Iwasawa Theory for supersingular primes:

F = number field

E/F elliptic curve

Selmer group: $Sel_p(E/F) = \ker\left(H^1(G_{F,S}, E[p^\infty]) \to \prod_{v \text{ prime of } F} \frac{H^1(G_{F_v}, E[p^\infty])}{E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$

One has an exact sequence:

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to Sel_p(E/F) \to Ш(E/F)_{p^\infty} \to 0$$

$v <_{\text{prime}} \mathcal{O}_F$, $k_v = \mathcal{O}_F/v$, $\ell = \text{char}(k_v)$

$a_v = 1 + Nmv - \#E(k_v)$

E has "ordinary" reduction at v if $\ell \nmid a_v$

E has "supersingular" reduction at v if $\ell \mid a_v$

(of course, assuming E has good reduction at v)

Let F_∞/F be a $\mathbb{Z}_p$-ext.

Mazur's Control Theorem: Let p be a prime. Suppose E has good ordinary reduction at every prime above p. Then the natural map

$$Sel_p(E/F_n) \to Sel_p(E/F_\infty)^{Gal(F_\infty/F_n)}$$

has finite kernel and cokernel and bounded as n varies.

Corollary: Under the same hypotheses, $E(F)$ and $Ш(E/F)_{p^\infty}$ are finite, then one knows

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

is finitely rank. (quotient by torsion prior.)

What if any prime above p is supersingular?

Then $Sel_p(E/F_\infty)^\vee$ has infinite rank. However one expect $E(F_\infty)$ to have finite rank over $\mathbb{Z}$.

A possible solution to this is to use Kobayashi's $\pm$-Selmer group theory.

Restrict to the case of $\mathbb{Q}_\infty/\mathbb{Q}$ the cyclotomic $\mathbb{Z}_p$-ext. Assume p Kobayashi defined

$$Sel_p^\pm(E/\mathbb{Q}_n) \subset Sel_p(E/\mathbb{Q}_n).$$

Let χ be a primitive character of $Gal(\mathbb{Q}_n/\mathbb{Q})$.

n is even for plus group

n is odd for minus group

More or less one has,

$$Sel_p^\pm(E/\mathbb{Q}_n)^\chi \approx Sel_p(E/\mathbb{Q}_n)^\chi$$

and

$$Sel_p^\pm(E/\mathbb{Q}_n) \longrightarrow Sel_p^\pm(E/\mathbb{Q}_\infty)^{Gal(\mathbb{Q}_\infty/\mathbb{Q})}$$

is "controlled".

Application: Parity conj.

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_p(E/\mathbb{Q}) \equiv \operatorname{ord}_{s=1} L(E,s) \pmod 2$$

This is a result of Nekovar '02 when p ordinary, Kim when p supersingular '03, Dokchitser '09 all prime.

Generalization:

i) $a_p \neq 0$?

ii) E/F and $F \neq \mathbb{Q}_p$. F local field of res. char p.

a) $F/\mathbb{Q}_p$ unram.

b) $F/\mathbb{Q}_p$ ram.

iii) modular forms of higher weight ($a_p = 0$ Antonia Zay)

iv) K_∞/K, K = imag. quad, $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p^2$.

(a) $\mathrm{Sel}_p^{\pm}$ (p splits completely $K/\mathbb{Q}$)

(b) $X_p^{\pm}$ f.g.

Let f be a cuspidal eigenform of wt 2, trivial char.

A = abelian variety associated to f

$$f(z) = \sum_{n \geq 1} a_n q^n$$

$R = \mathbb{Z}[\{a_n\}] \subset \mathrm{End}(A)$

Assume $\exists$ prime ideal $\wp \subset R$ above p so that $a_p \in \wp$.

Foundation of Kobayashi's theory:

The construction of $x_n \in A(\mathbb{Q}_{n,p})$ s.t.

$$\mathrm{Tr}_{n/n-1} x_n = x_{n-2}.$$

B. D. Kim

7-6-09

PS4

Fontaine-Lafaille's theory of smooth group schemes with Kobayashi's idea produces

- $x_n \in A(\mathbb{Q}_{n,p})$ so that

$$Tr_{n/n-1} x_n = a_p x_{n-1} + x_{n-2}$$

$$\equiv x_{n-2} \pmod{a_p A(\mathbb{Q}_{n-1,p})}$$

Construct algebraic p-adic function $\mathcal{L}_p^{\pm} \in (R_p/a_p)[\![X]\!]$ that satisfies

i) if $\mathcal{L}_p^{\pm}(0) \neq 0 \pmod{a_p}$, then

$$\mathcal{L}_p^{\pm}(0) = \#Sel_p(A[p^\infty]/\mathbb{Q}) \prod Tam$$

up to R_p/a_p unit

ii) $\forall$ prim char of $Gal(\mathbb{Q}_n/\mathbb{Q})$

n even for $\mathcal{L}_p^+$

n odd for $\mathcal{L}_p^-$

If $\mathcal{L}_p^{\pm}(\zeta_{p^n}-1) \neq 0 \pmod{a_p}$, then

$$\alpha^{-\frac{1}{p^{(p-1)}}} \leq v_p(\mathcal{L}_p^{\pm}(\zeta_{p^n}-1)) \leq \underbrace{v_p(\#Sel_p(A[p^\infty]/\mathbb{Q}_n)^\chi)}_{\alpha}$$

Analytic $\pm$-theory?

$a_p = 0$ (Pollack) $\mathcal{L}_{p,a_p}^{\pm}(E,X) \in \mathbb{Z}_p[\![X]\!]$

What if $a_p \neq 0$? Kato constructed Euler system

$$Z^{\pm} \in H^1_{IW}(\mathbb{Q}_\infty, T)$$

$$H^1_{IW}(\mathbb{Q}_\infty, T) \longrightarrow H^1_{IW}(\mathbb{Q}_{\infty,p}, T) \xrightarrow{PR^{\pm}} (R_p/a_p)[\![X]\!]$$

$Z^{\pm}$ ↑ using x_n

The image of $Z^{\pm} = \mathcal{L}_{p,an}^{\pm}$.

do

$$\mathcal{L}_p^{\pm} = \mathcal{L}_{p,an}^{\pm} \quad \text{in } (R_g/a_p)\mathbb{I} \times \mathbb{I} ?$$