

COMPOSITIO MATHEMATICA

ZHANG WENPENG

A problem of D. H. Lehmer and its generalization (II)

Compositio Mathematica, tome 91, n° 1 (1994), p. 47-56

http://www.numdam.org/item?id=CM_1994__91_1_47_0

© Foundation Compositio Mathematica, 1994, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

A problem of D. H. Lehmer and its generalization (II)*

ZHANG WENPENG

Department of Mathematics, Northwest University, Xi'an, China

Accepted 28 August 1992; accepted in final form 12 January 1993

Abstract. Let $q > 2$ be an odd number. For each integer x with $0 < x < q$ and $(q, x) = 1$, we define \bar{x} by $x\bar{x} \equiv 1 \pmod{q}$ and $0 < \bar{x} < q$. Let $r(q)$ be the number of integers x with $0 < x < q$ for which x and \bar{x} are of opposite parity. The main purpose of this paper is to give a sharper asymptotic formula for $r(q)$ for all odd numbers q .

1. Introduction

Let q be an odd integer > 2 . For each integer x with $0 < x < q$ and $(q, x) = 1$, we know that there exists one and only one \bar{x} with $0 < \bar{x} < q$ such that $x\bar{x} \equiv 1 \pmod{q}$. Let $r(q)$ be the number of cases in which x and \bar{x} are of opposite parity. For example, $r(3) = 0$, $r(5) = 2$, $r(7) = 0$, $r(13) = 6$. For $q = p$ a prime, D. H. Lehmer [1] asks us to find $r(p)$ or at least to say something nontrivial about it. It is known that $r(p) \equiv 2$ or $0 \pmod{4}$ according to $p \equiv \pm 1 \pmod{4}$. About this problem, the author [2] obtained an asymptotic formula for $r(p^2)$ and $r(p_1 p_2)$, where p , p_1 and p_2 are primes. In this paper, as an improvement of [2], we shall give an asymptotic formula for $r(q)$ for all odd numbers q . The constants implied by the O -symbols and the symbols \ll , \gg used in this paper do not depend on any parameter, unless otherwise indicated. By using estimates for character sum and Kloosterman sums, and the properties of Dirichlet L-functions, we prove the following two theorems:

THEOREM 1. *For every prime $p > 2$ we have the asymptotic formula*

$$r(p) = \frac{1}{2} p + \frac{1}{\pi^2} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ab} \{S(a, b; p) - S(a, -b; p) \\ + 4S(\bar{4}a, b; p) - 4S(\bar{4}a, -b; p) - 4S(\bar{2}a, b; p) \\ + 4S(\bar{2}a, -b; p)\} + O(\ln^3 p)$$

where $d\bar{d} \equiv 1 \pmod{p}$, $S(m, n; p) = \sum'_{d \pmod{p}} e\left(m \frac{d}{p} + n \frac{\bar{d}}{p}\right)$ is the Kloosterman sum, and $e(y) = e^{2\pi iy}$.

*Project supported by the National Natural Science Foundation of China.

THEOREM 2. For every odd integer $q > 2$ we have

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

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

From theorem 1 we can see that if we could get a nontrivial upper bound estimate for the mean value $\sum_{q=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ab} S(ma, b; p)$, then we may obtain a more accurate asymptotic formula. From theorem 2 we can also deduce the following:

COROLLARY. For every prime $p > 2$ we have the asymptotic formula

$$r(p) = \frac{1}{2}p + O(p^{1/2} \ln^2 p)$$

2. Some lemmas

To complete the proofs of the theorems, we need some lemmas. First we have:

LEMMA 1. Let $q > 2$ be an odd number. Then we have

$$r(q) = \frac{1}{2}\phi(q) - \frac{2}{\phi(q)} \sum_{\chi(-1)=-1} \chi(4) \left(\sum_{a=1}^{(q-1)/2} \chi(a) \right)^2$$

where the summation is over all odd characters mod q .

Proof. From the definition of $r(q)$ and the orthogonality of characters we get

$$\begin{aligned} r(q) &= \frac{1}{2} \sum_{a=1}^{q-1} \sum_{\substack{b=1 \\ ab \equiv 1(q)}}^{q-1} \{1 - (-1)^{a+b}\} \\ &= \frac{1}{2} \phi(q) - \frac{1}{2} \sum_{\substack{a=1 \\ ab \equiv 1(q)}}^{q-1} \sum_{b=1}^{q-1} (-1)^{a+b} \\ &= \frac{1}{2} \phi(q) - \frac{1}{2\phi(q)} \sum_{\chi \bmod q} \left(\sum_{a=1}^{q-1} (-1)^a \chi(a) \right)^2 \\ &= \frac{1}{2} \phi(q) - \frac{1}{2\phi(q)} \sum_{\chi \neq \chi^0} \left(\sum_{a=1}^{q-1} (-1)^a \chi(a) \right)^2 \end{aligned} \tag{1}$$

where $\sum_{\chi \neq \chi^0}$ denotes the summation over all nonprincipal characters mod q .

Now if $\chi(-1) = 1$ and $\chi \neq \chi^0$, then we have

$$\sum_{a=1}^{q-1} (-1)^a \chi(a) = 0 \tag{2}$$

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

$$\sum_{a=1}^{q-1} (-1)^a \chi(a) = 2 \sum_{a=1}^{(q-1)/2} \chi(2a) \tag{3}$$

Combining (1), (2) and (3) we may immediately deduce lemma 1. □

LEMMA 2. *Let $q > 1$ be any odd number and let χ be any Dirichlet character modulo q , not necessarily primitive. Then*

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

Proof. (See reference [3]). □

LEMMA 3. *Let m, n, q be integers with $q > 1$. Then*

$$S(m, n; q) = \sum_{d=1}^{q-1} e \left(m \frac{d}{q} + n \frac{\bar{d}}{q} \right) \ll (m, n, q)^{1/2} q^{1/2} d(q)$$

where $d\bar{d} \equiv 1 \pmod{q}$, $d(q)$ is the divisor function, and (m, n, q) denotes the greatest common factor of m, n and q . \sum'_a denotes the summation over a such that $(a, q) = 1$.

Proof. (See reference [4]). □

LEMMA 4. *Let q be an odd integer > 2 . Then for any integer b we have the estimate*

$$\sum_{\chi(-1)=-1} \tau^2(\chi) \chi(b) L^2(1, \bar{\chi}) \ll \phi(q) q^{1/2} d(q) \ln^2 q$$

where $L(s, \chi)$ is the Dirichlet L -function and $\tau(\chi)$ is the Gauss sum corresponding to χ .

Proof. First for any integer r with $(r, q) = 1$ we have

$$\sum_{\chi(-1)=-1} \chi(r) = \begin{cases} \frac{1}{2} \phi(q), & \text{if } r \equiv 1 \pmod{q}, \\ -\frac{1}{2} \phi(q), & \text{if } r \equiv -1 \pmod{q}, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

$$\begin{aligned} \frac{2}{p-1} \sum_{\chi_p(-1)=-1} \tau^2(\chi)\chi(b)L^2(1, \bar{\chi}) &= \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ac} S(\bar{b}, ac; p) \\ &- \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \frac{1}{ac} S(\bar{b}, -ac; p) + O(\ln^3 p) \end{aligned}$$

Proof. Let $K(r, q) = \sum_{a=1}^{p-1} a^q e\left(\frac{ra}{p}\right)$, $p \nmid r$, then we have the estimate

$$K(r, q) \ll \frac{p^q}{\left| \sin\left(\frac{\pi r}{p}\right) \right|} \tag{7}$$

Namely we have

$$\begin{aligned} K(\gamma, q) \left(1 - e\left(\frac{\gamma}{p}\right)\right) &= \sum_{a=1}^{p-1} a^q \left(e\left(\frac{\gamma a}{p}\right) - e\left(\frac{(a+1)\gamma}{p}\right)\right) \\ &= \sum_{a=1}^{p-2} ((a+1)^q - a^q) e\left(\frac{(a+1)\gamma}{p}\right) + e\left(\frac{\gamma}{p}\right) - (p-1)^q e\left(\frac{p\gamma}{p}\right) \\ &\ll p^q + \sum_{a=1}^{p-2} ((a+1)^q - a^q) \ll p^q. \end{aligned}$$

Thus

$$|K(\gamma, q)| \ll \frac{p^q}{\left|1 - e\left(\frac{\gamma}{p}\right)\right|} \ll \frac{p^q}{\left|\sin\left(\frac{\pi\gamma}{p}\right)\right|}.$$

This completes the proof of (7). □

By applying (6) with $q = p$, $N = p^2 + p$ we get

$$\begin{aligned} \frac{2}{p-1} \sum_{\chi_p(-1)=-1} \tau^2(\chi)\chi(b)L^2(1, \bar{\chi}) &= \sum'_{1 \leq m, n \leq p^2+p} \frac{1}{mn} \{S(1, \bar{b}mn; p) - S(1, -\bar{b}mn; p)\} + O\left(\frac{\ln^2 p}{\sqrt{p}}\right) \\ &= \sum_{a=1}^{p-1} \sum_{n=0}^p \sum_{c=1}^{p-1} \sum_{m=0}^p \frac{1}{(np+a)(mp+a)} \{S(1, \bar{b}ac; p) - S(1, -\bar{b}ac; p)\} \\ &+ O\left(\frac{\ln^2 p}{\sqrt{p}}\right) \end{aligned}$$

$$\begin{aligned}
&= \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \frac{1}{ac} \{S(\bar{b}, ac; p) - S(\bar{b}, -ac; p)\} + O\left(\frac{\ln^2 p}{\sqrt{p}}\right) \\
&\quad + \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^p \frac{1}{a(mp+c)} \{S(1, \bar{b}ac; p) - S(1, -\bar{b}ac; p)\} \\
&\quad + \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{n=1}^p \frac{1}{c(np+a)} \{S(1, \bar{b}ac; p) - S(1, -\bar{b}ac; p)\} \\
&\quad + \sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^p \sum_{n=1}^p \frac{1}{(np+a)(mp+c)} \{S(1, \bar{b}ac; p) - S(1, -\bar{b}ac; p)\} \\
&\equiv M_1 + O\left(\frac{\ln^2 p}{\sqrt{p}}\right) + M_2 + M_3 + M_4 \tag{8}
\end{aligned}$$

It is clear that M_1 is the main term of lemma 5. Now we shall estimate the other three terms M_2 , M_3 and M_4 . Using the power series expansion of $(1-x)^{-1}$ we get

$$\begin{aligned}
&\sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^p \frac{1}{a(mp+c)} S(1, \bar{b}ac; p) \\
&= \sum_{a=1}^{p-1} \frac{1}{a} \sum_{c=1}^{p-1} \sum_{m=1}^p \frac{1}{(m+1)p - (p-c)} S(1, \bar{b}ac; p) \\
&= \sum_{a=1}^{p-1} \frac{1}{a} \sum_{k=0}^{\infty} \frac{1}{p^{k+1}} \sum_{m=1}^p \frac{1}{(m+1)^{k+1}} \sum_{c=1}^{p-1} (p-c)^k S(1, \bar{b}ac; p) \\
&= \sum_{a=1}^{p-1} \frac{1}{a} \sum_{k=0}^{\infty} \frac{1}{p^{k+1}} \sum_{m=1}^p \frac{1}{(m+1)^{k+1}} \sum_{c=1}^{p-1} c^k S(1, -\bar{b}ac; p) \tag{9}
\end{aligned}$$

Applying (7) we get the estimate

$$\begin{aligned}
\sum_{c=1}^{p-1} c^k S(1, -\bar{b}ac; p) &= \sum_{d=1}^{p-1} e\left(\frac{d}{p}\right) \sum_{c=1}^{p-1} c^k e\left(\frac{-\bar{b}acd}{p}\right) \\
&\ll \sum_{d=1}^{p-1} \left| \frac{p^k}{\sin\left(\frac{\pi \bar{b}ad}{p}\right)} \right| \ll p^{k+1} \ln p \tag{10}
\end{aligned}$$

From (9) and (10) we immediately deduce the estimate

$$\sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^p \frac{1}{a(mp+c)} S(1, \bar{b}ac; p)$$

$$\begin{aligned} &\ll \sum_{a=1}^{p-1} \frac{1}{a} \sum_{m=1}^p \sum_{k=0}^{\infty} \frac{1}{(m+1)^{k+1} p^{k+1}} \cdot p^{k+1} \ln p \\ &\ll \sum_{a=1}^{p-1} \frac{1}{a} \sum_{m=1}^p \frac{1}{m+1} \ln p \ll \ln^3 p \end{aligned} \tag{11}$$

Similarly we can deduce that

$$\sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^p \frac{1}{a(mp+c)} S(1, -\bar{b}ac; p) \ll \ln^3 p \tag{12}$$

Combining (11) and (12) we get

$$M_2 \ll \ln^3 p \tag{13}$$

In the same way we get the estimates

$$M_3 \ll \ln^3 p \tag{14}$$

$$M_4 \ll \ln^3 p \tag{15}$$

Now lemma 5 follows at once from (8), (13), (14) and (15). □

LEMMA 6. *Suppose χ is an odd character mod q , generated by the primitive character χ_m mod m . Then we have*

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

Proof. Let l be the largest divisor of q that is coprime with m . Then we have

$$\begin{aligned} \sum_{a=1}^q a\chi(a) &= \sum_{i=0}^{(q/ml)-1} \sum_{j=1}^{ml} (iml+j)\chi(iml+j) \\ &= \sum_{i=0}^{(q/ml)-1} \sum_{j=1}^{ml} (iml+j)\chi(j) = \frac{q}{ml} \sum_{j=1}^{lm} j\chi(j) \\ &= \frac{q}{lm} \sum_{a=1}^{lm} a\chi_m(a) \sum_{\substack{d|a \\ d|l}} \mu(d) \\ &= \frac{q}{lm} \sum_{d|l} \mu(d) \sum_{\substack{a=1 \\ d|a}}^{lm} a\chi_m(a) \end{aligned}$$

$$\begin{aligned}
&= \frac{q}{lm} \sum_{d|l} \mu(d) d \chi_m(d) \sum_{b=1}^{lm/d} b \chi_m(b) \\
&= \frac{q}{lm} \sum_{d|l} \mu(d) d \chi_m(d) \sum_{i=0}^{(l/d)-1} \sum_{j=1}^m (im+j) \chi_m(im+j) \\
&= \frac{q}{lm} \sum_{d|l} \mu(d) d \chi_m(d) \cdot \frac{l}{d} \sum_{a=1}^m a \chi_m(a) \\
&= \frac{q}{m} \left(\prod_{\substack{p|q \\ p \nmid m}} (1 - \chi_m(p)) \right) \left(\sum_{a=1}^m a \chi_m(a) \right)
\end{aligned}$$

This proves lemma 6. \square

LEMMA 7. Let χ be a primitive character mod m with $\chi(-1) = -1$. Then we have

$$\frac{1}{m} \sum_{\gamma=1}^m \gamma \chi(\gamma) = -\frac{i}{\pi} \tau(\chi) L(1, \bar{\chi})$$

Proof. (See Theorem 12.11 and Theorem 12.20 of [5]). \square

3. Proof of the theorems

In this section, we shall complete the proofs of the theorems. First we prove theorem 2. From lemmas 2, 4, 6 and lemma 7 we know that for every odd integer $q > 2$,

$$\begin{aligned}
&\sum_{\chi(-1)=-1} \chi(4) \left(\sum_{a=1}^{(q-1)/2} \chi(a) \right)^2 \\
&= \frac{1}{q^2} \sum_{\chi(-1)=-1} (1 - 2\chi(2))^2 \left(\sum_{\gamma=1}^{q-1} \gamma \chi(\gamma) \right)^2 \\
&= \sum_{m|q} \sum_{\substack{\chi \bmod m \\ \chi(-1)=-1}}^* \frac{1}{m^2} (1 - 2\chi(2))^2 \left(\prod_{\substack{p|q \\ p \nmid m}} (1 - \chi_m(p)) \right)^2 \left(\sum_{a=1}^m a \chi_m(a) \right)^2 \\
&= -\frac{1}{\pi^2} \sum_{m|q} \sum_{\substack{\chi \bmod m \\ \chi(-1)=-1}}^* (1 - 2\chi_m(2))^2 \left(\prod_{\substack{p|q \\ p \nmid m}} (1 - \chi_m(p)) \right)^2 \tau^2(\chi_m) L^2(1, \bar{\chi}_m) \\
&= -\frac{1}{\pi^2} \sum_{m|q} \sum_{d|m} \mu\left(\frac{m}{d}\right) \sum_{\substack{\chi \bmod m \\ \chi(-1)=-1}} (1 - 2\chi(2))^2 \left(\prod_{\substack{p|q \\ p \nmid m}} (1 - \chi(p)) \right)^2 \tau^2(\chi) L^2(1, \bar{\chi})
\end{aligned}$$

$$\begin{aligned} &\ll \sum_{m|q} \sum_{k|m} 2^{\omega(q)-\omega(m)} k^{1/2} d(k) \phi(k) \ln^2 k \\ &\ll \phi(q) q^{1/2} d^2(q) \ln^2 q \end{aligned} \tag{16}$$

where $\omega(n)$ denotes the number of all distinct prime divisor of n . Now lemma 1 and (16) imply that

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

This completes the proof of theorem 2. □

Now we prove theorem 1. Let p be a prime > 2 . Note that every odd character $\chi \pmod p$ is a primitive character mod p . Thus, from lemma 2 and lemma 7 we derive

$$\begin{aligned} &\sum_{\chi_{p(-1)} = -1} \chi(4) \left(\sum_{a=1}^{(p-1)/2} \chi(a) \right)^2 \\ &= -\frac{1}{\pi^2} \sum_{\chi_{p(-1)} = -1} (1 - 2\chi(2))^2 \tau^2(\chi) L^2(1, \bar{\chi}) \\ &= -\frac{1}{\pi^2} \sum_{\chi_{p(-1)} = -1} (1 - 4\chi(2) + 4\chi(4)) \tau^2(\chi) L^2(1, \bar{\chi}) \end{aligned} \tag{17}$$

From (17), lemma 1 and lemma 5 we deduce that

$$\begin{aligned} r(p) &= \frac{1}{2} p + \frac{1}{\pi^2} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ab} \{S(1, ab; p) - S(1, -ab; p) \\ &\quad + 4S(\bar{4}, ab; p) - 4S(\bar{4}, -ab; p) - 4S(\bar{2}, ab; p) \\ &\quad + 4S(\bar{2}, -ab; p)\} + O(\ln^3 p) \end{aligned} \tag{18}$$

Notice that

$$\sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ab} S(m, ab; p) = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ab} S(ma, b; p).$$

Together with (18) this implies theorem 1.

References

- [1] Richard K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981, pp. 139–140.
- [2] Zhang Wenpeng, On a problem of D. H. Lehmer and its generalization, *Compositio Mathematica*, 86 (1993) 307–316.
- [3] Funakura, Takeo, On Kronecker's limit formula for Dirichlet series with periodic coefficients, *Acta Arith.*, 55 (1990), No. 1, pp. 59–73.
- [4] T. Estermann, On Kloostermann's sum, *Mathematica*, 8 (1961), pp. 83–86.
- [5] Apostol, Tom M, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
- [6] J.-M. Deshouillers and H. Iwaniec, Kloosterman Sums and Fourier coefficients of Cusp Forms, *Inventiones Mathematicae*, 70 (1982) pp. 219–288.