

LEHMER k -TUPLES

EMRE ALKAN, FLORIN STAN, AND ALEXANDRU ZAHARESCU

(Communicated by David E. Rohrlich)

ABSTRACT. Generalizing a classical problem of Lehmer, in this paper we provide an asymptotic result for the number of Lehmer k -tuples.

1. INTRODUCTION AND STATEMENT OF RESULTS

Given a prime number p , D.H. Lehmer (see Guy [2, Problem F12]) raised the problem of investigating the number $r(p)$ of integers $a \in \{1, 2, \dots, p-1\}$ for which a and \bar{a} are of opposite parity, where $\bar{a} \in \{1, 2, \dots, p-1\}$ is such that $a\bar{a} \equiv 1 \pmod{p}$. The problem was nicely treated by Wenpeng Zhang in [9], [10] and [11] who proved that

$$r(p) = \frac{p}{2} + O\left(p^{1/2} \log^2 p\right)$$

and then generalized this relation to the case when p is replaced by any odd number q . Next, he defined a *D.H. Lehmer number* to be any integer a coprime to q , $0 < a < q$, such that a and \bar{a} have opposite parity, and studied the distribution of the pairs (a, \bar{a}) , where a is a Lehmer number. The distribution function of a, \bar{a} is defined by

$$F_q(x, y) = \#\left\{a: 1 \leq a \leq xq, 1 \leq \bar{a} \leq yq, 2 \nmid a + \bar{a}\right\},$$

for $0 \leq x, y \leq 1$. It is proved in [11] that

$$F_q(x, y) = \frac{1}{2} xy \varphi(q) + O\left(q^{1/2} d^2(q) \log^2 q\right),$$

where $d(q)$ denotes the number of divisors of q . In [1], an absolutely irreducible algebraic curve \mathcal{C} of degree $\leq d$ defined over the finite field \mathbf{F}_p not contained in any hyperplane was considered. A Lehmer point for $\mathbf{a} = (a_1, \dots, a_r)$, $\mathbf{b} = (b_1, \dots, b_r) \in \mathbb{Z}^r$ with $a_1, \dots, a_r > 0$ was defined as an $\mathbf{x} = (x_1, \dots, x_r)$ with $0 \leq x_i < p$, such that $\mathbf{x} \pmod{p}$ belongs to \mathcal{C} and $x_j \equiv b_j \pmod{a_j}$ ($1 \leq j \leq r$). The set of Lehmer points is denoted as $\mathcal{L}(p, r, \mathcal{C}, a, b)$. In [1] it was shown that

$$\#\mathcal{L}(p, r, \mathcal{C}, a, b) = \frac{p}{a_1 \cdots a_r} + O_{r,d}(p^{1/2} \log^r p).$$

In the present paper we provide a different generalization of Lehmer's problem. Instead of the pair (a, \bar{a}) we consider $(k+1)$ -tuples of numbers with product congruent to 1 modulo q , and the parity condition is replaced by linear congruences with

Received by the editors April 18, 2005.

2000 *Mathematics Subject Classification*. Primary 11L05, 11K36.

Key words and phrases. Lehmer numbers, uniform distribution, Hyper-Kloosterman sums.

©2006 American Mathematical Society
 Reverts to public domain 28 years from publication

respect to more general moduli. Let $k \geq 1, q \geq 2$ be integers and let $a_1, \dots, a_{k+1} \geq 2$ and $b_1, \dots, b_{k+1} \geq 0$ with $0 \leq b_i < a_i$, for all $i \in \{1, 2, \dots, k + 1\}$, be integers such that $(q, a_1 a_2 \dots a_{k+1}) = 1$. We are interested in obtaining an asymptotic result for the number of points $(n_1, \dots, n_k) \in \mathbb{Z}^k$, with $1 \leq n_i \leq q - 1$, $(n_i, q) = 1$, for all $i \in \{1, \dots, k\}$, which satisfy the congruences

$$\begin{aligned} n_1 &\equiv b_1 \pmod{a_1} \\ &\dots \\ n_k &\equiv b_k \pmod{a_k} \end{aligned}$$

and

$$\overline{n_1 n_2 \dots n_k} \equiv b_{k+1} \pmod{a_{k+1}}.$$

We denote the number of points $(n_1, \dots, n_k) \in \mathbb{Z}^k$, $1 \leq n_1, \dots, n_k \leq q - 1$, satisfying the above congruences by $N(\mathbf{a}, \mathbf{b}; q)$. Then we prove the following result.

Theorem 1. *For any positive integers a_1, \dots, a_{k+1} , any integers b_1, \dots, b_{k+1} , any $\epsilon > 0$, and any $q \geq 2$ relatively prime to $a_1 \dots a_{k+1}$, the number $N(\mathbf{a}, \mathbf{b}; q)$ of Lehmer k -tuples satisfies*

$$N(\mathbf{a}, \mathbf{b}; q) = \frac{\phi(q)^k}{a_1 a_2 \dots a_{k+1}} + O_{k, \epsilon} \left(q^{k - \frac{1}{2} + \epsilon} \right).$$

A natural question that arises is to see how these Lehmer k -tuples are distributed in the cube $[0, q]^k$. To this end, we fix an arbitrary region Ω with piecewise smooth boundary in $[0, 1]^k$, and, with fixed $a_1, \dots, a_{k+1}, b_1, \dots, b_{k+1}$ and large q , we count the number, call it $N_\Omega(\mathbf{a}, \mathbf{b}, q)$, of Lehmer k -tuples as above, which lie inside the dilated region $q\Omega$. The next result shows in particular that for fixed $a_1, \dots, a_{k+1}, b_1, \dots, b_{k+1}$ and Ω , the ratio between the number $N_\Omega(\mathbf{a}, \mathbf{b}, q)$ of k -tuples that lie in $q\Omega$ over the total number $N(\mathbf{a}, \mathbf{b}, q)$ of Lehmer k -tuples approaches $vol(\Omega)$ as $q \rightarrow \infty$, i.e., if we scale the Lehmer k -tuples by a factor of $1/q$, then we can identify them with a set of points in $[0, 1]^k$ which are uniformly distributed in $[0, 1]^k$.

Theorem 2. *For any region $\Omega \subset [0, 1]^k$ with piecewise smooth boundary, any positive integers a_1, \dots, a_{k+1} , any integers b_1, \dots, b_{k+1} , any $\epsilon > 0$, and any $q \geq 2$ relatively prime to $a_1 \dots a_{k+1}$, one has*

$$N_\Omega(\mathbf{a}, \mathbf{b}, q) = vol(\Omega) \frac{\phi(q)^k}{a_1 \dots a_{k+1}} + O_{k, \Omega, \epsilon} \left(q^{k - \frac{1}{2(k+1)} + \epsilon} \right).$$

The main tool in the proof of the above results is provided by estimates for Hyper-Kloosterman sums. Another ingredient is the Lipschitz principle (see [3]), which states that the number of points of a cubical lattice of side s in a closed bounded region \mathcal{R} in \mathbf{R}^n is

$$Vol(\mathcal{R}) \left(\frac{1}{s} \right)^n + O_{\mathcal{R}} \left(\left(\frac{1}{s} \right)^{n-1} \right).$$

2. NOTATIONS AND PRELIMINARY RESULTS

For $t \in \mathbb{R}$, let $e(t) = e^{2\pi it}$. We denote by $\omega(n)$ the number of distinct prime divisors of n , and by (a, b, c) the greatest common divisor of a, b, c . Also, let $\sigma_k(n) =$

$\sum_{d|n} d^k$. For a positive integer q and arbitrary integers a_1, \dots, a_{k+1} , denote

$$S(a_1, \dots, a_{k+1}; q) = \sum e\left(\frac{a_1 x_1 + \dots + a_k x_k + a_{k+1} \overline{x_1 \dots x_k}}{q}\right),$$

where the summation runs through the k variables x_i , $1 \leq x_i \leq q - 1$, relatively prime to q . Using Deligne's deep work on Hyper-Kloosterman sums ([4], [7]), Weinstein ([8]) showed that for all integers q, a_1, \dots, a_{k+1} , $q \geq 2$, one has

$$\left|S(a_1, \dots, a_{k+1}; q)\right| \leq t_q(k+1)^{\omega(q)} q^{\frac{k}{2}} (a_1, a_{k+1}, q)^{\frac{1}{2}} (a_2, a_{k+1}, q)^{\frac{1}{2}} \dots (a_k, a_{k+1}, q)^{\frac{1}{2}},$$

where

$$t_q = \begin{cases} 1, & \text{if } q \text{ is odd,} \\ 2^{\frac{k+2}{2}}, & \text{if } q \text{ is even.} \end{cases}$$

A similar bound was also proved by Smith in [5] and [6]. We will need the following lemmas.

Lemma 1. *Let $u \geq 0$, $q \geq 2$, $0 \leq b < a$ be integers such that $(a, q) = 1$ and let*

$$J_q = \begin{cases} \{-\frac{q}{2} + 1, \dots, \frac{q}{2}\}, & \text{if } q \text{ is even,} \\ \{-\frac{q+1}{2}, \dots, \frac{q-1}{2}\}, & \text{if } q \text{ is odd.} \end{cases}$$

Then

$$\left| \sum_{\substack{m \equiv b \pmod{a} \\ 1 \leq m \leq q-1}} e\left(\frac{-um}{q}\right) \right| \ll \frac{q}{1+|r|},$$

where $r \in J_q$ is unique such that $au \equiv r \pmod{q}$.

Proof. Write $m = ak + b$, $0 \leq b < a$. Let $M = \lfloor \frac{q-b-1}{a} \rfloor$. Then

$$\begin{aligned} \left| \sum_{\substack{m \equiv b \pmod{a} \\ 1 \leq m \leq q-1}} e\left(\frac{-um}{q}\right) \right| &= \left| \sum_{k=0}^M e\left(\frac{-uak - ub}{q}\right) \right| = \left| e\left(\frac{-ub}{q}\right) \sum_{k=0}^M e\left(\frac{-uak}{q}\right) \right| \\ &= \left| \sum_{k=0}^M e\left(\frac{-uak}{q}\right) \right|. \end{aligned}$$

Let $z = e\left(\frac{-ua}{q}\right)$. Then

$$1 + z + z^2 + \dots + z^M = \begin{cases} \frac{1-z^{M+1}}{1-z}, & \text{if } z \neq 1 (\Leftrightarrow q \nmid u), \\ M + 1, & \text{if } z = 1 (\Leftrightarrow q \mid u). \end{cases}$$

For $z \neq 1$,

$$\begin{aligned} \left|1 + z + z^2 + \dots + z^M\right| &= \frac{|1 - z^{M+1}|}{|1 - z|} \leq \frac{2}{\left|1 - e\left(\frac{-au}{q}\right)\right|} = \frac{2}{\left|e\left(\frac{au}{2q}\right)\left(1 - e\left(\frac{-au}{q}\right)\right)\right|} \\ &= \frac{2}{\left|e\left(\frac{au}{2q}\right) - e\left(\frac{-au}{2q}\right)\right|} = \frac{2}{2\left|\sin 2\pi \frac{au}{2q}\right|} = \frac{1}{\left|\sin \frac{\pi au}{q}\right|}. \end{aligned}$$

But

$$\frac{1}{|\sin x|} \leq \frac{C}{|x|}, \forall x \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] - \{0\} \text{ (for some } C > 0\text{)}.$$

Now

$$\frac{au}{q} \equiv \frac{r}{q} \pmod{1} \Rightarrow \frac{\pi au}{q} \equiv \frac{\pi r}{q} \pmod{\pi} \Rightarrow \left| \sin \frac{\pi au}{q} \right| = \left| \sin \frac{\pi r}{q} \right|$$

and

$$\left| \frac{\pi r}{q} \right| \leq \frac{\pi}{2}, \text{ so } \frac{1}{\left| \sin \frac{\pi au}{q} \right|} = \frac{1}{\left| \sin \frac{\pi r}{q} \right|} \leq \frac{C}{\left| \frac{\pi r}{q} \right|} = \frac{C}{\pi} \frac{q}{|r|}.$$

For $z = 1$ ($\Leftrightarrow q \mid u \Leftrightarrow r = 0$),

$$\left| \sum_{\substack{m \equiv b \pmod{a} \\ 1 \leq m \leq q-1}} e\left(\frac{-um}{q}\right) \right| = M + 1 = \left[\frac{q-b-1}{a} \right] + 1 \ll q = \frac{q}{1+0},$$

which completes the proof of the lemma. □

Lemma 2.

$$\sum_{r \in J_q} \frac{(r, s, q)^{\frac{1}{2}}}{1 + |r|} \ll (\log q) \sigma_{-\frac{1}{2}}((s, q)) + (s, q)^{\frac{1}{2}} \ll q^\epsilon + (s, q)^{\frac{1}{2}}.$$

Proof.

$$\begin{aligned} \sum_{r \in J_q - \{0\}} \frac{(r, s, q)^{\frac{1}{2}}}{1 + |r|} &\ll \sum_{1 \leq r \leq \frac{q}{2}} \frac{(r, s, q)^{\frac{1}{2}}}{r} = \sum_{d|(s, q)} \sum_{\substack{1 \leq r \leq \frac{q}{2} \\ (r, s, q) = d}} \frac{d^{\frac{1}{2}}}{r} \\ &\leq \left(\sum_{d|(s, q)} d^{\frac{1}{2}} \right) \sum_{\substack{1 \leq r \leq \frac{q}{2} \\ d|r}} \frac{1}{r} = \left(\sum_{d|(s, q)} d^{\frac{1}{2}} \right) \sum_{1 \leq m \leq \left[\frac{q}{2d} \right]} \frac{1}{dm} \\ &= \left(\sum_{d|(s, q)} d^{-\frac{1}{2}} \right) \left(\sum_{1 \leq m \leq \left[\frac{q}{2d} \right]} \frac{1}{m} \right) \ll (\log q) \sigma_{-\frac{1}{2}}((s, q)). \end{aligned}$$

Now we use $d(n) \ll n^\epsilon$ to get the last part of the lemma. □

Corollary 1.

$$\sum_{r \in J_q} \frac{(r, q)^{\frac{1}{2}}}{1 + |r|} = q^{\frac{1}{2}} + O_\epsilon(q^\epsilon).$$

Proof.

$$\sum_{r \in J_q} \frac{(r, q)^{\frac{1}{2}}}{1 + |r|} - q^{\frac{1}{2}} = \sum_{r \in J_q - \{0\}} \frac{(r, q)^{\frac{1}{2}}}{1 + |r|} \ll (\log q) \sigma_{-\frac{1}{2}}(q) \ll (\log q) d(q) \ll_\epsilon q^\epsilon.$$

□

Lemma 3. *Let*

$$S = \sum_{(r_1, \dots, r_{k+1}) \in J_q^{k+1} - \{0\}} \frac{(r_1, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_1|} \cdots \frac{(r_k, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_k|} \frac{1}{1 + |r_{k+1}|}.$$

Then

$$S \ll q^{\epsilon + \frac{k-1}{2}}.$$

Proof. Split the sum S as

$$S = S_1 + S_2, \text{ where } S_1 = \sum_{(r_1, \dots, r_k, 0) \in J_q^{k+1} - \{0\}}, \quad S_2 = \sum_{\substack{(r_1, \dots, r_{k+1}) \in J_q^{k+1} \\ r_{k+1} \neq 0}}.$$

Now

$$\begin{aligned} S_1 &= \sum_{(r_1, \dots, r_k, 0) \in J_q^{k+1} - \{0\}} \frac{(r_1, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_1|} \cdots \frac{(r_k, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_k|} \frac{1}{1 + |r_{k+1}|} \\ &= \sum_{(r_1, \dots, r_k) \in J_q^k - \{0\}} \frac{(r_1, q)^{\frac{1}{2}}}{1 + |r_1|} \cdots \frac{(r_k, q)^{\frac{1}{2}}}{1 + |r_k|} = \left(\sum_{r \in J_q} \frac{(r, q)^{\frac{1}{2}}}{1 + |r|} \right)^k - q^{\frac{k}{2}} \\ &= \left(q^{\frac{1}{2}} + O_\epsilon(q^\epsilon) \right)^k - q^{\frac{k}{2}} = O_\epsilon\left(q^{\frac{k-1}{2} + \epsilon} \right). \end{aligned}$$

Also,

$$\begin{aligned} S_2 &= \sum_{\substack{(r_1, \dots, r_{k+1}) \in J_q^{k+1} \\ r_{k+1} \neq 0}} \frac{(r_1, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_1|} \cdots \frac{(r_k, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_k|} \frac{1}{1 + |r_{k+1}|} \\ &= \sum_{r_{k+1} \in J_q - \{0\}} \frac{1}{1 + |r_{k+1}|} \left(\sum_{r \in J_q} \frac{(r, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r|} \right)^k \\ &\ll \sum_{r_{k+1} \in J_q - \{0\}} \frac{1}{1 + |r_{k+1}|} \left(q^\epsilon + (r_{k+1}, q)^{\frac{1}{2}} \right)^k \\ &\ll \sum_{r_{k+1} \in J_q - \{0\}} \frac{q^\epsilon}{1 + |r_{k+1}|} + \sum_{r_{k+1} \in J_q - \{0\}} \frac{(r_{k+1}, q)^{\frac{k}{2}}}{1 + |r_{k+1}|} \\ &\ll (\log q)q^\epsilon + \sum_{r_{k+1} \in J_q - \{0\}} \frac{(r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_{k+1}|} (r_{k+1}, q)^{\frac{k-1}{2}} \\ &\ll (\log q)q^\epsilon + q^{\frac{k-1}{2}} \sum_{r_{k+1} \in J_q - \{0\}} \frac{(r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_{k+1}|} \ll_\epsilon q^{\frac{k-1}{2} + \epsilon} \end{aligned}$$

by the proof of Corollary 1, and the lemma follows. □

3. PROOF OF THEOREM 1

Proof. We compute the following exponential sum in two ways:

$$T = \frac{1}{q^{k+1}} \sum_{\substack{1 \leq n_1, \dots, n_k \leq q-1 \\ (n_i, q) = 1 \forall i \\ 1 \leq m_j \leq q-1 \\ m_j \equiv b_j \pmod{a_j} \\ 0 \leq u_j \leq q-1 \\ \forall 1 \leq j \leq k+1}} e\left(\frac{u_1(n_1 - m_1) + \cdots + u_k(n_k - m_k) + u_{k+1}(\overline{n_1 \dots n_k} - m_{k+1})}{q} \right).$$

First,

$$T = \frac{1}{q^{k+1}} \sum_{\substack{1 \leq n_1, \dots, n_k \leq q-1 \\ (n_i, q) = 1, \forall i}} \left(\sum_{m_1} \sum_{u_1} e\left(\frac{u_1(n_1 - m_1)}{q}\right) \right) \dots \left(\sum_{m_k} \sum_{u_k} e\left(\frac{u_k(n_k - m_k)}{q}\right) \right) \\ \times \left(\sum_{m_{k+1}} \sum_{u_{k+1}} e\left(\frac{u_{k+1}(\overline{n_1 \dots n_k} - m_{k+1})}{q}\right) \right) = N(\mathbf{a}, \mathbf{b}; q),$$

since

$$\sum_{u_1} e\left(\frac{u_1(n_1 - m_1)}{q}\right) = \begin{cases} q, & \text{if } n_1 = m_1, \\ 0, & \text{else,} \end{cases} \quad \text{so} \\ \sum_{m_1} \sum_{u_1} e\left(\frac{u_1(n_1 - m_1)}{q}\right) = \begin{cases} q, & \text{if } n_1 \equiv b_1 \pmod{a_1}, \\ 0, & \text{else,} \end{cases}$$

and similarly for the other variables. Second,

$$T = \frac{1}{q^{k+1}} \sum_{u_1, \dots, u_{k+1}} \sum_{m_1} \dots \sum_{m_{k+1}} \sum_{n_1, \dots, n_k} e\left(\frac{-u_1 m_1}{q}\right) \dots e\left(\frac{-u_{k+1} m_{k+1}}{q}\right) \\ \times e\left(\frac{u_1 n_1 + \dots + u_k n_k + u_{k+1} \overline{n_1 \dots n_k}}{q}\right) = M + E,$$

where

$$M = \frac{1}{q^{k+1}} \sum_{m_1, \dots, m_{k+1}} \sum_{n_1, \dots, n_k} 1 = \frac{1}{q^{k+1}} \left(\frac{q}{a_1} + O(1)\right) \dots \left(\frac{q}{a_{k+1}} + O(1)\right) \phi(q)^k \\ = \frac{\phi(q)^k}{a_1 \dots a_{k+1}} + O\left(\frac{\phi(q)^k}{q}\right) \text{ and} \\ E = \frac{1}{q^{k+1}} \sum_{(u_1, \dots, u_{k+1}) \neq 0} \left(\sum_{m_1} e\left(\frac{-u_1 m_1}{q}\right) \right) \dots \left(\sum_{m_{k+1}} e\left(\frac{-u_{k+1} m_{k+1}}{q}\right) \right) \\ \times \sum_{\substack{1 \leq n_1, \dots, n_k \leq q-1 \\ (n_i, q) = 1, \forall i}} e\left(\frac{u_1 n_1 + \dots + u_k n_k + u_{k+1} \overline{n_1 \dots n_k}}{q}\right).$$

By using Lemma 1 and Weinsten's bound, we get

$$|E| \ll \frac{1}{q^{k+1}} \sum_{(u_1, \dots, u_{k+1}) \neq 0} \frac{q}{1 + |r_1|} \dots \frac{q}{1 + |r_{k+1}|} (k + 1)^{\omega(q)} \\ \times q^{\frac{k}{2}} (u_1, u_{k+1}, q)^{\frac{1}{2}} \dots (u_k, u_{k+1}, q)^{\frac{1}{2}},$$

where $au_j \equiv r_j \pmod{q}$ for all j and the integers a, q, u_j, r_j satisfy the hypotheses of Lemma 1. It follows that $(u_j, u_{k+1}, q) = (r_j, r_{k+1}, q)$ for all $1 \leq j \leq k$, so

$$\begin{aligned} |E| &\ll (k+1)^{\omega(q)} q^{\frac{k}{2}} \sum_{(u_1, \dots, u_{k+1}) \neq 0} \frac{(u_1, u_{k+1}, q)^{\frac{1}{2}}}{1 + |r_1|} \cdots \frac{(u_k, u_{k+1}, q)^{\frac{1}{2}}}{1 + |r_k|} \frac{1}{1 + |r_{k+1}|} \\ &= (k+1)^{\omega(q)} q^{\frac{k}{2}} \sum_{(r_1, \dots, r_{k+1}) \in J_q^{k+1} - \{0\}} \frac{(r_1, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_1|} \cdots \frac{(r_k, r_{k+1}, q)^{\frac{1}{2}}}{1 + |r_k|} \frac{1}{1 + |r_{k+1}|} \\ &\ll q^{\frac{\log(k+1)}{\log \log q}} q^{\frac{k}{2}} q^{\epsilon + \frac{k-1}{2}} \ll q^{\frac{k}{2}} q^{\epsilon + \frac{k-1}{2}} = q^{\epsilon + k - \frac{1}{2}}. \end{aligned}$$

Here we applied Lemma 3 and used the bound $\omega(n) \ll \frac{\log n}{\log \log n}$. □

4. PROOF OF THEOREM 2

Proof. Let $a_1, \dots, a_{k+1}, b_1, \dots, b_{k+1}, \epsilon$, and q be as in the statement of the theorem. We split the cube $[0, 1]^k$ into little cubes with edge length $1/T$, where T is a positive integer. For each such cube \mathcal{J} one has $\text{vol}(\mathcal{J}) = \frac{1}{T^k}$. We denote by $\mathcal{D} = \mathcal{D}(T)$ the union of those cubes contained in Ω and by $\mathcal{E} = \mathcal{E}(T)$ the union of those cubes which have a nonempty intersection with Ω . Therefore $\mathcal{D}(T) \subset \Omega \subset \mathcal{E}(T)$. We now fix an arbitrary such cube \mathcal{J} and estimate the number $N_{\mathcal{J}}(\mathbf{a}, \mathbf{b}, q)$ of Lehmer points contained in $q\mathcal{J}$. Denote $J = [\alpha_1, \beta_1] \times \cdots \times [\alpha_k, \beta_k]$, with $\beta_j = \alpha_j + \frac{1}{T}$, $1 \leq j \leq k$. Also denote by $N_{\mathcal{D}}(\mathbf{a}, \mathbf{b}, q)$, $N_{\mathcal{E}}(\mathbf{a}, \mathbf{b}, q)$ the number of Lehmer points that lie in $q\mathcal{D}$, respectively in $q\mathcal{E}$. We compute an exponential sum, similar to the one considered in the proof of Theorem 1, in two ways:

$$T = \frac{1}{q^{k+1}} \sum_{\substack{1 \leq n_1, \dots, n_k \leq q-1 \\ (n_i, q) = 1 \forall i \\ \alpha_j q \leq m_j \leq \beta_j q \\ m_j \equiv b_j \pmod{a_j} \\ 0 \leq u_j \leq q-1 \\ \forall 1 \leq j \leq k+1}} e\left(\frac{u_1(n_1 - m_1) + \cdots + u_k(n_k - m_k) + u_{k+1}(\overline{n_1 \cdots n_k} - m_{k+1})}{q}\right).$$

First,

$$\begin{aligned} T &= \frac{1}{q^{k+1}} \sum_{\substack{1 \leq n_1, \dots, n_k \leq q-1 \\ (n_i, q) = 1, \forall i}} \left(\sum_{m_1} \sum_{u_1} e\left(\frac{u_1(n_1 - m_1)}{q}\right) \right) \cdots \left(\sum_{m_k} \sum_{u_k} e\left(\frac{u_k(n_k - m_k)}{q}\right) \right) \\ &\quad \times \left(\sum_{m_{k+1}} \sum_{u_{k+1}} e\left(\frac{u_{k+1}(\overline{n_1 \cdots n_k} - m_{k+1})}{q}\right) \right) = N_{\mathcal{J}}(\mathbf{a}, \mathbf{b}; q), \end{aligned}$$

since

$$\begin{aligned} \sum_{u_1} e\left(\frac{u_1(n_1 - m_1)}{q}\right) &= \begin{cases} q, & \text{if } n_1 = m_1, \\ 0, & \text{else,} \end{cases} \quad \text{so} \\ \sum_{m_1} \sum_{u_1} e\left(\frac{u_1(n_1 - m_1)}{q}\right) &= \begin{cases} q, & \text{if } n_1 \equiv b_1 \pmod{a_1}, \\ 0, & \text{else.} \end{cases} \end{aligned}$$

Second,

$$T = \frac{1}{q^{k+1}} \sum_{u_1, \dots, u_{k+1}} \sum_{m_1} \cdots \sum_{m_{k+1}} \sum_{n_1, \dots, n_k} e\left(\frac{-u_1 m_1}{q}\right) \cdots e\left(\frac{-u_{k+1} m_{k+1}}{q}\right) \\ \times e\left(\frac{u_1 n_1 + \cdots + u_k n_k + u_{k+1} \overline{n_1 \cdots n_k}}{q}\right) = M + E,$$

where

$$M = \frac{1}{q^{k+1}} \sum_{m_1, \dots, m_{k+1}} \sum_{n_1, \dots, n_k} 1 = \frac{1}{q^{k+1}} \left(\frac{q}{a_1 T} + O(1)\right) \\ \cdots \left(\frac{q}{a_k T} + O(1)\right) \left(\frac{q}{a_{k+1}} + O(1)\right) \phi(q)^k \\ = \frac{\phi(q)^k}{a_1 \cdots a_{k+1} T^k} + O\left(\frac{\phi(q)^k}{q}\right) = \text{vol}(\mathcal{J}) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O\left(\frac{\phi(q)^k}{q}\right)$$

and

$$E = \frac{1}{q^{k+1}} \sum_{(u_1, \dots, u_{k+1}) \neq 0} \left(\sum_{m_1} e\left(\frac{-u_1 m_1}{q}\right)\right) \cdots \left(\sum_{m_{k+1}} e\left(\frac{-u_{k+1} m_{k+1}}{q}\right)\right) \\ \times \sum_{\substack{1 \leq n_1, \dots, n_k \leq q-1 \\ (n_i, q) = 1, \forall i}} e\left(\frac{u_1 n_1 + \cdots + u_k n_k + u_{k+1} \overline{n_1 \cdots n_k}}{q}\right).$$

The estimates used in the proof of Theorem 1 to bound E continue to hold true in this second case, and we get $|E| \ll q^{k-\frac{1}{2}+\epsilon}$. We deduce that

$$N_{\mathcal{J}}(\mathbf{a}, \mathbf{b}, q) = \text{vol}(\mathcal{J}) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O_{k, \epsilon}\left(q^{k-\frac{1}{2}+\epsilon}\right).$$

Since there are at most T^k such small cubes in \mathcal{D} and in \mathcal{E} , we obtain

$$N_{\mathcal{D}}(\mathbf{a}, \mathbf{b}, q) = \text{vol}(\mathcal{D}) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O_{k, \epsilon}\left(T^k q^{k-\frac{1}{2}+\epsilon}\right) \quad \text{and} \\ N_{\mathcal{E}}(\mathbf{a}, \mathbf{b}, q) = \text{vol}(\mathcal{E}) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O_{k, \epsilon}\left(T^k q^{k-\frac{1}{2}+\epsilon}\right).$$

We obviously have $N_{\mathcal{D}}(\mathbf{a}, \mathbf{b}, q) \leq N_{\Omega}(\mathbf{a}, \mathbf{b}, q) \leq N_{\mathcal{E}}(\mathbf{a}, \mathbf{b}, q)$, so that

$$\text{vol}(\mathcal{D}) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O_{k, \epsilon}\left(T^k q^{k-\frac{1}{2}+\epsilon}\right) \leq N_{\Omega}(\mathbf{a}, \mathbf{b}, q) \\ \leq \text{vol}(\mathcal{E}) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O_{k, \epsilon}\left(T^k q^{k-\frac{1}{2}+\epsilon}\right).$$

By the Lipschitz principle for the number of integer points in a domain ([3]), we know that

$$\text{vol}(\mathcal{D}) = \text{vol}(\Omega) + O_{\Omega}\left(\frac{1}{T}\right) \quad \text{and} \quad \text{vol}(\mathcal{E}) = \text{vol}(\Omega) + O_{\Omega}\left(\frac{1}{T}\right),$$

so

$$N_{\Omega}(\mathbf{a}, \mathbf{b}, q) = \text{vol}(\Omega) \frac{\phi(q)^k}{a_1 \cdots a_{k+1}} + O_{\Omega}\left(\frac{q^k}{T}\right) + O_{k, \epsilon}\left(T^k q^{k-\frac{1}{2}+\epsilon}\right).$$

We now balance the two error terms by choosing T such that $T^{k+1} = q^{\frac{1}{2}}$, i.e. $T = q^{\frac{1}{2(k+1)}}$. We obtain

$$N_{\Omega}(\mathbf{a}, \mathbf{b}, q) = \text{vol}(\Omega) \frac{\phi(q)^k}{a_1 \dots a_{k+1}} + O_{k, \Omega, \epsilon} \left(q^{k - \frac{1}{2(k+1)} + \epsilon} \right),$$

which completes the proof of Theorem 2. □

ACKNOWLEDGMENT

The authors are grateful to the referee for many useful comments and suggestions.

REFERENCES

- [1] C. Cobeli, A. Zaharescu, *Generalization of a problem of Lehmer*, Manuscripta Math. **104** (2001), no. 3, 301–307. MR1828876 (2003a:11100)
- [2] R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, Berlin (1981) (second edition 1994). MR1299330 (96e:11002)
- [3] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183. MR0043821 (13:323d)
- [4] P. Deligne, *Seminaire Geometrie Algebrique 4 $\frac{1}{2}$* , Lecture Notes **569** (1977), 221–228. MR0463174 (57:3132)
- [5] R. A. Smith, *On n -dimensional Kloosterman sums*, J. Number Theory **11** (1979), 324–343. MR0544261 (80i:10052)
- [6] R. A. Smith, *A generalization of Kuznietsov's identity for Kloosterman sums*, C. R. Math. Rep. Acad. Sci. Canada **Vol. II** (1980), 315–320. MR0600568 (82j:10068)
- [7] A. Weil, *On some exponential sums*, Proc Nat. Acad. Sci. U.S.A. **34** (1948), 204–207. MR0027006 (10:234e)
- [8] L. Weinstein, *The hyper-Kloosterman sum*, Enseign. Math. (2) **27** (1981), no. 1-2, 29–40. MR0630958 (83b:10046)
- [9] W. Zhang, *On a problem of D. H. Lehmer and its generalization*, Compositio Math. **86** (1993), no. 3, 307–316. MR1219630 (94f:11104)
- [10] W. Zhang, *A problem of D. H. Lehmer and its generalization II*, Compositio Math. **91** (1994), no. 1, 47–56. MR1273925 (95f:11079)
- [11] W. Zhang, *On the difference between a D. H. Lehmer number and its inverse modulo q* , Acta Arith. **68** (1994), no. 3, 255–263. MR1308126 (96a:11100)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, ALTGELD HALL, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801

E-mail address: alkan@math.uiuc.edu

INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, P.O. BOX 1-764, 70700 BUCHAREST, ROMANIA – AND – DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, ALTGELD HALL, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801

E-mail address: fstan@math.uiuc.edu

INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, P.O. BOX 1-764, 70700 BUCHAREST, ROMANIA – AND – DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, ALTGELD HALL, 1409 W. GREEN STREET, URBANA, ILLINOIS 61801

E-mail address: zaharesc@math.uiuc.edu