

Iwasawa theory of CM elliptic curves at potentially supersingular primes

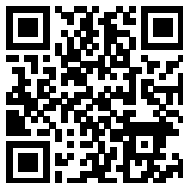
joint work with Antonio Lei

[arXiv:2609.13063]

Ben Forrás

University of Ottawa

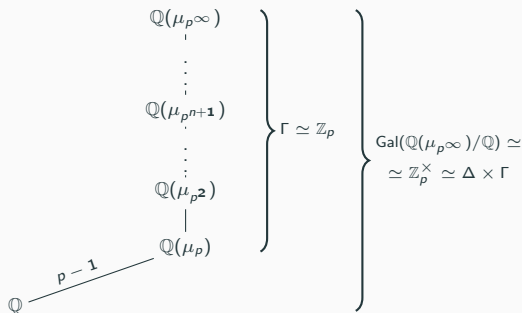
22 October 2026



$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \Delta \times \Gamma$ with $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\Gamma \simeq \mathbb{Z}_p$

$\mathbb{Q}_\infty := \mathbb{Q}(\mu_{p^\infty})^\Delta$ fixed field is called the **cyclotomic $\mathbb{Z}_p$ -extension** of $\mathbb{Q}$

For each $n \geq 0$, there is a unique subfield $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ with $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$



Fix a compatible system of primitive p -power roots of unity $(\zeta_{p^n})_{n \geq 0}$, i.e. $\zeta_{p^{n+1}}^p = \zeta_{p^n}$

$E/\mathbb{Q}$ elliptic curve, $p \geq 5$ fixed prime number

Iwasawa theory: study arithmetic invariants (Selmer group, Tate–Shafarevich group etc.) attached to E along the cyclotomic $\mathbb{Z}_p$ -tower

$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \Delta \times \Gamma$ with $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\Gamma \simeq \mathbb{Z}_p$

$\mathbb{Q}_\infty := \mathbb{Q}(\mu_{p^\infty})^\Delta$ fixed field is called the **cyclotomic $\mathbb{Z}_p$ -extension** of $\mathbb{Q}$

For each $n \geq 0$, there is a unique subfield $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ with $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$

$$\left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n) \\ \simeq p^n \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \mathbb{Q}_\infty \\ \vdots \\ \mathbb{Q}_n \\ \vdots \\ \mathbb{Q}_1 \\ \vdots \\ \mathbb{Q} \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \\ \simeq \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\} \left\{ \begin{array}{l} \mathbb{Q}(\mu_{p^\infty}) \\ \vdots \\ \mathbb{Q}(\mu_{p^{n+1}}) \\ \vdots \\ \mathbb{Q}(\mu_{p^2}) \\ \vdots \\ \mathbb{Q}(\mu_p) \end{array} \right\} \left\{ \begin{array}{l} \Delta \\ p-1 \\ p-1 \\ p-1 \end{array} \right\} \left\{ \begin{array}{l} \Gamma \simeq \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \\ \simeq \mathbb{Z}_p^\times \simeq \Delta \times \Gamma \end{array} \right\}$$

Fix a compatible system of primitive p -power roots of unity $(\zeta_{p^n})_{n \geq 0}$, i.e. $\zeta_{p^{n+1}}^p = \zeta_{p^n}$

$E/\mathbb{Q}$ elliptic curve, $p \geq 5$ fixed prime number

Iwasawa theory: study arithmetic invariants (Selmer group, Tate–Shafarevich group etc.) attached to E along the cyclotomic $\mathbb{Z}_p$ -tower

$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \Delta \times \Gamma$ with $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\Gamma \simeq \mathbb{Z}_p$

$\mathbb{Q}_\infty := \mathbb{Q}(\mu_{p^\infty})^\Delta$ fixed field is called the **cyclotomic $\mathbb{Z}_p$ -extension** of $\mathbb{Q}$

For each $n \geq 0$, there is a unique subfield $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ with $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$

$$\left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n) \simeq p^n\mathbb{Z}_p \\ \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\} \left\{ \begin{array}{l} \mathbb{Q}_\infty \xrightarrow{\Delta} \mathbb{Q}(\mu_{p^\infty}) \\ \vdots \\ \mathbb{Q}_n \xrightarrow{p-1} \mathbb{Q}(\mu_{p^{n+1}}) \\ \vdots \\ \mathbb{Q}_1 \xrightarrow{p-1} \mathbb{Q}(\mu_{p^2}) \\ \mathbb{Q} \xrightarrow{p-1} \mathbb{Q}(\mu_p) \end{array} \right\} \left\{ \begin{array}{l} \Gamma \simeq \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \\ \simeq \mathbb{Z}_p^\times \simeq \Delta \times \Gamma \end{array} \right\}$$

Fix a compatible system of primitive p -power roots of unity $(\zeta_{p^n})_{n \geq 0}$, i.e. $\zeta_{p^{n+1}}^p = \zeta_{p^n}$

$E/\mathbb{Q}$ elliptic curve, $p \geq 5$ fixed prime number

Iwasawa theory: study arithmetic invariants (Selmer group, Tate–Shafarevich group etc.) attached to E along the cyclotomic $\mathbb{Z}_p$ -tower

$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \Delta \times \Gamma$ with $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\Gamma \simeq \mathbb{Z}_p$

$\mathbb{Q}_\infty := \mathbb{Q}(\mu_{p^\infty})^\Delta$ fixed field is called the **cyclotomic $\mathbb{Z}_p$ -extension** of $\mathbb{Q}$

For each $n \geq 0$, there is a unique subfield $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ with $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$

$$\left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n) \\ \simeq p^n\mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \mathbb{Q}_\infty \\ \vdots \\ \mathbb{Q}_n \\ \vdots \\ \mathbb{Q}_1 \\ \vdots \\ \mathbb{Q} \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \\ \simeq \mathbb{Z}/p^n\mathbb{Z} \end{array} \right\} \left\{ \begin{array}{l} \mathbb{Q}(\mu_{p^\infty}) \\ \vdots \\ \mathbb{Q}(\mu_{p^{n+1}}) \\ \vdots \\ \mathbb{Q}(\mu_{p^2}) \\ \vdots \\ \mathbb{Q}(\mu_p) \end{array} \right\} \left\{ \begin{array}{l} \Delta \\ p-1 \\ p-1 \\ p-1 \end{array} \right\} \left\{ \begin{array}{l} \Gamma \simeq \mathbb{Z}_p \end{array} \right\} \left\{ \begin{array}{l} \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \\ \simeq \mathbb{Z}_p^\times \simeq \Delta \times \Gamma \end{array} \right\}$$

Fix a compatible system of primitive p -power roots of unity $(\zeta_{p^n})_{n \geq 0}$, i.e. $\zeta_{p^{n+1}}^p = \zeta_{p^n}$

$E/\mathbb{Q}$ elliptic curve, $p \geq 5$ fixed prime number

Iwasawa theory: study arithmetic invariants (Selmer group, Tate–Shafarevich group etc.) attached to E along the cyclotomic $\mathbb{Z}_p$ -tower

Recall: $\Gamma \simeq \mathbb{Z}_p$

Definition (Iwasawa algebra)

$\Lambda = \Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]] = \varprojlim_U \mathbb{Z}_p[\Gamma/U]$ as $U \subseteq \Gamma$ runs over open normal subgroups

By fixing a topological generator $\gamma \in \Gamma$, there is a non-canonical isomorphism

$$\Lambda(\Gamma) = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]], \gamma \mapsto 1 + T$$

Fix such a γ , and tacitly identify the two rings from now on.

Structure theorem

If M is a finitely generated $\Lambda = \Lambda(\Gamma)$ -module, then there is a homomorphism with finite kernel and cokernel:

$$M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

If M is Λ -torsion:

$$\text{char}_\Lambda(M) := p^{\sum m_i} \cdot \prod F_j$$

Pontryagin dual: $M^\vee := \text{Hom}_{\text{cts}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, compact $\leftrightarrow$ discrete

Recall: $\Gamma \simeq \mathbb{Z}_p$

Definition (Iwasawa algebra)

$\Lambda = \Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]] = \varprojlim_U \mathbb{Z}_p[\Gamma/U]$ as $U \subseteq \Gamma$ runs over open normal subgroups

By fixing a topological generator $\gamma \in \Gamma$, there is a non-canonical isomorphism

$$\Lambda(\Gamma) = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]], \gamma \mapsto 1 + T$$

Fix such a γ , and tacitly identify the two rings from now on.

Structure theorem

If M is a finitely generated $\Lambda = \Lambda(\Gamma)$ -module, then there is a homomorphism with finite kernel and cokernel:

$$M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

If M is Λ -torsion:

$$\text{char}_\Lambda(M) := p^{\sum m_i} \cdot \prod F_j$$

Pontryagin dual: $M^\vee := \text{Hom}_{\text{cts}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, compact $\leftrightarrow$ discrete

Recall: $\Gamma \simeq \mathbb{Z}_p$

Definition (Iwasawa algebra)

$\Lambda = \Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]] = \varprojlim_U \mathbb{Z}_p[\Gamma/U]$ as $U \subseteq \Gamma$ runs over open normal subgroups

By fixing a topological generator $\gamma \in \Gamma$, there is a non-canonical isomorphism

$$\Lambda(\Gamma) = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]], \gamma \mapsto 1 + T$$

Fix such a γ , and tacitly identify the two rings from now on.

Structure theorem

If M is a finitely generated $\Lambda = \Lambda(\Gamma)$ -module, then there is a homomorphism with finite kernel and cokernel:

$$M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

If M is Λ -torsion:

$$\text{char}_\Lambda(M) := p^{\sum m_i} \cdot \prod F_j$$

Pontryagin dual: $M^\vee := \text{Hom}_{\text{cts}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, compact $\leftrightarrow$ discrete

Recall: $\Gamma \simeq \mathbb{Z}_p$

Definition (Iwasawa algebra)

$\Lambda = \Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]] = \varprojlim_U \mathbb{Z}_p[\Gamma/U]$ as $U \subseteq \Gamma$ runs over open normal subgroups

By fixing a topological generator $\gamma \in \Gamma$, there is a non-canonical isomorphism

$$\Lambda(\Gamma) = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]], \gamma \mapsto 1 + T$$

Fix such a γ , and tacitly identify the two rings from now on.

Structure theorem

If M is a finitely generated $\Lambda = \Lambda(\Gamma)$ -module, then there is a homomorphism with finite kernel and cokernel:

$$M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

If M is Λ -torsion:

$$\text{char}_\Lambda(M) := p^{\sum m_i} \cdot \prod F_j$$

Pontryagin dual: $M^\vee := \text{Hom}_{\text{cts}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, compact $\leftrightarrow$ discrete

Definition (p -primary Selmer group)

For $n \geq 0$, define

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) := \ker \left(H^1(\mathbb{Q}_n, E[p^\infty]) \xrightarrow{\text{res}} \prod_v \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where v ranges over all places of $\mathbb{Q}_n$.

Here $E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}_{n,v}, E[p^\infty])$ via the Kummer map, defined on finite level as the boundary map coming from $0 \rightarrow E[p^k] \rightarrow E(\overline{\mathbb{Q}}) \xrightarrow{p^k} E(\overline{\mathbb{Q}}) \rightarrow 0$ by taking invariants

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}(E/\mathbb{Q}_n)$$

$X(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated Λ -module

Control theorem (Mazur 1972)

If E has good ordinary reduction at p , then the natural maps

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^{\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)}$$

have finite kernels and cokernels of uniformly bounded orders as $n \rightarrow \infty$.

Definition (p -primary Selmer group)

For $n \geq 0$, define

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) := \ker \left(H^1(\mathbb{Q}_n, E[p^\infty]) \xrightarrow{\text{res}} \prod_v \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where v ranges over all places of $\mathbb{Q}_n$.

Here $E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}_{n,v}, E[p^\infty])$ via the Kummer map, defined on finite level as the boundary map coming from $0 \rightarrow E[p^k] \rightarrow E(\overline{\mathbb{Q}}) \xrightarrow{p^k} E(\overline{\mathbb{Q}}) \rightarrow 0$ by taking invariants

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}(E/\mathbb{Q}_n)$$

$X(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated Λ -module

Control theorem (Mazur 1972)

If E has good ordinary reduction at p , then the natural maps

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^{\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)}$$

have finite kernels and cokernels of uniformly bounded orders as $n \rightarrow \infty$.

Definition (p -primary Selmer group)

For $n \geq 0$, define

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) := \ker \left(H^1(\mathbb{Q}_n, E[p^\infty]) \xrightarrow{\text{res}} \prod_v \frac{H^1(\mathbb{Q}_{n,v}, E[p^\infty])}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

where v ranges over all places of $\mathbb{Q}_n$.

Here $E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}_{n,v}, E[p^\infty])$ via the Kummer map, defined on finite level as the boundary map coming from $0 \rightarrow E[p^k] \rightarrow E(\overline{\mathbb{Q}}) \xrightarrow{p^k} E(\overline{\mathbb{Q}}) \rightarrow 0$ by taking invariants

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}(E/\mathbb{Q}_n)$$

$X(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated Λ -module

Control theorem (Mazur 1972)

If E has good ordinary reduction at p , then the natural maps

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^{\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)}$$

have finite kernels and cokernels of uniformly bounded orders as $n \rightarrow \infty$.

Once and for all fix algebraic closures and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$

Hasse–Weil L -function $L(E, s)$ has p -Euler factor $\frac{1}{(1 - \alpha_p p^{-1})(1 - \beta_p p^{-1})}$ with $\alpha_p \beta_p = p$, $\alpha_p + \beta_p = a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$, $p \nmid a_p$. Let α_p be the p -adic unit of the two.

Theorem (Mazur–Swinnerton-Dyer 1974)

There exists $L_p \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p) = \beta_p^n \tau(\chi) \frac{L(E, \chi, 1)}{\Omega_E} \quad \text{for } n \geq 1$$

$$\mathbb{1}(L_p) = (1 - \beta_p p^{-1})^2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi, s)$ Hasse–Weil L -function twisted by χ
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

Iwasawa main conjecture (Mazur)

ALGEBRAIC SIDE

$$\text{char}(X(E/\mathbb{Q}_\infty))\Lambda = (L_p)$$

ANALYTIC SIDE

Rubin: IMC holds if E has CM, Kato: one divisibility “ $\supseteq$ ” holds in general

Once and for all fix algebraic closures and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$

Hasse–Weil L -function $L(E, s)$ has p -Euler factor $\frac{1}{(1 - \alpha_p p^{-1})(1 - \beta_p p^{-1})}$ with $\alpha_p \beta_p = p$, $\alpha_p + \beta_p = a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$, $p \nmid a_p$. Let α_p be the p -adic unit of the two.

Theorem (Mazur–Swinnerton-Dyer 1974)

There exists $L_p \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p) = \beta_p^n \tau(\chi) \frac{L(E, \chi, 1)}{\Omega_E} \quad \text{for } n \geq 1$$

$$\mathbb{1}(L_p) = (1 - \beta_p p^{-1})^2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi, s)$ Hasse–Weil L -function twisted by χ
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

Iwasawa main conjecture (Mazur)

ALGEBRAIC SIDE

$$\text{char}(X(E/\mathbb{Q}_\infty))\Lambda = (L_p)$$

ANALYTIC SIDE

Rubin: IMC holds if E has CM, Kato: one divisibility “ $\supseteq$ ” holds in general

Once and for all fix algebraic closures and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$

Hasse–Weil L -function $L(E, s)$ has p -Euler factor $\frac{1}{(1 - \alpha_p p^{-1})(1 - \beta_p p^{-1})}$ with $\alpha_p \beta_p = p$, $\alpha_p + \beta_p = a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$, $p \nmid a_p$. Let α_p be the p -adic unit of the two.

Theorem (Mazur–Swinnerton-Dyer 1974)

There exists $L_p \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p) = \beta_p^n \tau(\chi) \frac{L(E, \chi, 1)}{\Omega_E} \quad \text{for } n \geq 1$$

$$\mathbb{1}(L_p) = (1 - \beta_p p^{-1})^2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi, s)$ Hasse–Weil L -function twisted by χ
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

Iwasawa main conjecture (Mazur)

ALGEBRAIC SIDE

$$\text{char}(X(E/\mathbb{Q}_\infty))\Lambda = (L_p)$$

ANALYTIC SIDE

Rubin: IMC holds if E has CM, Kato: one divisibility “ $\supseteq$ ” holds in general

Once and for all fix algebraic closures and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$

Hasse–Weil L -function $L(E, s)$ has p -Euler factor $\frac{1}{(1 - \alpha_p p^{-1})(1 - \beta_p p^{-1})}$ with $\alpha_p \beta_p = p$, $\alpha_p + \beta_p = a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$, $p \nmid a_p$. Let α_p be the p -adic unit of the two.

Theorem (Mazur–Swinnerton-Dyer 1974)

There exists $L_p \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p) = \beta_p^n \tau(\chi) \frac{L(E, \chi, 1)}{\Omega_E} \quad \text{for } n \geq 1$$

$$\mathbb{1}(L_p) = (1 - \beta_p p^{-1})^2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi, s)$ Hasse–Weil L -function twisted by χ
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

Iwasawa main conjecture (Mazur)

ALGEBRAIC SIDE

$$\text{char}(X(E/\mathbb{Q}_\infty))\Lambda = (L_p)$$

ANALYTIC SIDE

Rubin: IMC holds if E has CM, Kato: one divisibility “ $\supseteq$ ” holds in general

Once and for all fix algebraic closures and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$

Hasse–Weil L -function $L(E, s)$ has p -Euler factor $\frac{1}{(1 - \alpha_p p^{-1})(1 - \beta_p p^{-1})}$ with $\alpha_p \beta_p = p$, $\alpha_p + \beta_p = a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)|$, $p \nmid a_p$. Let α_p be the p -adic unit of the two.

Theorem (Mazur–Swinnerton-Dyer 1974)

There exists $L_p \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p) = \beta_p^n \tau(\chi) \frac{L(E, \chi, 1)}{\Omega_E} \quad \text{for } n \geq 1$$

$$\mathbb{1}(L_p) = (1 - \beta_p p^{-1})^2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi, s)$ Hasse–Weil L -function twisted by χ
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

Iwasawa main conjecture (Mazur)

ALGEBRAIC SIDE

$$\text{char}(X(E/\mathbb{Q}_\infty))\Lambda = (L_p)$$

ANALYTIC SIDE

Rubin: IMC holds if E has CM, Kato: one divisibility “ $\supseteq$ ” holds in general

Iwasawa main conjecture (Mazur)

If $E/\mathbb{Q}$ has good ordinary reduction at p then $\text{char}(X(E/\mathbb{Q}_\infty))\Lambda = (L_p)$.

Let $E/\mathbb{Q}$ have good **supersingular** reduction at p .

Facts: • $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is **not** $\Lambda(\Gamma)$ -cotorsion

- the Mazur–Swinnerton-Dyer p -adic L -function is **not** in $\Lambda(\Gamma) \otimes \overline{\mathbb{Q}_p}$

$E/\mathbb{Q}$ has good supersingular reduction at p

$\Phi_i(X)$ the p^i th cyclotomic polynomial, $\omega_n(X) := (1 + X)^{p^n} - 1 = \prod_{i=0}^n \Phi_i(X)$

$\omega_n^\pm(X) := X \prod_{\substack{1 \leq i \leq n \\ (-1)^i = \pm 1}} \Phi_i$, so $X \cdot \omega_n(X) = \omega_n^+(X) \cdot \omega_n^-(X)$

Theorem (Pollack 2003)

There exist $L_p^\pm \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p^+) = (-1)^{\frac{n+1}{2}} \frac{\tau(\chi)}{\chi(\omega_n^+)} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{for } n \text{ odd}$$

$$\chi(L_p^-) = (-1)^{\frac{n}{2}+1} \frac{\tau(\chi)}{\chi(\omega_n^-)} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{for } n \geq 2 \text{ even}$$

$$\mathbb{1}(L_p^+) = (p-1) \frac{L(E, 1)}{\Omega_E} \text{ and } \mathbb{1}(L_p^-) = 2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi^{-1}, s)$ Hasse–Weil L -function twisted by χ^{-1}
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

$E/\mathbb{Q}$ has good supersingular reduction at p

$\Phi_i(X)$ the p^i th cyclotomic polynomial, $\omega_n(X) := (1 + X)^{p^n} - 1 = \prod_{i=0}^n \Phi_i(X)$

$\omega_n^\pm(X) := X \prod_{\substack{1 \leq i \leq n \\ (-1)^i = \pm 1}} \Phi_i$, so $X \cdot \omega_n(X) = \omega_n^+(X) \cdot \omega_n^-(X)$

Theorem (Pollack 2003)

There exist $L_p^\pm \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p^+) = (-1)^{\frac{n+1}{2}} \frac{\tau(\chi)}{\chi(\omega_n^+)} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{for } n \text{ odd}$$

$$\chi(L_p^-) = (-1)^{\frac{n}{2}+1} \frac{\tau(\chi)}{\chi(\omega_n^-)} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{for } n \geq 2 \text{ even}$$

$$\mathbb{1}(L_p^+) = (p-1) \frac{L(E, 1)}{\Omega_E} \text{ and } \mathbb{1}(L_p^-) = 2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi^{-1}, s)$ Hasse–Weil L -function twisted by χ^{-1}
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

$E/\mathbb{Q}$ has good supersingular reduction at p

$\Phi_i(X)$ the p^i th cyclotomic polynomial, $\omega_n(X) := (1 + X)^{p^n} - 1 = \prod_{i=0}^n \Phi_i(X)$

$\omega_n^\pm(X) := X \prod_{\substack{1 \leq i \leq n \\ (-1)^i = \pm 1}} \Phi_i$, so $X \cdot \omega_n(X) = \omega_n^+(X) \cdot \omega_n^-(X)$

Theorem (Pollack 2003)

There exist $L_p^\pm \in \Lambda$ such that for any $\chi : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \rightarrow \mu_{p^n}$ of order p^n :

$$\chi(L_p^+) = (-1)^{\frac{n+1}{2}} \frac{\tau(\chi)}{\chi(\omega_n^+)} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{for } n \text{ odd}$$

$$\chi(L_p^-) = (-1)^{\frac{n}{2}+1} \frac{\tau(\chi)}{\chi(\omega_n^-)} \frac{L(E, \chi^{-1}, 1)}{\Omega_E} \quad \text{for } n \geq 2 \text{ even}$$

$$\mathbb{1}(L_p^+) = (p-1) \frac{L(E, 1)}{\Omega_E} \text{ and } \mathbb{1}(L_p^-) = 2 \frac{L(E, 1)}{\Omega_E} \quad \text{for } \chi = \mathbb{1} \text{ trivial}$$

- $L(E, \chi^{-1}, s)$ Hasse–Weil L -function twisted by χ^{-1}
- $\tau(\chi) = \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})} \chi(\sigma) \zeta_{p^n}^\sigma$ Gauß sum
- $\Omega_E \in \mathbb{R}$ real period of a minimal model of E

$E/\mathbb{Q}$ has good supersingular reduction at p

$$E^+(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ even}\}$$

$$E^-(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ odd}\}$$

Definition

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n) := \ker \left(\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n)$$

Theorem (Kobayashi 2003)

$X^\pm(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated *torsion* Λ -module.

Iwasawa Main Conjecture

$$\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda = (L_p^\pm)$$

Kobayashi: proved one divisibility " $\supseteq$ ". Pollack–Rubin 2004: equality for CM

$E/\mathbb{Q}$ has good supersingular reduction at p

$$E^+(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ even}\}$$

$$E^-(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ odd}\}$$

Definition

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n) := \ker \left(\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n)$$

Theorem (Kobayashi 2003)

$X^\pm(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated *torsion* Λ -module.

Iwasawa Main Conjecture

$$\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda = (L_p^\pm)$$

Kobayashi: proved one divisibility " $\supseteq$ ". Pollack–Rubin 2004: equality for CM

$E/\mathbb{Q}$ has good supersingular reduction at p

$$E^+(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ even}\}$$

$$E^-(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ odd}\}$$

Definition

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n) := \ker \left(\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n)$$

Theorem (Kobayashi 2003)

$X^\pm(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated **torsion** Λ -module.

Iwasawa Main Conjecture

$$\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda = (L_p^\pm)$$

Kobayashi: proved one divisibility " $\supseteq$ ". Pollack–Rubin 2004: equality for CM

$E/\mathbb{Q}$ has good supersingular reduction at p

$$E^+(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ even}\}$$

$$E^-(\mathbb{Q}_{n,p}) := \{P \in E(\mathbb{Q}_{n,p}) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_{m,p}) \text{ for all } 0 \leq m < n \text{ odd}\}$$

Definition

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n) := \ker \left(\text{Sel}_{p^\infty}(E/\mathbb{Q}_n) \longrightarrow \frac{H^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

$$\text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty) := \varinjlim_n \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n)$$

Theorem (Kobayashi 2003)

$X^\pm(E/\mathbb{Q}_\infty) := \text{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated **torsion** Λ -module.

Iwasawa Main Conjecture

$$\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda = (L_p^\pm)$$

Kobayashi: proved one divisibility “ $\supseteq$ ”. Pollack–Rubin 2004: equality for CM

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

*For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.*

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

*For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.*

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

*For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.*

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good reduction at p

Semistability defect: $e := \begin{cases} 1 & \text{if } E \text{ has good reduction at } p \\ \frac{12}{\gcd(12, \text{ord}_p(\Delta_E))} & \text{if } E \text{ has bad reduction at } p \end{cases}$

Fact (Serre–Tate 1968): e is the minimal degree such that E attains good reduction over a degree e extension of $\mathbb{Q}_p^{\text{nr}}$ (= maximal unramified extension of $\mathbb{Q}_p$)

In particular: $e \mid 12$, and in fact, $e \in \{1, 2, 3, 4, 6\}$ for $p \geq 5$ (assumed throughout)

Lemma (Delbourgo/Volkov 2002)

*For $e > 2$: E has potentially ordinary reduction at $p \Leftrightarrow e \mid p - 1$,
 E has potentially supersingular reduction at $p \Leftrightarrow e \mid p + 1$.*

Delbourgo: construction of p -adic L -functions for **potentially ordinary** elliptic curves, and $\text{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is Λ -cotorsion in this case

Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension

Idea: twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Delbourgo's strategy for potentially ordinary elliptic curves:

- Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension
- Twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good supersingular reduction at p ($\Rightarrow e \mid p+1$)

For simplicity, assume $e > 2$ ($e = 2$ slightly more cumbersome)

Good supersingular reduction is attained over $\mathbb{Q}_p(\pi)$ where $\pi = \sqrt[e]{-p}$ fixed
 $\mathbb{Q}_p(\mu_e, \pi) = \mathbb{Q}_{p^2}(\pi)$ Galois closure, **dihedral** and tamely ramified over $\mathbb{Q}$,
where $\mathbb{Q}_{p^2}$ = unique quadratic unramified extension of $\mathbb{Q}_p$

$\rightsquigarrow$ Delbourgo's twisting method does **not** work

Instead: use **formal groups** à la Kobayashi

Delbourgo's strategy for potentially ordinary elliptic curves:

- Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension
- Twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good supersingular reduction at p ($\Rightarrow e \mid p+1$)

For simplicity, assume $e > 2$ ($e = 2$ slightly more cumbersome)

Good supersingular reduction is attained over $\mathbb{Q}_p(\pi)$ where $\pi = \sqrt[e]{-p}$ fixed

$\mathbb{Q}_p(\mu_e, \pi) = \mathbb{Q}_{p^2}(\pi)$ Galois closure, **dihedral** and tamely ramified over $\mathbb{Q}$,
where $\mathbb{Q}_{p^2}$ = unique quadratic unramified extension of $\mathbb{Q}_p$

$\rightsquigarrow$ Delbourgo's twisting method does **not** work

Instead: use **formal groups** à la Kobayashi

Delbourgo's strategy for potentially ordinary elliptic curves:

- Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension
- Twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good supersingular reduction at p ($\Rightarrow e \mid p+1$)

For simplicity, assume $e > 2$ ($e = 2$ slightly more cumbersome)

Good supersingular reduction is attained over $\mathbb{Q}_p(\pi)$ where $\pi = \sqrt[e]{-p}$ fixed

$\mathbb{Q}_p(\mu_e, \pi) = \mathbb{Q}_{p^2}(\pi)$ Galois closure, **dihedral** and tamely ramified over $\mathbb{Q}$, where $\mathbb{Q}_{p^2}$ = unique quadratic unramified extension of $\mathbb{Q}_p$

$\rightsquigarrow$ Delbourgo's twisting method does **not** work

Instead: use **formal groups** à la Kobayashi

Delbourgo's strategy for potentially ordinary elliptic curves:

- Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension
- Twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good supersingular reduction at p ($\Rightarrow e \mid p+1$)

For simplicity, assume $e > 2$ ($e = 2$ slightly more cumbersome)

Good supersingular reduction is attained over $\mathbb{Q}_p(\pi)$ where $\pi = \sqrt[e]{-p}$ fixed

$\mathbb{Q}_p(\mu_e, \pi) = \mathbb{Q}_{p^2}(\pi)$ Galois closure, **dihedral** and tamely ramified over $\mathbb{Q}$, where $\mathbb{Q}_{p^2}$ = unique quadratic unramified extension of $\mathbb{Q}_p$

$\rightsquigarrow$ Delbourgo's twisting method does **not** work

Instead: use **formal groups** à la Kobayashi

Delbourgo's strategy for potentially ordinary elliptic curves:

- Good ordinary reduction is achieved over an abelian extension $\mathcal{K}/\mathbb{Q}_p \rightsquigarrow$ work over maximal cyclotomic extension
- Twist the representation by a finite order character of $\text{Gal}(\mathcal{K}/\mathbb{Q}_p)$ to get rid of bad reduction

Assume: $E/\mathbb{Q}$ has potentially good supersingular reduction at p ($\Rightarrow e \mid p+1$)

For simplicity, assume $e > 2$ ($e = 2$ slightly more cumbersome)

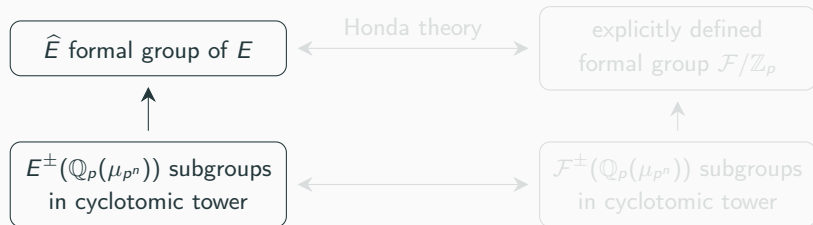
Good supersingular reduction is attained over $\mathbb{Q}_p(\pi)$ where $\pi = \sqrt[e]{-p}$ fixed

$\mathbb{Q}_p(\mu_e, \pi) = \mathbb{Q}_{p^2}(\pi)$ Galois closure, **dihedral** and tamely ramified over $\mathbb{Q}$, where $\mathbb{Q}_{p^2}$ = unique quadratic unramified extension of $\mathbb{Q}_p$

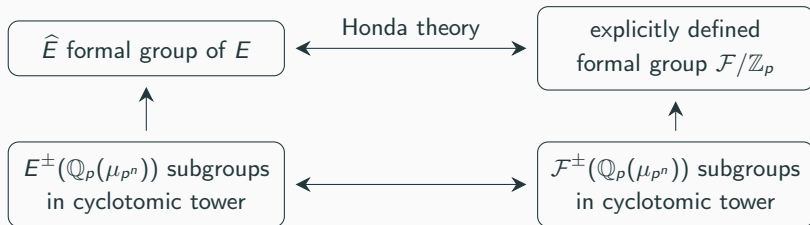
$\rightsquigarrow$ Delbourgo's twisting method does **not** work

Instead: use **formal groups** à la Kobayashi

$$E^{\pm}(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$

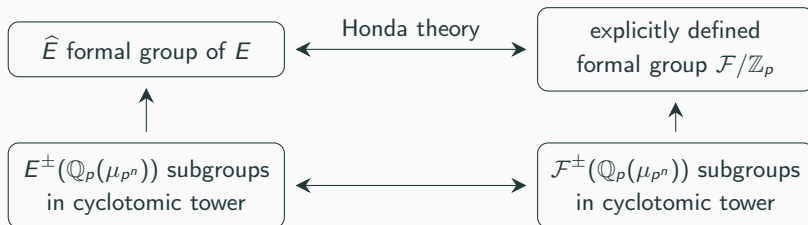


$$E^{\pm}(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$



Let $\ell(X) \in \mathbb{Z}_p[[X]]$ such that $\ell'(0) = 1$. If $u(X) = \sum_{i=0}^{\infty} u_i X^i \in \mathbb{Q}_p[[X]]$ such that $(u * \ell)(X) = \sum_{i=0}^{\infty} u_i \ell(X^{p^i}) \equiv 0 \pmod{p\mathbb{Z}_p[[X]]}$ then ℓ has **Honda type** u .

$$E^\pm(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$

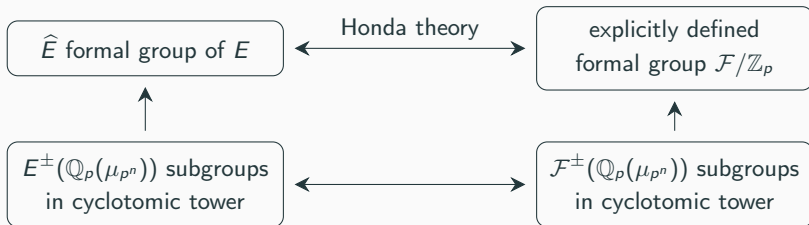


Let $\ell(X) \in \mathbb{Z}_p[[X]]$ such that $\ell'(0) = 1$. If $u(X) = \sum_{i=0}^{\infty} u_i X^i \in \mathbb{Q}_p[[X]]$ such that $(u * \ell)(X) = \sum_{i=0}^{\infty} u_i \ell(X^{p^i}) \equiv 0 \pmod{p\mathbb{Z}_p[[X]]}$ then ℓ has **Honda type** u .

Theorem (Honda 1968)

1. For every 1-dimensional formal group $\mathcal{G}$ over $\mathbb{Z}_p$, there exists a unique (Eisenstein) polynomial u such that the logarithm g of $\mathcal{G}$ has Honda type u .
2. If $\mathcal{G}$ and $\mathcal{G}'$ are formal groups over $\mathbb{Z}_p$ of the same Honda type $\Rightarrow$ isomorphic over $\mathbb{Z}_p$.

$$E^\pm(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$



Let $\ell(X) \in \mathbb{Z}_p[[X]]$ such that $\ell'(0) = 1$. If $u(X) = \sum_{i=0}^{\infty} u_i X^i \in \mathbb{Q}_p[[X]]$ such that $(u * \ell)(X) = \sum_{i=0}^{\infty} u_i \ell(X^{p^i}) \equiv 0 \pmod{p\mathbb{Z}_p[[X]]}$ then ℓ has **Honda type** u .

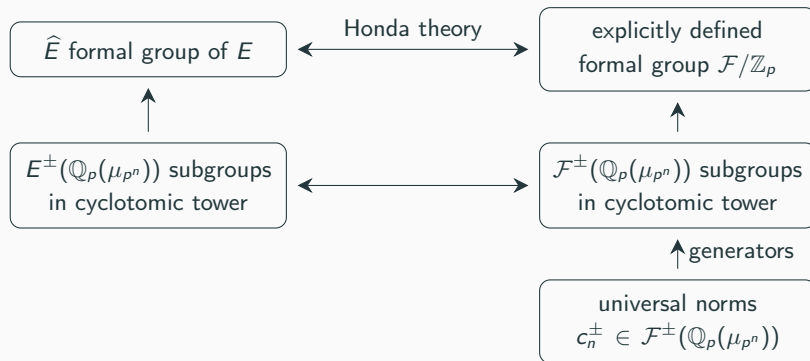
Theorem (Honda 1968)

1. For every 1-dimensional formal group $\mathcal{G}$ over $\mathbb{Z}_p$, there exists a unique (Eisenstein) polynomial u such that the logarithm g of $\mathcal{G}$ has Honda type u .
2. If $\mathcal{G}$ and $\mathcal{G}'$ are formal groups over $\mathbb{Z}_p$ of the same Honda type $\Rightarrow$ isomorphic over $\mathbb{Z}_p$.

$\hat{E}$ has Honda type $X^2 - a_p X + p = X^2 + p$,

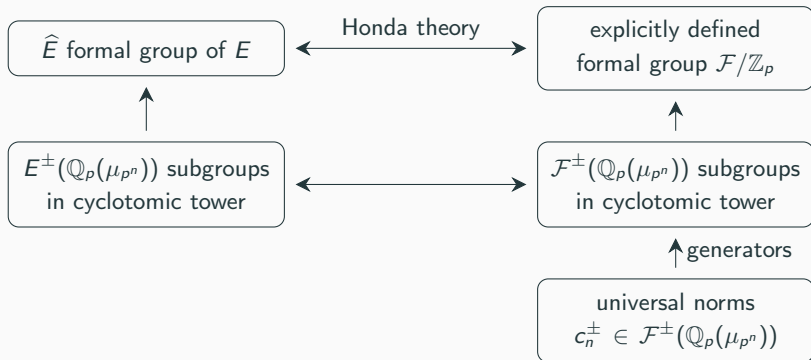
$\mathcal{F}$ has logarithm $\sum_{i=0}^{\infty} (-1)^i \frac{\omega_{2i}(X)}{p^i} = \sum_{i=0}^{\infty} (-1)^i \frac{(1+X)^{p^{2i}} - 1}{p^i}$

$$E^{\pm}(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$



- Universal norms:
- Trace compatibility: $\mathrm{Tr}_{n/n-1}^{\mathcal{F}} c_n^{\pm} = c_{n-2}^{\pm}$ for $(-1)^n = \pm 1$
 - $c_n^{\pm}$ generates $\mathcal{F}^{\pm}(\mathbb{Q}_p(\mu_{p^n}))$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)]$ -module

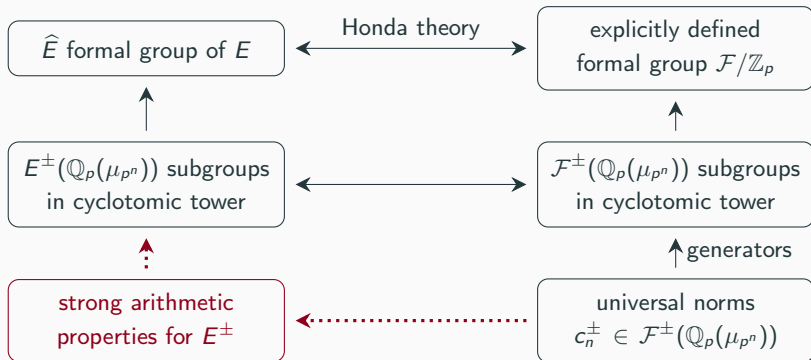
$$E^\pm(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \mathrm{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$



- Universal norms:
- Trace compatibility: $\mathrm{Tr}_{n/n-1}^{\mathcal{F}} c_n^\pm = c_{n-2}^\pm$ for $(-1)^n = \pm 1$
 - $c_n^\pm$ generates $\mathcal{F}^\pm(\mathbb{Q}_p(\mu_{p^n}))$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)]$ -module

Explicit construction: $\mathcal{F}$ has logarithm $\sum_{i=0}^{\infty} (-1)^i \frac{\omega_{2i}(X)}{p^i} = \sum_{i=0}^{\infty} (-1)^i \frac{(1+X)^{p^{2i}} - 1}{p^i}$,
 $(\zeta_{p^{n+1}} - 1)_n$ is an ω_1 -compatible system: $\omega_1(\zeta_{p^{n+1}} - 1) = \zeta_{p^n} - 1$ and $\omega_{2i} = \underbrace{\omega_1 \circ \dots \circ \omega_1}_{2i \text{ times}}$
 $\rightsquigarrow c_n^\pm := \varepsilon[+]_{\mathcal{F}}(\zeta_{p^{n+1}} - 1)$ for ε appropriately chosen

$$E^\pm(\mathbb{Q}_p(\mu_{p^n})) = \{P \in E(\mathbb{Q}_p(\mu_{p^n})) : \text{Tr}_{n/m+1} P \in E(\mathbb{Q}_p(\mu_{p^m})) \text{ for all } 0 \leq m < n \text{ even/odd}\}$$



- Universal norms:
- Trace compatibility: $\text{Tr}_{n/n-1}^{\mathcal{F}} c_n^\pm = c_{n-2}^\pm$ for $(-1)^n = \pm 1$
 - $c_n^\pm$ generates $\mathcal{F}^\pm(\mathbb{Q}_p(\mu_{p^n}))$ as a $\mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)]$ -module

Explicit construction: $\mathcal{F}$ has logarithm $\sum_{i=0}^{\infty} (-1)^i \frac{\omega_{2i}(X)}{p^i} = \sum_{i=0}^{\infty} (-1)^i \frac{(1+X)^{p^{2i}} - 1}{p^i}$,
 $(\zeta_{p^{n+1}} - 1)_n$ is an ω_1 -compatible system: $\omega_1(\zeta_{p^{n+1}} - 1) = \zeta_{p^n} - 1$ and $\omega_{2i} = \underbrace{\omega_1 \circ \dots \circ \omega_1}_{2i \text{ times}}$
 $\rightsquigarrow c_n^\pm := \varepsilon[+]_{\mathcal{F}}(\zeta_{p^{n+1}} - 1)$ for ε appropriately chosen

Lemma

There is an exact sequence $0 \rightarrow \hat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \hat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)$: annihilator of $E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the local Tate pairing
 $H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$

$$\begin{array}{ccc} H^1(\mathbb{Q}_p(\mu_{p^n}), T) & \xrightarrow{\exists! \text{ Col}_n^\pm} & \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm) \\ \downarrow & & \downarrow \omega_n^\pm/X \\ \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} & \xrightarrow{P_n^\pm} & \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)] \end{array}$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

Lemma

There is an exact sequence $0 \rightarrow \hat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \hat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T) : \text{annihilator of } E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p \text{ under the local Tate pairing}$$

$$H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

$$H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\exists! \text{ Col}_n^\pm} \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm)$$

$$\downarrow \qquad \qquad \qquad \downarrow \omega_n^\pm/X$$

$$\frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} \xrightarrow{P_n^\pm} \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)]$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

Lemma

There is an exact sequence $0 \rightarrow \hat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \hat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)$: annihilator of $E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the local Tate pairing
 $H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$

$$\begin{array}{ccc} H^1(\mathbb{Q}_p(\mu_{p^n}), T) & \xrightarrow{\exists! \text{ Col}_n^\pm} & \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm) \\ \downarrow & & \downarrow \omega_n^\pm/X \\ \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} & \xrightarrow{P_n^\pm} & \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)] \end{array}$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

Lemma

There is an exact sequence $0 \rightarrow \hat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \hat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)$: annihilator of $E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the local Tate pairing
 $H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$

$$\begin{array}{ccc} H^1(\mathbb{Q}_p(\mu_{p^n}), T) & \xrightarrow{\exists! \text{ Col}_n^\pm} & \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm) \\ \downarrow & & \downarrow \omega_n^\pm/X \\ \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} & \xrightarrow{P_n^\pm} & \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)] \end{array}$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

Lemma

There is an exact sequence $0 \rightarrow \widehat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \widehat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)$: annihilator of $E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the local Tate pairing
 $H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$

$$\begin{array}{ccc} H^1(\mathbb{Q}_p(\mu_{p^n}), T) & \xrightarrow{\exists! \text{ Col}_n^\pm} & \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm) \\ \downarrow & & \downarrow \omega_n^\pm/X \\ \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} & \xrightarrow{P_n^\pm} & \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)] \end{array}$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

Lemma

There is an exact sequence $0 \rightarrow \widehat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \widehat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)$: annihilator of $E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under the local Tate pairing
 $H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$

$$\begin{array}{ccc} H^1(\mathbb{Q}_p(\mu_{p^n}), T) & \xrightarrow{\exists! \text{ Col}_n^\pm} & \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm) \\ \downarrow & & \downarrow \omega_n^\pm/X \\ \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} & \xrightarrow{P_n^\pm} & \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)] \end{array}$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

Lemma

There is an exact sequence $0 \rightarrow \widehat{E}(\mathbb{Q}_p) \rightarrow E^+(\mathbb{Q}_{p,\infty}) \oplus E^-(\mathbb{Q}_{p,\infty}) \rightarrow \widehat{E}(\mathbb{Q}_{p,\infty}) \rightarrow 0$.

$T := T_p(E)$ Tate module

$$(\cdot, \cdot)_n : E^\pm(\mathbb{Q}_p(\mu_{p^n})) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\text{Kummer} \times \text{id}} H^1(\mathbb{Q}_p(\mu_{p^n}), T) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \xrightarrow{\cup} \mathbb{Z}_p$$

$$P_n^\pm : H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})], z \mapsto \sum_{\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q})} (c_n^{\pm, \sigma}, z)_n \cdot \sigma$$

$H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T) : \text{annihilator of } E^\pm(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p \text{ under the local Tate pairing}$

$$H^1(\mathbb{Q}_p(\mu_{p^n}), E[p^\infty]) \times H^1(\mathbb{Q}_p(\mu_{p^n}), T) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

$$\begin{array}{ccc} H^1(\mathbb{Q}_p(\mu_{p^n}), T) & \xrightarrow{\exists! \text{ Col}_n^\pm} & \mathbb{Z}_p[\Delta][X]/(\omega_n^\pm) \\ \downarrow & & \downarrow \omega_n^\pm/X \\ \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), T)}{H_\pm^1(\mathbb{Q}_p(\mu_{p^n}), T)} & \xrightarrow{P_n^\pm} & \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)] \end{array}$$

$$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_p(\mu_{p^\infty}), T) := \varprojlim_n H^1(\mathbb{Q}_p(\mu_{p^n}), T) \longrightarrow \Lambda$$

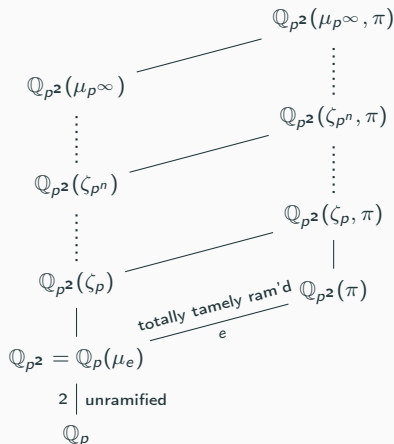
The image of Kato's zeta element under $\text{Col}^\pm$ is Pollack's $L_p^\pm$

$\Rightarrow$ one divisibility in the supersingular main conjecture

What goes wrong for **potentially** supersingular reduction?

1. Honda theory works over unramified extensions of $\mathbb{Q}_p$, but $\mathbb{Q}_{p^2}(\pi)/\mathbb{Q}_p$ is tamely ramified
2. The uniformisers $\zeta_{p^n} - 1$ live in the cyclotomic tower over $\mathbb{Q}_p$.
We need an ω_1 -compatible system of uniformisers in the cyclotomic tower over $\mathbb{Q}_{p^2}(\pi)$

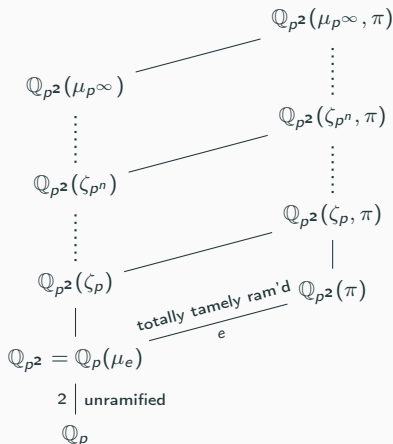
Unramified extensions of $\mathbb{Q}_p$ were handled by B.D. Kim (2007)



What goes wrong for **potentially** supersingular reduction?

1. Honda theory works over unramified extensions of $\mathbb{Q}_p$, but $\mathbb{Q}_{p^2}(\pi)/\mathbb{Q}_p$ is tamely ramified
2. The uniformisers $\zeta_{p^n} - 1$ live in the cyclotomic tower over $\mathbb{Q}_p$.
We need an ω_1 -compatible system of uniformisers in the cyclotomic tower over $\mathbb{Q}_{p^2}(\pi)$

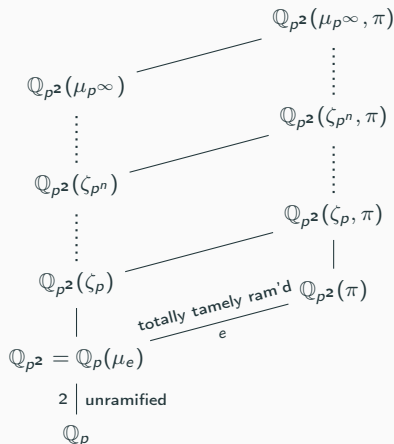
Unramified extensions of $\mathbb{Q}_p$ were handled by B.D. Kim (2007)



What goes wrong for **potentially** supersingular reduction?

1. Honda theory works over unramified extensions of $\mathbb{Q}_p$, but $\mathbb{Q}_{p^2}(\pi)/\mathbb{Q}_p$ is tamely ramified
2. The uniformisers $\zeta_{p^n} - 1$ live in the cyclotomic tower over $\mathbb{Q}_p$.
We need an ω_1 -compatible system of uniformisers in the cyclotomic tower over $\mathbb{Q}_{p^2}(\pi)$

Unramified extensions of $\mathbb{Q}_p$ were handled by B.D. Kim (2007)

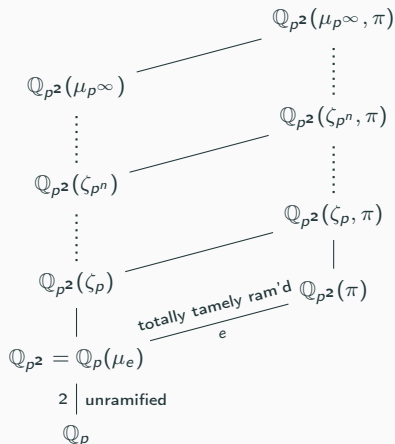


Theorem (Demchenko 2002)

The main results of Honda theory remain valid over finite extensions $\mathcal{K}$ of $\mathbb{Q}_p$ with absolute ramification index $< p$.

Idea: fixing a uniformiser of $\mathcal{O}_{\mathcal{K}}$ gives a power integral basis of $\mathcal{O}_{\mathcal{K}} = \bigoplus_{i=0}^{e-1} \mathcal{O}_{\mathcal{K}'} \pi^i$ over the maximal unramified subextension $\mathcal{K}'$
 $\rightsquigarrow$ generalisation of Honda type: tuple of polynomials, one for each component

Since $e \mid p+1$, we have $e < p$ except for $e=6, p=5$

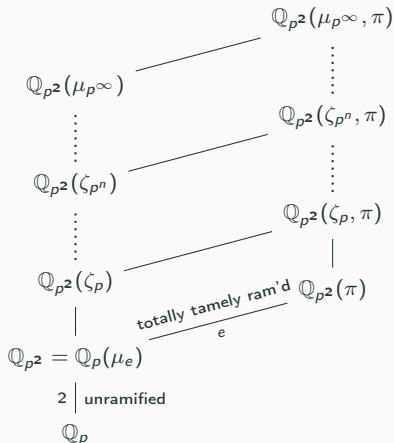


Theorem (Demchenko 2002)

The main results of Honda theory remain valid over finite extensions $\mathcal{K}$ of $\mathbb{Q}_p$ with absolute ramification index $< p$.

Idea: fixing a uniformiser of $\mathcal{O}_{\mathcal{K}}$ gives a power integral basis of $\mathcal{O}_{\mathcal{K}} = \bigoplus_{i=0}^{e-1} \mathcal{O}_{\mathcal{K}'} \pi^i$ over the maximal unramified subextension $\mathcal{K}'$
 $\rightsquigarrow$ generalisation of Honda type: tuple of polynomials, one for each component

Since $e \mid p+1$, we have $e < p$ except for $e = 6, p = 5$

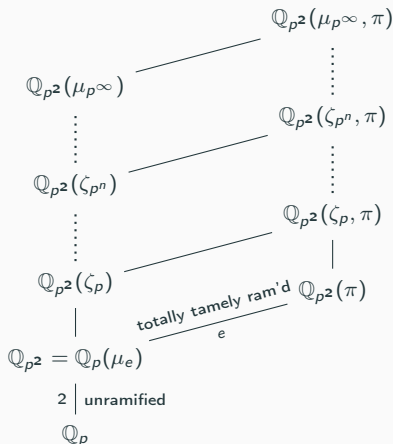


Theorem (Demchenko 2002)

The main results of Honda theory remain valid over finite extensions $\mathcal{K}$ of $\mathbb{Q}_p$ with absolute ramification index $< p$.

Idea: fixing a uniformiser of $\mathcal{O}_{\mathcal{K}}$ gives a power integral basis of $\mathcal{O}_{\mathcal{K}} = \bigoplus_{i=0}^{e-1} \mathcal{O}_{\mathcal{K}'} \pi^i$ over the maximal unramified subextension $\mathcal{K}'$
 $\rightsquigarrow$ generalisation of Honda type: tuple of polynomials, one for each component

Since $e \mid p+1$, we have $e < p$ except for $e = 6, p = 5$



Recall: $\pi = \sqrt[e]{-p}$

$$[\mathbb{Q}_{p^2}(\zeta_{p^n}, \pi) : \mathbb{Q}_{p^2}(\zeta_{p^n})] = e',$$

$$e' \in \{e, e/2\}$$

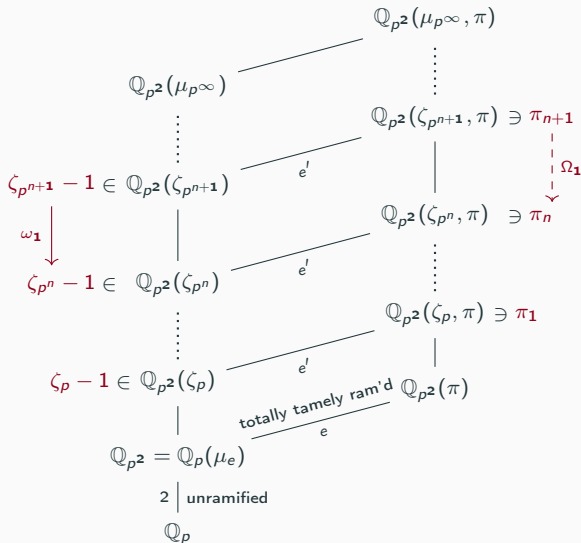
For $n \geq 1$, there exist

$\pi_n \in \mathbb{Q}_{p^2}(\zeta_{p^n}, \pi)$ such that:

- π_n is a uniformiser
- $\pi_n^{e/2} = 1 - \zeta_{p^n}$ for e even
- $\pi_n^{e'} = 1 - \zeta_{p^n}$
- $\Omega_1(\pi_{n+1}) = \pi_n$

where $\Omega_1(X) = \sqrt[e']{\omega_1(-X^{e'})}$
formal power series lifting ω_1

Define explicit formal group
with Ω_1 playing rôle of ω_1



$E/\mathbb{Q}$ potentially supersingular at $p \geq 5$, good over $\mathcal{L} := \mathbb{Q}_{p^2}(\pi)$

Summary: we have the Kobayashi-style results in the potentially supersingular setting

$\mathcal{L}_\infty$: cyclotomic $\mathbb{Z}_p$ -extension of $\mathcal{L}$

For all $n \geq 0$, $E^\pm(\mathcal{L}_n)$ is generated by Galois conjugates of $c_n^\pm$ up to $\mathbb{Q}_p/\mathbb{Z}_p$:

$$E^\pm(\mathcal{L}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathbb{Z}_{p^2}[\text{Gal}(\mathcal{L}_n/\mathbb{Q}_{p^2})](c_n^\pm) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

$\text{Col}^\pm : H_{\text{Iw}}^1(\mathbb{Q}_{p^2, \infty}, \mathbb{Z}_{p^2}(\chi_{\widehat{E}}^{-1} \chi_{\text{cyc}})) \longrightarrow \mathbb{Z}_{p^2}[[\Gamma]] =: \Lambda^{\mathbb{Z}_{p^2}}$ surjective Coleman maps,
 where $\chi_{\widehat{E}} : G_{\mathbb{Q}_{p^2}} \rightarrow \mathbb{Z}_{p^2}^\times$ Lubin–Tate character, χ_{cyc} cyclotomic character

$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_\infty = K\mathbb{Q}_\infty$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty,p}, E[p^\infty]) := E^\pm(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty,p}, E[p^\infty])$$

$$\text{Sel}_{p^\infty}^\pm(E/K_\infty) := \ker \left(\text{Sel}_{p^\infty}(E/K_\infty) \longrightarrow \frac{H^1(K_\infty, E[p^\infty])}{H_{\pm}^1(K_\infty, E[p^\infty])} \right)$$

$$X^\pm(E/K_\infty) := \text{Sel}_{p^\infty}^\pm(E/K_\infty)^\vee$$

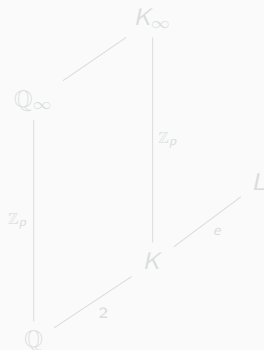
$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_\infty = K\mathbb{Q}_\infty$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty,p}, E[p^\infty]) := E^\pm(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty,p}, E[p^\infty])$$

$$\text{Sel}_{p^\infty}^\pm(E/K_\infty) := \ker \left(\text{Sel}_{p^\infty}(E/K_\infty) \longrightarrow \frac{H^1(K_\infty, E[p^\infty])}{H_{\pm}^1(K_\infty, E[p^\infty])} \right)$$

$$X^\pm(E/K_\infty) := \text{Sel}_{p^\infty}^\pm(E/K_\infty)^\vee$$

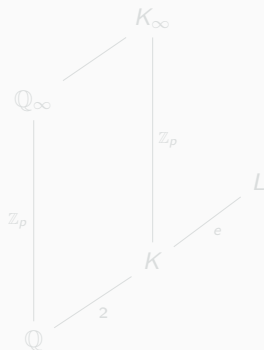
$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_\infty = K\mathbb{Q}_\infty$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty,p}, E[p^\infty]) := E^\pm(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty,p}, E[p^\infty])$$

$$\text{Sel}_{p^\infty}^\pm(E/K_\infty) := \ker \left(\text{Sel}_{p^\infty}(E/K_\infty) \longrightarrow \frac{H^1(K_\infty, E[p^\infty])}{H_{\pm}^1(K_\infty, E[p^\infty])} \right)$$

$$X^\pm(E/K_\infty) := \text{Sel}_{p^\infty}^\pm(E/K_\infty)^\vee$$

$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_\infty = K\mathbb{Q}_\infty$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty, p}, E[p^\infty]) := E^\pm(K_{\infty, p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty, p}, E[p^\infty])$$

$$\text{Sel}_{p^\infty}^\pm(E/K_\infty) := \ker \left(\text{Sel}_{p^\infty}(E/K_\infty) \rightarrow \frac{H^1(K_\infty, E[p^\infty])}{H_{\pm}^1(K_\infty, E[p^\infty])} \right)$$

$$X^\pm(E/K_\infty) := \text{Sel}_{p^\infty}^\pm(E/K_\infty)^\vee$$

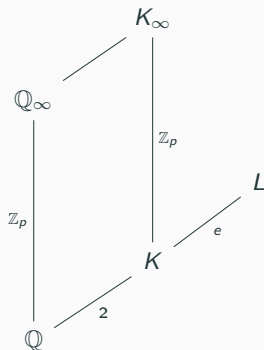
$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_{\infty} = K\mathbb{Q}_{\infty}$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty, p}, E[p^{\infty}]) := E^{\pm}(K_{\infty, p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty, p}, E[p^{\infty}])$$

$$\text{Sel}_{p^{\infty}}^{\pm}(E/K_{\infty}) := \ker \left(\text{Sel}_{p^{\infty}}(E/K_{\infty}) \longrightarrow \frac{H^1(K_{\infty}, E[p^{\infty}])}{H_{\pm}^1(K_{\infty}, E[p^{\infty}])} \right)$$

$$X^{\pm}(E/K_{\infty}) := \text{Sel}_{p^{\infty}}^{\pm}(E/K_{\infty})^{\vee}$$

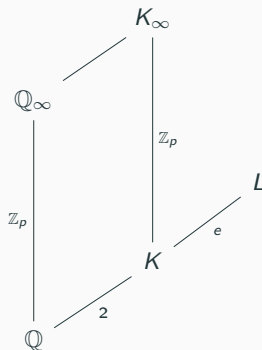
$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_{\infty} = K\mathbb{Q}_{\infty}$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty,p}, E[p^{\infty}]) := E^{\pm}(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty,p}, E[p^{\infty}])$$

$$\text{Sel}_{p^{\infty}}^{\pm}(E/K_{\infty}) := \ker \left(\text{Sel}_{p^{\infty}}(E/K_{\infty}) \longrightarrow \frac{H^1(K_{\infty}, E[p^{\infty}])}{H_{\pm}^1(K_{\infty}, E[p^{\infty}])} \right)$$

$$X^{\pm}(E/K_{\infty}) := \text{Sel}_{p^{\infty}}^{\pm}(E/K_{\infty})^{\vee}$$

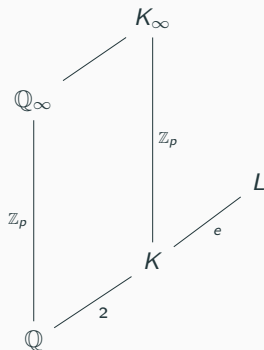
$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_\infty = K\mathbb{Q}_\infty$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty,p}, E[p^\infty]) := E^\pm(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty,p}, E[p^\infty])$$

$$\text{Sel}_{p^\infty}^\pm(E/K_\infty) := \ker \left(\text{Sel}_{p^\infty}(E/K_\infty) \longrightarrow \frac{H^1(K_\infty, E[p^\infty])}{H_{\pm}^1(K_\infty, E[p^\infty])} \right)$$

$$X^\pm(E/K_\infty) := \text{Sel}_{p^\infty}^\pm(E/K_\infty)^\vee$$

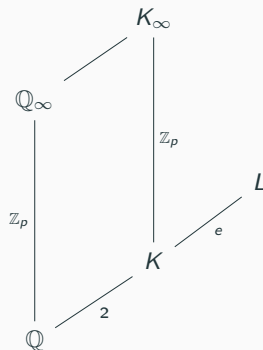
$E/\mathbb{Q}$ elliptic curve, $p \geq 7$ potentially good supersingular,
 e semistability defect, good reduction over $L = \mathbb{Q}(\mu_e, \pi)$,
 $\pi = \sqrt[e]{-p}$

K imaginary quadratic field contained in $\mathbb{Q}(\mu_e, \pi)$, so
 $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})\}$
 (assumed for simplicity, could be relaxed...)

Suppose E has **complex multiplication** by an order in $\mathcal{O}_K$,
 and p is inert in K

Then: $L(E_{\text{tor}})/K$ is abelian

$K_\infty = K\mathbb{Q}_\infty$ cyclotomic $\mathbb{Z}_p$ -extension of K



Definition

$$H_{\pm}^1(K_{\infty,p}, E[p^\infty]) := E^\pm(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_{\infty,p}, E[p^\infty])$$

$$\text{Sel}_{p^\infty}^\pm(E/K_\infty) := \ker \left(\text{Sel}_{p^\infty}(E/K_\infty) \longrightarrow \frac{H^1(K_\infty, E[p^\infty])}{H_{\pm}^1(K_\infty, E[p^\infty])} \right)$$

$$X^\pm(E/K_\infty) := \text{Sel}_{p^\infty}^\pm(E/K_\infty)^\vee$$

$\mathcal{C} := \varprojlim_F C_F \subset \mathcal{U} := \varprojlim_F U_F$, with $K \subseteq F \subset K(E[p^\infty])$, C_F : closure of elliptic units,
 U_F : pro- p part of $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$, $\Phi : G_K \rightarrow \mathcal{O}_{K_p}^\times$ character of action on $T_p(E)$

$$\mathcal{C}_{K_\infty}^\Phi := \mathcal{C} \otimes_{\mathcal{O}_K} \mathrm{Hom}(E[p^\infty], K_p/\mathcal{O}_{K_p}) \otimes_{\Lambda(\mathrm{Gal}(K(E[p^\infty])/K))} \Lambda(\mathrm{Gal}(K_\infty/K))$$

Theorem (Wiles, Coates–Wiles, Rubin)

$\mathcal{C}_{K_\infty}^\Phi$ is a free $\Lambda^{\mathrm{O}_K}(K_\infty)$ -module of rank one. It has a **generator** ξ such that for all $K \subset F \subset K_\infty$, $x \in E(F_p)$ and $\chi : \mathrm{Gal}(F/K) \rightarrow \mu_{p^\infty}$ character:

$$\sum_{\sigma \in \mathrm{Gal}(F/K)} \chi^{-1}(\sigma) \langle x^\sigma \otimes p^{-k}, \xi \rangle = p^{-k} \frac{L(\varphi\chi, 1)}{\Omega_E} \sum_{\sigma \in \mathrm{Gal}(F/K)} \chi^{-1}(\sigma) \lambda_E(x^\sigma),$$

$\langle \cdot, \cdot \rangle$ Kummer pairing, φ Hecke character of K , Ω_E real Néron period of E , λ_E logarithm

$$L_p^\pm(E, K_\infty) := \text{image of } \xi \text{ under } \mathcal{C}_{K_\infty}^\Phi \longrightarrow \mathcal{U}_{K_\infty}^\Phi \simeq H_{\mathrm{Iw}}^1(\mathbb{Q}_{p^2, \infty}, \mathbb{Z}_{p^2}(\chi_E^{-1} \chi_{\mathrm{cyc}})) \xrightarrow{\mathrm{Col}^\pm} \Lambda^{\mathrm{O}_{K_p}}$$

Interpolation formula

$L_p^\pm(E, K_\infty)$ differs from an element $h^\pm \in \Lambda$ satisfying the following by a unit in $\Lambda^{\mathrm{O}_{K_p}}$:
 for every $n \geq 0$ and every character $\chi : \mathrm{Gal}(L_\infty/K) \rightarrow \mu_{p^n}$ of order p^n :

$$\frac{L(\varphi\chi, 1)}{\Omega_E} \tau_{n+1}(\chi) = \chi(h^\pm) \chi\left(\frac{\omega_n^\mp(X)}{X}\right)$$

where $(-1)^n = \pm 1$, and τ_{n+1} is the Gauß sum

$\mathcal{C} := \varprojlim_F C_F \subset \mathcal{U} := \varprojlim_F U_F$, with $K \subseteq F \subset K(E[p^\infty])$, C_F : closure of elliptic units,
 U_F : pro- p part of $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$, $\Phi : G_K \rightarrow \mathcal{O}_{K_p}^\times$ character of action on $T_p(E)$

$$\mathcal{C}_{K_\infty}^\Phi := \mathcal{C} \otimes_{\mathcal{O}_K} \text{Hom}(E[p^\infty], K_p/\mathcal{O}_{K_p}) \otimes_{\Lambda(\text{Gal}(K(E[p^\infty])/K))} \Lambda(\text{Gal}(K_\infty/K))$$

Theorem (Wiles, Coates–Wiles, Rubin)

$\mathcal{C}_{K_\infty}^\Phi$ is a free $\Lambda^{\mathcal{O}_K}(K_\infty)$ -module of rank one. It has a **generator** ξ such that for all $K \subset F \subset K_\infty$, $x \in E(F_p)$ and $\chi : \text{Gal}(F/K) \rightarrow \mu_{p^\infty}$ character:

$$\sum_{\sigma \in \text{Gal}(F/K)} \chi^{-1}(\sigma) \langle x^\sigma \otimes p^{-k}, \xi \rangle = p^{-k} \frac{L(\varphi\chi, 1)}{\Omega_E} \sum_{\sigma \in \text{Gal}(F/K)} \chi^{-1}(\sigma) \lambda_E(x^\sigma),$$

$\langle \cdot, \cdot \rangle$ Kummer pairing, φ Hecke character of K , Ω_E real Néron period of E , λ_E logarithm

$$L_p^\pm(E, K_\infty) := \text{image of } \xi \text{ under } \mathcal{C}_{K_\infty}^\Phi \longrightarrow \mathcal{U}_{K_\infty}^\Phi \simeq H_{\text{Iw}}^1(\mathbb{Q}_{p^2, \infty}, \mathbb{Z}_{p^2}(\chi_E^{-1} \chi_{\text{cyc}})) \xrightarrow{\text{Col}^\pm} \Lambda^{\mathcal{O}_{K_p}}$$

Interpolation formula

$L_p^\pm(E, K_\infty)$ differs from an element $h^\pm \in \Lambda$ satisfying the following by a unit in $\Lambda^{\mathcal{O}_{K_p}}$:
 for every $n \geq 0$ and every character $\chi : \text{Gal}(L_\infty/K) \rightarrow \mu_{p^n}$ of order p^n :

$$\frac{L(\varphi\chi, 1)}{\Omega_E} \tau_{n+1}(\chi) = \chi(h^\pm) \chi \left(\frac{\omega_n^\mp(X)}{X} \right)$$

where $(-1)^n = \pm 1$, and τ_{n+1} is the Gauß sum

$\mathcal{C} := \varprojlim_F C_F \subset \mathcal{U} := \varprojlim_F U_F$, with $K \subseteq F \subset K(E[p^\infty])$, C_F : closure of elliptic units,
 U_F : pro- p part of $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$, $\Phi : G_K \rightarrow \mathcal{O}_{K_p}^\times$ character of action on $T_p(E)$

$$\mathcal{C}_{K_\infty}^\Phi := \mathcal{C} \otimes_{\mathcal{O}_K} \mathrm{Hom}(E[p^\infty], K_p/\mathcal{O}_{K_p}) \otimes_{\Lambda(\mathrm{Gal}(K(E[p^\infty])/K))} \Lambda(\mathrm{Gal}(K_\infty/K))$$

Theorem (Wiles, Coates–Wiles, Rubin)

$\mathcal{C}_{K_\infty}^\Phi$ is a free $\Lambda^{\mathcal{O}_K}(K_\infty)$ -module of rank one. It has a **generator** ξ such that for all $K \subset F \subset K_\infty$, $x \in E(F_p)$ and $\chi : \mathrm{Gal}(F/K) \rightarrow \mu_{p^\infty}$ character:

$$\sum_{\sigma \in \mathrm{Gal}(F/K)} \chi^{-1}(\sigma) \langle x^\sigma \otimes p^{-k}, \xi \rangle = p^{-k} \frac{L(\varphi\chi, 1)}{\Omega_E} \sum_{\sigma \in \mathrm{Gal}(F/K)} \chi^{-1}(\sigma) \lambda_E(x^\sigma),$$

$\langle \cdot, \cdot \rangle$ Kummer pairing, φ Hecke character of K , Ω_E real Néron period of E , λ_E logarithm

$$L_p^\pm(E, K_\infty) := \text{image of } \xi \text{ under } \mathcal{C}_{K_\infty}^\Phi \longrightarrow \mathcal{U}_{K_\infty}^\Phi \simeq H_{\mathrm{Iw}}^1(\mathbb{Q}_{p^2, \infty}, \mathbb{Z}_{p^2}(\chi_E^{-1} \chi_{\mathrm{cyc}})) \xrightarrow{\mathrm{Col}^\pm} \Lambda^{\mathcal{O}_{K_p}}$$

Interpolation formula

$L_p^\pm(E, K_\infty)$ differs from an element $h^\pm \in \Lambda$ satisfying the following by a unit in $\Lambda^{\mathcal{O}_{K_p}}$:
 for every $n \geq 0$ and every character $\chi : \mathrm{Gal}(L_\infty/K) \rightarrow \mu_{p^n}$ of order p^n :

$$\frac{L(\varphi\chi, 1)}{\Omega_E} \tau_{n+1}(\chi) = \chi(h^\pm) \chi\left(\frac{\omega_n^\mp(X)}{X}\right)$$

where $(-1)^n = \pm 1$, and τ_{n+1} is the Gauß sum

$\mathcal{C} := \varprojlim_F C_F \subset \mathcal{U} := \varprojlim_F U_F$, with $K \subseteq F \subset K(E[p^\infty])$, C_F : closure of elliptic units,
 U_F : pro- p part of $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$, $\Phi : G_K \rightarrow \mathcal{O}_{K_p}^\times$ character of action on $T_p(E)$

$$\mathcal{C}_{K_\infty}^\Phi := \mathcal{C} \otimes_{\mathcal{O}_K} \text{Hom}(E[p^\infty], K_p/\mathcal{O}_{K_p}) \otimes_{\Lambda(\text{Gal}(K(E[p^\infty])/K))} \Lambda(\text{Gal}(K_\infty/K))$$

Theorem (Wiles, Coates–Wiles, Rubin)

$\mathcal{C}_{K_\infty}^\Phi$ is a free $\Lambda^{\mathcal{O}_K}(K_\infty)$ -module of rank one. It has a **generator** ξ such that for all $K \subset F \subset K_\infty$, $x \in E(F_p)$ and $\chi : \text{Gal}(F/K) \rightarrow \mu_{p^\infty}$ character:

$$\sum_{\sigma \in \text{Gal}(F/K)} \chi^{-1}(\sigma) \langle x^\sigma \otimes p^{-k}, \xi \rangle = p^{-k} \frac{L(\varphi\chi, 1)}{\Omega_E} \sum_{\sigma \in \text{Gal}(F/K)} \chi^{-1}(\sigma) \lambda_E(x^\sigma),$$

$\langle \cdot, \cdot \rangle$ Kummer pairing, φ Hecke character of K , Ω_E real Néron period of E , λ_E logarithm

$$L_p^\pm(E, K_\infty) := \text{image of } \xi \text{ under } \mathcal{C}_{K_\infty}^\Phi \longrightarrow \mathcal{U}_{K_\infty}^\Phi \simeq H_{\text{Iw}}^1(\mathbb{Q}_{p^2, \infty}, \mathbb{Z}_{p^2}(\chi_{\hat{E}}^{-1} \chi_{\text{cyc}})) \xrightarrow{\text{Col}^\pm} \Lambda^{\mathcal{O}_{K_p}}$$

Interpolation formula

$L_p^\pm(E, K_\infty)$ differs from an element $h^\pm \in \Lambda$ satisfying the following by a unit in $\Lambda^{\mathcal{O}_{K_p}}$:
 for every $n \geq 0$ and every character $\chi : \text{Gal}(L_\infty/K) \rightarrow \mu_{p^n}$ of order p^n :

$$\frac{L(\varphi\chi, 1)}{\Omega_E} \tau_{n+1}(\chi) = \chi(h^\pm) \chi \left(\frac{\omega_n^\mp(X)}{X} \right)$$

where $(-1)^n = \pm 1$, and τ_{n+1} is the Gauß sum

$\mathcal{C} := \varprojlim_F C_F \subset \mathcal{U} := \varprojlim_F U_F$, with $K \subseteq F \subset K(E[p^\infty])$, C_F : closure of elliptic units,
 U_F : pro- p part of $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$, $\Phi : G_K \rightarrow \mathcal{O}_{K_p}^\times$ character of action on $T_p(E)$

$$\mathcal{C}_{K_\infty}^\Phi := \mathcal{C} \otimes_{\mathcal{O}_K} \text{Hom}(E[p^\infty], K_p/\mathcal{O}_{K_p}) \otimes_{\Lambda(\text{Gal}(K(E[p^\infty])/K))} \Lambda(\text{Gal}(K_\infty/K))$$

Theorem (Wiles, Coates–Wiles, Rubin)

$\mathcal{C}_{K_\infty}^\Phi$ is a free $\Lambda^{\mathcal{O}_K}(K_\infty)$ -module of rank one. It has a **generator** ξ such that for all $K \subset F \subset K_\infty$, $x \in E(F_p)$ and $\chi : \text{Gal}(F/K) \rightarrow \mu_{p^\infty}$ character:

$$\sum_{\sigma \in \text{Gal}(F/K)} \chi^{-1}(\sigma) \langle x^\sigma \otimes p^{-k}, \xi \rangle = p^{-k} \frac{L(\varphi\chi, 1)}{\Omega_E} \sum_{\sigma \in \text{Gal}(F/K)} \chi^{-1}(\sigma) \lambda_E(x^\sigma),$$

$\langle \cdot, \cdot \rangle$ Kummer pairing, φ Hecke character of K , Ω_E real Néron period of E , λ_E logarithm

$$L_p^\pm(E, K_\infty) := \text{image of } \xi \text{ under } \mathcal{C}_{K_\infty}^\Phi \longrightarrow \mathcal{U}_{K_\infty}^\Phi \simeq H_{\text{Iw}}^1(\mathbb{Q}_{p^2, \infty}, \mathbb{Z}_{p^2}(\chi_{\hat{E}}^{-1} \chi_{\text{cyc}})) \xrightarrow{\text{Col}^\pm} \Lambda^{\mathcal{O}_{K_p}}$$

Interpolation formula

$L_p^\pm(E, K_\infty)$ differs from an element $h^\pm \in \Lambda$ satisfying the following by a unit in $\Lambda^{\mathcal{O}_{K_p}}$:
 for every $n \geq 0$ and every character $\chi : \text{Gal}(L_\infty/K) \rightarrow \mu_{p^n}$ of order p^n :

$$\frac{L(\varphi\chi, 1)}{\Omega_E} \tau_{n+1}(\chi) = \chi(h^\pm) \chi \left(\frac{\omega_n^\mp(X)}{X} \right)$$

where $(-1)^n = \pm 1$, and τ_{n+1} is the Gauß sum

Putting everything together and using Pollack–Rubin’s methods:

Theorem (F–Lei)

$X^\pm(E/K_\infty)$ is a *torsion* $\Lambda^{\mathcal{O}_K}$ -module, and $\text{char}(X^\pm(E/K_\infty))\Lambda^{\mathcal{O}_K} = (L_p^\pm(E, K_\infty))$.

$$\mathbb{Z}_p[[\text{Gal}(K_\infty/K)]] \simeq \mathbb{Z}_p[[\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]], \quad L_p^\pm(E, K_\infty) \mapsto L_p^\pm(E, \mathbb{Q}_\infty)$$

Corollary

$X^\pm(E/\mathbb{Q}_\infty)$ is a *torsion* Λ -module, and $\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda = (L_p^\pm(E, \mathbb{Q}_\infty))$.

Putting everything together and using Pollack–Rubin's methods:

Theorem (F–Lei)

$X^\pm(E/K_\infty)$ is a *torsion* $\Lambda^{\mathcal{O}_K}$ -module, and $\text{char}(X^\pm(E/K_\infty))\Lambda^{\mathcal{O}_K} = (L_p^\pm(E, K_\infty))$.

$$\mathbb{Z}_p[[\text{Gal}(K_\infty/K)]] \simeq \mathbb{Z}_p[[\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]], \quad L_p^\pm(E, K_\infty) \mapsto L_p^\pm(E, \mathbb{Q}_\infty)$$

Corollary

$X^\pm(E/\mathbb{Q}_\infty)$ is a *torsion* Λ -module, and $\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda = (L_p^\pm(E, \mathbb{Q}_\infty))$.

Putting everything together and using Pollack–Rubin’s methods:

Theorem (F–Lei)

$X^\pm(E/K_\infty)$ is a *torsion* $\Lambda^{\mathcal{O}_K}$ -module, and $\text{char}(X^\pm(E/K_\infty))\Lambda^{\mathcal{O}_K} = (L_p^\pm(E, K_\infty))$.

$$\mathbb{Z}_p[[\text{Gal}(K_\infty/K)]] \simeq \mathbb{Z}_p[[\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]], \quad L_p^\pm(E, K_\infty) \mapsto L_p^\pm(E, \mathbb{Q}_\infty)$$

Corollary

$X^\pm(E/\mathbb{Q}_\infty)$ is a *torsion* Λ -module, and $\text{char}(X^\pm(E/\mathbb{Q}_\infty))\Lambda^{\mathcal{O}_K} = (L_p^\pm(E, \mathbb{Q}_\infty))$.

Recall: $X^\pm(E/K_\infty)$ is a finitely generated torsion Λ -module.

Structure theorem: there is a homomorphism with finite kernel and cokernel:

$$X^\pm(E/K_\infty) \longrightarrow \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

$$\mu^\pm = \mu(X^\pm(E/K_\infty)) := \sum m_i, \quad \lambda^\pm = \lambda(X^\pm(E/K_\infty)) := \sum \deg F_j$$

Theorem (F–Lei)

Assume that $\text{III}(E/K_n)[p^\infty]$ is finite with cardinality p^{e_n} for all $n \geq 0$.

Let $2r_\infty = \lim_{n \rightarrow \infty} \text{rank } E(K_n)$. For $n \gg 0$, we have

$$e_n - e_{n-1} = \begin{cases} 2(\deg \omega_n^- - 1 + \lambda^+ - r_\infty + \varphi(p^n)\mu^+) & \text{if } n \text{ is even,} \\ 2(\deg \omega_n^+ - 1 + \lambda^- - r_\infty + \varphi(p^n)\mu^-) & \text{if } n \text{ is odd.} \end{cases}$$

Corollary

The same formula holds for growth of $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ when $n \gg 0$, assuming finiteness.

This confirms a conjecture of Lei–Pollack–Pratap based on numerical data.

Recall: $X^\pm(E/K_\infty)$ is a finitely generated torsion Λ -module.

Structure theorem: there is a homomorphism with finite kernel and cokernel:

$$X^\pm(E/K_\infty) \longrightarrow \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

$$\mu^\pm = \mu(X^\pm(E/K_\infty)) := \sum m_i, \quad \lambda^\pm = \lambda(X^\pm(E/K_\infty)) := \sum \deg F_j$$

Theorem (F–Lei)

Assume that $\text{III}(E/K_n)[p^\infty]$ is finite with cardinality p^{e_n} for all $n \geq 0$.

Let $2r_\infty = \lim_{n \rightarrow \infty} \text{rank } E(K_n)$. For $n \gg 0$, we have

$$e_n - e_{n-1} = \begin{cases} 2(\deg \omega_n^- - 1 + \lambda^+ - r_\infty + \varphi(p^n)\mu^+) & \text{if } n \text{ is even,} \\ 2(\deg \omega_n^+ - 1 + \lambda^- - r_\infty + \varphi(p^n)\mu^-) & \text{if } n \text{ is odd.} \end{cases}$$

Corollary

The same formula holds for growth of $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ when $n \gg 0$, assuming finiteness.

This confirms a conjecture of Lei–Pollack–Pratap based on numerical data.

Recall: $X^\pm(E/K_\infty)$ is a finitely generated torsion Λ -module.

Structure theorem: there is a homomorphism with finite kernel and cokernel:

$$X^\pm(E/K_\infty) \longrightarrow \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

$$\mu^\pm = \mu(X^\pm(E/K_\infty)) := \sum m_i, \quad \lambda^\pm = \lambda(X^\pm(E/K_\infty)) := \sum \deg F_j$$

Theorem (F–Lei)

Assume that $\text{III}(E/K_n)[p^\infty]$ is finite with cardinality p^{e_n} for all $n \geq 0$.

Let $2r_\infty = \lim_{n \rightarrow \infty} \text{rank } E(K_n)$. For $n \gg 0$, we have

$$e_n - e_{n-1} = \begin{cases} 2(\deg \omega_n^- - 1 + \lambda^+ - r_\infty + \varphi(p^n)\mu^+) & \text{if } n \text{ is even,} \\ 2(\deg \omega_n^+ - 1 + \lambda^- - r_\infty + \varphi(p^n)\mu^-) & \text{if } n \text{ is odd.} \end{cases}$$

Corollary

The same formula holds for growth of $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ when $n \gg 0$, assuming finiteness.

This confirms a conjecture of Lei–Pollack–Pratap based on numerical data.

Recall: $X^\pm(E/K_\infty)$ is a finitely generated torsion Λ -module.

Structure theorem: there is a homomorphism with finite kernel and cokernel:

$$X^\pm(E/K_\infty) \longrightarrow \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/F_j(T)$$

with $F_j(T) \in \mathbb{Z}_p[T]$ certain polynomials.

$$\mu^\pm = \mu(X^\pm(E/K_\infty)) := \sum m_i, \quad \lambda^\pm = \lambda(X^\pm(E/K_\infty)) := \sum \deg F_j$$

Theorem (F–Lei)

Assume that $\text{III}(E/K_n)[p^\infty]$ is finite with cardinality p^{e_n} for all $n \geq 0$.

Let $2r_\infty = \lim_{n \rightarrow \infty} \text{rank } E(K_n)$. For $n \gg 0$, we have

$$e_n - e_{n-1} = \begin{cases} 2(\deg \omega_n^- - 1 + \lambda^+ - r_\infty + \varphi(p^n)\mu^+) & \text{if } n \text{ is even,} \\ 2(\deg \omega_n^+ - 1 + \lambda^- - r_\infty + \varphi(p^n)\mu^-) & \text{if } n \text{ is odd.} \end{cases}$$

Corollary

The same formula holds for growth of $\text{III}(E/\mathbb{Q}_n)[p^\infty]$ when $n \gg 0$, assuming finiteness.

This confirms a conjecture of Lei–Pollack–Pratap based on numerical data.

$E/\mathbb{Q}$ Main Conjectures		good	potentially ordinary	good	potentially supersingular
CM	p inert	—	—	= Pollack–Rubin	= F–Lei
	p ramified	—	—	$\supseteq$ Kobayashi	
	p split	= Rubin	= Delbourgo Müller	—	—
w/o CM		$\supseteq$ Kato $\subseteq$ Skinner–Urban	conjecture by Delbourgo	$\supseteq$ Kobayashi	