RIMS Kôkyûroku Bessatsu
B32 (2012), 51–60

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

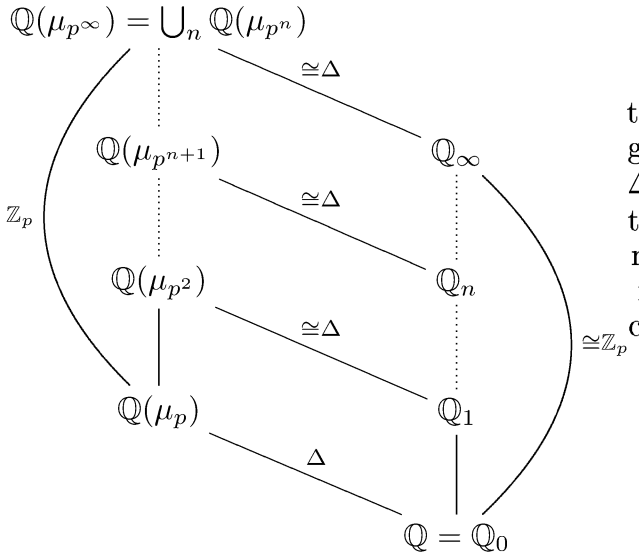
Iwasawa theory is a mysterious bridge between two mathematically faraway worlds, the analytic realm and the algebraic realm:

$$(analytic) \qquad \underleftrightarrow{\text{Iwasawa theory}} \qquad (algebraic)$$

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

Received April 1, 2011. Revised March 21, 2012.
2000 Mathematics Subject Classification(s): 2000 Mathematics Subject Classification(s):
Key Words: *Key Words*: Elliptic Curves, Tate-Shafarevich Groups, Iwasawa Theory
*Brown University, Providence, RI 02912, USA.
e-mail: ian.sprung@gmail.com

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 $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \Delta$.



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 *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 $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$ acts continuously on M, then M becomes a $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$-module. This ring Λ is called the *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 *Iwasawa Main Conjecture* usually states that the ideal generated in Λ by an analytic object, a p-adic L-function $L_p(X) \in \Lambda$, is equal to the *characteristic ideal* of an algebraic object:

$$\begin{array}{cc} (analytic) & (algebraic) \\ \Lambda & \Lambda \\ \cup & \cup \\ (L_p(X)) & = \mathrm{Char}_\Lambda(M) \end{array}$$

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 $\mathrm{Char}_\Lambda(M)$? We can only define this when M is a finitely generated torsion Λ-module. Before that, let's look at a baby example where we replace the ring Λ 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 *characteristic ideal*:

$$\mathrm{Char}_\mathbb{Z} G := (|G|) = (\prod_i p_i^{e_i}) \subset \mathbb{Z}.$$

Now suppose M is a finitely generated torsion Λ-module. It turns out that M then admits an exact sequence

$$0 \to \bigoplus_i \Lambda/f_i\Lambda \to M \to (finite) \to 0,$$

where we have chosen f_i so that $f_i | f_{i+1}$. These f_i are not uniquely determined, but the ideal that their product generates in Λ is. This is our characteristic ideal:

$$\mathrm{Char}_\Lambda(M) := (\prod_i f_i) \subset \Lambda.$$

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 μ, λ 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 Λ-module M, the integers μ and λ of the generator of $\mathrm{Char}_\Lambda(M)$ as above are called the *Iwasawa invariants* of M.

For proofs of all the above, we refer the reader to Washington's book on cyclotomic fields [26].

§ 2. Iwasawa Theory for Elliptic Curves

The idea of formulating an Iwasawa theory for elliptic curves by looking at their $\mathbb{Q}_n$-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 *algebraic* side, we have the following exact sequence (see e.g. [20]):

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

$E(\mathbb{Q}_n)$ 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 $\mathrm{Sel}(E/\mathbb{Q}_n)$ into which $E(\mathbb{Q}_n)$ injects - after tensoring away the torsion points. A folklore conjecture says that the cokernel Ш 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:

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

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_∞. 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

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

which has the structure of a Λ-module as it is a $\mathbb{Z}_p$-module which admits a continuous action of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ - but what makes this object truly nice is that *when p is ordinary*, $\mathcal{X}$ is a finitely generated torsion Λ-module. (This does not hold when p is supersingular, in which case $\mathcal{X}$ is still finitely generated, but not Λ-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 $\mathrm{Char}_\Lambda(\mathcal{X})$ and extract its Iwasawa invariants μ and λ. The following is a classical theorem that goes back to Mazur[1][11]:

Theorem 2.2. *(see e.g. [3, Theorem 1.10] Let p be ordinary. Assume that $\#Ш(E/\mathbb{Q}_n)[p^\infty] = p^{e_n} < \infty$. 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:*

$$(L_p(E, X)) = \mathrm{Char}_\Lambda(\mathcal{X}) \subset \Lambda.$$

[1]Mazur's version of Theorem 2.2 is that as a function of n, $e_n = \mu p^n + n(\lambda - r_\infty) + O(1)$.

That $L_p(E,X) \in \mathrm{Char}_\Lambda(\mathcal{X})$ is a result by Kato (see [5]) when the p-adic representation $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\mathbb{Z}_p}(T_p(E))$ 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 Λ.

Sketch of Kato's Method. Denote by $T_p(E) := \varprojlim_n E[p^n]$ 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 $\mathbf{z}$ in the (local) cohomology group below, whose image under a certain map Col becomes the p-adic L-function of Mazur and Swinnerton-Dyer[2]:

$$\begin{array}{ccc} \mathbb{Q} \otimes \varprojlim_n H^1(\mathbb{Q}_{n,p}, T_p(E)) & \xrightarrow{\mathrm{Col}} & \mathbb{Q} \otimes \Lambda \\ \cup & & \cup \\ \mathbf{z} & \mapsto & L_p(E,X) \end{array}$$

§ 2.2. The Supersingular Case

In the supersingular case, the two roots α and $\overline{\alpha}$ of the Hecke polynomial $Y^2 - a_p Y + p$ 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 $L_{p,\overline{\alpha}}(E,X)$ 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:

$$L_{p,\alpha}(E,X), L_{p,\overline{\alpha}}(E,X) \notin \Lambda,$$

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

[2](Kato, ICM 2006) 加藤和也先生のたとえによると、ゼータ元 $\mathbf{z}$ が娘、$L_p(E,X)$ は恩返しの綾錦の一部、解析的対象である Hasse-Weil L 関数 $L(E,s)$ は鶴である。[6]。

A *hint* on what to do was a guess by Greenberg [2], namely that

(*) $L_{p,\alpha}(E,X)$ and $L_{p,\overline{\alpha}}(E,X)$ 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*

$$L_{p,\alpha}(E,X) = L_p^\sharp(E,X)\log_p^+(1+X) + L_p^\flat(E,X)\log_p^-(1+X)\alpha$$

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

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 p^m-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 :*

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

where we define the following limit of products of matrices:

$$\mathcal{L}og_{a_p}(X) := \lim_{n\to\infty}\begin{pmatrix} a_p & -1 \\ \Phi_1 & 0\end{pmatrix}\cdots\begin{pmatrix} a_p & -1 \\ \Phi_n & 0\end{pmatrix}\begin{pmatrix} a_p & -1 \\ p & 0\end{pmatrix}^{-(n+2)}\begin{pmatrix} -1 & -1 \\ \overline{\alpha} & \alpha\end{pmatrix}.$$

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 Λ-torsion (although it is finitely generated):

$$\mathcal{X} \text{ is not a torsion } \Lambda\text{-module !!}$$

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 $\#Ш(E/\mathbb{Q}_n)[p^\infty] = p^{e_n} < \infty$. Then there are integers $\lambda, \tau^\sharp$, and $\tau^\flat$ so that for $n \gg 0$,*

$$e_n - e_{n-1} = \lambda + \begin{cases} q_n^\sharp + \tau^\sharp \text{ for odd } n, \text{ and} \\ q_n^\flat + \tau^\flat \text{ for even } n, \end{cases}$$

where $q_n^\sharp := p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p^2 - p$ and $q_n^\flat := p^{n-1} - p^{n-2} + \cdots + p - 1$.

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

Kurihara proved his conjecture [8] under assumptions that were strong enough to force $\lambda = \tau^\sharp = \tau^\flat = 0$. 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 $\mathrm{Col}^\sharp, \mathrm{Col}^\flat$ that send Kato's zeta element to the p-adic L-functions $L_p^\sharp(E,X)$ and $L_p^\flat(E,X)$:*

$$\begin{array}{ccc} \varprojlim_n H^1(\mathbb{Q}_{n,p}, T_p(E)) & \xrightarrow{(\mathrm{Col}^\sharp, \mathrm{Col}^\flat)} & \Lambda^{\oplus 2} \\ \cup & & \cup \\ \mathbf{z} & \mapsto & (L_p^\sharp(E,X), L_p^\flat(E,X)) \end{array}$$

The kernels $\ker \mathrm{Col}^{\sharp/\flat}$ give rise to Selmer groups $\mathcal{X}^{\sharp/\flat}$ that are **finitely generated torsion as Λ-modules.** The (tandem) main conjecture then becomes

Main Conjecture 2.4. *([7],[22]) The following ideals are equal:*

$$(L_p^\sharp(E,X)) = \mathrm{Char}_\Lambda(\mathcal{X}^\sharp) \subset \Lambda, \text{ and}$$

[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**二着**の綾錦を織ってくれるはずです。

$$(L_p^{\flat}(E,X)) = \mathrm{Char}_{\Lambda}(\mathcal{X}^{\flat}) \subset \Lambda.$$

The inclusions $(L_p^{\sharp/\flat}(E,X)) \subset \mathrm{Char}_{\Lambda}(\mathcal{X}^{\sharp/\flat})$ follow from Kato's methods in [5] when the p-adic representation $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{\mathbb{Z}_p}(T_p(E))$ 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 $\mathcal{X}^{\sharp/\flat}$ by $\mu_{\sharp/\flat}$ and $\lambda_{\sharp/\flat}$, and the rank of $E(\mathbb{Q}_\infty)$ (which is finite even in the supersingular case, cf. Rohrlich [17] and Kato [5]) by r_∞.

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

$$e_n - e_{n-1} = \begin{cases} \mu_\sharp(p^n - p^{n-1}) + \lambda_\sharp - r_\infty + q_n^\sharp & \text{when } n \text{ is odd,} \\ \mu_\flat(p^n - p^{n-1}) + \lambda_\flat - r_\infty + q_n^\flat & \text{when } n \text{ is even.} \end{cases}$$

Here, the integers $q_n^\sharp$ and $q_n^\flat$ come from values of Pollack's half-logarithms $\log_p^+$ and $\log_p^-$ 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 $\mathcal{L}og_{a_p}$ that play a role. The valuation of a_p can then be so small that there are cases when the growth of $Ш(E/\mathbb{Q}_n)[p^\infty]$ is only controlled by *one* of the two pairs of Iwasawa invariants:

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

$$\begin{cases} \text{(the above formula of Kobayashi)} & \text{when } a_p = 0 \text{ or } \mu_\sharp = \mu_\flat, \\ \mu_\sharp(p^n - p^{n-1}) + \lambda_\sharp - r_\infty + \begin{cases} q_n^\sharp & \text{for odd } n \\ q_{n+1}^\sharp & \text{for even } n \end{cases} & \text{when } \mu_\sharp < \mu_\flat \text{ and } a_p \neq 0, \\ \mu_\flat(p^n - p^{n-1}) + \lambda_\flat - r_\infty + \begin{cases} q_{n+1}^\flat & \text{for odd } n \\ q_n^\flat & \text{for even } n \end{cases} & \text{when } \mu_\flat < \mu_\sharp \text{ and } a_p \neq 0, \end{cases}$$

Perrin-Riou's invariants $\mu_\pm$ and $\lambda_\pm$ can be explained in terms of the pairs of Iwasawa invariants $\mu_{\sharp/\flat}$ and $\lambda_{\sharp/\flat}$. 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 $l^{e'_n} := \#Ш(E/\mathbb{Q}_n)[l^\infty]$ 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 $\#Ш(E/\mathbb{Q}_n)[l^\infty]$ is finite. Choose e'_n so that $l^{e'_n} = \#Ш(E/\mathbb{Q}_n)[l^\infty]$. Then for $n \gg 0$, we have*

$$e'_n - e'_{n-1} = 0.$$

Another general philosophy is that Ш is as small as possible, which gives an intuitive explanation of Theorem 2.8: When presented with two μ-invariants, Ш chooses the smaller one: Ш *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*

$$\min(\mu_\sharp, \mu_\flat) = 0.$$

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

[1] Amice, Y. and Vélu, J., *Distributions p-adiques associées aux séries de Hecke*, in Journées Arithmétiques de Bordeaux (Bordeaux, 1974), Astérisque **24-25**, Société Mathématique de France, Montrogue, 1975, 119-131.

[2] Greenberg, R., *Iwasawa theory - past and present*, Class field theory—its centenary and prospect, Tokyo, 1998, Advanced Studies in Pure Mathematics, Mathematical Society of Japan, Tokyo, **30** (2001), 335-385.

[3] Greenberg, R., *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves, Cetraro, 1997, Lecture Notes in Mathematics, **1716** (1999), 51-144, Springer, Berlin.

[4] Greenberg, R. and Vatsal, V., *On the Iwasawa invariants of elliptic curves*, Inventiones Mathematicae **142** (2000), no. 1, 17-63.

[5] Kato, K., *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117-290.

[6] Kato, K., 岩澤理論の発展, see e.g. www.mm.sophia.ac.jp/~shinoda/msj/pdffiles/kato.pdf.

[7] Kobayashi, S., *Iwasawa theory for elliptic curves at supersingular primes*, Inventiones Mathematicae **152** (2003), no.1, 1-36.

[8] Kurihara, M., *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Inventiones Mathematicae **149** (2002), 195-224.

[9] Kurihara, M., *The Iwasawa theory of elliptic curves that have supersingular reduction*, Algebraic number theory and related topics, Kyoto, 2000, Surikaisekikenkyusho Kokyuroku **1154** (2000), 33-43.

[10] Kurihara, M. and Otsuki, R., *On the growth of Selmer groups of an elliptic curve with supersingular reduction in the $\mathbb{Z}_2$-extension of $\mathbb{Q}$*, Pure and Applied Mathematics Quarterly **2** (2006), no. 2, part 2, 557-568.

[11] Mazur, B., *Rational points of abelian varieties with values in towers of number fields*, Inventiones Mathematicae **18** (1972), 183-266.

[12] Mazur, B. and Swinnerton-Dyer, P., *Arithmetic of Weil curves*, Inventiones Mathematicae **25** (1974), 1-61.

[13] Nasybullin, A., Elliptic curves with supersingular reduction over Γ-extensions (Russian), Uspehi Matematicheskih Nauk **32 (194)** (1977), 221-222.

[14] Perrin-Riou, B., *Arithmétique des courbes elliptiques à réduction supersingulière*, Experimental Mathematics, 2003.
[15] Pollack, R., *The p-adic L-function of a modular form at a supersingular prime*, Duke Mathematical Journal **118** (2003), no.3, 523-558.
[16] Pollack, R. and Rubin, K., *The main conjecture for CM elliptic curves at supersingular primes*, Annals of Mathematics **159**, no.1 (2004), 447-464.
[17] Rohrlich, D. E., *On L-functions of elliptic curves and cyclotomic towers*, Inventiones Mathematicae **75** (1984), 409 - 423.
[18] Rubin, K., *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Inventiones Mathematicae **93** (1988), 701-713.
[19] Scholl, A. J., *An introduction to Kato's Euler systems*, in Galois representations in arithmetic algebraic geometry (Durham, 1996), 379-460, London Mathematical Society Lecture Note Series **254** (1998), Cambridge University Press, Cambridge.
[20] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106** (1992), Springer, New York.
[21] Skinner, C. and Urban, E., *The Main Conjectures for $GL(2)$*, submitted; available at math.columbia.edu/∼urban/eurp/MC.pdf.
[22] Sprung, F., *Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures*, the Journal of Number Theory **132** (July 2012).
[23] Sprung, F., *The Šafarevič-Tate group of an elliptic curve in cyclotomic $\mathbb{Z}_p$-extensions at supersingular primes*, to appear in Crelle's Journal.
[24] Sprung, F., in preparation.
[25] Višik, M. M., *Nonarchimedean measures associated with Dirichlet series*, Matematičeskii Sbornik **99 (141)**, no. 2 (1976), pp. 248-260, 296.
[26] Washington, L., *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83** (1980), Springer, New York.