ZHANG WENPENG

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


<http://www.numdam.org/item?id=CM_1994__91_1_47_0>
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 \( \tilde{x} \) by \( x\tilde{x} \equiv 1 \pmod{q} \) and \( 0 < \tilde{x} < q \). Let \( r(q) \) be the number of integers \( x \) with \( 0 < x < q \) for which \( x \) and \( x \) 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 \( \tilde{x} \) with \( 0 < \tilde{x} < q \) such that \( x\tilde{x} \equiv 1 \pmod{q} \). Let \( r(q) \) be the number of cases in which \( x \) and \( \tilde{x} \) 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 \( r(p^a) \) and \( r(p_1p_2) \), 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 \( <<, >> \) 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

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

where \( d\bar{d} \equiv 1 \pmod{p} \), \( S(m, n; p) = \sum_{d \equiv 1 \pmod{p}} e(m \frac{d}{p} + n \frac{\bar{d}}{p}) \) 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 \( \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ab} S(ma, b; p) \), 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

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

where the summation is over all odd characters mod \( q \).

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

\[
r(q) = \frac{1}{2} \sum_{a=1}^{q-1} \sum_{b=1}^{q-1} \{1 - (-1)^{a+b}\}
\]

\[
= \frac{1}{2} \phi(q) - \frac{1}{2} \sum_{a=1}^{q-1} \sum_{b=1}^{q-1} (-1)^{a+b}
\]

\[
= \frac{1}{2} \phi(q) - \frac{1}{2 \phi(q)} \sum_{\chi \equiv 1(q)} \left( \sum_{a=1}^{(q-1)/2} \chi(a) \right)^2
\]

\[
= \frac{1}{2} \phi(q) - \frac{1}{2 \phi(q)} \sum_{\chi \equiv 1(q)} \left( \sum_{a=1}^{(q-1)/2} (-1)^a \chi(a) \right)^2
\]

(1)

where \( \sum_{\chi \equiv 1(q)} \) denotes the summation over all nonprincipal characters mod \( q \).
Now if $\chi(-1) = 1$ and $\chi \neq \chi^0$, then we have

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

(2)

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

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

(3)

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

**LEMMA 2.** Let $q > 1$ be any odd number and let $\chi$ 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

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

where $d \overline{d} \equiv 1 \pmod{q}$, $d(q)$ 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

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

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

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

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

(4)
Now for any $N > 1$, from the well-known Pólya-Vinogradov inequality (See Theorem 13.15 of [5]) we get for $\chi \neq \chi^0$

$$L(1, \tilde{\chi}) = \sum_{n \leq N} \frac{\bar{\chi}(n)}{n} + O\left(\frac{\sqrt{q \ln q}}{N}\right)$$ (5)

If $(b, q) > 1$, then $\chi(b) = 0$ and in this case it is clear that lemma 4 holds. Now we suppose that $(b, q) = 1$. On noticing that $|\tau(\chi)| \ll q^{1/2}$ and $\sum_{n \leq N} \bar{\chi}(n) \ll \ln N$, for $N \geq q$, we obtain from (4) and (5)

$$\sum_{\chi(-1) = -1} \tau^2(\chi)\chi(b)L^2(1, \tilde{\chi})$$

$$= \sum_{\chi(-1) = -1} \tau^2(\chi)\chi(b)\left(\sum_{n \leq N} \frac{\bar{\chi}(n)}{n} + O\left(\frac{\sqrt{q \ln q}}{N}\right)\right)^2$$

$$= \sum_{a=1}^{q-1} \sum_{c=1}^{q-1} \sum_{1 \leq m, n \leq N} \frac{1}{mn} \sum_{\chi(-1) = -1} \chi(a)\chi(b)\chi(c)\bar{\chi}(mn)e\left(\frac{a+c}{q}\right)$$

$$+ O\left(\frac{\phi(q)q^{3/2}\ln q \ln N}{N}\right)$$

$$= \frac{1}{2} \phi(q) \sum_{1 \leq m, n \leq N} \frac{1}{mn} \sum_{a=1}^{q-1} \sum_{c=1}^{q-1} e\left(\frac{a+c}{q}\right)$$

$$- \frac{1}{2} \phi(q) \sum_{1 \leq m, n \leq N} \frac{1}{mn} \sum_{a=1}^{q-1} \sum_{c=1, abc \equiv \pm mn(q)} e\left(\frac{a+c}{q}\right)$$

$$+ O\left(\frac{\phi(q)q^{3/2}\ln q \ln N}{N}\right)$$

$$= \frac{1}{2} \phi(q) \sum_{1 \leq m, n \leq N} \frac{1}{mn} \left\{S(1, \bar{b}mn; q) - S(1, -\bar{b}mn; q)\right\} + O\left(\frac{\phi(q)q^{3/2}\ln q \ln N}{N}\right)$$ (6)

Taking $N = q$, applying lemma 3 we may immediately get

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

This completes the proof of the lemma 4.

Lemma 5. Let $p$ be a prime $> 3$. Then for any integer $b$ with $(b, p) = 1$, we have
Proof. Let $K(r, q) = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ac} S(b, ac; p)$

Then we have the estimate

\[ \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ac} S(b, ac; p) + O(\ln^3 p) \]

Thus

This completes the proof of (7).

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

\[ \frac{2}{p-1} \sum_{x_p(-1) = -1} \tau^2(\chi) \chi(b) L^2(1, \chi) = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ac} S(b, ac; p) \]

Then

\[ \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \frac{1}{ac} S(b, ac; p) + O(\ln^3 p) \]

Thus

This completes the proof of (7).
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

\[
\sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^{p} \frac{1}{a(mp + c)} S(1, \overline{bac}; p) = \sum_{a=1}^{p-1} \frac{1}{a} \sum_{c=1}^{p-1} \sum_{m=1}^{p} \frac{1}{(m+1)p - (p-c)} S(1, \overline{bac}; p) = \sum_{a=1}^{p-1} \frac{1}{a} \sum_{k=0}^{\infty} \frac{1}{p^{k+1}} \sum_{m=1}^{p} \frac{1}{(m+1)^{k+1}} \sum_{c=1}^{p-1} (p - c)^k S(1, \overline{bac}; p) = \sum_{a=1}^{p-1} \frac{1}{a} \sum_{k=0}^{\infty} \frac{1}{p^{k+1}} \sum_{m=1}^{p} \frac{1}{(m+1)^{k+1}} \sum_{c=1}^{p-1} c^k S(1, \overline{bac}; p)
\]

Applying (7) we get the estimate

\[
\sum_{c=1}^{p-1} c^k S(1, \overline{bac}; p) = \sum_{d=1}^{p-1} e \left( \frac{d}{p} \right) \sum_{c=1}^{p-1} c^k e \left( \frac{-bac\overline{d}}{p} \right) \ll \sum_{d=1}^{p-1} \frac{p^k}{\sin \left( \frac{\pi b\overline{d}}{p} \right)} \ll p^{k+1} \ln p
\]

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

\[
\sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^{p} \frac{1}{a(mp + c)} S(1, \overline{bac}; p)
\]
Similarly we can deduce that

\[
\sum_{a=1}^{p-1} \sum_{c=1}^{p-1} \sum_{m=1}^{p} \frac{1}{a(mp + c)} S(1, -\beta ac; p) \ll \ln^3 p
\]  

(12)

Combining (11) and (12) we get

\[
M_2 \ll \ln^3 p
\]  

(13)

In the same way we get the estimates

\[
M_3 \ll \ln^3 p
\]  

(14)

\[
M_4 \ll \ln^3 p
\]  

(15)

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

\[ \square \]

**Lemma 6.** Suppose \( \chi \) is an odd character mod \( q \), generated by the primitive character \( \chi_m \mod m \). Then we have

\[
\sum_{a=1}^{q} a \chi(a) = \frac{q}{m} \left( \prod_{p \mid q} (1 - \chi_m(p)) \right) \left( \sum_{a=1}^{m} a \chi_m(a) \right)
\]

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

\[
\sum_{a=1}^{q} a \chi(a) = \sum_{i=0}^{(q/ml)-1} \sum_{j=1}^{ml} (iml + j) \chi(iml + j)
\]

\[
= \sum_{i=0}^{(q/ml)-1} \sum_{j=1}^{ml} (iml + j) \chi(j) = \frac{q}{ml} \sum_{j=1}^{lm} j \chi(j)
\]

\[
= \frac{q}{lm} \sum_{a=1}^{lm} a \chi_m(a) \sum_{d \mid a} \mu(d)
\]

\[
= \frac{q}{lm} \sum_{d \mid l} \mu(d) \sum_{a=1}^{lm} a \chi_m(a)
\]
LEMMA 7. Let \( \chi \) be a primitive character mod \( m \) with \( \chi(-1) = -1 \). Then we have

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

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

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 \( q > 2 \),

\[
\sum_{\chi(-1) = -1} \chi(4) \left( \sum_{a=1}^{\chi^{-1}/2} \chi(a) \right)^2
\]

\[
= \frac{1}{q^2} \sum_{\chi(-1) = -1} (1 - 2\chi(2))^2 \left( \sum_{\gamma=1}^{\chi^{-1}} \gamma \chi(\gamma) \right)^2
\]

\[
= \sum_{m|q} \sum_{\chi \mod m} \frac{1}{m^2} (1 - 2\chi(2))^2 \left( \prod_{p|q} (1 - \chi_m(p)) \right)^2 \left( \sum_{a=1}^{m} a\chi_m(a) \right)^2
\]

\[
= -\frac{1}{\pi^2} \sum_{m|q} \sum_{\chi \mod m} (1 - 2\chi_m(2))^2 \left( \prod_{p|q} (1 - \chi_m(p)) \right)^2 \tau^2(\chi_m) \mathcal{L}^2(1, \bar{\chi}_m)
\]

\[
= -\frac{1}{\pi^2} \sum_{m|q} \sum_{d|m} \frac{\mu(m)}{d} \sum_{\chi \mod m} (1 - 2\chi(2))^2 \left( \prod_{p|q} (1 - \chi(p)) \right)^2 \tau^2(\chi) \mathcal{L}^2(1, \bar{\chi})
\]
where \( \omega(n) \) denotes the number of all distinct prime divisors of \( n \). Now lemma 1 and (16) imply that

\[
\phi(q) q^{1/2} d(q) \ln^2 q
\]

This completes the proof of theorem 2.

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

\[
\sum_{\chi \mod p, \chi(-1) = -1} \chi(4) \left( \sum_{a=1}^{(p-1)/2} \chi(a) \right)^2
\]

\[
= -\frac{1}{p^2} \sum_{\chi \mod p, \chi(-1) = -1} (1 - 2\chi(2))^2 \tau^2(\chi)L^2(1, \tilde{\chi})
\]

\[
= -\frac{1}{p^2} \sum_{\chi \mod p, \chi(-1) = -1} (1 - 4\chi(2)^2 + 4\chi(4)) \tau^2(\chi)L^2(1, \tilde{\chi})
\]

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

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

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.
Zhang Wenpeng

References