Research Article

On the Generalization of Lehmer Problem and High-Dimension Kloosterman Sums

Guohui Chen¹ and Han Zhang²

¹ College of Mathematics and Statistics, Hainan Normal University, Hainan 571158, China

² School of Mathematics, Northwest University, Xi'an, Shaanxi 710127, China

Correspondence should be addressed to Han Zhang; micohanzhang@gmail.com

Received 1 April 2014; Accepted 8 July 2014; Published 16 July 2014

Academic Editor: Kinkar Ch Das

Copyright © 2014 G. Chen and H. Zhang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

For any fixed integer $k \geq 2$ and integer r with $(r, p) = 1$, it is clear that there exist k integers $1 \leq a_i \leq p-1$ ($i = 1, 2, \dots, k$) such that $a_1 a_2 \cdots a_k \equiv r \pmod{p}$. Let $N(k, r; p)$ denote the number of all $(a_1, a_2, \dots, a_k)$ such that $a_1 a_2 \cdots a_k \equiv r \pmod{p}$ and $2 \nmid (a_1 + a_2 + \cdots + a_k)$. In this paper, we will use the analytic method and the estimate for high-dimension Kloosterman sums to study the asymptotic properties of $N(k, r; p)$ and give two interesting asymptotic formulae for it.

1. Introduction

Let p be an odd number. For each integer a with $1 \leq a \leq p-1$, it is clear that there exists one and only one $\bar{a}$ with $0 \leq \bar{a} \leq p-1$ such that $a \cdot \bar{a} \equiv 1 \pmod{p}$. Let $N(p)$ denote the number of all $1 \leq a \leq p-1$ in which a and $\bar{a}$ are of opposite parity. Professor D. H. Lehmer [1] asked us to study $N(p)$ or at least to say something nontrivial about it. It is known that $N(p) \equiv 2$ or $0 \pmod{4}$ when $p \equiv \pm 1 \pmod{4}$. Some works related to the Lehmer problem can be found in references [2–5]. For example, Zhang [2, 4] proved the asymptotic formula

$$N(p) = \frac{1}{2} \cdot p + O(p^{1/2} \cdot \ln^2 p). \quad (1)$$

In this paper, we will study a new summation related to the Lehmer problem. For any fixed integer $k \geq 2$ and integer r with $(r, p) = 1$, we define the sums $N(k, r; p)$ as follows:

$$N(k, r; p) = \frac{1}{2} \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \cdots \sum_{a_k=1}^{p-1} (1 - (-1)^{a_1+a_2+\cdots+a_k}) \cdot \mathbf{1}_{a_1 a_2 \cdots a_k \equiv r \pmod{p}}. \quad (2)$$

In fact, $N(k, r; p)$ is a generalization of the Lehmer problem. For example, if $k = 2$ and $r = 1$, then from the definition of $N(2, 1; p)$ we have

$$\begin{aligned} N(2, 1; p) &= \frac{1}{2} \sum_{a=1}^{p-1} \sum_{\substack{b=1 \\ ab \equiv 1 \pmod{p}}}^{p-1} (1 - (-1)^{a+b}) \\ &= \frac{1}{2} \sum_{a=1}^{p-1} (1 - (-1)^{a+\bar{a}}) = N(p). \end{aligned} \quad (3)$$

So $N(2, 1; p)$ becomes $N(p)$, the Lehmer problem.

Now we are concerned about the arithmetical properties of $N(k, r; p)$. This problem is interesting, because it is a generalization of the Lehmer problem.

In this paper, we use the analytic method and the estimate for high-dimension Kloosterman sums to study the asymptotic properties of $N(k, r; p)$ and give two interesting asymptotic formulae for it. That is, we will prove the following.

Theorem 1. Let p be an odd prime. Then for any fixed integer $k \geq 2$ and integer r with $(r, p) = 1$, we have the asymptotic formula

$$N(k, r; p) = \frac{1}{2} \cdot (p-1)^{k-1} + O(p^{(k-1)/2} \cdot \ln^k p). \quad (4)$$

In order to facilitate the description of Theorem 2, we need to give the definition of high-dimension Kloosterman sums $C(k, m; q)$. Let $q \geq 3$ be an integer. For any integer m , we define

$$\begin{aligned} C(k, m; q) &= \sum_{\substack{a_1=1 \\ (a_1, q)=1}}^q \sum_{\substack{a_2=1 \\ (a_2, q)=1}}^q \cdots \\ &\sum_{\substack{a_k=1 \\ (a_k, q)=1}}^q e\left(\frac{a_1 + a_2 + \cdots + a_k + m\bar{a}_1\bar{a}_2 \cdots \bar{a}_k}{q}\right), \end{aligned} \quad (5)$$

where $e(y) = e^{2\pi i y}$, $a_i \cdot \bar{a}_i \equiv 1 \pmod{p}$, $i = 1, 2, \dots, k$.

About some arithmetical properties of $C(k, m; q)$, one can find them in [6–8]. Let $E(k, r; p) = N(k, r; p) - (1/2)(p-1)^{k-1}$ denote the error term in the asymptotic formula of $N(k, r; p)$. As another main content of this paper, we will study the asymptotic properties of the hybrid mean value of $C(k-1, r\bar{2}^k; p)$ and $E(k, r; p)$ and also give a sharp asymptotic formula for it. That is, we will prove the following.

Theorem 2. Let p be an odd prime. Then for any fixed integer $k \geq 2$, we have the asymptotic formula

$$\begin{aligned} \sum_{r=1}^{p-1} C(k-1, r\bar{2}^k; p) \cdot E(k, r; p) \\ = -\frac{4^{k-1} \cdot i^k}{\pi^k} \cdot p^k + O(p^{k-1+\epsilon}), \end{aligned} \quad (6)$$

where $i^2 = -1$, ϵ denotes any fixed positive number.

The constants $\bar{2}^k$ in Theorem 2 cannot be omitted. Otherwise, the main term in Theorem 2 is zero. If $k = 3$ and 4, then from Theorem 2 we can also deduce the following two corollaries.

Corollary 3. Let p be an odd prime. Then for any fixed positive number $\epsilon > 0$, we have the asymptotic formula

$$\sum_{r=1}^{p-1} C(2, \bar{8}r; p) \cdot E(3, r; p) = \frac{16 \cdot i}{\pi^3} \cdot p^3 + O(p^{2+\epsilon}). \quad (7)$$

Corollary 4. Let p be an odd prime. Then for any fixed positive number $\epsilon > 0$, we have the asymptotic formula

$$\sum_{r=1}^{p-1} C(3, \bar{16}r; p) \cdot E(4, r; p) = -\frac{64}{\pi^4} \cdot p^4 + O(p^{3+\epsilon}). \quad (8)$$

2. Several Lemmas

In this section, we will give several lemmas, which are necessary in the proofs of our theorems. Hereinafter, we will use many properties of Gauss sums and the estimate for high-dimension Kloosterman sums; all of these contents can be found in references [6, 9], so they will not be repeated here. First we have the following.

Lemma 5. Let p be an odd prime. Then for fixed integer $k \geq 1$ and any integer m , we have the estimate

$$\begin{aligned} |C(k, m; p)| &= \left| \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \cdots \sum_{a_k=1}^{p-1} e\left(\frac{a_1 + a_2 + \cdots + a_k + m\bar{a}_1\bar{a}_2 \cdots \bar{a}_k}{p}\right) \right| \\ &\ll p^{k/2}. \end{aligned} \quad (9)$$

Proof. See [6, 7]. $\square$

Lemma 6. Let p be an odd prime. Then for any odd character $\chi \pmod{p}$ (i.e., $\chi(-1) = -1$), we have the identity

$$\sum_{a=1}^{p-1} (-1)^a \cdot \chi(a) = 2(1 - 2\chi(2)) \cdot \left(\frac{1}{p} \cdot \sum_{a=1}^{p-1} a \cdot \chi(a)\right). \quad (10)$$

Proof. See [10] or Lemma 3 in [3]. $\square$

Lemma 7. Let p be an odd prime. Then for any integer $(r, p) = 1$, we have

$$\begin{aligned} N(k, r; p) &= \frac{1}{2} \cdot (p-1)^{k-1} - \frac{2^{k-1} \cdot i^k}{\pi^k (p-1)} \\ &\times \sum_{\chi(-1)=-1} \bar{\chi}(r) (1 - 2\chi(2))^k \tau^k(\chi) L^k(1, \bar{\chi}), \end{aligned} \quad (11)$$

where $\sum_{\chi(-1)=-1}$ denotes the summation over all odd characters $\chi \pmod{p}$, $\tau(\chi) = \sum_{a=1}^{p-1} \chi(a) \cdot e(a/p)$ denotes the classical Gauss sums, and $L(s, \chi)$ denotes the Dirichlet L-function corresponding to $\chi \pmod{p}$.

Proof. From the orthogonality of characters $\pmod{p}$ and the definition of $N(k, r; p)$ we have the identity

$$\begin{aligned} N(k, r; p) &= \frac{1}{2} \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \cdots \sum_{a_k=1}^{p-1} (1 - (-1)^{a_1+a_2+\cdots+a_k}) \\ &= \frac{1}{2} \cdot (p-1)^{k-1} - \frac{1}{2} \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \cdots \sum_{a_k=1}^{p-1} (-1)^{a_1+a_2+\cdots+a_k} \\ &= \frac{1}{2} \cdot (p-1)^{k-1} - \frac{1}{2(p-1)} \end{aligned}$$

$$\begin{aligned}
& \times \sum_{\chi \bmod p} \bar{\chi}(r) \left(\sum_{a=1}^{p-1} (-1)^a \cdot \chi(a) \right)^k \\
& \equiv \frac{1}{2} \cdot (p-1)^{k-1} - A(k, p).
\end{aligned} \tag{12}$$

For any odd character $\chi \bmod p$, from Theorems 12.11 and 12.20 of [9] we have

$$\frac{1}{p} \cdot \sum_{a=1}^{p-1} a \cdot \chi(a) = \frac{i}{\pi} \cdot \tau(\chi) \cdot L(1, \bar{\chi}). \tag{13}$$

Note that, for any even character $\chi \bmod p$, we have the identity

$$\sum_{a=1}^{p-1} (-1)^a \cdot \chi(a) = 0, \tag{14}$$

from (13) and Lemma 6 we have

$$\begin{aligned}
A(k, p) &= \frac{2^{k-1} \cdot i^k}{\pi^k (p-1)} \\
&\times \sum_{\chi(-1)=-1} \bar{\chi}(r) (1 - 2\chi(2))^k \tau^k(\chi) L^k(1, \bar{\chi}).
\end{aligned} \tag{15}$$

Now Lemma 7 follows from (12) and (15). $\square$

Lemma 8. Let p be an odd prime and k a fixed integer with $k \geq 2$. Then for any nonprincipal character $\chi \bmod p$ and any real numbers $y \geq p^3$, we have the estimate

$$\left| \sum_{n \leq y} \chi(n) \cdot d_k(n) \right| \ll y^{1-(1/2^{k-1})} \cdot \sqrt{p} \cdot \ln p. \tag{16}$$

Proof. We use mathematical induction to prove this lemma. If $k = 2$, then from the Pölya-Vinogradov inequality we have

$$\begin{aligned}
& \left| \sum_{n \leq y} \chi(n) d(n) \right| \\
&= \left| \sum_{mn \leq y} \chi(mn) \right| \\
&= \left| 2 \sum_{n \leq \sqrt{y}} \chi(n) \sum_{m \leq y/n} \chi(m) - \left(\sum_{n \leq \sqrt{y}} \chi(n) \right)^2 \right| \\
&\ll \sqrt{y} \sqrt{p} \ln p = y^{1-(1/2)} \cdot \sqrt{p} \cdot \ln p.
\end{aligned} \tag{17}$$

Assume that the lemma holds for $k = r$. That is,

$$\left| \sum_{n \leq y} \chi(n) \cdot d_r(n) \right| \ll y^{1-(1/2^{r-1})} \cdot \sqrt{p} \cdot \ln p. \tag{18}$$

Then for $k = r + 1$, note that $d_{r+1}(n) = \sum_{s|n} d_r(s)$; applying estimate (18) and the Pölya-Vinogradov inequality we have

$$\begin{aligned}
& \left| \sum_{n \leq y} \chi(n) d_{r+1}(n) \right| \\
&= \left| \sum_{mn \leq y} \chi(mn) d_r(m) \right| \\
&\leq \left| \sum_{n \leq \sqrt{y}} \chi(n) \sum_{m \leq y/n} \chi(m) d_r(m) \right. \\
&\quad \left. + \sum_{m \leq \sqrt{y}} \chi(m) d_r(m) \sum_{n \leq y/n} \chi(n) \right| \\
&\quad + \left| \sum_{n \leq \sqrt{y}} \chi(n) \right| \cdot \left| \sum_{m \leq \sqrt{y}} \chi(m) d_r(m) \right| \\
&\ll \sum_{n \leq \sqrt{y}} \left(\frac{y}{n} \right)^{1-(1/2^{r-1})} \cdot \sqrt{p} \cdot \ln p + y^{1-(1/2^r)} \cdot \sqrt{p} \cdot \ln p \\
&\ll y^{1-(1/2^r)} \cdot \sqrt{p} \cdot \ln p.
\end{aligned} \tag{19}$$

Now our lemma follows from the induction. $\square$

3. Proofs of the Theorems

In this section, we will prove our conclusions. First we prove Theorem 1. For any real number $N \geq p^k$, applying Abel's identity (see Theorem 4.2 of [9]) we have

$$\begin{aligned}
L^k(1, \bar{\chi}) &= \sum_{1 \leq n \leq N} \frac{\bar{\chi}(n) d_k(n)}{n} \\
&\quad + \int_N^\infty \frac{1}{y^2} \left(\sum_{N < n \leq y} \bar{\chi}(n) d_k(n) \right) dy.
\end{aligned} \tag{20}$$

For any integer $0 \leq i \leq k$, from Lemma 5 and the definition of $C(k, m; p)$ we have

$$\begin{aligned}
& \sum_{\chi(-1)=-1} \bar{\chi}(r) \chi(2^i) \tau^k(\chi) \sum_{1 \leq n \leq N} \frac{\bar{\chi}(n) d_k(n)}{n} \\
&= \frac{p-1}{2} \sum_{\substack{1 \leq n \leq N \\ (n,p)=1}} \frac{d_k(n)}{n} \\
&\quad \times \sum_{a_1=1}^{p-1} \cdots \sum_{a_{k-1}=1}^{p-1} e \left(\frac{a_1 + \cdots + a_{k-1} + nr 2^i \cdot \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{k-1}}{p} \right) \\
&\quad - \frac{p-1}{2} \sum_{\substack{1 \leq n \leq N \\ (n,p)=1}} \frac{d_k(n)}{n}
\end{aligned}$$

$$\begin{aligned} & \times \sum_{a_1=1}^{p-1} \cdots \sum_{a_{k-1}=1}^{p-1} e \left(\frac{a_1 + \cdots + a_{k-1} - nr\bar{2}^i \cdot \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{k-1}}{p} \right) \\ & \ll \frac{p-1}{2} \sum_{\substack{1 \leq n \leq N \\ (n,p)=1}} \frac{d_k(n)}{n} \cdot p^{(k-1)/2} \ll p^{(k+1)/2} \cdot \ln^k N. \end{aligned} \quad (21)$$

Applying (20) and the binomial expression we have the estimate

$$\begin{aligned} & \sum_{\chi(-1)=-1} \bar{\chi}(r) (1 - 2\chi(2))^k \tau^k(\chi) \sum_{1 \leq n \leq N} \frac{\bar{\chi}(n) d_k(n)}{n} \\ & \ll p^{(k+1)/2} \cdot \ln^k N. \end{aligned} \quad (22)$$

Taking $N = p^{2^{k-1}}$, note that $|\tau(\chi)| = \sqrt{p}$ and the identity

$$\sum_{N < n \leq y} \bar{\chi}(n) d_k(n) = \sum_{n \leq y} \bar{\chi}(n) d_k(n) - \sum_{n \leq N} \bar{\chi}(n) d_k(n), \quad (23)$$

and applying Lemma 8 we have the estimate

$$\begin{aligned} & \left| \sum_{\chi(-1)=-1} \bar{\chi}(r) (1 - 2\chi(2))^k \tau^k(\chi) \right. \\ & \quad \times \int_N^\infty \frac{1}{y^2} \left(\sum_{N < n \leq y} \bar{\chi}(n) d_k(n) \right) dy \Big| \\ & \ll p^{(k+2)/2} \cdot \frac{\sqrt{p}}{N^{1/2^{k-1}}} \cdot \ln p = p^{(k+1)/2} \cdot \ln p. \end{aligned} \quad (24)$$

Combining (20), (22), (24), and Lemma 7 we may immediately deduce the asymptotic formula

$$N(k, r; p) = \frac{1}{2} \cdot (p-1)^{k-1} + O(p^{(k-1)/2} \cdot \ln^k p). \quad (25)$$

The proof of Theorem 1 is right.

Now we prove Theorem 2. For any nonprincipal character $\chi \bmod p$, from the definition and properties of Gauss sums we have

$$\begin{aligned} & \sum_{r=1}^{p-1} \bar{\chi}(r) \cdot C(k-1, r\bar{2}^k; p) \\ & = \sum_{r=1}^{p-1} \bar{\chi}(r) \\ & \quad \times \sum_{a_1=1}^{p-1} \sum_{a_2=1}^{p-1} \cdots \sum_{a_{k-1}=1}^{p-1} e \left(\frac{a_1 + a_2 + \cdots + a_{k-1} + r\bar{2}^k \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{k-1}}{p} \right) \end{aligned}$$

$$\begin{aligned} & = \sum_{a_1=1}^{p-1} \cdots \sum_{a_{k-1}=1}^{p-1} e \left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{p} \right) \\ & \quad \times \sum_{r=1}^{p-1} \bar{\chi}(r) e \left(\frac{r\bar{2}^k \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{k-1}}{p} \right) \\ & = \tau(\bar{\chi}) \bar{\chi}(2^k) \\ & \quad \times \sum_{a_1=1}^{p-1} \cdots \sum_{a_{k-1}=1}^{p-1} \chi(\bar{a}_1 \bar{a}_2 \cdots \bar{a}_{k-1}) e \left(\frac{a_1 + a_2 + \cdots + a_{k-1}}{p} \right) \\ & = \bar{\chi}(2^k) \cdot \tau^k(\bar{\chi}). \end{aligned} \quad (26)$$

Note that $\tau^k(\bar{\chi}) \cdot \tau^k(\chi) = \bar{\chi}^k(-1) \tau(\chi)^k \cdot \tau^k(\chi) = \bar{\chi}^k(-1) \cdot p^k$; from Lemma 7 and the definition of $E(k, r; p)$ we have

$$\begin{aligned} & \sum_{r=1}^{p-1} C(k-1, r\bar{2}^k; p) \cdot E(k, r; p) \\ & = -\frac{2^{k-1} \cdot i^k}{\pi^k (p-1)} \cdot p^k \\ & \quad \cdot \sum_{\chi(-1)=-1} (-1)^k (1 - 2\chi(2))^k \bar{\chi}(2^k) L^k(1, \bar{\chi}) \\ & = (-1)^{k+1} \frac{2^{k-1} \cdot i^k}{\pi^k (p-1)} \cdot p^k \\ & \quad \cdot \sum_{j=0}^k \binom{j}{k} (-1)^j \cdot 2^j \cdot \sum_{\chi(-1)=-1} \bar{\chi}(2^{k-j}) \sum_{n=1}^{\infty} \frac{\bar{\chi}(n) \cdot d_k(n)}{n} \\ & = (-1)^{k+1} \frac{2^{k-1} \cdot i^k}{\pi^k (p-1)} \cdot p^k \cdot \frac{p-1}{2} (-1)^k \cdot 2^k + O(p^{k-1+\epsilon}) \\ & = -\frac{4^{k-1} \cdot i^k}{\pi^k} \cdot p^k + O(p^{k-1+\epsilon}), \end{aligned} \quad (27)$$

where $i^2 = -1$, $\binom{j}{k} = k!/(j! \cdot (k-j)!)$, ϵ denotes any fixed positive number and $d_k(n)$ denotes the k th divisor function. That is, $d_k(n) = (\sum_{d_1|n} \sum_{d_2|n} \cdots \sum_{d_k|n})_{d_1 d_2 \cdots d_k = n} 1$.

The proof of Theorem 2 is right.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank the referees for their very helpful and detailed comments, which have significantly improved the presentation of this paper. This work is supported by the P. S. F. (2013JZ001) and N. S. F. (11371291) of China.

References

- [1] R. K. Guy, *Unsolved problems in Number Theory*, Springer, New York, NY, USA, 2nd edition, 1994.
- [2] W. Zhang, "On a problem of D. H. Lehmer and its generalization," *Compositio Mathematica*, vol. 86, no. 3, pp. 307–316, 1993.
- [3] W. Zhang and Z. Wu, "A mean value related to the D. H. Lehmer problem and Kloosterman sums," *Acta Arithmetica*, vol. 143, no. 3, pp. 291–298, 2010.
- [4] W. Zhang, "A problem of D. H. Lehmer and its generalization (II)," *Compositio Mathematica*, vol. 91, no. 1, pp. 47–56, 1994.
- [5] W. Zhang, "A problem of D. H. Lehmer and its mean square value formula," *Japanese Journal of Mathematics*, vol. 29, no. 1, pp. 109–116, 2003.
- [6] P. Deligne, "Applications de la formule des traces aux sommes trigonométriques," in *Cohomologie Etale*, vol. 569 of *Lecture Notes in Mathematics*, pp. 168–232, Springer, New York, NY, USA, 1977.
- [7] R. A. Smith, "On n -dimensional Kloosterman sums," *Journal of Number Theory*, vol. 11, no. 3, pp. 324–343, 1979.
- [8] W. Luo, "Bounds for incomplete hyper-Kloosterman sums," *Journal of Number Theory*, vol. 75, no. 1, pp. 41–46, 1999.
- [9] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, NY, USA, 1976.
- [10] T. Funakura, "On Kronecker's limit formula for Dirichlet series with periodic coefficients," *Acta Arithmetica*, vol. 55, no. 1, pp. 59–73, 1990.