Proc. Indian Acad. Sci. (Math. Sci.) Vol. 120, No. 4, September 2010, pp. 507–513.

Mean value estimates of the error terms of Lehmer problem

DONGMEI REN[1] and YAMING LU[2]

[1]School of Mathematics and Statistics, Southwest University, Chongqing 400715, People's Republic of China
[2]Research Center for Basic Science, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, People's Republic of China
E-mail: dongmei.ren@gmail.com; lymxjtu@163.com

MS received 22 October 2009

Abstract. Let p be an odd prime and a be an integer coprime with p. Denote by $N(a, p)$ the number of pairs of integers b, c with $bc \equiv a(\text{mod } p)$, $1 \leq b, c < p$ and with b, c having different parity. The main purpose of this paper is to study the mean square value problem of $\left(N(a, p) - \frac{1}{2}(p-1)\right)$ over interval $(N, N+M]$ with M, N positive integers by using the analytic methods, and finally by obtaining a sharp asymptotic formula.

Keywords. Lehmer problem; Kloosterman sum; Gauss sum.

1. Introduction

Let p be an odd prime and a be an integer coprime with p. For each integer b with $1 \leq b < p$, there is a unique integer c with $1 \leq c < p$ such that $bc \equiv a(\text{mod } p)$. Let $N(a, p)$ denote the number of solutions of the congruence equation $bc \equiv a(\text{mod}\, p)$ with $1 \leq b, c < p$ such that b, c are of opposite parity. Lehmer posed the problem to find $N(1, p)$ or at least to say something nontrivial about it (see problem F12, p. 251 of [2]).

Zhang [5] proved that

$$N(1, p) = \frac{1}{2}(p-1) + O(p^{\frac{1}{2}} \ln^2 p).$$

For further properties of $N(a, p)$ in [6], he studied the mean square value of the error term $E(a, p) = N(a, p) - \frac{1}{2}(p-1)$ and obtained

$$\sum_{n=1}^{p-1} E^2(a, p) = \frac{3}{4}p^2 + O\left(p \exp\left(\frac{3 \ln p}{\ln \ln p}\right)\right),$$

where $\exp(y) = \mathrm{e}^y$. Zhang in [7] used the properties of Dedekind sum and Cochrane sum to study the Lehmer problem for the general case of an odd number $q \geq 3$, and proved the following asymptotic formula:

$$\sum_{a=1}^{q}{}' \left(N(a, q) - \frac{\phi(q)}{2}\right)^2$$

$$= \frac{3}{4}\phi^2(q) \prod_{p^\alpha \| q} \frac{(p+1)^3/p^2(p^2+1) - 1/p^{3\alpha}}{1 + 1/p + 1/p^2} + O\left(q \exp\left(\frac{4 \ln q}{\ln \ln q}\right)\right),$$

where $\sum'$ denotes the summation over all a such that $(a, q) = 1$.

In this paper, we will consider the mean square value of $E(a, p)$ over interval $(N, N+M]$, in fact, we will prove the following

Theorem. *Let p be an odd prime, M, N be positive integers. Then*

$$\sum_{N<a\le N+M} E^2(a,p) = \frac{3}{4}Mp + O\left(p^{\frac{3}{2}}\ln^5 p + M\exp\left(\frac{3\ln p}{\ln\ln p}\right)\right). \tag{1}$$

Obviously, this result is nontrivial for $M \ge p^{\frac{1}{2}+\epsilon}$ with ϵ an arbitrary positive real number.

The following symbols will be used in the proof of the theorem.

Let χ be the Dirichlet character modulo q, then $G(m,\chi) = \sum_{\substack{n\le q\\(n,q)=1}} \chi(n)e(mn/q)$ denotes the Gauss sum, and $\tau(\chi) = G(1,\chi)$; $L(s,\chi)$ is the well known Dirichlet L-function;

$\phi(n)$, $\mu(n)$ and $d(n)$ are Euler function, Möbius function and divisor function, respectively; $e(x) = \mathrm{e}^{2\pi i x}$; $[x]$ is the largest integer not exceeding x, $\{x\} = x - [x]$, $\|x\| = \min(\{x\}, 1-\{x\})$.

2. Some lemmas

To complete the proof of the theorem, we need several lemmas.

Lemma 1. *Let p be an odd prime. Then for any positive integer a with $(a,p)=1$ we have the identity*

$$E(a,p) = \frac{2}{\pi^2(p-1)} \sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}} \bar{\chi}(a)(1-2\chi(2))^2\tau^2(\chi)L^2(1,\bar{\chi}). \tag{2}$$

Proof. See ref. [6].

Lemma 2. *Under the condition of Lemma* 1, *we can obtain*

$$\begin{aligned}\sum_{n=1}^{p-1} E^2(a,p) &= \frac{4}{\pi^4(p-1)} \sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}} |1-4\chi(2)+4\chi(4)|^2\tau^2(\chi)\tau^2(\bar{\chi})L^2(1,\chi)L^2(1,\bar{\chi})\\ &= \frac{3}{4}p^2 + O\left(p\exp\left(\frac{3\ln p}{\ln\ln p}\right)\right).\end{aligned} \tag{3}$$

Proof. See ref. [6].

Lemma 3. *Let χ be the Dirichlet character modulo q, then for $N \ge q$, we get*

$$L^2(1,\chi) = \sum_{n\le N} \frac{\chi(n)d(n)}{n} + O\left(\frac{\sqrt{q}\ln q \ln N}{\sqrt{N}}\right) \qquad |L(1,\chi)|^4 \ll \ln^4 N.$$

Proof. From Pólya–Vinogradov theorem, for any $y > N$, we have

$$\sum_{N<n\leq y} \chi(n) \ll q^{\frac{1}{2}} \ln q,$$

so by Abel's identity we can get

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

Then

$$\begin{aligned} L^2(1,\chi) &= \left(\sum_{n\leq N} \frac{\chi(n)}{n} + O\left(\frac{\sqrt{q}\ln q}{N}\right)\right)^2 \\ &= \sum_{n\leq N^2} \frac{\chi(n)d(n)}{n} + O\left(\frac{\sqrt{q}\ln q\ln N}{N}\right) \\ &= \sum_{n\leq N} \frac{\chi(n)d(n)}{n} + O\left(\frac{\sqrt{q}\ln q\ln N}{\sqrt{N}}\right); \end{aligned}$$

and it is obvious

$$|L(1,\chi)|^4 \ll \ln^4 N.$$

This proves Lemma 3.

Let m, n be integers, and Q a positive integer, the well-known Kloosterman sum is defined as follows:

$$S(m,n;Q) = \sum_{\substack{d=1\\(d,Q)=1}}^{Q} e\left(m\frac{\bar{d}}{Q} + n\frac{d}{Q}\right).$$

Lemma 4. *Let $p > 2$ be a prime number, a and b be two integers satisfying $(ab, p) = 1$, then we have*

$$\sum_{c=1}^{p-1} e\left(\frac{c}{p}\right) S(a,c;p)S(b,c;p) \ll p^{\frac{3}{2}}.$$

Proof. See ref. [3].

3. Proof of the theorem

In this section we will complete the proof of the theorem. Making use of Lemmas 1 and 2, we have

$$\begin{aligned} &\sum_{N<a\leq N+M} E^2(a,p) \\ &= \frac{4}{\pi^4(p-1)^2} \sum_{N<a\leq N+M} \sum_{\substack{\chi_1 \bmod p\\ \chi_1(-1)=-1}} \sum_{\substack{\chi_2 \bmod p\\ \chi_2(-1)=-1}} \overline{\chi_1}(a)\overline{\chi_2}(a)(1-2\chi_1(2))^2(1-2\chi_2(2))^2 \\ &\quad\times \tau^2(\chi_1)\tau^2(\chi_2)L^2(1,\overline{\chi_1})L^2(1,\overline{\chi_2}) \end{aligned}$$

$$= \frac{4M}{\pi^4(p-1)^2} \sum_{\substack{\chi \bmod p \\ \chi(-1)=-1}} |1-4\chi(2)+4\chi(4)|^2 \tau^2(\chi)\tau^2(\bar{\chi}) L^2(1,\chi) L^2(1,\bar{\chi})$$

$$+ \frac{4}{\pi^4(p-1)^2} \sum_{N<a\le N+M} \sum_{\substack{\chi_1 \bmod p \\ \chi_1(-1)=-1}} \sum_{\substack{\chi_2 \bmod p \\ \chi_2(-1)=-1 \\ \chi_1\chi_2 \neq \chi_0}} \overline{\chi_1}(a)\overline{\chi_2}(a)(1-2\chi_1(2))^2$$

$$\times (1-2\chi_2(2))^2 \tau^2(\chi_1)\tau^2(\chi_2) L^2(1,\overline{\chi_1}) L^2(1,\overline{\chi_2})$$

$$= \frac{3}{4} Mp + \frac{4}{\pi^4(p-1)^2} E + O\left(M \exp\left(\frac{3 \ln p}{\ln \ln p} \right) \right), \tag{4}$$

where

$$E = \sum_{\substack{\chi_1 \bmod p \\ \chi_1(-1)=-1}} \sum_{\substack{\chi_2 \bmod p \\ \chi_2(-1)=-1 \\ \chi_1\chi_2 \neq \chi_0}} (1-2\chi_1(2))^2 (1-2\chi_2(2))^2$$

$$\times \tau^2(\chi_1)\tau^2(\chi_2) L^2(1,\overline{\chi_1}) L^2(1,\overline{\chi_2}) \sum_{N<a\le N+M} \overline{\chi_1\chi_2}(a). \tag{5}$$

Now we come to the estimation of E. Using

$$\chi(n) = \frac{1}{q} \sum_{l=1}^{q-1} G(l,\chi) e\left(-\frac{nl}{q}\right), \quad \text{if } \chi \bmod q,\ \chi \neq \chi_0,$$

we obtain

$$E = \sum_{\substack{\chi_1 \bmod p \\ \chi_1(-1)=-1}} \sum_{\substack{\chi_2 \bmod p \\ \chi_2(-1)=-1 \\ \chi_1\chi_2 \neq \chi_0}} (1-2\chi_1(2))^2 (1-2\chi_2(2))^2 \tau^2(\chi_1)\tau^2(\chi_2) L^2(1,\overline{\chi_1}) L^2(1,\overline{\chi_2})$$

$$\times \sum_{N<a\le N+M} \frac{1}{p} \sum_{l=1}^{p-1} G(l,\overline{\chi_1\chi_2}) e\left(-\frac{al}{p}\right)$$

$$= \frac{1}{p} \sum_{l=1}^{p-1} \frac{e(-(N+M+1)l/p) - e(-(N+1)l/p)}{e(l/p)-1}$$

$$\times \sum_{\substack{\chi_1 \bmod p \\ \chi_1(-1)=-1}} \sum_{\substack{\chi_2 \bmod p \\ \chi_2(-1)=-1 \\ \chi_1\chi_2 \neq \chi_0}} (1-2\chi_1(2))^2 (1-2\chi_2(2))^2 \tau^2(\chi_1)\tau^2(\chi_2)$$

$$\times L^2(1,\overline{\chi_1}) L^2(1,\overline{\chi_2}) G(l,\overline{\chi_1\chi_2})$$

$$
\begin{aligned}
&= \frac{1}{p}\sum_{l=1}^{p-1}\frac{e(-(N+M+1)l/p)-e(-(N+1)l/p)}{e(l/p)-1}\\
&\times \sum_{\substack{\chi_1 \bmod p\\ \chi_1(-1)=-1}}\ \sum_{\substack{\chi_2 \bmod p\\ \chi_2(-1)=-1}} (1-2\chi_1(2))^2(1-2\chi_2(2))^2\tau^2(\chi_1)\tau^2(\chi_2)\\
&\times L^2(1,\overline{\chi_1})L^2(1,\overline{\chi_2})G(l,\overline{\chi_1\chi_2}) - \frac{1}{p}\sum_{l=1}^{p-1}\frac{e(-(N+M+1)l/p)-e(-(N+1)l/p)}{e(l/p)-1}\\
&\times \sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}} |1-2\chi(2)|^4|\tau(\chi)|^4|L(1,\chi)|^4G(l,\chi_0)\\
&= E_1 - E_2. \qquad (6)
\end{aligned}
$$

From Lemma 3, it is easy to deduce that

$$
\begin{aligned}
E_2 &= \frac{1}{p}\sum_{l=1}^{p-1}\frac{e(-(N+M+1)l/p)-e(-(N+1)l/p)}{e(l/p)-1}\\
&\quad\times \sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}} |1-2\chi(2)|^4|\tau(\chi)|^4|L(1,\chi)|^4G(l,\chi_0)\\
&\ll p^2\ln^4 N\sum_{l=1}^{p-1}\frac{1}{|e(l/p)-1|}\\
&\ll p^2\ln^4 N\sum_{l=1}^{p-1}\frac{1}{\|l/p\|}\\
&\ll p^3\ln p\ln^4 N. \qquad (7)
\end{aligned}
$$

Before the estimation of E_1, first we will consider the inner sum of E_1. Let

$$
S = \sum_{\substack{\chi_1 \bmod p\\ \chi_1(-1)=-1}}\ \sum_{\substack{\chi_2 \bmod p\\ \chi_2(-1)=-1}} \chi_1(x)\chi_2(y)\tau^2(\chi_1)\tau^2(\chi_2)L^2(1,\overline{\chi_1})L^2(1,\overline{\chi_2})G(l,\overline{\chi_1\chi_2}), \qquad (8)
$$

where x, y are integers in the set $\{1, 2, 4\}$.

Making use of Lemma 3 and let $N = p^4$, we have

$$
\begin{aligned}
S &= \sum_{\substack{\chi_1 \bmod p\\ \chi_1(-1)=-1}}\ \sum_{\substack{\chi_2 \bmod p\\ \chi_2(-1)=-1}} \chi_1(x)\chi_2(y)\tau^2(\chi_1)\tau^2(\chi_2)\\
&\quad\times \sum_{n\le N}\frac{\overline{\chi_1}(n)d(n)}{n}\sum_{m\le N}\frac{\overline{\chi_1}(m)d(m)}{m}G(l,\overline{\chi_1\chi_2}) + O(p^3\ln^4 p)\\
&= S_1 + O(p^3\ln^4 p). \qquad (9)
\end{aligned}
$$

For S_1, from the definition of Gauss sum, we have

$$
\begin{aligned}
S_1 = & \sum_{\substack{n\le N\\(n,p)=1}} \frac{d(n)}{n} \sum_{\substack{m\le N\\(m,p)=1}} \frac{d(m)}{m} \sum_{\substack{\chi_1 \bmod p\\ \chi_1(-1)=-1}} \sum_{\substack{\chi_2 \bmod p\\ \chi_2(-1)=-1}} \\
& \times \chi_1(x\bar{n})\chi_2(y\bar{m})\tau^2(\chi_1)\tau^2(\chi_2)G(l,\overline{\chi_1\chi_2}) \\
= & \sum_{\substack{n\le N\\(n,p)=1}} \frac{d(n)}{n} \sum_{\substack{m\le N\\(m,p)=1}} \frac{d(m)}{m} \sum_{\substack{c\le p\\(c,p)=1}} e\left(\frac{lc}{p}\right) \sum_{\substack{a_1\le p\\(a_1,p)=1}} \sum_{\substack{a_2\le p\\(a_2,p)=1}} e\left(\frac{a_1+a_2}{p}\right) \\
& \times \sum_{\substack{b_1\le p\\(b_1,p)=1}} \sum_{\substack{b_2\le p\\(b_2,p)=1}} e\left(\frac{b_1+b_2}{p}\right) \sum_{\substack{\chi_1 \bmod p\\ \chi_1(-1)=-1}} \chi_1(a_1a_2)\chi_1(x\overline{cn}) \\
& \times \sum_{\substack{\chi_2 \bmod p\\ \chi_2(-1)=-1}} \chi_2(b_1b_2)\chi_2(y\overline{cm}) \\
= & \frac{(p-1)^2}{4} \sum_{\substack{n\le N\\(n,p)=1}} \frac{d(n)}{n} \sum_{\substack{m\le N\\(m,p)=1}} \frac{d(m)}{m} \sum_{\substack{a_1\le p\\(a_1,p)=1}} \sum_{\substack{a_2\le p\\(a_2,p)=1}} e\left(\frac{a_1+a_2}{p}\right) \\
& \times \sum_{\substack{b_1\le p\\(b_1,p)=1}} \sum_{\substack{b_2\le p\\(b_2,p)=1}} e\left(\frac{b_1+b_2}{p}\right) \sum_{\substack{c\le p\\(c,p)=1}} e\left(\frac{lc}{p}\right) \\
& \times \left(\sum_{a_1a_2x\overline{cn}\equiv 1 (\bmod p)} 1 - \sum_{a_1a_2x\overline{cn}\equiv -1 (\bmod p)} 1 \right) \\
& \times \left(\sum_{b_1b_2y\overline{cm}\equiv 1 (\bmod p)} 1 - \sum_{b_1b_2y\overline{cm}\equiv -1 (\bmod p)} 1 \right) \\
= & \frac{(p-1)^2}{4} \sum_{\substack{n\le N\\(n,p)=1}} \frac{d(n)}{n} \sum_{\substack{m\le N\\(m,p)=1}} \frac{d(m)}{m} \sum_{\alpha=1}^{2}\sum_{\beta=1}^{2}(-1)^{\alpha+\beta} A_{\alpha\beta}, \qquad (10)
\end{aligned}
$$

where

$$
\begin{aligned}
A_{\alpha\beta} = & \sum_{\substack{c\le p\\(c,p)=1}} e\left(\frac{lc}{p}\right) \sum_{\substack{a_1\le p\\(a_1,p)=1}} \sum_{\substack{a_2\le p\\(a_2,p)=1\\ a_1a_2x\overline{cn}\equiv(-1)^{\alpha}(\bmod p)}} e\left(\frac{a_1+a_2}{p}\right) \\
& \times \sum_{\substack{b_1\le p\\(b_1,p)=1}} \sum_{\substack{b_2\le p\\(b_2,p)=1\\ b_1b_2y\overline{cm}\equiv(-1)^{\beta}(\bmod p)}} e\left(\frac{b_1+b_2}{p}\right).
\end{aligned}
$$

Noting that

$$\sum_{\substack{a_1 \le p \\ (a_1,p)=1}} \sum_{\substack{a_2 \le p \\ (a_2,p)=1 \\ a_1 a_2 x \overline{cn} \equiv (-1)^\alpha (\bmod p)}} e\left(\frac{a_1+a_2}{p}\right) = S((-1)^\alpha \bar{x} cn, 1;\, p),$$

we obtain

$$A_{\alpha\beta} = \sum_{\substack{c \le p \\ (c,p)=1}} e\left(\frac{lc}{p}\right) S((-1)^\alpha \bar{x} cn, 1;\, p) S((-1)^\beta \bar{y} cm, 1;\, p)$$

$$= \sum_{\substack{c \le p \\ (c,p)=1}} e\left(\frac{lc}{p}\right) S((-1)^\alpha \bar{x} n, c;\, p) S((-1)^\beta \bar{y} m, c;\, p).$$

Notice that $(x, p) = (y, p) = 1$, $N = p^4$, and combining (9), (10) and Lemma 4 we have

$$S \ll p^{\frac{7}{2}} \ln^4 p. \tag{11}$$

So we get

$$E_1 \ll \frac{1}{p} \sum_{l=1}^{p-1} \frac{1}{|e(l/p) - 1|} |S|$$

$$\ll \frac{1}{p} \sum_{l=1}^{p-1} \frac{1}{\|l/p\|} |S|$$

$$\ll p^{\frac{7}{2}} \ln^5 p. \tag{12}$$

Our theorem follows at once from (4), (6), (7) and (12).

Acknowledgment

The authors greatly appreciate Prof. Wenpeng Zhang and Yuan Yi for their kind comments and suggestions. This work is supported by SWU (No. SWU110020) and NSF (No. 10601039) of People's Republic of China.

References

[1] Apostol Tom M, Introduction to Analytic Number Theory (New York: Springer-Verlag) (1976)
[2] Guy R K, Unsolved Problems in Number Theory (New York: Springer-Verlag) (1994)
[3] Lu Y and Yi Y, On Cochrane sum over short intervals, *J. Math. Anal. Appl.* **356** (2009) 502–516
[4] Pan C and Pan C, Goldbach Conjecture (Beijing: Science Press) (1981)
[5] Zhang W, A problem of D.H. Lehmer and its generalization (II), *Compositio Math.* **91** (1994) 47–56
[6] Zhang W, A problem of D.H. Lehmer and its mean square value formula, *Japanese J. Math.* **29** (2003) 109–116
[7] Zhang W, Xu Z and Yi Y, A problem of D.H. Lehmer and its mean square value formula, *J. Number Theory* **103** (2003) 197–213