NOTES ON THE DISTRIBUTION OF REDUCED RESIDUE CLASSES

XINGFENG LIN

Abstract. The aim of these notes is to present a study of the distribution of reduced residue classes—one of the central topics in analytic number theory—from a perspective that incorporates methods from other areas of mathematics. We will motivate the problem from the topic of difference of consecutive primes of Cramer, Erdös, and explain the work of Montgomery on reduced residues, with some additional results. The exposition is self-contained, and no prior knowledge of analytic number theory is assumed.

Contents

1. Introduction

Let p_i denotes the i-th prime number. There have been conjectures of bounding the distance between consecutive prime numbers, when the prime numbers are large.

Conjecture 1.1. *Fix $\gamma > 0$, then for $x > 1$,*

$$\sum_{p_i \leq x} (p_{i+1} - p_i)^\gamma \leq Cx(logx)^{\gamma-1},$$

for some constant $C > 0$.

Concerning the more precise estimates, on probabilistic grounds we might conjecture that

$$\#\{p_i \leq x : p_{i+1} - p_i \geq \alpha logp_i\} \sim e^{-\alpha}\frac{x}{logx}$$

for a fixed $\alpha > 0$, $x > 1$. Even stronger, we have the conjecture of Cramer that

$$limsup_{i\to\infty}\frac{p_{i+1} - p_i}{(logp_i)^2} = 1$$

The motivation of studying the distribution of reduced residue classes originates from the problems stated above, in the hope of finding tools to deal with the difference of consecutive primes.

Fix a positive integer q. Let $1 = a_1 < a_2 < \cdots$ be positive integers coprime with q. As an analogue of Conjecture 1.1, we have

Theorem 1.2. *Fix $\gamma > 0$, we have*

$$\sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^\gamma \lesssim_\gamma \phi(q) P^{-\gamma}, \tag{1}$$

where $\phi(q)$ denotes the number of reduced residue classes modulo q, $P := \phi(q)/q$, the probability of a residue class being reduced.

We will prove Theorem 1.2 by studying higher-order moments of the distribution of reduced residue classes in intervals of given length.

Definition 1.3. Fix a positive integer h. For a positive real number k, define the k-th moment of distribution of reduced residue classes to be

$$M_k(q,h) = \sum_{n=1}^{q} \left(\#\{a_i : n < a_i \le n+h\} - Ph\right)^k. \tag{2}$$

We expect that the k-moment satisfies the following estimate:

Conjecture 1.4. *For $h \ge 1/P, k > 0$, we have*

$$M_k(q,h) \lesssim_k q(Ph)^{k/2}. \tag{3}$$

An elementary proof of Conjecture 1.4 for $k = 2$ will be presented in section 2. Actually, Conjecture 1.4 is much stronger than Theorem 1.2. Instead, we will prove a weaker estimate of $M_k(q,h)$ which is also sufficient for our goal.

Theorem 1.5. *For $h \ge 1/P, k > 0$, we have*

$$M_k(q,h) \lesssim_k q(Ph)^{k/2}(1 + P^{k/2}(\log h)^{2^k}). \tag{4}$$

There are two distinct methods that we will apply. One is the probabilistic model, which works fairly well when factors of q are large. The other use Fourier expansion borrowed from harmonic analysis, which works with arbitrary q. Before we embark on the main arguments, some preliminary reductions are in order.

Proposition 1.6. *If Conjecture 1.4 and Theorem 1.5 is verified to be true for q square-free, then they are true for all positive integers.*

Proof. For a positive integer q, let q' be the largest square-free divisor of q. Let $P' = \phi(q')/q'$. Then we have $P' = P$. Therefore, the right hand side of (3)(4) change to the q'/q-mutiple of the original if q is replaced by q'. It suffices to show

$$M_k(q',h) = \frac{q'}{q} M_k(q,h).$$

For any positive integer $a \in (0, q')$ coprime with q', there exist exactly q/q' many $b \in (0, q)$ such that $a \equiv b \ mod \ q'$, and b is thus coprime to q. Therefore,

$$\begin{aligned} M_k(q,h) &= \sum_{k=0}^{q/q'-1} \sum_{kq'<n\leq(k+1)q'} (\#\{a_i : n < a_i < n+h\} - Ph)^k \\ &= \frac{q}{q'} \sum_{0<n\leq q'} (\#\{a_i : n < a_i < n+h\} - Ph)^k \\ &= \frac{q}{q'} M_k(q', h). \end{aligned}$$

□

Proposition 1.7. *Conjecture 1.4 and Theorem 1.5 can be reduced to the case where* $k \in \mathbb{Z}_{>0}$.

Proof. For any positive real number k, let $k' = [k] + 1$. By Holder's inequality we have

$$\left(\frac{1}{q} M_k(q,h)\right)^{1/k} \leq \left(\frac{1}{q} M_{k'}(q,h)\right)^{1/k'}$$

If (3) holds for k', then it follows that (3) holds for k. If (4) holds for k', then

$$\begin{aligned} M_k(q,h) &\leq q \left(\frac{1}{q} M_{k'}(q,h)\right)^{k/k'} \\ &\lesssim_{[k]+1} q(Ph)^{k/2}(1 + P^{k'/2}(logh)^{2^{k'}})^{k/k'} \\ &\leq q(Ph)^{k/2}(1 + P^{k/2}(logh)^{2^k}) \end{aligned}$$

Therefore (4) holds for k. □

We assume q is square-free and k is a positive integer in the following sections unless stated otherwise. It does no harm to assume k is even when necessary.

2. Proof of Conjecture 1.4 for $k = 2$

Theorem 2.1. *For $h \geq 1/P$, we have*

$$M_2(q,h) \leq qPh. \tag{5}$$

Proof. Put $X_n := \sum_{n+1}^{n+h} d(r)$, where

$$d(r) := \begin{cases} 1, & (r,q) = 1 \\ 0, & (r,q) \neq 1. \end{cases}$$

Expanding $M_2(q,h)$, we have

$$\begin{aligned} M_2(q,h) &= \sum_{n=1}^{q} X_n^2 - qP^2h^2 \\ &= \sum_{n=1}^{q} \sum_{r,s=n+1}^{n+h} d(r)d(s) - qP^2h^2. \end{aligned}$$

By interchanging the summations, we have

$$\sum_{n=1}^{q}\sum_{r,s=n+1}^{n+h} d(r)d(s) = h\sum_{r=1}^{q} d(r)^2 + 2\sum_{k=1}^{h-1}(h-k)\sum_{r=2}^{q+1} d(r)d(r+k).$$

Since

$$\begin{aligned}\sum_{r=2}^{q+1} d(r)d(r+k) &= \sum_{r=1}^{q} d(r)d(r+k)\\ &= \#\{0<r<q : (r,q)=1, (r+k,q)=1\}\\ &= q\prod_{p|q,p\nmid k}(1-\frac{2}{p})\prod_{p|(q,k)}(1-\frac{1}{p})\\ &= q\frac{\prod_{p|q}(1-\frac{2}{p})}{\prod_{p|(q,k)}(1-\frac{2}{p})}\prod_{p|(q,k)}(1-\frac{1}{p}),\end{aligned}$$

where one should interpret $\frac{1-\frac{2}{p}}{1-\frac{2}{p}} = 1$ if $p=2$, we have

$$\begin{aligned}\sum_{k=1}^{h-1}(h-k)\sum_{r=2}^{q+1} d(r)d(r+k) &= q\prod_{p|q}(1-\frac{2}{p})\sum_{k=1}^{h-1}(h-k)\prod_{p|(q,k)}(1+\frac{1}{p-2})\\ &= q\prod_{p|q}(1-\frac{2}{p})\sum_{k=1}^{h-1}(h-k)\sum_{d|(q,k)}\frac{\mu^2(d)}{\alpha(d)}\\ &= q\prod_{p|q}(1-\frac{2}{p})\sum_{d|q,d\le h}\frac{\mu^2(d)}{\alpha(d)}\sum_{k\le h,k\equiv 0\ mod\ d}(h-k)\\ &= q\prod_{p|q}(1-\frac{2}{p})\sum_{d|q,d\le h}\frac{\mu^2(d)}{\alpha(d)}\left(h[\frac{h}{d}]-\frac{([\frac{h}{d}]+1)d[\frac{h}{d}]}{2}\right),\end{aligned}$$

where $\alpha(d)=\prod_{p|d}(p-2)$. Write $[h/d] = h/d - \{h/d\}$ and the summation over d as a product, we obtain

$$\begin{aligned}\sum_{k=1}^{h-1}(h-k)\sum_{r=2}^{q+1} d(r)d(r+k) &= q\prod_{p|q}(1-\frac{2}{p})\left(\frac{1}{2}h^2\prod_{p|q}(1+\frac{1}{p(p-2)})-\frac{1}{2}h\prod_{p|q}(1+\frac{1}{p-2})\right)\\ &\quad+\frac{1}{2}q\prod_{p|q}(1-\frac{2}{p})\sum_{d|q}\frac{\mu^2(d)}{\alpha(d)}d\{h/d\}(1-\{h/d\})\\ &= \frac{h^2}{2q}\prod_{p|q}(p-1)^2-\frac{1}{2}h\prod_{p|q}(p-1)+\frac{1}{2}q\prod_{p|q}(1-\frac{2}{p})\sum_{d|q}\frac{\mu^2(d)}{\alpha(d)}d\{h/d\}(1-\{h/d\}).\end{aligned}$$

Note that $h\sum_{r=1}^{q} d(r)^2 = h\prod_{p|q}(p-1), qP^2h^2 = \frac{h^2}{q}\prod_{p|q}(p-1)^2$. We have

$$\begin{aligned} M_2(q,h) &= q\prod_{p|q}(1-\frac{2}{p})\sum_{d|q}\frac{\mu^2(d)}{\alpha(d)}d\{h/d\}(1-\{h/d\}) \\ &\leq qh\prod_{p|q}(1-\frac{2}{p})\sum_{d|q}\frac{\mu^2(d)}{\alpha(d)} \\ &= qPh. \end{aligned}$$

□

By Theorem 2.1 and Proposition 3.1 that we shall prove in the next section, we obtain a partial result that (1) holds for all $0 < \gamma < 2$.

3. Theorem 1.5 implies Theorem 1.2

Proposition 3.1. *Suppose (4) holds for $k > 0$. Then (1) holds for all $\gamma < \frac{k+1}{2}$. In particular, if (4) holds for all $k > 0$, then (1) holds for all $\gamma > 0$.*

Proof. For any positive integer l, Put

$$n(l) := \#\{0 < a_i < q : a_{i+1} - a_i = l\},$$
$$N(l) := \#\{0 < a_i < q : a_{i+1} - a_i \geq l\}.$$

Take $h = l/2$. For any fixed a_i such that $a_{i+1} - a_i \geq l$, we have

$$\#\{a_j : n < a_j \leq n + h\} = 0,$$

for all positive integers $n \in [a_i, a_i + l - h]$. Therefore, we have

$$M_k(q,h) \geq N(l)h(Ph)^k.$$

By (4), we obtain an estimate of $N(l)$

$$N(l) \lesssim_k \phi(q)(Pl)^{-1-k/2}(1 + P^{k/2}(logh)^{2^k}).$$

Therefore, by writing (1) as summation over all positive integers l and apply the estimate above, we have

$$\begin{aligned} \sum_{i=1}^{\phi(q)}(a_{i+1}-a_i)^\gamma &= \sum_{l=1}^{\infty} n(l)l^\gamma \\ &\sim \sum_{l=1}^{\infty} N(l)l^{\gamma-1} \\ &= \sum_{1\geq l\geq \frac{2}{P}} N(l)l^{\gamma-1} + \sum_{l>\frac{2}{P}} N(l)l^{\gamma-1} \\ &\lesssim_k \sum_{1\geq l\geq \frac{2}{P}} \phi(q)l^{\gamma-1} + \sum_{l>\frac{2}{P}} \phi(q)(Pl)^{-1-k/2}l^{\gamma-1}(1 + P^{k/2}(logh)^{2^k}) \\ &\lesssim_{k,\epsilon} \phi(q)P^{-\gamma} + \sum_{l>\frac{2}{P}} \phi(q)(Pl)^{-1-k/2}l^{\gamma-1}(1 + P^{k/2}l^\epsilon) \end{aligned}$$

For $\gamma < 1 + \frac{k}{2} - \epsilon$, the last sum converges. We have

$$\sum_{l>\frac{2}{P}} \phi(q)(Pl)^{-1-k/2} l^{\gamma-1}(1+P^{k/2}l^{\epsilon}) \sim_{\gamma} \phi(q)P^{-1-\frac{k}{2}} \sum_{l>2/P} l^{\gamma-2-k/2} + \phi(q)P^{-1} \sum_{l>2/P} l^{\gamma-2-k/2+\epsilon}$$
$$= \phi(q)P^{-\gamma} + \phi(q)P^{-\gamma+\frac{k}{2}-\epsilon}.$$

Take $\epsilon = 1/2$. Noting that $P < 1$, we obtain

$$\sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^{\gamma} \lesssim_{\gamma} \phi(q)P^{-\gamma},$$

for all $\gamma < \frac{k+1}{2}$, completing the proof. □

4. Proof of Theorem 1.5

4.1. **Probabilistic Model.** Suppose $h > 1/P$. Let $X_1, \cdots, X_h$ be independent random variables with the distribution

$$P(X_m = 1) = P$$
$$P(X_m = 0) = 1 - P,$$

and put $X = X_1 + \cdots + X_h$. Let $\mu_k = \mathbb{E}((X - hP)^k)$ be the k-th moment of X about its mean.

Proposition 4.1. $\mu_k \lesssim_k (hP)^{k/2}$.

Proof. Put $Y_m = X_m - P, m = 1, \cdots, h$, then,

$$\mu_k = \sum_{1 \le m_1, \cdots, m_k \le h} \mathbb{E}(Y_{m_1} \cdots Y_{m_k}).$$

Note that $\mathbb{E}(Y_{m_1} \cdots Y_{m_k}) = 0$ if one of the subsripts turns up only once. We have

$$\mu_k = \sum_{r=1}^{k/2} \sum_{1 \le m_1 < \cdots < m_r \le h} \sum_{\substack{l_1, \cdots, l_r \ge 2 \\ l_1 + \cdots + l_r = k}} \frac{l_1! \cdots l_r!}{k!} \mathbb{E}(Y_{m_1}^{l_1} \cdots Y_{m_r}^{l_r}).$$

For $l \ge 2$, we have $|\mathbb{E}(Y_m^l)| \le 2P$. By the independence of distinct variables, we obtain

$$\mu_k \le \sum_{r=1}^{k/2} (2P)^r \sum_{1 \le m_1 < \cdots < m_r \le h} \sum_{\substack{l_1, \cdots, l_r \ge 2 \\ l_1 + \cdots + l_r = k}} \frac{l_1! \cdots l_r!}{k!}$$
$$\lesssim_k \sum_{r=1}^{k/2} P^r \binom{h}{r}$$
$$\lesssim_k (hP)^{k/2}.$$

Therefore we have the estimate of μ_k. □

To estimate $M_k(q, h)$ when the factors of q are large, assume that all prime factors of q are greater than y, where y is a large positive real number greater than h. Expanding the

binomial terms, we rewrite

$$M_k(q,h) = \sum_{n=1}^{q} \left(\sum_{\substack{m=1 \\ (m+n,q)=1}}^{h} 1 - hP \right)^k$$
$$= \sum_{r=0}^{k} \binom{k}{r} \left(\sum_{n=1}^{q} \left(\sum_{\substack{m=1 \\ (m+n,q)=1}}^{h} 1 \right)^r \right) (-hP)^{k-r},$$

where

$$\sum_{n=1}^{q} \left(\sum_{\substack{m=1 \\ (m+n,q)=1}}^{h} 1 \right)^r = \sum_{\substack{m_1,\cdots,m_r \\ 1\le m_i\le h}} \sum_{\substack{1\le n\le q \\ (n+m_i,q)=1 \\ i=1,\cdots,r}} 1.$$

Fix any $m_1, \cdots, m_r$ and let $s = \#\{m_i\}_{i=1}^r$. Then

$$\sum_{\substack{1\le n\le q \\ (n+m_i,q)=1 \\ i=1,\cdots,r}} 1 = \prod_{p|q} (1 - \frac{s}{p}),$$

since $(s,p) = 1, \forall p|q$. To apply Proposition 4.1, note

$$\sum_{r=0}^{k} \binom{k}{r} \left(\sum_{\substack{m_1,\cdots,m_r \\ 1\le m_i\le h}} qP^s \right) (-hP)^{k-r} = q \sum_{r=0}^{k} \binom{k}{r} \mathbb{E}(X^r(-hP)^{k-r})$$
$$= q\mu_k.$$

Therefore it suffices to compare $\prod_{p|q}(1-\frac{s}{p})$ and $P^s = \prod_{p|q}(1-\frac{1}{p})^s$. Noting that $s \le r \le k$, we have

$$\prod_{p|q}(1 - \frac{s}{p})(1 - \frac{1}{p})^{-s} = 1 + O_k(\sum_{p|q} p^{-2}) = 1 + O_k(y^{-1}),$$

where the constant depending on k is uniform in s. This implies that

$$M_k(q,h) = \sum_{r=0}^{k} \binom{k}{r} \left(\sum_{\substack{m_1,\cdots,m_r \\ 1\le m_i\le h}} qP^s \left(1 + O_k(y^{-1})\right) \right) (-hP)^{k-r}$$
$$= q\mu_k + O_k(y^{-1} q\mu_k).$$

This proves Conjecture 1.4 with an additional assumption that all prime factors of q are larger than some positive integer $y > h$. If prime factors of q are small ($p|q, p < h$ happens, for example), we need a basic inequality in number theory, which is called the fundamental lemma.

4.2. **Fourier Techniques and the Fundamental Lemma.** Suppose f is a complex-valued function on positive integers having period q. We define the Fourier coefficients to

be

$$\hat{f}(a/q) = \frac{1}{q}\sum_{n=1}^{q} f(n)e(-an/q),$$

for $a/q \in \mathbb{Z}/q$. Every element in $\mathbb{Z}/q$ can be uniquely represented by some a/r with $0 < a < r+1, (a,r) = 1$. Thus, we can write the Fourier expansion of f as

$$\begin{aligned} f(n) &= \sum_{r|q} \sum_{0<a\leq r,(a,r)=1} \hat{f}(a/r)e(an/r) \\ &= \sum_{r|q} \sum_{\rho\in(\mathbb{Z}/r)^\times} \hat{f}(\rho)e(\rho n). \end{aligned}$$

To apply Fourier methods, we consider $f(n) := \#\{a_i : n < a_i \leq n+h\} - Ph$, and wish to estimate the k-th moment of f. Expanding $f(n)^k$, we have

$$\begin{aligned} \sum_{n=1}^{q} f(n)^k &= \sum_{n=1}^{q} \left(\sum_{r|q} \sum_{\rho\in(\mathbb{Z}/r)^\times} \hat{f}(\rho)e(\rho n) \right)^k \\ &= \sum_{r_1,\cdots,r_k|q} \sum_{\substack{\rho_i\in(\mathbb{Z}/r)^\times \\ i=1,\cdots,k}} (\prod_{i=1}^{k} \hat{f}(\rho_i)) \sum_{n=1}^{q} e((\rho_1+\cdots+\rho_k)n) \\ &= q \sum_{r_1,\cdots,r_k|q} \sum_{\substack{\rho_i\in(\mathbb{Z}/r_i)^\times \\ i=1,\cdots,k \\ \sum\rho_i=0}} \prod_{i=1}^{k} \hat{f}(\rho_i), \end{aligned}$$

noting that $\sum_{n=1}^{q} e((\rho_1+\cdots+\rho_k)n)$ vanishes if $\sum_{i=1}^{k}\rho_i \neq 0$. To estimate a sum of this expression, we employ the following inequality.

Lemma 4.2. *Let $r_1,\cdots,r_k$ be positive square-free integers, $r = lcm(r_i)_{i=1}^k$, such that every prime factor of r divides at least two of the r_i. Suppose G_i are complex-valued functions on $\mathbb{Z}/r_i$, $i = 1,\cdots,k$, respectively. Then,*

$$\left| \sum_{\substack{\rho_i\in\mathbb{Z}/r_i \\ i=1,\cdots,k \\ \sum\rho_i=0}} \prod_{i=1}^{k} G_i(\rho_i) \right| \leq \frac{1}{r}\prod_{i=1}^{k} \left(r_i \sum_{\rho_i\in\mathbb{Z}/r_i} |G_i(\rho_i)|^2 \right)^{1/2}. \tag{6}$$

Lemma 4.2 can be used to prove the following result:

Theorem 4.3. *For $h \geq 1/P$, we have*

$$M_k(q,h) \lesssim_k q h^{k/2} P^{k-2^k}. \tag{7}$$

Proof. Write $f(n) = P\sum_{r|q}\frac{1}{\phi(r)}\sum_{\rho\in(\mathbb{Z}/r)^\times} E(\rho)e(\rho n)$, we see that the coefficients of f are

$$\hat{f}(\rho) = P\frac{1}{\phi(r)}E(\rho),$$

where $E(\rho)=\sum_{m=1}^{h}e(\rho m)$. For any k-tuple $(r_1,\cdots,r_k)$ with each r_i dividing q such that $p|lcm(r_i)$ implies p divides at least two of the r_i, the fundamental lemma gives

$$\left|\sum_{\substack{\rho_i\in(\mathbb{Z}/r_i)^\times\\ i=1,\cdots,k\\ \sum\rho_i=0}}\prod_{i=1}^{k}\hat{f}(\rho_i)\right|\leq P^k\frac{\prod_{i=1}^{k}r_i^{1/2}}{lcm(r_i)\prod_{i=1}^{k}\phi(r_i)}\prod_{i=1}^{k}\left(\sum_{\rho_i\in(\mathbb{Z}/r_i)^\times}|E(\rho_i)|^2\right)^{1/2} \tag{8}$$

We claim that $\sum_{\rho_i\in(\mathbb{Z}/r_i)^\times}|E(\rho_i)|^2\lesssim r_ih$. In fact, since $|E(\rho)|\leq min\{h,\frac{1}{\|\rho\|}\}$, where $\|\rho\|$ denotes the distance of ρ from the nearest integer, we have

$$\begin{aligned}\sum_{\rho_i\in(\mathbb{Z}/r_i)^\times}|E(\rho_i)|^2&\leq\sum_{\rho_i\in\mathbb{Z}/r_i-\{0\}}|E(\rho_i)|^2\\&\leq h^2(\frac{r_i}{h})+r_i^2(\frac{1}{(r_i/h)^2}+\frac{1}{(r_i/h+1)^2}+\cdots+\frac{1}{[r_i/2]^2})\\&\sim r_ih.\end{aligned}$$

Therefore, the right hand side of (8) is

$$\lesssim_k h^{k/2}P^k\frac{1}{lcm(r_i)}\prod_{i=1}^{k}\frac{r_i}{\phi(r_i)}.$$

Since $\hat{f}$, when viewed as a function on $\mathbb{Z}/r_i$, is supported on $(\mathbb{Z}/r_i)^\times$, $\sum_{i=1}^{k}\rho_i=0$ cannot happen for any $\rho_i\in(\mathbb{Z}/r_i)^\times$ if there exists a prime p dividing one and only one of the r_i. This would forces the left hand side of (8) to be 0. Therefore, we have

$$\begin{aligned}M_k(q,h)&=\sum_{n=1}^{q}f(n)^k\\&\lesssim_k h^{k/2}P^k\sum_{r_1,\cdots,r_k|q}\frac{1}{lcm(r_i)}\prod_{i=1}^{k}\frac{r_i}{\phi(r_i)}\\&\leq qh^{k/2}P^k\sum_{r|q}\frac{1}{r}\sum_{r_1,\cdots,r_k|r}\prod_{i=1}^{k}\frac{r_i}{\phi(r_i)}\\&=qh^{k/2}P^k\sum_{r|q}\frac{1}{r}(\sum_{d|r}\frac{d}{\phi(d)})^k\\&=qh^{k/2}P^k\sum_{r|q}\frac{1}{r}\prod_{p|r}(1+\frac{p}{p-1})^k\\&=qh^{k/2}P^k\prod_{p|q}(1+\frac{1}{p}(1+\frac{p}{p-1})^k).\end{aligned}$$

Note that $1+\frac{1}{p}(1+\frac{p}{p-1})^k \leq (1+\frac{1}{p-1})^{2^k}$. (This follows from an elementary calculation that $f(x) := (x+1)^{2^k} - x(2+x)^k - 1 \geq 0, \forall x \in (0,1]$, for $k \geq 2$.) Therefore,

$$\begin{aligned} M_k(q,h) &\lesssim_k \prod_{p|q}(1+\frac{1}{p-1})^{2^k} q h^{k/2} P^k \\ &= q h^{k/2} P^{k-2^k}. \end{aligned}$$

□

Now we can prove Theorem 1.5 by combining the former results.

Given q, k, let $q_1 = \prod_{p|q, p\leq h^k} p, q_2 = \prod_{p|q,p>h^k,}$ and $P_1 = q_1/\phi(q_1), P_2 = q_2/\phi(q_2)$. From the bijection

$$\begin{aligned} \mathbb{Z}/q_1q_2 &\longrightarrow \mathbb{Z}/q_1 \times \mathbb{Z}/q_2 \\ a \bmod q_1q_2 &\longmapsto (a \bmod q_1, a \bmod q_2), \end{aligned}$$

which restricts to a bijection

$$(\mathbb{Z}/q_1q_2)^\times \longrightarrow (\mathbb{Z}/q_1)^\times \times (\mathbb{Z}/q_2)^\times,$$

we have

$$Mk(q,h) = \sum_{n_1=1}^{q_1}\sum_{n_2=1}^{q_2}\left(\sum_{\substack{m=1 \\ (m+ni,q_i)=1, i=1,2}}^{h} 1 - hP\right)^k.$$

Put $D(n_1,n_2) = \sum^h_{\substack{m=1 \\ (m+ni,q_i)=1,i=1,2}} 1-hP$, and

$$\begin{aligned} D_1(n_1,n_2) &:= P_2 \sum_{\substack{m=1 \\ (m+n_1,q_1)=1}}^{h} 1 - hP \\ D_2(n_1,n_2) &:= \sum_{\substack{m=1 \\ (m+ni,q_i)=1,i=1,2}}^{h} 1 - P_2 \sum_{\substack{m=1 \\ (m+n_1,q_1)=1}}^{h} 1. \end{aligned}$$

Then by Hölder's inequality, we have $D^k \leq 2^{k-1}(D_1^k + D_2^k)$, and consequently

$$M_k(q,h) \lesssim_k \sum_{n_1}\sum_{n_2} D_1^k + \sum_{n_1}\sum_{n_2} D_2^k. \tag{9}$$

D_1 is independent of n_2, we have

$$\begin{aligned} \sum_{n_1}\sum_{n_2} D_1^k &= q_2 P_2^k M_k(q_1,h) \\ &\lesssim q_2 P_2^k q_1 h^{k/2} P_1^{k-2^k} \\ &= q h^{k/2} P^k P_1^{-2^k}. \end{aligned}$$

Note that, by Mertens' third theorem, $P_1^{-1} \leq \prod_{p\leq h^k}(1-\frac{1}{p})^{-1} \sim e^{-\gamma} log(h^k) \lesssim_k logh$, where γ is the Euler-Mascheroni constant. We obtain

$$\sum_{n_1}\sum_{n_2} D^k \lesssim_k q(hP)^{k/2} P^{k/2} (logh)^{2^k}.$$

For the estimate of D_2, let $h(n_1) = \sum_{\substack{m=1 \\ (m+n_1,q_1)=1}} 1$, for $1 \le n_1 \le q_1$. Then we have

$$\begin{aligned}\sum_{n_2} D_2^k &= \sum_{n_2} \left(\sum_{\substack{m=1 \\ (m+n_1,q_1)=1 \\ (m+n_2,q_2)=1}}^{k} -P_2 h(n_1) \right)^k \\ &= M_k(q_2, h(n_1)).\end{aligned}$$

Therefore, since all prime factors of q_2 are greater than h^k, by the probabilistic estimate from the preceding subsection, we have

$$\begin{aligned}\sum_{n_1}\sum_{n_2} D_2^k &\lesssim_k \sum_{n_1} q_2 P_2^{k/2} h(n_1)^{k/2} \\ &\lesssim q_1 q_2 P_2^{k/2} (hP_1)^{k/2} \\ &= q(hP)^{k/2}.\end{aligned}$$

By (9), estimates of D_1 and D_2 implies that

$$M_k(q,h) \lesssim_k q(hP)^{k/2} + q(hP)^{k/2} P^{k/2} (logh)^{2^k},$$

completing the proof of Theorem 1.5.

5. Remarks on the fundamental lemma

Recall the fundamental lemma stated in the previous section. The hypothesis that if $p|lcm(r_i)$ then p divides at least two of the r_i may seem peculiar at first glance, but it is natural. Suppose $p|r_1, p \nmid r_i, i = 2, \cdots, k$. If $\rho_i \in \mathbb{Z}/r_i$ with $\sum \rho_i = 0$. Then $\rho_1 \in \mathbb{Z}/(\frac{r_1}{p})$. Replace r_1 by r_1/p. Then the left hand side of (6) does not change. To appreciate the importance of this hypothesis, suppose moreover G_1 is supported on $(\mathbb{Z}/r_1)^\times$. Then, as we have seen in the proof of Theorem 4.3, the left hand side of (6) is 0.

There is a trivial case where all $G_i \equiv 1$ leading the equality of (6) to hold. A more useful observation is

Proposition 5.1. *With assumptions as in Lemma 4.2, the equality of (6) holds if k is even and*

$(1')$ $r_{2i-1} = r_{2i}$

$(2')$ $G_{2i-1}(\rho) = \overline{G_{2i}(-\rho)}$

$(3')$ $r_2, r_4, \cdots, r_k$ *are pairwise coprime.*

We call these assumptions on k and $r_i, G_i, i = 1, \cdots k$ the diagonal configuration, and call a k-tuple $(r_1, \cdots r_k)$ diagonal if it satisfies (1')(3').

Proof. If $\sum \rho_i = 0$, since $r_2, r_4, \cdots, r_k$ are pairwise coprime, we have $\rho_{2i-1} = \rho_{2i}$. Thus, the left hand side of (6) is

$$\begin{aligned} &= \sum_{\substack{\rho_{2i} \in \mathbb{Z}/r_{2i} \\ i=1,\cdots,\frac{k}{2}}} \prod_{i=1}^{k/2} |G_{2i}(\rho_{2i})|^2 \\ &= \prod_{i=1}^{k/2} \sum_{\rho_{2i} \in \mathbb{Z}/r_{2i}} |G_{2i}(\rho_{2i})|^2, \end{aligned}$$

and the right hand side of (6) is

$$\begin{aligned} &= \frac{1}{r} \prod_{i=1}^{k} r_i^{1/2} \prod_{i=1}^{k} \left(\sum_{\rho_i \in \mathbb{Z}/r_i} |G_i(\rho_i)|^2 \right)^{1/2} \\ &= 1 \cdot \prod_{i=1}^{k/2} \sum_{\rho_{2i} \in \mathbb{Z}/r_{2i}} |G_{2i}(\rho_{2i})|^2. \end{aligned}$$

Hence the equality is achieved. □

To obtain a result better than Theorem 1.5, a much more elaborate inequality than the fundamental lemma is required. To notice the difficulty, fix r square-free, k even, then

$$\#\{(r_1, \cdots, r_k) : lcm(r_i) = r, p|r \ implies \ p| \ at \ two \ of \ r_i\} = (2^k - k - 1)^{w(r)},$$

where $w(r) = \#\{p : p|r\}$, while

$$\#\{(r_1, \cdots, r_k) : lcm(r_i) = r, (r_1 \cdots, r_k) \ diagonal \ \} = (k/2)^{w(r)},$$

which is far smaller than $(2^k - k - 1)^{w(r)}$. The number of those $(r_1, \cdots, r_k)$ such that

$$\begin{cases} lcm(r_i) = r \\ p|r \ implies \ p| \ exacly \ two \ of \ the \ r_i \end{cases}$$

(so that $\prod_{i=1}^{k} r_i^{1/2} = lcm(r_i)$) is $\binom{k}{2}^{w(r)}$. One may expect an easy lower bound for those k-tuples than the right hand side of (6), but the following example shows otherwise.

Example 5.2. *For each $i = 1, \cdots, k$, fix any $\rho_i' \in \mathbb{Z}/r_i$ such that $\sum_{i=1}^{k} \rho_i = 0$. Let*

$$G_i(\rho_i) = \begin{cases} 1, \ if \ \rho_i = \rho_i' \\ 0, \ otherwise. \end{cases}$$

Then the equality of (6) holds (both sides equal to 1), even though the configuration might be far from diagonal.

References

[1] H. Cramer, *On the order of magnitude of the difference between consecutive prime numbers*, Acta. Arith **2** (1937), 147–153.

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

[3] M. Hausman and H. N. Shapiro, *On the mean square distribution of primes in short intervals*, Comm. Pure App. Math. **26** (1973), 539–547.

[4] H. L. Montgomery and R. C. Vaughan, *On the distribution of reduced residues*, Ann. Math. **123** (1986), 311–333.

[5] C. Hooley, *On the difference of consecutive numbers prime to n*, Acta Arith. **8** (1963), 643–347.

Chern Insititute of Mathematics, Nankai University, Tianjin, China
Email address: 2211059@mail.nankai.edu.cn