin-Murty)

If $r_{an} = \operatorname{ord}_{s=1} L(E, s) \leq 1$ then $Ш(E)$ is finite. (and computable)