ACTA ARITHMETICA
LXVIII.3 (1994)

On the difference between a D. H. Lehmer number and its inverse modulo q

by

Wenpeng Zhang (Xi'an)

1. Introduction. Let $q > 2$ be an odd integer. For each integer x with $0 < x < q$ and $(q, x) = 1$, we know that there exists one and only one $\overline{x}$ with $0 < \overline{x} < q$ such that $x\overline{x} \equiv 1 \pmod{q}$. Let $r(q)$ be the number of cases in which x and $\overline{x}$ are of opposite parity. For $q = p$ a prime, D. H. Lehmer [2] asks us to find $r(p)$ or at least to say something nontrivial about it. For the sake of simplicity, we call such a number x as a *D. H. Lehmer number*. The main purpose of this paper is to study the distribution properties of D. H. Lehmer numbers and the asymptotic properties of the $2k$th power mean

$$M(q,k) = \sum_{\substack{a=1 \\ 2 \mid a+\overline{a}+1}}^{q}{}' (a-\overline{a})^{2k} \tag{1}$$

where $\sum_a'$ denotes the summation over all a such that $(a, q) = 1$.

It seems that no one has studied this problem yet; at least I have not seen expressions like (1) before. The problem is interesting because it can help us to find how large is the difference between a D. H. Lehmer number and its inverse modulo q. In this paper, we use estimates of Kloosterman's sums and properties of trigonometric sums to give a sharper asymptotic formula for $M(q, k)$ for any fixed positive integer k. That is, we shall prove the following:

Theorem 1. *For any odd number q and integer k, we have the asymptotic formula*

$$M(q,k) = \frac{1}{(2k+1)(2k+2)}\varphi(q)q^{2k} + O(4^k q^{(4k+1)/2}\tau^2(q)\ln^2 q)$$

where $\varphi(q)$ is the Euler function and $\tau(q)$ is the divisor function.

Project supported by the National Natural Science Foundation of China.

For $0 \le x, y \le 1$, define the distribution function of a, $\overline{a}$ as

$$F_q(x,y) \equiv \#\{a : a \le xq,\ \overline{a} \le yq,\ 2\nmid a+\overline{a}\}.$$

Then we can deduce the following limiting distribution theorem:

THEOREM 2. *For any odd number $q > 2$, we have*

$$F_q(x,y) = \tfrac{1}{2}xy\varphi(q) + O(q^{1/2}\tau^2(q)\ln^2 q).$$

From the theorems we can immediately deduce the following two corollaries:

COROLLARY 1. *For any odd prime number p, we have the asymptotic formula*

$$M(p,2) = \frac{1}{30}p^5 + O(p^{9/2}\ln^2 p).$$

COROLLARY 2. *For any real numbers $0 \le x, y \le 1$, we have*

$$\lim_{q\to\infty}\frac{F_q(x,y)}{\varphi(q)} = \frac{1}{2}xy.$$

2. Some elementary lemmas. In this section, we prove some elementary lemmas which are necessary in the proof of the theorems.

LEMMA 1. *Let q be an odd number. For any integer n and nonnegative integer r, define*

$$K(n,r) = \sum_{a=1}^{q} a^r e(an/q), \qquad H(n,r) = \sum_{a=1}^{q}(-1)^a a^r e(an/q)$$

where $e(y) = e^{2\pi iy}$. We have the estimates

$$K(n,r) \begin{cases} = \dfrac{q^{r+1}}{r+1} + O(q^r) & \text{if } q \mid n, \\ \ll \dfrac{q^r}{|\sin(\pi n/q)|} & \text{if } q \nmid n, \end{cases} \tag{2}$$

$$H(n,r) \ll \frac{q^r}{|\cos(\pi n/q)|}. \tag{3}$$

P r o o f. First we prove (2). For $r = 0$, from the trigonometric identity

$$\sum_{a=1}^{q} e\left(\frac{an}{q}\right) = \begin{cases} n, & q \mid n, \\ 0, & q \nmid n, \end{cases} \tag{4}$$

we immediately deduce that (2) holds.

For $r > 0$, if $q \nmid n$, then

$$\begin{aligned} K(n,r)\Big(1 - e\Big(\frac{n}{q}\Big)\Big) &= \Big(1 - e\Big(\frac{n}{q}\Big)\Big)\sum_{a=1}^{q} a^r e\Big(\frac{an}{q}\Big) \\ &= \sum_{a=1}^{q} a^r e\Big(\frac{an}{q}\Big) - \sum_{a=1}^{q} a^r e\Big(\frac{(a+1)n}{q}\Big) \\ &= (1-q^r)e\Big(\frac{n}{q}\Big) + \sum_{a=1}^{q-1}((a+1)^r - a^r)e\Big(\frac{n(a+1)}{q}\Big) \\ &\ll q^r + \sum_{a=1}^{q-1}((a+1)^r - a^r) \ll q^r. \end{aligned}$$

From this we can deduce that

$$|K(n,r)| \ll \frac{q^r}{|\sin(\pi n/q)|}. \tag{5}$$

If $q \mid n$, then from Euler's summation formula we get

$$\begin{aligned} K(n,r) &= \sum_{a=1}^{q} a^r e\Big(\frac{an}{q}\Big) = \sum_{a=1}^{q} a^r \\ &= \int_0^q x^r\,dx + O(q^r) = \frac{q^{r+1}}{r+1} + O(q^r). \end{aligned} \tag{6}$$

Combining (5) and (6) we obtain (2).

Now we prove (3). If $q \mid n$, then

$$H(n,r) = \sum_{a=1}^{q}(-1)^a a^r e\Big(\frac{an}{q}\Big) = \sum_{a=1}^{q}(-1)^a a^r \ll q^r. \tag{7}$$

If $q \nmid n$, then

$$\begin{aligned} &H(n,r)\Big(1 + e\Big(\frac{n}{q}\Big)\Big) \\ &\quad= \Big(1 + e\Big(\frac{n}{q}\Big)\Big)\sum_{a=1}^{q}(-1)^a a^r e\Big(\frac{an}{q}\Big) \\ &\quad= \sum_{a=1}^{q}(-1)^a a^r e\Big(\frac{an}{q}\Big) + \sum_{a=1}^{q}(-1)^a a^r e\Big(\frac{(a+1)n}{q}\Big) \\ &\quad\ll q^r + \sum_{a=1}^{q-1}((a+1)^r - a^r) \ll q^r. \end{aligned} \tag{8}$$

Noting that $|1+e(n/q)| = 2|\cos(\pi n/q)|$, (3) follows from (7) and (8). This completes the proof of Lemma 1.

LEMMA 2. *Let m, n and q be integers, and $q > 2$. Then we have the estimates*

$$S(m,n;q) = \sum_{\substack{d \pmod q \\ (d,q)=1}} e\Big(m\frac{\overline{d}}{d} + n\frac{d}{q}\Big) \ll (m,n,q)^{1/2} q^{1/2} \tau(q)$$

where $d\overline{d} \equiv 1 \pmod q$, $\tau(q)$ is the divisor function, (m,n,q) is the greatest common factor of m, n and q, and $e(y) = e^{2\pi i y}$.

Proof. See [1].

LEMMA 3. *Let r, s and q be positive integers and $q > 2$. Then*

$$\sum_{\substack{a=1 \\ ab\equiv 1\,(q)}}^{q}{}' \sum_{b=1}^{q}{}' a^r b^s = \frac{\varphi(q) q^{r+s}}{(r+1)(s+1)} + O(q^{r+s+1/2}\tau^2(q)\ln^2 q)$$

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

Proof. First notice that from (4) we get the identity

$$\begin{aligned}
(9)\quad & \sum_{\substack{a=1 \\ ab\equiv 1\,(q)}}^{q}{}' \sum_{b=1}^{q}{}' a^r b^s \\
&= \frac{1}{q^2} \sum_{\substack{a=1 \\ ab\equiv 1\,(q)}}^{q}{}' \sum_{b=1}^{q}{}' \sum_{c,d=1}^{q} c^r d^s \sum_{m,n=1}^{q} e\Big(\frac{m(a-c)+n(b-d)}{q}\Big) \\
&= \frac{1}{q^2} \sum_{m,n=1}^{q} \Big(\sum_{\substack{a=1 \\ ab\equiv 1\,(q)}}^{q}{}' \sum_{b=1}^{q}{}' e\Big(\frac{am+bn}{q}\Big)\Big) \\
&\qquad\qquad \times \Big(\sum_{c=1}^{q} c^r e\Big(\frac{-mc}{q}\Big)\Big)\Big(\sum_{d=1}^{q} d^s e\Big(\frac{-nd}{q}\Big)\Big) \\
&\equiv \frac{1}{q^2} \sum_{m=1}^{q}\sum_{n=1}^{q} S(m,n;q) K(-m,r) K(-n,s) \\
&= \frac{1}{q^2} \sum_{m=1}^{q-1} S(m,q;q) K(-m,r) K(-q,s)
\end{aligned}$$

$$+\frac{1}{q^2}\sum_{n=1}^{q-1}S(q,n;q)K(-q,r)K(-n,s)$$
$$+\frac{1}{q^2}\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}S(m,n;q)K(-m,r)K(-n,s)$$
$$+\frac{1}{q^2}S(q,q;q)K(-q,r)K(-q,s)$$

where $K(-m,r)$ is defined in Lemma 1. From (2) of Lemma 1, Lemma 2 and noting that $2/\pi \le (\sin x)/x$ for $|x| \le \pi/2$, we get

$$\frac{1}{q^2}S(q,q;q)K(-q,r)K(-q,s) = \frac{\varphi(q)}{q^2}\left(\frac{q^{r+1}}{r+1}+O(q^r)\right)\left(\frac{q^{s+1}}{s+1}+O(q^s)\right) = \frac{\varphi(q)q^{r+s}}{(r+1)(s+1)}+O(q^{r+s}), \tag{10}$$

$$\sum_{m=1}^{q-1}S(m,q;q)K(-m,r)K(-q,s) \ll \sum_{m=1}^{q-1}q^{1/2}(m,q)^{1/2}\tau(q)q^{s+1}\frac{q^r}{|\sin(\pi m/q)|} \ll q^{r+s+5/2}\tau(q)\sum_{m=1}^{q-1}\frac{(m,q)^{1/2}}{m} \ll q^{r+s+5/2}\tau^2(q)\ln q. \tag{11}$$

Similarly, we can get the estimates

$$\sum_{n=1}^{q-1}S(q,n;q)K(-q,r)K(-n,s) \ll q^{r+s+5/2}\tau^2(q)\ln q, \tag{12}$$

$$\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}S(m,n;q)K(-m,r)K(-n,s) \ll \sum_{m=1}^{q-1}\sum_{n=1}^{q-1}\frac{q^{1/2}\tau(q)(m,n,q)^{1/2}q^{r+s}}{|\sin(\pi m/q)|\,|\sin(\pi n/q)|} \ll q^{r+s+5/2}\tau(q)\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}\frac{(m,n,q)^{1/2}}{mn} \ll q^{r+s+5/2}\tau(q)\ln^2 q. \tag{13}$$

Combining (9)–(13) we immediately deduce that

$$\sideset{}{'}\sum_{\substack{a=1\\ ab\equiv 1\,(q)}}^{q}\sideset{}{'}\sum_{b=1}^{q} a^r b^s = \frac{\varphi(q)q^{r+s}}{(r+1)(s+1)} + O(q^{r+s+1/2}\tau^2(q)\ln^2 q).$$

This is the conclusion of Lemma 3.

LEMMA 4. *Let r, s and q be positive integers and $q > 2$. Then*

$$\sideset{}{'}\sum_{\substack{a=1\\ ab\equiv 1\,(q)}}^{q}\sideset{}{'}\sum_{b=1}^{q} (-1)^{a+b} a^r b^s = O(q^{r+s+1/2}\tau^2(q)\ln^2 q).$$

P r o o f. Similarly, we get

$$\begin{aligned}(14)\quad &\sideset{}{'}\sum_{\substack{a=1\\ ab\equiv 1\,(q)}}^{q}\sideset{}{'}\sum_{b=1}^{q} (-1)^{a+b} a^r b^s\\ &= \frac{1}{q^2}\sideset{}{'}\sum_{\substack{a=1\\ ab\equiv 1\,(q)}}^{q}\sideset{}{'}\sum_{b=1}^{q}\sum_{c,d=1}^{q} (-1)^{c+d} c^r d^s \sum_{m,n=1}^{q} e\Big(\frac{m(a-c)+n(b-d)}{q}\Big)\\ &= \frac{1}{q^2}\sum_{m,n=1}^{q}\Big(\sideset{}{'}\sum_{\substack{a=1\\ ab\equiv 1\,(q)}}^{q}\sideset{}{'}\sum_{b=1}^{q} e\Big(\frac{ma+nb}{q}\Big)\Big)\\ &\qquad\qquad \times\Big(\sum_{c,d=1}^{q} (-1)^{c+d} c^r d^s e\Big(\frac{-mc-nd}{q}\Big)\Big)\\ &\equiv \frac{1}{q^2}\sum_{m=1}^{q}\sum_{n=1}^{q} S(m,n;q)H(-m,r)H(-n,s)\end{aligned}$$

where $H(-m,r)$ is defined in Lemma 1.

Noting that $|\cos(\pi m/q)| = |\sin(\pi(q-2m)/(2q))|$ and $q - 2m \neq 0$, from (3) of Lemma 1, (14) and using the method of proof of Lemma 3 we easily deduce the conclusion of Lemma 4.

LEMMA 5. *Let $q > 2$ be an odd number. Then for any fixed $0 \le x, y \le 1$ we have*

$$(\mathrm{I})\qquad \sideset{}{'}\sum_{\substack{a\le xq\\ ab\equiv 1\,(q)}}\sideset{}{'}\sum_{b\le yq} 1 = \varphi(q)xy + O(q^{1/2}\tau^2(q)\ln^2 q),$$

$$\text{(II)} \qquad \sum_{\substack{a\le xq\\ ab\equiv 1\,(q)}}{}' \sum_{b\le yq}{}'(-1)^{a+b} = O(q^{1/2}\tau^2(q)\ln^2 q).$$

P r o o f. For fixed $0 \le x, y \le 1$, we define

$$K(x,n,q) = \sum_{a\le xq} e\Big(\frac{an}{q}\Big), \qquad H(x,n,q) = \sum_{a\le xq}(-1)^a e\Big(\frac{an}{q}\Big).$$

Using the method of proving Lemma 1 we can get the estimates

$$\text{(15)} \qquad K(x,n,q)\begin{cases} = xq + O(1) & \text{if } q \mid n,\\ \ll \dfrac{1}{|\sin(\pi n/q)|} & \text{if } q\nmid n,\end{cases}$$

$$\text{(16)} \qquad H(x,n,q) \ll \frac{1}{|\cos(\pi n/q)|}.$$

From (15), Lemma 2 and the method of proof of Lemma 3 we easily deduce that

$$\sum_{\substack{a\le xq\\ ab\equiv 1\,(q)}}{}' \sum_{b\le yq}{}' 1 = \frac{1}{q^2}\sum_{m=1}^{q}\sum_{n=1}^{q} S(m,n;q)K(x,-m,q)K(y,-n,q)$$
$$= \varphi(q)xy + O(q^{1/2}\tau^2(q)\ln^2 q).$$

This completes the proof of (I).

Similarly, from (16), Lemma 2 and the method of proof of Lemma 4 we deduce (II).

3. Proof of the theorems. First we prove Theorem 1. By the binomial formula, Lemma 3 and Lemma 4 we get

$$M(q,k) = \sum_{\substack{a=1\\ 2\mid a+\overline{a}+1}}^{q}{}' (a-\overline{a})^{2k} = \frac{1}{2}\sum_{\substack{a=1\\ ab\equiv 1\,(q)}}^{q}{}' \sum_{b=1}^{q}{}' (1-(-1)^{a+b})(a-b)^{2k}$$
$$= \frac{1}{2}\sum_{a=1}^{q}{}'(a-\overline{a})^{2k} - \frac{1}{2}\sum_{a=1}^{q}{}'(-1)^{a+\overline{a}}(a-\overline{a})^{2k}$$
$$= \frac{1}{2}\sum_{i=0}^{2k}\binom{2k}{i}(-1)^i\Big(\sum_{a=1}^{q}{}' a^{2k-i}(\overline{a})^i - \sum_{a=1}^{q}{}'(-1)^{a+\overline{a}}a^{2k-i}(\overline{a})^i\Big)$$

$$
\begin{aligned}
&= \frac{1}{2}\sum_{i=0}^{2k}\binom{2k}{i}(-1)^i\bigg(\frac{\varphi(q)q^{2k}}{(i+1)(2k-i+1)} \\
&\qquad\qquad + O(q^{2k+1/2}\tau^2(q)\ln^2 q)\bigg) \\
&\quad + O\bigg(\sum_{i=0}^{2k}\binom{2k}{i}q^{2k+1/2}\tau^2(q)\ln^2 q\bigg) \\
&= \frac{\varphi(q)q^{2k}}{2}\sum_{i=0}^{2k}\frac{(-1)^i\binom{2k}{i}}{(i+1)(2k-i+1)} + O(4^k q^{2k+1/2}\tau^2(q)\ln^2 q) \\
&= \frac{\varphi(q)q^{2k}}{2(2k+1)(2k+2)}\sum_{i=0}^{2k}(-1)^i\binom{2k+2}{i+1} \\
&\quad + O(4^k q^{2k+1/2}\tau^2(q)\ln^2 q) \\
&= \frac{\varphi(q)q^{2k}}{2(2k+1)(2k+2)}\bigg(-\sum_{i=0}^{2k+2}(-1)^i\binom{2k+2}{i}+2\bigg) \\
&\quad + O(4^k q^{2k+1/2}\tau^2(q)\ln^2 q) \\
&= \frac{\varphi(q)q^{2k}}{2(2k+1)(2k+2)}(-(1-1)^{2k+2}+2) + O(4^k q^{2k+1/2}\tau^2(q)\ln^2 q) \\
&= \frac{\varphi(q)q^{2k}}{(2k+1)(2k+2)} + O(4^k q^{2k+1/2}\tau^2(q)\ln^2 q).
\end{aligned}
$$

This is the conclusion of Theorem 1.

Applying Lemma 5 we can deduce that

$$
\begin{aligned}
F_q(x,y) &\equiv \#\{a : a \le xq,\ \overline{a} \le yq,\ 2\nmid a+\overline{a}\} \\
&= \frac{1}{2}\sum_{\substack{a\le xq\\ ab\equiv 1\,(q)}}{\sum_{b\le yq}}'(1-(-1)^{a+b}) \\
&= \frac{1}{2}\sum_{\substack{a\le xq\\ ab\equiv 1\,(q)}}{\sum_{b\le yq}}'1 - \frac{1}{2}\sum_{\substack{a\le xq\\ ab\equiv 1\,(q)}}{\sum_{b\le yq}}'(-1)^{a+b} \\
&= \frac{1}{2}\varphi(q)xy + O(q^{1/2}\tau^2(q)\ln^2 q).
\end{aligned}
$$

This completes the proof of Theorem 2.

Acknowledgements. The author expresses his gratitude to the referee for helpful comments.

References

[1] T. Estermann, *On Kloosterman's sums*, Mathematika 8 (1961), 83–86.
[2] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1981, 139–140.
[3] W. Zhang, *A problem of D. H. Lehmer and its generalization* (*II*), Compositio Math. 91 (1994), 47–56.

DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN SHAANXI
PEOPLE'S REPUBLIC OF CHINA

Received on 2.11.1993
and in revised form on 21.5.1994 (2513)