GENERALIZED D. H. LEHMER PROBLEM OVER SHORT INTERVALS

PING XI
School of Science, Xi'an Jiaotong University, Xi'an 710049, P. R. China
email: xprime@163.com

and YUAN YI
School of Science, Xi'an Jiaotong University, Xi'an 710049, P. R. China and Department of Mathematics, The University of Iowa, Iowa City, IA 52242-1419, USA
email: yuanyi@mail.xjtu.edu.cn

(Received 21 December 2009; accepted 1 July 2010; first published online 13 December 2010)

Abstract. Let \( n \geq 2 \) be a fixed positive integer, \( q \geq 3 \) and \( c, \ell \) be integers with \( (nc, q) = 1 \) and \( \ell \mid n \). Suppose \( A \) and \( B \) consist of consecutive integers which are coprime to \( q \). We define the cardinality of a set:

\[ N(A, B, c, n, \ell; q) = \# \{(a, b) \in A \times B | ab \equiv c \pmod{q}, (a + b, n) = \ell \}. \]

The main purpose of this paper is to use the estimates of Gauss sums and Kloosterman sums to study the asymptotic properties of \( N(A, B, c, n, \ell; q) \), and to give an interesting asymptotic formula for it.

2010 Mathematics Subject Classification. Primary 11A07, 11N37; Secondary 11L05.

1. Introduction. Let \( q \geq 3 \) be an integer. For each integer \( a \) with \( 1 \leq a < q \), \( (a, q) = 1 \), there is a unique integer \( b \) with \( 1 \leq b < q \) such that \( ab \equiv 1 \pmod{q} \). Let \( N(q) \) denote the number of solutions of the congruence equation \( ab \equiv 1 \pmod{q} \) with \( 1 \leq a, b < q \), \( 2 \nmid a + b \). That is

\[ N(q) = \# \{(a, b) \in [1, q] \times [1, q] | ab \equiv 1 \pmod{q}, 2 \nmid a + b \}, \]

where \( \#S \) denotes the cardinality of the set \( S \). Thus, \( N(q) \) denotes the number of integers \( a, 1 \leq a < q \), \( (a, q) = 1 \), such that \( a \) and its inverse \( b \pmod{q} \) are of opposite parity.

For an odd prime \( p \), D. H. Lehmer posed the problem to find \( N(p) \) or at least to say something nontrivial about it (see Problem F12 of [2], p. 381). Wenpeng Zhang [8] has given an asymptotic estimate:

\[ N(p) = \frac{1}{2} p + O \left( p^{1/2} \log^7 p \right). \quad (1) \]

Supported by N. S. F. (No.10601039) of P. R. China.
Later, Wenpeng Zhang [9, 10] also proved that for every odd integer \( q \geq 3 \),
\[
N(q) = \frac{1}{2} \varphi(q) + O\left(q^{1/2} \tau^2(q) \log^2 q\right),
\]
where \( \varphi(q) \) is the Euler function and \( \tau(q) \) is the divisor function.

The classical problem has been generalized by many scholars (see [5–7], et al.).
Recently, Yaming Lu and Yuan Yi [3] studied a generalization of the D. H. Lehmer problem over short intervals. Let \( n \geq 2 \) be a fixed positive integer, \( q \geq 3 \) and \( c \) be integers with \( (nc, q) = 1 \). We define
\[
r_n(\theta_1, \theta_2, c; q) = \#\{(a, b) \in [1, \theta_1 q] \times [1, \theta_2 q] | ab \equiv c \pmod{q}, \ n \nmid a + b\},
\]
where \( 0 < \theta_1, \theta_2 \leq 1 \). In [3], it is obtained that
\[
r_n(\theta_1, \theta_2, c; q) = \left(1 - \frac{1}{n}\right) \theta_1 \theta_2 \varphi(q) + O\left(q^{1/2} \tau^6(q) \log^2 q\right),
\]
where the \( O \)-constant depends only on \( n \).

In this paper, we consider a more extensive generalization of the D. H. Lehmer problem over short intervals, which may be of great arithmetical interest.

Suppose \( A \) and \( B \) consist of consecutive integers which are coprime to \( q \), that is,
\[
A = \{n \in \mathbb{Q} : M < n \leq M + A\},
\]
\[
B = \{n \in \mathbb{Q} : N < n \leq N + B\},
\]
where \( M, N, A > 0, B > 0 \) are integers, \( Q \) is a reduced residue system modulo \( q \). Let \( n \geq 2 \) be a fixed positive integer, \( q \geq 3 \) and \( c, \ell \) be integers with \( (nc, q) = 1 \) and \( \ell | n \), and define
\[
N(A, B, c, n, \ell; q) = \#\{(a, b) \in A \times B | ab \equiv c \pmod{q}, (a + b, n) = \ell\}.
\]

The main purpose of this paper is to use the estimates of Gauss sums and Kloosterman sums to study the asymptotic properties of \( N(A, B, c, n, \ell; q) \), and to give an interesting asymptotic formula for it. In fact, we have the following.

**Theorem 1.** Let \( n \geq 2 \) be a fixed positive integer, \( q \geq 3 \) and \( c, \ell \) be integers with \( (nc, q) = 1 \) and \( \ell | n \), the sets \( A \) and \( B \) are defined by (4) and (5). Then, as \( q \to +\infty \), we have the asymptotic formula
\[
N(A, B, c, n, \ell; q) = \frac{\#A \#B}{n} \varphi\left(\frac{n}{\ell}\right) \varphi^{-1}(q) + O\left(\sqrt{\frac{\#A \#B}{q}} \tau^3(q) \cdot n^{o(\ell/n)}\right)
\]
\[
+ O\left(q^{1/2} \tau^3(q) \log^2 q \cdot 2^{o(\ell/n)}\right),
\]
where \( \varphi(n) \) is the Euler function, \( \tau(q) \) is the divisor function, \( o(q) \) denotes the number of distinct prime factors of \( q \), \( \#A \) denotes the cardinality of \( A \) and two \( O \)-constants are both absolute.

We can see that the estimate is nontrivial when \( \#A \#B \gg q^{3/2+\epsilon} \), where the implied constant depends at most on \( n \) and \( \epsilon \).
2. Lemmas. In order to prove Theorem 1, we require the following lemmas. First, for integers \( m, n, q \), we introduce the classical Kloosterman sum:

\[
S(m, n; q) = \sum_{a \mod q \atop (a,q)=1} e\left(\frac{ma + n\overline{a}}{q}\right),
\]

where \( e(z) = e^{2\pi iz} \), \( a\overline{a} \equiv 1 \pmod{q} \).

**Lemma 1.** Let \( m, n, q \) be integers, \( q \geq 3 \), then we have the upper bound

\[
|S(m, n; q)| \leq q^{1/2}(m, n, q)^{1/2}\tau(q).
\]

*Proof.* See [1]. □

Denote by \( \chi \) a Dirichlet character mod \( q \), by \( \chi^0 \) the principal one, and by \( m \) an integer. The well known Gauss sum is defined by

\[
G(m, \chi) = \sum_{h \mod q} \chi(h)e\left(\frac{mh}{q}\right).
\]

We also require some properties of Gauss sums, which are stated as the following two lemmas.

**Lemma 2.** For any positive integers \( q \) and \( m \), we have

\[
G(m, \chi^0) = \mu\left(\frac{q}{(m, q)}\right) \varphi(q)\varphi^{-1}\left(\frac{q}{(m, q)}\right),
\]

where \( \mu(n) \) is the Möbius function.

*Proof.* See [4], Section 1.2, Lemma 2. □

**Lemma 3.** Let \( q \) and \( c \) be two integers with \( q \geq 3 \), \( (c, q) = 1 \). Then for any integers \( a \) and \( b \), we have

\[
\sum_{\chi \neq \chi^0} \chi(c)G(a, \chi)G(b, \chi) \ll \varphi(q)q^{1/2}(a, q)^{1/2}(b, q)^{1/2}\tau(q),
\]

where the \( O \)-constant is absolute.

*Proof.* By using Lemma 1, we can easily deduce that

\[
\sum_{\chi \mod q} \chi(c)G(a, \chi)G(b, \chi) = \sum_{\chi \mod q} \chi(c) \sum_{s=1}^{q} \chi(s)e\left(\frac{as}{q}\right) \sum_{t=1}^{q} \chi(t)e\left(\frac{bt}{q}\right)
\]

\[
= \sum_{s=1}^{q} \sum_{t=1}^{q} e\left(\frac{as + bt}{q}\right) \sum_{\chi \mod q} \chi(stc)
\]

\[
= \varphi(q) \sum_{s=1}^{q} \sum_{t=1}^{q} e\left(\frac{as + bt}{q}\right)
\]

\[
= \varphi(q)S(a, b\overline{c}; q)
\]

\[
\ll \varphi(q)q^{1/2}(a, b, q)^{1/2}\tau(q).
\]

(6)
On the other hand, Lemma 2 indicates that

\[ G(a, \chi^0)G(b, \chi^0) = \mu \left( \frac{q}{(a,q)} \right) \mu \left( \frac{q}{(b,q)} \right) \varphi^2(q) \varphi^{-1} \left( \frac{q}{(a,q)} \right) \varphi^{-1} \left( \frac{q}{(b,q)} \right) \]

\[ \ll \varphi^2(q) \left( \frac{(a,q)(b,q)}{q^2} \right) \tau \left( \frac{q}{(a,q)} \right) \tau \left( \frac{q}{(b,q)} \right) \]

\[ \ll \varphi^2(q) \left( \frac{(a,q)(b,q)}{q^2} \right) \frac{q}{\sqrt{(a,q)(b,q)}} \]

\[ \ll \varphi(q)(a,q)^{1/2}(b,q)^{1/2}. \]  

(7)

Then Lemma 3 follows from (6) and (7) immediately. □

Note: A slight weaker estimate than Lemma 3 can be found in [3].

The following two lemmas focus on the estimation for exponential sums.

**Lemma 4.** Let \( N \) be a positive integer, \( \alpha \) be a real number. Then we have

\[ \left| \sum_{n \leq N} e(\alpha n) \right| \leq \min \left( N, \frac{1}{2\|\alpha\|} \right), \]

where \( \|x\| = \min_{n \in \mathbb{Z}} |x - n| \).

*Proof.* The estimate is well known, the proof can be found in [4], Section 5.1. □

**Lemma 5.** Assume that \( U \) is a positive real number, \( K_0 \) an integer, \( K \) a positive integer, \( \alpha \) and \( \beta \) two arbitrary real numbers. If \( \alpha \) can be written in the form

\[ \alpha = \frac{h}{q} + \frac{\theta}{q^2} \quad (q,h) = 1, \quad q \geq 1, \quad |\theta| \leq 1, \]

we have

\[ \sum_{k=K_0+1}^{K+K} \min \left( U, \frac{1}{\|\alpha_k + \beta\|} \right) \ll \left( \frac{K}{q} + 1 \right) (U + q \log q), \]

where the implied constant is absolute.

*Proof.* See reference [4], Section 5.1, Lemma 3. □

3. **Proof of Theorem 1.** In this section, we shall complete the proof of Theorem 1. From the orthogonality relation for Dirichlet characters modulo \( q \), one can obtain that

\[ N(A, B, c, n, \ell; q) = \frac{1}{\varphi(q)} \sum_{\chi \mod q} \sum_{a \in A} \sum_{b \in B} \chi(ab)\overline{\chi}(c) \]

\[ = \frac{1}{\varphi(q)} \sum_{a \in A} \sum_{b \in B} 1 + \frac{1}{\varphi(q)} \sum_{\chi \not\equiv \chi^0} \sum_{a \in A} \sum_{b \in B} \chi(ab)\overline{\chi}(c) \]

\[ := I_1 + I_2. \]  

(8)
We shall estimate $I_1$ and $I_2$ respectively. Firstly,

$$I_1 = \frac{1}{\varphi(q)} \sum_{a \in A} \sum_{b \in B} \sum_{(a+b,n)=\ell} 1 = \frac{1}{\varphi(q)} \sum_{a \in A} \sum_{b \in B} \sum_{\ell | a+b} \mu(r)$$

$$= \frac{1}{\varphi(q)} \sum_{a \in A} \sum_{r \mid \ell} \mu(r) \sum_{b \equiv -a (\text{mod} \, \ell)} 1$$

$$= \frac{1}{\varphi(q)} \sum_{a \in A} \sum_{r \mid \ell} \mu(r) \left( \frac{\#B}{r\ell} + O(1) \right)$$

$$= \frac{\#B}{\varphi(q)\ell} \sum_{a \in A} \sum_{r \mid \ell} \frac{\mu(r)}{r} + O(2o(n/\ell))$$

$$= \frac{\#A\#B}{n} \varphi \left( \frac{n}{\ell} \right) \varphi^{-1}(q) + O(2o(n/\ell)). \quad (9)$$

Secondly,

$$I_2 = \frac{1}{\varphi(q)} \sum_{\chi \neq \chi^0} \sum_{(a+b,n)=\ell} \chi(ab) = \frac{1}{\varphi(q)} \sum_{\chi \neq \chi^0} \sum_{r \mid \ell} \sum_{m \leq r\ell} \sum_{a \in A} \sum_{b \in B} e \left( \frac{ma+b}{r\ell} \right) \chi(ab)$$

$$= \frac{1}{\varphi(q)\ell} \sum_{\chi \neq \chi^0} \sum_{r \mid \ell} \mu(r) \sum_{m \leq r\ell} \sum_{a \in A} \sum_{b \in B} e \left( \frac{ma+b}{r\ell} \right) \chi(ab)$$

$$= \frac{1}{\varphi(q)\ell} \sum_{\chi \neq \chi^0} \sum_{r \mid \ell} \mu(r) \sum_{m \leq r\ell} \chi(a) e \left( \frac{ma}{r\ell} \right) \sum_{b \in B} \chi(b) e \left( \frac{mb}{r\ell} \right). \quad (10)$$

Note that for any non-principal character $\chi$ mod $q$,

$$\chi(a) = \frac{1}{q} \sum_{s \leq q} G(s, \chi) e \left( -\frac{as}{q} \right);$$

thus,

$$\sum_{a \in A} \chi(a) e \left( \frac{ma}{r\ell} \right) = \frac{1}{q} \sum_{s \leq q} G(s, \chi) \sum_{a \in A} e \left( \left( \frac{m}{r\ell} - \frac{s}{q} \right) a \right). \quad (11)$$

Combining (10) and (11), and making use of Lemma 3 and 4, we have

$$I_2 = \frac{1}{q^2\varphi(q)\ell} \sum_{r \mid \ell} \mu(r) \sum_{m \leq r\ell} \sum_{s \leq q} \sum_{t \leq q} \sum_{a \in A} \sum_{b \in B} e \left( \left( \frac{m}{r\ell} - \frac{s}{q} \right) a \right) e \left( \left( \frac{m}{r\ell} - \frac{t}{q} \right) b \right)$$

$$\times \sum_{\chi \neq \chi^0} \chi(c)G(s, \chi)G(t, \chi)$$

$$\ll \frac{\tau(q)}{q^{3/2}\ell} \sum_{r \mid \ell} \mu^2(r) \sum_{m \leq r\ell} \sum_{s \leq q} \sum_{t \leq q} (s, q)^{1/2}(t, q)^{1/2}$$

$$\times \min \left( \#A, \left\| \frac{s}{q} - \frac{m}{r\ell} \right\|^{-1} \right) \cdot \min \left( \#B, \left\| \frac{t}{q} - \frac{m}{r\ell} \right\|^{-1} \right).$$
By Möbius transform, we have

\[
\sum_{s \leq q} (s, q)^{1/2} \min \left( \#A, \frac{s}{q} - \frac{m}{r \ell} \right)^{-1} = q^{1/2} \sum_{d|q} d^{-1/2} \sum_{(s, d) = 1 \atop s \leq d} \min \left( \#A, \frac{s}{d} - \frac{m}{r \ell} \right)^{-1}.
\]

(12)

Observe that \((n, q) = 1\); thus, for \(\ell \mid n\) and \(d \mid q\), we have

\[
\left\| \frac{s}{d} - \frac{m}{r \ell} \right\| \geq \frac{1}{d \ell},
\]

from which and Lemma 5, the left-hand side of (12) is bounded by

\[
q^{1/2} \sum_{d|q} d^{-1/2} \sum_{(s, d) = 1 \atop s \leq d} \min \left( \#A, dr \ell, \left\| \frac{s}{d} - \frac{m}{r \ell} \right\|^{-1} \right) \ll q^{1/2} \sum_{d|q} d^{-1/2} (\min(\#A, dr \ell) + d \log d)
\]

\[
= \#Aq^{1/2} \sum_{d|q \atop d > \#A/r \ell} d^{-1/2 + r \ell q} \sum_{d|q \atop d \leq \#A/r \ell} d^{1/2} + q^{1/2} \sum_{d|q} d^{1/2} \log d
\]

\[
\ll (r \ell)^{1/2}(\#A)^{1/2}q^{1/2}\tau(q) + q\tau(q) \log q.
\]

and similarly

\[
\sum_{t \leq q} (t, q)^{1/2} \min \left( \#B, \frac{t}{q} - \frac{m}{r \ell} \right)^{-1} \ll (r \ell)^{1/2}(\#B)^{1/2}q^{1/2}\tau(q) + q\tau(q) \log q.
\]

Thus,

\[
I_2 \ll \sqrt{\frac{\#A\#B}{q}} \tau(q) \cdot n 2^{\omega(n/\ell)} + q^{1/2} \tau^2(q) \log^2 q \cdot 2^{\omega(n/\ell)},
\]

(13)

where \(\omega(n)\) denotes the number of distinct prime factors of \(n\).

Combining (8), (9) and (13), we can deduce the theorem immediately.

4. Remarks. Recalling that \(Q\) is a reduced residue system modulo \(q\), and taking \(q = p\) as a prime number, \(A = B = Q, n = 2, \ell = 1\) in Theorem 1, we can obtain

\[
N(p) = \frac{1}{2} p + O(p^{1/2} \log^2 p),
\]

which is just the same as (1). Similarly, Theorem 1 yields (2) with a slightly weaker error term.

Taking \(A = \{n \in Q : 1 \leq n \leq \theta_1 q\}, B = \{n \in Q : 1 \leq n \leq \theta_2 q\},

\[r_n(\theta_1, \theta_2, c; q) = \sum_{\ell|n} N(A, B, c, n, \ell; q) - N(A, B, c, n, n; q),\]

where \(\theta_1, \theta_2\) are the relative density of \(A\) and \(B\), respectively.

Theorem 1 yields

\[
N(p) = \frac{1}{2} p + O(p^{1/2} \log^2 p),
\]

which is just the same as (1). Similarly, Theorem 1 yields (2) with a slightly weaker error term.

Taking \(A = \{n \in Q : 1 \leq n \leq \theta_1 q\}, B = \{n \in Q : 1 \leq n \leq \theta_2 q\},

\[r_n(\theta_1, \theta_2, c; q) = \sum_{\ell|n} N(A, B, c, n, \ell; q) - N(A, B, c, n, n; q),\]

where \(\theta_1, \theta_2\) are the relative density of \(A\) and \(B\), respectively.
and hence
\[ r_n(\theta_1, \theta_2, c; q) = \sum_{\ell | n} \frac{\theta_1 \theta_2}{n} \varphi\left(\frac{n}{\ell}\right) \varphi(q) - \frac{\theta_1 \theta_2}{n} \varphi(q) + (q^{1/2} \tau^3(q) n \tau^2(n) \log^2 q) \]
\[ = \left(1 - \frac{1}{n}\right) \theta_1 \theta_2 \varphi(q) + O\left(q^{1/2} \tau^3(q) n \tau^2(n) \log^2 q\right). \]

which is slightly better than (3).

Observing that the condition $2 \nmid a + b$ is equivalent to $a + b \equiv 1 \pmod{2}$, thus we can consider another generalization of the D. H. Lehmer problem over short intervals.

Let $q \geq 3$, $\ell \geq 1$ be fixed integers, $n$ and $c$ be integers with $(nc, q) = 1$. We define

\[ T(A, B, c, \ell; q, n) = \#\{(a, b) \in A \times B | ab \equiv c \pmod{q}, a + b \equiv \ell \pmod{n}\}, \]

where $A, B$ are defined as before. Using the same method above, we can also prove that

\[ T(A, B, c, \ell; q, n) = \frac{\#A \#B}{n} \varphi^{-1}(q) + O(q^{1/2} \tau^3(q) \log^2 q), \]

which also yields (1), (2) and (3).

ACKNOWLEDGEMENTS. The authors would like to express their sincere thanks to the referees for their helpful comments and suggestions.

REFERENCES