Uniform Distribution Theory **5** (2010), no.1, 45–52

ON LARCHER'S THEOREM CONCERNING GOOD LATTICE POINTS AND MULTIPLICATIVE SUBGROUPS MODULO p

Nikolay G. Moshchevitin — Dmitrii M. Ushanov

ABSTRACT. We prove the existence of two-dimensional good lattice points in thick multiplicative subgroups modulo p.

Communicated by Sergei Konyagin

Dedicated to the memory of Professor Edmund Hlawka

1. Introduction

Let $p \geq 3$ be a prime number. Take an integer a such that $1 \leq a \leq p-1$. Consider a sequence of points

$$\xi_x = \left(\frac{x}{p}, \left\{\frac{ax}{p}\right\}\right) \in [0,1]^2, \quad x = 0,1,2,\dots,p-1. \tag{1}$$

Let

$$N_p(\gamma_1,\gamma_2) = \#\{x : 0 \leq x < p,\ \xi_x \in [0,\gamma_1]\times[0,\gamma_2]\}$$

and let

$$D_p(a) = \sup_{\gamma_1,\ \gamma_2 \in [0,1]} |N_p(\gamma_1,\gamma_2) - \gamma_1\gamma_2 p|$$

be the discrepancy of the set (1).

In [1] G. Larcher proved a series of results on the existence of well-distributed sets of the form (1). For example, he proved the existence of $a \in [0,1,\dots,p-1]$ such that

$$D_p(a) \leq c \log p \log\log p$$

2010 Mathematics Subject Classification: 11K36.
Keywords: Good lattice points, multiplicative subgroups, characters, Burgess' inequality.
Research is supported by RFBR grant No 09-01-00371a.

with an absolute constant c.

In the present paper we generalize this result.

In the sequel $\mathbb{Z}_p^*$ denotes the multiplicative group of residues modulo p. U denotes a multiplicative subgroup of $\mathbb{Z}_p^*$ and $\|\cdot\|$ denotes the distance to the nearest integer.

For $1 \le a < p$ we need the continued fraction expansion

$$\frac{a}{p} = \cfrac{1}{b_1(a) + \cfrac{1}{b_2(a) + \cdots + \cfrac{1}{b_l(a)}}}, \quad l = l(a). \tag{2}$$

Theorem 1. *Let p be prime, U be a multiplicative subgroup in $\mathbb{Z}_p^*$. For $v \neq 0$ we consider the set $R = v \cdot U$ and let*

$$\#R \ge 10^5 p^{7/8} \log^{3/2} p.$$

Then for at least a half of elements $a \in R$ all partial quotients $b_j(a)$ in the continued fraction expansion (2) *are less than* $[16 \log p]$.

Theorem 1 improves a result from [3].

Theorem 2. *Let p be prime, U be a multiplicative subgroup in $\mathbb{Z}_p^*$. For $v \neq 0$ we consider the set $R = v \cdot U$ and let*

$$\#R \ge 10^8 p^{7/8} \log^{5/2} p.$$

Then there exists an element $a \in R$, $a/p = [b_1, b_2, \dots, b_l]$, $b_i = b_i(a)$, $l = l(a)$ with

$$\sum_{i=1}^{l} b_i \le 500 \log p \log\log p.$$

It is well known (see [4]) that

$$D_p(a) \ll \sum_{1 \le i \le l(a)} b_i(a).$$

So we immediately obtain the following

Corollary. *Under the conditions of Theorem 2 there exists an element $a \in R$ such that*

$$D_p(a) \ll \log p \log\log p.$$

We do not calculate optimal constants in our results. Of course constants 10^6 and 10^8 may be reduced.

2. Character sums

Let p be prime, $1 < t \le p$, $k = \left\lceil \sqrt{\frac{2p}{t}} \right\rceil$, $j = \lceil \log_2 \frac{p}{k} \rceil$. Define rectangles

$$\begin{aligned}
&\Pi_0 = [1,k] \times [1,k],\\
&\Pi_1 = [k+1, 2k] \times [1, k/2],\\
&\Pi_2 = [2k+1, 4k] \times [1, k/4],\\
&\cdots,\\
&\Pi_\nu = [2^{\nu-1}k+1, 2^\nu k] \times [1, k/2^\nu],\\
&\cdots;\\
&\Pi_{-1} = [1, k/2] \times [k+1, 2k],\\
&\Pi_{-2} = [1, k/4] \times [2k+1, 4k],\\
&\cdots,\\
&\Pi_{-\nu} = [1, k/2^\nu] \times [2^{\nu-1}k+1, 2^\nu k],\\
&\cdots,
\end{aligned}$$

and let $\Pi^t = \cup_{i=-j}^{j} \Pi_i$, so Π^t consists of $\le 2\log_2 p$ rectangles Π_i. It is clear that

$$\left\{(x,y) \in \mathbb{Z}^2 \mid 1 \le x < p,\ 1 \le y < p,\ xy \le p/t\right\} \subset \Pi^t. \tag{3}$$

Moreover, for different ν and μ we have

$$\Pi_\nu \cap \Pi_\mu = \varnothing.$$

Lemma 1. *Let p be prime, $c \ge 1$, $k = \sqrt{\frac{2p}{c}}$, χ be a non-principal character to prime modulo p. Then*

$$\left| \sum_{(x,u)\in\Pi^c} \chi(x)\overline{\chi(u)} \right| \le 10000 p^{\frac{7}{8}} \log^2 p/\sqrt{c}.$$

P r o o f. Dividing summation area into parts, we obtain

$$\left| \sum_{(x,u)\in\Pi^c} \chi(x)\overline{\chi(u)} \right| \le \sum_{i=-j}^{j} \left| \sum_{(x,u)\in\Pi_i} \chi(x)\overline{\chi(u)} \right|.$$

Let h denote the height of rectangle Π_i and w denote the width. Then $hw \le k^2$.

We will use following Burgess' result (see [4] for details) □

Theorem. *Let χ be a non-principal character to prime modulo. Then*

$$\left| \sum_{1\le x\le N} \chi(x) \right| \le 30 N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

Here r is an arbitrary positive integer.

Taking $r = 2$ in the Burgess' theorem we obtain

$$\left|\sum_{(x,u)\in P_i} \chi(x)\overline{\chi(u)}\right| \le 900\sqrt{hw}p^{\frac{3}{8}}\log p \le 900kp^{\frac{3}{8}}\log p = 900\sqrt{\frac{2p}{c}}p^{\frac{3}{8}}\log p.$$

Since there is only $\le 2\log_2 p$ rectangles Π_i

$$\left|\sum_{(x,u)\in\Pi^c} \chi(x)\overline{\chi(u)}\right| \le 10000p^{\frac{7}{8}}\log^2 p/\sqrt{c}$$

and the lemma follows.

3. Continued fractions

We will use two lemmas about continued fractions (see [5]).

Lemma A. *If* $\frac{p_n}{q_n} \ne \alpha$ *is the nth convergent to* α*, then*

$$\frac{1}{q_n(q_n+q_{n+1})} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}.$$

Lemma B. *If* $\alpha \in \mathbb{R}$, $\frac{a}{b} \in \mathbb{Q}, (a,b) = 1$ *and*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then $\frac{a}{b}$ *is a convergent to* α.

4. Proof of Theorem 1

Let $t = 16\log p$. Consider the sum

$$S(a) = \sum \delta_p(axy^* - 1),$$

where

$$\delta_p(x) = \begin{cases} 1, & x \equiv 0 \pmod p, \\ 0, & x \not\equiv 0 \pmod p, \end{cases}$$

$y^* \in \mathbb{Z}_p^*$ is defined from

$$yy^* \equiv 1 \pmod p,$$

and the summation is over all pairs $(x, |y|) \in \Pi^t$.

If $S(a) = 0$, then by (3) for all $1 \le x$, $1 \le |y| < p$, $x|y| \le p/t$ we have

$$ax - y \not\equiv 0 \pmod{p}.$$

Hence if

$$\begin{cases} ax - y & \equiv \ 0 \pmod{p}, \\ 1 & \le \ x \ < \ p, \\ 1 & \le \ |y| \ < \ p, \end{cases}$$

then

$$x|y| > \frac{p}{t}. \tag{4}$$

In particular (4) holds for $y = \pm \left\| \frac{ax}{p} \right\| p$. Therefore for each $1 \le x < p$ we have

$$\left\| \frac{ax}{p} \right\| > \frac{1}{xt}. \tag{5}$$

Using Lemma A we obtain

$$\left\| \frac{ax_{k-1}}{p} \right\| < \frac{1}{x_{k-1} b_k(a)}, \tag{6}$$

where x_{k-1} is the denominator of $(k-1)$th convergent to a/p. From (5) and (6) we see that $b_k(a) < t$ and all continued fraction coefficients of a/p are less than t.

Now we express $S(a)$ as a sum

$$S(a) = \frac{1}{p-1} \sum_{\chi \pmod{p}} \sum_{(x,|y|) \in \Pi^t} \chi(a)\chi(x)\overline{\chi(y)},$$

where the first summation is over all characters to modulo p. Consider the sum $S = \sum_{a \in R} S(a)$, then

$$S = \frac{\#R}{p-1} \sum_{\chi;U} \sum_{(x,|y|) \in \Pi^t} \chi(v)\chi(x)\overline{\chi(y)},$$

where $\chi; U$ denotes summation over all characters to prime modulo p trivial on U. It is now clear that

$$|S| \le \#R \frac{4p \log p}{(p-1)t} + 2 \max_{\chi \neq 1} \left| \sum_{(x,y) \in \Pi^t} \chi(x)\overline{\chi(y)} \right|.$$

Using Lemma 1 we obtain the following estimate

$$|S| \le \frac{\#R}{4} + 20000 p^{\frac{7}{8}} \log^2 p / \sqrt{t},$$

therefore

$$\frac{|S|}{\#R} < \frac{1}{2},$$

and the theorem follows.

5. Proof of Theorem 2

Let c be a positive integer. Define

$$B(c) = \left\{ (a,x) \middle| \left\| \frac{ax}{p} \right\| < \frac{1}{cx},\ a \in R,\ 1 \le x < p \right\}$$

Let $B(c,c') = B(c) \setminus B(c')$. Also we define a function $f_a(x)$ by the condition

$$f_a(x) = \begin{cases} c & \text{if } (a,x) \in B(c,c+1) \quad \text{for some } \ c \in \mathbb{N}, \\ 0, & \text{otherwise.} \end{cases}$$

Consider the sum

$$S_a = \sum_{x=1}^{p-1} f_a(x).$$

Let $f_a(x) = c$. Then

$$\frac{1}{(c+1)x} \le \left\| \frac{ax}{p} \right\| < \frac{1}{cx}.$$

If x is the denominator of some convergent to a/p, then by Lemma A

$$\frac{1}{(b_{n+1}+2)x} \le \left\| \frac{ax}{p} \right\| < \frac{1}{b_{n+1}x},$$

therefore either $b_{n+1} = c$, or $b_{n+1} = c-1$. So we see that

$$S_a \ge \sum b_i + \sum \delta_i,$$

where $\delta_i \in \{-1, 0\}$.

Therefore

$$S_a \ge \sum_{i=1}^{l} b_i - 5\log p,$$

where $5\log p$ is an upper bound for the continued fraction's length.

Let Ω be the subset in R such that all partial quotients to elements of the form a/p with $a \in \Omega$ are less than $t = [16\log p]$. Hence, by Theorem 1, $\#\Omega > \#R/2$.

Suppose that $a \in \Omega$. If $f_a(x) = c$, $c > 1$, then

$$\left\| \frac{ax}{p} \right\| < \frac{1}{cx}.$$

So there exists an element b with

$$\left| \frac{b}{x} - \frac{a}{p} \right| < \frac{1}{cx^2}.$$

By Lemma B we have that $b/x = p_\nu/q_\nu$ is a convergent to a/p. Because $q_{\nu+1} \le (b_{\nu+1}(a)+1)q_\nu$ by the left inequality from Lemma A we see that

$$\frac{1}{q_\nu^2(b_{\nu+1}(a)+2)} \le \frac{1}{q_\nu(q_\nu+q_{\nu+1})} \le \left|\frac{p_\nu}{q_\nu} - \frac{a}{p}\right| = \left|\frac{b}{x} - \frac{a}{p}\right| < \frac{1}{cx^2} \le \frac{1}{cq_\nu^2}.$$

So $c < b_{\nu+1}(a) + 2$ for some ν. It follows that $c \le b_{\nu+1}(a)+1$. As $b_{\nu+1}(a) < t$ we see that $c \le t$. So if $a \in \Omega$, then $f_a(x) \le t$. Hence by the partial summation

$$\sum_{a\in\Omega} S_a \le \sum_{c\le t} c \cdot \#B(c, c+1) \le \sum_{c \le t} \#B(c).$$

Let us estimate $\#B(c)$.

It is clear that

$$\begin{aligned} \#B(c) &\le 2\cdot\#\left\{(b,x) \mid b < \frac{p}{cx}, b \in x\cdot R\right\} \\ &\le 2\cdot\#\left\{(b,x)\in\Pi^c \mid b\in x\cdot R\right\} \\ &= 2\frac{\#R}{p-1}\sum_{\chi;U}\sum_{(x,u)\in\Pi^c}\chi(v)\chi(u)\overline{\chi(x)}, \end{aligned} \tag{7}$$

where the $\sum_{\chi;U}$ denotes the summation over characters χ trivial on U.

Note $\#U|(p-1)$ and there exist exactly $(p-1)/\#U$ trivial on U characters. Thus

$$\#B(c) \le 2\frac{\#R}{p-1}\#\Pi^c + 4\max_\chi\left|\sum_{(x,u)\in\Pi^c}\chi(u)\overline{\chi(x)}\right|,$$

where maximum is taken over all non-principal characters to modulo p. We can now use Lemma 1 to obtain an estimate

$$\#B(c) \le 4\frac{\#R}{p-1}\frac{p}{c}\log p + 40000 p^{\frac{7}{8}}\log^2 p/\sqrt{c}.$$

Therefore

$$\sum_{a\in\Omega} S_a \le 190\cdot\#R\log p\log\log p + 8\cdot 10^6 p^{7/8}\log^{5/2} p.$$

Dividing by $\#\Omega > \#R/2$ we get

$$\frac{1}{\#\Omega}\sum_{a\in\Omega} S_a \le 400\log p\log\log p$$

because of $\#R \ge 10^8 p^{7/8}\log^{5/2} p$. Hence there exists an element a in Ω such that $S_a \le 400\log p\log\log p$. Therefore there exists an element a in Ω such that

$$\sum b_i(a) \le 500\log p\log\log p.$$

Theorem 2 is proved.

Acknowledgement. The authors are grateful to Professor Sergei V. Konyagin for pointing out an opportunity of improvement of Lemma 1 and hence the main result of the paper. The authors are also grateful to the referee for several useful suggestions.

REFERENCES

[1] LARCHER, G.: *On the distribution of sequences connected with good lattice points.* Monatsh. Math. **101** (1986), no. 2, 135–150.

[2] IVANIEC, H.–KOWALSKI, E.: *Analytic Number Theory*. Amer. Math. Soc. Colloq. Publ. **53**, AMS, Providence, RI, 2004.

[3] MOSHCHEVITIN, N.G.: *Sets of the form* $\mathcal{A} + \mathcal{B}$ *and finite continued fractions*, Sb. Math. **198** (2007), no. 3–4, 537–557.

[4] KUIPERS, L.–NIEDERREITER, H.: *Uniform Distribution of Sequences*. Pure Appl. Math., Willey-Interscience [John Wiley & sons], New York, 1974.

[5] KHINCHIN, A.: *Continued Fractions*, Dover Publications, Mineola, NY, 1997.

Received June 21, 2009
Accepted December 17, 2009

Nikolay G. Moshchevitin
Dmitrii M. Ushanov
Department of Number Theory
Moscow State University
Vorobinovy Gory
Moscow 119992
Russia
E-mail: moshchevitin@rambler.ru
ushanov.dmitry@gmail.com