A generalization on the difference between an integer and its inverse modulo q. (II)

By Tianping ZHANG[*),**)] and Wenpeng ZHANG[*)]

(Communicated by Heisuke HIRONAKA, M. J. A., Jan. 12, 2005)

Abstract: Let $q > 2$ and c are two integers with $(q, c) = 1$, for each integer a with $0 < a < q$ and $(a, q) = 1$, there exists one and only one b with $0 < b < q$ such that $ab \equiv c \pmod q$. Let

$$M(q,k,c,n) = \sideset{}{'}\sum_{a_1=1}^{q} \cdots \sideset{}{'}\sum_{a_n=1}^{q} \sideset{}{'}\sum_{\substack{b=1 \\ a_1\cdots a_n b \equiv c \pmod q}}^{q} (a_1 \cdots a_n - b)^{2k},$$

the main purpose of this paper is to study the asymptotic behavior of $M(q, k, c, n)$, and prove that for any positive integers k and n with $n \geq 2$ we have

$$M(q,k,c,n) = \frac{\phi^n(q) q^{2kn}}{(2k+1)^n} + O\left(4^k q^{(2k+1)n-(1/2)} d^2(q) \ln q\right).$$

Key words: Generalization; asymptotic formula.

1. Introduction. Let $q \geq 1$ be a positive integer. For any integers a and b, the classical Kloosterman sums $S(a, b; q)$ is defined by:

$$S(a,b;q) = \sideset{}{'}\sum_{n=1}^{q} e\left(\frac{an + b\overline{n}}{q}\right), \tag{1}$$

where $\sum'$ denotes the summation over all n such that $(n, q) = 1$, $n\overline{n} \equiv 1 \pmod q$ and $e(y) = e^{2\pi i y}$.

The various properties of $S(a, b; q)$ were investigated by many authors. Perhaps the most famous property of $S(a, b; q)$ is the estimate (see [1] and [2]):

$$|S(a,b;q)| \leq d(q) q^{(1/2)} (a,b,q)^{(1/2)}, \tag{2}$$

where $d(q)$ is the divisor function, (a, b, q) denotes the greatest common divisor of a, b and q.

In reference [3], Professor Smith generalized the classical Kloosterman sums $S(a, b; q)$ by introducing the n-dimensional Kloosterman sums as

$$S_n(\mathbf{a};q) = \sum_{\mathbf{x} \bmod q}{}' e\left(\frac{\mathbf{a}\cdot\mathbf{x} + a_{n+1}\overline{N\mathbf{x}}}{q}\right),$$

where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ is a given vector from $\mathbf{Z}^n$, $a_{n+1} \in \mathbf{Z}$, summation is over vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ from $\mathbf{Z}^n$ each of whose components belongs to a residue class relatively prime to $q \geq 1$, $\mathbf{a} \cdot \mathbf{x} = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, $N\mathbf{x} = x_1x_2 \cdots x_n$, and $\overline{u}$ as in (1) denotes the multiplicative inverse of $u \pmod q$. Then he proved a number of results concerning $S_n(\mathbf{a}; q)$, among which is the upper bound,

$$|S_n(\mathbf{a};q)| \leq q^{(n/2)} (\mathbf{a};q)_n^{(n/2)} d_{n+1}(q),$$

where $(\mathbf{a}; q)_n$ is precisely defied, and $d_{n+1}(q)$ denotes the number of representations of q as a product of $n + 1$ factors.

Apparently this inequality generalized (2) for the one-dimensional Kloosterman sums $S(a, b; q)$.

Let $q > 2$ and c are two integers with $(q, c) = 1$. For each integer $0 < a < q$ with $(a, q) = 1$, we know that there exists one and only one integer $0 < b < q$ with $(b, q) = 1$ such that $ab \equiv c \pmod q$. Let

$$M(q,k,c) = \sideset{}{'}\sum_{\substack{a=1 \\ ab \equiv c \pmod q}}^{q} \sideset{}{'}\sum_{b=1}^{q} (a-b)^{2k},$$

where $\sum_{a=1}^{q}{}'$ denotes the summation over all a such that $(a, q) = 1$. In reference [4], the second author used the estimates for Kloosterman's sums and trigonometric sums to obtain a sharp asymptotic formula for $M(q, k, c)$, and proved the following theorem:

2000 Mathematics Subject Classification. 11N37(11F20).

*) Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China.

**) College of Mathematics and Information Science, Shannxi Normal University, Xi'an, Shaanxi, P.R. China.

Let $q > 2$ and c are two integers with $(q, c) = 1$. Then for any positive integer k, we have the asymptotic formula

$$M(q,k,c) = \frac{1}{(2k+1)(k+1)}\phi(q)q^{2k} + O\left(4^k q^{(4k+1)/2} d^2(q)\ln^2 q\right), \tag{3}$$

where $\phi(q)$ is the Euler function.

For $k = 1$ and any fixed positive integer c with $(q, c) = 1$, let

$$E(q,1,c) = M(q,1,c) - \frac{1}{6}\phi(q)q^2 - \frac{1}{3}q\prod_{p|q}(1-p).$$

The second author [5] showed that for any integer $q > 2$, we have the asymptotic formula

$$\sum_{c=1}^{q}{}' E^2(q,1,c) = \frac{5}{36}q^3\phi^3(q)\prod_{p^\alpha \| q}\frac{\frac{(p+1)^3}{p(p^2+1)} - \frac{1}{p^{3\alpha-1}}}{1+\frac{1}{p}+\frac{1}{p^2}} + O\left(q^5\exp\left(\frac{4\ln q}{\ln\ln q}\right)\right),$$

where $\prod_{p^\alpha \| q}$ denotes the product over all prime divisors of q with $p^\alpha | q$ and $p^{\alpha+1} \nmid q$.

This proves the error terms in (3) is the best possible.

Now we consider a generalization on this problem. For any integers $q > 2$ and $n \geq 1$, let

$$M(q,k,c,n) = \sum_{\substack{a_1=1\\ a_1\cdots a_n b \equiv c \pmod q}}^{q}{}' \cdots \sum_{a_n=1}^{q}{}' \sum_{b=1}^{q}{}' (a_1\cdots a_n - b)^{2k},$$

for $n = 1$, we have $M(q,k,c,1) = M(q,k,c)$, which has been stated above; while for $n \geq 2$, we still know nothing about it yet. In this paper, we shall use the estimates of n-dimensional Kloosterman sums and the properties of trigonometric sums to give an interesting asymptotic formula for $M(q,k,c,n)$. That is, we shall prove the following

Theorem. *Let $q > 2$ and c are two integers with $(q, c) = 1$, then for any positive integers n, k with $n \geq 2$, we have the asymptotic formula*

$$M(q,k,c,n) = \frac{\phi^n(q)q^{2kn}}{(2k+1)^n} + O\left(4^k q^{(2k+1)n-(1/2)} d^2(q)\ln q\right).$$

Taking $k = 1$, $q = p$, an odd prime in our Theorem, we immediately deduce the following

Corollary. *For any odd prime number p and positive integer n with $n \geq 2$, we have*

$$M(p,1,c,n) = \frac{p^{3n}}{3^n} + O\left(p^{3n-(1/2)}\ln p\right).$$

2. Several Lemmas. In this section, we shall derive the estimates from n-dimensional Kloostermann sums and trigonometric sums used in the proof of the theorem. First we have the following several lemmas.

Lemma 1. *Fixed integer $n > 2$. For any integer r and nonnegative integer p, we define $K(r,p) = \sum_{a=1}^{n} a^p e(\frac{ra}{n})$, where $e(y) = e^{2\pi i y}$. Then we we have*

$$K(r,p)\begin{cases} = \dfrac{n^{p+1}}{p+1} + O\left(n^p\right) & \text{if} \quad n \mid r; \\ \ll \dfrac{n^p}{|\sin\left(\frac{\pi s}{n}\right)|} & \text{if} \quad n \nmid r, \end{cases}$$

where $s = \min(r, n-r)$ with $1 \leq r \leq n-1$.

Proof. See reference [4]. □

Lemma 2. *For each prime p, and any $\mathbf{y} \in Z^{n+1}$, there exist a unique integer $r \geq 0$ such that $\mathbf{y} = p^r\mathbf{x}$ for some $\mathbf{x} \in Z^{n+1} - pZ^{n+1}$; let t denotes the number of components of $\mathbf{x}$ which are divisible by p so that $0 \leq t \leq n$. For each $\alpha \geq 0$, define*

$$(\mathbf{y}; p^\alpha)_n = p^{\sigma_n(\mathbf{y};p^\alpha)_n}$$

where

$$\sigma_n(\mathbf{y};p^\alpha)_n = \begin{cases} \alpha & \text{if} \ \ r \geq \alpha; \\ r & \text{if} \ \ r < \alpha - 1; \\ r & \text{if} \ \ r = \alpha - 1 \ \ \text{and} \ \ t = 0; \\ r - 1 + \frac{2(t-1)}{n} & \text{if} \ \ r = \alpha - 1 \ \ \text{and} \ \ 1 \leq t \leq n. \end{cases}$$

For any integer $q \geq 1$, we now define

$$(\mathbf{y}; q)_n = \prod_{p^\alpha \| q}(\mathbf{y}; p^\alpha)_n.$$

Then for all integers $n, q \geq 1$ and all $\mathbf{y} \in Z^{n+1}$, we have the upper bound

$$|S_n(\mathbf{y}; q)| \leq q^{n/2}(\mathbf{y}; q)_n^{n/2} d_{n+1}(q).$$

Proof. See reference [3]. □

Lemma 3. *Let $q > 2$ and c are two integers with $(q, c) = 1$, then for any positive integers n, p_i, $(1 \leq i \leq n)$, f with $n \geq 2$, we have the following asymptotic formula*

$$\sum_{\substack{a_1=1\\ a_1\cdots a_n b\equiv c \pmod q}}^{q}{}' \cdots \sum_{a_n=1}^{q}{}' \sum_{b=1}^{q}{}' a_1^{p_1}\cdots a_n^{p_n} b^f$$
$$= \frac{\phi^n(q) q^{p_1+\cdots+p_n+f}}{(p_1+1)\cdots(p_n+1)(f+1)} + O\left(q^{p_1+\cdots+p_n+f+n-(1/2)} d^2(q)\ln q\right).$$

Proof. Using the trigonometric identity

$$\sum_{a=1}^{q} \mathrm{e}\left(\frac{au}{q}\right) = \begin{cases} n, & \text{if} \quad n \mid u; \\ 0, & \text{if} \quad n \nmid u. \end{cases} \tag{4}$$

We obtain the identity

(5)

$$\sum_{\substack{a_1=1\\ a_1\cdots a_n b\equiv c \pmod q}}^{q}{}' \cdots \sum_{a_n=1}^{q}{}' \sum_{b=1}^{q}{}' a_1^{p_1}\cdots a_n^{p_n} b^f$$
$$= \frac{1}{q^{n+1}} \sum_{\substack{a_1=1\\ a_1\cdots a_n b\equiv c \pmod q}}^{q}{}' \cdots \sum_{a_n=1}^{q}{}' \sum_{b=1}^{q}{}' \sum_{c_1,\ldots,c_n,d=1}^{q} c_1^{p_1}\cdots c_n^{p_n} d^f$$
$$\times \sum_{y_1,\ldots,y_n,s=1}^{q} \mathrm{e}\Big(\frac{y_1(a_1-c_1)+\cdots+y_n(a_n-c_n)+s(b-d)}{q}\Big)$$
$$= \frac{1}{q^{n+1}} \sum_{y_1,\ldots,y_n,s=1}^{q} \sum_{a_1=1}^{q}{}' \cdots \sum_{a_n=1}^{q}{}' \mathrm{e}\left(\frac{y_1a_1+\cdots+y_na_n+sc\overline{a_1\cdots a_n}}{q}\right)$$
$$\times \sum_{c_1=1}^{q} c_1^{p_1} \mathrm{e}\left(\frac{-y_1c_1}{q}\right) \cdots \sum_{c_n=1}^{q} c_n^{p_n} \mathrm{e}\left(\frac{-y_nc_n}{q}\right) \sum_{d=1}^{q} d^f \mathrm{e}\left(\frac{-sd}{q}\right)$$
$$= \frac{1}{q^{n+1}} \sum_{y_1,\ldots,y_n,s=1}^{q} S(y_1,\ldots,y_n,sc;q) K(-y_1,p_1) \cdots K(-y_n,p_n) K(-s,f)$$
$$= \frac{1}{q^{n+1}} S(q,\ldots,q,qc;q) K(-q,p_1) \cdots K(-q,p_n) K(-q,f) + \sum_{r=1}^{n} \frac{C_n^r}{q^{n+1}} M + \sum_{r=1}^{n} \frac{C_n^{r-1}}{q^{n+1}} N + \frac{1}{q^{n+1}} \sum_{y_1=1}^{q-1} \cdots \sum_{y_n=1}^{q-1} \sum_{s=1}^{q-1} S(y_1,\ldots,y_n,sc;q) K(-y_1,p_1) \cdots K(-y_n,p_n) K(-s,f).$$

where $C_n^r = \frac{n!}{r!(n-r)!}$, $(1 \le r \le n)$, $K(r,p)$ and $S(y_1,\ldots,y_n,sc;q) = S_n(\mathbf{y};q)$ are defined on the above, and

$$M = \sum_{y_1=1}^{q-1} \cdots \sum_{y_r=1}^{q-1} S(y_1,\ldots,y_r,q,\ldots,q,qc;q) \times K(-y_1,p_1)\cdots K(-y_r,p_r) K(-q,p_{r+1}) \cdots K(-q,p_n) K(-q,f),$$

$$N = \sum_{y_1=1}^{q-1} \cdots \sum_{y_{r-1}=1}^{q-1} \sum_{s=1}^{q-1} S(y_1,\ldots,y_{r-1},q,\ldots,q,sc;q) \times K(-y_1,p_1)\cdots K(-y_{r-1},p_{r-1}) K(-q,p_r) \cdots K(-q,p_n) K(-s,f).$$

Since $2/\pi \le \sin(x/\pi)$ for $|x| \le \pi/2$, we obtain

$$\frac{1}{q^{n+1}} S(q,\ldots,q,qc;q) K(-q,p_1) \cdots K(-q,p_n) K(-q,f)$$
$$= \frac{\phi^n(q)}{q^{n+1}} \left(\frac{q^{p_1+1}}{p_1+1} + O(q^{p_1})\right) \cdots \left(\frac{q^{p_n+1}}{p_n+1} + O(q^{p_n})\right) \left(\frac{q^{f+1}}{f+1} + O(q^f)\right)$$
$$= \frac{\phi^n(q) q^{p_1+\cdots+p_n+f}}{(p_1+1)\cdots(p_n+1)(f+1)} + O\left(q^{p_1+\cdots+p_n+f+n-1}\right). \tag{6}$$

Similarly, we can get the estimates

(7)

$$M = \sum_{y_1=1}^{q-1} \cdots \sum_{y_r=1}^{q-1} \sum_{a_1=1}^{q}{}' \cdots \sum_{a_r=1}^{q}{}' \sum_{a_{r+1}=1}^{q}{}' \cdots \sum_{a_n=1}^{q}{}' \mathrm{e}\left(\frac{y_1a_1+\cdots+y_ra_r}{q}\right) K(-y_1,p_1) \cdots K(-y_r,p_r) K(-q,p_{r+1}) \cdots K(-q,p_n) K(-q,f)$$
$$\ll \phi^{n-r}(q) q^{r/2} d^r(q) \sum_{y_1=1}^{q-1} \cdots \sum_{y_r=1}^{q-1} \frac{(y_1,q)^{1/2} q^{p_1}}{|\sin(\frac{\pi y_1}{q})|} \cdots \frac{(y_r,q)^{1/2} q^{p_r}}{|\sin(\frac{\pi y_r}{q})|} \left(\frac{q^{p_{r+1}+1}}{p^{r+1}+1} + O(q^{p_{r+1}})\right)$$

$$\cdots\left(\frac{q^{p_n+1}}{p_n+1}+O(q^{p_n})\right)\left(\frac{q^{f+1}}{f+1}+O(q^f)\right)$$
$$\ll q^{(p_1+\cdots+p_n+f+2n-\frac{r}{2}+1)}d^r(q)\sum_{y_1=1}^{q-1}$$
$$\cdots\sum_{y_r=1}^{q-1}\frac{(y_1,q)^{1/2}\cdots(y_r,q)^{1/2}}{y_1\cdots y_r}$$
$$\ll q^{(p_1+\cdots+p_n+f+2n-\frac{r}{2}+1)}d^{2r}(q)\ln^r q,$$

$$N\ll\sum_{y_1=1}^{q-1}\cdots\sum_{y_{r-1}=1}^{q-1}\sum_{s=1}^{q-1}q^{n/2}(\mathbf{y};q)_n^{n/2}d_{n+1}(q)\tag{8}$$
$$\frac{q^{p_1}}{|\sin(\frac{\pi y_1}{q})|}\cdots\frac{q^{p_{r-1}}}{|\sin(\frac{\pi y_{r-1}}{q})|}\frac{q^f}{|\sin(\frac{\pi s}{q})|}$$
$$\times\left(\frac{q^{p_r+1}}{p_r+1}+O(q^{p_r})\right)$$
$$\times\cdots\times\left(\frac{q^{p_n+1}}{p_n+1}+O(q^{p_n})\right)$$
$$\ll q^{(p_1+\cdots+p_n+f+\frac{3n}{2}+1)}d_{n+1}(q)\sum_{y_1=1}^{q-1}$$
$$\cdots\sum_{y_{r-1}=1}^{q-1}\sum_{s=1}^{q-1}\frac{(y_1,\ldots,y_{r-1},s,q)^{n/2}}{y_1\cdots y_{r-1}s}$$
$$\ll q^{(p_1+\cdots+p_n+f+\frac{3n}{2}+1)}d_{n+1}(q)\sum_{d|q}\sum_{l_1=1}^{(q-1)/d}$$
$$\cdots\sum_{l_{r-1}=1}^{(q-1)/d}\sum_{l_r=1}^{(q-1)/d}\frac{d^{(n-2r)/2}}{l_1\cdots l_{r-1}l_r}$$
$$\ll q^{(p_1+\cdots+p_n+f+2n-r+1)}d_{n+1}(q)d(q)\ln^r q,$$

and

$$\frac{1}{q^{n+1}}\sum_{y_1=1}^{q-1}\cdots\sum_{y_n=1}^{q-1}\sum_{s=1}^{q-1}S(y_1,\ldots,y_n,sc;q)K(-y_1,p_1)\tag{9}$$
$$\cdots K(-y_n,p_n)K(-s,f)$$
$$\ll\frac{1}{q^{n+1}}\sum_{y_1=1}^{q-1}\cdots\sum_{y_n=1}^{q-1}\sum_{s=1}^{q-1}q^{n/2}(\mathbf{y};q)_n^{n/2}d_{n+1}(q)$$
$$\frac{q^{p_1}}{|\sin(\frac{\pi y_1}{q})|}\cdots\frac{q^{p_n}}{|\sin(\frac{\pi y_n}{q})|}\frac{q^f}{|\sin(\frac{\pi s}{q})|}$$
$$\ll q^{(p_1+\cdots+p_n+f+\frac{n}{2})}d_{n+1}(q)\sum_{y_1=1}^{q-1}$$
$$\cdots\sum_{y_n=1}^{q-1}\sum_{s=1}^{q-1}\frac{(y_1,\ldots,y_n,s,q)^{(n/2)}}{y_1\cdots y_n s}$$
$$\ll q^{(p_1+\cdots+p_n+f+\frac{n}{2})}d_{n+1}(q)\sum_{d|q}\sum_{l_1=1}^{(q-1)/d}$$
$$\cdots\sum_{l_n=1}^{(q-1)/d}\sum_{l_{n+1}=1}^{(q-1)/d}\frac{1}{d^{(n+2)/2}l_1\cdots l_n l_{n+1}}$$
$$\ll q^{(p_1+\cdots+p_n+f+\frac{n}{2})}d_{n+1}(q)\ln^{n+1}q.$$

Combining (5)–(9) we immediately deduce that

$$\sum_{\substack{a_1=1\\ a_1\cdots a_n b\equiv c\pmod q}}^{q}{}'\cdots\sum_{a_n=1}^{q}{}'\sum_{b=1}^{q}{}'a_1^{p_1}\cdots a_n^{p_n}b^f$$
$$=\frac{\phi^n(q)q^{p_1+\cdots+p_n+f}}{(p_1+1)\cdots(p_n+1)(f+1)}$$
$$+O\left(q^{p_1+\cdots+p_n+f+n-(1/2)}d^2(q)\ln q\right).$$

This completes the proof of Lemma 3. □

3. Proof of the theorem. In this section, we shall complete the proof of the Theorem. In fact by the expansion of the binomial expression and Lemma 3 we get

$$M(q,k,c,n)$$
$$=\sum_{\substack{a_1=1\\ a_1\cdots a_n b\equiv c\pmod q}}^{q}{}'\cdots\sum_{a_n=1}^{q}{}'\sum_{b=1}^{q}{}'(a_1\cdots a_n-b)^{2k}$$
$$=\sum_{i=0}^{2k}C_{2k}^i(-1)^i\sum_{\substack{a_1=1\\ a_1\cdots a_n b\equiv c\pmod q}}^{q}{}'\cdots\sum_{a_n=1}^{q}{}'\sum_{b=1}^{q}{}'(a_1\cdots a_n)^{2k-i}b^i$$
$$=\sum_{i=0}^{2k}C_{2k}^i(-1)^i\left\{\frac{\phi^n(q)q^{n(2k-i)+i}}{(2k-i+1)^n(i+1)}\right.$$
$$\left.+O\left(q^{n(2k-i)+i+n-(1/2)}d^2(q)\ln q\right)\right\}$$
$$=\sum_{i=1}^{2k}C_{2k}^i(-1)^i\left\{\frac{\phi^n(q)q^{n(2k-i)+i}}{(2k-i+1)^n(i+1)}\right.$$
$$\left.+O\left(q^{n(2k-i)+i+n-(1/2)}d^2(q)\ln q\right)\right\}$$
$$+\frac{\phi^n(q)q^{2kn}}{(2k+1)^n}+O\left(4^kq^{(2k+1)n-(1/2)}d^2(q)\ln q\right)$$
$$=\frac{\phi^n(q)q^{2kn}}{(2k+1)^n}+O\left(4^kq^{(2k+1)n-(1/2)}d^2(q)\ln q\right),$$

where $n\ge 2$.

This completes the proof of the theorem.

Acknowledgement. This work is supported by the N.S.F. (10271093, 60472068) and P.N.S.F of P. R. China.

References

[1] S. Chowla, On Kloosterman's sum, Norske Vid. Selsk. Forh. (Trondheim) **40** (1967), 70–72.

[2] T. Estermann, On Kloosterman's sum, Mathematika **8** (1961), 83–86.

[3] R. A. Smith, On n-dimensional Kloosterman sums, J. Number Theory **11** (1979), no. 3 S. Chowla Anniversary Issue, 324–343.

[4] W. P. Zhang, On the difference between an integer and its inverse modulo n, J. Number Theory **52** (1995), no. 1, 1–6.

[5] W. Zhang, On the difference between an integer and its inverse modulo n. II, Sci. China Ser. A **46** (2003), no. 2, 229–238.