The distribution of k-tuples of reduced residues

Farzad Aryan

Abstract

In 1940 Paul Erdős made a conjecture about the distribution of reduced residues. Here we study the distribution of k-tuple of reduced residues. As an application we prove estimates about distribution of the squares and the distribution of a general set modulo square-free number q.

Introduction

In 1936 Cramer [1], assuming the Riemann hypothesis (RH), showed that

\[ \sum_{p_n < x} (p_{n+1} - p_n)^2 \ll x (\log x)^{3+\varepsilon} \]  

from which he deduced \( p_{n+1} - p_n = O(\sqrt{p_n} \log p_n) \). Based on his probabilistic model for the primes he also conjectured that

\[ \limsup_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n^2} = 1. \]

Taking into account various sieve estimates in Cramer’s probabilistic model, Granville [2] in 1995 conjectured that

\[ \limsup_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n^2} \geq 2e^{-\gamma}, \]

which is bigger than 1. Note that \( \gamma \) is the Euler constant. Proving (0.1) unconditionally seems quite deep, which led P. Erdős to make an analogous conjecture:
Conjecture (Erdős [3]). Let \( q \) be a natural number, and let \( P = \phi(q)/q \) be the probability that a randomly chosen integer is relatively prime to \( q \). Let

\[
1 = a_1 < a_2 < \cdots
\]

be the integers co-prime to \( q \) in increasing order, and let

\[
V_\lambda(q) = \sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^\lambda.
\]

then

\[
V_2(q) \ll \phi(q)P^{-2} = qP^{-1}.
\]

More generally

\[
V_\lambda(q) \ll qP^{1-\lambda}.
\]

For \( \lambda < 2 \) this was derived by Hooley [4]. Hausman and Shapiro [5] gave weaker upper bounds for \( V_2 \). Finally Montgomery and Vaughan [6] in 1986 proved the conjecture for all \( \lambda \).

In this paper we investigate the distribution of of \( s \)-tuples of reduced residues which in some sense are similar to \( s \)-tuples of primes and we prove the analogy of Erdős’s conjecture for \( s \)-tuple reduced residues.

Let \( D = \{h_1, h_2, \cdots, h_s\} \) and \( \nu_p(D) \) be the number of distinct elements in \( D \mod p \). \( D \) is called admissible if \( \nu_p(D) < p \) for all primes \( p \). We call \( a + h_1, \ldots, a + h_s \) an \( s \)-tuple of reduced residues if they are each coprime with \( q \).

**Theorem 0.1.** Let \( q \) be a square-free number and \( D = \{h_1, h_2, \cdots, h_s\} \) be a fixed admissible set of integers. Let \( a_1 < a_2 < \cdots \) be those integers for which \( a_i + h_1, \ldots, a_i + h_s \) is an \( s \)-tuple of reduced residues. Then

\[
V^D_\lambda(q) := \sum_{i=1}^{\phi_D(q)} (a_{i+1} - a_i)^\lambda \ll \phi_D(q)P^{-s\lambda}
\]

where \( \phi_D(q) := \prod_{p|q}(p-\nu_p(D)) \), and the implied constant depends on \( D \) and \( \lambda \).

The theorem follows immediately for \( q \) non-square-free as well, by considering the result for \( Q = \prod_{p|q} p \). Motivated by Theorem 0.1 the analogy of this result for primes is:
Conjecture. Let \( p_1, \ldots \) be the set of primes for which \( p_i + h_j \) are prime for all \( h_j \in D \). We have

\[
\sum_{p_n < x} (p_{n+1} - p_n)^\lambda \ll_D x (\log x)^{\lambda(\lambda-1)+\epsilon}.
\]

As an application of distribution of \( s \)-tuples of reduced residues, in the last section we will improve the exponential sum estimate and consequently we prove results about distribution of squares modulo square-free number \( q \) and in general case of the Chinese Reminder Theorem. A few authors had worked on distribution of spacing between squares modulo \( q \). For \( q \) prime, a theorem of Davenport (see [11]) shows that the probability of two consecutive quadratic residues modulo \( q \) being spaced \( h \) units apart is \( 2^{-h} \), as \( q \) goes to infinity. For \( q \) be square-free Kurlberg and Rudnick [12] proved that distribution of spacing between squares goes to Poisson distribution as \( \omega(q) \to \infty \).

Roughly speaking they proved that if \( s_q = \) \# \{ \( s \) : \( s \) is square modulo \( q \) \}, and \( I \) is an interval in \( \mathbb{R} \) not having zero, then

\[
\frac{\#\{ (s_1, s_2) : s_1 - s_2 \in s_q I : s_1, s_2 \text{ are squares modulo } q \}}{\#\{ s \ : \ s \text{ is a square modulo } q \}} = |I|.
\]

Where for \( q \) square-free, \( s \) is a square modulo \( q \) if and only if \( s \) is a square modulo \( p \) for all primes \( p \) dividing \( q \). Here we give a sharp estimate about distribution of squares modulo \( q \).

**Theorem 0.2.** Let \( q \) be a square-free number and \( P = \phi(q)/q \). Then

\[
\sum_{n=0}^{q-1} \left( \sum_{n+m \equiv 1 \mod q}^h 1 - \frac{h}{2^{\omega(q)}P} \right)^2 \leq \frac{q \omega(q)P^h}{2^{\omega(q)}P} (0.2)
\]

**Remark 0.1.** In the case that \( q \) is prime, if the higher moments of (0.2) persist, it would imply Vinogradov’s conjecture about the smallest quadratic non residue. However, it looks like the moments will not persist.

More general question would be about the distribution of the set \( \Omega_q \) which just occupies congruent classes in a particular set (say \( \Omega_p \)) modulo each prime \( p \) dividing \( q \). Granville and Kulberg [8] proved that if \( \Omega_p \) is well distributed modulo \( p \) then then the spacings between elements in the sets \( \Omega_q \) become Poisson distributed as \( q/\Omega_q \to \infty \). In the last section (Theorem 4.1) we show that if for \( a \neq 0 \mod p \) we have that

\[
\left| \sum_{x \in \Omega_p} e(\frac{ax}{p}) \right| < c'_p \sqrt{p} \quad (0.3)
\]
for all \( p \mid q \), then \( \Omega_q \) is well distributed modulo \( q \). We show that this condition is necessary:

Let \( D^* = \{ h_1, h_2, \ldots, h_s \} \) be an admissible set such that

\[
D^*_p := \{ h \mod p : h \in D \} = \{ 0, 2, 4, \ldots, p - 1 \},
\]

for all \( p \mid q \). The probability that a random number modulo \( p \) does not belong to \( D^*_p \) is \( \frac{p - 1}{2p} \approx \frac{1}{2} \), and the probability that a random number modulo \( p \) does not belong to \( D^*_p \) for all \( p \mid q \) is

\[
\prod_{p \mid q} \frac{p - 1}{2p} \approx \frac{1}{2^{\omega(q)}}.
\]

Now consider the interval \((n, n + h]\). It is expected that the number of elements in this interval, which do not belong to any congruent classes in \( D^*_p \) for \( p \mid q \) is

\[
h \prod_{p \mid q} \frac{p - 1}{2p} = h \prod_{p \mid q} \frac{(1 - \frac{1}{p})}{2^{\omega(q)}}.
\]

Therefore, if these numbers are well distributed we expect to have

\[
\sum_{m \in (n, n + h], \ m \not\equiv D^*_p \mod p} 1 - \frac{hP}{2^{\omega(q)}} = o\left( \frac{hP}{2^{\omega(q)}} \right), \quad (0.4)
\]

in average over \( n \). Here as a corollary we show that that without the condition \((0.3)\) we would not have uniform distribution.

**Corollary 0.1.** Let \( q = p_1, \ldots, p_{\lfloor \log X \rfloor} \), where \( X < p_i < 2X \) and \( |p_2 - p_1| \ll \log p_1 \). For \( h < \frac{X^2}{\log X} \) we have

\[
q - 1 \left( \sum_{m \in (n, n + h], \ m \not\equiv D^*_p \mod p} 1 - \frac{hP}{2^{\omega(q)}} \right)^2 \gg q \left( \frac{hP}{2^{\omega(q)}} \right)^2.
\]

**Remark 0.2.** The set \( D^* \) is well distributed modulo \( p \) but it does not satisfy the condition \((0.3)\).
Acknowledgments

I am grateful to my advisor Andrew Granville for his support and helpful comments. Additionally, I would like to thank Dimitris Koukoulopoulos and Vorrapan Chandee for their careful analysis of my paper and their useful suggestions. Special appreciation for the Université de Montréal’s staff, my colleagues and friends, Mohammad Bardestani, François Charetté, Dimitri Dias, Daniel Fiorilli, Kevin Henriot, and Marzieh Mehdizadeh, for their support. Finally, I would like to dedicate this paper in loving memory of my father, Yahya Aryan, whom I lost last spring.

1 An exponential sum estimate

In this section we prove a preliminary estimate about the distribution of \( s \)-tuples of reduced residues, using exponential sums. The estimate we derive here is valid for every choice of \( q \), but this estimate is not the best we will give. We will prove a better estimate, using this exponential sum estimate, in section 3.

**Lemma 1.1.** Define \( k_q(m) \) as follows:

\[
k_q(m) = \begin{cases} 
1 & \text{if } \gcd(m, q) = 1, \\
0 & \text{otherwise}.
\end{cases}
\]

Then we have

\[
k_q(m) = P \sum_{r|q} \left( \sum_{0 \leq a < r} e \left( \frac{a}{r} \right) \frac{\mu(r)}{\phi(r)} \right)
\]

*Proof.* We have

\[
k_q(m) = \sum_{s|(m,q)} \mu(s) = \sum_{s|q} \frac{\mu(s)}{s} \sum_{0 \leq b < s} e \left( \frac{b}{s} \right),
\]

therefore

\[
k_q(m) = \sum_{r|q} \left( \sum_{0 < a \leq r \ (a,r)=1} e \left( \frac{a}{r} \right) \right) \left( \sum_{s} \frac{\mu(s)}{s} \right).
\]

Since

\[
\sum_{r|q} \frac{\mu(s)}{s} = P \frac{\mu(r)}{\phi(r)},
\]

we can deduce

\[
k_q(m) = P \sum_{r|q} \left( \sum_{0 < a \leq r \ (a,r)=1} e \left( \frac{a}{r} \right) \right) \frac{\mu(r)}{\phi(r)}.
\]
This completes the proof of the Lemma.

Remark 1.1. Important to note that \( \nu_p(D) \leq s \) with equality if \( p > h_s - h_1 \).

Also if \( D \) is admissible, then

\[
\frac{1}{p} \leq 1 - \frac{\nu_p(D)}{p} \leq 1 - \frac{1}{p}
\]

and we have that

\[
\prod_{p \leq h_s - h_1} \frac{1}{p} \leq \prod_{p \leq h_s - h_1} \left(1 - \frac{\nu_p(D)}{p}\right) \leq \prod_{p \leq h_s - h_1} \left(1 - \frac{1}{p}\right).
\]

Since \( h_s \) and \( h_1 \) are fixed integers, we therefore have

\[
\prod_{p \leq h_s - h_1} \left(1 - \frac{\nu_p(D)}{p}\right) \sim_{D} \prod_{p \leq h_s - h_1} \left(1 - \frac{1}{p}\right)^s.
\]

Moreover, if \( p > h_s - h_1 \) then \( 1 - \frac{\nu_p(D)}{p} = 1 - \frac{s}{p} \), so that

\[
\prod_{p > h_s - h_1} \left(1 - \frac{\nu_p(D)}{p}\right) = \prod_{p > h_s - h_1} \left(1 - \frac{s}{p}\right) \sim_{D} \prod_{p > h_s - h_1} \left(1 - \frac{1}{p}\right)^s.
\]

Putting these together we deduce that

\[
\frac{\phi_D(q)}{q} \sim_{D} \left(\frac{\phi(q)}{q}\right)^s = P^s.
\]

Now we state the Lemma which we will prove at the end of this section:

**Lemma 1.2.** Let

\[
M_k^D(q, h) = \sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - h \prod_{p \mid q} \left(1 - \frac{\nu_p(D)}{p}\right)^k \right).
\]

Then we have that

\[
M_k^D(q, h) \ll q k^{k/2} P^{-\frac{s}{2} k + k},
\]

where the implicit constant depends on \( k \) and \( s \).
In order to go toward the proof we use exponential sums to better understand the admissible set \( \mathcal{D} = \{ h_1, h_2, \ldots, h_s \} \). Also we need to prove some lemmas. We have that

\[
k_q(m) = \sum_{r \mid q} \left( \sum_{0 < a \leq r \atop (a, r) = 1} e\left( \frac{ma}{r} \right) \frac{\mu(r)}{\phi(r)} \right)
\]

by lemma 1.1. Thus,

\[
k_q(m + h_1) = \sum_{r \mid q} \left( \sum_{0 < a \leq r \atop (a, r) = 1} e\left( \frac{ma + h_1a}{r} \right) \frac{\mu(r)}{\phi(r)} \right)
\]

\[
k_q(m + h_s) = \sum_{r \mid q} \left( \sum_{0 < a \leq r \atop (a, r) = 1} e\left( \frac{ma + h_sa}{r} \right) \frac{\mu(r)}{\phi(r)} \right).
\]

So we deduce that

\[
k_q(m + h_1) \cdots k_q(m + h_s)
= \sum_{r_1, r_2, \ldots, r_s \mid q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i \atop (a_i, r_i) = 1} \left( \sum_{i=1}^{s} a_i \frac{h_i}{r_i} \right) e\left( m \sum_{i=1}^{s} a_i \frac{x}{r_i} \right) e\left( \sum_{i=1}^{s} h_i \frac{a_i}{r_i} \right).
\]

By summing the left-hand side of (1.1) we have

\[
\sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s)
= \sum_{r_1, r_2, \ldots, r_s \mid q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i \atop (a_i, r_i) = 1} \left( \sum_{i=1}^{s} a_i \frac{h_i}{r_i} \right) e\left( m \sum_{i=1}^{s} a_i \frac{x}{r_i} \right) e\left( \sum_{i=1}^{s} h_i \frac{a_i}{r_i} \right) e\left( n \left( \sum_{i=1}^{s} a_i \frac{x}{r_i} \right) \right)
\]

\[
= \sum_{r_1, r_2, \ldots, r_s \mid q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i \atop (a_i, r_i) = 1} \left( E_h \left( \sum_{i=1}^{s} a_i \frac{x}{r_i} \right) \right) e\left( \sum_{i=1}^{s} h_i \frac{a_i}{r_i} \right) e\left( n \left( \sum_{i=1}^{s} a_i \frac{x}{r_i} \right) \right),
\]

where

\[
E_h(x) = \sum_{m=1}^{h} e(mx).
\]
To proceed with the argument we have to consider the case \( \sum_{i=1}^{s} \frac{a_i}{r_i} \in \mathbb{Z} \) to extract the main term from the sum. We have that

\[
P^s \sum_{r_1,r_2,\ldots,r_s | q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i, \quad (a_i, r_i) = 1 \quad \sum_{i=1}^{s} \frac{a_i}{r_i} \in \mathbb{Z}} \left( E_h \left( \sum_{i=1}^{s} a_i \frac{h_i}{r_i} \right) e \left( n \left( \sum_{i=1}^{s} \frac{a_i}{r_i} \right) \right) \right)
\]

\[
= h P^s \sum_{r_1,r_2,\ldots,r_s | q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i, \quad (a_i, r_i) = 1 \quad \sum_{i=1}^{s} \frac{a_i}{r_i} \in \mathbb{Z}} e \left( \sum_{i=1}^{s} h_i \frac{a_i}{r_i} \right), \quad (1.2)
\]

since \( E_h(r) = h \) for all integers \( r \). Now, we need to use Lemma 3 of [10] (due to Hardy and Littlewood). Hardy and Littlewood proved that

\[
\mathcal{S}_q(D) = \sum_{r_1,r_2,\ldots,r_s | q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i, \quad (a_i, r_i) = 1 \quad \sum_{i=1}^{s} \frac{a_i}{r_i} \in \mathbb{Z}} e \left( \sum_{i=1}^{s} h_i \frac{a_i}{r_i} \right)
\]

where \( \mathcal{S} \) is the singular series

\[
\mathcal{S}_q(D) = \prod_{p \mid q} \left( 1 - \frac{1}{p} \right)^{-s} \left( 1 - \frac{\nu_p(D)}{p} \right).
\]

Using this we have

\[
\sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - h \prod_{p \mid q} \left( 1 - \frac{\nu_p(D)}{p} \right)
\]

\[
= P^s \sum_{r_1,r_2,\ldots,r_s | q} \frac{\mu(r_1) \cdots \mu(r_s)}{\phi(r_1) \cdots \phi(r_s)} \sum_{0 < a_i \leq r_i, \quad (a_i, r_i) = 1 \quad \sum_{i=1}^{s} \frac{a_i}{r_i} \in \mathbb{Z}} \left( E_h \left( \sum_{i=1}^{s} a_i \frac{h_i}{r_i} \right) e \left( n \left( \sum_{i=1}^{s} \frac{a_i}{r_i} \right) \right) \right)
\]
and, consequently,
\[
\left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - h \prod_{p|q} \left( 1 - \frac{\nu_p(D)}{p} \right) \right)^k
\]
(1.3)
\[
P^{ks} \sum_{r_{i,j} \in \mathbb{Z}} \left( \prod_{i,j} \frac{\mu(r_{i,j})}{\phi(r_{i,j})} \right) \sum_{i,j}
\left( E_h \left( \sum_{j=1}^{k} \frac{a_{1,j}}{r_{1,j}} \right) \cdots E_h \left( \sum_{j=1}^{s} \frac{a_{k,j}}{r_{k,j}} \right) e \left( \sum_{j} h_j \frac{a_{i,j}}{r_{i,j}} \right) \right)
\times e \left( n \left( \sum_{i,j} \frac{a_{i,j}}{r_{i,j}} \right) \right).
\]

Summing (1.3) over \( n \mod q \) and using the fact that when \( q \sum_i \rho_i \in \mathbb{Z} \)
\[
\sum_{n=0}^{q-1} e(n \left( \sum_i \rho_i \right)) = 0
\]
unless \( \sum_i \rho_i \in \mathbb{Z} \), we have that
\[
q^{ks} \sum_{r_{i,j} \in \mathbb{Z}} \left( \prod_{i,j} \frac{\mu(r_{i,j})}{\phi(r_{i,j})} \right) \sum_{i,j}
\left( E_h \left( \sum_{j=1}^{k} \frac{a_{1,j}}{r_{1,j}} \right) \cdots E_h \left( \sum_{j=1}^{s} \frac{a_{k,j}}{r_{k,j}} \right) e \left( \sum_{j} h_j \frac{a_{i,j}}{r_{i,j}} \right) \right).
\]

Let \( F(x) = \min(h, \frac{1}{\|x\|}) \) where \( \|x\| \) is the distance between \( x \) and the closest integer to \( x \). We have that \( |E_h(x)| \leq F(x) \), and consequently
\[
q^{ks} \sum_{r_{i,j} \in \mathbb{Z}} \sum_{\|r_{i,j}\| = r} \frac{S(\{r_{i,j}\})}{\prod \phi(r_{i,j})}
\]
(1.4)
where
\[
S(\{r_{i,j}\}) = \sum_{0 < a_{i,j} \leq r_{i,j}, (a_{i,j},r_{i,j})=1} \sum_{s_j=1}^{\sum a_{i,j}} \sum_{r_{i,j} \notin \mathbb{Z}} \sum_{i,j} \frac{a_{i,j}}{r_{i,j}} e \left( n \left( \sum_{i,j} \frac{a_{i,j}}{r_{i,j}} \right) \right)
\]
Lemma 1.3. Every element of the form

$$\sum_{j=1}^{s} \frac{a_{i,j}}{r_{i,j}} \quad \text{where} \quad 0 < a_{i,j} \leq r_{i,j}$$

can be written as

$$\frac{a}{[r_{i,1}, r_{i,2}, \ldots, r_{i,s}]} \quad \text{mod} \quad 1,$$

where $1 \leq a \leq [r_{i,1}, r_{i,2}, \ldots, r_{i,s}]$, and each fraction that has such a representation has exactly $r_{i,1}r_{i,2} \cdots r_{i,s}$ representations.

By $r_{i,1}r_{i,2} \cdots r_{i,s}$ representations we mean that the equation

$$\sum_{j=1}^{s} \frac{a_{i,j}}{r_{i,j}} = \tau \quad \text{mod} \quad 1$$

has exactly $r_{i,1}r_{i,2} \cdots r_{i,s}$ different answers, if it has any.

Proof. Let $d = (r_1, r_2)$ and we call $r'_i = \frac{r_i}{d}$ for $i = 1, 2$. For fixed $a, b$ we are interested in the number of solutions for the equation

$$\frac{a}{r_1} + \frac{b}{r_2} = \frac{x}{r_1} + \frac{y}{r_2} \quad \text{mod} \quad 1$$

where $1 \leq x \leq r_1$ and $1 \leq y \leq r_2$, which leads us to the number of solutions of

$$ar'_2 + br'_1 \equiv xr'_2 + yr'_1 \quad \text{mod} \quad r'_1r'_2d. \quad (1.5)$$

We have $a \equiv x \quad \text{mod} \quad r'_1$ and $b \equiv y \quad \text{mod} \quad r'_2$. Let $x = a + ir'_1$ and $y = b + jr'_2$. Then by using (1.5) we have

$$(a - x)r'_2 \equiv (y - b)r'_1 \quad \text{mod} \quad r'_1r'_2d.$$ 

Therefore we have $i + j \equiv 0 \quad \text{mod} \quad d$, which has exactly $d$ solutions. So we conclude that, given $a$ and $b$, there are exactly $d$ solutions $(x, y)$ with $1 \leq x \leq r_1$ and $1 \leq y \leq r_2$ to the equation

$$\frac{a}{r_1} + \frac{b}{r_2} = \frac{x}{r_1} + \frac{y}{r_2} \quad \text{mod} \quad Z.$$ 

Obviously $\frac{a}{r_1} + \frac{b}{r_2} \quad \text{mod} \quad 1 \in \left\{ \frac{t}{[r_1, r_2]} : 0 \leq t \leq [r_1, r_2] \right\}$ and as showed above, each element is repeated exactly $d = \frac{r'_1r'_2}{[r_1, r_2]}$ times. This proves the lemma for $s = 2$. Using induction, we have that

$$\frac{a_{i,1}}{r_{i,1}} + \cdots + \frac{a_{i,k-1}}{r_{i,k-1}} = \frac{a}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k-1}]}.$$
with exactly $\frac{[r_{i,1}, r_{i,2}, \ldots, r_{i,k-1}]}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k}]}$ repetitions each. And, by the first part of the proof there are exactly \\

$\frac{[r_{i,1}, r_{i,2}, \ldots, r_{i,k-1}]}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k}]}$ \text{ repetitions each. And, by the first part of the proof there are exactly}\\n
$\frac{[r_{i,1}, r_{i,2}, \ldots, r_{i,k-1}]}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k}]}$ \text{ ways to write} $a_{i,1} \frac{1}{r_{i,1}} + \cdots + a_{i,k} \frac{1}{r_{i,k}}$ as $\frac{a}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k}]} + a_{i,k} \frac{1}{r_{i,k}}$ (mod1). Now the total \text{ number of repetitions is}\\n
$\frac{[r_{i,1}, r_{i,2}, \ldots, r_{i,k-1}]}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k}]} \times \frac{[r_{i,1}, r_{i,2}, \ldots, r_{i,k-1}]}{[r_{i,1}, r_{i,2}, \ldots, r_{i,k}]} = \frac{r_{i,1}r_{i,2}\cdots r_{i,k}}{r_{i,1}r_{i,2}\cdots r_{i,k}}$\\n
Now our task is to bound (1.4), for which we need to use the idea of Montgomery and Vaughan’s Fundamental Lemma [6], slightly modified. In order to do that we use Lemma 2 from [10, Page 596].\\n
**Lemma 1.4.** Let $q_1, \ldots, q_k$ be square-free integers, each one strictly greater than 1, and put $d = [q_1, \ldots, q_k]$. Let $G$ be a complex-valued function defined on $(0, 1)$, and suppose that $G_0$ is a nondecreasing function on the positive integers such that\\n
$\sum_{a=1}^{q-1} |G(a/q)|^2 \leq qG_0(q)$,\\n
for all square-free integers $q > 1$. Then\\n
$\left| \sum_{\substack{a_1, \ldots, a_k \geq 0 \leq q_i \leq q, \sum a_i = Z}} G(a_i/q_i) \right| \leq \frac{1}{d} \prod_{i=1}^{k} q_i G_0(q_i)^{1/2}$.\\n
We now need to verify that $F$ satisfies the requirements for $G$ in the Lemma 1.4 Lemma 4 of [6] asserts that\\n
$\sum_{0 < a < q} F\left(\frac{a}{q}\right)^2 \ll q \min(q, h)$.\\n
Since $\min(q, h)$ is obviously a non-decreasing function of $q$, we can use Lemma 1.4 with $F$ and $\min(q, h)$ in place of $G$ and $G_0$ respectively. About the condition $q_i > 1$, note that, since we apply Lemma 1.4 for $q_i = [r_{i,1}, \ldots, r_{i,s}]$ and we have $\sum_{j=1}^{s} \frac{a_{i,j}}{r_{i,j}} \notin Z$, then $q_i = [r_{i,1}, \ldots, r_{i,s}] \neq 1$. From Lemma 1.3
we have
\[
S(\{r_{i,j}\}_{i,j}) = \sum_{0 < a_{i,j} \leq r_{i,j}} \sum_{j=1}^{s} F\left(\frac{a_{1,j}}{r_{1,j}}\right) \cdots F\left(\frac{a_{k,j}}{r_{k,j}}\right)
\]
\[
\leq T \sum_{0 < a_i \leq [r_{i,1}, \ldots, r_{i,s}]} \sum_{j=1}^{s} F\left(\frac{a_i}{r_{i,1}}\right) \cdots F\left(\frac{a_i}{r_{i,s}}\right),
\]
where
\[
T = \frac{r_{1,1} \cdots r_{1,s}}{[r_{1,1}, \ldots, r_{1,s}]} \cdots \frac{r_{k,1} \cdots r_{k,s}}{[r_{k,1}, \ldots, r_{k,s}]}.
\]

Now using Lemma 1.4 with \(G = F\) and \(q_i = [r_{i,1}, \ldots, r_{i,s}]\), we have that
\[
S(\{r_{i,j}\}_{i,j}) \ll \frac{r_{1,1} \cdots r_{k,s} h^{k/2}}{r} \tag{1.7}
\]
Now we are ready to prove Lemma 1.2.

**Proof of Lemma 1.2** We prove the result with \(q\) square-free. Then the Lemma follows for \(q\) non-square-free immediately by considering the result for \(Q = \prod_{p | q} p\). Now using relations (1.4) and (1.7), we have that
\[
\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - h \prod_{p | q} \left(1 - \frac{\nu_p(D)}{p}\right) \right)^k
\]
\[
\ll q^{P_k s} \sum_{r | q} \frac{1}{r} \sum_{r' | r} \phi(r) \phi(r', r) h^{k/2}
\]
\[
\leq q^{P_k s} \sum_{r | q} \frac{1}{r} \left( \sum_{r' | r} \phi(r') \right)^{k_s} h^{k/2} = q h^{k/2} P_k s \prod_{p | q} \left(1 + \frac{1}{p} \left(2 + \frac{1}{p - 1}\right)^{k_s}\right)
\]
\[
\ll q h^{k/2} P^{-2 q^s + k_s}.
\]

2 A probabilistic estimate

In this section we prove an estimate about the distribution of s-tuples of reduced residues using a probabilistic method. The estimate derived here
is valid only when $q$ is not divisible by any small prime, and in this case it is the best possible we can have. In particular, it’s much better than our earlier exponential sum estimate in this range.

Let $X_i$, for $1 \leq i \leq h$, be independent identically distributed random variables such that

$$\text{Prob}(X_i = 1) = 1 - \text{Prob}(X_i = 0) = P.$$ 

Then

$$X = X_1 + \cdots + X_h$$

is called a \textit{binomial random variable}. Given such a random variable $X$, we denote with $\mu_k(h, P)$ its $k$-th moment about its mean, that is to say,

$$\mu_k(h, P) := \mathbb{E}((X - hP)^k).$$

**Lemma 2.1.** Let $A$ be a set of $h$ integers and $h_1 < \cdots < h_s$. Suppose that for each prime divisor $p$ of $q$ we have $p > \max A - \min A + h_s - h_1$. Suppose also that $p > y$ for all $p|q$. Then for $y > h^k$ and for each fixed even $k > 1$

$$M_k^D(q, h) = \sum_{n=0}^{q-1} \left( \sum_{\substack{m \in A \\ (n+m+h_i, q) = 1 \\ 1 \leq i \leq s}} 1 - h\left(\frac{\phi(q)}{q}\right)^s\right)^k \ll q\left(h\left(\frac{\phi(q)}{q}\right)^s\right)^{\lfloor k/2 \rfloor} + qh\left(\frac{\phi(q)}{q}\right)^s,$$

which the implicit constant depends on $k$ and $|h_1 - h_s|$.

**Remark 2.1.** Under the conditions of Lemma 2.1 it provides a better estimate than Lemma 1.2. Indeed Lemma 1.2 yields the estimate

$$M_k^D(q, h) \ll qh^{k/2}P^{-2k_s+ks}$$

whereas by Lemma 2.1 we have that

$$M_k^D(q, h) \ll q\left(hP^s\right)^{\lfloor k/2 \rfloor} + qhP^s.$$ 

Comparing two bounds and using the fact that $q\left(hP^s\right)^{\lfloor k/2 \rfloor} \leq qh^{k/2}P^{-2k_s+ks}$ proves the point.

**Proof.** The proof is similar to the proof of Lemma 9 in [6], with a small variation which we explain. We have that

$$\sum_{\substack{m \in A \\ (m+h_i, q) = 1 \\ 1 \leq i \leq s}} 1 - hP^s = \sum_{1 \leq j \leq H} \left( \sum_{\substack{m \in A_j \\ (m+h_i, q) = 1 \\ 1 \leq i \leq s}} 1 - |A_j|P^s \right)$$

13
where
\[ A_j = \{ m \in A : m \equiv j \pmod{H} \}, \]
where \( H = |h_s - h_1| + 1 \). From Hölder’s inequality with, \( \frac{1}{k} + \frac{1}{k'} = 1 \), we have that
\[
\left| \sum_{i=1}^{H} a_i \right| \leq H^{k-1} \left( \sum_{i=1}^{H} |a_i|^k \right)^{\frac{1}{k}}
\]
and, consequently,
\[
\left( \sum_{m \in A_j} \left( 1 - h^{P^s} \right) \right)^k \leq H^{k-1} \sum_{1 \leq j \leq H} \left( \sum_{m \in A_j} \left( 1 - |A_j|^{P^s} \right) \right)^k.
\]
Now we focus on
\[
S_j = \sum_{n=0}^{q-1} \left( \sum_{m \in A_j} \left( 1 - |A_j|^{P^s} \right) \right)^k.
\]
We note that
\[
S_j = \sum_n \sum_r \left( \sum_{m \in A_j} \left( 1 - |A_j|^{P^s} \right) \right)^k
\]
Moreover, we have that
\[
\left( \sum_{m \in A_j} \left( 1 - |A_j|^{P^s} \right) \right)^k = \sum_{m_1, \ldots, m_r \in A_j} \left( \sum_{1 \leq i \leq s} \right)^k
\]
We will show that \( m_l + h_i \neq m_{l'} + h_{i'} \) for \( m_l \neq m_{l'} \). Without loss of generality, we assume that \( m_l < m_{l'} \) and therefore \( m_l + h_i < m_{l'} + h_{i'} \). This is true since \( m_l - m_{l'} \equiv 0 \pmod{H} \) and thus \( |m_l - m_{l'}| \geq H > |h_i - h_{i'}| \).
Now we claim that \( m_l + h_i \neq m_{l'} + h_{i'} \pmod{p} \) for all \( p|q \). Assume, on the contrary, that
\[
m_l + h_i \equiv m_{l'} + h_{i'} \pmod{p}
\]
for some \( p|q \). Then we have that \( p|m_l + h_i - (m_{l'} + h_{i'}) \). We already have shown \( m_l + h_i - (m_{l'} + h_{i'}) \neq 0 \), therefore
\[
p \leq |m_l - m_{l'}| + |h_i - h_{i'}|,
\]
14
which contradicts our assumption that $p > \max A - \min A + h_s - h_1$.

Applying these facts and changing the order of summation in $S_j$, we have that

$$
\sum_{n=0}^{q-1} 1 = \prod_{p \mid q} (p - st),
$$

(2.2)

where $t = \# \{m_1, \ldots, m_r\}$. Let $S(r, t)$ denote the Stirling number of the second kind, i.e. the number of ways of partitioning a set of cardinality $r$ into exactly $t$ non-empty subsets. Following the proof of Lemma 9 in [6], $S(r, t)!$ is the number of surjective maps from a set of cardinality $r$ to a set of cardinality $t$. We set $S(r, 0) = 0$ so that we have

$$
\sum_{n=0}^{q-1} \sum_{m_1, \ldots, m_r \in A_j} 1 \leq i \leq s \leq j \leq r
$$

As there are $(|A_j|)$ possible choices for $B$, the above is

$$
q \sum_{t=0}^{r} \binom{|A_j|}{t} S(r, t)! P^{st} \prod_{p \mid q} \left(1 - \frac{st}{p}\right) \left(1 - \frac{1}{p}\right)^{-st}
$$

and, since $p > y > h_s - h_1$ we have that

$$
\prod_{p \mid q} \left(1 - \frac{st}{p}\right) \left(1 - \frac{1}{p}\right)^{-st} = 1 + O_{st} \left(\frac{1}{y}\right)
$$

From Lemma 9 in [6, page.326] we have that

$$
S_j = q \sum_{r=0}^{k} \binom{k}{r} (-|A_j|) |P^s|^{k-r} \sum_{t=0}^{r} \binom{|A_j|}{t} S(r, t)! (P)^{st} \left(1 + O_{st} \left(\frac{1}{y}\right)\right)
$$

and

$$
q \sum_{r=0}^{k} \binom{k}{r} (-|A_j|) |P^s|^{k-r} \sum_{t=0}^{r} \binom{|A_j|}{t} S(r, t)! (P)^{st} = \mu_k(|A_j|, P^s)
$$

using [6, page.327]. Thus

$$
S_j = q \sum_{r=0}^{k} \binom{k}{r} (-|A_j|) |P^s|^{k-r} \sum_{t=0}^{r} \binom{|A_j|}{t} S(r, t)! (P)^{st} \left(1 + O_{st} \left(\frac{1}{y}\right)\right)
$$

$$
= q \mu_k \left(|A_j|, P^s\right) + O \left\{ \frac{q}{y} \left(hP^s\right)^k + hP^s \right\},
$$

15
using the fact that $|A_j| \leq h$. For the error term the dependence of the implicit constant on $t$ can be considered to be a dependence on $k$, since $t < s < k$ we also use
\[
\frac{q}{y} \sum_{t=0}^{r} \left( \frac{|A_j|}{t} \right) P^{st} \ll \frac{q}{y} \left( (h^s)^r + hP^s \right)
\]
Next note that Lemma 11 of \[6\] states that, for any fixed integer $k > 0$, \(\mu_k(h, P) \ll (hP)^{[k/2]} + hp\), uniformly for $0 < P < 1$, $h = 1, 2, 3, ...$. So
\[
\mu_k(|A_j|, P^s) \ll (|A_j|P^s)^{[k/2]} + |A_j|P^s \leq (hP^s)^{[k/2]} + hP^s.
\]
Using this and our assumption that $y > h^k$, we find that
\[
\sum_{n=0}^{q-1} \left( \sum_{m \in A \atop (n+m+h_i,q)=1} 1 - hP^s \right)^k \leq q \left( hP^s \right)^{[k/2]} + qhP^s, \tag{2.3}
\]
which concludes the proof of the Lemma. \qed

3 Proof of Theorem 0.1

In this section we will prove a estimate about the distribution of $s$-tuples of reduced residues, by combining both our probabilistic and exponential sum estimates. The new estimate that we derive here is valid for every $q$ and it is better than our exponential sum estimate. Using this estimate, we will be able to prove Theorem 0.1.

Lemma 3.1. Let $k$ be a given even number, and fix constant $A > k$. Let $q_1 = \prod_{p \mid q \atop p \leq y} p$ and $q_2 = \prod_{p \mid q \atop p > y} p$, where $h^A > y > h^k$. Correspondingly we set \(P_i = \frac{\phi(q_{i,1})}{q_{i,1}}\) for $i = 1, 2$. For $h > P^{-1}$ we have
\[
M_k^D(q, h) \ll q(hP^s)^{[k/2]} + qh(P)^s + qh^{k/2}P_1^{-2k^i + ks}P_2^{sk}.
\]
And the implicit constant depends on $k$ and $s$.

Proof. Since $q$ is square-free we have $q = q_1q_2$ and $(q_1, q_2) = 1$. By the Chinese Remainder Theorem we have that
\[
M_k^D(q, h) = \sum_{n_1=0}^{q_1-1} \sum_{n_2=0}^{q_2-1} D(n_1, n_2)^k,
\]
where
\[ D(n_1, n_2) = \sum_{m=1}^{h} \left( 1 - h \prod_{p/q} \left( 1 - \frac{\nu_p(D)}{p} \right) \right). \]

Following \[6\], we may write \( D = D_1 + D_2 \) where
\[ D_1 = \prod_{p/q_2} \left( 1 - \frac{\nu_p(D)}{p} \right) \sum_{m=1}^{h} \left( 1 - h \prod_{p/q} \left( 1 - \frac{\nu_p(D)}{p} \right) \right) \]
\[ D_2 = \prod_{p/q_2} \left( 1 - \frac{\nu_p(D)}{p} \right) \sum_{m=1}^{h} \left( 1 - h \prod_{p/q} \left( 1 - \frac{\nu_p(D)}{p} \right) \right) \]

From Holder’s inequality we have \( D_k \leq 2^k(D_1^k + D_2^k) \), and consequently
\[ M_k^D(q, h) \ll \sum_{n_1} \sum_{n_2} D_1^k + \sum_{n_1} \sum_{n_2} D_2^k. \]

Since \( D_1 \) is independent of \( n_2 \), we have that
\[ \sum_{n_1} \sum_{n_2} D_1^k \ll q_2 P_2^{k_1} M_k^D(q_1, h), \quad (3.1) \]

which by Lemma \[1,2\] leads to
\[ \sum_{n_1} \sum_{n_2} D_1^k \ll q_2 P_2^{k_1} q_1 h^{k/2} P_1^{k_1-2k} = q h^{k/2} P_1^{k_1-2k} P_2^{k_1}. \]

To estimate \( \sum_{n_1} \sum_{n_2} D_2^k \) let
\[ A_{n_1} = \{ 1 \leq m \leq h : (n_1 + m + h_j, q_1) = 1, 1 \leq j \leq s \}. \]

Note that the size of \( A_{n_1} \) is
\[ \sum_{m=1}^{h} \left( 1 - h \prod_{p/q_2} \left( 1 - \frac{\nu_p(D)}{p} \right) \right) \mid A_{n_1} \right)^k. \]

which, by a simple sieve argument, is \( \ll h P_1^k \). Therefore
\[ \sum_{n_2} D_2^k = \sum_{n_2} \left( \sum_{m \in A_{n_1}} \left( 1 - h \prod_{p/q_2} \left( 1 - \frac{\nu_p(D)}{p} \right) \right) \mid A_{n_1} \right)^k. \]
Now, since \( y > h^k \) and \( p | q_2 \), we have that \( p > h^k \) and consequently
\[
\prod_{p | q_2} \left(1 - \frac{\nu_p(D)}{p}\right) = \prod_{p | q_2} \left(1 - \frac{s}{p}\right) = \prod_{p | q_2} \left(1 - \frac{1}{p}\right)^s \left(1 + O\left(\frac{1}{y}\right)\right).
\]

Next we need to use Lemma 2.1 with \( A = A_{n_1} \) and \( q = q_2 \). In order to do this we need to verify that \( p > \max A_{n_1} - \min A_{n_1} + h_s - h_1 \) for all \( p | q_2 \). We have that \( \max A_{n_1} - \min A_{n_1} \leq h \) and, since for \( p | q_2 \) we have \( p > y > h^k \), it suffices to verify that \( h + H < h^k \). This is true because \( H \) is fixed, \( k \geq 2 \) and \( h > P^{-1} \). (Note that we may assume \( P^{-1} > H \) else, otherwise, \( P^{-1} \) is bounded and we can deduce the result desired here from Lemma 1.2.) Using Lemma 2.1, we have that
\[
\sum_{n_2} D_2^k \ll q_2 \left(|A_{n_1}| \left(\frac{\phi(q_2)}{q_2}\right)^s\right)^{[k/2]} + q_2 |A_{n_1}| \left(\frac{\phi(q_2)}{q_2}\right)^s.
\]

Since \( |A_{n_1}| \ll h P^s \), we have that
\[
\sum_{n_2} D_2^k \ll q_2 \left(h P^s\right)^{[k/2]} + q_2 h P^s,
\]
consequently we have that (with \( P = \frac{\phi(q)}{q} \))
\[
\sum_{n_1} \sum_{n_2} D_2^k \ll q(h P^s)^{[k/2]} + q h P^s.
\]

Finally, we arrive at our desired estimate
\[
M_k^D(q, h) \ll q(h P^s)^{[k/2]} + qh(P)^s + qh^{k/2} P_1^{-2k_s + k_s} P_2^{s_k}. \tag{3.2}
\]

Now, Using above estimate we will prove Theorem 0.1. Let \( a_1 < a_2 < \cdots \) be the integers, such that \( a_i + h_j \) is co-prime to \( q \) for each \( h_j \in D \). Let
\[
L(x) = \# \{ i : 1 \leq i \leq \phi_D(q), a_{i+1} - a_i > x \}.
\]

We have that
\[
V^D_\lambda(q) = \lambda \int_0^\infty L(x)x^{\lambda-1} \, dx.
\]

Obviously, \( L(x) \leq \prod_{p | q}(p - \nu_p(D)) < CqP^s \) for some constant \( C = C(D) \). Therefore for \( x < P^{-1}D \) (with \( P_D = \prod_{p | q} \left(1 - \frac{\nu_p(D)}{p}\right) \)), since \( P_D \gg P^s \), we have that
\[
\lambda \int_0^{P^{-1}D} L(x)x^{\lambda-1} \ll qP^s \int_0^{P^{-1}D} x^{\lambda-1} \ll q(P^s)^{1-\lambda}.
\]
To bound \( L(x) \) for larger \( x \), we note that if \( a_{i+1} - a_i > h \), for some integer \( h \). Then
\[
\sum_{m=1}^{h} 1 - hP_p = -hP_p
\]
for \( a_i \leq n < a_{i+1} - h \). Let \( k \) be a fixed even integer bigger than \( 2\lambda \). Then
\[
\sum_{i=1}^{qP_D} (a_{i+1} - a_i - h)(hP_p)^k \leq M^D_k(q, h). \tag{3.3}
\]
If \( h = \lfloor \frac{x}{2} \rfloor \) and \( a_{i+1} - a_i > x \), then \( a_{i+1} - a_i - h > h \), so the left-hand side of (3.1) is \( \geq h(hP_p)^kL(x) \). Combining this with our estimate in Lemma 3.1 yields
\[
x(P_P)^kL(x) \ll q((xP_p)^{h/2} + x^{k/2}P^{2k}\lambda_1).
\]
Now for \( x < e^{P-\alpha} \), if \( y = x^{2k} + 1 \) where, \( \alpha = \frac{ks}{2^{k-1}} \), then we have
\[
P_1^{-1} = \left( \prod_{p<\sqrt{y}} (1 - \frac{1}{p}) \right)^{-1} \ll \log y \ll \log x \ll P^{-\alpha}.
\]
Therefore
\[
P_1^{-2k} \ll (P^{-\alpha})^{2k} \ll P^{-\frac{4k}{2}}.
\]
So we have
\[
L(x) \ll \frac{qP_D}{(xP_p)^{\frac{k}{2}+1}}.
\]
By integrating both sides we deduce that
\[
\int_{P_0^{-1}}^{e^{P-\alpha/k}} L(x)x^{\lambda-1}dx \ll \int_{P_0^{-1}}^{e^{P-\alpha/k}} \frac{qP_D}{(xP_p)^{\frac{k}{2}+1}} x^{\lambda-1}dx.
\]
Since \( \frac{k}{2} + 1 > \lambda \) we have
\[
\int_{P_0^{-1}}^{P^{-\alpha/k}} L(x)x^{\lambda-1}dx \ll qP_1^{1-\lambda} \ll q(P^{\alpha})^{1-\lambda}.
\]
For larger \( x \) we use Lemma 1.2, which gives us that
\[
M^D_k(q, h) \ll q h^{1/2} P^{-2ks+k\lambda}.
\]
Therefore we have
\[
L(x) \ll \frac{qP^{-2ks}}{x^{\frac{k}{2}+1}}.
\]
and
\[
\int_{e^{P-\alpha/k}}^{\infty} L(x)x^{\lambda-1}dx \ll qP^{-2k} \int_{e^{P-\alpha/k}}^{\infty} \frac{x^{\lambda-1}}{x^2+1}dx
\]
So taking \( k = 2\lceil \lambda \rceil + 1 \) implies that
\[
\int_{e^{P-\alpha/k}}^{\infty} L(x)x^{\lambda-1}dx \ll qP^{-2k} \ll q(Ps)^{1-\lambda},
\]
for \( P^{-1} \) large enough, which finishes the proof.

4 Main estimates

In this section we prove a sharper estimate about the distribution of \( s \)-tuples of reduced residues. First we prove a Lemma then as an applications of the Lemma and other techniques in previous sections we prove results about distribution of squares and general sets in context of Chinese reminder theorem. We finish the discussions in this paper with using the Lemma to write the \( \mathcal{M}_k(q,h) \) in a way, that we are able to use Lemma 7 in [6] to achieve a sharper estimate.

Lemma 4.1. Let \( D = \{h_1, \cdots, h_s\} \) be an admissible set,
\[
k_q(m + h_1) \cdots k_q(m + h_s) = P_D \sum_{r | q} \frac{\mu(r)}{\phi_D(r)} \sum_{a < r \atop (a,r) = 1} e\left(m \frac{a}{r}\right) \mu_D(a, r).
\]
For
\[
\mu_D(a, r) = \prod_{p | r} \left( \sum_{s \in \mathcal{D}_p} e\left(sa(r/p)^{-1}_{p}\right) \right).
\]
Where \( \phi_D(r) = \prod_{p | r} (p - \nu_p(D)) \) and \( (r/p)^{-1}_{p} \) is the inverse of \( r/p \) in \( \mathbb{Z}_p \) and \( \mathcal{D}_p \) consist of elements of \( D \) modulo \( p \).

Proof. We have that
\[
k_q(m) = \sum_{r | q} \frac{\mu(r)}{r} \sum_{0 \leq b < r} e\left(m \frac{b}{r}\right),
\]
therefore
\[
k_q(m + h_1) \cdots k_q(m + h_s) = \sum_{r | q \atop a_i < r \atop (a_i,r) = 1} e\left(m \frac{a_1}{r_1}\right) \cdots \sum_{r | q \atop a_s < r \atop (a_s,r) = 1} e\left(m \frac{a_s}{r_s}\right) \mu(r_1) \cdots \mu(r_s) \sum_{0 < a_i \leq r_i \atop \sum_{i=1}^{s} \frac{a_i}{r_i} = \frac{m}{r}} e\left(\sum_{i=1}^{s} \frac{a_i}{r_i}\right).
\]
It is enough to show that
\[ \sum_{r_1,r_2,\ldots,r_s \mid q} \frac{\mu(r_1) \cdots \mu(r_s)}{r_1 \cdots r_s} \sum_{0 \leq a_i \leq r_i} e\left( \sum_{i=1}^{s} h_i \frac{a_i}{r_i} \right) \]  
(4.1)
\[ = \prod_{r \mid q} \frac{\mu(r)}{\phi(r)} \prod_{p \mid r} \left( \sum_{a \in \mathbb{F}_p} e\left( sa(r/p)^{-1} \right) \right). \]

To show this, note that we can write
\[ \frac{a}{r} \equiv \sum_{p \mid r} \frac{a_p}{p} \pmod{1} \]
uniquely where 0 ≤ a_p < p. Fix p_0 | r, we have that \[ \frac{a}{r} \equiv \frac{a_0}{p_0} \pmod{1}, \]
then a ≡ a_0 (r/p_0) (mod p_0), since r is square free \( \left( \frac{r}{p_0} \right) = 1 \), for a_0 ≠ 0, we have that a_0 ≡ a (r/p_0)^{-1} (mod p_0). Using uniqueness, we can can write
(4.1) in terms of prime divisors of q, and it is equal to
\[ \prod_{p \mid q} \sum_{q_i \mid p} \frac{\mu(q_1) \cdots \mu(q_s)}{q_1 \cdots q_s} \sum_{0 \leq a_i \leq q_i} e\left( \sum_{i=1}^{s} h_i \frac{a_i}{q_i} \right). \]

To simplify the condition \( \sum \frac{a_i}{q_i} = \frac{a_p}{p} \), we write
\[ \sum_{0 \leq a_i < q_i} e\left( \sum_{i=1}^{s} h_i \frac{a_i}{q_i} \right) = \prod_{r \mid q} \left( \sum_{0 \leq a_i < q_i} e\left( \frac{a_p}{p} - \sum_{i=1}^{s} \frac{a_i}{q_i} \right) \right) \]
Therefore (4.1) equals to
\[ \prod_{p \mid q} \sum_{q_i \mid p} \frac{\mu(q_1) \cdots \mu(q_s)}{q_1 \cdots q_s} \sum_{r=1}^{p} \frac{1}{p} \sum_{0 \leq a_i < q_i} e\left( \frac{a_p}{p} - \sum_{i=1}^{s} \frac{a_i}{q_i} \right) e\left( \sum_{i=1}^{s} h_i \frac{a_i}{q_i} \right) \]
\[ = \prod_{p \mid q} \sum_{r=1}^{p} e\left( \frac{a_p}{p} \right) \prod_{i=1}^{s} \frac{\mu(q_i)}{q_i} \sum_{0 \leq a < q} e\left( \frac{a}{q} (h_i - r) \right) \]
\[ = \prod_{p \mid q} \sum_{r=1}^{p} e\left( \frac{a_p}{p} \right) \prod_{i=1}^{s} \left( 1 - \frac{1}{p} \sum_{a \leq p} e\left( \frac{a}{p} (h_i - r) \right) \right) \]
\[ = \prod_{p \mid q} \sum_{r \mid h_i \mod p \atop r \neq h_i \mod p} e\left( \frac{a_p}{p} \right) \frac{\phi(q) r}{q \phi(r)} \prod_{p} \frac{\mu(p)}{p} \sum_{s \equiv h_i \mod p \atop h_i \in \mathbb{D} \atop a_p \neq 0} \frac{a_p}{p}. \]
The last equality is true since \( a_p = 0 \) for \( p \nmid r \), and for \( a_p \neq 0 \) we have that
\[
\sum_{\substack{r = 1 \\ r \neq h_i \mod p \\ h_i \in D}}^p e(r \frac{a_p}{p}) = - \sum_{s \in D_p} e(s \frac{a_p}{p}).
\]

As an application of distribution of \( s \)-tuples of reduced residues and Lemma 4.1, we prove results about distributions of some special set modulo square-free number \( q \).

**Distribution of squares modulo \( q \)**

For \( q \) square-free, \( x \) is a square modulo \( q \) if and only if \( x \) is a square modulo \( p \) for all primes \( p \) dividing \( q \). For each \( p \) which divides \( q \), let \( D_p := \{ h_1, p, \cdots, h_{\nu_p}, p \} \). Using Chinese Remainder Theorem it is not hard to see that we can find the set \( D = \{ h_1, \cdots, h_s \} \), such that \( D \) modulo \( p \) equals to \( D_p \), for all \( p | q \). Now if
\[
k_q(m + h_1) \cdots k_q(m + h_s) = 1,
\]
then \( m \neq -h_i, p \mod p \), for \( 1 \leq i \leq \nu_p \) and for all \( p \) divides \( q \). Coming back to squares, let \( D_p := \{ -n_1, \cdots, -n_{\nu_p-1} \} \), where \( n_i \) is quadratic non-residue modulo \( p \). From \( k_q(m + h_1) \cdots k_q(m + h_s) = 1 \), follows that \( m \) is a square modulo \( q \). Using Lemma 4.1 we have that
\[
k_q(m + h_1) \cdots k_q(m + h_s) = \prod_{\substack{r = q \\ r \equiv q \mod p}}^p \sum_{\mu(r) \frac{p+1}{2}} \sum_{a < r} e \left( m \frac{a}{r} \right) \mu_D(a, r)
\]
\[
= \frac{1}{2^{\omega(q)} P} \sum_{\mu(r) \frac{p+1}{2}} \sum_{a < r} e \left( m \frac{a}{r} \right) \mu_D(a, r).
\]

where \( P = \frac{\phi(q)}{q} \). Consequently using the same technique in 4.2 we have that
\[
\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - \frac{h}{2^{\omega(q)} P} \right)^2 =
\]
\[
\frac{q}{4^{\omega(q)} P^2} \sum_{r_1, r_2 \equiv 1} \mu(r_1) \mu(r_2) \sum_{a_1 < r_1} \mu_D(a_1, r_1) \mu_D(a_2, r_2)
\]
\[
E \left( \frac{a_1}{r_1} \right) E \left( \frac{a_2}{r_2} \right) \mu_D(a_1, r_1) \mu_D(a_2, r_2)
\]
\[
\sum_{a_1, a_2 \in \mathbb{Z}} \delta_{a_1 + a_2 \equiv 1, 2 \mod r_1 + r_2}
\]

22
Proof of Theorem 0.2. From the condition \( \frac{a_1}{r_1} + \frac{a_2}{r_2} \in \mathbb{Z} \) follows that \( r_1 = r_2 \) and \( a_2 = r - a_1 \), and we have

\[
\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} 1 - \frac{h}{2^{\omega(q)} P} \right)^2 = \frac{q}{4^{\omega(q)} P^2} \sum_{r|q} \prod_{p|r} (p + 1)^2 \sum_{a<r} \left| E \left( \frac{a}{r} \right) \mu_D(a, r) \right|^2.
\]

(4.3)

Now, we need to bound \( \mu_D(a, r) \). For each \( n_i \) in \( D_p \) we have

\[
\left( -n_i a(r/p)^{-1} \right) = -\left( -\frac{1}{p} \right) a \left( \frac{r}{p} \right) \left( \frac{r/p}{p} \right),
\]

and since \( a \neq 0 \) the sequence \( \{ -n_i a(r/p)^{-1} \} \) is either a sequence of quadratic residue or quadratic non-residue. Using the Gauss bound for exponential sum over quadratic residue and respectively non-residue \([9, \text{Page 13}]\), we have

\[
\left| \sum_{s \in D_p} e \left( \frac{sa(r/p)^{-1}}{p} \right) \right| \leq \frac{\sqrt{p}}{2^{\omega(r)}}.
\]

Consequently, for \( a \neq 0 \), we have that

\[
|\mu_D(a, r)| \leq \frac{\sqrt{p}}{2^{\omega(r)}}.
\]

(4.4)

Using this in (4.3) we have

\[
\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} 1 - \frac{h}{2^{\omega(q)} P} \right)^2 \leq \frac{q}{4^{\omega(q)} P^2} \sum_{r|q} \prod_{p|r} (p + 1)^2 \sum_{a<r} \left| E \left( \frac{a}{r} \right) \mu_D(a, r) \right|^2
\]

and finally using \( \sum_{a<r} \left| E \left( \frac{a}{r} \right) \right|^2 < r \min(r, h) \), we have

\[
\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} 1 - \frac{h}{2^{\omega(q)} P} \right)^2 \leq \frac{q}{2^{\omega(q)} P} h.
\]
The general case

Assume that $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$, by the Chinese Reminder Theorem there exist $\prod_{p \mid q}(p - |\Omega(p)|)$ numbers less than $q$, such that they do not occupy any congruent classes in $\Omega_p$ modulo $p$. A natural question to ask is about their distribution modulo $q$. Lemma 4.1 shows the connection between the distribution of these numbers and the exponential sum over elements in $\Omega_p$. Let $D = \{h_1, \cdots, h_s\}$ be a set such that $D_p = -\Omega_p$, if $k_q(m+h_1) \cdots k_q(m+h_s) = 1$, then $m$ is not congruent to any member of $\Omega_p$ modulo $p$. Now we take a look at the distribution of such numbers,

$$\sum_{m=1}^{h} k_q(m + h_1) \cdots k_q(m + h_s) = \prod_{p \mid q} \frac{p - |\Omega_p|}{p} \sum_{r \mid q} \frac{\mu(r)}{\prod_{p \mid r}(p - |\Omega_p|)} \sum_{a < r, (a, r) = 1} E \left( \frac{ma}{r} \right) \mu_D(a, r).$$

For the distribution of such numbers we have

$$\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - \prod_{p \mid q} \frac{p - |\Omega_p|}{p} \right)^2 = q \prod_{p \mid q} \left( \frac{p - |\Omega_p|}{p} \right)^2 \sum_{r \mid q, r > 1} \frac{1}{\prod_{p \mid r}(p - |\Omega_p|)^2} \sum_{0 < a < r, (a, r) = 1} \left| E_{\frac{a}{r}} \left( \frac{a}{r} \right) \mu_D(a, r) \right|^2.$$

**Theorem 4.1.** Assume that for each $p \mid q$, $|\Omega_p| = c_p p$ with $(p - |\Omega_p|) > p^{1/2 + \epsilon}$, and $|\mu_D(a, p)| < c_p' \sqrt{p}$, where $c_p, c_p' < 1$, then we have that

$$\sum_{n=0}^{q-1} \left( \sum_{m \in \{n, n + h\}, m \notin \Omega_p} \left( \frac{p - |\Omega_p|}{p} \right) \right)^2 \leq qh \prod_{p \mid q} (1 - c_p)^2 + c_p^2.$$

**Proof.** Using the assumption we have

$$\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - \prod_{p \mid q} \frac{p - |\Omega_p|}{p} \right)^2 = q \prod_{p \mid q} \left( \frac{p - c_p p}{p} \right)^2 \sum_{r > 1} \frac{h \prod_{p \mid r}(c_p')^2}{\prod_{p \mid r}(p - c_p p)^2} = qh \prod_{p \mid q} (1 - c_p)^2 \sum_{r > 1} \prod_{p \mid r} \left( \frac{c_p'}{1 - c_p} \right)^2$$

$$= qh \prod_{p \mid q} (1 - c_p)^2 \left( 1 + \left( \frac{c_p'}{1 - c_p} \right)^2 \right) = qh \prod_{p \mid q} (1 - c_p)^2 + c_p^2.$$

Which finishes the proof of the theorem.
Note that Theorem 4.1 is effective for $p - |\omega_p| > p^{1/2+\epsilon}$.

**Remark 4.1.** The condition $|\mu_D(a, p)| < c'_p\sqrt{p}$, known as Weyl’s criterion, implies uniform distribution of $\Omega_p$ modulo $p$.

**Remark 4.2.** In general for the distribution of the image of the polynomial $F$, one can use Theorem 4.1 if $|\text{Image of } F| = c_p p$ and also if $|\mu_D(a, p)| < c'_p\sqrt{p}$.

For a $F$ of degree $d$, A. Weil [14], proved that

$$
\sum_{0 \leq x < p} e(F(x/p)) < (d - 1)\sqrt{p},
$$

Under some conditions on $F$.

Now we come back to what we started, Let $D = \{h_1, \ldots, h_s\}$ be a fix admissible set, we have that

$$
q^{-1} \sum_{n=0}^{q-1} \left( \sum_{m=1}^{k} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - hP_D \right)^k = qP_D^k \sum_{r_1/q}^{r_i>1} \left( \prod_{i=1}^{k} \mu_D(r_i) \right) \sum_{0 < a_i \leq r_i}^{(a_i, r_i) = 1} \left( E_h\left( \frac{a_1}{r_1} \right) \mu_D(a_1, r_1) \cdots E_h\left( \frac{a_k}{r_k} \right) \mu_D(a_k, r_k) \right),
$$

where

$$
\mu_D(a, r) = \prod_{p|r} \left( \sum_{s \equiv h_i \mod p} e\left( sa(r/p)^{-1} \right) \right).
$$

Since $|\mu_D(a, r)| \leq \omega(r)$ we have

$$
M^D_k(q, h) \ll qP_D^k \sum_{r_1/q}^{r_i>1} \left( \prod_{i=1}^{k} \mu_D(r_i) \right) \sum_{0 < a_i \leq r_i}^{(a_i, r_i) = 1} \sum_{s \equiv h_i \mod p} e\left( sa(r/p)^{-1} \right) F\left( \frac{a_1}{r_1} \right) \cdots F\left( \frac{a_k}{r_k} \right). \quad (4.5)
$$

**Theorem 4.2.** For $h < e^{1/p^{1/2}}$ we have

$$
M^D_k(q, h) \ll q(hP^s)^{k/2} \quad (4.6)
$$

and in general

$$
M^D_k(q, h) \ll qh^{k/2} P^{s(k-1/2)} \quad (4.7)
$$

25
Proof. We use Lemma 7 and 8 in [6] to bound
\[
\sum_{0 < a_i \leq r_i}
\frac{a_i}{r_i} F\left(\frac{a_1}{r_1}\right) \cdots F\left(\frac{a_k}{r_k}\right)
\]
in (4.5). First we focus on diagonal configuration, 
\((r_1 = r_2 = r_3 = r_4, \cdots, r_{k-1} = r_k \text{ and } r_2, r_4, \cdots, r_k \text{ are relativity co-prime})
\). In non-diagonal configuration Lemma 7 in [6] allows us to save a small power of \(h\). In the diagonal configuration we have that
\[
\sum_{0 < a_i \leq r_i}
\frac{a_i}{r_i} F\left(\frac{a_1}{r_1}\right) \cdots F\left(\frac{a_k}{r_k}\right) \leq \sum_{0 < a_1 \leq r_1} F\left(\frac{a_1}{r_1}\right)^2 \sum_{0 < a_{k-1} \leq r_{k-1}} F\left(\frac{a_{k-1}}{r_{k-1}}\right)^2
\]
\[
\leq r_1 r_3 \cdots r_{k-1} h^{k/2} = [r_1 r_3 \cdots r_{k-1}] h^{k/2}.
\]
Consequently in the diagonal configuration (4.5) is less than \(q P k^D (q, h) \ll q h^{k/2} P^{sk - s^2 k/2} (1 + h^{-\frac{1}{P}} P^{-sk})\).

Now applying Lemma 7 in [6] we have
\[
M_k^D (q, h) \ll q h^{k/2} P^{sk - s^2 k/2} (1 + h^{-\frac{1}{P}} P^{-sk}).
\]
To achieve a sharper estimate we need a better estimate of
\[
\sum_{a \leq X} |\mu_D(a, r)|^2.
\]
Putting (4.9) in (3.1) gives a sharper estimate than (3.2)
\[
M_k^D (q, h) \ll_k q (h P^{s})^{k/2} + q h P^s + q h^{k/2} P^{sk - s^2 k/2} (1 + h^{-\frac{1}{P}} P^{sk}) P^{sk}.
\]
Now by considering \(y = h^k\) in Lemma 3.1 we have (4.7) and for \(h < e^{k P^{1/2}}\), we have (4.3), which completes the proof of the theorem.

Remark 4.3. For the constant depending on \(k\), see [10] and in the special case \(q\) composed only of prime factors \(p \geq h\) see [13].
We finish this section with the proof of the Corollary 0.1

Proof. Let $\frac{a}{r} = \sum_{p|r} \frac{a_p}{p}$, for $a_p = \frac{p \pm 1}{2}$, since $D^*_p = \{0, 2, \cdots, p-1\}$, applying Lemma 4.1 we have that

$$|\mu_{D^*}(a, r)| = \prod_{p|r} \left| \sum_{s \in D^*_p} e^{\frac{sa_p}{p}} \right| = \prod_{p|r} \left| \frac{e\left(\frac{1}{2p}\right) + 1}{e\left(\frac{1}{2p}\right) - 1} \right| \geq \frac{p}{\pi} \quad (4.10)$$

Here, similar to square case we have $P_{D^*} = \frac{\omega(q)}{2\omega(q)} P$ and $\phi_{D^*}(r) = \prod_{p|r} \frac{p - 1}{2}$ consequently using (4.10) and similar to (4.2) and (4.3) we have that

$$\sum_{n=0}^{q-1} \left( \sum_{m=1}^{h} k_q(n + m + h_1) \cdots k_q(n + m + h_s) - \frac{hP}{2\omega(q)} \right)^2$$

$$= \frac{qP^2}{2\omega(q)} \sum_{r|q, r > 1} \left( \frac{1}{\prod_{p|r} \frac{p - 1}{2}} \right)^2 \sum_{0 < a \leq r \atop (a, r) = 1} \left| E_h \left( \frac{a}{r} \right) \mu_{D^*}(a, r) \right|^2$$

$$\geq \frac{qP^2}{2\omega(q)} \sum_{r|q, r > 1} \frac{4\omega(r)r^2}{\phi(r)^2 \pi 2\omega(q)} \sum_{a_p = \pm \frac{1}{2} \atop p|r} \left| E_h \left( \sum_{p|r} \frac{1}{2} \pm \frac{1}{2} \right) \right|^2 \quad (4.11)$$

Now, for $r$ such that $\omega(r)$ be even and $\| \sum_{p|r} \pm \frac{1}{p} \| \ll 1/h$, we have that is

$$\left| E_h \left( \sum_{p|r} \frac{1}{2} \pm \frac{1}{2} \right) \right|^2 \gg h^2$$

and consequently (4.11) is

$$\gg \frac{qP^2}{2\omega(q)} h^2 \sum_{r|q, r > 1} \frac{4\omega(r)r^2}{\phi(r)^2 \pi 2\omega(q)} \| \sum_{p|r} \pm \frac{1}{p} \| \ll 1/h$$

Now let $r = p_1p_2$, with $a_{p_1} = \frac{p_1 + 1}{2}$ and $a_{p_2} = \frac{p_2 - 1}{2}$ we have

$$\| \frac{p_1 + 1}{2p_1} + \frac{p_2 - 1}{2p_2} \| = \| \frac{1}{2p_1} - \frac{1}{2p_2} \| \ll \frac{\log X}{X^2} \ll \frac{1}{h}.$$
which implies that
\[ qP^2 \gg \frac{2^\omega(q)}{2^\omega(q)} h^2. \]

This finishes the proof of Corollary.

Remark 4.4. We picked \( h = \frac{X^2}{\log X} \), so that the expectation of
\[ \# \{ m \in (n, n + h) : m \not\equiv D^* p \mod p, \text{ for all } p | q \} \]
which is
\[ h \prod_{p | q} \frac{p + 1}{2p} = \frac{X^2 P}{2^{\lfloor \log X \rfloor} \log X}, \]
be greater than 1.

Remark 4.5. In the case of \( q = \prod_{p < z} p \), with small effort one can prove that
there exist a set \( D \), with \( |D_p| \approx p/2 \) and
\[ \sum_{n=0}^{q-1} \left( \sum_{m \in [n, n+h], m \not\equiv D^*_p \mod p, \text{ for all } p | q} 1 - \frac{hP}{2^\omega(q)} \right)^2 \gg q \left( \frac{P}{2^\omega(q)} \right)^2 h^{2-\epsilon}. \]

But showing Corollary 0.1 for \( D^* \), where \( q = \prod_{p < z} p \), does not seem to be possible.

References

[1] H. Cramer, On the order of magnitude of the difference between consecutive prime numbers. Acta Arithmetica. (1936): 23–46.

[2] A. Granville, Harold Cramer and the distribution of prime numbers. Scandinavian Actuarial J. 1995, no. 1, pages 12-28.

[3] P. Erdős, The difference of consecutive primes. Duke Math. J. 6, (1940). 438–441

[4] C.Hooley, On the difference of consecutive numbers prime to n. Acta Arith. 8 1962/1963 343–347

[5] M. Hausman and H. Shapiro, On the mean square distribution of primitive roots of unity. Comm. Pure Appl. Math. 26 (1973), 539–547.

[6] H. Montgomery and R. Vaughan, On the distribution of reduced residues. Ann. of Math. (2) 123 (1986), no. 2, 311–333.

28
[7] H. Halberstam and H. E. Richert, *Sieve Methods*, London Mathematical Society monographs, No 4(London, New York: Academic Press, 1974).

[8] A. Granville, P. Kurlberg, Poisson statistics via the Chinese remainder theorem. Adv. Math., 218(6):2013-2042, 2008.

[9] H. Davenport, *Multiplicative number theory*, Springer Verlag, 2000.

[10] Hugh L. Montgomery and K. Soundararajan, Primes in short intervals, Comm. Math. Phys. 252 (2004), no. 1-3, 589-617.

[11] H. Davenport, On the distribution of quadratic residues (mod p). J. London Math. Soc. 6 (1931), 49-54; On the distribution of quadratic residues (mod p), J. London Math. Soc. 8 (1933), 46-52.

[12] P. Kurlberg, Z. Rudnick, The distribution of spacings between quadratic residues. Duke Math. J., 100(2):211-242, 1999.

[13] A. Chadozeau, Sur la ré partition des entiers premiers a un entier sans petit facteur premier. J. Number Theory 128 (2008)

[14] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204-207

*E-mail address: farzad.aryan@uleth.ca*