Pure and Applied Mathematics Quarterly
Volume 2, Number 2
(*Special Issue: In honor of
John H. Coates, Part 2 of 2*)
557—568, 2006

On the Growth of Selmer Groups of an Elliptic Curve with Supersingular Reduction in the $\mathbf{Z}_2$-extension of Q

Masato Kurihara and Rei Otsuki

0. Introduction

Let E be an elliptic curve defined over $\mathbf{Q}$. If E has good ordinary reduction at a prime p, the growth of Tate-Shafarevich groups (and Selmer groups) of E in a $\mathbf{Z}_p$-extension can be understood by usual Iwasawa theory. But if E has supersingular reduction at p, the growth of Selmer and Tate-Shafarevich groups is more complicated. For an odd prime p, the most basic case was dealt with in [6] where the main assumption was that p does not divide the L-value $L(E,1)/\Omega_E$ (where Ω_E is the Néron period). The aim of this paper is to study the case $p=2$ under the same assumption on the L-value, namely $2 \not| L(E,1)/\Omega_E$.

For a prime number p, we consider the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$ whose n-th layer we denote by $\mathbf{Q}_n$, namely $\mathbf{Q}_n$ is the intermediate field with $[\mathbf{Q}_n : \mathbf{Q}] = p^n$. For an odd p, the condition $p \not| L(E,1)/\Omega_E$ implies $\operatorname{rank} E(\mathbf{Q}_\infty) = 0$ (see [6]), but for $p=2$ this does not hold. We will see that for $p=2$ the condition $p=2 \not| L(E,1)/\Omega_E$ would imply that the Selmer groups over $\mathbf{Q}_n$ always have positive corank for $n \geq 1$, hence would imply $\operatorname{rank} E(\mathbf{Q}_n) > 0$ if we assume the Birch and Swinnerton-Dyer conjecture (see Corollary 1.2). So the situation is different.

As usual, put $a_p = p + 1 - \#E(\mathbf{F}_p)$. In the following, we suppose $p=2$ and E has good supersingular reduction at 2. When $a_2 = 0$, we have two nice Iwasawa functions which describe the p-adic L-function of E by Pollack [11], and we can define $\pm$ Selmer groups as in Kobayashi [5], and can study them by the same method as for $p > 2$. In this paper, we consider the case $a_2 \neq 0$ (so $a_2 = \pm 2$). Let $\mathrm{Sel}(E/\mathbf{Q}_n)$ be the Selmer group of E over $\mathbf{Q}_n$ of $E[2^\infty]$ (cf. 2.1). We will determine the Galois module structure (and the structure as an abelian group) of $\mathrm{Sel}(E/\mathbf{Q}_n)$ completely in the case $a_2 = \pm 2$ under the assumption

Received August 18, 2005.

$2 \nmid L(E,1)/\Omega_E$, in particular $\mathrm{Sel}(E/\mathbf{Q}_n)$ is of corank 1. (When $a_2 = 0$, the condition $2 \nmid L(E,1)/\Omega_E$ does not determine the structure of $\mathrm{Sel}(E/\mathbf{Q}_n)$ as an abelian group (see Remark 0.2 (3)).)

Our main assumption is just $2 \nmid L(E,1)/\Omega_E$. If the Birch and Swinnerton-Dyer conjecture is true, this would imply that 2 does not divide the Tamagawa factor $\mathrm{Tam}(E) = \Pi c_\ell = \Pi(E(\mathbf{Q}_\ell) : E_0(\mathbf{Q}_\ell))$ (where $E_0(\mathbf{Q}_\ell)$ is the subgroup consisting of points whose images in $E(\mathbf{F}_\ell)$ are nonsingular.) We will prove

Theorem 0.1. *Let E be an elliptic curve defined over $\mathbf{Q}$ with supersingular reduction at 2, and $L(E,s)$ be the L-function of E. We assume that $a_2 \neq 0$, namely $a_2 = \pm 2$, and*

$$\mathrm{ord}_2(L(E,1)/\Omega_E) = \mathrm{ord}_2(\mathrm{Tam}(E)) = 0$$

where $\mathrm{ord}_2 : \mathbf{Q}^\times \longrightarrow \mathbf{Z}$ is the normalized additive valuation at 2. Then,

(1) *For any $n \geq 0$, let $\theta_{\mathbf{Q}_n}$ be the modular element of Mazur and Tate (see §1, 1.2 for the definition). Suppose $n \geq 1$. Let $\nu : \mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_{n-1}/\mathbf{Q})] \longrightarrow \mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$ denote the $\mathbf{Z}_2$-homomorphism defined by $\sigma \mapsto \Sigma\tau$ for $\sigma \in \mathrm{Gal}(\mathbf{Q}_{n-1}/\mathbf{Q})$ where τ ranges over all elements of $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$ projecting to σ. Then, the Pontrjagin dual $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ of the Selmer group over $\mathbf{Q}_n$ of $E[2^\infty]$ is isomorphic to*

$$\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]/(\theta_{\mathbf{Q}_n}, \nu(\theta_{\mathbf{Q}_{n-1}}))$$

as a $\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$-module.

(2) *For $n \geq 2$, put*

$$q_n = \sum_{k=0}^{n-1} (-1)^k 2^{n-1-k}.$$

Then, we have $\mathrm{Sel}(E/\mathbf{Q}) = 0$, $\mathrm{Sel}(E/\mathbf{Q}_n) \simeq \mathbf{Q}_2/\mathbf{Z}_2$ for $n = 1, 2$ as an abelian group, and

$$\mathrm{Sel}(E/\mathbf{Q}_n) \simeq \mathbf{Q}_2/\mathbf{Z}_2 \oplus (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3-q_2} \oplus (\mathbf{Z}/2^{n-3}\mathbf{Z})^{q_4-q_3} \oplus \ldots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n-q_{n-1}}$$

for all $n \geq 3$. Hence, if we assume the finiteness of the 2-primary component $Ш(E/\mathbf{Q}_1)\{2\}$ of the Tate-Shafarevich group of $E/\mathbf{Q}_1$, we have

$$\mathrm{rank}\, E(\mathbf{Q}_n) = 1 \quad \textit{for all } n \geq 1,$$

$$Ш(E/\mathbf{Q}_1)\{2\} = Ш(E/\mathbf{Q}_2)\{2\} = 0, \textit{ and}$$

$$Ш(E/\mathbf{Q}_n)\{2\} \simeq (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3-q_2} \oplus \ldots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n-q_{n-1}}$$

for all $n \geq 3$.

(3) $\mathrm{Sel}(E/\mathbf{Q}_\infty)^\vee \simeq \mathbf{Z}_2[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$.

Remark 0.2. (1) There are many examples satisfying the conditions of Theorem 0.1. For example, $E = X_0(11)$ gives a typical example where $a_2 = -2$. Other examples are 67A, 75A, 75C, 99D, 115A, 141E, 147B, 147C, 179A, 187B, 189D, 195B, 195C, 195D,... in the notation of Cremona [3]. It is interesting that the simple conditions in Theorem 0.1 determine the structure of $\mathrm{Sel}(E/\mathbf{Q}_n)$.

(2) Theorem 0.1 corresponds to Theorem 0.1 and Theorem 7.4 in [6].

(3) Suppose that $a_2 = 0$. Then, by Pollack [11] Theorem 5.6 we know there are two power series $f(T)$, $g(T) \in \mathbf{Z}_2[[T]]$ such that

$$L_2(E)_\alpha = f(T)\log^-(T) + \frac{1}{2}g(T)\log^+(T)\alpha$$

where $L_2(E)_\alpha$ is the p-adic L-function corresponding to $\alpha = \sqrt{-2}$ (for other notations, see [11]). Since $f(0) = L(E,1)/\Omega_E$ and $g(0) = 4L(E,1)/\Omega_E$, if we assume $2 \nmid L(E,1)/\Omega_E$, $f(T)$ is a unit. But the condition $2 \nmid L(E,1)/\Omega_E$ is not sufficient to determine the ideal $(g(T))$ and to determine the structure of Kobayashi's Selmer group corresponding to $g(T)$. (We will see later (cf. Corollary 1.2) that $T+2$ divides $g(T)$, but it is still insufficient because 2 divides the constant term of $g(T)/(T+2)$.) For example, for $E = X_0(27)$ which satisfies $a_2 = 0$ and $2 \nmid L(E,1)/\Omega_E$, $g(T)$ is $(T+2)((T+1)^4+1)$ modulo unit, so the rank of $E(\mathbf{Q}_\infty)$ would be 5. But for $E' = X_0(19)$ which also satisfies $a_2 = 0$ and $2 \nmid L(E,1)/\Omega_E$, we know $\mathrm{rank}\, E'(\mathbf{Q}_\infty) = 1$. So the structures of the Selmer groups of E and E' over $\mathbf{Q}_n$ for $n \geq 3$ are different.

(4) For a general E and for (mainly) odd p, the asymptotic formula of $\#Ш(E/\mathbf{Q}_n)\{p\}$ as $n \to \infty$ was studied by Perrin-Riou [10], Kobayashi [5], Pollack [11] (analytic side) and the first author [7].

(5) The difference of the proof of Theorem 0.1 from the case for an odd p in [6] is in that we have $L(E/\mathbf{Q}_n, 1) = 0$ for all $n \geq 1$ in the case $p = 2$, and in the conductor f_n in the proof of Proposition 1.4. The rest of the proof is similar to [6].

We would like to express our hearty admiration to John Coates for his enthusiasm for mathematics, especially to the arithmetic of elliptic curves. His question to the first author on the behaviour of the Tate-Shafarevich groups in the supersingular case was the starting point of this study. Discussions with him on Iwasawa theory have always been encouraging. We would like to thank him sincerely. We would like to thank K. Matsuno very much for communicating to us Proposition 1.1 which plays an important role in this paper.

Notation

For a group G and a G-module M, M^G denotes the G-invariant part and M_G denotes the G-coinvariants. For a field F and a $G_F = \mathrm{Gal}(\overline{F}/F)$-module M, the Galois cohomology group $H^q(G_F, M)$ is denoted by $H^q(F, M)$.

1. Preliminaries

1.1. *Conductor of an elliptic curve E with $2 \nmid L(E,1)/\Omega_E$.*

The following proposition was communicated to us by K. Matsuno.

Proposition 1.1. *Suppose that E is an elliptic curve over $\mathbf{Q}$, and has good supersingular reduction at 2, and $\mathrm{Tam}(E)$ is odd. Then, the conductor N of E satisfies*

$$N \equiv 3, 5 \pmod 8.$$

Proof. Let

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$$

be the minimal Weierstrass equation of E over $\mathbf{Z}$. If E is a supersingular elliptic curve over $\mathbf{F}_2$, its j-invariant is 0, and it has a Weierstrass equation of the form $y^2 + y = x^3 + \beta_4 x + \beta_6$ (β_4, $\beta_6 \in \mathbf{F}_2$, cf. [14] p.325) . Hence, considering all possible changes of variables of the Weierstrass equation, we know that α_1 is even and α_3 is odd. This implies that the minimal discriminant $\Delta_E = \Delta_E(\alpha_1, ..., \alpha_6)$ satisfies $\Delta_E \equiv 5 \pmod 8$.

On the other hand, suppose that ℓ is a bad reduction prime for E. Since $\mathrm{Tam}(E)$ is odd, $c_\ell = (E(\mathbf{Q}_\ell) : E^0(\mathbf{Q}_\ell))$ is also odd, and the table by Néron and Kodaira tells us that the number of irreducible components of the Néron model of E over $\mathbf{Z}_\ell$ is odd. It follows from Ogg's formula that

$$\mathrm{ord}_\ell(N) \equiv \mathrm{ord}_\ell(\Delta_E) \pmod 2.$$

Hence, the absolute value of Δ_E/N is a square. Thus, we have $N \equiv 3, 5 \pmod 8$.

Corollary 1.2. *Let E' be the quadratic twist of E by the Dirichlet character corresponding to $\mathbf{Q}(\sqrt{2})$. If 2 is a supersingular prime for E, $2 \nmid L(E,1)/\Omega_E$, and $2 \nmid \mathrm{Tam}(E)$, then we have $L(E',1) = 0$.*

Proof. By Proposition 1.1, the conductor N of E satisfies $N \equiv 3, 5 \pmod 8$. Hence, the sign of the functional equation of E' is -1 (note that the sign of the functional equation of E is 1 because $L(E,1) \neq 0$). So we have $L(E',1) = 0$.

1.2. *Modular elements of Mazur and Tate.*

Let $f(z) = \Sigma a_n \exp(2\pi inz)$ be the modular form corresponding to E. For a rational number a/b, we define the modular symbol $[a/b]$ by

$$[a/b] = \mathrm{Re}(2\pi i \int_{a/b}^{i\infty} f(z)dz)/\Omega_E$$

where Ω_E is the Néron period. ($\Omega_E = 2\min\{\mathrm{Re}\,\omega > 0 \mid \omega \in \Lambda_E\}$ where Λ_E is the period lattice in $\mathbf{C}$ corresponding to the elliptic curve E. In this paper, we consider only real periods.) Then, we know $[a/b] \in \mathbf{Q}$ by Manin. For a positive integer $m > 0$, we consider a cyclotomic field $\mathbf{Q}(\mu_{2^m})$. For $k \in \mathbf{Z}$, the element of $\mathrm{Gal}(\mathbf{Q}(\mu_{2^m})/\mathbf{Q})$ corresponding to k mod 2^m by the natural isomorphism $\mathrm{Gal}(\mathbf{Q}(\mu_{2^m})/\mathbf{Q}) \simeq (\mathbf{Z}/2^m)^\times$ is denoted by σ_k. The modular element for 2^m is defined by

$$\theta_{2^m} = \sum_{\substack{k=1 \\ 2 \not| k}}^{2^m} [k/2^n]\sigma_k \in \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_{2^m})/\mathbf{Q})].$$

Suppose that 2 is a good reduction prime. Then, for any $m > 2$ we have a distribution relation

$$\pi(\theta_{2^m}) = a_2\theta_{2^{m-1}} - \nu(\theta_{2^{m-2}})$$

where $\pi : \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_{2^m})/\mathbf{Q})] \longrightarrow \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_{2^{m-1}})/\mathbf{Q})]$ is the natural projection, and $\nu : \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_{2^{m-2}})/\mathbf{Q})] \longrightarrow \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_{2^{m-1}})/\mathbf{Q})]$ is the $\mathbf{Z}_2$-homomorphism defined by $\sigma \mapsto \Sigma\tau$ for $\sigma \in \mathrm{Gal}(\mathbf{Q}(\mu_{2^{m-2}})/\mathbf{Q})$ where τ ranges over elements of $\mathrm{Gal}(\mathbf{Q}(\mu_{2^{m-2}})/\mathbf{Q})$ projecting to σ. Since the Hecke operator T_2 can be calculated by using the operation of $\begin{pmatrix}2&0\\0&1\end{pmatrix}+\begin{pmatrix}1&0\\0&2\end{pmatrix}+\begin{pmatrix}1&1\\0&2\end{pmatrix}$ (cf. [3] p.11), $a_2[0] = 2[0]+[1/2]$ and $a_2[1/2] = [0] + [1/4] + [3/4]$. Hence, we have

$$\theta_2 = -(a_2 - 2)L(E, 1)/\Omega_E$$

which follows from $\theta_2 = [1/2]$ and $[0] = -L(E, 1)/\Omega_E$. Suppose that $\pi : \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_4)/\mathbf{Q})] \longrightarrow \mathbf{Q}$ is the augmentation map. Then, we have

$$\pi(\theta_4) = -(a_2^2 - 2a_2 - 1)L(E, 1)/\Omega_E$$

which is obtained from $\pi(\theta_4) = [1/4] + [3/4] = a_2\theta_2 - [0]$.

We define $\theta_{\mathbf{Q}_n}$ to be the image of $\theta_{2^{n+2}}$ under the natural restriction map $\mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_{2^{n+2}})/\mathbf{Q})] \longrightarrow \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$ induced by $\sigma \mapsto \sigma_{|\mathbf{Q}_n}$ for $\sigma \in \mathrm{Gal}(\mathbf{Q}(\mu_{2^{n+2}})/\mathbf{Q})$. By what we described above, they satisfy

$$\pi(\theta_{\mathbf{Q}_n}) = a_2\theta_{\mathbf{Q}_{n-1}} - \nu(\theta_{\mathbf{Q}_{n-2}})$$

for $n \geq 2$ (where we used the same notation π and ν which are the maps induced by π and ν, namely the corresponding projection and the norm map, respectively),

$$\begin{aligned}\pi(\theta_{\mathbf{Q}_1}) &= -(a_2(a_2^2 - 2a_2 - 1) - 2(a_2 - 2))L(E,1)/\Omega_E \\ &= -(a_2 - 1)(a_2^2 - a_2 - 4)L(E,1)/\Omega_E,\end{aligned}$$

and

$$\theta_{\mathbf{Q}} = -(a_2^2 - 2a_2 - 1)L(E,1)/\Omega_E.$$

In the following, we assume that E satisfies the conditions of Theorem 0.1. Since E has supersingular reduction at 2, $E[2]$ is irreducible as a $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module. So the Manin constant of E is prime to 2 by [1]. Hence, $\theta_{\mathbf{Q}_n}$ is in $\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$ (cf. [15] Theorem Corollary 3.15, see also [8]).

Let ψ_n be a faithful character of $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$, namely the order of ψ_n is 2^n. We define $q_n = \sum_{k=0}^{n-1}(-1)^k 2^{n-1-k}$ as in Theorem 0.1 (2). The following proposition corresponds to Proposition 1.2 in [6].

Proposition 1.3. *We have $\psi_1(\theta_{\mathbf{Q}_1}) = 0$. For $n \geq 2$ we have $\psi_n(\theta_{\mathbf{Q}_n}) \neq 0$ and*

$$\mathrm{ord}_{\zeta_{2^n}-1}(\psi_n(\theta_{\mathbf{Q}_n})) = q_n$$

where $\mathrm{ord}_{\zeta_{2^n}-1}$ is the normalized additive valuation of $\mathbf{Q}(\mu_{2^n})$ at the prime above 2 (ζ_{2^n} is a primitive 2^n-th root of unity, and $\mathrm{ord}_{\zeta_{2^n}-1}(\zeta_{2^n} - 1) = 1$).

In [6] Proposition 1.2, q_n was defined separately depending on whether n is odd or even. Here, q_n is defined by a single formula.

Proof. We have $\psi_1(\theta_{\mathbf{Q}_1}) = 2\sqrt{2}L(E,\chi_8,1)/\Omega_E$ where χ_8 is the Dirichlet character corresponding to $\mathbf{Q}_1 = \mathbf{Q}(\sqrt{2})$. By Corollary 1.2, we get $L(E,\chi_8,1) = 0$, so $\psi_1(\theta_{\mathbf{Q}_1}) = 0$.

We write $\theta_{\mathbf{Q}_1} = a(1+\gamma)$ for some $a \in \mathbf{Z}_2$ where γ is a generator of $\mathrm{Gal}(\mathbf{Q}_1/\mathbf{Q})$. By the formula on $\pi(\theta_{\mathbf{Q}_1})$ which was mentioned before this proposition, we have $\pi(\theta_{\mathbf{Q}_1}) = 2a = 2L(E,1)/\Omega_E$ if $a_2 = 2$, and $2a = 6L(E,1)/\Omega_E$ if $a_2 = -2$. Hence, our assumption $\mathrm{ord}_2(L(E,1)/\Omega_E) = 0$ implies that a is a unit in $\mathbf{Z}_2$. Therefore, using the distribution property of $\theta_{\mathbf{Q}_n}$, we obtain $\mathrm{ord}_{\zeta_{2^n}-1}(\psi_n(\theta_{\mathbf{Q}_n})) = q_n$ for odd $n \geq 3$ by the argument of Proposition 1.2 in [6]. For even $n \geq 2$, the conclusion also follows from the distribution property and $\theta_{\mathbf{Q}} \in \mathbf{Z}_2^\times$.

1.3. *Norm maps of the formal group associated to an elliptic curve.*

In this subsection, we will give a result corresponding to Proposition 2.1 in [6]. Let F be the formal group associated to E which we assume satisfies the condition of Theorem 0.1. Let k be the completion of $\mathbf{Q}$ in the 2-adic topology (so $k = \mathbf{Q}_p$ the p-adic field with $p = 2$, here $\mathbf{Q}_2$ is not the field of degree 2^2 as in

Theorem 0.1), and we denote by k_n the intermediate field of the cyclotomic $\mathbf{Z}_2$-extension k_∞/k such that $[k_n : k] = 2^n$. We consider $F(k_n)$ which is the abelian group defined on the maximal ideal of the integer ring of k_n by the formal group F, and also the norm map $N : F(k_n) \longrightarrow F(k_{n-1})$ of F.

Proposition 1.4. *Let $q_n = \sum_{k=0}^{n-1}(-1)^k 2^{n-1-k}$ be as above. Then, we have*

$$\#(F(k_{n-1})/NF(k_n)) \geq 2^{q_n}.$$

Proof. This can be proved by the same method as [6] Proposition 2.1. The difference is only in the conductor of the extension k_n/k_{n-1}. Let m_{k_n} (resp. $m_{k_{n-1}}$) be the maximal ideal of the integer ring of k_n (resp. k_{n-1}). For general p, there is a positive integer f_n such that $\mathrm{Tr}_{k_n/k_{n-1}}(m_{k_n}^r) = m_{k_{n-1}}^{r'}$ where $r' = [\frac{(f_n+1)(p-1)+r}{p}]$ ([13] Chap.V §3 Lemma 4). It is not difficult to compute the value f_n for intermediate fields of the cyclotomic $\mathbf{Z}_p$-extension, and we have $f_n = (p^n-1)/(p-1)$ for odd p, and $f_n = p^n/(p-1) = 2^n$ for $p = 2$.

We define $s_n = [p^n/(p^2-1)] + 1$, so

$$s_n = \begin{cases} p^{n-2} + p^{n-4} + ... + p^2 + 2 & \text{for even } n \geq 2 \\ p^{n-2} + p^{n-4} + ... + p + 1 & \text{for odd } n \geq 3, \end{cases}$$

and $t_n = [\frac{(f_n+1)(p-1)+s_n}{p}]$. Then, by the method of Proposition 2.1 in [6], we have $\mathrm{ord}_2(\#(F(k_{n-1})/NF(k_n))) \geq t_n - s_n$. We can easily check that $t_n - s_n = q_n$ for $p = 2$. This completes the proof.

2. Proof of the main theorem

2.1. *Selmer groups.*

For any number field F, we define $\mathrm{Sel}(E/F)$ to be the Selmer group over F of $E[2^\infty]$ which is the group of 2-power division points, so

$$\mathrm{Sel}(E/F) = \mathrm{Ker}(H^1(F, E[2^\infty]) \longrightarrow \prod_v H^1(F_v, E[2^\infty])/(E(F_v) \otimes \mathbf{Q}_2/\mathbf{Z}_2))$$

where v ranges over all primes of F. (Here, $E(F_v) \otimes \mathbf{Q}_2/\mathbf{Z}_2$ is regarded to be a subgroup of $H^1(F_v, E[2^\infty])$ by the Kummer map.) Hence, $\mathrm{Sel}(E/F)$ sits in an exact sequence

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_2/\mathbf{Z}_2 \longrightarrow \mathrm{Sel}(E/F) \longrightarrow Ш(E/\mathbf{Q})\{2\} \longrightarrow 0$$

where $Ш(E/\mathbf{Q})\{2\}$ is the 2-primary component of the Tate-Shafarevich group of E over F. As in [6] §4, we define the fine Selmer group $\mathrm{Sel}_0(E/F)$ by

$$\mathrm{Sel}_0(E/F) = \mathrm{Ker}(\mathrm{Sel}(E/F) \longrightarrow \bigoplus_{v|2} H^1(F_v, E[2^\infty]))$$

where v ranges over primes of F lying over 2. (The terminology "fine Selmer group" was adopted by J. Coates.)

Let $T = T_p(E)$ be the Tate module of E with $p = 2$. For any prime v which is prime to 2 (v could be an infinite prime), we have $H^1(F_v, T) = \varprojlim(E(F_v) \otimes \mathbf{Z}/2^m\mathbf{Z})$, hence by Cassels-Tate-Poitou duality, we have

Lemma 2.1.

$$H^1(F,T) \longrightarrow \bigoplus_{v|2} H^1(F_v,T)/(E(F_v)\otimes \mathbf{Z}_2) \longrightarrow \mathrm{Sel}(E/F)^\vee$$
$$\longrightarrow \mathrm{Sel}_0(E/F)^\vee \longrightarrow 0.$$

is exact.

2.2. *Proof of Theorem* 0.1.

Suppose that E satisfies the conditions of Theorem 0.1. We use the argument in [6] §5. Kato constructed zeta elements

$$z_{\mathbf{Q}_\infty} = (z_{\mathbf{Q}_n}) \in \varprojlim H^1(\mathbf{Q}_n, T)$$

(cf. Kato [4] Theorems 12.4 and 12.5; the proofs of Theorem 12.4 (3) and Theorem 12.5 (4) can be applied to our case even for $p = 2$ because we are working on the cyclotomic $\mathbf{Z}_2$-extension) satisfying the following properties. For an even character ψ of conductor 2^{n+2} with $n \geq 1$,

$$\sum_{\sigma \in \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})} \psi(\sigma) \exp^*(\sigma(z_{\mathbf{Q}_n})) = \omega_E L(E,\psi,1)/\Omega_E$$

where ω_E is the Néron differential, and $\exp^*$ is the dual exponential map (cf. [2], [12]). For the trivial character,

$$\exp^*(z_{\mathbf{Q}}) = \omega_E(1 - \frac{a_2}{2} + \frac{1}{2})\frac{L(E,1)}{\Omega_E}.$$

Let k_n (resp. k) be the 2-adic completion of $\mathbf{Q}_n$ (resp. $\mathbf{Q}$) as in 1.3. Since the image of $\exp^* : H^1(k,T) \longrightarrow H^0(E,\Omega^1_E) \otimes k$ is $2^{-1}\mathbf{Z}_2\omega_E$ (cf. [12] Proposition 5.2), the image of $z_{\mathbf{Q}}$ generates $H^1(k,T)/E(k)\otimes\mathbf{Z}_2$ which is a free $\mathbf{Z}_2$-module of rank 1. The argument of the Euler system (cf. [4]) shows that $\mathrm{Sel}_0(E/\mathbf{Q}) = 0$, hence we have $\mathrm{Sel}(E/\mathbf{Q}) = 0$ (cf. [6] §5) by Lemma 2.1.

We have a control theorem

$$\mathrm{Sel}_0(E/\mathbf{Q}_n) \xrightarrow{\simeq} \mathrm{Sel}_0(E/\mathbf{Q}_\infty)^{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}_n)}$$

for all $n \geq 0$. This can be proved by the same method as Lemma 4.2 in [6]. Hence, $\mathrm{Sel}_0(E/\mathbf{Q}) = 0$ implies $\mathrm{Sel}_0(E/\mathbf{Q}_\infty) = 0$. Using the above isomorphism again, we obtain $\mathrm{Sel}_0(E/\mathbf{Q}_n) = 0$ for any $n \geq 0$.

By the same method as the proof of Proposition 5.2 in [6], we can see that $H^1(\mathbf{Q}, T)$ is a free $\mathbf{Z}_2$-module of rank 1, and $z_{\mathbf{Q}}$ generates it. Hence, $z_{\mathbf{Q}_\infty}$ generates $\varprojlim H^1(\mathbf{Q}_n, T)$, and $z_{\mathbf{Q}_n}$ generates $H^1(\mathbf{Q}_n, T)$. Hence, by Lemma 2.1, we have obtained

Lemma 2.2. $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ *is isomorphic to*

$$H^1(k_n, T)/(E(k_n) \otimes \mathbf{Z}_2 + < z_{\mathbf{Q}_n} >)$$

where $< z_{\mathbf{Q}_n} >$ *is the sub* $\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$*-module of* $H^1(k_n, T)$ *generated by* $z_{\mathbf{Q}_n}$.

Let γ be a generator of $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$. In the following, we assume $n \geq 1$. We set $\Lambda_n = \mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$ which is isomorphic to $\mathbf{Z}_2[t]/(t^{2^n} - 1)$. By Proposition 1.3, $\gamma + 1$ divides $\theta_{\mathbf{Q}_n}$. We write

$$\theta_{\mathbf{Q}_n} = (\gamma + 1)\theta'_{\mathbf{Q}_n}.$$

Then, $\theta'_{\mathbf{Q}_n}$ is well-defined in $\mathbf{Z}_2[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]/(g(\gamma))$ where $g(t)$ is the polynomial $g(t) = (t^{2^n} - 1)/(t+1)$. We saw in the proof of Proposition 1.3 that $\theta'_{\mathbf{Q}_1}$ is a unit. By the distribution property, we have $\theta_{\mathbf{Q}_2} \equiv -(\gamma+1)\theta_{\mathbf{Q}} + a_2\theta_{\mathbf{Q}_1} \pmod{(\gamma^2 - 1)}$, so it follows from $\theta_{\mathbf{Q}} \in \mathbf{Z}_2^\times$ that $\theta'_{\mathbf{Q}_2}$ is also a unit.

We put $\Lambda'_n = \Lambda_n/(g(\gamma))$ where $g(t) = (t^{2^n} - 1)/(t + 1)$ is as above. We denote by I_n the ideal $(\theta_{\mathbf{Q}_n}, \nu(\theta_{\mathbf{Q}_{n-1}}))$ of Λ_n where $\nu : \Lambda_{n-1} \longrightarrow \Lambda_n$ is the map defined in 1.2 ($\sigma \mapsto \Sigma_{\tau_{|\mathbf{Q}_{n-1}} = \sigma}\tau$). We also define I'_n to be the ideal $(\theta'_{\mathbf{Q}_n}, \nu(\theta'_{\mathbf{Q}_{n-1}}))$ of Λ'_n where $\nu : \Lambda'_{n-1} \longrightarrow \Lambda'_n$ is induced by $\nu : \Lambda_{n-1} \longrightarrow \Lambda_n$. We have an exact sequence

$$0 \longrightarrow \Lambda'_n/I'_n \xrightarrow{a} \Lambda_n/I_n \xrightarrow{b} \mathbf{Z}_2 \longrightarrow 0$$

where a is the map $x \mapsto (\gamma + 1)x$, and b is the map defined by $\gamma \mapsto -1$.

In order to prove Theorem 0.1, it is enough to show

Lemma 2.3. (1) $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ *is annihilated by* $\theta_{\mathbf{Q}_n}$.
(2) $\mathrm{ord}_2(\#(\Lambda'_n/I'_n)) \leq r_n$ *where* $r_n = \Sigma_{i=1}^n (q_i - 1)$.
(3) $\mathrm{ord}_2(\#(\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}) \geq r_n$.

We first prove Theorem 0.1 assuming Lemma 2.3. Since $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ is a cyclic Λ_n-module by Lemma 2.2, Lemma 2.3 (1) shows that $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ is a cyclic Λ_n/I_n-module (cf. [6] Lemma 7.1 (3)). In particular, for $n = 1$, we showed $I_1 = (\gamma + 1)$, so $\mathrm{Sel}(E/\mathbf{Q}_1)^\vee$ is cyclic as a $\mathbf{Z}_2$-module. On the other hand, $\psi_1(\theta_{\mathbf{Q}_1}) = 0$ implies $\exp^*((\gamma - 1)z_{\mathbf{Q}_1}) = 0$. Hence, $(\gamma - 1)z_{\mathbf{Q}_1}$ is in the Selmer group $\mathrm{Sel}(E/\mathbf{Q}_1, T)$ with respect to T. Since $(\gamma - 1)z_{\mathbf{Q}_1} \neq 0$ (note that $H^1(\mathbf{Q}_1, T)$ is a free Λ_1-module of rank 1, which is generated by $z_{\mathbf{Q}_1}$ (cf. [6] Proposition 5.2)), $\mathrm{rank}_{\mathbf{Z}_2} \mathrm{Sel}(E/\mathbf{Q}_1, T) > 0$, so $\mathrm{corank}\, \mathrm{Sel}(E/\mathbf{Q}_1) > 0$. Thus, we obtain

$$\mathrm{Sel}(E/\mathbf{Q}_1)^\vee \simeq \Lambda_1/I_1 \simeq \mathbf{Z}_2.$$

Since we showed $\mathrm{Sel}(E/\mathbf{Q}_n)^\vee$ is a cyclic Λ_n/I_n-module, there is a surjective homomorphism $f : \Lambda_n/I_n \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_n)^\vee$. We consider a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda_n'/I_n' & \longrightarrow & \Lambda_n/I_n & \longrightarrow & \Lambda_1/I_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \simeq} & & \\ 0 & \longrightarrow & (\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_n)^\vee & \xrightarrow{\alpha} & \mathrm{Sel}(E/\mathbf{Q}_1)^\vee & \longrightarrow & 0 \end{array}$$

Here, α is induced by the natural map $\mathrm{Sel}(E/\mathbf{Q}_1) \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_n)$. The exactness of the upper row follows from the exact sequence before Lemma 2.3 and the isomorphism $\Lambda_1/I_1 \simeq \mathbf{Z}_2$. Since f induces a surjective homomorphism $\Lambda_n'/I_n' \longrightarrow \mathrm{Ker}(\alpha : \mathrm{Sel}(E/\mathbf{Q}_n)^\vee \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_1)^\vee)$, the finiteness of Λ_n'/I_n' (Lemma 2.3 (2)) induces $\#\mathrm{Ker}(\alpha) < \infty$. Hence, $\mathrm{Ker}(\alpha) = (\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}$. The surjectivity of α follows from the injectivity of $\mathrm{Sel}(E/\mathbf{Q}_1) \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_n)$ which follows from the injectivity of $H^1(\mathbf{Q}_1, E[2^\infty]) \longrightarrow H^1(\mathbf{Q}_n, E[2^\infty])$. Thus, the bottom row is also exact.

Since f is surjective, f' which is induced by f is also surjective. Furthermore, by Lemma 2.3 (2) and (3), we obtain that $\#\Lambda_n'/I_n' = \#(\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}$, and that f' is bijective. This implies the bijectivity of f, and we have obtained Theorem 0.1 (1).

For the proof of Theorem 0.1 (2), it is enough to determine the structure of Λ_n/I_n, and enough to show that $\Lambda_2'/I_2' = 0$ and

$$\Lambda_n'/I_n' \simeq (\mathbf{Z}/2^{n-2}\mathbf{Z})^{q_3-q_2} \oplus (\mathbf{Z}/2^{n-3}\mathbf{Z})^{q_4-q_3} \oplus \ldots \oplus (\mathbf{Z}/2\mathbf{Z})^{q_n-q_{n-1}}$$

for $n \geq 3$. Since $\theta'_{\mathbf{Q}_2}$ is a unit, $\Lambda_2'/I_2' = 0$. By Proposition 1.3, we have $\mathrm{ord}_{\zeta_{2^n}-1}(\psi_n(\theta'_{\mathbf{Q}_n})) = q_n - 1$. Hence, the above isomorphism for Λ_n'/I_n' with $n \geq 3$ can be proved by the same method as Theorem 7.4 in [6].

Theorem 0.1 (3) follows from Theorem 0.1 (1) (or Lemma 2.2). This completes the proof of Theorem 0.1.

2.3. *Proof of Lemma* 2.3.

Lemma 2.3 (1) can be proved by the same method as Lemma 7.1 (2) in [6]. Let D be the Dieudonné module which is a 2-dimensional k-vector space ($k = \mathbf{Q}_2$, the 2-adic completion of $\mathbf{Q}$), and φ is the Frobenius on D satisfying $\varphi^{-2} - a_p\varphi^{-1} + p = 0$ (with $p = 2$). For $m = n + 2$, we define $\gamma_m : D \longrightarrow D \otimes k(\mu_{2^m})$ by $x \mapsto \Sigma_{i=0}^{m-1}\varphi^{i-m}(x) \otimes \zeta_{2^{m-i}} + (1-\varphi)^{-1}(x)$ where (ζ_{2^i}) is a generator of $\mathbf{Z}_2(1)$ (cf. [6] §3). For $x \in D$ and $z \in H^1(k(\mu_{2^m}), T)$, we define

$$P_m(x,z) = \sum_{\sigma \in \mathrm{Gal}(k(\mu_{2^m})/k)} \mathrm{Tr}_{k(\mu_{2^m})/k}[\gamma_m(x)^\sigma, \exp^*(z)]\sigma \in k[\mathrm{Gal}(k(\mu_{2^m})/k)]$$

where $[\ ,\ ]$ is the cup product of the de Rham cohomology (cf. [6] §3). Since the corestriction map induces an isomorphism $H^1(k(\mu_{2^m}), T)_{\mathrm{Gal}(k(\mu_{2^m})/k_n)} \simeq$

$H^1(k_n, T)$ (k_n is the n-th layer of the cyclotomic $\mathbf{Z}_2$-extension of k_∞/k), the map $z \mapsto P_m(x, z)$ induces a map $H^1(k_n, T) \longrightarrow k[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$ which we denote by $z \mapsto P_n(x, z)$. We have

$$\theta_{\mathbf{Q}_n} = [\varphi(\omega_E), \omega_E]^{-1} P_n(\varphi^{m+1}(\omega_E), z_{\mathbf{Q}_n})$$

which can be proved by the same method as Lemma 7.2 in [6]. Hence, by the same method as Lemma 7.1 (2) in [6], we obtain $\theta_{\mathbf{Q}_n} \mathrm{Sel}(E/\mathbf{Q}_n)^\vee = 0$.

Next, we prove Lemma 2.3 (2). By Proposition 1.3, we have

$$\mathrm{ord}_{\zeta_{2^n}-1}(\psi_n(\theta'_{\mathbf{Q}_n})) = q_n - 1.$$

Hence, by the same method as Lemma 7.1 (1) in [6], we get the conclusion.

Finally, we prove Lemma 2.3 (3). We may assume $n \geq 2$. Let S be the set of primes for which E has bad reduction, and primes lying over 2 and ∞. By induction on n, we know that the Selmer group $\mathrm{Sel}(E/\mathbf{Q}_{n-1}, T)$ over $\mathbf{Q}_{n-1}$ of T is isomorphic to $\mathbf{Z}_2$. By Cassels-Tate-Poitou duality,

$$0 \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_{n-1}) \longrightarrow H^1(O_{\mathbf{Q}_{n-1}}[1/S], E[2^\infty]) \longrightarrow \bigoplus_{v \in S} \frac{H^1((\mathbf{Q}_{n-1})_v, E[2^\infty])}{E((\mathbf{Q}_{n-1})_v) \otimes \mathbf{Q}_2/\mathbf{Z}_2}$$
$$\longrightarrow \mathrm{Sel}(E/\mathbf{Q}_{n-1}, T)^\vee$$

is exact, and the last term is isomorphic to $\mathbf{Q}_2/\mathbf{Z}_2$. Put $G = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}_{n-1})$. Writing down the corresponding exact sequence for $\mathbf{Q}_n$ and taking its G-invariant parts, we compare two exact sequences. Using the snake lemma and $\mathrm{Sel}(E/\mathbf{Q}_{n-1}, T)^\vee \simeq \mathbf{Q}_2/\mathbf{Z}_2$, we have

$$\begin{aligned} &\#\,\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}) \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_n)^G) \\ &\geq \frac{1}{2} \#\,\mathrm{Ker}\left(\frac{H^1(k_{n-1}, E[2^\infty])}{E(k_{n-1}) \otimes \mathbf{Q}_2/\mathbf{Z}_2} \longrightarrow \frac{H^1(k_n, E[2^\infty])}{E(k_n) \otimes \mathbf{Q}_2/\mathbf{Z}_2}\right) \\ &= \frac{1}{2} \#\,\mathrm{Coker}(N : E(k_n) \otimes \mathbf{Z}_2 \longrightarrow E(k_{n-1}) \otimes \mathbf{Z}_2). \end{aligned}$$

To get the third line, we used local Tate duality. Thus, by Proposition 1.4, we obtain

$$\mathrm{ord}_2(\#\,\mathrm{Coker}(\mathrm{Sel}(E/\mathbf{Q}_{n-1}) \longrightarrow \mathrm{Sel}(E/\mathbf{Q}_n)^G)) \geq q_n - 1.$$

Suppose $n \geq 2$, and consider a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathrm{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_n)^\vee & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_1)^\vee & \longrightarrow & 0 \\ & & \downarrow h_1 & & \downarrow h_2 & & \downarrow h_3 & & \\ 0 & \longrightarrow & (\mathrm{Sel}(E/\mathbf{Q}_{n-1})^\vee)_{\mathrm{tors}} & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_{n-1})^\vee & \longrightarrow & \mathrm{Sel}(E/\mathbf{Q}_1)^\vee & \longrightarrow & 0. \end{array}$$

Here, the horizontal sequences were proved to be exact in the previous subsection 2.2. The middle vertical map h_2 is induced by the natural map which is injective.

Hence, h_2 is surjective. The right vertical map h_3 is the identity map, so we have $\operatorname{Ker} h_1 = \operatorname{Ker} h_2$. We compute

$$\#\operatorname{Ker} h_1 = \#\operatorname{Ker} h_2 \geq \#\operatorname{Coker}(\operatorname{Sel}(E/\mathbf{Q}_{n-1}) \longrightarrow \operatorname{Sel}(E/\mathbf{Q}_n)^G) \geq 2^{q_n-1}$$

Thus,

$$\begin{aligned}\operatorname{ord}_2(\#(\operatorname{Sel}(E/\mathbf{Q}_n)^\vee)_{\mathrm{tors}}) &= \operatorname{ord}_2(\#\operatorname{Ker} h_1 \#(\operatorname{Sel}(E/\mathbf{Q}_{n-1})^\vee)_{\mathrm{tors}}) \\ &\geq q_n - 1 + r_{n-1} = r_n\end{aligned}$$

where we used $\operatorname{ord}_2(\#(\operatorname{Sel}(E/\mathbf{Q}_{n-1})^\vee)_{\mathrm{tors}}) \geq r_{n-1}$ which holds by induction on n. This completes the proof of Lemma 2.3 (3).

References

[1] Abbes, A., and Ullmo, E., A propos de la conjecture de Manin pour les courbes elliptiques modulaires, Compositio Math. 103 (1996), 269-286.

[2] Bloch, S. and Kato, K., L-functions and Tamagawa numbers of motives, in *The Grothendieck Festschrift Vol I*, Progress in Math. Vol 86, Birkhäuser (1990), 333-400.

[3] Cremona, J.E., *Algorithms for modular elliptic curves*, Cambridge University Press (1992).

[4] Kato, K., p-adic Hodge theory and values of zeta functions of modular forms, in *Cohomologies p-adiques et applications arithmétiques III*, Astérisque 295 (2004), 117-290.

[5] Kobayashi, S., Iwasawa theory for elliptic curves at supersingular primes, Invent. math. 152 (2003), 1-36.

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

[7] Kurihara, M., On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction II, in preparation.

[8] Manin, Y.I., Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk. SSSR Ser. Mat. 36 (1972), 19-66 (English translation Math. USSR-Izv. 6 (1972), 19-64).

[9] Mazur, B. and Tate, J., Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. 54 No. 2 (1987), 711-750.

[10] Perrin-Riou, B., Arithmétique des courbes elliptiques à réduction supersingulière en p, Experiment. Math. 12 (2003), 155-186.

[11] Pollack, R., On the p-adic L-function of a modular form at a supersingular prime, Duke Math. J. 118 No. 3 (2003), 523-558.

[12] Rubin, K., Euler systems and modular elliptic curves, in *Galois representations in Arithmetic Algebraic Geometry*, London Math Soc, Lecture Note Series 254 (1998), 351-367.

[13] Serre, J.-P., *Corps locaux* (3^e édition), Hermann, Paris, (1968).

[14] Silverman, J.H., *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag (1986)

[15] Stevens, G., Stickelberger elements and modular parametrizations of elliptic curves, Invent. math. 98 (1989), 75-106.

Masato Kurihara
Department of Mathematics
Keio University
3-14-1 Hiyoshi, Kohoku-ku
Yokohama, 223-8522, Japan
E-mail: kurihara@math.keio.ac.jp

Rei Otsuki
Department of Mathematics
Keio University
3-14-1 Hiyoshi, Kohoku-ku
Yokohama, 223-8522, Japan
E-mail: ray_otsuki@math.keio.ac.jp