Bull. Korean Math. Soc. **50** (2013), No. 2, pp. 407–416
http://dx.doi.org/10.4134/BKMS.2013.50.2.407

ON THE p-PRIMARY PART OF TATE-SHAFAREVICH GROUP OF ELLIPTIC CURVES OVER $\mathbb{Q}$ WHEN p IS SUPERSINGULAR

Dohyeong Kim

Abstract. Let E be an elliptic curve over $\mathbb{Q}$ and p be a prime of good supersingular reduction for E. Although the Iwasawa theory of E over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is well known to be fundamentally different from the case of good ordinary reduction at p, we are able to combine the method of our earlier paper with the theory of Kobayashi [5] and Pollack [8], to give an explicit upper bound for the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ occurring in the p-primary part of the Tate-Shafarevich group of E over $\mathbb{Q}$.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. We recall that the Tate-Shafarevich group of $E/\mathbb{Q}$ is defined by

$$Ш(E/\mathbb{Q}) = \operatorname{Ker}\left(H^1\left(\mathbb{Q}, E(\overline{\mathbb{Q}})\right) \longrightarrow \prod_v H^1\left(\mathbb{Q}_v, E(\overline{\mathbb{Q}}_v)\right)\right),$$

where v runs over all places of $\mathbb{Q}$, and $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ at v. It is well-known that the p-primary subgroup of $Ш(E/\mathbb{Q})$ has a finite $\mathbb{Z}_p$-corank, and we denote this corank by t_p. It is conjectured that $t_p = 0$ for every prime p, but this is unknown when the complex L-function has a zero of order at least 2 at $s = 1$. We say a prime p is good ordinary (resp. good supersingular) if E has good ordinary reduction (resp. good supersingular reduction) at p. The aim of present paper is to compute an upper bound for t_p for all good supersingular primes p. For the case of good ordinary primes, see the author's previous paper [4]. If E has complex multiplication and p is ordinary, then a better bound is obtained in [2].

Suppose from now on that p is a prime of good supersingular reduction for E. We recall that if F is a finite extension of $\mathbb{Q}$, then the (p^∞-)Selmer group

Received March 9, 2011; Revised March 8, 2012.
2010 *Mathematics Subject Classification.* 11G05.
Key words and phrases. Iwasawa theory, supersingular prime, elliptic curves, Tate-Shafarevich group.

of E over F is defined as

$$\mathrm{Sel}(E/F) := \mathrm{Ker}\Big(H^1(F, E[p^\infty]) \longrightarrow \prod_v H^1(F_v, E)\Big),$$

where v runs over all places of F, and F_v is the completion of F at v, and $E[p^\infty]$ is the Galois module of p-power division points in $E(\overline{\mathbb{Q}})$. Let $\mathbb{Q}^{cyc}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Put

$$\mathrm{Sel}(E/\mathbb{Q}^{cyc}) = \varinjlim \mathrm{Sel}(E/F),$$

where F runs over the finite extensions of $\mathbb{Q}$ contained in $\mathbb{Q}^{cyc}$ and the inductive limit is taken relative to the restriction maps. Let $\Gamma := \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q})$ and define the Iwasawa algebra $\Lambda(\Gamma)$ by

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Gamma/U],$$

where U runs over the open subgroups of Γ. The natural action of Γ on $H^1(\mathbb{Q}^{cyc}, E[p^\infty])$ gives rise to a continuous action of Γ on $\mathrm{Sel}(E/\mathbb{Q}^{cyc})$, which extends to an action of the whole Iwasawa algebra $\Lambda(\Gamma)$. For an abelian group A, denote by $A^\wedge$ the Pontryagin dual $\mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ of A. We write the Pontryagin dual of a Selmer group by

$$X(E/F) := \mathrm{Sel}(E/F)^\wedge := \mathrm{Hom}(\mathrm{Sel}(E/F), \mathbb{Q}_p/\mathbb{Z}_p).$$

Our previous method used in [4] heavily depends on the important theorem that $X(E/\mathbb{Q}^{cyc})$ is a torsion module over $\Lambda(\Gamma)$ when p is a good *ordinary* prime. In contrast, when p is a good supersingular prime, which is the case of our interest, it is known that $X(E/\mathbb{Q}^{cyc})$ is not a torsion $\Lambda(\Gamma)$-module. Nevertheless, we can use the ingenius idea of Kobayashi [5] of considering modified Selmer groups, the duals of which are torsion over $\Lambda(\Gamma)$. Combined with our earlier method in [4], we can compute an upper bound for t_p for supersingular primes p. Let $\delta = 1$ when the sign is $+$ and $\delta = 0$ otherwise. Our main results are:

Theorem 1.1. *Let $L_p^\pm(E, \alpha, T)$ be Pollack's modified p-adic L-functions. Let $T^{m_p^\pm(E)}$ be the exact power of T dividing $L_p^\pm(E, \alpha, T)$. Then for a constant $C = C(E)$ which depends on E but not on p, we have $m_p^\pm(E) \le Cp^{8+\delta}$ for all good supersingular primes p.*

The definition of the power series $L_p^\pm(E, \alpha, T)$ in $\mathbb{Z}_p[[T]]$ is given in Section 2. As a corollary, we prove:

Corollary 1.2. *Let g_E be the rank of $E(\mathbb{Q})$. For all primes p where E has good supersingular reduction, we have $t_p \le Cp^8 - g_E$.*

The proofs of Theorem 1.1 and Corollary 1.2 are similar to those in our earlier paper [4]. However, there are additional estimations involving the modified p-adic logarithm map. We remark that in the case when E has complex multiplication, an alternative method used in [2] to obtain a better bound for t_p for sufficiently large ordinary primes does not yet generalize to supersingular primes.

2. Iwawawa theory for a supersingular prime

In this section, we recall the Iwasawa theory of E at a supersingular prime p. On the algebraic side, we will define the modified Selmer groups following Kobayashi [5], while on the analytic side we will use the theory of Pollack [8] who constructed the modified p-adic L-functions $L_p^{\pm}(E, \alpha, T)$. We fist begin with the modified Selmer groups. For a each $n \geq 0$, let $F_n = \mathbb{Q}(\mu_{p^{n+1}})$ and let $F_{-1} = \mathbb{Q}$. Let K_n be the completion of F_n at the unique prime of F_n lying above p. Also let $\mathrm{Tr}_{n,m} \colon E(K_n) \longrightarrow E(K_m)$ be the trace map when $n \geq m$. Plainly, we have $E(K_m) \subset E(K_n)$ when $n \geq m$.

Definition 2.1. We define the n-th modified Selmer groups as

$$\mathrm{Sel}^{\pm}(E/F_n) := \mathrm{Ker}\left(\mathrm{Sel}(E/F_n) \longrightarrow \frac{H^1\left(K_n, E[p^{\infty}]\right)}{E^{\pm}\left(K_n\right) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where

$$E^{+}(K_n) := \{P \in E(K_n) | \mathrm{Tr}_{n,m+1}(P) \in E(K_m) \text{ for even } m \ (0 \leq m < n)\} \text{ and}$$
$$E^{-}(K_n) := \{P \in E(K_n) | \mathrm{Tr}_{n,m+1}(P) \in E(K_m) \text{ for odd } m \ (0 \leq m < n)\}.$$

We call $\mathrm{Sel}^{+}(E/F_n)$ (resp. $\mathrm{Sel}^{-}(E/F_n)$) the even (resp. odd) Selmer group over F_n.

We adopt the convention that $E^{\pm}(K_{-1}) = E(\mathbb{Q}_p)$, whence it is clear that we have

$$\mathrm{Sel}^{\pm}(E/\mathbb{Q}) = \mathrm{Sel}(E/\mathbb{Q}).$$

One sees easily that the restriction map from $\mathrm{Sel}(E/F_n)$ to $\mathrm{Sel}(E/F_{n+1})$ maps $\mathrm{Sel}^{\pm}(E/F_n)$ to $\mathrm{Sel}^{\pm}(E/F_{n+1})$ and so we can define

$$\mathrm{Sel}^{\pm}(E/\mathbb{Q}^{cyc}) = \varinjlim \mathrm{Sel}^{\pm}(E/F_n).$$

Also, it is proven in Lemma 9.1 of [5] that the map

$$\mathrm{Sel}^{\pm}(E/F_n) \longrightarrow \mathrm{Sel}^{\pm}(E/\mathbb{Q}^{cyc})$$

is injective. As usual Selmer groups, the modified Selmer groups over $\mathbb{Q}^{cyc}$ are also modules over $\Lambda(\Gamma)$. However, the modified Selmer groups are crucially different from usual Selmer groups in that they are torsion $\Lambda(\Gamma)$-modules. Kobayashi proved (Theorem 1.2 in [5]):

Theorem 2.2. *The modified dual Selmer groups*

$$X^{\pm}(E/\mathbb{Q}^{cyc}) := \mathrm{Sel}^{\pm}(E/\mathbb{Q}^{cyc})^{\wedge}$$

are finitely generated torsion $\Lambda(\Gamma)$-modules.

Let $R = \mathbb{Z}_p[[T]]$ be the power series ring in a variable T with coefficients in $\mathbb{Z}_p$. Fix a topological generator γ of Γ. The $\mathbb{Z}_p$-algebra homomorphism $\Lambda(\Gamma) \to R$ sending γ to $T + 1$ is an isomorphism. Using this isomorphism, elements in $\Lambda(\Gamma)$ will be considered as power series in the variable T. By the

structure theorem of finitely generated torsion R-modules, there exists non-zero elements $G_j^{\pm}(T) \in R$, finite R-modules $D^{\pm}$ and exact sequences

$$0 \longrightarrow \bigoplus_{j=1}^{k^{\pm}} R/G_j^{\pm}(T)R \longrightarrow X^{\pm}(E/\mathbb{Q}^{cyc}) \longrightarrow D^{\pm} \longrightarrow 0\ .$$

The products $G^{\pm}(T) = \prod_{j=1}^{k^{\pm}} G_j^{\pm}(T)$ are then well-defined up to multiplication by a unit in R, and $G^{\pm}(T)$ are called the characteristic power series of $X^{\pm}(E/\mathbb{Q}^{cyc})$. The Iwasawa main conjecture is an assertion that the above characteristic power series have analytic descriptions via the special values of the complex L-function, which we now explain. Let N_E be the conductor of E. Since E is modular, there is a primitive normalized Hecke eigenform $f(q) = \sum_{k=1}^{\infty} a_k q^k$ of level N_E weight 2 such that $a_p = p + 1 - |\tilde{E}_p(\mathbb{F}_p)|$ for all primes p prime to N_E. For a Dirichlet character χ whose conductor is prime to N_E, the twisted L-function attached to f defined by

$$L(f, \chi, s) = L(E, \chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n) a_n}{n^s}$$

has analytic continuation to the entire complex plane. Let α and β be the roots of the equation $X^2 - a_p X + p$ in $\overline{\mathbb{Q}}$. We fix embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$. Using these embeddings, α and β will be considered as elements of $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$. And let Ω_E^+ be the least positive real period of the Nèron differential on the minimal Weierstrass model of E. Mazur and Swinnerton-Dyer [6] proved that we can p-adically interpolate values $L(E, \chi, 1)$ as χ varies among Dirichlet characters of p-power conductor and order. We now recall a special form of such interpolation property (See Section 14 of [7]) expressed in terms of a power series. For a character χ of conductor p^{r+1}, we define the Gauss sum as

$$\sum_{i=1}^{p^{r+1}} \zeta^i \chi(i),$$

where ζ is a primitive p^{r+1}-th root of unity.

Theorem 2.3. *Fix a global minimal generalized Weierstrass equation for E. Let p be a prime of good supersingular reduction for E. Let χ be a non-trivial Dirichlet character of conductor p^{r+1} and order p^r. Then there exists a unique power series*

$$L_p(E, \alpha, T) \in \mathbb{Q}_p(\alpha)[[T]]$$

with the following properties. Firstly, $L_p(E, \alpha, \zeta - 1)$ converges for every p-power roots of unity ζ. Secondly, this power series interpolate the complex L-values in the sense that

$$L_p(E, \alpha, \chi(\gamma) - 1) = \frac{p^{r+1} L(E, \overline{\chi}, 1)}{\Omega_E^+ \alpha^{r+1} \tau(\overline{\chi})} \tag{1}$$

for every nontrivial Dirichlet characters χ of p-power order and conductor.

Note that for a supersingular prime p, the p-adic L-function $L_p(E,\alpha,T)$ is not in $\mathbb{Z}_p[[T]]$. As an analytic counterpart of the modified Selmer groups which are torsion over $\Lambda(\Gamma)$, Pollack [8] introduced the following p-adic logarithmic functions to define the corresponding modified p-adic L-functions which actually lie in $\mathbb{Z}_p[[T]]$. Let $\Phi_n(T) = \sum_{t=0}^{p-1} T^{tp^{n-1}}$ be the p^n-th cyclotomic polynomial.

Lemma 2.4. *The products*

$$\log_p^+(T) := \frac{1}{p}\prod_{n=1}^{\infty}\left(\frac{\Phi_{2n}(1+T)}{p}\right),$$
$$\log_p^-(T) := \frac{1}{p}\prod_{n=1}^{\infty}\left(\frac{\Phi_{2n-1}(1+T)}{p}\right)$$

converge and define power series in $\mathbb{Q}_p[[T]]$ which are convergent on the open unit disc. The zeros of $\log_p^+$ (resp., $\log_p^-$) are precisely $\zeta_{2n}-1$ (resp., $\zeta_{2n-1}-1$) for a p^n-th root of unity ζ_n with $n>0$, and these are all simple zeros.

Proof. See Lemma 4.1 of [8]. □

We remark that the above definition is the weight 2 case of the construction in Lemma 4.1 [8] where modular forms of weight $k \geq 2$ are considered. Furthermore, we can write explicit interpolation properties of them.

Lemma 2.5 ([8], Lemma 4.7)**.** *Let ζ_r be a primitive p^{r+1}-th root of unity. We write Φ_j for the p^j-th cyclotomic polynomial. Then we have*

$$\log_p^+(\zeta_r-1) = \begin{cases} 0 & \text{when } 2 \mid r, \\ p^{-(r+1)/2}\displaystyle\prod_{j=1}^{(r-1)/2}\Phi_{2j}(\zeta_r) & \text{when } 2 \nmid r \end{cases}$$

$$\log_p^-(\zeta_r-1) = \begin{cases} p^{-r/2-1}\displaystyle\prod_{j=1}^{r/2}\Phi_{2j-1}(\zeta_r) & \text{when } 2 \mid r, \\ 0 & \text{when } 2 \nmid r. \end{cases}$$

Proof. See Lemma 4.7 of [8]. □

The role of $\log_p^{\pm}$ is analogous to what a gamma function does to the Riemann zeta function. It exactly cancels out the trivial zeros and we are interested the remaining ones. In a more precise terms, we have:

Theorem 2.6 ([8], Theorem 5.6)**.** *Under the assumption that p is odd and $a_p = 0$, we have*

$$L_p(E,\alpha,T) = L_p^+(E,\alpha,T)\log_p^+(T) + L_p^-(E,\alpha,T)\log_p^-(T)\alpha, \tag{2}$$

with $L_p^{\pm}(T) \in \mathbb{Z}_p[[T]]$.

Note that the assumption that $a_p = 0$ is harmless for us since we can ignore finitely many primes when we prove Theorem 1.1, and $a_p = 0$ for every $p > 5$ due to the Hasse's bound $|a_p| \leq 2\sqrt{p}$. The Iwasawa main conjecture for the modified Selmer groups is the equality of $L_p^{\pm}(T)$ and $G^{\pm}(T)$ up to multiplication by unit in $\mathbb{Z}_p[[T]]$. Kobayashi proved the following in Theorem 1.3 [5] which amounts to one divisibility of the main conjecture, using Kato's Euler system.

Theorem 2.7. *Let $G^{\pm}(T)$ be a characteristic power series of $X^{\pm}(E/\mathbb{Q}^{cyc})$. Then $G^{\pm}(T)$ divides $L_p^{\pm}(T)$.*

3. Proofs of the main results

Let $Ш(E/\mathbb{Q})[p^\infty]$ be the p-primary part of $Ш(E/\mathbb{Q})$. Recall that the Tate-Shafarevich group and the Selmer groups are related by the short exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[p^\infty] \longrightarrow 0\,. \tag{3}$$

If $E(\mathbb{Q})$ is of rank g_E, and $X(E/\mathbb{Q})$ has $\mathbb{Z}_p$-rank h_p, then $t_p = h_p - g_E$. Therefore we obtain an upper bound for t_p from that for h_p. Thus it suffices to relate h_p and the order of vanishing of $L_p^{\pm}(E, \alpha, T)$. We first prove some preliminary results for the proof of the main theorem. Let $\varphi(m)$ be the Euler totient function.

Lemma 3.1. *Let k be an integer such that $0 < k < n$. Then we have*

$$|\Phi_k(\zeta_n)|_p = p^{-\varphi(p^{n-k})^{-1} + \varphi(p^{n-k+1})^{-1}}. \tag{4}$$

In particular, we have

$$|\log_p^{\pm}(\zeta_r - 1)|_p = p^{c(r,p)},$$

where $c(r,p)$ is a function which is very small in the sense that for each fixed $r > 1$, $0 < c(r,p) < r$ for all but finitely many primes p.

Proof. We prove it using the explicit cyclotomic polynomials. Write

$$\Phi_k(T) = \frac{T^{p^k} - 1}{T^{p^{k-1}} - 1}.$$

Then $\zeta_n^{p^k}$ and $\zeta_n^{p^{k-1}}$ are respectively primitive p^{n-k}-th and p^{n-k+1}-th roots of unity. By the formula $|\zeta_r - 1|_p = p^{-\varphi(p^r)^{-1}}$, we get equation (4). The second part comes from direct calculation using Lemma 2.5. Indeed, for odd positive integer r

$$\begin{aligned} \left|\log_p^{+}(\zeta_r - 1)\right|_p &= \left| p^{-(r+1)/2} \prod_{j=1}^{(r-1)/2} \Phi_{2j}(\zeta_r) \right|_p \\ &= p^{\frac{r+1}{2} + \sum\left(-\varphi(p^{r-2j})^{-1} + \varphi(p^{r-2j+1})^{-1}\right)}, \end{aligned}$$

where the summation runs over $j = 1, 2, \ldots, (r-1)/2$ in the second line. For a fixed r, the terms in the summation in the second line converges to zero, thus $c(r,p)$ is a decreasing function which converges to $\frac{r+1}{2}$ as p goes to infinity. In particular, for all but finitely many primes p, we have $0 < c(r,p) < r$. For an even positive r, a similar calculation shows $c(r,p)$ is bounded by r as p goes to infinity. □

For a Dirichlet character χ of conductor p^r and order p^{r-1} with $r \geq 2$, precisely one of the two values $\log_p^{\pm}(\chi(\gamma)-1)$ vanishes according to Lemma 2.5. Therefore, by (2), nonvanishing of twisted L-values will give nonvanishing of modified p-adic L-functions.

Proposition 3.2. *Let $T^{m_p^{\pm}(E)}$ be the exact powers of T dividing $L_p^{\pm}(E,\alpha,T)$. Then we have the inequality*

$$h_p \leq m_p^{\pm}(E).$$

Proof. Consider the restriction map

$$\mathrm{res}\colon \mathrm{Sel}(E/\mathbb{Q}) \longrightarrow \mathrm{Sel}^{\pm}(E/\mathbb{Q}^{cyc}).$$

As shown in the proof of Proposition 2 in [4], the image of res is fixed by Γ and the Pontryagin dual of Ker(res) is finite. Therefore, taking Pontryagin dual of res, we obtain Γ-equivariant surjections

$$X^{\pm}(E/\mathbb{Q}^{cyc})_{\Gamma} \longrightarrow X(E/\mathbb{Q})$$

with finite cokernels. This completes the proof. □

Lemma 3.3. *There exists a constant c_E which only depends on E but not on p such that $\alpha^{r+1}c_E L_p^{\pm}(E,\alpha,\chi(\gamma)-1)$ is an algebraic integer in $\mathbb{Q}(\chi)$.*

Proof. It is shown in Proposition 1 in Section 3 of [4] that there exists a constant c_E which only depends on E but not on p such that $\alpha^{r+1}c_E L_p(E,\alpha,\chi(\gamma)-1)$ is an algebraic integer in $\mathbb{Q}(\chi)$. Although we made the assumption that p is ordinary in [4], the proof therein does not use it. □

Finally, we can prove the main theorem. From now on, we assume that the conductor of χ is $p^{9+\delta}$ and the order of χ is $p^{8+\delta}$, where δ is 0 or 1.

Theorem 3.4. *Given an elliptic curve E defined over $\mathbb{Q}$, there is a constant C which depends on E but not on p, such that $m_p^{\pm}(E) \leq Cp^{8+\delta}$ for all supersingular primes p. Here $\delta = 1$ when the sign is $+$ and $\delta = 0$ otherwise.*

Proof. It suffices to prove the assertion for sufficiently large p since we can adjust C to cover the remaining finitely many cases. Let χ be a Dirichlet character of conductor $p^{9+\delta}$ and order $p^{8+\delta}$. By Theorem 3 of [1], we know the nonvanishing

$$L(E,\chi,1) \neq 0$$

for sufficiently large primes p. Now let $x = \alpha^{9+\delta} c_E L_p(E, \alpha, \chi(\gamma) - 1)$ and

$$y = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} x^\sigma.$$

Then y belongs to $\mathbb{Z}$ and is nonzero. We are going to apply the following formula

$$|a|_p^{-1} \leq |a|_\infty \tag{5}$$

to y, which is true for all nonzero integers a. Note that $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ has $\varphi(p^{8+\delta})$ elements. Firstly, we have

$$\begin{aligned} |x^\sigma|_p &= |\alpha^{9+\delta} c_E L_p^\pm(E, \alpha, \chi(\gamma)^\sigma - 1) \log_p^\pm(\chi(\gamma)^\sigma - 1)|_p \\ &= p^{\frac{9+\delta}{2}} |c_E L_p^\pm(E, \alpha, \chi(\gamma)^\sigma - 1) \log_p^\pm(\chi(\gamma)^\sigma - 1)|_p \\ &= p^{\frac{9+\delta}{2}} |c_E|_p \cdot |L_p^\pm(E, \alpha, \chi(\gamma)^\sigma - 1)|_p p^{c(8+\delta,p)} \\ &\leq p^{\frac{9+\delta}{2}} |c_E|_p \cdot |\chi(\gamma)^\sigma - 1|_p^{m_p^\pm(E)} p^{c(8+\delta,p)}. \end{aligned}$$

In the first line to the second, we used Lemma 2.5, (2) and (1). From the first line to the second, we used the fact that $|\alpha|_p = p^{1/2}$ for supersingular primes p. From the second line to the third, we used Lemma 3.1. The argument for the inequality between the third and forth lines is the following. Recall that by the definition of $m_p^\pm(E)$ we can write $L_p^\pm(E, \alpha, T) = T^{m_p^\pm(E)} H(T)$ for some $H(T) \in R$. Then $|H(\chi(\gamma)^\sigma - 1)|_p \leq 1$, whence $|L_p^\pm(E, \alpha, \chi(\gamma)^\sigma - 1)|_p \leq |\chi(\gamma)^\sigma - 1|_p$. Applying equation (5) to y and taking the logarithm with base p (not the p-adic logarithm), we obtain

$$\log_p |y|_p^{-1} = m_p^\pm(E) - \varphi(p^{8+\delta}) \left(\frac{1}{2}(9+\delta) + \log_p |c_E|_p + c(8+\delta, p) \right). \tag{6}$$

On the other hand, using (1) and the analytic bounds for complex L-functions, we can show that

$$|x^\sigma|_\infty \leq C_1 p^{9+\delta} \tag{7}$$

for sufficiently large primes p where C_1 is a constant depending on E but not on p. We give the argument for (7) briefly here. It is well known that the absolute value of the Gauss sum is $|\tau(\overline{\chi})|_\infty = p^{9+\delta}$. Thus (1) can be written as

$$|x^\sigma|_\infty = \left| \frac{c_E p^{9+\delta} L(E, \overline{\chi}, 1)}{\Omega_E^+ \tau(\overline{\chi})} \right|_\infty \tag{8}$$

$$= p^{\frac{9+\delta}{2}} \left| \frac{c_E L(E, \overline{\chi}, 1)}{\Omega_E^+} \right|_\infty. \tag{9}$$

Now (7) would follow from an upper bound of the form

$$|L(E, \overline{\chi}, 1)|_\infty \leq p^{\frac{9+\delta}{2}} \tag{10}$$

since Ω_E^+ and c_E are independent of p. In fact, subconvexity bounds such as Theorem 3 of [3] shows better result then (10). However, these better estimations will hardly improve our final result so we use (10). The definition of y together with (7) implies that

$$|y|_\infty \leq \left(C_1 p^{9+\delta}\right)^{\varphi\left(p^{8+\delta}\right)}. \tag{11}$$

Apply (5) to y, then (6) and (11) imply that

$$\begin{aligned} &\varphi(p^{8+\delta})\left(\log_p C_1 + 9 + \delta\right) \\ &\geq m_p^{\pm}(E) - \varphi(p^{8+\delta})\left(\frac{9+\delta}{2} + \log_p |c_E|_p + c(8+\delta, p)\right). \end{aligned} \tag{12}$$

Rewriting (12) as an upper bound for $m_p^{\pm}(E)$, we obtain

$$m_p^{\pm}(E) \leq \varphi(p^{8+\delta})\left(\log_p C_1 + \frac{3}{2}(9+\delta) + c(8+\delta, p) + \log_p |c_E|_p\right). \tag{13}$$

By Lemma 3.1, $c(8+\delta, p)$ is an bounded by $8+\delta$, and $\log_p |c_E|_p^{-1}$ is independent of p. Also we have $\varphi(p^{8+\delta}) \leq p^{8+\delta}$. Thus, for sufficiently large p, (13) becomes

$$m_p^{\pm}(E) \leq p^{8+\delta}\left(\log_p C_1 + \frac{9+\delta}{2} + (8+\delta)\right). \tag{14}$$

The assertion of the theorem follows if we take $C = \log_p C_1 + \frac{3}{2}(9+\delta) + (8+\delta) + \log_p |c_E|_p$. □

Corollary 3.5. *We have $t_p \leq Cp^8 - g_E$.*

Proof. Consider the Pontryagin dual of the short exact sequence (3). By Proposition 3.2 and Theorem 3.4, we have $h_p \leq Cp^{8+\delta}$. Since $\mathbb{Z}_p$-rank is additive in exact sequences we also have $h_p = g_E + t_p$. Taking $\delta = 0$, we obtain the assertion. □

References

[1] G. Chinta, *Analytic ranks of elliptic curves over cyclotomic fields*, J. Reine Angew. Math. **544** (2002), 13–24.

[2] J. Coates, Z. Liang, and R. Sujatha, *The Tate-Shafarevich group for elliptic curves with complex multiplication II*, Milan J. Math. **78** (2010), no. 2, 395–416.

[3] W. Duke, J. B. Friedlander, and H. Iwaniec, *Bounds for automorphic L-functions. II*, Invent. Math. **115** (1994), no. 2, 219–239.

[4] D. Kim, *On the Tate-Shafarevich group of elliptic curves over* $\mathbb{Q}$, Bull. Korean Math. Soc. **49** (2012), no. 1, 155–163.

[5] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[6] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil Cuves*, Invent. Math. **25** (1974), 1–61.

[7] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

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

Department of Mathematics
Pohang University of Science and Technology
Pohang 790-784, Korea
E-mail address: polygon0307@gmail.com