TOKYO J. MATH.
VOL. 29, NO. 2, 2006

A Remark on the Mordell-Weil Rank of Elliptic Curves over the Maximal Abelian Extension of the Rational Number Field

Emi KOBAYASHI

Tokyo Metropolitan University

(Communicated by Y. Ohnita)

Abstract. In this paper, we study the Mordell-Weil ranks of elliptic curves defined over the maximal abelian extension of the rational number field, assuming several conjectures on the Hasse-Weil L-functions. We prove that an elliptic curve defined over an abelian field with odd degree has infinite rank over the maximal abelian extension of the rational number field. This result gives affirmative evidence for 'the largeness' (in the sense of Pop) of the maximal abelian extension of the rational number field.

1. Introduction

In the arithmetic of elliptic curves, Mordell-Weil groups are very important objects. Let E be an elliptic curve defined over a number field K. If K' is a finite extension over K, $E(K')$ is a finitely generated abelian group by Mordell-Weil's theorem. But if K' is an infinite algebraic extension over K, $E(K')$ may be finitely generated and sometimes not. Let $\mathbf{Q}^{ab}$ be the maximal abelian extension of $\mathbf{Q}$. We consider an elliptic curve E defined over $\mathbf{Q}^{ab}$. Then E is defined over some finite abelian extension K over $\mathbf{Q}$. We study $E(\mathbf{Q}^{ab}) = \bigcup_{K \subset L \subset \mathbf{Q}^{ab},\ [L:K]<\infty} E(L)$ and conjecture the following.

CONJECTURE 1. $\mathrm{rank}_{\mathbf{Z}} E(\mathbf{Q}^{ab}) = \infty$.

As background for this problem, we will explain Pop's theory. In [1], Pop introduced the notion of large fields and proved the following theorem.

THEOREM 1 (Pop). *Let F be a field. Assume the following conditions*
(1) *F is hilbertian,*
(2) *F has cohomological dimension* 1,
(3) *F has countably infinite order,*
(4) *F is large.*
Then the absolute Galois group of F is isomorphic to the free group with countably infinitely many generators.

Received March 3, 2005

Shafarevich's conjecture asserts that the absolute Galois group of $\mathbf{Q}^{ab}$ is isomorphic to the free group with countably infnitely many generators. It is well-known that $\mathbf{Q}^{ab}$ satisfies the conditions (1)–(3) in Theorem 1. Therefore if $\mathbf{Q}^{ab}$ is a large field, Shafarevich's conjecture follows. We are interested in whether $\mathbf{Q}^{ab}$ is large or not, which is an open problem.

DEFINITION 1 (Pop). Let F be a field. F is a large field if and only if F satisfies the following two conditions which are equivalent.

(1) For any smooth curve C defined over F, $C(F) \neq \emptyset$ implies $\sharp C(F) = \infty$.

(2) For every integral variety X defined over F, $X(F) \neq \emptyset$ implies that $X(F)$ is Zariski dense in $X(\bar{F})$.

Thus if $\mathbf{Q}^{ab}$ is large, we have the following.

CONJECTURE 2. *If C is a smooth curve defined over $\mathbf{Q}^{ab}$ and $C(\mathbf{Q}^{ab}) \neq \emptyset$, we have $\sharp C(\mathbf{Q}^{ab}) = \infty$.*

To begin with, in the case that the genus of C is 0, clearly this is true. Next we proceed to the case that the genus of C is 1 and C has a rational point, namely the case that C is an elliptic curve. Let E be an elliptic curve defined over $\mathbf{Q}^{ab}$. We would like to know whether the order of $E(\mathbf{Q}^{ab})$ is infinite or not. It is known by a theorem of Ribet ([2]), that its torsion part $E(\mathbf{Q}^{ab})_{\mathrm{tors}}$ is a finite abelian group. Concerning the Mordell-Weil rank over large fields, we know the following by Tamagawa.

PROPOSITION 1 (Tamagawa). *Let E be an elliptic curve defined over a field K of characteristic* 0. *Assume that K is a large field. Then we have* $\mathrm{rank}_{\mathbf{Z}} E(K) = \infty$.

We prove this proposition in the last section. By this proposition, the largeness of $\mathbf{Q}^{ab}$ implies Conjecture 1. Note that if E is defined over $\mathbf{Q}$ it is easy to check Conjecture 1. Because we know that $\mathrm{rank}_{\mathbf{Z}} E(\mathbf{Q}^{quad}) = \infty$ where $\mathbf{Q}^{quad}$ is the compositum of all quadratic extensions over $\mathbf{Q}$. (For example, see[3].)

Hence, if $\mathbf{Q}^{ab}$ is large, Proposition 1 implies Conjecture 1. The main result in this paper is the following.

THEOREM 2. *Let E be an elliptic curve defined over a finite number field K. Assume for any quadratic character $\chi \in \mathrm{Gal}(\widehat{K\mathbf{Q}^{ab}}/K)$ that the Hasse-Weil L-function $L(E/K, \chi, s)$ admits an analytic continuation to the whole complex plane and satisfies the functional equation, and assume that the weak Birch and Swinnerton-Dyer conjecture is true. (See Conjectures* 3, 4 *and* 5 *in Section* 2.) *Then if at least $[K : \mathbf{Q}]$ is odd,* $\mathrm{rank}_{\mathbf{Z}} E(K\mathbf{Q}^{ab}) = \infty$.

From this we get affirmative evidence for the largeness of $\mathbf{Q}^{ab}$ assuming several conjectures on the Hasse-Weil L-function.

In Section 2, we explain conjectures we assumed to be true in Theorem 2. We prove Theorem 2 in Section 3.

2. Several conjectures

In this section, we state several conjectures mentioned in Theorem 2. Namely, the analytic continuation, the functional equation, and the weak Birch and Swinnerton-Dyer conjecture for $L(E/K, \chi, s)$, where E is an elliptic curve defined over a number field K and $\chi \in \mathrm{Gal}(\widehat{K^{ab}/K})$ is a quadratic character. Here the L-function is the infinite product of the local L-functions defined by means of the characteristic polynomials of the Frobenius automorphisms acting on the l-adic Tate module for E twisted by χ. Namely, the L-function is defined by using

$$W = (\mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l(E)) \otimes_{\mathbf{Q}_l} (\mathbf{Q}_l \otimes_{\mathbf{Q}} M_\chi)\,,$$

where M_χ is the one-dimensional $\mathbf{Q}$-vector space on which $\mathrm{Gal}(\bar{K}/K)$ acts via χ. We note that W is isomorphic to $\mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l(E_\chi)$, the $\mathrm{Gal}(\bar{K}/K)$-module obtained from the l-adic Tate module for E_χ which is the twist of E by χ. Thus we may identify the local factors of $L(E/K, \chi, s)$ with that of $L(E_\chi/K, s)$.

Let v be a finite place of K coprime to l, let $I_v \subset \mathrm{Gal}(\bar{K}/K)$ be the inertia subgroup at v, and let Frob_v be the Frobenius automorphism at v. The local L-function at v is defined by

$$L_v(E_\chi, s) = (\det(1 - {q_v}^{-s}\mathrm{Frob}_v|_{W^{I_v}}))^{-1}\,,$$

where q_v is the order of the residue field at v. We put

$$L(E/K, \chi, s) = \prod\nolimits_{v \in M_K^0} L_v(E_\chi, s)\,,$$

where $M_K^0 = \{\text{finite places of } K\}$. This product converges and gives an analytic function for all s with $\mathrm{Re}(s) > 3/2$. We define the complete L-function

$$\Lambda(E/K, \chi, s) = N_{K/\mathbf{Q}}(N_{E_\chi})^{s/2}(2(2\pi)^{-s}\Gamma(s))^{[K:\mathbf{Q}]}L(E/K, \chi, s)\,,$$

where N_{E_χ} is the conductor of E_χ. We state conjectures on $\Lambda(E/K, \chi, s)$.

CONJECTURE 3 (Analytic continuation). *$\Lambda(E/K, \chi, s)$ admits an analytic continuation to the whole complex plane.*

CONJECTURE 4 (Functional equation). *Suppose that Conjecture 3 is valid. Then we have the functional equation*

$$\Lambda(E/K, \chi, s) = W(E_\chi/K)\Lambda(E/K, \chi, 2 - s)\,,$$

where $W(E_\chi/K)$ is the root number and $W(E_\chi/K) = \pm 1$.

Assume that Conjectures 3 and 4 are valid. We write the power series expansion around $s = 1$

$$\Lambda(E/K, \chi, s) = \sum_{n=k}^{\infty} a_n (s-1)^n\,,$$

where $k = \mathrm{ord}_{s=1} L(E/K, \chi, s)$.

Comparing the leading terms of the functional equation, we have the following equation

$$W(E_\chi/K) = (-1)^{\mathrm{ord}_{s=1} L(E/K,\chi,s)} .$$

Finally, we state the weak Birch and Swinnerton-Dyer conjecture which asserts the relation between analytic and algebraic quantities for E_χ.

CONJECTURE 5 (weak Birch and Swinnerton-Dyer conjecure). *Suppose that Conjecture 3 is valid. If* $L(E/K, \chi, 1) = 0$, *then* $\mathrm{rank}_{\mathbf{Z}} E_\chi(K) > 0$.

3. Proof of Theorem 2

In this section, we shall prove Theorem 2. Throughout this section we assume Conjectures 3, 4 and 5 in the previous section. Let E be an elliptic curve defined over a number field K with conductor N_E. Let L/K be a quadratic extension and $\chi \in \mathrm{Gal}(\widehat{K^{ab}/K})$ be the corresponding character with conductor N_χ. We assume that N_χ is relatively prime to N_E. We write simply $W(E/K)$ for $W(E_\chi/K)$ if χ is the trivial character. We use the following relation between $W(E_\chi/K)$ and $W(E/K)$.

PROPOSITION 2 ([4] Corollary of Proposition 10). *We have*

$$W(E_\chi/K) = \mathrm{sign}(\chi)\chi(N_E)W(E/K) .$$

Here, $\mathrm{sign}(\chi)$ is defined as follows. We view the quadratic character χ as a Hecke character

$$\chi = \prod\nolimits_{v \in M_K^0 \cup M_K^\infty} \chi_v ,$$

where χ_v is the character of $K_v{}^\times$ whose order is at most 2 and $M_K^\infty = \{\text{infinite places of } K\}$. Then we define

$$\mathrm{sign}(\chi) = \prod\nolimits_{v \in M_K^\infty} \chi_v(\tau) ,$$

where τ is the complex conjugation. Namely,

$$\mathrm{sign}(\chi) = (-1)^{\sharp\{v \in M_K^\infty | v:\text{real place which is not decomposed in } L\}} .$$

Suppose that K is a number field of odd degree. Let l be a rational prime unramified in K, and let $L = K(\sqrt{(-1)^{\frac{l-1}{2}} l})$. Then, if $[K : \mathbf{Q}]$ is odd and $l \equiv 3 \pmod 4$, we have $\mathrm{sign}(\chi) = -1$, since every real place is not decomposed and K has odd real places. Assume that N_E is factorized into the form

$$N_E = \prod\nolimits_{v \in M_K^0} \mathfrak{p}_v^{a(E/K_v)} ,$$

where $\mathfrak{p}_v$ is the maximal ideal of the integer ring of K_v and $a(E/K_v)$ is a non-negative integer which is 0 for almost all $v \in M_K^0$. Then

$$\chi(N_E) = \prod_{\mathfrak{p}_v | N_E} \chi_v(\mathrm{Frob}_{v,\, L/K})^{a(E/K_v)},$$

where $\mathrm{Frob}_{v,\, L/K} \in \mathrm{Gal}(L/K)$ is Frobenius automorphism at v. Recall that if $v \in M_K^0$ is decomposed in L, we have

$$\chi_v(\mathrm{Frob}_{v,\, L/K}) = 1\,.$$

LEMMA 1. *Let K be a number field of odd degree. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be prime ideals of K. Then,* (1) *there exist infinitely many quadratic extensions L over K contained in $K\mathbf{Q}^{ab}$ such that $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are decomposed in L and no real place is decomposed in L.* (2) *there exist infinitely many quadratic extensions L over K contained in $K\mathbf{Q}^{ab}$ such that $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and all real places are decomposed in L.*

PROOF. To prove the case (1) (resp. (2)), we consider a quadratic extension $K(\sqrt{(-1)^{\frac{l-1}{2}} l})/K$, where l is a rational prime unramified in K such that $l \equiv 3 \pmod 4$ (resp. $l \equiv 1 \pmod 4$). Let p_i be the characteristic of the residue field of $\mathfrak{p}_i$. Since $[K : \mathbf{Q}]$ is odd, $\mathfrak{p}_i$ is decomposed in $K(\sqrt{(-1)^{\frac{l-1}{2}} l})$ if and only if p_i is decomposed in $\mathbf{Q}(\sqrt{(-1)^{\frac{l-1}{2}} l})$. So it is enough to take l such that $p_1, \dots, p_r$ are decomposed in $\mathbf{Q}(\sqrt{(-1)^{\frac{l-1}{2}} l})$. This is possible by Dirichlet's arithmetic progression theorem. □

By this lemma, if $[K : \mathbf{Q}]$ is odd, there are infinitely many quadratic extensions $L \subset K\mathbf{Q}^{ab}$ such that $\chi(N_E) = 1$ and $\mathrm{sign}(\chi) = -1$ (resp. $\mathrm{sign}(\chi) = 1$) in the case (1) (resp. (2)), where χ corresponds to L. Hence in each case of $W(E/K) = \pm 1$, using these characters, we have infinitely many quadratic extensions $L \subset K\mathbf{Q}^{ab}$ such that $W(E_\chi/K) = -1$.

Since we have an isomorphism

$$E(L) \otimes \mathbf{Q} \cong (E(K) \oplus E_\chi(K)) \otimes \mathbf{Q}$$

as $\mathrm{Gal}(L/K)$-modules, we have $\mathrm{rank}_{\mathbf{Z}} E(L) = \mathrm{rank}_{\mathbf{Z}} E(K) + \mathrm{rank}_{\mathbf{Z}} E_\chi(K)$.

By the remark in Section 2 followed after the statement of Conjecture 4, we have

$$W(E_\chi/K) = (-1)^{\mathrm{ord}_{s=1} L(E/K, \chi, s)}\,.$$

If $W(E_\chi/K) = -1$, $\mathrm{ord}_{s=1} L(E/K, \chi, s)$ is odd and hence positive since $L(E/K, \chi, s)$ is holomorphic. Therefore, Conjecture 5 implies

$$\mathrm{rank}_{\mathbf{Z}} E(L) - \mathrm{rank}_{\mathbf{Z}} E(K) > 0\,.$$

Let I be the set of quadratic characters $\chi \in \widehat{\mathrm{Gal}}(K\mathbf{Q}^{ab}/K)$ such that $W(E_\chi/K) = -1$. Then I is an infinitely dimensional $\mathbf{F}_2$-vacter space by Lemma 1 and the remark followed after Lemma 1. Take a basis I^* of I. We take $P_\chi \in E_\chi(K) \backslash E_\chi(K)_{\mathrm{tors}}$ for each $\chi \in I^*$. Then, $\{P_\chi\}_{\chi \in I^*}$ gives points of $E(K\mathbf{Q}^{ab})$ which are linearly independent. Hence $\mathrm{rank}_{\mathbf{Z}} E(K\mathbf{Q}^{ab}) = \infty$. This completes the proof.

4. Proof of Proposition 1

In this section, we prove Tamagawa's result mentioned in Section 1.

Let K be a field of characteristic 0 and let E be an elliptic curve defined over K. Assume that K is a large field. Let A be an abelian surface $E \times E$. Fix an embedding $A \hookrightarrow \mathbf{P}^n$ of A into the projective space. Let X be a smooth hyperplane section of A with respect to the projective embedding, passing through $O \in A$, which is a smooth, projective, connected curve over K. Then it is known that the canonical morphism $J \to A$ is surjective, where J is the Jacobian variety of X. In particular, we have genus$(X) \geq \dim(A) = 2$. Suppose that $E(K)$ is of finite rank, then $\Gamma = A(K)$ is also. Now, by Raynaud's theorem (Mordell's conjecture), $X(K) = \Gamma \cap X$ is finite. This contradicts the assumption that K is large, since $X(K)$ is non-empty because $O \in X(K)$.

REMARK 1. When char$(K) > 0$, Proposition 1 is still valid, if we assume that K is not algebraic over the prime field $\mathbf{F}_p$. (The above proof has to be slightly modified, though.)

ACKNOWLEDGEMENTS. The author would like to thank her thesis adviser Professor Masato Kurihara for his suggestion of the problem and helpful advice. She would also like to thank Professor Akio Tamagawa who gave her invaluable advice and kindly allowed her to use his proof of Proposition 1.

References

[1] F. POP, Embedding problems over large fields, Ann. of Math. **144** (1996), 1–34.
[2] K. A. RIBET, Torsion points of abelian varieties in cyclotomic extensions, Enseign. Math. **27** (1981), 315–319.
[3] M. ROSEN and S. WONG, The Rank of Abelian Varieties over Infinite Galois Extensions, Journal of Number Theory **92** (2002), 182–196.
[4] D. E. ROHRLICH, Galois theory, elliptic curves, and root numbers, Compositio Math. **100** (1996), 311–349.

Present Address:
SUMIYOSHI-CHO, FUCHU-SHI, TOKYO, 183–0034 JAPAN.
e-mail: kobaemi3@hotmail.com