Number Theory

Partial quotients and equidistribution

*Fractions continues et equidistribution*

Mei-Chu Chang

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

**Article info**

**Abstract**

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

© 2011 Published by Elsevier Masson SAS on behalf of Académie des sciences.

**Résumé**

Nous obtenons des bornes en moyenne pour les quotients partiels de certaines fractions \( \frac{b}{p} \), \( p \) un nombre premier, \( b \) dans un sous-groupe de \( \left( \mathbb{Z}/p\mathbb{Z} \right)^* \) ainsi que pour \( b \) un élément primitif “typique” \( (\text{mod} \, p) \). 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 \( b^j \text{(mod} \, p) \). On en déduit, comme corollaire, de meilleures estimations sur les corrélations partielles pour ces suites.

© 2011 Published by Elsevier Masson SAS on behalf of Académie des sciences.

**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 \( \left( \mathbb{Z}/p\mathbb{Z} \right)^* \) 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

\[
\sum_{i} a_i \left( \frac{b}{p} \right) < c \log p \cdot \log \log p.
\]

1 Partially supported by NSF.

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

1631-073X/$ – see front matter © 2011 Published by Elsevier Masson SAS on behalf of Académie des sciences.

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'équi-répartition (mod 1) entraîne que

\[
D\left(\left(\frac{b^{j-1}}{N} \cdot \frac{b^j}{p} \right) : j = 1, \ldots, p-1\right) < \frac{c}{p} \log p \cdot \log \log p.
\]

1. Introduction

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

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

Denote \( \{a_i(x)\} \), the partial quotients \([a_1, a_2, \ldots] \subseteq \mathbb{Z}^+ \) of \( x \).

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

\[
\sum_i a_i\left(\frac{b}{N}\right) < c \log N \cdot \log \log N.
\]

1. Introduction

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

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

Denote \( \{a_i(x)\} \), the partial quotients \([a_1, a_2, \ldots] \subseteq \mathbb{Z}^+ \) of \( x \).

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

\[
\sum_i a_i\left(\frac{b}{N}\right) < c \log N \cdot \log \log N.
\]

1. Introduction

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

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

Denote \( \{a_i(x)\} \), the partial quotients \([a_1, a_2, \ldots] \subseteq \mathbb{Z}^+ \) of \( x \).

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

\[
\sum_i a_i\left(\frac{b}{N}\right) < c \log N \cdot \log \log N.
\]

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

\[
\sum_i a_i\left(\frac{b}{N}\right) < c \log N \cdot \log \log N.
\]

1. Introduction

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

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

Denote \( \{a_i(x)\} \), the partial quotients \([a_1, a_2, \ldots] \subseteq \mathbb{Z}^+ \) of \( x \).

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

\[
\sum_i a_i\left(\frac{b}{N}\right) < c \log N \cdot \log \log N.
\]

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

\[
\min_{(b, N) = 1} \max_i a_i\left(\frac{b}{N}\right) < c.
\]

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 \( x_1, \ldots, x_N \in [0, 1]^d \), we define the discrepancy

\[
D(x_1, \ldots, x_N) = \sup_J \left| \frac{|\{x_1, \ldots, x_N\} \cap J|}{N} - |J| \right|,
\]

where sup is taken over all boxes \( J \subseteq [0, 1]^d \).

For \( r \in \mathbb{R} \), let \( \lfloor r \rfloor \) be the greatest integer less than or equal to \( r \). We denote the fractional part \( r - \lfloor r \rfloor \) of \( r \) by \( \{r\} \).

Recall that the convergents \( \frac{p_i(x)}{q_i(x)} \) of a continued fraction \( x = [a_1, a_2, \ldots] \) is \( \frac{p_i(x)}{q_i(x)} = \frac{p_i}{q_i} = [a_1, a_2, \ldots, a_i] \), 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 \( kx, k = 1, \ldots, N \) satisfies

\[
D([x], [2x], \ldots, [Nx]) \leq \frac{c}{N} \sum_{q_i(x) < N} a_i(x).
\]

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

**Proposition A’.**

\[
D\left(\left\{\frac{b}{N} \cdot \{2b/N\} \right., \ldots, \left\{Mb/N\right\}\right) \leq \frac{c}{M} \sum_i a_i\left(\frac{b}{N}\right)
\]

for \( M \leq N \).

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

**Proposition B.**

\[
D\left(\left(\frac{k}{N}, \{kb/N\}\right): k = 1, \ldots, N\right) \leq \frac{c}{N} \sum_i a_i\left(\frac{b}{N}\right).
\]
Hence, substituting (1) in (5) and (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 \((\text{mod } N)\) and consider the sequence
\[
\left\{ \frac{b}{N} \right\}, \left\{ \frac{b^2}{N} \right\}, \ldots, \left\{ \frac{b^\tau}{N} \right\},
\]
where \( \tau = \phi(N) \) is the order of \( b \) \((\text{mod } N)\).

When examining statistical properties of (7), the two quantities studied are
\[
D\left( \left\{ \frac{b}{N} \right\}, \left\{ \frac{b^2}{N} \right\}, \ldots, \left\{ \frac{b^\tau}{N} \right\} \right) \quad (\text{equidistribution})
\]
and
\[
D := D\left( \left\{ \frac{b^k}{N} \right\} : k = 1, \ldots, p - 2 \right) = D\left( \left\{ \frac{x}{p} \right\}, \left\{ \frac{xb}{p} \right\} : x = 1, \ldots, p - 1 \right) + O(1) \frac{1}{p}
\]
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 \( b \) \((\text{mod } N)\) such that
\[
\sum_i a_i \left( \frac{b}{N} \right) < c \frac{N}{\phi(\phi(N))} \log N \cdot \log \log N.
\]
(Proposition 1)

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

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

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

Theorem 3. For most primitive elements \((\text{mod } p)\), we have \( \max a_i \left( \frac{x}{p} \right) \leq \log p \).

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

Theorem 4. Let \( G \subset \mathbb{Z}_p^* \) be a subgroup with \( |G| > p^{7/8+\epsilon} \). Then most elements \( x \in G \) satisfy
\[
\sum_i a_i \left( \frac{x}{p} \right) \leq c \log p \cdot \log \log p.
\]
Theorem 5. For most primitive elements $x$ (mod $p$), we have

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

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

$$D\left( \left\{ \frac{x}{p} : k = 1, \ldots, M \right\} \right) \lesssim \frac{c \log p \cdot \log \log p}{M},$$
$$D\left( \left( \left\{ \frac{k}{p} \right\}, \left\{ \frac{kx}{p} \right\} : k = 1, \ldots, p \right) \right) \lesssim \frac{c \log p \cdot \log \log p}{p},$$
$$D\left( \left( \left\{ \frac{x}{p} \right\}, \left\{ \frac{xk}{p} \right\} : k = 1, \ldots, p - 2 \right) \right) \lesssim \frac{c \log p \cdot \log \log p}{p}.$$

2. The proofs

Let $p$ be prime and let $G \subset \mathbb{Z}_p^*$ be a multiplicative subgroup. Denote $\psi \geq 0$ a smooth bump function, $\psi = 1$ on $[-\frac{1}{4}, \frac{1}{4}]$ and $\text{supp } \psi \subset [-\frac{1}{2}, \frac{1}{2}]$. We define $\psi_x(t) = \psi(t/2^k)$ (as a function on $\mathbb{R}$).

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

$$\psi_x(t) = \sum_j \hat{\psi}_x(j)e(jt)$$

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

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

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

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 $\psi_x$ be the bump function defined above. Then we have

$$\sum_{k \in I} \sum_{x \in G} \hat{\psi}_x\left( \frac{kx}{p} \right) = |I||G| \int \psi_x - \frac{|I||G|}{p-1} \left( 1 - \int \psi_x \right) + O(A),$$

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

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

$$|I||G| \left( \int \psi_x \right) + \sum_{k \in I} \sum_{x \neq 0} \hat{\psi}_x(j) \sum_{x \in G} e_p(jkx).$$

Using multiplicative characters

$$\chi|G| = \frac{|G|}{p-1} \sum_{x \in G} \chi(x)$$

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

$$\left| \sum_{k \in I} \sum_{x \neq 0} \hat{\psi}_x(j) \sum_{x = 1}^{p-1} e_p(jkx) \right| \leq \max_{x \neq x_0} \left| \sum_{k \in I} \sum_{x \neq x_0} \hat{\psi}_x(j) \sum_{x = 1}^{p-1} \chi(x) e_p(jkx) \right| .$$

Clearly, the first term in (18) is

$$\left| \sum_{k \in I} \sum_{x \neq 0} \hat{\psi}_x(j) \sum_{x = 1}^{p-1} e_p(jkx) \right| = - |I||G| \left( \sum_j \hat{\psi}_x(j) - \hat{\psi}_x(0) \right) + \frac{|I||G|}{p-1} \left( 1 - \int \psi_x \right) .$$
For the second term in (18), we make changes of variable in $x$ to obtain

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

where $\hat{x}$ and $\hat{k}$ denote inverses of $x$ and $k \pmod{p}$.

Also

$$\left| \sum_{j} \hat{\psi}_e(j) \chi(j) \right| \leq V \max_{j \neq j} |\sum_j \chi(j)|,$$

where $V$ is the variation of $\hat{\psi}_e(j)$ and $J$ is an interval of size $< \frac{3}{2}$.

By Cauchy–Schwarz and Plancherel,

$$V = \sum_{\ell} |\hat{\psi}_e(j) - \hat{\psi}_e(j + 1)| = \sum_{\ell} \left| \left[ \psi_e(x)(1 - e(-x)) \right] \hat{\chi}(j) \right| \leq \frac{1}{\sqrt{\epsilon}} \| \psi_e(x)(1 - e(-x)) \|_{L^2} \leq \epsilon. \tag{21}$$

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

$$\left| \sum_{a < x < a + H} \chi(x) \right| \leq \begin{cases} H & \sqrt{\epsilon} \log p \\
\frac{H^2}{\epsilon^{1/2} + 1} \epsilon^{-1/2} p \epsilon^{1/2} \leq H^{2} \epsilon^{-1/2} p \epsilon^{-1}. \end{cases} \tag{22}$$

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

Hence

$$\left(20\right) \leq \epsilon \sqrt{\epsilon} \min(|I|, \sqrt{\epsilon}, |I|^{1/2} \epsilon^{1/2}) \min\left(\frac{1}{\epsilon}, \sqrt{\epsilon}, \epsilon^{-1/2} p \epsilon^{-1}\right) p^\epsilon \tag{24}$$

proving the lemma. \qed

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

**Lemma 7’**.

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

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

$$\left| \left\{ x \in G: \max_i \left( \frac{x}{p} \right) > M \right\} \right| \leq \sum_{\ell < 2^{\ell} < p^M} \left( 2^{\ell-1} |G| \int \psi_{\ell M} \right) + O\left( \frac{|G|}{M} \right) \tag{26}$$

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

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

Hence the last sum in (26) is bounded by

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

Taking $M \geq \log p$, we conclude the proof. \qed
Proof of Theorem 3. Lemma 7 together with inclusion–exclusion argument implies that
\[
\sum_{k \in I} \sum_{x \in \mathbb{Z}_p^*} \frac{\psi \left( \frac{kx}{p} \right)}{p} = |I| \varphi(p - 1) \left\{ \int \psi \frac{1}{p - 1} \left( 1 - \int \psi \right) \right\} + O(A)^2. \tag{28}
\]

Proof of Theorem 4. If we restrict ourselves to elements \( x \in G \) such that
\[
\max \left\{ \frac{a_i}{p} \right\} < M_0,
\]
we can bound
\[
\sum a_i \left( \frac{x}{p} \right) \lesssim \sum_{\text{dyadic}} M \sum_{\ell, 2^\ell < p M < 2^{\ell-1} k < 2^\ell} \psi \left( \frac{\frac{kx}{p}}{2^\ell M} \right). \tag{29}
\]

By Lemma 7, summing the right-hand side of (29) over \( x \in G \) gives
\[
|G| \sum_{\text{dyadic}} M \sum_{M < M_0} 2^{\ell-1} \left\{ \int \psi \left( \frac{\frac{kx}{p}}{2^\ell M} \right) - \frac{1}{p} \left( 1 - \int \psi \right) \right\} + O(p^{7/8 + \varepsilon}). \tag{30}
\]
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