数理解析研究所講究録
998巻 1997年 34-43

THE ORDERS OF THE REDUCTIONS OF A POINT IN THE MORDELL–WEIL GROUP OF AN ELLIPTIC CURVE

J. CHEON AND S. HAHN

ABSTRACT. We prove elliptic analogue of Bang's theorem. Consider an elliptic curve E over a number field K. For any non-torsion point $M \in E(K)$, the order of the reductions M mod $\mathfrak{p}$ runs through all but finitely many positive integers as $\mathfrak{p}$ runs through all good primes. Moreover, it runs through all positive integers for all but finitely many points $M \in E(K)$. At last, we present some examples to deduce $\mathbb{N} \setminus Imf_M$ for $M \in E(\mathbb{Q})$.

1. Introduction

To begin with, we introduce the famous Bang's theorem. Let a be a fixed rational number in $\mathbb{Q} - \{0, \pm 1\}$. Then a can be written as $a = c/d$ for some integers $c \neq 0$ and $d > 0$ with $(c, d) = 1$. Let D_a denote the set of positive prime numbers which do not divide cd and $\mathbb{N}$ the set of natural numbers. We define the function f_a as a map

$$f_a : D_a \longrightarrow \mathbb{N}$$

such that for any $p \in D_a$

$$f_a(p) = \text{ the multiplicative order of } (a \bmod p) \text{ in the finite field } \mathbb{F}_p .$$

Then we can state Bang's theorem as follows :

Theorem (Bang). *Using the same notations as above, the set $\mathbb{N} \setminus Im\, f_a$ is finite for any $a \in \mathbb{Q} - \{0, \pm 1\}$.*

This famous theorem was proved by Bang first [2], and by various other mathematicians. In particular, Zsigmondy proved the stronger version presented here [11] [15]. We say that a prime p is a primitive divisor of $A^n - B^n$ if $p | A^n - B^n$ and $p \nmid A^m - B^m$ for any $m < n$, i.e. $f_a(p) = n$.

1991 *Mathematics Subject Classification.* 11G05, 11G20, 14H52.
Key words and phrases. Bang's theorem, Elliptic curves, Reductions, Local height, Division Polynomials.

Theorem (Zigmondy). *Let A, B be integers with $A > B \geq 1$ and $\gcd(A, B) = 1$ and let $n \geq 1$.*

(a) $A^n - B^n$ has a primitive divisor with the following exceptions :

(i) $n = 1$, $A - B = 1$.

(ii) $n = 2$, $A + B$ is a power of 2.

(iii) $n = 6$, $A = 2$, $B = 1$.

(b) $A^n + B^n$ has a primitive divisor with the following exceptions :

$n = 3$, $A = 2$, $B = 1$.

More general theorem over algebraic number fields by Schinzel is as follows [9]:

Theorem (Schinzel). *If $\gcd(A, B) = 1$ and A/B is not a root of unity, then $A^n - B^n$ has a primitive divisor for all $n > n_0(d)$, where d is the degree of A/B and $n_0(d)$ is effectively computable.*

In particular, the first special formulation of Theorem (Bang) was presented by Y. Ihara in [4] [5] together with the sketch of proof using cyclotomic polynomials, which motivated us to study the elliptic analogue replacing cyclotomic polynomials by division polynomials of elliptic curves. The analogue on elliptic curves over $\mathbb{Q}$ was proved by J. Silverman [12]. In this paper, we extend the result to the cases of number fields and show that f_M is surjective for all but finitely many points M of an elliptic curve, which is the stronger result than Schinzel's original theorem over number fields since we have only finitely many exceptional cases. However, we don't have yet any effective method to compute the number of points M for which f_M is not surjective.

2. Some Preliminaries

We introduce some notations to use in this paper.

$\mathbb{N}$: the set of natural numbers.

$\mathbb{Q}$: the set of rational numbers.

K : a number field

R : the ring of integers of K

M_K : the complete set of normalized absolute values on K.

M_K^∞ : the set of archimedean absolute values in M_K

M_K^0 : the set of non-archimedean absolute values in M_K

$v(x) = -\log |x|_v$ for $v \in M_K$

$\mathfrak{p}_v = \{x \in R | v(x) > 0\}$ for $v \in M_K$

K_v : the completion of K at v for $v \in M_K$

For M_K, we use the specific normalization as follows :

To begin with, $M_{\mathbb{Q}}$ consists of the followings.

(i) $M_{\mathbb{Q}}$ contains one archimedean value, given by

$$|x|_\infty = \text{ usual absolute value } = \max\{x, -x\}.$$

(ii) For each prime $p \in \mathbb{Z}$, $M_{\mathbb{Q}}$ contains one non-archimedean absolute value, given by

$$|p^n \frac{a}{b}|_p = p^{-n} \text{ for } a,\ b \in \mathbb{Z},\ \gcd(p, ab) = 1.$$

M_K consists of all absolute values on K whose restriction to $\mathbb{Q}$ is one of the absolute values in $M_{\mathbb{Q}}$.

Consider an elliptic curve E over K given by a Weierstrass equation:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in R.$$

Let S be a finite subset of M_K containing

$$M_K^\infty \cup \{v \in M_K^0 | E \text{ has bad reduction at } v\} \cup \{v \in M_K^0 | v \text{ is ramified at } K/\mathbb{Q} \text{ or divides } 2\ \}.$$

Define the local height function $h_{x,v}$ for $v \in M_K \setminus S$ as follows :

$$\begin{aligned} h_{x,v} : E(K) \setminus \{O\} &\longrightarrow \quad \mathbb{R} \\ (x, y) \quad &\mapsto \frac{1}{2}\max\{-v(x), 0\}. \end{aligned} \tag{1}$$

Note that there is a constant C, depending only on E, such that

$$|\hat{h}(M) - \frac{1}{2}h_x(M)| < C \tag{2}$$

for all $M \in E(K)$ and

$$\frac{1}{2}h_x(M) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v h_{x,v}(M) \tag{3}$$

where n_v denotes the local degree $[K_v : \mathbb{Q}_v]$ [10] [11].

For $v \in M_K^0$, $M \bmod \mathfrak{p}_v$ denotes the image of M of the reduction map $E(K) \to E(R/\mathfrak{p}_v)$.

For the proof of the main theorem, we need the following famous theorem [10, p 245] :

Theorem (Siegel). *Let E/K be an elliptic curve with infinite points in $E(K)$, $f \in K(E)$ a non-constant even function, $v \in M_K$, and $Q \in E(\bar{K})$. Then*

$$\lim_{h_f(P)\to\infty} \frac{\log d_v(P,Q)}{h_f(P)} = 0, \tag{4}$$

where $h_f(P)$ denotes the Weil height of P and $d_v(P,Q)$ the v-adic distance from P to Q.

If we take $\mathbb{Q} = O$ and $f = x$ in the above theorem, we get the following useful corollary.

Corollary. *Let E/K be an elliptic curve and M be a non-torsion point of $E(K)$ and $v \in M_K$. Then*

$$\lim_{n\to\infty} \frac{h_{x,v}(nM)}{h_x(nM)} = 0. \tag{5}$$

3. Main Theorem

Lemma. *Let $v \in M_K \setminus S$ and M be a non-torsion point of $E(K)$. Suppose that $M \bmod \mathfrak{p}_v = O$ i.e. $h_{x,v}(M) > 0$. Then*

$$h_{x,v}(nM) = h_{x,v}(M) + v(n) \tag{6}$$

for any positive integer n.

Proof. Let $\mathfrak{M} = \{x \in K_v | v(x) > 0\}$, $\hat{E}$ the formal group associated to E and $\hat{G}_a(\mathfrak{M})$ the additive group $\mathfrak{M}$ with its usual addition. We have an isomorphism [10, IV, Theorem 6.4 (b)],

$$\log_{\hat{E}} : \hat{E}(\mathfrak{M}) \longrightarrow \hat{G}_a(\mathfrak{M}) \tag{7}$$

such that $v(z) = v(\log_{\hat{E}} z)$ for $z \in \mathfrak{M}$. Hence we can identify $\hat{E}(\mathfrak{M})$ with $\hat{G}_a(\mathfrak{M})$.

Moreover, if we let

$$E_1(K_v) = \{M \in E(K_v) | M \bmod \mathfrak{p}_v = O\},$$

we have an isomorphism [10, VII, Proposition 2.2],

$$z : E_1(K_v) \longrightarrow \hat{E}(\mathfrak{M}) \tag{8}$$

such that $v(x[M]) = -2v(z(M))$ for any $M \in E_1(K_v) \setminus \{O\}$, where $x[M]$ denotes the x-coordinate of M.

By (7) and (8), we get $v(x[nM]) = v(x[M]) - 2v(n)$ for any non-torsion point $M \in E_1(K_v) \setminus \{O\}$, because

$$v(z(nM)) = v(\log_{\hat{E}} z(nM)) = v(n \log_{\hat{E}} z(M)) = v(n) + v(z(M)).$$

We complete the proof by (1). □

Now we define a function f_M as a map

$$f_M : M_K \setminus S \to \mathbb{N}$$

such that

$$f_M(v) = \text{ the order of } M \bmod \mathfrak{p}_v \text{ in } E(R/\mathfrak{p}_v).$$

Theorem. *For any non-torsion point $M \in E(K)$, $\mathbb{N} \setminus Im f_M$ is finite. In particular, f_M is surjective for all but finitely many $M \in E(K)$.*

Proof. Given a positive integer n, put $n = \prod_{i=1}^{s} q_i^{r_i}$ for distinct primes q_i and positive integers r_i and let $S(n, M) = \{v \in M_K \setminus S | nM \bmod \mathfrak{p}_v = O \text{ in } E(R/\mathfrak{p}_v)\}$. Note that n belongs to the image of f_M if and only if there exists a prime $p \in S(n, M) - \cup_{i=1}^{s} S(\frac{n}{q_i}, M)$. (If $n = 1$, let $\cup_{i=1}^{s} S(\frac{n}{q_i}, M) = \phi$ by notation.) Suppose that $S(n, M) = \cup_{i=1}^{s} S(\frac{n}{q_i}, M)$. For $v \in M_K \setminus S$, there exists i with $1 \leq i \leq s$ such that

$$h_{x,v}(nM) = h_{x,v}(\frac{n}{q_i} M) + v(q_i) \tag{9}$$

by Lemma. Hence we get

$$h_{x,v}(nM) \leq \sum_{i=1}^{s}\{h_{x,v}(\frac{n}{q_i}M) + v(q_i)\}. \tag{10}$$

For $v \in S$, Siegel theorem (5) implies that for any $\epsilon > 0$,

$$h_{x,v}(nM) \leq \epsilon h_x(nM) \tag{11}$$

for all sufficiently large integer n.

If we let $N = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S} n_v$, by (3), (10) and (11),

$$\begin{aligned} \frac{1}{2}h_x(nM) &\leq \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K\setminus S} n_v\{\sum_{i=1}^{s} h_{x,v}(\frac{n}{q_i}M) + v(q_i)\} + \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S} n_v\epsilon h_x(nM) \\ &\leq N\epsilon h_x(nM) + \sum_{i=1}^{s}\frac{1}{2}h_x(\frac{n}{q_i}M) + \log n \end{aligned} \tag{12}$$

since $\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^0} n_v v(q_i) = \log q_i$. Hence we get

$$(\frac{1}{2} - N\epsilon)h_x(nM) \leq \frac{1}{2}\sum_{i=1}^{s} h_x(\frac{n}{q_i}M) + \log n. \tag{13}$$

On the contrary, if we take $\epsilon < \frac{1}{4N}$, for all sufficiently large integer n

$$\begin{aligned} &\frac{1}{2}\sum_{i=1}^{s} h_x(\frac{n}{q_i}M) + \log n \\ &< \sum_{i=1}^{s}\hat{h}(\frac{n}{q_i}M) + (1+2C)\log n \qquad \text{(by (2) and } s \leq 2\log n) \\ &= \sum_{i=1}^{s}\{\frac{n^2}{q_i^2}\hat{h}(M)\} + (1+2C)\log n \qquad \text{(by quadraticity of } \hat{h}) \\ &< \frac{1}{2}n^2\hat{h}(M) + (1+2C)\log n \qquad (\because \sum_{p:prime}\frac{1}{p^2} < \frac{1}{2}) \\ &< (1-2N\epsilon)(n^2\hat{h}(M) - C) \qquad (\because 1-2N\epsilon > \frac{1}{2} \text{ and } n \gg 0) \\ &< \frac{1}{2}(1-2N\epsilon)h_x(nM). \qquad \text{(by (2))} \end{aligned} \tag{14}$$

It contradicts with (13). Therefore for each sufficiently large integer n, there exists $v \in M_K \setminus S$ such that $v \in S(n, M) \setminus \cup_{i=1}^{s} S(\frac{n}{q_i}, M)$, i.e. the order of M mod $\mathfrak{p}_v$ in $E(R/\mathfrak{p}_v)$ is n.

For the second statement, take ϵ with $0 < \epsilon < \frac{1}{4N}$. If $h_x(M)$ is sufficiently large, $h_{x,v}(nM) < \epsilon h_x(nM)$ for all $n \geq 1$ and all $v \in S$. Hence for all but finitely many $M \in E(K)$, (13) holds for all $n \geq 1$. Also, if $\hat{h}(M)$ is sufficiently large, then

$$\frac{1}{2}n^2\hat{h}(M) + (1+2C)\log n < (1-2N\epsilon)(n^2\hat{h}(M) - C) \tag{15}$$

for all $n \geq 1$ so that for all but finitely many $M \in E(K)$, (14) holds for all $n \geq 1$. Therefore for all but finitely many $M \in E(K)$, $S(n,M) - \cup_{i=1}^{s} S(\frac{n}{q_i}, M) \neq \phi$ for all $n \geq 1$, which implies that f_M is surjective. □

4. Some Examples

In this section, we introduce some examples to deduce $\mathbb{N} \setminus Imf_M$ for an elliptic curve defined over $\mathbb{Q}$. Consider an elliptic curve E over $\mathbb{Q}$ given by a Weierstrass equation:

$$y^2 = x^3 + Ax + B;\ A, B \in \mathbb{Z}.$$

For any non-zero $M = (x, y) \in E(\mathbb{Q})$ and an integer n, the x-coordinate of the point nM is given by

$$x[nM] \doteq \frac{\phi_n(M)}{\psi_n^2(M)}, \tag{16}$$

where $\phi_n(M)$ and $\psi_n^2(M)$ are polynomials in $\mathbb{Z}[x]$, relatively prime in $\mathbb{Q}[x]$ [10, p107].

When we write $M = (\frac{a}{d^2}, \frac{b}{d^3})$ for a,b and $d \in \mathbb{Z}$ with $\gcd(a,d) = 1$ and $d > 0$, we set the following notations ; $\hat{\phi}_m(M) = d^{2m^2}\phi_m(M)$; $\hat{\psi}_m(M) = d^{m^2-1}\psi_m(M)$, where we take $\hat{\psi}_m(M)$ as a positive integer. Then (16) becomes

$$x[nM] = \frac{\phi_n(M)}{\psi_n^2(M)} = \frac{\hat{\phi}_n(M)}{d^2\hat{\psi}_n^2(M)} \tag{17}$$

so that

$$nM = O \text{ if and only if } \hat{\psi}_n(M) = 0 \tag{18}$$

for a non-zero point $M \in E(\mathbb{Q})$. Hence for a non-zero point $M \in E(\mathbb{Q})$, we have

(19) $f_M(p) = n$ if and only if $p|\hat{\psi}_n(M)$ and $p \nmid \hat{\psi}_m(M)$ for any integer $m < n$.

Example 1. Let $E : y^2 = x^3 + 4x + 20$ and $M = (1, 5) \in E(\mathbb{Q})$. $\Delta_E = -2^7 \cdot 167$. From (19) and the following calculation, we may expect that $\mathbb{N} \setminus Imf_M = \{1\}$.

$\hat{\psi}_1(M) = 1$

$\hat{\psi}_2(M) = 2 \cdot 5$

$\hat{\psi}_3(M) = 251$

$\hat{\psi}_4(M) = -2^2 \cdot 3 \cdot 5 \cdot 23 \cdot 47$

$\hat{\psi}_5(M) = -97 \cdot 831683$

$\hat{\psi}_6(M) = -2 \cdot 5 \cdot 251 \cdot 122741447$

$\hat{\psi}_7(M) = 3311717 \cdot 438695947$

$\hat{\psi}_8(M) = 2 \cdot 3 \cdot 5 \cdot 23 \cdot 47 \cdot 307 \cdot 3019 \cdot 4558056703$

$\hat{\psi}_9(M) = 19 \cdot 251 \cdot 94621387$

$\hat{\psi}_{10}(M) = 2 \cdot 5 \cdot 97 \cdot 4261 \cdot 831683 \cdot 3504419 \cdot 2372245029989$

$\hat{\psi}_{11}(M) = 7 \cdot 53 \cdot 71 \cdot 417493 \cdot 13430089 \cdot 18006074321808164774557$

$\hat{\psi}_{12}(M) = -2 \cdot 3 \cdot 5 \cdot 23 \cdot 47 \cdot 251 \cdot 5743 \cdot 11057 \cdot 61224103 \cdot 122741447 \cdot 4895634495812861$

$\hat{\psi}_{13}(M) = -3083 \cdot 3967 \cdot 1290001702772707986533036597725024991050866886591$

$\hat{\psi}_{14}(M) = 2 \cdot 5 \cdot 13 \cdot 3311717 \cdot 438695947 \cdot 34395428644587863980370679502875987956020839061$

$\hat{\psi}_{15}(M) = 97 \cdot 251 \cdot 3727 \cdot 831683 \cdot 6806119882392492984321469567241869862164735927053679025443 37$

Example 2. Let $E : y^2 = x^3 - x + 1$ and $M = (1, 1) \in E(\mathbb{Q})$. $\Delta_E = -2^4 \cdot 23$. From (19) and the following calculation, we may expect that $\mathbb{N} \setminus Imf_M = \{1, 2, 3, 4, 5, 6, 9\}$.

$\hat{\psi}_1(M) = 1$

$\hat{\psi}_2(M) = 2$

$\hat{\psi}_3(M) = 2^3$

$\hat{\psi}_4(M) = 2^5$

$\hat{\psi}_5(M) = -2^8$

$\hat{\psi}_6(M) = -2^{13}$

$\hat{\psi}_7(M) = -2^{16} \cdot 3$

$\hat{\psi}_8(M) = -2^{21} \cdot 5$

$\hat{\psi}_9(M) = -2^{27}$

$\hat{\psi}_{10}(M) = 2^{33} \cdot 11$

$\hat{\psi}_{11}(M) = 2^{40} \cdot 19$

$\hat{\psi}_{12}(M) = 2^{50} \cdot 7$

$\hat{\psi}_{13}(M) = 2^{56} \cdot 53$

$\hat{\psi}_{14}(M) = -2^{65} \cdot 3 \cdot 17$

$\hat{\psi}_{15}(M) = -2^{75} \cdot 223$

$\hat{\psi}_{16}(M) = -2^{85} \cdot 5 \cdot 103$

$\hat{\psi}_{17}(M) = -2^{96} \cdot 1381$

$\hat{\psi}_{18}(M) = -2^{109} \cdot 419$

$\hat{\psi}_{19}(M) = 2^{120} \cdot 13 \cdot 509$

$\hat{\psi}_{20}(M) = 2^{133} \cdot 11 \cdot 1861$

$\hat{\psi}_{21}(M) = 2^{147} \cdot 3^2 \cdot 4903$

$\hat{\psi}_{22}(M) = 2^{161} \cdot 19 \cdot 23 \cdot 347$

$\hat{\psi}_{23}(M) = -2^{176} \cdot 119417 \cdot$

$\hat{\psi}_{24}(M) = -2^{195} \cdot 5 \cdot 7 \cdot 4931$

$\hat{\psi}_{25}(M) = -2^{208} \cdot 71 \cdot 137 \cdot 521$

$\hat{\psi}_{26}(M) = -2^{225} \cdot 43 \cdot 53 \cdot 9281$

$\hat{\psi}_{27}(M) = -2^{243} \cdot 29485343 \cdot$

$\hat{\psi}_{28}(M) = 2^{261} \cdot 3 \cdot 17 \cdot 4231459$

$\hat{\psi}_{29}(M) = 2^{280} \cdot 1243809367$

$\hat{\psi}_{30}(M) = 2^{301} \cdot 11 \cdot 59 \cdot 223 \cdot 13597$

$\hat{\psi}_{31}(M) = 2^{320} \cdot 23663249429$

$\hat{\psi}_{32}(M) = -2^{341} \cdot 5 \cdot 61 \cdot 103 \cdot 173 \cdot 1319$

$\hat{\psi}_{33}(M) = -2^{363} \cdot 19 \cdot 1213 \cdot 20517719$

$\hat{\psi}_{34}(M) = -2^{385} \cdot 149 \cdot 701 \cdot 1381 \cdot 19801$

$\hat{\psi}_{35}(M) = -2^{408} \cdot 3 \cdot 31 \cdot 63649 \cdot 3046601$

References

1. M. Ayad, *Points S-Entiers des Elliptiques*, Manuscripta Math. **76** (1992), 305–324.

2. A. Bang, *Taltheoretiske Untersogelser*, Tidskrift f. Math. **(5) 4** (1886), 70–80 and 130–137.

3. G. D. Birkhoff and H. S. Vandiver, *On the Integral Divisors of $a^n - b^n$*, Annals of Math. **5 (2)** (1904), 173–180.

4. Y. Ihara, *On Fermat Quotient and "Differentiation of Numbers" (in Japanese)*, Rims Kokyuroku 810 (Algebraic Analysis and Number Theory) (1992), 324–341.

5. Y. Ihara (Translated and Supplemented by S. Hahn), *On Fermat Quotient and "Differentiation of Numbers"*, Univ. of Georgia Math. Preprint Ser. **9** (1994).

6. Dale Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.

7. A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.

8. P. Ribenboim, *Catalan's Conjecture*, Academic Press, 1994.

9. A. Schinzel, *Primitive Divisors of the Expression $A^n - B^n$ in Algebraic Number Fields*, J. Reine Angew. Math. **268** (1974), 27–33.

10. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

11. J. Silverman, *The Difference between the Weil Height and the Canonical Height on Elliptic Curves*, Math. Comp. **55** (1990), 723–743.

12. J. Silverman, *Wieferich's Criterion and the abc-Conjecture*, Journal of Number Theory **30** (1988), 226–237.

13. J. Tate, *The Arithmetic of Elliptic Curves*, Invent. Math. **23** (1974), 179–206.

14. L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1979.

15. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. f. Math. **3** (1892), 265–284.

Electronics and Telecommunications Research Institute, 161 Kajong-Dong, Yusong-Gu, Taejon 305-350, Republic of Korea. E-mail address : cheon@crypt.kaist.ac.kr

Department of Mathematics, Korea Advanced Institute of Science and Technology, 373-1 Gusong-Dong, Yusong-Gu, Taejon 305-701, Republic of Korea. E-mail address : sghahn@mathx.kaist.ac.kr