ON EXISTENCE OF GENERALISED LEHMER NUMBERS MODULO PRIMES

BIKRAM MISRA, BIDISHA ROY AND B. SURY

Abstract. In this article, we discuss a multivariable analogue of Lehmer's parity problem. We generalise the notions of Lehmer numbers as Lehmer q-tuples for a fixed odd prime q. We count the number of Lehmer q-tuples and derive an asymptotic estimate with explicit error terms. This deals with estimating various character sums and Deligne's bound for incomplete exponential sums.

1. introduction

Throughout this article, let p denote an odd prime and $\bar{a}$ denote the multiplicative inverse of a natural number $a < p$ in the group $(\mathbb{Z}/p\mathbb{Z})^\times := \{1, \ldots, p-1\}$. In 1981, Lehmer asked the question that 'How often a number and its inverse have opposite parity?' (see [5, §F12]). From a probabilistic point of view, one may expect that the question has an affirmative answer approximately half the times. In the context of this question, we begin by defining the Lehmer numbers modulo p.

An integer a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is said to be a Lehmer number modulo p if a and $\bar{a} \pmod p$, within the same range, have opposite parity. In other words, we say a to be a Lehmer number modulo p if $a + \bar{a}$ is not divisible by 2. It is easy to see that there is no Lehmer number modulo 3 and 7.

For a randomly chosen residue class $a \pmod p$, the parity of $\bar{a}$ is independent of the parity of a. Hence, it is natural to expect that exactly half of the elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ are Lehmer numbers modulo p. In fact, if M_p denotes the number of Lehmer numbers modulo p, then Zhang [17] showed that the sum defining $M_p - (p-1)/2$ exhibits square-root cancellations. To be precise, for a sufficiently large prime p, it was shown that

$$M_p = \frac{p-1}{2} + O(p^{\frac{1}{2}} \log^2 p). \tag{1.1}$$

In [4], Cohen and Trudian derived explicit constant in (1.1) by proving the following inequality;

$$\left| M_p - \frac{p-1}{2} \right| < T_p^2 \sqrt{p} (\log p)^2 \leq \frac{1}{2} \sqrt{p} (\log p)^2,$$

where

$$T_m := \frac{2 \sum_{j=1}^{(m-1)/2} \tan\left(\frac{\pi j}{m}\right)}{m \log m} \text{ for } m \geq 3 \text{ and while } m \to \infty, T_m \to \frac{2}{\pi}.$$

2020 *Mathematics Subject Classification.* 11A07.

Key words and phrases. Lehmer numbers, Orthogonality relations.

Furthermore, in [16], Zhang introduced Lehmer numbers modulo any odd positive integer $s > 2$ and proved a similar asymptotic result for the number of Lehmer numbers modulo s.

As understanding the distribution of primitive roots is an active topic of research in number theory, it is worthwhile to study Lehmer numbers that are (resp. are not) primitive roots; for simplicity, we will use the notations LPR and LNPR, respectively. LPRs were first introduced by Wang and Wang in [11]. Later it was studied effectively in [4]. A similar explicit result was obtained by the second author for LNPRs in [10].

In this direction of Lehmer numbers, various other generalisations have been studied in different ways; see, for instance, [2, 3, 7, 8, 9, 14, 15, 18]. One of these was done by Alkan, Stan and Zaharescu in [1]. They replaced the parity condition of Lehmer numbers by the linear congruences with the product of the residues being unity. Let $k, t \geq 2$ and $c_1, \ldots, c_{k+1} \geq 2$ with $0 \leq b_i < c_i$ be the residue classes such that $(t, c_1 \cdots c_{k+1}) = 1$. Let $N(\boldsymbol{c}, \boldsymbol{b}; t)$ counts the number of points $(n_1, \ldots, n_k)$ inside the k-dimensional box $[1, t-1]^k$ which satisfy the following system of linear congruences

$$n_1 \equiv b_1 \bmod c_1, \cdots, n_k \equiv b_k \bmod c_k$$
$$\text{and}$$
$$\overline{n_1 \cdots n_k} \equiv b_{k+1} \bmod c_{k+1}.$$

To be precise, they proved that

$$N(\boldsymbol{c}, \boldsymbol{b}; t) = \frac{\phi(t)^k}{c_1 \cdots c_{k+1}} + O_{k,\epsilon}\left(t^{k-\frac{1}{2}+\epsilon}\right), \tag{1.2}$$

for every $\epsilon > 0$.

Their proof relies on applying the orthogonality of the additive characters along with the Deligne's bound for the hyper-Kloosterman sums. Shapliniski [12] used the orthogonality of multiplicative characters and the Burgess bounds to improve the error term in (1.2). In particular, he proved that

$$N(\boldsymbol{c}, \boldsymbol{b}; t) = \frac{\phi(t)^k}{c_1 \cdots c_{k+1}} + O\left(\frac{\|\boldsymbol{c}\| t^{k-1+o(1)}}{c_1 \cdots c_{k+1}} + \frac{t^{\frac{k+1}{2}+o(1)}}{(c_1 \cdots c_{k+1})^{\frac{1}{k+1}}}\right),$$

where $\|\boldsymbol{c}\|$ denotes the Euclidean norm of c.

In this article, we further generalise the notion of Lehmer numbers from a different perspective, namely Lehmer q-tuples for a fixed odd prime q, defined as follows.

Definition 1.1. *A tuple* $\mathbf{a} = (a_1, \ldots, a_{q-1}) \in \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^{q-1}$ *is called a generalised Lehmer q-tuple modulo p if*

$$a_1 + \cdots + a_{q-1} + \overline{a_1 a_2 \cdots a_{q-1}} \not\equiv 0 \pmod q.$$

The aim of this article is to derive an asymptotic formula with an explicit error term for $\mathcal{M}_{p,q}$, which counts the number of generalised Lehmer q-tuples modulo p for primes $p > q$. We also give special attention to the case $q = 3$.

Remark 1.1. *It is worth noting that, if we choose $t = p$, $k = q-1$, and $c_i = q$ for all $1 \le i \le q$ in equation (1.2), then we have*

$$\mathcal{M}_{p,q} = \sum_{\substack{0\le b_1,\dots,b_q\le q-1\\ b_1+\cdots+b_q\not\equiv 0 \pmod q}} N((q,\dots,q),\boldsymbol{b};p).$$

Here $b_1,\dots,b_{q-1}$ are the reductions of $a_1,\dots,a_{q-1}$ modulo q, while b_q is the reduction modulo q of the representative of $\overline{a_1\cdots a_{q-1}}$ in $\{1,\dots,p-1\}$. These residue classes are allowed to be zero, since a nonzero residue modulo p may be divisible by q.

In other words, we count the tuples considered by Alkan et al. [1] whose associated residue classes satisfy the additional additive condition $b_1+\cdots+b_q \not\equiv 0 \pmod q$. For fixed q, summing their estimate over the $(q-1)q^{q-1}$ admissible residue vectors gives

$$\mathcal{M}_{p,q} = \frac{q-1}{q}(p-1)^{q-1} + O_{q,\epsilon}\left(p^{q-\frac{3}{2}+\epsilon}\right).$$

To obtain a sharper estimate with an explicit constant, we treat the additive and multiplicative conditions together using the orthogonality of additive characters. Hence, hyper-Kloosterman sums appear naturally in this context. In this context, we remark that although Shparlinski demonstrated in the case of multidimensional generalizations, that multiplicative character sums can produce better cancellations than exponential sums (see [12]), our case is more complicated in the fact that we need to use a Kloosterman-type estimate to handle both additive and multiplicative conditions together. Indeed, our method produces better asymptotics than if we were to use only multiplicative character sums.

1.1. **Notations.** Let $\zeta_q = e^{2\pi i/q}$ denote a primitive q-th root of unity and ψ denote the additive character modulo p. For an integer a, we define $\psi(a) = e^{2\pi i a/p}$. Let $h \in \{1,\dots,q-1\}$ be determined by $p \equiv h \pmod q$. For $1 \le m, h \le q-1$, we introduce the following notations:

$$c_{q,m}(h) := \sum_{r=1}^{h-1} \zeta_q^{mr}, \qquad \mathcal{C}_q(h) := \sum_{m=1}^{q-1} c_{q,m}(h)^q.$$

The empty sum is understood to be zero. We note in passing the following. If tr denotes trace of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}$, then we have

$$\mathcal{C}_q(h) = tr\left(\frac{1-\zeta_q^{h-1}}{1-\zeta^q}\right)^q.$$

In particular,

$$\mathcal{C}_q(2) = q-1,\ \mathcal{C}_q(h) = -\mathcal{C}_q(q+2-h)\ \forall\ 2 \le h \le q-1.$$

Next, we introduce the following notations:

$$S_{q,m}(j) := \sum_{r\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta_q^{mr}\psi(-jr), \qquad T_{q,m} := \sum_{j=1}^{p-1} S_{q,m}(j), \qquad A_{q,m} := \sum_{j=1}^{p-1} |S_{q,m}(j)|.$$

For a tuple $\mathbf{a} \in \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^{q-1}$, we also define

$$F_q(\mathbf{a}) := a_1 + \cdots + a_{q-1} + \overline{a_1 a_2 \cdots a_{q-1}}.$$

With these notations in place, we now state the main theorem of this article. Note that, the probability that a natural number is not divisible by q is $(q-1)/q$. Therefore, it is heuristically excepted that the asymptotic behaviour of $\mathcal{M}_{p,q}$ is closely related to $(q-1)(p-1)^{q-1}/q$. To be precise, we prove the following.

Theorem 1.1. *For odd primes $q > 2$ and $p > q$, with $p \equiv h \pmod q$, we have*

$$\left|\mathcal{M}_{p,q} - \frac{q-1}{q}(p-1)^{q-1} + \frac{1+p+\cdots+p^{q-1}}{qp^q}\mathcal{C}_q(h)\right| \leq (q-1)p^{\frac{q-1}{2}}\left(3+\frac{2}{\pi}\log p\right)^q,$$

where

$$\mathcal{C}_q(h) = q\sum_{t=1}^{h-1}\sum_{j=0}^{\left[\frac{q(t-1)}{h-1}\right]}(-1)^j\binom{q}{j}\binom{tq-j(h-1)-1}{q-1} - (h-1)^q.$$

Remark 1.2. *If $p \equiv 1 \pmod q$, then $h = 1$ and consequently $c_{q,m}(1) = 0$ for every $1 \leq m \leq q-1$. Hence, in this case, the second term in the above expression does not occur.*

For $q = 3$, we have the following corollary from Theorem 1.1.

Corollary 1.1. *For the primes $p \equiv 1, 2 \pmod 3$, we have*

$$\left|\mathcal{M}_{p,3} - \frac{2}{3}(p-1)^2\right| \leq 2p\left(\frac{\sqrt{3}}{2\pi}\left(\frac{9}{2}+2\log p\right)+\frac{1}{2}\right)^3,$$

and

$$\left|\mathcal{M}_{p,3} - \frac{2}{3}(p-1)^2 + \frac{2(1+p+p^2)}{3p^3}\right| \leq 2p\left(\frac{\sqrt{3}}{2\pi}\left(\frac{9}{2}+2\log p\right)+\frac{1}{2}\right)^3,$$

respectively.

2. Auxiliary results

In this section we collect the necessary results which are needed to prove Theorem 1.1. We first observe that the function

$$\frac{1}{2}\left(1-(-1)^{a+\bar{a}}\right)$$

serves as a characteristic function for Lehmer numbers a modulo p. For the generalised Lehmer q-tuples, we have the condition $F_q(\mathbf{a}) \not\equiv 0 \pmod q$. Hence, we note the following characteristic equation

$$\frac{1}{q}\left((q-1)-\sum_{m=1}^{q-1}\zeta_q^{mF_q(\mathbf{a})}\right) = \begin{cases}1 & \text{if } F_q(\mathbf{a}) \not\equiv 0 \pmod q,\\ 0 & \text{otherwise.}\end{cases} \tag{2.1}$$

For $a, r \in \mathbb{Z}/p\mathbb{Z}$, the additive-character orthogonality relation gives

$$\frac{1}{p}\sum_{j\in\mathbb{Z}/p\mathbb{Z}}\psi(j(a-r)) = \begin{cases}1 & \text{if } a = r,\\ 0 & \text{otherwise.}\end{cases} \tag{2.2}$$

For a fixed residue class m modulo q, we multiply the equation (2.2) by ζ_q^{mr}. Then summing over $r \in (\mathbb{Z}/p\mathbb{Z})^\times$, for an integer $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we obtain the following finite Fourier expansion:

$$\zeta_q^{ma} = \frac{1}{p} \sum_{r \in (\mathbb{Z}/p\mathbb{Z})^\times} \sum_{j \in \mathbb{Z}/p\mathbb{Z}} \zeta_q^{mr} \psi(j(a-r)). \tag{2.3}$$

Next, we will estimate the sum $T_{q,m}$.

Lemma 2.1. *For $1 \le m, h \le q-1$, we have $T_{q,m} = -c_{q,m}(h)$.*

Proof. Applying (2.2) for $a = 0$, we first note that

$$\sum_{j=1}^{p-1} \psi(-jr) = -1, \tag{2.4}$$

for every $r \neq 0$. Now envoking the above character sum from (2.4), we get

$$T_{q,m} = \sum_{j=1}^{p-1} S_{q,m}(j) = \sum_{r=1}^{p-1} \zeta_q^{mr} \sum_{j=1}^{p-1} \psi(-jr) = -\sum_{r=1}^{p-1} \zeta_q^{mr} = -S_{q,m}(0) = -c_{q,m}(h).$$

□

We now consider the sum $A_{q,m}$ and derive the following upper bound.

Lemma 2.2. *Let $1 \le m, h \le q-1$, and $r \in \{1, \dots, q-1\}$ be determined by*

$$r \equiv mh \pmod{q}.$$

Then we get

$$A_{q,m} \le p \left[\left| \cos\left(\frac{\pi r}{q}\right) \right| + \frac{\sin\left(\frac{\pi r}{q}\right)}{\pi} \times \left(\frac{q}{r} + \frac{q}{q-r} + 2\log p \right) \right]. \tag{2.5}$$

In particular,

$$A_{q,m} \le p\left(3 + \frac{2}{\pi}\log p\right) < p(3 + \log p).$$

Proof. Recall that

$$A_{q,m} = \sum_{j=1}^{p-1} |S_{q,m}(j)| = \sum_{j=1}^{p-1} \left| \sum_{r \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta_q^{mr} \psi(-jr) \right|.$$

We first write $S_{q,m}(j)$ as the following geometric sum for $1 \le j \le p-1$,

$$S_{q,m}(j) = \sum_{r=1}^{p-1} e^{2i\pi r\left(\frac{m}{q} - \frac{j}{p}\right)} = e^{ip\pi\left(\frac{m}{q} - \frac{j}{p}\right)} \frac{\sin\left((p-1)\pi\left(\frac{m}{q} - \frac{j}{p}\right)\right)}{\sin\left(\pi\left(\frac{m}{q} - \frac{j}{p}\right)\right)}. \tag{2.6}$$

Let us assume that $\theta = r/q$. Since $r \equiv mh \pmod{q}$, the numbers $\pi mh/q$ and $\pi\theta$ differ by an integral multiple of π. Hence, we have

$$\left|\sin\left(\frac{\pi mh}{q}\right)\right| = \sin(\pi\theta) \qquad \text{and} \qquad \left|\cos\left(\frac{\pi mh}{q}\right)\right| = |\cos(\pi\theta)|.$$

From (2.6), we have

$$|S_{q,m}(j)| \leq |\cos(\pi\theta)| + \sin(\pi\theta)\left|\cot\left(\pi\left(\frac{m}{q}-\frac{j}{p}\right)\right)\right|.$$

For a real number of x, let $\|x\|$ denotes the distance from x to the nearest integer. Then for $0 \leq j \leq p-1$, we define the following

$$d_j := \left\|\frac{m}{q}-\frac{j}{p}\right\|.$$

Since $\gcd(p,q)=1$, observe that $d_j \neq 0$ for all j. Moreover, we have the following inequality

$$\left|\cot\left(\pi\left(\frac{m}{q}-\frac{j}{p}\right)\right)\right| = |\cot(\pi d_j)| \leq \frac{1}{\pi d_j}.$$

Let us assume $p = 2N+1$ for some $N \geq 1$. Since the fractional part of pm/q is θ, translating the indices modulo p, we note that the numbers pd_j are obtained from the sequences $\{n+\theta\}_{n\geq 0}$ and $\{n-\theta\}_{n\geq 0}$, truncated when the distance reaches $p/2$. Consequently,

$$\sum_{j=0}^{p-1}\frac{1}{pd_j} \leq \frac{1}{\theta}+\frac{1}{1-\theta}+\sum_{k=1}^{N}\left(\frac{1}{k+\theta}+\frac{1}{k+1-\theta}\right).$$

For $0<\theta<1$ and $k \geq 1$, we have

$$\frac{1}{k+\theta}+\frac{1}{k+1-\theta} \leq \frac{1}{k}+\frac{1}{k+1}.$$

Therefore, we have

$$\sum_{k=1}^{N}\left(\frac{1}{k+\theta}+\frac{1}{k+1-\theta}\right) \leq \sum_{k=1}^{N}\frac{1}{k}+\sum_{k=1}^{N+1}\frac{1}{k} \leq 2\log p,$$

and consequently,

$$\sum_{j=0}^{p-1}\left|\cot\left(\pi\left(\frac{m}{q}-\frac{j}{p}\right)\right)\right| \leq \frac{p}{\pi}\left(\frac{1}{\theta}+\frac{1}{1-\theta}+2\log p\right).$$

We now sum the estimate for $|S_{q,m}(j)|$ over $1 \leq j \leq p-1$, to obtain the following upper bound of $A_{q,m}$:

$$A_{q,m} \leq p\left[|\cos(\pi\theta)| + \frac{\sin(\pi\theta)}{\pi}\left(\frac{1}{\theta}+\frac{1}{1-\theta}+2\log p\right)\right].$$

Substituting $\theta = r/q$ we get (2.5).

As $\sin(\pi\theta) \leq \pi\theta$ and $\sin(\pi\theta) \leq \pi(1-\theta)$ we conclude that

$$A_{q,m} \leq p\left(3+\frac{2}{\pi}\log p\right) < p(3+\log p).$$

□

Remark 2.1. *When $q = 3$, we have $r \in \{1, 2\}$. Therefore, we have*

$$\left|\cos\left(\frac{\pi r}{3}\right)\right| = \frac{1}{2}, \qquad \sin\left(\frac{\pi r}{3}\right) = \frac{\sqrt{3}}{2},$$

and

$$\frac{3}{r} + \frac{3}{3-r} = \frac{9}{2}.$$

Putting this all together, we get

$$A_{3,m} \leq p\left(\frac{\sqrt{3}}{2\pi}\left(\frac{9}{2} + 2\log p\right) + \frac{1}{2}\right). \tag{2.7}$$

For a fixed residue class h modulo q, we now derive a formula for the sum $\mathcal{C}_q(h)$. If tr denotes trace of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}$, then we obtain

$$\mathcal{C}_q(h) = tr\left(\frac{1-\zeta_q^{h-1}}{1-\zeta^q}\right)^q.$$

In particular, we have

$$\mathcal{C}_q(2) = q-1,\ \mathcal{C}_q(h) = -\mathcal{C}_q(q+2-h)\ \forall\ 2 \leq h \leq q-1.$$

Lemma 2.3. *For $h \in \{1, \ldots, q-1\}$ we have*

$$\mathcal{C}_q(h) = q\sum_{t=1}^{h-1}\sum_{j=0}^{\left[\frac{q(t-1)}{h-1}\right]}(-1)^j\binom{q}{j}\binom{tq-j(h-1)-1}{q-1} - (h-1)^q.$$

Proof. Note that, we have

$$\mathcal{C}_q(h) = \sum_{m=1}^{q-1}\left(\sum_{r_1=1}^{h-1}\zeta_q^{mr_1}\right)\cdots\left(\sum_{r_q=1}^{h-1}\zeta_q^{mr_q}\right) = \sum_{r_1,\ldots,r_q=1}^{h-1}\sum_{m=1}^{q-1}\zeta_q^{m(r_1+\cdots+r_q)}.$$

Now we note the following orthogonality relation

$$\sum_{m=1}^{q-1}\zeta_q^{m(r_1+\cdots+r_q)} = \begin{cases}(q-1) & \text{if } q \mid (r_1+\cdots+r_q),\\ -1 & \text{otherwise.}\end{cases} \tag{2.8}$$

Applying (2.8), we write $\mathcal{C}_q(h)$ as

$$\begin{aligned}\mathcal{C}_q(h) &= (q-1)\sum_{\substack{1\leq r_1,\ldots,r_q\leq h-1\\ r_1+\cdots+r_q\equiv 0 \bmod q}} 1 - \sum_{\substack{1\leq r_1,\ldots,r_q\leq h-1\\ r_1+\cdots+r_q\not\equiv 0 \bmod q}} 1\\ &= q\sum_{\substack{1\leq r_1,\ldots,r_q\leq h-1\\ r_1+\cdots+r_q\equiv 0 \bmod q}} 1 - \sum_{1\leq r_1,\ldots,r_q\leq h-1} 1\\ &= qN_q(h) - (h-1)^q\end{aligned}$$

where $N_q(h)$ counts the number of solutions of the equation $r_1 + \cdots + r_q \equiv 0 \bmod q$ where $1 \leq r_1, \ldots, r_q \leq h-1$. Hence, $r_1 + \cdots + r_q = tq$ for some $t \in \{1, \ldots, h-1\}$. Therefore, we are left to count the number of non-negative integral solutions of the equation

$$r_1 + \cdots + r_q = q(t-1); \qquad \text{with} \qquad 0 \leq r_i \leq h-2.$$

Using the theory of generating functions, one can show that

$$N_q(h) = \sum_{t=1}^{h-1} \sum_{j=0}^{\left[\frac{q(t-1)}{h-1}\right]} (-1)^j \binom{q}{j} \binom{tq - j(h-1) - 1}{q-1}. \tag{2.9}$$

This completes the proof of Lemma 2.3 and hence the proof of Theorem 1.1.

□

Finally, we end this section by recording Deligne's bound for the hyper-Kloosterman sums. For $(j_1, \ldots, j_q) \in (\mathbb{Z}/p\mathbb{Z})^q$, let $K_q(j_1, \ldots, j_q; p)$ denote the following hyper-Kloosterman sums

$$K_q(j_1, \ldots, j_q; p) := \sum_{a_1, \ldots, a_{q-1} \in (\mathbb{Z}/p\mathbb{Z})^\times} \psi\left(\sum_{r=1}^{q-1} j_r a_r + j_q \overline{a_1 a_2 \cdots a_{q-1}}\right).$$

In this context, we note the following bound due to Deligne. With $x_r = j_r a_r$ for $1 \leq r \leq q-1$ and $x_q = (j_1 \cdots j_q)\overline{(x_1 \cdots x_{q-1})}$, one can define $K_q(j_1, \ldots, j_q; p)$ as per the formula of Kowalski et al. [6] with $a = j_1 \cdots j_q$. As a consequence of the deep results of Deligne on Weil's conjecture, we quote the following upper bound.

Lemma 2.4. [6] *For $j_1 j_2 \cdots j_q \neq 0$, we have*

$$|K_q(j_1, \ldots, j_q; p)| \leq q p^{\frac{q-1}{2}}.$$

3. Proof of Theorem 1.1

We begin with the characteristic function of the generalised Lehmer q-tuples. Applying (2.1), we have

$$\mathcal{M}_{p,q} = \frac{1}{q} \sum_{a_1, \ldots, a_{q-1} \in (\mathbb{Z}/p\mathbb{Z})^\times} \left((q-1) - \sum_{m=1}^{q-1} \zeta_q^{mF_q(\mathbf{a})}\right) = \frac{q-1}{q}(p-1)^{q-1} - \frac{1}{q}\sum_{m=1}^{q-1} E_{p,q}^{(m)}, \tag{3.1}$$

where

$$E_{p,q}^{(m)} := \sum_{a_1, \ldots, a_{q-1} \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta_q^{m(a_1 + \cdots + a_{q-1} + \overline{a_1 \cdots a_{q-1}})}.$$

We need to estimate the sum $\sum_{m=1}^{q-1} E_{p,q}^{(m)}$. Applying (2.3) to each of the $q-1$ variables and to $\overline{a_1 \cdots a_{q-1}}$, we rewrite $E_{p,q}^{(m)}$ as

$$E_{p,q}^{(m)} = \frac{1}{p^q} \sum_{j_1, \ldots, j_q \in \mathbb{Z}/p\mathbb{Z}} E_{p,q}^{(m)}(j_1, \ldots, j_q), \tag{3.2}$$

where

$$E_{p,q}^{(m)}(j_1,\dots,j_q) := K_q(j_1,\dots,j_q;p)\prod_{\nu=1}^{q} S_{q,m}(j_\nu).$$

To estimate the above terms, we consider the following two cases, namely, when at least one of $j_1,\dots,j_q$ is zero and when all of them are non-zero. In other words, we write

$$\begin{aligned}\mathcal{M}_{p,q} - \frac{q-1}{q}(p-1)^{q-1} &= -\frac{1}{qp^q}\sum_{j_1,\dots,j_q\in\mathbb{Z}/p\mathbb{Z}}\sum_{m=1}^{q-1} E_{p,q}^{(m)}(j_1,\dots,j_q)\\ &= -\frac{1}{qp^q}\sum_{\substack{j_1,\dots,j_q\in\mathbb{Z}/p\mathbb{Z}\\ j_1\cdots j_q=0}}\sum_{m=1}^{q-1} E_{p,q}^{(m)}(j_1,\dots,j_q)\\ &\quad -\frac{1}{qp^q}\sum_{\substack{j_1,\dots,j_q\in\mathbb{Z}/p\mathbb{Z}\\ j_1\cdots j_q\neq 0}}\sum_{m=1}^{q-1} E_{p,q}^{(m)}(j_1,\dots,j_q). \qquad (3.3)\end{aligned}$$

3.1. **At least one of $j_1,\dots,j_q$ is zero.** We first analyse the terms $E_{p,q}^{(m)}(j_1,\dots,j_q)$ when at least one of $j_1,\dots,j_q$ is zero. Note that, for a prime $p\equiv h \bmod q$, we have

$$S_{q,m}(0) = \sum_{r=1}^{p-1}\zeta_q^{mr} = \sum_{r=1}^{h-1}\zeta_q^{mr} = c_{q,m}(h), \qquad (3.4)$$

where we have divided the first sum into complete blocks of length q.

Remark 3.1. *Suppose that $p\equiv 1 \pmod q$. Then $h=1$, and hence $S_{q,m}(0)=0$ by (3.4). Therefore, if at least one of $j_1,\dots,j_q$ is zero, the product $\prod_{\nu=1}^{q} S_{q,m}(j_\nu)$ vanishes. Consequently, $E_{p,q}^{(m)}(j_1,\dots,j_q)=0$.*

Using the above observation, we first obtain a more general statement for every prescribed set of non-zero coordinates. For $\mathbf{j}=(j_1,\dots,j_q)$, let

$$\operatorname{supp}(\mathbf{j}) := \{\nu\in\{1,\dots,q\} : j_\nu\neq 0\}.$$

Proposition 3.1. *Let $I\subseteq\{1,\dots,q\}$ be a set of cardinality s, where $0\le s\le q-1$. For every $1\le m\le q-1$, we have*

$$\sum_{\substack{j_1,\dots,j_q\in\mathbb{Z}/p\mathbb{Z}\\ \operatorname{supp}(\mathbf{j})=I}} E_{p,q}^{(m)}(j_1,\dots,j_q) = (p-1)^{q-1-s}c_{q,m}(h)^q. \qquad (3.5)$$

Proof. Suppose first that $q\notin I$. In this case the inverse term in (2) does not occur. Hence,

$$K_q(j_1,\dots,j_q;p) = (p-1)^{q-1-s}\prod_{r\in I}\sum_{a_r\in(\mathbb{Z}/p\mathbb{Z})^\times}\psi(j_r a_r).$$

The orthogonality relation (2.2) for $r = 0$ gives

$$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \psi(ja) = \begin{cases} -1 & \text{if } j \in \operatorname{supp}(\mathbf{j}), \\ (p-1) & \text{otherwise.} \end{cases} \tag{3.6}$$

Applying (3.6) we get

$$K_q(j_1, \ldots, j_q; p) = (-1)^s (p-1)^{q-1-s}. \tag{3.7}$$

Suppose now that $q \in I$. Since $s \leq q-1$, there exists an index $t \in \{1, \ldots, q-1\} \setminus I$. We fix all the variables other than a_t and put

$$b := \prod_{\substack{1\leq r\leq q-1 \\ r\neq t}} \overline{a_r}.$$

Then $b \neq 0$, and the part of the character sum involving a_t is $\sum_{a_t\in(\mathbb{Z}/p\mathbb{Z})^\times} \psi\left(j_q b\overline{a_t}\right) = -1$, because the map $a_t \mapsto \overline{a_t}$ permutes $(\mathbb{Z}/p\mathbb{Z})^\times$ and $j_q b \neq 0$. After summing over a_t, the inverse term no longer occurs. The s non-zero linear coordinates contribute -1 each, while the remaining $q-1-s$ variables are free. Consequently,

$$K_q(j_1, \ldots, j_q; p) = (-1)^s (p-1)^{q-1-s}. \tag{3.8}$$

Thus, (3.7) and (3.8) give the same value in both cases.

For a fixed set I, the $q-s$ zero coordinates contribute $S_{q,m}(0)^{q-s} = c_{q,m}(h)^{q-s}$. On the other hand, summing each of the s non-zero coordinates gives $T_{q,m}$. Therefore, using Lemma 2.1, we get

$$\begin{aligned} \sum_{\substack{j_1,\ldots,j_q\in\mathbb{Z}/p\mathbb{Z} \\ \operatorname{supp}(\mathbf{j})=I}} E_{p,q}^{(m)}(j_1, \ldots, j_q) &= (-1)^s (p-1)^{q-1-s} c_{q,m}(h)^{q-s} T_{q,m}^s \\ &= (p-1)^{q-1-s} c_{q,m}(h)^q. \end{aligned}$$

□

Summing over all the possible supports gives the following exact contribution from the tuples having at least one zero coordinate. Hence we obtain the following corollary.

Corollary 3.1. *We have*

$$\frac{1}{qp^q} \sum_{m=1}^{q-1} \sum_{\substack{j_1,\ldots,j_q\in\mathbb{Z}/p\mathbb{Z} \\ j_1 j_2 \cdots j_q = 0}} E_{p,q}^{(m)}(j_1, \ldots, j_q) = \frac{1 + p + \cdots + p^{q-1}}{qp^q} \mathcal{C}_q(h).$$

Proof. For a fixed s, there are $\binom{q}{s}$ possible supports of cardinality s. Therefore, Proposition 3.1 gives

$$\sum_{\substack{j_1,\dots,j_q\in\mathbb{Z}/p\mathbb{Z}\\ j_1j_2\cdots j_q=0}} E_{p,q}^{(m)}(j_1,\dots,j_q) = c_{q,m}(h)^q \sum_{s=0}^{q-1}\binom{q}{s}(p-1)^{q-1-s}$$
$$= (1+p+\cdots+p^{q-1})c_{q,m}(h)^q.$$

Finally, summing over $m=1,\dots,q-1$ completes the proof. □

Using Corollary 3.1, we rewrite (3.3) as

$$\mathcal{M}_{p,q} - \frac{q-1}{q}(p-1)^{q-1} + \frac{1+p+\cdots+p^{q-1}}{q\,p^q}\sum_{m=1}^{q-1} c_{q,m}(h)^q$$
$$= -\frac{1}{q\,p^q}\sum_{\substack{j_1,\dots,j_q\in\mathbb{Z}/p\mathbb{Z}\\ j_1\cdots j_q\neq 0}}\sum_{m=1}^{q-1} E_{p,q}^{(m)}(j_1,\dots,j_q).$$

3.2. **All of $j_1,\dots,j_q$ are non-zero.** We now discuss the contribution from the tuples $(j_1,\dots,j_q)\in((\mathbb{Z}/p\mathbb{Z})^\times)^q$. Applying Lemma 2.4, for a fixed $m\in\{1,\dots,q-1\}$ we have

$$\frac{1}{qp^q}\sum_{j_1,\dots,j_q\in(\mathbb{Z}/p\mathbb{Z})^\times}\left|E_{p,q}^{(m)}(j_1,\dots,j_q)\right| \le \frac{q\,p^{(q-1)/2}}{qp^q}\sum_{j_1,\dots,j_q\in(\mathbb{Z}/p\mathbb{Z})^\times}\prod_{\nu=1}^{q}|S_{q,m}(j_\nu)|$$
$$= \frac{p^{(q-1)/2}}{p^q}\prod_{\nu=1}^{q}\left(\sum_{j_\nu\in(\mathbb{Z}/p\mathbb{Z})^\times}|S_{q,m}(j_\nu)|\right) = \frac{p^{(q-1)/2}}{p^q}A_{q,m}^q, \tag{3.9}$$

Hence, it remains to estimate the sum $\sum_{m=1}^{q-1} A_{q,m}^q$. From Lemma 2.2, we get

$$\sum_{m=1}^{q-1} A_{q,m}^q \le (q-1)p^q(3+\log p)^q.$$

This completes the proof of Theorem 1.1. The proof of corollary 1.1 follows from Theorem 1.1 along with (2.7).

4. Concluding Remarks

As we briefly mentioned in the introduction, it may be interesting to study generalised Lehmer numbers which are primitive roots. For the usual Lehmer numbers, this was introduced in [11] and later also studied in [4]. More precisely, let us introduce the following definition.

Definition 4.1. *Let q be an odd prime and let $p > q$ be a prime. An ordered tuple*

$$\mathbf{a} = (a_1, \ldots, a_{q-1}) \in \{1, \ldots, p-1\}^{q-1}$$

is called a ***generalised Lehmer primitive q-tuple modulo*** *p if each a_i is a primitive root modulo p and*

$$a_1 + \cdots + a_{q-1} + \overline{a_1 \cdots a_{q-1}} \not\equiv 0 \pmod{q},$$

where $\overline{a_1 \cdots a_{q-1}}$ denotes the multiplicative inverse of $a_1 \cdots a_{q-1}$ modulo p, chosen in $\{1, \ldots, p-1\}$.

For better understanding, using a standard computer, one can compute that for $p = 11$ and $q = 3$, there are 72 ordered generalised Lehmer 3-tuples modulo 11, of which 11 are generalised Lehmer primitive 3-tuples, that is, all entries of those tuples are primitive roots modulo 11. For example $(2, 7)$ is one of them.

Now, naturally, we can ask that *how many generalised Lehmer primitive q-tuples modulo p are there?*

Wang and Xu [13] also studied the problem of whether a given integer can be written as the sum of two Lehmer numbers. Their estimates imply that any integer can be written as the sum of two Lehmer numbers in $\mathbb{Z}/q\mathbb{Z}$ for sufficiently large odd integers q. Cohen and Trudgian [4] proved results on the following analogue of this problem: are there Lehmer primitive roots a and b whose sum is $1 \pmod{p}$? If p is sufficiently large, the answer is yes.

For any odd prime q, we have defined a notion of generalised Lehmer q-tuples modulo p for primes $p > q$ and derived an asymptotic formula with an explicit constant for the number of generalised Lehmer q-tuples modulo p for primes $p > q$. In the special case $q = 3$, we have proved a more refined result. We mention that Cohen and Trudgian [4] considered the following problem: are there Lehmer primitive roots a and b whose sum is $1 \pmod{p}$? If p is sufficiently large, they showed that the answer is in the affirmative. Using the results of the present paper, it may be worthwhile to study the analogous problem for Lehmer q-tuples.

5. Acknowledgment

We thank Prof. Igor Sparlinski for bringing some interesting references to our attention. The first author acknowledges the support of the Department of Mathematics and Statistics, IIT Tirupati for the wonderful working environment. The second author would like to thank INSPIRE Grant No: IFA-23 MA 190 and ANRF Grant No: ANRF/ECRG/2025/003044/PMS.

6. Declaration

There is no competing interests and no conflict of interests to declare.

References

[1] E. Alkan, F. Stan and A. Zaharescu, Lehmer k-tuples, Proc. Amer. Math. Soc. **134** (2006), no. 10, 2807–2815.

[2] J. Bourgain, T. Cochrane, J. Paulhus and C. Pinner, On the parity of k-th powers modulo p. A generalization of a problem of Lehmer, Acta Arith. **147** (2011), no. 2, 173–203.

[3] C. Cobeli and A. Zaharescu, Generalization of a problem of Lehmer, Manuscripta Math. **104** (2001), no. 3, 301–307.

[4] S. D. Cohen and T. Trudgian, Lehmer numbers and primitive roots modulo a prime, J. Number Theory **203** (2019), 68—79.
[5] R. K. Guy, *Unsolved problems in number theory*, Problem Books in Mathematics Unsolved Problems in Intuitive Mathematics, 1, Springer, New York-Berlin, 1981.
[6] E. Kowalski, P. G. Michel and W. F. Sawin, Bilinear forms with Kloosterman sums and applications, Ann. of Math. (2) **186** (2017), no. 2, 413–500.
[7] H. N. Liu, A note on Lehmer k-tuples, Int. J. Number Theory **5** (2009), no. 7, 1169–1178.
[8] Y. M. Lu and Y. Yi, On the generalization of the D. H. Lehmer problem, Acta Math. Sin. (Engl. Ser.) **25** (2009), no. 8, 1269–1274.
[9] Y. M. Lu and Y. Yi, On the generalization of the D. H. Lehmer problem. II, Acta Arith. **142** (2010), no. 2, 179–186.
[10] B. Roy, On the existence of certain Lehmer numbers modulo a prime, Expo. Math. **42** (2024), 21 pp.
[11] T. Wang and X. Wang, On the Golomb's conjecture and Lehmer's numbers, Open Math. **15** (2017), no. 1, 1003–1009.
[12] I. E. Shparlinski, On a generalisation of a Lehmer problem, Math. Z. **263** (2009), no. 3, 619–631.
[13] J. Wang and Z. F. Xu, Partitions into two Lehmer numbers in $\mathbb{Z}_q$, Math. Slovaca **75** (2025), no. 1, 45–54.
[14] W. L. Yao, On the generalization of the D. H. Lehmer problem and its mean value, JP J. Algebra Number Theory Appl. **6** (2006), no. 3, 479–491.
[15] Y. Yi and W. Zhang, On generalization of Lehmer D H problem, Gongcheng Shuxue Xuebao **20** (2003), no. 1, 60–64.
[16] W. Zhang, A problem of D. H. Lehmer and a generalization of it, J. Northwest Univ. **23** (1993), no. 2, 103–108.
[17] W. Zhang, A problem of D. H. Lehmer and its generalization, Compos. Math. **91** (1994) 47—51.
[18] W. Zhang, A problem of D. H. Lehmer and its generalization. II, Compos. Math. **91** (1994), no. 1, 47–56.

Bikram Misra and Bidisha Roy
Department of Mathematics and Statistics, Indian Institute of Technology Tirupati, Yerpedu 517619, India
Email address: bikram.misra@iittp.ac.in,bidisha.roy@iittp.ac.in

B. Sury
Indian Statistical Institute, 8th Mile Mysore Rd, Bengaluru 560059, India
&
International Centre for Theoretical Sciences, Survey No. 151, Shivakote Village, Hesaragatta Hobli, Bengaluru 560089, India
Email address: surybang@gmail.com