Czechoslovak Mathematical Journal

Jung-Jo Lee

On the ranks of elliptic curves in families of quadratic twists over number fields

Czechoslovak Mathematical Journal, Vol. 64 (2014), No. 4, 1003–1018

Persistent URL: http://dml.cz/dmlcz/144157

Czechoslovak Mathematical Journal, 64 (139) (2014), 1003–1018

ON THE RANKS OF ELLIPTIC CURVES IN FAMILIES OF QUADRATIC TWISTS OVER NUMBER FIELDS

Jung-Jo Lee, Daegu

(Received September 18, 2013)

Abstract. A conjecture due to Honda predicts that given any abelian variety over a number field K, all of its quadratic twists (or twists of a fixed order in general) have bounded Mordell-Weil rank. About 15 years ago, Rubin and Silverberg obtained an analytic criterion for Honda's conjecture for a family of quadratic twists of an elliptic curve defined over the field of rational numbers. In this paper, we consider this problem over number fields. We will prove that the existence of a uniform upper bound for the ranks of elliptic curves in this family is equivalent to the convergence of a certain infinite series. This result extends the work of Rubin and Silverberg over $\mathbb{Q}$.

Keywords: elliptic curve; rank; quadratic twist

MSC 2010: 11G05

1. Introduction

Fix integers a, b, c such that the polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ has three distinct complex roots, and let E be the elliptic curve

$$E\colon\ y^2 = f(x). \tag{1.1}$$

For $D \in \mathbb{Z} \setminus \{0\}$, let E_D be the quadratic twist of E given by

$$E_D\colon\ Dy^2 = f(x). \tag{1.2}$$

For an abelian variety A defined over a number field K, let $A(K)$ denote the group of K-rational points of A, which is finitely generated and abelian (Mordell-Weil theorem). Denote by $\operatorname{rank} A(K)$ the number of maximally independent points

This research was supported by NRF grant No. 2012-005700, Republic of Korea.

in $A(K)/A(K)_{\mathrm{tor}}$ with respect to the ring of rational integers, where $A(K)_{\mathrm{tor}}$ denotes the subgroup of torsion points in $A(K)$. In this paper, we will consider the cases where A is the elliptic curve E or E_D defined above.

Much work have been done to give an explicit upper bound for the ranks of elliptic curves. For example, for elliptic curves $E_{(D)}\colon\ y^2 = x^3 + Dx$, where D is a fourth-power-free integer, it is well known that

$$\operatorname{rank} E_{(D)}(\mathbb{Q}) \leqslant 2\nu(2D),$$

where $\nu(2D)$ denotes the number of prime divisors of $2D$. (See [13], Chapter X, Section 6.)

In the case where E is defined over $\mathbb{Q}$ and has no rational point of order two, Brumer and Kramer gave an upper bound for the rank of E in terms of the dimension of the ideal class group of the cubic subfield of 2-division field of E modulo squares, and the number of primes of bad reduction. (For the precise statement, see [2], Proposition 7.1.) Notice that the 2-division field of E_D is just the field generated over $\mathbb{Q}$ by the solutions of $f(x) = 0$ in $\overline{\mathbb{Q}}$, where $f(x)$ is as given in Equation (1.2), so it is independent of D in a family of quadratic twists.

In [10] and [11], Rubin and Silverberg reformulated the question of whether there is a constant $C \in \mathbb{R}$ such that $\operatorname{rank} E_D(\mathbb{Q}) < C$ for every $D \in \mathbb{Z} \setminus \{0\}$, into a question of whether a certain infinite series converges. The significance of their work is the translation of a purely arithmetic question into an analytic one. So far, we do not know a single example of a family of quadratic twists of an elliptic curve for which we could prove the existence of such a uniform upper bound for the ranks.

Our main theorem, which is Theorem 3.1 in Section 3, is as follows.

Main Theorem. *Let E/K be an elliptic curve and E_m be its quadratic twist as given in Equation* (1.2)*. Let j and k be non-negative real numbers such that $j > 0$. There is a series $S_{E,K}(j,k)$ such that the following conditions are equivalent:*

(a) $\operatorname{rank} E_m(K) < 2j$ *for every* $m \in \mathbb{Z} \setminus \{0\}$*;*
(b) $S_{E,K}(j,k)$ *converges for every* $k > 1$*;*
(c) $S_{E,K}(j,k)$ *converges for some* $k > 1$.

(For the definition of the series $S_{E,K}(j,k)$, see Equation (3.1) *in Section* 3.*)*

The existence of such a uniform upper bound for the ranks of elliptic curves was first conjectured by Honda in 1960 in a more general context [4]. In that paper, he proved Theorems 1.1 and 1.2 below.

Theorem 1.1. *Let A be an abelian variety defined over a number field. Then there exists a constant $c_1(A)$ which depends only on A and has the following property: for every prime l and for every number field K over which A is defined and such that $A(K) \supset A[l]$, we have*

$$\operatorname{rank} A(K) \leqslant c_1(A)[K : \mathbb{Q}] + 2rh_K(l).$$

Here, $A[l]$ is the subgroup of l-torsion points of $A(\overline{K})$, r is the dimension of the variety A and $h_K(l)$ is the l-rank of the absolute ideal class group of K.

P r o o f. This is the Corollary of Theorem 5 of [4]. □

Remark. There is a result of T. Ooe and J. Top which is similar to Theorem 1.1 but more general. For the reference, see Theorem 1 of [9].

Let K/k be a finite extension of algebraic number fields with $[K : k] > 1$. For an abelian variety A, let $\mathcal{A}(A)$ be the set of all automorphisms of A and $\mathcal{A}_0(A) = \mathcal{A}(A) \otimes \mathbb{Q}$. Let A be a simple abelian variety of dimension r, defined over a number field k, such that $\mathcal{A}_0(A)$ is isomorphic to a number field F of degree $2r$ over $\mathbb{Q}$. Let ι be an isomorphism of F onto $\mathcal{A}_0(A)$.

Theorem 1.2. *Let (A, ι) be a simple abelian variety, belonging to a CM-type $(F; \{\varphi_i\})$, and assume that A is defined over a number field k. Denote by $(F^*; \{\psi_i\})$ the dual of $(F; \{\varphi_i\})$ and put $K = kF^*$. Then we have*

$$\operatorname{rank} A(K) = [K : k] \operatorname{rank} A(k).$$

P r o o f. This is Theorem 6 of [4]. For the notions used here, see [12], Chapter II. □

Based on Theorems 1.1 and 1.2 above, together with an analogy of Dirichlet's unit theorem, Honda conjectured the following.

Conjecture 1.1 (Honda)**.** *For every abelian variety A defined over a number field, there exists a constant $c(A)$ which depends only on A such that*

$$\operatorname{rank} A(K) \leqslant c(A)[K : \mathbb{Q}]$$

for every number field K over which A is defined, where $[K : \mathbb{Q}]$ denotes the extension degree of K over $\mathbb{Q}$.

In this paper, we will prove (see Theorem 3.1 below) that the convergence of a certain infinite series is equivalent to the existence of a uniform upper bound for

the ranks of elliptic curves in a family of quadratic twists of an elliptic curve over a *number field*. This extends the result of Rubin and Silverberg ([10], [11]), which was obtained over the *field of rational numbers* $\mathbb{Q}$.

It deals with a special case of Honda's conjecture, which implies for quadratic extensions that there is a constant $c(E)$ independent of $m \in \mathbb{Z}$ such that

$$\operatorname{rank} E(K(\sqrt{m})) \leqslant c(E)[K(\sqrt{m}) : \mathbb{Q}] \leqslant 2c(E)[K : \mathbb{Q}].$$

Then, as $\operatorname{rank} E_m(K) \leqslant \operatorname{rank} E(K(\sqrt{m}))$ (see [13], Chapter X, Exercises 10.16 or 10.22), we can conclude that $\operatorname{rank} E_m(K) \leqslant 2c(E)[K : \mathbb{Q}]$.

To prove the above mentioned result regarding the special case of Honda's conjecture, Rubin and Silverberg used the convergence property of an Epstein zeta function, by identifying a related series as such a function ([10], [11]).

Many of Rubin and Silverberg's proofs remain true over a number field (see Remark 2.5 of [11]). To get the result of this paper using their method, we need another estimation of the size of the canonical height. For any $P \in E_D(\mathbb{Q}) \setminus E_D(\mathbb{Q})_{\mathrm{tor}}$, the estimation that they use is $\hat{h}_D(P) > \frac{1}{12} \log |D|$ for sufficiently large D, which is valid only over $\mathbb{Q}$. Over a number field, there is a related conjecture by Lang (Chapter VIII, Conjecture 9.9 of [13]).

Conjecture 1.2 (Lang)**.** *Let E/K be an elliptic curve with j-invariant j_E and minimal discriminant $\mathcal{D}_{E/K}$. There is a constant $C > 0$, depending only on $[K : \mathbb{Q}]$, such that for all non-torsion points $P \in E(K)$ we have*

$$\hat{h}(P) > C \max\{h(j_E), \log N_{K/\mathbb{Q}} \mathcal{D}_{E/K}, 1\}.$$

(Here, h is the absolute logarithmic height.)

However, in this paper, we will use Abel's summation formula and a lattice point estimate due to Lenstra and Silverman [15]. Another important ingredient for our proof is the estimation of the size of the canonical height due to Silverman [14] (see Theorem 2.7 below).

Finally, it seems to be possible to get the result of this paper using the method of Rubin and Silverberg if we apply the estimation of Silverman (Theorem 2.7) and Northcott's theorem [6]. So the purpose of this paper is to state and prove the result explicitly over number fields with a completely different approach.

2. Bounds on heights and a counting lemma

To state our theorem over a number field, we first have to define the *height* of points over number fields. The definitions and basic properties of heights can be found in [13], Chapter VIII, Section 5, where the heights are more generally defined on the projective space over number fields. Now, we briefly explain these.

Let $K/\mathbb{Q}$ be a number field, and let M_K be the set of *standard* absolute values on K. Thus, M_K contains an archimedean absolute value for each embedding of K into $\mathbb{R}$ or $\mathbb{C}$ and a p-adic absolute value for each prime ideal in the ring of integers of K.

Definition 2.1. The height of a point $x \in K$ is defined by

$$H_K(x) = \prod_{v \in M_K} \max\{1, |x|_v\}^{n_v},$$

where $n_v = [K_v : \mathbb{Q}_v]$, the local degree at v, and K_v and $\mathbb{Q}_v$ denote the completions of the indicated fields with respect to the absolute value v.

For $x \in K$, we define the absolute logarithmic height as

$$h(x) = \frac{1}{[K : \mathbb{Q}]} \log H_K(x). \tag{2.1}$$

(The "log" in the definition denotes the natural logarithm.)

If $P \in E(K)$, write $P = (x(P), y(P))$. Then we define

$$h(P) := h(x(P)). \tag{2.2}$$

Definition 2.2. Let E/K be an elliptic curve defined over an algebraic number field K. For $P \in E(\overline{K})$, the canonical height of P is given by the formula

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{4^n} h(2^n P).$$

Important properties of the canonical heights are summarized in the following theorem.

Theorem 2.3. *The canonical height $\hat{h}(P)$ satisfies the following properties:*

(a) $\hat{h}(P) = h(P) + O(1)$, *where the implied constant depends on E but not on P.*
(b) $\langle P, Q\rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$ *is bi-additive.*
(c) $\hat{h}(mP) = m^2\hat{h}(P)$ *for all $m \in \mathbb{Z}$.*
(d) $\hat{h}(P) \geqslant 0$, *with equality holding if and only if P is a torsion point.*
(e) *If $g(P)$ is any function satisfying* (a) *and* (c), *then $g = \hat{h}$.*

P r o o f. This is Theorem 20.4.4 of [5]. □

We can view $E(K)$ mod $E(K)_{\mathrm{tor}}$ as a lattice in the vector space $E(K) \otimes \mathbb{R}$ with the positive definite quadratic form $\hat{h}$, whose associated norm is defined by $|P| = \sqrt{\langle P, P\rangle}$. Then $\operatorname{rank} E(K)$ is the dimension of $E(K) \otimes \mathbb{R}$ over $\mathbb{R}$.

Definition 2.4. Let E/K be an elliptic curve defined over an algebraic number field K. Let $P_1, P_2, \ldots, P_r$ be a basis for $E(K)$ mod $E(K)_{\mathrm{tor}}$. Then $R(E/K)$, the elliptic regulator of E/K, is defined to be

$$R(E/K) := \det(\langle P_i, P_j\rangle)_{1 \leqslant i,\, j \leqslant r}.$$

(If $r = 0$, we set $R(E/K) = 1$ by convention.)

Remark 2.5. The elliptic regulator $R(E/K)$ is the square of the volume of a fundamental domain of the lattice $E(K)/E(K)_{\mathrm{tor}}$ in $E(K) \otimes \mathbb{R}$.

It satisfies the property that $R(E/K) > 0$. (See [13], Chapter VIII, Section 9, Corollary 9.7.)

Using this geometric interpretation and some standard arguments from the geometry of numbers, one can deduce the following result about the distribution of rational points on an elliptic curve.

Lemma 2.6. *Let E be an elliptic curve defined over a number field K. Suppose that $E(K)$ has rank r. Let $N(x)$ be the number of elements $P \in E(K)$ such that $\hat{h}(P) \leqslant x$. Then there is a constant C such that*

$$N(x) = Cx^{r/2} + O(x^{(r-1)/2+\varepsilon}).$$

More precisely, $C = \pi^{r/2}|E(K)_{\mathrm{tor}}|/\Gamma(1 + r/2)\sqrt{R(E/K)}$. The implied constant in the error term depends on E.

P r o o f. This is Lemma 13 of [3]. In [3], the statement is made for elliptic curves over $\mathbb{Q}$, but exactly the same proof is valid for elliptic curves over K. Indeed, the proof uses only the properties of the lattice points in the r-dimensional ellipsoid determined by the quadratic form. Notice also that Lemma 13 of [3] proves the result modulo the torsion points. □

One of the key ingredients in our proof is the following result due to Silverman about a lower bound for the canonical height on elliptic curves. This result was proved by M. Baker for all cases except when $j(E)$ is an algebraic integer and E does not have a complex multiplication [1].

Theorem 2.7 (Silverman)**.** *Let E/K be an elliptic curve defined over a number field, let $\hat{h} : E(\overline{K}) \to \mathbb{R}$ be the canonical height on E, and let K^{ab}/K be the maximal abelian extension of K. There is a constant $c_1 = c_1(E/K) > 0$ such that every non-torsion point $P \in E(K^{ab})$ satisfies*

$$\hat{h}(P) > c_1.$$

P r o o f. This is Theorem 1 of [14]. □

Corollary 2.8. *Let $\hat{h}_m \colon E_m(\overline{K}) \to \mathbb{R}$ be the canonical height on E_m. Under the same conditions as in Theorem 2.7, there is a constant $c_1 > 0$ such that every non-torsion point $P \in E_m(K)$ satisfies*

$$\hat{h}_m(P) > c_1,$$

where c_1 is a constant independent of m.

P r o o f. If $\sqrt{m} \in K$, then $E_m(K) = E(K)$. Thus, we only need to consider m such that $\sqrt{m} \notin K$. Consider the trace map defined by

$$\mathrm{Tr}_m \colon E(K(\sqrt{m})) \to E(K), \quad P \mapsto P + P^{\sigma}, \tag{2.3}$$

where σ is the non-trivial automorphism in $\mathrm{Gal}(K(\sqrt{m})/K)$. It is a homomorphism whose kernel is isomorphic to $E_m(K)$ ([13], Chapter X, Exercise 10.22). Thus, we have an injection $E_m(K) \xrightarrow{\iota} E(K(\sqrt{m})) \subset E(K^{ab})$ given by $(x, y) \overset{\iota}{\mapsto} (x, \sqrt{m}y)$.

Let $P = (x, y) \in E_m(K)$. By using the tangent-chord method (see [13], Chapter III, Section 2), it can be verified that the x-coordinate of $2P$ in $E_m(K)$ is

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4my^2} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},$$

where E_m is defined by a Weierstrass equation as given in (1.2).

Next, consider $\iota(P) = (x, \sqrt{m}y) \in E(K(\sqrt{m})) \subset E(K^{ab})$, and using the same method (or duplication formula), we compute the x-coordinate of $2\iota(P)$ in $E(K(\sqrt{m}))$ to be

$$x(2\iota(P)) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Therefore, if $2P = (x_1, y_1) \in E_m(K)$, then $2\iota(P) = (x_1, \sqrt{m}y_1) = \iota(2P) \in E(K(\sqrt{m}))$, so

$$x(2P) = x(2\iota(P)).$$

Repeating this, we can conclude that

$$x(2^n P) = x(2^n \iota(P)) \quad \text{for all } n \geqslant 0,$$

where duplications are done in $E_m(K)$ for $2^n P$, and in $E(K(\sqrt{m}))$ for $2^n \iota(P)$.

Since the canonical height is defined as a limit of x-heights (see Definition 2.2), we have that $\hat{h}_m(P) = \hat{h}(\iota(P))$ for all $P \in E_m(K)$. As $\hat{h}(\iota(P)) > c_1$ by Theorem 2.7, we have the desired result. □

Silverman derived the following upper bound, which when applied to the Mordell-Weil group of K-rational points gives an effective bound on the number of rational points [15]. The idea goes back to Hendrik Lenstra.

Lemma 2.9. *Let E be an elliptic curve defined over a number field K. Suppose that $E(K)$ has rank r. Let $N(x)$ be the number of elements $P \in E(K)$ such that $\hat{h}(P) \leqslant x$. Then*

$$N(x) \leqslant |E(K)_{\mathrm{tor}}| \left(2\sqrt{\frac{x}{c}} + 1\right)^r,$$

if c satisfies

$$\min\{\hat{h}(P) | P \in E(K) \setminus E(K)_{\mathrm{tor}}\} \geqslant c.$$

P r o o f. This follows from Lemma 7 of [15] and Theorem 2.7. □

3. Main theorem

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ be a cubic polynomial with three distinct complex roots. Let $E\colon\ y^2 = f(x)$ and $E_m\colon\ my^2 = f(x)$. For any real numbers $j > 0$ and $k \geqslant 0$, define an infinite series

$$S_{E,K}(j,k) = \sum_{m \in \mathbb{Z} \setminus \{0\}} \frac{\mu^2(|m|)}{|m|^k} \sum_{P \in E_m(K) \setminus E_m(K)_{\mathrm{tor}}} \frac{1}{\hat{h}_m(P)^j}. \tag{3.1}$$

Here μ denotes the Möbius function and $\hat{h}_m\colon\ E_m(K) \to \mathbb{R}_{\geqslant 0}$ is the canonical height.

The purpose of this paper is to prove the following theorem.

Theorem 3.1. *Let j and k be non-negative real numbers such that $j > 0$. Then the following conditions are equivalent:*

(a) $\operatorname{rank} E_m(K) < 2j$ *for every* $m \in \mathbb{Z} \setminus \{0\}$;
(b) $S_{E,K}(j,k)$ *converges for every* $k > 1$;
(c) $S_{E,K}(j,k)$ *converges for some* $k > 1$.

Let us rewrite the expression (3.1) of $S_{E,K}(j,k)$ as

$$S_{E,K}(j,k) = \sum_{m \in \mathbb{Z}\setminus\{0\}} \frac{\mu^2(|m|)}{|m|^k} S_m,$$

that is,

$$S_m = \sum_{P \in E_m(K)\setminus E_m(K)_{\mathrm{tor}}} \frac{1}{\hat{h}_m(P)^j}. \tag{3.2}$$

For each non-zero integer m, define T_m as

$$T_m = \sum_{n=2}^{\infty} \frac{a_{m,n}}{(\log n)^j}, \tag{3.3}$$

where

$$a_{m,n} = \#\{P \in E_m(K) \setminus E_m(K)_{\mathrm{tor}} : \log(n-1) < \hat{h}_m(P) \leqslant \log n\} \tag{3.4}$$

for all positive integers $n \geqslant 2$. Define

$$T_{E,K}(j,k) = \sum_{m \in \mathbb{Z}\setminus\{0\}} \frac{\mu^2(|m|)}{|m|^k} T_m. \tag{3.5}$$

One can also define

$$a_{m,1} := \#\{P \in E_m(K) \setminus E_m(K)_{\mathrm{tor}} : -\infty < \hat{h}_m(P) \leqslant 0\} = 0.$$

Lemma 3.2. *Fix a positive real number j. For a non-negative real number k, $S_{E,K}(j,k)$ converges if and only if $T_{E,K}(j,k)$ converges.*

P r o o f. Because $\log(n-1) > \frac{1}{2}\log n$ for all $n \geqslant 3$, if $\log(n-1) < \hat{h}_m(P) \leqslant \log n$ for some x, then

$$\frac{1}{(\log n)^j} \leqslant \frac{1}{\hat{h}_m(P)^j} \leqslant \frac{1}{\left(\frac{1}{2}\log n\right)^j}.$$

Thus, we have that

$$T_m \leqslant S_m \leqslant 2^j T_m,$$

which implies that $S_{E,K}(j,k)$ converges if and only if $T_{E,K}(j,k)$ converges. □

In view of Lemma 3.2, what we will actually prove is the following theorem, which is equivalent to Theorem 3.1:

Theorem 3.1′. *Let j and k be non-negative real numbers such that $j > 0$. Then the following conditions are equivalent:*

(a) $\operatorname{rank} E_m(K) < 2j$ *for every* $m \in \mathbb{Z} \setminus \{0\}$;
(b) $T_{E,K}(j,k)$ *converges for every* $k > 1$;
(c) $T_{E,K}(j,k)$ *converges for some* $k > 1$.

The proof of Theorem 3.1′ is based on the application of the following elementary theorem of analytic number theory, called Abel's summation formula (or the partial summation theorem).

Theorem 3.3 (Abel's Summation Formula)**.** *Suppose $\{a_n\}_{n=a}^{\infty}$ is a sequence of complex numbers and $f(t)$ is a continuously differentiable function on $[a,x]$. Set*

$$A(t) = \sum_{a \leqslant n \leqslant t} a_n.$$

Then

$$\sum_{a \leqslant n \leqslant x} a_n f(n) = A(x)f(x) - \int_a^x A(t)f'(t)\,\mathrm{d}t.$$

P r o o f. See [8], Chapter 2. □

We now apply the above theorem to our situation.

Fix a real number $t \geqslant 2$, and for integers n such that $2 \leqslant n \leqslant t$, let us define

$$A_m(t) := \sum_{2 \leqslant n \leqslant t} a_{m,n}. \tag{3.6}$$

(See Equation (3.4) for the definition of $a_{m,n}$.) Then

$$A_m(t) = \#\{P \in E_m(K) \setminus E_m(K)_{\mathrm{tor}} \colon \hat{h}_m(P) \leqslant \log t\}. \tag{3.7}$$

For $t < 2$, we may set $A_m(t) = 0$, since $a_{m,1} = 0$ for all $m \in \mathbb{Z} \setminus \{0\}$. Substituting x by $\log t$ in Lemma 2.9, we have that

$$A_m(t) \leqslant |E_m(K)_{\mathrm{tor}}| \left(2\sqrt{\frac{\log t}{c_1}} + 1\right)^{r_m}, \tag{3.8}$$

where c_1 is a constant independent of m by Corollary 2.8.

Observe that if $r_m = 0$, then $E_m(K) = E_m(K)_{\mathrm{tor}}$ and $A_m(t) = 0$.

Lemma 3.4. *For $m \in \mathbb{Z} \setminus \{0\}$ and a real number $x \geqslant 2$, let $T_m(x) = \sum_{2 \leqslant n \leqslant x} a_{m,n}/(\log n)^j$. Then*

$$T_m(x) = \frac{A_m(x)}{(\log x)^j} + j \int_2^x \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t.$$

P r o o f. This is immediate from Theorem 3.3 by replacing $a_n = a_{m,n}$, $a = 2$, $A(t) = A_m(t)$, and $f(t) = 1/(\log t)^j$, which is continuously differentiable on the interval $[2, x]$. □

Proposition 3.5. *For $m \in \mathbb{Z} \setminus \{0\}$ and a real number $x \geqslant \max\{2, \mathrm{e}^{c_1}\}$, where c_1 is the constant that appears in Corollary 2.8, we have an estimate of*

$$T_m(x) \leqslant |E_m(K)_{\mathrm{tor}}|\left\{\frac{(3/\sqrt{c_1})^{r_m}}{(\log x)^{j-r_m/2}} + j\int_{c_1}^{\log x} \frac{(3/\sqrt{c_1})^{r_m}}{u^{j+1-r_m/2}}\,\mathrm{d}u + \frac{3^{r_m}}{(\log 2)^j} - \frac{3^{r_m}}{c_1^j}\right\}$$
if $\mathrm{e}^{c_1} > 2$,

and

$$T_m(x) \leqslant |E_m(K)_{\mathrm{tor}}|\left\{\frac{(3/\sqrt{c_1})^{r_m}}{(\log x)^{j-r_m/2}} + j\int_{\log 2}^{\log x} \frac{(3/\sqrt{c_1})^{r_m}}{u^{j+1-r_m/2}}\,\mathrm{d}u\right\}, \quad \textit{otherwise.}$$

P r o o f. From Lemma 3.4, we know that

$$T_m(x) = \frac{A_m(x)}{(\log x)^j} + j \int_2^x \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t, \tag{3.9}$$

and we apply Formula (3.8) to this. Our assumption of $x \geqslant \mathrm{e}^{c_1}$ implies that

$$\left(2\sqrt{\frac{\log x}{c_1}} + 1\right)^{r_m} \leqslant \left(3\sqrt{\frac{\log x}{c_1}}\right)^{r_m} = \left(\frac{3}{\sqrt{c_1}}\right)^{r_m} (\log x)^{r_m/2},$$

so

$$A_m(x) \leqslant |E_m(K)_{\mathrm{tor}}|\left(\frac{3}{\sqrt{c_1}}\right)^{r_m} (\log x)^{r_m/2}.$$

Now, let $\mathrm{e}^{c_1} > 2$. For any t satisfying $2 \leqslant t < \mathrm{e}^{c_1}$, we have

$$\left(2\sqrt{\frac{\log t}{c_1}} + 1\right)^{r_m} < 3^{r_m},$$

thus

$$A_m(t) < |E_m(K)_{\mathrm{tor}}|\, 3^{r_m}.$$

Therefore,

$$\begin{aligned}\int_2^x \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t &= \int_2^{\mathrm{e}^{c_1}} \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t + \int_{\mathrm{e}^{c_1}}^x \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t \\ &\leqslant |E_m(K)_{\mathrm{tor}}|\biggl\{\int_2^{\mathrm{e}^{c_1}} \frac{3^{r_m}}{t(\log t)^{j+1}}\,\mathrm{d}t + \int_{\mathrm{e}^{c_1}}^x \frac{(3/\sqrt{c_1})^{r_m}}{t(\log t)^{j+1-r_m/2}}\,\mathrm{d}t\biggr\} \\ &= |E_m(K)_{\mathrm{tor}}|\biggl\{\int_{\log 2}^{c_1} \frac{3^{r_m}}{u^{j+1}}\,\mathrm{d}u + \int_{c_1}^{\log x} \frac{(3/\sqrt{c_1})^{r_m}}{u^{j+1-r_m/2}}\,\mathrm{d}u\biggr\} \\ &= |E_m(K)_{\mathrm{tor}}|\biggl\{\int_{c_1}^{\log x} \frac{(3/\sqrt{c_1})^{r_m}}{u^{j+1-r_m/2}}\,\mathrm{d}u + \frac{1}{j}\biggl(\frac{3^{r_m}}{(\log 2)^j} - \frac{3^{r_m}}{c_1^j}\biggr)\biggr\}.\end{aligned}$$

Similarly, if $\mathrm{e}^{c_1} \leqslant 2$,

$$\int_2^x \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t \leqslant |E_m(K)_{\mathrm{tor}}| \int_{\log 2}^{\log x} \frac{(3/\sqrt{c_1})^{r_m}}{u^{j+1-r_m/2}}\,\mathrm{d}u.$$

By putting these back into (3.9), we get the result. □

Before we give the proof of Theorem 3.1′, we prove the following lemma.

Lemma 3.6. *There is a constant B such that $|E_m(K)_{\mathrm{tor}}| \leqslant B$ for all m.*

P r o o f. Northcott's theorem tells us that for all numbers d and H, the set

$$\{P \in E(\overline{K})\colon\ [K(P):K] \leqslant d \text{ and } h(P) \leqslant H\}$$

is finite [6]. By this theorem and the fact that $h(P) = \hat{h}(P) + O(1)$ (see [6]), the set

$$\bigcup_{m\in\mathbb{Z}} E(K(\sqrt{m}))_{\mathrm{tor}}$$

is finite, since the torsion points are those with canonical height equal to 0. Therefore, there is a constant B such that

$$\#\biggl(\bigcup_{m\in\mathbb{Z}} E(K(\sqrt{m}))_{\mathrm{tor}}\biggr) \leqslant B,$$

which implies the result, since this set contains an isomorphic image of $E_m(K)_{\mathrm{tor}}$ for all m. □

Remark 3.1. The above lemma implies that $|E_m(K)_{\mathrm{tor}}| \leqslant 4$ for all but finitely many square-free integers m.

Remark 3.2. Lemma 3.6 could also be obtained as an immediate consequence of a theorem of Merel. Indeed, Merel proved that there exists a constant $B(d) \geqslant 0$ such that for all elliptic curves defined over a number field K with $[K : \mathbb{Q}] = d$, we have $|E(K)_{\mathrm{tor}}| \leqslant B(d)$ (see [7]). In a family of quadratic twists of E, $E_m(K)$ is isomorphic to a subgroup of $E(K(\sqrt{m}))$, thus $|E_m(K)_{\mathrm{tor}}| \leqslant |E(K(\sqrt{m}))_{\mathrm{tor}}| \leqslant \max\{B(d), B(2d)\}$ for all m.

Now we prove Theorem 3.1′.

P r o o f of Theorem 3.1′. Let us define

$$T_{E,K}(j,k,x,y) := \sum_{-y \leqslant m \leqslant y,\, m \neq 0} \frac{\mu^2(|m|)}{|m|^k} T_m(x), \tag{3.10}$$

where

$$T_m(x) := \sum_{2 \leqslant n \leqslant x} \frac{a_{m,n}}{(\log n)^j}.$$

(See Lemma 3.4.)

(a) $\Longrightarrow$ (b): $r_m < 2j$ implies that

$$\left(\frac{3}{\sqrt{c_1}}\right)^{r_m} < \left(\frac{3}{\sqrt{c_1}}\right)^{2j} = \left(\frac{9}{c_1}\right)^j$$

and

$$\frac{3^{r_m}}{(\log 2)^j} - \frac{3^{r_m}}{c_1^j} < \frac{3^{2j}}{(\log 2)^j} - \frac{3^{2j}}{c_1^j}$$

for all $m \in \mathbb{Z} \setminus \{0\}$.

We know that there is a constant B such that $|E_m(K)_{\mathrm{tor}}| \leqslant B$ for all m by Lemma 3.6.

Let us put

$$\alpha_1 = B\left(\frac{9}{c_1}\right)^j \quad \text{and} \quad \alpha_2 = B\left(\frac{3^{2j}}{(\log 2)^j} - \frac{3^{2j}}{c_1^j}\right).$$

Let $\mathrm{e}^{c_1} > 2$. Then by Proposition 3.5, for $x \geqslant 2$, we have

$$\begin{aligned} T_{E,K}(j,k,x,y) &\leqslant \sum_{-y \leqslant m \leqslant y,\, m \neq 0} \frac{1}{|m|^k} \left(\frac{\alpha_1}{(\log x)^{j - r_m/2}} + j \int_{c_1}^{\log x} \frac{\alpha_1}{u^{j+1-r_m/2}}\, \mathrm{d}u + \alpha_2 \right) \\ &= \sum_{-y \leqslant m \leqslant y,\, m \neq 0} \frac{1}{|m|^k} \left(\frac{\alpha_1}{(\log x)^{j - r_m/2}} + \frac{j}{j - r_m/2} \frac{\alpha_1}{c_1^{j - r_m/2}} \right. \\ &\quad \left. - \frac{j}{j - r_m/2} \frac{\alpha_1}{(\log x)^{j - r_m/2}} + \alpha_2 \right) \end{aligned}$$

$$= \sum_{-y\leqslant m\leqslant y,\, m\neq 0} \frac{1}{|m|^k}\bigg(\frac{j}{j-r_m/2}\frac{\alpha_1}{c_1^{j-r_m/2}} + \Big(1-\frac{j}{j-r_m/2}\Big)\frac{\alpha_1}{(\log x)^{j-r_m/2}} + \alpha_2\bigg)$$
$$\leqslant \sum_{-y\leqslant m\leqslant y,\, m\neq 0} \frac{1}{|m|^k}\bigg(\frac{j}{j-r_m/2}\frac{\alpha_1}{c_1^{j-r_m/2}} + \alpha_2\bigg),$$

where the last inequality holds because $1 - j/(j - r_m/2) \leqslant 0$ and $\log x \geqslant \log 2 > 0$.

Now, taking limits $x \to \infty$ and $y \to \infty$ on $T_{E,K}(j,k,x,y)$, we get

$$T_{E,K}(j,k) \leqslant \sum_{m\in\mathbb{Z}\setminus\{0\}} \frac{1}{|m|^k}\bigg(\frac{j}{j-r_m/2}\frac{\alpha_1}{c_1^{j-r_m/2}} + \alpha_2\bigg). \tag{3.11}$$

The right hand side of the inequality (3.11) converges for $k > 1$. This is because

$$0 < \frac{j}{j-r_m/2}\frac{1}{c_1^{j-r_m/2}} \leqslant \beta$$

for some constant β independent of m. For example, we could take β as

$$\beta = \max_{0\leqslant k<2j,\, k\in\mathbb{Z}} \bigg\{\frac{j}{j-k/2}\frac{1}{c_1^{j-k/2}}\bigg\}.$$

Similarly, we can prove the convergence of the series $T_{E,K}(j,k)$ for $k > 1$ in the case where $\mathrm{e}^{c_1} < 2$.

It is clear that (b) $\Longrightarrow$ (c).

(c) $\Longrightarrow$ (a): Suppose

$$T_{E,K}(j,k) = \sum_{m\in\mathbb{Z}\setminus\{0\}} \frac{\mu^2(|m|)}{|m|^k} T_m$$

converges for some $k > 1$. Then for every square-free m, the inner sum $T_m = \lim\limits_{x\to\infty} T_m(x)$ converges. (For the definition of T_m, see (3.3).)

According to Lemma 3.4, we have

$$T_m(x) = \frac{A_m(x)}{(\log x)^j} + j\int_2^x \frac{A_m(t)}{t(\log t)^{j+1}}\,\mathrm{d}t.$$

We apply Lemma 2.6 to the formula (3.7) for $A_m(t)$, and get

$$A_m(t) = C_m(\log t)^{r_m/2} + O\big((\log t)^{(r_m-1)/2+\varepsilon}\big),$$

where C_m and the implied constant depend on m. If $r_m = 0$, there is nothing to prove for this m. Hence, for each m with $r_m \neq 0$, we have

$$\begin{aligned} T_m(x) &= \frac{C_m}{(\log x)^{j-r_m/2}} + j\int_2^x \frac{C_m}{t(\log t)^{j+1-r_m/2}}\,\mathrm{d}t \\ &\quad + O\bigg(\frac{1}{(\log x)^{j-(r_m-1)/2-\varepsilon}} + j\int_2^x \frac{1}{t(\log t)^{j+1-(r_m-1)/2-\varepsilon}}\,\mathrm{d}t\bigg) \\ &= \frac{C_m}{(\log x)^{j-r_m/2}} + j\int_{\log 2}^{\log x} \frac{C_m}{u^{j+1-r_m/2}}\,\mathrm{d}u \\ &\quad + O\bigg(\frac{1}{(\log x)^{j-(r_m-1)/2-\varepsilon}} + j\int_{\log 2}^{\log x} \frac{1}{u^{j+1-(r_m-1)/2-\varepsilon}}\,\mathrm{d}u\bigg). \end{aligned}$$

Thus, $T_m = \lim_{x\to\infty} T_m(x)$ converges for all m if and only if $j - r_m/2 > 0$, that is, if and only if $r_m < 2j$ for all $m \in \mathbb{Z} \setminus \{0\}$. □

Acknowledgement. I am grateful to Professor Ram Murty for suggesting this problem, reading the first manuscript and providing various comments. I am also grateful to Professor Joseph Silverman for giving me valuable comments.

References

[1] *M. H. Baker*: Lower bounds for the canonical height on elliptic curves over abelian extensions. Int. Math. Res. Not. *2003* (2003), 1571–1589.
[2] *A. Brumer, K. Kramer*: The rank of elliptic curves. Duke Math. J. *44* (1977), 715–743.
[3] *R. Gupta, M. R. Murty*: Primitive points on elliptic curves. Compos. Math. *58* (1986), 13–44.
[4] *T. Honda*: Isogenies, rational points and section points of group varieties. Jap. J. Math. *30* (1960), 84–101.
[5] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics 84, Springer, New York, 1982.
[6] *S. Lang*: Fundamentals of Diophantine Geometry. Springer, New York, 1983.
[7] *L. Merel*: Bounds for the torsion of elliptic curves over number fields. Invent. Math. *124* (1996), 437–449. (In French.)
[8] *M. R. Murty*: Problems in Analytic Number Theory (2nd edition). Graduate Texts in Mathematics 206, Readings in Mathematics, Springer, New York, 2008.
[9] *T. Ooe, J. Top*: On the Mordell-Weil rank of an abelian variety over a number field. J. Pure Appl. Algebra *58* (1989), 261–265.
[10] *K. Rubin, A. Silverberg*: Ranks of elliptic curves. Bull. Am. Math. Soc., New Ser. *39* (2002), 455–474.
[11] *K. Rubin, A. Silverberg*: Ranks of elliptic curves in families of quadratic twists. Exp. Math. *9* (2000), 583–590.
[12] *G. Shimura, Y. Taniyama*: Complex Multiplication of Abelian Varieties and Its Applications to Number Theory. Publications of the Mathematical Society of Japan 6, Mathematical Society of Japan, Tokyo, 1961.
[13] *J. H. Silverman*: The Arithmetic of Elliptic Curves (2nd edition). Graduate Texts in Mathematics 106, Springer, New York, 2009.

[14] *J. H. Silverman*: A lower bound for the canonical height on elliptic curves over abelian extensions. J. Number Theory *104* (2004), 353–372.
[15] *J. H. Silverman*: Representations of integers by binary forms and the rank of the Mordell-Weil group. Invent. Math. *74* (1983), 281–292.

Author's address: Jung-Jo Lee, Department of Mathematics, Kyungpook National University, 80 Daehak-ro Buk-gu, Daegu 702-701, Korea, e-mail: jungjolee@gmail.com.