doi: 103969/j. issn. 0490-6756. 2019. 01. 001

广义 Lehmer 数的渐近行为

敖凌峰[1], 骆元媛[2], 谭千蓉[3]
(1. 四川大学数学学院, 成都 610064; 2. 西华大学理学院, 成都 610039;
3. 攀枝花学院数学与计算机学院, 攀枝花 617000)

摘 要: 整数 a 称为模 p 的 Lehmer 数是指 $1\leqslant a\leqslant p-1$ 且 $a+a^{-1}$ 为奇数,其中 a^{-1} 表示 a 模 p 的逆. 令 M_p 为模 p 的 Lehmer 数的个数. 1994 年,张证明了 $M_p=\frac{p-1}{2}+O(p^{\frac{1}{2}}\log^3 p)$. 设整数 $c\geqslant 2$,整数 $d\in[0,c-1]$. 对每个素数 $p\equiv 1(\mathrm{mod}\ c)$,如果 $a+a^{-1}\equiv d(\mathrm{mod}\ c)$,则称整数 a 为关于模 p 的 (c,d)-Lehmer 数. 令 $M_{c,d,p}$ 表示模 p 的 (c,d)-Lehmer 数的个数. 本文得到 $M_{c,d,p}=\frac{p-1}{c}+O(p^{\frac{1}{2}}\log^2 p)$,推广了张的结果.

关键词: 广义 Lehmer 数; Kloosterman 和; 渐近估计
中图分类号: O156.4 **文献标识码**: A **文章编号**: 0490-6756(2019)01-0001-04

Asymptotic behavior of the number of generalized Lehmer numbers

AO Ling-Feng[1], *LUO Yuan-Yuan*[2], *TAN Qian-Rong*[3]
(1. School of Mathematics, Sichuan University, Chengdu 610064, China;
2. School of Science, Xihua University, Chengdu 610039, China;
3. School of Mathematics and Computer Science, Panzhihua University, Panzhihua 617000, China)

Abstract: A Lehmer number modulo an odd prime p is an integer a with $1\leqslant a\leqslant p-1$ and $a+a^{-1}$ is odd. Let M_p denote the number of Lehmer number modulo p, Zhang has shown that $M_p=\frac{p-1}{2}+O(p^{\frac{1}{2}}\log^3 p)$ in 1994. Let $c\geqslant 2$ be an positive integer, $d\in[0,c-1]$ be an integer. For every $p\equiv 1\ (\mathrm{mod}\ c)$, a is called to be a (c,d)-Lehmer number modulo p, if $a+a^{-1}\equiv d\ (\mathrm{mod}\ c)$. Let $M_{c,d,p}$ denote the number of (c,d)-Lehmer number modulo p. In this paper, it is proved that $M_{c,d,p}=\frac{p-1}{c}+O(p^{\frac{1}{2}}\log^2 p)$. If $c=2,d=1$, the Zhang's formula is recovered.

Keywords: Generalized Lehmer number; Kloosterman sum; Asymptotic estimate
(2010 MSC 11R09, 11R04)

1 Introduction

Let p be an odd prime and a an integer with $1\leqslant a\leqslant p-1$. Define a^{-1} to be the integer with $1\leqslant a^{-1}\leqslant p-1$ such that $aa^{-1}\equiv 1\ (\mathrm{mod}\ p)$. We say a that is a Lehmer number[1-9] modulo p if $a+a^{-1}\equiv 1\ (\mathrm{mod}\ 2)$, i. e. $a+a^{-1}$ is odd. From this definition, we see that if a is a Lehmer number, then

收稿日期: 2018-04-18
基金项目: 国家自然科学基金(11771304); 中央高校基本科研业务费专项基金
作者简介: 敖凌峰(1992-), 男, 四川大竹人, 硕士研究生, 主要研究方向为数论. E-mail: 3182869731@qq.com
通讯作者: 骆元媛. E-mail: yuanyuanluoluo@163.com

a^{-1} will also be a Lehmer number. An easy calculation shows that there are no Lehmer numbers modulo p when $p=3$ or 7. Zhang[7] showed that M_p, the number of Lehmer numbers modulo p, satisfies that

$$M_p=\frac{p-1}{2}+O(p^{\frac{1}{2}}\log^3 p).$$

In this paper, we introduce the concept of generalized Lehmer number, i. e., the so-called (c,d)-Lehmer number. Let $c\geqslant 2$ and $d\in[0,c-1]$ be integers. From Dirichlet's theorem, we know there are infinitely many prime number p, such that $p\equiv 1 \pmod c$. We say a is a (c,d)-Lehmer number modulo p if $1\leqslant a\leqslant p-1$ and $a+a^{-1}\equiv d \pmod c$. We are interested in the asymptotic behavior of such number. Let $M_{c,d,p}$ denote the number of Lehmer number modulo p, Then we will show that

Theorem 1.1 Let $M_{c,d,p}$ be the number of (c,d)-Lehmer numbers in $[1,p-1]$. Then

$$M_{c,d,p}=\frac{p-1}{c}+O(p^{\frac{1}{2}}\log^2 p).$$

When $c=2,d=1$, it reduces to Zhang's formula.

2 Preliminary lemmas

In this section, we give some lemmas of the main result of this paper.

We give some notations at first, which will be used through the whole paper. In this paper, c will always denote a positive integer and $c\geqslant 2$, d is an integer satisfies $0\leqslant d\leqslant c-1$, p will denote a prime number satisfies $p\equiv 1 \pmod c$. From Lemma 2.1, we know such p are infinitely many. For positive integer a, $1\leqslant a\leqslant p-1$, a^{-1} denote a positive integer smaller than p, satisfies $aa^{-1}\equiv 1 \pmod p$. And for any positive integer n, let $\zeta_n=e^{\frac{2\pi i}{n}}$, i. e. ζ_n is a primitive n-th root of unity.

Let $R(x)$ be Riemann-ζ function's partial sum at $s=1$, i. e.,

$$R(x):=\sum_{n\leqslant x}\frac{1}{n}.$$

Let $K(j,k,p)$ denote the Kloosterman sum of variable j,k, i. e.,

$$K(j,k,p):=\sum_{a=1}^{p-1}\zeta_p^{ja+ka^{-1}}.$$

Lemma 2.1[2,4] Let k and l be integers such that $k\geqslant 2, 1\leqslant l<k$ and $\gcd(l,k)=1$. Let $A(k,l):=\{l+kt\mid t\geqslant 0\}=\{n>0: n\equiv l \pmod k\}$. Then $A(k,l)$ contains infinitely many prime numbers.

Lemma 2.2 Let a be a real number such that $0<a\leqslant 1$ and let $S_p(a):=\sum_{j=0}^{p}\frac{1}{a+j}$. Then

$$S_p(a)=O(\log p).$$

Proof We know that for the partial sum of Riemann zeta function $R(x)$, we have the following asymptotic function

$$R(x)=\sum_{n\leqslant x}\frac{1}{n}=\log x+C+O(\frac{1}{x}),$$

where $C=0.577\ldots$ is the Euler constant. Therefore

$$S_p(a)=\frac{1}{a}+\sum_{j=1}^{p}\frac{1}{a+j}<\frac{1}{a}+\sum_{j=1}^{p}\frac{1}{j}=$$
$$\frac{1}{a}+R(p)=\log p+C_2+O(\frac{1}{p}),$$

where C_2 is a constant depended only on a.

Lemma 2.3[5,9] We have

$$|K(j,k,p)|\leqslant 2p^{\frac{1}{2}}.$$

Lemma 2.4 Let $1\leqslant t\leqslant c-1$ and

$$T_p:=\sum_{i=0}^{p-1}\frac{1}{|\zeta_p^i-\zeta_c^t|}.$$

Then $T_p=O(p\log p)$.

Proof We see clearly that ζ_p^i and ζ_c^t are points on the unit circle. And their angles between the x-axis are $\frac{2\pi i}{p}$ and $\frac{2\pi t}{c}$. Let $2\theta=|\frac{2\pi i}{p}-\frac{2\pi t}{c}|$, so $\theta=|\frac{\pi i}{p}-\frac{\pi t}{c}|$. From the geometric meaning of $|\zeta_p^i-\zeta_c^t|$, it denotes the distance of the point ζ_p^i between the point ζ_c^t, so we have $|\zeta_p^i-\zeta_c^t|=2\sin\theta$. We should consider the situation that $0<\theta<\frac{\pi}{2}$ and $\frac{\pi}{2}<\theta<\pi$, so we will divide T_p into two parts. Therefore

$$T_p=\sum_{\substack{i=1,\\ |\frac{\pi i}{p}-\frac{\pi t}{c}|<\frac{\pi}{2}}}^{p-1}\frac{1}{2\sin|\frac{\pi i}{p}-\frac{\pi t}{c}|}+\sum_{\substack{i=1,\\ \frac{\pi}{2}<|\frac{\pi i}{p}-\frac{\pi t}{c}|<\pi}}^{p-1}\frac{1}{2\sin|\frac{\pi i}{p}-\frac{\pi t}{c}|}.$$

We will estimate them separately. First of all, we have the inequality $\frac{2}{\pi}\leqslant\frac{\sin x}{x}<1$ with $0<x\leqslant\frac{\pi}{2}$, and then we have $\frac{1}{\sin x}\leqslant\frac{\pi}{2x}$. Using the last inequality on the first sum, we have

$$\sum_{\substack{p-1\\ |\frac{\pi i}{p}-\frac{\pi t}{c}|<\frac{\pi}{2}}}\frac{1}{2\sin|\frac{\pi i}{p}-\frac{\pi t}{c}|}<\sum_{i=0}^{p-1}\frac{\pi}{4|\frac{\pi i}{p}-\frac{\pi t}{c}|}=\frac{1}{4}\sum_{i=0}^{p-1}\frac{1}{|\frac{i}{p}-\frac{t}{c}|}=\frac{p}{4}\sum_{i=0}^{p-1}\frac{1}{|i-\frac{pt}{c}|}.$$

Since $p\equiv 1 \pmod c$, so $p=mc+1$, where m is a positive integer, so $\frac{pt}{c}=mt+\frac{t}{c}$ and $p-2-mt>0$. Thus

$$\frac{p}{4}\sum_{i=0}^{p-1}\frac{1}{|i-\frac{pt}{c}|}=\frac{p}{4}\sum_{i=0}^{p-1}\frac{1}{|i-mt-\frac{t}{c}|}=\frac{p}{4}\Big(\sum_{i=mt+1}^{p-1}\frac{1}{i-mt-\frac{t}{c}}+\sum_{i=0}^{mt}\frac{1}{\frac{t}{c}+mt-i}\Big)=\frac{p}{4}\Big(\sum_{i=mt+1}^{p-1}\frac{1}{i-mt-\frac{t}{c}}+\sum_{i=0}^{mt}\frac{1}{\frac{t}{c}+i}\Big)=\frac{p}{4}\Big(\sum_{i=0}^{p-2-mt}\frac{1}{1+i-\frac{t}{c}}+\sum_{i=0}^{mt}\frac{1}{\frac{t}{c}+i}\Big)<\frac{p}{4}\Big(\sum_{i=0}^{p}\frac{1}{i+(1-\frac{t}{c})}+\sum_{i=0}^{p}\frac{1}{\frac{t}{c}+i}\Big).$$

By Lemma 2.2, we have

$$\sum_{i=0}^{p}\frac{1}{i+(1-\frac{t}{c})}+\sum_{i=0}^{p}\frac{1}{\frac{t}{c}+i}=O(\log p),$$

so the first sum is bounded by $p\log p$.

Similarly, one has

$$\sum_{\substack{i=0,\\ \frac{\pi}{2}<|\frac{\pi i}{p}-\frac{\pi t}{c}|<\pi}}^{p-1}\frac{1}{2\sin|\frac{\pi i}{p}-\frac{\pi t}{c}|}<\frac{1}{4}\sum_{i=0}^{p-1}\frac{\pi}{\pi-|\frac{\pi i}{p}-\frac{\pi t}{c}|}=\frac{p}{4}\sum_{i=0}^{p-1}\frac{1}{p-|i-\frac{pt}{c}|}=\frac{p}{4}\Big(\sum_{i=0}^{p-1}\frac{1}{p-|i-mt-\frac{t}{c}|}<\frac{p}{4}\Big(\sum_{i=0}^{p}\frac{1}{i+(1-\frac{t}{c})}+\sum_{i=0}^{p}\frac{1}{\frac{t}{c}+i}\Big)=O(p\log p).$$

This finishes the proof of Lemma 2.4.

3　Proofs of Theorem 1.1

In this section, we prove Theorem 1.1. First of all, from the definition of (c,d)-Lehmer number, we can easily check that

$$cM_{c,d,p}=\sum_{a=1}^{p-1}\sum_{t=0}^{c-1}\zeta_c^{t(a+a^{-1}-d)} \tag{1}$$

From (1), we have

$$M_{c,d,p}=\frac{1}{c}\sum_{a=1}^{p-1}\sum_{t=0}^{c-1}\zeta_c^{t(a+a^{-1}-d)}=\frac{p-1}{c}+\frac{1}{c}\sum_{a=1}^{p-1}\sum_{t=1}^{c-1}\zeta_c^{t(a+a^{-1}-d)}.$$

Let

$$E=\frac{1}{c}\sum_{a=1}^{p-1}\sum_{t=1}^{c-1}\zeta_c^{t(a+a^{-1}-d)} \tag{2}$$

Now we will mainly estimate (2), for every $1\leqslant t\leqslant c-1$, we have

$$\zeta_c^{ta}=\frac{1}{p}\sum_{r=0}^{p-1}\sum_{i=0}^{p-1}\zeta_c^{tr}\zeta_p^{i(a-r)}.$$

Similarly, one has

$$\zeta_c^{ta^{-1}}=\frac{1}{p}\sum_{s=0}^{p-1}\sum_{j=0}^{p-1}\zeta_c^{ts}\zeta_p^{j(a^{-1}-r)}.$$

For any $1\leqslant t\leqslant c-1$, let

$$E_t=\sum_{a=1}^{p-1}\zeta_c^{t(a+a^{-1}-d)}.$$

Then we have

$$E_t=\zeta_c^{-td}\sum_{a=1}^{p-1}\zeta_c^{ta}\zeta_c^{ta^{-1}}=\zeta_c^{-td}\sum_{a=1}^{p-1}\frac{1}{p^2}\Big(\sum_{r=0}^{p-1}\sum_{i=0}^{p-1}\zeta_c^{tr}\zeta_p^{i(a-r)}\Big)\cdot\Big(\sum_{s=0}^{p-1}\sum_{j=0}^{p-1}\zeta_c^{ts}\zeta_p^{j(a^{-1}-s)}\Big)=\frac{\zeta_c^{-td}}{p^2}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\Big(\sum_{a=1}^{p-1}\zeta_p^{ia+ja^{-1}}\Big)\cdot\Big(\sum_{r=0}^{p-1}\zeta_c^{tr}\zeta_p^{-ir}\Big)\Big(\sum_{s=0}^{p-1}\zeta_c^{ts}\zeta_p^{-js}\Big).$$

Now $\sum_{a=1}^{p-1}\zeta_p^{ia+ja^{-1}}$ is a Kloosterman sum. From Lemma 2.3, for every i,j we have

$$|K(i,j,p)|=|\sum_{a=1}^{p-1}\zeta_p^{ia+ja^{-1}}|\leqslant 2p^{\frac{1}{2}} \tag{3}$$

Let $S_{i,t}=\sum_{r=0}^{p-1}\zeta_c^{tr}\zeta_p^{-ir}$. Then we have

$$\zeta_p^{-i}\zeta_c^{t}S_{i,t}=\sum_{r=0}^{p-1}\zeta_c^{t(r+1)}\zeta_p^{-i(r+1)}=S_{i,t}-1+\zeta_c^{t}.$$

The last identity used $\zeta_c^p=\zeta_c$, since $p\equiv 1 \pmod c$. An easy calculation shows that

$$S_{i,t}=\frac{\zeta_c^t-1}{\zeta_p^{-i}\zeta_c^t-1}=\frac{\zeta_c^t-1}{\zeta_c^t-\zeta_p^i}\zeta_p^i.$$

Similarly, we have

$$S_{j,t}=\sum_{s=0}^{p-1}\zeta_c^{ts}\zeta_p^{-js}=\frac{\zeta_c^t-1}{\zeta_c^t-\zeta_p^j}\zeta_p^j.$$

By triangle inequality and easy calculations, we have

$$|\sum_{i=0}^{p-1}S_{i,t}|\leqslant\sum_{i=0}^{p-1}|S_{i,t}|\leqslant\sum_{i=0}^{p-1}|\frac{\zeta_c^t-1}{\zeta_c^t-\zeta_p^i}|\leqslant$$

$$\sum_{i=0}^{p-1}\left|\frac{\zeta_c^t}{\zeta_c^t-\zeta_p^i}\right|+\sum_{i=0}^{p-1}\left|\frac{1}{\zeta_c^t-\zeta_p^i}\right|=2\sum_{i=0}^{p-1}\left|\frac{1}{\zeta_c^t-\zeta_p^i}\right|.$$

It follows from Lemma 2.4 that

$$\left|\sum_{i=0}^{p-1}S_{i,t}\right|=O(p\log p) \tag{4}$$

Similarly,

$$\left|\sum_{j=0}^{p-1}S_{j,t}\right|=O(p\log p) \tag{5}$$

So by (3),(5), we have

$$\begin{aligned}|E_t|&=\left|\frac{\zeta_c^{-td}}{p^2}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\left(\sum_{a=1}^{p-1}\zeta_p^{ia+ja^{-1}}\right)\cdot\left(\sum_{r=0}^{p-1}\zeta_c^{tr}\zeta_p^{-ir}\right)\left(\sum_{s=0}^{p-1}\zeta_c^{ts}\zeta_p^{-js}\right)\right|\leqslant\\&\frac{2p^{\frac{1}{2}}}{p^2}\left|\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}S_{i,t}S_{j,t}\right|=\\&\frac{2p^{\frac{1}{2}}}{p^2}\left|\left(\sum_{i=0}^{p-1}S_{i,t}\right)\left(\sum_{j=0}^{p-1}S_{j,t}\right)\right|\leqslant\\&\frac{2p^{\frac{1}{2}}}{p^2}C_1p\log p\cdot C_2p\log p\\&=O(p^{\frac{1}{2}}\log^2 p).\end{aligned}$$

But $E=\sum_{t=1}^{c-1}E_t$, so $E=O(p^{\frac{1}{2}}\log^2 p)$. This finishes the proof of Theorem 1.1.

References:

[1] Ahlfors L. Complex analysis [M]. New York: McGraw-Hill, 1966.

[2] Apostol T M. Introduction to analytic number theory. New York: Springer-Verlag, 1976.

[3] Cohen S D. Trudgian T. Lehmer numbers and primitive roots modulo a prime [J]. arXiv: 1712.03990.

[4] Ireland K, Rosen M. A classic introduction to modern number theory [M]. New York/Berlin: Springer-Verlag, 1990.

[5] Iwaniec H, Kowalski E. Analytic number theory [M]. Providence: American Mathematical Society, 2004.

[6] Ruy R K. Unsolved problems in number theory [M]. New York: Springer-Verlag, 2004.

[7] Zhang W P. A problem of D. H. Lehmer and its generalization [J]. Compos Math, 1994, 91: 47.

[8] Wang T T, Wang X N. On the Golomb's conjecture and Lehmer's numbers [J]. Open Math, 2017, 15: 1003.

[9] Weil A. On some exponential sums [J]. Proc Nat Acad Sci, 1948, 34: 204.

引用本文格式:

中 文: 敖凌峰, 骆元媛, 谭千蓉. 广义 Lehmer 数的渐近行为 [J]. 四川大学学报: 自然科学版, 2019, 56: 1.

英 文: Ao L F, Luo Y Y, Tan Q R. Asymptotic behavior of the number of generalized Lehmer numbers [J]. J Sichuan Univ: Nat Sci Ed, 2019, 56: 1.