ACTA ARITHMETICA
143.3 (2010)

A mean value related to the D. H. Lehmer problem and Kloosterman sums

by

Wenpeng Zhang (Xi'an) and Zhaoxia Wu (Urmq)

1. Introduction. Let $q > 2$ be an odd integer, and c be any integer with $(c, q) = 1$. For each integer a with $1 \le a \le q-1$ and $(a, q) = 1$, we know that there exists one and only one integer b with $1 \le b \le q-1$ and $(b, q) = 1$ such that $ab \equiv c \bmod q$. Let $N(c, q)$ denote the number of cases in which a and b are of opposite parity. For example, $N(1, 3) = 0$, $N(1, 5) = 2$, and $N(1, 13) = 6$. For $q = p$ an odd prime, D. H. Lehmer asked to find $N(1, p)$ or at least to say something nontrivial about it (see [3]). It is known that $N(1, p) \equiv 2$ or $0 \bmod 4$ according as $p \equiv \pm 1 \bmod 4$. The first author proved in [5] and [6] that for any odd integer $q > 3$, we have the asymptotic formula

$$N(1, q) = \frac{1}{2}\phi(q) + O(q^{1/2} d^2(q) \ln^2 q),$$

where $\phi(q)$ is the Euler function, and $d(q)$ is the Dirichlet divisor function.

For any integer c with $(c, q) = 1$, using the method in [6] we can also deduce that

$$N(c, q) = \frac{1}{2}\phi(q) + O(q^{1/2} d^2(q) \ln^2 q), \tag{1}$$

where the big-O constant is uniform in c.

Let

$$E(c, q) = N(c, q) - \frac{1}{2}\phi(q).$$

The first author also proved in [7] and [8] that

$$\sum_{c=1}^{p-1} E^2(c, p) = \frac{3}{4}p^2 + O\left(p \cdot \exp\left(\frac{3 \ln p}{\ln \ln p}\right)\right)$$

2010 *Mathematics Subject Classification*: Primary 11M20.
Key words and phrases: D. H. Lehmer problem, Kloosterman sums, hybrid mean value, asymptotic formula.

DOI: 10.4064/aa143-3-8

and

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

where the last summation is over all $1 \le c \le q$ with $(c,q)=1$, and $p^\alpha \parallel q$ denotes that p^α divides q, but $p^{\alpha+1}$ does not divide q.

The formula (2) shows that the error term in the asymptotic formula (1) is the best possible. In this paper, we find that there exist close relations between the error terms $E(c,q)$ and the classical Kloosterman sums

$$K(m,n,q) = \sum_{b=1}^{q}{}' e\bigg(\frac{mb+n\bar{b}}{q}\bigg),$$

where $e(y) = e^{2\pi i y}$, and $b\cdot\bar{b}\equiv 1 \bmod q$.

We shall use the properties of the Gauss sums and the analytic method to study the mean value properties of $K(c,1;q)E(4c,q)$, and give a sharper asymptotic formula for it. We shall prove the following:

THEOREM. *For any odd integer $q \ge 3$, we have the asymptotic formula*

$$\sum_{c=1}^{q}{}' K(c,1;q)E(4c,q) = \frac{4}{\pi^2}\,q\phi(q)\prod_{p\|q}\bigg(1-\frac{1}{p(p-1)}\bigg) + O\bigg(q\cdot\exp\bigg(\frac{13\ln q}{\ln\ln q}\bigg)\bigg).$$

2. Some lemmas. In this section, we give some simple lemmas which are necessary in the proof of our Theorem. First we have the following:

LEMMA 1 (see Theorem 7.2 in [4]). *Let q be a square-full number (i.e. $p \mid k$ if and only if $p^2 \mid k$). Then for any nonprimitive character χ modulo q, we have the identity*

$$\tau(\chi) = \sum_{a=1}^{q}\chi(a)e\bigg(\frac{a}{q}\bigg) = 0.$$

LEMMA 2. *Let u be a square-full number or $u=1$, and v be a square-free number with $(u,v)=1$. Then we have the identity*

$$\sum_{h\mid v} h^2 \sum_{k\mid uh}\mu(k)\phi\bigg(\frac{uh}{k}\bigg) = \frac{v\phi^2(uv)}{u}\prod_{p\mid v}\bigg(1-\frac{1}{p(p-1)}\bigg).$$

Proof. Since $\phi(n)$ and $\mu(n)$ are multiplicative functions, and v is a square-free number, we have

$$\sum_{h|v} h^2 \sum_{k|uh} \mu(k)\phi\left(\frac{uh}{k}\right) = \sum_{h|v} h^2 \sum_{r|h} \mu(r)\phi\left(\frac{h}{r}\right) \sum_{s|u} \mu(s)\phi\left(\frac{u}{s}\right)$$
$$= \left(\sum_{s|u} \mu(s)\phi\left(\frac{u}{s}\right)\right) \sum_{h|v} h^2 \prod_{p|h} (p-2)$$
$$= \left(\sum_{s|u} \mu(s)\phi\left(\frac{u}{s}\right)\right) \prod_{p|v} (1 + p^2(p-2)). \tag{3}$$

If $u = 1$, then $\sum_{s|u} \mu(s)\phi(u/s) = 1 = \phi^2(u)/u$; if $u > 1$ is a square-full number, then also

$$\sum_{s|u} \mu(s)\phi\left(\frac{u}{s}\right) = \prod_{p^\alpha \| u} (\phi(p^\alpha) - \phi(p^{\alpha-1}))$$
$$= \phi(u) \prod_{p^\alpha \| u} \left(1 - \frac{1}{p}\right) = \frac{\phi^2(u)}{u}. \tag{4}$$

Note the identity

$$\prod_{p|v} (1 + p^2(p-2)) = \prod_{p|v} p(p-1)^2 \left(1 - \frac{1}{p(p-1)}\right)$$
$$= v\phi^2(v) \prod_{p|v} \left(1 - \frac{1}{p(p-1)}\right).$$

Combining (3) and (4) we may immediately deduce Lemma 2.

LEMMA 3 (see [2] and Lemma 6 in [6]). *Suppose χ is an odd character mod q, generated by the primitive character χ_m mod m. Then we have the identities*

$$(1 - 2\chi(2)) \sum_{a=1}^{q} a\chi(a) = \chi(2) q \sum_{a=1}^{(q-1)/2} \chi(a)$$

and

$$\sum_{a=1}^{q} a\chi(a) = \frac{q}{m} \Big(\prod_{\substack{p|q \\ p \nmid m}} (1 - \chi_m(p)) \Big) \Big(\sum_{a=1}^{m} a\chi_m(a) \Big).$$

LEMMA 4. *Let $q \geq 3$ be an odd number. Then for any integer c with $(c, q) = 1$, we have*

$$E(c, q) = -\frac{2}{\phi(q)} \sum_{\substack{\chi \bmod q \\ \chi(-1) = -1}} \overline{\chi}(c)(1 - 2\chi(2))^2 \left(\frac{1}{q} \sum_{a=1}^{q} a\chi(a)\right)^2.$$

Proof. From the definition of $N(c,q)$ and the orthogonality of characters mod q we have

$$N(c,q)=\frac{1}{2}\sum_{\substack{a=1\\ ab\equiv c \bmod q}}^{q}\sum_{b=1}^{q}(1-(-1)^{a+b})=\frac{1}{2}\phi(q)-\frac{1}{2}\sum_{\substack{a=1\\ ab\equiv c \bmod q}}^{q}\sum_{b=1}^{q}(-1)^{a+b}.$$

Hence

$$E(c,q)=N(c,q)-\frac{1}{2}\phi(q)=-\frac{1}{2}\sum_{\substack{a=1\\ ab\equiv c \bmod q}}^{q}\sum_{b=1}^{q}(-1)^{a+b} \tag{5}$$

$$=-\frac{1}{2\phi(q)}\sum_{\chi \bmod q}\overline{\chi}(c)\Big(\sum_{a=1}^{q}(-1)^a\chi(a)\Big)^2.$$

Note that if $\chi(-1)=1$, then

$$\sum_{a=1}^{q}(-1)^a\chi(a)=0, \tag{6}$$

and if $\chi(-1)=-1$, then

$$\sum_{a=1}^{q}(-1)^a\chi(a)=2\chi(2)\sum_{a=1}^{(q-1)/2}\chi(a). \tag{7}$$

Combining (5)–(7) and Lemma 3 we immediately deduce Lemma 4.

3. Proof of Theorem. Let $q=u\cdot v$, where u is a square-full number or $u=1$, and v is a square-free number with $(u,v)=1$. Then for any nonprincipal character χ mod q, we have $\chi=\chi_1\chi_2$, where χ_1 is a character mod u and χ_2 is a character mod v. If χ_1 is a nonprimitive character mod u, then from the multiplicative properties of the Gauss sums and Lemma 1 we know that $\tau(\chi)=\tau(\chi_1\chi_2)=0$. Note that if χ is a primitive character mod m with $\chi(-1)=-1$, then (see Theorems 12.11 and 12.20 of [1])

$$\frac{1}{m}\sum_{a=1}^{m}a\chi(a)=\frac{i}{\pi}\tau(\chi)L(1,\overline{\chi}),$$

$$\sum_{c=1}^{q}{}'\overline{\chi}(c)K(c,1;q)=\sum_{b=1}^{q}{}'\sum_{c=1}^{q}{}'\overline{\chi}(c)e\Big(\frac{cb+\bar{b}}{q}\Big)=\tau^2(\overline{\chi}),$$

$$\sum_{\substack{\chi \bmod q\\ \chi(-1)=-1}}^{*}\chi(a)=\sum_{d|q}\mu(d)\sum_{\chi \bmod q/d}\chi(r)=\sum_{d|(q,a-1)}\mu\Big(\frac{q}{d}\Big)\phi(d),$$

and for any nonprincipal character χ mod q, from the Pólya and Vinogradov inequality (see Theorem 8.21 of [1]) we know that

$$\sum_{n=N+1}^{N+H} \chi(n) \ll q^{1/2} \ln q.$$

By this estimate and the partition identities (see Theorem 3.17 of [1]) we can deduce that ($q^3 \le y$)

$$\begin{aligned} A(\chi, y) &= \sum_{q^3 < n \le y} \chi(n) d(n) = \sum_{mn \le y} \chi(m)\chi(n) - \sum_{mn \le q^3} \chi(m)\chi(n) \\ &= 2 \sum_{n \le \sqrt{y}} \chi(n) \sum_{m \le y/n} \chi(m) - \Big(\sum_{n \le \sqrt{y}} \chi(n) \Big)^2 \\ &\quad - 2 \sum_{n \le \sqrt{q^3}} \chi(n) \sum_{m \le q^3/n} \chi(m) + \Big(\sum_{n \le \sqrt{q^3}} \chi(n) \Big)^2 \ll \sqrt{qy} \ln q. \end{aligned}$$

Applying this estimate and Abel's identity we have the asymptotic formula

$$\begin{aligned} L^2(1, \chi) &= \sum_{1 \le n \le q^3} \frac{d(n)\chi(n)}{n} + \int_{q^3}^{+\infty} \frac{A(\chi, y)}{y^2}\, dy \\ &= \sum_{1 \le n \le q^3} \frac{d(n)\chi(n)}{n} + O\Big(\frac{\ln q}{q} \Big). \end{aligned} \tag{8}$$

Let $h \,|\, v$, $\chi = \chi_1 \chi_2$ be a character mod uh, where χ_1 is a character mod u and χ_2 is a character mod h. If χ_1 is a primitive character mod u, χ_2 is a primitive character mod h, and χ_v^0 denotes the principal character mod v, then we have the identity

$$\tau^2(\overline{\chi}\chi_v^0)\tau^2(\chi) = \overline{\chi}^2\Big(\frac{v}{h}\Big)\chi(-1)^{2\omega(v/h)}\tau^2(\overline{\chi})\tau^2(\chi) = \overline{\chi}^2\Big(\frac{v}{h}\Big)u^2h^2,$$

where $\omega(n)$ denotes the number of different prime divisors of n.

Let χ_1 be a nonprimitive character mod u. Then from the multiplicative properties of the Gauss sums and Lemma 1 we know that $\tau(\overline{\chi}\chi_v^0) = 0$.

By Lemma 3, Lemma 4 and the above identities we have

$$\begin{aligned} &\sum_{c=1}^{q}{}' K(c, 1; q) E(4c, q) \\ &\quad = -\frac{2}{\phi(q)} \sum_{\substack{\chi \bmod q \\ \chi(-1) = -1}} \sum_{c=1}^{q}{}' \overline{\chi}(4c) K(c, 1; q) (1 - 2\chi(2))^2 \Big(\frac{1}{q} \sum_{a=1}^{q} a\chi(a) \Big)^2 \end{aligned} \tag{9}$$

$$= -\frac{2}{\phi(q)} \sum_{\substack{\chi \bmod q \\ \chi(-1)=-1}} \tau^2(\overline{\chi})(\overline{\chi}(2)-2)^2 \Big(\frac{1}{q}\sum_{a=1}^{q} a\chi(a)\Big)^2$$

$$= -\frac{2}{\phi(q)} \sum_{\substack{\chi_1 \bmod u \\ \chi_1\chi_2(-1)=-1}} \sum_{\chi_2 \bmod v} \tau^2(\overline{\chi_1\chi_2})(\overline{\chi_1\chi_2}(2)-2)^2 \Big(\frac{1}{q}\sum_{a=1}^{q} a\chi_1\chi_2(a)\Big)^2$$

$$= -\frac{2}{\phi(q)} \sum_{\substack{\chi_1 \bmod u \\ \chi_1\chi_2(-1)=-1}}^{*} \sum_{\chi_2 \bmod v} \tau^2(\overline{\chi_1\chi_2})(\overline{\chi_1\chi_2}(2)-2)^2 \Big(\frac{1}{q}\sum_{a=1}^{q} a\chi_1\chi_2(a)\Big)^2$$

$$= \frac{2}{\pi^2\phi(q)} \sum_{h|v} \sum_{\substack{\chi \bmod uh \\ \chi(-1)=-1}}^{*} \tau^2(\overline{\chi}\chi_v^0)(\overline{\chi}(2)-2)^2 \Big(\sum_{\substack{r|v \\ (r,uh)=1}} \chi(r)\mu(r)\Big)^2 \tau^2(\chi) L^2(1,\overline{\chi})$$

$$= \frac{2u^2}{\pi^2\phi(q)} \sum_{h|v} h^2 \sum_{\substack{\chi \bmod uh \\ \chi(-1)=-1}}^{*} (\overline{\chi}(2)-2)^2 \Big(\overline{\chi}\Big(\frac{v}{h}\Big)\sum_{r|v/h} \chi(r)\mu(r)\Big)^2 L^2(1,\overline{\chi})$$

$$= \frac{2u^2}{\pi^2\phi(q)} \sum_{h|v} h^2 \sum_{k|uh} \mu(k) \sum_{\substack{\chi \bmod uh/k \\ \chi(-1)=-1}} (\overline{\chi}(2)-2)^2 \Big(\sum_{r|v/h} \overline{\chi}(r)\mu(r)\Big)^2 L^2(1,\overline{\chi}),$$

where $\sum_{\chi \bmod k}^{*}$ denotes summation over all primitive characters mod k.

On the other hand, note that

$$\sum_{\substack{\chi \bmod uh/k \\ \chi(-1)=-1}} |\overline{\chi}(2)-2|^2 \Big|\sum_{r|v/h} \overline{\chi}(r)\mu(r)\Big|^2 \ll 4^{\omega(v/h)}\,\frac{uh}{k}.$$

From (8) we also have

$$\begin{aligned}(10)\qquad &\sum_{\substack{\chi \bmod uh/k \\ \chi(-1)=-1}} (\overline{\chi}(2)-2)^2 \Big(\sum_{r|v/h} \overline{\chi}(r)\mu(r)\Big)^2 L^2(1,\overline{\chi}) \\ &= \sum_{n\le q^3}{}' \frac{d(n)}{n} \sum_{r|v/h} \sum_{s|v/h} \sum_{\substack{\chi \bmod uh/k \\ \chi(-1)=-1}} (\overline{\chi}(4)-4\overline{\chi}(2)+4)\overline{\chi}(rs)\overline{\chi}(n)\mu(r)\mu(s) \\ &\quad + O(4^{\omega(v/h)}\ln q) \\ &= \frac{\phi(uh/k)}{2} \sum_{\substack{n\le q^3 \\ 4rsn\equiv 1 \bmod uh/k}}{}' \sum_{r|v/h} \sum_{s|v/h} \frac{d(n)\mu(r)\mu(s)}{n}\end{aligned}$$

$$
\begin{aligned}
&- \frac{\phi(uh/k)}{2} \sum_{\substack{n\le q^3 \\ 4rsn\equiv -1 \bmod uh/k}}{}' \sum_{r|v/h} \sum_{s|v/h} \frac{d(n)\mu(r)\mu(s)}{n} \\
&- 4\frac{\phi(uh/k)}{2} \sum_{\substack{n\le q^3 \\ 2rsn\equiv 1 \bmod uh/k}}{}' \sum_{r|v/h} \sum_{s|v/h} \frac{d(n)\mu(r)\mu(s)}{n} \\
&+ 4\frac{\phi(uh/k)}{2} \sum_{\substack{n\le q^3 \\ 2rsn\equiv -1 \bmod uh/k}}{}' \sum_{r|v/h} \sum_{s|v/h} \frac{d(n)\mu(r)\mu(s)}{n} \\
&+ 4\frac{\phi(uh/k)}{2} \sum_{\substack{n\le q^3 \\ rsn\equiv 1 \bmod uh/k}}{}' \sum_{r|v/h} \sum_{s|v/h} \frac{d(n)\mu(r)\mu(s)}{n} \\
&- 4\frac{\phi(uh/k)}{2} \sum_{\substack{n\le q^3 \\ rsn\equiv -1 \bmod uh/k}}{}' \sum_{r|v/h} \sum_{s|v/h} \frac{d(n)\mu(r)\mu(s)}{n} + O(4^{\omega(v/h)}\ln q) \\
&= 2\phi\Big(\frac{uh}{k}\Big) + O\Big(\sum_{r|v/h}\sum_{s|v/h}\sum_{l\le q^3k/uh} \frac{d(luh/k \pm rs)}{l}\Big) + O(4^{\omega(v/h)}\ln q) \\
&= 2\phi\Big(\frac{uh}{k}\Big) + O\Big(\exp\Big(\frac{11\ln q}{\ln\ln q}\Big)\Big),
\end{aligned}
$$

where we have used the estimate $d(n) \ll \exp\big(\frac{2\ln n}{\ln\ln n}\big)$, and $\sum'_{n\le N}$ denotes summation over all integers $1 \le n \le N$ with $(n, uh/k) = 1$.

In fact in (10), the main term comes from the sum with the condition $rsn = 1 \bmod uh/k$ when $r = s = n = 1$, and the other error terms are bounded by

$$
\begin{aligned}
\sum_{r|v/h}\sum_{s|v/h}\sum_{l\le q^3k/uh} \frac{d(uh/k \pm rs)}{l} &\ll \exp\Big(\frac{6\ln q}{\ln\ln q}\Big)\ln q\Big(\sum_{r|v/h} 1\Big)^2 \\
&\ll \exp\Big(\frac{11\ln q}{\ln\ln q}\Big).
\end{aligned}
$$

On the other hand, note the identity

$$
\frac{u^2}{\phi(q)} \sum_{h|v} h^2 \cdot 2^{\omega(uh)} = \frac{q^2}{\phi(q)v^2} \sum_{h|v} h^2 \cdot 2^{\omega(uh)},
$$

since u and h are coprime, and thus

$$
\frac{u^2}{\phi(q)} \sum_{h|v} h^2 \cdot 2^{\omega(uh)} = \frac{q^2 2^{\omega(u)}}{\phi(q)} \frac{1}{v^2} \sum_{h|v} h^2 \cdot 2^{\omega(h)}.
$$

Now using the fact that v is square-free and $h^2 2^{\omega(h)}$ is multiplicative we get

$$\begin{aligned}(11)\qquad \frac{u^2}{\phi(q)}\sum_{h|v} h^2\cdot 2^{\omega(uh)} &= \frac{q^2 2^{\omega(u)}}{\phi(q)}\,\frac{1}{v^2}\prod_{p|v}(1+2p^2)\\ &\le \frac{q^2 2^{\omega(u)}}{\phi(q)}\prod_{p|v}\left(1+\frac{2}{(v/p)^2}\right)\\ &\ll \frac{q^2 2^{\omega(u)}}{\phi(q)}\prod_{n=1}^{\infty}\left(1+\frac{2}{n^2}\right)\ll \frac{q^2 2^{\omega(u)}}{\phi(q)}\\ &\ll q2^{\omega(u)}\ln q \ll q\cdot\exp\left(\frac{2\ln q}{\ln\ln q}\right).\end{aligned}$$

Combining (9)–(11) we immediately deduce the asymptotic formula of the Theorem.

Acknowledgments. The authors express their gratitude to the referee for his very helpful and detailed comments.

This work was supported by the N.S.F. (10671155) of P.R. China.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.
[2] T. Funakura, *On Kronecker's limit formula for Dirichlet series with periodic coefficients*, Acta Arith. 55 (1990), 59–73.
[3] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1981, 139–140.
[4] L. K. Hua, *Introduction to Number Theory*, Science Press, Beijing, 1979.
[5] W. P. Zhang, *On a problem of D. H. Lehmer and its generalization*, Compos. Math. 86 (1993), 307–316.
[6] —, *A problem of D. H. Lehmer and its generalization (II)*, ibid. 91 (1994), 47–56.
[7] —, *A problem of D. H. Lehmer and its mean value formula*, Japan. J. Math. 29 (2003), 109–116.
[8] —, *On the difference between an integer and its inverse modulo n (II)*, Sci. China Ser. A 46 (2003), 229–238.

Wenpeng Zhang
Department of Mathematics
Northwest University
Xi'an, Shaanxi, 710069
P.R. China
E-mail: wpzhang@nwu.edu.cn

Zhaoxia Wu
School of Applied Mathematics
Xinjiang University of Finance and Economics
Urmq, 830011
P.R. China
E-mail: wuzhaoxia828@163.com

Received on 23.7.2009
and in revised form on 6.1.2010 (6095)