

## SOME NEW SUMS RELATED TO D. H. LEHMER PROBLEM

HAN ZHANG, WENPENG ZHANG, Xi'an

(Received May 4, 2014)

*Abstract.* About Lehmer's number, many people have studied its various properties, and obtained a series of interesting results. In this paper, we consider a generalized Lehmer problem: Let  $p$  be a prime, and let  $N(k; p)$  denote the number of all  $1 \leq a_i \leq p-1$  such that  $a_1 a_2 \dots a_k \equiv 1 \pmod{p}$  and  $2 \mid a_i + \bar{a}_i + 1$ ,  $i = 1, 2, \dots, k$ . The main purpose of this paper is using the analytic method, the estimate for character sums and trigonometric sums to study the asymptotic properties of the counting function  $N(k; p)$ , and give an interesting asymptotic formula for it.

*Keywords:* Lehmer number; analytic method; trigonometric sums; asymptotic formula

*MSC 2010:* 11L05, 11L40

## 1. INTRODUCTION

Let  $p$  be an odd prime. For each integer  $a$  with  $1 \leq a \leq p-1$ , it is clear that there exists one and only one  $\bar{a}$  with  $0 \leq \bar{a} \leq p-1$  such that  $a\bar{a} \equiv 1 \pmod{p}$ . Let  $N(p)$  denote the number of all  $1 \leq a \leq p-1$  in which  $a$  and  $\bar{a}$  are of opposite parity. Professor D. H. Lehmer [3] asked us to study  $N(p)$  or at least to say something nontrivial about it. It is known that  $N(p) \equiv 2$  or  $0 \pmod{4}$  when  $p \equiv \pm 1 \pmod{4}$ . For the sake of convenience, we call such a number the Lehmer number. Some works related to the Lehmer number can be found in references [7]–[10]. For example, Zhang [9] and [10] proved the asymptotic formula

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

where  $f(x) = O(g(x))$  means that the quotient  $|f(x)/g(x)|$  is bounded for  $x \geq a$ . That is, there exists a constant  $M > 0$  such that  $|f(x)| \leq M|g(x)|$  for all  $x \geq a$ .

---

This work was supported by the P.S.F. (2013JZ001) and N.S.F. (11371291) of P. R. China.

In this paper, we study two new problems related to the Lehmer number. For any fixed integer  $k \geq 2$ , we define the sums  $N(k, p)$  and  $M(k, p)$  as follows:

$$N(k, p) = \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod{p}}}^{p-1} \dots \sum_{a_k=1}^{p-1} (1 - (-1)^{a_1 + \bar{a}_1}) \dots (1 - (-1)^{a_k + \bar{a}_k})$$

and

$$M(k, p) = \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod{p} \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (1 - (-1)^{a_1 + \bar{a}_1}) \dots (1 - (-1)^{a_k + \bar{a}_k}).$$

In fact, the estimation of  $N(k, p)$  is a generalization and extension of Lehmer's problem. For example, if  $k = 2$ , then from the definition of  $N(2, p)$  we have

$$\begin{aligned} (1.1) \quad N(2, p) &= \frac{1}{4} \sum_{\substack{a=1 \\ ab \equiv 1 \pmod{p}}}^{p-1} \sum_{b=1}^{p-1} (1 - (-1)^{a+\bar{a}})(1 - (-1)^{b+\bar{b}}) \\ &= \frac{1}{4} \sum_{a=1}^{p-1} (1 - (-1)^{a+\bar{a}})^2 = \frac{1}{2} \sum_{a=1}^{p-1} (1 - (-1)^{a+\bar{a}}) = N(p). \end{aligned}$$

So  $N(2, p)$  is just  $N(p)$ , the Lehmer number.

Obviously, people will naturally ask for the asymptotic properties of these sums. In regard to this question, it seems that no authors have studied it yet, at least we have not seen any related result before. The problems are interesting, because they are actually the Lehmer problem with some conditions.

In this paper, we shall use the analytic method and the properties of trigonometric sums to study the asymptotic properties of  $N(k, p)$  and  $M(k, p)$ , and give two sharp asymptotic formulae for them. Namely, we shall prove the following two conclusions:

**Theorem 1.** *Let  $p$  be an odd prime. Then for any integer  $k \geq 2$ , we have the asymptotic formula*

$$N(k, p) = \begin{cases} \frac{1}{2}p + O(p^{1/2} \ln^2 p) & \text{if } k = 2, \\ \frac{1}{8}p^2 + O(p^{3/2} \ln^6 p) & \text{if } k = 3, \\ \frac{1}{2^k}p^{k-1} + O\left(p^{k-3/2} \left(\frac{1}{2} + \frac{3 \ln^2 p}{2\sqrt{p}}\right)^k \ln^2 p\right) \\ \quad + O\left(\frac{(3\sqrt{p} \ln^2 p)^k}{2^k}\right) & \text{if } k \geq 4, \end{cases}$$

where the constant  $O$  does not depend on  $k$ .

**Theorem 2.** *Let  $p$  be an odd prime. Then for any integer  $k \geq 4$ , we have the asymptotic formula*

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

It is clear that if  $k \geq 5$ , then Theorem 2 yields an asymptotic formula for  $M(k, p)$ . In particular, for  $k = 5$  and  $7$ , we have the following two corollaries:

**Corollary 1.** *Let  $p$  be an odd prime. Then we have the asymptotic formula*

$$M(5, p) = \frac{1}{32} p^3 + O(p^{5/2} \ln^{10} p).$$

**Corollary 2.** *Let  $p$  be an odd prime. Then we have the asymptotic formula*

$$M(7, p) = \frac{1}{128} p^5 - \frac{3}{64} p^4 + O(p^{7/2} \ln^{14} p).$$

## 2. SEVERAL LEMMAS

In this section, we shall give several lemmas which are necessary in the proofs of our theorems. Hereinafter, we shall use many properties of Gauss sums and trigonometric sums. All these prerequisites can be found in references [1] and [5], so they will not be repeated here. First we have the following:

**Lemma 1.** *Let  $p$  be an odd prime. Then for any character  $\chi \bmod p$  and any integers  $m$  and  $n$ , we have the estimate*

$$\sum_{a=1}^{p-1} \chi(a) \exp\left(\frac{ma + n\bar{a}}{p}\right) \leq 2p^{1/2}(m, n, p)^{1/2},$$

where  $(m, n, p)$  denotes the greatest common divisor of  $m$ ,  $n$  and  $p$ .

**Proof.** From the methods of [2], [4] and [6] with some minor modifications we may immediately deduce the estimate

$$\sum_{a=1}^{p-1} \chi(a) \exp\left(\frac{ma + n\bar{a}}{p}\right) \leq 2(m, n, p)^{1/2} p^{1/2}.$$

□

**Lemma 2.** Let  $p$  be an odd prime, and let  $\chi$  be any character mod  $p$ . Then for any integer  $m$ , we have the estimate

$$\left| \sum_{a=1}^{p-1} (-1)^{a+\bar{a}} \chi(a) \exp\left(\frac{ma}{p}\right) \right| \leq 3p^{1/2} \ln^2 p.$$

*Proof.* For any integer  $r$  with  $(r, p) = 1$ , from Lemma 1 and the trigonometric identities

$$(2.1) \quad \sum_{a=1}^p \exp\left(\frac{ma}{p}\right) = \begin{cases} p & \text{if } (p, m) = p, \\ 0 & \text{if } (p, m) = 1 \end{cases}$$

and

$$\sum_{a=1}^{p-1} (-1)^a \exp\left(\frac{-ra}{p}\right) = \frac{1 - \exp\left(\frac{-r}{p}\right)}{1 + \exp\left(\frac{-r}{p}\right)} = \frac{i \sin\left(\frac{\pi r}{p}\right)}{\cos\left(\frac{\pi r}{p}\right)},$$

we have

$$\begin{aligned} & \sum_{a=1}^{p-1} (-1)^{a+\bar{a}} \chi(a) \exp\left(\frac{ma}{p}\right) \\ &= \frac{1}{p^2} \sum_{\substack{a=1 \\ ab \equiv 1 \pmod{p}}}^{p-1} \sum_{b=1}^{p-1} \chi(a) \exp\left(\frac{ma}{p}\right) \\ & \quad \times \sum_{c=1}^{p-1} \sum_{d=1}^{p-1} (-1)^{c+d} \sum_{r=1}^p \exp\left(\frac{r(a-c)}{p}\right) \sum_{s=1}^p \exp\left(\frac{s(b-d)}{p}\right) \\ &= \frac{1}{p^2} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \left( \sum_{a=1}^{p-1} \chi(a) \exp\left(\frac{(r+m)a + s\bar{a}}{p}\right) \right) \\ & \quad \times \left( \sum_{c=1}^{p-1} (-1)^c \exp\left(\frac{-rc}{p}\right) \right) \left( \sum_{d=1}^{p-1} (-1)^d \exp\left(\frac{-sd}{p}\right) \right) \\ &\leq \frac{2\sqrt{p}}{p^2} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \frac{2}{\left| 1 + \exp\left(\frac{-r}{p}\right) \right|} \frac{2}{\left| 1 + \exp\left(\frac{-s}{p}\right) \right|} \\ &\leq \frac{2\sqrt{p}}{p^2} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \frac{1}{\left| \sin\left(\frac{\pi}{2} - \frac{r\pi}{p}\right) \right|} \frac{1}{\left| \sin\left(\frac{\pi}{2} - \frac{s\pi}{p}\right) \right|} \\ &\leq \frac{2\sqrt{p}}{p^2} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \frac{p}{|p-2r|} \frac{p}{|p-2s|} \leq 3p^{1/2} \ln^2 p. \end{aligned}$$

This proves Lemma 2. □

**Lemma 3.** *Let  $p$  be an odd prime, and let  $k \geq 3$  be any fixed integer. Then for any integer  $1 \leq i \leq k$ , we have the estimate*

$$\left| \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1 + \bar{a}_1} \dots (-1)^{a_i + \bar{a}_i} \right| = O(3^i p^{k/2} \ln^{2i} p).$$

*Proof.* From the properties of Gauss sums we have

$$\sum_{b=1}^{p-1} \chi(b) \exp\left(\frac{rb}{p}\right) = \bar{\chi}(r) \tau(\chi).$$

Note that  $|\tau(\chi)| = \sqrt{p}$ , if  $\chi$  is not a principal character mod  $p$ . From (2.1), Lemma 2 and the orthogonality of characters mod  $p$  we have

$$\begin{aligned} & \left| \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1 + \bar{a}_1} \dots (-1)^{a_i + \bar{a}_i} \right| \\ &= \left| \sum_{r=1}^p \sum_{\chi \pmod p} \sum_{a_1=1}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1 + \bar{a}_1} \dots (-1)^{a_i + \bar{a}_i} \chi(a_1 \dots a_k) \right. \\ & \quad \left. \times \exp\left(\frac{r(a_1 + a_2 + \dots + a_k)}{p}\right) \right| \frac{1}{p(p-1)} \\ &= \frac{1}{p(p-1)} \left| \sum_{r=1}^p \sum_{\chi \pmod p} \left( \sum_{a=1}^{p-1} (-1)^{a + \bar{a}} \chi(a) \exp\left(\frac{ra}{p}\right) \right)^i \left( \sum_{b=1}^{p-1} \chi(b) \exp\left(\frac{rb}{p}\right) \right)^{k-i} \right| \\ &= \frac{1}{p(p-1)} \left| \sum_{r=1}^p \sum_{\chi \pmod p} \bar{\chi}^{k-i}(r) \left( \sum_{a=1}^{p-1} (-1)^{a + \bar{a}} \chi(a) \exp\left(\frac{ra}{p}\right) \right)^i \tau^{k-i}(\chi) \right| \\ &\leq \frac{1}{p(p-1)} \sum_{r=1}^p \sum_{\chi \pmod p} 3^i p^{k/2} \ln^{2i} p = 3^i p^{k/2} \ln^{2i} p. \end{aligned}$$

This proves Lemma 3. □

**Lemma 4.** *Let  $p$  be an odd prime, and let  $k \geq 3$  be any fixed integer. Then we have the asymptotic formula*

$$\sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} 1 = \frac{(p-1)^{k-1}}{p} + O(p^{k/2-1}).$$

Proof. From (2.1) and the orthogonality of characters mod  $p$  we have

$$\begin{aligned}
 \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} 1 &= \frac{1}{p(p-1)} \sum_{r=1}^p \sum_{\chi \pmod p} \left( \sum_{a=1}^{p-1} \chi(a) \exp\left(\frac{ra}{p}\right) \right)^k \\
 &= \frac{(p-1)^k}{p(p-1)} + \frac{1}{p(p-1)} \sum_{r=1}^{p-1} \sum_{\chi \pmod p} \bar{\chi}^k(r) \tau^k(\chi) \\
 &= \frac{(p-1)^{k-1}}{p} + \frac{(-1)^k}{p} + \frac{1}{p} \sum_{\substack{\chi \pmod p \\ \chi^k = \chi_0}} \tau^k(\chi) = \frac{(p-1)^{k-1}}{p} + O(p^{k/2-1}),
 \end{aligned}$$

where  $\chi_0$  denotes the principal character mod  $p$ . This proves Lemma 4.  $\square$

### 3. PROOFS OF THE THEOREMS

In this section, we shall complete the proofs of our theorems.

Proof. First we prove Theorem 1. If  $k = 2$ , then from (1.1) and Lemma 2 with  $\chi = \chi_0$ , the principal character mod  $p$ , we have the asymptotic formula

$$\begin{aligned}
 (3.1) \quad N(2, p) &= \frac{1}{2} \sum_{a=1}^{p-1} (1 - (-1)^{a+\bar{a}}) = \frac{1}{2} (p-1) + O(p^{1/2} \ln^2 p) \\
 &= \frac{1}{2} p + O(p^{1/2} \ln^2 p).
 \end{aligned}$$

If  $k \geq 3$ , then from Lemma 2, the orthogonality of characters mod  $p$ , the definition of  $N(k, p)$  and the binomial expansion we have

$$\begin{aligned}
 (3.2) \quad N(k, p) &= \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p}}^{p-1} \dots \sum_{a_k=1}^{p-1} (1 - (-1)^{a_1+\bar{a}_1}) \dots (1 - (-1)^{a_k+\bar{a}_k}) \\
 &= \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p}}^{p-1} \dots \sum_{a_k=1}^{p-1} 1 - \frac{k}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1+\bar{a}_1} \\
 &\quad + \frac{k(k-1)}{2^{k+1}} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1+\bar{a}_1} (-1)^{a_2+\bar{a}_2} + \dots \\
 &\quad + \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \pmod p}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^k (-1)^{a_1+\bar{a}_1} (-1)^{a_2+\bar{a}_2} \dots (-1)^{a_k+\bar{a}_k}
 \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2^k} (p-1)^{k-1} - \frac{k}{2^k} (p-1)^{k-2} \left( \sum_{a=1}^{p-1} (-1)^{a+\bar{a}} \right) \\
&\quad + \frac{k(k-1)}{2^{k+1}} (p-1)^{k-3} \left( \sum_{a=1}^{p-1} (-1)^{a+\bar{a}} \right)^2 + \dots \\
&\quad + \frac{(-1)^k}{2^k} \frac{1}{p-1} \sum_{\chi \bmod p} \left( \sum_{a=1}^{p-1} (-1)^{a+\bar{a}} \chi(a) \right)^k \\
&= \frac{1}{2^k} (p-1)^{k-1} + O\left( \frac{p^{k-1}}{2^k} \sum_{i=1}^{k-1} \binom{k}{i} \left( \frac{3\sqrt{p} \ln^2 p}{p} \right)^i \right) + O\left( \frac{(3\sqrt{p} \ln^2 p)^k}{2^k} \right) \\
&= \frac{1}{2^k} p^{k-1} + O\left( p^{k-3/2} \left( \frac{1}{2} + \frac{3 \ln^2 p}{2\sqrt{p}} \right)^{k-1} \ln^2 p \right) + O\left( \frac{(3\sqrt{p} \ln^2 p)^k}{2^k} \right).
\end{aligned}$$

Combining (3.1) and (3.2) we may immediately deduce the asymptotic formula

$$N(k, p) = \begin{cases} \frac{1}{2} p + O(p^{1/2} \ln^2 p) & \text{if } k = 2, \\ \frac{1}{8} p^2 + O(p^{3/2} \ln^6 p) & \text{if } k = 3, \\ \frac{1}{2^k} p^{k-1} + O\left( p^{k-3/2} \left( \frac{1}{2} + \frac{3 \ln^2 p}{2\sqrt{p}} \right)^k \ln^2 p \right) + O\left( \frac{(3\sqrt{p} \ln^2 p)^k}{2^k} \right) & \text{if } k \geq 4. \end{cases}$$

This proves Theorem 1.  $\square$

**Proof.** Now we prove Theorem 2. For any integer  $k \geq 4$ , from the definition of  $M(k, p)$ , Lemma 4, Lemma 5 and the binomial expansion we have

$$\begin{aligned}
M(k, p) &= \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \bmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (1 - (-1)^{a_1 + \bar{a}_1}) \dots (1 - (-1)^{a_k + \bar{a}_k}) \\
&= \frac{1}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \bmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} 1 - \frac{k}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \bmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1 + \bar{a}_1} \\
&\quad + \frac{k(k-1)}{2^{k+1}} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \bmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1 + \bar{a}_1} (-1)^{a_2 + \bar{a}_2} + \dots \\
&\quad + \frac{(-1)^k}{2^k} \sum_{\substack{a_1=1 \\ a_1 a_2 \dots a_k \equiv 1 \bmod p \\ p \mid a_1 + a_2 + \dots + a_k}}^{p-1} \dots \sum_{a_k=1}^{p-1} (-1)^{a_1 + \bar{a}_1} (-1)^{a_2 + \bar{a}_2} \dots (-1)^{a_k + \bar{a}_k}
\end{aligned}$$

$$\begin{aligned}
&= \frac{(p-1)^{k-1}}{2^k p} + O\left(\frac{1}{2^k} \sum_{i=1}^k \binom{k}{i} 3^i p^{k/2} \ln^{2i} p\right) \\
&= \frac{(p-1)^{k-1}}{2^k p} + O(2^k p^{k/2} \ln^{2k} p).
\end{aligned}$$

This completes the proof of Theorem 2.  $\square$

**Acknowledgement.** The authors would like to thank the referee for his/her very helpful and detailed comments, which have significantly improved the presentation of this paper.

### References

- [1] *T. M. Apostol*: Introduction to Analytic Number Theory. Undergraduate Texts in Mathematics, Springer, New York, 1976. [zbl](#) [MR](#)
- [2] *S. Chowla*: On Kloosterman's sum. Norske Vid. Selsk. Forhdl. 40 (1967), 70–72. [zbl](#) [MR](#)
- [3] *R. K. Guy*: Unsolved Problems in Number Theory. Unsolved Problems in Intuitive Mathematics, I. Problem Books in Mathematics, Springer, New York, 1994. [zbl](#) [MR](#)
- [4] *A. V. Mal'šev*: A generalization of Kloosterman sums and their estimates. Vestnik Leningrad. Univ. 15 (1960), 59–75. [zbl](#) [MR](#)
- [5] *C. Pan, C. Pan*: Goldbach Conjecture. Science Press, Beijing, 1992. [zbl](#) [MR](#)
- [6] *A. Weil*: Sur les courbes algébriques et les variétés qui s'en déduisent. Actualités Sci. Ind. 1041, deuxième partie, § IV, Hermann et Cie., Paris, 1948 (In French.); Publ. Inst. Math. Univ. Strasbourg, 7 (1945). [zbl](#) [MR](#)
- [7] *W. Zhang*: A mean value related to D. H. Lehmer's problem and the Ramanujan's sum. Glasg. Math. J. 54 (2012), 155–162. [zbl](#) [MR](#)
- [8] *W. Zhang*: A problem of D. H. Lehmer and its mean square value formula. Japan J. Math., New Ser. 29 (2003), 109–116. [zbl](#) [MR](#)
- [9] *W. Zhang*: A problem of D. H. Lehmer and its generalization. II. Compos. Math. 91 (1994), 47–56. [zbl](#) [MR](#)
- [10] *W. Zhang*: On a problem of D. H. Lehmer and its generalization. Compos. Math. 86 (1993), 307–316. [zbl](#) [MR](#)

*Authors' address:* Han Zhang, Wenpeng Zhang, School of Mathematics, Northwest University, Xuefu Avenue No. 1, Chang'an, Xi'an, Shaanxi, 710127, P. R. China, e-mail: micohanzhang@gmail.com, wpzhang@nwu.edu.cn.