GAPS IN THE SPECTRUM OF NATHANSON HEIGHTS OF PROJECTIVE POINTS

Kevin O'Bryant[1]
Department of Mathematics, City University of New York, College of Staten Island, New York, NY
kevin@member.ams.org

Received: 6/28/07, Revised: 8/20/07, Accepted: 8/22/07, Published: 8/28/07

Abstract

Let $\mathbb{Z}_m$ be the ring of integers modulo m (not necessarily prime), $\mathbb{Z}_m^*$ its multiplicative group, and let $x \bmod m$ be the least nonnegative residue of x modulo m. The *Nathanson height* of a point $r = \langle r_1, \dots, r_d \rangle \in (\mathbb{Z}_m^*)^d$ is $h_m(r) = \min \left\{ \sum_{i=1}^d (kr_i \bmod m) \colon k = 1, \dots, p-1 \right\}$. For $d = 2$, we give an explicit formula in terms of the convergents to the continued fraction expansion of $\bar{r}_1 r_2/m$. Further, we show that the multiset $\{m^{-1} h_m((r_1, r_2)) : m \in \mathbb{N}, r_i \in \mathbb{Z}_m^*\}$, which is trivially a subset of $[0, 2]$, has only the numbers $1/k$ ($k \in \mathbb{Z}^+$) and 0 as accumulation points.

1. Introduction

In [3], Nathanson and Sullivan raised the problem of bounding the height of points in $(\mathbb{Z}_p^*)^d$, where p is a prime. After proving some general bounds for $d > 2$, they move to identifying those primes p and residues r with $h_p(\langle 1, r \rangle) > (p-1)/2$. In particular, they prove that if $h_p(\langle 1, r \rangle) < p$, then it is in fact at most $(p+1)/2$. Nathanson has further proven [2] that if p is a sufficiently large prime and $h_p(\langle 1, r \rangle) < (p+1)/2$, then it is in fact at most $(p+4)/3$. In other words, $p^{-1} h_p(\langle 1, r \rangle)$ is either near 1, near 1/2, or at most 1/3.

In this paper we show that these gaps in the values of $p^{-1} h_p(\langle 1, r \rangle)$ continue all the way to 0, even if p is not restricted to be prime. The main tool is the simple continued fraction of r/p.

To avoid confusion, as we do not use primeness here, and since the numerators of continued fractions are traditionally denoted by p, we denote our modulus by m. We denote $a^{-1} \bmod m$ by $\bar{a}$. We use the traditional notation for the floor function ($\lfloor x \rfloor$ is the largest integer that isn't larger than x) and the fractional part ($\{x\} = x - \lfloor x \rfloor$).

[1]Supported by PSC-CUNY grant 60070-36 37

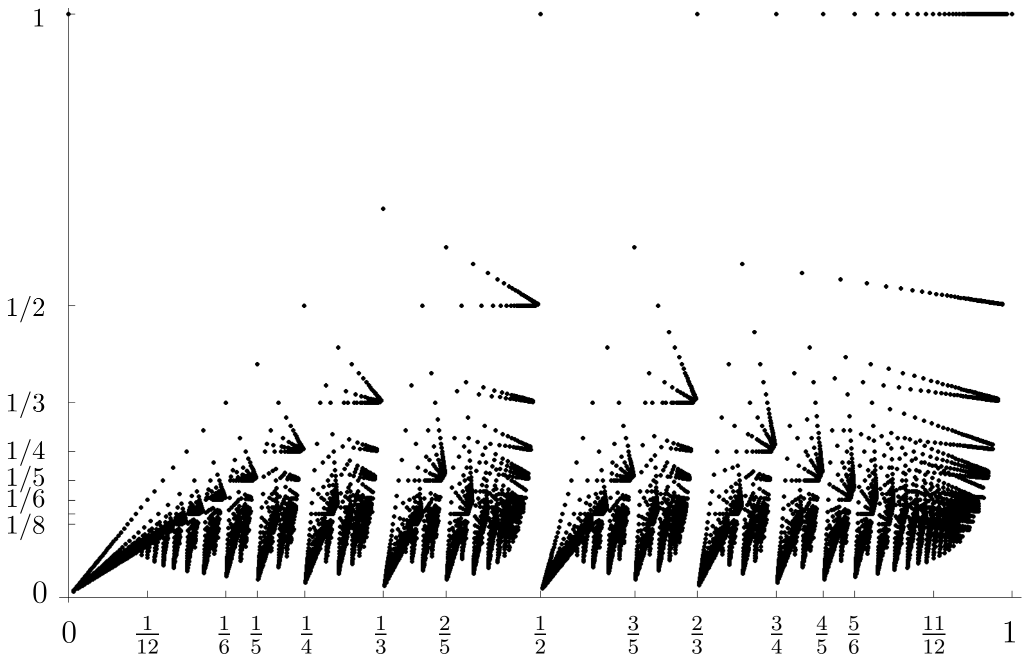

Figure 1: The points $(\frac{r}{m}, H(\frac{r}{m}))$, for all $0 < r < m \leq 200$.

If $\gcd(r_1, m) = 1$, then $h_m(\langle r_1, r_2 \rangle) = h_m(\langle 1, \bar{r}_1 r_2 \rangle)$, and so we may assume without loss of generality that $r_1 = 1$. We are thus justified in making the following definition for relatively prime positive integers r, m:

$$\begin{aligned} H(r/m) &:= m^{-1} \cdot h_m(\langle 1, r \rangle) \\ &= m^{-1} \cdot \min\{k + (kr \bmod m) \colon 1 \leq k < m\} \\ &= \min\left\{ \frac{k}{m} + \left\{ \frac{kr}{m} \right\} : 1 \leq k < m \right\}. \end{aligned}$$

Figure 1 shows the points $(\frac{r}{m}, H(\frac{r}{m}))$ for all $r, m \leq 200$.

The spectrum of a set $M \subseteq \mathbb{N}$, written $\textsc{Spec}(M)$, is the set of real numbers ß with the property that there are $m_i \in M$, $m_i \to \infty$, and a sequence r_i with $\gcd(r_i, m_i) = 1$, and $H(r_i/m_i) \to$ ß. Nathanson [2] and Nathanson and Sullivan [3] proved that

$$\textsc{Spec}(\textsc{primes}) \cap [\frac{1}{3}, \infty) = \left\{ \frac{1}{3}, \frac{1}{2}, 1 \right\}.$$

Our main theorem concerns the spectrum of Nathanson heights, and applies to both $\mathbb{N}$ and to the set of primes.

Theorem 1.1. *Let $M \subseteq \mathbb{Z}^+$. If $\{m \in M \colon \gcd(m, n) = 1\}$ is infinite for every positive integer n, then*

$$\textsc{Spec}(M) = \{0\} \cup \left\{ \frac{1}{k} \colon k \in \mathbb{Z}^+ \right\}.$$

2. Continued Fractions

For a rational number $0 < r/m < 1$, let $[0; a_1, a_2, \ldots, a_n]$ be (either one of) its simple continued fraction expansion, and let p_k/q_k be the k-th convergent. In particular

$$\frac{p_0}{q_0} = \frac{0}{1}$$
$$\frac{p_2}{q_2} = \frac{a_2}{1 + a_1 a_2}$$
$$\frac{p_4}{q_4} = \frac{a_2 + a_4 + a_2 a_3 a_4}{1 + a_1 a_2 + a_1 a_4 + a_3 a_4 + a_1 a_2 a_3 a_4}$$

The q_i satisfy the recurrence $q_{-2} = 1, q_{-1} = 0, q_n = a_n q_{n-1} + q_{n-2}$ (with $a_0 = 0$), and are called the *continuants*. The *intermediants* are the numbers $\alpha q_{n-1} + q_{n-2}$, where α is an integer with $1 \le \alpha \le a_n$.

Let $E[a_0, a_1, \ldots, a_n]$ be the denominator $[a_0; a_1, \ldots, a_n]$, considered as a polynomial in $a_0, \ldots, a_n$, and set $E[\,] = 1$. Then $p_k = E[a_0, \ldots, a_k]$ and $q_k = E[a_1, \ldots, a_k]$. We will make use of the following combinatorial identities, which are in [4, Chapter 13], with $0 < s < t < n$:

$$q_\ell = q_k E[a_{k+1}, \ldots, a_\ell] + q_{k-1} E[a_{k+2}, \ldots, a_\ell],$$

$$p_n E[a_s, \ldots, a_t] - p_t E[a_s, \ldots, a_n] = (-1)^{t-s+1} E[a_0, \ldots a_{s-2}] E[a_{t+2}, \ldots, a_n].$$

The following lemmas are well known. The first is a special case of the "best approximations theorem" [1, Theorems 154 and 182], and the second is an application of [1, Theorem 150], the identity $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$. The third and fourth lemmas follow from the identities for E given above.

Lemma 2.1. *Fix a real number $x = [0; a_1, a_2, \ldots]$, and suppose that the positive integer ℓ has the property that $\{\ell x\} \le \{kx\}$ for all positive integers $k \le \ell$. Then there are nonnegative integers $n, \alpha \le a_n$ such that $\ell = \alpha q_{2n-1} + q_{2n-2}$.*

Lemma 2.2. *Let $\frac{p_{2k}}{q_{2k}} = [0; a_1, a_2 \ldots, a_{2k}]$, and let $x = [0; a_1, a_2 \ldots, a_{2k-1}, a_{2k} + 1]$. Then*

$$q_{2k} \cdot x - p_{2k} = \frac{1}{2q_{2k} + q_{2k-1}}.$$

We will use Fibonacci numbers, although the only property we will make use of is that they tend to infinity: $F_1 = 1$, $F_2 = 2$, and $F_n = F_{n-1} + F_{n-2}$.

Lemma 2.3. *For all $k \ge 1$, we have $q_k \ge F_k$. Further, for $\ell > k$, we have*

$$q_\ell > q_k F_{\ell-k}, \qquad \text{and} \qquad q_\ell > a_\ell q_k.$$

Lemma 2.4. *For $0 < 2k+2 \leq n$, we have*

$$q_{2k}p_n - p_{2k}q_n = E[a_{2k+2}, \ldots, a_n].$$

Moreover, if $2k+2 = n+1$, then $q_{2k}p_n - p_{2k}q_n = 1$.

We now state and prove our formula for heights.

Theorem 2.5. *Let $\frac{r}{m} = [0; a_1, a_2, \ldots, a_n]$ (with $\gcd(r, m) = 1$). Then*

$$H(\frac{r}{m}) = \min_{0 \leq k < n/2} \{q_{2k}\frac{r+1}{m} - p_{2k}\}.$$

Proof. First, recall that

$$H(r/m) = \min\{k/m + \{kr/m\} : 1 \leq k < m\}.$$

Set

$$I := \{\alpha q_{2i-1} + q_{2i-2} \colon 0 \leq \alpha \leq a_{2i}, 0 \leq i \leq n/2\}.$$

We call ℓ a best multiplier if

$$\ell/m + \{\ell r/m\} < k/m + \{kr/m\}$$

for all positive integers $k < \ell$. We begin by proving by induction that the set of best multipliers is contained in the set I. Certainly 1 is a best multiplier and also $1 = 0 \cdot q_{-1} + q_{-2} \in I$. Our induction hypothesis is that the best multipliers that are less than ℓ are all contained in I.

Suppose that ℓ is a best multiplier: we know that

$$\frac{k}{m} + \left\{k\frac{r}{m}\right\} > \frac{\ell}{m} + \left\{\ell\frac{r}{m}\right\}$$

for all $1 \leq k < \ell$. Since $k < \ell$, we then know that $\{kr/m\} > (\ell - k)/m + \{\ell r/m\} > \{\ell r/m\}$. Lemma 2.1 now tells us that $\ell \in I$. This confirms the induction hypothesis, and establishes that

$$H(r/m) = \min\{k/m + \{kr/m\} : k \in I\}. \tag{1}$$

Now, note that the function f_i defined by

$$f_i(x) := \frac{xq_{2i-1} + q_{2i-2}}{m} + \left\{(xq_{2i-1} + q_{2i-2})\frac{r}{m}\right\}$$

is monotone on the domain $0 \leq x \leq a_{2i}$. As $0q_{2i-1} + q_{2i-2} = q_{2i-2}$ and $a_{2i}q_{2i-1} + q_{2i-2} = q_{2i}$, this means that the minimum in Eq. (1) can only occur at q_{2i}, with $0 \leq 2i \leq n$.

As a final observation, we note that $q_0/m + \{q_0 r/m\} = (r+1)/m$ is at most as large as $q_n/m + \{q_n r/m\} = 1$ (as $q_n = m$). Thus, the minimum in Eq. (1) cannot occur exclusively at $k = q_n = m$. □

Corollary 2.6. *Let* $0 < r < m$, *with* $\gcd(r, m) = 1$, *and let* $\frac{r}{m} = [0; a_1, \ldots, a_n]$, *with* $a_n \geq 2$. *For all* $k \in (0, n/2)$,

$$H(\frac{r}{m}) \leq \frac{q_{2k}}{m} + \frac{1}{2q_{2k}}.$$

Proof. First, note that $\frac{r}{m} < [0; a_1, a_2, \ldots, a_{2k-1}, a_{2k} + 1]$. Now, as a matter of algebra (using Lemma 2.2),

$$q_{2k}\frac{r+1}{m} - p_{2k} \leq q_{2k}\left([0; a_1, a_2, \ldots, a_{2k} + 1] + \frac{1}{m}\right) - p_{2k} = \frac{q_{2k}}{m} + \frac{1}{2q_{2k} + q_{2k-1}}$$
$$\leq \frac{q_{2k}}{m} + \frac{1}{2q_{2k}}.$$

□

3. Proof of Theorem 1.1

First, we note that $H(a_2/(1 + a_1 a_2)) = (1 + a_2)/(1 + a_1 a_2) \to 1/a_1$, where a_1 is fixed and $a_2 \to \infty$. Thus, $1/k \in \text{Spec}(\mathbb{N})$ for every k. Also, $H(1/a_1) = 2/a_1 \to 0$ as $a_1 \to \infty$, so $0 \in \text{Spec}(\mathbb{N})$. The remainder of this section is devoted to proving that if ß > 0 is in $\text{Spec}(\mathbb{N})$, then ß is rational with numerator 1.

Fix a large integer s. Let r/m be a sequence (we will suppress the index) with $\gcd(r, m) = 1$ and with $H(r/m) \to$ ß $> \frac{1}{F_{2s}}$, where F_{2s} is the $2s$-th Fibonacci number.

Define $a_1, a_2, \ldots$ by

$$\frac{r}{m} = [0; a_1, a_2, \ldots, a_n],$$

and we again remind the reader that r/m is a sequence, so that each of $a_1, a_2, \ldots,$ is a sequence, and n is also a sequence. To ease the psychological burden of considering sequences that might not even be defined for every index, we take this occasion to pass to a subsequence of r/m that has n nondecreasing. Further, we also pass to a subsequence on which each of the sequences a_i is either constant or monotone increasing.

First, we show that n is bounded. Note that q_{2s}/m (fixed s) is the same as q_{2s}/q_n, and by Lemma 2.3 this is at most $1/(2F_{2s})$, provided that n is large enough so that $F_{n-2s} > 2F_{2s}$. Take such an n. We have from Corollary 2.6 that

$$H(\frac{r}{m}) \leq \frac{q_{2s}}{m} + \frac{1}{2q_{2s}} < \frac{1}{2F_{2s}} + \frac{1}{2F_{2s}} < \frac{1}{F_{2s}} < \text{ß}.$$

This contradicts the hypothesis that $H(r/m) \to$ ß > 0, and proves that n must be small enough so that $F_{n-2s} > 2F_{2s}$.

Since $m \to \infty$ but n is bounded, some a_i must be unbounded. Let i be the least natural number such that a_i is unbounded.

First, we show that i is not odd. If $i = 2k+1$, then

$$H(\frac{r}{m}) \leq q_{2k}\frac{r+1}{m} - p_{2k}$$

and p_{2k} and q_{2k} are constant. Since $a_{2k+1} \to \infty$, the ratio

$$\frac{r}{m} \to [0; a_1, a_2, \ldots, a_{2k}] = \frac{p_{2k}}{q_{2k}}.$$

Thus, since $q_{2k}/m \leq 1/a_{2k+1} \to 0$,

$$H(\frac{r}{m}) \leq q_{2k}\frac{r+1}{m} - p_{2k} = q_{2k}\frac{r}{m} + \frac{q_{2k}}{m} - p_{2k} \to q_{2k}\frac{p_{2k}}{q_{2k}} + 0 - p_{2k} = 0,$$

contradicting the hypothesis that ß > 0.

Now we show that there are not two a_i's that are unbounded. Suppose that a_{2k} and a_j are both unbounded, with $j > 2k$. Then

$$H(\frac{r}{m}) \leq \frac{q_{2k}}{m} + \frac{1}{2q_{2k}}.$$

Since a_{2k} is unbounded, $\frac{1}{2q_{2k}} \to 0$. And since a_j is also unbounded,

$$\frac{q_{2k}}{m} \leq \frac{q_{2k}}{q_j} < \frac{q_{2k}}{q_{j-1}} \cdot \frac{q_{j-1}}{q_j} < \frac{1}{F_{j-1-2k}} \cdot \frac{1}{a_j} \to 0.$$

Thus

$$\frac{q_{2k}}{m} + \frac{1}{2q_{2k}} \to 0.$$

We have shown that there is exactly one a_i that is unbounded, and that i is even.

We have $\frac{r}{m} = [0; a_1, \ldots, a_{2k}, \ldots, a_n]$, with all of the a_i fixed except a_{2k}, and $a_{2k} \to \infty$. Now

$$\begin{aligned}
\lim H(r/m) &= \lim_{a_{2k}\to\infty} \min_{0\leq j<n/2} q_{2j}\frac{r+1}{m} - p_{2j} \\
&= \lim_{a_{2k}\to\infty} \min_{0\leq j<n/2} \left(\frac{q_{2j}p_n - p_{2j}q_n + q_{2j}}{q_n}\right) \\
&= \min_{0\leq j<n/2} \lim_{a_{2k}\to\infty} \left(\frac{E[a_{2j+2}, \ldots, a_n] + E[a_1, \ldots, a_{2j}]}{E[a_1, \ldots, a_n]}\right)
\end{aligned}$$

Using the general identity (for $s \leq \ell \leq t$)

$$\begin{aligned}
E[a_s, \ldots, a_t] = a_\ell E[a_s, \ldots, a_{\ell-1}]E[a_{\ell+1}, \ldots, a_t] + \\
E[a_s, \ldots, a_{\ell-2}]E[a_\ell + 1, \ldots, a_t] + E[a_s, \ldots, a_{\ell-1}]E[a_{\ell+2}, \ldots, a_t]
\end{aligned}$$

with $\ell = 2k$, we can evaluate the limit as $a_{2k} \to \infty$. We arrive at

$$\begin{aligned}
ß = \lim H(\frac{r}{m}) &= \min\left\{ \min_{0\le j<k} \frac{E[a_{2j+2},\ldots,a_{2k-1}]E[a_{2k+1},\ldots,a_n]}{E[a_1,\ldots,a_{2k-1}]E[a_{2k+1},\ldots,a_n]}, \right. \\
&\qquad \left. \min_{k\le j<n/2} \frac{E[a_1,\ldots,a_{2k-1}]E[a_{2k+1},\ldots,a_{2j}}{E[a_1,\ldots,a_{2k-1}]E[a_{2k+1},\ldots,a_n]} \right\} \\
&= \min\left\{ \min_{0\le j<k} \frac{E[a_{2j+2},\ldots,a_{2k-1}]}{E[a_1,\ldots,a_{2k-1}]}, \min_{k\le j<n/2} \frac{E[a_{2k+1},\ldots,a_{2j}}{E[a_{2k+1},\ldots,a_n]} \right\} \\
&= \min\left\{ \frac{1}{E[a_1,\ldots,a_{2k-1}]}, \frac{1}{E[a_{2k+1},\ldots,a_n]} \right\}.
\end{aligned}$$

In either case, the numerator of ß is 1, and the proof of Theorem 1.1 is concluded.

We note that we have actually proved (with a small bit of additional algebra) a quantitative version of the Theorem.

Theorem 3.1. *Let (r_i, m_i) be a sequence of pairs of positive integers with $\gcd(r_i, m_i) = 1$, $m_i \to \infty$ and $\limsup H(r_i/m_i) > 0$. Then there is a pair of relatively prime positive integers a, b, with $a \le b$, a positive integer c, and an increasing sequence $i_1, i_2, \ldots$ with*

$$r_{i_j} = \frac{am_{i_j} - c}{b} \qquad \text{and} \qquad H(\frac{r_{i_j}}{m_{i_j}}) \to \frac{1}{\max\{c, b\}}.$$

Conversely, if $m_i \to \infty$, and $a \le b$ are two relatively prime positive integers, c is a positive integer, and $r_i = \frac{am_i - c}{b}$ is an integer relatively prime to m_i, then $\lim H(r_i/m_i) \to \frac{1}{\max\{c,b\}}$.

In particular, if for every n there are arbitrarily large $m \in M$ with $\gcd(m, n) = 1$, then $\textsc{Spec}(M) = \textsc{Spec}(\mathbb{N})$.

References

[1] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press Oxford University Press, New York, 1979.

[2] Melvyn B. Nathanson, *Heights on the finite projective line* (2007), available at `http://arxiv.org/math.NT/0703646`.

[3] Melvyn Nathanson and Blair Sullivan, *Heights in finite projective space, and a problem on directed graphs* (2007), available at `http://arxiv.org/math.NT/0703418`.

[4] Joe Roberts, *Elementary number theory—a problem oriented approach*, MIT Press, Cambridge, Mass., 1977.