ACTA ARITHMETICA
LXXXVIII.3 (1999)

The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve

by

J. Cheon and S. Hahn (Taejon)

In 1886, A. Bang showed that there exists a constant $M > 0$ so that for each non-zero rational number x, $x \neq \pm 1$, and every integer $n > M$, there exists a prime number p so that the order of x modulo p is equal to n (see [1]). Since then his result was extended and generalized by other mathematicians. In 1892, K. Zsigmondy found a stronger version (see [8], [3, p. 20]). But most of all, in 1974, A. Schinzel proved that for any number field K there exists a constant $M > 0$ so that for each $x \in K^\times$ which is not a root of unity, and every integer $n > M$, there exists a prime ideal $\wp$ of K so that the order of x modulo $\wp$ is equal to n (see [4]). Motivated by Y. Ihara's interpretation of Bang's theorem (see [2]), in this paper we prove the following elliptic analogue.

Theorem. *Let E be an elliptic curve over a number field K and let $P \in E(K)$ be a point of infinite order. Then for every sufficiently large integer n there exists a prime $\wp$ of good reduction so that the order of P in the group of points of E modulo $\wp$ is equal to n. Moreover, for all but finitely many P there exists such a prime $\wp$ for each $n > 0$.*

J. Silverman proved the above theorem for elliptic curves defined over $\mathbb{Q}$ (see [7]) which we prove first by explicit valuations of division polynomials. To prove the full theorem, we use essentially the same techniques, namely formal groups and heights, as Silverman did. In Schinzel's result the constant M which depends on the number field K was effectively computable. Though we obtain a stronger result for the elliptic analogue, namely $n > 0$ is enough for all but finitely many P, we could not get an effective estimate for those finitely many exceptions.

1991 *Mathematics Subject Classification*: 11G05, 11G20, 14H52.
Key words and phrases: Bang's theorem, elliptic curves, reductions, local heights.

From now on, we use the following notations:

- K : a number field,
- R : the ring of integers of K,
- v : a normalized absolute value on K as described in [5, Ch. VIII, §5],
- $\wp_v = \{x \in R \mid v(x) > 0\}$: the prime ideal of R associated with v,
- K_v : the quotient field of the completion of R at v.

Consider an elliptic curve E over K. Let S be a finite set of primes of K, containing the infinite primes, the primes over 2, the primes that are ramified in K and the primes for which E has bad reduction.

Define a local height function $h_{x,v}$ temporarily for a prime v on K as follows:

$$h_{x,v} : E(K) \setminus \{O\} \to \mathbb{R}, \quad (x,y) \mapsto \tfrac{1}{2}\max\{-v(x), 0\}, \tag{1}$$

and denote by $\widehat{h}$ the canonical height on E and by h_x the Weil height on E. By [6] there is a constant C, depending only on E, such that

$$|\widehat{h}(M) - h_x(M)| < C \tag{2}$$

for all $M \in E(K)$. We have

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

where n_v denotes the local degree $[K_v : \mathbb{Q}_v]$ (see [5, Ch. VIII, §5]).

From now on, $M \bmod \wp_v$ denotes the image of M under the reduction map $E(K) \to E(R/\wp_v)$ for a finite prime v.

Lemma. *Let v be a prime not in S and M be a non-torsion point of $E(K)$. Suppose that $M \bmod \wp_v = O$, i.e. $h_{x,v}(M) > 0$. Then*

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

for any positive integer n.

Proof. Let $\mathcal{M} = \{x \in K_v \mid v(x) > 0\}$, $\widehat{E}$ the formal group associated with E and $\widehat{G}_a(\mathcal{M})$ the additive group $\mathcal{M}$ with its usual addition. We have an isomorphism [5, Ch. IV, Theorem 6.4(b)]

$$\log_{\widehat{E}} : \widehat{E}(\mathcal{M}^r) \to \widehat{G}_a(\mathcal{M}^r) \tag{4}$$

for any $r > 0$, because v is not in S. Hence we identify $\widehat{E}(\mathcal{M})$ with $\widehat{G}_a(\mathcal{M})$ and we get $v(z) = v(\log_{\widehat{E}} z)$ for $z \in \mathcal{M}$.

Moreover, letting

$$E_1(K_v) = \{M \in E(K_v) \mid M \bmod \wp_v = O\},$$

we have an isomorphism [5, Ch. VII, Proposition 2.2]

$$z : E_1(K_v) \to \widehat{E}(\mathcal{M}) \tag{5}$$

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 (4) and (5), we get $v(x[nM]) = v(x[M]) - 2v(n)$ for any non-torsion point $M \in E_1(K_v) \setminus \{O\}$, because

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

Since $v(x[M]) < 0$ by assumption, we have $h_{x,v}(nM) = h_{x,v}(M) + v(n)$ by (1). ∎

Using the above Lemma, we can prove the Theorem.

Proof of Theorem. Suppose n does not occur as the order of M modulo $\wp_v$. That means that for every v with $h_{x,v}(nM) > 0$, there exists a prime q dividing n so that $h_{x,v}\big(\frac{n}{q}M\big) > 0$. Therefore, for every such $v \notin S$, the Lemma shows that

$$h_{x,v}(nM) = h_{x,v}\left(\frac{n}{q}M\right) + v(q) \le \sum_{q|n} \left\{ h_{x,v}\left(\frac{n}{q}M\right) + v(q) \right\}. \tag{6}$$

Combining this estimate with formula (3) we find that

$$h_x(nM) \le \sum_{q|n} h_x\left(\frac{n}{q}M\right) + \sum_{v \in S} h_{x,v}(nM) + \sum_{q|n} \sum_{v \notin S} v(q). \tag{7}$$

The last term on the right is easily seen to be less than $\log n$. Since M is not a torsion point, we can apply Siegel's Theorem [7, Ch. IX, Theorem 3.1] to the second term: for every $\varepsilon > 0$ and sufficiently large n we have

$$h_{x,v}(nM) \le \varepsilon h_x(nM). \tag{8}$$

Finally, we use the fact that the difference between the naive height h_x and the canonical height $\widehat{h}$ is bounded on the Mordell–Weil group $E(K)$. Since the canonical height is a quadratic function, this gives the following inequality:

$$n^2 \widehat{h}(M) \le n^2 \widehat{h}(M) \sum_{q|n} \frac{1}{q^2} + \#S \cdot n^2 \varepsilon \widehat{h}(M) + \log n + C, \tag{9}$$

for some constant C and for sufficiently large n. Therefore

$$\left(1 - \varepsilon \#S - \sum_{q|n} \frac{1}{q^2}\right) \widehat{h}(M) \le \frac{\log n + C}{n^2}. \tag{10}$$

Since $\sum_{q|n} 1/q^2 \le \sum_{q \text{ prime}} 1/q^2 \le 1/2$, we can choose $\varepsilon > 0$ so small that the coefficient $1 - \varepsilon \#S - \sum_{q|n} 1/q^2$ is positive. Since M is not torsion, we have $\widehat{h}(M) > 0$ so that the inequality implies that n is bounded, as required.

For the second statement of the Theorem, we observe that for any $\varepsilon > 0$, Siegel's inequality $h_{x,v}(nM) \le \varepsilon h_x(nM)$ actually holds for all $n \ge 1$ if the

height of M is sufficiently large. Therefore the final inequality implies that $n < 1$ whenever the height of M is sufficiently large. Since there are only finitely many points $M \in E(K)$ of bounded height, the second statement follows. ∎

Acknowledgements. We would like to thank the anonymous referee for a number of helpful suggestions.

References

[1] A. Bang, *Taltheoretiske Undersøgelser*, Tidsskr. Math. (5) 4 (1886), 70–80 and 130–137.
[2] Y. Ihara, *On Fermat quotient and "differentiation of numbers"*, RIMS Kokyuroku 810 (Algebraic Analysis and Number Theory) (1992), 324–341 (in Japanese).
[3] P. Ribenboim, *Catalan's Conjecture*, Academic Press, 1994.
[4] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. 268 (1974), 27–33.
[5] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
[6] —, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723–743.
[7] —, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237.
[8] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. 3 (1892), 265–284.

J. Cheon
Section 0710
Electronics and Telecommunications
Research Institute
Taejon 305-350
Republic of Korea
E-mail: jhcheon@etri.re.kr

S. Hahn
Department of Mathematics
Korea Advanced Institute
of Science and Technology
Taejon 305-701
Republic of Korea
E-mail: sghahn@math.kaist.ac.kr

Received on 10. 6. 1997
and in revised form on 26.10.1998 (3201)