Mathematics

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

AIMS Mathematics, 9(2): 4021–4031.
DOI: 10.3934/math.2024196
Received: 14 September 2023
Revised: 19 November 2023
Accepted: 29 November 2023
Published: 12 January 2024

Research article

Partitions into three generalized D. H. Lehmer numbers

Mingxuan Zhong[1] **and Tianping Zhang**[1,2,*]

[1] School of Mathematics and Statistics, Shaanxi Normal University, Xi'an 710119, Shaanxi, China
[2] Research Center for Number Theory and Its Applications, Northwest University, Xi'an 710127, Shaanxi, China

* **Correspondence:** Email: tpzhang@snnu.edu.cn.

Abstract: In this paper, we derived that a sufficiently large integer N can always be represented as the sum of three generalized D. H. Lehmer numbers. As a consequence, we deduced Lu and Yi's original result (*Monatsh. Math.*, **159** (2010), 45–58).

Keywords: D. H. Lehmer number; circle method; exponential sums; Bombieri-Weil bound
Mathematics Subject Classification: 11P55, 11L05

1. Introduction and main results

Let q be an odd integer and c be a fixed integer with $q \geq 3$, $(c, q) = 1$. For any $1 \leq a < q$, $(a, q) = 1$, there exists a unique integer $b \in [1, q)$ that satisties $(b, q) = 1$ and $ab \equiv c \,(\mathrm{mod}\ q)$. If a and b have different parity, then we call a a D. H. Lehmer number. Furthermore, let $r(q)$ denote the number of D. H. Lehmer numbers. The classical problem of D. H. Lehmer numbers is saying something nontrivial about $r(q)$ when $c = 1$.

Zhang's pioneering works [23, 24] implied that

$$r(q) = \frac{\phi(q)}{2} + O\left(q^{\frac{1}{2}} d^2(q) \log^2 q\right),$$

where ϕ, d are Euler's function and divisor function, respectively. $U = O(V)$ means $|U| \leq cV$ for some constant $c > 0$.

From then on, many authors generalized the D. H. Lehmer problem from various directions (see [1, 3, 5–7, 9, 10, 14, 16, 19–22] and references therein).

In 2010, Lu and Yi [11] used circle method and proved that for every sufficiently large integer N, it can be expressed as the sum of three D. H. Lehmer numbers $a \in \mathfrak{L}'(q)$ with

$$\mathfrak{L}'(q) = \{a \in \mathbb{Z} : a > 0, (a, q) = 1, n \nmid a + \overline{a}_c\},$$

where $n \geq 2$ is a fixed integer, q, c are two integers with $q > n \geq 2$ and $(n, q) = (c, q) = 1$, $\overline{a}_c$ satisfies $1 \leq \overline{a}_c \leq q$ and $a\overline{a}_c \equiv c(\text{mod } q)$. Denoting $R'(N)$ the number of ways in which N can be represented as the sum of three D. H. Lehmer numbers, for a sufficiently large integer q, $N \geq q^2 \log q$ and $2 \nmid (q, N)$ they obtained

$$R'(N) = \frac{N^2}{2}\left(1 - \frac{1}{n}\right)^3 \frac{\phi^3(q)}{q^3} A(q, N) + O\left(N^2 q^{-\frac{1}{2}} d^9(q) \log^3(q)\right),$$

where

$$\begin{aligned} A(q, N) &= \sum_{r|q} \frac{\mu(r)}{\phi^3(r)} G\left(-N, \chi_r^0\right) \\ &= \prod_{p|(q,N)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|q, p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right). \end{aligned}$$

Also in 2010, Shparlinski and Winterhof [17] proved that a sufficiently large integer also can be expressed as the sum of two such numbers under some natural restrictions and that

$$\begin{aligned} R''(N) = &\left(1 - \frac{1}{n}\right)^2 N \prod_{p|(N,q)} \left(1 - \frac{1}{p}\right) \prod_{p|q, p\nmid N} \left(1 - \frac{2}{p}\right) \\ &+ O\left(\left(\frac{N(N, q)^{\frac{1}{2}}}{q^{\frac{1}{2}}} + (N, q)^{\frac{1}{3}} q^{\frac{2}{3}}\right) q^{o(1)}\right) \end{aligned}$$

holds for an odd integer q or (N, q) is even. Here, $R''(N)$ denotes the number of ways in which N can be represented as the sum of two D. H. Lehmer numbers.

It seems interesting to see whether the same results hold for a more general number set. In this paper, we prove that for a sufficiently large integer N, it can also be represented as the sum of three more general D. H. Lehmer numbers $a \in \mathfrak{L}(q)$ under some mild restrictions. $\mathfrak{L}(q)$ is defined as follows: Let $n \geq 2$ be a fixed integer, $m \geq 1$ be a positive integer and q, c be two integers satisfying $q > n$ and $(c, q) = (n, q) = 1$. Denote that

$$\mathfrak{L}(q) = \{a \in \mathbb{Z} : a > 0, (a, q) = 1, n \nmid a + b\},$$

where b is the unique integer $1 \leq b \leq q$ satisfying $a^m b \equiv c(\text{mod } q)$.

The new ingredient of our method is deriving a sharp upper bound for the so-called "k-th Kloosterman sum" defined as

$$S(a, b; q) = \sum_{n=1}^{q}{}' e\left(\frac{an + b\overline{n}^k}{q}\right),$$

where q and k are two positive integers, $\sum'$ means the sum over integers co-prime to q and $e(x) = e^{2\pi i x}$.

Let $R(N)$ denote the number of ways in which N can be represented as the sum of three D. H. Lehmer numbers $a \in \mathfrak{L}(q)$, then we give the main theorem.

Theorem 1. *Let N be an integer that satisfies $N \geq q^2 \log q$ and $2 \nmid (q, N)$, ϵ be a small enough positive real number, then for a sufficiently large integer q and $m \leq q^{\frac{1}{2}}$ we have*

$$R(N) = \frac{N^2}{2}\left(1 - \frac{1}{n}\right)^3 \frac{\phi^3(q)}{q^3} A(q, N) + O\left(\min\left\{(m+1)^{6\omega(q)}, q^{\epsilon}\right\} N^2 q^{-\frac{1}{2}} d^6(q) \log^3 q\right),$$

where $\omega(q)$ denotes the number of different prime factors of q.

Corollary 1. *If we take $m = 1$ in Lehmer numbers set $\mathfrak{L}(q)$, then $\mathfrak{L}(q)$ and $\mathfrak{L}'(q)$ will represent the same set and Theorem 1 implies*

$$R(N) = \frac{N^2}{2}\left(1 - \frac{1}{n}\right)^3 \frac{\phi^3(q)}{q^3} A(q, N) + O\left(N^2 q^{-\frac{1}{2}} d^{12}(q) \log^3 q\right),$$

which is almost the original result of Lu and Yi's in 2010.

Remark 1. *It is worthy of pointing out that the circle method is not applicable for the problem where N is the sum of two such generalized D. H. Lehmer numbers. Meanwhile for the method in [17], we need a better upper bound for*

$$\sum_{\substack{x=0 \\ (q,g(x))=1}}^{q-1} e\left(\frac{f(x)}{g(x)}\right), \ q \in \mathbb{Z}, \ f(x), g(x) \in \mathbb{Z}[x],$$

which still goes beyond the reach of our ability.

2. Some lemmas

The following lemmas are needed for proving theorems.

Lemma 1. *Let k and q be two positive integers and ϵ be a small enough positive real number. Let $S(a, b; q)$ be defined as above, then*

$$|S(a, b; q)| \ll \min\left\{(k+1)^{2\omega(q)}, q^{\epsilon}\right\} (a, b, q)^{\frac{1}{2}} q^{\frac{1}{2}}.$$

Proof. We state Lemma 4 in [4] and follow roughly the same approach. First, suppose $q = rs$ with $(r, s) = 1$. By the "reciprocity" formula

$$s\bar{s} + r\bar{r} \equiv 1 (\mathrm{mod}\ q),$$

where $\bar{s}, \bar{r}$ satisfies $s\bar{s} \equiv 1(\mathrm{mod}\ r)$, $r\bar{r} \equiv 1(\mathrm{mod}\ s)$, respectively. Applying additive multiplicity for the exponential function

$$e\left(\frac{an + b\overline{n}^k}{q}\right) = e\left(\frac{a\bar{s}n + b\overline{sn}^k}{r}\right) e\left(\frac{a\bar{r}n + b\overline{rn}^k}{s}\right)$$

where $n = sx + ry$ and $1 \le x \le r$, $1 \le y \le s$, $(x, r) = 1$, $(y, s) = 1$, it leads to

$$\begin{aligned} S(a, b; q) &= {\sum_{x=1}^{r}}' {\sum_{y=1}^{s}}' e\left(\frac{a\bar{s}x + b\overline{sx}^k}{r}\right) e\left(\frac{a\bar{r}y + b\overline{ry}^k}{s}\right) \\ &= S(a\bar{s}, b\bar{s}; r) S(a\bar{r}, b\bar{r}; s). \end{aligned} \tag{1}$$

We need discuss the following cases:

(I) $q = p$: Prime moduli case. One can verify that Lemma 1 is correct by Moreno and Moreno [13]. It is also a special form of the Bombieri-Weil bound [2], which states

$$|S(a, b; q)| \le (k+1)(a, b, p)^{\frac{1}{2}} p^{1/2}, \tag{2}$$

provided that $\frac{ax^{k+1}+b}{x^k}$ is not in the shape of $h^p(x) - h(x)$, where $h(x) \in \overline{\mathbb{F}}_p[x]$ and $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. Suppose not and let

$$\frac{ax^{k+1}+b}{x^k} = \frac{f^p(x)}{g^p(x)} - \frac{f(x)}{g(x)},$$

with $f(x), g(x) \in \overline{\mathbb{F}}_p[x]$ and $(f(x), g(x)) = 1$. Further, we get

$$g^p(x) \mid x^k$$

obtained from

$$g^p(x)\left(ax^{k+1}+b\right) = x^k\left(f^p(x) - g^{p-1}(x)f(x)\right).$$

This is impossible if $p > k$, by comparing the degrees of both sides from above. If $p \leq k$, the validity of (2) is trivial.

(II) $q = p^\beta$: Prime power moduli case with $\beta > 1$. Without losing generality, we assume that $(a, b, p) = 1$. Lemmas 12.2 and 12.3 in [8] tell us that for $S(a, b; q)$ we have

$$S\left(a, b; p^{2\alpha}\right) = p^\alpha \sideset{}{'}\sum_{\substack{y=1 \\ g'(y)\equiv 0(\bmod p^\alpha)}}^{p^\alpha} e\left(\frac{g(y)}{p^{2\alpha}}\right), \tag{3}$$

$$S\left(a, b; p^{2\alpha+1}\right) = p^\alpha \sideset{}{'}\sum_{\substack{y=1 \\ g'(y)\equiv 0(\bmod p^\alpha)}}^{p^\alpha} e\left(\frac{g(y)}{p^{2\alpha+1}}\right)G_p(y), \tag{4}$$

where

$$g(y) = \frac{ay^7+b}{y^4},$$

$$G_p(y) = \sum_{z=1}^{p} e\left(\frac{h(y)z^2 + g'(y)p^{-\alpha}z}{p}\right),$$

with $h(y) = \frac{g''(y)}{2}$.

Note that $g'(y) = \frac{ay^{2k}-bky^{k-1}}{y^{2k}}$, and $h(y) = \frac{bk(k+1)y^{3k-2}}{2y^{4k}}$. For last part we focus on the solutions for the congruence equation $g'(y) \equiv 0 \,(\bmod\ p^\alpha)$ with $(y, p) = 1$.

✠ For $\beta = 2\alpha$ where $\alpha \geq 1$. The congruence equation above reduces to

$$3ay^{k+1} - bk \equiv 0 \,(\bmod\ p^\alpha). \tag{5}$$

If $(b, p) = p$, it leads to $(a, p) = 1$. From the properties of indices, one can verify that (5) has no solution. Next, we assume $(b, p) = 1$. If $p^\beta \| k$ with $1 \leq \beta \leq \alpha$, then (5) has at most $k+1$ solutions when $p^\beta \| a$. For $(p, k) = 1$, $(a, p) = 1$, the number of solutions for (5) is still $k+1$. We derive that

$$|S\left(a, b; p^{2\alpha}\right)| \leq (k+1)p^\alpha \text{ if } (a, b, p) = 1. \tag{6}$$

✠ For $\beta = 2\alpha + 1$ where $\alpha \geq 1$. First, from the case $\beta = 2\alpha$, one can check that if $(b, p) = p$, the sum in (4) vanishes. Supposing $(b, p) = 1$ and recalling the results of Chapter 3 in [8], we know if $p \nmid 2h(y)$ holds, then $|G_p(y)| \le p^{1/2}$. Therefore, if $p \ne k, k+1$ (otherwise, $p \mid bk(k+1)y^{k+2}$ implies $p \mid k(k+1)b$, a contradiction), we have $|G_p(y)| \le p^{1/2}$. Hence, $|S\left(a, b; p^{2\alpha+1}\right)| \le (k+1)p^{\alpha+1/2}$, as there are at most $(k+1)$ solutions to (5). If $p \mid k$ or $p \mid k+1$, we know that $|G_p(y)| \le k+1$ and $|S\left(a, b; p^{2\alpha+1}\right)| \le (k+1)^2 p^{\alpha}$.

In summary, we get

$$|S\left(a, b; p^{2\alpha+1}\right)| \le (k+1)^2 p^{\alpha+1/2} \text{ if } (a, b, p) = 1. \tag{7}$$

Combining (1), (2), (6) and (7), we come to the conclusion that

$$|S\,(a, b; q)| \le (k+1)^{2\omega(q)}(a, b, q)^{1/2} q^{1/2}.$$

From Lemma 1 in [18] and Lemma 2 in [15] we know that

$$S\,(a, b; q) \ll (a, b, q)^{\frac{1}{2}} q^{\frac{1}{2}+\epsilon},$$

then Lemma 1 is proved. □

Lemma 2. *Let $q \ge 2$, m be integers and $\chi(n)$ be Dirichlet character of modulo q, then we have*

$$G(m, \chi) = \sum_{m=1}^{q} \chi(l) e\left(\frac{ml}{q}\right) \ll q^{\frac{1}{2}}(m, q).$$

Proof. See Lemma 2 in [12]. □

Lemma 3. *Let q, c be integers satisfying $(c, q) = 1$ and m be a positive integer. For $k_1, k_2 \in \mathbb{Z}$, we have*

$$\sum_{\substack{\chi \bmod q \\ \chi \ne \chi_0 \\ \chi^m \ne \chi_0}} \overline{\chi}(c) G\left(k_1, \chi^m\right) G\left(k_2, \chi\right) \ll \min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} \phi(q) q^{\frac{1}{2}}\left(k_2, q\right),$$

where χ denotes Dirichlet character of modulo q.

Proof. From the definition of Gauss sum and Lemma 1, we obtain

$$\begin{aligned}
\sum_{\chi \bmod q} \overline{\chi}(c) G\left(k_1, \chi^m\right) G\left(k_2, \chi\right) &= \sum_{\chi \bmod q} \overline{\chi}(c) \sideset{}{'}\sum_{s=1}^{q} \chi^m(s) e\left(\frac{k_1 s}{q}\right) \sideset{}{'}\sum_{t=1}^{q} \chi(t) e\left(\frac{k_2 t}{q}\right) \\
&= \sideset{}{'}\sum_{s=1}^{q} \sideset{}{'}\sum_{t=1}^{q} e\left(\frac{k_1 s + k_2 t}{q}\right) \sum_{\chi \bmod q} \overline{\chi}(c) \chi\left(s^m t\right) \\
&= \phi(q) \sideset{}{'}\sum_{s=1}^{q} \sideset{}{'}\sum_{\substack{t=1 \\ s^m t \equiv c (\bmod q)}}^{q} e\left(\frac{k_1 s + k_2 t}{q}\right) \\
&= \phi(q) \sideset{}{'}\sum_{s=1}^{q} e\left(\frac{k_1 s + k_2 c \overline{s}^m}{q}\right) \\
&\ll \min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} \phi(q) q^{\frac{1}{2}}\left(k_1, k_2 c, q\right)
\end{aligned}$$

$$\ll \min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} \phi(q) q^{\frac{1}{2}} (k_2, q) .$$

On the other hand, from the property of Ramanujan sum we know that

$$\begin{aligned} G\left(k_1,\chi^0\right) G\left(k_2,\chi^0\right) =& \mu\left(\frac{q}{(k_1,q)}\right)\mu\left(\frac{q}{(k_2,q)}\right)\phi^2(q)\phi^{-1}\left(\frac{q}{(k_1,q)}\right)\phi^{-1}\left(\frac{q}{(k_2,q)}\right) \\ \ll& \phi^2(q)\frac{(k_1,q)(k_2,q)}{q^2} d\left(\frac{q}{(k_1,q)}\right) d\left(\frac{q}{(k_2,q)}\right) \\ \ll& (k_1,q)(k_2,q) d^2(q), \end{aligned}$$

and when $\chi^m = \chi_0$,

$$\overline{\chi}(c) G\left(k_1,\chi_0\right) G\left(k_2,\chi\right) \ll \phi(q) q^{\frac{1}{2}} (k_2, q)$$

holds, then Lemma 3 can be obtained from the above results. □

Lemma 4. *Assuming q, N are as described in Theorem 1 and $\alpha = s/r + z$, where*

$$1 \le r \le \tau = N/q,\ 0 \le s \le r-1,\ (r,s) = 1,\ |z| < \frac{1}{r\tau},$$

we have

$$\sum_{\substack{a\le N\\(a,q)=1}} e(\alpha a) = \begin{cases} \dfrac{\mu(r)\phi(q)}{q\phi(r)} \displaystyle\sum_{h=0}^{N-1} e(zh) + O\left((|z|N+1) r d(q)\right), & \text{if } r \mid q; \\ O\left((|z|N+1) r d(q)\right), & \text{if } r \nmid q. \end{cases}$$

Proof. Proof. See Lemma 5 in [11]. □

Lemma 5. *Assuming q, m and N are as described in the Theorem 1 and α satisfies Lemma 4, then we have*

$$S(\alpha) = \begin{cases} \left(1-\dfrac{1}{n}\right)\dfrac{\mu(r)\phi(q)}{q\phi(r)} \displaystyle\sum_{h=0}^{N-1} e(zh) \\ +O\left(\min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} N q^{-\frac{1}{2}} d^2(q) \log q\right), & \text{if } r \mid q; \\ O\left(\min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} N q^{-\frac{1}{2}} d^2(q) \log q\right), & \text{if } r \nmid q, \end{cases}$$

where $S(\alpha)$ is defined below.

Proof. From the proof of Lemma 6 in [11], we can easily obtain

$$S(\alpha) = \left(1-\frac{1}{n}\right) \sum_{a\le N}{}' e(\alpha a) - E(\alpha) + O\left(N q^{-1} d(q)\right),$$

where

$$E(\alpha) = \frac{1}{n\phi(q)} \sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} \overline{\chi}(c) \sum_{l=1}^{n} \left(\sum_{a\le N} \chi^m(a) e\left(a\left(\frac{l}{n}+\alpha\right)\right)\right)\left(\sum_{b\le q} \chi(b) e\left(\frac{l}{n} b\right)\right).$$

If $\chi \neq \chi_0$ and $\chi^m \neq \chi_0$, we have

$$\chi^m(a) = \frac{1}{q}\sum_{k=1}^{q} G(k,\chi^m)e\left(\frac{-ak}{q}\right).$$

Therefore, by using the above formula, $E(\alpha)$ can be transformed to the form in Lemma 3.

Using the proof of Lemma 6 in [11], when $\chi^m \neq \chi_0$, we can further obtain

$$E(\alpha) \ll \min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} Nq^{-\frac{1}{2}}d^2(q)\log q.$$

When $\chi^m = \chi_0$, we have

$$\begin{aligned}
E(\alpha) =& \frac{1}{n\phi(q)}\sum_{\chi^m=\chi_0}\overline{\chi}(c)\sum_{a\leq N}{}' e(a\alpha)\sum_{b\leq q}\chi(b)\sum_{l=1}^{n} e\left(\frac{l(a+b)}{q}\right)\\
=& \frac{1}{\phi(q)}\sum_{\chi^m=\chi_0}\overline{\chi}(c)\sum_{a\leq N}{}' e(a\alpha)\sum_{\substack{b\leq q\\ b\equiv -a(\bmod q)}}\chi(b)\\
=& \frac{1}{\phi(q)}\sum_{\chi^m=\chi_0}\overline{\chi}(c)\sum_{a\leq N}{}' e(a\alpha)\chi(-a)\\
\ll& \frac{mN}{\phi(q)}.
\end{aligned}$$

In summary, we obtain

$$S(\alpha) = \left(1-\frac{1}{n}\right)\sum_{a\leq N}{}' e(\alpha a) + O\left(\min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} Nq^{-\frac{1}{2}}d^2(q)\log q\right).$$

Combining with Lemma 4, Lemma 5 follows immediately. □

3. Proof of theorem

First, from circle method we let

$$R(N) := \sum_{\substack{a_1+a_2+a_3=N\\ a_i\in\mathfrak{Q}(q)}} 1 = \int_0^1 S^3(\alpha)e(-\alpha N)d\alpha,$$

where

$$S(\alpha) = \sum_{a\leq N, a\in\mathfrak{Q}(q)} e(\alpha a).$$

Taking $\tau = N/q$, we further get

$$R(N) = \int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}} S^3(\alpha)e(-\alpha N)d\alpha.$$

For using circle method, we write

$$\mathfrak{M}_1 = \bigcup_{r|q} \bigcup_{\substack{0\le s\le r-1\\(s,r)=1}} \left[\frac{s}{r} - \frac{1}{r\tau}, \frac{s}{r} + \frac{1}{r\tau}\right], \ \mathfrak{M}_2 = \left[-\frac{1}{\tau}, 1 - \frac{1}{\tau}\right] \setminus \mathfrak{M}_1,$$

where $0 \le s \le r-1$, $(s,r) = 1$ and $1 \le r \le \tau$. Clearly, when $\tau > q\log q$ for a sufficiently large integer q, we can see that the intervals in $\mathfrak{M}_1$ are pairwise disjoint.

If $\alpha \in \mathfrak{M}_2$, there exists integers r and s such that

$$|\alpha - \frac{s}{r}| < \frac{1}{r\tau},$$

where $0 \le s < r \le \tau$, $(s,r) = 1$ and $r \nmid q$.

Thus, we have

$$R(N) = R_1(N) + R_2(N),$$

and now we just need to estimate $R_i(N)$ for $i = 1, 2$.

Note that $(A+B)^3 = A^3 + O\left(|A^2B| + |B^3|\right)$. Therefore, Lemma 5 implies that for $\alpha \in \mathfrak{M}_1$,

$$\begin{aligned}S^3(\alpha) =& \left(1 - \frac{1}{n}\right)^3 \frac{\mu(r)\phi^3(q)}{q^3\phi^3(r)} \left(\sum_{h=0}^{N-1} e(zh)\right)^3\\ &+ O\left(\frac{1}{\phi^2(r)} \min\left(N^2, \frac{1}{|z|^2}\right) \min\left\{(m+1)^{2\omega(q)}, q^\epsilon\right\} Nq^{-\frac{1}{2}} d^2(q) \log q\right)\\ &+ O\left(\min\left\{(m+1)^{6\omega(q)}, q^\epsilon\right\} N^3 q^{-\frac{3}{2}} d^6(q) \log^3 q\right).\end{aligned}$$

From the proof of Theorem in [11] for the principal part of $R_1(N)$, this leads to

$$\begin{aligned}R_1(N) = \int_{\mathfrak{M}_1} S^3(\alpha)e(-\alpha N)d\alpha =& \sum_{r|q} \sum_{\substack{0\le s\le r-1\\(s,r)=1}} \int_{\frac{s}{r}-\frac{1}{r\tau}}^{\frac{s}{r}+\frac{1}{r\tau}} S^3(\alpha)e(-\alpha N)d\alpha\\ =& \left(1 - \frac{1}{n}\right)^3 \frac{\phi^3(q)}{q^3} \sum_{r|q} \frac{\mu(r)}{\phi^3(r)} G\left(-N, \chi_r^0\right) \int_{-\frac{1}{r\tau}}^{\frac{1}{r\tau}} \left(\sum_{h=0}^{N-1} e(zh)\right)^3 e(-zN)dz\\ &+ O\left(\min\left\{(m+1)^{6\omega(q)}, q^\epsilon\right\} N^2 q^{-\frac{1}{2}} d^6(q) \log^3 q\right)\\ =& \frac{N^2}{2} \left(1 - \frac{1}{n}\right)^3 \frac{\phi^3(q)}{q^3} A(q,N)\\ &+ O\left(\min\left\{(m+1)^{6\omega(q)}, q^\epsilon\right\} N^2 q^{-\frac{1}{2}} d^6(q) \log^3 q\right),\end{aligned}$$

where

$$\begin{aligned}A(q,N) = \sum_{r|q} \frac{\mu(r)}{\phi^3(r)} G\left(-N, \chi_r^0\right) =& \prod_{p|q} \left(1 - \frac{1}{(p-1)^3} G\left(-N, \chi_p^0\right)\right)\\ =& \prod_{p|(q,N)} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|q, p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right)\end{aligned}$$

with $G(N,\chi)$ as Gauss sum and χ as Dirichlet character modulo q.

For $\alpha \in \mathfrak{M}_2$, which also means $r \nmid q$, from Lemma 5 we obtain

$$S(\alpha) \ll \min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} Nq^{-\frac{1}{2}} d^2(q) \log q.$$

Noting that

$$\int_{E_2} |S(\alpha)|^2 d\alpha \ll \int_0^1 |S(\alpha)|^2 d\alpha \ll \sum_{a \le N, a \in \mathfrak{L}(q)} 1 \ll N,$$

we get

$$R_2(N) \ll \min\left\{(m+1)^{2\omega(q)}, q^{\epsilon}\right\} N^2 q^{-\frac{1}{2}} d^2(q) \log q.$$

Consequently, we obtain

$$R(N) = \frac{N^2}{2}\left(1 - \frac{1}{n}\right)^3 \frac{\phi^3(q)}{q^3} A(q,N) + O\left(\min\left\{(m+1)^{6\omega(q)}, q^{\epsilon}\right\} N^2 q^{-\frac{1}{2}} d^6(q) \log^3 q\right),$$

which completes the proof.

4. Conclusions

The main result of this paper was to prove that a sufficiently large integer can always be represented as the sum of three generalized D. H. Lehmer numbers. We used the elementary methods, the properties of the exponential sums and the circle method to give an asymptotic formula.

Use of AI tools declaration

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

Acknowledgments

Supported by the National Natural Science Foundation of China (Nos. 12271320, 11871317), and the Natural Science Basic Research Plan for Distinguished Young Scholars in Shaanxi Province of China (No. 2021JC-29). The authors are grateful to the anonymous referee for helpful comments and suggestions.

Conflict of interest

The authors declare that no conflicts of competing interests exist.

References

1. E. Alkan, F. Stan, A. Zaharescu, Lehmer *k*-tuples, *Proc. Amer. Math. Soc.*, **134** (2006), 2807–2815. https://doi.org/10.1090/S0002-9939-06-08484-X
2. E. Bombieri, On exponential sums in finite fields, *Amer. J. Math.*, **88** (1966), 71–105. https://doi.org/10.2307/2373048

3. J. Bourgain, T. Cochrane, J. Paulhus, C. Pinner, On the parity of k-th powers modulo p. A generalization of a problem of Lehmer, *Acta Arith.*, **147** (2011), 173–203. https://doi.org/10.4064/aa147-2-6

4. T. H. Chan, Squarefull numbers in arithmetic progression, II, *J. Number Theory*, **147** (2011), 173–203. https://doi.org/10.1016/j.jnt.2014.12.019

5. C. Cobeli, A. Zaharescu, Generalization of a problem of Lehmer, *Manuscripta Math.*, **104** (2001), 304–307. https://doi.org/10.1007/s002290170028

6. S. D. Cohen, T. Trudgian, Lehmer numbers and primitive roots modulo a prime, *J. Number Theory*, **203** (2019), 68–79. https://doi.org/10.1016/j.jnt.2019.03.004

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. H. Iwaniec, E. Kowalski, *Analytic Number Theory*, New York: American Mathematical Society Colloquium Publications, 2004. https://doi.org/10.1090/coll/053

9. S. R. Louboutin, J. Rivat, A. Sárközy, On a problem of D. H. Lehmer, *Proc. Amer. Math. Soc.*, **135** (2007), 969–975. https://doi.org/10.1090/S0002-9939-06-08558-3

10. Y. M. Lu, Y, Yi, On the generalization of the D. H. Lehmer problem, *Acta Math. Sin. (English Series)*, **25** (2009), 1269–1274. https://doi.org/10.1007/s10114-009-7652-3

11. Y. M. Lu, Y, Yi, Partitions involving D. H. Lehmer numbers, *Monatsh. Math.*, **159** (2010), 45–58. https://doi.org/10.1007/s00605-008-0049-z

12. Y. K. Ma, H, Chen, Z. Z. Qin, T. P. Zhang, Character sums over generalized Lehmer numbers, *J. Inequal. Appl.*, **2016** (2016), 270. https://doi.org/10.1186/s13660-016-1213-y

13. C. J. Moreno, O. Moreno, Exponential sums and Goppa codes. I, *Proc. Amer. Math. Soc.*, **111** (1991), 523–531. https://doi.org/10.2307/2048345

14. I. E. Shparlinski, On exponential sums with sparse polynomials and rational functions, *J. Number Theory*, **60** (1996), 233–244. https://doi.org/10.1006/jnth.1996.0121

15. I. E. Shparlinski, On a generalised Lehmer problem for arbitrary powers, preprint paper, 2008. https://doi.org/10.48550/arXiv.0803.3487

16. I. E. Shparlinski, On a generalisation of a Lehmer problem, *Math. Z.*, **263** (2009), 619–631. https://doi.org/10.1007/s00209-008-0434-2

17. I. E. Shparlinski, A. Winterhof, Partitions into two Lehmer numbers, *Monatsh. Math.*, **160** (2010), 429–441. https://doi.org/10.1007/s00605-009-0130-2

18. I. E. Shparlinski, Modular hyperbolas, *Monatsh. Math.*, **7** (2012), 235–294. https://doi.org/10.1007/s11537-012-1140-8

19. Z. F. Xu, On the difference between an integer and its m-th power mod n, *Sci. China Math.*, **56** (2013), 1597–1606. https://doi.org/10.1007/s11425-013-4639-4

20. 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

21. Z. F. Xu, W. P. Zhang, On a problem of D. H. Lehmer over short intervals, *J. Math. Anal. Appl.*, **320** (2006), 756–770. https://doi.org/10.1016/j.jmaa.2005.07.054

22. T. P. Zhang, W. P. Zhang, On the r-th hyper-Kloosterman sums and its hybrid mean value, *J. Korean Math. Soc.*, **43** (2006), 1199–1217. https://doi.org/10.4134/JKMS.2006.43.6.1199

23. W. P. Zhang, On a problem of D. H. Lehmer and its generalization, *Compositio Math.*, **86** (1993), 307–316.

24. W. P. Zhang, A problem of D. H. Lehmer and its generalization. II, *Compositio Math.*, **91** (1994), 47–56.