BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 63, No. 1, 2015

NUMBER THEORY

Height Functions for Groups of S-units of Number Fields and Reductions Modulo Prime Ideals

by

Stefan BARAŃCZUK

Presented by Jerzy KACZOROWSKI

Summary. A result on the orders of the reductions of an element of the group of S-units of a number field is obtained by investigating three height functions for groups of S-units of number fields which are analogous to local, global and canonical height functions for elliptic curves.

1. Introduction. Let K be a number field, v a prime ideal of K, and $x \in K^\times$ such that $|x|_v = 0$. For $\varepsilon \geq 0$ define

$$C_\varepsilon = \left\{ n \in \mathbb{N} \colon \sum_{q|n} \frac{1}{q} \leq 1 - \varepsilon \right\}$$

where the sum is taken over distinct prime divisors of n. In this paper we will prove the following

THEOREM 1.1. *If K is a number field, S a finite set of primes of K and $\varepsilon > 0$ then for almost all $x \in \mathcal{O}_{K,S}^\times$ and for every $n \in C_\varepsilon$ there is a prime v of K such that the multiplicative order of x modulo v equals n.*

This result is inspired by an analogous theorem for elliptic curves over number fields due to J. Cheon and S. Hahn [ChH, Theorem], generalizing a result of J. Silverman [Si2, Proposition 10], and by similarities between the Mordell–Weil groups of elliptic curves and the groups of S-units. In their proof Cheon and Hahn used three height functions on elliptic curves (local, Weil and canonical). In order to prove our theorem we will consider three

2010 *Mathematics Subject Classification*: Primary 11G50, 11R27; Secondary 11J68.
Key words and phrases: S-units, reductions, height functions, primitive divisors.

DOI: 10.4064/ba63-1-4

analogous heights for the groups of S-units, slightly modifying the height of an algebraic number.

Our theorem is closely related to the following classical result by A. Schinzel [Sch, Theorem 1]:

THEOREM. *If K is a number field and $x \in K$ is not a root of unity then there exists a natural number N, depending only on the degree of x, such that for every $n > N$ there is a prime v of K such that the multiplicative order of x modulo v equals n.*

In Theorem 1.1 we have a different restriction on the orders n than that in Schinzel's theorem, in particular the conclusion of our theorem holds for all natural numbers smaller than 30. Generally, all natural numbers having at most two distinct prime divisors belong to $C_{1/6}$ and according to unpublished computations of M. Filaseta the density of the set

$$\Big\{n \in \mathbb{N}\colon \sum_{q|n} \frac{1}{q} \le 1\Big\}$$

where the sum is taken over distinct prime divisors of n is at least 0.94.

2. Height functions. We will use the following notation:

K	a number field
M_K	the set of places of K
$\mathcal{O}_K$	the ring of integers of K
S	a finite set of primes of K
$\mathcal{O}_{K,S}^{\times}$	the group of S-units
$\log^+ t = \max(0, \log t)$	for positive real numbers t
$\log^+ 0 = 0$	
$h(\alpha) = \sum_{v \in M_K} \log^+ \lvert\alpha\rvert_v$	the height of an algebraic number α

Let $x \in K^{\times}$. We denote

- the *local contribution to the shifted height of x relative to $v \in M_K$* (analogous to the local height function on an elliptic curve) by

$$\boldsymbol{w}_v(x) := \log^+ \lvert 1 - x\rvert_v^{-1} \quad \text{for } x \neq 1,$$
$$\boldsymbol{w}_v(1) := 0;$$

- the *shifted height of x* (analogous to the global height function on an elliptic curve) by

$$\boldsymbol{w}(x) := \sum_{v \in M_K} \boldsymbol{w}_v(x) = h(1 - x)$$

(note that $h(1/\alpha) = h(\alpha)$ for $\alpha \neq 0$, see [BG, Lemma 1.5.18]);

- the *Weil height of x* (analogous to the canonical height function on an elliptic curve) by
$$\hat{\boldsymbol{w}}(x) := h(x).$$
(We keep the same symbols as in the elliptic curves case.)

The following property is a trivial analogue of [Zim, Theorem]:

PROPOSITION 2.1. *For every $x \in \bar{\mathbb{Q}}$,*
$$|\hat{\boldsymbol{w}}(x) - \boldsymbol{w}(x)| \leq \log 2.$$

Proof. By [BG, Prop. 1.5.15] we get
$$h(1-x) \leq h(1) + h(-x) + \log 2 = h(x) + \log 2,$$
hence $h(1-x) - h(x) \leq \log 2$. Substitution of $y = 1-x$ gives
$$h(y) - h(1-y) \leq \log 2. \ \blacksquare$$

Let $\tilde{S}$ 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 belonging to S. The following immediate consequence of [Sch, Lemma 3] is an analogue of [ChH, Lemma]:

LEMMA 2.2. *Let v be a prime not in $\tilde{S}$ and $x \in \mathcal{O}_{K,S}^{\times}$ be such that x is not a root of unity and $x = 1 \bmod v$. Then*
$$\boldsymbol{w}_v(x^n) = \boldsymbol{w}_v(x) + \log |n|_v^{-1}$$
for every positive integer n.

Proof. Let ε denote the normalized exponential valuation defined by v. Since $x = 1 \bmod v$, we have $\varepsilon(1-x) \geq 1$. Let p be the prime number below v. Since we assume that $v \notin \tilde{S}$ we have $\varepsilon(p) = 1$ (because v is not ramified) and $p \geq 3$, so $\varepsilon(p)/(p-1) < 1$. Hence the assumptions of [Sch, Lemma 3] are satisfied and its assertion immediately gives the desired conclusion. $\blacksquare$

The following property is an analogue of Siegel's theorem (see [Si1, Chapter IX, Theorem 3.1]) and might be viewed as a multiplicative Roth theorem (see Remark 2.4 below):

THEOREM 2.3. *Let S be a finite set of places of a number field K and let $v \in S$. If $\xi \in K_v$ is algebraic over K, then*
$$\lim_{\boldsymbol{w}(x)\to\infty} \frac{\boldsymbol{w}_v(x/\xi)}{\boldsymbol{w}(x)} = 0$$
where the limit is taken over $x \in \mathcal{O}_{K,S}^{\times}$.

Proof. The proof is analogous to the proof of Siegel's theorem. Choose a sequence of distinct numbers x_i such that
$$\lim_{i\to\infty} \frac{-\boldsymbol{w}_v(x_i/\xi)}{\boldsymbol{w}(x_i)} = \liminf_{\boldsymbol{w}(x)\to\infty} \frac{-\boldsymbol{w}_v(x/\xi)}{\boldsymbol{w}(x)} = L.$$

Since by the definition of heights

$$\frac{-\boldsymbol{w}_v(x/\xi)}{\boldsymbol{w}(x)} \leq 0,$$

it suffices to check that $L \geq 0$.

Let m be a large natural number. By Dirichlet's S-unit theorem the group $\mathcal{O}_{K,S}^{\times}/(\mathcal{O}_{K,S}^{\times})^m$ is finite, hence one of the cosets, say with representative r, contains infinitely many numbers x_i. Let us denote $\{x_i\}_{i\in\mathbb{N}} \cap r(\mathcal{O}_{K,S}^{\times})^m$ again by $\{x_i\}_{i\in\mathbb{N}}$. Then $x_i = y_i^m r$ for some $y_i \in \mathcal{O}_{K,S}^{\times}$. We will show that

$$m\boldsymbol{w}(y_i) \leq \boldsymbol{w}(x_i) + O(1) \tag{1}$$

where $O(1)$ is independent of i but depends on m. Indeed, since h is a homogeneous function, by Proposition 2.1 we get

$$m\boldsymbol{w}(y_i) = \boldsymbol{w}(y_i^m) + O(1) = \boldsymbol{w}(x_i/r) + O(1),$$

and by the definition of the height h we have $h(\alpha\beta) \leq h(\alpha) + h(\beta)$, so $h(x_i/r) \leq h(x_i) + h(r)$.

If $\boldsymbol{w}_v(x_i/\xi)$ is bounded then we easily get $L = 0$. So suppose that this is not the case, i.e. there is a subsequence so that $x_i \to \xi$ with respect to the v-adic topology. Then one of the mth roots of ξ/r, which will be denoted by $\sqrt[m]{\xi/r}$, must be an accumulation point of the sequence $\{y_i\}$. Hence we have two sequences, denoted again by $\{y_i\}$ and $\{x_i\}$, such that $y_i \to \sqrt[m]{\xi/r}$ and $x_i \to \xi$. An easy computation shows that

$$\lim_{i\to\infty} \frac{\min(0, \log|\xi - x_i|_v)}{\min(0, \log|\sqrt[m]{\xi/r} - y_i|_v)} = 1.$$

Combining this formula with (1) we conclude that

$$L = \lim_{i\to\infty} \frac{-\boldsymbol{w}_v(x_i/\xi)}{\boldsymbol{w}(x_i)} \geq \liminf_{i\to\infty} \frac{\min(0, \log|\sqrt[m]{\xi/r} - y_i|_v)}{m\boldsymbol{w}(y_i) + O(1)}.$$

Now by Roth's theorem (see [BG, Theorem 6.2.3]) and Proposition 2.1 we get

$$\liminf_{i\to\infty} \frac{\min(0, \log|\sqrt[m]{\xi/r} - y_i|_v)}{\boldsymbol{w}(y_i) + O(1)} \geq -2,$$

and thus

$$L \geq -\frac{2}{m}.$$

But m was arbitrary, therefore $L \geq 0$. ∎

Remark 2.4. Theorem 2.3 is the analogue of Siegel's theorem for our heights and if $H(\alpha) = e^{h(\alpha)}$ denotes the absolute exponential height of an algebraic number then using Proposition 2.1 we can rewrite Theorem 2.3 as follows:

Let S be a finite set of places of a number field K. Let $v \in S$ and let $\xi \in K_v$ be algebraic over K. Then for every $\kappa > 0$ there are only finitely many $x \in \mathcal{O}_{K,S}^{\times}$ such that

$$\min\left(1, \left|1 - \frac{x}{\xi}\right|_v\right) \le H(x)^{-\kappa}.$$

Thus we can call it a multiplicative Roth theorem for S-units. We are indebted to Grzegorz Banaszak for demonstrating to us that it can also be obtained from [L, Corollary 1.2, p. 161]. In our proof we follow the lines of the proof of Siegel's theorem in order to emphasize the link with elliptic curves.

3. Proof of Theorem 1.1. In most of the proof we will follow [ChH, proof of Theorem].

Suppose that $x \in \mathcal{O}_{K,S}^{\times}$ is not a root of unity. Let v be a prime satisfying $x^n = 1 \bmod v$, i.e. $\boldsymbol{w}_v(x^n) > 0$. Assume that n is not the order of $x \bmod v$, which means that there exists a prime number q dividing n such that $x^{n/q} = 1 \bmod v$, i.e. $\boldsymbol{w}_v(x^{n/q}) > 0$. If additionally $v \notin \tilde{S}$ then by Lemma 2.2,

$$\boldsymbol{w}_v(x^n) = \boldsymbol{w}_v(x^{n/q}) + \log|q|_v^{-1} \le \sum_{q|n} [\boldsymbol{w}_v(x^{n/q}) + \log|q|_v^{-1}].$$

Combining this with the definition of the global height $\boldsymbol{w}$ we get

$$\begin{aligned}
\boldsymbol{w}(x^n) &= \sum_{v\in\tilde{S}} \boldsymbol{w}_v(x^n) + \sum_{v\notin\tilde{S}} \boldsymbol{w}_v(x^n)\\
&\le \sum_{v\in\tilde{S}} \boldsymbol{w}_v(x^n) + \sum_{v\notin\tilde{S}} \sum_{q|n} [\boldsymbol{w}_v(x^{n/q}) + \log|q|_v^{-1}]\\
&\le \sum_{v\in\tilde{S}} \boldsymbol{w}_v(x^n) + \sum_{q|n} \sum_{v} \boldsymbol{w}_v(x^{n/q}) + \sum_{q|n} \sum_{v\notin\tilde{S}} \log|q|_v^{-1}\\
&\le \sum_{v\in\tilde{S}} \boldsymbol{w}_v(x^n) + \sum_{q|n} \boldsymbol{w}(x^{n/q}) + \log n
\end{aligned}$$

since clearly $\sum_{q|n} \sum_{v\notin\tilde{S}} \log|q|_v^{-1} \le \log n$. Now by Theorem 2.3 we get, for $\mu > 0$ and $\boldsymbol{w}(x)$ large enough,

$$\boldsymbol{w}_v(x^n) \le \mu \boldsymbol{w}(x^n),$$

hence finally

$$\boldsymbol{w}(x^n) \le \sharp\tilde{S}\mu\boldsymbol{w}(x^n) + \sum_{q|n} \boldsymbol{w}(x^{n/q}) + \log n.$$

Using Proposition 2.1 and the fact that $\hat{\boldsymbol{w}} = h$ is a homogeneous function we have

$$n\hat{\boldsymbol{w}}(x) - \log 2 \le \sharp\tilde{S}\mu(n\hat{\boldsymbol{w}}(x) + \log 2) + \sum_{q|n}\left(\frac{n}{q}\hat{\boldsymbol{w}}(x) + \log 2\right) + \log n,$$

so

$$\left(1 - \sharp\tilde{S}\mu - \sum_{q|n}\frac{1}{q}\right)\hat{\boldsymbol{w}}(x) \le \frac{\log n + (1 + \sharp\tilde{S}\mu + d(n))\log 2}{n}$$

where $d(n)$ denotes the number of divisors of n. Choosing $\mu > 0$ small enough so that

$$1 - \sharp\tilde{S}\mu - \sum_{q|n}\frac{1}{q} \ge \varepsilon > 0$$

we see that $\hat{\boldsymbol{w}}(x)$ must be bounded since $\frac{\log n + (1+\sharp\tilde{S}\mu + d(n))\log 2}{n}$ is bounded. But by Northcott's theorem (see [BG, Theorem 1.6.8]) there exist only finitely many $x \in \mathcal{O}_{K,S}^{\times}$ with bounded height. Since by Schinzel's theorem cited in the Introduction we need to consider only finitely many numbers n, the proof is complete.

Remark 3.1. Note that in [ChH, Theorem] there is no additional condition on the numbers n. The difference from our result is caused by the fact that $\hat{\boldsymbol{w}}$ is a homogeneous function while the canonical height $\hat{h}$ on an elliptic curve is a quadratic function. Hence instead of the sum $\sum_{q|n}\frac{1}{q}$ we obtain at the end of the proof, they get $\sum_{q|n}\frac{1}{q^2}$ which is bounded by $\frac{1}{2}$, so there exists $\mu > 0$ small enough such that $1 - \sharp\tilde{S}\mu - \sum_{q|n}\frac{1}{q^2}$ is positive for all natural numbers n.

Acknowledgments. The author would like to thank Université Louis Pasteur, Institut de Recherche Mathématique Avancée, for cordial hospitality and financial support during his post-doc stay in 2007 (Marie Curie Research Training Network Fellowship) when his interest in the topic of the article begun. He is deeply obliged to Grzegorz Banaszak for his remarks and encouragement. He is also grateful to Yann Bugeaud, Wojciech Gajda, Krzysztof Górnisiewicz, Jerzy Kaczorowski and Francesco Veneziano for discussions, to Adrian Łydka for drawing the author's attention to Filaseta's unpublished result described at the end of the Introduction, and to the anonymous referees for their remarks and corrections of inaccuracies.

References

[BG] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge Univ. Press, 2006.

[ChH] J. Cheon and S. Hahn, *The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve*, Acta Arith. 88 (1999), 219–222.

[L] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.
[Sch] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. 268 (1974), 27–33.
[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
[Si2] J. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237.
[Zim] H. G. Zimmer, *On the difference of the Weil height and the Néron–Tate height*, Math. Z. 147 (1976), 35–51.

Stefan Barańczuk
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
61-614 Poznań, Poland
E-mail: stefbar@amu.edu.pl

Received March 20, 2015;
received in final form August 11, 2015 (8015)