IJMMS 2003:50, 3189–3194
PII. S0161171203206074
http://ijmms.hindawi.com

DISTRIBUTION OF SPECIAL SEQUENCES MODULO A LARGE PRIME

M. Z. GARAEV and KA-LAM KUEH

Received 18 June 2002

We study the sets $\{g^x - g^y \pmod{p} : 1 \le x,\ y \le N\}$ and $\{xy : 1 \le x,\ y \le N\}$ where p is a large prime number, g is a primitive root, and $p^{2/3} < N < p$.

2000 Mathematics Subject Classification: 11A07.

1. Introduction. Let p be a large prime number, g a primitive root $(\bmod p)$, and N a given positive integer, $N < p$. In a series of papers, the distribution of powers $g^n \pmod{p}$ has been investigated by [1, 2, 4, 5]. Vâjâitu and Zaharescu [5] considered the question of A. Odlyzko concerning the set of differences

$$A := \{g^x - g^y \pmod{p} : 1 \le x,\ y \le N\}. \tag{1.1}$$

As it was indicated in [5], A. Odlyzko asks for which values of N the set A contains all residue classes $(\bmod p)$. The conjecture is that one can take N to be as small as $p^{1/2+\varepsilon}$, for any positive ε and $p > c$ with some $c = c(\varepsilon)$. From the result of Rudnick and Zaharescu [4] it follows that in Odlyzko's problem one can take $N = c_0 p^{3/4} \log p$ for some absolute constant c_0.

One of the main results of [5] is that for the exceptional set of Odlyzko's problem we have

$$\#\{h \pmod{p} : h \notin A\} \ll \frac{p^3 \log p}{N^3}. \tag{1.2}$$

It then follows that for $N > p^{2/3+\varepsilon}$ almost all the residues $(\bmod p)$ belong to A.

Denote

$$B = \{xy \pmod{p} : 1 \le x,\ y \le N\}. \tag{1.3}$$

Vâjâitu and Zaharescu [5] put another problem similar to that of Odlyzko: for which values of N can we be sure that the set B contains all residue classes $(\bmod p)$? They conjectured that N can be taken to be as small as $p^{1/2+\varepsilon}$ and observed that one can take $N = c_1 p^{3/4}\log p$. This problem is also related to the pair correlation problem for sequences of the form $\alpha n^2 \pmod 1$. For this account, see Rudnick et al. [3].

In this paper, using an elementary approach we slightly improve by a factor of $\log p$ estimate (1.2) and the estimate for N in Odlyzko's problem and obtain estimate (1.2) with the set B instead of A, see Theorems 1.1, 1.2, and 1.3.

Theorem 1.1. *For any prime number p, any primitive root $g \pmod p$, and $N = 10p^{3/4}$, the set A contains the complete residue system $\pmod p$.*

Theorem 1.2. *For any prime number p, any primitive root $g \pmod p$, and any positive integer $N < p$,*

$$\#\{h \pmod p : h \notin A\} \ll \frac{p^3}{N^3}. \tag{1.4}$$

Theorem 1.3. *For any prime number p and any positive integer $N < p$,*

$$\#\{h \pmod p : h \notin B\} \ll \frac{p^3 \log p}{N^3}. \tag{1.5}$$

We require the following lemma (see [6, Exercise 14, page 92] and the solution in [6, page 142]) which will be used in the proof of Theorems 1.1 and 1.2.

Lemma 1.4. *Let $m > 1$, $(a,m) = 1$. Then*

$$\left|\sum_{x=0}^{m-1}\sum_{y=0}^{m-1} \nu(x)\varrho(y)e^{2\pi i(axy/m)}\right| \le \sqrt{mXY}, \tag{1.6}$$

where $\nu(x)$, $\varrho(y)$ are complex numbers and

$$\sum_{x=0}^{m-1} |\nu(x)|^2 = X, \qquad \sum_{y=0}^{m-1} |\varrho(y)|^2 = Y. \tag{1.7}$$

2. Proof of Theorem 1.1. Note that $0 \in A$. Let h be any integer, $h \not\equiv 0 \pmod p$, $N = 10p^{3/4}$, and denote $N_1 = [N/4]$. Our aim is to prove that $J > 0$, where J is the number of solutions in integers x, y, z, and t of the congruence equation

$$g^{x+z} - g^y - hg^t \equiv 0 \pmod p \tag{2.1}$$

subject to the condition

$$N_1 + 1 \le x, y, z \le 2N_1, \quad 1 \le t \le N_1. \tag{2.2}$$

In order to prove it we write J in terms of rational trigonometric sums:

$$pJ = \sum_{a=0}^{p-1}\sum_{x=N_1+1}^{2N_1}\sum_{y=N_1+1}^{2N_1}\sum_{z=N_1+1}^{2N_1}\sum_{t=1}^{N_1} e^{2\pi i(a(g^{x+z}-g^y-hg^t)/p)}. \tag{2.3}$$

Picking up the term with $a = 0$ and estimating other terms by their absolute values, we obtain

$$pJ \geq N_1^4 - \sum_{a=1}^{p-1} \left| \sum_{x=N_1+1}^{2N_1} \sum_{z=N_1+1}^{2N_1} e^{2\pi i (a g^x g^z / p)} \right| \times \left| \sum_{y=N_1+1}^{2N_1} e^{2\pi i (a g^y / p)} \right| \left| \sum_{t=1}^{N_1} e^{2\pi i (a h g^t / p)} \right|. \tag{2.4}$$

We will apply Lemma 1.4 to the double inner sum. To do that, we define $\nu(u) = \varrho(u) = 1$ if $u \equiv g^x (\bmod p)$ for some $N_1 + 1 \leq x \leq 2N_1$. For all other u, we put $\nu(u) = \varrho(u) = 0$. Then Lemma 1.4 gives

$$\left| \sum_{x=N_1+1}^{2N_1} \sum_{z=N_1+1}^{2N_1} e^{2\pi i (a g^x g^z / p)} \right| \leq \sqrt{p N_1^2}. \tag{2.5}$$

Hence,

$$pJ \geq N_1^4 - \sqrt{p N_1^2} \sum_{a=0}^{p-1} \left| \sum_{y=N_1+1}^{2N_1} e^{2\pi i (a g^y / p)} \right| \left| \sum_{t=0}^{N_1} e^{2\pi i (a h g^t / p)} \right|. \tag{2.6}$$

For the sum over a, we apply Cauchy inequality. Since g is a primitive root, then

$$\sum_{a=0}^{p-1} \left| \sum_{y=N_1+1}^{2N_1} e^{2\pi i (a g^y / p)} \right|^2 = p N_1, \qquad \sum_{a=0}^{p-1} \left| \sum_{t=1}^{N_1} e^{2\pi i (a h g^t / p)} \right|^2 = p N_1. \tag{2.7}$$

Therefore, for each integer h,

$$pJ > N_1^4 - p^{3/2} N_1^2 \tag{2.8}$$

and Theorem 1.1 follows in view of $N_1 = [N/4]$.

3. Proof of Theorem 1.2. Denote $\overline{A} = \{h (\bmod p) : h \notin A\}$, $N_1 = [N/2]$, and let $|\overline{A}|$ denote the cardinality of $\overline{A}$. Then

$$\sum_{h \in \overline{A}} \sum_{a=0}^{p-1} \sum_{x=1}^{N_1} \sum_{z=1}^{N_1} \sum_{y=1}^{N} e^{2\pi i (a (g^{x+z} - g^y - h) / p)} = 0. \tag{3.1}$$

Picking up the term with $a = 0$, we obtain

$$N_1^2 N |\overline{A}| \leq \sum_{a=1}^{p-1} \left| \sum_{x=1}^{N_1} \sum_{z=1}^{N_1} e^{2\pi i (a g^x g^z / p)} \right| \left| \sum_{y=1}^{N} e^{2\pi i (a g^y / p)} \right| \left| \sum_{h \in \overline{A}} e^{2\pi i (a h / p)} \right|. \tag{3.2}$$

We will apply Lemma 1.4 to the double inner sum in the same way as we did in the proof of Theorem 1.1. We obtain

$$\left|\sum_{x=1}^{N_1}\sum_{z=1}^{N_1} e^{2\pi i(ag^x g^z/p)}\right| \le \sqrt{pN_1^2}. \tag{3.3}$$

Hence,

$$N_1^2 N|\overline{A}| \le \sqrt{pN_1^2}\sum_{a=0}^{p-1}\left|\sum_{y=1}^{N} e^{2\pi i(ag^y/p)}\right|\left|\sum_{h\in\overline{A}} e^{2\pi i(ah/p)}\right|. \tag{3.4}$$

In analogy with Section 2, we apply Cauchy inequality to the sum over a. Since

$$\begin{aligned}\sum_{a=0}^{p-1}\left|\sum_{y=1}^{N} e^{2\pi i(ag^y/p)}\right|^2 &= pN,\\ \sum_{a=0}^{p-1}\left|\sum_{h\in\overline{A}} e^{2\pi i(ah/p)}\right|^2 &= p|\overline{A}|,\end{aligned} \tag{3.5}$$

then

$$N_1^2 N|\overline{A}| \le \sqrt{pN_1^2 pNp|\overline{A}|}. \tag{3.6}$$

Hence, from $N_1 = [N/2]$, we obtain

$$|\overline{A}| \le \frac{10p^3}{N^3}. \tag{3.7}$$

This proves Theorem 1.2.

4. Proof of Theorem 1.3.

Using Gauss method of estimation of trigonometric sums, one can prove the validity of the following lemma.

Lemma 4.1. *Let $1 \le N \le p$, $(a,p) = 1$. Then*

$$\left|\sum_{x=1}^{N} e^{2\pi i(ax^2/p)}\right| \ll \sqrt{p\log p}. \tag{4.1}$$

Indeed, if we denote by $|S|$ the value of the left-hand side, then

$$|S|^2 = \sum_{x=1}^{N}\sum_{y=1}^{N} e^{2\pi i(a(y^2-x^2)/p)} \le N + 2\left|\sum_{1\le x<y\le N} e^{2\pi i(a(y^2-x^2)/p)}\right|. \tag{4.2}$$

Substituting $y = x+t$ gives

$$|S|^2 \ll N + \left|\sum_{x=1}^{N-1}\sum_{t=1}^{N-x} e^{2\pi i(at^2+2atx/p)}\right|. \tag{4.3}$$

Changing the order of summation, we obtain

$$|S|^2 \ll N + \sum_{t=1}^{N-1} \left| \sum_{x=1}^{N-t} e^{2\pi i(2atx/p)} \right| \ll N + \sum_{t=1}^{p-1} \frac{1}{|\sin(\pi 2at/p)|}. \tag{4.4}$$

When t runs through reduced residue system $(\bmod p)$ so does $2at$. Hence,

$$|S|^2 \ll N + \sum_{t=1}^{p-1} \frac{1}{|\sin(\pi t/p)|} \ll N + \sum_{t=1}^{(p-1)/2} \frac{1}{t/p} \ll p \log p. \tag{4.5}$$

We now proceed to prove Theorem 1.3. Put $N_1 = [N/4]$ and denote by B_1 the set

$$B_1 = \{x^2 - y^2 (\bmod p),\ N_1 \le x \le 2N_1,\ 1 \le y < N_1\}. \tag{4.6}$$

Since $B_1 \subset B$, then $|\overline{B}| \le |\overline{B_1}|$ where $\overline{B}$ and $\overline{B}_1$ denote the complement of B and B_1 in the complete residue system $(\bmod p)$, accordingly. Now, as in the proof of Theorem 1.2, we have

$$\sum_{h \in \overline{B_1}} \sum_{a=0}^{p-1} \sum_{x=N_1}^{2N_1} \sum_{y=1}^{N_1-1} e^{2\pi i(a(x^2-y^2-h)/p)} = 0. \tag{4.7}$$

Then it follows that

$$N^2 |\overline{B_1}| \ll \sum_{a=1}^{p-1} \left| \sum_{x=N_1}^{2N_1} e^{2\pi i(ax^2/p)} \right| \left| \sum_{y=1}^{N_1-1} e^{2\pi i(ay^2/p)} \right| \left| \sum_{h \in \overline{B_1}} e^{2\pi i(ah/p)} \right|. \tag{4.8}$$

Now, apply Lemma 4.1 for the sum over x and then use Cauchy inequality as we did in the proof of Theorems 1.1 and 1.2. Then, we obtain

$$N^2 |\overline{B_1}| \ll \sqrt{p \log p} \sqrt{pNp |\overline{B_1}|} \tag{4.9}$$

whence, we get

$$|\overline{B_1}| \ll \frac{p^3 \log p}{N^3}. \tag{4.10}$$

Now, Theorem 1.3 follows from $|\overline{B}| \le |\overline{B_1}|$.

Acknowledgment. This paper is supported by the NSC Grant 91-2115-M-001-020.

References

[1] C. I. Cobeli, S. M. Gonek, and A. Zaharescu, *On the distribution of small powers of a primitive root*, J. Number Theory **88** (2001), no. 1, 49–58.

[2] H. L. Montgomery, *Distribution of small powers of a primitive root*, Advances in Number Theory (Kingston, Ontario, 1991), Oxford Sci. Publ., Oxford University Press, New York, 1993, pp. 137–149.

[3] Z. Rudnick, P. Sarnak, and A. Zaharescu, *The distribution of spacings between the fractional parts of $n^2\alpha$*, Invent. Math. **145** (2001), no. 1, 37–57.

[4] Z. Rudnick and A. Zaharescu, *The distribution of spacings between small powers of a primitive root*, Israel J. Math. **120** (2000), 271–287.

[5] M. Vâjâitu and A. Zaharescu, *Differences between powers of a primitive root*, Int. J. Math. Math. Sci. **29** (2002), no. 6, 325–331.

[6] I. M. Vinogradov, *An Introduction to the Theory of Numbers*, Pergamon Press, London, 1955.

M. Z. Garaev: Institute of Mathematics, Academia Sinica, Nankang, Taipei 11529, Taiwan

E-mail address: garaev@math.sinica.edu.tw

Ka-Lam Kueh: Institute of Mathematics, Academia Sinica, Nankang, Taipei 11529, Taiwan

E-mail address: maklk@ccvax.sinica.edu.tw