ON THE GENERALIZATION OF A PROBLEM OF D. H. LEHMER

Yi YUAN and Zhang WENPENG

(Received 6 November 2000 and revised 23 May 2001)

1. Introduction

Let $q$ be an odd integer $\geq 3$. For each least positive residue $a \mod q$, relatively prime to $q$, we denote by $\overline{a}$ the inverse of $a \mod q$ taken as the least positive residue mod $q$ (only in this place; in general $\overline{a}$ denotes the inverse of $a \mod q$). Let $r(q)$ denote the number of cases in which $a$ and $\overline{a}$ are of opposite parity (namely $a$ is even [odd] and $\overline{a}$ is odd [even]). For $q = p$ a prime, D. H. Lehmer asks for a closed form for $r(p)$ or for something non-trivial to be said about it [2, p. 251].

The second author [3, 4] considered $r(q)$ and obtained a sharp asymptotic formula for it, which reads as follows.

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

where $\phi(q)$ denotes Euler’s function, $d(q) = \sum_{d|q} 1$ the divisor function ($d|q$ signifying that $d$ is the divisor of $q$) and $\ln q = \log_e q$ the natural logarithm.

For $q = p$ a prime, this gives an answer to Lehmer’s problem.

It is quite natural and interesting to consider the case of power residues, i.e. the least positive residues of $a^k$ and $\overline{a}^k$ with opposite parity (as suggested to us by Professor S. Kanemitsu during his stay in Xi’an).

To be more precise, let $N(k, q)$ ($k$ an integer $\geq 1$) denote the number of cases in which

$$q \left\{ \frac{a^k}{q} \right\} \text{ and } q \left\{ \frac{\overline{a}^k}{q} \right\}$$

are of opposite parity, where $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of $x$, $\lfloor x \rfloor$ denotes the integral part of $x$, thus $q\{a^k/q\}$ is the least positive residue mod $q$ of $a^k$.

In this paper we use estimate (10) in the second section for the general Kloosterman sums $S^k(r, s, q)$ to prove a sharp asymptotic formula for $N(k, q)$ in the same setting as in our former papers [3, 4].

Our main result is the following.
THEOREM. Let \( q \geq 3 \) be an odd integer and let \( k \) be a fixed positive integer. Then we have the asymptotic formula

\[
N(k, q) = \frac{1}{2} \varphi(q) + O(q^{3/4} d^{1/2}(q) \ln^2 q).
\] (2)

For \( k = 1 \), this gives

\[
r(q) = N(1, q) = \frac{1}{2} \varphi(q) + O(q^{3/4} d^{1/2}(q) \ln^2 q)
\]

which is much worse than (1), while for \( q = p \) a prime, it reads as follows.

\[
N(k, p) = \frac{1}{2} p + O(p^{3/4} \ln^2 p).
\] (3)

In view of (1), the estimate \( d(q) \ll q^\epsilon \) and a possible improvement in the estimate in Lemma 3, we conjecture that

\[
\Delta(k, q) = N(k, q) - \frac{1}{2} \varphi(q) = O(q^{1/2 + \epsilon}),
\]

for every \( \epsilon > 0 \).

2. Some lemmas

To complete the proof of the theorem, we need some lemmas. We use the following best possible estimate for the Kloostermann sums.

LEMMA 1. \([1]\) Let \( m, n, q \) be integers with \( q > 2 \) and let \( e(x) = e^{2\pi ix} \). Then we have

\[
S(m, n, q) = \sum'_{d \mod q} e \left( \frac{m d}{q} + \frac{n d}{q} \right) \ll (m, n, q)^{1/2} q^{1/2} d(q),
\]

where \( d \) denotes the inverse of \( d \mod q \) and the prime on the summation sign means that the sum is over reduced residue classes \( a \mod q \).

What we actually need is an estimate for the \( k \)th power analogue \( S^k(m, n, q) \) of the Kloostermann sum:

\[
S^k(m, n, q) = \sum'_{e \mod q} e \left( \frac{m e^k + n e^k}{q} \right). \quad (4)
\]

LEMMA 2. If \( q = uv (\geq 3) \) is a decomposition into relatively prime factors of the odd integer \( q \), then for any fixed positive integer \( k \) we have

\[
S^k(m, n, q) = S^k(m \overline{v}, n \overline{v}, u) S^k(m \overline{u}, n \overline{u}, v),
\]

where (here only) \( \overline{v} \) (respectively \( \overline{u} \)) is defined by \( v \overline{v} \equiv 1 \mod u \) (respectively \( u \overline{u} \equiv 1 \mod v \)).
Proof. Since the sum over reduced residue classes \( c \mod uv \) is the double sum \( c = av + bu \) over reduced residue classes \( a \mod u \) and \( b \mod v \), we have

\[
S^k(m, n, q) = S^k(m, n, uv)
\]

\[
= \sum_{a \mod u} \sum_{b \mod v} e\left( \frac{(m(av + bu)^k + n(av + bu)^k)}{uv} \right). \tag{5}
\]

Noting the congruence

\[
(av + bu)^k \equiv (av)^k + (bu)^k \pmod{uv},
\]

and

\[
(av + bu)^k \equiv av^k + bu^k \pmod{uv}
\]

we may factor the summand on the right-hand side of (5) as

\[
e\left( \frac{(av)^k}{u} + \frac{(av)}{v} \right) e\left( \frac{(bu)^k}{u} + \frac{(bu)}{v} \right).
\]

Hence,

\[
S^k(m, n, uv) = \sum_{a \mod u} e\left( \frac{(av)^k}{u} + \frac{(av)}{v} \right) \sum_{b \mod v} e\left( \frac{(bu)^k}{u} + \frac{(bu)}{v} \right). \tag{6}
\]

Since \( av \) and \( a \) (respectively \( bu \) and \( b \)) run through the reduced residue classes \( \mod u \) (respectively \( \mod v \)), it follows that identity (6) is exactly the assertion of Lemma 2. \[\square\]

By Lemma 2, we may restrict ourselves to the prime power case.

Lemma 3. Let \( p \) be an odd prime, \( \alpha \) a positive integer and let \( m \) and \( n \) be integers. Then for any fixed positive integer \( k \), we have the estimate

\[
S^k(m, n, p^\alpha) \ll (m, n, p^\alpha)^{1/4} p^{3\alpha/4} d^{1/2}(p^\alpha).
\]

Proof. Let \( g \) be any fixed primitive root modulo \( p^\alpha \) and let \( h = (k, \phi(p^\alpha)) \). Then for any integer \( r, 0 \leq r \leq k - 1 \), we have

\[
|S^k(mg^r, n_{p^\alpha}, p^\alpha)|^2 = \sum_{a \mod p^\alpha} \sum_{b \mod p^\alpha} e\left( \frac{mg^rb^k((ab)^k - 1) + n_{p^\alpha}p^k((ab)^k - 1)}{p^\alpha} \right).
\]
Writing \( b = g^j \), \( 0 \leq j \leq \phi(p^\alpha) - 1 \), and \( \overline{a} \) as \( a \), we deduce that

\[
|S^k(mg^r, n\overline{g}, p^\alpha)|^2 = \sum_{a \mod p^\alpha} \phi(p^\alpha) \sum_{j=0}^{\phi(p^\alpha) - 1} e\left( \frac{mg^{rk}(a^k - 1) + n\overline{g}^{rk}(\overline{a}^k - 1)}{p^\alpha} \right).
\]

Adding these equalities for \( r = 0, \ldots, h - 1 \), we obtain

\[
|S^k(m, n, p^\alpha)|^2 \leq \sum_{r=0}^{h-1} |S^k(mg^r, n\overline{g}, p^\alpha)|^2
\]

\[
= \sum_{a \mod p^\alpha} S(m(a^k - 1), n(\overline{a}^k - 1), p^\alpha).
\]

(7)

Now the inner double sum on the right-hand side of (7) is the same as the sum over reduced residue classes \( b \mod p^\alpha \), we may write (7) as

\[
|S^k(m, n, p^\alpha)|^2 \leq \sum_{a \mod p^\alpha} S(m(a^k - 1), n(\overline{a}^k - 1), p^\alpha).
\]

Hence, by Lemma 1,

\[
|S^k(m, n, p^\alpha)|^2 \leq \sum_{a=1}^{p^\alpha} S(m(a^k - 1), n(\overline{a}^k - 1), p^\alpha)p^{\alpha/2}d(p^\alpha)
\]

\[
\leq (m, n, p^\alpha)^{1/2}p^{\alpha/2}d(p^\alpha)S,
\]

(8)

say, where

\[
S = \sum_{a=1}^{p^\alpha} (a^k - 1, p^\alpha)^{1/2}.
\]

and \( \ll \) is Vinogradov’s symbolism equivalent to Landau’s symbol \( O \), that is, if there exists a constant \( m > 0 \) such that \( |f(x)| \leq mg(x) \) for all \( x \geq a \), then we write \( f(x) \ll g(x) \) or \( f(x) = O(g(x)) \).

It remains to estimate the sum \( S \) in (8). Writing \( (a^k - 1, p^\alpha) = d \), we note that \( d \) runs through all divisors of both \( p^\alpha \) and \( a^k - 1 \). Hence, \( d \) must be of the form \( d = p^i \), \( i = 0, \ldots, \alpha \). Hence,

\[
S = \sum_{i=0}^{\alpha} \sum_{a=1}^{p^\alpha} p^{i/2}.
\]
Now we write
\[ a = p^i q_i + d_i, \quad 1 \leq q_i \leq p^{a_i - i}, \quad 1 \leq d_i \leq p^i \]
and note that \( d|a^k - 1 \) is equivalent to \( p^i|a^k - 1 \). Then we have
\[
S = \sum_{i=0}^{a} \left( \sum_{q_i=1}^{p^{a_i-i}} \right) \sum_{d_i=1}^{p^i} \frac{p^{i/2}}{p^i|a^k-1} \]
\[ = p^a \sum_{i=0}^{a} \sum_{a_i=1}^{p^i} \left( \frac{1}{\sqrt{p}} \right)^i \ll p^a. \] (9)

By (8) and (9), the conclusion of Lemma 3 follows. \( \square \)

From Lemmas 2 and 3 we obtain an estimate for \( S^k(m, n, q) \):
\[ S^k(m, n, q) \ll (m, n, q)^{1/4} q^{3/4} d^{1/2}(q). \] (10)

**Lemma 4.** Let \( q \geq 3 \) be an odd integer. Then for any integer \( r \), we have the identity
\[ \sum_{a=1}^{q} (-1)^a e\left( -\frac{ra}{q} \right) = -1 + i \tan \left( \frac{\pi r}{q} \right). \]

**Proof.** This follows on noting that the left-hand side is the sum of the geometric sequence of common ratio \(-e(-r/q)\). \( \square \)

### 3. Proof of the theorem

From the definition of \( N(k, q) \) given in Section 1, we have
\[
N(k, q) = \sum_{a=1}^{q} \sum_{b=1}^{q} 1_{2q[a^k/q]+q[b^k/q] = 1} \\
= \frac{1}{2} \sum_{a=1}^{q} \sum_{b=1}^{q} (1 - (-1)^{q[a^k/q]+q[b^k/q]}) \\
= \frac{1}{2} \phi(q) - \frac{1}{2} \sum_{a=1}^{q} \sum_{b=1}^{q} (-1)^{q[a^k/q]+q[b^k/q]}. \] (11)
Using the orthogonality property of the additive character $e(nr/q)$,

$$\frac{1}{q} \sum_{r \mod q} e\left(\frac{rn}{q}\right) = \begin{cases} 1, & \text{if } q | n, \\ 0, & \text{if } q \nmid n, \end{cases}$$

we express $(-1)^{q\{a^k/q\}}$ as

$$\frac{1}{q} \sum_{c=1}^{q} (-1)^c \sum_{r \mod q} e\left(\frac{r(q\{a^k/q\} - c)}{q}\right)$$

$$= \frac{1}{q} \sum_{c=1}^{q} (-1)^c e\left(\frac{rq\{a^k/q\}}{q}\right) \sum_{c=1}^{q} (-1)^c e\left(\frac{-rc}{q}\right)$$

$$= \frac{1}{q} \sum_{c=1}^{q} e\left(\frac{rq}{q}\right) \left(-1 + i \tan \frac{\pi r}{q}\right), \quad (12)$$

by Lemma 4, and similarly for $q\{b^k/q\} = q\{a^k/q\}$:

$$(-1)^{q\{b^k/q\}} = \frac{1}{q} \sum_{c=1}^{q} e\left(\frac{cr}{q}\right) \left(-1 + i \tan \frac{\pi s}{q}\right). \quad (13)$$

Substituting (12) and (13) in (11) and expanding out, thereby extracting the special case $r = q, s = q$, we obtain

$$N(k, q) = \frac{1}{2} \phi(q) - \frac{1}{2q^2} \phi(q) + \frac{1}{q^2} S_1 - \frac{1}{2q^2} S_2 - \frac{1}{q^2} S_3 + \frac{1}{2q^2} S_4, \quad (14)$$

where

$$S_1 = \sum_{r=1}^{q-1} \sum_{a \mod q} e\left(\frac{ra^k}{q}\right) \left(-1 + i \tan \frac{\pi r}{q}\right),$$

$$S_2 = \sum_{r=1}^{q-1} \sum_{s=1}^{q-1} S^k(r, s, q),$$

$$S_3 = \sum_{r=1}^{q-1} \sum_{s=1}^{q-1} S^k(r, s, q)i \tan \frac{\pi r}{q},$$

$$S_4 = \sum_{r=1}^{q-1} \sum_{s=1}^{q-1} S^k(r, s, q) \tan \frac{\pi r}{q} \tan \frac{\pi s}{q}. \quad (15)$$

It is enough to estimate $S_4$ (the others can be found in the same way). To this end we note the estimate $\cot(\pi x) \ll 1/x$ if $0 < x \leq \frac{1}{2}$, so that we have the estimate

$$\tan\left(\frac{\pi r}{q}\right) = \cot\left(\frac{\pi}{2} - \frac{\pi r}{q}\right) \ll \frac{q}{|q - 2r|}.$$

Thus, from (10) we deduce that

$$S_4 \ll \sum_{r=1}^{q-1} \sum_{s=1}^{q-1} (r, s, q)^{1/4} q^{3/4} d^{1/2} (q) \frac{q}{|q - 2r||q - 2s|}.$$

Now, writing $(r, s, q) = d$, we see that

$$S_4 \ll q^{3/4} d^{1/2} (q) \sum_{d|q} d^{1/4} \sum_{r \leq q/d} \sum_{s \leq q/d} (q/d)^2 \frac{(q/d)^2}{|q/2d - r||q/2d - s|} \leq q^{11/4} d^{1/2} (q) \ln^2 q. \tag{16}$$

Similarly, we have

$$S_1 \ll q^{7/4}, \quad S_2 \ll q^{11/4} d^{1/2} (q), \quad S_3 \ll q^{11/4} d^{1/2} (q) \ln q. \tag{17}$$

Using estimates (16) and (17) in (14) completes the proof of the theorem. \qed

**Acknowledgements.** The authors express their gratitude to the referees for their very helpful and detailed comments. This work is supported by the Doctorate Foundation of Xi’an Jiaotong University.

**REFERENCES**


Yi Yuan and Zhang Wenpeng
Research Centre for Basic Science
Xi’an Jiaotong University
Xi’an
Shaanxi 710049
People’s Republic of China