PARTIAL QUOTIENTS AND DISTRIBUTION OF SEQUENCES

[1] Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521
mcc@math.ucr.edu

Abstract.

In this paper we establish average bounds on the partial quotients of fractions b/p, with p prime and b from a multiplicative subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$. As a consequence, we obtain estimates for the partial quotients of b/p, 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 $(modp)$. As a corollary, estimates on their pair correlation are refined.

§1. Introduction.

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

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

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

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

$$\sum_i a_i\Big(\frac{b}{N}\Big) < c \log N \ \log\log N. \tag{1.1}$$

---

[1]partially supported by NSF.
2000 Mathematics Subject Classification. 11K, 11L, 11J, 11B.
Keywords: partial quotients of continued fractions, distribution of sequences modulo 1.

The question whether one can remove the $\log\log N$ factor in (1.1) is still open and would follow from an affirmative answer to Zaremba's conjecture (see [Z1], p.69), stating that

$$\min_{(b,N)=1} \max_i a_i\Big(\frac{b}{N}\Big) < c, \tag{1.2}$$

where c is an absolute constant (independent of N). (See [Z2] and [C] 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

$$D(x_1, \dots, x_N) = \sup_J \left| \frac{|\{x_1, \dots, x_N\} \cap J|}{N} - |J| \right|, \tag{1.3}$$

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 [KN], p 126).

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

$$D\big(\{x\}, \{2x\}, \dots, \{Nx\}\big) \le \frac{c}{N} \sum_{q_i(x) < N} a_i(x). \tag{1.4}$$

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

Proposition A'.

$$D\bigg(\Big\{\frac{b}{N}\Big\}, \Big\{\frac{2b}{N}\Big\}, \dots, \Big\{\frac{Mb}{N}\Big\}\bigg) \le \frac{c}{M} \sum_i a_i\Big(\frac{b}{N}\Big) \tag{1.5}$$

for $M \le N$.

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.

$$D\Big(\Big(\frac{k}{N}, \Big\{\frac{kb}{N}\Big\}\Big) : k = 1, \dots, N\Big) \leq \frac{c}{N}\sum_i a_i\Big(\frac{b}{N}\Big). \tag{1.6}$$

Hence, substituting (1.1) in (1.5) and (1.6), we obtain discrepancy bounds of the form $D \leq \frac{c}{N}\log N \log\log N$ for these sequences.

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

$$\Big\{\frac{b}{N}\Big\}, \Big\{\frac{b^2}{N}\Big\}, \dots, \Big\{\frac{b^\tau}{N}\Big\}, \tag{1.7}$$

where $\tau = \varphi(N)$ is the order of b $(\operatorname{mod} N)$.

When examining statistical properties of (1.7), the two quantities studied are

$$D\Big(\Big\{\frac{b}{N}\Big\}, \Big\{\frac{b^2}{N}\Big\}, \dots, \Big\{\frac{b^\tau}{N}\Big\}\Big) \qquad \text{(equidistribution)} \tag{1.8}$$

and

$$D\Big(\Big(\Big\{\frac{b}{N}\Big\}, \Big\{\frac{b^2}{N}\Big\}\Big), \dots, \Big(\Big\{\frac{b^{\tau-1}}{N}\Big\}, \Big\{\frac{b^\tau}{N}\Big\}\Big)\Big) \qquad \text{(pair serial-test).} \tag{1.9}$$

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

$$(1.9) < \frac{c}{\varphi(\varphi(n))}\log N \ \log\log N, \tag{1.10}$$

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

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

$$D\Big(\Big(\Big\{\frac{b^k}{p}\Big\}, \Big\{\frac{b^{k+1}}{p}\Big\}\Big); k = 1, \dots, p-2\Big)$$

$$= D\Big(\Big(\Big\{\frac{x}{p}\Big\}, \Big\{\frac{xb}{p}\Big\}\Big) : x = 1, \dots, p-1\Big) + O(1)\frac{1}{p} \tag{1.11}$$

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* $b \pmod N$ such that

$$\sum_i a_i\Big(\frac{b}{N}\Big) < c\frac{N}{\varphi(\varphi(N))}\log N \ \log\log N. \tag{1.12}$$

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

Our aim is to improve (1.12) $\big($ See Theorem 5$\big)$, at least when p is prime, by removing the factors $\frac{N}{\varphi(\varphi(N))}$.

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

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

The next theorem is a direct consequence of Proposition 1.

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

Note that even for $G = \mathbb{Z}_p^*$, the bound $c\log p$ is the best result known (towards Zaremba's conjecture). (See [Z2] and [C].)

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

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

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

$$\sum_i a_i\Big(\frac{x}{p}\Big) \lesssim c\log p \ \log\log p.$$

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

$$\sum_i a_i\Big(\frac{x}{p}\Big) \lesssim c\log p \ \log\log p.$$

Together with Proposition A', Proposition B and (1.11), Theorem 5 implies

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

$$D\Big(\Big\{k\frac{x}{p}\Big\} : k = 1, \dots, M\Big) \leq \frac{c\log p \ \log\log p}{M}$$

$$D\Bigg(\Big(\Big\{\frac{k}{p}\Big\}, \Big\{\frac{kx}{p}\Big\}\Big) : k = 1, \dots, p\Bigg) \leq \frac{c\log p \ \log\log p}{p}$$

$$D\Bigg(\Big(\Big\{\frac{x^k}{p}\Big\}, \Big\{\frac{x^{k+1}}{p}\Big\}\Big) : k = 1, \dots, p-2\Bigg) \leq \frac{c\log p \ \log\log p}{p}.$$

§2. The proofs.

Let p be prime and let $G < \mathbb{Z}_p^*$ be a multiplicative subgroup. Denote $\psi \geq 0$ a smooth bump function, $\psi = 1$ on $[-\frac{1}{4}, \frac{1}{4}]$ and 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

$$\psi_\varepsilon(t) = \sum_j \hat{\psi}_\varepsilon(j) e(jt) \tag{2.1}$$

and where in (2.1) the summation may be restricted to $|j| < \frac{C}{\varepsilon}$.

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

$$\Big|\Big\{x \in G : \max_i \ a_i\Big(\frac{x}{p}\Big) > M\Big\}\Big| \leq \Big|\Big\{x \in G : \min_{0<k<p/M} k\Big\|\frac{kx}{p}\Big\| < \frac{1}{M}\Big\}\Big|$$
$$< \sum_{\ell,\ 2^{\ell-1}<p/M} \ \sum_{2^{\ell-1}<k\leq 2^\ell} \ \sum_{x\in G} \psi_{\frac{8}{2^\ell M}}\Big(\frac{kx}{p}\Big). \tag{2.2}$$

We will use character sums to bound the double sum of the bump functions in (2.2).

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

$$\sum_{k\in I}\sum_{x\in G}\psi_\varepsilon\Big(\frac{kx}{p}\Big) = |I|\,|G|\int\psi_\varepsilon - \frac{|I|\,|G|}{p-1}\Big(1-\int\psi_\varepsilon\Big) + O(A), \tag{2.3}$$

where $A = \varepsilon\sqrt{p}\ \min(|I|, \sqrt{p}\ , |I|^{\frac12}p^{\frac{3}{16}})\min\Big(\frac{1}{\varepsilon}, \sqrt{p}\ , \varepsilon^{-\frac12}p^{\frac{3}{16}}\Big)p^{\,\varepsilon}$.

Proof. Using (2.1), the left-hand-side of (2.3) equals

$$|I|\,|G|\Big(\int\psi_\varepsilon\Big) + \sum_{k\in I}\sum_{j\neq 0}\hat\psi_\varepsilon(j)\sum_{x\in G}e_p(jkx). \tag{2.4}$$

Using multiplicative characters

$$1_G(x) = \frac{|G|}{p-1}\sum_{\chi=1 \text{ on } G}\chi(x) \tag{2.5}$$

for the second term in (2.4), we obtain the bound

$$\frac{|G|}{p-1}\Big[\sum_{k\in I}\sum_{j\neq 0}\hat\psi_\varepsilon(j)\sum_{x=1}^{p-1}e_p(jkx)\Big] + \max_{\chi\neq\chi_0}\Big|\sum_{k\in I}\sum_{j\neq 0}\hat\psi_\varepsilon(j)\sum_{x=1}^{p-1}\chi(x)e_p(jkx)\Big|. \tag{2.6}$$

Clearly, the first term in (2.6) is

$$\begin{aligned}\frac{|G|}{p-1}\Big[\sum_{k\in I}\sum_{j\neq 0}\hat\psi_\varepsilon(j)\sum_{x=1}^{p-1}e_p(jkx)\Big] &= -\frac{|G|}{p-1}|I|\Big(\sum_j\hat\psi_\varepsilon(j) - \hat\psi_\varepsilon(0)\Big)\\ &= -\frac{|I|\,|G|}{p-1}\Big(1-\int\psi_\varepsilon\Big).\end{aligned} \tag{2.7}$$

For the second term in (2.6), we make changes of variable in x to obtain

$$\Big[\sum_{k\in I}\chi(\bar k)\Big]\Big[\sum_{j\neq 0}\hat\psi_\varepsilon(j)\ \chi(\bar j)\Big]\Big[\sum_{x=1}^{p-1}\chi(x)e_p(x)\Big], \tag{2.8}$$

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

Also

$$\Big|\sum_j\hat\psi_\varepsilon(j)\chi(\bar j)\Big| \le V\ \max_J\Big|\sum_{j\in J}\chi(j)\Big|,$$

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

By Cauchy-Schwarz,

$$\begin{aligned} V &= \sum \big|\hat{\psi}_\varepsilon(j) - \hat{\psi}_\varepsilon(j+1)\big| \\ &= \sum_j \Big|\big[\psi_\varepsilon(x)\big(1-e(-x)\big)\big]^\wedge(j)\Big| \\ &\lesssim \frac{1}{\sqrt{\varepsilon}}\Big\|\psi_\varepsilon(x)\big(1-e(-x)\big)\Big\|_2 \lesssim \varepsilon. \end{aligned} \tag{2.9}$$

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

$$\Big|\sum_{a<x<a+H} \chi(x)\Big| \lesssim \begin{cases} H \\ \sqrt{p}\ \log p & (2.10) \\ H^{\frac{1}{2}} p^{\frac{1}{2}-\frac{3}{4.2}+\frac{1}{4.2^2}+\varepsilon} < H^{\frac{1}{2}} p^{\frac{3}{16}+0}. & (2.11) \end{cases}$$

For the last factor in (2.8), we have the bound $\sqrt{p}$.

Hence

$$(2.8) \lesssim \varepsilon\sqrt{p}\ \min(|I|, \sqrt{p}\,, |I|^{\frac{1}{2}} p^{\frac{3}{16}}) \min\Big(\frac{1}{\varepsilon}, \sqrt{p}\,, \varepsilon^{-\frac{1}{2}} p^{\frac{3}{16}}\Big) p^{\,\varepsilon} \tag{2.12}$$

proving the lemma. □

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

Lemma 7'.

$$\sum_{k\in I}\sum_{x\in G} \psi_\varepsilon\Big(\frac{kx}{p}\Big) = |I|\,|G| \int \psi_\varepsilon + \frac{|I|\,|G|}{p} + O(A), \tag{2.13}$$

This is obtained by a rough estimate of (2.7).

$$(2.7) < \frac{|G|}{p-1}|I| \sum |\hat{\psi}_\varepsilon(j)| \lesssim \frac{|G|}{p}|I|.$$

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 (2.2), we have

$$\begin{aligned}\Big|\Big\{x\in G:\max_i\ a_i\Big(\frac{x}{p}\Big)>M\Big\}\Big|\le&\sum_{\ell,\ 2^\ell<p/M}2^{\ell-1}|G|\int\psi_{\frac{8}{2^\ell M}}+O\Big(\frac{|G|}{M}\Big)\\&+\sum_\ell\frac{\sqrt{p}}{2^\ell M}\min(2^\ell,\sqrt{p},\sqrt{2}^\ell p^{3/16})\min(2^\ell M,\sqrt{p},\sqrt{2^\ell M}\,p^{3/16})p^{\ \varepsilon}.\end{aligned}\tag{2.14}$$

The first sum in (2.14) is bounded by $\frac{\log p}{M}|G|$. For the range of M considered, we can ignore M in (2.14). Observe that

$$\min(2^\ell,\sqrt{p},\sqrt{2}^\ell p^{3/16})=\begin{cases}2^\ell, & \text{if } 2^\ell<p^{3/8}\\ \sqrt{2}^\ell p^{3/16}, & \text{if } p^{3/8}\le 2^\ell<p^{5/8}\\ \sqrt{p}, & \text{if } 2^\ell\ge p^{5/8}.\end{cases}\tag{2.15}$$

Hence the last sum in (2.14) is bounded by

$$\begin{aligned}&p^{\frac12+\varepsilon}\Big\{\sum_{2^\ell<p^{3/8}}2^{-\ell}\,4^\ell+\sum_{p^{3/8}\le 2^\ell<p^{5/8}}2^{-\ell}\,2^\ell\,p^{3/8}+\sum_{2^\ell>p^{5/8}}2^{-\ell}p\Big\}\\&<p^{\frac12+\varepsilon}\{p^{3/8}+(\log p)p^{3/8}+p^{3/8}\}<p^{7/8+\varepsilon}.\end{aligned}\tag{2.16}$$

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

Proof of Theorem 3.

Lemma 7 together with inclusion-exclusion argument implies that

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

Proof of Theorem 4.

If we restrict ourselves to elements $x\in G$ such that

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

we can bound

$$\sum_i a_i\Big(\frac{x}{p}\Big) \lesssim \sum_{\substack{m \text{ dyadic}\\ M<M_0}} M \sum_{\ell,\ 2^\ell<\frac{p}{M}} \ \sum_{2^{\ell-1}<k\le 2^\ell} \psi_{\frac{8}{2^\ell M}}\Big(\frac{kx}{p}\Big). \tag{2.17}$$

By Lemma 7, summing the right-hand-side of (2.17) over $x \in G$ gives

$$|G| \sum_{\substack{M \text{ dyadic}\\ M<M_0}} M \sum_{\ell,\ 2^\ell<\frac{p}{M}} 2^{\ell-1}\Big\{\int \psi_{\frac{8}{2^\ell M}} - \frac{1}{p}\Big(1-\int \psi_{\frac{8}{2^\ell M}}\Big)\Big\} + O(p^{7/8+\varepsilon}). \tag{2.18}$$

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 (2.18) together with an exclusion-inclusion argument.

References

[C]. T. W. Cusick, *Zaremba's conjecture and sums of the divisor function*, Math. Comput. Vol 61, 203, (1993), 171-176.

[GK]. M. Z. Garaev, A. A. Karatsuba, *On character sums and the exceptional set of a congruence problem*, J. Number Theory 114 (2005), 182-192.

[KN]. L. Kuipers, H. Niederreiter, *Uniform Distribution of Sequences*, New York : Wiley (1974).

[L]. G. Larcher, *On the distribution of sequences connected with good lattice points*, Monatsh. Math., Vol 101, 2, (1986), 135-150.

[RS]. A. M. Rockett, P. Szusz, *Continued Fractions*, World Scientific, (1992).

[Z1]. S. K. Zaremba, *Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.)*, Academic Press, New York, (1972), 39-119.

[Z2]. ______, *Good lattice points modulo composite numbers*, Monatsh. Math. 78 (1974), 446-460.