MANY INTEGERS HAVING SMALL DIFFERENCES UNDER PRIME MODULI

Yaming LU and Yuan YI

(Received 3 April 2014)

Abstract. In this paper, we study the distribution behavior of integer n -tuples $(a_1, \dots, a_n)$ satisfying $a_1 \cdots a_n \equiv 1 \pmod{p}$ and $|a_i - a_j| \leq A$ (for all i, j), an asymptotic formula will be given for the corresponding counting function.

1. Introduction

Let p be an odd prime. For integer tuple $(a_1, \dots, a_n)$ with $a_1 \cdots a_n \equiv 1 \pmod{p}$, the components can be seen as eigenvalues of matrix on $\mathbb{Z}_p$ with determinate 1. It is interesting to ask the distribution behavior of such eigenvalues that any two of them having small differences. In this paper, we will study this problem by considering the following counting function:

$$S_n(A, p) = \sum_{\substack{a_1 < p \\ a_1 \cdots a_n \equiv 1 \pmod{p}}} \cdots \sum_{\substack{a_n < p \\ |a_i - a_j| \leq A, \forall i, j}} 1, \quad (1.1)$$

where A is a real number smaller than p . For the case $n = 2$, it is just the problem of counting integers having small difference with its multiple inverse mod p , and Zhang [5] gave

$$S_2(\eta p, p) = \eta(2 - \eta)p + O(p^{1/2} \log^2 p) \quad (1.2)$$

with $\eta \in (0, 1)$. (Actually, he obtained a result corresponding to modulo q with $q > 2$ an arbitrary integer.) Using Zhang's method, Xu and Yi [4] generalized the above result and considered the case of short interval, they produced an asymptotic formula for

$$\#\{a : 1 \leq a \leq \xi q, (a, q) = 1, |a - \bar{a}| \leq \eta q\},$$

where $0 < \xi, \eta < 1$ and $\bar{a}$ is the multiple inverse of a modulo q . However, it seems that their method can hardly be used to attack $S_n(A, p)$ for larger n , and this task is exactly what we want to achieve in this paper. We have the following result.

THEOREM 1.1. *Let p be an odd prime, A be a positive real number smaller than p . Then for any integer $n \geq 2$,*

$$S_n(A, p) = \left(n - (n-1) \frac{A}{p}\right) A^{n-1} + O(p^{(n-1)/2} (\log p)^{2n-2} + p^{n-2}),$$

where the O -constant depends only on n .

Note that (1.2) is a simple consequence of Theorem 1.1.

2010 Mathematics Subject Classification: Primary 11N69.

Keywords: n -tuples; small differences; asymptotic formula.

Notation. In this paper, we write $e(x) = e^{2\pi ix}$ as usual. Here $G(m, \chi)$ is the Gauss sum corresponding to Dirichlet character $\chi \pmod{q}$, that is,

$$G(m, \chi) = \sum_{j=1}^q \chi(j) e\left(\frac{mj}{q}\right).$$

For real number x , we write $\|x\|$ as the distance of x from the nearest integer.

2. Basic treatment

The total contribution of the terms that there are at least two equal variables in the summation of (1.1) is $O(p^{n-2})$, therefore

$$\begin{aligned} S_n(A, p) &= \sum_{\substack{a_1 < p \\ a_1 \cdots a_n \equiv 1 \pmod{p} \\ 0 < |a_i - a_j| \leq A, \forall i, j}} \cdots \sum_{\substack{a_n < p \\ a_n < p \\ a_1 < a_2 < \cdots < a_n \leq a_1 + A}} 1 + O(p^{n-2}) = n! \sum_{\substack{a_1 < p \\ a_1 \cdots a_n \equiv 1 \pmod{p} \\ a_1 < a_2 < \cdots < a_n \leq a_1 + A}} \cdots \sum_{\substack{a_n < p \\ a_n < p \\ a_1 < a_2 < \cdots < a_n \leq a_1 + A}} 1 + O(p^{n-2}) \\ &= n! \sum_{\substack{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A \\ a(a+l_1) \cdots (a+l_{n-1}) \equiv 1 \pmod{p}}} \cdots \sum_{\substack{a \leq p-l_{n-1} \\ a \leq p-l_{n-1} \\ a(a+l_1) \cdots (a+l_{n-1}) \equiv 1 \pmod{p}}} 1 + O(p^{n-2}). \end{aligned}$$

The orthogonality of Dirichlet character implies

$$\begin{aligned} S_n(A, p) &= \frac{n!}{p-1} \sum_{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A} \cdots \sum_{\substack{a \leq p-l_{n-1} \\ a \leq p-l_{n-1} \\ a(a+l_1) \cdots (a+l_{n-1}) \equiv 1 \pmod{p}}} \sum_{\chi \pmod{p}} \chi(a) \chi(a+l_1) \cdots \chi(a+l_{n-1}) \\ &\quad + O(p^{n-2}). \end{aligned}$$

We denote by $M_n(A, p)$ the sum of terms corresponding to the principal character and

$$E_n(A, p) = \frac{n!}{p-1} \sum_{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A} \cdots \sum_{\substack{a \leq p-l_{n-1} \\ a \leq p-l_{n-1} \\ a(a+l_1) \cdots (a+l_{n-1}) \equiv 1 \pmod{p}}} \sum_{\chi \neq \chi^0} \chi(a) \chi(a+l_1) \cdots \chi(a+l_{n-1}), \quad (2.1)$$

then

$$S_n(A, p) = M_n(A, p) + E_n(A, p) + O(p^{n-2}). \quad (2.2)$$

In the following sections, we shall evaluate $M_n(A, p)$ as the main term and estimate $E_n(A, p)$ as the remainder term.

3. Evaluation of the main term

We begin with a lemma.

LEMMA 3.1. For $\alpha \geq 0$ write

$$T_\alpha(n) = \sum_{1 \leq l_1 < l_2 < \cdots < l_n \leq A} l_n^\alpha. \quad (3.1)$$

Then

$$T_\alpha(n) = A^{\alpha+n} \sum_{j=1}^n \frac{(-1)^{j+1}}{(\alpha+1)(\alpha+2) \cdots (\alpha+j) \cdot (n-j)!} + O(A^{\alpha+n-1}),$$

where the O -constant depends on n and α .

Proof. It is obvious that

$$\begin{aligned} T_\alpha(n) &= \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} \sum_{l_{n-1} < l_n \leq A} l_n^\alpha \\ &= \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} \left\{ \frac{1}{\alpha+1} (A^{\alpha+1} - l_{n-1}^{\alpha+1}) + O(A^\alpha) \right\} \\ &= \frac{A^{\alpha+1}}{\alpha+1} T_0(n-1) - \frac{1}{\alpha+1} T_{\alpha+1}(n-1) + O(A^{\alpha+n-1}). \end{aligned}$$

After $n-1$ iterations we arrive at

$$\begin{aligned} T_\alpha(n) &= \sum_{j=1}^{n-1} \frac{(-1)^{j+1} A^{\alpha+j}}{(\alpha+1) \dots (\alpha+j)} T_0(n-j) + \frac{(-1)^{n+1}}{(\alpha+1) \dots (\alpha+n-1)} T_{\alpha+n-1}(1) \\ &\quad + O(A^{\alpha+n-1}). \end{aligned}$$

Note that

$$T_0(n-j) = \frac{1}{(n-j)!} \left(\sum_{l \leq A} 1 \right)^{n-j} + O(A^{n-j-1}) = \frac{A^{n-j}}{(n-j)!} + O(A^{n-j-1})$$

and

$$T_{\alpha+n-1}(1) = \frac{A^{\alpha+n}}{\alpha+n} + O(A^{\alpha+n-1}),$$

the desired result is obtained. $\square$

Now we come to calculate $M_n(A, p)$:

$$\begin{aligned} M_n(A, p) &= \frac{n!}{p-1} \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} \sum_{a \leq p-l_{n-1}} 1 \\ &= \frac{n!}{p-1} \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} (p - l_{n-1}) = \frac{n!}{p-1} (p T_0(n-1) - T_1(n-1)). \end{aligned}$$

Since $T_0(n-1) = A^{n-1}/(n-1)! + O(A^{n-2})$ and from Lemma 3.1 we know that

$$\begin{aligned} T_1(n-1) &= A^n \sum_{j=1}^{n-1} \frac{(-1)^{j+1}}{(j+1)!(n-j-1)!} + O(A^{n-1}) \\ &= \frac{A^n}{n!} \sum_{j=1}^{n-1} (-1)^{j+1} \binom{n}{j+1} + O(A^{n-1}) = \frac{n-1}{n!} A^n + O(A^{n-1}), \end{aligned}$$

whence

$$\begin{aligned} M_n(A, p) &= \frac{n!}{p-1} \left\{ p \left(\frac{A^{n-1}}{(n-1)!} + O(A^{n-2}) \right) - \left(\frac{(n-1)}{n!} A^n + O(A^{n-1}) \right) \right\} \\ &= \frac{A^{n-1}}{p-1} (np - (n-1)A) + O(A^{n-2}) \\ &= \left(n - (n-1) \frac{A}{p} \right) A^{n-1} + O(A^{n-2}). \end{aligned} \tag{3.2}$$

Next we shall estimate $E_n(A, p)$, for this purpose we need some tools of Gauss sum and hyper-Kloosterman sum.

4. Hyper-Kloosterman sum and Gauss sum

For hyper-Kloosterman sum we means the exponential sum of the following type:

$$\text{Kl}_n(p) = \sum_{x_1 \leq p-1} \cdots \sum_{x_n \leq p-1} e\left(\frac{x_1 + \cdots + x_n + \overline{zx_1 \cdots x_n}}{p}\right),$$

was introduced by Mordell, where $(z, p) = 1$ and $\overline{zx_1 \cdots x_n}$ is the multiple inverse of $x_1 \cdots x_n$ modulo p . Deligne [1] gave the optimal bound for hyper-Kloosterman sum:

$$|\text{Kl}_n(p)| \leq (n+1)p^{n/2}. \quad (4.1)$$

From this inequality we may deduce the following result.

LEMMA 4.1. Suppose $n \geq 2$, and let $k_0, \dots, k_{n-1}$ be integers satisfying $p \nmid k_0 \cdots k_{n-1}$. Then

$$\sum_{\substack{\chi \bmod p \\ \chi \neq \chi^0}} G(k_0, \chi) \cdots G(k_{n-1}, \chi) \ll p^{(n+1)/2},$$

where the implied constant depends on n .

Proof. We have

$$\begin{aligned} & \sum_{\chi \bmod p} G(k_0, \chi) \cdots G(k_{n-1}, \chi) \\ &= \sum_{\chi \bmod p} \sum_{j_0 \leq p-1} \chi(j_0) e\left(\frac{k_0 j_0}{p}\right) \cdots \sum_{j_{n-1} \leq p-1} \chi(j_{n-1}) e\left(\frac{k_{n-1} j_{n-1}}{p}\right) \\ &= \sum_{j_0 \leq p-1} \cdots \sum_{j_{n-1} \leq p-1} e\left(\frac{k_0 j_0 + \cdots + k_{n-1} j_{n-1}}{p}\right) \sum_{\chi \bmod p} \chi(j_0 \cdots j_{n-1}) \\ &= (p-1) \sum_{j_0 \leq p-1} \cdots \sum_{j_{n-2} \leq p-1} e\left(\frac{k_0 j_0 + \cdots + k_{n-1} \overline{j_0 \cdots j_{n-2}}}{p}\right), \end{aligned}$$

so it follows from (4.1) that

$$\sum_{\chi \bmod p} G(k_0, \chi) \cdots G(k_{n-1}, \chi) \ll p^{(n+1)/2}.$$

The lemma is obtained by remarking that $G(k_0, \chi^0) \cdots G(k_{n-1}, \chi^0) = (-1)^n$. $\square$

5. Estimation of $E_n(A, p)$

Before we begin to calculate $E_n(A, p)$, we introduce two auxiliary lemmas.

LEMMA 5.1. Assume that U is a positive real number, K is a positive integer and that α and β are two real numbers. If

$$\alpha = \frac{s}{r} + \frac{\theta}{r^2}, \quad (r, s) = 1, \quad r \geq 1, \quad |\theta| \leq 1,$$

then

$$\sum_{k \leq K} \min\left(U, \frac{1}{\|\alpha k + \beta\|}\right) \ll \left(\frac{K}{r} + 1\right)(U + r \log r).$$

Proof. The proof is analogous to that given for Lemma 4.11 in [3]. $\square$

LEMMA 5.2. (Truncated Perron's formula) Suppose $\rho, \gamma > 0, \rho \neq \gamma, T \geq 1$. Then

$$\frac{1}{\pi} \int_{-T}^T e^{i\gamma t} \frac{\sin(\rho t)}{t} dt = \delta + O\left(\frac{1}{T|\rho - \gamma|}\right),$$

where

$$\delta = \begin{cases} 0 & \text{if } \gamma > \rho, \\ 1 & \text{if } \gamma < \rho. \end{cases} \quad (5.1)$$

Proof. This is Lemma 2.2 of [2]. $\square$

From the definition of Gauss sum we know that for $\chi \neq \chi^0$,

$$\chi(m) = \frac{1}{p} \sum_{k \leq p-1} G(k, \chi) e\left(-\frac{mk}{p}\right).$$

Therefore,

$$\begin{aligned} E_n(A, p) &= \frac{n!}{p-1} \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} \sum_{a \leq p-l_{n-1}} \sum_{\chi \neq \chi^0} \left\{ \frac{1}{p} \sum_{k_0=1}^{p-1} G(k_0, \chi) e\left(-\frac{ak_0}{p}\right) \right\} \\ &\quad \times \left\{ \frac{1}{p} \sum_{k_1=1}^{p-1} G(k_1, \chi) e\left(-\frac{(a+l_1)k_1}{p}\right) \right\} \times \dots \\ &\quad \times \left\{ \frac{1}{p} \sum_{k_{n-1}=1}^{p-1} G(k_{n-1}, \chi) e\left(-\frac{(a+l_{n-1})k_{n-1}}{p}\right) \right\} \\ &= \frac{n!}{(p-1)p^n} \sum_{k_0=1}^{p-1} \sum_{k_1=1}^{p-1} \dots \sum_{k_{n-1}=1}^{p-1} \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} \dots \sum \\ &\quad \times e\left(-\frac{k_1 l_1 + \dots + k_{n-1} l_{n-1}}{p}\right) \\ &\quad \times \sum_{a \leq p-l_{n-1}} e\left(-\frac{k_0 + k_1 + \dots + k_{n-1}}{p} a\right) \sum_{\chi \neq \chi^0} G(k_0, \chi) \dots G(k_{n-1}, \chi), \end{aligned}$$

Lemma 4.1 implies that

$$\begin{aligned} E_n(A, p) &\ll p^{-(n+1)/2} \sum_{k_0=1}^{p-1} \sum_{k_1=1}^{p-1} \dots \sum_{k_{n-1}=1}^{p-1} \left| \sum_{1 \leq l_1 < l_2 < \dots < l_{n-1} \leq A} \dots \sum e\left(-\frac{k_1 l_1 + \dots + k_{n-1} l_{n-1}}{p}\right) \right| \\ &\quad \times \sum_{a \leq p-l_{n-1}} e\left(-\frac{k_0 + k_1 + \dots + k_{n-1}}{p} a\right) \left| \right| \end{aligned}$$

$$= p^{-(n+1)/2} \sum_{d=0}^{p-1} \sum_{k_1=1}^{p-1} \cdots \sum_{k_{n-1}=1}^{p-1} \left| \sum_{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A} e\left(-\frac{k_1 l_1 + \cdots + k_{n-1} l_{n-1}}{p}\right) \right. \\ \left. \times \sum_{a \leq p-l_{n-1}} e\left(-\frac{d}{p}a\right) \right|.$$

We denote by E' the sum of terms corresponding to $d = 0$ and E'' the others, then

$$E_n(A, p) \ll p^{-(n+1)/2} (E' + E''). \quad (5.2)$$

We estimate E' first:

$$E' = \sum_{k_1=1}^{p-1} \cdots \sum_{k_{n-1}=1}^{p-1} \left| \sum_{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A} (p - l_{n-1}) e\left(-\frac{k_1 l_1 + \cdots + k_{n-1} l_{n-1}}{p}\right) \right|.$$

In order to given a proper upper bound for E' , we need to remove the cross-conditions between l_j s in the inner sum. Write $T = p^{2n}$, $\mathcal{J} = [-T, T] \setminus [-1/T, 1/T]$, then from Lemma 5.2 we know that

$$\frac{1}{\pi} \int_{\mathcal{J}} e^{i\gamma t} \frac{\sin(\rho t)}{t} dt = \delta + O\left(\frac{1}{T|\rho - \gamma|} + \frac{1}{T}\right)$$

with δ given in (5.1). We now use the above formula with $\gamma = l_j + \frac{1}{2}$ and $\rho = l_{j+1}$ for $1 \leq j \leq n-2$, thus

$$E' = \frac{1}{\pi^{n-2}} \sum_{k_1=1}^{p-1} \cdots \sum_{k_{n-1}=1}^{p-1} \left| \sum_{l_1 \leq A} \cdots \sum_{l_{n-1} \leq A} (p - l_{n-1}) e\left(-\frac{k_1 l_1 + \cdots + k_{n-1} l_{n-1}}{p}\right) \right. \\ \left. \times \prod_{j=1}^{n-2} \left(\int_{\mathcal{J}} e^{i(l_j + \frac{1}{2})t_j} \frac{\sin(l_{j+1}t_j)}{t_j} dt_j + O(T^{-1}) \right) \right| \\ \ll \int_{\mathcal{J}} \cdots \int_{\mathcal{J}} \frac{1}{|t_1 \cdots t_{n-2}|} \sum_{k_1=1}^{p-1} \left| \sum_{l_1 \leq A} e\left(\left(-\frac{k_1}{p} + \frac{t_1}{2\pi}\right)l_1\right) \right| \\ \times \prod_{j=2}^{n-2} \left\{ \sum_{k_j=1}^{p-1} \left| \sum_{l_j \leq A} e\left(\left(-\frac{k_j}{p} + \frac{t_j}{2\pi}\right)l_j\right) \sin(l_j t_{j-1}) \right| \right\} \\ \times \sum_{k_{n-1}=1}^{p-1} \left| \sum_{l_{n-1} \leq A} (p - l_{n-1}) e\left(\left(-\frac{k_{n-1}}{p} + \frac{t_{n-1}}{2\pi}\right)l_{n-1}\right) \sin(l_{n-1} t_{n-2}) \right| dt_1 \cdots dt_{n-2} \\ + O\left(\frac{p^{2n-1}(\log T)^{n-3}}{T}\right).$$

Using Lemma 5.1 we can get

$$\sum_{k_1=1}^{p-1} \left| \sum_{l_1 \leq A} e\left(\left(-\frac{k_1}{p} + \frac{t_1}{2\pi}\right)l_1\right) \right| \ll \sum_{k_1=1}^{p-1} \min\left(A, \left\| \frac{k_1}{p} - \frac{t_1}{2\pi} \right\|^{-1}\right) \ll p \log p,$$

analogously, by writing $\sin(l_j t_{j-1}) = (1/2i)(e^{il_j t_{j-1}} - e^{-il_j t_{j-1}})$ we find that

$$\sum_{k_j=1}^{p-1} \left| \sum_{l_j \leq A} e\left(\left(-\frac{k_j}{p} + \frac{t_j}{2\pi}\right)l_j\right) \sin(l_j t_{j-1}) \right| \ll p \log p,$$

and at last by partial summation we have

$$\sum_{k_{n-1}=1}^{p-1} \left| \sum_{l_{n-1} \leq A} (p - l_{n-1}) e \left(\left(-\frac{k_{n-1}}{p} + \frac{t_{n-1}}{2\pi} \right) l_{n-1} \right) \sin(l_{n-1} t_{n-2}) \right| \ll p^2 \log p.$$

Summing up and noticing that $T = p^{2n}$, we finally arrive at

$$E' \ll p^n (\log p)^{n-1} \int_{\mathcal{J}} \cdots \int_{\mathcal{J}} \frac{1}{|t_1 \cdots t_{n-2}|} dt_1 \cdots dt_{n-2} \ll p^n (\log p)^{2n-3}. \quad (5.3)$$

The estimation of E'' is similar. At this stage,

$$\begin{aligned} E'' &\ll \sum_{d=1}^{p-1} \sum_{k_1=1}^{p-1} \cdots \sum_{k_{n-1}=1}^{p-1} \\ &\quad \times \left| \sum_{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A} e \left(-\frac{k_1 l_1 + \cdots + k_{n-1} l_{n-1}}{p} \right) \frac{e(-d(p - l_{n-1})/p) - 1}{e(-d/p) - 1} \right| \\ &\ll \sum_{d=1}^{p-1} \left\| \frac{d}{p} \right\|^{-1} \sum_{k_1=1}^{p-1} \cdots \sum_{k_{n-1}=1}^{p-1} \\ &\quad \times \left| \sum_{1 \leq l_1 < l_2 < \cdots < l_{n-1} \leq A} e \left(-\frac{k_1 l_1 + \cdots + k_{n-1} l_{n-1}}{p} \right) \left\{ e \left(\frac{d}{p} l_{n-1} \right) - 1 \right\} \right|, \end{aligned}$$

by using the same method as above we may also get

$$E'' \ll p^n (\log p)^{2n-2}. \quad (5.4)$$

Inserting (5.3) and (5.4) into (5.2) implies

$$E_n(A, p) \ll p^{(n-1)/2} (\log p)^{2n-2}, \quad (5.5)$$

this, with (2.2) and (3.2), proves the theorem.

Acknowledgements. The first and the second authors are supported by N.S.F. grants No. 11201363 and No. 11171265 of P. R. China, respectively.

REFERENCES

- [1] P. Deligne. Applications de la formule des traces aux sommes trigonométriques. In *Cohomologie Étale. Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 $\frac{1}{2}$* (Lecture Notes in Mathematics, 569). Springer, New York, 1977, pp. 168–232. Zbl 0349.10031, MR0463174.
- [2] G. Harman. *Prime-Detecting Sieves* (London Mathematical Society Monographs, 33). Princeton University Press, Princeton, NJ, 2007. Zbl 1220.11118, MR2331072.
- [3] M. Nathanson. *Additive Number Theory. The Classical Bases* (Graduate Texts in Mathematics, 164). Springer, New York, 1996. Zbl 0859.11002, MR1395371.
- [4] Z. Xu and Y. Yi. Differences of integers and their inverses over incomplete intervals (in Chinese). *Sci. Sin. Math.* **41**(8) (2011), 669–679.
- [5] W. Zhang. On the distribution of inverses modulo n . *J. Number Theory* **61** (1996), 301–310. Zbl 0874.11006, MR1423056.

Yaming Lu

School of Mathematics and Statistics

Xi'an Jiaotong University

Xi'an, Shaanxi, 710049, P. R. China

(E-mail: yaminglu@mail.xjtu.edu.cn)

Yuan Yi

School of Mathematics and Statistics

Xi'an Jiaotong University

Xi'an, Shaanxi, 710049, P. R. China

(E-mail: yuanyi@mail.xjtu.edu.cn)