Birch-Swinnerton-Dyer Conjecture:

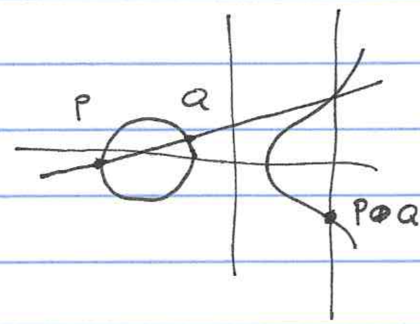
E/K an elliptic curve over a number field

$$E: \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in K$$

$E(K) = \{$solutions of eqn in $K\} \cup \{$pt. at infinity$\}$

- abelian group.

Over $\mathbb{R}$:



<u>Theorem (Mordell-Weil):</u> $E(K)$ is finitely generated, i.e.

$$E(K) \simeq \mathbb{Z}^r \oplus (\text{finite grp}).$$

<u>Def:</u> $\text{rk } E/K$ = rank of $E(K)$

$= r$ if $E(K) \simeq \mathbb{Z}^r \oplus (\text{finite grp})$

(known as ~~algebraic~~ arithmetic rank or Mordell-Weil rank)

<u>Remark:</u> Q: Can $\text{rk}(E/\mathbb{Q})$ be arbitrarily large?

Recently:

- Every E/K has a quadratic twist of rank ≤ 1. (Mazur Rubin)
- A positive proportion of $E/\mathbb{Q}$ have rank 0.

<u>Def:</u> The L-function of E/K is given by

$$L(E/K, s) = \prod_{\substack{v \\ E \text{ has good} \\ \text{red.}}} \left(1 - a_v Nm v^{-s} + (Nm v)^{1-2s}\right)^{-1}$$

$$\cdot \prod_{\substack{v \\ \text{mult.} \\ \text{red}}} \left(1 - a_v Nm v^{-s}\right)^{-1} \qquad \operatorname{Re}(s) > 3/2$$

Remark: $\forall v$, the local factor at $s=1$ is $Nm v / |\tilde{E}(k_v)|$
where $\tilde{E}(k_v)$ = points on E mod v.
(Look over $\mathbb{Q}$ to see you get the familiar thing)

Remark: The Hasse-Weil conjecture is that $L(E/K, s)$ has analytic continuation to $\mathbb{C}$ and satisfies a functional equation $s \longleftrightarrow 2-s$.
This is known for $E/\mathbb{Q}$ by (Wiles, Taylor-Wiles, BCDT).

Def: The analytic rank of E/K is
$$\operatorname{rk}_{an}(E/K) = \operatorname{ord}_{s=1} L(E/K, s).$$

Over $\mathbb{Q}$ the BSD conjecture is due to Birch and Swinnerton-Dyer, over K it is due to Tate.

BSD Conj: 1) $\operatorname{rk}(E/K) = \operatorname{rk}_{an}(E/K)$

2) Fix a K-rational invariant differential form for E/K
(ex: $\omega = \dfrac{dx}{2y + a_1 x + a_3}$)

The leading term of $L(E/K, s)$ at $s=1$ is

$$\frac{1}{r!} L^{(r)}(E/K, 1) = \frac{\mathrm{Reg}(E/K)\, \#Ш(E/K) \prod_{v|\infty} \Omega(E,\omega) \prod_{v\nmid\infty} \mathcal{E}_v(E/K,\omega)}{\sqrt{|\Delta_K|}\ |E(K)_{tors}|^2}.$$

where

- Δ_K = discriminant of K
- $\Omega_v(E,\omega) = \begin{cases} \int_{E(K_v)} |\omega| & K_v = \mathbb{R} \\ \left| 2\int_{E(K_v)} \bar{\omega} \times \omega \right| & K_v = \mathbb{C} \end{cases}$
- $E(K)_{tors}$ = points of finite order in $E(K)$

  Recall: · $E(K)[p] \leq \tilde{E}(k_v)$ when E has good reduction at $v \nmid p$, k_v = residue field.

  · $\forall\, E/\mathbb{Q}$, $|E(\mathbb{Q})_{tors}| \leq 16$
- $\mathrm{Reg}(E/K)$ = regulator = $\det H$

  H $r \times r$ matrix $\quad r = \mathrm{rk}(E/K)$

  if $E(K)/E(K)_{tors}$ is generated by $P_1, \dots, P_r$

  then $H_{ij} = \langle P_i, P_j \rangle$ (canonical height pairing)
- $\mathcal{E}_v(E/K,\omega) = c_v \left| \frac{\omega}{\omega_v^\circ} \right|_v$

  c_v = local Tamagawa number $= \# E(K_v)/E_0(K_v)$

  pts that reduce to 0

  ω_v° = Neron diff. at v

  = diff. that corresponds to $\frac{dx}{2y + a_1 x + a_3}$ for a minimal model.

  Over $\mathbb{Q}$, there is a global minimal model so can choose $\omega = \omega_v^\circ$ and we get only Tamagawa number contribution.
- $Ш(E/K)$ = Shafarevich-Tate group

  $\mathrm{Ker}\left(H^1(K,E) \to \prod_v H^1(K_v, E) \right)$.

  · scary thing.

- Conjecture (S-T) $|Ш(E/K)| < \infty$
- If finite, it has square order (Cassels)

We want to compute r: $E(K)/E(K)_{tors}$ with $\mathbb{Z}$-basis $P_1, \dots, P_r$. Consider $\frac{1}{5}P$, $P = P_i$ some i.
(i.e, take Q with $5Q = P$)
Assume $E[5] \leq E(K)$.
$P \longmapsto K(\frac{1}{5}P) = F$
$Gal(F/K) \leq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
This map is almost injective, so we can study this problem via Galois theory.
So we can study $Gal(F/K) \leq (\mathbb{Z}/5\mathbb{Z})^2$ where locally F comes from $\frac{1}{5}P$.
e.x. for $v \nmid 5$, good reduction, F/K must be unramified.
There are only finitely many such field extension and can use class field theory to compute.
Really are studying $E(K)/5E(K)$.
Finding the subgrps is like studying $Hom(G_K, (\mathbb{Z}/5\mathbb{Z})^2)$ via looking at kernel to get subgroups and then fixed field of this to get field ext.
If one removes the assumption that $E[5] \leq E(K)$, one get $H^1(K, E[5])$ instead of Hom's. Imposing the local conditions then gives the 5-Selmer group.
Then $Ш(E/K)[5]$ morally is the extensions one gets with correct Galois structure and local properties not coming from global points.

Vlad
6-27-11
pg 5

Exercises: 1) Suppose $E/\mathbb{Q}$ has good reduction at 2 & 3, prove $\# E(\mathbb{Q})_{tors} \leq 21$

2) $E/\mathbb{Q}$; $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$, $\alpha, \beta, \gamma \in \mathbb{Q}$

Compute an upper bound on rk $E/\mathbb{Q}$.

Today we will talk about $\tau_v(E,\omega) = c_v \left|\frac{\omega}{\omega_v^\circ}\right|_v$.

Reduction mod v:

Recall: j_E = j-invariant

Δ_E = discriminant of a fixed model

For $y^2 = x^3 + Ax + B$, then

$$j_E = \frac{-1728(4A)^3}{\Delta_E}$$

$$\Delta_E = -16(4A^3 + 27B^2).$$

A change of coordinates $x = u^2x' + s$, $y = u^3y' + u^2sx' + t$ gives $u^{12}\Delta_E' = \Delta_E$ and j_E is the same. This gives them for more general models.

Fix a place v and consider E/K_v.

Minimal model for E = a model with $a_i \in \mathcal{O}_{K_v}$ and $\mathrm{ord}_v(\Delta_E)$ as small as possible. Corresponding discriminant is $\Delta_{E,v}^{\min}$. This is well-defined only up to scaling by u^{12} for $u \in \mathcal{O}_{K_v}^\times$ since it is only defined via ord_v.

Now reduce this mod v: $\tilde{E}$ = the non-singular part of the curve mod v.

$$E(K_v) \supset E_0(K_v) \supseteq E_1(K_v)$$

$E_0(K_v)$: pts of non-singular reduction; $E_1(K_v)$: pts that reduce to O.

Then $\cdot\ E_0(K_v)/E_1(K_v) \simeq \tilde{E}(k_v)$ where k_v is the residue field. (finite)

$\cdot\ \left|E(K_v)/E_0(K_v)\right| = c_v$. Thus for good reduction, $c_v = 1$.

(finite)

$\cdot\ E_1(K_v) \simeq \hat{E}(\mathfrak{m}_v)$ max ideal at v.

$\hat{E}$: formal grp

Reduction types:		$\mathrm{ord}_v(\Delta_{E_v}^{min})$	c_v
Good reduction	$\tilde{E}$ is an ell. curve	0	1
Split mult. red.	$\tilde{E}(\bar{k}_v) = \bar{k}_v^*$ if split, $\tilde{E}(k_v) = k_v^*$	any $n \in \mathbb{Z}_{>0}$	n
nonsplit mult red.	becomes split mult over imag. quad. unram. ext	any $n \in \mathbb{Z}_{>0}$	1 n odd 2 n even
add. red.	$\tilde{E}(\bar{k}_v) = (\bar{k}_v, +)$ becomes good or mult. after a suitable ramified ext	if potentially good, res. char $\neq 2,3$, then 2,3,4,6,8,9,10	<4 given by Tate's alg.

If reduction is semistable (good/mult), it remains good/mult in all field extensions. (split remains split, nonsplit may become split). and the minimal model is the same.

If $\quad \mathrm{ord}_v(j_E) \geq 0 \iff$ good or potentially good red.

$\quad \mathrm{ord}_v(j_E) < 0 \iff$ mult./pot. mult. $\quad K_v(\sqrt{-6B})$ check this

For $y^2 = x^3 + Ax + B$ mult/pot. mult, then $K_v(\sqrt{B})/K_v$ is trivial/quad. unram./ramified $\iff$ split mult/nonsplit/add. pot. mult.

<u>Remark:</u> If $\quad \omega = \dfrac{dx}{2y + a_1 x + a_3}$ for a given model, then

$$\left|\frac{\omega}{\omega_v^\circ}\right|_v^{12} = \left|\frac{\Delta_E}{\Delta_{E,v}^{min}}\right|_v .$$

(because for the min. model $\omega = \omega_v^\circ$ and in general change of coordinates changes $\omega' = u^{-1}\omega$.)

<u>Remark:</u> For $E/\mathbb{Q}$, there is a global minimal model (so for $\omega = \dfrac{dx}{2y + a_1 x + a_3}$, $\left|\frac{\omega}{\omega_v^\circ}\right|_v = 1 \ \forall v$). and if semistable, this remains minimal $\forall F/\mathbb{Q} \Rightarrow \left|\frac{\omega}{\omega_v^\circ}\right|_v = 1$.

<u>Exercise:</u>

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt[3]{m}, \zeta_3) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{m}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$E: \; y^2 + y = x^3 - x^2 \qquad (11a3).$

This has split mult. red. at 11 and good elsewhere.

$c_{11} = 1 \; (\mathbb{Q})$

Compute $\prod_{v \nmid \infty} \tau_v(E, \omega)$ for each of the fields above.

Compatibility of BSD with isogenies:

Lemma: E/K, $\varphi: E \to E'$ an isogeny over K. Then

1) $L(E/K, s) = L(E'/K, s)$ for $\mathrm{Re}(s) > 3/2$.
2) $\mathrm{rk}(E/K) = \mathrm{rk}(E'/K)$

Proof: 1) $V_\ell(E) \simeq V_\ell(E')$

2) $\varphi: E(K) \to E'(K)$ has finite kernel and cokernel. (because $\varphi \circ \hat{\varphi} = [\deg \varphi] = \hat{\varphi} \circ \varphi$ have finite kernel and cokernel) ∎

Write

$$BSD(E/K) = \frac{\mathrm{Reg}(E/K)\, |Ш(E/K)| \prod_{v|\infty} \Omega_v(E,\omega) \prod_{v\nmid\infty} C_v(E,\omega)}{\sqrt{|\Delta_K|}\ \ |E(K)_{tors}|^2}.$$

Theorem (Cassels, Tate for ab. var.): Suppose $\varphi: E \to E'$ is an isogeny over K and $|Ш(E/K)| < \infty$, then $|Ш(E'/K)| < \infty$ and $BSD(E/K) = BSD(E'/K)$.

This is a hard theorem. The terms individually certainly can change.

Cor (Birch): $\varphi: E \to E'$ of prime degree p, $|Ш(E/K)| < \infty$. Then

$$\mathrm{rk}(E/K) \equiv \mathrm{ord}_p\left(\prod_{v|\infty} \frac{\Omega_v(E,\omega_E)}{\Omega_v(E',\omega_{E'})} \prod_{v\nmid\infty} \frac{c(E,\omega_E)}{c(E',\omega_{E'})} \right) \pmod 2.$$

Remark:
$$\frac{\Omega_v(E, \varphi^*(\omega_{E'}))}{\Omega_v(E, \omega_E)} = \left| \frac{\#\ \mathrm{coker}\ \varphi_E|_{E(K_v)}}{\#\ \ker \varphi_E|_{E(K_v)}} \right|^{\pm 1}$$

For p odd,
$$= \begin{cases} p^{\pm 1} & K_v = \mathbb{C} \\ 1 \text{ or } p^{\pm 1} & \text{if } \ker \varphi_E \subseteq E(K_v) \\ & \qquad \not\subseteq E(K_v) \quad , K_v = \mathbb{R}. \end{cases}$$

There is an analogue for the quotient of c_v's..

Proof (Cor): $BSD(E/K) = BSD(E'/K)$.

$$\frac{Reg(E/K)}{Reg(E'/K)} \cdot \frac{\prod \Omega_v(E)}{\prod \Omega_v(E')} \frac{\prod c_v(E)}{\prod c_v(E')} \cdot \underbrace{\frac{|Ш(E/K)|}{|Ш(E'/K)|} \cdot \frac{|E'(K)_{tors}|^2}{|E(K)_{tors}|^2}}_{\square \text{ in } \mathbb{Q}.} = 1$$

$$\Rightarrow \frac{Reg(E/K)}{Reg(E'/K)} = \square \frac{\prod \Omega_v(E')}{\prod \Omega_v(E)} \frac{\prod c_v(E')}{\prod c_v(E)}.$$

L.H.S? Suppose $P_1, \dots, P_r$ is a $\mathbb{Z}$-basis for $E(K)/E(K)_{tors}$.
Then $\varphi(P_1), \dots, \varphi(P_r)$ generates an index $M < \infty$ sublattice inside $E'(K)/E'(K)_{tors}$.

$Reg(E/K) = \det(\langle P_i, P_j \rangle)$

$Reg(E'/K) = M^{-2} \det(\langle \varphi(P_i), \varphi(P_j) \rangle)$ (uses $\langle,\rangle$ is symm. bilinear)

$= M^{-2} \det(\langle P_i\ \hat{\varphi} \circ \varphi(P_j) \rangle)$ ($\varphi, \hat{\varphi}$ adjoint wrt. $\langle,\rangle$)

$= M^{-2} \det(\langle P_i, p P_j \rangle)$ ($\varphi \circ \hat{\varphi} = [p]$)

Vlad
6-28-11
PS6

$$= M^{-2}\, p^{\mathrm{rk}(E/K)} \cdot \mathrm{Reg}(E/K).$$

So we obtain:

$$p^{\mathrm{rk}(E/K)} = \square \frac{\mathrm{Reg}(E/K)}{\mathrm{Reg}(E'/K)} = \square' \prod_{v \mid \infty} \frac{\Omega_v(E')}{\Omega_v(E)} \prod_{v \nmid \infty} \frac{c_v(E')}{c_v(E)}.$$

$\Rightarrow$

$$\mathrm{rk}(E/K) \equiv \mathrm{ord}_p \left(\prod_{v \mid \infty} \frac{\Omega_v(E')}{\Omega_v(E')} \prod_{v \nmid \infty} \frac{c_v(E')}{c_v(E')} \right). \blacksquare$$

<u>Prop.</u> Suppose E_i/K_i, E_j'/K_j' s.t.

$$\prod_i L(E_i/K_i, s) = \prod_j L(E_j'/K_j', s).$$

Then

1) $\sum_i \mathrm{rk}(E_i/K_i) = \sum_j \mathrm{rk}(E_j'/K_j')$.

2) If $|Ш(E_i/K_i)| < \infty$ $\forall i$, then $|Ш(E_j'/K_j')| < \infty$

and

$$\prod \mathrm{BSD}(E_i/K_i) = \prod \mathrm{BSD}(E_j'/K_j').$$

<u>Exercise:</u>

$$\begin{tikzcd}
 & F = \mathbb{Q}(\zeta, \sqrt[3]{m}) \arrow[dl, dash] \arrow[ddr, dash] & \\
L = \mathbb{Q}(\sqrt[3]{m}) \arrow[ddr, dash] & & \\
 & & \mathbb{Q}(\zeta) = M \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

<u>Fact:</u> $\forall\, E/\mathbb{Q}$,

$$L(E/F, s)\, L(E/\mathbb{Q}, s)^2 = L(E/L, s)^2\, L(E/M, s).$$

$m \in \mathbb{Z}$ a non-cube.

$E: y^2 + y = x^3 - x^2$ 11a3

E/M has rank 0.

1) Check the ranks add up correctly

2) Apply BSD(2) (Δ_K cancel, as do Ω_v and $\left|\frac{\omega}{\omega_v^\circ}\right|_v$ for $\frac{dx}{2y+1}$)

- Prove that if $11 \mid m$, then $\mathrm{rk}(E/F) > 0$. In fact, $\mathrm{rk}(E/L)$ is odd! use $\langle , \rangle$ is symm. bil. nondeg, Galois inv. and $\langle P, Q \rangle_F = [F:K] \langle P, Q \rangle_K$ for $P, Q \in E(K)$ and F/K

Interlude on twisted L-functions:

E/K , F/K Galois, $Gal(F/K) = G$.
G acts on $E(F)$.
Write $E(F)_{\mathbb{C}} = E(F) \otimes_{\mathbb{Z}} \mathbb{C}$, this throws away the torsion and gives a f.d. G-representation of $\dim = rk\, E/F$.
We can decompose

$$E(F)_{\mathbb{C}} = \bigoplus_i \rho_i^{\oplus n_i}$$

into irred. reps. ρ_i of G.

Example: $G = \mathbb{Z}_2$. $E(F)_{\mathbb{C}} = \underbrace{E(F)_{\mathbb{C}}^{+}}_{\substack{\text{trivial eigenspace} \\ = \mathbb{1}^{\oplus n_i}}} \oplus \underbrace{E(F)_{\mathbb{C}}^{-}}_{\varepsilon^{\oplus n_i}}$, ε = sgn. rep.

Can construct $L(E/K, \rho, s)$ for reps. ρ of G. This will be defined in another lecture series.

- $L(E/K, \mathbb{1}, s) = L(E/K, s)$
- $L(E/K, \mathbb{C}[G], s) = L(E/F, s)$
- $L(E/K, \mathbb{C}[G/H], s) = L(E/F^H, s)$. $H \leq G$.

Conjecture: For ρ irreducible,

$$\operatorname*{ord}_{s=1} L(E/K, \rho, s) = \langle \rho, E(F)_{\mathbb{C}} \rangle$$
$$= \text{mult. of } \rho \text{ in } E(F)_{\mathbb{C}}.$$

Exercise: Suppose F/K Galois of degree 3. Prove

$$rk\, E/K \equiv rk\, E/F \pmod 2.$$

(true for any odd degree Galois F/K.)

Quadratic Twists:

$E: y^2 = x^3 + ax + b$

$E_d: dy^2 = x^3 + ax + b.$

Exercise: • $E \simeq E_d$ over $K(\sqrt{d})$

• $rk(E/K) + rk(E_d/K) = rk\, E/K(\sqrt{d})$.

• $L(E/K, s)\, L(E_d/K, s) = L(E/K(\sqrt{d}), s)$.

$L(E_d, s) = L(E, \chi_d, s)$

$\chi_d : G \to \{\pm 1\}$.

Results over $\mathbb{Q}$ on BSD(1):

Theorem (Kolyvagin, Gross-Zagier): If $rk_{an}(E/\mathbb{Q}) \leq 1$, then

$rk(E/\mathbb{Q}) = rk_{an}(E/\mathbb{Q})$

and $\# Ш(E/\mathbb{Q}) < \infty$.

Theorem: $\forall\ E/\mathbb{Q}$, there exists a quadratic twist E_d with $rk_{an} E_d = 0$. Similarly, $\exists\, d$ s.t. $rk_{an} E_d = 1$. For given a, n, among $d \equiv a \pmod n$ and prescribed sign, $\exists\, d$ s.t. $rk_{an} E_d \leq 1$.

Theorem (Kato): If $F/\mathbb{Q}$ abelian, χ a 1-dim. rep. of $G = Gal(F/\mathbb{Q})$.

If $\operatorname{ord}_{s=1} L(E, \chi, s) = 0$ then $\langle \chi, E(F)_{\mathbb{C}} \rangle = 0$

(i.e., $\dim E(F)_{\mathbb{C}}^{\chi} = 0$).

Theorem (Rohrlich): p prime. Let F_n = degree p^n subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$. Then for sufficiently large n and all doesn't come from $\mathrm{Gal}(F_n/\mathbb{Q})$

faithful repn. χ of $\mathrm{Gal}(F_n/\mathbb{Q})$, $L(E,\chi,1) \neq 0$.

<u>Cor:</u> $\mathrm{rk}(E/F_n)$ is bounded as $n \to \infty$.

<u>Anticyclotomic extension:</u>

K = imag. quad.

p prime (odd)

There is a tower of fields $K \subset F_1 \subset F_2 \subset \cdots$

$$\mathrm{Gal}(F_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$$

$$\mathrm{Gal}(F_n/\mathbb{Q}) \cong D_{2p^n}.$$

<u>Theorem (Cornut-Vatsal, Gross-Zagier-Zhang):</u> Assume p, N_E, Δ_K are coprime and all primes of bad reduction of E split in $K/\mathbb{Q}$. Then for all n sufficiently large and ρ faithful irred. rep of $\mathrm{Gal}(F_n/\mathbb{Q})$,

$$\operatorname*{ord}_{s=1} L(E/\mathbb{Q}, \rho, s) = 1.$$

<u>Theorem (Bertolini-Darmon, ...):</u> In this setting

$$\operatorname*{ord}_{s=1} L(E/\mathbb{Q}, \rho, s) = 1 \Rightarrow \langle \rho, E(F_n)_{\mathbb{C}} \rangle = 1.$$

<u>Remark:</u> There are more general (weaker assumptions on p, K, and conductor) versions of these two.

Parity Conjecture:

BSD(1) $\Rightarrow$ $rk_{an}(E/K) \equiv rk(E/K) \pmod 2$.

Recall: $L(E/K,s)$ satisfies a functional equation

$$(*)\ L(E/K,s) = W(E/K)\, L(E/K, 2-s)$$

$W(E/K) = \pm 1$ is the global root number.

If $W(E/K) = 1$, then $rk_{an}(E/K)$ must be even.

If $W(E/K) = -1$, then $rk_{an}(E/K)$ must be odd.

Thus,

$$(-1)^{rk_{an}(E/K)} = W(E/K). = \prod_v W(E_v/K_v)$$

Parity Conjecture (PC): $(-1)^{rk(E/K)} = \prod_v W(E/K_v)$.

Example: $E: y^2+y = x^3+x^2+x$ (19a3) split mult. at 19. PC $\Rightarrow (-1)^{rk(E/\mathbb{Q})} = \prod_v W(E/\mathbb{Q}_v)$

$$= W(E/\mathbb{R})\, W(E/\mathbb{Q}_{19}).$$

$$= (-1)(-1) = 1.$$ (classification of local root #'s.)

Thus, the rank should be even. In fact, it is 0.

PC $\Rightarrow$

$$(-1)^{rk(E/\mathbb{Q}(\sqrt[3]{m}))} = W(E/\mathbb{R})\, W(E/\mathbb{C}) \prod_{v|19} W(E/K_v)$$

(where $K = \mathbb{Q}(\sqrt[3]{m})$.) $= (-1)(-1)\,(-1)^{\#v|19}$

$$= (-1)^{\#(v|19)}$$

$$= \begin{cases} (-1)^3 & \text{if 19 splits in top cubic} \\ (-1) & \text{if 19 inert in top cubic} \\ (-1) & \text{if 19 ramifies in top cubic} \end{cases}$$

$$= -1$$

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\zeta_3, \sqrt[3]{m}) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt[3]{m}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_3) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

So $rk(E/\mathbb{Q}(\sqrt[3]{m})) \geq 1. \quad \forall m.$

Exercise: 1) $E: y^2 = x^3 + x^2 - 12x - 67/4$

$\Delta_E = 37^3$ pot. good red. at 37.

Prove that subject to the parity conjecture that $E(K)$ is infinite for every $K/\mathbb{Q}$ imaginary quadratic

2) $\forall E/\mathbb{Q}$, prove that $PC \Rightarrow rk(E/\mathbb{Q}(i,\sqrt{17}))$ is even

(Hint: every prime splits in $\mathbb{Q}(i,\sqrt{17})/\mathbb{Q}$.)

When E admits a p-isogeny $\varphi: E \to E'$:

Recall: If $|Ш(E/K)| < \infty$, then

$$rk(E/K) \equiv \sum_{v \nmid \infty} ord_p\left(\frac{c_v(E, \varphi^*(\omega_{E'}))}{c_v(E', \omega_{E'})}\right) + \sum_{v \mid \infty} ord_p\left(\frac{\Omega_v(E, \varphi^*(\omega_{E'}))}{\Omega_v(E', \omega_{E'})}\right) \pmod 2$$

Define

$$\sigma_v = \begin{cases} +1 & ord_p\left(\frac{c_v(E, \varphi^* \omega_{E'})}{c_v(E', \omega_{E'})}\right) \text{ is even} \\ -1 & \text{otherwise} \end{cases}$$

and similarly with Ω_v for $v \mid \infty$.

So

$$(-1)^{rk(E/K)} = \prod_v \sigma_v.$$

Now compare σ_v to $W(E/K_v)$. This is purely a local problem.

We hope to get

$$(-1)^{rk(E/K)} = \prod \sigma_v = \prod W(E/K_v) = (-1)^{rk_{an}(E/K)}.$$

Theorem (Vlad-Tim): Suppose $\varphi: E \to E'$ a p-isogeny / K.

1) If $p \geq 3$ and ($v \nmid p$ or E is semistable at $v | p$), then

$$W(E/K_v) = \sigma_v \cdot (-1, K_v(\varphi)/K_v)$$

where $K_v(\varphi)/K$ is the extension where the points of $\ker\varphi$ lie and

$$(-1, K_v(\varphi)/K_v) = \begin{cases} +1 & \text{if } -1 \in K_v \text{ is a norm from } K_v(\varphi) \\ -1 & \text{o/w.} \end{cases}$$

= Artin Symbol

2) If $p=2$, pick a model $E: y^2 = x^3 + ax^2 + bx$, $a, b \in \mathcal{O}_K$, $\ker\varphi = \{\mathcal{O}, (0,0)\}$, Then

$$W(E/K_v) = \sigma_v \, (a,-b)_v \, (-2a, a^2-4b)_v$$

where the Hilbert symbol is

$$(\alpha, \beta)_v = \begin{cases} 1 & \text{if } \alpha \in Nm(K_v(\sqrt{\beta})) \\ -1 & \text{else.} \end{cases}$$

Cor: If $\varphi: E \to E'$ is a p-isogeny, E is semi-stable at $v|p$, if $p \geq 3$, $|Ш(E/K)| < \infty$, then PC holds.

Proof: $(p \geq 3)$ $(-1)^{rk_{an}(E/K)} = W(E/K) = \prod_v W(E/K_v)$

$$= \prod \sigma_v \prod (-1, K_v(\varphi)/K_v)$$

$$= (-1)^{rk(E/K)}$$ by product formula for Artin symbol.

$(p=2)$ same thing.

$$\begin{tikzcd} & F \arrow[dl, dash, "\mathbb{Z}_2"'] \arrow[dr, dash, "\mathbb{Z}_3"] \arrow[dd, dash, "S_3"] & \\ L \arrow[dr, dash] & & M \arrow[dl, dash] \\ & K & \end{tikzcd}$$

$$L(E/F, s)\, L(E/K, s)^2 = L(E/L, s)^2 L(E/M, s).$$

This follows from Tim's lecture yesterday.

S_3-relation:

Fix F/K an S_3-extension, E/K an elliptic curve, and ω on E defined over K. We have from previous lecture that if $|Ш(E/F)| < \infty$, then $BSD(E/F)\, BSD(E/K)^2 = BSD(E/L, s)^2\, BSD(E/M, s)$.

Working up to squares (discriminants cancel by conductor-discriminant formula) $\Rightarrow$

$$\frac{Reg(E/F)(Reg(E/K))^2}{(Reg(E/L))^2\, Reg(E/M)} = \square\, \frac{\mathcal{C}(L)^2\, \mathcal{C}(M)}{\mathcal{C}(F)\, \mathcal{C}(K)^2}$$

where

$$\mathcal{C}(K) = \prod_{\substack{v \text{ of } K \\ v \nmid \infty}} c_v(E, \omega) \prod_{v \mid \infty} \Omega_v(E, \omega).$$

Prop. A:
$$\frac{Reg(E/F)\, (Reg(E/K))^2}{(Reg(E/L))^2\, Reg(E/M)} = \square\, 3^{rk(E/K) + rk(E/M) + rk(E/L)}.$$

Hence, if $|Ш(E/F)| < \infty$ then $rk(E/K) + rk(E/L) + rk(E/M)$
$$\equiv ord_3\left(\frac{\mathcal{C}(L)^2\, \mathcal{C}(M)}{\mathcal{C}(F)\, \mathcal{C}(K)^2}\right) \pmod 2.$$

We would now hope

$$(-1)^{\text{sum of these rks}} = (-1)^{\left(\frac{\mathcal{C}(L)^2\, \mathcal{C}(M)}{\mathcal{C}(F)\, \mathcal{C}(K)^2}\right)} = \prod_v \left(\text{local stuff}\right)$$

$$= \prod_v (\text{local root data}) = W(E/K)\, W(E/L)\, W(E/M).$$

For $k = K, L, M, F$, let $\{v$ place of $K\}$

$$W_v(k) = \prod_{z|v} W(E/k_z)$$

$$\tau_v(k) = \begin{cases} \prod_{z|v} \tau_z(E,\omega) \\ \prod_{z|v} \Omega_z(E,\omega) \end{cases}$$

Prop. B: $\mathrm{ord}_3\left(\frac{\tau_v(F)\tau_v(K)^2}{\tau_v(M)\tau_v(L)^2}\right)$ is even iff

$$W_v(K)W_v(M)W_v(L) = 1.$$

Proof: Case-by-Case local computation. One can do some cases as an exercise. Additive reduction over 2 or 3 is a ~~bit~~ bit of a pain. (One needs for these cases not only reduction type, but how the prime ramifies.. there are loads of cases.)

Cor: Let E/K be an elliptic curve, $\mathrm{Gal}(F/K) \cong S_3$ and and assume $\#Ш(E/F) < \infty$. Then

$$(-1)^{rk(E/K) + rk(E/M) + rk(E/K)} = W(E/K)W(E/M)W(E/L).$$

Proof: $$\mathrm{RHS} = \prod_v W_v(K)W_v(L)W_v(M)$$

$$= \prod (-1)^{\mathrm{ord}_3 \frac{\tau_v(F)\tau_v(K)^2}{\tau_v(M)\tau_v(L)^2}}$$

$$\overset{*}{=} (-1)^{rk(E/K) + rk(E/L) + rk(E/M)}.$$

■

Vlad
7-1-11
pg3

<u>Theorem (D.-D.):</u> E/K an elliptic curve, $Ш(E/F)$ finite where $F = K(E[2])$. Then the P.C. holds, i.e.,

$$(-1)^{rk(E/K)} = W(E/K).$$

<u>Proof:</u> Let $G = Gal(F/K) \leq GL_2(\mathbb{F}_2) \cong S_3$

- If $G = \{1\}$ or $\mathbb{Z}_2 \Rightarrow E(K)[2] \neq 0$. Then E admits a 2-isogeny and so we are done by the previous lecture's result.
- If $G = \mathbb{Z}_3$ then $rk(E/K) \equiv rk(E/F) \pmod 2$ by a previous exercise. Moreover, $W(E/K) = W(E/F)$ (requires proof.) So then

$$(-1)^{rk(E/K)} = (-1)^{rk(E/F)}$$

$$\overset{\text{2-isog. case}}{=} W(E/F) = W(E/K).$$

- If $G = S_3$, by the previous two cases we know the parity is correct over L and M, i.e.

$$(-1)^{rk(E/L)} = W(E/L)$$

$$(-1)^{rk(E/M)} = W(E/M).$$

Moreover, by the Cor. we also know

$$(-1)^{rk(E/K)+rk(E/M)+rk(E/L)} = W(E/K)W(E/M)W(E/L).$$

Thus,

$$(-1)^{rk(E/K)} = W(E/K). \blacksquare$$