DISTRIBUTION OF GAPS BETWEEN THE INVERSES mod q

C. COBELI¹, M. VĂJĂÎTU¹ AND A. ZAHARESCU¹,²

¹Institute of Mathematics of the Romanian Academy,
PO Box 1-764, Bucharest 70700, Romania
(ecobeli@stoilow.imar.ro; mvaja@stoilow.imar.ro)
²Department 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 I = I(q) and J = J(q) be subintervals of integers in [1, q] and let M be the set of elements of I that are invertible modulo q and whose inverses lie in 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 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 \(\{\alpha P(n)\}\), \(n \in \mathbb{N}\), provide another class of sequences which are believed to have a Poissonian distribution. Rudnick and Sarnak [16] proved that for almost all \(\alpha \in \mathbb{R}\) 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 \(\{\alpha P(n)\}\), \(1 \leq n \leq N\), 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 $I = I(q)$ and $J = J(q)$ 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 $n \mod q$, that is the unique integer from $\{1, \ldots, q\}$ satisfying $n\bar{n} \equiv 1 \pmod{q}$.

We consider the set

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

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

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

We think of $\theta$ 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 $J$. Then $M$ should be about $|I|/\theta$ and the average distance between two consecutive elements of $M$ should be $|I|/M \sim 1/\theta$. Thus, on these probabilistic grounds, concerning the spacing between consecutive members of $M$ one might conjecture that

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

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 $I = [1, q]$, $J = [1, q]$, 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], Erdős 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

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

where $a_1, \ldots, a_{\varphi(q)}$ are the reduced residues modulo $q$. Hooley proved (1.1) for $0 \leq \alpha < 2$ 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 $0 \leq \alpha < 2$ 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 $r \geq 1$, the groups of $r$ consecutive gaps between the elements of the sequence $a_1, \ldots, a_{\varphi(q)}$ 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 $\alpha > 0.$
Here we show that the distribution function calculated by Hooley remains the same if one picks up in the sampling only reduced residues from \( M \). To see this, for \( \lambda_1, \ldots, \lambda_r > 0 \) we define
\[
g(\lambda_1, \ldots, \lambda_r) = g(\lambda_1, \ldots, \lambda_r; I, J, q)
\]
to be the proportion of \( \gamma_i \in M \) which satisfies \( \gamma_i + j - \gamma_{i+j-1} \leq \lambda_j/\theta \), for \( 1 \leq j \leq r \).

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 \( M \) are independent of one another, that is, one expects to have
\[
g(\lambda_1, \ldots, \lambda_r) \approx g(\lambda_1) \cdots g(\lambda_r).
\]

Theorem 1.1 below shows that this is true, providing additionally an explicit expression for \( g(\lambda_1, \ldots, \lambda_r) \). 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 Erdős (see [6]) when \( I = J = [1, q] \) were complete intervals and \( q \) was a product \( q = 2 \cdot 3 \cdot \cdots \cdot p \) of consecutive primes.)

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

2. **Bounds for some exponential sums**

Let \( A = \{a_1, \ldots, a_s\} \) be a set of integers and \( k = (k_1, \ldots, k_s) \) a vector with integer components. If \( x \) is an integer, we write \( x = (x, \ldots, x) \), \( x + a = (x + a_1, \ldots, x + a_s) \) and \( \bar{x} + \bar{a} = (\bar{x} + \bar{a}_1, \ldots, \bar{x} + \bar{a}_s) \). 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:
\[
S(u, k, A, q) = \sum_{x=1}^{q} e\left(\frac{ux + k \cdot \bar{x} + \bar{a}}{q}\right).
\]

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

**Lemma 2.1.** Suppose that \( a_1, \ldots, a_s \) are distinct mod \( p \) and \( p \nmid (u, k_1, \ldots, k_s) \). Then
\[
|S(u, k, A, p)| \leq 2s \sqrt{p}.
\]

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 \( q_1, \ldots, q_r \) be pairwise coprime positive integers, \( q = q_1 \cdots q_r \), \( \tilde{q}_j = q/q_j \), and denote by \( \tilde{x}^{(j)} \) the inverse of \( x \) modulo \( q_j \), that is \( 1 \leq \tilde{x}^{(j)} \leq q_j - 1 \) and \( x \tilde{x}^{(j)} \equiv 1 \pmod{q_j} \). Then

\[
S(u, k, A, q) = \prod_{j=1}^{r} S(\tilde{q}_j^{(j)} u, \tilde{q}_j^{(j)} k, A, q_j) \tag{2.1}
\]

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 \( n \geq 2 \) and \( 0 \leq r \leq \lfloor n/2 \rfloor \) 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

\[
|S(u, k, A, p^n)| \leq 2^{2s-1} p^n - \left( \lfloor n/2 \rfloor - r \right)/(2s).
\]

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

**Lemma 2.4.** Let \( n \geq 2 \). Then

\[
|S(u, k, A, p^n)| \leq 2^{2s-1} (p^{[n/2]}, u)^{1/(2s)} p^n - \left( \lfloor n/2 \rfloor / (2s) \right).
\]

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

\[
S_I(u, k, A, q) = \sum_{x \in I'} e\left( \frac{ux + k \cdot \overline{x} + a}{q} \right),
\]

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

\[
S_I(u, k, A, q) = \frac{1}{q} \sum_{x=1}^{q} e\left( \frac{ux + k \cdot \overline{x} + a}{q} \right) \sum_{z \in I} \sum_{l=1}^{q} e\left( \frac{lx - z}{q} \right).
\]

Inverting the order of summation, we obtain

\[
S_I(u, k, A, q) = \frac{1}{q} \sum_{l=1}^{q} \sum_{z \in I} e\left( \frac{-lz}{q} \right) \sum_{x=1}^{q} e\left( \frac{(u + l)x + k \cdot \overline{x} + a}{q} \right)
\]

\[
= \frac{|I|}{q} S(u, k, A, q) + \frac{1}{q} \sum_{l=1}^{q-1} \sum_{z \in I} e\left( \frac{-lz}{q} \right) S(u + l, k, A, q). \tag{2.2}
\]
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 $(n + a_1, \ldots, n + a_s)$ 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 $|\mathcal{I}| |\mathcal{A}|$ 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

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

This can be written as an exponential sum as follows:

$$\delta(x) = \frac{1}{q} \sum_{k=1}^{q} \sum_{y \in \mathcal{J}} e\left(\frac{ky - \bar{x}}{q}\right).$$

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

$$\delta(x) = \frac{1}{q} \sum_{k=1}^{q} \sum_{y \in \mathcal{J}} e\left(\frac{ky - x}{q}\right). \quad (3.2)$$

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

$$N_{\mathcal{I}}(\mathcal{A}) = \sum_{x \in \mathcal{I}} \prod_{a \in \mathcal{A}} \delta(x + a)$$

$$= \frac{1}{q^s} \sum_{x \in \mathcal{I}'} \prod_{a \in \mathcal{A}} \sum_{k=1}^{q} \sum_{y \in \mathcal{J}} e\left(\frac{ky - x + a}{q}\right).$$

Inverting the order of summation, we get

$$N_{\mathcal{I}}(\mathcal{A}) = \frac{1}{q^s} \sum_{x \in \mathcal{I}'} \sum_{k_1=1}^{q} \sum_{y_1 \in \mathcal{J}} \cdots \sum_{k_s=1}^{q} \sum_{y_s \in \mathcal{J}} e\left(\frac{k_1 y_1 - x + a_1}{q}\right) \cdots e\left(\frac{k_s y_s - x + a_s}{q}\right)$$

$$= \frac{1}{q^s} \sum_{k_1=1}^{q} \sum_{y_1 \in \mathcal{J}} \cdots \sum_{k_s=1}^{q} \sum_{y_s \in \mathcal{J}} e\left(\frac{k_1 y_1}{q}\right) \cdots e\left(\frac{k_s y_s}{q}\right) S_{\mathcal{I}}(0, -\mathbf{k}, \mathcal{A}, q),$$

where $\mathbf{k} = (k_1, \ldots, k_s)$. 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

$$N_{\mathcal{I}}(\mathcal{A}) = \frac{|\mathcal{I}'| |\mathcal{J}|^s}{q^s} + \frac{1}{q^s} \prod_{j=1}^{s} \left\{ \sum_{k_j=1}^{q} \sum_{y_j \in \mathcal{J}} e\left(\frac{k_j y_j}{q}\right) \right\} S_{\mathcal{I}}(0, -\mathbf{k}, \mathcal{A}, q), \quad (3.3)$$

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 \( N_I(A) \) depends proportionally on \(|I|\), so it is enough to estimate \( N(A) \).

4. Reduction to the case \( I = [1, q] \)

We need an estimate for \(|I'|\). Following Hooley [11], we introduce

\[
\nu(d, A) = \{ n : 1 \leq n \leq d, \ (n + a_1) \cdots (n + a_s) \equiv 0 \pmod{d} \}.
\]

Clearly, if \( p \) is prime, then

\[
1 \leq \nu(p, A) \leq \min(p, s).
\]

Note that \( \nu(d, A) \) is multiplicative, that is

\[
\nu(d_1d_2, A) = \nu(d_1, A)\nu(d_2, A)
\]

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

\[
\Pi_1(q, A) = \prod_{p \mid q} \left( 1 - \frac{\nu(p, A)}{p} \right).
\]

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

\[
\frac{1}{q} \leq \prod_{p \mid q} \frac{1}{p} = \prod_{p \mid q} \left( 1 - \frac{p-1}{p} \right) \leq \Pi_1(q, A).
\]

A better bound is given by the following lemma.

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

\[
\Pi_1(q, A) \geq q^{-3/(\log q)^{1/3}}.
\]

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

\[
\Pi_1(q, A) = \prod_{p \mid q \atop p < (\log q)^{2/3}} \left( 1 - \frac{\nu(p, A)}{p} \right) \prod_{p \mid q \atop p \geq (\log q)^{2/3}} \left( 1 - \frac{\nu(p, A)}{p} \right) = P_1P_2,
\]

say. Since \( \nu(p, A) \leq p - 1 \), for the first product we have

\[
P_1 \geq \prod_{p \mid q \atop p < (\log q)^{2/3}} \left( 1 - \frac{p-1}{p} \right) \geq \prod_{p < (\log q)^{2/3}} \frac{1}{p}.
\]
Distribution of gaps between the inverses mod \( q \)

A trivial estimate for \( \pi(x) \), the number of primes \( \leq x \), gives
\[
\prod_{p \leq x} p^\pi(x) \leq x^{2x/(\log x)} = e^{2x},
\] (4.7)
for \( x \geq 2 \). By (4.6) and (4.7) we obtain
\[
P_1 \geq e^{-2(\log q)^{2/3}} = q^{-2/((\log q)^{1/3})}.
\] (4.8)

By (4.1), for \( P_2 \) we have
\[
P_2 \geq \prod_{p | q^{2/3}} \left( 1 - \frac{s}{p} \right) \geq \left( 1 - \frac{s}{(\log q)^{2/3}} \right)^{\omega(q)} \geq e^{-es\omega(q)/((\log q)^{2/3})},
\] (4.9)
because \( 1 - x \geq e^{-ex} \) for any \( x \in [0,1/e] \). Here \( \omega(q) \) is the number of distinct prime factors of \( q \). It is well known that
\[
1 \leq \omega(q) \leq \frac{2 \log q}{\log \log q}
\] (4.10)
for \( q \) large enough. Using (4.9), (4.10) and our hypothesis on \( s \), we obtain
\[
P_2 \geq \exp \left[ - \frac{2e \log q}{\log q} \right] = q^{-2e/((\log \log q)(\log q)^{2/3})},
\] (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 \( A = \{a_1, \ldots, a_s\} \) be a set of integers, \( I \) a subinterval of integers in \([1,q] \), and denote \( I' = \{n \in I : (n + a, q) = 1 \text{ for all } a \in A\} \). Then
\[
|I'| - \Pi_1(q,A)|I| \leq (2s)^{\omega(q)}
\] (4.12)
and
\[
|I'| = q\Pi_1(q,A).
\] (4.13)

**Proof.** Let \( P(x) = (x + a_1) \cdots (x + a_s) \). Then we have
\[
|I'| = \sum_{x \in I} \sum_{P(x) \equiv 0 \pmod{d}} \mu(d)
\]
\[
= \sum_{d | q} \mu(d) \sum_{x \in I} \sum_{P(x) \equiv 0 \pmod{d}} 1
\]
\[
= \sum_{d | q} \mu(d) \left( \frac{|I|}{d} + \theta_d \right) \sum_{1 \leq x \leq d} \sum_{P(x) \equiv 0 \pmod{d}} 1,
\]
where $\theta_d$ are real numbers with $|\theta_d| \leq 1$. Using the multiplicativity of the sum
\[
\sum_{\substack{1 \leq x \leq d \\ \nu(x) \equiv 0 \pmod{d}}} 1,
\]
which coincides with $\nu(d, A)$, we obtain
\[
|I'| = |I| \sum_{d|q} \frac{\mu(d)}{d} \nu(d, A) + \sum_{d|q} \mu(d) \theta_d \nu(d, A)
= |I| \prod_{p|q} \left(1 - \frac{\nu(p, A)}{p}\right) + \sum_{d|q} \mu(d) \theta_d \nu(d, A). \tag{4.14}
\]

We bound the last sum trivially:
\[
\left| \sum_{d|q} \mu(d) \theta_d \nu(d, A) \right| \leq \sum_{d|q} \nu(d, A) \leq \prod_{p|q} (1 + \nu(p, A)) \leq \prod_{p|q} (1 + s) \leq (1 + s)^{\omega(q)} \leq (2s)^{\omega(q)}. \tag{4.15}
\]

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

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

We return now to the $s$-tuple problem. By (3.3) we deduce that
\[
\left| N_{I}(A) - \frac{|I|}{q} N(A) \right| \leq E_1 + E_2, \tag{4.16}
\]
where
\[
E_1 = \left| \frac{|I'|}{q^s} - \frac{|I|}{q} \right| \left| [1, q'] [J]^{s} q^s \right| - \left| \frac{|J|}{q^s} \right| \left| [1, q'][J]^{s} q^s \right| \right|
\]
and
\[
E_2 = \left| \frac{1}{q^s} \prod_{j=1}^{s} \left( \sum_{k_j=1}^{q} \sum_{y_j \in J} e\left( \frac{k_j y_j}{q} \right) \right) \left( S_{I}(0, -k, A, q) - \frac{|I|}{q} S(0, -k, A, q) \right) \right|.
\]

To bound $E_1$ we use Lemma 4.2 to obtain
\[
E_1 = \left| \frac{|J|}{q^s} \right| \left| [1, q'] [J]^{s} q^s \right| \left| [J]^{s} q^s \right| \left( \theta_1(2s)^{\omega(q)} - \frac{|I|}{q} q \right)
\]
where $\theta_1$ is a real number with $|\theta_1| \leq 1$. This gives
\[
E_1 \leq \frac{|J|}{q^s} (2s)^{\omega(q)}. \tag{4.17}
\]
To obtain an upper bound for $E_2$ we first use (2.2) to replace the incomplete exponential sums by complete ones to get

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

Then we bound the geometric progressions to obtain

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

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 $n \geq n(s, \varepsilon)$ and any $\mathcal{A}_n \subseteq [-q_n^{s}, q_n^{s}]$ with $|\mathcal{A}_n| = s$ we have

$$|N_{\mathcal{I}_n}(\mathcal{A}_N, \mathcal{J}_n, q_n) - |\mathcal{I}_n| \left( \frac{|\mathcal{J}_n|}{q_n} \right)^s H_1(q_n, \mathcal{A}_n)| \leq \varepsilon |\mathcal{I}_n| \left( \frac{|\mathcal{J}_n|}{q_n} \right)^s H_1(q_n, \mathcal{A}_n).$$

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 $p_1, p_2, \ldots, p_r$ be distinct primes and $q = p_1 p_2 \ldots p_r$. Then

$$|S(0, k, \mathcal{A}, q)| \leq (2s)^{\varphi(q)} \left( \frac{2 \max_{1 \leq j \leq s} |a_j|}{a_j} \right)^{(s-1)/4} (k_1, \ldots, k_s, q)^{1/2} q^{1/2}.$$

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

$$|S(0, k, \mathcal{A}, p)| \leq \begin{cases} p - \nu(p, \mathcal{A}), & \text{if } L_1(x) \equiv 0 \pmod{p}, \\ 2sp^{1/2}, & \text{otherwise.} \end{cases} \quad (5.1)$$
Set
\[ B = \{ p : p \text{ prime}, \ p|q, \ L_1(x) \equiv 0 \pmod{p} \} \]

Then Lemma 2.2 and (5.1) give
\[
|S(0, k, A, q)| \leq \prod_{j=1}^{r} |S(0, f_j^{(j)} k, A, p_j)| \leq \prod_{p \in B} p \prod_{p \notin B} 2sp^{1/2}. \tag{5.2}
\]

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 \( p \in B \) in (5.2) can be written as
\[
\prod_{p \in B} p = \prod_{p \in B \atop p|D_1 \cdots D_s} p \prod_{p \in B \atop p \nmid D_1 \cdots D_s} p. \tag{5.3}
\]

Note that \( p|D_1 \cdots D_s \) is equivalent to \( p|\Delta \). This implies that
\[
\prod_{p \in B \atop p|D_1 \cdots D_s} p \leq |\Delta| \leq \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{(s-1)/2}. \tag{5.4}
\]

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
\[
0 \equiv L_1(-a_h) = k_h \prod_{1 \leq j \leq s \atop j \neq h} (-a_h + a_j) = k_h D_h \pmod{p},
\]

therefore \( p|k_h D_h \) for all \( h \) with \( 1 \leq h \leq s \).

Now it is easy to see that Remark 5.2 implies that
\[
\prod_{p \in B \atop p|D_1 \cdots D_s} p \leq (k_1, \ldots, k_s, q). \tag{5.5}
\]

By (5.3)–(5.5) we obtain
\[
\prod_{p \in B} p \leq (k_1, \ldots, k_s, q) \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{(s-1)/2}. \tag{5.6}
\]

The lemma follows by inserting estimate (5.6) into (5.2). \( \square \)
Suppose from now on that the modulus $q$ has the decomposition $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $p_1, \ldots, p_r$ are distinct primes. Here $q$ is not necessarily square free. We use the following notation:

$$q_0 = \prod_{p \mid q} p, \quad q_1 = \prod_{p^2 \mid q} p,$$

and

$$q_2 = \prod_{p \mid q^{\alpha_p}} p, \quad \tilde{q}_2 = \prod_{p \mid q^{[\alpha_p/2]}} p.$$

It is clear that $q_1q_2 = q$.

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

**Lemma 5.3.** We have

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

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

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

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

$$q_1^{-1/2}q_2^{-1/(2s)} = q^{-1/2}q_2^{-1/(2s)} \leq q^{-1/(6s)}.$$  \hfill (5.7)

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

$$|S(l, k, \mathcal{A}, q)| \leq \prod_{p \mid q_1} (2s(p, l)^{1/2}p^{1/2}) \prod_{p \mid q_2} (2s(p^{\alpha_p}/2, l)^{1/(2s)}p^{\alpha_p-([\alpha_p/2]/(2s)))}

\leq (2s)^{\omega(q_1)2(2s-1)\omega(q_2)}(q_1, l)^{1/2}(\tilde{q}_2, l)^{1/(2s)}q_1^{-1}s^{-1/2}q_2^{-1/(2s)}.$$  \hfill (5.8)

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

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

**Lemma 5.4.** We have

$$|S(0, k, \mathcal{A}, q)| \leq (2s)^{\omega(q_1)2(2s-1)\omega(q_2)}\left(\max_{1 \leq j \leq s} |a_j|\right)^{(s-1)(s+2)/4}

\times (k_1, \ldots, k_s, q_1)^{1/2}(k_1, \ldots, k_s, \tilde{q}_2)^{1/(2s)}q^{1-(1/(6s))}.$$
C. Cobeli, M. Văjăitu and A. Zaharescu

Proof. We begin by splitting \( S(0,k,A,q) \) using Lemma 2.2:
\[
S(0,k,A,q) = \prod_{p|q_1} S(0,c(p,q)k,A,p) \prod_{p|q_2} S(0,c(p^{\alpha_p},q)k,A,p^{\alpha_p}).
\]

To bound the first product we appeal to Lemma 5.1, which gives
\[
\left| \prod_{p|q_1} S(0,c(p,q)k,A,p) \right| \leq (2s)^{\omega(q_1)} \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{(s-1)/4} (k_1, \ldots, k_s, q_1)^{1/2} q_1^{1/2}. \quad (5.9)
\]

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 \( \beta_p \) be such that
\[
L_2(x) \equiv 0 \pmod{p^{2\beta_p}} \quad \text{and} \quad L_2(x) \not\equiv 0 \pmod{p^{2\beta_p+1}}.
\]

Then we apply Lemma 2.3 for the primes for which \( \beta_p < \lfloor \alpha_p/2 \rfloor \), while for the other primes we use the trivial bound. Thus we get
\[
\left| \prod_{p|q_2} S(0,c(p^{\alpha_p},q)k,A,p^{\alpha_p}) \right| = \prod_{p|q_2} \left| \cdots \prod_{\beta_p < \lfloor \alpha_p/2 \rfloor} \cdots \prod_{\beta_p \geq \lfloor \alpha_p/2 \rfloor} \cdots \right|
\leq 2^{(2s-1)\omega(q_2)} q_2 \prod_{p|q_2} (p^{\lfloor \alpha_p/2 \rfloor - \beta_p})^{-1/(2s)}. \quad (5.10)
\]

Now using the same argument as in Remark 5.2 we see that if \( L_2(x) \equiv 0 \pmod{p^{2\beta_p}} \), then \( p^{2\beta_p} | k_j D_j^2 \) for any \( j \) (\( 1 \leq j \leq s \)), which further implies that
\[
\prod_{p|q_2} (p^{\lfloor \alpha_p/2 \rfloor - \beta_p})^{-1/(2s)} \leq q_2^{1/(2s)} (k_1, \ldots, k_s)^{1/(2s)} |\Delta|^{1/s}. \quad (5.11)
\]

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
\[
E_2 \leq (2s)^{\omega(q_1)2^{(2s-1)\omega(q_2)}} q^{1/(6s)} \left( \prod_{j=1}^{q} \min \left\{ |\mathcal{I}|, \frac{1}{2\|k_j/q\|} \right\} \right) \times \sum_{l=1}^{q-1} \min \left\{ \frac{1}{\|l/q\|}, \frac{1}{2\|l/q\|} \right\} (q_1, l)^{1/2} (q_2, l)^{1/2s}.
\]
The sums over \( k \) are bounded by
\[ q^s \left(1 + \sum_{k=1}^{\lfloor q/2 \rfloor} \frac{1}{k}\right)^s \leq q^s (2 + \log q)^s, \]
while the sum over \( l \) is less than
\[
q \sum_{l=1}^{\lfloor q/2 \rfloor} \frac{(q_1, l)^{1/2} (\tilde{q}_2, l)^{1/2s}}{l} \leq q \sum_{d_1 | q_1, d_2 | \tilde{q}_2} d_1^{1/2} d_2^{1/(2s)} \sum_{l=1}^{\lfloor q/(2d_1 d_2) \rfloor} \frac{1}{l}
\]
\[
= q \sum_{d_1 | q_1, d_2 | \tilde{q}_2} d_1^{-1/2} d_2^{1/(2s) - 1} \sum_{m=1}^{\lfloor q/(2d_1 d_2) \rfloor} \frac{1}{m}
\]
\[
\leq q (2 + \log q) s_{1/2} \sigma_{1/(2s)} (\tilde{q}_2)(2 + \log q)^s q_1^{1 - (1/(6s))}. \]

We remark 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
\[ E_2 \leq (2s)^{\omega(q_1) + \omega(q_2)} (2^{2s-1})^{\omega(q_2)} \sigma_{1/(2s) - 1} (\tilde{q}_2) (2 + \log q)^s q_1^{1 - (1/(6s))}. \]

We obtain the required reduction formula by combining (4.16), (4.17) and the above estimation for \( E_2 \):
\[
\left| N_{\Xi}(\mathcal{A}) - \frac{\mid \mathcal{J} \mid}{q} N(\mathcal{A}) \right| \leq (2s)^{\omega(q_1) + \omega(q_2)} (2^{2s-1})^{\omega(q_2)} \sigma_{1/(2s) - 1} (\tilde{q}_2) (2 + \log q)^s q_1^{1 - (1/(6s))}. \quad (5.12)
\]

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

Using the estimate provided by Lemma 5.4 in (3.3), we obtain
\[
\left| N(\mathcal{A}) - q \Pi_1(q, \mathcal{A}) \left( \frac{\mid \mathcal{J} \mid}{q} \right)^s \right| \leq \frac{1}{q^s (2s)^{\omega(q_1) + \omega(q_2)}} \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{s-1} \left( 2^{2s-1} \right)^{\omega(q_2)} \left( 2 + \log q \right)^s q_1^{s - (1/(6s))}
\]
\[
\times \sum_{k \pmod{q}} \prod_{j=1}^{s} \min \left\{ \frac{1}{|\mathcal{J}|}, \frac{1}{2\|k_j/q\|} \right\} (k_1, \ldots, k_s, q_1)^{1/2} (k_1, \ldots, k_s, \tilde{q}_2)^{1/(2s)}. \quad (5.13)
\]

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
\[ \Pi(s) = \Sigma_1(s) + \Sigma_2(s), \quad (5.14) \]
where
\[ \Sigma_1(s) = \sum_{k_1=1}^{q-1} \cdots \sum_{k_s=1}^{q-1} \frac{1}{2\|k_i/q\|} \cdots \frac{1}{2\|k_s/q\|} \cdot (k_1, \ldots, k_s, q_1^{1/2}(k_1, \ldots, k_s, \tilde{q}_2)^{1/(2s)} \]
and
\[ \Sigma_2(s) \leq s \cdot |\mathcal{J}| \cdot \sum_{k_1, \ldots, k_s=1}^{\mathcal{J}} \min_{j=1}^{s} \left( \frac{1}{2\|k_j/q\|} \right) \times (k_1, \ldots, k_s, q_1^{1/2}(k_1, \ldots, k_s, \tilde{q}_2)^{1/(2s)} \right). \]
(Here the prime means that the terms with \( k_1 = \cdots = k_s = q \) 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,
\[ \Sigma_2(s) \leq s \cdot |\mathcal{J}| \cdot \Pi(s-1), \] (5.15)
so it is enough to get an estimate for \( \Sigma_1 \). A standard calculation gives
\[ \Sigma_1 \leq \sum_{k_1, \ldots, k_s=1}^{(s+1)/2} \frac{q}{k_1} \cdots \frac{q}{k_s} \cdot (k_1, \ldots, k_s, q_1^{1/2}(k_1, \ldots, k_s, \tilde{q}_2)^{1/(2s)} \]
\[ \leq q^s \sum_{d_1|q_1} d_1^{-1/2} \sum_{d_2|\tilde{q}_2} d_2^{1/(2s-1)} \sum_{k_1=1}^{(s+1)/(2d_1 d_2)} \cdots \sum_{k_s=1}^{(s+1)/(2d_1 d_2)} \frac{1}{k_1} \cdots \frac{1}{k_s} \]
\[ \leq q^s \sigma_{s-1/2}(q_1) \sigma_{1/(2s)-1}(\tilde{q}_2)(2 + \log q)^s. \] (5.16)
By (5.14)–(5.16) we derive
\[ \Pi(s) \leq q^s \sigma_{s-1/2}(q_1) \sigma_{1/(2s)-1}(\tilde{q}_2)(2 + \log q)^s + s \cdot |\mathcal{J}| \cdot \Pi(s-1), \]
from which, recursively, we get
\[ \Pi(s) \leq 2slq^s \sigma_{s-1/2}(q_1) \sigma_{1/(2s)-1}(\tilde{q}_2)(2 + \log q)^s. \]
Inserting this estimate in (5.13), and then using (5.12), we obtain the following theorem.

**Theorem 5.5.** We have
\[ \left| N(\mathcal{A}) - q \Pi_1(q, \mathcal{A}) \left( \frac{|J|}{q} \right) \right| \leq 2sl(2s)^{\omega(q_1)} q^{(2s-1)\omega(q_2)} \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{(s-1)(s+2)/4} \]
\[ \times \sigma_{s-1/2}(q_1) \sigma_{1/(2s)-1}(\tilde{q}_2)(2 + \log q)^s q^{1-(1/(6s))} \] (5.17)
and
\[ \left| N_{\mathcal{T}}(\mathcal{A}) - |\mathcal{T}| \Pi_1(q, \mathcal{A}) \left( \frac{|\mathcal{J}|}{q} \right) \right| \leq 6sl(2s)^{\omega(q_1)} q^{(2s-1)\omega(q_2)} \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{(s-1)(s+2)/4} \]
\[ \times \sigma_{s-1/2}(q_1) \sigma_{1/(2s)-1}(\tilde{q}_2)(2 + \log q)^s q^{s+1} q^{1-(1/(6s))}. \] (5.18)
Distribution of gaps between the inverses mod $q$

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

\[
s = |A| \leq \frac{1}{8} (\log \log q)^{1/2}, \tag{5.19}
\]

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

\[
|\mathcal{J}| \geq q^{-1/(36s^2)} \tag{5.21}
\]

and

\[
|\mathcal{I}| \geq q^{1-1/(36s)}. \tag{5.22}
\]

Then

\[
N_x(A) = |\mathcal{I}| \Pi_1(q, A) \left( \frac{|\mathcal{J}|}{q} \right)^s (1 + O(q^{-1/(18s)} + o(1/s))). \tag{5.23}
\]

**Proof.** First note that (5.19) implies

\[
2^{s^2} \leq 2^{\log \log q} = q^{o(1/s)},
\]

\[
\log^s q \leq q^{(1/s)((\log \log q)^3/(\log q))} = q^{o(1/s)}
\]

and

\[
s! \leq s^s \leq \log^s q = q^{o(1/s)}.
\]

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

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

and

\[
2^{2s^\omega(q)} \leq q^{2s(1+\varepsilon)(\log q/\log \log q)(\log 2/\log q)} \leq q^{1/(36s)}.
\]

By (5.20) we get

\[
\left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{(s-1)(s+2)/4} \leq \left( 2 \max_{1 \leq j \leq s} |a_j| \right)^{s^2/2} \leq q^{1/(36s)}.
\]

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

\[
\left( \frac{q}{|\mathcal{J}|} \right)^s \leq q^{1/(36s)}
\]

and by (5.22) we have

\[
\frac{q}{|\mathcal{I}|} \leq q^{1/(36s)}.
\]
Using these and Lemma 4.1, we then get
\[ N_\mathcal{I}(A) = |\mathcal{I}| \Pi_1(q, A) \left( \frac{|\mathcal{J}|}{q} \right)^s \left( 1 + O \left( \left( \frac{q}{|\mathcal{J}| |\mathcal{I}|} q^{1-(1/(9s))+o(1/s)} \right) \right) \right) \]

\[ = |\mathcal{I}| \Pi_1(q, A) \left( \frac{|\mathcal{J}|}{q} \right)^s \left( 1 + O(q^{-(1/(18s))+o(1/s)}) \right), \]
as required. \hfill \square

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

With the notation as in § 1, for any integer \( r \geq 1 \) let \( y = (y_1, \ldots, y_r) \) with \( y_j = \lambda_j/\theta \), for \( 1 \leq j \leq r \). For any \( s = (s_1, \ldots, s_r) \) with integer entries greater than or equal to 2, we define \( N_\mathcal{s} = N_\mathcal{s}(y, \mathcal{I}, \mathcal{J}) \) to be the number of sets \( \{ \xi_0, \ldots, \xi_{\lambda_1 - \lambda_r} \} \subset \mathcal{M} \) satisfying the following conditions:

\[ \xi_0 < \cdots < \xi_{\lambda_1 - \lambda_r}, \]
\[ \xi_{s_1 - 1} - \xi_0 \leq y_1, \]
\[ \xi_{s_1 + s_2 - 2} - \xi_{s_1 - 1} \leq y_2, \]
\[ \vdots \]
\[ \xi_{s_1 + \cdots + s_{r-1} - (r-1)} - \xi_{s_1 + \cdots + s_{r-1} - (r-1)} \leq y_r. \]

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

\[ g(\lambda_1, \ldots, \lambda_r) = \frac{G(\lambda_1, \ldots, \lambda_r)}{|\mathcal{M}|}. \quad (6.1) \]

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

\[ G(\lambda_1, \ldots, \lambda_r) = \sum_{2r \leq \lambda_1, \ldots, \lambda_r < n} (-1)^{\lambda_1 + \cdots + \lambda_r} N_\mathcal{s} + \eta \sum_{\lambda_1, \ldots, \lambda_r = n} N_\mathcal{s}, \quad (6.2) \]

for some real number \( \eta \), with \( |\eta| \leq 1 \).

7. Estimation of \( N_\mathcal{s} \)

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

\[ N_\mathcal{s}(y, \mathcal{I}, \mathcal{J}) = \sum_{\text{cond}(s, y)} N_\mathcal{I}(\{0, m_1, \ldots, m_{\lambda_1 - \lambda_r} \}), \]
in which \(\text{cond}(s, y)\) indicates that the summation is over the integers \(m_1, \ldots, m_{\lambda_1, \ldots, \lambda_r - r}\) satisfying the set of conditions

\[
0 < m_1 < \cdots < m_{\lambda_1, \ldots, \lambda_r - r}, \\
m_{s_1 - 1} \leq y_1, \\
m_{s_1 + s_2 - 2} - m_{s_1 - 1} \leq y_2, \\
\vdots \\
m_{\lambda_1, \ldots, \lambda_r - r} - m_{s_1 + \cdots + s_{r-1} - (r-1)} \leq y_r.
\]

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

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

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

\[
N_s(y, I, J) = \sum_{\text{cond}(s, y)} |I| \Pi_1(q, \mathcal{A}) \left( \frac{|J|}{q} \right)^{\lambda_1, \ldots, \lambda_r - r + 1} [1 + o(1)]
\]

\[
= \frac{|I|}{q} \left( \frac{|J|}{q} \right)^{\lambda_1, \ldots, \lambda_r - r + 1} \left( \sum_{\text{cond}(s, y)} q\Pi_1(q, \mathcal{A}) \right)[1 + o(1)].
\]

The sum above is in fact equal to \(N_s(y, [1, q], [1, q])\), therefore we find that

\[
N_s(y, I, J) = \frac{|I|}{q} \left( \frac{|J|}{q} \right)^{\lambda_1, \ldots, \lambda_r - r + 1} N_s(y, [1, q], [1, q])[1 + o(1)]. \tag{7.1}
\]

In [11, § 9, (22)] for \(r = 1\) and in [12, § 2] for \(r \geq 2\), Hooley shows that if \(y_j = c_j q/\varphi(q)\) for \(1 \leq j \leq q\), one has

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

If further applied in (7.1), this estimation gives

\[
N_s(y, I, J) = \frac{|I|}{q} \left( \frac{|J|}{q} \right)^{\lambda_1, \ldots, \lambda_r - r + 1} \frac{c_1^{s_1 - 1}}{(s_1 - 1)!} \cdots \frac{c_r^{s_r - 1}}{(s_r - 1)!} \varphi(q)[1 + o(1)]
\]

\[
= \frac{|I|}{q} \left( \frac{|J|}{q} \right)^{\lambda_1, \ldots, \lambda_r - r + 1} \left( \frac{\varphi(q)}{q} \right)^{\lambda_1, \ldots, \lambda_r - r} \frac{y_1^{s_1 - 1}}{(s_1 - 1)!} \cdots \frac{y_r^{s_r - 1}}{(s_r - 1)!} \varphi(q)[1 + o(1)]. \tag{7.2}
\]

With \(y_j\) given by

\[
y_j = \frac{\lambda_j}{\theta} = \frac{c_j q}{\varphi(q)}
\]
for $1 \leq j \leq r$, we get

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

(7.3)

8. Completion of the proof

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

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

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

Since

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

by taking $n$ sufficiently large, we see that

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

By letting $n$ go to infinity, we find that

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

(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

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

which completes the proof of Theorem 1.1.

References

Distribution of gaps between the inverses mod $q$  


