Trends in Mathematics
Information Center for Mathematical Sciences
Volume 9, Number 1, June, 2006, Pages 49–53

ELLIPTIC CURVES WITH LARGE TATE-SHAFAREVICH GROUPS

KAZUO MATSUNO

The Tate-Shafarevich group $Ш(E/K)$ of an elliptic curve E over a number field K is defined as

$$Ш(E/K) := \mathrm{Ker}\Big(H^1(K, E(\overline{K})) \longrightarrow \prod_v H^1(K_v, E(\overline{K_v}))\Big),$$

where v runs over all (archimedean and non-archimedean) primes of K. This $Ш(E/K)$ describes the failure of "Hasse principle" for the torsors of E/K. It is conjectured that $Ш(E/K)$ is finite (still unknown in general).

The following question is very natural, but we don't know the answer.

Question 1. *For each prime p, does there exist an elliptic curve E over $\mathbb{Q}$ such that the p-torsion subgroup $Ш(E/\mathbb{Q})[p]$ of $Ш(E/\mathbb{Q})$ is nonzero?*

We can give examples of such elliptic curves for small primes.

- $E : y^2 = x^3 + 17x \Rightarrow Ш(E/\mathbb{Q})[2] \neq 0$. (Lind, Reichardt, '40s)
- $E : y^2 = x^3 - 24300 \Rightarrow Ш(E/\mathbb{Q})[3] \neq 0$. (Selmer, 1951)
- $E : y^2 + xy = x^3 - 3301465x - 2309192023 \Rightarrow Ш(E/\mathbb{Q})[5] \neq 0$.
- $E : y^2 + xy = x^3 - 3674496x - 2711401518 \Rightarrow Ш(E/\mathbb{Q})[7] \neq 0$.
- $E : y^2 = x^3 + x^2 - 21477749985x - 1211529110734587 \Rightarrow Ш(E/\mathbb{Q})[13] \neq 0$.

Remark. One can verify the above assertions for $p = 5$ and 7 by a p-descent argument (cf. [Be], [Fi]) or by a result of Cassels [Ca2] together with the fact that $\mathrm{rank} E(\mathbb{Q}) = 0$. The second argument also works for $p = 13$ (cf. [Ma]).

- $E : y^2 = x^3 - 20675209x \Rightarrow Ш(E/\mathbb{Q})[11] \neq 0$.
- $E : y^2 = x^3 - 239228089x \Rightarrow Ш(E/\mathbb{Q})[17] \neq 0$.
- $E : y^2 = x^3 - 258904415517049x \Rightarrow Ш(E/\mathbb{Q})[211] \neq 0$.

Remark. These curves have complex multiplication by $\mathbb{Z}[\sqrt{-1}]$. For such CM curves, Rubin [Ru] proved the full Birch and Swinnerton-Dyer conjecture (modulo 2-parts). The above assertions is verified by using this fact and a result of Tunnell [Tu]. Another computation can be found in [Ro].

Moreover the following question has already been solved affirmatively for $p \leq 5$.

Question 2. *For each prime p, can $\dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p]$ be arbitrarily large as E varies?*

Theorem (Cassels, Bölling, Fisher, ...). *Assume that $p \leq 5$. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p] \mid E \in \mathcal{E}_{\mathbb{Q}}\} = +\infty.$$

Here $\mathcal{E}_{\mathbb{Q}}$ is the set of (the $\mathbb{Q}$-isomorphism classes of) elliptic curves defined over $\mathbb{Q}$.

This result was first obtained for $p = 3$ by Cassels [Ca1] by extending previous works of Selmer. The case $p = 2$ (in a more general statement) was proved by Bölling [Bö] and another proofs and generalizations were given by several authors (e.g., Kramer [Kr]). The case $p = 5$ was proved by Fisher [Fi].

For $p = 7$ and 13, Kloosterman and Schaefer gave the following partial result.

Theorem (Kloosterman-Schaefer [KS]). *Assume that p is an odd prime with $p \leq 7$ or $p = 13$. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p] + \mathrm{rank} E(\mathbb{Q}) \mid E \in \mathcal{E}_{\mathbb{Q}}\} = +\infty.$$

Especially, either $\mathrm{rank} E(\mathbb{Q})$ or $\dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p]$ can be arbitrarily large as E varies.

The first result of this note is an affirmative answer to Question 2 for $p = 7, 13$.

Theorem A ([Ma]). *Assume that $p = 3, 5, 7, 13$. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p] \mid E \in \mathcal{E}_{\mathbb{Q}}\} = +\infty.$$

To prove this theorem (and some results mentioned above), we need the fact that there exist infinitely many elliptic curves defined over $\mathbb{Q}$ (non-isomorphic over $\overline{\mathbb{Q}}$) with isogenies of degree p. This assumption is equivalent to assuming that the genus of the modular curve $X_0(p)$ is 0. Therefore we cannot prove the assertion of Question 2 for $p = 11$ or $p \geq 17$ by a similar argument. The following question (easier than Question 2) can be handled.

Question 3. *For each prime p, can $\dim_{\mathbb{F}_p} Ш(E/K)[p]$ be arbitrarily large as K and E vary?*

Theorem. (i) ([KS]) *Let $g(p)$ denote the genus of $X_0(p)$. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] + \mathrm{rank} E(K) \mid [K:\mathbb{Q}] \leq g(p) + 1,\ E \in \mathcal{E}_K\} = +\infty.$$

(ii) (Kloosterman [Kl]) *There exists a function $h : \mathbb{Z} \to \mathbb{Z}$ such that*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] \mid [K:\mathbb{Q}] \leq h(p),\ E \in \mathcal{E}_K\} = +\infty$$

and $h(p) = O(p^4)$ for $p \to \infty$.

Remark. We have $g(p) \leq \frac{p+1}{12}$ for any p. In particular, $g(p) = O(p)$ for $p \to \infty$.

The above theorem says the answer to Question 3 is "yes" even if the range of number fields K is limited by some bounded degree (depending on p). Our next task is to consider Question 3 in more smaller range of K and E (e.g., for fixed K or E, for more smaller bound of degree of K, etc.). Clark [Cl] proved that the assertion of Question 3 is still valid when an elliptic curve E is fixed.

Theorem (Clark [Cl])**.** *Let E be an elliptic curve defined over a number field F. Assume that $E[p]$ is contained in $E(F)$. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] \mid [K:F]=p\}=+\infty.$$

This theorem implies that $Ш(E/K)[p]$ can be arbitrarily large as K varies between degree p extensions of $\mathbb{Q}(E[p])$ for any fixed elliptic curve E defined over $\mathbb{Q}$. We have $[\mathbb{Q}(E[p]):\mathbb{Q}] \le \#GL_2(\mathbb{F}_p) = p(p-1)^2(p+1)$ in general and further $[\mathbb{Q}(E[p]):\mathbb{Q}] \le 2(p-1)^2$ if E has complex multiplication. Therefore Clark's result also refines Kloosterman's result mentioned above as follows.

Corollary. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication. Then*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] \mid [K:\mathbb{Q}] \le 2p(p-1)^2\}=+\infty.$$

Another refinement for small primes was recently obtained by Naganuma by using arguments given in [KS] and [Ma].

Theorem (Naganuma [Na])**.** *Let K be a number field such that $X_0(p)$ has infinitely many K-rational points. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] + \mathrm{rank} E(K) \mid E \in \mathcal{E}_K\}=+\infty.$$

Furthermore, if K is totally real and "modularity conjecture" for elliptic curves defined over K is valid, then

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] \mid E \in \mathcal{E}_K\}=+\infty.$$

As mentioned before, $X_0(p)$ has infinitely many $\mathbb{Q}$-rational points if $p \le 7$ or $p = 13$. Since the modularity conjecture over $\mathbb{Q}$ (Taniyama-Shimura conjecture) is known, Theorem A is included in Naganuma's result. His result also refines the result of [KS] for the case $g(p) = 1$, i.e., $p = 11, 17, 19$. Indeed, for such p, there exist infinitely many (real) quadratic fields K such that $\#X_0(p)(K) = +\infty$. For example, $\#X_0(11)(\mathbb{Q}(\sqrt{2})) = +\infty$. By applying a result of Skinner-Wiles [SW], we can prove the following as a consequence.

Corollary. $\sup\{\dim_{\mathbb{F}_{11}} Ш(E/\mathbb{Q}(\sqrt{2}))[11] \mid E \in \mathcal{E}_{\mathbb{Q}(\sqrt{2})}\} = +\infty.$

However, Naganuma's result does not cover the case $p \ge 23$ since the genus of $X_0(p)$ is greater than 1 and hence $\#X_0(p)(K)$ is finite for any number field K. The second result of this note is the unboundedness of the p-rank of Tate-Shafarevich groups over a (fixed) number field of degree p.

Theorem B. *Let K be a cyclic Galois extension of $\mathbb{Q}$ of degree p. Then we have*

$$\sup\{\dim_{\mathbb{F}_p} Ш(E/K)[p] \mid E \in \mathcal{E}_{\mathbb{Q}}\}=+\infty.$$

The proofs of Theorems A and B are separated into two steps:

(i) To give a condition that the p-Selmer group of an elliptic curve is large enough.

(ii) To construct an elliptic curve satisfying the condition given by (i) and having small Mordell-Weil rank.

Here the p-Selmer group $\mathrm{Sel}^{(p)}(E/K)$ of an elliptic curve E over K is a subgroup of $H^1(K, E[p])$ satisfying some local conditions. We have an exact sequence

$$0 \longrightarrow E(K)/pE(K) \longrightarrow \mathrm{Sel}^{(p)}(E/K) \longrightarrow Ш(E/K)[p] \longrightarrow 0.$$

This implies an inequality

$$\dim_{\mathbb{F}_p} Ш(E/K)[p] \geq \dim_{\mathbb{F}_p} \mathrm{Sel}^{(p)}(E/K) - \mathrm{rank} E(K) - 2.$$

Therefore the above (i) and (ii) are enough to prove the theorems.

- Theorem A-(i): Assume that there exists an isogeny $E \to E'$ of degree p and the number of bad primes of E' such that the Tamagawa number is divisible by p is large enough than that for E. Then the p-Selmer group of E becomes large. One can prove this by using a result of Cassels [Ca2] as in [KS]. Another proof based on Iwasawa theory for elliptic curves, especially on Mazur's control theorem (cf. [Gr]), is given in [Ma].
- Theorem B-(i): The condition is similar to the above, but a p-isogeny is not needed. We use an analogue of Mazur's control theorem for cyclic extensions of degree p.
- Theorem A-(ii): We first construct an elliptic curve E with large $\mathrm{Sel}^{(p)}(E/\mathbb{Q})$ by (i). Then we take a quadratic twist E'' of E so that the condition in (i) is again satisfied and the central value of the L-function of E'' is nonzero. The existence of such twists is ensured by Waldspurger's theorem (cf. [BFH, §0]). Then we have $\mathrm{rank} E''(\mathbb{Q}) = 0$ by Kolyvagin's result and $\mathrm{Sel}^{(p)}(E''/\mathbb{Q})$ is large by (i).
- Theorem B-(ii): In order to bound the Mordell-Weil rank, we use an argument given in [Kr] and a result obtained by sieve methods ([HR, Theorem 10.5]).

References

[Be] C. D. Beaver, *5-torsion in the Shafarevich-Tate group of a family of elliptic curves*, J. Number Theory **82** (2000), 25–46.

[Bö] R. Bölling, *Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig groß werden*, Math. Nachr. **67** (1975), 157–179.

[BFH] D. Bump, S. Friedberg and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. math. **102** (1990), 543–618.

[Ca1] J. W. S. Cassels, *Arithmetic on curves of genus 1, VI. The Tate-Šafarevič group can be arbitrarily large*, J. reine angew. Math. **214/215** (1964), 65–70.

[Ca2] J. W. S. Cassels, *Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **217** (1965), 180–199.

[Cl] P. L. Clark, *The period-index problem in WC-groups I: elliptic curves*, J. Number Theory **114** (2005), 193–208.

[Fi] T. Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\mathbb{Q}$, J. Eur. Math. Soc. **3** (2001), 169–201.

[Gr] R. Greenberg, *Iwasawa theory for elliptic curves*, in "Arithmetic Theory of Elliptic Curves", Lecture Notes in Math., vol. 1716, Springer-Verlag, 1999, pp. 51–144.

[HR] H. Halberstam and H.-E. Richert, "Sieve Methods", Academic Press, 1974.

[Kl] R. Kloosterman, *The p-part of Shafarevich-Tate groups of elliptic curves can be arbitrarily large*, J. Theorie Nombres Bordeaux **17** (2005), 787–800.

[KS] R. Kloosterman and E. F. Schaefer, *Selmer groups of elliptic curves that can be arbitrarily large*, J. Number Theory **99** (2003), 148–163.

[Kr] K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Amer. Math. Soc. **89** (1983), 379–386.

[Ma] K. Matsuno, *Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups*, preprint, 2005 (submitted).

[Na] K. Naganuma, talk at Waseda University, October, 2005.

[Ro] H. E. Rose, *On some elliptic curves with large Sha*, Experimental Math. **9** (2000), 85–89.

[Ru] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. math. **103** (1991), 25–68.

[SW] C. M. Skinner and A. J. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse **10** (2001), 185–215.

[Tu] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. math. **72** (1983), 323–334.

Department of Mathematics and Information Sciences, Tokyo Metropolitan University
1-1, Minami-Ohsawa, Hachioji, Tokyo, 192-0397, Japan
E-mail address: matsuno@comp.metro-u.ac.jp