ACTA ARITHMETICA
133.2 (2008)

On heights of multiplicatively dependent algebraic numbers

by

C. L. Stewart (Waterloo, ON)

Dedicated to Professor Wolfgang Schmidt on his 75th birthday

1. Introduction. Our objective in this note is to prove that if A is a set of non-zero algebraic numbers, any t of which are multiplicatively dependent, then, provided that the cardinality of A is large enough, two of the algebraic numbers will have a quotient of small height. As a consequence of our result we are able to give an upper bound for the number of powers of rational numbers of small height in short intervals. A second application may be found in [9].

Let K be a finite extension of $\mathbb{Q}$ of degree d. Let M_K be the set of places on K. In each place v of M_K we choose a valuation $|\ |_v$ on K in the following way. If v is a finite place, so v only contains non-Archimedean valuations, then v restricted to $\mathbb{Q}$ belongs to a prime p. We put $d_v = [K_v : \mathbb{Q}_p]$, where K_v and $\mathbb{Q}_p$ denote the completions of K at v and $\mathbb{Q}$ at p, respectively. We choose v so that

$$|\alpha|_v = |\alpha|_p^{d_v/d} \quad \text{for } \alpha \text{ in } \mathbb{Q},$$

where $|\ |_p$ denotes the usual p-adic valuation on $\mathbb{Q}$ normalized so that $|p|_p = p^{-1}$. If v is an infinite place we choose v so that

$$|\alpha|_v = |\alpha|^{d_v/d} \quad \text{for } \alpha \text{ in } \mathbb{Q},$$

where $|\ |$ denotes the ordinary absolute value on $\mathbb{Q}$ and where $d_v = [K_v : \mathbb{R}]$ so that d_v is 1 if K is contained in $\mathbb{R}$ and 2 otherwise.

For any α in K we define the *height* of α, denoted by $H(\alpha)$, by

$$H(\alpha) = \prod_{v \in M_K} \max(1, |\alpha|_v).$$

2000 *Mathematics Subject Classification*: 11G50, 11J87.
Key words and phrases: heights, powers in short intervals.
This research was supported in part by grant A3528 from the Natural Sciences and Engineering Research Council of Canada and by the Canada Research Chairs Program.

Notice that the height of α does not depend on the field K. Further, for any non-zero integer k,

$$H(\alpha^k) = (H(\alpha))^{|k|} \tag{1}$$

for any α. In addition, $H(\alpha) = 1$ if and only if α is a root of unity or $\alpha = 0$. Furthermore, if $\alpha_1, \ldots, \alpha_r$ are in K then

$$H(\alpha_1 \cdots \alpha_r) \le H(\alpha_1) \cdots H(\alpha_r), \tag{2}$$

$$H(\alpha_1 + \cdots + \alpha_r) \le rH(\alpha_1) \cdots H(\alpha_r). \tag{3}$$

For any real number x let $\lceil x \rceil$ denote the smallest integer greater than or equal to x.

Theorem 1. *Let ε be a real number with $0 < \varepsilon < 1$ and let t be an integer with $t \ge 2$. Let $\alpha_1, \ldots, \alpha_k$ be non-zero algebraic numbers with the property that any t of them are multiplicatively dependent. Suppose that*

$$k \ge t\left(1 + \left\lceil \frac{1}{\varepsilon} \right\rceil^{t-1}\right). \tag{4}$$

Then there exist distinct integers $i_0, \ldots, i_t$ for which

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \le (H(\alpha_{i_2}) \cdots H(\alpha_{i_t}))^{\varepsilon}.$$

Theorem 1 may be contrasted with the results of van der Poorten and Loxton [7], Matveev [6], and Loher and Masser [4], where the authors prove that if $\alpha_1, \ldots, \alpha_t$ are multiplicatively dependent algebraic numbers then there is a relation of the form

$$\alpha_1^{l_1} \cdots \alpha_t^{l_t} = 1$$

with $l_1, \ldots, l_t$ integers, not all zero, and with $\max_{1 \le i \le t} |l_i|$ explicitly bounded from above in terms of the heights and degrees of $\alpha_1, \ldots, \alpha_t$.

2. Proof of Theorem 1. There are $\binom{k}{t}$ t-tuples $(i_1, \ldots, i_t)$ with $1 \le i_1 < i_2 < \cdots < i_t \le k$. Since any t of the α_i's are multiplicatively dependent, $\alpha_{i_1}, \ldots, \alpha_{i_t}$ are multiplicatively dependent and so there are integers $l_{i_1}, \ldots, l_{i_t}$, not all zero, for which

$$\alpha_{i_1}^{l_{i_1}} \cdots \alpha_{i_t}^{l_{i_t}} = 1. \tag{5}$$

Associate $(l_{i_1}, \ldots, l_{i_t})$ to $(i_1, \ldots, i_t)$ and suppose that i_j is an index for which

$$|l_{i_j}| \ge |l_{i_n}| \quad \text{for } 1 \le n \le t.$$

We then associate to $(i_1, \ldots, i_t)$ the $t-1$-tuple $(i_1, \ldots, \widehat{i_j}, \ldots, i_t)$, where the symbol $\widehat{}$ indicates that the jth coordinate has been dropped. Put

$$m = \left\lceil \binom{k}{t} \Big/ \binom{k}{t-1} \right\rceil = \left\lceil \frac{k-t+1}{t} \right\rceil.$$

Since there are $\binom{k}{t-1}$ $t-1$-tuples, at least one of them is associated with m t-tuples.

Pick that $t-1$-tuple. By reordering the α_i's we may assume, without loss of generality, that the $t-1$-tuple is $(1,\dots,t-1)$ and the associated m t-tuples are $(1,\dots,t-1,t-1+j)$ for $j=1,\dots,m$. Then there are integers $l_{1,j},\dots,l_{t-1,j}$ and l_j for $j=1,\dots,m$ with $|l_{i,j}|\le|l_j|$ and $l_j>0$ and for which

$$\alpha_1^{l_{1,j}}\cdots\alpha_{t-1}^{l_{t-1,j}}=\alpha_{j+t-1}^{l_j}. \tag{6}$$

Put $b_{i,j}=l_{i,j}/l_j$ for $i=1,\dots,t-1$ and $j=1,\dots,m$ and put $B_j=(b_{1,j},\dots,b_{t-1,j})$ for $j=1,\dots,m$. Notice that B_j is in $[0,1]^{t-1}$. Thus, by the box principle, for

$$m>\left\lceil\frac{1}{\varepsilon}\right\rceil^{t-1}, \tag{7}$$

there exist two vectors B_u and B_s with $1\le u<s\le m$ for which

$$|b_{i,u}-b_{i,s}|\le\varepsilon\quad\text{for } i=1,\dots,t-1. \tag{8}$$

We have

$$\alpha_1^{l_sl_{1,u}-l_ul_{1,s}}\cdots\alpha_{t-1}^{l_sl_{t-1,u}-l_ul_{t-1,s}}=\left(\frac{\alpha_{u+t-1}}{\alpha_{s+t-1}}\right)^{l_ul_s}. \tag{9}$$

Therefore,

$$H\left(\frac{\alpha_{u+t-1}}{\alpha_{s+t-1}}\right)^{l_ul_s}\le H(\alpha_1)^{|l_sl_{1,u}-l_ul_{1,s}|}\cdots H(\alpha_{t-1})^{|l_sl_{t-1,u}-l_ul_{t-1,s}|}$$

and so, by (8),

$$H\left(\frac{\alpha_{u+t-1}}{\alpha_{s+t-1}}\right)\le(H(\alpha_1)\cdots H(\alpha_{t-1}))^{\varepsilon},$$

provided (7) holds. But since $m\ge(k-t+1)/t$, condition (4) shows that (7) holds and the result follows. ■

3. Some corollaries of Theorem 1

COROLLARY 1. *Let δ and ε be real numbers with $0<\varepsilon<1$ and $0\le\delta$. Let t be an integer with $t\ge2$ and let T be a real number with $T\ge1$. Let $\alpha_1,\dots,\alpha_k$ be distinct non-zero algebraic numbers with the property that any t of them are multiplicatively dependent. Suppose that*

$$k\ge t\left\lceil\frac{t-1}{\varepsilon}\right\rceil^{t-1}+t \tag{10}$$

and that

$$T^{1-\delta}\le H(\alpha_i)\le 2T\quad\textit{for } i=1,\dots,k. \tag{11}$$

Then there exist i_0 and i_1, with $1 \le i_0 < i_1 \le k$, for which

$$H(\alpha_{i_0} - \alpha_{i_1}) \ge \frac{1}{4} T^{1-\delta-\varepsilon}.$$

Proof. On replacing ε by $\varepsilon/(t-1)$ in the statement of Theorem 1 we find that, provided (10) holds, there exist distinct integers $i_0, \ldots, i_t$ for which

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \le ((H(\alpha_{i_2}) \cdots H(\alpha_{i_t}))^{1/(t-1)})^{\varepsilon}$$

and so, by (11),

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \le (2T)^{\varepsilon}.$$

But

$$\alpha_{i_0} = (\alpha_{i_0} - \alpha_{i_1})\left(1 - \frac{\alpha_{i_1}}{\alpha_{i_0}}\right)^{-1}$$

so, by (1) with $k = -1$ and (2),

$$H(\alpha_{i_0}) \le H\left(1 - \frac{\alpha_{i_1}}{\alpha_{i_0}}\right) H(\alpha_{i_0} - \alpha_{i_1}) \le 2H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) H(\alpha_{i_0} - \alpha_{i_1})$$

and therefore, by (11),

$$H(\alpha_{i_0} - \alpha_{i_1}) \ge (2(2T)^{\varepsilon})^{-1} T^{1-\delta} \ge \frac{1}{4} T^{1-\delta-\varepsilon},$$

as required. ∎

Corollary 2. *Let ε be a real number with $0 < \varepsilon < 1$ and let t and N be positive integers. Let $a_1, \ldots, a_k$ be distinct positive integers with*

$$N \le a_i \le 2N \quad \text{for } i = 1, \ldots, k.$$

Suppose that any t integers from $\{a_1, \ldots, a_k\}$ are multiplicatively dependent. Suppose also that

$$k \ge t \left\lceil \frac{t-1}{\varepsilon} \right\rceil^{t-1} + t.$$

Then there exist i_0, i_1 with $1 \le i_0 < i_1 \le k$ for which

$$|a_{i_0} - a_{i_1}| \ge \frac{1}{4} N^{1-\varepsilon}.$$

Proof. We apply Corollary 1 with $\delta = 0$ and $\alpha_i = a_i$ for $i = 1, \ldots, k$. Our result follows on noting that if a is a non-zero integer then $H(a) = |a|$. ∎

Corollary 3. *Let ε be a real number with $0 < \varepsilon < 1$. Let N be a positive integer and let $a_1, \ldots, a_k$ be distinct integers with*

$$N \le a_i < N + \frac{1}{4} N^{1-\varepsilon} \tag{12}$$

for $i = 1, \ldots, k$. If t is a positive integer and

$$k \geq t\left\lceil\frac{t-1}{\varepsilon}\right\rceil^{t-1} + t$$

then there are at least t integers from $\{a_1, \ldots, a_k\}$ which are multiplicatively independent.

Proof. If every set of t integers chosen from $\{a_1, \ldots, a_k\}$ is multiplicatively dependent then by Corollary 2 there exist two of the a_i's which differ by at least $(1/4)N^{1-\varepsilon}$, which is impossible by (12). ■

4. Powers in short intervals. We are able to deduce from Theorem 1 an estimate for the number of perfect powers of integers in a short interval. In 1986 Loxton [5] asserted that if N exceeds 16 then the interval $[N, N+N^{1/2}]$ contains at most

$$\exp(40(\log\log N \cdot \log\log\log N)^{1/2})$$

perfect powers. His result improved on that of Turk [11], who proved in 1980 that there exists a positive number c for which such an interval contains at most $c(\log N)^{1/2}$ perfect powers. Loxton deduced his result from a lower bound he had established for simultaneous linear forms in the logarithms of algebraic numbers. However, his argument is not complete in the case that the integers he considers are multiplicatively dependent. In particular, Loxton reduces the set of multiplicatively dependent integers to a subset of the powers which are multiplicatively independent. It may be, though, that the rank of the matrix of coefficients associated with the linear forms Λ_i after the reduction is not full. This difficulty is overcome in a paper of Bernstein [2] from 1998 by means of an ingenious argument which Bernstein attributes to Loxton. One purpose of this section is to give a simple alternative proof of Loxton's result by means of Theorem 1. Another purpose is to extend the result to include rational numbers which are powers.

It is an easy consequence of the *abc* conjecture (see e.g. [10]) that if there are arbitrarily large integers N for which the interval $[N, N+N^{1/2}]$ contains distinct ath and bth powers then $1/a+1/b \geq 1/2$. If a and b are both bigger than 2 then (a, b) is one of $(3,4)$, $(3,5)$ or $(3,6)$. Certainly $(3,6)$ is not a possibility since two distinct cubes do not lie in an interval $[N, N+N^{1/2}]$. Also, two distinct squares do not lie in such an interval. Accordingly, we conjecture that there are infinitely many integers N for which $[N, N+N^{1/2}]$ contains three distinct integers one of which is a square, one a cube and one a fifth power. Further, we conjecture that there exists a positive number C such that if N exceeds C then the interval $[N, N+N^{1/2}]$ does not contain four distinct powers and if it contains three distinct powers then one is a square, one is a cube and the third is a fifth power.

The reason that Turk and Loxton considered the interval $[N, N+N^{1/2}]$ and not a larger one is that for any $\varepsilon > 0$ the interval $[N, N+N^{1/2+\varepsilon}]$ contains at least $(1/2)N^{\varepsilon}(1+o(1))$ squares. If we exclude the squares then it is reasonable to consider an interval of length $N^{2/3}$ starting at N and, more generally, if we exclude the rth powers for r less than k then we should focus our attention on intervals of the form $[N, N+N^{1-1/k}]$. We may also study perfect powers of rational numbers in short intervals. If we consider intervals of the form $[N, N+N^{\theta}]$ with θ strictly less than $1-1/k$ then we may estimate the number of rational numbers which are perfect rth powers with $r \ge k$ in the interval provided that the heights of the rational numbers, which are at least N in size, are not too large. Note that if there is no restriction placed on the heights, one can find infinitely many kth powers of rationals in any interval of the form $[N, N+1]$. The natural restriction on the height to require is one which ensures that there are not two kth powers in the interval. In particular, it suffices to consider rational numbers of heights at most $2N^{1+\gamma}$ where $\gamma = (k-1-k\theta)/2$ (see Lemma 2). With this in mind we shall prove the following result.

THEOREM 2. *Let k be an integer with $k \ge 2$ and let θ be a real number with $0 \le \theta \le (k-1)/k$. There is a positive number c_1, which is effectively computable in terms of k, such that if N exceeds c_1 then the number of rational numbers which are perfect rth powers with $r \ge k$ of height at most $2N^{1+(k-1-k\theta)/2}$ in the interval $[N, N+N^{\theta}]$ is at most*

$$\exp(30(\log\log N \cdot \log\log\log N)^{1/2}).$$

On taking $\theta = (k-1)/k$ and noting that all of the integers in $[N, N+N^{1-1/k}]$ have height at most $2N$ we see that the number of perfect rth powers of integers with $r \ge k$ in $[N, N+N^{1-1/k}]$ is at most $\exp(30(\log\log N \cdot \log\log\log N)^{1/2})$ provided that N is sufficiently large.

The estimate of Loxton [5] for simultaneous linear forms in the logarithms of algebraic numbers is the following. Let n and t be integers with $n \ge 2$ and $t \ge 1$ and let $\alpha_1, \ldots, \alpha_n$ be non-zero multiplicatively independent algebraic numbers. Let $b_{i,j}$ for $i = 1, \ldots, t$ and $j = 1, \ldots, n$ be algebraic numbers and suppose that the matrix $(b_{i,j})$ formed by the $b_{i,j}$'s has rank t. Put

$$\Lambda_i = b_{i,1}\log\alpha_1 + \cdots + b_{i,n}\log\alpha_n \quad \text{for } i = 1, \ldots, t,$$

where the logarithms are principal. For any algebraic number α, let $H'(\alpha)$ denote the maximum of the absolute values of the relatively prime integer coefficients in the minimal defining polynomial for α. If α is of degree m then the two heights $H(\alpha)$ and $H'(\alpha)$ satisfy the inequalities

$$2^{1-m}H'(\alpha) \le H(\alpha)^m \le \sqrt{m+1}\,H'(\alpha)$$

(see Chapter 3, Theorem 2.8 of Lang [3]).

We shall suppose that $H'(\alpha_j) \le A_j$ with $A_j \ge 4$ for $j = 1, \ldots, n$ and that $H'(b_{i,j}) \le B$ with $B \ge 4$ for $i = 1, \ldots, t$ and $j = 1, \ldots, n$. Let d be the degree of the field generated by the α_j's and the $b_{i,j}$'s over the rationals. Put $\Omega = \log A_1 \cdots \log A_n$. Building on an estimate of Baker [1] for the case $t = 1$, Loxton [5] proved the following result.

LEMMA 1.

$$\max_{1\le i\le t} |\Lambda_i| > \exp(-C(\Omega \log \Omega)^{1/t} \log(B\Omega))$$

where $C = (16nd)^{200n}$.

Improvements of Lemma 1 should be possible given the developments associated with the case $t = 1$ since 1977.

For the proof of Theorem 2 we also require an estimate for the length of an interval which ensures that the interval does not contain two rational numbers of small height which are kth powers of rational numbers.

LEMMA 2. *Let k and N be positive integers with $k \ge 2$. Let θ be a real number with $0 \le \theta \le (k-1)/k$. There is at most one positive rational number α from the interval $[N, N+N^\theta]$ which is the kth power of a rational number and for which*

$$H(\alpha) \le 2N^{1+(k-1-k\theta)/2}. \tag{13}$$

Proof. Suppose that α_1 and α_2 are distinct rational numbers from the interval $[N, N+N^\theta]$ and that they have height at most $2N^{1+(k-1-k\theta)/2}$. Suppose also that they are perfect kth powers so that

$$H(\alpha_i) = (a_i/b_i)^k \quad \text{for } i = 1, 2,$$

where $a_1,\ a_2,\ b_1,\ b_2$ are positive integers with a_1 and b_1 coprime and with a_2 and b_2 coprime.

Observe that $x^k - y^k = (x-y)(x^{k-1} + kx^{k-2}y + \cdots + y^{k-1})$ and so

$$N^\theta \ge |\alpha_1 - \alpha_2| \ge \frac{|(a_1b_2)^k - (a_2b_1)^k|}{(b_1b_2)^k} > \frac{k|a_1b_2 - a_2b_1|(\min(a_1b_2, a_2b_1))^{k-1}}{(b_1b_2)^k}.$$

Since $(a_i/b_i)^k \ge N$ it follows that

$$a_i \ge b_i N^{1/k} \quad \text{for } i = 1, 2. \tag{14}$$

Therefore $\min(a_1b_2, a_2b_1) \ge b_1b_2N^{1/k}$ and so, since α_1 and α_2 are distinct whence $|a_1b_2 - a_2b_1| \ge 1$,

$$b_1b_2 > kN^{(k-1)/k-\theta}. \tag{15}$$

But, by (13),

$$H(\alpha_i) = H\left(\frac{a_i}{b_i}\right)^k = a_i^k \le 2N^{1+(k-1-k\theta)/2} \quad \text{for } i = 1, 2$$

and so, by (14),

$$b_i \le 2^{1/k} N^{(k-1-k\theta)/2k} \quad \text{for } i = 1,2.$$

In particular,

$$b_1 b_2 \le 2^{2/k} N^{(k-1)/k-\theta},$$

which contradicts (15). The result now follows. ∎

We shall also need the following simple proposition.

Lemma 3. *Let N be a positive integer and let θ be a real number with $0 \le \theta \le 1$. Suppose that α_1 and α_2 are distinct rational numbers in the interval $[N, N+N^\theta]$. Then*

$$H\left(\frac{\alpha_1}{\alpha_2}\right) \ge N^{1-\theta}.$$

Proof. Let $\alpha_i = a_i/b_i$ for $i = 1,2$, where a_1, a_2, b_1 and b_2 are positive integers with a_1 and b_1 coprime and a_2 and b_2 coprime. Then

$$H\left(\frac{\alpha_1}{\alpha_2}\right) = H\left(\frac{a_1 b_2}{a_2 b_1}\right) = \frac{\max\{a_1 b_2, a_2 b_1\}}{\gcd(a_1 b_2, a_2 b_1)}. \tag{16}$$

But

$$\gcd(a_1 b_2, a_2 b_1) \le |a_1 b_1 - a_2 b_1| = b_1 b_2 \left|\frac{a_1}{b_1} - \frac{a_2}{b_2}\right| \le b_1 b_2 N^\theta. \tag{17}$$

Since a_1/b_1 is in the interval $[N, N+N^\theta]$ we see that $a_1 \ge b_1 N$. Therefore, by (16) and (17),

$$H\left(\frac{\alpha_1}{\alpha_2}\right) \ge \frac{b_1 b_2 N}{b_1 b_2 N^\theta} = N^{1-\theta},$$

as required. ∎

5. Proof of Theorem 2. Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of k. Put

$$t = \left\lceil \frac{1}{15}\left(\frac{\log\log N}{\log\log\log N}\right)^{1/2} \right\rceil, \tag{18}$$

$$L = t(1 + ((k+1)^2(t-1))^{t-1}), \tag{19}$$

$$M = \exp(29(\log\log N \cdot \log\log\log N)^{1/2}). \tag{20}$$

We shall suppose that N is sufficiently large that $t \ge 2$.

Suppose that there are positive rational numbers $x_1, \ldots, x_L$ and integers $b_1, \ldots, b_L$ of size at least M such that $x_1^{b_1}, \ldots, x_L^{b_L}$ are distinct and lie in the interval $[N, N+N^\theta]$. Put $\alpha_i = x_i^{b_i}$ for $i = 1, \ldots, L$ and suppose that $H(\alpha_i) \le 2N^{1+(k-1-k\theta)/2}$ for $i = 1, \ldots, L$. Notice that at least t of the rationals $x_1, \ldots, x_L$ are multiplicatively independent. For otherwise we may apply Theorem 1 with $\varepsilon^{-1} = (t-1)(k+1)^2$ to conclude that there exist distinct integers $i_0, \ldots, i_t$ for which

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \le (H(\alpha_{i_2}) \cdots H(\alpha_{i_t}))^{\varepsilon} \le (2N^{1+(k-1-k\theta)/2})^{1/(k+1)^2},$$

hence for which

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \le (2N^{1/2})^{1/(k+1)}. \tag{21}$$

On the other hand, by Lemma 3,

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \ge N^{1-\theta} \ge N^{1/k}. \tag{22}$$

Since (21) and (22) are incompatible for $N \ge 4$ at least t of the powers are multiplicatively independent.

By reordering the powers we may assume, without loss of generality, that $x_1^{b_1}, \ldots, x_t^{b_t}$ are multiplicatively independent and that $b_i \le b_t$ for $i = 1, \ldots, t-1$.

Put

$$\Lambda_i = b_i \log x_i - b_t \log x_t$$

for $i = 1, \ldots, t-1$. Note that

$$|\Lambda_i| = \left|\log\left(\frac{x_i^{b_i}}{x_t^{b_t}}\right)\right| \le \log\left(\frac{N+N^{\theta}}{N}\right) \le N^{-1/k}$$

for $i = 1, \ldots, t-1$ and that the $(t-1) \times t$ matrix

$$\begin{pmatrix} b_1 & 0 & \cdots & 0 & -b_t \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & b_{t-1} & -b_t \end{pmatrix}$$

has rank $t-1$. Observe that, for $i = 1, \ldots, t$,

$$H'(x_i^{b_i}) = H(x_i^{b_i}) \le 2N^{1+(k-1-k\theta)/2} \le 2N^{(k+1)/2} < N^k$$

and so

$$H'(x_i) < N^{k/b_i} \le N^{k/M}. \tag{23}$$

For $N > c_1$, by (23),

$$\log\max(4, H'(x_i)) \le \frac{k \log N}{M}, \tag{24}$$

for $i = 1, \ldots, t$. Further, by (23), for $N > c_2$,

$$4 \le M \le b_t \le \frac{k \log N}{\log 2}. \tag{25}$$

Therefore, by Lemma 1,

$$N^{-1/k} > \exp(-(16t)^{200t}(\Omega\log\Omega)^{1/(t-1)}\log(b_t\Omega)),$$

where

$$\Omega = \prod_{i=1}^{t}\log\max(4, H'(x_i)).$$

Thus, by (24) and (25),

$$\frac{\log N}{k} < (16t)^{200t}\biggl(t\biggl(\frac{k\log N}{M}\biggr)^t\log\biggl(\frac{k\log N}{M}\biggr)\biggr)^{1/(t-1)} \times\log\biggl(2k\log N\biggl(\frac{k\log N}{M}\biggr)^t\biggr)$$

so, for $N > c_3$,

$$(\log N)^{t-1} < k^{2t-1}(16t)^{200t(t-1)}t\biggl(\frac{\log N}{M}\biggr)^t\log\log N\cdot((t+2)\log\log N)^{t-1}.$$

Thus, for $N > c_4$,

$$M^t < k^{2t-1}(32t)^{200t(t-1)}\log N\cdot(\log\log N)^t,$$

hence

$$M < k^2(32t)^{200(t-1)}(\log N)^{1/t}\log\log N.$$

But this is impossible by (18) and (20) for $N > c_5$. Therefore there are fewer than L powers of rationals of height at most $2N^{1+(k-1-k\theta)/2}$ in the interval $[N, N+N^\theta]$ with the power at least M in size.

It follows from Lemma 2 that there is at most one rth power of height at most $2N^{1+(k-1-k\theta)/2}$ in the interval for each r with $r \ge k$. Thus the total number of rth powers in the interval with $r \ge k$ is at most $L + M$. Our result now follows from (18), (19) and (20). ∎

6. Néron–Tate height. The simple counting argument used to establish Theorem 1 can be readily applied in other settings where there is a height function on an abelian group. For instance, let K be a finite extension of $\mathbb{Q}$ and let E be an elliptic curve defined over K. Denote by $E(K)$ the Mordell–Weil group of points with coordinates in K. The group $E(K)$ is finitely generated by the Mordell–Weil theorem. We denote the rank of the group by r. The *Néron–Tate* or *canonical height* on E/K is a map $\widehat{h}$ from $E(\overline{K})$ to $\mathbb{R}$ where $\overline{K}$ denotes an algebraic closure of K. For all points P in $E(\overline{K})$,

$$\widehat{h}(P) \ge 0 \tag{26}$$

and $\widehat{h}(P)$ is zero if and only if P is a torsion point in $E(\overline{K})$. Further, for all points P in $E(\overline{K})$ and integers m,

$$\widehat{h}(mP) = m^2\widehat{h}(P), \tag{27}$$

where mP denotes the sum of m copies of P in the group $E(\overline{K})$ when $m > 0$, $0P$ is the zero element and, when $m < 0$, mP denotes the sum of $-m$ copies of $-P$. Further for all P, Q in $E(\overline{K})$,

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q) \tag{28}$$

(see Theorem 9.3 of [8]).

It follows from (26) and (28) that for all P, Q in $E(\overline{K})$,

$$\widehat{h}(P+Q) \le 2\widehat{h}(P) + 2\widehat{h}(Q). \tag{29}$$

Further, it follows from repeated application of (29) that for each positive integer k and any points $P_1, \ldots, P_{2^k}$ in $E(\overline{K})$ we have

$$\begin{aligned} \widehat{h}(P_1 + \cdots + P_{2^k}) &\le 2\widehat{h}(P_1 + \cdots + P_{2^{k-1}}) + 2\widehat{h}(P_{2^{k-1}+1} + \cdots + P_{2^k}) \\ &\le 2^k(\widehat{h}(P_1) + \cdots + \widehat{h}(P_{2^k})). \end{aligned} \tag{30}$$

Therefore, by (30), for each positive integer t and any points $P_1, \ldots, P_t$ in $E(\overline{K})$,

$$\widehat{h}(P_1 + \cdots + P_t) \le 2t(\widehat{h}(P_1) + \cdots + \widehat{h}(P_t)). \tag{31}$$

We shall make use of (27) and (31) in our proof of the following result.

THEOREM 3. *Suppose that the rank r of $E(K)$ is positive. Let ε be a real number with $0 < \varepsilon < 1$. Let $P_1, \ldots, P_k$ be distinct points in $E(K)$. If*

$$k > (r+1)\left(1 + \left\lceil \frac{1}{\varepsilon} \right\rceil^r\right) \tag{32}$$

then there exist distinct points $P_{i_0}, \ldots, P_{i_{r+1}}$ such that

$$\widehat{h}(P_{i_0} - P_{i_1}) < 2r\varepsilon^2(\widehat{h}(P_{i_2}) + \cdots + \widehat{h}(P_{i_{r+1}})).$$

7. Proof of Theorem 3. There are $\binom{k}{r+1}$ $r+1$-tuples $(i_1, \ldots, i_{r+1})$ with $1 \le i_1 < i_2 < \cdots < i_{r+1} \le k$. Since the rank of $E(K)$ is r and since the torsion subgroup of $E(K)$ is finite, there are integers $l_{i_1}, \ldots, l_{i_{r+1}}$, not all zero, for which

$$l_{i_1}P_{i_1} + \cdots + l_{i_{r+1}}P_{i_{r+1}} = O, \tag{33}$$

where O denotes the origin, hence the zero element, of $E(K)$. We now proceed as in the proof of Theorem 1 with t replaced by $r+1$ and the relation (33) in place of (5). We then obtain

$$l_{1,j}P_1 + \cdots + l_{1,j}P_r = l_jP_{j+r} \tag{34}$$

in place of (6) for $j = 1, \ldots, m$ with $m = \lceil \frac{k-r}{r+1} \rceil$. Further, on choosing s and u as in the proof of Theorem 1, we have

$$(35) \qquad (l_s l_{1,u} - l_u l_{1,s})P_1 + \cdots + (l_s l_{r,u} - l_u l_{r,s})P_r = l_u l_s (P_{u+r} - P_{s+r})$$

in place of (9). Therefore, by (31) and (35),

$$\widehat{h}(l_u l_s (P_{u+r} - P_{s+r})) \le 2r(\widehat{h}((l_s l_{1,u} - l_u l_{1,s})P_1) + \cdots + \widehat{h}((l_s l_{r,u} - l_u l_{r,s})P_r))$$

and so, by (27),

$$(l_u l_s)^2 \widehat{h}(P_{u+r} - P_{s+r}) \le 2r((l_s l_{1,u} - l_u l_{1,s})^2 \widehat{h}(P_1) + \cdots + (l_s l_{r,u} - l_u l_{r,s})^2 \widehat{h}(P_r)).$$

Therefore, by (8),

$$\widehat{h}(P_{u+r} - P_{s+r}) \le 2r\varepsilon^2 (\widehat{h}(P_1) + \cdots + \widehat{h}(P_r))$$

provided (7) holds with r in place of $t - 1$. But this follows from (32) since $m \ge (k - r)/(r + 1)$. This completes the proof. ■

References

[1] A. Baker, *The theory of linear forms in logarithms*, in: Transcendence Theory: Advances and Applications, A. Baker and D. W. Masser (eds.), Academic Press, 1977, 1–27.

[2] D. J. Bernstein, *Detecting perfect powers in essentially linear time*, Math. Comp. 67 (1998), 1253–1283.

[3] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, Berlin, 1983.

[4] T. Loher and D. W. Masser, *Uniformly counting points of bounded height*, Acta Arith. 111 (2004), 277–297.

[5] J. H. Loxton, *Some problems involving powers of integers*, ibid. 46 (1986), 113–123.

[6] E. M. Matveev, *On linear and multiplicative relations*, Mat. Sb. 184 (1993), no. 4, 23–40 (in Russian); English transl.: Russian Acad. Sci. Sb. Math. 78 (1994), 411–425.

[7] A. J. van der Poorten and J. H. Loxton, *Multiplicative relations in number fields*, Bull. Austral. Math. Soc. 16 (1977), 83–98.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[9] C. L. Stewart, *On sets of integers whose shifted products are powers*, J. Combin. Theory Ser. A 115 (2008), 662–673.

[10] C. L. Stewart and K. R. Yu, *On the abc conjecture*, *II*, Duke Math. J. 108 (2001), 169–181.

[11] J. Turk, *Multiplicative properties of integers in short intervals*, Proc. Kon. Ned. Akad. Wet. (A) 83 (1980) = Indag. Math. 42 (1980), 429–436.

Department of Pure Mathematics
University of Waterloo
Waterloo, ON, Canada, N2L 3G1
E-mail: cstewart@uwaterloo.ca

Received on 18.7.2006
and in revised form on 14.11.2007 (5242)