Bull. Korean Math. Soc. **49** (2012), No. 1, pp. 155–163
http://dx.doi.org/10.4134/BKMS.2012.49.1.155

ON THE TATE-SHAFAREVICH GROUP OF ELLIPTIC CURVES OVER $\mathbb{Q}$

Dohyeong Kim

Abstract. Let E be an elliptic curve over $\mathbb{Q}$. Using Iwasawa theory, we give what seems to be the first general upper bound for the order of vanishing of the p-adic L-function at $s = 0$, and the $\mathbb{Z}_p$-corank of the Tate-Shafarevich group for all sufficiently large good ordinary primes p.

1. Introduction

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

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

where v runs over all places of $\mathbb{Q}$, and $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ at v. Let p be a prime number. 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 $s = 1$. In principle, arguments from Galois cohomology give an upper bound for t_p, but the estimate is so bad that no one has ever written it down. In this paper, we will use p-adic arguments from Iwasawa main conjecture, combined with a theorem in [1] on the non-vanishing of twisted complex L-functions, to give an upper bound for the order of vanishing of p-adic L-function at at the Birch-Swinerton-Dyer point in the p-adic plane, which we normalize to be the point $s = 0$. We prove:

Theorem 1. *Let p be a prime of good ordinary reduction for E. Let h'_p be the order of vanishing at $s = 0$ of the p-adic L-function of E. Then, $h'_p \leq Cp^8$, where $C > 0$ is independent of p but dependent on E.*

As a corollary, we prove:

Received September 24, 2010; Revised January 1, 2011.
2010 *Mathematics Subject Classification.* 11G05.
Key words and phrases. good ordinary reduction, Tate-Shafarevich group, elliptic curves, Iwasawa theory.

Corollary 1. *Let C be the constant appearing in the above theorem. Then $t_p \leq Cp^8 - g_E$ for all good ordinary primes p.*

Our proof uses some deep arithmetic results, which includes the modularity of E, the non-vanishing theorem in [1], and Kato's proof of a weak form of the Iwasawa main conjecture for E over the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{cyc}$ of $\mathbb{Q}$ [4]. We hope to prove an analogous result for supersingular primes in a subsequent paper. In the special case in which E admits complex multiplication, the stronger result is proven in [2] that $t_p \leq (1/2 + \epsilon)p$ for all sufficiently large good ordinary primes p, but the proof is special to elliptic curves with complex multiplication.

Acknowledgments. I would like to thank John Coates for introducing the field of Iwasawa theory of elliptic curves and suggesting the problem to me. Without the valuable discussions we had, this article would not have been written. I wish to thank YoungJu Choie from whom I learned the analytic theory of modular forms. Jeehoon Park is also acknowledged for carefully reading the manuscript and giving me numerous suggestions. Finally, I would like to thank David Rohrlich for pointing out the improved result on non-vanishing proved in [1].

2. The complex and p-adic L-function

Let N be the conductor of E. By the modularity theorem, there exists a primitive cusp form of weight 2 for $\Gamma_0(N)$

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n}$$

such that the complex L-function $L(E, s)$ is equal to $L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}$. In particular, this deep result establishes the analytic continuation and functional equation for $L(E, s)$, and all its twists by Dirichlet characters. Unfortunately, even though it is predicted by the conjecture of Birch and Swinnerton-Dyer no way is known at present for showing that $L(E, s)$ has a zero at $s = 1$ of order greater than or equal to g_E, the rank of $E(\mathbb{Q})$. However, using Iwasawa theory, one can show this holds for the p-adic analogue of the complex L-function. Let p be a prime number not dividing N and let χ be a Dirichlet character of conductor p^r for some positive integer r. Write f_χ (resp. $L(f, \chi, s)$) for the twist of f (resp. $L(E, s)$) by χ defined by $f_\chi(\tau) = \sum_{n=1}^{\infty} a_n \chi(n) e^{2\pi i n}$ (resp. $L(E, \chi, s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$). Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and fix embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$. Further assume that E has good ordinary reduction at p. It is well known that p is an ordinary prime for E if and only if p does not divide a_p. In this case, there is a unique root α of $X^2 - a_p X + p$, which is a p-adic unit. Let Ω_E^+ be the smallest positive real period of a Néron differential on a global minimal equation for E over $\mathbb{Q}$. If χ is a dirichlet character, let $\overline{\chi}$ be its complex conjugate and let $\tau(\overline{\chi})$ be the associated Gauss sum. For $s \in \mathbb{Z}_p$, we have the p-adic L-function $L_p(f, \chi, s)$, which has the following interpolation property (See §14 of [6]).

Theorem 2. *Let p be any prime of good ordinary reduction. Then, if χ is a nontrivial Dirichlet character of conductor $p^r > 1$, we have*

$$L_p(f, \chi, 0) = \frac{p^r L(f, \overline{\chi}, 1)}{\Omega_E^+ \alpha^r \tau(\overline{\chi})}. \tag{1}$$

We need an interpretration of this p-adic L-function in terms of formal power series with coefficients in $\mathbb{Z}_p$. Put $\Gamma = \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q})$ and pick a topological generator γ for Γ. We identify the Iwasawa algebra $\Lambda(\Gamma)$ with $\mathbb{Z}_p[[T]]$ by sending γ to $1 + T$. Fix an isomorphism $\mathbb{Z}_p^\times \cong \Delta \times \mathbb{Z}_p$ and identify $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ with $\mathbb{Z}_p^\times$ via the p-adic cyclotomic character. Now we can regard Dirichlet characters of p-power conductor and p-power order as characters for Γ.

It is then well-known (See Theorem in §14 of [6]) that there exists an integer c_E and an element

$$G(T) \in c_E^{-1} \mathbb{Z}_p[[T]] \tag{2}$$

such that $L_p(f, \chi, 0) = G(\chi(\gamma) - 1)$ for all Dirichlet characters χ of p-power conductor and p-power order. Note that, by the Weierstrass preparation theorem, such a $G(T)$ is uniquely determined by the values $G(\chi(\gamma) - 1)$ for all Dirichlet characters χ. We remark that c_E is known to be 1 in most cases, but it is not important for us.

3. Integrality of certain L-values

Define

$$\phi(r) := 2\pi i \int_\infty^r f(z) dz$$

for r in $\mathbb{Q} \cup \{\infty\}$. Write Φ for the image of ϕ. Let Ω_E^- be the least purely imaginary period of the Néron differential. It is well-known that there is an integer c_E satisfying the equation (2) and such that $c_E \Phi$ is contained in the lattice generated by $\Omega_E^\pm$ (See Thm 1.2. of [5]).

Proposition 1. *Let χ be an even Dirichlet character of conductor p^r. Then, $\alpha^r c_E L_p(f, \chi, 0)$ is an algebraic integer in $\mathbb{Q}(\chi)$, the field generated by the values of χ.*

Proof. By Birch's lemma, if χ is a Dirichlet character of conductor m, then we have

$$f_\chi(z) = \frac{1}{\tau(\bar{\chi})} \sum_{a \bmod m} \bar{\chi}(a) f(z + \frac{a}{m}).$$

Applying it to the equation (1), we obtain

$$L_p(f, \chi, 0) = \frac{p^r L(f, \overline{\chi}, 1)}{\Omega_E^+ \alpha^r \tau(\overline{\chi})} = \frac{1}{\Omega_E^+ \alpha^r} \sum_{a \bmod m} \chi(a) \phi(\frac{a}{m}).$$

In the last line, we used the representation of the complex L-function by the integral

$$L(f,\overline{\chi},1)=2\pi i\int_{\infty}^{0} f_{\overline{\chi}}(z)dz \tag{3}$$

and the formula $|\tau(\chi)|^2 = p^r$. Multiplying both sides by $c_E\alpha^r$, we get the result from the assumption that χ is an even character. □

4. p-adic L-function and the main conjecture

We recall the structure theory of finitely generated torsion $\Lambda(\Gamma)$-modules. Let A be a finitely generated torsion $\Lambda(\Gamma)$-module. Then there is an exact sequence

$$0 \longrightarrow \bigoplus_{j=1}^{k} \Lambda(\Gamma)/F_j\Lambda(\Gamma) \longrightarrow A \longrightarrow D \longrightarrow 0\ ,$$

where D is finite and F_j's are nonzero elements in $\Lambda(\Gamma)$. Let F be the product of all F_j's. We call F a characteristic power series of A and it is well-defined up to multiplication by a unit of $\Lambda(\Gamma)$. If we have a short exact sequence of torsion $\Lambda(\Gamma)$-modules

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0\ ,$$

then $F\cdot\Lambda(\Gamma) = F'F''\cdot\Lambda(\Gamma)$, where F, F' and F'' denote characteristic power series of A, A' and A'' respectively. We recall that the (p-primary) Selmer group is defined by

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

where K is a finite extension of $\mathbb{Q}$ and $E[p^\infty]$ denotes the Galois module of p-power division points of $E(\overline{\mathbb{Q}})$. Put

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

where K runs over the finite extensions of $\mathbb{Q}$ contained in $\mathbb{Q}^{cyc}$, and the inductive limit is taken with respect to the restriction maps on the Galois groups. Define the Pontryagin dual of the Selmer group as

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

The following deep theorem (Theorem 17.4 in [4]), which says that one divisibility of the Iwasawa main conjecture is true, is due to Kato.

Theorem 3. *Let $G(T)$ be the power series from Section 2 corresponding to $L_p(f,\chi,s)$. Then $X(E/\mathbb{Q}^{cyc})$ is a torsion $\Lambda(\Gamma)$-module and its characteristic power series $F(T)$ divides $p^nG(T)$ for some non-negative integer n.*

Using the above theorem of Kato, we will prove the following theorem which is one of the main ingredients for the proof of Theorem 1.

Proposition 2. *Let h_p be the $\mathbb{Z}_p$-corank of* $\mathrm{Sel}(E/\mathbb{Q})$. *Then $G(T)=T^{h_p}G_0(T)$, where $G_0(T)$ is an element of $c_E^{-1}\mathbb{Z}_p[[T]]$. In other words, $h_p \le h'_p$, where h'_p denotes the exact power of T dividing $G(T)$.*

Proof. Let S be the set containing p and the primes where E has bad reduction. Denote by $\mathbb{Q}_S$ the maximal extension of $\mathbb{Q}$ unramified outside S and the archimedean places. Consider following exact sequence

$$0 \longrightarrow \mathrm{Ker}(\alpha) \longrightarrow \mathrm{Sel}(E/\mathbb{Q}) \xrightarrow{\alpha} \mathrm{Sel}(E/\mathbb{Q}^{cyc}) ,$$

where α is the restriction map. To simplify notation, let B' be $E[p^\infty]$ and B be $E[p^\infty](\mathbb{Q}^{cyc})$. I claim that the image of α is contained in $\mathrm{Sel}(E/\mathbb{Q}^{cyc})^\Gamma$. Indeed, we have $\mathrm{Sel}(E/\mathbb{Q}) \subset H^1(G_S, B')$ and $\mathrm{Sel}(E/\mathbb{Q}^{cyc}) \subset H^1(G_S^{cyc}, B')$, where $G_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ and $G_S^{cyc} = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{cyc})$ (See Ch.X Cor4.4, [7]). Then it follows from the inflation-restriction sequence that

$$0 \longrightarrow H^1(\Gamma, B) \longrightarrow H^1(G_S, B') \xrightarrow{\alpha'} H^1(G_S^{cyc}, B')^\Gamma .$$

Since $G_S^{cyc} = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}^{cyc})$ and α is restriction of α', Γ acts trivially on the image of α. Now note that the group $H^1(\Gamma, B)$ sits inside the 4-term exact sequence

$$0 \longrightarrow B^\Gamma \longrightarrow B \xrightarrow{1-\gamma} B \longrightarrow H^1(\Gamma, B) \longrightarrow 0 .$$

Since $B^\Gamma = E[p^\infty](\mathbb{Q})$ is finite and the alternating sum of $\mathbb{Z}_p$-corank is 0 in an exact sequence, it follows that $\mathrm{Ker}(\alpha)$ is also finite. Taking the Pontryagin dual of α, we have a map

$$X(E/\mathbb{Q}^{cyc})_\Gamma \longrightarrow X(E/\mathbb{Q}) = \mathbb{Z}_p^{h_p} \times \text{a finite group}$$

with finite cokernel. Taking further quotient of the latter, we may assume that $X(E/\mathbb{Q}^{cyc})$ maps surjectively onto $\mathbb{Z}_p^{h_p}$. Composing the above map with the natural surjection from $X(E/\mathbb{Q}^{cyc})$ to $X(E/\mathbb{Q}^{cyc})_\Gamma$, we obtain a Γ-equivariant surjective homomorphism

$$\beta\colon X(E/\mathbb{Q}^{cyc}) \longrightarrow \mathbb{Z}_p^{h_p},$$

where Γ acts trivially on $\mathbb{Z}_p^{h_p}$. In other words, we have a Γ-equivariant short exact sequence

$$0 \longrightarrow \mathrm{Ker}(\beta) \longrightarrow X(E/\mathbb{Q}^{cyc}) \xrightarrow{\beta} \mathbb{Z}_p^{h_p} \longrightarrow 0 .$$

Note that then a characteristic power series of $\mathbb{Z}_p^{h_p}$ as $\Lambda(\Gamma)$-module is T^{h_p}. If we denote by $F_0(T)$ a characteristic power series of $\ker(\beta)$, we have $F(T) = T^{h_p}F_0(T)$ from the above short exact sequence. Now we apply Theorem 3 to obtain

$$T^{h_p}F_0(T)F_1(T) = p^n G(T)$$

for some $F_1(T)$ in $\Lambda(\Gamma)$. Since $\mathbb{Z}_p[[T]]$ is a UFD, the assertion follows. □

We remark that no analogue of this argument is known for the complex L-function.

5. The proof of the main theorem

We need the following result (Theorem 3 in [1]) due to Chinta.

Theorem 4. *Let E be an elliptic curve of level N. Let q be a power of an odd prime number with $(q, N) = 1$, and χ a primitive Dirichlet character* mod q. *Then*

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

provided that

$$\sigma_1\left(\frac{\varphi(q)}{\operatorname{ord}(\chi)}\right) \leq q^{\delta}, \qquad \delta < 1/8$$

and

$$q \gg_{\epsilon} N^{1/(1-8\delta-\epsilon)}. \tag{4}$$

The implied constant depends only on δ and ϵ, and $\sigma_1(m)$ is the sum of positive divisors of m.

For our application, we fix δ and ϵ and, therefore, the right side of the equation (4) is a constant independent of p. An immediate corollary is the following.

Corollary 2. *Under the same assumptions as above,*

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

for all primitive Dirichlet characters χ modulo p^r of p-power order provided that $r \geq 9$ and p is sufficiently large.

Proof. If χ has conductor p^r and p-power order, then $\varphi(q) = \operatorname{ord}(\chi)(p-1)$. From elementary number theory, we have a bound $\sigma_1(m) = o(m^{1+\epsilon})$ for any ϵ (For the proof see Theorem 322 of [3]). Therefore, the conditions of Theorem 4 are satisfied if p is sufficiently large and $r \geq 9$. □

Suppose now that χ is a Dirichlet character of conductor p^r and order p^{r-1}. By class field theory, we can view such a χ as a character of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Put $x = \alpha^r c_E L_p(f, \chi, 0)$. For $\sigma \in \operatorname{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$, we write x^σ for the image of x under σ. We will apply the product formula to $\prod_\sigma x^\sigma$ to prove Theorem 1. From now assume that x is nonzero, which is guaranteed by Theorem 4 when $r \geq 9$ and p is sufficiently large. We first prove the following estimations which will be used in the proof of Theorem 1. Recall that $T^{h'_p}$ is the exact power of p dividing the formal power series $G(T)$, say $G(T) = T^{h'_p} G_1(T)$.

Lemma 1. *For all sufficiently large good ordinary primes p, we have $|x^\sigma|_p \leq p^{-h'_p/\varphi(p^{r-1})}$.*

Proof. Without loss of generality, we assume that σ is the identity. If we put $\zeta := \chi(\gamma)$, then ζ is a primitive p^{r-1}-th root of unity. By Proposition 2, we have

$$L_p(f, \chi, 0) = (\zeta - 1)^{h'_p} G_1(\zeta - 1).$$

Applying Proposition 2, we obtain

$$\begin{aligned} |x|_p &= |\alpha^r c_E L_p(f, \chi, 0)|_p \\ &= |(\zeta - 1)^{h'_p} G_1(\zeta - 1)|_p \\ &\leq p^{-h'_p/\varphi(p^{r-1})}. \end{aligned}$$

□

Lemma 2. *Suppose χ is a Dirichlet character of conductor p^r. Let χ^σ be the Dirichlet character defined by $\chi^\sigma(n) = \sigma(\chi(n))$. We have $|L(f, \overline{\chi}^\sigma, 1)| \leq C_1 p^{r/2}$.*

Proof. Without loss of generality, we may assume σ is the identity. We use Birch's lemma. Recall that there are finitely many cusps and there is a bound C_1 which depends only on E such that $C_1 \geq |\phi(r)|$ for all $r \in \mathbb{Q} \cup \{\infty\}$.

$$\begin{aligned} |L(f_{\overline{\chi}}, 1)| &= \left| 2\pi \int_0^\infty f_{\overline{\chi}}(it) dt \right| \\ &= \left| 2\pi \int_0^\infty \frac{1}{\tau(\chi)} \sum_a \chi(a) f(it + \frac{a}{p^r}) dt \right| \\ &\leq C_1 p^{r/2}. \end{aligned}$$

In the last line we used the formula $|\tau(\chi)| = p^{r/2}$ and the integral of one of the p^r terms in the summation is at most C_1. □

To connect the estimations of p-adic absolute value and complex one, we observe the following. For each place v of $\mathbb{Q}$, let $| \, |_v$ be the corresponding valuation. Then the product formula asserts that

$$\prod_v |a|_v = 1$$

for all non-zero a in $\mathbb{Q}$. In particular, if a is a non-zero integer, this implies that

$$|a|_v \geq |a|_\infty^{-1}$$

for every finite place v. Using this, we obtain the following inequality.

Proposition 3. *We have*

$$h'_p \leq r\varphi(p^{r-1}) + \varphi(p^{r-1}) \log_p C_2.$$

In particular, there is a constant C_0 such that we have

$$h'_p \leq C_0 r p^{r-1}. \tag{5}$$

Proof. We begin from the product formula;

$$\Big|\prod_\sigma x^\sigma\Big|_p^{-1} \le \Big|\prod_\sigma x^\sigma\Big|_\infty.$$

Here σ runs through $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ which has $\varphi(p^{r-1})$ elements. Applying Lemma 1 to the left-hand-side, we obtain

$$C_1^{-\varphi(p^{r-1})} p^{h'_p} \le \Big|\prod_\sigma x^\sigma\Big|_p^{-1}. \tag{6}$$

To the right-hand-side, we apply Lemma 2 and Theorem 2 to obtain

$$\Big|\prod_\sigma x^\sigma\Big|_\infty \le \big|C_1 p^r c_E/\Omega_E^+\big|_\infty^{\varphi(p^{r-1})} = C_2^{\varphi(p^{r-1})} p^{r\varphi(p^{r-1})}, \tag{7}$$

where $C_2 = c_E C_1/\Omega_E^+$ only depends on E. Here we used $|\tau(\chi)| = p^{r/2}$ and Theorem 2. Combining the equations (6) and (7) and taking logarithms to the base p, we obtain

$$h'_p \le \varphi(p^{r-1}) \log_p C_2 + r\varphi(p^{r-1}). \qquad \square$$

Now we can prove Theorem 1. Taking a Dirichlet character χ of conductor p^9 and order p^8 with a sufficiently large prime p, x is nonzero by Corollary 2. Then the equation (5) is now

$$h'_p \le 9C_0 p^8. \tag{8}$$

By Theorem 2, we have $h_p \le h'_p$ and the proof of Theorem 1 is complete.

Now we prove Corollary 1. Consider the exact sequence

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

Since $\mathbb{Z}_p$-corank of $E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is g_E and the $\mathbb{Z}_p$ corank is additive in a short exact sequence of abelian groups, we have $g_E + t_p = h_p$. Therefore, we have $t_p \le Cp^8 - g_E$ by Theorem 1.

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] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford Science Publications, 1938.

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

[5] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[6] 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.

[7] J. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Graduate Texts in Mathematics, vol. **106**, Springer, 2008.

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