Iwasawa Theory of Elliptic Curves and BSD in Rank Zero

Jordan Schettler

Department of Mathematics
University of Arizona

10/27/09
Fix a rational prime $p$ and a number field $F$.

Let $F_\infty / F$ be a $\mathbb{Z}_p$-extension, i.e. as topological groups

$$\Gamma := \text{Gal}(F_\infty / F) \cong \mathbb{Z}_p$$

where $\Gamma$ is given the Krull topology.
Setup

Infinite Galois theory gives an inclusion reversing bijection

\[
\text{closed subgroups} \leftrightarrow \text{intermediate fields}.
\]

Also, all nontrivial closed subgroups of \(\mathbb{Z}_p\) are of the form

\[p^n\mathbb{Z}_p\]

for some \(n \in \mathbb{N}_0\).
Thus the extensions of $F$ contained in $F_\infty$ form a tower

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_\infty$$

such that $\forall n \geq 0$

$$\Gamma_n := \text{Gal}(F_\infty/F_n)$$

has index $p^n$ in $\Gamma$ and

$$\text{Gal}(F_n/F) \cong \Gamma/\Gamma_n \cong \mathbb{Z}/(p^n).$$
Cyclotomic Extensions

There is always at least one $\mathbb{Z}_p$-extension of $F$.

In particular, there is a unique subfield

$$F^c_\infty \subseteq F(\zeta_p)$$

s.t. $F^c_\infty / F$ is a $\mathbb{Z}_p$-extension, so-called cyclotomic.

Note: Kronecker-Weber $\Rightarrow \mathbb{Q}_\infty^c$ is the only $\mathbb{Z}_p$-ext’n of $\mathbb{Q}$. 
We define the cyclotomic character

\[ \chi : \text{Gal}(F(\zeta_{p\infty})/F) \rightarrow \mathbb{Z}_p^\times \cong (\text{finite group}) \times \mathbb{Z}_p \]

by

\[ \sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi(\sigma)} \quad \text{for all } n \in \mathbb{N}_0. \]

For example, if \( \zeta_{2p} \in F \), then \( \text{im}(\chi) \cong \mathbb{Z}_p \), so

\[ F_\infty^c = F(\zeta_{p\infty}). \]
Moreover,

\[ F^c_\infty = F^c \mathbb{Q}^c_\infty \]

with

\[ \mathbb{Q}^c_\infty \subseteq \mathbb{Q}(\zeta_p^\infty)_+ \subseteq \mathbb{R}. \]

E.g., if \( p = 3 \) and \( F = \mathbb{Q} \), then

\[ F^c_\infty = \mathbb{Q}(\zeta_3^\infty)_+ = \bigcup_{n=0}^{\infty} \mathbb{Q}(\zeta_{3n+1} + \zeta_{3n+1}^{-1}). \]
Theorem (Iwasawa’s Growth Formula)

Let $F_{\infty}/F$ be as above. Then $\exists \lambda, \mu, \nu \in \mathbb{Z}$ with $\lambda, \mu \geq 0$ s.t. $\forall n \gg 0$

$$\text{ord}_p |C(F_n)| = \lambda n + \mu p^n + \nu$$

where $C(F_n)$ is the class group of $F_n$. 
Idea Behind Growth Formula

Let $L_n$ denote the $p$-Hilbert class field of $F_n$, so

$$X_n := \text{Gal}(L_n/F_n) \cong \text{Sylow-} p \text{ subgroup of } C(F_n).$$

Then $\text{Gal}(F_n/F)$ acts on $X_n$ via the SES

$$1 \rightarrow X_n \rightarrow \text{Gal}(L_n/F) \rightarrow \text{Gal}(F_n/F) \rightarrow 1.$$
Explicitly,

\[ \sigma \cdot x_n := \tilde{\sigma} x_n \tilde{\sigma}^{-1} \]

where \( x_n \in X_n \) and

\[ \tilde{\sigma} \in \text{Gal}(L_n/F) \]

extends

\[ \sigma \in \text{Gal}(F_n/F). \]
The Iwasawa Module

Thus each $X_n$ is a module (given the discrete topology) over

$$\mathbb{Z}_p[\text{Gal}(F_n/F)]$$

(given the product topology), so

$$X := \lim_{\leftarrow} X_n$$

is a $\Lambda$-module where

$$\Lambda := \lim_{\leftarrow} \mathbb{Z}_p[\text{Gal}(F_n/F)].$$
Description of Λ

Now

\[ \Gamma \cong \varprojlim \text{Gal}(F_n/F), \]

so we may view

\[ \mathbb{Z}_p[\Gamma] \subseteq \Lambda. \]

In fact, \( \mathbb{Z}_p[\Gamma] \) is dense in \( \Lambda \).
Description of $\Lambda$

There is an identification

$$\Lambda \sim \mathbb{Z}_p[[T]] : \gamma \mapsto T + 1$$

where $\gamma \in \Gamma$ has $\gamma|_{F_1}$ nontrivial.

Here $\gamma$ is a topological generator, i.e.

$$\Gamma = \langle \gamma \rangle.$$
Λ-module Decomposition

Λ is not a PID, but there is a structure theorem...

**Theorem**

If \( M \) is finitely generated \( \Lambda \)-module, \( \exists \) pseudo-isomorphism

\[
M \sim \Lambda^r \bigoplus_{i=1}^{s} \frac{\Lambda}{(p^{n_i})} \bigoplus_{j=1}^{t} \frac{\Lambda}{(f_j^{m_j})}
\]

where each \( f_j \in \mathbb{Z}_p[T] \) is distinguished and irreducible.
Connection Between Growth Formula and $X$

It turns out that $X$ is a finitely generated torsion $\Lambda$-module.

Taking $M = X$, there’s a well-defined characteristic polynomial

$$\text{char}(X) := \left( \prod_{i=1}^{s} p^{n_i} \right) \left( \prod_{j=1}^{t} f_j \right)$$

which generates the so-called characteristic ideal of $X$. 
We can compute $\lambda, \mu$ in the growth formula:

$$
\mu = n_1 + \cdots + n_s = \text{ord}_p(\text{char}(X))
$$

$$
\lambda = m_1 \deg(f_1) + \cdots + m_t \deg(f_t) = \deg(\text{char}(X))
$$
The \( p \)-adic \( L \)-function Attached to a Character

From now on, suppose \( p \) is odd for simplicity.

Fix \( \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p \) and let \( \chi \) be a primitive Dirichlet character.

\[ \exists \text{ } p \text{-adic meromorphic function } L_p(s, \chi) \text{ with } \]

\[ L_p(1 - n, \chi) = (1 - \chi(p)p^{n-1})L(1 - n, \chi) \]

whenever \( p - 1 | n \geq 1 \).
Framework for Main Conjecture

Take $F = \mathbb{Q}(\zeta_p)$.

Then $G := \text{Gal}(F/\mathbb{Q}) \circlearrowleft X$ via

$$
\sigma \cdot (x_n) = (\sigma|_{F_n} \cdot x_n)
$$

where

$$
\sigma_\omega \in \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})
$$

is the “Teichmüller lift.”
We define $\sigma_\omega$ as follows: if $\sigma(\zeta_p) = \zeta_p^a$, take

$$\sigma_\omega(\zeta_p^n) = \zeta_p^{\omega(a)n}$$

for all $n \in \mathbb{N}$ where

$$\omega : (\mathbb{Z}/(p))^\times \to \mu_{p-1} \subseteq \mathbb{Z}_p^\times$$

is determined by

$$a \equiv \omega(\overline{a}) \pmod{p}.$$
Now \( \hat{G} = \langle \omega \rangle \), so

\[
X = \bigoplus_{i=0}^{p-2} \varepsilon_i X
\]

as \( \mathbb{Z}_p[G] \)-modules where

\[
\varepsilon_i = \frac{1}{p-1} \sum_{g \in G} \omega^i(g)g^{-1}.
\]
Let $i \in \{3, 5, \ldots, p - 2\}$. Then we have the following result.

**Theorem (Mazur, Wiles)**

There is a generator $f$ of $(\text{char}(\varepsilon_i X))$ such that

$$f(\kappa^s - 1) = L_p(s, \omega^{1-i})$$

for all $s \in \mathbb{Z}_p$ where $\gamma = \chi^{-1}(\kappa)$.

Note: We can choose $\kappa = 1 + p$. 
Pontryagin Dual

Define a functor on topological $\Lambda$-modules

$(-)^*: = \text{Hom}_{\text{cont}}(-, \mathbb{Q}_p/\mathbb{Z}_p)$.

With diagonal $\Gamma$-action and compact-open topology this functor interchanges compact and discrete $\Lambda$-modules.

Note: $\mathbb{Q}_p/\mathbb{Z}_p$ is taken to have trivial $\Gamma$-action.
First Observation

(1) For $m \in \mathbb{N}_0 \cup \{\infty\}$ we may view

$$X_m^* \leq H^1(F_m, \mathbb{Q}_p/\mathbb{Z}_p)$$

as the classes which are unramified at all places of $F_m$. 
Second Observation

(2) The natural maps

\[ X_{\Gamma_n} \cong X / (\gamma^{p^n} - 1)X \rightarrow X_n \]

induce

\[ X_n^* \rightarrow (X^*)^{\Gamma_n} \]

which are isos when there is a unique prime \( \mathfrak{p} \) in \( F \) lying over \( p \) and \( \mathfrak{p} \) is totally ramified in \( F_\infty / F \).
(1) reminds us of a Selmer group for an elliptic curve $E/F_m$:

$$\text{Sel}_E(F_m)_p \leq H^1(F_m, E[p^\infty])$$

consists of the classes $[\phi]$ with certain local restrictions.
Selmer Groups

In detail, taking $K := F_m$, such $[\phi]$ satisfy

$$[\phi|_{G_{K_v}}] \in \text{im}(\kappa_v)$$

for all places $v$ of $K$ where

$$\kappa_v : E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(K_v, E[p^\infty])$$

are the Kummer homomorphisms.
Let $[\phi] \in H^1(F_\infty, E[p^\infty])$ and suppose 

$$\tilde{\gamma} \in G_F$$

extends $\gamma \in \Gamma$.

Then we define

$$\gamma \cdot [\phi] := [\phi_{\tilde{\gamma}}]$$

where for $\alpha \in G_{F_\infty}$

$$\phi_{\tilde{\gamma}}(\alpha) = \tilde{\gamma}\phi(\tilde{\gamma}^{-1}\alpha\tilde{\gamma}).$$
\( H^1, \text{Sel as } \Lambda\text{-modules} \)

\( \text{Sel}_E(F_{\infty})_p \) is \( \Gamma \)-invariant under this action.

Every \([\phi] \in H^1(F_{\infty}, E[p^\infty])\) is killed by a power of \( T \), so both

\[
H^1(F_\infty, E[p^\infty]) \text{ and } \text{Sel}_E(F_\infty)_p
\]

are torsion \( \Lambda \)-modules which we give the discrete topology.
Continuing this analogy, the corresponding maps in (2) are pseudo-isos under the right assumptions on $p$.

**Theorem (Mazur)**

Suppose $E/F$ has good, ordinary reduction at every prime of $F$ lying over $p$. Then the natural maps

$$\text{Sel}_E(F_n^c)_p \rightarrow \text{Sel}_E(F_{\infty}^c)^{\Gamma_n}_p$$

have finite ker, coker of bounded order as $n$ varies.
Working Assumption

Definition

Say $E/F$ is “nice at $p$” if it has good, ordinary reduction at every prime of $F$ lying over $p$ and $|\text{Sel}_E(F)_p| < \infty$.

Note: The assumption $|\text{Sel}_E(F)_p| < \infty$ is equivalent to

$$\text{rank}_{\mathbb{Z}}(E(F)) = 0 \text{ and } |\text{Tor}_E(F)_p| < \infty.$$
Corollary

If $E/F$ is nice at $p$, then

$$X := Sel_E(F_c^\infty)_p$$

is a finitely generated torsion $\Lambda$-module.
Proof of Corollary

Proof.

Apply control theorem for \( n = 0 \), and get

\[
X / TX \cong X_\Gamma \cong (\text{Sel}_E(F_\infty^c)_p)^* \sim \text{Sel}_E(F)_p^* \text{ is finite.}
\]

Done by Nakayama’s lemma and structure theorem.
Analog of Fundamental Theorem

**Theorem (Growth Formula)**

*If $E/F$ is nice at $p$, then $\exists \lambda, \mu, \nu \in \mathbb{Z}$ with $\lambda, \mu \geq 0$ s.t. $\forall n \gg 0$

\[
\text{ord}_p |\sha(F_n^c)| = \lambda n + \mu p^n + \nu
\]

assuming the LHS is always finite.*
Connection Between Growth Formula and $X$

In fact, if $\lambda_E, \mu_E$ are the invariants of $X$, we can compute

$$\mu = \mu_E$$

$$\lambda = \lambda_E - \text{rank}_\mathbb{Z}(E(F_c^c)).$$

E.g., we can find $\lambda$ by applying $(-)^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ to the SES

$$0 \rightarrow E(F_c^c) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \text{Sel}_E(F_c^c)_p \rightarrow \text{III}_E(F_c^c)_p \rightarrow 0.$$
Main Conjecture for Elliptic Curves

Take $F = \mathbb{Q}$. Then we have the following conjecture.

**Conjecture**

If $E/\mathbb{Q}$ is nice at $p$, there is a generator $f_E$ of $(\text{char}(X))$ s.t.

$$f_E(\kappa^{s-1} - 1) = L_p(E/\mathbb{Q}, s)$$

for all $s \in \mathbb{Z}_p$ where $\gamma = \chi^{-1}(\kappa)|_{\mathbb{Q}_\infty}$.

Note: Again we can choose $\kappa = 1 + p$. 
A Couple of Remarks

Suppose $E/\mathbb{Q}$ is nice at $p$ and $(f_E) = (\text{char}(X))$. We know

$$|E(\mathbb{Q})| < \infty,$$

so

$$E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0 \quad \text{and} \quad \text{Sel}_E(\mathbb{Q})_p \cong \text{III}_E(\mathbb{Q})_p.$$
Moreover, we’ve seen

\[ |X/ TX| < \infty, \]

but if \( Y = \Lambda/(T^k) \), then

\[ Y/ TY \cong \Lambda/(T) \cong \mathbb{Z}_p \]

is infinite, so \( T \nmid f_E(T) \), and, in particular,

\[ f_E(0) \neq 0. \]
Interpolation

$L_p(E/\mathbb{Q}, s)$ interpolates $L(E/\mathbb{Q}, s)$ in the following way:

If $\phi$ is a finite order character of $\mathbb{Z}_p^\times / \mu_{p-1}$ with conductor $p^n$,

$$L_p(E/\mathbb{Q}, \bar{\phi}, 1) = \beta_p^n (1 - \phi(p) \beta_p p^{-1})^2 \frac{L(E/\mathbb{Q}, \phi, 1)}{\Omega_E \tau(\phi)}$$

where $\tau(-)$ denotes a Gauss sum.
The Value at $s = 1$

If $f_E$ is as in the main conjecture and $\phi$ is trivial, then

$$\phi = \bar{\phi} \text{ has conductor } 1 = p^0,$$

so

$$f_E(0) = L_p(E/\mathbb{Q}, 1) = (1 - \beta_p p^{-1})^2 \frac{L(E/\mathbb{Q}, 1)}{\Omega_E}.$$
Here

\[ \Omega_E = \int_{E(\mathbb{R})} \left| \frac{dx}{2y + a_1 x + a_3} \right| \]

where

\[ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \]

is a global minimal Weierstrass equation.
Also, \[ \frac{1}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})} \]
is the Euler factor at \( p \) in \( L(E/\mathbb{Q}, s) \) with
\[
\alpha_p + \beta_p = 1 + p - |\tilde{E}(\mathbb{F}_p)| \\
\alpha_p \beta_p = p
\]
and choosing 
\[
\alpha_p \in \mathbb{Z}_p^\times.
\]
Featured Result

Theorem

If $E/\mathbb{Q}$ is nice at $p$ and $f_E$ generates $(\text{char}(X))$, then

$$f_E(0) \equiv \frac{(1 - \beta_p p^{-1})^2 \mid \mathcal{M}_E(\mathbb{Q})_p \mid \prod_{\text{bad } \ell} c^{(p)}_{\ell}}{|E(\mathbb{Q})_p|^2} \prod_{\text{bad } \ell} c^{(p)}_{\ell} \mod \mathbb{Z}_p$$

where $c^{(p)}_{\ell} = p$-part of the Tamagawa factor for a prime $\ell$. 

where $c^{(p)}_{\ell} = p$-part of the Tamagawa factor for a prime $\ell$. 
The Payoff

Assuming the main conjecture and $|\Sha_E(\mathbb{Q})| < \infty$, we get...

Corollary

If $E/\mathbb{Q}$ is nice at $p$, then

$$\frac{L(E/\mathbb{Q}, 1)}{\Omega_E} \equiv \frac{|\Sha_E(\mathbb{Q})| \prod \ell c_\ell}{|E(\mathbb{Q})|^2} \mod \mathbb{Z}_p^\times.$$
Outline of Proof for Featured Result

If \( Y = \Lambda/(g) \) with \( g(0) \neq 0 \), then \(|Y^\Gamma| = 1\) and

\[
|Y^\Gamma| = \left| \frac{Y}{TY} \right| = \left| \frac{\Lambda}{(T, g)} \right| = \left| \frac{\mathbb{Z}_p}{(g(0))} \right| \equiv g(0) \mod \mathbb{Z}_p^\times.
\]
Taking Euler characteristics yields

\[ \left| \frac{S^\Gamma}{S_\Gamma} \right| = \left| \frac{X^\Gamma}{X_\Gamma} \right| \equiv f_E(0) \mod \mathbb{Z}_p^\times \]

where we fix the notation \( S = \text{Sel}_E(\mathbb{Q}_\infty^c)_\rho \).
Outline of Proof Continued

We have a commutative diagram with exact rows

\[
\begin{array}{cccccc}
\text{Sel}_E(\mathbb{Q})_p & \rightarrow & H^1(\mathbb{Q}, E[p^\infty]) & \rightarrow & G_E(\mathbb{Q}) \\
\downarrow s & & \downarrow h & & \downarrow g \\
S^\Gamma & \rightarrow & H^1(\mathbb{Q}_c^c, E[p^\infty])^\Gamma & \rightarrow & G_E(\mathbb{Q}_\infty^c)^{\Gamma}.
\end{array}
\]
Turns out $\text{coker}(h) = 0$, so we get an exact sequence

$$0 \rightarrow \ker(s) \rightarrow \ker(h) \rightarrow \ker(g) \rightarrow \text{coker}(s) \rightarrow 0.$$ 

Thus

$$|S^S|/|\text{Sel}_E(\mathbb{Q})_p| = |\text{coker}(s)|/|\ker(s)| = |\ker(g)|/|\ker(h)|.$$
Since $E(\mathbb{Q}^c_\infty)_p$ is known to be finite, we get

$$\left| \ker(h) \right| = \left| H^1(\Gamma, E(\mathbb{Q}^c_\infty)_p) \right| = \left| (E(\mathbb{Q}^c_\infty)_p)\Gamma \right| = \left| E(\mathbb{Q}^c_\infty)_p \right| = \left| E(\mathbb{Q})_p \right|$$

so

$$f_E(0) \equiv \frac{\left| \text{III}_{E(\mathbb{Q})_p} \right| \cdot \left| \ker(g) \right|}{\left| S_\Gamma \right| \cdot \left| E(\mathbb{Q})_p \right|} \mod \mathbb{Z}_p^\times.$$
The snake lemma (again) and a theorem of Cassels imply

$$|\ker(g)| = \frac{|\ker(r)| \cdot |S_\Gamma|}{|E(\mathbb{Q})_p|}$$

where we have a natural map

$$r : \mathcal{P}_E(\mathbb{Q}) \to \mathcal{P}_E(\mathbb{Q}_\infty^c)$$

with

$$\mathcal{P}_E(K) := \prod_{\text{places } \nu \text{ on } K} \text{coker}(\kappa_\nu).$$
Combining the above expressions gives

\[ f_E(0) \equiv \frac{\prod E(\mathbb{Q})_p \cdot |\ker(r)|}{|E(\mathbb{Q})_p|^2} \mod \mathbb{Z}_p^\times. \]

It remains to compute

\[ |\ker(r)| = |\ker(r_p)| \prod_{\text{bad } \ell} |\ker(r_\ell)| \]

where

\[ r_v : \text{coker}(\kappa_v) \rightarrow \text{coker}(\kappa_w) \]

for some place \( w \mid \nu \) of \( \mathbb{Q}_\infty \).
Outline of Proof Continued

If $E/\mathbb{Q}$ has bad reduction at $\ell$, then

$$|\ker(r_\ell)| = c_\ell^{(p)},$$

while

$$|\ker(r_p)| = |\tilde{E}(\mathbb{F}_p)_p|^2 \equiv |\tilde{E}(\mathbb{F}_p)|^2 = (1 + p - \alpha_p - \beta_p)^2$$

$$= (1 - \beta_p)^2(1 - \alpha_p)^2 \equiv (1 - \alpha_p)^2$$

$$\equiv (1 - \beta_p p^{-1})^2 \mod \mathbb{Z}_p^\times,$$

which completes the sketch.
Example 1.

Consider the elliptic curve \( E : y^2 = x^3 - x \). We have

\[ \Delta = 2^6 \quad \text{and} \quad j = 2^6 \cdot 3^3, \]

so \( E \) has additive reduction at 2 & good reduction otherwise.
Example 1. Continued

Let \( p \) be a prime with \( p \equiv 1 \pmod{4} \).

Then the coefficient of \( x^{p-1} \) in

\[
(x^3 - x)^{(p-1)/2}
\]

is

\[
(-1)^{(p-1)/4} \not\equiv 0 \pmod{p},
\]

whence \( E \) has ordinary reduction at \( p \).
Example 1. Continued

Note that

\[(x, y) \mapsto (-x, iy)\]

has order 4 in \(\text{Aut}_{\mathbb{Q}(i)}(E)\), so \(E\) has complex mult over \(\mathbb{Q}(i)\).

In fact, the Coates-Wiles theorem applies, and we get

\[E(\mathbb{Q}) \subseteq E(\mathbb{Q}(i)) = E(\mathbb{Q}(i))_{\text{tors}}.\]
Example 1. Continued

If $\tilde{E}_3, \tilde{E}_5$ denote the reduction mod 3, 5, resp, then

$$\tilde{E}_3(\mathbb{F}_3) = \{\mathcal{O}, (0, 0), (\pm 1, 0)\}$$

and

$$\tilde{E}_5(\mathbb{F}_5) = \{\mathcal{O}, (0, 0), (\pm 1, 0), (2, \pm 1), (-2, \pm 2)\},$$

so

$$E(\mathbb{Q}) = E[2^\infty] = E[2] = \{\mathcal{O}, (0, 0), (\pm 1, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$
Example 1. Continued

In fact, it can also be shown that

\[ \text{III}_E(\mathbb{Q}) = 0. \]

In particular, \( E \) is nice at \( p \) and \( |E(\mathbb{Q})_\rho| = 1 \), so

\[ f_E(0) \equiv |\tilde{E}(\mathbb{F}_p)_\rho|^2 \cdot c_2^{(p)} \mod \mathbb{Z}_p^\times. \]
Example 1. Continued

Now \( c_2 \leq 4 \) since \( E \) has add red’n at 2, so \( p \nmid c_2 \).

Also,

\[
E(\mathbb{Q}) \hookrightarrow E(\mathbb{Q}_p)[2] \hookrightarrow \tilde{E}(\mathbb{F}_p),
\]

so if \( |\tilde{E}(\mathbb{F}_p)_p| > 1 \), then

\[
4p \leq |\tilde{E}(\mathbb{F}_p)| < 1 + p + 2\sqrt{p}
\]

which is a contradiction.
Example 1. Continued

Thus

\[ f_E(0) \equiv 1 \mod \mathbb{Z}_p, \]

so

\[ \mu_E = \lambda_E = 0 \]

and

\[ \chi \sim 0. \]
Example 2.

Now consider $E : y^2 = x^3 + x^2 - 647x - 6555$. We have

$$\Delta = 2^9 \cdot 3^5 \quad \text{and} \quad j = \frac{2^6 \cdot 971^3}{3^5},$$

so $E$ has additive reduction at 2, multiplicative reduction at 3, & good reduction otherwise.
Example 2. Continued

Let $p = 5$.

Then the reduction of $E \mod 5$ is $\tilde{E} : y^2 = x^3 + x^2 + 3x$.

The coefficient of $x^{5-1}$ in

$$(x^3 + x^2 + 3x)^{(5-1)/2}$$

is

$$7 \not\equiv 0 \pmod{5},$$

whence $E$ has ordinary reduction at 5.
Example 2. Continued

$E$ is related by a 5-isogeny defined over $\mathbb{Q}$ to

$$E' : y^2 = x^3 + x^2 - 7x + 5.$$  

This curve has the property that

$$\text{Sel}_{E'}(\mathbb{Q})_5 \rightarrow \text{Sel}_{E'}(\mathbb{Q}_\infty^c)_{\Gamma_5}$$

is surjective.
Example 2. Continued

\[ \tilde{E}' = \tilde{E} \mod 5, \text{ so again we have good, ord red'n at 5.} \]

\[ \text{Sel}_{E'}(\mathbb{Q}) = 0 \text{ assuming BSD, so } E' \text{ is nice at 5 and} \]

\[ X'/TX' = X' \cong (\text{Sel}_{E'}(\mathbb{Q}_\infty^c))^{\Gamma_5} \ast = 0. \]

Thus \( X' = 0 \) by Nakayama’s lemma, giving

\[ \mu_{E'} = \lambda_{E'} = 0. \]
Example 2. Continued

\( E, E' \) are isogenous over \( \mathbb{Q} \) and \( E \) is also nice at 5, so

\[
\lambda_E = \lambda_{E'} = 0.
\]

E.g., we can find \( \lambda_E \) by applying \((-)^* \otimes \mathbb{Z}_5 \mathbb{Q}_5 \) to the map

\[
\text{Sel}_E(\mathbb{Q}_\infty^c)_5 \to \text{Sel}_{E'}(\mathbb{Q}_\infty^c)_5 = 0
\]

with ker and coker of exponent 5 induced by an isogeny.
Example 2. Continued

Now $c_2 \leq 4$ since $E$ has add red’n at 2, so $5 \nmid c_2$.

Also, $E$ has split mult red’n at 3 since

$$b_2 := a_1^2 + 4a_2 = 0^2 + 4 \cdot 1$$

is a square in $\mathbb{F}_3$, so $c_3 = -\text{ord}_3(j) = 5$. 
Example 2. Continued

In fact, \( |E(\mathbb{Q})| = 2 \) and \( |\widetilde{E}(\mathbb{F}_5)| = 4 \), so

\[ f_E(0) \equiv 5 \pmod{\mathbb{Z}_5^\times}. \]

Thus \( \mu_E = 1 \) and

\[ X \sim \Lambda/(5). \]
Example 3.

Now consider $E : y^2 + xy = x^3 - 3x + 1$. We have

$$\Delta = 2^6 \cdot 17 \quad \text{and} \quad j = \frac{5^3 \cdot 29^3}{2^6 \cdot 17},$$

so $E$ has multiplicative reduction at 2, 17 & good reduction otherwise.
Example 3. Continued

Let $p = 3$.

Then we can check that

$$\tilde{E}(F_3) = \{0, (0, \pm 1), (\pm 1, 1), (-1, 0)\} \cong \mathbb{Z}/(6),$$

whence $E$ has ord red’n at 3.

$\text{Sel}_E(\mathbb{Q}) = 0$ assuming BSD, so $E$ is nice at 3.
Example 3. Continued

In fact, if \( \tilde{E}_5 \) denotes the reduction mod 5, then

\[
\{ \mathcal{O}, (\pm 2, 1), (0, \pm 1) \} \subseteq E(\mathbb{Q}) \hookrightarrow \tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/(6),
\]

so

\[
E(\mathbb{Q}) \cong \mathbb{Z}/(6).
\]
Example 3. Continued

Also, $E$ has split mult red’n at 2, 17, so

$$c_2 = -\text{ord}_2(j) = 6 \quad \text{and} \quad c_{17} = -\text{ord}_{17}(j) = 1.$$ 

Hence

$$f_E(0) \equiv 3 \mod \mathbb{Z}_3^\times,$$

and, in particular, $f_E$ is irreducible.
Example 3. Continued

Note that

$$Q^c_1 = Q(\alpha)$$

and

$$(\alpha, -\alpha) \in E(Q^c_1)$$

where

$$\alpha := \zeta_9 + \zeta_9^{-1}.$$
Example 3. Continued

It turns out that

\[ E(\mathbb{Q}_\infty^c)_{\text{tors}} = E(\mathbb{Q}), \]

so

\[ V := E(\mathbb{Q}_1^c) \otimes \mathbb{Q}_3 \]

is a nonzero, faithful \( \mathbb{Q}_3 \)-representation of

\[ G := \text{Gal}(\mathbb{Q}_1^c/\mathbb{Q}) \cong \mathbb{Z}/(3). \]
Example 3. Continued

We know

$$\dim_{\mathbb{Q}_3}(V) = \text{rank}_{\mathbb{Z}}(E(\mathbb{Q}_1^c)) < \infty$$

and $\exists$ exactly 2 finite dim’l, simple $\mathbb{Q}_3 G$-modules up to iso...

namely, $\mathbb{Q}_3$ with trivial $G$-action and the module $W$ afforded by the matrix representation

$$\rho : G \rightarrow \text{GL}_2(\mathbb{Q}_3) : \gamma|_{\mathbb{Q}_1^c} \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$
Example 3. Continued

Therefore \( \exists n \in \mathbb{N} \) s.t.

\[ V \cong W^n \]

since no point of infinite order in \( E(\mathbb{Q}_1^c) \) can be fixed by \( G \).

Consider

\[ M := \left( W \otimes_{\mathbb{Z}_3} \mathbb{Q}_3 / \mathbb{Z}_3 \right)^n \cong V \otimes_{\mathbb{Z}_3} \mathbb{Q}_3 / \mathbb{Z}_3 \cong E(\mathbb{Q}_1^c) \otimes \mathbb{Q}_3 / \mathbb{Z}_3 \]

as \( \Lambda \)-mods where \( \rho : \mathbb{Z}_3[\Gamma] \to M_2(\mathbb{Q}_3) \) is a hom of rings.
Note that

$$
\rho(T) = \rho(\gamma - 1) = \begin{pmatrix} -1 & -1 \\ 1 & -2 \end{pmatrix}
$$

has characteristic polynomial

$$
\theta(x) = x^2 + 3x + 3,
$$

so

$$
\text{char}(M^*) = \theta(T)^n.
$$
Example 3. Continued

On the other hand, $M$ is a submodule of $X^*$, so

$$\theta(T)^n|f_E(T),$$

giving $(\theta) = (f_E)$. Thus $\mu_E = 0$, $\lambda_E = 2$ and

$$X \sim \Lambda/(T^2 + 3T + 3).$$