Pollack
PS1

Iwasawa Theory of Elliptic Curves:

$F/\mathbb{Q}$ finite extension

E/F elliptic curve

L/F finite extension. $\to$ $E(L)$ f.g. abelian group ($\longleftrightarrow$ analogue to classical $\mathcal{O}_L^\times$)

$\to$ $Ш(E/L)$ conjecturally a finite group. ($\longleftrightarrow Cl(L)$).

Towers of number fields:

Fix a prime p. (odd)

$$\begin{tikzcd}
 & K_\infty = \mathbb{Q}(\mu_{p^\infty}) \arrow[dd, dash] \arrow[dl, dash, "p-1"'] \arrow[dddl, bend right, dash, "\mathbb{Z}_p^\times"'] \\
\mathbb{Q}_\infty \arrow[dd, dash, "\mathbb{Z}_p"] & \\
 & K_n = \mathbb{Q}(\mu_{p^{n+1}}) \arrow[d, dash, "p^n"] \\
 & K_0 = \mathbb{Q}(\mu_p) \arrow[dl, dash, "p-1"] \\
\mathbb{Q} &
\end{tikzcd}$$

$1+p\mathbb{Z}_p$ ($\simeq \mathbb{Z}_p$)

non canonical

$\mathbb{Q}_\infty$ = Cyclotomic $\mathbb{Z}_p$-extension

Can do the same construction for any number field, not just $\mathbb{Q}$.

$$\begin{tikzcd}
F_\infty \arrow[d, dash] \\
F_n \arrow[d, dash, "p^n"'] \\
F \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
\qquad \left.\right\} \; Gal(F_\infty/F) \simeq \mathbb{Z}_p$$

$\mathbb{Z}_p$-extension

<u>Thm:</u> (Mazur) Assume all primes of F over p are ordinary for E.

If $E(F)$ finite and $Ш(E/F)[p^\infty]$ finite then

$\mathrm{rk}(E/F_n)$ is bounded as $n \to \infty$.

Note that we believe $Ш(E/F)$ is finite, and so $Ш(E/F)[p^\infty]$ should always be finite, we just don't know how to prove it.

• $F = \mathbb{Q}$, p supersingular the same condition holds (Perrin-Riou ~90).

<u>Non-examples:</u>

1) $F/\mathbb{Q}$ quadratic imag. ext., F_∞^{ac} = anticyclo. $\mathbb{Z}_p$-ext.

$$\begin{tikzcd}
& M \arrow[dl, dash] \arrow[dd, dash, "\mathbb{Z}_p^2"] \arrow[dr, dash] & \\
F_\infty^{ac} \arrow[dr, dash] & & F_\infty^{cycl} \subseteq F(\mu_{p^\infty}) \arrow[dl, dash] \\
& F \arrow[d, dash, "2"'] & \\
& \mathbb{Q} \arrow[uul, dash, bend left, "\text{dihedral}"] &
\end{tikzcd}$$

F_∞^{ac} has action of -1 by $\mathrm{Gal}(F/\mathbb{Q})$.

and F_∞^{cycl} is fixed field of action of $\mathrm{Gal}(F/\mathbb{Q})$ on M.

E does not have CM by F (+other conditions)

& sign of functional eq. for $E/F = -1 \Rightarrow \mathrm{rk}(E/F_n) \to \infty$

as $n \to \infty$.

Moreover, $\mathrm{rk}(E/F_n) = p^n + O(1)$

If E has CM by F, p ordinary, then

$$\mathrm{rk}(E/F_n) = \begin{cases} 2p^n + O(1) & \text{sgn of f.e. } E/\mathbb{Q} = -1 \\ O(1) & \quad \text{"} \quad = 1 \end{cases}$$

If p is supersingular, then

$$\mathrm{rk}(E/F_n) = 2\sum_{k>0}^{n} \varphi(p^k) + O(1)$$

constants depend on F and E.

where $(-1)^k = \varepsilon \leftarrow$ sgn of F.E.

So $\mathrm{rk}(E/F_n) \to \infty$ as $n \to \infty$ in all cases..

Selmer group:

$$\mathrm{Sel}_p(E/F) \subseteq H^1(\mathrm{Gal}(\bar{F}/F), E[p^\infty](\bar{F})) = H^1(F, E[p^\infty]).$$

this is cut out by local conditions

v is a place of F, fix some $n \geq 0$

$$E(F_v)/p^n E(F_v) \xhookrightarrow{\text{by Kummer map}} H^1(F_v, E[p^n])$$

$\downarrow$ let $n \to \infty$

$$E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(F_v, E[p^\infty])$$

So when we restrict to F_v, they should be in the image of

$$0 \to \underset{\substack{\text{IS} \\ (\mathbb{Q}_p/\mathbb{Z}_p)^{rk(E/F)}}}{E(F)\otimes \mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow Sel_p(E/F) \longrightarrow \underbrace{Ш(E/F)[p^\infty]}_{\text{conjecturally finite}} \longrightarrow 0$$

So the Selmer group tells you the rank, given that $Ш(E/F)[p^\infty]$ is finite.'

$F_\infty/F = \mathbb{Z}_p$ - ext.

$$\lim_{n\to\infty} Sel_p(E/F_n) = Sel_p(E/F_\infty).$$

$\Gamma = Gal(F_\infty/F)$

$\mathbb{Z}_p[Gal(F_n/F)]$ acts on $Sel_p(E/F_n)$; $\varprojlim_n \mathbb{Z}_p[Gal(F_n/F)] = \mathbb{Z}_p[[\Gamma]]$ acts on $Sel_p(E/F_\infty)$

$= \Lambda =$ Iwasawa algebra

compact

$$X_\infty = X(E/F_\infty) = Sel_p(E/F_\infty)^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(Sel_p(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p).$$

One looks at this because the exact sequence above shows Sel_p looks like a power of $\mathbb{Q}_p/\mathbb{Z}_p$.

<u>Conjecture:</u> (Mazur) F_∞ = cycl. $\mathbb{Z}_p$-ext., p-ord.

$\Rightarrow X_\infty$ is f.g. torsion Λ-module.

Remarks:

1) conj. $\Rightarrow$ $\mathrm{rk}(E/F_n)$ is bounded as $n \to \infty$.

$$0 \to \text{finite} \to E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_p(E/F_\infty)$$

$$E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rk}(E/F_n)}$$

$$X_\infty \to \mathbb{Z}_p^{\mathrm{rk}(E/F_n)} \to \text{finite}$$

In fact, one has

$$X_\infty / (X_\infty)_{\mathbb{Z}_p\text{-torsion}} \to \mathbb{Z}_p^{\mathrm{rk}(E/F_n)}$$

$\cong$ ← module results, true for any f.g. torsion Λ-module

$\mathbb{Z}_p^\lambda$ for some $\lambda \in \mathbb{Z}_{\geq 0}$.

and so $\mathrm{rk}(E/F_n) \leq \lambda$.

<u>Bad case</u> What if $X_\infty = \Lambda$?

$\Lambda \cong \mathbb{Z}_p[[T]]$ ← non-can.

In this case we get no bound.

2) $F = \mathbb{Q}$

BSD: $\chi : \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to \overline{\mathbb{Q}}^\times$

$$L(E, \chi, 1) = 0 \Leftrightarrow E(\mathbb{Q}_n)^\chi \text{ is infinite.}$$

So Mazur's conjecture + BSD $\Rightarrow$ $L(E,\chi,1) \neq 0$ for almost all χ.

- signs of f.e. don't hurt
- proven by D. Rohrlich ($\sim$88)

3) Rohrlich's theorem works for supersingular p.

However, the analogue of Mazur's conjecture is false.

The reason is that even though we believe Ш (E/F_n) are finite, they can grow into $(\mathbb{Q}_p/\mathbb{Z}_p)^a$ or even worse into ∞'ly many copies of $\mathbb{Q}_p/\mathbb{Z}_p$.

Thm (Mazur): F_∞/F any $\mathbb{Z}_p$-ext. Assume X_∞ is Λ-torsion, → forces p to be ordinary or pot. mult.

assume $|Ш(E/F_n)[p^\infty]| < \infty$ $\forall n \geq 0$. Then $\exists$ $\mu, \lambda, \nu \in \mathbb{Z}^{\geq 0}$

s.t.

$$\mathrm{ord}_p(|Ш(E/F_n)[p^\infty]|) = \mu p^n + \lambda n + \nu$$

for all $n \gg 0$.

Thm (Perrin-Riou / Kurihara ~2000): $F = \mathbb{Q}$, p good supersingular prime,

Assume $|Ш(E/\mathbb{Q}_n)[p^\infty]| < \infty$ for all $n \geq 0$. $\varepsilon = \mathrm{sgn}\,(-1)^n$

Then $\exists$ constants $\mu^+, \mu^-, \lambda^+, \lambda^- \in \mathbb{Z}_{\geq 0}$ s.t.

$$\mathrm{ord}_p\left(\frac{|Ш(E/\mathbb{Q}_n)|}{|Ш(E/\mathbb{Q}_{n-1})|}\right) = \mu^\varepsilon(p^n - p^{n-1}) + \lambda^\varepsilon + (p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots)$$

Control Theorem (Mazur): $\overset{F_\infty/F = \mathbb{Z}_p\text{-ext}}{\vee}$ p good ordinary. For each $n \geq 0$, there is a map

$$\mathrm{Sel}_p(E/F_n) \longrightarrow \mathrm{Sel}_p(E/F_\infty)^{\Gamma_n} \qquad (\Gamma_n = \mathrm{Gal}(F_\infty/F_n))$$

which has finite kernel and cokernel w/ size bounded indep. of n.

We rephrase the earlier theorem:

<u>Thm:</u> F_∞/F arbitrary $\mathbb{Z}_p$-ext., p good ordinary

$\mathrm{Sel}_p(E/F)$ finite $\Rightarrow$ $\mathrm{rk}(E/F_n)$ is bounded as $n \to \infty$.

<u>Remark:</u> ① The control theorem is false in the supersingular case.

The cokernel is always infinite and grows exponentially.

② The control theorem and Λ-module theory imply the growth formulas for $Ш(E/F_n)[p^\infty]$.

③ The control theorem implies the theorem above.

<u>Prop:</u> p good ordinary, $\mathrm{Sel}_p(E/F)$ is finite $\Rightarrow$ X_∞ is Λ-torsion

(Prop $\Rightarrow$ theorem above)

<u>Pf of Prop:</u> $n=0$ the control theorem implies $\mathrm{Sel}_p(E/F_\infty)^\Gamma$ is finite. $\Leftrightarrow$ $\mathrm{Sel}_p(E/F_\infty)[\gamma-1]$ is finite $(\Gamma = \langle\gamma\rangle)$

$\Rightarrow$ $X_\infty/(\gamma-1)X_\infty$ is finite.

$\Rightarrow$ X_∞ is Λ-torsion by standard args. ∎

<u>Thm (Kato):</u> Mazur's conjecture is true when $F/\mathbb{Q}$ is abelian.

(and he needs E defined over $\mathbb{Q}$)

Note in the classical case where we replace the Selmer group with the class group, the class group is always finite which makes things easier.

Thm: $\Lambda \simeq \mathbb{Z}_p[\![T]\!]$. If X is a f.g Λ-module, then one has Pollack pg 7

$$X \xrightarrow{\varphi} \Lambda^r \oplus \left(\bigoplus_i \Lambda/(f_i^{e_i})\right)$$

with φ having finite kernel and cokernel and the f_i irred.

This theorem allows one to define the characteristic power series of a torsion Λ-module X by

$$\mathrm{char}_\Lambda X = \left(\prod f_i^{e_i}\right)\Lambda \subseteq \Lambda.$$

By looking at $\mathrm{char}_\Lambda X$ you lose some info (kernel, cokernel, etc) but it still holds a lot of info!

$F = \mathbb{Q}$:

Control Thm

$$\mathrm{char}_\Lambda X_\infty \longleftrightarrow X_\infty \overset{CT}{\longleftrightarrow} \mathrm{Sel}_p(E/\mathbb{Q}_n) \overset{BSD}{\longleftrightarrow} L(E,\chi,1).$$

where $\chi : \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to \overline{\mathbb{Q}}^\times$.

Thm (Mazur/Swinnerton-Dyer): $F = \mathbb{Q}$, p good ordinary. If $E/\mathbb{Q}$ is a (modular) (which it always is) elliptic curve, $\exists!$ $\mathcal{L}_p(E/\mathbb{Q}_\infty) \in \Lambda \otimes \mathbb{Q}_p$ s.t. if $\chi : \Gamma \to \mathbb{C}_p^\times$ of finite order p^n, (induces $\Lambda \xrightarrow{\chi} \mathbb{C}_p$) cond p^{n+1}, then

$$\chi(\mathcal{L}_p(E/\mathbb{Q}_\infty)) = \begin{cases} \dfrac{1}{\alpha^{n+1}}\,\tau(\chi)\,\dfrac{L(E,\chi,1)}{\Omega_E} & n \geq 1 \\[2ex] \left(1 - \dfrac{1}{\alpha}\right)^2 \dfrac{L(E,1)}{\Omega_E} & n = 0 \end{cases}$$

where α is the unique unit root of $x^2 - a_p x + p$ (ok b/c ord)

$\tau(\chi)$ = Gauss sum, Ω_E = Neron period, and we have fixed $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

<u>Main Conjecture:</u> $\mathrm{char}_\Lambda X_\infty = L_p(E/\mathbb{Q}_\infty)\cdot\Lambda$

(equality of ideals)

We can now use BSD & p-adic L-function to conjecturally compute $Ш(E/\mathbb{Q}_n)[p^\infty]$.

<u>BSD:</u> $L(E/\mathbb{Q}_n, 1) \neq 0$, then

$$\frac{L(E/\mathbb{Q}_n, 1)}{\Omega_{E/\mathbb{Q}_n}} = \frac{|Ш(E/\mathbb{Q}_n)|\ |Tam(E/\mathbb{Q}_n)|}{|E_{tor}(\mathbb{Q}_n)|^2\ (Disc(\mathbb{Q}_n))^{1/2}}$$

where $\underset{\substack{\shortparallel \\ D(\mathbb{Q}_n)}}{Disc(\mathbb{Q}_n)}$ is the discriminant of $\mathbb{Q}_n$ to $\mathbb{Q}$.

Examine $\dfrac{|Ш(E/\mathbb{Q}_n)|}{|Ш(E/\mathbb{Q}_{n-1})|}$. We assume $E(\mathbb{Q}_n)$ is finite so we don't have any regulators.

Choose n large enough so that $Tam(E/\mathbb{Q}_n)$ stabilizes and $E(\mathbb{Q}_\infty)_{tor}$ is finite $\Rightarrow$ $E_{tor}(\mathbb{Q}_n)$ stabilizes. (result of Imai)

$L(E/\mathbb{Q}_n, 1) = \prod_\chi L(E, \chi, 1)$ where χ runs over $\widehat{Gal(\mathbb{Q}_n/\mathbb{Q})} \doteq G_n$

So

$$\frac{|Ш(E/\mathbb{Q}_n)|}{|Ш(E/\mathbb{Q}_{n-1})|} \overset{BSD}{=} \prod_{\substack{\chi \text{ of order} \\ p^n \\ \text{in } G_n}} \frac{L(E,\chi,1)}{\Omega_E}\left(\frac{D(\mathbb{Q}_n)}{D(\mathbb{Q}_{n-1})}\right)^{1/2}$$

$$\operatorname{ord}_p\left(\frac{|Ш(E/\mathbb{Q}_n)|}{|Ш(E/\mathbb{Q}_{n-1})|}\right) = \tfrac{1}{2}\operatorname{ord}_p\left(\frac{D(\mathbb{Q}_n)}{D(\mathbb{Q}_{n-1})}\right) + \sum_\chi \operatorname{ord}_p\left(\frac{L(E,\chi,1)}{\Omega_E}\right)$$

$$= \cancel{\tfrac{1}{2}\operatorname{ord}_p\left(\frac{D(\mathbb{Q}_n)}{D(\mathbb{Q}_{n-1})}\right)} + \sum_\chi \operatorname{ord}_p\left(\chi(L_p(E/\mathbb{Q}_\infty))\right)$$

$$\cancel{- \sum_\chi \operatorname{ord}_p(\tau(\chi))}.$$

(computation shows these cancel out) $\qquad p^{n-1}(p-1)$ terms

$$= \sum_\chi \operatorname{ord}_p\left(\chi(L_p(E/\mathbb{Q}_\infty))\right).$$

p-adic Weierstrass prep. thm:

$0 \neq f \in \Lambda$, then

$$f = p^\mu\left(T^\lambda + a_{\lambda-1}T^{\lambda-1} + \cdots + a_0\right) u(T)$$

$$p \mid a_i$$

$u(T) \in \Lambda^\times$.

Then $\quad \chi(f) = f(\zeta_{p^n} - 1) \qquad \underset{\chi(\gamma)}{\overset{\zeta_{p^n}}{\|}} = p^n$ th root of unity

$$\operatorname{ord}_p(\zeta_{p^n} - 1) = \frac{1}{(p-1)p^{n-1}}$$

$$\Rightarrow \quad \operatorname{ord}_p(\chi(f)) = p^\mu + \frac{\lambda}{(p-1)p^{n-1}}$$

So $\quad \operatorname{ord}_p\left(\frac{|Ш(E/\mathbb{Q}_n)|}{|Ш(E/\mathbb{Q}_{n-1})|}\right) = p^{n-1}(p-1)\left(\mu + \frac{\lambda}{p^{n-1}(p-1)}\right) \qquad \mu, \lambda$ of $L_p(E/\mathbb{Q}_\infty)$.

$$= \mu(p^n - p^{n-1}) + \lambda.$$

Construction of $L_p(E/\mathbb{Q}_\infty)$:

Set $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$

$$\sigma_a \longleftrightarrow a$$

Analogue to Stickelberger elements:

of course could always do this .. point is that this is indep. of n!

$$\tilde{\Theta}_n \in \mathbb{Q}[\mathcal{G}_n] \quad \left(\in \tfrac{1}{2}\mathbb{Z}[\mathcal{G}_n] \right)$$

s.t. $\quad \chi(\tilde{\Theta}_n) = \tau(\chi) \dfrac{L(E,\chi,1)}{\Omega_E}, \quad \chi \in \hat{\mathcal{G}}_n.$

$$\tilde{\Theta}_n = \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} c_a \sigma_a \qquad c_a \in \mathbb{Q},$$

$$E/\mathbb{Q} \xleftrightarrow{\text{modularity}} f_E = \text{normalized newform of } \overset{\text{wt } 2}{\vee} \text{ level } N_E$$

where $\quad c_a = \dfrac{1}{2}\left(\displaystyle\int_{a/p^n}^{\infty} f_E(z)\,dz + \int_{-a/p^n}^{\infty} f_E(z)\,dz \right) \Big/ \Omega_E \in \mathbb{Q}.$

(almost in $\mathbb{Z}$!)

Amazingly, this works out.

$n = 0$:

$$\frac{\int_0^\infty f_E(z)}{\Omega_E} = \frac{L(f_E,1)}{\Omega_E} = \frac{L(E,1)}{\Omega_E}$$

and so the general one above is just a twisted version of this.

We now want to use these $\tilde{\Theta}_n$ to construct L_p.

$$\pi : \mathbb{Q}[\mathcal{G}_n] \to \mathbb{Q}[\mathcal{G}_{n-1}]$$

$$u : \mathbb{Q}[\mathcal{G}_{n-1}] \to \mathbb{Q}[\mathcal{G}_n]$$
$$\sigma \longmapsto \sum_{\tau \to \sigma} \tau$$

<u>Prop:</u> $\pi(\tilde{\Theta}_n) = a_p \tilde{\Theta}_{n-1} - u\,\tilde{\Theta}_{n-2}$

<u>Pf:</u> $f|T_p = a_p f$.

<u>Trick:</u>

$$\tilde{\Psi}_n = \tilde{\Theta}_n - \frac{1}{\alpha} u \tilde{\Theta}_{n-1}$$

(exercise)
$$\Rightarrow \quad \pi \tilde{\Psi}_n = \alpha \tilde{\Psi}_{n-1}$$

Define Ψ_n to be the projection of $\tilde{\Psi}_{n+1}$ to $\frac{1}{d}\mathbb{Z}_p[G_n]$ $\quad G_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$

and $\quad L_p(E/\mathbb{Q}_\infty) = \varprojlim_n \frac{1}{\alpha^n} \Psi_n \in \Lambda \otimes \mathbb{Q}_p.$

A little more about the "trick".

$$E \longleftrightarrow f \in S_2(\Gamma_0(N)), \quad p \nmid N, \quad f|T_p = a_p f$$
$$f_\alpha \in S_2(\Gamma_0(Np)) \quad : f_\alpha | U_p = \alpha f_\alpha$$

with $f_\alpha = f(z) - \frac{1}{\alpha} f(pz)$. This is called "p-stabilization".

<u>Remarks:</u>

① If p is supersingular, then $x^2 - a_p x + p$ does not have a unit root. However, you can still construct $L_p(E/\mathbb{Q}_\infty)$ in $\mathbb{Q}_p[[T]]$. It is at least in the subring of convergent power series in the open unit disc.

② One can actually compute $\tilde{\Theta}_n$ using modular symbols.

<u>Algebraic side:</u>

$$0 \to Sel_p(E/\mathbb{Q}_\infty) \to H^1(\mathbb{Q}_\infty, E[p^\infty]) \to \prod_v \frac{H^1(\mathbb{Q}_{\infty,v}, E[p^\infty])}{E(\mathbb{Q}_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

$v \mid \ell \qquad E(\mathbb{Q}_{n,v}) \simeq \mathbb{Z}_\ell^{[\mathbb{Q}_{n,v}:\mathbb{Q}_\ell]} \times (\text{finite group})$

If $\ell \neq p$, then $E(\mathbb{Q}_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$.

$$0 \to Sel_p(E/\mathbb{Q}_\infty) \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \left(\bigoplus_{\substack{v \mid \ell \in \Sigma \\ \ell \neq p}} H^1(\mathbb{Q}_{\infty,v}, E[p^\infty])\right) \times \frac{H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])}{E(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

where Σ = primes of bad reduction for E, p, ∞, $\mathbb{Q}_\Sigma$ is the maximal extension of $\mathbb{Q}$ unramified outside of Σ.

<u>Facts:</u> (Greenberg: Iwasawa Th. of p-adic reps)

- $v \nmid p$ $\quad H^1(\mathbb{Q}_{\infty,v}, E[p^\infty])$ is Λ-cotorsion module
- $H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])$ has Λ-corank 2.

(follows from facts in local Euler characteristics)

- $\operatorname{cork}_\Lambda H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) - \operatorname{cork}_\Lambda H^2(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) = 1.$

$\quad \Rightarrow \operatorname{cork}_\Lambda H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \geq 1.$

- $\mathrm{cork}_\Lambda\, E(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \begin{cases} 1 & p \text{ ordinary} \\ 2 & p \text{ supersingular} \end{cases}$

If p is s.s., then $\mathrm{cork}_\Lambda\, \mathrm{Sel}_p(E/\mathbb{Q}_\infty) \geq 1$ ($=1$ if some H^2 is small).

Tate local duality:

$$H^1(\mathbb{Q}_{n,p}, E[p^\infty]) \times H^1(\mathbb{Q}_{n,p}, T_pE) \xrightarrow{\text{cup prod}} H^2(\mathbb{Q}_{n,p}, \mu_{p^\infty}) \simeq \mathbb{Q}_p/\mathbb{Z}_p$$
is a perfect pairing

$$\begin{array}{ccc} H^1(\mathbb{Q}_{n,p}, E[p^\infty]) & & H^1(\mathbb{Q}_{n,p}, T_pE) \\ \cup\!\text{l} & & \cup\!\text{l} \\ E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & & E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \end{array}$$

exact annihilators under the pairing.

$$\Rightarrow \left(\frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \simeq E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p .$$

$p>2$

$$0 \longrightarrow \underset{\substack{\uparrow \\ \text{formal grp.}}}{\hat{E}(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \longrightarrow E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \longrightarrow \underbrace{\tilde{E}(\mathbb{F}_p) \otimes \mathbb{Z}_p}_{=0 \text{ if } a_p \not\equiv 1 \ (\mathrm{mod}\ p)} \longrightarrow 0.$$

$$\frac{H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])}{E(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} = \varinjlim \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

$$\left(\frac{H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])}{E(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^\vee \approx \varprojlim \hat{E}(\mathbb{Q}_{n,p})$$
(maps by trace for $\varprojlim$).

Thm: For $n \geq 0$, $\exists\, c_n \in \hat{E}(\mathbb{Q}_{n,p})$ s.t. $\langle c_n, c_{n-1}, \ldots, c_0 \rangle$ span $\hat{E}(\mathbb{Q}_{n,p})$ over $\mathbb{Z}_p[Gal(\mathbb{Q}_{n,p}/\mathbb{Q}_p)]$.

If p is ordinary,

$$Tr^n_{n-1}(c_n) = \alpha c_{n-1} \qquad n \geq 2$$
$$Tr^1_0(c_1) = (\alpha - 1) c_0.$$

If p is s.s.

$$\left.\begin{aligned} Tr^n_{n-1}(c_n) &= a_p c_{n-1} - c_{n-2} \qquad n \geq 2 \\ Tr^1_0(c_n) &= u\, c_0 \qquad u \in \mathbb{Z}_p^\times \end{aligned}\right\} \text{Kobayashi}$$

Consequences:

① if $a_p \not\equiv 1 \pmod p$ ($p \nmid a_p$) $\Rightarrow \hat{E}(\mathbb{Q}_{n,p})$ is a free $\mathbb{Z}_p[G_n]$-module generated by c_n.

$\mathbb{Z}_p$-rk are both p^n.

$$\mathbb{Z}_p[G_n] \xrightarrow{\sim} \hat{E}(\mathbb{Q}_{n,p})$$
$$1 \longmapsto c_n$$

$$\varprojlim_n \hat{E}(\mathbb{Q}_{n,p}) \simeq \Lambda$$

$\Rightarrow$ we get $\operatorname{cork}_\Lambda = 1$.

Still true if $a_p \equiv 1 \pmod p$, just have to work harder!

② $p \mid a_p$

Assume $a_p = 0$ ($p > 3$ this is true).

Looking back at the trace relations, we see we need c_n and c_{n-1} to get all the terms. Thus $\hat{E}(\mathbb{Q}_{n,p})$ needs 2 generators as a Galois module

$\mathrm{Tr}^{n}_{n-1}(c_n) = -c_{n-2}$

$\mathrm{Tr}^{n}_{n-2}(c_n) = -p\,c_{n-2}$

Can continue this ... get more powers of p.

$\Rightarrow \varprojlim \hat{E}(\mathbb{Q}_{n,p}) = 0$ (each time we lift, divide by a power of p so base has to be divisible by p^m for all m ... $\Rightarrow$ trivial)

$\Rightarrow E(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = H^1(\mathbb{Q}_{\infty,p}, E[p^\infty])$.

Control theorem

$$\mathcal{H}_{n,\ell} = \bigoplus_{\substack{v \mid \ell \\ \text{in } \mathbb{Q}_n}} H^1(\mathbb{Q}_{n,v}, E[p^\infty]) \qquad , \; n \le \infty \qquad \ell \neq p$$

$$\mathcal{H}_{n,p} = \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \qquad , \; n \le \infty$$

$$\begin{tikzcd}
& \ker(s_n) \arrow[r, hook] \arrow[d, hook] & H^1(\mathbb{Q}_\infty/\mathbb{Q}_n, E[p^\infty](\mathbb{Q}_\infty)) \arrow[d, hook] & \leftarrow \text{finite (exercise)} \\
0 \arrow[r] & \mathrm{Sel}_p(E/\mathbb{Q}_n) \arrow[r] \arrow[d, "s_n"] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]) \arrow[r] \arrow[d, "h_n"] & \bigoplus_{\ell \in \Sigma} \mathcal{H}_{n,\ell} \arrow[d, "\oplus r_{n,\ell}"] \\
0 \arrow[r] & \mathrm{Sel}_p(E/\mathbb{Q}_\infty)^{\Gamma_n} \arrow[r] \arrow[d] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n} \arrow[r] \arrow[d] & \bigoplus_{\ell \in \Sigma} \mathcal{H}_{\infty,\ell}^{\Gamma_n} . \\
& \mathrm{coker}\, s_n & 0 = H^2(\Gamma_n, E[p^\infty]) &
\end{tikzcd}$$

Γ_n has cohom. dim 1.

$\cancel{H^1(\Gamma_n, E[p^\infty](\mathbb{Q}_\infty)) = (E[p^\infty](\mathbb{Q}_\infty))_{\Gamma_n}}$ $\leftarrow$ coinvariants

$\cancel{E[p^\infty](\mathbb{Q}_\infty) \xrightarrow{\gamma^{p^n}-1} E[p^\infty](\mathbb{Q}_\infty) \to \bigcirc \to 0}$

$\cancel{0 \to E[p^\infty](\mathbb{Q}_n)}$ $\leftarrow$ finite

<u>Exercise:</u> $\ker(r_{n,p})$ is finite bounded indep. of n.

$$\mathcal{H}_{n,p} \xhookrightarrow{r_{n,p}} \mathcal{H}_{\infty,p} \qquad\qquad a_p \not\equiv 1 \pmod p$$

$\downarrow$ dualize

$$\varprojlim_m \hat{E}(\mathbb{Q}_{m,p}) \twoheadrightarrow \hat{E}(\mathbb{Q}_{n,p})$$

We begin by cleaning up the arg from last time:

$$\begin{tikzcd}
 & \ker(s_n) \arrow[r, hook] \arrow[d, hook] & (E[p^\infty](\mathbb{Q}_\infty))_\Gamma \arrow[r] \arrow[d, hook] & \oplus\, \ker(r_{n,v}) \cap \operatorname{im}(\alpha) \arrow[dddll, dashed, bend left] \\
0 \arrow[r] & \mathrm{Sel}_p(E/\mathbb{Q}_n) \arrow[r] \arrow[d, "s_n"] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]) \arrow[r, "\alpha"] \arrow[d, "h_n"] & \bigoplus_v \mathcal{H}_{n,v} \arrow[d] \\
0 \arrow[r] & \mathrm{Sel}_p(E/\mathbb{Q}_\infty)^{\Gamma_n} \arrow[r] \arrow[d] & H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n} \arrow[r] \arrow[d] & \bigoplus_w \mathcal{H}_{\infty,w}^{\Gamma_n} \\
 & \operatorname{coker}(s_n) \arrow[r] & 0 = H^2 &
\end{tikzcd}$$

- $\ker(s_n)$ is finite bounded indep of n b/c $(E[p^\infty](\mathbb{Q}_\infty))_\Gamma$ is.

  In fact, $E(\mathbb{Q})[p] = 0 \Rightarrow \ker(s_n) = 0$.

- $v \nmid p$ $\quad |\ker(r_{n,v})| \underset{\uparrow}{\sim} \mathrm{Tam}_v(E/\mathbb{Q}_n)$ bounded indep. of n.

  equal up to p-adic unit

- $\ker(r_{n,p}) = 0$ if $a_p \not\equiv 1 \pmod p$ and finite bounded indep of p regardless of a_p (as long as $p \nmid a_p$).

$$\varprojlim_m \hat{E}(\mathbb{Q}_{m,p}) \twoheadrightarrow \hat{E}(\mathbb{Q}_{n,p})$$

$a_p \not\equiv 1 \pmod p$ (look at explicit c_n's).

So this gives the Control theorem.

Cor: Assume $E(\mathbb{Q})$ finite, $Ш(E/\mathbb{Q})[p]=0$, $p \nmid \mathrm{Tam}(E/\mathbb{Q})$

$a_p \neq 0,1 \pmod p$, then $E(\mathbb{Q}_n)$ is finite for all $n \geq 0$

and $Ш(E/\mathbb{Q}_n)[p]=0$.

Remark: Under BSD, $\dfrac{L(E,1)}{\Omega_E}$ is a p-unit, $(1-\frac{1}{\alpha})^2$ is a p-unit.

Proof: $\mathrm{Sel}_p(E/\mathbb{Q})=0 \overset{CT}{\Rightarrow} \mathrm{Sel}_p(E/\mathbb{Q}_n)^{\Gamma}=0$

$\Rightarrow X_\infty/TX_\infty = 0 \overset{\text{Nakayama}}{\Longrightarrow} X_\infty = 0$.

$\overset{CT}{\Rightarrow} \mathrm{Sel}_p(E/\mathbb{Q}_n)=0$. ∎

We now switch to the supersingular case.

$p | a_p$ $\mathcal{H}_{\infty,p}=0$ and as $\ker(r_{n,p}) = \mathcal{H}_{n,p}$

$\Rightarrow \ker(r_{n,p})^\vee = \hat{E}(\mathbb{Q}_{n,p}) \simeq \mathbb{Z}_p^{p^n}$.

Write $S_n = \mathrm{Sel}_p(E/\mathbb{Q}_n)$ $n \leq \infty$, $X_n = S_n^\vee$ $n \leq \infty$.

$$0 \to S_n \to S_\infty^{\Gamma_n} \to \left(\oplus \ker r_{n,v}\right) \cap \mathrm{im}(\alpha)$$

$$\cap \mid$$

$$\oplus(\ker r_{n,v})$$

dualizing:

$$\hat{E}(\mathbb{Q}_{n,p}) \times \text{finite} \longrightarrow (X_\infty)_{\Gamma_n} \longrightarrow X_n \longrightarrow 0 \qquad (*)$$

"Simplest case" (p | a_p still).

- $\mathrm{Sel}_p(E/\mathbb{Q}) = 0$ ← So
- $p \nmid \mathrm{Tam}(E/\mathbb{Q})$ (says "finite" is gone)

$\boxed{n=0}$ $(*) \Rightarrow$

$$\mathbb{Z}_p \twoheadrightarrow (X_\infty)_\Gamma \longrightarrow X_0 = 0 .$$

!

$\mathrm{rk}_\Lambda X_\infty \geq 1 \Rightarrow \mathrm{rk}_{\mathbb{Z}_p}(X_\infty)_\Gamma \geq 1. \Rightarrow \mathrm{rk}_{\mathbb{Z}_p}(X_\infty)_\Gamma = 1.$

general theory

$\Rightarrow X_\infty \simeq \Lambda .$

$\boxed{n \geq 1}$

$$\hat{E}(\mathbb{Q}_{n,p}) \xrightarrow{P_n} \mathbb{Z}_p[G_n] \longrightarrow X_n \longrightarrow 0$$

$G_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ generated by c_n, c_{n-1}.

So $X_n \simeq \mathbb{Z}_p[G_n] / (P_n(c_n), P_n(c_{n-1})).$

(finite, but big)

Facts: ① One can define μ, λ-invariants for elements of $\mathbb{Z}_p[G_n]$.

② $\exists$ exact formulas for $\lambda(P_n(c_n))$ for all $n \geq 0$ and $\mu(P_n(c_n)) = 0$ for all $n \geq 0$ (in this simple case) and these tend to ∞ in n but in a very regular way.

③ $\mathrm{ord}_p |Ш_n| = \sum_{k=0}^{n} \lambda(P_k(c_k)) < \infty$.

Now we remove the simplest case assumption:

$$\hat{E}(\mathbb{Q}_{n,p}) \times (\text{finite}) \to (X_\infty)_{\Gamma_n} \to X_n \to 0$$

(Kato) $\Rightarrow$ X_∞ has Λ-rk $= 1$.

$$\begin{tikzcd} Y \arrow[r] & X_\infty \arrow[r] & Z \arrow[r] & 0 \end{tikzcd}$$

↑ submodule of Λ-torsion

↑ Λ-torsion-free

$$\mathcal{B} \to Z \to \Lambda \to \underset{\text{finite}}{H} \to 0$$

As we get

$$\begin{tikzcd} \hat{E}(\mathbb{Q}_{n,p}) \arrow[r] \arrow[d, shift right, "Tr"'] \arrow[rrr, bend right, "P_n"] & (X_\infty)_{\Gamma_n} \arrow[r] & Z_{\Gamma_n} \arrow[r] & \Lambda_{\Gamma_n} = \mathbb{Z}_p[G_n] \arrow[d, shift right, "\pi"'] \\ \hat{E}(\mathbb{Q}_{n-1,p}) \arrow[u, shift right] \arrow[rrr, "P_{n-1}"] & & & \mathbb{Z}_p[G_{n-1}] \arrow[u, shift right, "\nu"'] \end{tikzcd}$$

Define $\varphi_n = P_n(c_n) \in \mathbb{Z}_p[G_n]$.

Recall $\mathrm{Tr}^n_{n-1}(c_n) = a_p c_{n-1} - c_{n-2}$

$\Downarrow$

$$\pi \varphi_n = a_p \varphi_{n-1} - \nu \varphi_{n-2}$$

Let $\tau = \mathrm{Char}_\Lambda Y$, $\Theta_n^{alg} = \varphi_n \cdot \tau$, Θ_n^{an} = Mazur-Tate elts.
(analogue of Stickelberger elt)

<u>Main conjecture:</u> $\Theta_n^{an} = \Theta_n^{alg} \cdot u$ where $u \in \mathbb{Z}_p[G_n]^\times$

$n \geq 0$

(Perrin-Riou ~90)

Kato $\Rightarrow$ $\Theta_n^{alg} \mid \Theta_n^{an}$ in $\mathbb{Z}_p[G_n]$.

- $\lambda(\Theta_n^*)$ - there exist "exact" formulas for these invariants which go to ∞ as $n \to \infty$.

$* = $ an or alg

<u>Prop:</u> χ char. of order p^n on G_n. Then $\chi(\Theta_n^{alg}) = 0$ iff $\mathrm{Sel}_p(E/\mathbb{Q}_n)^\chi$ infinite.

$$\text{BSD} \;\&\; \text{mc} \Rightarrow \chi(\Theta_n^{alg}) = 0 \overset{mc}{\Longleftrightarrow} \chi(\Theta_n^{an}) = 0$$

$$\Longleftrightarrow L(E, \chi, 1) = 0$$

$$\overset{BSD}{\Longleftrightarrow} E(\mathbb{Q}_n)^\chi = \infty.$$

<u>Prop:</u> if $\varphi_0 \neq 0$, then $\chi(\Theta_n^{alg}) = 0$ for only finitely many such χ.

order p^n

<u>Cor:</u> $\mathrm{Sel}_p(E/\mathbb{Q}) < \infty \Rightarrow \mathrm{Cork}_{\mathbb{Z}_p}(\mathrm{Sel}_p(E/\mathbb{Q}_n))$ is bounded indep. of n. (Perrin Riou)

Proof: combine the two propositions.

Open questions:

1) We have assumed $F = \mathbb{Q}$. Can we replace all of this with

$F/\mathbb{Q}$ fin. ext.

2) We were taking $F_\infty = \mathbb{Q}_\infty$ $\rightsquigarrow$ replace this with arb. $\mathbb{Z}_p$-ext.

3) Replace $E/\mathbb{Q}$ with a modular form of higher weight.

(non-ordinary forms)

4) Non-abelian case

5) Main conjecture is open for non-ordinary case.