Bull. Korean Math. Soc. **53** (2016), No. 2, pp. 487–494
http://dx.doi.org/10.4134/BKMS.2016.53.2.487

A MEAN VALUE FUNCTION AND ITS COMPUTATIONAL FORMULA RELATED TO D. H. LEHMER'S PROBLEM

Tingting Wang

Abstract. Let p be an odd prime and c be a fixed integer with $(c,p)=1$. For each integer a with $1 \le a \le p-1$, it is clear that there exists one and only one b with $0 \le b \le p-1$ such that $ab \equiv c \bmod p$. Let $N(c,p)$ denote the number of all solutions of the congruence equation $ab \equiv c \bmod p$ for $1 \le a, b \le p-1$ in which a and $\overline{b}$ are of opposite parity, where $\overline{b}$ is defined by the congruence equation $b\overline{b} \equiv 1 \bmod p$. The main purpose of this paper is using the mean value theorem of Dirichlet L-functions and the properties of Gauss sums to study the computational problem of one kind mean value function related to $E(c,p) = N(c,p) - \frac{1}{2}\phi(p)$, and give its an exact computational formula.

1. Introduction

Let $q \ge 3$ be an odd number and c be a fixed integer with $(c,q)=1$. For each integer a with $1 \le a \le q-1$, it is clear that there exists one and only one b with $0 \le b \le q-1$ such that $ab \equiv c \bmod q$. Let $M(c,q)$ denote the number of cases in which a and b are of opposite parity. In reference [5], Professor D. H. Lehmer asked to study $M(1,p)$ or at least to say something nontrivial about it, where p is a prime. It is known that $M(1,p) \equiv 2$ or $0 \bmod 4$ when $p \equiv \pm 1 \bmod 4$. The second author [8] studied the asymptotic properties of $M(1,q)$, and obtained a sharp asymptotic formula for $M(1,q)$.

Let $R(a,p) = M(a,p) - \frac{p-1}{2}$. The first author [12] also studied the mean square value of $R(a,p)$, and proved the asymptotic formula

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

where $\exp(y) = e^y$.

Received February 24, 2015.
2010 *Mathematics Subject Classification.* Primary 11L40, 11F20.
Key words and phrases. Lehmer's problem, error term, mean value, computational formula.
This work is supported by the N. S. F. (11501452) and the P. S. F. (2014JQ2-1005) of P. R. China.

Now, we let p be an odd prime, c be any integer with $(c,\ p) = 1$, $N(c,p)$ denote the number of pairs of integers a, b with $ab \equiv c \bmod p$ for $1 \le a, b \le p-1$ in which a and $\overline{b}$ are of opposite parity. We define $E(c,p)$ as follows:

$$E(c,p) = N(c,p) - \frac{1}{2}\phi(p).$$

Some contents related to $E(c,p)$ can also be found in [13]. For convenience, we assume that $E(c,p) = 0$, if $p \mid c$. The main purpose of this paper is using the mean value theorem of Dirichlet L-functions and the properties of Gauss sums to study the computational problem of one kind mean value function related to $E(c,p)$, and give its an exact computational formula. That is, we shall prove the following:

Theorem. *Let $p > 3$ be a prime. Then for any integers $m \ge 0$ and a, b, c with $(abc, p) = (a^2 - 4b, p) = 1$, we have the identity*

$$\frac{1}{p}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} E^{2m+1}\left(r^2 + ars + bs^2 + c, p\right) = \left(\frac{a^2-4b}{p}\right) \cdot E^{2m+1}\left(c,p\right),$$

where $\left(\frac{*}{p}\right)$ denotes the Legendre symbol.

It is clear that $\left(\frac{a^2-4b}{p}\right) = \pm 1$, if $(a^2 - 4b, p) = 1$. So for any integer c with $(c,p) = 1$, $E^{2m+1}(c,p)$ in the above theorem on the mean value transform is unchanged. Especially taking $c = 1$, 2 and -1, then from our theorem we may immediately deduce the following three interesting corollaries:

Corollary 1. *Let $p > 3$ be a prime. Then for any integers $m \ge 0$ and a, b with $(ab, p) = (a^2 - 4b, p) = 1$, we have the identity*

$$\frac{1}{p}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} E^{2m+1}\left(r^2 + ars + bs^2 + 1, p\right) = -\left(\frac{a^2-4b}{p}\right) \cdot \frac{(p-1)^{2m+1}}{2^{2m+1}}.$$

Corollary 2. *Let $p > 3$ be a prime. Then for any integers $m \ge 0$ and a, b with $(ab, p) = (a^2 - 4b, p) = 1$, we have the identity*

$$\frac{1}{p}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} E^{2m+1}\left(r^2 + ars + bs^2 + 2, p\right) = \begin{cases} \left(\frac{a^2-4b}{p}\right), & \text{if } p \equiv 3 \bmod 4; \\ 0, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Corollary 3. *Let $p > 3$ be a prime. Then for any integers a and b with $(ab, p) = (a^2 - 4b, p) = 1$, we have the identity*

$$\frac{1}{p}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} E\left(r^2 + ars + bs^2 - 1, p\right) = \left(\frac{a^2-4b}{p}\right) \cdot \frac{p-1}{2}.$$

For general odd number $q \ge 3$, whether there exists a similar formula (as in Theorem) is an open problem.

2. Several lemmas

In this section, we shall give several lemmas, which are necessary in the proof of our theorem. First we have the following:

Lemma 1. *Suppose* χ *is an odd character* mod q. *Then we have the identity*

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

Proof. See reference [4]. □

Lemma 2. *Let* p *be an odd prime. Then for any integer* c *with* $(c,p)=1$, *we have the identity*

$$E(c,p) = -\frac{2\pi^{-2}p}{p-1}\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}\overline{\chi}(c)\cdot|1-2\chi(2)|^2\cdot|L(1,\chi)|^2,$$

where $\sum\limits_{\substack{\chi \bmod p\\ \chi(-1)=-1}}$ *denotes the summation over all odd characters* χ mod p, $L(1,\chi)$ *denotes Dirichlet* L*-function corresponding to character* χ.

Proof. From the orthogonality relation for character sums mod p and the definition of $N(c,p)$, we have

$$\begin{aligned}
N(c,p) &= \frac{1}{2}\sum_{a=1}^{p}\sideset{}{'}\sum_{\substack{b=1\\ ab\equiv c(p)}}^{p}\left(1-(-1)^{a+\overline{b}}\right) = \frac{1}{2}\phi(p) - \frac{1}{2}\sum_{a=1}^{p}\sum_{\substack{b=1\\ ab\equiv c(p)}}^{p}(-1)^{a+\overline{b}}\\
&= \frac{1}{2}\phi(p) - \frac{1}{2\phi(p)}\sum_{\chi \bmod p}\overline{\chi}(c)\left(\sum_{a=1}^{p}(-1)^a\chi(a)\right)\left(\sum_{b=1}^{p}(-1)^{\overline{b}}\chi(b)\right)\\
&= \frac{1}{2}\phi(p) - \frac{1}{2\phi(p)}\sum_{\chi \bmod p}\overline{\chi}(c)\left(\sum_{a=1}^{p}(-1)^a\chi(a)\right)\left(\sum_{b=1}^{p}(-1)^{b}\chi(\overline{b})\right)\\
&= \frac{1}{2}\phi(p) - \frac{1}{2\phi(p)}\sum_{\chi \bmod p}\overline{\chi}(c)\left(\sum_{a=1}^{p}(-1)^a\chi(a)\right)\overline{\left(\sum_{b=1}^{p}(-1)^{b}\chi(b)\right)}
\end{aligned}$$

$$= \frac{1}{2}\phi(p) - \frac{1}{2\phi(p)}\sum_{\chi \bmod p}\overline{\chi}(c)\left|\sum_{a=1}^{p}(-1)^a\chi(a)\right|^2. \tag{1}$$

If $\chi(-1)=1$, then

$$\sum_{a=1}^{q}(-1)^a\chi(a) = 0. \tag{2}$$

If $\chi(-1) = -1$, then

$$\sum_{a=1}^{q}(-1)^a\chi(a) = 2\chi(2)\sum_{a=1}^{\frac{q-1}{2}}\chi(a). \tag{3}$$

If $\chi(-1) = -1$, then from Theorems 12.11 and 12.20 of [1] we also have

$$\frac{1}{p}\sum_{b=1}^{p} b\chi(b) = \frac{i}{\pi}\tau(\chi)L(1,\overline{\chi}), \tag{4}$$

where $\tau(\chi)$ denotes the Gauss sums associated with χ and $|\tau(\chi)| = \sqrt{p}$.

Combining (1), (2), (3), (4) and Lemma 1 we may immediately deduce

$$E(c,p) = -\frac{2\pi^{-2}p}{p-1}\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}\overline{\chi}(c)|1-2\chi(2)|^2\cdot|L(1,\chi)|^2.$$

This proves Lemma 2. $\square$

Lemma 3. *Let p be an odd prime, a, b and c are integers with $(abc,p) = (a^2-4b,p) = 1$. Then for any non-principal character $\chi \bmod p$, we have the identity*

$$\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}\chi\left(r^2+ars+bs^2+c\right) = \chi(c)\cdot\left(\frac{a^2-4b}{p}\right)\cdot p,$$

where $\left(\frac{*}{p}\right)$ denotes the Legendre symbol.

Proof. Since any non-principal character $\chi \bmod p$ is a primitive character mod p, so from the properties of Gauss sums we conclude that

$$\begin{aligned}
&\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}\chi\left(r^2+ars+bs^2+c\right)\\
&= \frac{1}{\tau(\overline{\chi})}\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}\sum_{t=1}^{p-1}\overline{\chi}(t)\,e\left(\frac{t(r^2+ars+bs^2+c)}{p}\right)\\
&= \frac{1}{\tau(\overline{\chi})}\sum_{t=1}^{p-1}\overline{\chi}(t)\,e\left(\frac{ct}{p}\right)\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}e\left(\frac{tr^2+tars+tbs^2}{p}\right)\\
&= \frac{1}{\tau(\overline{\chi})}\sum_{t=1}^{p-1}\overline{\chi}(t)\,e\left(\frac{ct}{p}\right)\left(\sum_{r=0}^{p-1}e\left(\frac{tr^2}{p}\right)+\sum_{r=0}^{p-1}\sum_{s=1}^{p-1}e\left(\frac{t(r^2+ars+bs^2)}{p}\right)\right)\\
&= \frac{1}{\tau(\overline{\chi})}\sum_{t=1}^{p-1}\overline{\chi}(t)\,e\left(\frac{ct}{p}\right)\left(\sum_{r=0}^{p-1}e\left(\frac{tr^2}{p}\right)+\sum_{r=0}^{p-1}\sum_{s=1}^{p-1}e\left(\frac{ts^2(r^2+ar+b)}{p}\right)\right)
\end{aligned}$$

$$= \frac{1}{\tau(\overline{\chi})}\sum_{t=1}^{p-1}\overline{\chi}(t)\,e\left(\frac{ct}{p}\right)\left(\sum_{r=0}^{p-1}e\left(\frac{tr^2}{p}\right)-p+\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}e\left(\frac{ts^2(r^2+ar+b)}{p}\right)\right). \tag{5}$$

From Theorem 7.5.4 of Hua's book [6] we know that for any integer u with $(u,p)=1$, we have

$$\sum_{r=0}^{p-1} e\left(\frac{tr^2}{p}\right) = \left(\frac{t}{p}\right)\sum_{r=0}^{p-1} e\left(\frac{r^2}{p}\right) \equiv \left(\frac{t}{p}\right)\cdot G(p). \tag{6}$$

For any integer n with $(n,p)=1$, from [6] (§7.8, Theorem 8.2) we also have

$$\sum_{r=0}^{p-1}\left(\frac{r^2+n}{p}\right) = -1. \tag{7}$$

Therefore,

$$\begin{aligned}
&\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} e\left(\frac{ts^2(r^2+ar+b)}{p}\right)\\
&= \sum_{r=0}^{p-1}\left(\frac{t(r^2+ar+b)}{p}\right)\cdot G(p) + p\cdot \sum_{\substack{r=0\\ r^2+ar+b\equiv 0 \bmod p}}^{p-1} 1\\
&= \left(\frac{t}{p}\right)\cdot G(p)\cdot\sum_{r=0}^{p-1}\left(\frac{(2r+a)^2+4b-a^2}{p}\right) + p\cdot \sum_{\substack{r=0\\ (2r+a)^2+4b-a^2\equiv 0 \bmod p}}^{p-1} 1\\
&= -\left(\frac{t}{p}\right)\cdot G(p) + \left(1+\left(\frac{a^2-4b}{p}\right)\right)\cdot p. \qquad (8)
\end{aligned}$$

Then from (5), (6), (7) and (8) we deduce the identity

$$\begin{aligned}
&\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}\chi\left(r^2+ars+bs^2+c\right)\\
&= \frac{1}{\tau(\overline{\chi})}\sum_{t=1}^{p-1}\overline{\chi}(t)\, e\left(\frac{ct}{p}\right)\left(\left(\frac{t}{p}\right)\cdot G(p) - p - \left(\frac{t}{p}\right)\cdot G(p) + \left(1+\left(\frac{a^2-4b}{p}\right)\right)\cdot p\right)\\
&= \left(\frac{a^2-4b}{p}\right)\cdot p\cdot\frac{1}{\tau(\overline{\chi})}\sum_{t=1}^{p-1}\overline{\chi}(t)\, e\left(\frac{ct}{p}\right)\\
&= \chi(c)\cdot\left(\frac{a^2-4b}{p}\right)\cdot p.
\end{aligned}$$

This proves Lemma 3. □

To introduce Lemma 4, we need to give the definition of the Dedekind sums. For a positive integer q and an arbitrary integer h, the classical Dedekind sums $S(h,q)$ is defined by

$$S(h,q) = \sum_{a=1}^{q}\left(\left(\frac{a}{q}\right)\right)\left(\left(\frac{ah}{q}\right)\right),$$

where

$$((x)) = \begin{cases} x - [x] - \frac{1}{2}, & \text{if } x \text{ is not an integer;} \\ 0, & \text{if } x \text{ is an integer.} \end{cases}$$

The various properties of $S(h,k)$ had been studied by many authors, see [2, 3, 7, 9, 10, 11]. For example, L. Carlitz [2] proved the reciprocity theorem of $S(h,q)$. That is, for all positive integers h and q with $(h,q)=1$, we have the identity

$$S(h,q) + S(q,h) = \frac{h^2+q^2+1}{12hq} - \frac{1}{4}. \tag{9}$$

For Dedekind sums $S(h,q)$, there is also another kind of expression as follows:

Lemma 4. *Let $q>2$ be an integer, then for any integer a with $(a,q)=1$, we have the identity*

$$S(a,q) = \frac{1}{\pi^2 q} \sum_{d|q} \frac{d^2}{\phi(d)} \sum_{\substack{\chi \bmod d \\ \chi(-1)=-1}} \chi(a)|L(1,\chi)|^2.$$

Proof. See Lemma 2 of reference [10]. $\square$

3. Proof of Theorem

In this section, we will use the lemmas from Section 2 to prove our theorem. First note that if all χ_i $(i=1,2,\ldots,2m+1)$ are odd characters $\bmod p$, then the product $\chi_1\chi_2\cdots\chi_{2m+1}$ is also an odd character $\bmod p$. So from Lemma 2 and Lemma 3 we have

$$\begin{aligned}
&\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} E^{2m+1}\left(r^2+ars+bs^2+c,p\right) \\
&= \sum_{r=0}^{p-1}\sum_{s=0}^{p-1} \left(\frac{-2\pi^{-2}p}{p-1} \sum_{\substack{\chi \bmod p \\ \chi(-1)=-1}} \overline{\chi}\left(r^2+ars+bs^2+c\right) |1-2\chi(2)|^2 \cdot |L(1,\chi)|^2 \right)^{2m+1} \\
&= \left(\frac{-2\pi^{-2}p}{p-1}\right)^{2m+1} \sum_{\substack{\chi_1 \bmod p \\ \chi_1(-1)=-1}} \cdots \sum_{\substack{\chi_{2m+1} \bmod p \\ \chi_{2m+1}(-1)=-1}} \sum_{r=0}^{p-1}\sum_{s=0}^{p-1} \overline{\chi_1}\cdots\overline{\chi}_{2m+1}\left(r^2+ars+bs^2+c\right) \\
&\quad \times |1-2\chi_1(2)|^2\cdot|L(1,\chi_1)|^2 \cdots |1-2\chi_{2m+1}(2)|^2\cdot|L(1,\chi_{2m+1})|^2 \\
&= \left(\frac{a^2-4b}{p}\right)\cdot p\cdot\left(\frac{-2\pi^{-2}p}{p-1}\right)^{2m+1} \sum_{\substack{\chi_1 \bmod p \\ \chi_1(-1)=-1}} \cdots \sum_{\substack{\chi_{2m+1} \bmod p \\ \chi_{2m+1}(-1)=-1}} \overline{\chi_1}\cdots\overline{\chi}_{2m+1}(c) \\
&\quad \times |1-2\chi_1(2)|^2\cdot|L(1,\chi_1)|^2 \cdots |1-2\chi_{2m+1}(2)|^2\cdot|L(1,\chi_{2m+1})|^2
\end{aligned}$$

$$= \left(\frac{a^2-4b}{p}\right)\cdot p\cdot\left(\frac{-2\pi^{-2}p}{p-1}\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}\overline{\chi}(c)\cdot|1-2\chi(2)|^2\cdot|L(1,\chi)|^2\right)^{2m+1}$$

$$= \left(\frac{a^2-4b}{p}\right)\cdot p\cdot E^{2m+1}(c,p).$$

This proves our theorem.

Now we prove Corollary 1, Corollary 2 and Corollary 3. From (9) and Lemma 4 we have

$$\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}\chi(a)|L(1,\chi)|^2 = \pi^2\cdot\frac{p-1}{p}\cdot S(a,p), \tag{10}$$

$$\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}|L(1,\chi)|^2 = \frac{\pi^2}{12}\cdot\frac{(p-1)^2(p-2)}{p^2}, \tag{11}$$

$$\begin{aligned}&\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}\chi(2)|L(1,\chi)|^2 = \pi^2\cdot\frac{p-1}{p}\cdot S(2,p)\\ &= \pi^2\cdot\frac{p-1}{p}\cdot\left(\frac{p^2+4+1}{24p}-\frac{1}{4}-S(p,2)\right) = \frac{\pi^2}{24}\cdot\frac{(p-1)^2(p-5)}{p^2}\end{aligned} \tag{12}$$

and

$$\begin{aligned}&\sum_{\substack{\chi \bmod p\\ \chi(-1)=-1}}\chi(4)|L(1,\chi)|^2 = \pi^2\cdot\frac{p-1}{p}\cdot S(4,p)\\ &= \pi^2\cdot\frac{p-1}{p}\cdot\left(\frac{p^2+16+1}{48p}-\frac{1}{4}-S(p,4)\right)\\ &= \begin{cases}\frac{\pi^2}{48}\cdot\frac{(p-1)^2(p-17)}{p^2}, & \text{if } p\equiv 1 \bmod 4;\\ \frac{\pi^2}{48}\cdot\frac{(p-1)(p^2-6p+17)}{p^2}, & \text{if } p\equiv 3 \bmod 4.\end{cases}\end{aligned} \tag{13}$$

From (11), (12) and Lemma 2 we can deduce the identity

$$E(1,p) = -\frac{1}{2}\cdot(p-1). \tag{14}$$

Combining Theorem and (14) we may immediately obtain the identity

$$\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}E^{2m+1}\left(r^2+ars+bs^2+1,p\right) = -\left(\frac{a^2-4b}{p}\right)\cdot p\cdot\frac{(p-1)^{2m+1}}{2^{2m+1}}.$$

This proves Corollary 1.

From (11), (12), (13) and Lemma 2 we can also deduce the identity

$$E(2,p) = -\frac{2\pi^{-2}p}{p-1} \sum_{\substack{\chi \bmod p \\ \chi(-1)=-1}} \overline{\chi}(2) \cdot |1-2\chi(2)|^2 \cdot |L(1,\chi)|^2$$

$$(15) \qquad = \begin{cases} 0, & \text{if } p \equiv 1 \bmod 4; \\ 1, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Combining Theorem and (15) we may immediately obtain the identity

$$\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} E^{2m+1}\left(r^2+ars+bs^2+2,p\right) = \begin{cases} \left(\frac{a^2-4b}{p}\right) \cdot p, & \text{if } p \equiv 3 \bmod 4; \\ 0, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

This proves Corollary 2.

Note that $E(-c,p) = -E(c,p)$, so Corollary 3 follows from Theorem and Corollary 1 with $m = 0$. This completes the proof of all results.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] L. Carlitz, *The reciprocity theorem for Dedekind sums*, Pacific J. Math. **3** (1953), 513–522.

[3] J. B. Conrey, E. Fransen, R. Klein, and C. Scott, *Mean values of Dedekind sums*, J. Number Theory **56** (1996), no. 2, 214–226.

[4] T. Funakura, *On Kronecker's limit formula for Dirichlet series with periodic coefficients*, Acta Arith. **55** (1990), no. 1, 59–73.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, (Second Edition), Springer-Verlag, New York, 1994.

[6] L. K. Hua, *Introduction to Number Theory*, Science Press, Beijing, 1979.

[7] C. Jia, *On the mean value of Dedekind sums*, J. Number Theory **87** (2001), no. 2, 173–188.

[8] W. Zhang, *On a problem of D.H.Lehmer and its generalization*, Composito Math. **86** (1993), no. 3, 307–316.

[9] ______, *A problem of D. H. Lehmer and its generalization (II)*, Compositio Math. **91** (1994), no. 1, 47–56.

[10] ______, *On the mean values of Dedekind sums*, J. Theór. Nombres Bordeaux **8** (1996), no. 2, 429–442.

[11] ______, *A note on the mean square value of the Dedekind sums*, Acta Math. Hungar. **86** (2000), no. 4, 275–289.

[12] ______, *A problem of D. H. Lehmer and its mean square value formula*, Japan. J. Math. **29** (2003), no. 1, 109–116.

[13] ______, *A mean value related to D. H. Lehemer's problem and the Ramanujan's sum*, Glasg. Math. J. **54** (2012), no. 1, 155–162.

College of Science
Northwest A&F University
Yangling, Shaanxi 712100, P. R. China
E-mail address: ttwang@nwsuaf.edu.cn