Limiting behaviour of large Frobenius numbers

by

J. Bourgain[1] and Ya. G. Sinai[2]

Dedicated to

V.I. Arnold

on the occasion of his 70th birthday

[1]School of Mathematics, Institute for Advanced Study, Princeton, New Jersey, U.S.A.
[2]Mathematics Department, Princeton University, Princeton, New Jersey, U.S.A.

§1. Introduction

Consider n-tuples $a = (a_1, a_2, \ldots, a_n)$ of positive integers which are co-prime, i.e., the largest common divisor (lcd) of all a_j is 1. Frobenius number $F(a)$ of a is the smallest F such that any integer $t \geqslant F$ can be written in the form

$$t = \sum_{j=1}^{n} x_j a_j$$

with non-negative integers x_j. V.I. Arnold in [1] introduced the ensembles of a for which $a_1 + a_2 + \cdots + a_n = \sigma$ tend to infinity and studied the behaviour of $F(a)$ under the limit transition $\sigma \to \infty$. In particular, he formulated the hypothesis according to which $F(a)$ grows for typical a as $\sigma^{1+\frac{1}{n-1}}$. Other hypotheses and results of Arnold can be found in [2].

In this paper we consider different ensembles of large a and study the same question of the growth of $F(a)$ in these ensembles. Namely, take N and denote by Ω_N the set of all a for which $1 \leq a_j \leq N$, $j = 1, 2, \ldots, n$, and lcd $(a) = 1$. Using elementary probability methods one can show that the limit $\lim_{N\to\infty} \frac{1}{N^n} |\Omega_N|$ exists and is positive (see, for example, [3]). It gives "the probability" of $a \in \Omega_N$ in the ensemble of all possible n-tuples a with entries less than N. Below P_N denotes the uniform probability distribution on Ω_N. We study in this paper the behaviour of $F(a)$ for typical a (in the sense of P_N) as $N \to \infty$. The case $n = 2$ follows easily from the famous result of Sylvester according to which $F(a) = (a_1 - 1)(a_2 - 1)$ (see [5]). This implies that $\frac{1}{N^2} F(a)$ has the limiting distribution as $N \to \infty$.

Below in Sections 2 and 3 we consider the next case $n = 3$. Based on some facts from the theory of continued fractions we prove

Theorem 1. *As $N \to \infty$ there exists the limiting distribution of $\frac{1}{N^{3/2}} F(a)$.*

The proofs of the needed facts will be a subject of another paper by C. Ulcigrai and one of us (Ya. Sinai). It is hopeless to write down explicitly the limiting distribution in Theorem 1. Probably the methods of this paper can be used for estimating its decay at infinity.

Below we introduce another function $F_1(a)$ about which we prove in Lemma 1 that in typical situations it behaves as $F(a)$. But $F_1(a)$ is much easier for the analysis of the problem because it is formulated as a "max-min" problem.

In Section 2 we discuss the case $n = 3$ when $\text{lcd}(a_i, a_j) = 1$ for at lease one pair a_i, a_j. In Section 3 we discuss the general case of $n = 3$.

In Section 4 we consider $n > 3$. Theorem 2 of this section shows that for slightly modified ensembles the distributions of $\frac{F(a)}{N^{1+\frac{1}{n-1}}}$ are (uniformly in N) bounded in the sense that

$$P_{N,\alpha}\left\{\frac{F(a)}{N^{1+\frac{1}{n-1}}} \geqslant D\right\} \leq \epsilon(D)$$

where $\Omega_{N,\alpha}$ is the ensemble of a for which $a_j \geq \alpha N$, $1, \leq j \leq n$ and $P_{N,\alpha}$ is the uniform distribution in this ensemble, $0 < \alpha < 1$ is the fixed number, $\epsilon(D)$ does not depend on N and $\epsilon(D) \to 0$ ad $D \to \infty$. In Appendix 1 we prove a general Lemma which was used in an earlier version of this paper and can have different applications. Namely, we show that

$$\ell\left\{\alpha : \sum_{m=1}^{M} \frac{1}{|e^{2\pi i m\alpha} - 1|} \geq DM\ln M\right\} \leq \epsilon_1(D)$$

where ℓ is the Lebesgue measure on $[0,1]$ and $\epsilon_1(\mathcal{D})$ does not depend on M, $\epsilon_1(D) \to 0$ as $D \to \infty$.

The analysis of the behaviour of $\frac{1}{M}\sum\limits_{m=1}^{M} \frac{1}{e^{2\pi i m\alpha}-1}$ as function of M for typical α is of some importance but we do not go further in this direction.

Now we give the defintion of the function $F_1(a)$ and prove Lemma 1 which shows in what sense $F(a)$ and $F_1(a)$ are equivalent. For any $a \in \Omega_N$ introduce the arithmetic progression $\Pi_r = \{r + ma_n, m \geqslant 0\}$, $0 \leq r < a_n$. Consider the equality

$$x_1a_1 + x_2a_2 + \cdots + x_{n-1}a_{n-1} = r + m(x_1, \ldots, x_{n-1})a_n$$

which shows that

$$x_1a_1 + x_2a_2 + \cdots + x_{n-1}a_{n-1} \equiv r \pmod{a_n}. \tag{1}$$

Here $x_j \geqslant 0$ are integers. Put $\bar{m}_r = \min_{0 \leq x_1, x_2, \ldots, x_{n-1} < a_n} m(x_1, x_2, \ldots, x_{n-1})$ and denote $F_1(a) = \max_r(r + \bar{m}_r a_n)$.

Lemma 1. *$F_1(a) - a_n \leq F(a) \leq F_1(a)$ provided that $F_1(a) - a_n > 0$.*

Proof. Take $t \geqslant F_1(a)$. Then $t \in \Pi_r$ for some $r, 0 \leq r < a_n$, i.e., $t = r + ma_n$. Therefore

$$t = r + \bar{m}_r a_n + (m - \bar{m}_r)a_n = x_1a_1 + \cdots + x_{n-1}a_{n-1} + (m - \bar{m}_r)a_n$$

for some $0 \le x_j < a_n, j = 1, \dots, n-1$. Since $t \geqslant F_1(a)$ we have $x_1a_1 + \dots + x_{n-1}a_{n-1} \le F_1(a)$ and $m \geqslant \bar{m}_r$. This gives the needed representation of t and the inequality $F(a) \le F_1(a)$.

To prove the inequality from the other side, take r_1 such that $F_1(a) = r_1 + \bar{m}_{r_1}a_n = \max_r(r + \bar{m}_r a_n)$. We shall show that $t_1 = r_1 + (\bar{m}_{r_1} - 1)a_n$ cannot be represented in the form $t_1 = y_1a_1 + \dots + y_na_n$ with non-negative $y_j, 1 \leqslant j \leqslant n$. Indeed, if such representation is possible we would have

$$y_1a_1 + \dots + y_{n-1}a_{n-1} = r_1 + ma_n$$

for some $m \geqslant \bar{m}_{r_1}$ and by definition of t_1

$$t_1 = y_1a_1 + \dots + y_{n-1}a_{n-1} + y_na_n = r_1 + ma_n + y_na_n = r_1 + (\bar{m}_{r_1} - 1)a_n\,.$$

Therefore $m + y_n = \bar{m}_{r_1} - 1$. Since $m \geqslant \bar{m}_r$ this is possible only if $y_n < 0$. Lemma is proved. $\square$

Certainly, instead of a_n we could take any other a_j. In a typical situation we expect that x grow as $N^{\frac{1}{n-1}}$. Therefore typically $F(a) \sim F_1(a)$.

The financial support from NSF, Grant No. 0600996 given to the second author is highly appreciated.

§2. The case $n = 3$ and $\mathrm{lcd}(a_i, a_j) = 1$ for some a_i, a_j

Without any loss of generality we may assume that $i = 1$, $j = 3$. In this case the "max-min" problem for $F_1(a)$ can be solved more or less explicitly. Write for positive integers x_1, x_2

$$x_1a_1 + x_2a_2 \;=\; r + m(x_1, x_2)a_3 \tag{2}$$

or

$$x_1a_1 + x_2a_2 \;\equiv r \pmod{a_3} \tag{3}$$

where $0 \le r < a_3$. Since a_1, a_3 are co-prime there exists a_1^{-1}, $1 \le a_1^{-1} < a_3$ for which $a_1 \cdot a_1^{-1} \equiv 1 \pmod{a_3}$. It follows easily from the estimates of Kloosterman sums that for any fixed $0 < \alpha_1 < \alpha_2 < 1$ and $N\alpha_1 \le a_1 \le N\alpha_2$ the inverse a_1^{-1} is asymptotically uniformly distributed on $[1, \dots, a_3]$. Presumably this is also true in our ensemble. Rewrite (3) as follows:

$$x_1 + a_{1\,2}x_2 \;\equiv\; r_1 \pmod{a_3} \tag{4}$$

where $r_1 \equiv r a_1^{-1} \pmod{a_3}$, $a_{12} = a_1^{-1} \cdot a_2 \pmod{a_3}$ and

$$a_{1\,2}x_2 \;\equiv\; (r_1 - x_1) \pmod{a_3} \tag{5}$$

The equation (5) has a natural geometric interpretation. Consider $S = [0, 1, \dots, a_3 - 1]$ as a "discrete circle." The shift R by $a_{1\,2} \pmod{a_3}$ is the rotation of the circle S and $\{a_{1\,2}x_2\}$ is the orbit under the action of R of the point zero. Then (5) means that $r_1 - x_1$ belongs to this orbit.

From Lemma 1

$$\begin{aligned}
F_1(a) \;&=\; \max_r \min_{x_1a_1+x_2a_2 \equiv r \pmod{a_3}\; 0 \,\le\, x_1, x_2 < a_3} (x_1a_1 + x_2a_2) \;= \\
&= N^{3/2} \max_r \min_{x_1a_1+x_2a_2 \equiv r \pmod{a_3}} \left(\frac{x_1}{\sqrt{N}}\, \frac{a_1}{N} \;+\; \frac{x_2}{\sqrt{N}}\, \frac{a_2}{N} \right) \\
&= N^{3/2} \max_{r_1} \min_{x_1+x_2a_{1\,2} \equiv r_1 \pmod{a_3}} \left(\frac{x_1}{\sqrt{N}}\, \frac{a_1}{N} \;+\; \frac{x_2}{\sqrt{N}}\, \frac{a_2}{N} \right).
\end{aligned} \tag{6}$$

First we localize our ensemble. Choose $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, $0 < \alpha_j < 1$ for $j = 1, 2, 3$ and $\epsilon > 0$ and define $\Omega_{N,\alpha,\epsilon} \subset \Omega_N$ as a subset of those $a = (a_1, a_2, a_3)$ for which $\left|\frac{a_j}{N} - \alpha_j\right| \le \epsilon$. Then $P_{N,\alpha,\epsilon}$ is the notation for the uniform probability distribution on $\Omega_{N,\alpha,\epsilon}$. Theorem 1 will follow if we prove Theorem 1 *wrt* to the distribution $P_{N,\alpha,\epsilon}$ (see also the end of this section). In the ensemble $\Omega_{N,\alpha,\epsilon}$ the ratios $\frac{a_1}{N}$, $\frac{a_2}{N}$ are ϵ-close to α_1, α_2.

We shall use some facts from the theory of continued fractions and from the theory of rotations of the circle (see [5]). Take $\rho = \frac{a_{1\,2}}{a_3}$ and expand it into continued fraction:

$$\rho = \cfrac{1}{h_1 + \cfrac{1}{h_2 + \cfrac{1}{h_3 + \ddots + \cfrac{1}{h_{s_0}}}}} \tag{7}$$

where $h_j \geq 1$ are integers. Let

$$\rho_s = \cfrac{1}{h_1 + \cfrac{1}{h_2 + \ddots + \cfrac{1}{h_s}}} = \frac{p_s}{q_s}$$

be the s-approximant of ρ. One can find "odd" intervals $\triangle_1^{(2p-1)} = \{0, 1, \ldots, m_{2p-1}\}$ and "even" intervals $\triangle^{2p}$ $\{a_3 - m_{2p}, \ldots, a_3 - 1\}$, $p \geq 1$, such that if $\triangle_j^{(2p-1)} = R^j \triangle^{(2p-1)}$, $\triangle_{j_1}^{(2p)} = R^{j_1} \triangle^{(2p)}$ then the intervals $\triangle_j^{(2p-1)}$, $0 \leq j < q_{2p}$ and $\triangle_{j_1}^{(2p)}$, $0 \leq j_1 < q_{2p-1}$ are pair-wise disjoint and their union gives the whole circle S. This means that $\triangle_j^{(2p-1)}$, $\triangle_j^{(2p)}$, constitute some partition of S which we denote by $\eta^{(p)}$. The partitions $\eta^{(p)}$ increase, $\eta^{(p+1)} \geq \eta^{(p)}$. Their exact structure depends on the elements of the continued fraction (7).

We shall show that in (6) it is enough to consider $x_1 \leq \mathcal{D}_1 \sqrt{N}$, $x_2 \leq \mathcal{D}_1 \sqrt{N}$ where $\mathcal{D}_1$ is sufficiently large depending on ρ (see below). Take s_1 such that $q_{s_1 - 1} \leq \sqrt{N} < q_{s_1}$. If $x_2 > \mathcal{D}_1 \sqrt{N}$ choose k so that $q_{s_1 + k_1} \leq x_2 < q_{s_1 + k_1 + 1}$. Clearly, k_1 increases of $\mathcal{D}_1$ increases. Put $x_1' = x_1 + (a_{12}\, q_{s_1+k_1} - p_{s_1+k_1} a_3) = x_1 + a_3(\rho\, q_{s_1+k_1} - p_{s_1+k_1})$, $x_2' = x_2 - q_{s_1+k_1}$. It is easy to see that

$$x_1' + a_{1\,2}\, x_2' \equiv x_1 + a_{12}\, x_2 \pmod{a_3}$$

and

$$\frac{x_1'}{\sqrt{N}} \frac{a_1}{N} + \frac{x_2'}{\sqrt{N}} \cdot \frac{a_2}{N} = \frac{x_1}{\sqrt{N}} \frac{a_1}{N} + \frac{x_2}{\sqrt{N}} \cdot \frac{a_2}{N} +$$

$$+ \frac{a_3(\rho\, q_{s_1+k_1} - p_{s_1+k_1})}{\sqrt{N}} \frac{a_1}{N} - \frac{q_{s_1+k_1}}{\sqrt{N}} \cdot \frac{a_2}{N}\,. \tag{8}$$

The expression $\frac{a_3(\rho\, q_{s_1+k_1} - p_{s_1+k_1})}{\sqrt{N}} \cdot \frac{a_1}{N} = \frac{a_3}{N} \cdot \sqrt{N}(\rho\, q_{s_1+k_1} - p_{s_1+k_1}) \cdot \frac{a_1}{N}$ decreases as k_1 increases because $(\rho\, q_{s_1+k_1} - p_{s_1+k_1})$ behaves as $\frac{1}{q_{s_1+k_1}}$. On the other hand, $\frac{q_{s_1+k_1}}{\sqrt{N}}$ takes values $O(1)$ and increases as k_1 increases. Therefore, the sum of the last two terms in (8) becomes negative if k_1 is large enough. Since in (6) we are interested in the minimal values of x_2', $x_2' = x_2 - q_{s_1+k_1}$ give smaller values for the expression (6). Thus it is enough to consider $x_2 \le \mathcal{D}_1\sqrt{N}$ for sufficiently large $\mathcal{D}_1$ depending on ρ.

Let us show that $x_2 > \mathcal{D}_2^{-1}\sqrt{N}$ for another sufficiently large $\mathcal{D}_2$. Indeed, take k_2 so that $q_{s_1-k_2} < \mathcal{D}_2^{-1}\sqrt{N} \le q_{s_1-k_2+1}$ and consider the partition $\eta^{(s_1-k_2)}$. Take any element $\triangle = [y_1, y_2]$ of this partition and for $r_1 = y_2 - 1$ the value of x_1 are $(y_2-y_1)-1$, $(y_2-y_1-1)+\ell_1$, $(y_2-y_1-1)+\ell_1+\ell_2, \dots$ where $\ell_1, \ell_2, \dots$ are the lengths of the elements of $\eta^{(s_1-k_2)}$ which follow $\triangle$. If $x_2 \le \mathcal{D}_2^{-1}\sqrt{N} \le q_{s_1-k_2+1}$ then it is clear that min of $\frac{x_1}{\sqrt{N}}\frac{a_1}{N} + \frac{x_2}{\sqrt{N}}\frac{a_2}{N}$ is attained at $x_1 = y_2 - y_1 - 1$. On the other hand, for r_1 consider an element $\triangle'$ of the partition $\eta^{(s_1)}$ containing r_1. Take $x_1' = |\triangle'| - 1$. It is clear that $x_2' \le q_{s_1+1}$ and $\frac{x_1'}{\sqrt{N}} \cdot \frac{a_1}{N} + \frac{x_2'}{\sqrt{N}}\frac{a_2}{N}$ is much smaller than in the previous case. Thus $\mathcal{D}_2^{-1}\sqrt{N} \le x_2 \le \mathcal{D}_1\sqrt{N}$.

In the above mentioned paper by C. Ulcigrai and the second author ([6], in preparation) the following problem was considered. Take large R and some fixed number k. For any irrational ρ consider q_s such that $q_{s-1} \le R < q_s$ and $h_{s-k}, \dots, h_s, \dots, h_{s+k}$. In [7] it is proven that with respect to the Gauss density $\frac{1}{\ln 2(1+\rho)}$ there exists the joint limiting distribution of q_{s-1}/R, q_s/R, $h_{s-k}, \dots, h_s, \dots, h_{s+k}$. Presumably, the same limiting distribution appears for any probability distribution $P_{N,\alpha,\epsilon}$ but we do not consider this question in more detail.

For any s_1 and k, consider the elements $\triangle'$, $\triangle''$ of $\eta^{(s_1-k)}$ which contain 0 (for $\triangle'$ the point 0 is the right end-point while for $\triangle''$ it is the left end-point). The partitions $\eta^{(s-k+1)}$, $\eta^{(s-k+2)}, \dots, \eta^{(s+k)}$ generate a finite partition of $\triangle' \cup \triangle''$ which we denote by ν. The structure of this partition is determined by h_{s-k}, $h_{s-k+1}, \dots, h_{s+k}$. Denote by N the finite set of end-points of elements of ν.

Take $b = a_3 - a_{1\,2}$ and $N' = N - a_{1\,2} (\operatorname{mod} a_3)$.

Denote

$$f_k = \max_{y \in N'} \min_{\substack{x_1 + a_{1\,2}\, x_2 \equiv y \,(\operatorname{mod} a_3) \\ a_{1\,2}\, x_2 \in N'}} \left(\frac{x_1}{\sqrt{N}} \cdot \frac{a_1}{N} + \frac{x_2}{\sqrt{N}}\frac{a_2}{N} \right).$$

The same arguments as before show with $P_{N,\alpha,\epsilon}$-probability tending to 1 as $k \to \infty$ the solution of the main max-min problem for F_1 is given by f_k. In this sense it is a function of $\frac{q_{s-1}}{R}$, $\frac{q_s}{R}$ and $h_{s-k}, \dots, h_{s+k}$ and has a limiting distribution as $N \to \infty$.

§3. The case $n = 3$ and arbitrary $b_{ij} = \operatorname{lcd}(a_i, a_j)$

Since all a_j have no common divisors, b_{13} and b_{23} are co-prime. Again for given $r, 0 \le r < a_3$, we consider the equation

$$x_1 a_1 + x_2 a_2 = r + m(x_1, x_2) a_3 .$$

We write $a_1 = b_{13} a'_1, a_2 = b_{23} a'_2$, $a_3 = b_{13} b_{23} a'_3$. Clearly a'_1 and a'_3, a'_2 and a'_3 are co-prime. Let

$$\begin{aligned} r &= r' b_{13} b_{23} + r'', && 0 \le r'' < b_{13} b_{23} , \\ x_1 &= b_{23} x'_1 + x''_1, && 0 \le x''_1 < b_{23} , \\ x_2 &= b_{13} x'_2 + x''_2, && 0 \le x''_2 < b_{13} , \\ a'_1 &= b_{23} a''_1 + a'''_1, && 0 \le a'''_1 < b_{23} , \\ a'_2 &= b_{13} a''_2 + a'''_2, && 0 \le a'''_2 < b_{13} . \end{aligned}$$

First we consider the equation

$$x''_1 b_{13} a'''_1 + x''_2 b_{23} a'''_2 \equiv r'' \pmod{b_{13} b_{23}} . \tag{9}$$

We can find unique solution which we denote by $\bar{x}''_1, \bar{x}''_2$ such that

$$x''_1 a'''_1 + x''_2 a'''_2 = r'' + t b_{13} b_{23}$$

where t can take values 0 or 1. After that we consider the equation which remains after dividing both sides of (8) by $b_{13} b_{23}$:

$$x'_1 a'_1 + a'_2 a'_2 = r' - x''_1 a''_1 - x''_2 a''_2 - t + m a'_3 . \tag{10}$$

Denote $r'_1 = r' - x''_1 a''_1 - x''_2 a''_2 + t$. Clearly $x''_1 a''_1 - x''_2 a''_2 + t$ can take finitely many values depending only on $\{b_{ij}\}$. It is easy to see that the limits of probabilities of these values exist as $N \to \infty$.

The equation (9) is similar to (6) because a_1' and a_3' are co-prime. We can write

$$x_1' + x_2'a_2'(a_1')^{-1} = r_1'(a_1')^{-1} + m_1a_3'$$

and use the same arguments as in Section 2. In particular, we consider the expansion of $a_2'(a_1')^{-1}$ into continued fraction, take s_1 for which $q_{s_1} \geqslant \sqrt{N}$, $q_{s_1} - 1 < \sqrt{N}$ and find the value of s for which $\frac{|\triangle_1^{(s)}|}{\sqrt{N}} + \frac{q_s}{\sqrt{N}}$ takes its minimum. The limiting distribution of the last number gives the limiting distribution of $\frac{1}{N^{3/2}}F_1(a)$.

§4. The case $n > 3$

For $n > 3$ our result is weaker. Again we consider the equation

$$x_1a_1 + x_2a_2 + \cdots + x_{n-1}\,a_{n-1} = r + ma_n \tag{11}$$

or

$$x_1a_1 + x_2a_2 + \cdots x_{n-1}\,a_{n-1} \equiv r \pmod{a_n}\,. \tag{12}$$

The left-hand side is the orbit of the abelian group generated by $(n-1)$ commuting rotations R_j where R_j is the shift $\mod a_n$ of $S = \{0, 1, \ldots, a_n - 1\}$ by a_j, $1 \leq j \leq n-1$. We shall prove the following theorem.

Theorem 2. *Consider the ensemble $\Omega_{N,\alpha} \subset \Omega_N$ such that $\alpha N < a_j$, $1 \leq j \leq n$, where $0 < \alpha < 1$ is a fixed number. Take the set $\sum_{\mathcal{D}} \subset \Omega_{N,\alpha}$ of $(a_1, a_2, \ldots, a_n) \in \Omega_{N,\alpha}$ such that for any $r \in S$ the equation (12) has a solution with $0 \leq x_j \leq \mathcal{D}N^{\frac{1}{n-1}}$. Then $P_{N,\alpha}(\sum_{\mathcal{D}}) \geq 1 - \epsilon(\mathcal{D})$ where $\epsilon(\mathcal{D}) \to 0$ as $\mathcal{D} \to \infty$. Here $P_{N,\alpha}$ is the uniform probability distribution on $\Omega_{N,\alpha}$.*

Proof. It is easy to see that

$$\frac{1}{a_n}\sum_{m=0}^{a_n-1} \exp\left\{-\frac{2\pi im \cdot r}{a_n}\right\} \exp\left\{-2\pi i\sum_{j=1}^{n-1}\frac{ma_j}{a_n} \cdot x_j\right\} = \begin{cases} 1 & \text{if} \quad (12) \text{ holds} \\ 0 & \text{if} \quad (12) \text{ fails} \end{cases}$$

Take $M > 0$ and consider the weight on $\mathbb{Z}$

$$c(x) \;=\; \begin{cases} 1 - \frac{|x-M|}{M}\,, & 0 \,\le\, x \,\le\, 2M \\ \\ 0 & \text{otherwise}\,. \end{cases}$$

To show that (12) has a solution for any $r \in S$, it will suffice to show that for any r

$$Z_a(r) \;=\; \sum_{x_1,x_2,\ldots,x_n \in \mathbb{Z}} c(x_1)\,c(x_2)\cdots\,c(x_{n-1})\,\frac{1}{a_n}\sum_{m=0}^{a_n-1}\exp\left\{-\,\frac{2\pi imr}{a_n}\right\}\cdot$$
$$\exp\left\{2\pi im\sum_{j=1}^{n-1}\frac{a_j}{a_n}\,x_j\right\} \neq 0\,. \tag{13}$$

We write

$$Z_a(r) \;=\; \frac{1}{a_n}\sum_{m=0}^{a_n-1}\exp\left\{-\,2\pi i\,\frac{mr}{a_n}\right\}\prod_{j=1}^{n-1}\sum_{x\in\mathbb{Z}} c(x)\,\exp\left\{2\pi i\,\frac{ma_j}{a_n}\,x\right\}.$$

It is easy to check that

$$\sum_{x\in\mathbb{Z}^1} c(x)\,e^{-2\pi i\theta x} \;=\; e^{2\pi iM\theta}\,\frac{1}{2M+1}\,\left\{\frac{\sin\,\pi(2M+1)\theta}{2\sin\,\pi\theta}\right\}^2 \tag{14}$$

for any θ. Separating in (13) the contribution of $m = 0$ and $m \neq 0$ we can write

$$Z_a(r) \;=\; \frac{M^{n-1}}{a_n} \,+\, Z_a^{(1)}(r) \;=\; \frac{M^{n-1}}{a_n} \,+\, \frac{1}{a_n}\sum_{m=1}^{a_n-1} e^{-2\pi i\,\frac{mr}{a_n}}\prod_{j=1}^{n-1}\left(\sum_{x\in\mathbb{Z}'} c(x)\,e^{2\pi i\,\frac{ma_j}{a_n}\,x}\right).$$

We shall consider $M = A\,N^{\frac{1}{n-1}}$. Therefore $\frac{M^{n-1}}{a_n} = \frac{A^{n-1}\cdot N}{a_n}$. In our case $\alpha \le \frac{a_n}{N} \le 1$. In view of (14) for $Z_a^{(1)}(r)$ we have the estimate

$$|Z_a^{(1)}| \,\le\, \frac{1}{a_n}\sum_{m=1}^{a_n-1}\prod_{j=1}^{n-1}\left(\frac{\sin\,\pi(2M+1)\theta_j}{2\,\sin\,\pi\theta_j}\right)^2\,\frac{1}{2M+1} \tag{15}$$

where $\theta_j = \frac{ma_j}{a_n}$. This estimate does not depend on r. Therefore, if we show that the expectation of the *rhs* of (15) is bounded by some constant then the Chebyshev inequality gives the statement of the theorem.

It is easy to check that

$$\left(\frac{\sin\,\pi(2M+1)\theta_j}{2\,\sin\,\pi\theta_j}\right)^2 \le \frac{C_1}{\left(\sin\left(\frac{\pi m a_j}{a_n}\right)\right)^2 + M^{-2}}$$

for some absolute constant C_1. Therefore

$$|Z_a^{(1)}| \le \frac{C_2}{a_n}\sum_{m=1}^{a_n-1}\prod_{j=1}^{n-1}\left\{\frac{1}{M}\,\frac{1}{\left(\sin\,\pi m\,\frac{a_j}{a_n}\right)^2 + M^{-2}}\right\} =$$

$$\le \frac{C_2}{a_n}\sum_{m=1}^{a_n-1}\prod_{j=1}^{n-1}\frac{1}{M\parallel \frac{ma_j}{a_n}\parallel^2 + M^{-1}}\,. \qquad (16)$$

for another absolute constant C_2. In the last formula $\parallel\cdot\parallel$ is the distance till the nearest integer number. Let us average the *rhs* of (16) *wrt* $P_{N,\alpha}$, i.e., consider

$$Z^{(2)} = \frac{1}{N^{n+1}}\sum_{\alpha N\le a_n\le N}\sum_{m=1}^{a_n-1}\sum_{\substack{\alpha N\le a_1,\dots,a_{n-1}\le N\\ \ell cd(a_1,\dots,a_n)=1}}\prod_{j=1}^{n-1}\frac{1}{M\parallel\frac{ma_j}{a_n}\parallel^2 + M^{-1}}\,. \qquad (17)$$

Assume that $\frac{m}{a_n} = b/q$ for some $1\le b\le q$ and $(b,q)=1$. Then the *rhs* of (17) can be written as

$$N^{-n-1}\sum_{q=1}^{N}\frac{N}{q}\cdot\sum_{\substack{1\le b\le q\\(b,q)=1}}\sum_{\substack{\alpha N\le a_1,\dots,a_n\le N\\ \ell cd(a_1,\dots,a_{n-1},q)=1}}\prod_{j=1}^{n-1}\frac{1}{M\parallel\frac{b}{q}\,a_j\parallel^2 + M^{-1}}\,. \qquad (18)$$

If $\ell cd(a_1,\dots,a_{n-1},q) = 1$ then certainly a_k is not a multiple of q for some $k = 1,\dots,n-1$. Hence

$$\sum_{\alpha N \le a_1,\dots,a_n \le N} \prod_{j=1}^{n-1} \frac{1}{M \parallel \frac{b}{q} a_j \parallel^2 + M^{-1}} \le \sum_{k=1}^{n-1} \sum_{\substack{\alpha N \le a_1,\dots,a_{n-1} \le N \\ a_k \notin q\mathbb{Z}}} \prod_{j=1}^{n-1} \frac{1}{M \parallel \frac{b}{q} a_j \parallel^2 + M^{-1}} =$$

$$= (n-1) \sum_{\substack{\alpha N \le a \le N \\ a \ne q\mathbb{Z}}} \frac{1}{M \parallel \frac{ba}{q} \parallel^2 + M^{-1}} \cdot \left(\sum_{\alpha N \le a \le N} \frac{1}{M \parallel \frac{b}{q} a \parallel^2 + M^{-1}} \right)^{n-2} \tag{19}$$

Now we shall estimate both sums in (19).

Lemma 2.

(i) If $q > M$ then

$$\sum_{\alpha N \le a \le N} \frac{1}{M \parallel \frac{b}{q} a \parallel^2 + M^{-1}} \le N\,;$$

(ii) If $q \le M$ then

$$\sum_{\alpha N \le a \le N} \frac{1}{M \parallel \frac{b}{q} a \parallel^2 + M^{-1}} \le \frac{M}{q} \cdot N\,;$$

(iii) If $q \le M$ then

$$\sum_{\substack{\alpha N \le a \le N \\ a \notin q\mathbb{Z}}} \frac{1}{M \parallel \frac{ba}{q} \parallel^2 + M^{-1}} \le \frac{q}{M} N\,.$$

Proof. Partition $[\alpha N, N]$ onto approximately $\frac{(1-\alpha)N}{q}$ intervals I_γ of the length q. Denote by π_q the quotient map $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$. Then for each I_γ we have $\{\pi_q(ba) | a \in I_\gamma\} = Z_q$ and

$$\{\pi_q(ba) | a \in I_\gamma,\, \pi_q(a) \ne 0\} = \mathbb{Z}_q \setminus \{0\}\,.$$

Therefore the sum

$$\sum_{\alpha N \le a \le N} \frac{1}{M \parallel \frac{b}{q} a \parallel^2 + M^{-1}}$$

behaves as

$$\frac{N}{q}\sum_{z=0}^{q-1}(q-1)\,\frac{1}{M\parallel\frac{z}{q}\parallel^2+M^{-1}}$$

and for another absolute constant C_3

$$\sum_{z=0}^{q-1}\frac{1}{M\parallel\frac{z}{q}\parallel^2+M^{-1}}\leq C_3q$$

if $q\geq M$

and

$$\sum_{z=0}^{q-1}\frac{1}{M\parallel\frac{z}{q}\parallel^2+M^{-1}}\leq C_3M$$

if $q<M$.

This gives the statements (i) and (ii) of the lemma. For $q<M$ the sum

$$\sum_{z=1}^{q-1}\frac{1}{M\parallel\frac{z}{q}\parallel^2+M^{-1}}\leq\frac{q^2}{M}\,.$$

Lemma is proven. □

Return back to (19). For $q\geq M$ Lemma 2 shows that it is not more than N^{n-1} while for $q<M$ it is not more than $\frac{q}{M}\cdot N\cdot\left(\frac{M}{q}n\right)^{n-2}=\left(\frac{M}{q}\right)^{n-3}\cdot N^{n-1}$. Substituting these estimates into (17) we get assuming $n>3$

$$Z^{(2)}\leq\frac{1}{N^{n+1}}\cdot\sum_{M\leq q\leq N}\cdot\frac{N}{q}\sum_{\substack{1\leq b\leq q\\(b,q)=1}}N^{n-1}+$$

$$+\frac{1}{N^{n+1}}\sum_{1\leq q\leq M}\frac{N}{q}\sum_{\substack{1\leq b\leq q\\(b,q)=1}}\left(\frac{M}{q}\right)^{n-3}\cdot N^{n-1}<$$

$$< C_4 + C_4 \frac{M^{n-3}}{N} \sum_{1 \le q \le M} \frac{1}{q^{n-3}} < C_4 \left(1 + \frac{M^{n-2}}{N}\right)$$

for another constant C_4. Thus $Z^{(2)}$ is bounded. This implies the statement of the theorem.

Theorem 2 shows that in any ensemble $\Omega_{N,\alpha}$ the family of probability distributions of $F_1(a)/N^{1+\frac{1}{n-1}}$ is weakly compact. However, it does not imply the existence of the limiting distribution of $F_1(a)/N^{1+\frac{1}{n-1}}$ but gives only the existence of limiting points.

References

[1] V.I. Arnold, "Weak asymptotics for the number of solutions of Diophantine problems," *Funct. Anal. Appl.*, **33:4** (1999), 292-293.

[2] V.I. Arnold, "Arithmetical turbulence of self-similar fluctuations statistics of large Frobenius numbers of additive semi-groups of integers," Preprint IC/2006/037, ICTP, Miramare, 2006. *Funct. Anal., Appl.*, **24:3** (1990), 1-8.

[3] L.B. Koralov and Ya. G. Sinai, "Probability Theory and Random Processes," Springer-Verlag, (in press).

[4] J.J. Sylvester, "Mathematical questions with their solutions," Educational Times, **41**, (1884), 21.

[5] Ya. G. Sinai, "Topics in Ergodic Theory," Princeton University Press, 1994.

[6] Ya. G. Sinai and C. Ulcigrai, "Renewal-type Limit Theorem for the Gauss Map and Continued Fractions," (in preparation).

Appendix 1.

Below we prove some estimate which was not used in the previous proofs but is of some independent interest. A similar statement was proven by A. Kochergin (private communication).

Lemma *Let for* $0 < \alpha < 1$

$$S_T(\alpha) = \frac{1}{T} \sum_{t=1}^{T} \frac{1}{|\exp\{2\pi i t\alpha\} - 1|}$$

and

$$A_T(\mathcal{D}) = \{\alpha : |S_T(\alpha)| \geq \mathcal{D} \ln T\}.$$

Then $\ell(A_T(\mathcal{D})) \leq \epsilon_1(\mathcal{D})$ *where* $\epsilon_1(\mathcal{D}) \to 0$ *as* $\mathcal{D} \to \infty$*, where* ℓ *is the Lebesgue measure.*

Proof. Take two positive numbers $C_1, C_2, 1 < C_1 < 2C_1 < C_2$, introduce the intervals $\triangle_T(k) = \left\{\alpha : \frac{C_1^k}{T} \leq \alpha \leq \frac{C_1^{k+1}}{T}\right\}, k = 0, 1, \dots, K$. Without any loss of generality we may assume that $C_1^{K+1} = T$. Clearly, $K \sim \frac{\ln T}{\ln C_1}$. Consider

$$B_{T,k}(C_1, C_2) = \{\alpha : \nu_{T,k}(\alpha) \leq C_2 C_1^k\}$$

where $\nu_{M,k}(\alpha)$ is the number of $m, 1 \leq m \leq M$, such that $\{m\alpha\} \in \triangle_M(k)$, and

$$B_T(C_1, C_2) = \bigcap_{k=0}^{K} B_{T,k}(C_1, C_2).$$

Then for $\alpha \in B_T(C_1, C_2)$

$$|S_T(\alpha)| = \frac{1}{T} \sum_{t=1}^{T} \frac{1}{|\exp\{2\pi i t\alpha\} - 1|} \leq \frac{1}{T} \sum_{k=0}^{K} \frac{T}{2\pi C_1^k} \nu_{T,k}(\alpha)$$

$$\leq \frac{C_2}{2\pi}(K + 1) \leq \frac{C_2 \ln T}{2\pi \ln C_1}.$$

This is the needed inequality with $\mathcal{D} = \frac{C_2}{2\pi \ln C_1}$. Thus we have to estimate the measure of the complement of $B_T(C_1, C_2)$. Clearly

$$\ell(\bar{B}_T(C_1, C_2)) \le \sum_{k=0}^{K} \ell(\bar{B}_{T,k}(C_1, C_2))$$

where $\bar{B}$ is the complement to B. Let $\chi_k(\alpha)$ be the indicator of $B_{T,k}(C_1, C_2)$. Then

$$\nu_{T,k}(C_1, C_2) = \sum_{t=1}^{T} \chi_k(t\alpha)$$

and by Chebyshev inequality

$$\ell\{\alpha : \nu_{T,k}(\alpha) \ge C_2 C_1^k\} = \ell\left\{\alpha : \sum_{t=1}^{T} \chi_k(t\alpha) \ge C_2 C_1^k\right\}$$

$$= \ell\left\{\alpha : \sum_{t=1}^{T} \left(\chi_k(t\alpha) - \frac{C_1^k(C_1-1)}{T}\right) \ge (C_2 - C_1 + 1)C_1^k\right\}$$

$$\le \frac{E\left[\sum_{t=1}^{T}\left(\chi_k(t\alpha) - \frac{C_1^k(C_1-1)}{T}\right)^2\right]}{(C_2 - C_1 + 1)^2 C_1^{2k}}$$

$$= \frac{E_{j=1}^{T}(T-j)(E\chi_k(\alpha)\chi_k(j\alpha) - \left(\frac{C_1^k(C_1-1)}{T})\right)}{(C_2 - C_1 + 1)^2 C_1^{2k}}.$$

The expectation is taken with respect to the Lebesgue measure. We shall estimate the last sum. It will be done separately in four steps.

<u>Step 1</u>: $j < C_1$. Here $E\chi_k(\alpha)\chi - k(j\alpha) \le E\chi_k(\alpha) = \frac{C_1^k(C_1-1)}{T}$ and

$$\frac{\sum_{j<C_1}(M-j)\left[E\chi_k(\alpha)\chi_k(j\alpha) - \left(\frac{C_1^k(C_1-1)}{T}\right)^2\right]}{(C_2 - C_1 + 1)^2 C_1^{2k}} \le \frac{C_1^k(C_1-1))C_1}{C_1^{2k}(C_2 - C_1 + 1)^2} \le \frac{1}{C_1^{k+1}}$$

since $C_2 > 2C_1$.

Step 2: $C_1 \le j < \frac{T}{C_1^{k+1}}$. In this case $E\chi_k(\alpha)\chi_k(j\alpha) = 0$ and therefore there is nothing to estimate. Indeed, $\chi_k(\alpha)$ is the indicator of the set $\triangle_T(k)$. The function $\chi_k(j\alpha)$ is the indicator of the arithmetic progression of the intervals $\left[\frac{1}{j}\frac{C_1^k}{T} + \frac{s}{j}, \frac{1}{j}\frac{C_1^{k+1}}{T} + \frac{s}{j}\right]$, $s \ge 0$. From our condition on j it follows that $\triangle_T(k)$ can intersect only with the interval for which $t = 0$ this intersection is empty.

Step 3: $\frac{T}{C_1^{k+1}} \le j \le \frac{3T}{C_1^k(C_1-1)}$. The number 3 does not play any essential role and can be replaced by any bigger number. Here $\triangle_T(k)$ intersects with not more than three intervals from the above mentioned arithmetic progression. Therefore $E\chi_k(\alpha)\chi_k(j\alpha) \le \frac{3C_1^k}{jT}$ and

$$\frac{\sum_j (T-j)\left[E\chi_k(\alpha)\chi_k(j\alpha) - \left(\frac{C_1^k(C_1-1)}{T}\right)^2\right]}{(C_2-C_1+1)^2 C_1^{2k}}$$

$$\le \frac{3C_1^k}{(C_2-C_1+1)^2 C_1^{2k}} \sum_{\frac{T}{C_1^{k+1}} \le j \le \frac{3T}{C_1^k(C_1-1)}} \frac{1}{j}$$

$$\le \frac{3}{C_1^k(C_2-C_1+1)^2} \frac{C_1^{k+1} \cdot 2T}{T \cdot C_1^k(C_1-1)^2} = \frac{24}{C_1^k C_2}.$$

This is the estimate which we need.

Step 4: $j \ge \frac{3T}{C_1^k(C_1-1)}$. In this case $E\chi_k(\alpha)\chi_k(j\alpha)$ is close to $(E\chi_k(\alpha))^2 = \left(\frac{C_1^k(C_1-1)}{T}\right)^2$. Indeed, we can increase $\triangle_T(k)$ by adding an interval near each end-point so that the new set $\triangle'_T(k)$ will consist of an integer number of intervals $\left[\frac{s}{j}, \frac{s+1}{j}\right]$. Therefore

$$E\chi_k(\alpha)\chi_k(j\alpha) \le \ell(\triangle'_T(k))\frac{C_1^k(C_1-1)}{T} \le \left(\ell(\triangle_T(k)) + \frac{2}{j}\right)\frac{C_1^k(C_1-1)}{T}$$

$$= \ell^2(\triangle_T(k)) + \frac{2C_1^k(C_1-1)}{Tj}$$

and

$$\sum_{\frac{3T}{C_1^k(C-1)} \le j \le T} \frac{(T-j)\left[E\chi_k(\alpha)\chi_k(j\alpha) - \left(\frac{C_1^k(C_1-1)}{T}\right)^2\right]}{(C_2-C_1+1)^2 C_1^{2k}}$$

$$\leq \sum_{\frac{3T}{C^k(C-1)} \leq j \leq T} \frac{(T-j)2C_1^k(C_1-1)}{Tj(C_2-C_1+1)^2 C_1^{2k}}$$

$$\leq \frac{2C_1^k(C_1-1)}{(C_2-C_1+1)^2 C_1^k} \ln \frac{TC_1^k(C-1)}{3T} = \frac{4(C_1-1)k \ln C_1}{(C_2-C_2+1)^2 C_1^k}.$$

Now we can finish the proof of the Lemma. From all our estimates it follows that

$$\ell \left\{ \alpha : \nu_{T,k}(\alpha) \geq C_2 C_1^k \right\} \leq \frac{4 \ln C_1}{C_1} \frac{k}{C_1^k}$$

and therefore

$$\sum_k \ell\{\alpha : \nu_{T,k}(\alpha) \geq C_2 C_1^k\} \leq \text{const} \frac{\ln C_1}{C_1}.$$

This implies the statement of the lemma. $\square$