Algebraic theory for supersingular primes:

\[ F = \text{number field} \]
\[ E/F = \text{elliptic curve} \]
\[ \text{Selmer group: } \text{Sel}_p(E/F) = \ker(H'(G_{F_p}, E_{p^n}) \rightarrow \prod_{\text{prime } \ell} H'(G_{F_{p^n}}, E_{p^n})) \]

\[ E \text{ has an exact sequence:} \]
\[ 0 \rightarrow E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow \text{Sel}_p(E/F) \rightarrow \text{H}lll(E/F)_{p^n} \rightarrow 0 \]

\[ v \in \text{prin } O_F, \quad \varphi = O_{p^n}, \quad \ell = \text{char}(\mathbb{F}_v) \]
\[ a_v = 1 + N_{\mathbb{F}_v} - \#E(\mathbb{F}_v) \]

\[ E \text{ has "ordinary" reduction at } v \neq \ell x_\mathbb{F}_v \]
\[ E \text{ has "supersingular" reduction at } v = \ell x_\mathbb{F}_v \]

(\text{Of course, assuming } E \text{ has good reduction at } v)

Let \( F_{\ell^n}/F \) be a \( \mathbb{Z}_p \)-extension.

Mazur's Control Theorem: Let \( p \) be a prime. Suppose
\[ E \text{ has good ordinary reduction at every prime above} \]
\[ p. \text{ Then the natural map} \]
\[ \text{Sel}_p(E/F_{\ell^n}) \rightarrow \text{Sel}_p(E/F) \]

has finite kernel and cokernel and bounded as \( \ell \rightarrow \infty \).

Corollary: Under the same hypotheses, \( E(F) \) and \( \text{H}lll(E/F)_{p^n} \)
are finite, then one knows
\[ \text{Sel}_p(E/F_\infty)^* = \text{Hom}(\text{Sel}_p(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p) \]

in infinitely many cases (quotient by torsion prior.)

What if any prime above \( p \) is supersingular?

Then \( \text{Sel}_p(E/F_\infty)^* \) has infinite rank. However one expects \( E(F_\infty) \) to have finite rank over \( \mathbb{Z} \).

A possible solution to this is to use Kobayashi's ±-Selmer group theory.

Restrict to the case of \( \mathbb{Q}_n/\mathbb{Q} \), the cyclotomic \( \mathbb{Z}_p \)-extension. Assume \( \chi = \pm \) is Kobayashi defined

\[ \text{Sel}_p^\pm(E/\mathbb{Q}_n) \subset \text{Sel}_p(E/\mathbb{Q}_n) \]

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

- \( n \) is even for plus group
- \( n \) is odd for minus group

More or less one has,

\[ \text{Sel}_p^\pm(E/\mathbb{Q}_n)^* \cong \text{Sel}_p(E/\mathbb{Q}_n)^* \]

and

\[ \text{Sel}_p(E/\mathbb{Q}_n) \to \text{Sel}_p^\pm(E/\mathbb{Q}_n) \]

is "controlled".
Application: Parity conj.

corank \( \text{Sel}_p(E/Q) \equiv \text{ord} L(E,s) \pmod{2} \)

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

Generalization:

1) \( q_p \neq 0 \)?

2) \( E/F \) and \( F \neq \mathbb{Q} \) finite fields \( \neq \mathbb{Q} \) char \( p \).
   a) \( F/\mathbb{Q}_p \) unram.
   b) \( F/\mathbb{Q}_p \) ram.

3) modular forms of \( \mathfrak{p} \)-twist weight \( (\mathfrak{p} =\mathfrak{p} \text{ Artin} \, \text{loc}) \)

4) \( K_{10}/K \), \( K = \text{max. good} \), \( \mathcal{O}_K(K_{10}/K) = \mathbb{Z}_p^2 \).
   a) \( \text{Sel}_p^+ \) (\( p \)-split completely \( K/\mathbb{Q} \))
   b) \( \text{Sel}_p^+ \) f. in.

Let \( f \) be a cuspidal eigenform at \( \mathfrak{p} \), trivial char.

\( \mathcal{A} \) abelian variety associated to \( f \)

\[ f(\mathfrak{a}) = \sum a_n q^n \]

\[ R = \mathbb{Z}[[q]] \subset \text{End}(\mathcal{A}) \]

Assume \( \mathfrak{p} \) prime ideal \( \mathfrak{p} \subset \mathcal{O}_K \) above \( p \) so that \( \mathfrak{p} \mathfrak{p} = \mathfrak{p} \).

Foundation of Kolyagin's theory:

the construction of \( \mathcal{X}_n \in \mathcal{A}(\mathcal{O}_K, \mathfrak{p}) \) s.t.

\[ T_{\mathfrak{p}^{n+1}} \mathcal{X}_n = \mathcal{X}_{n-1} \]
Fontaine-Laffaille's theory of smooth group schemes with
Kohrashi's idea produces

\[ x_n \in A(\mathbb{Q}_p) \text{ so that} \]

\[ T_{n-1} x_n = A_{x_{n-1} + x_{n-2}} \]

\[ \equiv x_{n-2} \pmod{a_p A(\mathbb{Q}_{n-1})} \]

Construct algebraic p-adic function \( \mathcal{L}_p \in \left( \mathbb{Q}/\mathbb{Z} \right)[X] \) that satisfies

1. If \( \mathcal{L}_p^\pm(0) \neq 0 \pmod{a_p} \), then

\[ \mathcal{L}_p^\pm(0) = \# \text{Sel}_p(A_{\mathbb{Q}^\infty}/\mathbb{Q}) \cap T_{n-1} \]

up to \( \mathbb{Q}/\mathbb{Z} \)-unit

2. If \( \mathcal{L}_p^\pm(3p-2) \neq 0 \pmod{a_p} \), then

\[ a \equiv \frac{1}{1+\frac{1}{p-1}} \cdot \mathcal{L}_p^\pm(3p-2) \equiv \mathcal{L}_p^\pm(\# \text{Sel}_p(A_{\mathbb{Q}^\infty}/\mathbb{Q})) \]

Analytic \( \pm \)-theory?

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

What if \( a_p \neq 0 \)? Kohm constructed Euler system

\[ Z^\pm \subset H_{I}^{\mathfrak{R}}(\mathbb{Q}_p, T) \]

\[ H_{I}^{\mathfrak{R}}(\mathbb{Q}_p, T) \rightarrow H_{I}^{\mathfrak{R}}(\mathbb{Q}_{p, \mathfrak{p}}, T) \xrightarrow{\mathfrak{p}^* \text{pr}^*} (\mathbb{Q}/\mathbb{Z})[[X]] \]

\[ Z^\pm \equiv \text{using } X_n \]
The image of $Z^\pm = \mathcal{X}_{\text{ran}}^\pm$.

\[ \mathcal{X}_{\text{ran}}^\pm = \mathcal{X}_{\text{ran}}^\pm \quad \text{in} \quad (\mathbb{R}^{+}/\mathbb{A}) \times \mathbb{I}? \]