Some Discussions on the Distribution of Reduced Residue Classes

Lin Xingfeng and Jiao Pengyu
Nankai University

Jan. 5, 2026

Presentation Outline

1. Introduction: motivation, definitions and preliminary reductions
2. Proof of Conjecture 1.4 for $k = 2$
3. Theorem 1.5 implies Theorem 1.2
4. Proof of Theorem 1.5
    1. Probabilistic Model
    2. Fourier Techniques and the Fundamental Lemma

Conjectures on consecutive prime gaps (p_i: the i-th prime):

Conjecture (1.1)

Fix $\gamma > 0$, for $x > 1$:

$$\sum_{p_i \le x} (p_{i+1} - p_i)^{\gamma} \le Cx(\log x)^{\gamma - 1}$$

for some constant $C > 0$.

Stronger conjectures:

$$\#\{p_i \le x : p_{i+1} - p_i \ge \alpha \log p_i\} \sim e^{-\alpha} \frac{x}{\log x}, \quad \limsup_{i \to \infty} \frac{p_{i+1} - p_i}{(\log p_i)^2} = 1.$$

Introduction: Definitions

Fix $q \in \mathbb{N}^*$, $1 < a_1 < a_2 < \ldots$: positive integers coprime to q. Analogue of Conjecture 1.1:

Theorem (1.2)

Fix $\gamma > 0$, we have:

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

where $\phi(q)$: reduced residue classes modulo q, $P := \phi(q)/q$.

Definition (1.3)

Fix $h \in \mathbb{N}^*$, $k > 0$. Define the k-th moment:

$$M_k(q,h) := \sum_{n=1}^{q} \Big(\#\{a_i : n < a_i \leq n+h\} - Ph \Big)^k$$

Conjecture 1.4 & Theorem 1.5

Conjecture (1.4)

For $h \geq \frac{1}{P}$, $k > 0$*:*

$$M_k(q,h) \lesssim_k q(Ph)^{\frac{k}{2}}$$

We prove a weaker estimate yet strong enough to deduce Theorem 1.2:

Theorem (1.5)

For $h \geq \frac{1}{P}$, $k > 0$*:*

$$M_k(q,h) \lesssim_k q(Ph)^{\frac{k}{2}} \left(1 + P^{\frac{k}{2}}(\log h)^{2^k}\right)$$

Preliminary Reductions: Prop 1.6

Proposition (1.6)

Conjecture 1.4 or Theorem 1.5 holds for all q if it holds for square-free q.

Proof: Let q' be the largest square-free divisor of q. Then, the RHS of Conjecture 1.4 or Theorem 1.5 for q, q' differ by a factor q/q' since $P = \phi(q)/q = \phi(q')/q'$. Note

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

□

Proposition (1.7)

Conjecture 1.4 and Theorem 1.5 reduce to $k \in \mathbb{Z}_{>0}$.

Proof: For $k > 0$, $k' = \lfloor k \rfloor + 1$, by Hölder's inequality:

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

Using the above inequality gives the conclusion. $\square$

Proof of Conjecture 1.4 (for $k = 2$)

Theorem (2.1)

For $h \geq \frac{1}{P}$: $M_2(q, h) \leq qPh$.

Proof: Let $d(r) = \begin{cases} 1, & (r, q) = 1, \\ 0, & \text{otherwise.} \end{cases}$ Set $X_n = \sum_{r=n+1}^{n+h} d(r)$, then

$$M_2(q, h) = \sum_{n=1}^{q} (X_n - Ph)^2 = \sum_{n=1}^{q} X_n^2 - qP^2h^2.$$

Expand the square:

$$X_n^2 = \sum_{r=n+1}^{n+h} d(r)^2 + 2 \sum_{n+1 \leq r < s \leq n+h} d(r)d(s).$$

Sum from $n = 1$ to q, by interchanging the summations we get

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

Proof of Conjecture 1.4 (for $k = 2$) (continued)

Since $d(r)^2 = d(r)$ and $\sum_{r=1}^{q} d(r) = qP$, the single-sum term satisfies:

$$h \sum_{r=1}^{q} d(r)^2 = h \cdot qP.$$

For $\sum_{r=2}^{q+1} d(r)d(r+k)$, we have the key identity:

$$\sum_{r=2}^{q+1} d(r)d(r+k) = q \prod_{\substack{p|q \\ p\nmid k}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p|q \\ p|k}} \left(1 - \frac{1}{p}\right).$$

Let $\alpha(d) = \prod_{p|d}(p-2)$, μ the Möbius function:

$$\sum_{r=2}^{q+1} d(r)d(r+k) = q\prod_{p|q}\left(1-\frac{2}{p}\right)\sum_{\substack{d|q\\d|k}}\frac{\mu^2(d)}{\alpha(d)}.$$

Use the inequality in the double sum and change the summation order:

$$\sum_{k=1}^{h-1}(h-k)\sum_{r=2}^{q+1} d(r)d(r+k) = q\prod_{p|q}\left(1-\frac{2}{p}\right)\sum_{d|q}\frac{\mu^2(d)}{\alpha(d)}\sum_{\substack{k\le h\\d|k}}(h-k).$$

Proof of Conjecture 1.4 (for $k = 2$) (continued)

Estimate the arithmetic sum: $\sum_{\substack{k \le h \\ d | k}} (h-k) \le \frac{h^2}{2d}$, which gives

$$2 \sum_{k=1}^{h-1} (h-k) \sum_{r=2}^{q+1} d(r) d(r+k) \le qP^2 h^2.$$

Combine the two estimates for X_n^2:

$$\sum_{n=1}^{q} X_n^2 \le qPh + qP^2 h^2.$$

Thus

$$M_2(q,h) = \sum_{n=1}^{q} X_n^2 - qP^2 h^2 \le qPh.$$

Theorem 1.5 Implies Theorem 1.2

Proposition (3.1)

For $h \geq \frac{1}{P}$, $k > 0$, if $M_k(q,h) \lesssim_k q(Ph)^{\frac{k}{2}}\left(1 + P^{\frac{k}{2}}(\log h)^{2^k}\right)$, then $\forall \gamma < \frac{k+1}{2}$:

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

Proof: $a_1 < a_2 < \ldots$: positive integers coprime to q,
$N(l) = \#\{i : a_{i+1} - a_i \geq l\}$. Fix $l \geq 1$. Let $h = \lfloor l/2 \rfloor$, for $a_{i+1} - a_i \geq l$,
$X_n = \#\left\{a_j : n < a_j \leq n + h\right\} = 0$ for $n \in [a_i, a_i + l - h]$.

Proof of Proposition 3.1 (continued)

Hence we get a lower bound for $M_k(q,h)$:

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

Combined with the assumed upper bound for $M_k(q,h)$:

$$N(l) \lesssim_k \phi(q)(Pl)^{-\frac{k}{2}} \left(1 + P^{\frac{k}{2}}(\log l)^{2^k}\right).$$

Rewite the sum:

$$\sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^\gamma = \sum_{l=1}^{\infty} N(l)\left(l^\gamma - (l-1)^\gamma\right) \lesssim_\gamma \sum_{l=1}^{\infty} N(l) l^{\gamma-1}.$$

Proof of Proposition 3.1 (continued)

$$\sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^{\gamma} = \sum_{l=1}^{\infty} (N(l) - N(l+1)) l^{\gamma} \sim \sum_{l=1}^{\infty} N(l) l^{\gamma-1}.$$

Split the sum into two parts ($l \leq \frac{2}{P}$ and $l > \frac{2}{P}$):

$$\sum_{l=1}^{\infty} N(l) l^{\gamma-1} = \sum_{1 \leq l \leq \frac{2}{P}} N(l) l^{\gamma-1} + \sum_{l > \frac{2}{P}} N(l) l^{\gamma-1}.$$

For the first sum: $N(l) \leq \phi(q)$, so it is bounded by $\phi(q) P^{-\gamma}$.

Proof of Proposition 3.1 (continued)

For the second sum, use $N(l) \lesssim_k \phi(q)(Pl)^{-1-\frac{k}{2}}(1 + P^{\frac{k}{2}}(\log h)^{2^k})$:

$$\sum_{l > \frac{2}{P}} N(l) l^{\gamma-1} \lesssim_k \phi(q) P^{-1-\frac{k}{2}} \sum_{l > \frac{2}{P}} l^{\gamma-2-\frac{k}{2}}(1 + P^{\frac{k}{2}} l^{\varepsilon}),$$

where we use $(\log h)^{2^k} \lesssim_{k,\varepsilon} l^{\varepsilon}$ (for $\varepsilon > 0$).
Take $\varepsilon = \frac{1}{2}$: the sum converges when $\gamma < 1 + \frac{k}{2} - \varepsilon = \frac{k+1}{2}$. Thus:

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

The inequality is valid for all $\gamma < \frac{k+1}{2}$. $\square$

Proof of Theorem 1.5: Probabilistic Model

Assume $h > \frac{1}{P}$. $X_1, \ldots, X_h$ independent,
$P(X_m = 1) = P,\ P(X_m = 0) = 1 - P.\ X = \sum_{m=1}^{h} X_m,$
$\mu_k = \mathbb{E}\big((X - Ph)^k\big).$

Proposition (4.1)

$\mu_k \lesssim_k (hP)^{\frac{k}{2}}.$

Proof: $Y_m = X_m - P$, $X - Ph = \sum_{m=1}^{h} Y_m$, so

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

$\mathbb{E}(Y_{m_1} \ldots Y_{m_k}) = 0$ if any index appears only once.

Proof of Proposition 4.1 (continued)

Let r be the number of distinct indices turning up in $\mathbb{E}(Y_{m_1} \dots Y_{m_k})$, then $r \leq k/2$. An elementary estimate of $\mathbb{E}$ gives

$$\mu_k \leq \sum_{r=1}^{\lfloor k/2 \rfloor} \binom{h}{r} \sum_{\substack{l_1+\cdots+l_r=k \\ l_i \geq 2}} \frac{k!}{l_1! \cdots l_r!} (2P)^r$$

Thus $\mu_k \lesssim_k (hP)^{\frac{k}{2}}$. $\square$

Proof of Theorem 1.5: Expansion

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

We compute the inner sum:

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

Proof of Theorem 1.5: Large Prime Factors

Fix $m_1, \dots, m_r$, and denote $s = \#\{m_i\}_{i=1}^r$. Then:

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

Assume $p > y > h$ for some real number $y > 0$ and all $p|q$. Apply Proposition 4.1 and note that:

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

This proves Conjecture 1.4 for q with large prime factors ($> h$).

4.2 Fourier Techniques and the Fundamental Lemma

For small prime factors $p \mid q$, we need the Fundamental Lemma:

Lemma (4.2)

$r_1, \ldots, r_k$ square-free, $r = lcm(r_i)$ (each prime divides ≥ 2 r_i).
$G_i : \mathbb{Z}/r_i\mathbb{Z} \to \mathbb{C}$, then:

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

where $e(x) = e^{2\pi i x}$.
Fourier coefficients for the period-q f:

$$\hat{f}\left(\frac{a}{q}\right) = \frac{1}{q} \sum_{n=1}^{q} f(n) e\left(-\frac{an}{q}\right), \quad f(n) = \sum_{r \mid q} \sum_{\substack{0 \leq a < r \\ (a,r)=1}} \hat{f}\left(\frac{a}{r}\right) e\left(\frac{an}{r}\right)$$

Fourier Expansion of $f(n)$

$f(n) = \#\{a_i : n < a_i \leq n + h\} - Ph$, expand $f(n)^k$:

$$\sum_{n=1}^{q} f(n)^k = \sum_{n=1}^{q} \left(\sum_{r|q} \sum_{\rho \in (\mathbb{Z}/r\mathbb{Z})^*} \hat{f}(\rho) e(\rho n) \right)^k$$

Expanding the k-th power, only terms with $\sum_{i=1,\ldots,k} \rho_i = 0$ survive:

$$\sum_{n=1}^{q} f(n)^k = q \sum_{r_1,\ldots,r_k|q} \sum_{\substack{\rho_i \in (\mathbb{Z}/r_i\mathbb{Z})^* \\ \sum \rho_i = 0}} \prod_{i=1}^{k} \hat{f}(\rho_i)$$

Theorem (4.3)

For $h > \frac{1}{P}$: $M_k(q, h) \lesssim_k q h^{\frac{k}{2}} P^{k-2^k}$.

Proof of Theorem 4.3 (continued)

Recall the Fourier coefficient: $\hat{f}(\rho) = \dfrac{P}{\phi(r)} E(\rho)$, where we define

$$E(\rho) = \sum_{m=1}^{h} e(\rho m).$$

A key elementary estimate for the exponential sum:

$$|E(\rho)| = \left| \sum_{m=1}^{h} e(\rho m) \right| \leq \min\left\{ h, \ \frac{1}{\|\rho\|} \right\},$$

where $\|x\| = \min_{n \in \mathbb{Z}} |x - n|$ denotes the distance to the nearest integer. We have the summation bound:

$$\sum_{p \in (\mathbb{Z}/r\mathbb{Z})^*} |E(\rho)|^2 \lesssim rh.$$

Proof of Theorem 4.3 (continued)

Plug $\hat{f}(\rho_i) = \frac{P}{\phi(r_i)} E(\rho_i)$ into the product term, apply the fundamental lemma:

$$\left| \sum_{\substack{\rho_i \in (\mathbb{Z}/r_i\mathbb{Z})^* \\ \sum_{i=1}^k \rho_i = 0}} \prod_{i=1}^k \hat{f}(\rho_i) \right| \leq P^k \cdot \frac{\prod_{i=1}^k r_i^{1/2}}{\operatorname{lcm}(r_1, \ldots, r_k) \prod_{i=1}^k \phi(r_i)} \prod_{i=1}^k \left(\sum_{\rho_i} |E(\rho_i)|^2 \right)^{1/2}.$$

Insert the bound $\sum_{\rho_i} |E(\rho_i)|^2 \lesssim r_i h$ and simplify the product:

$$\prod_{i=1}^k \left(\sum_{\rho_i} |E(\rho_i)|^2 \right)^{1/2} \lesssim h^{k/2} \cdot \prod_{i=1}^k r_i^{1/2}.$$

Proof of Theorem 4.3 (continued)

Combine the above estimates to get the simplified bound for the inner sum:

$$\left| \sum_{\substack{\rho_i \in (\mathbb{Z}/r_i\mathbb{Z})^* \\ \sum \rho_i = 0}} \prod_{i=1}^{k} \hat{f}(\rho_i) \right| \lesssim_k P^k h^{k/2} \cdot \frac{\prod_{i=1}^k r_i}{\mathrm{lcm}(r_1, \ldots, r_k) \prod_{i=1}^k \phi(r_i)}.$$

Sum over all divisors $r_1, \ldots, r_k \mid q$:

$$\sum_{r_1,\ldots,r_k \mid q} \frac{\prod_{i=1}^k r_i}{\mathrm{lcm}(r_i) \prod \phi(r_i)} = \prod_{p \mid q} \left(1 + \frac{1}{p}(1 + \frac{p}{p-1})\right)^k \lesssim \prod_{p \mid q} \left(1 + \frac{1}{p-1}\right)^{2^k}.$$

Final Estimate of $M_k(q,h)$

Recall $M_k(q,h) = \sum_{n=1}^{q} f(n)^k$, and use all estimates we obtained earlier:

$$M_k(q,h) \lesssim_k q \cdot P^k h^{k/2} \sum_{r_1,\dots,r_k | q} \frac{\prod_{i=1}^{k} r_i}{\mathrm{lcm}(r_i) \prod \phi(r_i)}$$

$$\lesssim_k qP^k h^{k/2} \prod_{p|q} \left(1 + \frac{1}{p-1}\right)^{2^k} = qh^{\frac{k}{2}} P^{k-2^k}$$

Finally we obtain:

$$M_k(q,h) \lesssim_k qh^{\frac{k}{2}} P^{k-2^k}.$$

□

Final Proof of Theorem 1.5

Step 1:Split q into two parts By Chinese Remainder Theorem, split q into small and large prime factors:

$$q = q_1 q_2, \quad (q_1, q_2) = 1,$$

where

$$q_1 = \prod_{\substack{p \mid q \\ p \le h^k}} p, \qquad q_2 = \prod_{\substack{p \mid q \\ p > h^k}} p.$$

Denote $P_i = \frac{\phi(q_i)}{q_i}$ $(i = 1, 2)$, then $P = \frac{\phi(q)}{q} = P_1 P_2$.

Final Proof of Theorem 1.5 (continued)

Step 2: Split the function $D(n_1, n_2)$. Let

$$D(n_1, n_2) = \sum_{m=1, (m+n_i, q_i)=1 \forall i}^{h} 1 - Ph$$

decompose $D = D_1 + D_2$, where

$$D_1(n_1, n_2) = P_2 \sum_{m=1, (m+n_1, q_1)=1}^{h} 1 - Ph$$

$$D_2(n_1, n_2) = \sum_{m=1, (m+n_i, q_i)=1 \forall i}^{h} 1 - P_2 \sum_{m=1, (m+n_1, q_1)=1}^{h} 1$$

.

By Hölder's inequality and summing over all n, we get the estimate:

$$M_k(q, h) = \sum_{n_1=1}^{q_1} \sum_{n_2=1}^{q_2} D(n_1, n_2)^k \lesssim_k \sum_{n_1, n_2} D_1^k + \sum_{n_1, n_2} D_2^k.$$

Step 3: Estimate for small primes (q_1, D_1). Apply Theorem 4.3 to q_1:

$$\sum_{n_1,n_2} D_1^k = q_2 P_2^k \cdot M_k(q_1, h).$$

By Theorem 4.3: $M_k(q_1, h) \lesssim_k q_1 h^{\frac{k}{2}} P_1^{k-2^k}$. Use **Mertens' Theorem** ($P_1^{-1} \le \prod_{p \le h^k} \left(1 - \frac{1}{p}\right)^{-1} \sim e^\gamma log(h^k) \lesssim \log h$):

$$\sum_{n_1,n_2} D_1^k \lesssim_k q \cdot (hP)^{\frac{k}{2}} P^{\frac{k}{2}} (\log h)^{2^k}.$$

Final Proof of Theorem 1.5 (continued)

Step 4: Estimate for large primes (q_2, D_2). For large primes $p > h^k$, use the **probabilistic large prime estimate**:

$$\sum_{n_1, n_2} D_2^k = \sum_{n_1} M_k(q_2, h(n_1)) \lesssim_k q \cdot (hP)^{\frac{k}{2}}.$$

Final Combination: Combine the estimates of D_1^k and D_2^k:

$$M_k(q, h) \lesssim_k q(hP)^{\frac{k}{2}} \cdot \left(1 + P^{\frac{k}{2}}(\log h)^{2^k}\right).$$

This completes the proof of Theorem 1.5. □

References

1. H. Cramer, *On the order of magnitude of the difference between consecutive prime numbers*, Acta. Arith. 2 (1937), 147–153.
2. P. Erdős, *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. Montgomery, H. L. and Vaughan, 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), 343–347.

Thank you for listening!

Any questions are welcome