*Glasgow Math. J.* **53** (2011) 293–299. © Glasgow Mathematical Journal Trust 2010.
doi:10.1017/S0017089510000704.

# 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 $n \geqslant 2$ be a fixed positive integer, $q \geqslant 3$ and $c, \ell$ be integers with $(nc, q) = 1$ and $\ell | n$. Suppose $\mathcal{A}$ and $\mathcal{B}$ consist of consecutive integers which are coprime to $q$. We define the cardinality of a set:

$$N(\mathcal{A}, \mathcal{B}, c, n, \ell; q) = \#\{(a, b) \in \mathcal{A} \times \mathcal{B} | ab \equiv c (\text{mod } q), (a + b, n) = \ell\}.$$

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

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

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

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

where $\#\mathcal{S}$ denotes the cardinality of the set $\mathcal{S}$. Thus, $N(q)$ denotes the number of integers $a$, $1 \leqslant a < q$, $(a, q) = 1$, such that $a$ and its inverse $b$ $(\text{mod } q)$ 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:

$$N(p) = \frac{1}{2}p + O\left(p^{1/2} \log^2 p\right). \tag{1}$$

Supported by N. S. F. (No.10601039) of P. R. China.

Later, Wenpeng Zhang [**9, 10**] also proved that for every odd integer $q \geqslant 3$,

$$N(q) = \frac{1}{2}\varphi(q) + O\left(q^{1/2}\tau^2(q)\log^2 q\right), \tag{2}$$

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 $n \geqslant 2$ be a fixed positive integer, $q \geqslant 3$ and $c$ be integers with $(nc, q) = 1$. We define

$$r_n(\theta_1, \theta_2, c; q) = \#\{(a, b) \in [1, \theta_1 q] \times [1, \theta_2 q] | ab \equiv c (\bmod q),\ n \nmid a + b\},$$

where $0 < \theta_1, \theta_2 \leqslant 1$. In [**3**], it is obtained that

$$r_n(\theta_1, \theta_2, c; q) = \left(1 - \frac{1}{n}\right)\theta_1\theta_2\varphi(q) + O\left(q^{1/2}\tau^6(q)\log^2 q\right), \tag{3}$$

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 $\mathcal{A}$ and $\mathcal{B}$ consist of consecutive integers which are coprime to $q$, that is,

$$\mathcal{A} = \{n \in \mathcal{Q} : M < n \leqslant M + A\}, \tag{4}$$

$$\mathcal{B} = \{n \in \mathcal{Q} : N < n \leqslant N + B\}, \tag{5}$$

where $M, N, A > 0, B > 0$ are integers, $\mathcal{Q}$ is a reduced residue system modulo $q$. Let $n \geqslant 2$ be a fixed positive integer, $q \geqslant 3$ and $c, \ell$ be integers with $(nc, q) = 1$ and $\ell | n$, and define

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

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

THEOREM 1. *Let $n \geqslant 2$ be a fixed positive integer, $q \geqslant 3$ and $c, \ell$ be integers with $(nc, q) = 1$ and $\ell | n$, the sets $\mathcal{A}$ and $\mathcal{B}$ are defined by* (4) *and* (5)*. Then, as $q \to +\infty$, we have the asymptotic formula*

$$N(\mathcal{A}, \mathcal{B}, c, n, \ell; q) = \frac{\#\mathcal{A}\#\mathcal{B}}{n}\varphi\left(\frac{n}{\ell}\right)\varphi^{-1}(q) + O\left(\sqrt{\frac{\#\mathcal{A}\#\mathcal{B}}{q}}\tau^3(q) \cdot n2^{\omega(n/\ell)}\right) + O\left(q^{1/2}\tau^3(q)\log^2 q \cdot 2^{\omega(n/\ell)}\right),$$

*where $\varphi(n)$ is the Euler function, $\tau(q)$ is the divisor function, $\omega(q)$ denotes the number of distinct prime factors of $q$, $\#\mathcal{A}$ denotes the cardinality of $\mathcal{A}$ and two $O$-constants are both absolute.*

We can see that the estimate is nontrivial when $\#\mathcal{A}\#\mathcal{B} \gg q^{3/2+\epsilon}$, 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:

$$S(m,n;q) = \sum_{\substack{a \bmod q \\ (a,q)=1}} e\left(\frac{ma+n\bar{a}}{q}\right),$$

where $e(x) = e^{2\pi i x}$, $a\bar{a} \equiv 1(\bmod q)$.

LEMMA 1. *Let $m, n, q$ be integers, $q \geqslant 3$, then we have the upper bound*

$$|S(m,n;q)| \leqslant q^{1/2}(m,n,q)^{1/2}\tau(q).$$

*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

$$G(m,\chi) = \sum_{h \bmod q} \chi(h) e\left(\frac{mh}{q}\right).$$

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 $q \geqslant 3$, $(c,q)=1$. 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

$$\begin{aligned}
\sum_{\chi \bmod q} \chi(c) G(a,\chi) G(b,\chi) &= \sum_{\chi \bmod q} \chi(c) \sum_{s=1}^{q} \chi(s) e\left(\frac{as}{q}\right) \sum_{t=1}^{q} \chi(t) e\left(\frac{bt}{q}\right) \\
&= \sum_{s=1}^{q}\sum_{t=1}^{q} e\left(\frac{as+bt}{q}\right) \sum_{\chi \bmod q} \chi(stc) \\
&= \varphi(q) \sum_{\substack{s=1 \\ st \equiv \bar{c} (\bmod q)}}^{q} \sum_{t=1}^{q} e\left(\frac{as+bt}{q}\right) \\
&= \varphi(q) S(a, b\bar{c}; q) \\
&\ll \varphi(q) q^{1/2}(a,b,q)^{1/2}\tau(q). \qquad (6)
\end{aligned}$$

https://doi.org/10.1017/S0017089510000704 Published online by Cambridge University Press

On the other hand, Lemma 2 indicates that

$$
\begin{aligned}
G(a,\chi^0)G(b,\chi^0) &= \mu\left(\frac{q}{(a,q)}\right)\mu\left(\frac{q}{(b,q)}\right)\varphi^2(q)\varphi^{-1}\left(\frac{q}{(a,q)}\right)\varphi^{-1}\left(\frac{q}{(b,q)}\right)\\
&\ll \varphi^2(q)\frac{(a,q)(b,q)}{q^2}\tau\left(\frac{q}{(a,q)}\right)\tau\left(\frac{q}{(b,q)}\right)\\
&\ll \varphi^2(q)\frac{(a,q)(b,q)}{q^2}\frac{q}{\sqrt{(a,q)(b,q)}}\\
&\ll \varphi(q)(a,q)^{1/2}(b,q)^{1/2}. \qquad (7)
\end{aligned}
$$

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*

$$
\left|\sum_{n\leqslant N} e(\alpha n)\right| \leqslant \min\left(N, \frac{1}{2\|\alpha\|}\right),
$$

*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*

$$
\alpha = \frac{h}{q} + \frac{\theta}{q^2} \qquad (q,h)=1, \quad q\geqslant 1, \quad |\theta|\leqslant 1,
$$

*we have*

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

*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

$$
\begin{aligned}
N(\mathcal{A},\mathcal{B},c,n,\ell;q) &= \frac{1}{\varphi(q)}\sum_{\chi \bmod q}\sum_{\substack{a\in\mathcal{A}\\(a+b,n)=\ell}}\sum_{b\in\mathcal{B}}\chi(ab)\overline{\chi}(c)\\
&= \frac{1}{\varphi(q)}\sum_{\substack{a\in\mathcal{A}\\(a+b,n)=\ell}}\sum_{b\in\mathcal{B}}1 + \frac{1}{\varphi(q)}\sum_{\chi\neq\chi^0}\sum_{\substack{a\in\mathcal{A}\\(a+b,n)=\ell}}\sum_{b\in\mathcal{B}}\chi(ab)\overline{\chi}(c)\\
&:= I_1 + I_2. \qquad (8)
\end{aligned}
$$

https://doi.org/10.1017/S0017089510000704 Published online by Cambridge University Press

We shall estimate $I_1$ and $I_2$ respectively. Firstly,

$$\begin{aligned}
I_1 &= \frac{1}{\varphi(q)} \sum_{\substack{a\in\mathcal{A}\\(a+b,n)=\ell}} \sum_{b\in\mathcal{B}} 1 = \frac{1}{\varphi(q)} \sum_{\substack{a\in\mathcal{A}\\ \ell\mid a+b}} \sum_{b\in\mathcal{B}} \sum_{r\mid\left(\frac{a+b}{\ell},\frac{n}{\ell}\right)} \mu(r)\\
&= \frac{1}{\varphi(q)} \sum_{a\in\mathcal{A}} \sum_{r\mid\frac{n}{\ell}} \mu(r) \sum_{\substack{b\in\mathcal{B}\\ b\equiv -a(\bmod r\ell)}} 1\\
&= \frac{1}{\varphi(q)} \sum_{a\in\mathcal{A}} \sum_{r\mid\frac{n}{\ell}} \mu(r) \left(\frac{\#\mathcal{B}}{r\ell} + O(1)\right)\\
&= \frac{\#\mathcal{B}}{\varphi(q)\ell} \sum_{a\in\mathcal{A}} \sum_{r\mid\frac{n}{\ell}} \frac{\mu(r)}{r} + O(2^{\omega(n/\ell)})\\
&= \frac{\#\mathcal{A}\#\mathcal{B}}{n} \varphi\left(\frac{n}{\ell}\right) \varphi^{-1}(q) + O(2^{\omega(n/\ell)}).
\end{aligned} \tag{9}$$

Secondly,

$$\begin{aligned}
I_2 &= \frac{1}{\varphi(q)} \sum_{\chi\neq\chi^0} \overline{\chi}(c) \sum_{\substack{a\in\mathcal{A}\\(a+b,n)=\ell}} \sum_{b\in\mathcal{B}} \chi(ab) = \frac{1}{\varphi(q)} \sum_{\chi\neq\chi^0} \overline{\chi}(c) \sum_{r\mid\frac{n}{\ell}} \mu(r) \sum_{\substack{a\in\mathcal{A}\\ r\mid\frac{a+b}{\ell}}} \sum_{b\in\mathcal{B}} \chi(ab)\\
&= \frac{1}{\varphi(q)\ell} \sum_{\chi\neq\chi^0} \overline{\chi}(c) \sum_{r\mid\frac{n}{\ell}} \frac{\mu(r)}{r} \sum_{m\leqslant r\ell} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} e\left(\frac{m(a+b)}{r\ell}\right) \chi(ab)\\
&= \frac{1}{\varphi(q)\ell} \sum_{\chi\neq\chi^0} \overline{\chi}(c) \sum_{r\mid\frac{n}{\ell}} \frac{\mu(r)}{r} \sum_{m\leqslant r\ell} \sum_{a\in\mathcal{A}} \chi(a) e\left(\frac{ma}{r\ell}\right) \sum_{b\in\mathcal{B}} \chi(b) e\left(\frac{mb}{r\ell}\right).
\end{aligned} \tag{10}$$

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

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

thus,

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

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

$$\begin{aligned}
I_2 &= \frac{1}{q^2\varphi(q)\ell} \sum_{r\mid\frac{n}{\ell}} \frac{\mu(r)}{r} \sum_{m\leqslant r\ell} \sum_{s\leqslant q} \sum_{t\leqslant q} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} e\left(\left(\frac{m}{r\ell} - \frac{s}{q}\right) a\right) e\left(\left(\frac{m}{r\ell} - \frac{t}{q}\right) b\right)\\
&\quad \times \sum_{\chi\neq\chi^0} \overline{\chi}(c) G(s,\chi) G(t,\chi)\\
&\ll \frac{\tau(q)}{q^{3/2}\ell} \sum_{r\mid\frac{n}{\ell}} \frac{\mu^2(r)}{r} \sum_{m\leqslant r\ell} \sum_{s\leqslant q} \sum_{t\leqslant q} (s,q)^{1/2} (t,q)^{1/2}\\
&\quad \times \min\left(\#\mathcal{A}, \left\| \frac{s}{q} - \frac{m}{r\ell} \right\|^{-1}\right) \cdot \min\left(\#\mathcal{B}, \left\| \frac{t}{q} - \frac{m}{r\ell} \right\|^{-1}\right).
\end{aligned}$$

https://doi.org/10.1017/S0017089510000704 Published online by Cambridge University Press

By Möbius transform, we have

$$\sum_{s\leqslant q}(s,q)^{1/2}\min\left(\#\mathcal{A},\left\|\frac{s}{q}-\frac{m}{r\ell}\right\|^{-1}\right)=q^{1/2}\sum_{d|q}d^{-1/2}\sum_{\substack{s\leqslant d\\(s,d)=1}}\min\left(\#\mathcal{A},\left\|\frac{s}{d}-\frac{m}{r\ell}\right\|^{-1}\right). \tag{12}$$

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

$$\left\|\frac{s}{d}-\frac{m}{r\ell}\right\|\geqslant\frac{1}{dr\ell},$$

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

$$\begin{aligned}
&q^{1/2}\sum_{d|q}d^{-1/2}\sum_{\substack{s\leqslant d\\(s,d)=1}}\min\left(\#\mathcal{A},dr\ell,\left\|\frac{s}{d}-\frac{m}{r\ell}\right\|^{-1}\right)\\
&\quad\ll q^{1/2}\sum_{d|q}d^{-1/2}(\min(\#\mathcal{A},dr\ell)+d\log d)\\
&\quad=\#\mathcal{A}q^{1/2}\sum_{\substack{d|q\\d>\#\mathcal{A}/r\ell}}d^{-1/2}+r\ell q^{1/2}\sum_{\substack{d|q\\d\leqslant\#\mathcal{A}/r\ell}}d^{1/2}+q^{1/2}\sum_{d|q}d^{1/2}\log d\\
&\quad\ll(r\ell)^{1/2}(\#\mathcal{A})^{1/2}q^{1/2}\tau(q)+q\tau(q)\log q,
\end{aligned}$$

and similarly

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

Thus,

$$I_2\ll\sqrt{\frac{\#\mathcal{A}\#\mathcal{B}}{q}}\tau^3(q)\cdot n2^{\omega(n/\ell)}+q^{1/2}\tau^3(q)\log^2 q\cdot 2^{\omega(n/\ell)}, \tag{13}$$

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 $\mathcal{Q}$ is a reduced residue system modulo $q$, and taking $q=p$ as a prime number, $\mathcal{A}=\mathcal{B}=\mathcal{Q}$, $n=2$, $\ell=1$ 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 $\mathcal{A}=\{n\in\mathcal{Q}:1\leqslant n\leqslant\theta_1 q\}$, $\mathcal{B}=\{n\in\mathcal{Q}:1\leqslant n\leqslant\theta_2 q\}$,

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

and hence

$$r_n(\theta_1, \theta_2, c; q) = \sum_{\ell|n} \frac{\theta_1\theta_2}{n}\varphi\left(\frac{n}{\ell}\right)\varphi(q) - \frac{\theta_1\theta_2}{n}\varphi(q) + \left(q^{1/2}\tau^3(q)n\tau^2(n)\log^2 q\right)$$
$$= \left(1 - \frac{1}{n}\right)\theta_1\theta_2\varphi(q) + O\left(q^{1/2}\tau^3(q)n\tau^2(n)\log^2 q\right),$$

which is slightly better than (3).

Observing that the condition $2 \nmid a + b$ is equivalent to $a + b \equiv 1(\mathrm{mod}\ 2)$, thus we can consider another generalization of the D. H. Lehmer problem over short intervals. Let $q \geqslant 3$, $\ell \geqslant 1$ be fixed integers, $n$ and $c$ be integers with $(nc, q) = 1$. We define

$$T(\mathcal{A}, \mathcal{B}, c, \ell; q, n) = \#\{(a, b) \in \mathcal{A} \times \mathcal{B} | ab \equiv c(\mathrm{mod}\ q), a + b \equiv \ell(\mathrm{mod}\ n)\},$$

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

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

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

**1.** T. Estermann, On Kloosterman's sum, *Mathematika* **8** (1961), 83–86.

**2.** R. K. Guy, *Unsolved Problems in Number Theory*, 3rd. edn (Springer-Verlag, New York, 2004).

**3.** Y. Lu and Y. Yi, On the generalization of the D. H. Lehmer problem, *Acta Math. Sinica, English Ser.* **9** (2009), 1269–1274.

**4.** C. D. Pan and C. B. Pan, *Goldbach Conjecture* (Science Press, Beijing, 1981).

**5.** I. E. Shparlinski, On a generalised Lehmer problem for arbitrary powers, *East-West J. Math.* Special Vol. (2008), 197–204.

**6.** I. E. Shparlinski, On a generalisation of a Lehmer problem, *Math. Zeitschrift* **263** (2009), 619–631.

**7.** Y. Yi and W. Zhang, On the generalization of a problem of D. H. Lehmer, *Kyushu J. Math.* **56** (2002), 235–241.

**8.** W. Zhang, On D. H. Lehmer problem, *Chin. Sci. Bull.* **21** (1992), 1765–1769.

**9.** W. Zhang, A problem of D. H. Lehmer and its generalization, *Compos. Math.* **86** (1993), 307–316.

**10.** W. Zhang, A problem of D. H. Lehmer and its generalization(II), *Compos. Math.* **91** (1994), 47–56.