& Parity course in Barcelona

Tim Dokchitser
30 Nov – 4 Dec 2009
CRM

[All results joint with
Vladimir Dokchitser]

§1: Points on curves

$C/\mathbb{Q}$ curve [e.g. $f(x,y)=0$ ← poly. with $\mathbb{Q}$-coeffs]

$C(\mathbb{Q}) :=$ {rational points on C} [e.g. $\{a,b\in\mathbb{Q} \mid f(a,b)=0\}$]

$\underline{Q}$ How large is $C(\mathbb{Q})$? Is it infinite?

Say C non-singular projective, $g(C)=$ its genus

$g=0$ $C(\mathbb{Q})=\emptyset$ or $C(\mathbb{Q})$ infinite (+algorithm to determine which)

$g\geq 2$ $C(\mathbb{Q})$ finite (Faltings)

$g=1$ Unsolved

If $g=1$ and $C(\mathbb{Q})\neq\emptyset$, fix $O\in C(\mathbb{Q})$ $\rightsquigarrow$ makes $C=E$ into elliptic curve.

Can be put into Weierstrass model

$$E: y^2 = x^3+Ax+B \subseteq \mathbb{P}^2 \quad (A,B\in\mathbb{Q})$$

- $O=$ pt at infinity $=(0:1:0)$
- non-singular $\Leftrightarrow \Delta_E = -16(4A^3+27B^2)\neq 0$
  ↳ RHS no multiple rts.
- over a general field E/K
  $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$

$\uparrow O$
$E(\mathbb{R})$

Thm (Mordell-Weil) K finitely generated field (e.g. $\underbrace{\mathbb{Q}, \text{number field}}$, $\mathbb{F}_q(t_1,t_2)$, $\mathbb{Q}(t)$),
E/K ell. curve. Then $E(K)$ fin. gen. abelian group.

So $E(K)\cong\mathbb{Z}^r\oplus \underset{\text{finite}}{T}$

Def $T=E(K)_{\text{tors}}$ torsion of E/K
$r=\text{rk}\,E/K$ Mordell-Weil rank

Note $E(K)$ infinite $\Leftrightarrow$ $\text{rk}\,E/K>0$

Unsolved:

Q1 Given $E/\mathbb{Q}$, compute $\text{rk}\,E/\mathbb{Q}$.

Q2 Given $E/\mathbb{Q}$, is $\text{rk}\,E/\mathbb{Q}>0$?

Q3 Vary $E/\mathbb{Q}$. Can rk be arbitrarily large?

[Q4 Given num. field K, $\exists$ there E/K with $\text{rk}\,E/K=0$? YES – Mazur-Rubin Apr 09

Rank records

$K = \mathbb{Q}$ $\quad \mathrm{rk} \geq 28$ $\quad$ (Elkies)

$K = \mathbb{Q}(t)$ $\quad \mathrm{rk} \geq 18$ $\quad$ (—"—)

$K = \mathbb{C}(t)$ $\quad \mathrm{rk} \geq 68$ $\quad$ ($y^2 = x^3 + t^{360} + 1$ Shioda ; and this is maximal for $y^2 = x^3 + t^n + 1$ $\forall n$)

$K = \mathbb{F}_p(t)$ $\quad$ rk can be arbitrarily large (Shafarevich-Tate)

§2 Elliptic curves over finite fields & naïve BSD

$K = \mathbb{F}_q$ finite
E/K ell. curve $\quad \Rightarrow$ $E(K)$ finite abelian group.

Thm (Hasse-Weil) $\quad$ Given $E/\mathbb{F}_q$, for all $n \geq 1$

$$\# E(\mathbb{F}_{q^n}) = q^n - \alpha^n - \beta^n + 1 \qquad ; \alpha, \beta \in \mathbb{C} \text{ fixed (indep. of } n), \ |\alpha| = |\beta| = \sqrt{q}$$

Cor $\# E(\mathbb{F}_q) = q + 1 - a_q \quad , \ |a_q| \leq 2\sqrt{q}$ $\qquad$ "Hasse-Weil inequality"

[a_q "trace of Frobenius". Note that it determines α, β, so $\# E(\mathbb{F}_{q^n})$ for all n].

Equivalently, the ζ-function of $E/\mathbb{F}_q$,

$$\zeta_{E/\mathbb{F}_q}(T) = \exp\left(- \sum_{n=1}^{\infty} \frac{\# E(\mathbb{F}_{q^n})}{n} T^n \right) \quad \leftarrow$$

rational func. of T for any variety $V/\mathbb{F}_q$ (Weil Conj.; Dwork)

has the form

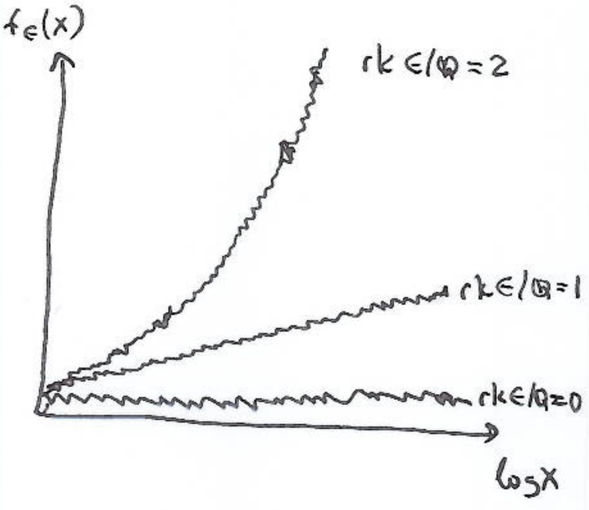
$$\zeta_{E/\mathbb{F}_q}(T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1 - a_q T + q T^2}{(1-T)(1-qT)}$$

Now take $E/\mathbb{Q}$: $\ y^2 = x^3 + ax + b$, say $a, b \in \mathbb{Z}$.

Reduce mod $p \nmid \Delta_E$ $\rightsquigarrow$ $\tilde{E}/\mathbb{F}_p$ ell. curve, $|\tilde{E}(\mathbb{F}_p)| \approx p$ by Hasse-Weil.

BSD heuristic : "$\mathrm{rk}\, E/\mathbb{Q}$ large $\Rightarrow$ Reductions tend to have more points"

$$f_E(X) := \prod_{p \leq X} \frac{\# \tilde{E}(\mathbb{F}_p)}{p}$$



Conj (Naïve form of BSD)

$$f_E(X) \sim c_E (\log X)^{\mathrm{rk}\, E/\mathbb{Q}} \quad \text{as } X \to \infty.$$

§3 ζ- and L-functions

$E/\mathbb{Q}$ ell. curve. Find a model

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \quad , \; a_i \in \mathbb{Z} \, , \; \Delta \in \mathbb{Z} \text{ minimal} \quad (\text{minimal Weier strass model})$$

<u>Def</u> $\zeta_{E/\mathbb{Q}}(s) := \prod_p \zeta_{\tilde{E}/\mathbb{F}_p}(p^{-s}) = \prod_p \frac{F_p(p^{-s})}{(1-p^{-s})(1-p^{1-s})}$; $F_p(T) = \begin{cases} 1-a_pT+pT^2 & , p \nmid \Delta \\ 1-a_pT & , p \mid \Delta \end{cases}$

$$= \frac{\zeta(s)\zeta(s-1)}{L(E/\mathbb{Q},s)} \quad \left[= \frac{L(H^0_{et}(E),s)\,L(H^2_{et}(E),s)}{L(H^1_{et}(E),s)} \right. \; ; \quad \text{similar } \prod_i L(H^i(V))^{(-1)^i} \text{ for any variety } V/\mathbb{Q} .$$

K number field, E/K ell. curve. Same defn:
↑ or function field $\mathbb{F}_q(C)$, $C/\mathbb{F}_q$ (non-sing. proj.) curve.

<u>Def</u> $L(E/K,s) = \prod_{\mathfrak{p}} \frac{1}{F_{\mathfrak{p}}(q^{-s})}$ Converses for $\operatorname{Re} s > \frac{3}{2}$

$\mathfrak{p}$ primes of K

$q = \operatorname{Norm}_{K/\mathbb{Q}} \mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$

} will always use this notation for primes of K & their residue fields (will use $\prod_v$ for product over all places $= \prod_{\mathfrak{p}} \cdot \prod_{v|\infty}$)

with

$$F_{\mathfrak{p}}(T) = \begin{cases} 1-a_{\mathfrak{p}}T+qT^2 & \text{if } E/K_{\mathfrak{p}} \text{ has \underline{good} reduction } (\tilde{E} \text{ ell. curve}) \\ 1-a_{\mathfrak{p}}T & \text{if } E/K_{\mathfrak{p}} \text{ has \underline{bad} reduction } (\tilde{E} \text{ singular}) \end{cases}$$

↑

reduction mod $\mathfrak{p}$ of any Weierstrass model which is minimal at $\mathfrak{p}$

($v_{\mathfrak{p}}(a_i) \geq 0$, $v_{\mathfrak{p}}(\Delta)$ minimal)

Global minimal model at all primes exists over $\mathbb{Q}$, but in general not if K has class number $\neq 1$.

Conj. (Hasse-Weil) $L(E/K,s)$ has analytic continuation to $\mathbb{C}$ and satisfies fun.eq.

$$L^*(E/K,s) := \sqrt{N}^{\,s} \cdot \underbrace{\left[\tfrac{1}{\pi^s}\Gamma(\tfrac{s}{2})\Gamma(\tfrac{s+1}{2})\right]^{(K:\mathbb{Q})}}_{\text{from } v|\infty} \cdot \underbrace{L(E/K,s)}_{\text{finite places}}$$

[like for
Riemann ζ.

Then

$$L^*(E/K, 2-s) = w(E/K)\, L^*(E/K,s)$$; $w(E/K) = \pm 1$ global root number

$N = \Delta_{K/\mathbb{Q}}^2 \cdot \mathrm{Norm}_{K/\mathbb{Q}} N_{E/K}$ conductor of the L-function

$N_{E/K} = \prod_p p^{n_p}$ conductor of E/K, n_p conductor exponent at p

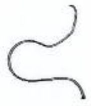
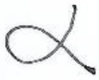
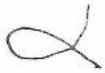
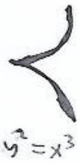
$w(E/K) = \prod_v w(E/K_v) = \prod_{v|\infty}(-1) \cdot \prod_p w(E/K_p)$; $\underset{(\pm 1)}{w(E/K_p)}$ local root numbers

) Explicit in lecture

Table of invariants in most cases:

$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ minimal model at p $(v_p(a_i) \geq 0,\ v_p(\Delta)$ minimal$)$

$\tilde{E}/\mathbb{F}_q$ reduced curve

	$\tilde{E}$	$F_p(T)$	n_p	$w(E/K_p)$
good reduction	 $\Delta \bmod p \neq 0$	$1 - a_pT + qT^2$ $a_p = q+1-\#\tilde{E}(\mathbb{F}_q)$	0	$+1$
split multiplicative reduction	 $y^2 = x^3 + \eta x^2,\ \eta \in \mathbb{F}_q^*$ square	$1-T$	1	-1
non split multiplicative reduction	 $y^2 = x^3 + \eta x^2$ $\eta \in \mathbb{F}_q^\times$ non-square	$1+T$	1	$+1$
additive reduction	 $y^2 = x^3$	1	2 if $p \nmid 2,3$	$(-1)^{\lfloor \frac{q}{I} \rfloor}$ if $p \neq 2,3$

} semistable reduction

(minimal model stays minimal in every extension of K_p; good stays good; mult. stays mult.)

$$I = \begin{cases} \frac{12}{v_p(\Delta)} & \text{if } v_p(j(E)) \geq 0 \text{ (pot. good. red.)} \\ 2 & \text{if } v_p(j(E)) < 0 \text{ (pot. mult. red.)} \end{cases}$$

Known cases of the Hasse-Weil conjecture:

- Over function fields $[\ \zeta_{E/\mathbb{F}_q(t)} = \zeta_{\text{surface}/\mathbb{F}_q} =$ rational function (by Weil Conj.)$\ ]$
- Over $K = \mathbb{Q}$ [Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor]
- Know meromorphic continuation + fun.eq. over totally real fields K

⌈ E/K totally real

a) Taylor's Potential Modularity Thm: $\exists\, K'/K$ Galois tot.real s.t. E/K' is modular ⇒ $L(E/K',s)$ analytic + fun.eq.

b) Cyclic base change: If K'/K tot.real cyclic (or solvable) then E/K modular $\Leftrightarrow$ E/K' modular

c) Solomon Induction Thm.: G finite gp $\Rightarrow$ $\mathbb{1}_G = \sum n_i \mathrm{Ind}_{H_i}^G \mathbb{1}_{H_i}$, $H_i \leq G$ solvable

⌊ a) + b) + c) ⇒ ■

§4 Birch-Swinnerton-Dyer Conjecture I

For $E/\mathbb{Q}$,

at $s=1$ this is $\frac{1}{1-a_p\frac{1}{p}+\frac{1}{p}} = \frac{p}{p+1-a_p} = \frac{p}{\#\tilde{E}(\mathbb{F}_p)}$

$$L(E/\mathbb{Q},s) = \sum_{n\geq 1} a_n n^{-s} = \prod_{p\nmid\Delta_E} \frac{1}{1-a_p p^{-s}+p^{1-2s}} \cdot \prod_{p\mid\Delta_E} \cdots \quad ; \quad \mathrm{Re}\, s > \frac{3}{2}$$

So, formally,

$$\text{"}\ L(E/\mathbb{Q},1) = \Big[\prod_p \frac{\#\tilde{E}(\mathbb{F}_p)}{p}\Big]^{-1}\ \text{"}$$

; naive BSD : this is $\neq 0 \Leftrightarrow \mathrm{rk}\, E/\mathbb{Q} = 0$

Conj (BSD I) K global field (number field or func. field), E/K ell. curve or abelian variety.

Then

$$\underset{\text{analytic rank } \mathrm{rk}_{an} E/K}{\mathrm{ord}_{s=1} L(E/K,s)} = \underset{\text{Mordell-Weil rank}}{\mathrm{rk}\, E/K}$$

Known cases :

- Over function fields if $Ш(p^\infty)$ finite for some p (Artin-Tate; Milne, Schneider)
- over $\mathbb{Q}$ if $\mathrm{rk}_{an} E/\mathbb{Q} \leq 1$ (Coates-Wiles, Gross-Zagier, Kolyvagin)
- over tot. real fields K if E/K modular and $\mathrm{rk}_{an} E/K \leq 1$ (Zhang '01 $j(E)$ non-integral
Tian-Zhang (announced) always)

Recall $\overset{*}{L}(E/K, 2-s) = \overset{\pm 1}{W(E/K)} \cdot L^*(E/K,s) \Rightarrow \mathrm{rk}_{an} E/K$ even $\Leftrightarrow W=1$
odd $\Leftrightarrow W=-1$

Thus BSD implies

Parity Conjecture $(-1)^{\mathrm{rk}\, E/K} = W(E/K)$

- Sort of "BSD modulo 2"
- Avoids L-functions & Hasse-Weil
- But seems as hard as BSD I !

Goals Thm A Assuming finiteness of Ш, Parity Conjecture holds for all ECs over all number fields [CM/$\mathbb{Q}$ Birch-Stephens, Greenberg-Guo, /$\mathbb{Q}$ Monsky, /tot.real Nekovář, /all K D.-D.]

Thm B Explicit formula for $W(E/K)$ [and for local root numbers]

§5 Parity predictions

Ex1 $E/\mathbb{Q}$ semistable (only good/mult. red.; e.g. Δ square-free).

$$w(E/\mathbb{Q}) = \underset{\text{from }\infty}{-1} \cdot (-1)^{\#P} \qquad \begin{array}{l} P = \{\text{split mult. primes for } E\} \\ Q = \{\text{non-split} \quad -\text{''}- \} \end{array}$$

Parity Conj. (P.C.) $\operatorname{rk} E/\mathbb{Q} \equiv 1 + \#P \mod 2.$

For any finite $K/\mathbb{Q}$,

$$w(E/K) = (-1)^{\#\{v|\infty\}} \times \underset{\text{split stays split}}{(-1)^{\{\mathfrak{p}|p \;\mid\; p\in P\}}} \times (-1)^{\{\mathfrak{p}|p \;\mid\; p\in Q,\ (k_\mathfrak{p}:\mathbb{F}_p) \underset{\substack{\uparrow \\ \text{non-split becomes split}}}{\text{even}}\}}$$

$\Rightarrow$ parity prediction.

Ex $E = 19A3$: $y^2 + y = x^3+x^2+x$, $\Delta = 19$, split mult. at 19.

P.C. $\Rightarrow$ $\operatorname{rk} E/\mathbb{Q}$ even [in fact 2-descent $\Rightarrow$ 0]

Take $K_m = \mathbb{Q}(\sqrt[3]{m})$

$$\text{P.C.} \Rightarrow \operatorname{rk} E/K_m \equiv \underset{\#\{v|\infty\}}{2} + \underset{\#\{v|19\}}{\begin{cases} 3 & 19 \text{ splits in } K_m \\ 1 & \text{otherwise} \end{cases}} \quad (\zeta_3 \in \mathbb{Q}_{19}) \qquad \equiv 1 \mod 2.$$

Get

Conj $E(\mathbb{Q}(\sqrt[3]{m}))$ is infinite for all $m \geq 1$, (not cubes) [only know: true for infinitely many m]

Ex2 Number fields K s.t. $w(E/K) = 1$ for all $E/\mathbb{Q}$

$K := \mathbb{Q}(\sqrt{-1}, \sqrt{17})$

- 2 places $v|\infty$
- $p \neq 2, 17$ unr. $\Rightarrow$ cyclic decgp. $\Rightarrow$ split into 2 or 4 primes in K
- $p = 2$ split in $\mathbb{Q}(\sqrt{17})$
- $p = 17$ split in $\mathbb{Q}(\sqrt{-1})$

K has even no. of places above any v of $\mathbb{Q}$.

For any $E/\mathbb{Q}$,

$$w(E/K) = \prod_p w(E/K_\mathfrak{p}) = \prod_p (\pm 1)^{\text{even}} = +1.$$

Conj. Every $E/\mathbb{Q}$ has even rank over $\mathbb{Q}(\sqrt{-1}, \sqrt{17})$.

Ex3 No local expression for the rank

P.C. $\Rightarrow$ There are local invariants

$$\begin{matrix}\text{ell. curves} \\ \text{over local fields}\end{matrix} \xmapsto{\lambda} \mathbb{Z}/2\mathbb{Z} \qquad [(-1)^{\lambda(E/k)} := w(E/k).]$$

such that for all ell. curves over number fields E/K,

$$\operatorname{rk} E/K \equiv \sum_v \lambda(E/K_v) \mod 2.$$

This only possible for parity of the rank

Thm (a) $\nexists$ local invariants $\{\text{e.c.}/\text{l.f.}\} \xrightarrow{\lambda} \mathbb{Z}$ s.t. for all e.c./n.f.

$$\operatorname{rk} E/K = \sum_v \lambda(E/K_v)$$

(b) $\nexists \{\text{e.c.}/\text{l.f.}\} \xrightarrow{\lambda} \mathbb{Z}/4\mathbb{Z}$ s.t. for all e.c./n.f.

$$\operatorname{rk} E/K \equiv \sum_v \lambda(E/K_v) \mod 4. \qquad (*)$$

Pf (b) $\Rightarrow$ (a)

(a) Take $E: y^2 = x(x+2)(x-3)$, $K = \mathbb{Q}(\sqrt{-1}, \sqrt{41}, \sqrt{73})$ ← all places split into 4 or 8.

$(*) \Rightarrow \operatorname{rk} E/K \equiv 0 \mod 4$

But 2-descent $\Rightarrow \operatorname{rk} E/K = 6$.

Rmk $$L(E/K,s) = 1 \cdot \left(\frac{1}{1-3^{-2s}}\right)^4 \left(\frac{1}{1-5^{-2s}}\right)^4 \left(\frac{1}{1+14\cdot 7^{-2s} + 7^{2-4s}}\right)^4 \cdots$$

- every local factor is a 4th power
- But $L \neq$ 4th power of an entire fnc. ($\operatorname{ord}_{s=1} = 6$).

(in fact not even a 2nd power – simple zeroes on $1+it$)

Ex4 Failure of Goldfeld over number fields

$E/\mathbb{Q}: \quad y^2 = f(x)$

Def Quad. twist of E by $d \in \mathbb{Q}^*$ is

$E_d: dy^2 = f(x)$

$E \cong E_d$ over $\mathbb{Q}(\sqrt{d})$; not over $\mathbb{Q}$

In fact, $L(E/\mathbb{Q}(\sqrt{d}),s) = L(E/\mathbb{Q},s)\,L(E_d/\mathbb{Q},s)$ "Artin formalism".

Conj (Goldfeld) For 50% of square-free d's $\operatorname{rk} E_d/\mathbb{Q} = 0$ $\quad \geq \frac{X}{\log X}$ of these (Ono-Skinner)

50% $\operatorname{rk} E_d/\mathbb{Q} = 1$ $\quad \geq X^{1-\varepsilon}$ of these (Pomykala-Perelli)

0% $\operatorname{rk} E_d/\mathbb{Q} \geqslant 2.$ $\quad$ (of these! (Stewart-

$\geq c X^{1/7}/\log^2 X$

$\uparrow$

$$\left(\frac{\{d : |d| \leq X \text{ sq.-free} \mid \operatorname{rk} E_d = 0\}}{\{d : |d| \leq X \text{ sq.-free}\}} \longrightarrow \frac{1}{2} \text{ as } X \to \infty \right).$$

(

Pick $d_0 < 0$ s.t. all $p \mid 2\Delta_E$ split in $\mathbb{Q}(\sqrt{d_0})$. Then

$$w(E_d) = -w(E_{dd_0}) \qquad \forall d \qquad (\text{Exc.})$$

I.e. the involution $d \leftrightarrow dd_0$ on $\mathbb{Q}^*/\mathbb{Q}^{*2}$ swaps $w=1 \leftrightarrow w=-1$, so

for 50% d's $w = +1$
50% d's $w = -1$

Goldfeld's heuristic : "<u>Rank is usually as small as possible, as allowed by the root number</u>"

[This is a general phenomenon : e.g. if we construct a family of ECs parametrised by t that pass through 2 points in $\mathbb{Q}^2$, $\leftarrow$ take $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and force them to pass through $(0,0)$ and $(1,1)$ - 2 lin. eqns in 5 variables $a_1, \dots, a_6$ $\Rightarrow$ can find a 1-dim. (even 3-dim.) family

it is not in general true that a fiber will have rank 2 - it will have rank 2 or 3, depending on its root number].

Over number fields, Goldfeld's Conjecture is false :

<u>Example</u> Take $\underset{(121C1)}{E/\mathbb{Q}}$: $y^2 = x^3 + \frac{5}{4}x^2 - 2x - 7$; $\Delta_E = -11^4$

Over $K = \mathbb{Q}(\zeta_3, \sqrt[3]{11})$ it has good reduction everywhere, and so

$$w(E/K) = (-1)^{\#\{v \mid \infty\}} = (-1)^3 = -1$$

But for any quad. ext. $K(\sqrt{\alpha})/K$, $\alpha \in K^*$

$$w(E/K(\sqrt{\alpha})) = (-1)^{\#\{v \mid \infty\}} = (-1)^6 = +1 \qquad \Rightarrow \qquad w(E_\alpha/K) = -1.$$

So <u>every</u> quadratic twist of E/K has root number -1 $\Rightarrow$ it should have $rk > 0$.

This gives a very elementary

<u>Conj</u> Poly. $x^3 + \frac{5}{4}x^2 - 2x - 7 \in K[x]$ takes <u>every</u> value in $K^\times/K^{\times 2}$ $(K = \mathbb{Q}(\zeta_3, \sqrt[3]{11}))$.

§6 Tate module & L-functions

K number field, $G_K := \mathrm{Gal}(\bar{K}/K)$

E/K ell. curve

Def n-torsion $E[n] = \{P \in E(\bar{K}) \mid nP = 0\} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ as ab. gp.

$\circlearrowleft$ G_K

$\left[\begin{array}{l} E(\mathbb{C}) \cong \mathbb{C}/\Lambda \text{ lattice} \\ E(\mathbb{C})[n] \cong \tfrac{1}{n}\Lambda/\Lambda \end{array}\right]$

For ℓ prime

Def The ℓ-adic Tate module

$$T_\ell E := \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell \quad \circlearrowleft \quad G_K$$

$$V_\ell E := T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$$

Get 2-dim. representation

$$\rho_\ell : G_K \longrightarrow GL_2(\mathbb{Q}_\ell)$$

← very important object

(by Weil pairing $\det \rho_\ell = \bigwedge^2 \rho_\ell = \ell$-adic cyc. character

$$G_K \longrightarrow \mathbb{Z}_\ell^\times = \mathrm{Aut}(\varprojlim_n \zeta_{\ell^n}) \ ]$$

Local properties of this action:

$\mathfrak{p} \nmid \ell$ prime of K, $k = \mathbb{F}_q$ residue field.

$$\begin{tikzcd} 1 \arrow[r] & I_\mathfrak{p} \arrow[r] & G_{K_\mathfrak{p}} \arrow[r] \arrow[d, phantom, "\subset" rotate=90] & G_k \arrow[r] \arrow[d, phantom, "\cong" rotate=90] & 1 \\ & \text{inertia gp at } \mathfrak{p} & G_K & \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}, \text{ gen. by } x \to x^q & \end{tikzcd}$$

Def $\mathrm{Frob}_\mathfrak{p}$ = any elt of $G_{K_\mathfrak{p}}$ mapping to $(x \to x^q)$.

Def $G_{K_\mathfrak{p}} \circlearrowright V$ v. space. We say V is <u>unramified at $\mathfrak{p}$</u> if $I_\mathfrak{p}$ acts trivially.

[Then V is a G_k-module]

Thm (Néron-Ogg-Shafarevich) $T_\ell E$ unramified at $\mathfrak{p}$ $\iff$ E has good red. at $\mathfrak{p}$

(in which case $\mathrm{Frob}_\mathfrak{p} \circlearrowright V_\ell E$ and has char. pol. $1 - a_\mathfrak{p} T + qT^2$

$\Big]$ ∀ ... ℓ

Defn of L-function (alternative) & of the conductor

$$L(E/K, s) = \prod_\mathfrak{p} F_\mathfrak{p}(q^{-s})^{-1} \ ; \quad F_\mathfrak{p}(T) = \det(1 - T \cdot \mathrm{Frob}_\mathfrak{p} \mid (V_\ell E)^{I_\mathfrak{p}})$$

$$n_\mathfrak{p} = 2 - \dim (V_\ell E)^{I_\mathfrak{p}} + (\text{wild contribution } \delta \geq 0)$$

, $\delta = 0 \iff$ pro-q part of $I_\mathfrak{p}$ (wild inertia) acts trivially

Ex $E/\mathbb{Q} : y^2 = x^3 + 1$, $\Delta = -2^4 3^3$; $p=3$, $\ell=2$.

What is the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_3 | \mathbb{Q}_3)$ on $E[2]$, $E[4]$, $E[8]$, ... T_2E ?

- (Explicitly) On $E[2] = \{O, (-1,0), (-\zeta, 0), (-\zeta^2, 0)\}$ ζ 3rd root of 1.

  $G_{\mathbb{Q}_3}$ acts through $\mathrm{Gal}(\underset{\mathbb{Q}_3(\sqrt{-3})}{\underset{\shortparallel}{\mathbb{Q}_3(\zeta_3)}} / \mathbb{Q}_3) \cong C_2$; ramified quad. ext.

  I_3 acts through C_2 on $E[2]$ $\Rightarrow$ $E[2]$ ramified, T_2E ramified.

  [$\overset{\text{N.O.S.}}{\Rightarrow}$ E has bad reduction at 3].

  Similar computation $\Rightarrow$

  I_3 acts through C_4 on $E[4]$ and on $E[8]$,

  (may guess : true for all $E[2^k]$, $k \geq 2$)

- (using N.O.S.) E acquires good red over $\mathbb{Q}_3(\sqrt[4]{3})$ (use Tate's algorithm)

  $F := \mathbb{Q}_3(i, \sqrt[4]{3})$ $\leftarrow$ Galois, Gal. gp. D_8, Inertia C_4

  N.O.S. $\Rightarrow$ Over F I_3 acts trivially

  $\Rightarrow$ over $\mathbb{Q}_3$ I_3 acts through $I_{F|\mathbb{Q}_3} \cong C_4$.

  (and cannot be smaller : need at least deg 4 ram. ext. to get good red.,

  as good red $\Rightarrow v(\Delta) \equiv 0 \mod 12$, and over $\mathbb{Q}_3$ $v(\Delta) = 3$.)

Summary $E : y^2 = x^3 + 1$ $/\mathbb{Q}_3$.

$G_{\mathbb{Q}_3}$ acts on V_2E through $\mathrm{Gal}(\mathbb{Q}_3(\sqrt[4]{3})^{nr} / \mathbb{Q}_3) \cong \underset{\text{unr}}{\hat{\mathbb{Z}}} \ltimes \underset{\text{inertia}}{C_4}$

C_4 acts as $\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$ in some basis (eigenvalues $\pm i \notin \mathbb{Q}_3$).

$2\hat{\mathbb{Z}}$ acts as scalars (central, V_2E irr. rep)

$(V_2E)^{I_3} = \{0\}$ so $F_3(T) = 1$ and $n_3 = 2$ (3-part of I_3 acts trivial

In general (Serre-Tate)

: E/K_p potentially mult $(v_p(j)<0)$

$E : y^2 = x^3 + Ax + B$

Tate curve theory $\Rightarrow E$ has mult. red. $/ K_p(\sqrt{-6B})$ ← $= K_p$ when split mult.
quad. unr. $/K_p$ when nonsplit
quad. ram $/K_p$ when additive.

G_{K_p} acts on $V_\ell E$ as $\pm 1 \times \begin{pmatrix} \chi & \varphi \\ 0 & 1 \end{pmatrix}$ [and on $(V_\ell E)^*$ as $\pm 1 \cdot \begin{pmatrix} \chi & 0 \\ \varphi & 1 \end{pmatrix}$]

χ cyc. character, φ tame char. $I_p \longrightarrow \varprojlim \zeta_{\ell^n} \cong \mathbb{Z}_\ell$

$\sigma \longmapsto \sigma(\pi^{1/\ell^n})/\pi^{1/\ell^n}$ π unit of K_p.

$$\pm 1 : \sigma \longmapsto \frac{\sigma(\sqrt{-6B})}{\sqrt{-6B}}$$

So,

split $\Rightarrow$	$\dim (V_\ell E^*)^{I_p} = 1$,	$n_p = 1$,	$F_p = 1 - T$	(Frob$_p$ acts as 1)
non-split $\Rightarrow$	$= 1$	$= 1$	$= 1 + T$	(— " — -1)
additive $\Rightarrow$	$= 0$	$= 2$ $(p \nmid 2)$	$= 1$	

If E/K_p pot. good $(v_p(j) \geq 0)$, additive

E has good red. over a fin. ext. of K_p; I_p acts through

$$\underbrace{C_2, C_3, C_4, C_6}, \underbrace{Q_8, SL_2(\mathbb{F}_3), S_3, C_4 \rtimes C_3}_{\text{only for } p \mid 2,3}$$

Exc $p \nmid 2,3 \Rightarrow I_p$ acts through C_n, $n = \dfrac{12}{v_p(\Delta)}$

In all cases, $\underset{(p \nmid 2,3)}{n_p = 2}$, $(V_\ell E^*)^{I_p} = 0$, $F_p(T) = 1$.

§7 General varieties

$V/K_\mathfrak{p}$ nonsingular proj. variety $\rightsquigarrow$ $H^i(V) = H^i_{et}(V, \mathbb{Q}_\ell)$ étale cohomology gps, $0 \le i \le 2\dim V$.

$\mathbb{Q}_\ell$-vector spaces with $G_{K_\mathfrak{p}}$-action. [for ECs $H^1 = (V_\ell E)^*$]

Grothendieck Monodromy Thm After fin. ext. $F/K_\mathfrak{p}$, $I_\mathfrak{p}$ acts on H^i as $1+\varphi\cdot N$, [$\mathfrak{p} \nmid \ell$]

$\varphi: G_F \to \mathbb{Z}_\ell$ tame character as before, $N \in \mathrm{End}(H^i)$ nilpotent matrix [$N=0$ and $\begin{pmatrix}0&1\\0&0\end{pmatrix}$ for ECs with good/mult. red / F]

Def If $G_{K_\mathfrak{p}} \circlearrowright \rho$ like this, we say that ρ is a Weil-Deligne representation

[$\rho: G_{K_\mathfrak{p}} \to GL_n(\mathbb{Q}_\ell)$, or, usually $GL_n(\mathbb{C})$ by embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ in some way]

Ex A 1-dim Weil-Deligne representation is a quasi-character, i.e. $G_{K_\mathfrak{p}} \to \mathbb{Q}_\ell^\times$ s.t. image $(I_\mathfrak{p})$ is finite. [Ex cyclotomic char. χ : $I_\mathfrak{p} \mapsto 1$, $\mathrm{Frob}_\mathfrak{p} \to q$]

Def For a variety V/K, K number field,

$$L(H^i(V), s) := \prod_\mathfrak{p} F_\mathfrak{p}(q^{-s})^{-1}, \quad F_\mathfrak{p}(T) = \det\left(1 - \mathrm{Frob}_\mathfrak{p} T \mid H^i(V)^{I_\mathfrak{p}}\right) \leftarrow$$

Problem Not known to be indep. of ℓ and of embeddings $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ for bad. red. primes $\mathfrak{p}$

[ok for curves & AVs]

Generally, this definition applies to any "compatible system of ℓ-adic representations":

$\rho = (\rho_\ell)_\ell$, $\rho_\ell: G_K \to GL_n(\mathbb{Q}_\ell)$

- must all be unramified outside $\{\ell\} \cup$ fixed finite set of primes (i.e. $\rho_\ell(I_\mathfrak{p}) = 1$)
- and have same char poly. of $\mathrm{Frob}_\mathfrak{p}$ on $\rho_\ell^{I_\mathfrak{p}}$ for all ℓ s.t. $\mathfrak{p} \nmid \ell$.

Ex Artin representations $G_K \to GL_n(\mathbb{C})$; $L(\rho, s)$ = Artin L-function.

These L-functions satisfy "Artin formalism":

1) $L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s) L(\rho_2, s)$

2) For F/K finite, $L(\rho, s) = L(\mathrm{Ind}_{G_F}^{G_K} \rho, s)$ for ρ system of reps of G_F.

§8 Root numbers

Consider all finite extensions $F/K_\mathfrak{p}$, and all Weil-Deligne representations

$\rho: G_F \to GL_n(\mathbb{C})$, all n. [again: we had $\to GL_n(\mathbb{Q}_\ell)$ before, but fix $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$]

Thm (Langlands-Deligne) There is a unique way to associate to each such ρ its ε-factor $\varepsilon(\rho) \in \mathbb{C}^\times$ s.t.

1. (Multiplicativity) $\varepsilon(\rho_1 \oplus \rho_2) = \varepsilon(\rho_1)\varepsilon(\rho_2)$
2. (Inductivity in deg. 0) If $\rho_1, \rho_2 : G_F \to GL_n(\mathbb{C})$, same n, then $\dfrac{\varepsilon(\rho_1)}{\varepsilon(\rho_2)} = \dfrac{\varepsilon(\mathrm{Ind}_{G_F}^{G_K} \rho_1)}{\varepsilon(\mathrm{Ind}_{G_F}^{G_K} \rho_2)}$

   (i.e. $\varepsilon(W) = \varepsilon(\mathrm{Ind} W)$ for W virtual rep. of degree 0)
3. (1-dim.) For a quasi-character $\psi: G_F \to \mathbb{C}^\times$, $\varepsilon(\psi)$ is as in Tate's thesis.

__Proof__ Uniqueness: Automatic from 2) + 3) + Brauer induction

Existence: Understanding relations between inductions + Stickelberger's Thm.

⌈ __Tate's thesis__ $\psi : G_F \to \mathbb{C}^\times$; via local reciprocity write $\psi : F^\times \longrightarrow \mathbb{C}^\times$

$$\begin{tikzcd} F^\times \arrow[rr] \arrow[dr, "\text{loc. recip}"'] & & \mathbb{C}^\times \\ & G_F^{ab} \arrow[ur, "\psi"'] & \end{tikzcd}$$

$n(\psi) :=$ conductor exponent of ψ

$b(F) := V_p(\Delta_{F/\mathbb{Q}_p})$

$h :=$ any elt of $F^\times$ of valuation $-n(\psi)-b(F)$; e.g. $\pi_F^{-n(\psi)-b(F)}$

$$\varepsilon(\psi) := \begin{cases} \int_{h\mathcal{O}_F^\times} \psi(x^{-1}) e^{2\pi i \, Tr_{F/\mathbb{Q}_p}(x)} dx & \text{for } \psi \text{ ramified} \\ \int_{h\mathcal{O}_F^\times} \psi(h^{-1}) \, dx = \frac{\psi(h^{-1})}{|h|_F} \cdot \int_{\mathcal{O}_F^\times} dx & \text{for } \psi \text{ unramified} \end{cases}$$

(← may be rewritten as finite sums)

⌊

So Tate's theory of signs in the functional eqns for quasi-characters extends uniquely to a theory for all representations.

__Def__ The local root number

$$w(\rho) := \frac{\varepsilon(\rho)}{|\varepsilon(\rho)|} \in \{z \mid |z|=1\} \subseteq \mathbb{C}^\times$$

"sign of $\varepsilon(\rho)$" [we'll write $\operatorname{sgn} z = \frac{z}{|z|}$ for $z \in \mathbb{C}^\times$]

__Ex__ $\rho = \psi$ 1-dim. unr. $\Rightarrow w(\psi) = \frac{\psi(h^{-1})}{|\psi(h^{-1})|} = \left(\frac{\psi(Frob_p)}{|\psi(Frob_p)|}\right)^{b(F)}$

__Ex__ $w(\text{triv. rep.}) = 1$

__Ex__ $\psi = \chi$ cyc. char. also has $\psi(\chi) = 1$

} use ; $\mathbb{1} : I_p \to 1, \; Frob_p \to 1$
$\chi : I_p \to 1, \; Frob_p \to q$

Properties of root numbers (Tate-Deligne): Multiplicative, inductive in deg. 0 (because ε-factors are),

- $w(\rho \oplus \rho^*) = (\det \rho)(-1)$ ← i.e. image of $-1 \in F^\times \xrightarrow{\text{loc. recip}} G_F^{ab} \xrightarrow{\det \rho} \mathbb{C}^\times$
- $w(\rho_1 \otimes \rho_2) = w(\rho_1)^{\dim \rho_2} \cdot \operatorname{sgn}(\det \rho_2)(\pi_F^{n(\rho_1) + \dim \rho_1 \cdot b(F)})$ if ρ_2 is unramified
- $w(\rho) := w(\rho^{ss}) \cdot \frac{\operatorname{sgn} \det(-Frob_p \mid (\rho^{ss})^{I_p})}{\operatorname{sgn} \det(-Frob_p \mid \rho^{I_p})}$ for ρ non-semisimple.

__Def__ E/K_p elliptic curve. Its local root number

$$w(E/K_p) := w(\rho) \quad ; \quad \rho = (V_\ell E^*) \otimes_{\mathbb{Q}_\ell} \mathbb{C}$$

[known to be indep. of $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ for ECs and AVs

__Ex__ E good red. N.O.S. $\Rightarrow \rho$ unramified, so

$$w(E/K_p) = w(\rho) = w(\mathbb{1} \otimes \rho) = \underbrace{w(\mathbb{1})^2}_{1} \cdot \operatorname{sgn}\underbrace{(\det \rho)}_{\chi^{-1}}(\pi_F^{\cdots}) = \operatorname{sgn}(q^{\cdots}) = +1$$

Ex E split mult. red: $V_\ell E = \begin{pmatrix} \chi & \varphi \\ 0 & 1 \end{pmatrix}$, $\rho = \begin{pmatrix} \chi^{-1} & 0 \\ \varphi & 1 \end{pmatrix}$, $\rho^{ss} = \begin{pmatrix} \chi^{-1} & 0 \\ 0 & 1 \end{pmatrix}$

$$w(\rho) = \underset{\substack{\text{unr., det} = \chi^{-1} \\ \Rightarrow w = 1 \text{ again}}}{w\begin{pmatrix} \chi^{-1} & 0 \\ 0 & 1 \end{pmatrix}} \cdot \frac{\operatorname{sgn} \det \left(-\mathrm{Frob}_p \mid \begin{pmatrix} \chi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right)}{\operatorname{sgn} \det (-\mathrm{Frob}_p \mid 1)} = \frac{\operatorname{sgn} \det \begin{pmatrix} -q^{-1} & 0 \\ 0 & -1 \end{pmatrix}}{\operatorname{sgn} \det (-1)} = \frac{1}{-1} = -1.$$

Ex E non-split mult red. $\Rightarrow$ $w(\rho) = +1$ (same computation)

Conclusion: Understand ρ well $\Rightarrow$ enough formulae to compute its root number.

Example (Root numbers of elliptic curves with an ℓ-isogeny)

E/K_p, $p \nmid \ell$. Suppose $G_{K_p} \circlearrowright E[\ell]$ reducibly, i.e. $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ in some basis.

Equivalently, there is an isogeny [$\overset{\text{def}}{\leftarrow}$ non-constant morphism taking O to O; autom. preserves addition]

$$\varphi : E \longrightarrow E'$$

of degree ℓ, defined over K_p.

Def $F := K_p\left(\begin{smallmatrix} \text{coords of} \\ \text{pts in } \ker \varphi \end{smallmatrix}\right)$ $\leftarrow$ Galois, Galois group image of
$\underset{K_p(E[\ell])}{\cap}$

$$G_{K_p} \xrightarrow{\rho \bmod \ell} \left\{\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\right\} \xrightarrow{\text{top left corner}} \alpha \in \mathbb{F}_\ell^\times$$

so $\mathrm{Gal}(F/K_p) \hookrightarrow \mathbb{F}_\ell^\times$, in particular F/K_p cyclic. (of degree $\mid \ell - 1$).

Def $(-1, F/K_p) := \begin{cases} +1 & \text{if } -1 \text{ is a norm from } F \text{ to } K_p \\ -1 & \text{otherwise} \end{cases}$ (Artin symbol)

Thm If E/K_p has additive reduction and $p \nmid \ell$, and $\ell \geq 5$, then

$$w(E/K_p) = (-1, F/K_p)$$

Proof Suppose E/K_p has pot. good reduction (pot. mult. similar but easier - Exc.)

① $E[\ell]$ is unramified over F.

Pf Image of G_F in $\mathrm{Aut}(E[\ell]) = GL_2(\mathbb{F}_\ell)$ is in $\subseteq \begin{pmatrix} \overset{\text{defn of } F.}{1} & * \\ 0 & \chi \end{pmatrix} \leftarrow$ because $\det = \chi$

So $I = $ Image of I_p over F $\subseteq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ $\leftarrow$ order ℓ. (χ unr.)

But $|I| \mid 24$ by class. of inertia action in pot. good case, $\ell \geq 5 \Rightarrow I = 1$,

so $E[\ell]$ is unramified over F.

② $\underline{E[\ell^n] \text{ unramified over } F \text{ for all } n \geq 1}$

Pf let $\pi : GL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \twoheadrightarrow GL_2(\mathbb{Z}/\ell\mathbb{Z})$

$|\ker \pi| =$ power of ℓ, so π injective on the image of I_p (← again, using $|\text{image}| \mid 24$.)

But $I = 1$!

③ $\underline{E/F \text{ has good reduction}}$

Pf. N.O.S.

④ $\underline{\text{Action of } G_{K_p} \text{ on } V_\ell E \text{ is abelian}}$

[as semisimple abelian actions can be diagonalised, this $\Rightarrow G_{K_p}$ acts as $\begin{pmatrix} \psi & 0 \\ 0 & \chi\psi^{-1} \end{pmatrix}$ for some quasi-character ψ]

Pf Want to show G'_{K_p} (commutator sgp) acts trivially

- $G'_{K_p} \subseteq I_{K_p}$ as $G_{K_p}/I_{K_p} \cong \text{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$ is abelian
- Image of G'_{K_p} in $\text{Gal}(F/K_p)$ is trivial as $\text{Gal}(F/K_p)$ abelian

$\Big\}\ G'_{K_p} \subseteq I_{\bar{F}/F}$

But we know that $I_{\bar{F}/F}$ acts trivially on $V_\ell E$ by ②.

⑤ Now $\rho = \begin{pmatrix} \psi & 0 \\ 0 & \chi\psi^{-1} \end{pmatrix} \Rightarrow$

$$\begin{aligned} w(\rho) &= w(\psi)\, w(\chi\psi^*) \overset{\text{unr. twist formula}}{=} w(\psi)\, w(\psi^*) \\ &= w(\psi \oplus \psi^*) \overset{\rho\oplus\rho^* \text{ formula}}{=} \psi(-1) \\ &= \tilde{\psi}(-1) \end{aligned}$$

for any prim. char. $\tilde{\psi}$ of F/K_p that agrees with ψ on inertia

$$\overset{\text{local CFT}}{=} (-1, F/K_p) \qquad ∎$$

Rmk

When the action $G_{K_p} \circlearrowleft V_\ell E$ is not abelian, the following is very useful:

Thm (Fröhlich-Queyrut)

$$\begin{tikzcd} \bar{F} \arrow[d, dash] \\ F(\sqrt{\xi}) \arrow[d, dash, "\text{quad ext.}"] \\ F \end{tikzcd}$$

If $\psi : G_{F(\sqrt{\xi})} \to \mathbb{C}^\times$ is a quasi-character s.t. $\psi|_{F^\times} = 1$ then $w(\psi) = \psi(\xi)$.

Abelian + F.Q. Thm $\Rightarrow$ enough to get $w(E/K_p)$ in all cases when $p \nmid 2,3$ (Rohrlich)

[P13 Kobayashi

P12 Whitehouse - D.-D. ; in terms of ε-factors of 1-dim chars in $\text{Gal}(K_p(E[3])/K_p)$

less satisfactory, as less explicit

Over $\mathbb{Q}_2, \mathbb{Q}_3$: finitely many cases to consider (w locally constant as func. of coeffs of E),

all cases tabulated by Halberstadt].

§9 BSD II

K number field (or function field), E/K elliptic curve

<u>Conj</u> (BSD I) $\operatorname{ord}_{s=1} L(E/K, s) = \operatorname{rk} E/K =: r$

<u>Conj</u> (BSD II) $\displaystyle\lim_{s\to 1} \frac{L(E/K,s)}{(s-1)^r} = \frac{C \cdot |\text{Ш}| \cdot R}{\sqrt{|\Delta_K|} \cdot |E(K)_{tors}|^2}$

- Δ_K <u>discriminant of K</u>
- $E(K)_{tors}$ <u>torsion</u> subgroup of $E(K)$
- R <u>regulator</u> $= \det(\langle P_i, P_j \rangle)$, $P_1, \dots, P_r$ basis of $E(K)/_{E(K)_{tors}}$ – free part of Mordell-Weil gp,

  $[=1$ if $r=0]$

  $\langle\, , \rangle : E(K) \times E(K) \longrightarrow \mathbb{R}$ Néron-Tate <u>height pairing</u>.

  Bilinear, symmetric, positive-definite on $\frac{E(K)}{\text{torsion}}$, Galois invariant $\langle \sigma P, \sigma Q \rangle = \langle P, Q \rangle$ $\forall \sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

  and for $E \xrightarrow{\varphi} E'$ isogeny of degree n,
  $E \xleftarrow{\varphi^t} E'$ dual isogeny ($\exists! \varphi^t$ s.t. $\varphi\varphi^t = [n]$, $\varphi^t\varphi = [n]$) : $\underset{\text{on } E'}{\langle \varphi(P), Q \rangle} = \underset{\text{on } E}{\langle P, \varphi^t(Q) \rangle}$

  for all $P \in E(K)$, $Q \in E'(K)$.

  For F/K finite extension, $P, Q \in E(K)$,

  $$\langle P, Q \rangle_{E(F)} = [F:K] \cdot \langle P, Q \rangle_{E(K)}.$$

  [For AVs, $\langle\, , \rangle : A(K) \times \hat{A}^t(K) \to \mathbb{R}$; A^t dual AV. For ppAVs same as for Ecs].

- Ш <u>Tate-Shafarevich</u> group. $= \bigcap_v \ker\left(H^1(G_K, E(\bar{K})) \longrightarrow H^1(G_{K_v}, E(\bar{K}_v)) \right)$ abelian torsion gp.

  <u>Conj</u> ("Shafarevich-Tate") Ш is finite.

  <u>Facts</u> • $\text{Ш}[p^\infty] = \bigcup_{n \geq 1} \text{Ш}[p^n]$ = elts of p-power order is "cofinitely generated", i.e.

  $\cong \underbrace{(\mathbb{Q}_p/\mathbb{Z}_p)^a}_{\text{divisible elements } \text{Ш}[p^\infty]_{div}} \oplus$ finite ab. p-group

  [for ppAVs it is only antisymmetric, so Ш may have $2\times$square order]

  • $\exists$ Cassels pairing : perfect, bilinear, alternating $\frac{\text{Ш}}{\text{Ш}_{div}} \times \frac{\text{Ш}}{\text{Ш}_{div}} \longrightarrow \mathbb{Q}/\mathbb{Z}$

  <u>Cor</u> If finite, Ш has square order.

  In fact, each $\frac{\text{Ш}[p^\infty]}{\text{Ш}[p^\infty]_{div}}$ has square order.

- $C = \prod_v C_v$ <u>Tamagawa factor</u>. To define C_v,

fix an invariant differential $\omega \neq 0$ on E/K [on $y^2 = x^3 + ax^2 + bx + c$, $\omega = \alpha \cdot \frac{dx}{y}$ $\forall \alpha \neq 0$]

$v | \infty$ real : $C_v := \int_{E(K_v)} |\omega|$

$v | \infty$ complex : $C_v := 2i \int_{E(K_v)} \omega \wedge \overline{\omega}$

$v \nmid \infty$, $v = \mathfrak{p}$: $C_{\mathfrak{p}} := c_{\mathfrak{p}} \cdot \left| \frac{\omega}{\omega_v^0} \right|_{K_{\mathfrak{p}}}$

- ω_v^0 Néron (minimal) differential at v
- $|x|_{K_{\mathfrak{p}}} = q^{-v_{\mathfrak{p}} x}$ $\mathfrak{p}$-adic abs. value

$$c_{\mathfrak{p}} = [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})] = \begin{cases} 1 & \text{good reduction at } \mathfrak{p} \\ n & \text{split mult. red.} \\ \left.\begin{matrix} 1 & n \text{ odd} \\ 2 & n \text{ even} \end{matrix}\right\} & \text{, non-split mult} \\ 1,2,3,4 & \text{additive red} \end{cases} \quad \Bigg\} \; n = v_{\mathfrak{p}}(\Delta_{E,\mathfrak{p}}) = -v_{\mathfrak{p}}(j(E))$$

local Tamagawa number

disc. of minimal model at $\mathfrak{p}$

Thus C_v depends on the choice of ω, but $C = \prod_v C_v$ does not $\Big(\underbrace{\prod_v |\alpha|_v = 1 \quad \forall \alpha \in K^\times}_{\text{product formula}} \Big)$.

<u>Rmk</u> For AVs same conj., except $|A(K)_{tors}| \cdot |A^t(K)_{tors}|$ in the denominator (Tate)

<u>Rmk</u> R, Ш global (hard) invariants

<u>Rmk</u> BSD II : lead. coeff of $L(E/K, s)$ at $s=1$ $= \dfrac{C \cdot |\text{Ш}| \cdot R}{\sqrt{|\Delta_K|} \cdot |E(K)_{tors}|^2}$

class number formula : lead coeff. of $\zeta_K(s)$ at $s=1$ $= \dfrac{2^{r_1} (2\pi)^{r_2} \cdot h \cdot R}{\sqrt{|\Delta_K|} \cdot |(\mathcal{O}_K^\times)_{tors}|}$

on free part of $E(K)$

$$\begin{tikzcd} \text{Ш} \arrow[d, leftrightarrow] & R \arrow[d, leftrightarrow] & C_\infty \arrow[d, leftrightarrow] & E(K)_{tors} \arrow[d, leftrightarrow] \\ h & R & \Pi & (\mathcal{O}_K^\times)_{tors} \end{tikzcd}$$

on free part of $\mathcal{O}_K^\times$

Except don't know analogues of two most important thms in algebraic number theory: "finiteness of h" for Ш, "rank of unit gp" for $E(K)$

Known cases:

- Over function fields if $|\text{Ш}[p^\infty]| < \infty$ for some p (Artin-Tate, Schneider, Kato-Trihan)
- K tot. real, E/K modular, $\mathrm{rk}_{an} E/K \leq 1$ [published : in addition need $[K:\mathbb{Q}]$ odd or $j(E)$ non-integral]
  then BSD I holds, Ш finite, BSD II holds "up to a few primes"
  (Gross-Zagier, Kolyvagin, Rubin, Zhang, Tian-Zhang)
- Over $\mathbb{Q}$ for $N_E < 130{,}000$ with $\mathrm{rk}_{an} E/K \leq 1$, BSD II is ok [Stein-W.]

<u>Rmk</u> When $\mathrm{rk}_{an} > 1$, BSD II is not known for a <u>single elliptic curve $E/\mathbb{Q}$</u> !

<u>Rmk</u> Also, for twists of ECs $E/\mathbb{Q}$ by Artin representations τ [even 1-dim. of order 3] don't know an explicit formula, even conjecturally, for leading term of $L(E, \tau, s)$ at $s=1$ [but see Gross & Fearnley-Kisilevsky]

<u>Def</u> $\mathrm{BSD}_{E/K} := \dfrac{C \cdot R \cdot |Ш|}{\sqrt{|\Delta_K|} \cdot |E(K)_{\mathrm{tors}}|^2}$ BSD-quotient

<u>Thm</u> (Cassels - Tate-Milne) E/K ell. curve or abelian variety, $E \xrightarrow{\Phi} E'$ isogeny. Then
ECs AVs

$$\mathrm{BSD}_{E/K} = \mathrm{BSD}_{E'/K}$$

(easy: $Ш_{E/K}$ finite $\Leftrightarrow$ $Ш_{E'/K}$ finite)

<u>Rmk</u> Φ induces

$$\begin{tikzcd} V_\ell E \arrow[r, "\phi"] \arrow[rr, bend right, "{[\deg \phi]\ \cong !}"'] & V_\ell E' \arrow[r, "\phi^t"] & V_\ell E \end{tikzcd}$$

$\Rightarrow V_\ell E \cong V_\ell E$ as G_K-modules $\rightarrow L(E,s) = L(E',s)$.

So we expect from BSD: (I) $\mathrm{rk}\, E/K = \mathrm{rk}\, E'/K$ ✓ (replace $V_\ell E$ by $E(K) \otimes \mathbb{Q}$, use same argument for ϕ, ϕ^t)

(II) $\mathrm{BSD}_{E/K} = \mathrm{BSD}_{E'/K}$ ✓ by Thm.

I.e. <u>BSD is compatible with isogenies.</u>

<u>Note</u> All individual terms in $\mathrm{BSD}_{E/K}$ are <u>not</u> isogeny-invariant!

← We'll give this a positive spin and extract plactical info. out of this, related to parity

§10 Parity example

<u>Ex</u> $E: y^2+y = x^3+x^2-7x+5, \quad \Delta = -7 \cdot 13$ (91b1)

$E': y^2+y = x^3+x^2+13x+42, \quad \Delta = -7^3 \cdot 13^3$ (91b2)

ϕ 3-isogeny; over $K = \mathbb{Q}$

Choose global minimal ω, ω' $\left[= \frac{dx}{2y+1}\right]$, so $c'_p = c_p \ \forall p$.

E split mult. at 7, 13 $\Rightarrow c_7 = v_7(\Delta_E) = 1, \ c_{13} = 1$; $C_\infty = 6.039\ldots$
⇓ (same L-fun.!)
E' split mult. at 7, 13 $\Rightarrow c'_7 = 3, \ c'_{13} = 3$; $C'_\infty = 2.013\ldots$

$C_\infty = 3 \cdot C'_\infty$ (for a p-isogeny$/\mathbb{Q}$, $C_\infty = p \cdot C'_\infty$ or C'_∞ always; if $\phi^* \omega' = \omega$; see below)

So $C_{E/\mathbb{Q}} = 1 \cdot 1 \cdot C_\infty = C_\infty$ ← not equal ; so some other term in BSD must also not be equal
$C_{E'/\mathbb{Q}} = 3 \cdot 3 \cdot \frac{1}{3} C_\infty = 3 C_\infty$

Assume Ш finite. Then Cassels $\Rightarrow$

$$\frac{R_{E/\mathbb{Q}}}{R_{E'/\mathbb{Q}}} = \frac{C_{E'/\mathbb{Q}}}{C_{E/\mathbb{Q}}} \cdot \frac{|Ш_{E'/\mathbb{Q}}|}{|Ш_{E/\mathbb{Q}}|} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{|E'(\mathbb{Q})_{\mathrm{tors}}|^2} = 3 \times \text{rational square} \times \text{rational square} \neq 1$$

<u>Rmk</u> $R/R' \in \mathbb{Q} \Rightarrow$ suspicious! must have easy interpret

So cannot have $R_{E/\mathbb{Q}} = R_{E'/\mathbb{Q}} = 1 \Rightarrow \boxed{\mathrm{rk}\, E/\mathbb{Q} > 0}$

In fact, let $P_1 \ldots P_n$ = basis of $\Lambda := E(\mathbb{Q})/\text{torsion}$, $\Lambda' := E'(\mathbb{Q})/\text{torsion}$; $n = \mathrm{rk}\, E/\mathbb{Q}$.

As $\phi^t \phi = [3]$,

$$3^n R_{E/\mathbb{Q}} = \det \langle 3P_i, P_j \rangle = \det \langle \phi^t \phi P_i, P_j \rangle = \det \langle \phi P_i, \phi P_j \rangle = R_{E'/\mathbb{Q}} \cdot [\Lambda' : \phi(\Lambda)]^2$$

So $\dfrac{R_{E/\mathbb{Q}}}{R_{E'/\mathbb{Q}}} = \text{rational square} \times 3^{\mathrm{rk}\, E/\mathbb{Q}}$; so we've shown $\boxed{\mathrm{rk}\, E/\mathbb{Q} \text{ is odd}}$

Because $w(E/\mathbb{Q}) = -1$ [2 split places + 1 infinite], we proved that

Finiteness of Ш $\Rightarrow$ Parity Conj. for $E = 91b1/\mathbb{Q}$

§11 Parity for curves with a p-isogeny.

K number field, $p \geq 5$.

$E/K \xrightarrow{\phi} E'/K$ isogeny of degree p; suppose $|Ш(E)| < \infty$.

Normalize differentials by $\omega = \phi^* \omega'$. Then not hard to see that

$$\frac{C_v(E'/K)}{C_v(E/K)} = \frac{|\mathrm{coker}\,\phi_v|}{|\ker \phi_v|} \quad ; \quad \phi_v : E(K_v) \longrightarrow E'(K_v)$$

induced map on local pts

$$= \frac{c_v(E'/K)}{c_v(E/K)} \quad \text{for } v \nmid \mathfrak{p}, \infty.$$

Cassels $\Rightarrow$ $p^{\mathrm{rk} E/K} \equiv \frac{R_{E/K}}{R_{E'/K}} \equiv \frac{C_{E'/K}}{C_{E/K}} \mod \mathbb{Q}^{*2}$, so

$$\boxed{\mathrm{rk}\, E/K \equiv \sum_v \mathrm{ord}_p \frac{|\mathrm{coker}\,\phi_v|}{|\ker \phi_v|} \mod 2} \leftarrow$$

local expression for parity of the rank for curves with an isogeny

Def $\sigma_\phi(E/K_v) := (-1)^{\mathrm{ord}_p \frac{|\mathrm{coker}\,\phi_v|}{|\ker \phi_v|}}$ $\left[\text{so } (-1)^{\mathrm{rk} E/K} = \prod_v \sigma_\phi(E/K_v)\right]$

Parity Conjecture for E/K $\iff$ $\prod_v w(E/K_v) = \prod_v \sigma_\phi(E/K_v)$, so compare $w(E/K_v)$ and $\sigma_\phi(E/K_v)$ for all v.

	w	σ_ϕ	
v complex	-1	-1	$\phi_v : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ surj., kernel $\mathbb{Z}/p\mathbb{Z}$
v real pts in $\ker\phi$ real	-1	1	$\lvert\ker \phi_v\rvert = p$ and $\lvert\mathrm{coker}\,\phi_v\rvert = 1$
v real pts in $\ker\phi$ complex	-1	-1	$\lvert\ker \phi_v\rvert = 1$
$v \nmid p$ good	1	1	$c_v, c_v' = 1$
$v \nmid p$ nonsplit	1	1	$c_v, c_v' \in \{1, 2\}$
$v \nmid p$ split	-1	-1	$\frac{c_v}{c_v'} \in \{p, \frac{1}{p}\}$ from Tate curve theory
$v \nmid p$ additive	$(-1, K_v, \phi/K_v)$	1	$c_v, c_v' \in \{1, 2, 3, 4\}$

They don't quite agree! Stare at discrepancy for log enough $\Rightarrow$

p-isogeny Conj For $p \geq 3$ $w(E/K_v) = \sigma_\phi(E/K_v) \cdot (-1, K_v, \phi/K_v)$, all local fields K_v (incl $v|p$)

Check this : v Archimedean $(-1, \mathbb{R}/\mathbb{R}) = 1$

$(-1, \mathbb{C}/\mathbb{C}) = 1$

$(-1, \mathbb{C}/\mathbb{R}) = -1$

So $(-1, K_v, \phi/K_v) = -1$

$\iff$ v real, pts in $\ker\phi$ complex ✓

$v \nmid p$ additive : ok for $p > 3$, $p = 3$ similar.

$v \nmid p$ semistable : want to show $K_{v,\varphi}/K_v$ unramified $\left(\Rightarrow \text{all units are norms} \Rightarrow (-1, K_{v,\varphi}/K_v) = 1\right)$

good red : $K_{v,\varphi} \subseteq K(E[p])$ ← unramified $/K_v$ by N.O.S

mult. red: $|I_{K_v(E[p])/K_v}|$ divides p (action $\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}$)

but we know $[K_{v,\varphi} : K_v] \mid p-1$ ⇒ unramified

$v | p$ semistable : slightly trickier

$v | p$ additive : don't know how to prove !

We showed : p-isogeny conjecture holds, unless $v|p$, E/K_v additive red.

<u>Cor</u> K number field, $E \longrightarrow E'$ p-isogeny $/K$, p odd. If Ш finite, E semistable $\forall v | p$ then

$$(-1)^{\operatorname{rk} E/K} = w(E/K).$$

<u>Proof</u> $\prod_v (-1, K_{v,\varphi}/K_v) = 1$ ← product formula for Artin symbols.

<u>Fact</u> (Coates-Fukaya-Kato-Sujatha) Conj. holds for $v|p \geq 5$, E/K_v additive, good red. after ab. ext of K_v. (incl. pot. ord. red.) ← uses crystalline coh. instead of $V_\ell E$.

<u>Fact</u> (Trihan-Wuthrich) Have a func. field analogue (in part. applies to Frob: $\mathbb{E} \to E$).

<u>§11 2-isogeny</u>

<u>Thm</u> $E/K \xrightarrow{\varphi} E'/K$ 2-isogeny, Ш finite. If E semistable & not supersingular at $v|2$,

$$(-1)^{\operatorname{rk} E/K} = w(E/K)$$

(better ⇒ more curves!)

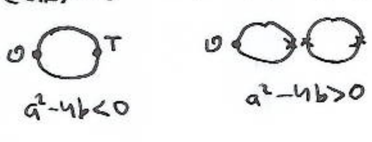
<u>Proof</u> $\ker \varphi = \langle O, T \rangle$, $T \in E(K)$. Move T to $(0,0)$ ⇒ get

$$\varphi \left(\begin{array}{ll} E : y^2 = x^3 + ax^2 + bx & ; \ \Delta = 16b^2(a^2-4b) \\ E' : y^2 = x^3 - 2ax^2 + (a^2-4b)x & ; \ \Delta = 256b(a^2-4b)^2 \end{array} \right.$$

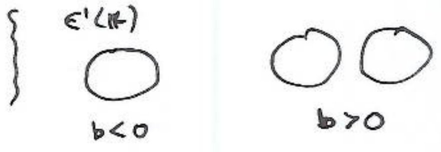
[<u>Note</u> $K_{v,\varphi} = K_v$ here!

Need to compare $w(E/K_v)$ with $\sigma_\varphi(E/K_v) = (-1)^{\operatorname{ord}_2 \frac{|\operatorname{coker} \varphi_v|}{|\ker \varphi_v|}}$

$/\mathbb{R}$ $E(\mathbb{R}) \approx S^1$ or $S^1 \times \mathbb{Z}/2\mathbb{Z}$

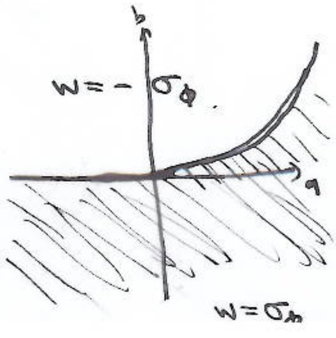


$E'(\mathbb{R})$



$w(E/\mathbb{R}) = -1$; $|\ker \varphi_v| = 2$; $|\operatorname{coker} \varphi_v| = \begin{cases} 1 & b<0 \\ 2 & b>0,\ a^2-4b<0 \\ \begin{cases} 1 & \text{if } 0 \text{ rightmost root} \Leftrightarrow a>0 \\ 2 & \text{if } a<0 \end{cases} & b>0 \ ; \ a^2-4b>0 \end{cases}$

"we were horrified"



⇒ Correction term $(a,-b)_{\mathbb{R}}(-a, a^2-4b)_{\mathbb{R}}$

└ Hilbert symbol : $(x,y)_{\mathbb{R}} = -1$ if $x,y<0$, $+1$ otherwise.

Experiment $\Rightarrow$ for all v

$$w(E|K_v) = \sigma_\varphi(E|K_v) \cdot (a,-b)_{K_v} \cdot (-2a, a^2-4b)_{K_v}$$

Prove this by case-by-case analysis,

Take $\prod_v$ $\Rightarrow$ done ■

$(x,y)_{K_v}$ = Hilbert symbol $:= (y, K_v(\sqrt{x})/K_v)$

For $x,y \in K$

$$\prod_v (x,y)_{K_v} = 1$$

Q Conceptual explanation of the correction terms?

Q $A|K$ ppAV, $A \xrightarrow{\Phi} A$ isogeny s.t. $\phi\phi^t = [2]$ and $\ker\phi$ totally isotropic for the Weil pairing ($\Rightarrow A'$ ppAV). Can one prove parity?

[one difficulty: Ш non-square. Find a local formula for $(-1)^{\operatorname{ord}_2 \frac{|Ш(A)|}{|Ш(A')|}}$?

---

§12 Deforming to totally real fields

Finish off 2-isogeny:

<u>Thm</u> $E|K_v \xrightarrow{\varphi} E'|K_v$ 2-isogeny; equations as before.

$$\varphi \circlearrowleft \begin{array}{l} E: y^2 = x^3+ax^2+bx \\ E': y^2 = x^3-2ax^2+(a^2-4b)x \end{array}$$

Then $w(E|K_v) \overset{(*)}{=} \sigma_\varphi(E|K_v) \cdot \begin{cases} (a,-b)_{K_v}(-2a, a^2-4b)_{K_v} & \text{if } a \neq 0 \\ (-2,-b)_{K_v} & \text{if } a = 0 \end{cases}$ in all cases.

<u>Proof</u> May assume $v|2$.

Main idea: LHS, RHS are continuous (i.e. locally constant) fncs of a,b (easy)

$\Rightarrow$ may vary a,b slightly.

Take a totally real field F, place w_0 of F s.t. $F_{w_0} \cong K_v$, and take $\tilde{E}/F$: $y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x$ s.t.

- $|\tilde{a}-a|_{w_0} < \varepsilon$, $|\tilde{b}-b|_{w_0} < \varepsilon$
- $\tilde{E}$ split mult. (say) ~~at~~ all places $w \neq w_0$ above 2 ($\Rightarrow (*)_w$ holds for all $w \neq w_0$)
- $j(\tilde{E})$ non-integral

Suppose for the moment $\tilde{E}/F$ is modular. Bumb Friedberg-Hofstein $\Rightarrow \exists \underset{F^*}{\underset{\cap}{\tilde{d}}}, |\tilde{d}-d|_{w_0} < \varepsilon$ s.t.

$\tilde{E}_{\tilde{d}}$: $\tilde{d}y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x$ ($\leftarrow$ close to $E|K_v$, and $(*)_{w_0} \Leftrightarrow$ P.C.)

has $rk_{an} \leq 1$. Zhang's Thm. $\Rightarrow |Ш_{\tilde{E}_{\tilde{d}}}| < \infty$, $rk_{an} = rk$ $\Rightarrow$ P.C. holds for it.

$\Rightarrow (*)$ holds for $\tilde{E}_{\tilde{d}}/F$ $\Rightarrow$ for $E|K_v$

(+ Brauer induction like argument to reduce to the case $\tilde{E}$ is modular)

<u>Cor</u> If $E|K$ has a 2-isogeny, then Ш finite $\Rightarrow$ P.C. for $E|K$.

Same deformation argument $\Rightarrow$ <u>Thm</u> p-isogeny Conj. holds for $p = 3$ [, 5, 7, 13] $X_0(p)$ genus 0

Q Can one prove p-parity Conj. for all p like this?

[E.g. using Moret-Bailly/Pop's result on pts of varieties over tot. real fields to get pts of $X_0(p)$?]

§13 Brauer relations in Galois groups

Lemma K_i, K_j' number fields, E_i/K_i, E_j'/K_j' ell. curves. If

$$\prod_i L(E_i/K_i, s) = \prod_j L(E_j'/K_j', s) \qquad \text{for } \mathrm{Re}\, s > \tfrac{3}{2}$$

then $$\prod_i \mathrm{BSD}_{E_i/K_i} = \prod_j \mathrm{BSD}_{E_j'/K_j'}$$

Proof $W_i :=$ Weil restriction of E_i/K_i to $\mathbb{Q}$

$AV_{/\mathbb{Q}}$ of dim $[K_i:\mathbb{Q}]$; $E_i(K_i) = A(\mathbb{Q})$, $\Omega_{E_i/K_i} = \Omega_{A/\mathbb{Q}}$, Ш, $C = C$, $R = R$, BSD = BSD etc.

$A := \prod W_i$, $A' := \prod W_j'$. Then

$$L(A/\mathbb{Q}, s) = L(A'/\mathbb{Q}, s) \overset{\text{Serre}}{\Longrightarrow} V_\ell A \cong V_\ell A' \overset{\text{Faltings}}{\Longrightarrow} A \sim A' \text{ isogenous}$$

$$\Rightarrow \mathrm{BSD}_{A/\mathbb{Q}} = \mathrm{BSD}_{A'/\mathbb{Q}} \Rightarrow \text{claim} \ ■$$

BREAK?

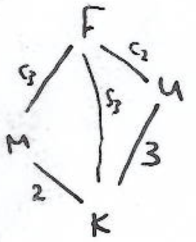
Can use any such relation to prove a case of Parity Conj.

[all cases I know can be proved like that)

Ex F/K Galois, $G = \mathrm{Gal}(F/K) \cong S_3$. ← 3 irr. reps; $\mathbb{1}$, sign ε, 2-dim ρ.

E/K elliptic curve ⇒ by Artin formalism, for $H < G$

$$L(E/F^H) = L(V_\ell E \otimes \mathbb{C}[G/H], s)$$ — decomposes as a product of $L(E,s)$, $L(E,\varepsilon,s)$, $L(E,\rho,s)$.

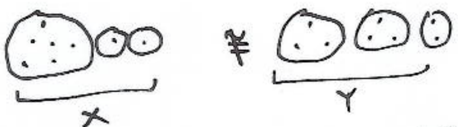


$$\mathbb{C}[G/\{1\}] = 1 \oplus \varepsilon \oplus \rho^2$$
$$\mathbb{C}[G/C_3] = 1 \oplus \varepsilon$$
$$\mathbb{C}[G/C_2] = 1 \oplus \rho$$
$$\mathbb{C}[G/G] = \mathbb{1}.$$

$$\Rightarrow \mathbb{C}[G] \oplus \mathbb{C} \oplus \mathbb{C} \cong \mathbb{C}[G/C_3] \oplus \mathbb{C}[G/C_2] \oplus \mathbb{C}[G/C_2]$$

Recall:

transitive G-sets	$\xleftrightarrow{1:1}$	conj. classes of sgps of G
X	$\longmapsto$	Stab(x_1) $(x_1 \in X)$
G/H.	$\longleftarrow$	H

So we set  as G-sets, but $\mathbb{C}[X] \cong \mathbb{C}[Y]$.

Def G finite grp, $H_i < G$, $n_i \in \mathbb{Z}$. We say $\Theta = \sum n_i H_i$ is a Brauer relation if $\sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1} = 0$.

In S_3-case $\Theta = 1 + 2G - C_3 - 2C_2$ Brauer relation ⇒, $L(E/F, s) L(E/K, s)^2 = L(E/M, s) L(E/U, s)^2$.

Lemma ⇒ assuming Ш finite,

$$\frac{R_{E/F} R_{E/K}^2}{R_{E/U}^2 R_{E/M}} = \frac{C_{E/U}^2 C_{E/M}}{C_{E/F} C_{E/K}^2} \times \begin{pmatrix}\text{rational}\\ \text{square}\end{pmatrix}$$

What is LHS?

<u>Def</u> $\Theta = \sum n_i H_i$ Brauer relation in G, [read $V := E(F)\otimes\mathbb{Q}$] $\quad F$ — K

V $\mathbb{Q}$-representation of G

$\langle,\rangle$ pos. def. G-invariant pairing $V\times V\to\mathbb{R}$ [read $\langle,\rangle$ ht. pairing on $E(F)$]

The <u>regulator constant</u>

$$\mathcal{C}_\Theta(V) := \prod_i \det\left(\tfrac{1}{|H|}\langle,\rangle \,\middle|\, V^{H}\right) \in \mathbb{R}^\times/\mathbb{Q}^{\times 2}$$

computed on any $\mathbb{Q}$-basis of V^H; well-defined up to $\mathbb{Q}^{\times 2}$

<u>Prop</u> $\mathcal{C}_\Theta(V)$ is independent of $\langle,\rangle$ on V.

<u>Cor</u> $\mathcal{C}_\Theta(V)\in\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ (may take $\langle,\rangle$ $\mathbb{Q}$-valued)

<u>Cor</u> $\mathcal{C}_{\Theta_1+\Theta_2}(V) = \mathcal{C}_{\Theta_1}(V)\,\mathcal{C}_{\Theta_2}(V)$

<u>Cor</u> $\mathcal{C}_\Theta(V\oplus W) = \mathcal{C}_\Theta(V)\,\mathcal{C}_\Theta(W)$.

In S_3-case, decompose $V = E(F)\otimes\mathbb{Q} = \mathbb{1}^{n_1}\oplus\varepsilon^{n_\varepsilon}\oplus\rho^{n_\rho}$

$$\left[\begin{array}{l}\text{so } \operatorname{rk}E/K = n_1\\ \operatorname{rk}E/M = n_1+n_\varepsilon\\ \operatorname{rk}E/L = n_1+n_\rho\\ \operatorname{rk}E/F = n_1+n_\varepsilon+2n_\rho\end{array}\right]$$

$$\Theta = 1+2S_3-2C_2-C_3 \;\Rightarrow\; \mathcal{C}_\Theta(\mathbb{1}) = \frac{1\cdot(\frac{1}{6})^2}{(\frac{1}{2})^2\cdot\frac{1}{3}} = \frac{1}{3} = 3 \in \mathbb{Q}^*/\mathbb{Q}^{*2}$$

$$\mathcal{C}_\Theta(\varepsilon) = 3\;;\;\mathcal{C}_\Theta(\rho) = 3 \qquad \text{(similar).}$$

$$\text{So}\quad \frac{R_{E/F}R_{E/K}^2}{R_{E/M}R_{E/L}^2} = \mathcal{C}_\Theta(V) = 3^{n_1+n_\varepsilon+n_\rho}\in\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

$$\left(= 3^{\operatorname{rk}E/K+\operatorname{rk}E/M+\operatorname{rk}E/L}\right)$$

← like in the isogeny case we get a formula for this parity in terms of C's.

Compare with root numbers (+ deformation argument in horrible cases) ⇒

<u>Thm</u> $w(E/K_v, 1\oplus\varepsilon\oplus\rho) \overset{(**)}{=} (-1)^{\operatorname{ord}_3 \frac{c_v(E/F)\,c_v(E/K)^2}{c_v(E/L)^2\,c_v(E/M)}}$

← no correction term!
(actually products over all places of K,M,L,F above given v of K in RHS)

<u>Cor</u> F/K S_3-ext, E/K ell. curve. Assuming Ш finite,

$$(-1)^{\operatorname{rk}E/K+\operatorname{rk}E/L+\operatorname{rk}E/M} = w(E/K)\,w(E/M)\,w(E/L)$$

(i.e. Parity Conj. for the twist of E by $1\oplus\varepsilon\oplus\rho$)

<u>§14 Main Theorem</u>

<u>Thm A</u> K number field, E/K ell. curve, assume Ш$(E/K(E[2]))[6^\infty]$ finite. Then

$$(-1)^{\operatorname{rk}E/K} = w(E/K).$$

<u>Proof</u> $F := K(E[2])$, $G = \operatorname{Gal}(F/K)\subseteq GL_2(\mathbb{F}_2) = S_3$ (G permutes 3 non-zero 2-torsion pts)

(a) <u>$G = C_1$ or C_2</u> E has a K-rational 2-torsion pt ⇒ 2-isogeny ⇒ done.

(b) $\left.\begin{array}{l}\operatorname{rk}E/K\equiv\operatorname{rk}E/F \bmod 2 \quad \text{(easy)}\\ w(E/K) = w(E/F)\end{array}\right\}$ ⇒ done by (a)

c) $\underline{G = S_3}$

$$\begin{tikzcd} & F \arrow[dl, dash, "C_2"'] \arrow[dr, dash, "C_3"] & \\ U \arrow[dr, dash] & & M = K(\sqrt{D_E}) \arrow[dl, dash] \\ & K & \end{tikzcd}$$

a), b) $\Rightarrow$ P.C. for $\mathrm{rk}\,E/M$, $\mathrm{rk}\,E/U$, $\mathrm{rk}\,E/F$
also know P.C. for $\mathrm{rk}\,E/K + \mathrm{rk}\,E/M + \mathrm{rk}\,E/U$ } $\Rightarrow$ done!

Combining (*) and (**) gives a formula for the global root number:

<u>Thm B</u> K number field, E/K elliptic curve. Fix non-zero $P \in E[2]$, defined $/K$ if possible; let $F := K(E[2])$. Let $U := K(P)$, $E' = E/\{O,P\}$ 2-isogenous curve. Then

$$w(E/K) = \begin{cases} (-1)^{\mathrm{ord}_2 \frac{c_{E/M}}{c_{E'/M}}} & \text{if } [F:K] < 6 \\ (-1)^{\mathrm{ord}_2 \frac{c_{E/M} c_{E/F}}{c_{E'/M} c_{E'/F}} + \mathrm{ord}_3 \frac{c_{E/F} c_{E/K}^2}{c_{E/K(\sqrt{D_E})} c_{E/U}^2}} & \text{if } [F:K] = 6 \end{cases}$$

[+analogous formula for the local root numbers]

---

§15 Final remarks

- Instead of thms "finiteness of Ш implies parity" have unconditional analogues for p^∞-Selmer rank

$$\mathrm{rk}_p = \mathrm{rk}\,E/K + \{\mathbb{Q}_p/\mathbb{Z}_p \text{ in } Ш(E/K)\}$$

[E.g. p-isogeny thm is for rk_p. Also over $\mathbb{Q}$ know $(-1)^{\mathrm{rk}_p E/\mathbb{Q}} = w(E$ for all $E/\mathbb{Q}$, all p.

- Compatibility <u>Selmer rks $\leftrightarrow$ Tamagawa numbers</u> works in all Brauer relations and for all abelian varieties.

  Compatibility <u>Tamagawa numbers $\leftrightarrow$ Root numbers</u> also, except for add. red. at $v|2,3$ for ECs and additive reduction for AVs.

  [Also: may not look up to $\mathbb{Q}^{\times 2}$ – work by Alex Bartel; applications to p-Selmer growth and rels between class numbers]

- Example: $\mathrm{Gal}(F/K) = D_{2p}$ has a relation $\Theta = 1 + 2C_2 - C_p - 2D_{2p}$, p odd

$$\rightsquigarrow (-1)^{\mathrm{rk}_p(E, 1\oplus\varepsilon\oplus\tau)} = (-1)^{\mathrm{ord}_p \frac{c(E/F)\,c(E/K)^2}{c(E/M)\,c(E/U)^2}} \overset{\uparrow}{=} w(E, 1\oplus\varepsilon\oplus\tau) \quad \forall\, 2\text{-dim. rep. } \tau \text{ of } D_{2p}$$

  - when E semistable at $v|2,3$.
  - when $p \equiv 3 \mod 4$ (deformation argument)
  - for all $p \geq 5$ (Thomas de la Rochefoucauld)
  - [for AVs – work in progress]

<u>Q</u> Can one do more than parity?