



Research article

Effective multiplicative representations over short intervals modulo primes: Cases $C = 4$ and $C = 6$

Qing Xiao*

School of Information and Electrical Engineering, Hunan University of Science and Technology,
Xiangtan 411201, China

* **Correspondence:** Email: qxiao@mail.hnust.edu.cn.

Abstract: This paper investigates the problem of short-interval multiplicative representations modulo primes. For a given positive integer C , an explicit lower bound $p_0(C)$ exists such that for every prime $p \geq p_0(C)$, every element of the reduced residue system modulo p can be expressed as the product modulo p of two distinct integers in the interval $[1, p/C)$. The overall argument proceeds by contradiction combined with strong induction on prime powers. For $C = 4$, we construct the inductive base via case analysis and derive the explicit lower bound $p \geq 199$ by combining the divisibility properties of arithmetic progressions with a lower bound of the Chebyshev ψ -function. Building on this, we formulate an offset-screening and inductive framework for a specified positive integer C , in which a successful finite screening supplies the inductive base required by the subsequent theoretical argument. We carry out the complete implementation of this framework for $C = 6$ and obtain the explicit lower bound $p \geq 601$.

Keywords: multiplicative representation in short intervals; explicit lower bound; Chebyshev ψ -function; computer enumeration

1. Introduction

Let p be a prime and let N be a positive integer satisfying $N < p$. Define

$$H_N(p) = \{xy \bmod p : 1 \leq x, y \leq N\}.$$

The problem of determining how many nonzero residue classes modulo p are contained in $H_N(p)$, in particular when $H_N(p)$ contains all nonzero residue classes, has been studied extensively.

Garaev [1] studied the multiplication table $H_N(p)$ and recalled the previously known result that $H_N(p)$ contains all nonzero residue classes when N is a sufficiently large constant multiple of $p^{3/4}$. He further

investigated the exceptional set for shorter ranges and proved that, for almost all primes p , the choice

$$N = \left\lfloor p^{1/2}(\log p)^{1+\delta+\varepsilon} \right\rfloor, \quad \delta = 1 - \frac{\log(e \log 2)}{\log 2},$$

gives $|H_N(p)| = p(1 + o(1))$.

Garaev and Karatsuba [2] obtained related estimates for products of small integers. In particular, if $\Delta = \Delta(p) \rightarrow \infty$ as $p \rightarrow \infty$, then the set of products $qy \bmod p$ contains $(1 + O(\Delta^{-1}))p$ residue classes, where $q \leq p^{1/2}$ is prime and $1 \leq y \leq \Delta p^{1/2} \log p$.

A related product-set problem was considered by Cilleruelo and Garaev [3]. They proved that if $I = \{1, 2, \dots, H\} \pmod{p}$ is an initial interval satisfying $|I| > p^{5/8+\varepsilon}$ and G is either a multiplicative subgroup or a set of the form $\{1, g, g^2, \dots, g^{m-1}\} \pmod{p}$, where g is a primitive root, with $|G| > p^{3/8}$, then $|I \cdot G| = p + O(p^{1-\delta})$ for some $\delta = \delta(\varepsilon) > 0$. Here, the two factors belong to sets of different types, whereas in the present problem, both factors are required to lie in the same initial interval.

Shparlinski [4] obtained a uniform asymptotic formula for the number of solutions to

$$xy \equiv \mu \pmod{p}$$

with x and y restricted to two intervals. In particular, his Theorem 13 has the form

$$\#\{(x, y) \in X \times Y : xy \equiv \mu \pmod{p}\} = \frac{p-1}{p^2} |X||Y| + O(p^{1/2+o(1)}).$$

Taking

$$X = Y = \left\{1, \dots, \left\lfloor \frac{p}{C} \right\rfloor\right\}$$

shows that for every fixed C , the main term is of order p and dominates the error term as $p \rightarrow \infty$, uniformly in μ . Moreover, the congruence $x^2 \equiv \mu \pmod{p}$ has at most two solutions modulo p . Hence, for all sufficiently large primes p , every nonzero residue class has a product representation with $x \neq y$. An explicit estimate of Heath-Brown [5], based on Weil's bound for Kloosterman sums, makes this conclusion effective and yields a computable sufficient threshold for every fixed C .

The results above are principally concerned with shortening the ranges of the variables or estimating the number of residue classes excluded from the corresponding product sets. The present paper focuses on an explicit-threshold version of the full-coverage problem. For a fixed C , we ask for a specific prime threshold such that for every prime p at or above that threshold and every nonzero residue class μ , there are two distinct integers x and y satisfying

$$1 \leq x, y < \frac{p}{C}, \quad xy \equiv \mu \pmod{p}.$$

We first address the case $C = 4$ and present the core result for this interval.

Proposition 1. *Let p be a prime with $p \geq 199$. For any element μ in the reduced residue system modulo p , two distinct integers x, y exist within the interval $[1, p/4)$ such that*

$$xy \equiv \mu \pmod{p}, \quad x \neq y.$$

The threshold 199 is sharp among prime moduli. Indeed, for the preceding prime $p = 197$, the residue class $\mu = 121$ has no representation as the product modulo p of two distinct integers in $[1, p/4)$.

To prove Proposition 1, we first establish the following auxiliary proposition, which characterizes the residue classes that cannot be expressed as the product of two distinct integers in the target interval.

Auxiliary Proposition 1. Let p be a prime with $p > 256$. Define the sets $S = \{1, 2, \dots, \lfloor p/4 \rfloor\}$ and $T = \{xy \mid x, y \in S, x \neq y\}$. Let μ be an integer with $1 \leq \mu < p$, and let θ denote a prime. If $\mu \notin T$, then μ must fall into one of the following five categories:

- (1) $\mu = 1$;
- (2) $\mu = \theta$, where $p/4 < \theta < p$;
- (3) $\mu = \theta^2$, where $\sqrt{p/4} < \theta < \sqrt{p}$;
- (4) $\mu = 2\theta$, where $p/4 < \theta < p/2$;
- (5) $\mu = 3\theta$, where $p/4 < \theta < p/3$.

The proof of Auxiliary Proposition 1 is presented in Section 2. We prove Proposition 1 by contradiction combined with strong induction on prime powers, which requires case analysis and the construction of inductive bases. For $C \geq 5$, we formulate a finite offset-screening procedure for constructing the required inductive base. The screening is successful for a specified value of C when all surviving configurations reduce to the common-offset form. In the present paper, the detailed screening and the ensuing inductive proof are carried out for $C = 6$, for which the corresponding core conclusion is stated below.

Proposition 2. Let p be a prime with $p \geq 601$. For any element μ in the reduced residue system modulo p , two distinct integers x, y exist within the interval $[1, p/6)$ such that

$$xy \equiv \mu \pmod{p}, \quad x \neq y.$$

The threshold 601 is likewise sharp among prime moduli. For the preceding prime $p = 599$, the residue class $\mu = 263$ has no representation as the product modulo p of two distinct integers in $[1, p/6)$.

The auxiliary proposition supporting the proof of Proposition 2 is given next.

Auxiliary Proposition 2. Let p be a prime with $p > 1296$. Define the sets $S = \{1, 2, \dots, \lfloor p/6 \rfloor\}$ and $T = \{xy \mid x, y \in S, x \neq y\}$. Let μ be an integer with $1 \leq \mu < p$, and let θ denote a prime. If $\mu \notin T$, then μ must fall into one of the following seven categories:

- (1) $\mu = 1$;
- (2) $\mu = \theta$, where $p/6 < \theta < p$;
- (3) $\mu = \theta^2$, where $\sqrt{p/6} < \theta < \sqrt{p}$;
- (4) $\mu = 2\theta$, where $p/6 < \theta < p/2$;
- (5) $\mu = 3\theta$, where $p/6 < \theta < p/3$;
- (6) $\mu = 4\theta$, where $p/6 < \theta < p/4$;
- (7) $\mu = 5\theta$, where $p/6 < \theta < p/5$.

The proofs of both auxiliary propositions are provided in Section 2.

2. Preliminary

2.1. Auxiliary Proposition 1

Proof. If $\mu = 1$, the only factorization over positive integers is 1×1 , which violates the condition $x \neq y$; hence, $\mu = 1$ is not representable. If $1 < \mu < \frac{p}{4}$, we may take $x = 1$ and $y = \mu$, so such a value of μ lies in T . It remains to consider the case $\frac{p}{4} < \mu < p$.

We partition the elements μ with $\frac{p}{4} < \mu < p$ into three categories: (1) Composite numbers that are not perfect powers, (2) powers of composite numbers, and (3) prime powers. We discuss each category separately.

Case 1: Composite numbers that are not perfect powers

Suppose that μ is a composite number that cannot be written as n^r for any integer $r \geq 2$. Write $\mu = d_1 \cdot d_2$ with $d_1 < \sqrt{\mu} < d_2$, where d_1 is the largest divisor of μ that is smaller than $\sqrt{\mu}$. Since $\mu > p/4 > 1$ and μ is composite, we have $d_1 \geq 2$.

If $d_1 \geq 4$, then $d_2 = \frac{\mu}{d_1} < \frac{p}{4}$. Taking $x = d_1$ and $y = d_2$, we have $d_1 < \sqrt{\mu} < \sqrt{p} < \frac{p}{4}$ ($p > 256$), so $x, y \in S$ and $x \neq y$. Thus $\mu \in T$ and μ is representable.

Now suppose that $d_1 \leq 3$. If d_2 is composite, we can write $d_2 = a \cdot b$ with $2 \leq a \leq \sqrt{d_2} \leq b$. Then $\mu = d_1 \cdot d_2 = (d_1 \cdot a) \cdot b$. If $d_1 a = \sqrt{\mu}$, then we would have $\mu = (d_1 a)^2$, contradicting the assumption that μ is not a perfect power. Therefore, only the following two cases need to be considered:

- If $d_1 a < \sqrt{\mu}$, then $d_1 a$ is a divisor of μ smaller than $\sqrt{\mu}$ and strictly larger than d_1 , which contradicts the maximality of d_1 .
- If $d_1 a > \sqrt{\mu}$, then $b = \frac{\mu}{d_1 a} < \sqrt{\mu}$, so b is a divisor of μ smaller than $\sqrt{\mu}$. Hence $a \leq b \leq d_1 \leq 3$, and therefore $\mu = d_1 a b \leq 27$, contradicting $\mu > \frac{p}{4} > 64$.

Therefore, d_2 must be a prime, which we denote as θ . If $d_1 = 2$ and $\theta < p/4$, then 2 and θ are two distinct elements of S whose product is μ , so $\mu \in T$. Hence, the only possible nonrepresentable case with $d_1 = 2$ is

$$\mu = 2\theta, \quad \frac{p}{4} < \theta < \frac{p}{2}.$$

Similarly, when $d_1 = 3$, the only possible nonrepresentable case is

$$\mu = 3\theta, \quad \frac{p}{4} < \theta < \frac{p}{3}.$$

Thus, the only nonrepresentable composite numbers that are not perfect powers are precisely those in the two forms above; all other composite numbers that are not perfect powers lie in T .

Case 2: Powers of composite numbers

Suppose that μ is a perfect power but not a prime power, and write

$$\mu = n^r, \quad r \geq 2,$$

where n is composite. Since μ is not a prime power, n is not a prime power either. Let a be the smallest prime divisor of n and put $b = n/a$. Then

$$2 \leq a < b, \quad n = ab,$$

because $a = b$ would imply that $n = a^2$ is a prime power. Therefore

$$\mu = (ab)^r = a^r b^r.$$

Take $x = a^r$ and $y = b^r$. Then $\mu = xy$ and $x < y$. Since $a \geq 2$ and $r \geq 2$, we have $x = a^r \geq 4$, and hence

$$y = \frac{\mu}{x} < \frac{p}{4}.$$

Moreover

$$x < \sqrt{\mu} < \sqrt{p} < \frac{p}{4},$$

where the last inequality follows from $p > 256$. Thus x and y are two distinct elements of S , and hence $\mu \in T$. Therefore, every perfect power that is not a prime power can be expressed as the product of two distinct elements of S .

Case 3: Prime powers

Let $\mu = \theta^r$ with $\frac{p}{4} < \mu < p$, where θ is prime and $r \geq 1$.

- If $r = 1$, then $\mu = \theta$. The only factor pair is $(1, \theta)$. Since $\frac{p}{4} < \mu = \theta < p$, we have $\theta \notin S$, so μ is not directly representable.
- If $r = 2$, then $\mu = \theta^2$ with $\sqrt{\frac{p}{4}} < \theta < \sqrt{p}$. The factor pairs are $(1, \theta^2)$ and (θ, θ) . For $(1, \theta^2)$, we have $\theta^2 > \frac{p}{4}$, so $\theta^2 \notin S$; for (θ, θ) , the two factors are equal, violating $x \neq y$. Hence, μ is not directly representable.
- If $r \geq 3$, all such prime powers are directly representable. We split by the parity of r as follows:
 - When r is odd ($r = 2s + 1$, $s \geq 1$): Take $x = \theta^s$, $y = \theta^{s+1}$. Since $p > 256$, we have

$$\theta^s < \theta^{s+1} < p^{\frac{s+1}{2s+1}} \leq p^{\frac{2}{3}} < \frac{p}{4},$$

so $x, y \in S$ and $\mu \in T$.

- When r is even ($r = 2s$, $s \geq 2$): Take $x = \theta^{s-1}$, $y = \theta^{s+1}$. Since $p > 256$, we have

$$\theta^{s-1} < \theta^{s+1} < p^{\frac{s+1}{2s}} \leq p^{\frac{3}{4}} < \frac{p}{4},$$

so $x, y \in S$ and $\mu \in T$.

Consequently, among prime powers only $\mu = \theta$ ($\frac{p}{4} < \theta < p$) and $\mu = \theta^2$ ($\sqrt{\frac{p}{4}} < \theta < \sqrt{p}$) fail to be directly representable; all other prime powers can be written as a product of two distinct elements of S . $\square$

2.2. Auxiliary Proposition 2

Proof. The overall argument framework is identical to that of Auxiliary Proposition 1. We divide μ into three categories: (1) Composite numbers that are not perfect powers, (2) powers of composite numbers, and (3) prime powers. Most derivations follow the same reasoning as before; we only elaborate on the differentiated parts here.

Case 1: Composite numbers that are not perfect powers

Suppose that μ is a composite number that cannot be written as n^r for any integer $r \geq 2$. Write $\mu = d_1 \cdot d_2$ with $d_1 < \sqrt{\mu} < d_2$, where d_1 is the largest divisor of μ that is smaller than $\sqrt{\mu}$. Since $\mu > p/6 > 1$ and μ is composite, we have $d_1 \geq 2$.

If $d_1 \geq 6$, then $d_2 = \frac{\mu}{d_1} < \frac{p}{6}$. Taking $x = d_1$ and $y = d_2$, we have $d_1 < \sqrt{\mu} < \sqrt{p} < \frac{p}{6}$ ($p > 1296$), so $x, y \in S$ and $x \neq y$. Thus $\mu \in T$ and μ is representable.

Now suppose that $d_1 \leq 5$. If d_2 is composite, we can write $d_2 = a \cdot b$ with $2 \leq a \leq \sqrt{d_2} \leq b$. Then $\mu = d_1 \cdot d_2 = (d_1 \cdot a) \cdot b$. If $d_1 a = \sqrt{\mu}$, then we would have $\mu = (d_1 a)^2$, contradicting the assumption that μ is not a perfect power. Therefore, only the following two cases need to be considered:

- If $d_1 a < \sqrt{\mu}$, then $d_1 a$ is a divisor of μ smaller than $\sqrt{\mu}$ and strictly larger than d_1 , which contradicts the maximality of d_1 .
- If $d_1 a > \sqrt{\mu}$, then $b = \frac{\mu}{d_1 a} < \sqrt{\mu}$, so b is a divisor of μ smaller than $\sqrt{\mu}$. Hence $a \leq b \leq d_1 \leq 5$, and therefore $\mu = d_1 a b \leq 125$, contradicting $\mu > \frac{p}{6} > 216$.

Therefore, d_2 must be a prime, which we denote as θ . If $\theta < p/6$, then d_1 and θ are two distinct elements of S whose product is μ , so $\mu \in T$. Hence, the only possible nonrepresentable forms are

$$\mu = j\theta, \quad j \in \{2, 3, 4, 5\}, \quad \frac{p}{6} < \theta < \frac{p}{j},$$

where θ is prime. Conversely, each of these forms is nonrepresentable because one factor in every factorization is divisible by $\theta > p/6$.

Case 2: Powers of composite numbers

Suppose that μ is a perfect power but not a prime power. By the factorization established in Case 2 of the proof of Auxiliary Proposition 1, we may write

$$\mu = (ab)^r = a^r b^r, \quad 2 \leq a < b, \quad r \geq 2.$$

If $a^r \geq 6$, take $x = a^r$ and $y = b^r$. Then

$$y = \frac{\mu}{x} < \frac{p}{6}, \quad x < \sqrt{\mu} < \sqrt{p} < \frac{p}{6},$$

so x and y are two distinct elements of S .

It remains to consider the case $a^r < 6$. Since $a \geq 2$ and $r \geq 2$, this is possible only when $a = 2$ and $r = 2$. Hence

$$\mu = (2b)^2 = 4b^2.$$

If b is a power of 2, then μ is itself a prime power and belongs to the next case. If b is composite and has an odd prime divisor ℓ with $\ell \geq 3$, then

$$\mu = (2b)^2 = \ell^2 \left(\frac{2b}{\ell} \right)^2.$$

Take

$$x = \ell^2, \quad y = \left(\frac{2b}{\ell} \right)^2.$$

Since b is composite, $b/\ell \geq 2$. Therefore, $x \geq 9$ and $y \geq 16$, and hence

$$x = \frac{\mu}{y} < \frac{p}{16} < \frac{p}{6}, \quad y = \frac{\mu}{x} < \frac{p}{9} < \frac{p}{6}.$$

Moreover, x is odd and y is even, so $x \neq y$. Thus μ is representable. Consequently, the only remaining possibility is that b is an odd prime, which we denote as θ . Hence

$$\mu = 4\theta^2 = (2\theta)^2.$$

If $\theta^2 < p/6$, then the distinct factors 4 and θ^2 already belong to S . Since $p > 3$ is prime, the equality $\theta^2 = p/6$ is impossible. It therefore remains only to consider

$$\sqrt{\frac{p}{6}} < \theta < \frac{\sqrt{p}}{2},$$

where the upper bound follows from $4\theta^2 = \mu < p$. In this range, take $x = \theta$ and $y = 4\theta$. Since

$$\theta < 4\theta < 2\sqrt{p} < \frac{p}{6} \quad (p > 144),$$

both factors belong to S and are distinct. Hence, $\mu = 4\theta^2$ is also representable and does not yield a new exceptional class.

Case 3: Prime powers

Let $\mu = \theta^r$ with $\frac{p}{6} < \mu < p$, where θ is prime and $r \geq 1$. The cases $r = 1$ and $r = 2$ give, respectively

$$\mu = \theta, \quad \frac{p}{6} < \theta < p,$$

and

$$\mu = \theta^2, \quad \sqrt{\frac{p}{6}} < \theta < \sqrt{p}.$$

As in the proof of Auxiliary Proposition 1, neither of these two forms admits a factorization into two distinct elements of S .

Now suppose that $r \geq 3$. If $r = 2s + 1$ is odd, take $x = \theta^s$ and $y = \theta^{s+1}$. Then

$$x < y < p^{\frac{s+1}{2s+1}} \leq p^{2/3} < \frac{p}{6},$$

where the last inequality holds for $p > 216$.

If $r = 2s$ is even, where $s \geq 2$, take $x = \theta^{s-1}$ and $y = \theta^{s+1}$. Then

$$x < y < p^{\frac{s+1}{2s}} \leq p^{3/4} < \frac{p}{6},$$

where the last inequality holds for $p > 1296$.

Since the present auxiliary proposition assumes $p > 1296$, both estimates hold. Therefore, all prime powers with $r \geq 3$ are representable, and the only exceptional prime-power forms are $\mu = \theta$ and $\mu = \theta^2$ with the ranges stated above.

In summary, all values of μ that lack such a representation precisely fall into the seven categories listed in the present auxiliary proposition. $\square$

2.3. General lemmas

We first fix the notation used throughout this subsection. Let p be a prime, let $1 \leq \mu < p$, and define

$$a_i = (i-1)p + \mu, \quad i \geq 1.$$

We present four fundamental lemmas that will be used repeatedly in the subsequent proofs.

Lemma 1 Let C be a positive integer. Suppose that there is a positive integer x dividing a_k such that $Ck \leq x < \frac{p}{C}$. Let $y = a_k/x$. Then

$$x, y \in \left[1, \frac{p}{C}\right)$$

and $xy \equiv \mu \pmod{p}$.

Proof. Since $a_k < kp$ and $x \geq Ck$, we have

$$y = \frac{a_k}{x} < \frac{kp}{Ck} = \frac{p}{C}.$$

The assumed upper bound on x gives $x < p/C$. Therefore, $x, y \in [1, p/C)$, and

$$xy = a_k \equiv \mu \pmod{p}.$$

□

Lemma 2 Let k be a positive integer satisfying $\gcd(k, p) = 1$, and let s be the smallest positive index such that $k \mid a_s$. Then $s \leq k$.

Proof. Consider the first k terms of the sequence modulo k

$$a_i \equiv (i-1)p + \mu \pmod{k}, \quad i = 1, 2, \dots, k.$$

Since $\gcd(p, k) = 1$, as $i-1$ runs through $0, 1, \dots, k-1$, the residues $(i-1)p + \mu$ form a complete residue system modulo k . Hence, there is an index $i \in \{1, 2, \dots, k\}$ such that $k \mid a_i$. Therefore, the smallest such index satisfies $s \leq k$. □

Lemma 3 Let k be a positive integer satisfying $\gcd(k, p) = 1$. If $k \mid a_s$, then, for every positive index j , we have

$$k \mid a_j \iff j \equiv s \pmod{k}.$$

Proof. Since

$$a_j - a_s = (j-s)p,$$

if $j \equiv s \pmod{k}$, then $k \mid a_j - a_s$. Together with $k \mid a_s$, this gives $k \mid a_j$.

Conversely, if $k \mid a_j$, then

$$k \mid a_j - a_s = (j-s)p.$$

Since $\gcd(k, p) = 1$, it follows that $k \mid j-s$, or, equivalently, $j \equiv s \pmod{k}$. □

Lemma 4 Let $n < p$. To prove that $k \mid a_k$ for every integer $2 \leq k \leq n$, it suffices to prove that

$$q^\beta \mid a_{q^\beta}$$

for every prime power $q^\beta \leq n$.

Proof. Let $2 \leq k \leq n$ and write its prime factorization as

$$k = \prod_{i=1}^m q_i^{\beta_i}, \quad \beta_i \geq 1,$$

where $q_1, \dots, q_m$ are distinct primes. By assumption

$$q_i^{\beta_i} \mid a_{q_i^{\beta_i}} \quad (i = 1, \dots, m).$$

For each i , since $q_i^{\beta_i} \mid k$, we have

$$k \equiv q_i^{\beta_i} \pmod{q_i^{\beta_i}}.$$

Therefore, the full index-class statement of Lemma 3 gives

$$q_i^{\beta_i} \mid a_k \quad (i = 1, \dots, m).$$

The prime powers $q_i^{\beta_i}$ are pairwise coprime, and hence

$$\prod_{i=1}^m q_i^{\beta_i} \mid a_k.$$

Therefore, $k \mid a_k$. □

The proofs of Lemmas 3 and 4 use only the fact that the sequence is an arithmetic progression with a common difference p . Consequently, the same statements and proofs apply verbatim to every shifted progression

$$u_k = (k - r)p + \lambda,$$

which is used later in this paper, provided that all the indices involved belong to the domain of the corresponding sequence.

In each induction below, prime powers are considered in increasing order. When treating a prime power Q , we assume that $P \mid u_P$ has already been established for every prime power $P < Q$. If

$$s = \prod_{i=1}^m r_i^{\alpha_i}, \quad \alpha_i \geq 1,$$

where $r_1, \dots, r_m$ are distinct primes, and if, for every i , the divisibility $r_i^{\alpha_i} \mid u_{r_i^{\alpha_i}}$ has already been established either as a base divisibility or by the induction hypothesis, then Lemma 4 gives $s \mid u_s$. We shall use this implication repeatedly below.

2.4. Roadmap of the proofs

The proofs for $C = 4$ and $C = 6$ follow the same general strategy. First, the auxiliary propositions reduce the problem to finitely many exceptional forms of μ . For each such form, we introduce an appropriate arithmetic progression

$$u_k = (k - r)p + \mu, \quad u_k \equiv \mu \pmod{p}.$$

Assuming that the desired representation does not exist, we first establish the required divisibility relations for small prime powers. For $C = 4$, this is done by the case analysis in Section 3.1. For $C = 6$, the offset screening shows that only the common-offset configurations remain and provides the divisibility base

$$2^8 \mid a_{2^8-\sigma}, \quad 3^5 \mid a_{3^5-\sigma}, \quad 5^3 \mid a_{5^3-\sigma}, \quad 0 \leq \sigma \leq 4.$$

We then use **strong induction on prime powers**. For a prime power $Q = q^\beta$, let h be the smallest admissible index such that $Q \mid u_h$. Lemmas 2 and 3 restrict the possible values of h . If $h \neq Q$, the induction hypothesis and Lemma 4 provide additional divisors of u_h . Combining these divisors with Q produces a factor x of u_h satisfying the size conditions in Lemma 1, and hence gives the desired representation, a contradiction. The few exceptional minimal indices arising from shifted progressions are handled separately. Therefore, one must have

$$Q \mid u_Q$$

for every relevant prime power Q .

Finally, Lemma 4 extends these divisibility relations from prime powers to all relevant integers. The explicit formula for u_k then implies that a large least common multiple divides an integer of order p . This contradicts the lower bound supplied by the Chebyshev function. Thus both proofs have the same overall structure.

3. Proof of Proposition 1

We divide the primes p into two ranges:

- (1) If $199 \leq p \leq 6000$, we verify Proposition 1 directly by computer enumeration;
- (2) If $p > 6000$, we prove Proposition 1 theoretically by contradiction and strong induction on prime powers.

The finite range $199 \leq p \leq 6000$ contains 738 primes. For each of these primes, the program sets

$$N_p = \left\lfloor \frac{p}{4} \right\rfloor$$

and enumerates all pairs of integers satisfying $1 \leq x < y \leq N_p$. It then computes all residues $xy \bmod p$ and verifies that

$$\{xy \bmod p : 1 \leq x < y \leq N_p\} = \{1, 2, \dots, p-1\}.$$

Thus every nonzero residue class modulo p is represented by two distinct integers satisfying the strict inequalities $1 \leq x, y < \frac{p}{4}$. No failure occurs for any of the 738 primes in this range.

3.1. Construction of base cases

We introduce the arithmetic sequence

$$a_k = (k-1)p + \mu^*,$$

where μ^* takes one of the following three forms:

$$\mu^* = 1, \quad \mu^* = \theta \text{ with } \frac{p}{4} < \theta < p, \quad \mu^* = \theta^2 \text{ with } \sqrt{\frac{p}{4}} < \theta < \sqrt{p},$$

and θ is prime in both cases involving θ .

We conduct a case analysis assuming that Proposition 1 is false, and prove that this forces

$$2 \mid a_2, \quad 3 \mid a_3, \quad 4 \mid a_4, \quad 5 \mid a_5, \quad 6 \mid a_6, \quad 7 \mid a_7.$$

Note that 1, θ , and θ^2 are all odd, so $a_2 = p + \mu^*$ is always even, which implies that $2 \mid a_2$ holds unconditionally. We then carry out case classification to construct the base cases.

Case 1: $4 \mid a_2$

If we suppose that $8 \mid a_s$, then $4 \mid a_s$. Since $4 \mid a_2$, Lemma 3 gives

$$s \equiv 2 \pmod{4}.$$

On the other hand, Lemma 2 applied to 8 shows that such an index s may be chosen with $1 \leq s \leq 8$. The only indices in this range satisfying $s \equiv 2 \pmod{4}$ are $s = 2$ and $s = 6$. Therefore

$$8 \mid a_2 \quad \text{or} \quad 8 \mid a_6.$$

We divide this into the following subcases. The corresponding divisibility results, construction methods, and range verifications are summarized below.

Subcase		x	y	Range verification
$3 \mid a_2$	$12 \mid a_2$	12, 24, 36	$\frac{p + \mu^*}{12}$	$8 \leq x < 500 < y < \frac{p}{4}$
$8 \mid a_2$	$8 \mid a_2$	8, 16, 24	$\frac{p + \mu^*}{8}$	$8 \leq x < 750 < y < \frac{p}{4}$
$8 \mid a_6$ and $3 \mid a_3$	$24 \mid a_6$	24, 48, 72	$\frac{5p + \mu^*}{24}$	$24 \leq x < 1250 < y < \frac{p}{4}$

We take the first subcase as an example to illustrate the derivation. If $3 \mid a_2$, then $12 \mid a_2$. Take $x = 12, 24, 36$ and set $y = \frac{a_2}{12} = \frac{p + \mu^*}{12}$. Then

$$8 \leq x \leq 36 < 500 < \frac{p + \mu^*}{12} < \frac{p}{4},$$

and the three corresponding products satisfy

$$xy \equiv \mu^*, \quad 2\mu^*, \quad 3\mu^* \pmod{p},$$

respectively.

This construction is valid for every $\mu^* \in \{1, \theta, \theta^2\}$, covering all the target cases: $\mu = 1$, $\mu = \theta$, $\mu = \theta^2$, $\mu = 2\theta$, and $\mu = 3\theta$.

Therefore, Proposition 1 holds when $4 \mid a_2$. Suppose that Proposition 1 fails. Then $4 \nmid a_2$. Since $2 \mid a_2$, every index s satisfying $4 \mid a_s$ must satisfy

$$s \equiv 2 \pmod{2}$$

by Lemma 3. Lemma 2 applied to 4 gives such an index with $1 \leq s \leq 4$, so the only possibilities are $s = 2$ and $s = 4$. The first possibility has been excluded; hence, $4 \mid a_4$.

Case 2: $2 \mid a_2$, $3 \mid a_2$, and $4 \mid a_4$

By Lemma 3, $4 \mid a_4 \implies 4 \mid a_8$ and $3 \mid a_2 \implies 3 \mid a_5$ and $3 \mid a_8$.

Suppose that $9 \mid a_s$. Then $3 \mid a_s$, and hence Lemma 3 gives

$$s \equiv 2 \pmod{3}.$$

Lemma 2 applied to 9 shows that such an index may be chosen with $1 \leq s \leq 9$. The only indices in this range satisfying $s \equiv 2 \pmod{3}$ are $s = 2, 5, 8$. Therefore

$$9 \mid a_2, \quad 9 \mid a_5, \quad \text{or} \quad 9 \mid a_8.$$

Subcase			x	y	Range verification
$9 \mid a_2$	—	$18 \mid a_2$	18, 36, 54	$\frac{p + \mu^*}{18}$	$8 \leq x \leq 54 < 333 < y < \frac{p}{4}$
$9 \mid a_8$	—	$36 \mid a_8$	36, 72, 108	$\frac{7p + \mu^*}{36}$	$32 \leq x \leq 108 < 1166 < y < \frac{p}{4}$
$9 \mid a_5$	$5 \mid a_2$	$10 \mid a_2$	10, 20, 30	$\frac{p + \mu^*}{10}$	$8 \leq x \leq 30 < 600 < y < \frac{p}{4}$
	$5 \mid a_3$	$60 \mid a_8$	60, 120, 180	$\frac{7p + \mu^*}{60}$	$32 \leq x \leq 180 < 700 < y < \frac{p}{4}$
	$5 \mid a_4$	$20 \mid a_4$	20, 40, 60	$\frac{3p + \mu^*}{20}$	$16 \leq x \leq 60 < 900 < y < \frac{p}{4}$
	$5 \mid a_5$	$45 \mid a_5$	45, 90, 135	$\frac{4p + \mu^*}{45}$	$20 \leq x \leq 135 < 533 < y < \frac{p}{4}$

Thus Proposition 1 holds when $2 \mid a_2$, $3 \mid a_2$, and $4 \mid a_4$. If Proposition 1 still fails, then $3 \nmid a_2$. Moreover

$$3 \nmid a_1 = \mu^*,$$

because $\mu^* \in \{1, \theta, \theta^2\}$ and the prime θ satisfies $\theta > \sqrt{p/4} > 3$. Lemma 2 applied to 3 gives an index $s \leq 3$ such that $3 \mid a_s$. Since $s = 1$ and $s = 2$ have both been excluded, it follows that $3 \mid a_3$. Thus we are left with

$$2 \mid a_2, \quad 3 \mid a_3, \quad 4 \mid a_4.$$

Completion of base case construction

Suppose that $5 \mid a_k$ for some $k \in \{2, 3, 4\}$. From the known divisibility $k \mid a_k$ and $\gcd(5, k) = 1$, we obtain $5k \mid a_k$. Take

$$x = 5k, 10k, 15k, \quad y = \frac{a_k}{5k} = \frac{(k-1)p + \mu^*}{5k}.$$

Then

$$5k \leq x \leq 15k < \frac{(k-1)p}{5k} < y < \frac{p}{5} < \frac{p}{4}.$$

Thus Proposition 1 holds in this case.

Therefore, if Proposition 1 fails, then

$$5 \nmid a_2, \quad 5 \nmid a_3, \quad 5 \nmid a_4.$$

We also have $5 \nmid a_1 = \mu^*$, since $\theta > \sqrt{p/4} > 5$ is prime. Lemma 2 applied to 5 gives an index $s \leq 5$ such that $5 \mid a_s$. Since the indices $s = 1, 2, 3, 4$ have been excluded, we must have $5 \mid a_5$.

From $2 \mid a_2$, Lemma 3 gives $2 \mid a_6$, while $3 \mid a_3$ gives $3 \mid a_6$. Since $\gcd(2, 3) = 1$, it follows that $6 \mid a_6$.

Suppose that $7 \mid a_k$ for some $k \in \{2, 3, 4, 5, 6\}$. From the known divisibility $k \mid a_k$ and $\gcd(7, k) = 1$, we obtain $7k \mid a_k$. Take

$$x = 7k, 14k, 21k, \quad y = \frac{a_k}{7k} = \frac{(k-1)p + \mu^*}{7k}.$$

Then

$$7k \leq x \leq 21k < \frac{(k-1)p}{7k} < y < \frac{p}{7} < \frac{p}{4}.$$

Thus Proposition 1 holds in this case.

Therefore, if Proposition 1 fails, then

$$7 \nmid a_2, \quad 7 \nmid a_3, \quad 7 \nmid a_4, \quad 7 \nmid a_5, \quad 7 \nmid a_6.$$

We also have $7 \nmid a_1 = \mu^*$, since $\theta > \sqrt{p/4} > 7$ is prime. Lemma 2 applied to 7 gives an index $s \leq 7$ such that $7 \mid a_s$. Since the indices $s = 1, 2, \dots, 6$ have been excluded, we must have $7 \mid a_7$.

To summarize, if Proposition 1 fails, then

$$k \mid a_k \quad (k = 2, 3, 4, 5, 6, 7),$$

where $\mu^* \in \{1, \theta, \theta^2\}$ and θ is prime.

3.2. Inductive step

By Auxiliary Proposition 1, it suffices to prove that Proposition 1 holds for the following three types of μ :

- (1) $\mu = 1, \theta, \theta^2$;
- (2) $\mu = 2\theta$;
- (3) $\mu = 3\theta$.

In the following, we use proof by contradiction combined with strong induction on prime powers to complete the proof of Proposition 1 for the three cases. Define

$$n = \left\lfloor \sqrt{\frac{p}{4}} \right\rfloor.$$

If $p > 6000$, then $n \geq 38$.

3.2.1. $\mu = 1, \theta, \theta^2$

We define the arithmetic sequence $\{a_k\}$ by

$$a_k = (k-1)p + \mu, \quad k \geq 1,$$

where μ takes the values $1, \theta$ with $\frac{p}{4} < \theta < p$, and θ^2 with $\frac{p}{4} < \theta^2 < p$, where θ is prime. The restriction $q^\beta \leq n$ will be imposed only on the prime powers considered in the induction.

For every integer $2 \leq k \leq n < \sqrt{\frac{p}{4}}$ we have $\gcd(k, \mu) = 1$, and hence $k \nmid a_1$. Let s be the smallest positive index such that $k \mid a_s$. By Lemma 2, we have $2 \leq s \leq k$.

We aim to prove that if Proposition 1 fails and $\mu \in \{1, \theta, \theta^2\}$, then

$$k \mid a_k$$

for every integer $2 \leq k \leq n$.

The construction of the base cases has already established this divisibility for $k = 2, 3, 4, 5, 6, 7$. By Lemma 4, it therefore suffices to prove it for every prime power $k = q^\beta$ satisfying $8 \leq k \leq n$. We use strong induction on prime powers, according to the convention stated after Lemma 4.

For the prime power $k = q^\beta$ currently under consideration, let s be the smallest positive index such that $k \mid a_s$. By Lemma 2,

$$2 \leq s \leq k.$$

If $s = k$, the required divisibility already holds. It remains to exclude $s < k$. In this case, write

$$\gcd(k, s) = q^\gamma.$$

According to q and γ , the proof is divided as follows:

$$\left\{ \begin{array}{l} \text{Case 1: } k = 2^\beta, \beta \geq 3 \\ \text{Case 2: } k = 3^\beta, \beta \geq 2 \\ \text{Case 3: } k = q^\beta, q \geq 5 \end{array} \right\} \left\{ \begin{array}{l} \text{Subcase 1.1: } 0 \leq \gamma \leq \beta - 2, \\ \text{Subcase 1.2: } \gamma = \beta - 1; \\ \text{Subcase 2.1: } 0 \leq \gamma \leq \beta - 2, \\ \text{Subcase 2.2: } \gamma = \beta - 1; \\ 0 \leq \gamma \leq \beta - 1. \end{array} \right.$$

We now consider these cases in order.

Case 1: $k = 2^\beta$ with $\beta \geq 3$

Suppose that $s < 2^\beta$. Every prime-power divisor of s is smaller than 2^β , so the induction convention above gives $s \mid a_s$. Since

$$\gcd(2^\beta, s) = 2^\gamma,$$

we have

$$d = \text{lcm}(2^\beta, s) = 2^{\beta-\gamma} s, \quad d \mid a_s.$$

Subcase 1.1: $0 \leq \gamma \leq \beta - 2$

Here, $d \geq 4s$. Set $x = d$ and $y = \frac{a_s}{d}$. Since $x = d \leq 2^\beta \cdot s < 2^{2\beta} < \frac{p}{4}$ and

$$y = \frac{a_s}{d} < \frac{sp}{4s} = \frac{p}{4},$$

we have $x, y < \frac{p}{4}$ and $xy = a_s \equiv \mu \pmod{p}$. Therefore, Proposition 1 holds whenever $x \neq y$.

If $x = y$, then $d^2 = a_s$. When $\gamma = 0$, take $x' = s^2$ and $y' = 2^{2\beta}$; it follows that $x' < y' < \frac{p}{4}$. When $1 \leq \gamma \leq \beta - 2$, take $x' = \frac{d}{2}$ and $y' = 2d$. In this case, $x' < d < \frac{p}{4}$ and $y' = 2^{\beta-\gamma+1} \cdot s \leq 2^\beta \cdot s < \frac{p}{4}$. Hence, Proposition 1 holds for all $0 \leq \gamma \leq \beta - 2$.

Subcase 1.2: $\gamma = \beta - 1$

If $\gcd(2^\beta, s) = 2^{\beta-1}$ and $s < 2^\beta$, then necessarily $s = 2^{\beta-1}$. By the inductive hypothesis, $s \mid a_s$.

If $2^{\beta+1} \mid a_{2^{\beta-1}}$, set $x = 2^{\beta+1}$. We have $x = 2^{\beta+1} = 4s < 2^{2\beta} < \frac{p}{4}$. Let $y = \frac{a_s}{x}$; Lemma 1 implies $y < \frac{p}{4}$, and $xy = a_s \equiv \mu \pmod{p}$. If $x \neq y$, Proposition 1 holds. If $x = y$, then $a_s = x^2 = 2^{2\beta+2}$. Take $x' = 2^\beta$ and $y' = 2^{\beta+2}$, which satisfy $x' \neq y'$ and $x' < y' < 2^{2\beta} < \frac{p}{4}$. Thus Proposition 1 holds.

Now suppose that $2^\beta \parallel a_{2^{\beta-1}}$ (i.e., $2^\beta \mid a_{2^{\beta-1}}$ but $2^{\beta+1} \nmid a_{2^{\beta-1}}$). Write $a_s = 2^\beta \cdot u$ where u is odd. Let $h = 3s = 3 \cdot 2^{\beta-1}$. Then

$$a_h = a_{3s} = a_s + 2s \cdot p = 2^\beta(u + p).$$

Since u is odd and p is an odd prime, $u + p$ is even, so $2 \mid (u + p)$ and, consequently, $2^{\beta+1} \mid a_h$.

We have $h = 3 \cdot 2^{\beta-1}$. Since $3 \mid a_3$, Lemma 3 yields $3 \mid a_h$, and hence $3 \cdot 2^{\beta+1} \mid a_h$. Set $x = 3 \cdot 2^{\beta+1} = 6 \cdot 2^\beta$, and observe

$$4h = 6 \cdot 2^\beta \leq x < 2^{2\beta} < \frac{p}{4}.$$

Let $y = \frac{a_h}{x}$. If $x \neq y$, Proposition 1 holds.

If $x = y$, then $x^2 = (6 \cdot 2^\beta)^2 = a_h$. Take $x' = 6 \cdot 2^{\beta-1}$ and $y' = 6 \cdot 2^{\beta+1}$. When $\beta = 3$, we get $x' < y' < 1500 < \frac{p}{4}$; when $\beta \geq 4$, we have

$$x' < y' = 12 \cdot 2^\beta \leq 2^{2\beta} < \frac{p}{4}.$$

In either subcase, Proposition 1 holds.

To summarize, Proposition 1 holds whenever $\gcd(2^\beta, s) = 2^\gamma$ with $0 \leq \gamma \leq \beta - 1$. If Proposition 1 fails, we must have $\gcd(2^\beta, s) = 2^\beta$, which forces $s = 2^\beta$ and $2^\beta \mid a_{2^\beta}$ for all $2^\beta \leq n$.

Case 2: $k = 3^\beta$ with $\beta \geq 2$

In this case, $3^2 \leq 3^\beta \leq n < \sqrt{\frac{p}{4}}$. Let s be the minimal positive index such that $3^\beta \mid a_s$. We prove below that if $s < 3^\beta$, then Proposition 1 holds.

Since $s < 3^\beta$, every prime-power divisor of s is smaller than 3^β . Hence the induction convention above gives $s \mid a_s$. Let $\gcd(3^\beta, s) = 3^\gamma$, where $0 \leq \gamma \leq \beta - 1$, and let $d = \text{lcm}(3^\beta, s) = 3^{\beta-\gamma} \cdot s$. Then $d \mid a_s$.

Subcase 2.1: $0 \leq \gamma \leq \beta - 2$

In this case, $4s < 9s \leq d < 3^{2\beta} < \frac{p}{4}$. Set $x = d$ and $y = \frac{a_s}{x}$. Then $x, y < \frac{p}{4}$ and $xy = a_s \equiv \mu \pmod{p}$.

If $x \neq y$, Proposition 1 holds. If $x = y$, i.e., $d^2 = a_s$, we have

(1) When $\gamma = 0$, take $x' = s^2$ and $y' = 3^{2\beta}$. Then $x'y' = d^2 = a_s$, and $x' < y' < \frac{p}{4}$.

(2) When $1 \leq \gamma \leq \beta - 2$, take $x' = \frac{d}{3}$ and $y' = 3d$. Then $x' < y' \leq 3^{2\beta} < \frac{p}{4}$.

Hence, Proposition 1 holds for all $0 \leq \gamma \leq \beta - 2$.

Subcase 2.2: $\gamma = \beta - 1$

In this case, $\gcd(3^\beta, s) = 3^{\beta-1}$. Hence $3^{\beta-1} \mid s$. Since $s < 3^\beta$, the only possibilities are

$$s = 3^{\beta-1} \quad \text{or} \quad s = 2 \cdot 3^{\beta-1}.$$

If $s = 3^{\beta-1}$, then $3^\beta \mid a_{3^{\beta-1}}$. By Lemma 3, we have

$$3^\beta \mid a_{3^{\beta-1}}, \quad 3^\beta \mid a_{4 \cdot 3^{\beta-1}}, \quad 3^\beta \mid a_{7 \cdot 3^{\beta-1}}.$$

Note that $a_{4 \cdot 3^{\beta-1}} = a_{3^{\beta-1}} + 3^\beta \cdot p$ and $a_{7 \cdot 3^{\beta-1}} = a_{3^{\beta-1}} + 2 \cdot 3^\beta \cdot p$. Dividing the three terms above by 3^β , we obtain

$$\frac{a_{3^{\beta-1}}}{3^\beta}, \quad \frac{a_{3^{\beta-1}}}{3^\beta} + p, \quad \frac{a_{3^{\beta-1}}}{3^\beta} + 2p.$$

The three terms above run through a complete residue system modulo 3, so exactly one of them is divisible by 3, and thus the corresponding term is divisible by $3^{\beta+1}$.

Let h be the smallest positive index such that $3^{\beta+1} \mid a_h$. Since $3^{\beta+1} \mid a_h$ implies $3^\beta \mid a_h$, while $3^\beta \mid a_{3^{\beta-1}}$, Lemma 3 gives

$$h \equiv 3^{\beta-1} \pmod{3^\beta}.$$

On the other hand, Lemma 2 applied to $3^{\beta+1}$ gives $h \leq 3^{\beta+1}$. Therefore, the only possible values of h are

$$h = 3^{\beta-1}, \quad h = 4 \cdot 3^{\beta-1}, \quad h = 7 \cdot 3^{\beta-1}.$$

The corresponding constructions are given in the table below.

h	Divisibility	d	$x \neq y$	$x = y$
$3^{\beta-1}$	$3^{\beta+1} \mid a_h$	$3^{\beta+1}$	$4h \leq x = 3^{\beta+1} < 3^{2\beta} < \frac{p}{4}$	$x' = 3^\beta, y' = 3^{\beta+2}, x' < y' = 3^{\beta+2} \leq 3^{2\beta} < \frac{p}{4}$
$4 \cdot 3^{\beta-1}$	$4 \cdot 3^{\beta+1} \mid a_h$	$6 \cdot 3^\beta$	$4h \leq x = 6 \cdot 3^\beta < 3^{2\beta} < \frac{p}{4}$	$x' = 3^{\beta+1}, y' = 12 \cdot 3^\beta$. For $\beta = 2$, $x' = 27, y' = 108$, both less than $\frac{p}{4}$; for $\beta \geq 3$, $x' < y' < 3^{2\beta} < \frac{p}{4}$
$7 \cdot 3^{\beta-1}$	$7 \cdot 3^{\beta+1} \mid a_h$	$21 \cdot 3^\beta$	$4h \leq x = 21 \cdot 3^\beta < \frac{p}{4}$ ($189 < 1500$ for $\beta = 2$, $x < 3^{2\beta} < \frac{p}{4}$ for $\beta \geq 3$)	$x' = 49 \cdot 3^{\beta-1}, y' = 3^{\beta+3}$. For $\beta = 2$, $x' = 147, y' = 243$, both less than $\frac{p}{4}$; for $\beta \geq 3$, $x' < y' \leq 3^{2\beta} < \frac{p}{4}$

Conclusion: In all three cases, we can construct solutions satisfying the conditions. If $3^\beta \mid a_{3^{\beta-1}}$, then Proposition 1 holds.

If $s = 2 \cdot 3^{\beta-1}$, then $3^\beta \mid a_{2 \cdot 3^{\beta-1}}$. Let h be the smallest positive index such that $3^{\beta+1} \mid a_h$. Since $3^{\beta+1} \mid a_h$ implies $3^\beta \mid a_h$, Lemma 3 gives

$$h \equiv 2 \cdot 3^{\beta-1} \pmod{3^\beta}.$$

Lemma 2 applied to $3^{\beta+1}$ also gives $h \leq 3^{\beta+1}$. Consequently, the only possible values of h are

$$h = 2 \cdot 3^{\beta-1}, \quad h = 5 \cdot 3^{\beta-1}, \quad h = 8 \cdot 3^{\beta-1}.$$

In this case, $8 < 3^2 \leq 3^\beta$. By the inductive hypothesis, $8 \mid a_8$.

h	Divisibility	d	$x \neq y$	$x = y$
$2 \cdot 3^{\beta-1}$	$3^{\beta+1} \mid a_h$	$3^{\beta+1}$	$4h \leq x = 3^{\beta+1} < 3^{2\beta} < \frac{p}{4}$	$x' = 3^\beta, y' = 3^{\beta+2}, y' = 3^{\beta+2} \leq 3^{2\beta} < \frac{p}{4}; x' < y'$
$5 \cdot 3^{\beta-1}$	$5 \cdot 3^{\beta+1} \mid a_h$	$15 \cdot 3^\beta$	$x = 135 < \frac{p}{4}$ for $\beta = 2$; for $\beta \geq 3, 4h \leq x = 15 \cdot 3^\beta < 3^{2\beta} < \frac{p}{4}$	$x' = 3^{\beta+2}, y' = 25 \cdot 3^\beta$. For $\beta = 2, x' = 81, y' = 225$, both less than $\frac{p}{4}$; for $\beta \geq 3, x' < y' < 3^{2\beta} < \frac{p}{4}$
$8 \cdot 3^{\beta-1}$	$24 \cdot 3^\beta \mid a_h$	$12 \cdot 3^\beta$	$x = 108 < 1500$ for $\beta = 2$; for $\beta \geq 3, 4h \leq x = 12 \cdot 3^\beta < 3^{2\beta} < \frac{p}{4}$	$x' = 3^{\beta+2}, y' = 16 \cdot 3^\beta$. For $\beta = 2, x' = 81, y' = 144$, both less than $\frac{p}{4}$; for $\beta \geq 3, x' < y' < 3^{2\beta} < \frac{p}{4}$

Conclusion: In all three cases, we can construct solutions satisfying the conditions. If $3^\beta \mid a_{2 \cdot 3^{\beta-1}}$, then Proposition 1 holds.

To sum up, if $\gcd(3^\beta, s) = 3^\gamma$ with $0 \leq \gamma \leq \beta - 1$, then Proposition 1 holds. If Proposition 1 fails, we must have $\gcd(3^\beta, s) = 3^\beta$, i.e., $s = 3^\beta$ and $3^\beta \mid a_{3^\beta}$ for $3^\beta \leq n$.

Case 3: $k = q^\beta$ where $q \geq 5$ is prime

At this stage, $q^\beta \leq n < \sqrt{\frac{p}{4}}$, which implies $q^{2\beta} < \frac{p}{4}$. Let s denote the minimal positive index satisfying $q^\beta \mid a_s$. Lemma 2 yields $s \leq q^\beta$.

Suppose $s < q^\beta$. Every prime-power divisor of s is smaller than q^β , so the induction convention above gives $s \mid a_s$. Let $\gcd(q^\beta, s) = q^\gamma$ with $0 \leq \gamma \leq \beta - 1$. Define

$$d = \text{lcm}(q^\beta, s) = q^{\beta-\gamma} \cdot s,$$

and we have $d \mid a_s$. Since $\gamma \leq \beta - 1$, we get $\beta - \gamma \geq 1$. Combined with $q \geq 5$, we have

$$4s < 5s \leq d = q^{\beta-\gamma} \cdot s < q^{2\beta} < \frac{p}{4}.$$

Set $x = d$ and $y = \frac{a_s}{d} < \frac{p}{4}$; then $xy = a_s \equiv \mu \pmod{p}$. If $x \neq y$, Proposition 1 holds. If $x = y$, then $d^2 = q^{2\beta-2\gamma} \cdot s^2 = a_s$. Since $q^\gamma \mid s$, $\frac{s}{q^\gamma}$ is an integer. Take $x' = \frac{s^2}{q^{2\gamma}}$ and $y' = q^{2\beta}$. We verify $x'y' = d^2 = a_s$ and $x' < y' < \frac{p}{4}$, so Proposition 1 holds.

To summarize, Proposition 1 holds whenever $q^\beta \mid a_s$ with $s < q^\beta$. We only need to consider the case $s = q^\beta$, i.e., $q^\beta \mid a_{q^\beta}$.

Proof of Proposition 1: $\mu = 1, \theta, \theta^2$

From the previous analysis, if Proposition 1 fails, then $k \mid a_k$ holds for all integers $1 \leq k \leq n$. It follows that $\text{lcm}(1, 2, \dots, n) \mid (p - \mu)$, so

$$\text{lcm}(1, 2, \dots, n) \leq p - \mu < p.$$

Take the natural logarithm of both sides. Let $\psi(n) = \ln \text{lcm}(1, 2, \dots, n)$ denote the second Chebyshev function. We then have

$$\psi(n) < \ln p.$$

Indeed, $\psi(x) \geq \vartheta(x)$, while Theorem 10 of Rosser and Schoenfeld [6, Theorem 10] gives

$$\vartheta(x) > 0.86x \quad (x \geq 149).$$

For the remaining integers $17 \leq n < 149$, the inequality $\psi(n) > 0.85n$ can be verified directly. Therefore

$$\psi(n) > 0.85n \quad (n \geq 17).$$

Since $p > 6000$, we have $n \geq 38$. It follows that

$$\psi(n) > 0.85 \left\lfloor \sqrt{\frac{p}{4}} \right\rfloor > 0.85 \left(\sqrt{\frac{p}{4}} - 1 \right) = 0.425 \sqrt{p} - 0.85 > \ln p.$$

This gives a contradiction. Therefore, the assumption that $k \mid a_k$ for every $k \leq n$ is false. There must be some prime power $q^\beta \leq n$ whose minimal index s satisfying $q^\beta \mid a_s$ has $s < q^\beta$. As proven in the preceding cases, we can always construct the integers x, y satisfying the required constraints, which completes the proof of Proposition 1.

3.2.2. $\mu = 2\theta$

Let

$$a_k = (k-1)p + \theta, \quad k \geq 1,$$

where θ is a prime satisfying $\frac{p}{4} < \theta < \frac{p}{2}$. Define

$$b_k = (k-2)p + 2\theta, \quad k \geq 2.$$

Then

$$b_k = 2a_k - kp.$$

Consequently, whenever $k \mid a_k$, we also have $k \mid b_k$. The previously established base divisibilities for the sequence $\{a_k\}$ therefore give

$$2 \mid b_2, \quad 3 \mid b_3, \quad 4 \mid b_4, \quad 5 \mid b_5, \quad 6 \mid b_6, \quad 7 \mid b_7.$$

The restriction $q^\beta \leq n-1$ will be imposed only on the prime powers considered in the induction.

If $x \mid b_k$ satisfies

$$4k-4 \leq x < \frac{p}{4},$$

then, upon setting $y = b_k/x$, we obtain

$$y < \frac{p}{4}, \quad xy = b_k \equiv 2\theta \pmod{p}.$$

Thus, if $x \neq y$, Proposition 1 holds.

For any integer k considered below, let s be the smallest index such that $k \mid b_s$. Since $\{b_k\}$ begins at b_2 and exactly one term among any k consecutive terms is divisible by k , we have $2 \leq s \leq k+1$. Moreover, for $3 \leq k \leq \sqrt{\frac{p}{4}}$, we have $k < \theta$ and hence $\gcd(k, \theta) = 1$. Therefore, $k \nmid b_2 = 2\theta$, and the range of the minimal index becomes $3 \leq s \leq k+1$.

By Lemma 4, it suffices to prove that

$$q^\beta \mid b_{q^\beta}$$

for every prime power $q^\beta \leq n - 1$. Compared with the preceding subsection, the only new possibility is the additional minimal index $s = k + 1$. Accordingly, the proof is organized as follows:

$$\left\{ \begin{array}{ll} \text{Case 1: } k = 2^\beta, \beta \geq 3 & \left\{ \begin{array}{l} 3 \leq s \leq 2^\beta, \\ s = 2^\beta + 1; \end{array} \right. \\ \text{Case 2: } k = 3^\beta, \beta \geq 2 & \left\{ \begin{array}{l} 3 \leq s \leq 3^\beta, \\ s = 3^\beta + 1; \end{array} \right. \\ \text{Case 3: } k = q^\beta, q \geq 5 & \left\{ \begin{array}{l} \text{Subcase 3.1: } \beta = 1 \left\{ \begin{array}{l} 3 \leq s \leq q, \\ s = q + 1; \end{array} \right. \\ \text{Subcase 3.2: } \beta \geq 2 \left\{ \begin{array}{l} 3 \leq s \leq q^\beta, \\ s = q^\beta + 1. \end{array} \right. \end{array} \right. \end{array} \right.$$

We now treat the additional index in each case and then reduce the remaining range to the corresponding argument in the preceding subsection.

Case 1: $k = 2^\beta$ with $\beta \geq 3$

For use both in the present induction and in Subcase 3.1 below, we establish this case for every power $2^\beta \leq n$, although the divisibility required in the present case only concerns prime powers not exceeding $n - 1$.

Let s be the smallest index such that $2^\beta \mid b_s$. Then $3 \leq s \leq 2^\beta + 1$. Since $b_{2^\beta+1}$ is odd, we have $s \neq 2^\beta + 1$, and hence

$$3 \leq s \leq 2^\beta.$$

The argument from Case 1 of Section 3.2.1 applies without change and gives $2^\beta \mid b_{2^\beta}$ for every power $2^\beta \leq n$.

Case 2: $k = 3^\beta$ with $\beta \geq 2$

By the induction hypothesis, $3^{\beta-1} \mid b_{3^{\beta-1}}$. Lemma 3 shows that every index whose corresponding term is divisible by $3^{\beta-1}$ must be a multiple of $3^{\beta-1}$. If $s = 3^\beta + 1$, then $3^\beta \mid b_s$ would imply $3^{\beta-1} \mid b_s$, which is impossible because

$$3^\beta + 1 \not\equiv 0 \pmod{3^{\beta-1}}.$$

Therefore, $3 \leq s \leq 3^\beta$, and the argument from Case 2 of Section 3.2.1 applies without change.

Case 3: $k = q^\beta$ with $q \geq 5$

In this case, we have

$$3 \leq s \leq q^\beta + 1.$$

Subcase 3.1: $\beta = 1$

Suppose that $s = q + 1$. Let ℓ^α be any prime-power divisor of $q + 1$.

- If $\ell^\alpha < q + 1$, then ℓ^α is a proper divisor of $q + 1$, and hence

$$\ell^\alpha \leq \frac{q+1}{2} < q.$$

By the induction hypothesis for smaller prime powers, we have

$$\ell^\alpha \mid b_{\ell^\alpha}.$$

- If $\ell^\alpha = q + 1$, then $q + 1$ is itself a prime power. Since $q \geq 5$ is odd, $q + 1$ is even and therefore must be a power of 2. This case has already been established in Case 1.

Thus every prime-power divisor ℓ^α of $q + 1$ satisfies $\ell^\alpha \mid b_{\ell^\alpha}$. Applying Lemma 4 to the shifted sequence $\{b_k\}$ gives $q + 1 \mid b_{q+1}$. Since $\gcd(q, q + 1) = 1$, it follows that $q(q + 1) \mid b_{q+1}$.

Take

$$x = q(q + 1), \quad y = \frac{b_{q+1}}{x}.$$

Since $q \leq n - 1$, we have $q + 1 < \sqrt{\frac{p}{4}}$, and hence $4(q + 1) - 4 < x = q(q + 1) < \frac{p}{4}$. Therefore, $y < p/4$. If $x \neq y$, then Proposition 1 holds. If $x = y$, take

$$x' = q^2, \quad y' = (q + 1)^2.$$

Then $x'y' = b_{q+1}$, $x' \neq y'$, $x', y' < \frac{p}{4}$. Thus Proposition 1 also holds in this case.

It remains only to consider $3 \leq s \leq q$. The argument from Case 3 of Section 3.2.1, with $\beta = 1$, now applies without change.

Subcase 3.2: $\beta \geq 2$

Suppose that $s = q^\beta + 1$. Then $q^\beta \mid b_s$ implies $q^{\beta-1} \mid b_s$. On the other hand, the induction hypothesis gives $q^{\beta-1} \mid b_{q^{\beta-1}}$. By Lemma 3, every index whose corresponding term is divisible by $q^{\beta-1}$ must be a multiple of $q^{\beta-1}$. This is impossible because

$$q^\beta + 1 \not\equiv 0 \pmod{q^{\beta-1}}.$$

Hence $s \neq q^\beta + 1$, $3 \leq s \leq q^\beta$. The argument from Case 3 of Section 3.2.1 now applies without change.

Combining the three cases, we obtain $q^\beta \mid b_{q^\beta}$ for every prime power $q^\beta \leq n - 1$. Therefore, Lemma 4 gives $k \mid b_k$ for every integer $2 \leq k \leq n - 1$.

Since

$$b_k = (k - 2)p + 2\theta = kp - 2(p - \theta),$$

we have $k \mid 2(p - \theta)$. Consequently

$$\text{lcm}(1, 2, \dots, n - 1) \mid 2(p - \theta).$$

Since $p > 6000$, we have $n - 1 \geq 37 > 17$, and hence

$$\psi(n - 1) > 0.85 \left(\sqrt{\frac{p}{4}} - 2 \right) = 0.425 \sqrt{p} - 1.7 > \ln(2p).$$

This contradicts the preceding least common multiple divisibility relation. Therefore, Proposition 1 holds.

3.2.3. $\mu = 3\theta$

Let

$$a_k = (k - 1)p + \theta, \quad k \geq 1,$$

where θ is a prime satisfying $\frac{p}{4} < \theta < \frac{p}{3}$. Define

$$c_k = (k-3)p + 3\theta, \quad k \geq 3.$$

Then

$$c_k = 3a_k - 2kp.$$

Consequently, whenever $k \mid a_k$, we also have $k \mid c_k$. The previously established base divisibilities for the sequence $\{a_k\}$ therefore give

$$3 \mid c_3, \quad 4 \mid c_4, \quad 5 \mid c_5, \quad 6 \mid c_6, \quad 7 \mid c_7.$$

We shall also use the following parity observation. Since p and θ are both odd, for every even integer $k \geq 4$, we have

$$c_k = (k-3)p + 3\theta \equiv 1 + 1 \equiv 0 \pmod{2}.$$

Therefore

$$2 \mid c_k \quad \text{for every even } k \geq 4.$$

This supplies the divisibility corresponding to the prime power 2^1 , although the term c_2 is not defined.

Accordingly, when Lemma 4 is applied to the shifted sequence $\{c_k\}_{k \geq 3}$, the required prime-power divisibilities are proved for all odd prime powers and for 2^β with $\beta \geq 2$. If an integer k satisfies $v_2(k) = 1$, its factor 2 divides c_k by the parity observation above, while its odd prime-power factors are handled by Lemmas 3 and 4. Thus the absence of the term c_2 causes no difficulty in passing from prime powers to general indices.

The restriction $q^\beta \leq n-2$ will be imposed on the prime powers considered in the induction, except that in Case 1, the powers of 2 will be treated up to n for later use in Subcase 3.1.

For every integer $4 \leq k \leq n-2$, we have $k < \theta$ and hence $\gcd(k, \theta) = 1$. Since $c_3 = 3\theta$ and $k \geq 4$, it follows that $k \nmid c_3$. Let s be the smallest index such that $k \mid c_s$. Lemma 2, applied to the shifted sequence $\{c_k\}$, then gives

$$4 \leq s \leq k+2.$$

If x exists such that $x \mid c_k$ and $4k-8 \leq x < \frac{p}{4}$, let $y = \frac{c_k}{x}$. Then

$$y = \frac{(k-3)p + 3\theta}{x} < \frac{(k-2)p}{4(k-2)} = \frac{p}{4},$$

and $xy = c_k \equiv 3\theta \pmod{p}$. If $x \neq y$, then Proposition 1 holds.

It suffices to prove that

$$q^\beta \mid c_{q^\beta}$$

for every prime power q^β satisfying $3 \leq q^\beta \leq n-2$. Compared with the first subsection, the shifted sequence $\{c_k\}$ introduces the two additional possible minimal indices $s = k+1$ and $s = k+2$. Accordingly,

the proof is organized as follows:

$$\left\{ \begin{array}{ll} \text{Case 1: } k = 2^\beta, \beta \geq 3 & \left\{ \begin{array}{l} 4 \leq s \leq 2^\beta, \\ s = 2^\beta + 1, \\ s = 2^\beta + 2; \end{array} \right. \\ \text{Case 2: } k = 3^\beta, \beta \geq 2 & \left\{ \begin{array}{l} 4 \leq s \leq 3^\beta, \\ s = 3^\beta + 1, \\ s = 3^\beta + 2; \end{array} \right. \\ \text{Case 3: } k = q^\beta, q \geq 5 & \left\{ \begin{array}{ll} \text{Subcase 3.1: } \beta = 1 & \left\{ \begin{array}{l} 4 \leq s \leq q, \\ s = q + 1, \\ s = q + 2; \end{array} \right. \\ \text{Subcase 3.2: } \beta \geq 2 & \left\{ \begin{array}{l} 4 \leq s \leq q^\beta, \\ s = q^\beta + 1, \\ s = q^\beta + 2. \end{array} \right. \end{array} \right. \end{array} \right.$$

In Subcase 3.1, the branch $s = q + 2$ is further divided according to whether $q + 2$ is composite but not a prime power, is a prime power, or is a prime. We now consider the above cases in order.

Case 1: $k = 2^\beta$ with $\beta \geq 3$

For use both in the present induction and in Subcase 3.1 below, we establish this case for every power $2^\beta \leq n$, although the divisibility required in the present case only concerns prime powers not exceeding $n - 2$.

Let s be the smallest index such that $2^\beta \mid c_s$, with $4 \leq s \leq 2^\beta + 2$. Since $c_{2^\beta+1}$ is odd, we have $s \neq 2^\beta + 1$. If $s = 2^\beta + 2$, then $2^\beta \mid c_s$ and $\beta \geq 3$ imply $4 \mid c_{2^\beta+2}$. On the other hand, since $4 \mid c_4$, Lemma 3 implies $2^\beta + 2 \equiv 4 \pmod{4}$, which is impossible because $2^\beta + 2 \equiv 2 \pmod{4}$. Hence, $4 \leq s \leq 2^\beta$.

We are thus left with exactly the range treated in Case 1 of Section 3.2.1. Since $2^\beta \leq n$, all the size estimates used there remain valid. Consequently, $2^\beta \mid c_{2^\beta}$ for every power $2^\beta \leq n$.

Case 2: $k = 3^\beta$ with $\beta \geq 2$

Suppose $3^\beta \mid c_s$ with $4 \leq s \leq 3^\beta + 2$. By the inductive hypothesis, $3^{\beta-1} \mid c_{3^{\beta-1}}$. Combined with Lemma 3, the indices of all terms divisible by $3^{\beta-1}$ must be multiples of $3^{\beta-1}$. If $s = 3^\beta + 1$ or $s = 3^\beta + 2$ for $\beta \geq 2$, then necessarily $3^{\beta-1} \mid c_s$, which is a contradiction. Hence, the minimal index s for $k = 3^\beta$ satisfies $s \leq 3^\beta$, and the subsequent proof is completely identical to that for 3^β in the case of $\mu = 1, \theta, \theta^2$ and can be directly reused.

Case 3: $k = q^\beta$ with $q \geq 5$

In this case, the minimal index satisfies

$$4 \leq s \leq q^\beta + 2.$$

Subcase 3.1: $\beta = 1$

Since $5 \mid c_5$ is already guaranteed by the inductive base, we only need to consider $q \geq 7$.

If $s = q + 1$, applying the argument established in the preceding case $\mu = 2\theta$ to the shifted sequence $\{c_k\}$ gives $q(q + 1) \mid c_{q+1}$. Take $x = q(q + 1)$ and $y = c_{q+1}/x$. Then $4(q + 1) - 8 < x < p/4$ and $y < p/4$. If $x \neq y$, Proposition 1 holds. If $x = y$, take $x' = q^2$ and $y' = (q + 1)^2$, and Proposition 1 still holds.

If $s = q + 2$, the discussion is as follows.

- If $q + 2$ is composite but not a prime power, then all its prime-power divisors are proper divisors and hence are less than q . By the inductive hypothesis and Lemmas 3 and 4, we obtain $q + 2 \mid c_{q+2}$. Since $\gcd(q, q + 2) = 1$, it follows that $q(q + 2) \mid c_{q+2}$. Take $x = q(q + 2)$ and $y = c_{q+2}/x$. Then $4(q + 2) - 8 < x < (q + 2)^2 < p/4$, and $y < p/4$. If $x \neq y$, Proposition 1 holds. If $x = y$, take $x' = q^2$ and $y' = (q + 2)^2$. Then

$$x'y' = x^2 = c_{q+2}, \quad x' \neq y', \quad x', y' < \frac{p}{4}.$$

Thus Proposition 1 also holds.

- If $q + 2 = \ell^\alpha$ with $\alpha \geq 2$, then $\ell < q$. The inductive hypothesis gives $\ell \mid c_\ell$, and Lemma 3 gives $\ell \mid c_{q+2}$. If $\ell \geq 5$, take $x = q\ell$. If $\ell = 3$, then $9 \mid q + 2$ and the preceding 3-power case gives $9 \mid c_9$; hence, Lemma 3 gives $9 \mid c_{q+2}$, and we take $x = 9q$. In either case, $x \mid c_{q+2}$ and $4(q + 2) - 8 < x < (q + 2)^2 < p/4$. Let $y = c_{q+2}/x$; then $y < p/4$. If $x \neq y$, Proposition 1 holds. If $x = y$ and $\ell \geq 5$, take $x' = \ell^2$ and $y' = q^2$. If $x = y$ and $\ell = 3$, take $x' = 81$ and $y' = q^2$. In either case, we have

$$x'y' = x^2 = c_{q+2}, \quad x' \neq y', \quad x', y' < \frac{p}{4}.$$

Thus Proposition 1 also holds.

- If $q + 2$ is prime, then from $q \mid c_{q+2}$, Lemma 3 gives $q \mid c_{2q+2}$. Since all prime-power factors of $2q + 2$ are less than q , the inductive hypothesis, Lemma 3, and Lemma 4 give $2q + 2 \mid c_{2q+2}$. Since $\gcd(q, 2q + 2) = 1$, we obtain

$$q(2q + 2) \mid c_{2q+2}.$$

In particular, we have

$$x = q(q + 1) \mid c_{2q+2}.$$

Since $q \leq n - 2$, we have $q + 1 < \sqrt{\frac{p}{4}}$, so $4(2q + 2) - 8 = 8q \leq x < p/4$. Let $y = c_{2q+2}/x$. If $x \neq y$, Proposition 1 holds. If $x = y$, take $x' = q^2$ and $y' = (q + 1)^2$; then $x'y' = c_{2q+2}$ with $x', y' < p/4$, and Proposition 1 still holds.

Therefore, it remains only to consider $4 \leq s \leq q$. The subsequent argument is the same as that for a single prime in the case $\mu = \theta$ and may be applied directly.

Subcase 3.2: $\beta \geq 2$

Consider the minimal index s of divisibility for the prime power q^β , with $4 \leq s \leq q^\beta + 2$. If $s = q^\beta + 1$ or $s = q^\beta + 2$, then necessarily $q^{\beta-1} \mid c_s$. By the inductive hypothesis, $q^{\beta-1} \mid c_{q^{\beta-1}}$. Furthermore, by Lemma 3, the indices of all terms divisible by $q^{\beta-1}$ must be multiples of $q^{\beta-1}$, which yields a contradiction. Hence $s \leq q^\beta$, and the subsequent proof is completely identical to that for q^β in the arithmetic sequence $\{a_k\}$ and can be directly reused.

Combining Cases 1–3, we obtain

$$q^\beta \mid c_{q^\beta}$$

for every prime power q^β satisfying $3 \leq q^\beta \leq n - 2$.

Therefore, if Proposition 1 fails, then $k \mid c_k$ for all $3 \leq k \leq n - 2$. From

$$c_k = (k - 3)p + 3\theta = kp - 3(p - \theta),$$

we obtain $k \mid 3(p - \theta)$, ($3 \leq k \leq n - 2$). Moreover, since p and θ are both odd, we have $2 \mid p - \theta$, and hence $2 \mid 3(p - \theta)$. Therefore, we have

$$\text{lcm}(1, 2, \dots, n - 2) \mid 3(p - \theta).$$

Since $p > 6000$, we have $n - 2 \geq 36 > 17$, so

$$\psi(n - 2) > 0.85 \left(\sqrt{\frac{p}{4}} - 3 \right) = 0.425 \sqrt{p} - 2.55 > \ln(3p),$$

which leads to a contradiction. Hence, Proposition 1 holds.

4. Proof of Proposition 2

Before giving the detailed proof for $C = 6$, we first establish a general existence result for an arbitrary fixed positive integer C . We then formulate an offset-screening and inductive framework for a specified value of C . Once the finite screening reaches the common-offset condition and supplies the required inductive base, the subsequent theoretical argument can be applied. We carry out the complete implementation of this framework for $C = 6$.

4.1. An explicit general existence bound

Proposition 3. *For every fixed integer $C \geq 2$, a constant $p_0(C)$ exists such that for any prime $p \geq p_0(C)$ and any reduced residue μ modulo p , there are two distinct positive integers $x, y \in \left[1, \frac{p}{C}\right)$ satisfying*

$$xy \equiv \mu \pmod{p}, \quad x \neq y.$$

Proof. For sufficiently large p , we may assume that $p > C$. Denote

$$N = \left\lfloor \frac{p}{C} \right\rfloor$$

and define

$$R_\mu(N) = \#\{(x, y) : 1 \leq x, y \leq N, xy \equiv \mu \pmod{p}\}.$$

The qualitative conclusion also follows from the asymptotic result discussed in the Introduction. To obtain an explicitly computable sufficient value of $p_0(C)$, we use the explicit counting estimate derived by Heath-Brown from the Weil bound for Kloosterman sums [5]. This estimate gives

$$\left| R_\mu(N) - \frac{N^2}{p} \right| \leq 2(\log p)(1 + \log p) \sqrt{p}, \quad (4.1)$$

uniformly for all $\mu \not\equiv 0 \pmod{p}$.

Consider the congruence

$$x^2 \equiv \mu \pmod{p}.$$

If z is one solution, then the only other possible solution modulo p is $p - z$. Therefore, the congruence has at most one solution in the interval $1 \leq x \leq N < \frac{p}{2}$, and $R_\mu(N) > 1$ guarantees the existence of a solution satisfying $x \neq y$.

Because $\frac{p-C+1}{C} \leq N < \frac{p}{C}$, it follows from (4.1) that

$$R_\mu(N) \geq \frac{(p-C+1)^2}{C^2 p} - 2(\log p)(1 + \log p) \sqrt{p}.$$

Therefore, the inequality

$$\frac{(p-C+1)^2}{C^2 p} - 2(\log p)(1 + \log p) \sqrt{p} > 1 \quad (4.2)$$

is a sufficient condition for the required off-diagonal representation, and (4.2) can be written as

$$\frac{(p-C+1)^2}{C^2 p^{3/2}} - 2(\log p)(1 + \log p) > \frac{1}{\sqrt{p}} > 0.$$

For every fixed C , the left-hand side tends to $+\infty$ as $p \rightarrow \infty$, whereas $1/\sqrt{p}$ tends to 0. Hence, (4.2) holds for all sufficiently large values of p and provides an explicitly computable sufficient value of $p_0(C)$. $\square$

The numerical evaluation of (4.2) gives the following sufficient choices:

$$p_0(4) = 140,797,667, \quad p_0(6) = 1,062,682,837.$$

These values are merely sufficient analytic thresholds and are much larger than the explicit thresholds 199 and 601 established in this paper. Under the prime-by-prime and nonzero-residue-by-nonzero-residue verification procedure, it would not be practically feasible to extend the finite computation to these analytic thresholds.

4.2. General offset-screening and inductive framework

We now describe the general offset-screening and inductive framework for a specified positive integer C . It follows the same idea as the proof of Proposition 1. For any specified C , all parameters and screening criteria below are defined explicitly. The computational stage seeks a finite certificate reducing all surviving configurations to the common-offset form. If such a certificate is obtained, it supplies the base cases required by the subsequent proof by contradiction and strong induction on prime powers.

Let $L = \text{lcm}\{1, 2, \dots, C-1\}$, and let $m = \pi(C-1)$ be the total number of primes less than C . For each prime $u_i < C$ ($i = 1, 2, \dots, m$), define the integers α_i, η_i such that

$$u_i^{\alpha_i} < LC \leq u_i^{\alpha_i+1}, \quad u_i^{\eta_i} < C \leq u_i^{\eta_i+1}, \quad i = 1, 2, \dots, m.$$

(1) **Computer enumeration for base case construction.** Define the arithmetic sequence

$$a_k = (k-1)p + \mu, \quad (k \geq 1).$$

Take any prime $u_i < C$. Let s_i be the smallest positive index such that $u_i^{\alpha_i} \mid a_{s_i}$, and define the forward offset $\sigma_i = u_i^{\alpha_i} - s_i$. By Lemma 2, we have $0 \leq \sigma_i \leq u_i^{\alpha_i} - 1$.

For a specified value of C , exhaustive enumeration is used to determine whether every noncommon-offset configuration can be eliminated. If the screening is successful, then the failure of Proposition 3 implies that all surviving offsets satisfy $\sigma_1 = \sigma_2 = \dots = \sigma_m = \sigma$, where $\sigma \in \{0, 1, 2, \dots, C-1\}$.

2}. This finite common-offset certificate then serves as the preliminary result for the subsequent inductive argument.

(2) **Mathematical induction.** Let $n < \sqrt{\frac{p}{C}}$. Once the common-offset condition has been verified by computer enumeration, the next step is to establish, for each surviving $\sigma \in \{0, 1, 2, \dots, C-2\}$ and under the assumption that Proposition 3 fails, that $k \mid a_{k-\sigma}$ for all integers k with $\gcd(k, L) = 1$ and $C \leq k \leq n$. This inductive step requires a separate proof for each fixed C and is carried out below for $C = 6$. Once these divisibilities have been established, they imply

$$\text{lcm}\{k \mid C \leq k \leq n, \gcd(k, L) = 1\} \mid ((\sigma + 1)p - \mu).$$

Verification strategy: For any term of the arithmetic sequence $a_k = (k-1)p + \mu$, if there is a divisor $d_k \mid a_k$ satisfying $d_k \geq C \cdot k$, let λ_k be the smallest positive divisor of d_k greater than 1, i.e.,

$$\lambda_k = \min\{s \mid s \mid d_k, s > 1\},$$

take the prime p such that $p > C \cdot \lambda_k d_k$. We then have

$$C \cdot k \leq d_k < \lambda_k d_k < \frac{p}{C}.$$

Let $x = d_k$ and $y = \frac{a_k}{d_k}$. By Lemma 1, we have $1 \leq x, y < \frac{p}{C}$. If $x \neq y$, then Proposition 3 holds; if $x = y$, i.e., $a_k = d_k^2$, we can take $x' = \frac{d_k}{\lambda_k}$ and $y' = \lambda_k d_k$, which still makes Proposition 3 hold.

For a specified value of C , we perform exhaustive computer enumeration on the offset groups $(\sigma_1, \sigma_2, \dots, \sigma_m)$ corresponding to the prime powers $u_1^{\alpha_1}, u_2^{\alpha_2}, \dots, u_m^{\alpha_m}$. The enumeration checks whether every configuration outside the common-offset form $\sigma_1 = \sigma_2 = \dots = \sigma_m = \sigma$ (where $\sigma \in \{0, 1, 2, \dots, C-2\}$) admits a divisor $d_k \mid a_k$ satisfying $d_k \geq C \cdot k$. If this is verified, the preceding divisor construction gives the required representation for every such configuration under the corresponding lower bound on p . The surviving configurations then satisfy the common-offset condition and remain to be treated by strong induction on prime powers.

Parameter setting: Before performing enumeration, we need to determine the range of the index k , denoted $1 \leq k \leq N$. The selection of N is discussed as follows.

Take any prime $u < C$, and define the exponents α, η such that

$$u^\alpha < LC \leq u^{\alpha+1}, \quad u^\eta < C \leq u^{\eta+1}.$$

Let s be the smallest index such that $u^\alpha \mid a_s$. When $s < u^\alpha$, s can be decomposed as

$$s = t \cdot u^\gamma, \quad 1 \leq t < u^{\alpha-\gamma}, \quad 0 \leq \gamma < \alpha,$$

where $\gcd(t, u) = 1$ and $u^\gamma \parallel s$. If $tu^\alpha \mid a_s$ and $\alpha - \gamma \leq \eta$, then $u^{\alpha-\gamma} \leq u^\eta < C$, and thus $tu^\alpha < Cs$. In this case, the divisor $d_s = tu^\alpha$ does not satisfy $d_s \geq Cs$.

It follows from Lemma 3 that if the first divisible index of u^α has a forward shift (i.e., $u^\alpha \mid a_s$ and $s < u^\alpha$), then the first divisible index of any higher power u^β ($\beta > \alpha$) also shifts forward. Taking

$\beta = \alpha + \eta$, let h be the smallest index such that $u^{\alpha+\eta} \mid a_h$. Since $u^\alpha \mid a_h$, we have $h \equiv s \pmod{u^\alpha}$, and hence

$$h = c \cdot u^\alpha + s = c \cdot u^\alpha + t \cdot u^\gamma = u^\gamma \cdot (c \cdot u^{\alpha-\gamma} + t).$$

Since $\gcd(t, u) = 1$, we have $u \nmid (c \cdot u^{\alpha-\gamma} + t)$, and therefore $u^\gamma \parallel h$.

If $\text{lcm}(u^{\alpha+\eta}, h) \mid a_h$, then $h \cdot u^{\alpha+\eta-\gamma} \mid a_h$. Combined with $\gamma < \alpha$, we have $\alpha - \gamma \geq 1$, and thus

$$h \cdot u^{\alpha+\eta-\gamma} \geq h \cdot u^{\eta+1} \geq hC.$$

Given the above derivation, the upper bound of the indices to be verified is taken as

$$N = \max_{1 \leq i \leq m} \{u_i^{\alpha+\eta_i}\},$$

and it is easy to show that $N < LC^2$.

Let a_h denote the first term of the arithmetic sequence divisible by the prime power $u^{\alpha+\eta}$, and define the forward offset $\Delta_u = u^{\alpha+\eta} - h$, so that $h = u^{\alpha+\eta} - \Delta_u$. By the general term $a_k = (k-1)p + \mu$ of the sequence, taking the difference of the two terms gives

$$a_h - a_k = (h - k)p = (u^{\alpha+\eta} - \Delta_u - k)p.$$

Since $u^{\alpha+\eta} \mid a_h$, it follows that $u^\gamma \mid a_h$ for any $0 \leq \gamma \leq \alpha + \eta$. If in addition $u^\gamma \mid a_k$, then

$$0 \equiv u^{\alpha+\eta} - \Delta_u - k \pmod{u^\gamma} \Rightarrow \Delta_u + k \equiv u^{\alpha+\eta} \pmod{u^\gamma}.$$

Therefore, taking γ to be the largest integer satisfying $0 \leq \gamma \leq \alpha + \eta$ and $u^\gamma \mid a_k$, we obtain $u^\gamma = \gcd(k + \Delta_u, u^{\alpha+\eta})$.

The complete computer verification procedure is as follows.

Step (1) Parameter preprocessing

Let $\{U_j\}$ be the set of all primes involved in the verification, where the subset $\{u_i\} \subset \{U_j\}$ consists of all primes satisfying $u_i < C$. All primes involved in the verification follow exactly the same computation and screening rules, regardless of whether they are less than the constant C . For each prime U_j , compute the corresponding exponents

$$\alpha_j = \left\lceil \frac{\ln(LC)}{\ln U_j} \right\rceil - 1, \quad \eta_j = \left\lceil \frac{\ln C}{\ln U_j} \right\rceil - 1.$$

Define the range of indices to be verified as $1 \leq k \leq N$, where

$$N = \max_{1 \leq i \leq m} \{u_i^{\alpha_i+\eta_i}\}, \quad u_i < C.$$

Step (2) Criterion for offset combinations

For any given offset combination, traverse all indices $k = 1, 2, \dots, N$ and compute the product of divisors

$$D_k = \prod_j \gcd(k + \Delta_{U_j}, U_j^{\alpha_j+\eta_j}).$$

If $D_k \geq Ck$, traverse all its positive divisors $d_k \mid D_k$; for each divisor satisfying $d_k \geq C \cdot k$, compute $\lambda_k d_k$ (where $\lambda_k = \min\{s \mid s \mid d_k, s > 1\}$), and among all such divisors d_k , record the minimum value of $\lambda_k d_k$.

- If there is a qualified d_k , record this offset combination and the corresponding minimum $\lambda_k d_k$, and conclude that this offset combination validates the proposition;
- If no qualified d_k is found after traversing all indices k , record this offset combination and mark it as a surviving configuration.

Step (3) Initial screening with all combinations of two primes

Take the first two primes $U_1 = 2$, $U_2 = 3$, whose offsets range over $0 \leq \Delta_{U_j} \leq U_j^{\alpha_j + \eta_j} - 1$ ($j = 1, 2$). Enumerate all offset combinations of the two primes, judge each one according to the rule in Step 2, and only retain all unsolvable configurations.

Step (4) Incremental iterative screening

Add the remaining primes $U_3, U_4, \dots$ one by one in ascending order. Each time a new prime is added, take the Cartesian product of all unsolvable configurations retained from the previous round and all offsets of the current prime to generate new joint offset combinations; after that, judge each combination according to the rule in Step 2, record the offset combinations that validate the proposition and the corresponding $\lambda_k d_k$, and retain the unsolvable configurations. If, after finitely many layers, all remaining unsolved configurations satisfy the common-offset condition $\sigma_1 = \sigma_2 = \dots = \sigma_m = \sigma$ ($\sigma \in \{0, 1, 2, \dots, C - 2\}$), then the screening criterion has been reached and the iteration is stopped. The corresponding congruence relation is

$$\sigma_i \equiv \Delta_{u_i} \pmod{u_i^{\alpha_i}}, \quad u_i < C, \quad i = 1, 2, \dots, m.$$

Step (5) Determine the lower bound of prime p

Take the maximum value among all $\lambda_k d_k$ recorded throughout the process, and let

$$\frac{p}{C} > \max(\lambda_k d_k) \Rightarrow p > C \cdot \max(\lambda_k d_k),$$

which guarantees that all constructed divisors fall within the interval $[1, p/C)$.

For a given constant C , if the procedure above reaches the common-offset screening criterion, the resulting finite verification confirms the base conditions required for strong induction on prime powers

$$u_i^{\alpha_i} \mid a_{u_i^{\alpha_i} - \sigma} \Rightarrow u_i^{\gamma_i} \mid a_{u_i^{\gamma_i} - \sigma}, \\ u_i < C, \quad 1 \leq \gamma_i \leq \alpha_i, \quad u_i^{\gamma_i} > \sigma, \quad 0 \leq \sigma \leq C - 2.$$

4.3. Construction of base cases for $C = 6$

The results of this verification procedure for the case $C = 6$ are presented in Table 1.

In the table, (Δ_2, Δ_3) denotes the coupled offset configuration of the primes 2 and 3. Using Δ_2 or Δ_3 alone does not provide sufficient divisibility information to complete the screening. We therefore begin with the joint screening of (Δ_2, Δ_3) . At the Δ_{23} layer, 300 offset combinations remain.

For $C = 6$, the primes involved in the common-offset condition are 2, 3, and 5, with the corresponding offset parameters σ_1, σ_2 , and σ_3 , respectively. Reducing the 300 remaining offset configurations according to

$$\begin{cases} \sigma_1 \equiv \Delta_2 \pmod{2^8}, \\ \sigma_2 \equiv \Delta_3 \pmod{3^5}, \\ \sigma_3 \equiv \Delta_5 \pmod{5^3}, \end{cases}$$

Table 1. Results of offset combination screening for $C = 6$.

Offset label	Remaining offset combinations	$\max(\lambda_k d_k)$	Final effective bound
(Δ_2, Δ_3)	3127	18,432	5832
Δ_5	1648	16,875	5625
Δ_7	600	21,875	7168
Δ_{11}	540	27,500	6875
Δ_{13}	480	40,625	8125
Δ_{17}	420	53,125	10,625
Δ_{19}	360	59,375	11,875
Δ_{23}	300	71,875	14,375
Δ_{29}	300	1508	—
Δ_{31}	300	1519	—
Δ_{37}	300	2331	—
Δ_{41}	300	2296	—

we obtain $\sigma_1 = \sigma_2 = \sigma_3 = \sigma$, where $\sigma \in \{0, 1, 2, 3, 4\}$. Therefore, the common-offset termination criterion in Step 4 has already been reached at the Δ_{23} layer, and no additional screening layer is required.

As can be seen from Table 1, the results of the original global offset screening exhibit two prominent features

- (1) When the offset layers $\Delta_5, \Delta_7, \dots, \Delta_{23}$ are added sequentially, $\max(\lambda_k d_k)$ rises continuously with the addition of primes and reaches a global peak of 71,875 at the Δ_{23} layer.
- (2) After the prime of the added offset layer exceeds 23, $\max(\lambda_k d_k)$ drops sharply.

The reason for this phenomenon is as follows. Initially, constraints are constructed only from the prime factors 2 and 3, resulting in insufficient constraint strength. To satisfy the judgment condition $d_k \geq Ck$, a larger d_k must be taken, which pushes up the value of $\lambda_k d_k$. When sufficiently many prime factors are added (after the prime exceeds 23), the constraint strength increases significantly, and the judgment condition can be satisfied without a large d_k , and hence the value drops substantially. In addition, to avoid the case $d_k^2 = a_k$ (which corresponds to $x = y = d_k$ and directly violates the premise $x \neq y$ of the proposition), the algorithm introduces λ_k and takes $\lambda_k d_k$ as the lower bound of $\frac{p}{C}$. This operation also raises the lower bound of the prime p .

Table 2. (d_k, k) and verification intervals of prime p for each Δ_q configuration.

d_k	k for (Δ_2, Δ_3)	Interval of prime p
1701	185, 186, 187, 188, 189	[15, 310, 15, 725]
2560	256	[25, 601, 25, 700]
2560	316, 317, 318, 319, 320	[20, 481, 20, 805]
2560	384	[17, 067, 17, 111]
2916	320, 321, 322, 323, 324	[26, 245, 26, 655]
3072	380, 381, 382, 383, 384	[24, 577, 24, 900]
3402	378	[30, 619, 30, 699]
3584	444, 445, 446, 447, 448	[28, 673, 28, 995]

Continued on next page

Continued from previous page

d_k	k	Interval of prime p
3840	384	[38, 401, 38, 500]
3840	576	[25, 601, 25, 644]
4480	448	[44, 801, 44, 900]
4860	648	[36, 451, 36, 506]
5120	636, 637, 638, 639, 640	[40, 961, 41, 282]
5832	644, 645, 646, 647, 648	[52, 489, 52, 896]
d_k	k for Δ_5	Interval of prime p
1375	217, 218, 219, 220	[8594, 8752]
1875	221, 222, 223, 224, 225	[15, 626, 15, 980]
2560	316, 317, 318, 319, 320	[20, 481, 20, 805]
2625	313, 314, 315	[21, 876, 22, 085]
3584	444, 445, 446, 447, 448	[28, 673, 28, 995]
3645	401, 402, 403, 404, 405	[32, 806, 33, 215]
3750	446, 447, 448, 449, 450	[31, 251, 31, 601]
3750	596, 597, 598, 599, 600	[23, 438, 23, 634]
4375	171, 172, 173, 174, 175	[109, 376, 112, 591]
4375	346, 347, 348, 349, 350	[54, 688, 55, 480]
4375	521, 522, 523, 524, 525	[36, 459, 36, 808]
5103	563, 564, 565, 566, 567	[45, 928, 46, 335]
5120	636, 637, 638, 639, 640	[40, 961, 41, 282]
5625	896, 897, 898, 899, 900	[35, 157, 35, 352]
d_k	k for Δ_7	Interval of prime p
1625	63, 64, 65	[40, 626, 42, 590]
1715	241, 242, 243, 244, 245	[12, 006, 12, 255]
4375	346, 347, 348, 349, 350	[54, 688, 55, 480]
4375	521, 522, 523, 524, 525	[36, 459, 36, 808]
5103	563, 564, 565, 566, 567	[45, 928, 46, 335]
6875	546, 547, 548, 549, 550	[85, 938, 86, 725]
7168	892, 893, 894, 895, 896	[57, 345, 57, 665]
d_k	k for Δ_{11}	Interval of prime p
6875	546, 547, 548, 549, 550	[85, 938, 86, 725]
d_k	k for Δ_{13}	Interval of prime p
8125	321, 322, 323, 324, 325	[203, 126, 206, 298]
d_k	k for Δ_{17}	Interval of prime p
1445	81, 82, 83, 84, 85	[24, 566, 26, 100]
1445	166, 167, 168, 169, 170	[12, 283, 12, 654]
2023	115, 116, 117, 118, 119	[34, 392, 35, 899]
2023	234, 235, 236, 237, 238	[17, 196, 17, 564]
2601	149, 150, 151, 152, 153	[44, 218, 45, 710]
3179	183, 184, 185, 186, 187	[54, 044, 55, 527]

Continued on next page

Continued from previous page

d_k	k	Interval of prime p
3757	217, 218, 219, 220, 221	[63, 870, 65, 347]
4335	251, 252, 253, 254, 255	[73, 696, 75, 168]
10625	421, 422, 423, 424, 425	[265, 626, 268, 787]
d_k	k for Δ_{19}	Interval of prime p
11875	471, 472, 473, 474, 475	[296, 876, 300, 033]
d_k	k for Δ_{23}	Interval of prime p
14375	571, 572, 573, 574, 575	[359, 376, 362, 527]

To tighten the lower bound of p , this paper adopts a local small forward-shift pruning strategy for offset configurations with $\lambda_k d_k > 5000$ to reduce the value of $\lambda_k d_k$. We take (Δ_2, Δ_3) as an example to illustrate the idea.

According to the results of the first-round initial screening for (Δ_2, Δ_3) , for each offset configuration with $\lambda_k d_k > 5000$, we superimpose the divisibility effects of the primes 5 and 7, consider the 30 offset configurations given by $5 \mid a_{5-\delta_5}$ and $7 \mid a_{7-\delta_7}$ with $\delta_5 \in \{0, 1, 2, 3, 4\}$ and $\delta_7 \in \{0, 1, 2, 3, 4, 5\}$, recalculate the value of $\lambda_k d_k$, and take the maximum value among them as the $\lambda_k d_k$ value for this (Δ_2, Δ_3) configuration. For example, when $(\Delta_2 = 16, \Delta_3 = 0)$, we obtain $\lambda_k d_k = 18,432$, corresponding to $9216 \mid a_{1008}$. After superimposing the primes 5 and 7 and considering the 30 configurations $(\Delta_2 = 16, \Delta_3 = 0, \delta_5, \delta_7)$, the maximum value of $\lambda_k d_k$ is only 1792.

Similarly, for the cases of $\Delta_5, \Delta_7, \Delta_{11}, \Delta_{13}, \Delta_{17}, \Delta_{19}, \Delta_{23}$ in the table, after each round of initial screening, for each offset configuration with $\lambda_k d_k > 5000$, we superimpose the offsets corresponding to the next two primes and recalculate $\lambda_k d_k$. For instance, for Δ_5 , for each offset configuration with $\lambda_k d_k > 5000$, we superimpose the divisibility effects of the primes 7 and 11, and recalculate $\lambda_k d_k$ on the basis of the offsets $(\Delta_2, \Delta_3, \Delta_5, \delta_7, \delta_{11})$ with $\delta_7 \in \{0, 1, \dots, 5\}$ and $\delta_{11} \in \{0, 1, \dots, 9\}$.

It should be noted that superimposing subsequent small offsets on global bases such as $\Delta_5, \Delta_7, \dots, \Delta_{23}$ may not reduce the peak value of $\max(\lambda_k d_k)$, but it can converge all configurations that generate large values of $\lambda_k d_k$ to a very small number of indices k . The results are shown in Table 2.

By the definition of the sequence $\{a_k\}$: $a_k = (k-1)p + \mu$ with $1 \leq \mu < p$, if $d_k^2 = a_k = kp - (p - \mu)$, we have

$$\frac{d_k^2}{k} < p \leq \frac{d_k^2 - 1}{k - 1} \quad \Rightarrow \quad \left\lfloor \frac{d_k^2}{k} \right\rfloor + 1 \leq p \leq \left\lfloor \frac{d_k^2 - 1}{k - 1} \right\rfloor.$$

For a fixed value of d_k , the interval containing the prime p can be obtained from the given index k , and then the value of μ is given by

$$\mu = d_k^2 - (k - 1)p.$$

As long as the obtained μ can be expressed as the product of two distinct elements in $\left[1, \frac{p}{C}\right)$, the lower bound $\lambda_k d_k$ can be replaced by d_k .

Taking the Δ_5 layer as an example, the raw maximum $\max(\lambda_k d_k) = 16,875$ at the global screening stage is reached by 48 offset configurations. Their minimizing witnesses have $d_k = 5625$, $\lambda_k = 3$, and $k = 313, 314, 315$, with 16 configurations corresponding to each index.

To reduce the lower bound on p , local pruning is applied to every offset configuration whose global screening value exceeds 5000. The offsets corresponding to the next two primes are superimposed, and

the minimum value of $\lambda_k d_k$ is recomputed for each resulting local configuration. Configurations whose new screening value is at most 5000 require no further verification. For every configuration whose value remains above 5000, Table 2 records the smallest admissible divisor d_k and its corresponding index k for the finite verification of the possible equality case $a_k = d_k^2$.

Among the certificate pairs recorded for the Δ_5 layer, the largest value of d_k is 5625, occurring at $k = 896, 897, 898, 899, 900$. These indices refer to the post-pruning certificates rather than to the raw maximum 16,875. The finite verification confirms the required off-diagonal representation in all the corresponding equality cases. Therefore, the final effective bound for the Δ_5 layer is $\max\{5000, 5625\} = 5625$.

The definitions and screening procedure above can be instantiated for any specified positive integer C . Their successful completion, however, depends on whether all noncommon-offset configurations are eliminated after finitely many screening layers. No uniform termination theorem for arbitrary C is claimed here. In the present paper, the detailed global screening and the subsequent inductive argument are carried out for $C = 6$. As C increases, the number of candidate offset combinations may grow rapidly, and the computational feasibility of the screening must therefore be assessed separately for each value of C .

4.4. Inductive step for $C = 6$

For each value of μ under consideration, define

$$a_k = (k - 1)p + \mu, \quad k \geq 1.$$

The restriction $Q = q^b \leq n$ will be imposed only on the prime powers considered in the induction. If $\mu = 2\theta$ with θ being a prime and $p/6 < \theta < p/2$, then $a_1 = 2\theta$ and $2 \mid a_1 = a_{2-1}$. Therefore, the seven types of μ in Auxiliary Proposition 2 can be reduced to five types, corresponding to the offsets $\sigma = 0, 1, 2, 3, 4$, respectively. The correspondence is given in Table 3.

Table 3. Correspondence between the offset σ and the form of μ .

σ	μ (with θ prime)
0	$1, \theta(\frac{p}{6} < \theta < p), \theta^2(\sqrt{\frac{p}{6}} < \theta < \sqrt{p})$
1	$2\theta(\frac{p}{6} < \theta < \frac{p}{2})$
2	$3\theta(\frac{p}{6} < \theta < \frac{p}{3})$
3	$4\theta(\frac{p}{6} < \theta < \frac{p}{4})$
4	$5\theta(\frac{p}{6} < \theta < \frac{p}{5})$

In this paper, the primes p are treated in two ranges:

- (1) If $601 \leq p \leq 86,250$, Proposition 2 is verified by computer enumeration;
- (2) If $p > 86,250$, Proposition 2 is proved by contradiction and strong induction on prime powers.

The finite range $601 \leq p \leq 86,250$ contains 8276 primes. For each of these primes, the program sets

$$N_p = \left\lfloor \frac{p}{6} \right\rfloor$$

and enumerates all pairs of integers satisfying $1 \leq x < y \leq N_p$. It then computes all residues $xy \bmod p$ and verifies that

$$\{xy \bmod p : 1 \leq x < y \leq N_p\} = \{1, 2, \dots, p-1\}.$$

Thus every nonzero residue class modulo p is represented by two distinct integers satisfying the strict inequalities $1 \leq x, y < p/6$. No failure occurs for any of the 8276 primes in this range.

It remains to consider the case $p > 86,250$. Throughout the remainder of the proof, suppose, for contradiction, that Proposition 2 does not hold. The computer-assisted offset screening then shows that for the value $\sigma \in \{0, 1, 2, 3, 4\}$ corresponding to the residue class under consideration, we have

$$2^8 \mid a_{2^8-\sigma}, \quad 3^5 \mid a_{3^5-\sigma}, \quad 5^3 \mid a_{5^3-\sigma}.$$

Let

$$n = \left\lfloor \frac{1}{2} \sqrt{\frac{p}{6}} \right\rfloor - 1.$$

Since $p > 86,250$, we have $n \geq 58$.

We now fix $\sigma \in \{0, 1, 2, 3, 4\}$. For each fixed σ , we establish the required divisibilities by strong induction on prime powers ordered by their size. More precisely, when treating a prime power q^β , the induction hypothesis is applied only to prime powers smaller than q^β , in accordance with the induction convention stated after Lemma 4.

By Lemma 4, it suffices to prove that

$$q^\beta \mid a_{q^\beta-\sigma}$$

for every prime power $q^\beta \leq n$ satisfying $\gcd(q, L) = 1$.

4.4.1. $\sigma = 0, 1, 2, 3, 4$

Fix $\sigma \in \{0, 1, 2, 3, 4\}$, and let μ be one of the corresponding values listed in Table 3. Thus, when $\sigma = 0$, we have $\mu \in \{1, \theta, \theta^2\}$, with θ satisfying the conditions in Table 3; when $1 \leq \sigma \leq 4$, we have $\mu = (\sigma + 1)\theta$. Define

$$b_k = a_{k-\sigma} = (k - \sigma - 1)p + \mu, \quad k \geq \sigma + 1,$$

so that $b_k = a_k$ when $\sigma = 0$. The restriction $Q = q^\beta \leq n$ will be imposed only on the prime powers considered in the induction. Since $0 < \mu < p$, we have $b_k < (k - \sigma)p$. Hence, if $x \mid b_k$ and $x \geq 6(k - \sigma)$, then $b_k/x < p/6$.

The preceding computational verification gives

$$2^8 \mid b_{2^8}, \quad 3^5 \mid b_{3^5}, \quad 5^3 \mid b_{5^3}. \quad (4.3)$$

Suppose that Proposition 2 does not hold. Put

$$Q = q^\beta \leq n, \quad q \geq 7. \quad (4.4)$$

We prove the required divisibility by strong induction on the prime powers Q , ordered by their size.

Let h be the smallest index such that $Q \mid b_h$. The conditions in Table 3 imply that $n < \theta$ whenever θ occurs. Since $Q \leq n$, $q > \sigma + 1$, and $b_{\sigma+1} = \mu$, we have $Q \nmid b_{\sigma+1}$. By Lemma 2, we have

$$2 \leq h - \sigma \leq Q \iff \sigma + 2 \leq h \leq Q + \sigma. \quad (4.5)$$

In this subsection, we prove that $h = Q$.

Since $n = \left\lfloor \frac{1}{2} \sqrt{\frac{p}{6}} \right\rfloor - 1$ and $n \geq 58$, for $0 \leq \sigma \leq 4$, we have

$$n + \sigma < 2(n + 1), \quad (n + \sigma)^2 < 4(n + 1)^2 < \frac{p}{6}.$$

It follows from Eqs (4.4) and (4.5) that

$$Q^2 < \frac{p}{6}, \quad h^2 < \frac{p}{6}. \quad (4.6)$$

We now assume that $h \neq Q$. We first treat the cases where $h < Q$, or where $Q < h \leq Q + \sigma$ and h is composite. For $\sigma = 0$, only the first of these possibilities can occur. For $1 \leq \sigma \leq 4$, after these cases are eliminated, parity shows that the only remaining possibilities are the prime indices $h = Q + 2$ and $h = Q + 4$.

Case 1: $h < Q$, or $Q < h \leq Q + \sigma$ and h is composite.

Case 1.1: $v_2(h) \leq 8$, $v_3(h) \leq 5$, $v_5(h) \leq 3$, and h is not of the form $h = \ell^\alpha > Q$ with $\ell \geq 7$.

Let z^α be any prime-power divisor of h . If $z \in \{2, 3, 5\}$, then Eq (4.3), $z^\alpha \mid h$, and Lemma 3 give $z^\alpha \mid b_h$. If $z \geq 7$, then the conditions of Case 1.1 imply that $z^\alpha < Q$. The induction hypothesis gives $z^\alpha \mid b_{z^\alpha}$, and Lemma 3 then yields $z^\alpha \mid b_h$. Therefore, every prime-power divisor of h divides b_h , and hence $h \mid b_h$.

Write $h = q^r t$, where $q \nmid t$. If $h < Q$, then clearly $0 \leq r \leq \beta - 1$. If $h > Q$, then by Eq (4.5), we may write $h = Q + j$, where $1 \leq j \leq \sigma < q$. Hence, $q \nmid h$, and in this case, $r = 0$. Therefore, we have

$$\text{lcm}(h, Q) = Qt, \quad Qt \mid b_h.$$

Take $x = Qt$ and $y = b_h/x$. By Eq (4.5)

$$x = \frac{Q}{q^r} h \geq qh > 6(h - \sigma), \quad x \leq Qh \leq (Q + \sigma)^2 \leq (n + \sigma)^2 < \frac{p}{6},$$

and hence $y < p/6$. If $x \neq y$, Proposition 2 holds. If $x = y$, then

$$b_h = x^2 = t^2 Q^2.$$

Take $x' = t^2$ and $y' = Q^2$. Since $q \nmid t$, we have $t^2 \neq Q^2$. Moreover, since $t \leq h$, it follows from Eq (4.6) that $t^2 < p/6$, $Q^2 < p/6$. Thus Proposition 2 also holds in this case.

Case 1.2: $v_2(h) > 8$, $v_3(h) > 5$, or $v_5(h) > 3$.

Accordingly, take

$$d = 2^8, \quad d = 3^5, \quad \text{or} \quad d = 5^3.$$

By Eq (4.3), Lemma 3, and $d \mid h$, we obtain $d \mid b_h$. Since $\gcd(Q, d) = 1$, it follows that $Qd \mid b_h$. Take $x = Qd$ and $y = b_h/x$. By Eq (4.5), we have $d \geq 125$ and $h - \sigma \leq Q$, and therefore

$$x = Qd > 6(h - \sigma), \quad x \leq Qh \leq (n + \sigma)^2 < \frac{p}{6}.$$

Hence, $y < p/6$. If $x \neq y$, Proposition 2 holds. If $x = y$, then

$$b_h = x^2 = d^2 Q^2.$$

Take $x' = d^2$ and $y' = Q^2$. Since $\gcd(Q, d) = 1$, these two factors are distinct. Moreover, since $d \leq h$, it follows from Eq (4.6) that $d^2, Q^2 < p/6$. Thus Proposition 2 also holds in this case.

Case 1.3: $h = Q + j = \ell^\alpha$, where $\ell \geq 7$ and $\alpha \geq 2$.

By Eq (4.5), we have $1 \leq j \leq \sigma \leq 4$. Since $\ell^\alpha = Q + j$, we have $\ell < Q$. Moreover, $\ell \neq q$; otherwise, $q \mid h - Q = j$, contradicting $1 \leq j \leq \sigma < q$. Therefore, $\gcd(Q, \ell) = 1$.

The induction hypothesis gives $\ell \mid b_\ell$. Since $\ell \mid h$, Lemma 3 gives $\ell \mid b_h$, and hence $Q\ell \mid b_h$. Take $x = Q\ell$ and $y = b_h/x$. By Eq (4.5), $h - \sigma \leq Q$, and therefore

$$x > 6(h - \sigma), \quad x \leq Qh \leq (n + \sigma)^2 < \frac{p}{6}.$$

Thus $y < p/6$. If $x \neq y$, Proposition 2 holds. If $x = y$, then

$$b_h = x^2 = \ell^2 Q^2.$$

Take $x' = \ell^2$ and $y' = Q^2$. Since $\ell < Q$, it follows from Eq. (4.6) that $\ell^2 < p/6, Q^2 < p/6$. Thus Proposition 2 also holds in this case.

Cases 1.1–1.3 show that Proposition 2 holds whenever $h < Q$, or whenever $h > Q$ and h is composite. For $\sigma = 0$, this exhausts all possibilities with $h \neq Q$. For $1 \leq \sigma \leq 4$, it remains to consider the case in which $h > Q$ and h is prime.

Since Q is odd, both $Q + 1$ and $Q + 3$ are even integers. Therefore, the only remaining possibilities are $h = Q + 2$ and $h = Q + 4$.

Case 2: $h = Q + 2$ is prime.

This case can occur only for $\sigma = 2, 3, 4$. Since neither Q nor $Q + 2$ is divisible by 2 or 3, we must have $Q \equiv 5 \pmod{6}$, and hence

$$12 \mid 2Q + 2.$$

Since $Q \mid b_{Q+2}$, Lemma 3 gives $Q \mid b_{2Q+2}$. On the other hand, Eq (4.3), Lemma 3, and $12 \mid 2Q + 2$ give $12 \mid b_{2Q+2}$. Since $\gcd(Q, 12) = 1$, we have

$$12Q \mid b_{2Q+2}.$$

Take $x = 12Q$ and $y = b_{2Q+2}/x$. For $\sigma = 2, 3, 4$, we have

$$x = 12Q \geq 6((2Q + 2) - \sigma), \quad x = 12Q \leq 12n < 4(n + 1)^2 \leq \frac{p}{6}.$$

Therefore, $y < p/6$. If $x \neq y$, Proposition 2 holds. If $x = y$, then

$$b_{2Q+2} = x^2 = 144Q^2.$$

Take $x' = 144$ and $y' = Q^2$. These two factors are distinct. Moreover, Eq (4.6) gives $Q^2 < p/6$, while $144 < p/6$. Thus Proposition 2 also holds in this case.

Case 3: $h = Q + 4$ is prime.

This case can occur only for $\sigma = 4$. Put

$$T = 4(Q + 1) = 4Q + 4.$$

Since $Q \mid b_{Q+4}$ and $T \equiv Q + 4 \pmod{Q}$, Lemma 3 gives $Q \mid b_T$. Moreover, $\gcd(Q, T) = 1$.

Since $Q + 4$ is prime, we have $Q \equiv 1 \pmod{3}$, and hence $3 \nmid T$.

Case 3.1: $v_2(T) \leq 8$ and $v_5(T) \leq 3$.

Let z^α be any prime-power divisor of T . Since $3 \nmid T$, we have the following two possibilities:

- If $z = 2$ or 5 , then the conditions of Case 3.1 give $z^\alpha \mid 2^8$ or $z^\alpha \mid 5^3$, respectively. It follows from Eq (4.3) and Lemma 3 that $z^\alpha \mid b_T$.
- If $z \geq 7$, then $z^\alpha \mid Q + 1$, and hence

$$z^\alpha \leq \frac{Q+1}{2} < Q.$$

The induction hypothesis gives $z^\alpha \mid b_{z^\alpha}$, and Lemma 3 then yields $z^\alpha \mid b_T$.

Therefore, every prime-power divisor of T divides b_T , and hence $T \mid b_T$. Take

$$x = QT = 4Q(Q + 1), \quad y = \frac{b_T}{x}.$$

Since

$$x > 24Q = 6(T - 4), \quad x = 4Q(Q + 1) \leq 4n(n + 1) < \frac{p}{6},$$

we have $y < p/6$. If $x \neq y$, Proposition 2 holds. If $x = y$, then

$$b_T = x^2 = 16Q^2(Q + 1)^2.$$

Take $x' = 4Q^2, y' = 4(Q + 1)^2$. We have

$$4Q^2 < 4(Q + 1)^2 < \frac{p}{6}.$$

Therefore, Proposition 2 also holds in this case.

Case 3.2: $v_2(T) > 8$ or $v_5(T) > 3$.

If $v_2(T) > 8$, take $d = 2^8 = 256$; if $v_5(T) > 3$, take $d = 5^3 = 125$. By Eq (4.3) and Lemma 3, we have $d \mid b_T$, and hence $Qd \mid b_T$. Take $x = Qd$ and $y = b_T/x$. Clearly

$$x > 24Q = 6(T - 4).$$

If $d = 256$, then $v_2(T) > 8$ implies $2^7 \mid Q + 1$, and hence $Q \geq 127$. If $d = 125$, then $5^3 \mid Q + 1$, and hence $Q \geq 124$. In both cases, we have

$$Qd < 4(Q + 1)^2 < \frac{p}{6}, \quad d^2 \leq 4(Q + 1)^2 < \frac{p}{6}.$$

Therefore, $x, y < p/6$. If $x \neq y$, Proposition 2 holds. If $x = y$, then

$$b_T = x^2 = d^2 Q^2.$$

Take $x' = d^2$ and $y' = Q^2$. These two factors are distinct, and the preceding inequalities together with Eq (4.6) show that both are less than $p/6$. Thus Proposition 2 also holds in this case.

In conclusion, whenever $h \neq Q$, we can construct two distinct factors satisfying Proposition 2, contradicting our assumption. Therefore, we have

$$Q \mid b_Q$$

for every prime power $Q = q^\beta \leq n$ with $q \geq 7$.

By Lemma 4, $k \mid b_k$ for every integer k satisfying

$$\sigma + 1 \leq k \leq n, \quad \gcd(k, L) = 1.$$

Since 1 does not affect the least common multiple and

$$b_k = kp - ((\sigma + 1)p - \mu),$$

we obtain

$$\text{lcm} \{1 \leq k \leq n : \gcd(k, L) = 1\} \mid (\sigma + 1)p - \mu.$$

When $\sigma = 0$, we have

$$\text{lcm} \{1 \leq k \leq n : \gcd(k, L) = 1\} \leq p - \mu < p.$$

When $1 \leq \sigma \leq 4$, we have

$$(\sigma + 1)p - \mu = (\sigma + 1)(p - \theta) < (\sigma + 1)p \leq 5p.$$

Thus, for every $\sigma \in \{0, 1, 2, 3, 4\}$, we have

$$\text{lcm} \{1 \leq k \leq n : \gcd(k, L) = 1\} < 5p.$$

4.4.2. Contradiction and completion of the proof

Let

$$M_n = \text{lcm} \{1 \leq k \leq n : \gcd(k, 60) = 1\}.$$

From the preceding discussion, if Proposition 2 does not hold, then

$$M_n < 5p.$$

The prime-power contributions omitted from M_n are precisely those corresponding to the primes 2, 3, and 5. Each of these three contributions to $\psi(n)$ is at most $\ln n$. Therefore

$$\ln M_n \geq \psi(n) - 3 \ln n.$$

Consequently

$$\psi(n) - 3 \ln n < \ln(5p).$$

Since $p > 86,250$, we have $n \geq 58$. Hence, by the estimate established in Section 3.2.1, $\psi(n) > 0.85n$. Since $n = \left\lfloor \frac{1}{2} \sqrt{\frac{p}{6}} \right\rfloor - 1$, we have

$$\frac{1}{2} \sqrt{\frac{p}{6}} - 2 \leq n \leq \frac{1}{2} \sqrt{\frac{p}{6}} - 1.$$

Hence, for $p > 86,250$,

$$\begin{aligned} \psi(n) - 3 \ln n &> 0.85n - 3 \ln n \\ &\geq 0.85 \left(\frac{1}{2} \sqrt{\frac{p}{6}} - 2 \right) - 3 \ln \left(\frac{1}{2} \sqrt{\frac{p}{6}} - 1 \right) \\ &> \ln(5p). \end{aligned}$$

Here, the last inequality holds for every $p > 86,250$. A direct calculation shows that the difference between its left-hand side and right-hand side is positive at $p = 86,250$, and direct differentiation shows that this difference is increasing thereafter. This contradicts

$$\psi(n) - 3 \ln n < \ln(5p).$$

Therefore, the assumption that Proposition 2 does not hold is false, and Proposition 2 follows.

Use of AI tools declaration

The author used AI to assist with English translation. The translated text was reviewed and revised by the author.

Acknowledgments

The author is deeply grateful to the anonymous reviewers for an exceptionally careful reading of the manuscript and for constructive comments. These contributions have substantially improved the rigor and presentation of the manuscript.

This work was partially supported by the National Natural Science Foundation of China (Grant No. 12271155) and the Doctoral Research Start-up Fund of Hunan University of Science and Technology (Grant No. E52170).

Conflict of interest

The author declares no conflict of interest.

References

1. M. Z. Garaev, Character sums in short intervals and the multiplication table modulo a large prime, *Monatsh. Math.*, **148** (2006), 127–138. <https://doi.org/10.1007/s00605-005-0390-6>
2. M. Z. Garaev, A. A. Karatsuba, The representation of residue classes by products of small integers, *Proc. Edinb. Math. Soc.*, **50** (2007), 363–375. <https://doi.org/10.1017/S0013091504001145>

3. J. Cilleruelo, M. Z. Garaev, Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications, *Math. Proc. Cambridge Philos. Soc.*, **160** (2016), 477–494. <https://doi.org/10.1017/S0305004116000051>
4. I. E. Shparlinski, Modular hyperbolas, *Jpn. J. Math.*, **7** (2012), 235–294. <https://doi.org/10.1007/s11537-012-1140-8>
5. D. R. Heath-Brown, Arithmetic applications of Kloosterman sums, *Nieuw Arch. Wiskunde*, **1** (2000), 380–384.
6. J. B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6** (1962), 64–94. <https://doi.org/10.1215/ijm/1255631807>



AIMS Press

©2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0>)