C. R. Acad. Sci. Paris, Ser. I 349 (2011) 713–718

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number Theory

Partial quotients and equidistribution

Fractions continues et equidistribution

Mei-Chu Chang [1]

Department of Mathematics, University of California, 900 University Avenue, Riverside, CA 92521, USA

ARTICLE INFO

Article history:
Received 15 April 2011
Accepted after revision 7 June 2011
Available online 24 June 2011

Presented by Jean Bourgain

ABSTRACT

We establish average bounds on the partial quotients of fractions b/p, with p prime, b taken in a multiplicative subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ and for "most" primitive elements b. Our result improves upon earlier work due to G. Larcher. The behavior of the partial quotients of b/p is well known to be crucial to the statistical properties of the pseudo-congruential number generator $(\bmod p)$. As a corollary, estimates on their pair correlation are refined.

RÉSUMÉ

Nous obtenons des bornes en moyenne pour les quotients partiels de certaines fractions b/p, p un nombre premier, b dans un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ ainsi que pour b un élément primitif « typique » $(\bmod p)$. Ceci donne en particulier une amélioration de résultats de G. Larcher. Il est bien connu que le comportement des quotients partiels de $\frac{b}{p}$ détermine les propriétés statistiques de la distribution $b^j (\bmod p)$. On en déduit, comme corollaire, de meilleures estimations sur les corrélations partielles pour ces suites.

Version française abrégée

Pour $x \in [0,1]$, soit $a_i = a_i(x)$, $i = 1, 2, \ldots,$ les quotients partiels de $x = [a_1, a_2, \ldots]$. Soit p un nombre premier suffisamment grand et G un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ de taille $|G| > p^{7/8+\varepsilon}$. On montre que la plupart des éléments $b \in G$ satisfont les inégalités

$$\max_i a_i\left(\frac{b}{p}\right) < c \log p$$

ainsi que

$$\sum_i a_i\left(\frac{b}{p}\right) < c \log p \cdot \log\log p.$$

E-mail address: mcc@math.ucr.edu.

[1] Partially supported by NSF.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2011.06.007

Cette dernière propriété est également vraie pour la majorité des éléments primitifs $b \pmod p$, et la théorie classique d'equi-répartition $(\bmod 1)$ entraîne que

$$D\left(\left(\frac{b^{j-1}}{p}, \frac{b^j}{p}\right)\colon\ j = 1, \dots, p-1\right) < \frac{c}{p} \log p \cdot \log\log p.$$

1. Introduction

Let $x \in [0,1]$ be a real number with continued fraction [5]

$$x = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}} = [a_1, a_2, \dots].$$

Denote $\{a_i(x)\}_i$ the partial quotients $\{a_1, a_2, \dots\} \subset \mathbb{Z}^+$ of x.

It was proven by G. Larcher [4] that given a modulus N, there exists $1 \leqslant b < N$, $(b, N) = 1$ such that

$$\sum_i a_i\left(\frac{b}{N}\right) < c \log N \cdot \log\log N. \tag{1}$$

The question whether one can remove the $\log\log N$ factor in (1) is still open and would follow from an affirmative answer to Zaremba's conjecture (see [6, p. 69]), stating that

$$\min_{(b,N)=1} \max_i a_i\left(\frac{b}{N}\right) < c, \tag{2}$$

where c is an absolute constant (independent of N). (See [7] and [1] for results related to the conjecture.)

The quantity $\sum_i a_i(x)$ is important in the study of equidistributions.

For a sequence $x_1, \dots, x_N \in [0,1]^d$, we define the discrepancy

$$D(x_1, \dots, x_N) = \sup_J \left| \frac{|\{x_1, \dots, x_N\} \cap J|}{N} - |J| \right|, \tag{3}$$

where sup is taken over all boxes $J \subset [0,1]^d$.

For $r \in \mathbb{R}$, let $[r]$ be the greatest integer less than or equal to r. We denote the fractional part $r - [r]$ of r by $\{r\}$.

Recall that the convergents $\frac{p_i(x)}{q_i(x)}$ of a continued fraction $x = [a_1, a_2, \dots]$ is $\frac{p_i(x)}{q_i(x)} = \frac{p_i}{q_i} = [a_1, a_2, \dots, a_i]$, and we have $q_i = a_i q_{i-1} + q_{i-2}$.

The following are classical results relating discrepancy of an arithmetic progression (with difference x) modulo 1 to the sum of partial quotients of x. (See [3, p. 126].)

Proposition A. *Let $x \in [0,1]$. Then the sequence kx, $k = 1, \dots, N$ satisfies*

$$D\big(\{x\}, \{2x\}, \dots, \{Nx\}\big) \leqslant \frac{c}{N} \sum_{q_i(x) < N} a_i(x). \tag{4}$$

In particular, when $x = \frac{b}{N}$ with $(b, N) = 1$, Proposition A implies

Proposition A′.

$$D\left(\left\{\frac{b}{N}\right\}, \left\{\frac{2b}{N}\right\}, \dots, \left\{\frac{Mb}{N}\right\}\right) \leqslant \frac{c}{M} \sum_i a_i\left(\frac{b}{N}\right) \tag{5}$$

for $M \leqslant N$.

Also, considering the sequence $(\frac{k}{N}, \{\frac{kb}{N}\})$, $k = 1, \dots, N$ in $[0,1] \times [0,1]$, there is the following:

Proposition B.

$$D\left(\left(\frac{k}{N}, \left\{\frac{kb}{N}\right\}\right)\colon\ k = 1, \dots, N\right) \leqslant \frac{c}{N} \sum_i a_i\left(\frac{b}{N}\right). \tag{6}$$

Hence, substituting (1) in (5) and (6), we obtain discrepancy bounds of the form $D \leqslant \frac{c}{N} \log N \log\log N$ for these sequences.

Next, consider the discrepancy for the linear congruential generator modulo N, i.e. we take b primitive $(\bmod N)$ and consider the sequence

$$\left\{\frac{b}{N}\right\}, \left\{\frac{b^2}{N}\right\}, \dots, \left\{\frac{b^\tau}{N}\right\}, \tag{7}$$

where $\tau = \varphi(N)$ is the order of b $(\bmod N)$.

When examining statistical properties of (7), the two quantities studied are

$$D\left(\left\{\frac{b}{N}\right\}, \left\{\frac{b^2}{N}\right\}, \dots, \left\{\frac{b^\tau}{N}\right\}\right) \quad \text{(equidistribution)} \tag{8}$$

and

$$D := D\left(\left(\left\{\frac{b}{N}\right\}, \left\{\frac{b^2}{N}\right\}\right), \dots, \left(\left\{\frac{b^{\tau-1}}{N}\right\}, \left\{\frac{b^\tau}{N}\right\}\right)\right) \quad \text{(pair serial-test).} \tag{9}$$

Larcher proved that if $N = p^s$, p prime, then there is b primitive $(\bmod N)$, such that

$$D < \frac{c}{\varphi(\varphi(n))} \log N \cdot \log\log N, \tag{10}$$

where $\varphi(n)$ is the Euler's totient function.

If $N = p$, Larcher's argument consists in observing that $\tau(b) = p - 1$ for b primitive, and one has trivially that

$$D\left(\left(\left\{\frac{b^k}{p}\right\}, \left\{\frac{b^{k+1}}{p}\right\}\right);\ k = 1, \dots, p-2\right) = D\left(\left(\left\{\frac{x}{p}\right\}, \left\{\frac{xb}{p}\right\}\right):\ x = 1, \dots, p-1\right) + O(1)\frac{1}{p} \tag{11}$$

and the case is reduced to Proposition B.

The method of proving Proposition B (that proceeds by averaging over b) implies that there is a *primitive* b $(\bmod N)$ such that

$$\sum_i a_i\left(\frac{b}{N}\right) < c\frac{N}{\varphi(\varphi(N))} \log N \cdot \log\log N. \tag{12}$$

(Note that $\varphi(\varphi(N))$ is the number of primitive elements $(\bmod N)$.)

Our aim is to improve (12) (see Theorem 5), at least when p is prime, by removing the factors $\frac{N}{\varphi(\varphi(N))}$.

Proposition 1. *Let $G \subset \mathbb{Z}_p^*$ be a subgroup with $|G| > p^{7/8+\varepsilon}$. Then for $M < (\log p)^c$ we have*

$$\left|\left\{x \in G:\ \max_i a_i\left(\frac{x}{p}\right) > M\right\}\right| < c\frac{\log p}{M}|G|.$$

The next theorem is a direct consequence of Proposition 1.

Theorem 2. *Let $G \subset \mathbb{Z}_p^*$ be a subgroup with $|G| > p^{7/8+\varepsilon}$. Then most elements $x \in G$ satisfy* $\max a_i(\frac{x}{p}) \lesssim \log p$.

Note that even for $G = \mathbb{Z}_p^*$, the bound $c \log p$ is the best result known (towards Zaremba's conjecture). (See [7] and [1].)

Theorem 3. *For most primitive elements* $(\bmod p)$, *we have* $\max a_i(\frac{x}{p}) \lesssim \log p$.

As for $\sum_i a_i(\frac{x}{p})$ with $x \in G$, we have the following result:

Theorem 4. *Let $G \subset \mathbb{Z}_p^*$ be a subgroup with $|G| > p^{7/8+\varepsilon}$. Then most elements $x \in G$ satisfy*

$$\sum_i a_i\left(\frac{x}{p}\right) \lesssim c \log p \cdot \log\log p.$$

Theorem 5. *For most primitive elements* $x \pmod p$, *we have*

$$\sum_i a_i\left(\frac{x}{p}\right) \lesssim c\log p \cdot \log\log p.$$

Together with Proposition A′, Proposition B and (11), Theorem 5 implies

Corollary 6. *Let* p *be a large prime. Then there exists* x *primitive* mod p *such that*

$$D\left(\left\{k\frac{x}{p}\right\}\colon k=1,\dots,M\right) \leqslant \frac{c\log p\cdot\log\log p}{M},$$
$$D\left(\left(\left\{\frac{k}{p}\right\},\left\{\frac{kx}{p}\right\}\right)\colon k=1,\dots,p\right) \leqslant \frac{c\log p\cdot\log\log p}{p},$$
$$D\left(\left(\left\{\frac{x^k}{p}\right\},\left\{\frac{x^{k+1}}{p}\right\}\right)\colon k=1,\dots,p-2\right) \leqslant \frac{c\log p\cdot\log\log p}{p}.$$

2. The proofs

Let p be prime and let $G \subset \mathbb{Z}_p^*$ be a multiplicative subgroup. Denote $\psi \geqslant 0$ a smooth bump function, $\psi = 1$ on $[-\frac{1}{4}, \frac{1}{4}]$ and $\operatorname{supp}\psi \subset [-\frac{1}{3}, \frac{1}{3}]$. We define $\psi_\varepsilon(x) = \psi(\frac{x}{\varepsilon})$ (as a function on $\mathbb{R}$).

We then view ψ_ε as a function on $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, given by

$$\psi_\varepsilon(t) = \sum_j \hat{\psi}_\varepsilon(j)e(jt) \tag{13}$$

and where in (13) the summation may be restricted to $|j| < \frac{C}{\varepsilon}$.

Choose $M > 1$. Let $\|r\| = \min(\{r\}, 1-\{r\})$. Clearly,

$$\left|\left\{x\in G\colon \max_i a_i\left(\frac{x}{p}\right) > M\right\}\right| \leqslant \left|\left\{x\in G\colon \min_{0<k<p/M} k\left\|\frac{kx}{p}\right\| < \frac{1}{M}\right\}\right| < \sum_{\ell, 2^{\ell-1}<p/M}\ \sum_{2^{\ell-1}<k\leqslant 2^\ell}\ \sum_{x\in G}\psi_{\frac{8}{2^\ell M}}\left(\frac{kx}{p}\right). \tag{14}$$

We will use character sums to bound the double sum of the bump functions in (14).

Lemma 7. *Let* $I \subset (0,p)$ *be an interval and* ψ_ε *be the bump function defined above. Then we have*

$$\sum_{k\in I}\sum_{x\in G}\psi_\varepsilon\left(\frac{kx}{p}\right) = |I||G|\int\psi_\varepsilon - \frac{|I||G|}{p-1}\left(1-\int\psi_\varepsilon\right) + O(A), \tag{15}$$

where $A = \varepsilon\sqrt{p}\min(|I|, \sqrt{p}, |I|^{\frac{1}{2}}p^{\frac{3}{16}})\min(\frac{1}{\varepsilon}, \sqrt{p}, \varepsilon^{-\frac{1}{2}}p^{\frac{3}{16}})p^\varepsilon$.

Proof. Using (13), the left-hand side of (14) equals

$$|I||G|\left(\int\psi_\varepsilon\right) + \sum_{k\in I}\sum_{j\neq 0}\hat{\psi}_\varepsilon(j)\sum_{x\in G}e_p(jkx). \tag{16}$$

Using multiplicative characters

$$1_G(x) = \frac{|G|}{p-1}\sum_{\chi=1\text{ on }G}\chi(x) \tag{17}$$

for the second term in (16), we obtain the bound

$$\frac{|G|}{p-1}\left[\sum_{k\in I}\sum_{j\neq 0}\hat{\psi}_\varepsilon(j)\sum_{x=1}^{p-1}e_p(jkx)\right] + \max_{\chi\neq\chi_0}\left|\sum_{k\in I}\sum_{j\neq 0}\hat{\psi}_\varepsilon(j)\sum_{x=1}^{p-1}\chi(x)e_p(jkx)\right|. \tag{18}$$

Clearly, the first term in (18) is

$$\frac{|G|}{p-1}\left[\sum_{k\in I}\sum_{j\neq 0}\hat{\psi}_\varepsilon(j)\sum_{x=1}^{p-1}e_p(jkx)\right] = -\frac{|G|}{p-1}|I|\left(\sum_j\hat{\psi}_\varepsilon(j) - \hat{\psi}_\varepsilon(0)\right) = -\frac{|I||G|}{p-1}\left(1-\int\psi_\varepsilon\right). \tag{19}$$

For the second term in (18), we make changes of variable in x to obtain

$$\left[\sum_{k\in I}\chi(\bar{k})\right]\left[\sum_{j\neq 0}\hat{\psi}_\varepsilon(j)\chi(\bar{j})\right]\left[\sum_{x=1}^{p-1}\chi(x)e_p(x)\right], \tag{20}$$

where $\bar{x}$ and $\bar{k}$ denote inverses of x and k $(\operatorname{mod} p)$.

Also

$$\left|\sum_j \hat{\psi}_\varepsilon(j)\chi(\bar{j})\right| \leqslant V \max_J \left|\sum_{j\in J}\chi(j)\right|,$$

where V is the variation of $\hat{\psi}_\varepsilon(j)$ and J is an interval of size $< \frac{C}{\varepsilon}$.

By Cauchy–Schwarz and Plancherel,

$$V = \sum\left|\hat{\psi}_\varepsilon(j) - \hat{\psi}_\varepsilon(j+1)\right| = \sum_j \left|\left[\psi_\varepsilon(x)\left(1-e(-x)\right)\right]^\wedge(j)\right| \lesssim \frac{1}{\sqrt{\varepsilon}}\left\|\psi_\varepsilon(x)\left(1-e(-x)\right)\right\|_2 \lesssim \varepsilon. \tag{21}$$

To estimate character sums over an interval, we use Polya–Vinogradov and Garaev–Karatsuba ([2] with $r=2$), and have

$$\left|\sum_{a<x<a+H}\chi(x)\right| \lesssim \begin{cases} H \\ \sqrt{p}\log p & (22)\\ H^{\frac{1}{2}} p^{\frac{1}{2}-\frac{3}{4.2}+\frac{1}{4.2^2}+\varepsilon} < H^{\frac{1}{2}} p^{\frac{3}{16}+0}. & (23)\end{cases}$$

For the last factor in (20), we have the bound $\sqrt{p}$.

Hence

$$(20) \lesssim \varepsilon\sqrt{p}\min\left(|I|, \sqrt{p}, |I|^{\frac{1}{2}} p^{\frac{3}{16}}\right)\min\left(\frac{1}{\varepsilon}, \sqrt{p}, \varepsilon^{-\frac{1}{2}} p^{\frac{3}{16}}\right) p^\varepsilon \tag{24}$$

proving the lemma. □

Sometimes it is more convenient to use the following version of Lemma 7:

Lemma 7′.

$$\sum_{k\in I}\sum_{x\in G}\psi_\varepsilon\left(\frac{kx}{p}\right) = |I||G|\int\psi_\varepsilon + \frac{|I|\,|G|}{p} + O(A). \tag{25}$$

Proof of Proposition 1. Fix ℓ, apply Lemma 7′ with $I=[2^{\ell-1}, 2^\ell]$, $\varepsilon = \frac{8}{2^\ell M}$. After summation over ℓ in (14), we have

$$\begin{aligned}\left|\left\{x\in G\colon \max_i a_i\left(\frac{x}{p}\right) > M\right\}\right| \leqslant{}& \sum_{\ell, 2^\ell<p/M} 2^{\ell-1}|G|\int\psi_{\frac{8}{2^\ell M}} + O\left(\frac{|G|}{M}\right)\\ &+ \sum_\ell \frac{\sqrt{p}}{2^\ell M}\min\left(2^\ell, \sqrt{p}, \sqrt{2}^\ell p^{3/16}\right)\min\left(2^\ell M, \sqrt{p}, \sqrt{2^\ell M}\, p^{3/16}\right)p^\varepsilon.\end{aligned} \tag{26}$$

The first sum in (26) is bounded by $\frac{\log p}{M}|G|$. For the range of M considered, we can ignore M in (26). Observe that

$$\min\left(2^\ell, \sqrt{p}, \sqrt{2}^\ell p^{3/16}\right) = \begin{cases} 2^\ell, & \text{if } 2^\ell < p^{3/8},\\ \sqrt{2}^\ell p^{3/16}, & \text{if } p^{3/8}\leqslant 2^\ell < p^{5/8},\\ \sqrt{p}, & \text{if } 2^\ell \geqslant p^{5/8}.\end{cases} \tag{27}$$

Hence the last sum in (26) is bounded by

$$p^{\frac{1}{2}+\varepsilon}\left\{\sum_{2^\ell<p^{3/8}} 2^{-\ell}4^\ell + \sum_{p^{3/8}\leqslant 2^\ell<p^{5/8}} 2^{-\ell}2^\ell\, p^{3/8} + \sum_{2^\ell>p^{5/8}} 2^{-\ell}p\right\} < p^{\frac{1}{2}+\varepsilon}\left\{p^{3/8} + (\log p)p^{3/8} + p^{3/8}\right\} < p^{7/8+\varepsilon}. \tag{28}$$

Taking $M \gtrsim \log p$, we conclude the proof. □

Proof of Theorem 3. Lemma 7 together with inclusion–exclusion argument implies that

$$\sum_{k\in I}\sum_{\substack{x\in\mathbb{Z}_p^*\\ x\text{ primitive}}}\psi_\varepsilon\left(\frac{kx}{p}\right)=|I|\varphi(p-1)\left\{\int\psi_\varepsilon-\frac{1}{p-1}\left(1-\int\psi_\varepsilon\right)\right\}+O(A)p^\varepsilon. \qquad \square$$

Proof of Theorem 4. If we restrict ourselves to elements $x\in G$ such that

$$\max a_i\left(\frac{x}{p}\right)<M_0,$$

we can bound

$$\sum_i a_i\left(\frac{x}{p}\right)\lesssim\sum_{\substack{m\text{ dyadic}\\ M<M_0}}M\sum_{\ell,2^\ell<\frac{p}{M}}\sum_{2^{\ell-1}<k\leqslant 2^\ell}\psi_{\frac{8}{2^\ell M}}\left(\frac{kx}{p}\right). \tag{29}$$

By Lemma 7, summing the right-hand side of (29) over $x\in G$ gives

$$|G|\sum_{\substack{M\text{ dyadic}\\ M<M_0}}M\sum_{\ell,2^\ell<\frac{p}{M}}2^{\ell-1}\left\{\int\psi_{\frac{8}{2^\ell M}}-\frac{1}{p}\left(1-\int\psi_{\frac{8}{2^\ell M}}\right)\right\}+O\left(p^{7/8+\varepsilon}\right). \tag{30}$$

The first term is bounded by $|G|\ c(\log M_0)\log p$. Since by Proposition 1, we may take $M_0\sim\log p$, the theorem follows by averaging. $\square$

Theorem 5 follows from (30) together with an exclusion–inclusion argument.

References

[1] T.W. Cusick, Zaremba's conjecture and sums of the divisor function, Math. Comput. 61 (203) (1993) 171–176.
[2] M.Z. Garaev, A.A. Karatsuba, On character sums and the exceptional set of a congruence problem, J. Number Theory 114 (2005) 182–192.
[3] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, Wiley, New York, 1974.
[4] G. Larcher, On the distribution of sequences connected with good lattice points, Monatsh. Math. 101 (2) (1986) 135–150.
[5] A.M. Rockett, P. Szusz, Continued Fractions, World Scientific, 1992.
[6] S.K. Zaremba, La méthode des « bons treillis » pour le calcul des integrales multiples, in: S.K. Zaremba (Ed.), Applications of Number Theory to Numerical Analysis, Academic Press, New York, 1972, pp. 39–119.
[7] S.K. Zaremba, Good lattice points modulo composite numbers, Monatsh. Math. 78 (1974) 446–460.