Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 32(3): 1864–1872.
DOI: 10.3934/era.2024085
Received: 25 September 2023
Revised: 26 January 2024
Accepted: 29 January 2024
Published: 01 March 2024

Research article

On an exponential D. H. Lehmer problem

Zhefeng Xu, Jiankang Wang*and Lirong Zhu

Research Center for Number Theory and Its Applications, Northwest University, Xi'an, 710127, China

* **Correspondence:** Email: wangjiankang@stumail.nwu.edu.cn.

Abstract: For an odd prime p and a positive integer α, let g be of multiplicative order τ modulo q and $q = p^\alpha$. Denote by $N(h, g, q)$ the number of a such that $h \nmid (a + (g^a)_q)$ for any $1 \le a \le \tau$ and a fixed integer $h \ge 2$ with $(h, q) = 1$. The main purpose of this paper is to give a sharp asymptotic formula for

$$N(k, h, g, q) = \sum_{\substack{a=1 \\ h\nmid(a+(g^a)_q)}}^{\tau} \left|a - (g^a)_q\right|^{2k}$$

where k is any nonnegative integer and $(a)_q$ denotes the smallest positive residue of a modulo q. In addition, we know that $N(h, g, q) = N(0, h, g, q)$.

Keywords: primitive roots; exponential Lehmer problem; exponential functions; asymptotic formula

1. Introduction

Let p be an odd prime. For each $a = 1, \ldots, p-1$, there is a unique $\bar{a} \in \{1, \ldots, p-1\}$ such that $a\bar{a} \equiv 1 \pmod{p}$. If $a \in \{1, \ldots, p-1\}$ and $\bar{a}$ (the inverse of a modulo p) are of opposite parity, then we call a a Lehmer number. D. H. Lehmer asked for something nontrivial about

$$L(p) = \#\{1 \le a \le p-1 : \ 2 \nmid a + \bar{a}\}$$

(the total number of Lehmer numbers among $1, \ldots, p-1$) (see Problem F12 of [1]), this is called the D. H. Lehmer problem. Zhang [2, 3] obtained an asymptotic estimate of $L(p)$:

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

For an odd integer q, Zhang [4] gave the following result

$$\sum_{\substack{a=1\\2|(a+\bar{a}+1)}}^{q}{}' (a-\bar{a})^{2k} = \frac{\phi(q)q^{2k}}{(2k+1)(2k+2)} + O(4^k q^{2k+\frac{1}{2}} d^2(q)\ln^2 q),$$

where $\sum_{a=1}^{q}{}'$ denotes the summation over all a such that $(a,q)=1$ and $1\le a\le q$, $d(q)$ is the divisor function. For any nonnegative integer k and any real numbers x, y with $0<x,y\le 1$, let

$$F_q(x,y,k) = \sum_{\substack{b=1\\bc\equiv 1 \pmod q\\2\nmid(b+c)}}^{xq}{}' \sum_{c=1}^{yq}{}' (b-c)^{2k}.$$

Zhang also proved

$$F_q(x,y,0) = \frac{1}{2}xy\phi(q) + O(q^{\frac{1}{2}} d^2(q)\ln^2 q).$$

Recently, Niu, Ma, and Wang [5] gave a sharp asymptotic formula for $F_q(1,y,k)$ by using estimates of Kloosterman sums and properties of trigonometric sums.

Let $q\ge 3$ be an integer, and d and $n\ge 2$ be fixed integers with $(n,q)=(d,q)=1$. For $0<\lambda_1,\lambda_2\le 1$, Lu and Yi [6] obtained

$$\sum_{\substack{b=1\\bc\equiv d \pmod q\\n\nmid(b+c)}}^{[\lambda_1 q]}{}' \sum_{c=1}^{[\lambda_2 q]}{}' 1 = \left(1-\frac{1}{n}\right)\lambda_1\lambda_2\phi(q) + O(q^{\frac{1}{2}} d^6(q)\ln^2 q).$$

Han and Xu et al. [7, 8] studied the high-dimensional D. H. Lehmer problem over incomplete intervals by using the properties of trigonometric sums and the estimates of n-dimensional Kloosterman sums.

Let $\mathcal{A}\subset\mathbb{Z}_p$ be the set of the primitive roots modulo p. For a fixed integer $k\ge 0$ and any real number $0<\sigma\le 1$, Zhang [9] considered the distribution of primitive roots by studying

$$M(p,k,\sigma) = \sum_{a\in\mathcal{A},|a-\bar{a}|<\sigma p} |a-\bar{a}|^k.$$

Cobeli and Zaharescu et al. [10, 11] conducted an in-depth discussion on the distribution of the power of primitive roots. Shparlinski [12] studied the distribution of powers u^n in the residue ring modulo a large power of a fixed prime for a fixed integer $u\ge 2$.

Let $q=p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For a fixed integer $h\ge 2$ with $(h,q)=1$, we define $N(h,g,q)$ as the number of $a\in\mathbb{Z}_\tau$ such that $h\nmid(a+(g^a)_q)$, where $\mathbb{Z}_\tau=\{1,\dots,\tau\}$. If $h=2$ and g is a primitive root modulo p, then we have

p	5	7	11	13	17	19	23	29	31	37	41	43	47
g	2	3	2	2	3	2	5	2	3	2	6	3	5
$N(2,g,p)$	2	2	7	6	8	12	8	14	12	18	20	24	18

E.g., for $p=11$ and a primitive root 2 modulo 11, $(a,(3^a)_{11}) = (1,2), (3,8), (4,5), (5,10), (6,9), (8,3)$, and $(6,1)$ are of opposite parity. For $p=13$ and a primitive root 2 modulo 13, $(a,(2^a)_{13}) = (1,2)$, $(3,8)$, $(4,3)$, $(5,6)$, $(8,9)$, and $(12,1)$ are of opposite parity.

In combination with the D. H. Lehmer problem, we propose to find $N(h, g, q)$, or at least to say something nontrivial about it, the problem of finding $N(h, g, q)$ being what we call the exponential D. H. Lehmer problem. The main purpose of this paper is to give an asymptotic formula for

$$N(k, h, g, q) = \sum_{\substack{a=1 \\ h\nmid(a+(g^a)_q)}}^{\tau} \left|a - (g^a)_q\right|^{2k},$$

where k is any nonnegative integer and $(a)_q$ denotes the smallest positive residue of a modulo q. If $k = 0$ then we have $N(0, h, g, q) = N(h, g, q)$. We get the following results:

Theorem 1. Let $q = p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For any nonnegative integer k and a fixed integer $h \geq 2$ with $(h, q) = 1$, we obtain the following asymptotic formula:

$$N(k, h, g, q) = \left(1 - \frac{1}{h}\right)\left(1 + \left(\frac{\tau}{q}\right)^{2k+2} - \left(1 - \frac{\tau}{q}\right)^{2k+2}\right)\frac{q^{2k+1}}{(2k+2)(2k+1)} + O\left(4^k q^{2k+\frac{1}{2}} d(q) \ln^2 q\right).$$

Taking $h = 2$ in Theorem 1, we see that a and $(g^a)_q$ are of opposite parity for any $a \in \mathbb{Z}_\tau$. Then, we have the following result:

Corollary 1. Let $q = p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For any nonnegative integer k, we have

$$N(k, 2, g, q) = \frac{q^{2k+1}}{2(2k+2)(2k+1)}\left(1 + \left(\frac{\tau}{q}\right)^{2k+2} - \left(1 - \frac{\tau}{q}\right)^{2k+2}\right) + O\left(4^k q^{2k+\frac{1}{2}} d(q) \ln^2 q\right).$$

Taking $k = 0$ in Theorem 1, we can get the following asymptotic formula for $N(h, g, q)$:

Corollary 2. Let $q = p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For a fixed integer $h \geq 2$ with $(h, q) = 1$, we obtain

$$N(h, g, q) = \left(1 - \frac{1}{h}\right)\tau + O\left(q^{\frac{1}{2}} d(q) \ln^2 q\right).$$

If g is of multiplicative order $\frac{\phi(p^\alpha)}{2}$ modulo p^α, then we see that the range of the exponential function g^a with $a \in \mathbb{Z}_{\frac{\phi(p^\alpha)}{2}}$ is the set of quadratic residues modulo p^α. Theorem 1 gives the distribution behaviour of $\left|a - (g^a)_{p^\alpha}\right|$ with $h \nmid (a + (g^a)_{p^\alpha})$, and helps us to study the distribution of $(g^a)_{p^\alpha}$.

If $g = g_0$ is a primitive root modulo p^α, then we have that the exponential function g_0^a with $a \in \mathbb{Z}_{\phi(p^\alpha)}$ maps a complete residue system modulo $\phi(p^\alpha)$ to a reduced residue system modulo p^α, this exponential function rearranges the reduced residue system modulo p^α. It is also interesting to study the distribution of $(g_0^a)_{p^\alpha}$.

Corollary 3. Let g_0 be a primitive root modulo an odd prime p. For any nonnegative integer k, we have

$$N(k, 2, g_0, p) = \frac{p^{2k+1}}{(2k+2)(2k+1)} + O\left(4^k p^{2k+\frac{1}{2}} \ln^2 p\right).$$

Theorem 2. Let $q = p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For any nonnegative integer k, we have

$$\sum_{a=1}^{\tau} \left|a - (g^a)_q\right|^{2k} = \left(1 + \left(\frac{\tau}{q}\right)^{2k+2} - \left(1 - \frac{\tau}{q}\right)^{2k+2}\right) \frac{q^{2k+1}}{(2k+2)(2k+1)} + O\left(4^k q^{2k+\frac{1}{2}} d(q) \ln^2 q\right).$$

We see that the asymptotic formulas of Theorems 1 and 2 and corollaries are nontrivial provided that $\tau \gg 4^k q^{\frac{1}{2}} d(q) \ln^2 q$.

2. Some Lemmas

To prove Theorems 1 and 2, we need the following lemmas:

Lemma 1. Let q and l be integers with $q > 2$ and $l \geq 0$. Let r and s be integers with $1 \leq s \leq q$ and $1 \leq r \leq h$. For any given integer $h \geq 2$, we have

$$\sum_{a=1}^{q} a^l e\left(a\frac{-rq+sh}{hq}\right) = \begin{cases} \frac{q^{l+1}}{l+1} + O\left(q^l\right), & \text{if } hq \mid (-rq+sh), \\ O\left(\frac{q^l}{\left|\sin\frac{\pi(-rq+sh)}{hq}\right|}\right), & \text{if } hq \nmid (-rq+sh). \end{cases}$$

Proof. See [7].

Lemma 2. Let p be an odd prime and a positive integer α, and let g be of multiplicative order τ modulo p^α. For any integers a and b, we have the following estimate:

$$\left|\sum_{x=1}^{\tau} e\left(\frac{bx}{\tau} + \frac{ag^x}{p^\alpha}\right)\right| \leq (a, p^\alpha)^{\frac{1}{2}} p^{\frac{\alpha}{2}}.$$

Proof. Letting χ_k denote the k-th order Dirichlet character modulo p^α with $k = \frac{\phi(p^\alpha)}{\tau}$, we know that

$$\sum_{s=0}^{k-1} \chi_k^s(c) = \begin{cases} k, & c \text{ is a } k\text{-th residue modulo } p^\alpha; \\ 0, & \text{otherwise.} \end{cases}$$

We can write $g \equiv g_0^k \pmod{p^\alpha}$ for a primitive root g_0 modulo p^α. Thus, we have that $\mathcal{K} = \left\{(g^x)_{p^\alpha} \mid x \in \mathbb{Z}_\tau\right\}$ is the set of k-th residues modulo p^α. For a Dirichlet character χ modulo p^α, we have

$$\frac{1}{k}\sum_{s=0}^{k-1}\sum_{c=1}^{p^\alpha-1} \chi\chi_k^s(c) e\left(\frac{ac}{p^\alpha}\right) = \sum_{\substack{c=1 \\ c\in\mathcal{K}}}^{p^\alpha-1} \chi(c) e\left(\frac{ac}{p^\alpha}\right) = \sum_{x=1}^{\tau} \chi(g^x) e\left(\frac{ag^x}{p^\alpha}\right),$$

and there exists a Dirichlet character χ_b modulo p^α satisfying

$$\sum_{x=1}^{\tau} e\left(\frac{bx}{\tau} + \frac{ag^x}{p^\alpha}\right) = \sum_{x=1}^{\tau} \chi_b(g^x) e\left(\frac{ag^x}{p^\alpha}\right).$$

Since $\left|\sum_{c=1}^{p^\alpha-1}\chi(c)e\left(\frac{ac}{p^\alpha}\right)\right| \le (a,p^\alpha)^{\frac{1}{2}}p^{\frac{\alpha}{2}}$, we have

$$\left|\sum_{x=1}^{\tau} e\left(\frac{bx}{\tau}+\frac{ag^x}{p^\alpha}\right)\right| \le \frac{1}{k}\sum_{s=0}^{k-1}\left|\sum_{c=1}^{p^\alpha-1}\chi_b\chi_k^s(c)e\left(\frac{ac}{p^\alpha}\right)\right| \le (a,p^\alpha)^{\frac{1}{2}}p^{\frac{\alpha}{2}}.$$

This proves Lemma 2.

Lemma 3. Let $q = p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For any nonnegative integers s and j, we have

$$\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} a^s b^j = \frac{\tau^{s+1}p^j}{(s+1)(j+1)} + O\left(\tau^s p^{j+\frac{1}{2}}d(q)\ln^2 q\right).$$

Proof. From the orthogonality of trigonometric sums,

$$\sum_{r=1}^{q} e\left(\frac{mr}{q}\right) = \begin{cases} q, & q \mid m,\\ 0, & q \nmid m.\end{cases}$$

It is clear that

$$\begin{aligned}
&\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} a^s b^j\\
&= \frac{1}{q\tau}\sum_{m=1}^{\tau}\sum_{n=1}^{q}\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} e\left(\frac{ma}{\tau}+\frac{nb}{q}\right)\sum_{c=1}^{\tau}c^s e\left(\frac{-mc}{\tau}\right)\sum_{d=1}^{q}d^j e\left(\frac{-nd}{q}\right)\\
&= \frac{1}{q\tau}\left(\sum_{a=1}^{\tau}1\right)\left(\sum_{c=1}^{\tau}c^s\sum_{d=1}^{q}d^j\right) + \frac{1}{q\tau}\sum_{m=1}^{\tau-1}\left(\sum_{a=1}^{\tau}e\left(\frac{ma}{\tau}\right)\right)\left(\sum_{c=1}^{\tau}c^s e\left(\frac{-mc}{\tau}\right)\sum_{d=1}^{q}d^j\right)\\
&\quad + \frac{1}{q\tau}\sum_{n=1}^{q-1}\left(\sum_{a=1}^{\tau}e\left(\frac{ng^a}{q}\right)\right)\left(\sum_{c=1}^{\tau}c^s\sum_{d=1}^{q}d^j e\left(\frac{-nd}{q}\right)\right)\\
&\quad + \frac{1}{q\tau}\sum_{m=1}^{\tau-1}\sum_{n=1}^{q-1}\left(\sum_{a=1}^{\tau}e\left(\frac{ma}{\tau}+\frac{ng^a}{q}\right)\right)\left(\sum_{c=1}^{\tau}c^s e\left(\frac{-mc}{\tau}\right)\sum_{d=1}^{q}d^j e\left(\frac{-nd}{q}\right)\right)\\
&= R_1 + R_2 + R_3 + R_4.
\end{aligned}$$

Now, we calculate each term in the above formula one by one. According to Lemma 1, we can get

$$\begin{aligned}
R_1 &= \frac{1}{q\tau}\left(\sum_{a=1}^{\tau}1\right)\left(\sum_{c=1}^{\tau}c^s\sum_{d=1}^{q}d^j\right) = \frac{1}{q}\left(\frac{\tau^{s+1}}{s+1}+O(\tau^s)\right)\left(\frac{q^{j+1}}{j+1}+O(q^j)\right)\\
&= \frac{\tau^{s+1}q^j}{(s+1)(j+1)} + O\left(\tau^s q^j\right),
\end{aligned}$$

and

$$R_2 = \frac{1}{q\tau}\sum_{m=1}^{\tau-1}\left(\sum_{a=1}^{\tau}e\left(\frac{ma}{\tau}\right)\right)\left(\sum_{c=1}^{\tau}c^s e\left(\frac{-mc}{\tau}\right)\sum_{d=1}^{q}d^j\right) = 0.$$

Similarly, from Lemma 1 and Lemma 2 we have

$$\begin{aligned} R_3 &= \frac{1}{q\tau}\sum_{n=1}^{q-1}\left(\sum_{a=1}^{\tau} e\left(\frac{ng^a}{q}\right)\right)\left(\sum_{c=1}^{\tau} c^s \sum_{d=1}^{q} d^j e\left(\frac{-nd}{q}\right)\right) \\ &\ll q^{-\frac{1}{2}}\tau^s q^j \sum_{n=1}^{q-1}\frac{(n,q)^{\frac{1}{2}}}{|\sin\frac{\pi n}{q}|} \ll \tau^s q^{j+\frac{1}{2}} \sum_{n=1}^{q-1}\frac{(n,q)^{\frac{1}{2}}}{n} \\ &\ll \tau^s q^{j+\frac{1}{2}} \sum_{d|q} d^{-\frac{1}{2}} \sum_{t=1}^{\frac{q-1}{d}} \frac{1}{t} \\ &\ll \tau^s q^{j+\frac{1}{2}} d(q)\ln q, \end{aligned}$$

where we used the Jordan inequality

$$\frac{2}{\pi} \le \frac{\sin x}{x}, \qquad |x| \le \frac{\pi}{2}.$$

Next, we estimate R_4 according to Lemma 1 and Lemma 2, and we see that

$$\begin{aligned} R_4 &= \frac{1}{q\tau}\sum_{m=1}^{\tau-1}\sum_{n=1}^{q-1}\left(\sum_{a=1}^{\tau} e\left(\frac{ma}{\tau}+\frac{ng^a}{q}\right)\right)\left(\sum_{c=1}^{\tau} c^s e\left(\frac{-mc}{\tau}\right)\sum_{d=1}^{q} d^j e\left(\frac{-nd}{q}\right)\right) \\ &\ll \frac{\tau^s q^j}{q\tau}\sum_{m=1}^{\tau-1}\sum_{n=1}^{q-1}\left|\sum_{a=1}^{\tau} e\left(\frac{ma}{\tau}+\frac{ng^a}{q}\right)\right| \frac{1}{|\sin\frac{\pi m}{\tau}|}\frac{1}{|\sin\frac{\pi n}{q}|} \\ &\ll \frac{\tau^s q^{j+\frac{1}{2}}}{q\tau}\sum_{m=1}^{\tau-1}\frac{1}{|\sin\frac{\pi m}{\tau}|}\sum_{n=1}^{q-1}\frac{(n,q)^{\frac{1}{2}}}{|\sin\frac{\pi n}{q}|} \\ &\ll \tau^s p^{j+\frac{1}{2}} d(q)\ln^2 q. \end{aligned}$$

Finally, combining the relevant conclusions of R_1, R_2, R_3, and R_4, we immediately get

$$\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} a^s b^j = \frac{\tau^{s+1}q^j}{(s+1)(j+1)} + O\left(\tau^s q^{j+\frac{1}{2}} d(q)\ln^2 q\right).$$

This proves Lemma 3.

Lemma 4. Let $q = p^\alpha$ with an odd prime p and a positive integer α, and let g be of multiplicative order τ modulo q. For any nonnegative integers s, j, and a fixed integer $h \ge 2$ with $(h, q) = 1$, we have

$$\sum_{\substack{a=1\\ b\equiv g^a \pmod q\\ h\nmid(a+b)}}^{\tau}\sum_{b=1}^{q} a^s b^j = \left(1-\frac{1}{h}\right)\frac{\tau^{s+1}q^j}{(s+1)(j+1)} + O\left(\tau^s q^{j+\frac{1}{2}} d(q)\ln^2 q\right).$$

Proof. It is clear that

$$\sum_{\substack{a=1\\ b\equiv g^a \pmod q\\ h\nmid(a+b)}}^{\tau}\sum_{b=1}^{q} a^s b^j = \sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} a^s b^j - \sum_{\substack{a=1\\ b\equiv g^a \pmod q\\ h\mid(a+b)}}^{\tau}\sum_{b=1}^{q} a^s b^j,$$

and

$$\sum_{\substack{a=1\\ b\equiv g^a \pmod q\\ h\mid(a+b)}}^{\tau}\sum_{b=1}^{q} a^s b^j = \frac{1}{h}\sum_{l=1}^{h}\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} a^s b^j e\left(\frac{(a+b)l}{h}\right)$$

$$=\frac{1}{hq\tau}\sum_{l=1}^{h}\sum_{m=1}^{\tau}\sum_{n=1}^{q}\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} e\left(\frac{ma}{\tau}+\frac{nb}{q}\right)\sum_{c=1}^{\tau} c^s e\left(\frac{-mc}{\tau}+\frac{lc}{h}\right)\sum_{d=1}^{q} d^j e\left(\frac{-nd}{q}+\frac{ld}{h}\right)$$

$$=\frac{1}{h}\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} a^s b^j$$

$$+\frac{1}{hq\tau}\sum_{l=1}^{h-1}\sum_{m=1}^{\tau}\sum_{n=1}^{q}\sum_{\substack{a=1\\ b\equiv g^a \pmod q}}^{\tau}\sum_{b=1}^{q} e\left(\frac{ma}{\tau}+\frac{nb}{q}\right)\sum_{c=1}^{\tau} c^s e\left(c\frac{-mh+l\tau}{h\tau}\right)\sum_{d=1}^{q} d^j e\left(d\frac{-nh+lq}{hq}\right)$$

$$=\Sigma_1+\Sigma_2.$$

For $1\le l\le h-1$ and $1\le m\le \tau$, we know that there are $(h,\tau)-1$ pairs of m,l such that $h\tau \mid (-mh+l\tau)$. By the properties of complete residue systems, Lemma 1, and the proof method of Lemma 3, we have

$$\Sigma_2 \ll \frac{\tau^{s+1}q^{j+\frac{1}{2}}}{hq\tau}\sum_{\substack{l=1\\ h\tau\mid(-mh+l\tau)}}^{h-1}\sum_{m=1}^{\tau}\sum_{n=1}^{q-1}\frac{(n,q)^{\frac{1}{2}}}{|\sin\frac{\pi(-nh+lq)}{hq}|}$$

$$+\frac{\tau^s q^{j+\frac{1}{2}}}{hq\tau}\sum_{\substack{l=1\\ h\tau\nmid(-mh+l\tau)}}^{h-1}\sum_{m=1}^{\tau}\sum_{n=1}^{q-1}\frac{1}{|\sin\frac{\pi(-mh+l\tau)}{h\tau}|}\frac{(n,q)^{\frac{1}{2}}}{|\sin\frac{\pi(-nh+lq)}{hq}|}+\frac{\tau^s q^j}{hq\tau}\tau\sum_{l=1}^{h-1}\frac{1}{|\sin\frac{\pi l}{h}|}\frac{1}{|\sin\frac{\pi l}{h}|}$$

$$\ll (h,\tau)\tau^s q^{j+\frac{1}{2}}d(q)\ln^2 q \ll \tau^s q^{j+\frac{1}{2}}d(q)\ln^2 q.$$

From Lemma 3, we also have the upper bound estimate of Σ_1. Thus, we can get Lemma 4.

3. Proofs of the Theorems

In this section, we will complete the proofs of Theorems 1 and 2. First, we can write

$$N(k,h,g,q)=\sum_{\substack{a=1\\ h\nmid(a+(g^a)_q)}}^{\tau}\left|a-(g^a)_q\right|^{2k}=\sum_{\substack{a=1\\ b\equiv g^a \pmod q\\ h\nmid(a+b)}}^{\tau}\sum_{b=1}^{q}|a-b|^{2k}$$

$$=\sum_{s=0}^{2k}\binom{2k}{s}(-1)^{2k-s}\sum_{\substack{a=1\\ b\equiv g^a \pmod q\\ h\nmid(a+b)}}^{\tau}\sum_{b=1}^{q} a^s b^{2k-s}$$

$$=\left(1-\frac{1}{h}\right)\sum_{s=0}^{2k}\binom{2k}{s}(-1)^{2k-s}\left\{\frac{\tau^{s+1}q^{2k-s}}{(s+1)(2k-s+1)}+O\left(\tau^s p^{2k-s+\frac{1}{2}}d(q)\ln^2 q\right)\right\},$$

we also have

$$\begin{aligned}
&\sum_{s=0}^{2k}\binom{2k}{s}(-1)^{2k-s}\frac{\tau^s q^{-s}}{(2k-s+1)(s+1)}\\
&=\sum_{s=0}^{2k}\binom{2k}{s}\left(-\frac{\tau}{q}\right)^s\frac{1}{(2k-s+1)(s+1)}\\
&=\frac{1}{(2k+2)(2k+1)}\sum_{s=0}^{2k}\binom{2k+2}{s+1}\left(-\frac{\tau}{q}\right)^s\\
&=\frac{-q}{(2k+2)(2k+1)\tau}\left(\sum_{s=0}^{2k+2}\binom{2k+2}{s}\left(-\frac{\tau}{q}\right)^s-1-\left(\frac{\tau}{q}\right)^{2k+2}\right)\\
&=\frac{q}{(2k+2)(2k+1)\tau}\left(1+\left(\frac{\tau}{q}\right)^{2k+2}-\left(1-\frac{\tau}{q}\right)^{2k+2}\right).
\end{aligned}$$

It follows that

$$\begin{aligned}
N(k,h,g,q)=&\left(1-\frac{1}{h}\right)\left(1+\left(\frac{\tau}{q}\right)^{2k+2}-\left(1-\frac{\tau}{q}\right)^{2k+2}\right)\frac{q^{2k+1}}{(2k+2)(2k+1)}\\
&+O\left(4^k q^{2k+\frac{1}{2}}d(q)\ln^2 q\right).
\end{aligned}$$

This completes the proof of Theorem 1.

Combining Lemma 3 and the proof of Theorem 1, we immediately get Theorem 2.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work is supported by National Natural Science Foundation of China (11971381, 12371007) and Shaanxi Fundamental Science Research Project for Mathematics and Physics (Grant No. 22JSY007).

Conflict of interest

The authors declare there is no conflicts of interest.

References

1. R. K. Guy, *Unsolved Problem in Number Theory, 3rd.edn*, Springer-Verlag, New York, 2004.
2. W. P. Zhang, On a problem of D. H. Lehmer and its generalization, *Compos. Math.*, **86** (1993), 307–316.

3. W. P. Zhang, A problem of D.H.Lehmer and its generalization (II), *Compos. Math.*, **91** (1994), 47–56.
4. W. P. Zhang, On the difference between a D. H. Lehmer number and its inverse modulo q, *Acta Arith.*, **68** (1994), 255–263. https://doi.org/10.4064/aa-68-3-255-263
5. Y. N. Niu, R. Ma, H. D. Wang, On the difference between a D. H. Lehmer number and its inverse over short interval, *arXiv preprint*, (2021), arXiv:2104.00216. https://doi.org/10.48550/arXiv.2104.00216
6. Y. M. Lu, Y. Yi, On the generalization of the D. H. Lehmer problem, *Acta Math. Sin. (Engl. Ser.)*, **25** (2009), 1269–1274. https://doi.org/10.1007/s10114-009-7652-3
7. D. Han, Z. F. Xu, Y. Yi, T. P. Zhang, A Note on High-dimensional D. H. Lehmer Problem, *Taiwanese J. Math.*, **25** (2021), 1137–1157. https://doi.org/10.11650/tjm/210705
8. Z. F. Xu, T. P. Zhang, High-dimensional D. H. Lehmer problem over short intervals, *Acta Math. Sin. (Engl. Ser.)*, **30** (2014), 213–228. https://doi.org/10.1007/s10114-014-3324-z
9. W. P. Zhang, On the distribution of primitive roots modulo p, *Publ. Math. Debrecen*, **53** (1998), 245–255. https://doi.org/10.5486/pmd.1998.1750
10. C. I. Cobeli, S. M. Gonek, A. Zaharescu, On the distribution of small powers of a primitive root, *J. Number Theory*, **88** (2001), 49–58. https://doi.org/10.1006/jnth.2000.2604
11. Z. Rudnick, A. Zaharescu. The distribution of spacings between small powers of a primitive root, *Israel J. Math.*, **120** (2000), 271–287. https://doi.org/10.1007/s11856-000-1280-z
12. I. E. Shparlinski, Distribution of exponential functions modulo a prime power, *J. Number Theory*, **143** (2014), 224–231. https://doi.org/10.1016/j.jnt.2014.04.010

AIMS Press