Proceedings of the Edinburgh Mathematical Society (2003) **46**, 185–203 ©
DOI:10.1017/S0013091501000724 Printed in the United Kingdom

DISTRIBUTION OF GAPS BETWEEN THE INVERSES mod q

C. COBELI[1], M. VÂJÂITU[1] AND A. ZAHARESCU[1,2]

[1] *Institute of Mathematics of the Romanian Academy, PO Box 1-764, Bucharest 70700, Romania*
(ccobeli@stoilow.imar.ro; mvajaitu@stoilow.imar.ro)
[2] *Department of Mathematics, University of Illinois at Urbana-Champaign, Altgeld Hall, 1409 W. Green St., Urbana, IL 61801, USA* (zaharesc@math.uiuc.edu)

(Received 23 January 2001)

Abstract Let q be a positive integer, let $\mathcal{I} = \mathcal{I}(q)$ and $\mathcal{J} = \mathcal{J}(q)$ be subintervals of integers in $[1, q]$ and let $\mathcal{M}$ be the set of elements of $\mathcal{I}$ that are invertible modulo q and whose inverses lie in $\mathcal{J}$. We show that when q approaches infinity through a sequence of values such that $\varphi(q)/q \to 0$, the r-spacing distribution between consecutive elements of $\mathcal{M}$ becomes exponential.

Keywords: Poissonian distribution; inverses; exponential sums

AMS 2000 *Mathematics subject classification:* Primary 11K06; 11B05; 11N69

1. Introduction

There are many sequences of interest in number theory that are believed to have a Poissonian distribution, but in very few cases has one been able to prove the relevant conjectures. We mention first of all the classical results of Hooley [**10–13**] on the distribution of residue classes which are coprime with a large modulus q, which will be discussed in more detail below, and also the well-known conditional result of Gallagher [**8**] on the distribution of prime numbers.

More recently, in [**4**], it was proved that the distribution of primitive roots mod p becomes Poissonian as $p \to \infty$ such that $\varphi(p-1)/p \to 0$, while the distribution of squares modulo highly composite numbers was shown to be Poissonian by Kurlberg and Rudnick in [**14**]. Fractional parts of polynomial sequences $\{\alpha P(n)\}$, $n \in \boldsymbol{N}$, provide another class of sequences which are believed to have a Poissonian distribution. Rudnick and Sarnak [**16**] proved that for almost all $\alpha \in \boldsymbol{R}$ the pair correlation of this sequence is Poissonian (see also [**1**]). Here the degree of P is at least 2. If $\deg P = 1$, the distribution is not Poissonian. In fact in this case the gaps between the fractional parts $\{\alpha P(n)\}$, $1 \leqslant n \leqslant N$, take at most three values (see Sós [**17**] and Świerczkowski [**18**]). In this paper our aim is to find out whether the inverses, modulo a large number q, of integers from an interval have a Poissonian distribution when the interval's length is large enough.

To make things more precise, let q be an integer and let $\mathcal{I} = \mathcal{I}(q)$ and $\mathcal{J} = \mathcal{J}(q)$ be subintervals of integers in $[1, q]$. For any integer $n \in [1, q]$, $(n, q) = 1$, we denote by $\bar{n}$ the inverse of $n \bmod q$, that is the unique integer from $\{1, \dots, q\}$ satisfying $n\bar{n} \equiv 1 \pmod q$. We consider the set

$$\mathcal{M} = \mathcal{M}(\mathcal{I}, \mathcal{J}, q) = \{\gamma \in \mathcal{I} : (\gamma, q) = 1,\ \bar{\gamma} \in \mathcal{J}\}$$

and suppose its elements $\gamma_1, \gamma_2, \dots, \gamma_M$ are sorted in ascending order. (Here $M = |\mathcal{M}(\mathcal{I}, \mathcal{J}, q)|$ is the cardinality of $\mathcal{M}$.) One might expect that if $|\mathcal{I}|$ and $|\mathcal{J}|$ are sufficiently large, then the elements of $\mathcal{M}$ are randomly distributed. Let

$$\theta = \frac{\varphi(q)}{q} \frac{|\mathcal{J}|}{q}.$$

We think of θ as being the probability that a randomly chosen integer from $[1, q]$ is invertible modulo q (i.e. it is coprime with q) and that its inverse modulo q lies in $\mathcal{J}$. Then M should be about $|\mathcal{I}|\theta$ and the average distance between two consecutive elements of $\mathcal{M}$ should be $|\mathcal{I}|/M \sim 1/\theta$. Thus, on these probabilistic grounds, concerning the spacing between consecutive members of $\mathcal{M}$ one might conjecture that

$$\#\left\{\gamma_i \in \mathcal{M} : \gamma_i - \gamma_{i-1} > \frac{\lambda}{\theta}\right\} \sim \mathrm{e}^{-\lambda} |\mathcal{I}| \theta,$$

for each fixed $\lambda > 0$. In particular, the proportion of gaps that are greater than the average should be about e^{-1}. This may be regarded as a generalization of the problem studied by Hooley in [**11**] and [**12**], who investigated the case $\mathcal{I} = [1, q]$, $\mathcal{J} = [1, q]$, that is the set of reduced residue classes. He proved that the r-spacing distribution of the gaps between reduced residue classes becomes exponential as $q \to \infty$ such that $\varphi(q)/q \to 0$. In this paper we show that this property is inherited by subsets naturally constructed by the *taking the inverse* operation.

In [**5**], Erdös originally made a series of conjectures concerning the distribution of the residue classes, the most celebrated of which was the special case $\alpha = 2$ of the bound

$$\sum_{i=1}^{\varphi(q)-1} (a_{i+1} - a_i)^{\alpha} = O\left\{q\left(\frac{\varphi(q)}{q}\right)^{\alpha-1}\right\}, \tag{1.1}$$

where $a_1, \dots, a_{\varphi(q)}$ are the reduced residues modulo q. Hooley proved (1.1) for $0 \leqslant \alpha < 2$ in [**10**], and in [**11**] he calculated the distribution of the consecutive differences $a_{i+1} - a_i$, showing that they behave statistically like a gamma-random variable with parameter 1. As a consequence he showed that for $0 \leqslant \alpha < 2$ the estimate (1.1) can be replaced by an asymptotic formula when $\varphi(q)/q \to 0$. In [**12**], Hooley proved more generally that for any $r \geqslant 1$, the groups of r consecutive gaps between the elements of the sequence $a_1, \dots, a_{\varphi(q)}$ are statistically independent, in the sense explained below. Later on, in a famous article [**15**], Montgomery and Vaughan settled the conjecture by proving (1.1) for all $\alpha > 0$.

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

Here we show that the distribution function calculated by Hooley remains the same if one picks up in the sampling only reduced residues from $\mathcal{M}$. To see this, for $\lambda_1, \dots, \lambda_r > 0$ we define

$$g(\lambda_1, \dots, \lambda_r) = g(\lambda_1, \dots, \lambda_r; \mathcal{I}, \mathcal{J}, q)$$

to be the proportion of $\gamma_i \in \mathcal{M}$ which satisfies $\gamma_{i+j} - \gamma_{i+j-1} \leqslant \lambda_j/\theta$, for $1 \leqslant j \leqslant r$. Based on the presumption that the inverses from a sufficiently large interval are randomly distributed in $[1, q]$, one would conjecture that the differences of consecutive elements of $\mathcal{M}$ are independent of one another, that is, one expects to have

$$g(\lambda_1, \dots, \lambda_r) \approx g(\lambda_1) \dots g(\lambda_r).$$

Theorem 1.1 below shows that this is true, providing additionally an explicit expression for $g(\lambda_1, \dots, \lambda_r)$. It also confirms that the same distribution is inherited by shorter intervals, and that the distribution of r-groups of consecutive differences is essentially independent of q as $\varphi(q)/q \to 0$. (This was also conjectured by Erdös (see [**6**]) when $\mathcal{I} = \mathcal{J} = [1, q]$ were complete intervals and q was a product $q = 2 \cdot 3 \cdot \cdots \cdot p$ of consecutive primes.)

Theorem 1.1. *Let $\lambda_1, \dots, \lambda_r > 0$. Then, as $q \to \infty$ through a sequence of values such that $\varphi(q)/q \to 0$ and the lengths of the intervals $\mathcal{I}$ and $\mathcal{J}$ grow with q satisfying the conditions $|\mathcal{I}| > q^{1-(2/9(\log\log q)^{1/2})}$ and $|\mathcal{J}| > q^{1-(1/(\log\log q)^2)}$, we have*

$$\lim_{q\to\infty} g(\lambda_1, \dots, \lambda_r; \mathcal{I}, \mathcal{J}, q) = (1 - \mathrm{e}^{-\lambda_1}) \cdots (1 - \mathrm{e}^{-\lambda_r}).$$

2. Bounds for some exponential sums

Let $\mathcal{A} = \{a_1, \dots, a_s\}$ be a set of integers and $\boldsymbol{k} = (k_1, \dots, k_s)$ a vector with integer components. If x is an integer, we write $\boldsymbol{x} = (x, \dots, x)$, $\boldsymbol{x} + \boldsymbol{a} = (x + a_1, \dots, x + a_s)$ and $\overline{\boldsymbol{x} + \boldsymbol{a}} = (\overline{x + a_1}, \dots, \overline{x + a_s})$. Here and later the bar represents the inverse modulo q (most often) or modulo an integer understood from the context.

We consider the following exponential sum:

$$S(u, \boldsymbol{k}, \mathcal{A}, q) = \sideset{}{'}\sum_{x=1}^{q} \mathrm{e}\biggl(\frac{ux + \boldsymbol{k} \cdot \overline{\boldsymbol{x} + \boldsymbol{a}}}{q}\biggr).$$

Here $\sum'$ means that the summation is only over those x for which $(x + a, q) = 1$ for all $a \in \mathcal{A}$. Using the Bombieri–Weil inequality [**2**, Theorem 6], we obtain (see [**3**]) the following result.

Lemma 2.1. *Suppose that $a_1, \dots, a_s$ are distinct* mod p *and $p \nmid (u, k_1, \dots, k_s)$. Then*

$$|S(u, \boldsymbol{k}, \mathcal{A}, p)| \leqslant 2s\sqrt{p}.$$

These exponential sums behave nicely and, in particular, there is some sort of multiplicity. Using this property, in order to get bounds for a general modulus, one needs estimates only for sums with a prime power modulus. This subject was also treated in [**3**], from which we quote the following three lemmas. The proofs of these lemmas are based on the method used by Esterman in [**7**].

Lemma 2.2. *Let $q_1, \dots, q_r$ be pairwise coprime positive integers, $q = q_1 \dots q_r$, $\hat{q}_j = q/q_j$, and denote by $\bar{x}^{(j)}$ the inverse of x modulo q_j, that is $1 \leqslant \bar{x}^{(j)} \leqslant q_j - 1$ and $x\bar{x}^{(j)} \equiv 1 \pmod{q_j}$. Then*

$$S(u, \boldsymbol{k}, \mathcal{A}, q) = \prod_{j=1}^{r} S(\bar{\hat{q}}_j^{(j)} u, \bar{\hat{q}}_j^{(j)} \boldsymbol{k}, \mathcal{A}, q_j). \tag{2.1}$$

Let $L(y)$ be the polynomial given by

$$L(y) = \left(u - \sum_{j=1}^{s} \frac{k_j}{(y + a_j)^2}\right) \prod_{j=1}^{s} (y + a_j)^2.$$

Lemma 2.3. *Let $n \geqslant 2$ and $0 \leqslant r \leqslant [\frac{1}{2}n]$ be integers. Suppose that all the coefficients of $L(y)$ are divisible by p^r but at least one of them is not divisible by p^{r+1}. Then*

$$|S(u, \boldsymbol{k}, \mathcal{A}, p^n)| \leqslant 2^{2s-1} p^{n-(([n/2]-r)/(2s))}.$$

Since from the hypothesis of Lemma 2.3 it follows that $p^r \leqslant (p^{[n/2]}, u)$, we have the following.

Lemma 2.4. *Let $n \geqslant 2$. Then*

$$|S(u, \boldsymbol{k}, \mathcal{A}, p^n)| \leqslant 2^{2s-1} (p^{[n/2]}, u)^{1/(2s)} p^{n-([n/2]/(2s))}.$$

We also need partial sums, where the variable of summation runs over $\mathcal{I}$, a subinterval of integers in $[1, q]$. We write

$$S_{\mathcal{I}}(u, \boldsymbol{k}, \mathcal{A}, q) = \sum_{x \in \mathcal{I}'} \mathrm{e}\left(\frac{ux + \boldsymbol{k} \cdot \overline{\boldsymbol{x} + \boldsymbol{a}}}{q}\right),$$

where $\mathcal{I}' = \{x \in \mathcal{I} : (x + a, q) = 1 \text{ for all } a \in \mathcal{A}\}$. The estimation of the incomplete sums can be reduced to that of complete ones. To see this, we write

$$S_{\mathcal{I}}(u, \boldsymbol{k}, \mathcal{A}, q) = \frac{1}{q} \sideset{}{'}\sum_{x=1}^{q} \mathrm{e}\left(\frac{ux + \boldsymbol{k} \cdot \overline{\boldsymbol{x} + \boldsymbol{a}}}{q}\right) \sum_{z \in \mathcal{I}} \sum_{l=1}^{q} \mathrm{e}\left(l \frac{x - z}{q}\right).$$

Inverting the order of summation, we obtain

$$\begin{aligned} S_{\mathcal{I}}(u, \boldsymbol{k}, \mathcal{A}, q) &= \frac{1}{q} \sum_{l=1}^{q} \sum_{z \in \mathcal{I}} \mathrm{e}\left(\frac{-lz}{q}\right) \sideset{}{'}\sum_{x=1}^{q} \mathrm{e}\left(\frac{(u + l)x + \boldsymbol{k} \cdot \overline{\boldsymbol{x} + \boldsymbol{a}}}{q}\right) \\ &= \frac{|\mathcal{I}|}{q} S(u, \boldsymbol{k}, \mathcal{A}, q) + \frac{1}{q} \sum_{l=1}^{q-1} \sum_{z \in \mathcal{I}} \mathrm{e}\left(\frac{-lz}{q}\right) S(u + l, \boldsymbol{k}, \mathcal{A}, q). \end{aligned} \tag{2.2}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

3. The s-tuple problem

The key to obtaining Theorem 1.1 is to solve the so-called s-tuple problem. In this section our aim is to estimate $N_{\mathcal{I}}(\mathcal{A}) = N_{\mathcal{I}}(\mathcal{A}; \mathcal{J}, q)$, the number of $n \in \mathcal{I}$ for which all the components of the s-tuple $(n + a_1, \dots, n + a_s)$ have inverses modulo q in $\mathcal{J}$. If $\mathcal{I} = [1, q]$, we omit the indicial notation and for short write $N(\mathcal{A})$ instead of $N_{[1,q]}(\mathcal{A})$.

For q large and $\mathcal{A}$ a set of integers distinct modulo q, a probabilistic argument leads us to expect that $N_{\mathcal{I}}(\mathcal{A})$ is about $|\mathcal{I}|\theta^{|\mathcal{A}|}$ when q is prime, and for general q it is a similar term multiplied by a factor involving the prime factors of q. This is confirmed by Theorem 5.5 below. The first step in the proof is to write $N_{\mathcal{I}}(\mathcal{A})$ in terms of the exponential sums defined above. For this we introduce the characteristic function

$$\delta(x) = \begin{cases} 1 & \text{if } \bar{x} \in \mathcal{J}, \\ 0 & \text{if } \bar{x} \notin \mathcal{J}. \end{cases} \tag{3.1}$$

This can be written as an exponential sum as follows:

$$\delta(x) = \frac{1}{q} \sum_{k=1}^{q} \sum_{y \in \mathcal{J}} \mathrm{e}\biggl(k \frac{xy - 1}{q}\biggr).$$

If $(x, q) = 1$, this is

$$\delta(x) = \frac{1}{q} \sum_{k=1}^{q} \sum_{y \in \mathcal{J}} \mathrm{e}\biggl(k \frac{y - \bar{x}}{q}\biggr). \tag{3.2}$$

Then, by the definition of the $N_{\mathcal{I}}(\mathcal{A})$ and (3.2) we have

$$\begin{aligned} N_{\mathcal{I}}(\mathcal{A}) &= \sum_{x \in \mathcal{I}} \prod_{a \in \mathcal{A}} \delta(x + a) \\ &= \frac{1}{q^s} \sum_{x \in \mathcal{I}'} \prod_{a \in \mathcal{A}} \sum_{k=1}^{q} \sum_{y \in \mathcal{J}} \mathrm{e}\biggl(k \frac{y - \overline{x + a}}{q}\biggr). \end{aligned}$$

Inverting the order of summation, we get

$$\begin{aligned} N_{\mathcal{I}}(\mathcal{A}) &= \frac{1}{q^s} \sum_{x \in \mathcal{I}'} \sum_{k_1=1}^{q} \cdots \sum_{k_s=1}^{q} \sum_{y_1 \in \mathcal{J}} \cdots \sum_{y_s \in \mathcal{J}} \mathrm{e}\biggl(k_1 \frac{y_1 - \overline{x + a_1}}{q}\biggr) \cdots \mathrm{e}\biggl(k_s \frac{y_s - \overline{x + a_s}}{q}\biggr) \\ &= \frac{1}{q^s} \sum_{k_1=1}^{q} \sum_{y_1 \in \mathcal{J}} \mathrm{e}\biggl(\frac{k_1 y_1}{q}\biggr) \cdots \sum_{k_s=1}^{q} \sum_{y_s \in \mathcal{J}} \mathrm{e}\biggl(\frac{k_s y_s}{q}\biggr) S_{\mathcal{I}}(0, -\boldsymbol{k}, \mathcal{A}, q), \end{aligned}$$

where $\boldsymbol{k} = (k_1, \dots, k_s)$. Here the main contribution is (we do not yet know that it is the dominant term) given by the term with $k_1 = \cdots = k_s = q$. Isolating this term we obtain

$$N_{\mathcal{I}}(\mathcal{A}) = \frac{|\mathcal{I}'|\,|\mathcal{J}|^s}{q^s} + \frac{1}{q^s} {\prod_{j=1}^{s}}' \biggl\{ \sum_{k_j=1}^{q} \sum_{y_j \in \mathcal{J}} \mathrm{e}\biggl(\frac{k_j y_j}{q}\biggr) \biggr\} S_{\mathcal{I}}(0, -\boldsymbol{k}, \mathcal{A}, q), \tag{3.3}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

where the prime in the product means that the terms with $k_1 = \cdots = k_s = q$ are excluded.

In the next section we show that $N_{\mathcal{I}}(\mathcal{A})$ depends proportionally on $|\mathcal{I}|$, so it is enough to estimate $N(\mathcal{A})$.

4. Reduction to the case $\mathcal{I} = [1, q]$

We need an estimate for $|\mathcal{I}'|$. Following Hooley [**11**], we introduce

$$\nu(d, \mathcal{A}) = \{n : 1 \leqslant n \leqslant d,\ (n + a_1) \cdots (n + a_s) \equiv 0 \ (\mathrm{mod}\, d)\}.$$

Clearly, if p is prime, then

$$1 \leqslant \nu(p, \mathcal{A}) \leqslant \min(p, s). \tag{4.1}$$

Note that $\nu(d, \mathcal{A})$ is multiplicative, that is

$$\nu(d_1 d_2, \mathcal{A}) = \nu(d_1, \mathcal{A})\nu(d_2, \mathcal{A}) \tag{4.2}$$

whenever $(d_1, d_2) = 1$. Also note that if p is prime, then $\nu(p, \mathcal{A})$ equals the number of $a \in \mathcal{A}$ that are distinct modulo p. We denote

$$\Pi_1(q, \mathcal{A}) = \prod_{p|q} \biggl(1 - \frac{\nu(p, \mathcal{A})}{p}\biggr). \tag{4.3}$$

If $\Pi_1(q, \mathcal{A}) \neq 0$, then using (4.1) we get the following trivial lower bound for $\Pi_1(q, \mathcal{A})$:

$$\frac{1}{q} \leqslant \prod_{p|q} \frac{1}{p} = \prod_{p|q} \biggl(1 - \frac{p-1}{p}\biggr) \leqslant \Pi_1(q, \mathcal{A}). \tag{4.4}$$

A better bound is given by the following lemma.

Lemma 4.1. *Suppose* $0 < s < (\log q)^{1/3}$ *and* $\Pi_1(q, \mathcal{A}) \neq 0$. *Then for* q *large enough one has*

$$\Pi_1(q, \mathcal{A}) \geqslant q^{-3/((\log q)^{1/3})}.$$

Proof. We estimate the factors of the product (4.3) differently according to their size. Correspondingly, we split $\Pi_1(q, \mathcal{A})$ as follows:

$$\Pi_1(q, \mathcal{A}) = \prod_{\substack{p|q \\ p<(\log q)^{2/3}}} \biggl(1 - \frac{\nu(p, \mathcal{A})}{p}\biggr) \prod_{\substack{p|q \\ p\geqslant(\log q)^{2/3}}} \biggl(1 - \frac{\nu(p, \mathcal{A})}{p}\biggr) = P_1 P_2, \tag{4.5}$$

say. Since $\nu(p, \mathcal{A}) \leqslant p - 1$, for the first product we have

$$P_1 \geqslant \prod_{\substack{p|q \\ p<(\log q)^{2/3}}} \biggl(1 - \frac{p-1}{p}\biggr) \geqslant \prod_{p<(\log q)^{2/3}} \frac{1}{p}. \tag{4.6}$$

A trivial estimate for $\pi(x)$, the number of primes $\leqslant x$, gives

$$\prod_{p\leqslant x} p \leqslant x^{\pi(x)} \leqslant x^{2x/(\log x)} = \mathrm{e}^{2x}, \tag{4.7}$$

for $x \geqslant 2$. By (4.6) and (4.7) we obtain

$$P_1 \geqslant \mathrm{e}^{-2(\log q)^{2/3}} = q^{-2/((\log q)^{1/3})}. \tag{4.8}$$

By (4.1), for P_2 we have

$$P_2 \geqslant \prod_{\substack{p\mid q\\ p\geqslant(\log q)^{2/3}}} \left(1-\frac{s}{p}\right) \geqslant \left(1-\frac{s}{(\log q)^{2/3}}\right)^{\omega(q)} \geqslant \mathrm{e}^{-\mathrm{e}s\omega(q)/((\log q)^{2/3})}, \tag{4.9}$$

because $1-x \geqslant \mathrm{e}^{-\mathrm{e}x}$ for any $x \in [0, 1/\mathrm{e}]$. Here $\omega(q)$ is the number of distinct prime factors of q. It is well known that

$$1 \leqslant \omega(q) \leqslant \frac{2\log q}{\log\log q} \tag{4.10}$$

for q large enough. Using (4.9), (4.10) and our hypothesis on s, we obtain

$$P_2 \geqslant \exp\left[-\frac{2\mathrm{e}\log q}{\log\log q}\frac{(\log q)^{1/3}}{(\log q)^{2/3}}\right] = q^{-2e/((\log\log q)(\log q)^{1/3})}. \tag{4.11}$$

The lemma then follows by (4.5), (4.8) and (4.11). □

The next lemma gives an estimate for the number of admissible s-tuples, that is those s-tuples with all the components invertible modulo q.

Lemma 4.2. *Let $\mathcal{A} = \{a_1, \dots, a_s\}$ be a set of integers, $\mathcal{I}$ a subinterval of integers in $[1, q]$, and denote $\mathcal{I}' = \{n \in \mathcal{I} : (n + a, q) = 1$ for all $a \in \mathcal{A}\}$. Then*

$$||\mathcal{I}'| - \mathit{\Pi}_1(q,\mathcal{A})|\mathcal{I}|| \leqslant (2s)^{\omega(q)} \tag{4.12}$$

and

$$|[1,q]'| = q\mathit{\Pi}_1(q,\mathcal{A}). \tag{4.13}$$

Proof. Let $P(x) = (x + a_1)\cdots(x + a_s)$. Then we have

$$\begin{aligned} |\mathcal{I}'| &= \sum_{\substack{x\in\mathcal{I}\\ (P(x),q)=1}} 1 = \sum_{x\in\mathcal{I}} \sum_{\substack{d\mid P(x)\\ d\mid q}} \mu(d) \\ &= \sum_{d\mid q} \mu(d) \sum_{\substack{x\in\mathcal{I}\\ P(x)\equiv 0 \pmod d}} 1 \\ &= \sum_{d\mid q} \mu(d)\left(\frac{|\mathcal{I}|}{d} + \theta_d\right) \sum_{\substack{1\leqslant x\leqslant d\\ P(x)\equiv 0 \pmod d}} 1, \end{aligned}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

where θ_d are real numbers with $|\theta_d| \leqslant 1$. Using the multiplicativity of the sum

$$\sum_{\substack{1\leqslant x\leqslant d\\ P(x)\equiv 0 \pmod d}} 1,$$

which coincides with $\nu(d,\mathcal{A})$, we obtain

$$\begin{aligned} |\mathcal{I}'| &= |\mathcal{I}| \sum_{d|q} \frac{\mu(d)}{d}\nu(d,\mathcal{A}) + \sum_{d|q}\mu(d)\theta_d\nu(d,\mathcal{A}) \\ &= |\mathcal{I}| \prod_{p|q}\left(1-\frac{\nu(p,\mathcal{A})}{p}\right) + \sum_{d|q}\mu(d)\theta_d\nu(d,\mathcal{A}). \end{aligned} \tag{4.14}$$

We bound the last sum trivially:

$$\begin{aligned} \left|\sum_{d|q}\mu(d)\theta_d\nu(d,\mathcal{A})\right| &\leqslant \sum_{d|q}\nu(d,\mathcal{A}) = \prod_{p|q}(1+\nu(p,\mathcal{A})) \\ &\leqslant \prod_{p|q}(1+s) \leqslant (1+s)^{\omega(q)} \leqslant (2s)^{\omega(q)}. \end{aligned} \tag{4.15}$$

By combining (4.3), (4.14) and (4.15) we obtain (4.12).

Observing that if $\mathcal{I} = [1,q]$ then in the above calculation $\theta_d = 0$ for all $d|q$, we see that (4.13) follows as well. □

We return now to the s-tuple problem. By (3.3) we deduce that

$$\left|N_{\mathcal{I}}(\mathcal{A}) - \frac{|\mathcal{I}|}{q}N(\mathcal{A})\right| \leqslant E_1 + E_2, \tag{4.16}$$

where

$$E_1 = \left|\frac{|\mathcal{I}'|\,|\mathcal{J}|^s}{q^s} - \frac{|\mathcal{I}|}{q}\frac{|[1,q]'|\,|\mathcal{J}|^s}{q^s}\right|$$

and

$$E_2 = \left|\frac{1}{q^s}\prod_{j=1}^{s}{}'\left(\sum_{k_j=1}^{q}\sum_{y_j\in\mathcal{J}} \mathrm{e}\left(\frac{k_j y_j}{q}\right)\right)\left(S_{\mathcal{I}}(0,-\boldsymbol{k},\mathcal{A},q) - \frac{|\mathcal{I}|}{q}S(0,-\boldsymbol{k},\mathcal{A},q)\right)\right|.$$

To bound E_1 we use Lemma 4.2 to obtain

$$E_1 = \frac{|\mathcal{J}|^s}{q^s}\left||\mathcal{I}|\Pi_1(q,\mathcal{A}) + \theta_1(2s)^{\omega(q)} - \frac{|\mathcal{I}|}{q}q\Pi_1(q,\mathcal{A})\right|,$$

where θ_1 is a real number with $|\theta_1| \leqslant 1$. This gives

$$E_1 \leqslant \frac{|\mathcal{J}|^s}{q^s}(2s)^{\omega(q)}. \tag{4.17}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

To obtain an upper bound for E_2 we first use (2.2) to replace the incomplete exponential sums by complete ones to get

$$E_2 = \left|\frac{1}{q^s}\prod_{j=1}^{s}{}'\left\{\sum_{k_j=1}^{q}\sum_{y_j\in\mathcal{J}}\mathrm{e}\left(\frac{k_jy_j}{q}\right)\right\}\frac{1}{q}\sum_{l=1}^{q-1}\sum_{z\in\mathcal{I}}\mathrm{e}\left(\frac{-lz}{q}\right)S(l,-\boldsymbol{k},\mathcal{A},q)\right|.$$

Then we bound the geometric progressions to obtain

$$E_2 \leqslant \frac{1}{q^{s+1}}\prod_{j=1}^{s}{}'\left(\sum_{k_j=1}^{q}\min\left\{|\mathcal{J}|,\frac{1}{2\|k_j/q\|}\right\}\right)\sum_{l=1}^{q-1}\min\left\{|\mathcal{I}|,\frac{1}{2\|-l/q\|}\right\}|S(l,-\boldsymbol{k},\mathcal{A},q)|, \tag{4.18}$$

where $\|x\|$ is the distance of x from the nearest integer.

5. The estimation of $N_{\mathcal{I}}(\mathcal{A})$

Our aim is to prove a result of the following type. Given the sequence of integers $\{q_n\}_{n\in\mathbb{N}}$ and a sequence $\{\varepsilon_n\}_{n\in\mathbb{N}}$ of real numbers such that $q_n\to\infty$ and $\varepsilon_n\to 0$, let us consider the intervals $\mathcal{I}_n,\mathcal{J}_n\subseteq[1,q_n]$ with $|\mathcal{I}_n|,|\mathcal{J}_n|>q_n^{1-\varepsilon_n}$. Then, for any positive integer s and any $\varepsilon>0$ there exists an integer $n(s,\varepsilon)$ such that for any integer $n\geqslant n(s,\varepsilon)$ and any $\mathcal{A}_n\subseteq[-q_n^{\varepsilon_n},q_n^{\varepsilon_n}]$ with $|\mathcal{A}_n|=s$ we have

$$\left|N_{\mathcal{I}_n}(\mathcal{A}_N,\mathcal{J}_n,q_n)-|\mathcal{I}_n|\left(\frac{|\mathcal{J}_n|}{q_n}\right)^s\Pi_1(q_n,\mathcal{A}_n)\right|\leqslant\varepsilon|\mathcal{I}_n|\left(\frac{|\mathcal{J}_n|}{q_n}\right)^s\Pi_1(q_n,\mathcal{A}_n).$$

To proceed, we need bounds for exponential sums, which, as we have seen, depend heavily on the divisors of q, so we need to split the discussion up accordingly.

5.1. More estimates for exponential sums

The first estimate is for the case when the modulus q is square free.

Lemma 5.1. *Let $p_1,p_2,\dots,p_r$ be distinct primes and $q=p_1p_2\dots p_r$. Then*

$$|S(0,\boldsymbol{k},\mathcal{A},q)|\leqslant(2s)^{\omega(q)}\left(2\max_{1\leqslant j\leqslant s}|a_j|\right)^{s(s-1)/4}(k_1,\dots,k_s,q)^{1/2}q^{1/2}.$$

Proof. Let $L_1(x)$ be the polynomial given by

$$L_1(x)=\left(\frac{k_1}{x+a_1}+\cdots+\frac{k_s}{x+a_s}\right)\prod_{j=1}^{s}(x+a_j).$$

We split $S(0,\boldsymbol{k},\mathcal{A},q)$ using Lemma 2.2 and estimate the factors $S(0,\boldsymbol{k},\mathcal{A},p)$ with p prime, either trivially or using Lemma 2.1. Thus we have

$$|S(0,\boldsymbol{k},\mathcal{A},p)|\leqslant\begin{cases}p-\nu(p,\mathcal{A}), & \text{if } L_1(x)\equiv 0\ (\mathrm{mod}\,p),\\ 2sp^{1/2}, & \text{otherwise.}\end{cases} \tag{5.1}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

Set

$$\mathcal{B} = \{p : p \text{ prime},\ p|q,\ L_1(x) \equiv 0 \pmod p\}.$$

Then Lemma 2.2 and (5.1) give

$$|S(0, \boldsymbol{k}, \mathcal{A}, q)| \leqslant \prod_{j=1}^{r} |S(0, \bar{\tilde{p}}_j^{(j)} \boldsymbol{k}, \mathcal{A}, p_j)| \leqslant \prod_{p \in \mathcal{B}} p \prod_{p \notin \mathcal{B}} 2sp^{1/2}. \tag{5.2}$$

Next let us denote

$$D_j = \prod_{i \neq j} (a_i - a_j)$$

and

$$\Delta = \prod_{i<j} (a_i - a_j).$$

With this notation the product over $p \in \mathcal{B}$ in (5.2) can be written as

$$\prod_{p \in \mathcal{B}} p = \prod_{\substack{p \in \mathcal{B} \\ p | D_1 \cdots D_s}} p \prod_{\substack{p \in \mathcal{B} \\ p \nmid D_1 \cdots D_s}} p. \tag{5.3}$$

Note that $p | D_1 \cdots D_s$ is equivalent to $p | \Delta$. This implies that

$$\prod_{\substack{p \in \mathcal{B} \\ p | D_1 \cdots D_s}} p \leqslant |\Delta| \leqslant \Bigl(2 \max_{1 \leqslant j \leqslant s} |a_j|\Bigr)^{s(s-1)/2}. \tag{5.4}$$

To estimate the other product in (5.3) we make the following remark, which will also be referred to later.

Remark 5.2. If $L_1(x) \equiv 0 \pmod p$, then

$$0 \equiv L_1(-a_h) = k_h \prod_{\substack{1 \leqslant j \leqslant s \\ j \neq h}} (-a_h + a_j) = k_h D_h \pmod p,$$

therefore $p | k_h D_h$ for all h with $1 \leqslant h \leqslant s$.

Now it is easy to see that Remark 5.2 implies that

$$\prod_{\substack{p \in \mathcal{B} \\ p \nmid D_1 \cdots D_s}} p \leqslant (k_1, \dots, k_s, q). \tag{5.5}$$

By (5.3)–(5.5) we obtain

$$\prod_{p \in \mathcal{B}} p \leqslant (k_1, \dots, k_s, q) \Bigl(2 \max_{1 \leqslant j \leqslant s} |a_j|\Bigr)^{s(s-1)/2}. \tag{5.6}$$

The lemma follows by inserting estimate (5.6) into (5.2). □

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

Suppose from now on that the modulus q has the decomposition $q = p_1^{\alpha_{p_1}} \cdots p_r^{\alpha_{p_r}}$, where $p_1, \dots, p_r$ are distinct primes. Here q is not necessarily square free. We use the following notation:

$$q_0 = \prod_{p|q} p, \qquad q_1 = \prod_{\substack{p|q \\ p^2 \nmid q}} p,$$

and

$$q_2 = \prod_{\substack{p|q \\ p^2|q}} p^{\alpha_p}, \qquad \tilde{q}_2 = \prod_{p|q_2} p^{[\alpha_p/2]}.$$

It is clear that $q_1 q_2 = q$.

To evaluate E_2 we use (4.18), and this requires a bound for $S(l, \boldsymbol{k}, \mathcal{A}, q)$.

Lemma 5.3. *We have*

$$|S(l, \boldsymbol{k}, \mathcal{A}, q)| \leqslant (2s)^{\omega(q_1)} 2^{(2s-1)\omega(q_2)} (q_1, l)^{1/2} (\tilde{q}_2, l)^{1/(2s)} q^{1-(1/(6s))}.$$

Proof. First we split $S(l, \boldsymbol{k}, \mathcal{A}, q)$ using Lemma 2.2:

$$S(l, \boldsymbol{k}, \mathcal{A}, q) = \prod_{p|q_1} S(c(p,q)l, c(p,q)\boldsymbol{k}, \mathcal{A}, p) \prod_{p|q_2} S(c(p^{\alpha_p}, q)l, c(p^{\alpha_p}, q)\boldsymbol{k}, \mathcal{A}, p^{\alpha_p}).$$

Here we used the fact that by their definition all the coefficients $c(m, q)$ are relatively prime to m. A simple calculation shows that

$$q_1^{1/2} q_2 \tilde{q}_2^{-1/(2s)} = q q_1^{-1/2} \tilde{q}_2^{-1/(2s)} \leqslant q^{1-(1/(6s))}. \tag{5.7}$$

We then apply Lemma 2.1 for the primes $p|q_1$ and Lemma 2.4 for the primes $p|q_2$ to obtain

$$\begin{aligned} |S(l, \boldsymbol{k}, \mathcal{A}, q)| &\leqslant \prod_{p|q_1} (2s(p,l)^{1/2} p^{1/2}) \prod_{p|q_2} (2^{2s-1} (p^{[\alpha_p/2]}, l)^{1/(2s)} p^{\alpha_p - ([\alpha_p/2]/(2s))}) \\ &\leqslant (2s)^{\omega(q_1)} 2^{(2s-1)\omega(q_2)} (q_1, l)^{1/2} (\tilde{q}_2, l)^{1/(2s)} q_1^{1/2} q_2 \tilde{q}_2^{-1/(2s)}. \end{aligned} \tag{5.8}$$

The lemma then follows by (5.8) and (5.7). □

Finally, in order to apply (3.3) we need to estimate $S(0, \boldsymbol{k}, \mathcal{A}, q)$ and this is done in the following lemma.

Lemma 5.4. *We have*

$$\begin{aligned} |S(0, \boldsymbol{k}, \mathcal{A}, q)| \leqslant (2s)^{\omega(q_1)} 2^{(2s-1)\omega(q_2)} \Big(2 \max_{1 \leqslant j \leqslant s} |a_j|\Big)^{(s-1)(s+2)/4} \\ \times (k_1, \dots, k_s, q_1)^{1/2} (k_1, \dots, k_s, \tilde{q}_2)^{1/(2s)} q^{1-(1/(6s))}. \end{aligned}$$

Proof. We begin by splitting $S(0,\boldsymbol{k},\mathcal{A},q)$ using Lemma 2.2:

$$S(0,\boldsymbol{k},\mathcal{A},q)=\prod_{p|q_1}S(0,c(p,q)\boldsymbol{k},\mathcal{A},p)\prod_{p|q_2}S(0,c(p^{\alpha_p},q)\boldsymbol{k},\mathcal{A},p^{\alpha_p}).$$

To bound the first product we appeal to Lemma 5.1, which gives

$$\left|\prod_{p|q_1}S(0,c(p,q)\boldsymbol{k},\mathcal{A},p)\right|\leqslant(2s)^{\omega(q_1)}\Bigl(2\max_{1\leqslant j\leqslant s}|a_j|\Bigr)^{s(s-1)/4}(k_1,\dots,k_s,q_1)^{1/2}q_1^{1/2}. \tag{5.9}$$

To bound the second product we introduce the polynomial

$$L_2(x)=\left(\frac{k_1}{(x+a_1)^2}+\cdots+\frac{k_s}{(x+a_s)^2}\right)\prod_{j=1}^{s}(x+a_j)^2.$$

Also, for the primes $p|q_2$ let β_p be such that

$$L_2(x)\equiv 0 \pmod{p^{\beta_p}}\qquad\text{and}\qquad L_2(x)\not\equiv 0 \pmod{p^{\beta_p+1}}.$$

Then we apply Lemma 2.3 for the primes for which $\beta_p<[\alpha_p/2]$, while for the other primes we use the trivial bound. Thus we get

$$\begin{aligned}\left|\prod_{p|q_2}S(0,c(p^{\alpha_p},q)\boldsymbol{k},\mathcal{A},p^{\alpha_p})\right|&=\prod_{\substack{p|q_2\\ \beta_p<[\alpha_p/2]}}|\cdots|\times\prod_{\substack{p|q_2\\ \beta_p\geqslant[\alpha_p/2]}}|\cdots|\\ &\leqslant 2^{(2s-1)\omega(q_2)}q_2\prod_{\substack{p|q_2\\ \beta_p<[\alpha_p/2]}}(p^{[\alpha_p/2]-\beta_p})^{-1/(2s)}.\end{aligned} \tag{5.10}$$

Now using the same argument as in Remark 5.2 we see that if $L_2(x)\equiv 0 \pmod{p^{\beta_p}}$, then $p^{\beta_p}|k_jD_j^2$ for any j ($1\leqslant j\leqslant s$), which further implies that $\prod_{p|\tilde q_2}p^{\beta_p}$ divides $(k_1,\dots,k_s)\Delta^2$. This shows that

$$\prod_{\substack{p|q_2\\ \beta_p<[\alpha_p/2]}}(p^{[\alpha_p/2]-\beta_p})^{-1/(2s)}\leqslant\tilde q_2^{-1/(2s)}(k_1,\dots,k_s,\tilde q_2)^{1/(2s)}|\Delta|^{1/s}. \tag{5.11}$$

The lemma follows by (5.9)–(5.11) and (5.4). □

5.2. Reduction to the case $\mathcal{I}=[1,q]$

By Lemma 5.3 and (4.18) we deduce that

$$\begin{aligned}E_2\leqslant(2s)^{\omega(q_1)}2^{(2s-1)\omega(q_2)}q^{1-(1/(6s))}\frac{1}{q^{s+1}}\prod_{j=1}^{s}{}'\left(\sum_{k_j=1}^{q}\min\left\{|\mathcal{J}|,\frac{1}{2\|k_j/q\|}\right\}\right)\\ \times\sum_{l=1}^{q-1}\min\left\{|\mathcal{I}|,\frac{1}{2\|-l/q\|}\right\}(q_1,l)^{1/2}(\tilde q_2,l)^{1/(2s)}.\end{aligned}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

The sums over k_j are bounded by

$$q^s\left(1+\sum_{k=1}^{[q/2]}\frac{1}{k}\right)^s \leqslant q^s(2+\log q)^s,$$

while the sum over l is less than

$$\begin{aligned} q\sum_{l=1}^{[q/2]}\frac{(q_1,l)^{1/2}(\tilde{q}_2,l)^{1/(2s)}}{l} &\leqslant q\sum_{d_1\mid q_1}\sum_{d_2\mid\tilde{q}_2} d_1^{1/2}d_2^{1/(2s)}\sum_{\substack{l=1\\ d_1\mid l\\ d_2\mid l}}^{[q/2]}\frac{1}{l} \\ &= q\sum_{d_1\mid q_1}\sum_{d_2\mid\tilde{q}_2} d_1^{-1/2}d_2^{(1/(2s))-1}\sum_{m=1}^{[q/(2d_1d_2)]}\frac{1}{m} \\ &\leqslant q(2+\log q)\sigma_{-1/2}(q_1)\sigma_{(1/(2s))-1}(\tilde{q}_2). \end{aligned}$$

We remind the reader here that q_1 and $\tilde{q}_2$ are coprime, so that d_1 and d_2 are. Putting these together we get

$$E_2 \leqslant (2s)^{\omega(q_1)}2^{(2s-1)\omega(q_2)}\sigma_{-1/2}(q_1)\sigma_{(1/(2s))-1}(\tilde{q}_2)(2+\log q)^{s+1}q^{1-(1/(6s))}.$$

We obtain the required reduction formula by combining (4.16), (4.17) and the above estimation for E_2:

$$\begin{aligned} \left|N_{\mathcal{I}}(\mathcal{A})-\frac{|\mathcal{I}|}{q}N(\mathcal{A})\right| &\leqslant (2s)^{\omega(q_1)+\omega(q)}2^{(2s-1)\omega(q_2)} \\ &\quad\times\sigma_{-1/2}(q_1)\sigma_{(1/(2s))-1}(\tilde{q}_2)(2+\log q)^{s+1}q^{1-(1/(6s))}. \end{aligned} \tag{5.12}$$

5.3. Estimation of $N_{\mathcal{I}}(\mathcal{A})$

Using the estimate provided by Lemma 5.4 in (3.3), we obtain

$$\begin{aligned} &\left|N(\mathcal{A})-q\Pi_1(q,\mathcal{A})\left(\frac{|\mathcal{J}|}{q}\right)^s\right| \\ &\quad\leqslant\frac{1}{q^s}(2s)^{\omega(q_1)}2^{(2s-1)\omega(q_2)}\Bigl(2\max_{1\leqslant j\leqslant s}|a_j|\Bigr)^{(s-1)(s+2)/4}q^{1-(1/(6s))} \\ &\qquad\times\sideset{}{'}\sum_{\boldsymbol{k}\pmod q}\prod_{j=1}^{s}\min\left\{|\mathcal{J}|,\frac{1}{2\|k_j/q\|}\right\}(k_1,\dots,k_s,q_1)^{1/2}(k_1,\dots,k_s,\tilde{q}_2)^{1/(2s)}. \end{aligned} \tag{5.13}$$

To evaluate the last line in (5.13), call it $\Pi(s)$, we separate the sum of the terms with no $k_j=q$ in a sum, denoted by $\Sigma_1(s)$, and the remaining terms in a sum, denoted $\Sigma_2(s)$. Thus we have

$$\Pi(s)=\Sigma_1(s)+\Sigma_2(s), \tag{5.14}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

where

$$\Sigma_1(s) = \sum_{k_1=1}^{q-1} \cdots \sum_{k_s=1}^{q-1} \frac{1}{2\|k_1/q\|} \cdots \frac{1}{2\|k_s/q\|} \cdot (k_1, \dots, k_s, q_1)^{1/2} (k_1, \dots, k_s, \tilde{q}_2)^{1/(2s)}$$

and

$$\Sigma_2(s) \leqslant s \cdot |\mathcal{J}| \cdot \sideset{}{'}\sum_{k_1,\dots,k_{s-1}=1}^{q} \biggl(\prod_{j=1}^{s-1} \min\biggl\{ |\mathcal{J}|, \frac{1}{2\|k_j/q\|} \biggr\} \biggr) \times (k_1, \dots, k_s, q_1)^{1/2} (k_1, \dots, k_s, \tilde{q}_2)^{1/(2s)}.$$

(Here the prime means that the terms with $k_1 = \dots = k_s = q$ are excluded from the summation.) If we delete k_s from the greatest common divisors above, the right-hand side increases and the sum is exactly $\Pi(s-1)$. Therefore,

$$\Sigma_2(s) \leqslant s \cdot |\mathcal{J}| \cdot \Pi(s-1), \tag{5.15}$$

so it is enough to get an estimate for Σ_1. A standard calculation gives

$$\begin{aligned} \Sigma_1 &\leqslant \sum_{k_1=1}^{(q+1)/2} \cdots \sum_{k_s=1}^{(q+1)/2} \frac{q}{k_1} \cdots \frac{q}{k_s} \cdot (k_1, \dots, k_s, q_1)^{1/2} (k_1, \dots, k_s, \tilde{q}_2)^{1/(2s)} \\ &\leqslant q^s \sum_{d_1 \mid q_1} d_1^{-1/2} \sum_{d_2 \mid \tilde{q}_2} d_2^{1/2s-1} \sum_{k'_1=1}^{(q+1)/(2d_1 d_2)} \cdots \sum_{k'_s=1}^{(q+1)/(2d_1 d_2)} \frac{1}{k'_1} \cdots \frac{1}{k'_s} \\ &\leqslant q^s \sigma_{-1/2}(q_1) \sigma_{(1/(2s))-1}(\tilde{q}_2)(2 + \log q)^s. \end{aligned} \tag{5.16}$$

By (5.14)–(5.16) we derive

$$\Pi(s) \leqslant q^s \sigma_{-1/2}(q_1) \sigma_{(1/(2s))-1}(\tilde{q}_2)(2 + \log q)^s + s \cdot |\mathcal{J}| \cdot \Pi(s-1),$$

from which, recursively, we get

$$\Pi(s) \leqslant 2s! q^s \sigma_{-1/2}(q_1) \sigma_{(1/(2s))-1}(\tilde{q}_2)(2 + \log q)^s.$$

Inserting this estimate in (5.13), and then using (5.12), we obtain the following theorem.

Theorem 5.5. *We have*

$$\biggl| N(\mathcal{A}) - q\Pi_1(q, \mathcal{A}) \biggl(\frac{|\mathcal{J}|}{q} \biggr)^s \biggr| \leqslant 2s!(2s)^{\omega(q_1)} 2^{(2s-1)\omega(q_2)} \Bigl(2 \max_{1 \leqslant j \leqslant s} |a_j| \Bigr)^{(s-1)(s+2)/4} \times \sigma_{-1/2}(q_1) \sigma_{(1/(2s))-1}(\tilde{q}_2)(2 + \log q)^s q^{1-(1/(6s))} \tag{5.17}$$

and

$$\biggl| N_{\mathcal{I}}(\mathcal{A}) - |\mathcal{I}| \Pi_1(q, \mathcal{A}) \biggl(\frac{|\mathcal{J}|}{q} \biggr)^s \biggr| \leqslant 6s!(2s)^{\omega(q_1)} 2^{(2s-1)\omega(q_2)} \Bigl(2 \max_{1 \leqslant j \leqslant s} |a_j| \Bigr)^{(s-1)(s+2)/4} \times \sigma_{-1/2}(q_1) \sigma_{(1/(2s))-1}(\tilde{q}_2)(2 + \log q)^{s+1} q^{1-(1/(6s))}. \tag{5.18}$$

We will use the following consequence of Theorem 5.5, which gives a simpler form for the error term.

Corollary 5.6. *Let q be a positive integer. Assume*

$$s = |\mathcal{A}| \leqslant \tfrac{1}{8}(\log\log q)^{1/2}, \tag{5.19}$$

$$\mathcal{A} \subset [-q^{1/(18s^3)}, q^{1/(18s^3)}], \tag{5.20}$$

$$|\mathcal{J}| \geqslant q^{1-(1/(36s^2))} \tag{5.21}$$

and

$$|\mathcal{I}| \geqslant q^{1-(1/(36s))}. \tag{5.22}$$

Then

$$N_{\mathcal{I}}(\mathcal{A}) = |\mathcal{I}|\Pi_1(q,\mathcal{A})\biggl(\frac{|\mathcal{J}|}{q}\biggr)^s(1 + O(q^{-(1/(18s))+o(1/s)})). \tag{5.23}$$

Proof. First note that (5.19) implies

$$2^{s^2} \leqslant 2^{\log\log q} = q^{o(1/s)},$$
$$\log^s q \leqslant q^{(1/s)((\log\log q)^3/(\log q))} = q^{o(1/s)}$$

and

$$s! \leqslant s^s \leqslant \log^s q = q^{o(1/s)}.$$

Using (5.19) and (4.10), we see that

$$s^{\omega(q)} = q^{o(1/s)},$$

and

$$2^{2s\omega(q)} \leqslant q^{2s(1+\varepsilon)(\log q/\log\log q)(\log 2/\log q)} \leqslant q^{1/(36s)}.$$

By (5.20) we get

$$\Bigl(2\max_{1\leqslant j\leqslant s}|a_j|\Bigr)^{(s-1)(s+2)/4} \leqslant \Bigl(2\max_{1\leqslant j\leqslant s}|a_j|\Bigr)^{s^2/2} \leqslant q^{1/(36s)}.$$

These show that the right-hand side of the relation (5.18) is

$$O(q^{1-(1/(6s))+(1/(36s))+(1/(36s))+o(1/s)}) = O(q^{1-(1/(9s))+o(1/s)}).$$

Next, by (5.21) we see that

$$\biggl(\frac{q}{|\mathcal{J}|}\biggr)^s \leqslant q^{1/(36s)}$$

and by (5.22) we have

$$\frac{q}{|\mathcal{I}|} \leqslant q^{1/(36s)}.$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

Using these and Lemma 4.1, we then get

$$N_{\mathcal{I}}(\mathcal{A}) = |\mathcal{I}|\Pi_1(q,\mathcal{A})\left(\frac{|\mathcal{J}|}{q}\right)^s\left(1+O\left(\left(\frac{q}{|\mathcal{J}|}\right)^s\frac{q}{|\mathcal{I}|}q^{1-(1/(9s))+o(1/s)}\right)\right)$$
$$= |\mathcal{I}|\Pi_1(q,\mathcal{A})\left(\frac{|\mathcal{J}|}{q}\right)^s(1+O(q^{-(1/(18s))+o(1/s)})),$$

as required. □

6. A formula for $g(\lambda_1,\dots,\lambda_r)$

With the notation as in § 1, for any integer $r \geqslant 1$ let $\boldsymbol{y} = (y_1,\dots,y_r)$ with $y_j = \lambda_j/\theta$, for $1 \leqslant j \leqslant r$. For any $\boldsymbol{s} = (s_1,\dots,s_r)$ with integer entries greater than or equal to 2, we define

$$N_{\boldsymbol{s}} = N_{\boldsymbol{s}}(\boldsymbol{y},\mathcal{I},\mathcal{J})$$

to be the number of sets $\{\xi_0,\dots,\xi_{\lambda_1,\dots,\lambda_r-r}\} \subset \mathcal{M}$ satisfying the following conditions:

$$\xi_0 < \cdots < \xi_{\lambda_1,\dots,\lambda_r-r},$$
$$\xi_{s_1-1} - \xi_0 \leqslant y_1,$$
$$\xi_{s_1+s_2-2} - \xi_{s_1-1} \leqslant y_2,$$
$$\vdots$$
$$\xi_{\lambda_1,\dots,\lambda_r-r} - \xi_{\boldsymbol{s}_1+\cdots+s_{r-1}-(r-1)} \leqslant y_r.$$

Also, let $G(\lambda_1,\dots,\lambda_r)$ denote the number of $\gamma_i \in \mathcal{M}$ for which $\gamma_{i+j} - \gamma_{i+j-1} \leqslant \lambda_j/\theta$, for $1 \leqslant j \leqslant r$. By definition, $g(\lambda_1,\dots,\lambda_r)$ is the probability that an element of $\mathcal{M}$ is counted by $G(\lambda_1,\dots,\lambda_r)$. Therefore,

$$g(\lambda_1,\dots,\lambda_r) = \frac{G(\lambda_1,\dots,\lambda_r)}{|\mathcal{M}|}. \tag{6.1}$$

This shows that we need to know the size of $G(\lambda_1,\dots,\lambda_r)$, and ultimately that of $N_{\boldsymbol{s}}$, which is closely related to $G(\lambda_1,\dots,\lambda_r)$. Using the inclusion–exclusion principle, we get a lower as well as an upper bound for $G(\lambda_1,\dots,\lambda_r)$. Indeed (see [**9**]), for any positive integer $n > 2r$ we have

$$G(\lambda_1,\dots,\lambda_r) = \sum_{2r\leqslant\lambda_1,\dots,\lambda_r<n}(-1)^{\lambda_1,\dots,\lambda_r}N_{\boldsymbol{s}} + \eta\sum_{\lambda_1,\dots,\lambda_r=n}N_{\boldsymbol{s}}, \tag{6.2}$$

for some real number η, with $|\eta| \leqslant 1$.

7. Estimation of $N_{\boldsymbol{s}}$

We first express $N_{\boldsymbol{s}}(\boldsymbol{y},\mathcal{I},\mathcal{J})$ in terms of $N_{\mathcal{I}}(\mathcal{A})$ and then we use our earlier work to bound $N_{\mathcal{I}}(\mathcal{A})$. We have

$$N_{\boldsymbol{s}}(\boldsymbol{y},\mathcal{I},\mathcal{J}) = \sum_{\mathrm{cond}(\boldsymbol{s},\boldsymbol{y})} N_{\mathcal{I}}(\{0,m_1,\dots,m_{\lambda_1,\dots,\lambda_r-r}\}),$$

in which cond$(\boldsymbol{s},\boldsymbol{y})$ indicates that the summation is over the integers $m_1,\dots m_{\lambda_1,\dots,\lambda_r-r}$ satisfying the set of conditions

$$\begin{gathered} 0<m_1<\cdots<m_{\lambda_1,\dots,\lambda_r-r},\\ m_{s_1-1}\leqslant y_1,\\ m_{s_1+s_2-2}-m_{s_1-1}\leqslant y_2,\\ \vdots\\ m_{\lambda_1,\dots,\lambda_r-r}-m_{\boldsymbol{s}_1+\cdots+s_{r-1}-(r-1)}\leqslant y_r. \end{gathered}$$

We wish to apply Corollary 5.6, and for that we need to make sure that the hypotheses are satisfied. For this we take $|\mathcal{I}|$ and $|\mathcal{J}|$ large enough, specifically

$$|\mathcal{I}|>q^{1-(2/(9(\log\log q)^{1/2}))}\quad\text{and}\quad|\mathcal{J}|>q^{1-(1/(\log\log q)^2)}.$$

Then, since $\varphi(q)/q>b/\log\log q$, for some positive constant b, one can check all the required conditions for $\mathcal{A}=\{0,m_1,\dots,m_{\lambda_1,\dots,\lambda_r-r}\}$. Substituting $N_{\mathcal{I}}(\mathcal{A})$ with the estimate (5.23), we get

$$\begin{aligned} N_{\boldsymbol{s}}(\boldsymbol{y},\mathcal{I},\mathcal{J})&=\sum_{\text{cond}(\boldsymbol{s},\boldsymbol{y})}|\mathcal{I}|\mathit{\Pi}_1(q,\mathcal{A})\biggl(\frac{|\mathcal{J}|}{q}\biggr)^{\lambda_1,\dots,\lambda_r-r+1}[1+o(1)]\\ &=\frac{|\mathcal{I}|}{q}\biggl(\frac{|\mathcal{J}|}{q}\biggr)^{\lambda_1,\dots,\lambda_r-r+1}\biggl(\sum_{\text{cond}(\boldsymbol{s},\boldsymbol{y})}q\mathit{\Pi}_1(q,\mathcal{A})\biggr)[1+o(1)]. \end{aligned}$$

The sum above is in fact equal to $N_{\boldsymbol{s}}(\boldsymbol{y},[1,q],[1,q])$, therefore we find that

$$N_{\boldsymbol{s}}(\boldsymbol{y},\mathcal{I},\mathcal{J})=\frac{|\mathcal{I}|}{q}\biggl(\frac{|\mathcal{J}|}{q}\biggr)^{\lambda_1,\dots,\lambda_r-r+1}N_{\boldsymbol{s}}(\boldsymbol{y},[1,q],[1,q])[1+o(1)]. \tag{7.1}$$

In [**11**, § 9, (22)] for $r=1$ and in [**12**, § 2] for $r\geqslant 2$, Hooley shows that if $y_j=c_jq/\varphi(q)$ for $1\leqslant j\leqslant q$, one has

$$N_{\boldsymbol{s}}(\boldsymbol{y},[1,q],[1,q])=\frac{c_1^{s_1-1}}{(s_1-1)!}\cdots\frac{c_r^{s_r-1}}{(s_r-1)!}\varphi(q)[1+o(1)].$$

If further applied in (7.1), this estimation gives

$$\begin{aligned} N_{\boldsymbol{s}}(\boldsymbol{y},\mathcal{I},\mathcal{J})&=\frac{|\mathcal{I}|}{q}\biggl(\frac{|\mathcal{J}|}{q}\biggr)^{\lambda_1,\dots,\lambda_r-r+1}\frac{c_1^{s_1-1}}{(s_1-1)!}\cdots\frac{c_r^{s_r-1}}{(s_r-1)!}\varphi(q)[1+o(1)]\\ &=\frac{|\mathcal{I}|}{q}\biggl(\frac{|\mathcal{J}|}{q}\biggr)^{\lambda_1,\dots,\lambda_r-r+1}\biggl(\frac{\varphi(q)}{q}\biggr)^{\lambda_1,\dots,\lambda_r-r}\frac{y_1^{s_1-1}}{(s_1-1)!}\cdots\frac{y_r^{s_r-1}}{(s_r-1)!}\varphi(q)[1+o(1)]. \end{aligned}\tag{7.2}$$

With λ_j given by

$$y_j=\frac{\lambda_j}{\theta}=\frac{c_jq}{\varphi(q)}$$

https://doi.org/10.1017/S0013091501000724 Published online by Cambridge University Press

for $1 \leqslant j \leqslant r$, we get

$$N_{\boldsymbol{s}}(\boldsymbol{y}, \mathcal{I}, \mathcal{J}) = |\mathcal{I}|\theta \frac{\lambda_1^{s_1-1}}{(s_1-1)!} \cdots \frac{\lambda_r^{s_r-1}}{(s_r-1)!}[1+o(1)]. \tag{7.3}$$

8. Completion of the proof

The way we deduce the final expression of $g(\lambda_1, \dots, \lambda_r)$ follows the procedure indicated for $r = 1$ in [**11**, § 10]. Substituting the estimation (7.3) in (6.2) we have, for any integer $n > 2r$,

$$G(\lambda_1, \dots, \lambda_r) = |\mathcal{I}|\theta \sum_{2r \leqslant \lambda_1, \dots, \lambda_r < n} (-1)^r \frac{(-\lambda_1)^{s_1-1}}{(s_1-1)!} \cdots \frac{(-\lambda_r)^{s_r-1}}{(s_r-1)!}[1+o(1)]$$
$$+ \eta |I| \theta \sum_{\lambda_1, \dots, \lambda_r = n} \frac{\lambda_1^{s_1-1}}{(s_1-1)!} \cdots \frac{\lambda_r^{s_r-1}}{(s_r-1)!}[1+o(1)].$$

Since

$$\sum_{s=m}^{\infty} \frac{\lambda^{s-1}}{(s-1)!} \leqslant \frac{\lambda^{m-1}}{(m-1)!},$$

by taking n sufficiently large, we see that

$$G(\lambda_1, \dots, \lambda_r) = |\mathcal{I}|\theta(1-\mathrm{e}^{-\lambda_1}) \dots (1-\mathrm{e}^{-\lambda_r}) + |I|\theta O_r\left(\frac{\lambda_1^n}{n!} + \dots + \frac{\lambda_r^n}{n!}\right)[1+o(1)].$$

By letting n go to infinity, we find that

$$\frac{G(\lambda_1, \dots, \lambda_r)}{|\mathcal{I}|\theta} = (1-\mathrm{e}^{-\lambda_1}) \cdots (1-\mathrm{e}^{-\lambda_r})[1+o(1)]. \tag{8.1}$$

On the other hand, although we know a sharp estimate for the number of elements of $\mathcal{M}$, for our needs it suffices to use (5.23), which gives

$$|\mathcal{M}| = |\mathcal{I}|\theta[1+o(1)].$$

By combining this with (6.1) and (8.1), we obtain

$$g(\lambda_1, \dots, \lambda_r) = (1-\mathrm{e}^{-\lambda_1}) \cdots (1-\mathrm{e}^{-\lambda_r})[1+o(1)],$$

which completes the proof of Theorem 1.1.

References

1. F. Boca and A. Zaharescu, Pair correlation of values of rational functions (mod p), *Duke Math. J.* **105** (2000), 267–307.
2. E. Bombieri, On exponential sums in finite fields, *Am. J. Math.* **88** (1966), 71–105.
3. C. Cobeli and A. Zaharescu, The order of inverses mod q, *Mathematika* **47** (2000), 87–108.

4. C. Cobeli and A. Zaharescu, On the distribution of primitive roots (mod p), *Acta Arithm.* **83** (1998), 143–153.
5. P. Erdös, The difference of consecutive primes, *Duke Math. J.* **6** (1940), 438–441.
6. P. Erdös, Some unsolved problems, *Magyar Tud. Akad. Kutató Int. Közl.* **6** (1961), 221–254.
7. T. Esterman, On Kloosterman's sums, *Mathematika* **8** (1961), 83–86.
8. P. X. Gallagher, On the distribution of primes in short intervals, *Mathematika* **23** (1976), 4–9.
9. H. Halberstam and H.-E. Richert, *Sieve methods* (Academic, 1974).
10. C. Hooley, On the difference of consecutive numbers prime to n, *Acta Arithm.* **8** (1962/1963), 343–347.
11. C. Hooley, On the difference between consecutive numbers prime to n, II, *Publ. Math. Debrecen* **12** (1965), 39–49.
12. C. Hooley, On the difference between consecutive numbers prime to n, III, *Math. Z.* **90** (1965), 355–364.
13. C. Hooley, On the intervals between consecutive terms of sequences, Analytic number theory, in *Proc. Symp. Pure Mathematics, St Louis, MO, 1972*, vol. XXIV, pp. 129–140 (American Mathematical Society, Providence, RI, 1973).
14. P. Kurlberg and Z. Rudnick, The distribution of spacings between quadratic residues, *Duke Math. J.* **100** (1999), 211–242.
15. H. L. Montgomery and R. C. Vaughan, On the distribution of reduced residues, *Ann. Math.* **123** (1986), 311–333.
16. Z. Rudnick and P. Sarnak, The pair correlation function of fractional parts of polynomials, *Commun. Math. Phys.* **194** (1998), 61–70.
17. V. T. Sós, On the distribution mod 1 of the sequence $n\alpha$, *Ann. Univ. Sci. Budap. Rolando Eotvos Nominatae Sect. Math.* **1** (1958), 127–134.
18. S. Świerczkowski, On successive settings of an arc on the circumference of a circle, *Fund. Math.* **46** (1958), 187–189.