The $p$-parts of Tate-Shafarevich groups of elliptic curves:

Dedicated to Takeshi Tsuji (Algebraic Number Theory and Related Topics 2010)

Author(s)

ITO SPRUNG, Florian E.

Citation

数理解析研究所講究録別冊 = RIMS Kokyuroku Bessatsu

(2012), B32: 51-60

Issue Date

2012-07

URL

http://hdl.handle.net/2433/196249

Type

Departmental Bulletin Paper

Textversion

publisher

Kyoto University
The \( p \)-parts of Tate-Shafarevich Groups of Elliptic Curves

Dedicated to Takeshi Tsuji

By

Florian E. Ito SPRUNG*

Abstract

We give an overview of Iwasawa theory for elliptic curves, and what this theory can tell us about the size of the Tate-Shafarevich group in towers of number fields. What is new is that we formulate this theory and derive its consequences at \( any \) odd prime of good reduction.

§1. Basic Results in Iwasawa theory

Iwasawa theory is a mysterious bridge between two mathematically faraway worlds, the analytic realm and the algebraic realm:

\[
\begin{array}{ccc}
\text{(analytic)} & \text{Iwasawa theory} & \text{(algebraic)} \\
\end{array}
\]

For the rest of this article, let \( p \) be an odd prime. Iwasawa looked at the following towers of number fields:

\[\text{key words: Elliptic Curves, Tate-Shafarevich Groups, Iwasawa Theory}\]

* Brown University, Providence, RI 02912, USA.

\[\text{e-mail: ian.sprung@gmail.com}\]

© 2012 Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.
After adjoining successively large $p$-power roots of unity, we obtain a tower of extensions whose union is $\mathbb{Q}(\mu_p^\infty)$ so that $\text{Gal}(\mathbb{Q}(\mu_p^\infty)/\mathbb{Q}) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \Delta$. By basic Galois theory, we can fix these fields by Galois groups isomorphic to $\Delta \cong \mathbb{Z}/(p-1)\mathbb{Z}$. We then get the tower of number fields on the right. This tower is called the \emph{cyclotomic $\mathbb{Z}_p$-extension}.

Given a $\mathbb{Z}$-module $M$, its $p$-primary part $M[p^\infty]$ is a $\mathbb{Z}_p$-module. For simplicity, let’s suppose that $M = M[p^\infty]$. If the Galois group $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ acts continuously on $M$, then $M$ becomes a $\Lambda := \mathbb{Z}_p[[\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$-module. This ring $\Lambda$ is called the \emph{Iwasawa algebra} and is also a power series ring $\Lambda \cong \mathbb{Z}_p[[X]]$, and thus is a ring of (special) $p$-adically continuous functions.

An \emph{Iwasawa Main Conjecture} usually states that the ideal generated in $\Lambda$ by an analytic object, a $p$-adic $L$-function $L_p(X) \in \Lambda$, is equal to the \emph{characteristic ideal} of an algebraic object:

\[
\begin{align*}
\text{(analytic)} & \quad \Lambda \\
\cup & \quad \cup \\
(L_p(X)) & = \text{Char}_\Lambda(M)
\end{align*}
\]

The analytic object $L_p(X)$ knows the (usual) $L$-function by $p$-adically interpolating a family of its special values, but we won’t get into any very analytic definitions, because the title of this conference is “Algebraic Number Theory and Related Topics”.

What is the characteristic ideal $\text{Char}_\Lambda(M)$? We can only define this when $M$ is a finitely generated torsion $\Lambda$-module. Before that, let’s look at a baby example where we replace the ring $\Lambda$ by $\mathbb{Z}$: Recall that a finitely generated torsion $\mathbb{Z}$-module $G$, i.e. a finite abelian group, admits an exact sequence

\[
0 \to \bigoplus_i \mathbb{Z}/p_i^{e_i} \mathbb{Z} \to G \to 0.
\]

The most important invariant of $G$ is its size $|G|$. Note that the ideal in $\mathbb{Z}$ generated by $|G|$ encodes this information as well. We call it the \emph{characteristic ideal}:

\[
\text{Char}_G := (|G|) = \left(\prod_i p_i^{e_i}\right) \subset \mathbb{Z}.
\]
Now suppose $M$ is a finitely generated torsion $\Lambda$-module. It turns out that $M$ then admits an exact sequence
\[ 0 \to \bigoplus_i \Lambda/\mathbf{f}_i \Lambda \to M \to (\text{finite}) \to 0, \]
where we have chosen $\mathbf{f}_i$ so that $\mathbf{f}_i |\mathbf{f}_{i+1}$. These $\mathbf{f}_i$ are not uniquely determined, but the ideal that their product generates in $\Lambda$ is. This is our characteristic ideal:
\[ \text{Char}_{\Lambda}(M) := (\prod_i \mathbf{f}_i) \subset \Lambda. \]

Elements of the Iwasawa algebra also have two canonical invariants:

**The $p$-adic Weierstrass Preparation Theorem** states that for $g(X) \in \Lambda$, there are (uniquely determined) non-negative integers $\mu, \lambda$ so that
\[ g(X) = p^{\mu}(X^{\lambda} + a_1 X^{\lambda-1} + \cdots + a_\lambda) U(X), \]
where $a_i \in p\mathbb{Z}_p$, and $U(X) \in \Lambda^\times$ is a unit.

For a finitely generated torsion $\Lambda$-module $M$, the integers $\mu$ and $\lambda$ of the generator of $\text{Char}_{\Lambda}(M)$ as above are called the Iwasawa invariants of $M$.

For proofs of all the above, we refer the reader to Washington’s book [26].

### § 2. Iwasawa Theory for Elliptic Curves

The idea of formulating an Iwasawa theory for elliptic curves by looking at their $\mathbb{Q}_p$-rational points goes back to Mazur. We will use freely a few basic results and terminology from elliptic curve theory and refer the reader to Silverman’s book [20] when stumbling across an unfamiliar term.

We fix an elliptic curve over $\mathbb{Q}$:
\[ E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}. \]

Suppose that $p$ is a good prime.

**Definition 2.1.** Let $a_p := p + 1 - \#E(\mathbb{F}_p)$. A prime $p$ that does not divide $a_p$ we call ordinary. If $p$ does divide $a_p$, we call it supersingular.

We thus have two stories, the ordinary and the supersingular one:

### § 2.1. The Ordinary Case

On the analytic side, Mazur and Swinnerton-Dyer defined in [12] a $p$-adic $L$-function $L_p(E, X) \in \Lambda \otimes \mathbb{Q}$ in the early 1970s which conjecturally lives in the Iwasawa algebra, i.e. we should have $L_p(E, X) \in \Lambda$. 
On the \textit{algebraic} side, we have the following exact sequence (see e.g. [20]):

$$0 \to E(\mathbb{Q}_n) \otimes \mathbb{Q}/\mathbb{Z} \to \text{Sel}(E/\mathbb{Q}_n) \to \text{III}(E/\mathbb{Q}_n) \to 0.$$  

$E(\mathbb{Q}_n)$ is the Mordell-Weil group of $\mathbb{Q}_n$-rational points of $E$, which is in general hard to understand. Galois cohomology provides us with a tool that lets us define a simpler object, the Selmer group $\text{Sel}(E/\mathbb{Q}_n)$ into which $E(\mathbb{Q}_n)$ injects - after tensoring away the torsion points. A folklore conjecture says that the cokernel III of this injection, the Tate-Shafarevich group, has finite size.

Looking at the $p$-part (i.e. $p$-primary part) of the above exact sequence gives us a slightly simpler one:

$$0 \to E(\mathbb{Q}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}_p(E/\mathbb{Q}_n) \to \text{III}(E/\mathbb{Q}_n)[p^\infty] \to 0.$$  

Going up the cyclotomic tower, the rank of $E(\mathbb{Q}_n)$ is known to stabilize via work of Rohrlich [17] and Kato [5]. We denote it by $r_\infty$. An amenable algebraic object for Iwasawa theory which contains information about $E(\mathbb{Q}_\infty)$ is then the Pontryagin dual of the $p$-Selmer group

$$\mathcal{X} := \varprojlim_n \text{Hom}(\text{Sel}_p(E/\mathbb{Q}_n), \mathbb{Q}_p/\mathbb{Z}_p),$$  

which has the structure of a $\Lambda$-module as it is a $\mathbb{Z}_p$-module which admits a continuous action of $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ - but what makes this object truly nice is that when $p$ is ordinary, $\mathcal{X}$ is a finitely generated torsion $\Lambda$-module. (This does not hold when $p$ is supersingular, in which case $\mathcal{X}$ is still finitely generated, but not $\Lambda$-torsion.) Mazur conjectured this nice property in the 1970s, which is now a result by Rubin [18] (in the CM case) and Kato [5] (in the non-CM case). It is this fact that allows us to define $\text{Char}_\Lambda(\mathcal{X})$ and extract its Iwasawa invariants $\mu$ and $\lambda$. The following is a classical theorem that goes back to Mazur\footnote{Mazur’s version of Theorem 2.2 is that as a function of $n$, $e_n = \mu p^n + n(\lambda - r_\infty) + O(1)$.}:[11]:

**Theorem 2.2.** (see e.g. [3, Theorem 1.10] Let $p$ be ordinary. Assume that $\#\text{III}(E/\mathbb{Q}_n)[p^\infty] = p^{e_n} < \infty$. Then for $n \gg 0$, we have

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

This theorem is an analogue of a result by Iwasawa concerning the $p$-part of class numbers in $\mathbb{Z}_p$-extensions, which one may say started Iwasawa theory in the first place.

The Main Conjecture links the two objects:

**Main Conjecture 2.1.** The following ideals are equal:

$$(L_p(E, X)) = \text{Char}_\Lambda(\mathcal{X}) \subset \Lambda.$$
That \( L_p(E, X) \in \text{Char}_\lambda(X) \) is a result by Kato (see [3]) when the \( p \)-adic representation \( \text{Gal}({\overline{\mathbb{Q}}}/\mathbb{Q}) \to \text{GL}_{\mathbb{Z}_p}(T_p(E)) \) on the automorphism group of the \( p \)-adic Tate module \( T_p(E) \) is surjective. Skinner and Urban have announced a proof for the other inclusion under certain assumptions, cf. [21].

**Remark 2.2.** Greenberg and Vatsal show in [4] that \( L_p(E, X) \in \Lambda \) in some cases. In the supersingular case, the main conjecture can be formulated using (two copies of) the Iwasawa algebra \( \Lambda \).

**Sketch of Kato’s Method.** Denote by \( T_p(E) := \varprojlim E[p^n] \) the \( p \)-adic Tate-module, i.e. the inverse limit of the \( p \)-power torsion points of \( E \), and by \( \mathbb{Q}_{n,p} \) the completion of \( \mathbb{Q}_n \) in the \( p \)-adic topology. The main part of Kato’s method is to construct an Euler system called *Kato’s zeta element* which lives in global cohomology. It is this Euler system that brings the two mathematically faraway worlds mentioned at the very beginning of this article together! See for example [19] for details. One of the important properties of Kato’s Euler system is that it induces the special element \( z \) in the (local) cohomology group below, whose image under a certain map \( \text{Col} \) becomes the \( p \)-adic \( L \)-function of Mazur and Swinnerton-Dyer:

\[
\mathbb{Q} \otimes \varprojlim_n H^1(\mathbb{Q}_{n,p}, T_p(E)) \xrightarrow{\text{Col}} \mathbb{Q} \otimes \Lambda \\
\downarrow \quad \downarrow \\
z \mapsto L_p(E, X)
\]

**§ 2.2. The Supersingular Case**

In the supersingular case, the two roots \( \alpha \) and \( \bar{\alpha} \) of the Hecke polynomial \( Y^2 - a_pY + p \) have positive \( p \)-adic valuation. This causes problems on both the analytic and the algebraic sides:

**2.2.1. The Analytic Side.** On the analytic side, Amice and Vélu [1] and Višik [25] constructed two \( p \)-adic \( L \)-functions \( L_{p,\alpha}(E, X) \) and \( L_{p,\bar{\alpha}}(E, X) \) generalizing Mazur’s and Swinnerton-Dyer’s \( L_p(E, X) \). The *problem* in this case is that the ring in which their functions live is too big:

\[
L_{p,\alpha}(E, X), L_{p,\bar{\alpha}}(E, X) \not\in \Lambda,
\]

since they have infinitely many zeros in the unit disk, which would for example contradict the \( p \)-adic Weierstrass Preparation Theorem.

---

\(^2\text{(Kato, ICM 2006) 加藤和也先生のたとえによると，ゼータ元} \ \text{が既報に登場，} L_p(E, X) \ \text{は恩返しの綴錦の一部，解析的対象である Hasse-Weil} L \ \text{関数} L(E, s) \ \text{は錦である。[6]。)}\)
A hint on what to do was a guess by Greenberg [2], namely that

\[ (*) \quad L_{p,\alpha}(E, X) \text{ and } L_{p,\overline{\alpha}}(E, X) \text{ have finitely many common zeros. } \]

The following theorems resolve this problem.

**Theorem 2.3.** (Pollack [15], 2003) Let \( a_p = 0 \). Then there are two \( p \)-adic \( L \)-functions \( L_p^\sharp(E, X) \in \Lambda \) and \( L_p^\flat(E, X) \in \Lambda \) so that

\[
L_{p,\alpha}(E, X) = L_p^\sharp(E, X) \log^+(1 + X) + L_p^\flat(E, X) \log^-(1 + X) \alpha
\]

\[
L_{p,\overline{\alpha}}(E, X) = L_p^\sharp(E, X) \log^+(1 + X) + L_p^\flat(E, X) \log^-(1 + X) \overline{\alpha},
\]

where \( \log^+_p(1 + X) = \frac{1}{p} \prod_{n \geq 1} \frac{\Phi_{2n}}{p} \) and \( \log^-_p(1 + X) = \frac{1}{p} \prod_{n \geq 1} \frac{\Phi_{2n-1}}{p} \), and

\( \Phi_m := \sum_{i=0}^{p-1} (1+X)^{p^{m-1}i} \) is the \( pm \)-th cyclotomic polynomial for the variable \( 1+X \).

We point out that Pollack’s theorem covers almost all supersingular primes, since \( p|a_p \) and \( p \geq 5 \) imply \( a_p = 0 \) by the Hasse-Weil bound \( |a_p| < 2\sqrt{p} \).

**Theorem 2.4.** (S. [22], 2011) Let \( p|a_p \). Then there are two \( p \)-adic \( L \)-functions \( L_p^\sharp(E, X) \in \Lambda \) and \( L_p^\flat(E, X) \in \Lambda \) so that:

\[
(L_{p,\alpha}(E, X), L_{p,\overline{\alpha}}(E, X)) = (L_p^\sharp(E, X), L_p^\flat(E, X)) \mathcal{L}og_{a_p}(X),
\]

where we define the following limit of products of matrices:

\[
\mathcal{L}og_{a_p}(X) := \lim_{n \rightarrow \infty} \left( \begin{array}{ccc}
a_p & -1 & 0 \\
a_p & -1 & 0 \\
p & 0 & 0
\end{array} \right)^{-n} \left( \frac{-1}{\alpha} \frac{-1}{\alpha} \right).
\]

The two pairs of \( p \)-adic \( L \)-functions \( L_p^\sharp(E, X), L_p^\flat(E, X) \) agree in both theorems (since we are assuming that \( p \) is odd).

**Corollary 2.5.** Greenberg’s guess (*) above is right.

**Proof.** This follows from using the \( p \)-adic Weierstrass Preparation Theorem. See [24]. QED

2.2.2. **The Algebraic Side.** On the algebraic side, we can still define the exact sequences and objects as in the ordinary case, but the problem is that the dual of the \( p \)-Selmer group of \( \mathbb{Q}_\infty \) is not \( \Lambda \)-torsion (although it is finitely generated):

\( \mathcal{X} \) is not a torsion \( \Lambda \)-module !!

A hint in this case is a growth formula for the Tate-Shafarevich group conjectured by Kurihara and first presented at this conference ten years ago:
Conjecture 2.3.  (Kurihara [9], 2000) Let \( p \geq 5 \) be supersingular. Assume that 
\[ \# \mathrm{III}(E/\mathbb{Q}_{n})[p^{\infty}] = p^{e_{n}} < \infty. \]
Then there are integers \( \lambda, \tau^{d}, \) and \( \tau^{b} \) so that for \( n \gg 0, \)
\[ e_{n} - e_{n-1} = \lambda + \begin{cases} q_{n}^{d} + \tau^{d} & \text{for odd } n, \\ q_{n}^{b} + \tau^{b} & \text{for even } n, \end{cases} \]
where \( q_{n}^{d} := p^{n-1} - p^{n-2} + \cdots + p - 1. \)

(This conjecture is a slightly stronger modification of the original one in [9]. Kurihara’s \( \lambda \) satisfies \( \lambda + \frac{1}{2} = \lambda \), which is assumed to be a rational number. Only after making the slightly stronger assumption that \( \lambda \) is integral can we state his conjecture as above, where we distinguish between even and odd \( n \), by introducing the two adjustment constants \( \tau^{d} \) and \( \tau^{b} \).)

Kurihara proved his conjecture [8] under assumptions that were strong enough to force \( \lambda = \tau^{d} = \tau^{b} = 0 \). This theorem was generalized by Kurihara and Otsuki [10] who worked with the prime 2, and a very big hint on what to do was given by Perrin-Riou in [14], who generalized Kurihara’s work and gave a formula for \( e_{n} \) (that covered almost all cases\(^3\)) with unspecified pairs of invariants, which she suggestively called \( \mu_{\pm} \) and \( \lambda_{\pm} \).

This hint and the results on the analytic side suggest that there should be two algebraic objects as well, which work in tandem to make the Tate-Shafarevich group grow\(^4\).

This is the content of the following theorem:

Theorem 2.6.  (Kobayashi [7] for \( a_{p} = 0 \) 2003, S. [22] for \( p|a_{p} \) 2011) Let \( p|a_{p} \).
Then there are maps \( \mathrm{Col}^{d}, \mathrm{Col}^{b} \) that send Kato’s zeta element to the \( p \)-adic \( L \)-functions \( L^{d}_{p}(E, X) \) and \( L^{b}_{p}(E, X) \):
\[
\lim_{n} H^{1}(\mathbb{Q}_{n, p}, T_{p}(E)) \xrightarrow{(\mathrm{Col}^{d}, \mathrm{Col}^{b})} \Lambda^{\oplus 2} \xrightarrow{\Lambda} (L^{d}_{p}(E, X), L^{b}_{p}(E, X))
\]

The kernels \( \ker \mathrm{Col}^{d/b} \) give rise to Selmer groups \( \chi^{d/b} \) that are finitely generated torsion as \( \Lambda \)-modules. The (tandem) main conjecture then becomes

Main Conjecture 2.4.  ([7],[22]) The following ideals are equal:
\[
(L^{d}_{p}(E, X)) = \mathrm{Char}_{\Lambda}(\chi^{d}) \subset \Lambda, \text{ and } \]

\(^3\)See Section 5 in [23] for a detailed discussion. We also have two historical remarks. Firstly, similar formulas had been announced by Anas Nasybullin in [13], but without any proofs. Secondly, the reason that the title of [8] is numbered as part I was that similar results had also been obtained by Kurihara - to be published in a part II.

\(^4\)ですので超特異な素数の場合、娘が二番の縄縄を繋ってくるはずです。
\[(L_p^b(E, X)) = \text{Char}_\Lambda(\mathcal{X}^b) \subset \Lambda.\]

The inclusions \((L_p^{\#b}(E, X)) \subset \text{Char}_\Lambda(\mathcal{X}^{\#b})\) follow from Kato’s methods in [5] when the \(p\)-adic representation \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_{\mathbb{Z}_p}(T_p(E))\) on the automorphism group of the \(p\)-adic Tate module \(T_p(E)\) is surjective. The other inclusion is known when \(E\) has complex multiplication (see [16]), but unknown in general.

Now denote the Iwasawa invariants of \(\mathcal{X}^{\#b}\) by \(\mu_{\#b}\) and \(\lambda_{\#b}\), and the rank of \(E(\mathbb{Q}_\infty)\) (which is finite even in the supersingular case, cf. Rohrlich [17] and Kato [5]) by \(r_\infty\).

**Theorem 2.7.** (Kobayashi [7], 2003) Let \(a_p = 0\). Assume that \(#\text{III}(E/\mathbb{Q}_n)[p^\infty] = p^{e_n} < \infty\). Then for \(n \gg 0\), we have

\[
e_n - e_{n-1} = \begin{cases} 
\mu_2(p^n - p^{n-1}) + \lambda_2 - r_\infty + q_n^b & \text{when } n \text{ is odd,} \\
\mu_b(p^n - p^{n-1}) + \lambda_b - r_\infty + q_n^b & \text{when } n \text{ is even.}
\end{cases}
\]

Here, the integers \(q_n^b\) come from values of Pollack’s half-logarithms \(\log_{p^b}^+\) at \(p\)-power roots of unity. But when one includes the case \(a_p \neq 0\), it is not these half-logarithms, but four entries appearing in the definition of \(\text{Log}_{a_p}\) that play a role. The valuation of \(a_p\) can then be so small that there are cases when the growth of \(\text{III}(E/\mathbb{Q}_n)[p^\infty]\) is only controlled by one of the two pairs of Iwasawa invariants:

**Theorem 2.8.** (S. [23]) Let \(p|a_p\). Assume that \(#\text{III}(E/\mathbb{Q}_n)[p^\infty] = p^{e_n} < \infty\). Then for \(n \gg 0\), we have \(e_n - e_{n-1} = \)

\[
\begin{cases} 
\mu_2(p^n - p^{n-1}) + \lambda_2 - r_\infty + \frac{q_n^2}{q_n^{n+1}} & \text{for odd } n \\
\mu_b(p^n - p^{n-1}) + \lambda_b - r_\infty + \frac{q_n^b}{q_n^{n+1}} & \text{for even } n
\end{cases}
\]

Perrin-Riou’s invariants \(\mu_\pm\) and \(\lambda_\pm\) can be explained in terms of the pairs of Iwasawa invariants \(\mu_{\#b}\) and \(\lambda_{\#b}\). For a precise discussion, see [23, Section 5].

We end this article with two open questions.

It is natural to ask how the \(l\)-part behaves, i.e. how fast \(l^{e'_n} := #\text{III}(E/\mathbb{Q}_n)[l^\infty]\) grows for a prime \(l \neq p\). That the \(l\)-part should stay constant is a folklore conjecture, but seems to not have been written up yet:

**Conjecture 2.5.** Let \(l \neq p\) be a prime of good reduction and assume that \(#\text{III}(E/\mathbb{Q}_n)[l^\infty]\) is finite. Choose \(e'_n\) so that \(l^{e'_n} = #\text{III}(E/\mathbb{Q}_n)[l^\infty]\). Then for \(n \gg 0\), we have

\[e'_n - e'_{n-1} = 0.\]
Another general philosophy is that III is as small as possible, which gives an intuitive explanation of Theorem 2.8: When presented with two $\mu$-invariants, III chooses the smaller one: III is modest! In view of Kurihara’s Conjecture 2.3 above, we make the following conjecture:

**Conjecture 2.6.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at an odd prime $p$ with Iwasawa invariants as above. Then

$$\min(\mu_2, \mu_3) = 0.$$ 

**Acknowledgments.** We would like to thank the organizers for a wonderful conference, and Shinichi Kobayashi for inviting the author to speak. We also thank the anonymous referee for helpful comments.

**References**


