THE INDEX OF SMALL LENGTH SEQUENCES

DAVID J. GRYNKIEWICZ AND UZI VISHNE

ABSTRACT. Let \( n \geq 2 \) be a fixed integer. Define \( (x)_n \) to be the unique integer in the range \( 0 \leq (x)_n < n \) which is congruent to \( x \) modulo \( n \). Given \( x_1, \ldots, x_\ell \in \mathbb{Z} \), let

\[
\| (x_1, \ldots, x_\ell) \|_1 = \min \{ (ux_1)_n + \cdots + (ux_\ell)_n : u \in \mathbb{Z}, \gcd(u, n) = 1 \}
\]

and define \( \text{Ind}(x_1, \ldots, x_\ell) = \frac{1}{n} \| (x_1, \ldots, x_\ell) \|_1 \) to be the index of the sequence \((x_1, \ldots, x_\ell)\). If \( x_1, \ldots, x_\ell \in \mathbb{Z} \) have \( \sum_{x \in I} x \equiv 0 \pmod{n} \) but \( \sum_{x \in I} x \neq 0 \) for all proper, nonempty subsets \( I \subseteq [1, \ell] \), then a still open conjecture asserts that \( \text{Ind}(S) = 1 \). We give an alternative proof, that does not rely on computer calculations, verifying this conjecture when \( n \) is a product of two prime powers.

1. INTRODUCTION

Let \( n \geq 2 \) be a fixed integer. For every integer \( x \in \mathbb{Z} \), we define \( (x)_n \) to be the unique integer in the range \( 0 \leq (x)_n < n \) which is congruent to \( x \) modulo \( n \). This integer representative is defined in the same way for \( x \in \mathbb{Z}/n\mathbb{Z} \). Let \( S = (x_1, \ldots, x_\ell) \) be a sequence of elements (allowing repetition) \( x_1, \ldots, x_\ell \in \mathbb{Z} \) or \( x_1, \ldots, x_\ell \in \mathbb{Z}/n\mathbb{Z} \). We call

\[
|S|_1 = \| (x_1, \ldots, x_\ell) \|_1 = \min \{ (ux_1)_n + \cdots + (ux_\ell)_n : u \in \mathbb{Z}, \gcd(u, n) = 1 \} \tag{1}
\]

the projective \( \ell_1 \)-norm of the sequence \( S \), and \( \text{Ind}(S) = \frac{1}{n} |S|_1 \) is called the index of \( S \). The sequence \( S \) (assuming the elements are from \( \mathbb{Z} \), with analogous definitions when they are from \( \mathbb{Z}/n\mathbb{Z} \)) is called

- a zero-sum sequence (modulo \( n \)) if \( x_1 + \cdots + x_\ell \equiv 0 \pmod{n} \),
- a zero-sum free sequence if \( \sum_{x \in I} x \neq 0 \pmod{n} \) for all nonempty subsets \( I \subseteq [1, \ell] \), and
- a minimal zero-sum sequence (modulo \( n \)) if it is a zero-sum sequence but \( \sum_{x \in I} x \neq 0 \pmod{n} \) for all proper, nonempty subsets \( I \subseteq [1, \ell] \).

Clearly, if \( u \in \mathbb{Z} \) is an element attaining the minimum in Equation (1), then \( |S|_1 = u \sum_{x \in I} x \pmod{n} \).

In particular, if \( S \) is a zero-sum sequence, then \( \text{Ind}(S) \) is a non-negative integer that has been the subject of much study \([1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]\). Assume \( S \) is a minimal zero-sum sequence. Then, when \( \ell \leq 3 \), a simple argument shows that \( \text{Ind}(S) = 1 \) \([9]\). When either \( 5 \leq \ell \leq \frac{n}{2} + 1 \) or else \( \ell = 4 \) and \( \gcd(n, 6) \neq 1 \), examples are known showing \( \text{Ind}(S) > 1 \) is possible \([9]\). For \( \ell > \frac{n}{2} + 1 \), \( \text{Ind}(S) = 1 \) is known to once more hold \([1, 15]\). For the remaining case, namely, when \( \ell = 4 \) and \( \gcd(n, 6) = 1 \), computer calculations for \( n \leq 1000 \) indicated that \( \text{Ind}(S) = 1 \) might always hold \([9]\) \([6]\), leading to the following conjecture.

**Conjecture 1.1.** If \( S = (x_1, x_2, x_3, x_4) \) is a minimal zero-sum sequence modulo \( n \geq 5 \) and \( \gcd(n, 6) = 1 \), then \( |S|_1 = n \).

Many of the previous citations were devoted to partial progress proving Conjecture 1.1. In particular, Conjecture 1.1 is known when \( n \) is a prime power \([7]\), when \( \gcd(x_i, n) \neq 1 \) for some \( i \in [1, 4] \) \([8]\),
when \( n \) is a product of two prime powers [12], and more recently, when \( \gcd(n, 30) = 1 \) [10]. These results each build upon the prior result and are reliant on numerical calculations for small \( n \), including [7], which is needed in turn for [8] and for [12], while all of these papers are needed for the argument in [10]. The goal of this paper is to give an alternative proof when \( n \) is a product of two prime powers that does not rely on computer computations, allowing direct verification of the conjecture for the relevant \( n \leq 1000 \) and combining the results of [7] and [12] simultaneously. Indeed, our result covers all \( n \leq 1000 \) with \( \gcd(n, 30) = 1 \), removing all computational calculations previously needed for [10]. As will be seen in the proof, the majority of the complications that arise in our arguments happen only when \( 5 \mid n \) (more than half our arguments are devoted solely to this case), giving further indication that the case when \( 5 \mid \) is fundamentally harder than the case \( \gcd(n, 30) = 1 \).

2. Basic Observations

Given \( x, y \in \mathbb{R} \), we use interval notation \([x, y] = \{ z \in \mathbb{Z} : x \leq z \leq y \}\) for discrete intervals. The intervals \([x, y)\), \([x, y)\) and \((x, y]\) are also discrete and analogously defined. Let \( S = (x_1, \ldots, x_\ell) \) with \( x_i \in \mathbb{Z} \). We begin with some easy observations. First, the order of entries in the sequence \( S \) does not change the projective norm. Secondly, multiplying each \( x_i \) by an integer relatively prime to \( n \) does not change the projective norm. Thirdly, a zero entry can be removed, reducing to a shorter sequence, without changing the value of the projective norm, meaning it suffices to only consider \( x_i \in \mathbb{Z} \) which are nonzero modulo \( n \). For \( x \in \mathbb{Z} \), we have

\[
(x)_n = x - \left\lfloor \frac{x}{n} \right\rfloor n.
\]

When \( x \equiv 0 \pmod{n} \), we have \((-x)_n = n - (x)_n\), so that

\[
(-x)_1 + \ldots + (-x)_n = \ell n - ((x)_1 + \ldots + (x)_n)
\]

when all \( x_i \) are nonzero modulo \( n \). This has an important consequence for bounding \( \|(x_1, \ldots, x_\ell)_n\|_1 \).

**Proposition 2.1.** Let \( \ell \geq 0 \) and \( n \geq 2 \) be integers and let \( x_1, \ldots, x_\ell \in \mathbb{Z} \).

1. If \( x_1 + \cdots + x_\ell \equiv 0 \pmod{n} \), then \( \|(x_1, \ldots, x_\ell)_n\|_1 \leq \left\lfloor \frac{\ell}{2} \right\rfloor n \).

2. If \( x_1 + \cdots + x_\ell \equiv -x_{\ell+1} \pmod{n} \) with \( \gcd(x_{\ell+1}, n) = y < n \), then \( \|(x_1, \ldots, x_\ell)_n\|_1 \leq \frac{\ell-1}{2} n + y \) for \( \ell \) odd and \( \|(x_1, \ldots, x_\ell)\|_1 \leq \frac{\ell}{2} n - y \) for \( \ell \) even.

**Proof.** If some \( x_i \equiv 0 \pmod{n} \), then this entry can be erased from the vector, and the result follows by induction on the length \( \ell \) (note \( 2y \leq n \) under the hypotheses of Part 2). So we assume all \( x_i \not\equiv 0 \). Consider the numbers

\[
s_u = (ux_1)_n + \ldots + (ux_\ell)_n
\]

for \( u \in \mathbb{Z} \). If \( x_1 + \cdots + x_\ell \equiv 0 \pmod{n} \), then \( s_u \equiv 0 \pmod{n} \) for every \( u \), and \( s_u \in \{0, n, \ldots, (\ell - 1)n\} \). When \( \gcd(u, n) = 1 \), we have \( s_u + s_{n-u} = \ell n \) by Equation (3) with both \( s_u \) and \( s_{n-u} \) divisible by \( n \), so that one of the two values is at most \( \left\lfloor \frac{\ell}{2} \right\rfloor n \), giving the upper bound for \( \|(x_1, \ldots, x_\ell)_n\|_1 \) from Part 1.

Now assume \( x_1 + \cdots + x_\ell \equiv -x_{\ell+1} \pmod{n} \) with \( \gcd(x_{\ell+1}, n) = y < n \). Then \( y \leq n - y \). Let \( u \in \mathbb{Z} \) be an integer with \( \gcd(u, n) = 1 \) and \( -ux_{\ell+1} \equiv y \pmod{n} \). Then \( s_u + s_{n-u} = \ell n \) by Equation (3) with \( s_u \in \{y, n+y, \ldots, (\ell-2)n+y\} \) and \( s_{n-u} \in \{n-y, 2n-y, \ldots, (\ell-1)n-y\} \). If \( \ell \) is odd, and \( s_u = \frac{\ell-1}{2} n + tn + y \), then \( s_{n-u} = \frac{\ell-1}{2} n - (t-1)n - y \). Thus \( \min\{s_u, s_{n-u}\} \leq \frac{\ell-1}{2} n + y \). If \( \ell \) is even, and \( s_u = \frac{\ell}{2} n + tn + y \), then \( s_{n-u} = \frac{\ell}{2} n - tn - y \). Thus \( \min\{s_u, s_{n-u}\} \leq \frac{\ell}{2} n - y \). □
When \( \ell \leq 2 \), it is relatively routine to determine \( \|(x_1, x_2)\|_1 \) or \( \|(x_1)\|_1 \) using the observations mentioned above. Thus the first case of principal interest is \( \ell = 3 \). If \((x_1, x_2, x_3)\) is a sequence with nonzero entries modulo \( n \) and \( x_1 + x_2 + x_3 \equiv 0 \) (mod \( n \)), then \( \|(x_1, x_2, x_3)\|_1 = n \) by Proposition 2.1. If some subsequence is zero-sum modulo \( n \), say \( x_1 + x_2 \equiv 0 \) (mod \( n \)), then Equation (3) assures us that \( (ux_1)_\ell + (ux_2)_\ell = n \) for any \( u \in \mathbb{Z} \) with \( \gcd(u, n) = 1 \). Thus \( \|(x_1, x_2, x_3)\|_1 = n + \gcd(x_3, n) \) in this case. The case when \((x_1, x_2, x_3)\) is zero-sum free is much more difficult.

Given a sequence \( S = (x_1, \ldots, x_\ell) \) with \( x_i \in \mathbb{Z}/n\mathbb{Z} \), one can extend \( S \) to zero-sum sequence \( S^* = (x_1, \ldots, x_\ell, x_\ell+1) \), where \( x_\ell := -\sum_{i=1}^\ell x_i \). If \( S \) is zero-sum free with \( \ell \geq 1 \), it is easily observed that \( S^* \) is then a minimal zero-sum sequence, for any zero-sum subsequence of \( S^* \) together with its complement partitions the terms of \( S^* \) into a pair of disjoint zero-sum subsequences. Conversely, given any such minimal zero-sum sequence \((x_1, \ldots, x_\ell, x_\ell+1)\) and removing any coordinate yields a zero-sum free sequence of length \( \ell \).

Since each \( x_i \) must be nonzero in a minimal zero-sum vector with \( \ell \geq 2 \), Conjecture 1.1 implies that \( \|(x_1, x_2, x_3)\|_1 < \|(x_1, x_2, x_3, -x_1 - x_2 - x_3)\|_1 \) for any zero-sum free vector \((x_1, x_2, x_3)\). On the other hand, if \((x_1, x_2, x_3)\) is zero-sum free, then we have \( \|(x_1, x_2, x_3, -x_1 - x_2 - x_3)\|_1 = \|(x_1, x_2, x_3)\|_1 + 1 \). Since the projective norm of a zero-sum sequence must be a multiple of \( n \), it then follows that \( \|(x_1, x_2, x_3)\|_1 \leq n \) implies that \( \|(x_1, x_2, x_3, -x_1 - x_2 - x_3)\|_1 = n \). Consequently, from the relationship between minimal zero-sum and zero-sum free vectors mentioned above, we see that Conjecture 1.1, regarding minimal zero-sum sequences of length four, is equivalent to the following conjecture, regarding zero-sum free sequences of length three.

**Conjecture 2.2.** If \( S = (x_1, x_2, x_3) \) is a zero-sum free sequence modulo \( n \geq 5 \) and \( \gcd(n, 6) = 1 \), then \( |S|_1 < n \).

Our main result is a proof of the following theorem.

**Theorem 2.3.** Let \( n \geq 5 \) be an integer relatively prime to 6 and let \((x_1, x_2, x_3, x_4)\) be a minimal zero-sum (modulo \( n \)) sequence, where \( x_i \in \mathbb{Z} \). Suppose

- \( n = p^\alpha \) with \( p \) prime and \( \alpha \geq 1 \), or
- \( n = p^{\alpha}q^\beta \) with \( p < q \) distinct primes, \( \alpha, \beta \geq 1 \) and \( \gcd(x_i, n) = 1 \) for all \( i \in [1, 4] \).

Then

\[
\|(x_1, x_2, x_3, x_4)\|_1 = n.
\]

Before beginning the proof of Theorem 2.3, we proceed with a lemma that describes some basic properties of certain "discrete lines", which will be our main tool for tackling Theorem 2.3. In what follows, given a set \( Y \), we use \( 1_Y \) for the characteristic function of \( Y \): \( 1_Y(u) = 1 \) when \( u \in Y \), and \( 1_Y(u) = 0 \) when \( u \notin Y \).

**Lemma 2.4.** For \( x \in [1, n-1] \) and \( n \geq 2 \), let

\[
X(x) = \left\{ \left\lfloor \frac{n}{x} \right\rfloor, \left\lfloor \frac{2n}{x} \right\rfloor, \ldots, \left\lfloor \frac{(x-1)n}{x} \right\rfloor \right\} \subseteq [2, n-1] \quad \text{and}
\]

\[
X'(x) = 1 + \left\{ \left\lfloor \frac{n}{x} \right\rfloor, \left\lfloor \frac{2n}{x} \right\rfloor, \ldots, \left\lfloor \frac{(x-1)n}{x} \right\rfloor \right\} \subseteq [2, n-1].
\]

Then
We now proceed with the proof of our main result.

1. \(|X(x)| = |X'(x)| = x - 1\).
2. Let \(d = \lceil \frac{n}{x} \rceil - 1\) and \(d' = \lfloor \frac{n}{x} \rfloor\). The difference between any two consecutive elements in \(\{0\} \cup X(x) \cup \{n\}\) is either \(d\) or \(d + 1\), and the difference between any two consecutive element in \(\{1\} \cup X'(x) \cup \{n + 1\}\) is either \(d'\) or \(d' + 1\).
3. The final element in \(X(x)\) is \(n - d'\), and the final element in \(X'(x)\) is \(n - d\).
4. \(\lceil \frac{ux}{n} \rceil \sum_{v=1}^{u} 1_{X(x)}(v) + \lceil \frac{ux}{n} \rceil - 1 = \sum_{v=1}^{u} 1_{X'(x)}(v)\) for \(u \in [1, n - 1]\).
5. \(X(x) \cup X'(n - x)\) is a disjoint partition of \([2, n - 1]\).
6. If, \(t\) times in a row, the consecutive difference of elements of \(X(x)\) is \(d\), then \(x > \frac{n}{d + 1/\ell}\). If, \(t\) times in a row, the consecutive difference of elements of \(X'(x)\) is \(d'\), then \(x > \frac{n}{d' + 1/\ell}\). If, \(t\) times in a row, the consecutive difference of elements of \(X'(x)\) is \(d' + 1\), then \(x < \frac{n}{d' + 1/\ell}\).

**Proof.**

1. Clear because \(\frac{(t+1)x}{n} - \frac{tn}{x} = \frac{n}{x} > 1\).
2. Indeed, for \(t \in \mathbb{Z}\), write \(\lceil \frac{tn}{x} \rceil = \frac{tn}{x} + \epsilon\) and \(\lfloor \frac{tn}{x} \rfloor = \frac{tn}{x} + \epsilon'\), where \(0 \leq \epsilon, \epsilon' < 1\). Then \(\lfloor \frac{tn}{x} \rfloor - \lceil \frac{tn}{x} \rceil = \frac{n}{x} + \epsilon' - \epsilon\) is an integer in the open segment \((\frac{n}{x} - 1, \frac{n}{x} + 1)\), so equal to \(d\) or \(d + 1\). A similar calculation shows \((1 + \frac{(t+1)n}{x}) - (1 + \lfloor \frac{tn}{x} \rfloor)\) is always \(d' + 1\) or \(d'\).
3. From the identity \(\lceil \alpha \rceil + \lfloor -\alpha \rfloor = 0\) for \(\alpha \in \mathbb{R}\), we find that \(1 + \lfloor \frac{(x-1)n}{x} \rfloor = 1 + n + \lfloor -\frac{n}{x} \rfloor = n - (\lfloor \frac{n}{x} \rfloor - 1)\) and \(\lceil \frac{(x-1)n}{x} \rceil = n + \lceil -\frac{n}{x} \rceil = n - \lfloor \frac{n}{x} \rfloor\).
4. For any \(u \in \mathbb{Z}\), we have \(\lceil \frac{ux}{n} \rceil\) equal to the integer \(t\) such that \(\frac{tn}{x} \leq u < \frac{(t+1)n}{x}\), which for any \(u \in [0, n - 1]\) is equal to the number of elements of \(X(x)\) that are at most \(u\). Likewise, for any \(u \in \mathbb{Z}\), we have \(\lfloor \frac{ux}{n} \rfloor - 1\) equal to the integer \(t\) such that \(\frac{tn}{x} < u \leq \frac{(t+1)n}{x}\), which for any \(u \in [1, n]\) is equal to the number of elements of \(X'(x)\) that are at most \(u\). The identities in Part 4 now readily follow.
5. For \(u \in [1, n - 1]\), we have, by Part 4,
\[
\sum_{v=1}^{u} 1_{X(x)}(v) + \sum_{v=1}^{u} 1_{X'(n-x)}(v) = \left\lceil \frac{ux}{n} \right\rceil + \left\lfloor \frac{u(n-x)}{n} \right\rfloor - 1 = u - 1,
\]
where the second equality follows from the identity \(\left\lceil -\frac{u}{x} \right\rceil + \left\lfloor \frac{u}{x} \right\rfloor = 0\). Taking the difference of the above equation for \(u\) and \(u - 1\), we find that \(1_{X(x)}(u) + 1_{X'(n-x)}(u) = 1\) for all \(u \in [2, n - 1]\), and the claim follows.
6. Let \(\lceil \frac{ux}{n} \rceil, \ldots, \lceil \frac{(t+1)n}{x} \rceil\) be \(t + 1\) consecutive elements of \(X(x)\) such that the \(t\) successive differences between these elements are each equal to \(d\). Then \(td = \lceil \frac{(y+1)n}{x} \rceil - \lceil \frac{yn}{x} \rceil > \frac{(y+1)n}{x} - \frac{yn}{x} - 1 = \frac{tn}{x} - 1\), which implies \(x > \frac{n}{d + 1/\ell}\). If, instead, each of the \(t\) consecutive differences is equal to \(d + 1\), then we obtain \(td + 1 = \lceil \frac{(y+1)n}{x} \rceil - \lceil \frac{yn}{x} \rceil < \frac{(y+1)n}{x} + 1 - \frac{yn}{x} = \frac{tn}{x} + 1\), which implies \(x < \frac{n}{d + 1/\ell}\). Similar arguments yield the analogous results for the set \(X'(x)\).

\(\square\)

3. The Proof of Theorem 2.3

We now proceed with the proof or our main result.
Proof of Theorem 2.3. The following makes use of the explanation above Conjecture 2.2. To prove Theorem 2.3, it suffices to consider a minimal zero-sum (modulo \(n\)) sequence \(S = (y_1, y_2, y_3, y_4)\), where \(y_i \in \mathbb{Z}\), and show that \(|S|_1 = n\). If \(n\) is divisible by two distinct primes, then our hypotheses ensure gcd\((y_i, n) = 1\) for all \(i\), and thus gcd\((y_1, y_2, y_3, y_4, n) = 1\). On the other hand, if \(n = p^a\) and \(p^7 = \text{gcd}(y_1, y_2, y_3, y_4, n)\), then we must have \(\gamma < \alpha\) as each \(y_i\) is non-zero modulo \(n\) (as \(S\) is a minimal zero-sum sequence). In this case, setting \(y'_i = p^{-\gamma} y_i\) for all \(i\), we find that gcd\((y'_1, y'_2, y'_3, y'_4, p^{\alpha - \gamma}) = 1\). If we knew the theorem held in this case, then we could find some \(u \in \mathbb{Z}\) with gcd\((u, p^{\alpha - \gamma}) = \text{gcd}(u, p^a) = 1\) such that \((uy'_1)^{p^{\alpha - \gamma}} + (uy'_2)^{p^{\alpha - \gamma}} + (uy'_3)^{p^{\alpha - \gamma}} + (uy'_4)^{p^{\alpha - \gamma}} = p^a\). But then, since \((uy_i)_n = p^7(uy'_i)^{p^{\alpha - \gamma}}\), the desired conclusion \((uy_i)_n + (uw_2)_n + (uw_2)_n + (uw_2)_n = p^a = n\) follows. Thus it suffices to prove the theorem when gcd\((y_1, y_2, y_3, y_4, n) = 1\), which we now assume.

For \(i \in [1, 4]\), let \(S_i\) be the length three subsequence of \(S\) obtained by removing the \(i\)-th coordinate. If \(|S_j|_1 \leq n\) for some \(j \in [1, 4]\), then \(|S|_1 = n\) follows, in turn implying \(|S_i|_1 < n\) for all \(i \in [1, 4]\). Thus it suffices to show \(|S_j|_1 \leq n\) for some \(j \in [1, 4]\). Since each \(S_i\) is zero-sum free, we have \(y_i \neq 0\) (mod \(n\)) for all \(i \in [1, 4]\). By hypothesis of Theorem 2.3, we either have gcd\((y_i, n) = 1\) for all \(i \in [1, 4]\) or that \(n = p^a\) is a prime power. In the latter case, gcd\((y_1, y_2, y_3, y_4, n) = 1\) ensures that some \(y_j\) has gcd\((y_j, n) = 1\), and we can re-index the \(y_i\) to w.l.o.g. assume \(y_j = y_4\) is relatively prime to \(n\). Of course, if there is more than one \(y_j\) with gcd\((y_j, n) = 1\), then we have multiple choices for which \(y_j\) should be re-indexed to become \(y_4\). For the moment, simply select one possible \(y_j\) (we will add a further restriction on which one to choose later). Since multiplying \(S\) by a number relatively prime to \(n\) does not change that \(S\) is a minimal zero-sum sequence, we can multiply each term of \(S\) by some number congruent to \(-y_4^{-1}\) modulo \(n\) and thereby assume \(y_4 = -1\) and

\[
y_1 + y_2 + y_3 \equiv -y_4 = 1 \pmod{n}.
\]

We may also assume each \(y_i \in [1, n - 1]\) for \(i \in [1, 3]\) and re-index the \(y_1, y_2, y_3 \in [1, n - 1]\) so that \(y_3 \leq y_2 \leq y_1\). Let \(\omega \in \{1, 2\}\) be the number of distinct prime divisors in \(n\).

Since gcd\((2, n) = 1\), we can multiply each term of \(S\) by \(2\) and re-index appropriately to result in a sequence \((z_1, z_2, z_3, z_4)\) with \(z_4 = -2\),

\[
z_1 + z_2 + z_3 \equiv -z_4 = 2 \pmod{n},
\]

\(z_i \in [1, n - 1]\) for \(i \in [1, 3]\), and \(z_3 \leq z_2 \leq z_1\). We will only use the \(z_i\) when

\[
\omega = 2, \quad \frac{n}{3} < y_2 < \frac{n}{2} < y_1 < \frac{2}{3}n \quad \text{and} \quad 4 \leq y_3 \leq \frac{n + 1}{6}, \tag{4}
\]

which allows us to assume

\[
\frac{2}{3}n < z_1 < n - 1 \quad \text{and} \quad z_2 \leq \frac{n + 1}{3}. \tag{5}
\]

Indeed, \(z_1 = (2y_2)_n = 2y_2\) is even, while \((2y_1)_n = 2y_1 - n\) is odd and \((2y_3)_n = 2y_3\) is even. Since either \(z_2 = (2y_1)_n\) and \(z_3 = (2y_3)_n\) or else \(z_3 = (2y_1)_n\) and \(z_2 = (2y_3)_n\), we conclude that

\[
z_1 \equiv 0 \pmod{2} \quad \text{and} \quad z_2 + z_3 \equiv 1 \pmod{2}. \tag{6}
\]

If Condition (4) holds, then gcd\((y_i, n) = 1\) for all \(i\) (in view of \(\omega = 2\) and the hypotheses of the theorem), meaning we have four choices for which \(y_j\) chosen above (in the initial normalization of \(S\)) will be the one re-indexed to equal \(y_4\). In such circumstances, assume we originally chose \(y_j\) so that either Condition (4) fails or else (4) holds no matter which \(y_j\) is re-indexed to equal \(y_4\) and, in such case, further assume \(y_j\) is chosen so that the resulting value of \(z_3\) is maximal.
As we will see in the proof, depending on the exact values of the terms of $S$, it will sometimes be easier to work with the normalized form for $S$ given by the $y_i$ and sometimes with the normalized form given by the $z_i$. Regardless, to prove the theorem holds for $S$, we need only prove it holds using either the $y_i$ or the $z_i$, whichever is more convenient. However, many arguments will need to work in both cases. Rather than repeating them for the $y_i$ and then for the $z_i$, we let $(x_1, x_2, x_3, x_4) \in \{(y_1, y_2, y_3, y_4), (z_1, z_2, z_3, z_4)\}$ be arbitrary and prove most arguments for the $x_i$, and thus for the $y_i$ and the $z_i$ at the same time. Note either $x_i = y_i$ for all $i$ or $x_i = z_i$ for all $i$. Let

$$x_1 + x_2 + x_3 \equiv \kappa \pmod{n}$$

with $\kappa \in \{1, 2\}$.

Note $\kappa = 2$ implies $\omega = 2$ and $x_i = z_i$ for all $i$, while $\kappa = 1$ implies $\omega \in \{1, 2\}$ and $x_i = y_i$ for all $i$.

We assume by contradiction that $||(x_1, x_2, x_3)|_1 > n$.

**Claim 1:** For every $u \in [1, n-1]$ with $\gcd(u, n) = 1$, we have

$$(uy_1)_n + (uy_2)_n + (uy_3)_n = n + u.$$ 

For every $u \in [1, n-1]$ with $\gcd(u, n) = 1$, we have

$$(uz_1)_n + (uz_2)_n + (uz_3)_n = n + 2u.$$ 

For every $u \in [\frac{n+1}{2}, n-1]$ with $\gcd(u, n) = 1$, we have

$$(uz_1)_n + (uz_2)_n + (uz_3)_n = 2u.$$ 

In particular, $x_1 + x_2 + x_3 = n + \kappa$.

**Proof.** We have $(ux_1)_n + (ux_2)_n + (ux_3)_n \equiv u(x_1 + x_2 + x_3) \equiv \kappa u \pmod{n}$ and, trivially, $3 \leq (ux_1)_n + (ux_2)_n + (ux_3)_n \leq 3(n-1)$. If $(ux_1)_n + (ux_2)_n + (ux_3)_n \leq n$, then the desired conclusion of the theorem follows, contrary to assumption. If $2n \leq (ux_1)_n + (ux_2)_n + (ux_3)_n \leq 3(n-1)$, then Equation (3) ensures that $-(ux_1)_n + (ux_2)_n + (ux_3)_n \leq n$, also as desired. Therefore $(ux_1)_n + (ux_2)_n + (ux_3)_n \in [n+1, 2n-1]$ is the unique integer congruent to $\kappa u$ modulo $n$, and the claim follows. Note the case $u = 1$ shows $x_1 + x_2 + x_3 = n + \kappa$. \hfill \Box

**Claim 2:** If $x_i = x_j$ with $i, j \in [1, 3]$ distinct, then $\gcd(x_i, n) \neq 1$.

**Proof.** Suppose $x_i = x_j = x$ with $\gcd(x, n) = 1$ for some distinct $i, j \in [1, 3]$. Then we can find some $u \in \mathbb{Z}$ congruent to $x^{-1}$ modulo $n$, in which case $(ux_1)_n + (ux_2)_n + (ux_3)_n \leq 1 + 1 + y$, where $y = (x_k)_n \in [1, n-1]$ and $\{i, j, k\} = [1, 3]$. However, since $(x_1, x_2, x_3)$, and thus also $(ux_2, ux_3, ux_4)$, is zero-sum free, we have $y \leq n - 3$, whence $(ux_1)_n + (ux_2)_n + (ux_3)_n \leq n - 1$, contrary to Claim 1. \hfill \Box

**Claim 3:** $2 \leq y_3 \leq y_2 \leq y_1 \leq n - 4$, $y_2 \geq 3$, $y_1 \geq 4$ and $n \geq 11$. Furthermore, if $\kappa = 2$, then $5 \leq z_3 \leq z_2 \leq z_1 \leq n - 11$, $z_2 \geq 8$ and $z_3 \neq 6$.

**Proof.** Since $(y_1, y_2, y_3)$ is zero-sum free (modulo $n$) with $y_i \in [1, n-1]$, Claim 1 ensures that $2 \leq y_3 \leq y_2 \leq y_1 \leq n - 3$. Moreover, since $\gcd(2, n) = 1$, we cannot have $y_3 = y_2 = 2$ (in view of Claim 2), so $y_2 \geq 3$ implying $y_1 = n + 1 - (y_3 + y_2) \leq n - 4$. Likewise, we cannot have $y_1 = y_2 = 3$, so $y_1 \geq 4$ and $n + 1 = y_1 + y_2 + y_3 \geq 4 + 3 + 2 = 9$, implying $n \geq 11$ in view of $\gcd(n, 6) = 1$. 


Next assume that $\kappa = 2$ but $z_3 \leq 4$ or $z_3 = 6$. From Condition (4), we have $8 \leq (2y_3)_n \leq \frac{n+1}{3}$ and $8 \leq \frac{2n+2}{3} \leq (2y_2)_n \leq n - 1$, so that we must have $z_2 \geq 8$ and $(2y_1)_n = z_3 \in [1, 4] \cup \{6\}$. Thus
\[
y_1 = \frac{n + z_3}{2} \quad \text{with} \quad z_3 \in \{1, 3\}, \quad \text{and} \quad y_2 = n + 1 - y_1 - y_3 = \frac{n + 2 - z_3 - 2y_3}{2}.
\]
Let $u \in \mathbb{Z}$ be an integer congruent to $-y_1^{-1}$ modulo $n$, say
\[
u = 2 \cdot \frac{an - 1}{z_3} = \frac{2an - 2}{z_3}
\]
for some $a \in [1, z_3]$ (recall that $\gcd(n, z_3) = 1$ in view of $\gcd(6, n) = 1$, so such an $a \in [1, z_3]$ can be chosen so that $u/2$ is an integer). Recall that $8 \leq 2y_3 \leq \frac{n+1}{3}$ by Condition (4). Now
\[
(uy_4)_n = \frac{a_4n + 2}{z_3}, \quad (uy_3)_n = \frac{a_3n - 2y_3}{z_3}, \quad \text{and} \quad (uy_2)_n = \frac{a_2n - 2 + z_3 + 2y_3}{z_3}
\]
for some integers $a_4, a_2 \in [0, z_3 - 1]$ and $a_3 \in [1, z_3]$. Claim 1 ensures that $(y_1)_{n} + (y_2)_{n} + (y_3)_{n} = n + 1$ when $y_1 \equiv -1 \mod n$. Thus, since $uy_1 \equiv -1 \mod n$, applying Claim 1 to $uy_2$, $uy_3$ and $uy_4$ yields $(uy_2)_n + (uy_3)_n + (uy_4)_n = n + 1$ as well. Hence $a_4 + a_2 + a_3 = z_3$. We aim to show that swapping $y_4$ for $y_1$ contradicts the extremal conditions imposed on $y_4$ from the beginning of the proof.

Suppose $z_3 = 1$. Then $a_4 = a_2 = 0$, $(uy_4)_n = 2 < \frac{n}{3}$ and $(uy_2)_n = 2y_3 - 1 \leq \frac{n-2}{3}$. Since Condition (4) ensures that precisely one $y_i$ is less than $\frac{n}{3}$, we see that (4) does not hold when swapping $y_4$ for $y_1$, contrary to our setup for $\kappa = 2$ (we only assume $\kappa = 2$ when every choice of which $y_j$ to re-index so that $y_j = y_4$ results in Condition (4) holding).

Suppose $z_3 = 3$. If $a_3 = 1$, then $\frac{n+1}{6} < \frac{2n-1}{9} \leq (uy_3)_n = \frac{n-2y_3}{3} < \frac{n}{3}$, and if $a_3 = 3$, then $(uy_3)_n = \frac{3n-2y_3}{3} \geq \frac{2}{3}n$, both ensuring that Condition (4) cannot hold when swapping $y_4$ for $y_1$, contrary to the setup of $\kappa = 2$. Therefore we must have $a_3 = 2$, whence $\frac{2}{3}n > (uy_3)_n = \frac{2n-2y_3}{3} \geq \frac{5n}{9}$, implying $\frac{n-2}{3} \geq (2uy_3)_n \geq \frac{n-2}{9} > 3 = z_3$ (as $\kappa = 2$ implies $\omega = 2$, forcing $n \geq 35$). We cannot have $a_4 = 0$, as $\frac{2}{3}$ is not an integer. Consequently, since $a_2 + 2 + a_4 = a_2 + a_3 + a_4 = z_3 = 3$, we conclude that $a_2 = 0$ and $a_4 = 1$. But now $(uy_4)_n = \frac{n+2}{3}$, implying $(2uy_4)_n = \frac{2n+4}{3} > 3 = z_3$, and $\frac{n+4}{9} \geq (uy_2)_n = \frac{2y_3+1}{3} \geq 3$, implying $(2uy_4)_n \geq 6 > 3 = z_3$. But this contradicts the choice of which $y_j$ was chosen to be re-indexed to equal $y_4$ (as either Condition (4) does not hold when swapping $y_4$ for $y_1$ or else the size of $z_3$ increases). This establishes that either $z_3 = 5$ or $z_3 \geq 7$. Since $z_2 \geq 8$ as seen earlier, it follows that $z_1 = n + 2 - z_2 - z_3 \leq n - 11$, and the claim is complete. 

\[
\square
\]

For $i \in [1, 3]$, let
\[
X_i = X(x_i), \quad d_i = \left\lceil \frac{n}{x_i} \right\rceil - 1, \quad x_i' = n - x_i = x_2 + x_3 - \kappa, \quad X_i' = X'(n - x_i) \quad \text{and} \quad d = \left\lceil \frac{n}{x_i'} \right\rceil,
\]
with $X(x_i)$ and $X'(n - x_i)$ as defined in Lemma 2.4. Since $x_i' = x_2 + x_3 - \kappa \geq x_2 + 1$ (by Claim 3), we have
\[
x_3 \leq x_2 < x_1'.
\]
By Lemma 2.4.5, \( X_1' = [2, n - 1] \setminus X_1 \). Let
\[
\Lambda(u) = 1_{X_1}(u) + 1_{X_2}(u) + 1_{X_3}(u)
\]
and
\[
\Lambda'(u) = \Lambda(u) - 1_{X_1}(u),
\]
where \( X_4 = \{\frac{n+1}{2}\} \) if \( \kappa = 2 \), and \( X_4 = \emptyset \) if \( \kappa = 1 \). Thus \( \Lambda'(u) = \Lambda(u) \) for \( u \in [1, n - 1] \setminus X_4 \) and \( \Lambda'(\frac{n+1}{2}) = \Lambda(\frac{n+1}{2}) - 1 \) when \( \kappa = 2 \). Now \( \frac{n+1}{2} \in X_4 \) precisely when \( x_i \) is even. Combined with Equation (6), we conclude that
\[
u \in X_4 \text{ implies } u \in X_1.
\]
(7)
For \( u \in [1, n - 1] \), consider
\[
(u x_1)_n + (u x_2)_n + (u x_3)_n = u x_1 - \left[\frac{u x_1}{n}\right] n + u x_2 - \left[\frac{u x_2}{n}\right] n + u x_3 - \left[\frac{u x_3}{n}\right] n
\]
\[
= \kappa u - \left(\left[\frac{u x_1}{n}\right] + \left[\frac{u x_2}{n}\right] + \left[\frac{u x_3}{n}\right]\right) + u n
\]
\[
= \kappa u + \left(u - \sum_{v=1}^{u} \Lambda'(v)\right)n,
\]
(8)
where the final equality follows by Lemma 2.4.4, the second from the equality \( x_1 + x_2 + x_3 = n + \kappa \) (from Claim 1), and the first from Equation (2). The above equality together with Claim 1 forces
\[
\sum_{v=1}^{u} \Lambda'(v) = u - 1 \text{ for } u \in [1, n - 1] \text{ with } \gcd(u, n) = 1.
\]
(9)
Moreover, since \( \kappa u \leq (u x_1)_n + (u x_2)_n + (u x_3)_n \leq 3n - 3 \) (if \( \kappa = 1 \) or else \( \kappa = 2 \) and \( u \leq \frac{n+1}{2} \)) and \( 2u - n \leq (u x_1)_n + (u x_2)_n + (u x_3)_n \leq 3n - 3 \) (if \( \kappa = 2 \) and \( u \geq \frac{n+1}{2} \)), we always have \( \sum_{v=1}^{u} \Lambda'(v) \in \{u - 2, u - 1, u\} \) in view of Equation (8). Let
\[
\delta(u) = \sum_{v=1}^{u} \Lambda'(v) - u + 1 \in \{-1, 0, 1\}.
\]
By Equation (9), \( \delta(u) = 0 \) whenever \( \gcd(u, n) = 1 \). Observe that
\[
\delta(u) - \delta(u - 1) = \Lambda'(u) - 1 \quad \text{for all } u \in [2, n - 1]
\]
and
\[
\delta(u) - \delta(u - 1) = \Lambda'(u) - 1 = \Lambda(u) - 1 \in \{2, 1, 0, -1\} \quad \text{for } u \in [1, n - 1] \setminus X_4,
\]
(10)
with the inclusion in view of the definition of \( \Lambda(u) \). On the other hand, if \( \kappa = 2 \), then
\[
\Lambda\left(\frac{n+1}{2}\right) - 2 = \Lambda\left(\frac{n+1}{2}\right) - 1 = \delta\left(\frac{n+1}{2}\right) - \delta\left(\frac{n-1}{2}\right) = 0 - 0 = 0
\]
as \( \frac{n+1}{2} \) and \( \frac{n-1}{2} \) are both relatively prime to \( n \). Thus \( \Lambda(\frac{n+1}{2}) = 2 \) when \( \kappa = 2 \). In particular,
\[
\Lambda(u) \geq 1 \quad \text{implies} \quad \Lambda'(u) \geq 1.
\]
(11)
More generally, if both \( u \) and \( u - 1 \) are relatively prime to \( n \), then Equation (9) implies \( \Lambda'(u) = 1 \).
Since \( n = p^\alpha q^\beta \) with \( p < q \) primes, this means
\[
\Lambda(u) = 1 \quad \text{for } u \in [2, p - 1] \cup [n - p + 2, n - 1].
\]
(12)
Since \( \gcd(2, n) = \gcd(n - 1, n) = 1 \), we find that \( \delta(2) = \delta(n - 1) = 0 \). As a useful observation, note
\[
\delta(u) \neq 0 \quad \text{implies} \quad \frac{n+1}{2} \notin [u - 1, u + 2],
\]
(13)
for \( \frac{n+1}{2} \in [u - 1, u + 2] \) forces \( \gcd(u, n) = 1 \).

**Claim 4:** \( 1 = d_1 < d_2 \leq d_3 \) and \( d \geq 2 \).

*Proof.* Since \( \min X_1 = d_1 + 1 \) with \( d_1 \leq d_2 \leq d_3 \) (in view of Claim 3), the case \( u = 2 \) in Equation (12) yields \( 1 = d_1 < d_2 \leq d_3 \), in turn implying \( 2 \leq x_3 \leq x_2 < \frac{d}{2} \leq x_1 \leq n - 4 \). Hence \( x_1' = n - x_1 < \frac{d}{2} \) and \( d = \left\lceil \frac{n}{x_1'} \right\rceil \geq 2 \), completing the claim. \( \square \)

**Claim 5:** If \( I \subseteq [1, n - 1] \) is an interval with \( |I| \geq \omega + 1 \), then \( \delta(u) = 0 \) for some \( u \in I \).

*Proof.* Since \( n \) has \( \omega \leq 2 \) distinct prime divisors, each at least 5 as \( \gcd(n, 6) = 1 \), there can be at most \( \omega \) consecutive numbers that are non-relatively prime to \( n \). The claim now follows since \( \delta(u) = 0 \) when \( \gcd(u, n) = 1 \). \( \square \)

**Claim 6:** Suppose \( \Lambda'(u) \geq 2 \) for some \( u \in [1, n - 1] \). Then \( \delta(u) \geq 0 \) and \( \Lambda(v) = 0 \) for some \( v \in I \) with \( |u - v| \leq \omega \). Indeed, if \( \Lambda(u + 1), \Lambda(u + \omega) \geq 1 \), then \( \delta(u) = 0 \) and \( \Lambda(u) = \Lambda'(u) = 2 \); and if \( \Lambda(u - 1), \Lambda(u - \omega) \geq 1 \), then \( \delta(u) = 1 \) and \( \Lambda(u) = \Lambda'(u) = 2 \).

*Proof.* Since \( \Lambda'(u) \geq 2 \), we have \( 5 \leq p \leq u \leq n - p + 1 \leq n - 4 \) by Equation (12). Moreover, \( \delta(u) = \delta(u - 1) + \Lambda'(u) - 1 > \delta(u - 1) \geq -1 \), meaning \( \delta(u) \geq 0 \) with equality only possible if \( \Lambda'(u) = 2 \). The numbers \( n - 3, n - 1, n + 1 \) and \( n + 3 \) are all relatively prime to \( n \) and hence have \( \delta \) value 0. Since \( \delta(u) - \delta(u - 1) = \Lambda'(u) - 1 \), this implies that \( \Lambda'(n - 1) = \Lambda'(n + 1) = \Lambda'(n + 3) = 1 \), whence we can assume \( u \notin [n - 2, n + 3] \) in view of the hypothesis \( \Lambda'(u) \geq 2 \). In particular, \( \Lambda(u) = \Lambda'(u) \).

Suppose \( \Lambda(u + 1), \Lambda(u + \omega) \geq 1 \). Then \( \delta(u) \leq \delta(u + 1) \leq \delta(u + \omega) \) (in view of \( \Lambda(u + 1) \geq 1 \), \( \Lambda(u + \omega) \geq 1 \) and Equation (11)), whence Claim 5 implies that \( \delta(u) \leq 0 \). However, as \( 0 \geq \delta(u) = \delta(u - 1) + \Lambda(u) - 1 \geq -2 + \Lambda(u) \geq 0 \), this is only possible if \( \delta(u) = 0 \) and \( \Lambda(u) = 2 \), as desired. Next, suppose \( \Lambda(u - 1), \Lambda(u - \omega) \geq 1 \). Then \( \delta(u - \omega - 1) \leq \delta(u - \omega) \leq \delta(u - 1) < \delta(u) \), with the final inequality in view of \( \Lambda'(u) \geq 2 \) and the prior inequalities in view of \( \Lambda(u - 1) \geq 1, \Lambda(u - \omega) \geq 1 \) and Equation (11). Combined with Claim 5, we conclude that \( \delta(u) = 1 \) and \( \delta(u - 1) = 0 \). Since \( 1 = \delta(u) = \delta(u - 1) + \Lambda(u) - 1 = \Lambda(u) - 1 \), we also conclude that \( \Lambda(u) = 2 \), as desired. Since \( \delta(u) \) cannot simultaneously be equal to 1 and 0, it now follows that \( \Lambda(v) = 0 \) for some \( v \in I \) with \( |u - v| \leq \omega \), completing the proof of the claim. \( \square \)

**Claim 7:** \( d \leq d_2 \).

*Proof.* Indeed, \( x_3 \leq x_2 < x_1' \) ensures \( d - 1 \leq d_1 \leq d_3 \) with \( d_2 = d - 1 \) only possible if \( x_2 \mid n \), which in view of the hypotheses of the theorem, ensures that \( \omega = 1 \). In such case, \( \kappa = 1 \) and the elements of \( \{0\} \cup X_2 \cup \{n\} \) will be in arithmetic progression with difference \( d = d_2 + 1 = 0 \pmod{p} \), so \( X_2 = \{d, 2d, \ldots, n - d\} \) and \( d \geq p \geq 5 \). By Lemma 2.4.2, the difference between consecutive elements of \( X_1' \) is either \( d \) or \( d + 1 \). If it is always \( d \), then the \( i \)-th element of \( X_1' \) will always be exactly one more than the \( i \)-th element of \( X_2 \), implying (by Lemma 2.4.1) that \( x_2 - 1 = |X_2| = |X_1'| = x_1' - 1 = x_2 + x_3 - 2 \), which contradicts that \( x_3 \geq 2 \). Therefore the difference of consecutive elements \( u, v \in X_1' \) must be equal to \( u - v = d + 1 \) for some \( u \in X_1' \setminus \{d + 1\} \). Consider the first such \( u \) for which this occurs. Then \( v = u - d - 1 \in X_1' \) is contained in the arithmetic progression \( d + 1, 2d + 1, 3d + 1, \ldots \), ensuring that \( u \equiv 2 \pmod{d} \). Thus, since \( X_2 = \{d, 2d, \ldots, n - d\} \), we have \( u - 2 \in X_2 \). As \( u \) and \( u - d - 1 \) are consecutive elements of \( X_1' = [2, n - 1] \setminus X_1 \), we also have \( [u - 5, u - 1] \subseteq [u - d, u - 1] \subseteq X_1 \). As a
result, since $u - 2 \in X_2$, we conclude that $\Lambda'(u - 2) = \Lambda(u - 2) \geq 2$ and $\Lambda(v) \geq 1$ for $v \in [u - 5, u - 1]$, contradicting Claim 6 in view of $\omega = 1$.

Let

$$d + 1 = a'_1 < a'_2 < \ldots < a'_{x'_{d+1}} = n + 1$$

be the elements of $X'_1 \cup \{n + 1\}$, let

$$d_2 + 1 = b_1 < b_2 < \ldots < b_{x_2-1} < n$$

be the elements of $X_2 \cup \{n\}$, and let

$$d_3 + 1 = c_1 < c_2 < \ldots < c_{x_3-1} < n$$

be the elements of $X_3 \cup \{n\}$. Since $X_1 = [2, n - 1] \setminus X'_1$ (by Lemma 2.4.5), the elements of $X_1$ are precisely those integers from $[2, n - 1]$ excluding the $a'_i$. For $j \in [1, x'_1 - 1]$, let

$$I_j = [a'_j, a'_{j+1}).$$

Since the difference of consecutive elements in $X'_1 \cup \{n + 1\}$ is either $d$ or $d + 1$ (by Lemmas 2.4.2 and 2.4.3), we have

$$|I_j| := d + \epsilon_j \in [d, d + 1]$$

for all $j$, where $\epsilon_j \in \{0, 1\}$. We call the interval $I_j$ short if $|I_j| = d$ and long if $|I_j| = d + 1$. Each element $x \in [a'_1, a'_n - 1] = [d + 1, n]$ can be written uniquely in the form

$$x = a'_\sigma(x) + \rho(x), \quad \text{where } \sigma(x) \in [1, x'_1 - 1] \quad \text{and} \quad \rho(x) \in [0, d + 1 + \epsilon_{\sigma(x)}].$$

To simplify notation some, set for every $i \in [1, x_2 - 1]$:

$$\varsigma(i) := \sigma(b_i),$$

$$\varepsilon_i := \epsilon_{\sigma(b_i)} \quad \text{and} \quad \varrho(i) := \rho(b_i).$$

**Claim 8:** $d_2 \leq d + 1$.

**Proof.** Suppose $d_2 \geq d + 2$. Then $n - 1 \geq \min(X_2 \cup X_3) = d_2 + 1 \geq d + 3$, ensuring $\Lambda(u) \leq 1$ for $u \leq d + 2$ (implying $[1, d + 2] \subseteq [1, n - 1] \setminus X_1$). Hence $0 = \delta(2) \geq \delta(3) \geq \ldots \geq \delta(d + 2)$. As a result, since $d + 1 = \min X'_1$ is the first element missing from $X_1 = [2, n - 1] \setminus X'_1$ (by Lemma 2.4), ensuring that $\Lambda(d + 1) = 0$, it follows that $\delta(d + 1) = \delta(d + 2) = -1$. In view of Claim 5, this forces $\omega = 2$. Furthermore, since $\delta(u) = 0$ for $\gcd(u, n) = 1$, we must in fact have either $p \mid d + 1$ and $q \mid d + 2$ or else $q \mid d + 1$ and $p \mid d + 2$, with $p$ and $q$ distinct primes both at least 5. A quick scan of the first few integers shows that this is only possible if $d \geq 9$. If $d_2 > d + 2$, then the above argument can be improved to show $\delta(d + 1) = \delta(d + 2) = \delta(d + 3) = -1$, contrary to Claim 5. Therefore we may assume $d_2 = d + 2$.

In view of $3 \leq x_2 < x'_1$ and Lemma 2.4.2, we have $|X'_1| = x'_1 - 1 \geq 3$ and $|X_2| = x_2 - 1 \geq 2$. Now $a'_1 = d + 1$, $a'_2 \in [2d + 1, 2d + 2]$ and $a'_3 \in [3d + 1, 3d + 3]$ while $b_1 = d_2 + 1 = d + 3$ and $b_2 \in [2d + 5, 2d + 6]$ (in view of Lemma 2.4.2). Note that $a'_1 < b_1 < a'_2 < b_2 < a'_3 < n$. Indeed, since $X_1 = [2, n - 1] \setminus X'_1$ (by Lemma 2.4.5), we have

$$\Lambda(b_2) \geq 2 \quad \text{and} \quad \Lambda(u) \geq 1 \quad \text{for } u \in [a'_2 + 1, a'_3 - 1]. \tag{14}$$
However, since $a'_2 \leq 2d + 2$ and $b_2 \geq 2d + 5$, we have at least 2 elements in $[a'_2 + 1, b_2 - 1]$, while since $b_2 \leq 2d + 6$, $a'_3 \geq 3d + 1$ and $d \geq 9$, we have at least 3 elements in $[b_2 + 1, a'_3 - 1]$, in which case Equation (14) contradicts Claim 6 unless $b_2 = \frac{n+1}{2}$ with $\kappa = 2$. However, in the latter case, $x_2 = z_2 \geq 5$ (by Claim 3), in which case $b_2 = \lceil \frac{2n}{x_2} \rceil \leq \lceil \frac{2n}{b} \rceil < \frac{n+1}{2} = b_2$, which is also a contradiction. \hfill $\Box$

Claim 9: $d_2 = d$.

Proof. In view of Claims 7 and 8, assume by contradiction that $d_2 = d + 1$.

In this case, since $a'_1 = d + 1 < d_2 + 1 = b_1 = \min(X_2 \cup X_3)$ is the first element missing from $X_1 = [2, n - 1] \setminus X'_1$ (all in view of Lemma 2.4 and $d_2 \leq d_3$), we have $\Lambda(d + 1) = 0$ and $\delta(d + 1) = -1$. Hence $d \equiv -1$ modulo some prime from $\{p, q\}$ (as $\delta(u) = 0$ when $\gcd(u, n) = 1$), implying $d \geq p - 1 \geq 4$.

Moreover, unless $d + p = 5$, then $d \geq 6$. Lemma 2.4.3 gives

$$b_{x_2-1} = \begin{cases} n - d = n - d - 1, & \text{if } x_2 \mid n \\ n - d - 1 = n - d - 2, & \text{if } x_2 \nmid n \end{cases} \quad \text{and} \quad a'_{x_1 - 1} = \begin{cases} n - d, & \text{if } x'_1 \mid n \\ n - d - 1, & \text{if } x'_1 \nmid n. \end{cases}$$

Note that $x_2 \mid n$ implies that $\omega = 1$ and $p \mid \frac{n}{x_2} = d_2 + 1 = d + 2$, while $x'_1 \mid n$ implies that $\omega = 1$ and $p \mid \frac{n}{x'_1} = d$, both contradicting that $d \equiv -1$ (mod $p$) for $\omega = 1$. Therefore we must have $x_2 \nmid n$, $x'_1 \nmid n$, $\zeta(x_2 - 1) = x'_1 - 2$ and $g(x_2 - 1) = d - 1 + \varepsilon_{x_2-1}$.

Since the difference of consecutive elements in $X_2$ is either $d_2 = d + 1$ or $d_2 + 1 = d + 2$ (by Lemma 2.4.2), we conclude that each $I_j$, for $j \in [1, x'_1 - 1]$, contains at most one element of $X_2$. Indeed, since $d + 2 \geq b_{i+1} - b_i \geq d + 1 \geq a'_{j+1} - a'_j = |I_j| \geq d \geq 2$ for all $i \in [1, x_2 - 2]$ and $j \in [1, x'_1 - 1]$, we deduce that

$$\zeta(i) + 1 \leq \zeta(i + 1) \leq \zeta(i) + 2. \quad (15)$$

Moreover, if $\zeta(i + 1) = \zeta(i) + 1$, then $g(i + 1) \in g(i) + \{0, 1, 2\}$ with $g(i + 1) = g(i) + 2$ only possible when $b_{i+1} - b_i = d_2 + 1 = d + 2$ with $I_{i+1}(i)$ short. On the other hand, if $\zeta(i + 1) = \zeta(i) + 2$, then $g(i) \in d - 1 + \varepsilon_i + \{0, -1\}$ and $g(i + 1) \leq 1$ with $g(i) = d - 2 + \varepsilon_i$ only possible if $I_{\zeta(i)+1}$ is short and $b_{i+1} = a'_{\zeta(i)+2} = b_i + d + 2$.

Let $Y \subseteq [1, x_2 - 1]$ be all those indices $j \in [1, x_2 - 1]$ such that $X_2 \cap I_{\zeta(j)+1} = \emptyset$. In view of $b_{x_2-1} < a'_{x_1-1}$, we have $x_2 - 1 \in Y$, and for $j \in [1, x_2 - 2]$, we have $j \in Y$ precisely when $\zeta(j + 1) = \zeta(j) + 2$. But now, in view of Inequality (15), $\zeta(x_2 - 1) = x'_1 - 2$, and $\zeta(1) = 1$ (as $b_1 = d + 2 \leq 2d + 1 \leq a'_2$), we see that $x_2 + x_3 - 1 - \kappa = n - x_1 - 1 = x'_1 - 1 = |X'_1| = |Y| + |X_2| = |Y| + x_2 - 1$, whence

$$|Y| = x_3 - \kappa \leq |X_3|. \quad (16)$$

In view of Claim 6, we have $\delta(b_i) = 0$ whenever $1 \leq g(i) \leq d - 3 + \varepsilon_i$, and $\delta(b_i) = 1$ whenever $g(i) \geq 3$ and $b_i \notin X_4$. In particular, we have

$$g(i) \notin [3, d - 3 + \varepsilon_i] \quad \text{for all } i \in [1, x_2 - 1] \text{ with } b_i \notin X_4. \quad (17)$$

Suppose $d \geq 7$. We recall that $g(i)$ can only increase by 0, 1 or 2. Thus, if $g(i_1) \leq 1$ and $g(i_2) \geq d - 2 + \varepsilon_j$ for some $i_1 < i_2$, then there must be some $k \in [i_1 + 1, i_2 - 1]$ with $g(k) \in [3, 4] \subseteq [3, d - 3 + \varepsilon_i]$. Such an event must occur at least once for every $j \in [1, x_2 - 2]$ with $\zeta(j + 1) = \zeta(j) + 2$ (for every $b_j$ with $\zeta(j + 1) = \zeta(j) + 2$, we have $g(j) \geq d - 2 + \varepsilon_j$ and $g(j + 1) \leq 1$ as remarked after Inequality (15)). Also, since $g(x_2 - 1) = d - 1 + \varepsilon_{x_2-1}$ as noted at the beginning of the claim, it must also happen once
more between \(\max(Y \setminus \{x_2 - 1\})\) and \(x_2 - 1\). Thus, in total, we have \(g(k) \in [3, 4] \subseteq [3, d - 3 + \varepsilon]\)

occurring at least \(|Y| = x_3 - \kappa \geq 2\kappa - 1\) times (by Claim 3). However, in view of Condition (17), it can only occur at most \(\kappa - 1\) times, yielding \(\kappa - 1 \geq 2\kappa - 1\), which contradicts that \(\kappa \geq 1\). So we may instead assume \(d \leq 6\). If \(d = 6\), then we can repeat these arguments. As before, for each element of \(Y\), the function \(g(i)\) must progress between the values 1 and \(d - 2 + \varepsilon_i\), thus passing across the nonempty interval \([3, d - 3 + \varepsilon]\) at least \(|Y| = x_3 - \kappa \geq 2\kappa - 1\) times. Each time it does so, we must either have \(g(j) = 3 \in [3, d - 3 + \varepsilon]\), which can only happen once if \(b_j \notin X_4\), or else \(g(j) = 2\) and \(g(j + 1) = 4\). As this must happen at least \(2\kappa - 1\) times, we conclude that there must be \(j \in [1, x_2 - 2]\) with \(\zeta(j) = 2\), \(g(j + 1) = 4 \geq d - 2 + \varepsilon_{j+1}\) and \(b_j, b_{j+1} \notin X_4\), which is only possible if \(\varepsilon_{j+1} = 0\) and \(b_j + 1 - b_j = d + 2 = 8\).

Thus Claim 6 ensures that \(1 = \delta(b_{j+1}) \leq \delta(b_{j+1} + 1)\) and \(\delta(b_j - 2) \leq \delta(b_j - 1) \leq \delta(b_j) - 1 = -1\). However, since \(\delta(u) = 0\) for \(\gcd(u, n) = 1\), it follows that the integers \(b_j - 2, b_j - 1, b_{j+1}\) and \(b_{j+1} + 1\) are all non-relatively prime to \(n\). Since \(n\) is divisible by at most two distinct primes \(p, q \geq 5\), this is only possible if either \(b_{j+1} - (b_j - 1) = 9\) is divisible by one of the primes from \(\{p, q\}\) and \((b_{j+1} + 1) - (b_j - 2) = 11\) is divisible by the other or else \(b_{j+1} - (b_j - 2) = (b_{j+1} + 1) - (b_j - 1) = 10\) is divisible by both \(p\) and \(q\), all of which are impossible in view of \(p, q \geq 5\). It remains to handle the case when \(d < 6\). However, as remarked at the beginning of the proof of Claim 9, this is only possible if \(p = 5\), \(d = 4\) and \(d_2 = d + 1 = 5\).

This remaining case is one of the more difficult ones in the proof. We proceed with a series of subclaims that will eventually lead to a contradiction.

**Subclaim 9.1:** \(\delta(b_{y+1}) = 0\) for every \(y \in Y \setminus \{x_2 - 1\}\). Furthermore, if \(y \in Y \setminus \{x_2 - 1\}\) with \(\delta(b_y) = 0\), then \(\omega = 2\) and there is precisely one element \(v \in X_3 \cap [b_y, b_{y+1}]\), and this element satisfies \(v \in [b_y + 2, b_y + 4] \subseteq (b_y, b_{y+1}]\). Moreover, if \(\delta(b_0) = 0\) and \(b_0 \notin X_4\), then \(v = a'_{\varsigma(y)+1} = b_y + 2\) with \(v\) either congruent to 3 or 4 modulo \(q\).

**Proof.** Let \(y \in Y \setminus \{x_2 - 1\}\) be arbitrary. Then \(\varsigma(y + 1) = \varsigma(y) + 2\) follows (as noted after the definition of \(Y\)) implying \(g(y) \in d - 1 + \varepsilon_y + \{0, -1\} = 3 + \varepsilon_y + \{0, -1\}\) with \(g(y) = 2 + \varepsilon_y\) only possible if \(I_{\varsigma(y)+1}\) is short and \(b_{y+1} = a'_{\varsigma(y)+2} = b_y + 6\) (all noted after Inequality (15)).

First suppose \(b_y \in X_4\). Then \(\omega = 2, b_y = n/2, \Lambda(b_y) = 2, \) and \(\delta(b_y) = 0\). Since \(g(y) \geq 2 + \varepsilon_y > 0\), we have \(\frac{n+1}{2} = b_y \notin X'_1\), which implies that \(x'_1\) is odd. Thus \(a'_{\varsigma(y)+1} = \lfloor \frac{\left(\frac{n+1}{2}\right)I_{\varsigma(y)+1}}{\varsigma(y)} \rfloor + 1 = \lfloor \frac{\left(\frac{n+1}{2}\right)n}{2\varsigma(y)} \rfloor + 1\).

Since \(4 = d = \left\lceil \frac{n}{\varsigma(y)} \right\rceil\), we have \(\frac{n}{\varsigma(y)} < x'_1 < \frac{n}{2}\), which implies that \(a'_{\varsigma(y)+1} - \frac{n+1}{2} > 1\). Consequently, since \(g(y) \in d - 1 + \varepsilon_y + \{0, -1\}\), we conclude that \(g(y) = d - 2 + \varepsilon_y = 2 + \varepsilon_y\), which (as noted above) implies \(I_{\varsigma(y)+1}\) is short and \(b_{y+1} = a'_{\varsigma(y)+2} = b_y + 6\). Observing that \(b_y + 4 = \frac{n+1}{2}\) is relatively prime to \(n\), we must have \(\delta(b_y + 4) = 0\), which is only possible if there is some \(v \in X_3 \cap [b_y, b_y + 4]\). We cannot have \(v = b_y = \frac{n+1}{2}\) as that would imply \(\Lambda(\frac{n+1}{2}) = 3 \neq 2\). We cannot have \(v = b_y + 1\), as that would imply \(\delta(b_y + 1) = \delta(b_y) + 1 = 1\), contradicting that \(\delta(\frac{n+1}{2}) = 0\) in view of \(\gcd(\frac{n+1}{2}, n) = 1\). Thus \(v \in [b_y + 2, b_y + 4]\). Since the difference between consecutive elements of \(X_3\) is either \(d_3\) or \(d_3 + 1\) with \(d_3 \geq d_2 = 5\), it follows that \(v\) is the unique element from \(X_3\) in \([b_y, b_y + 1] = [b_y, b_y + 6]\). Hence

\[
\sum_{i=b_y+1}^{b_y+1} (\Lambda'(i) - 1) = 0,
\]

implying \(\delta(b_{y+1}) = \delta(b_y) = 0\), as desired.
Next suppose $\delta(b_y) = 0$ but $b_y \notin X_4$. Then we must have $g(b_y) \leq 2$ by Claim 6. As noted earlier, $g(y) \geq 2 + \varepsilon_y$, whence $g(y) = 2 + \varepsilon_y = 2$, implying that $I_{(y)}$ is short. Moreover, the equality conditions described above ensure that $I_{(y) + 1}$ is short and $b_y + 1 = \alpha_{(y) + 2} = b_y + 6$. Now $\delta(b_y - 2) \leq \delta(b_y - 1) < \delta(b_y) = 0$ in view of $\Lambda'(b_y) = \Lambda(b_y) \geq 2$ and $\Lambda(b_y - 1) \geq 1$ (both of which follow from $g(y) \geq 2$) and Equation (11). It follows that both $b_y - 1$ and $b_y - 2$ are not relatively prime to $n$, and thus one of them is divisible by $p$ and the other by $q$ with $\omega = 2$. Since $p, q \geq 5$, this ensures that $\delta(v) = 0$ for $v \in \{b_y, b_y + 1, b_y + 2\}$. In particular, since $b_y + 2 = \alpha'(y)$ and $\delta(b_y) = 0$, we must have $v := \alpha'(y) + 1 = b_y + 2 \in X_3$. Since $q$ divides either $b_y - 1$ or $b_y - 2$ with $p$ dividing the other, it follows that $v = b_y + 2$ is either congruent to 3 (mod $q$) and 4 (mod $p$), or else congruent to 4 (mod $p$) and 3 (mod $q$). Now $d_3 \geq d_2 = d + 1 = 5$ from Claim 4, meaning any element prior to $v$ in $X_3$ must come strictly before $v - 4 = b_y - 2$ or strictly after $v + 4 = b_y + 6 = \alpha'(y) + 2 = b_y + 1$. It follows that $\Lambda(i) = 1$ for each $i \in \{b_y + 1, b_y + 2\}$. Consequently, $[b_y + 1, b_y + 1] \subseteq [1, n - 1 \setminus X_4$ (as $\Lambda(\frac{n + 1}{2}) = 2$ when $\kappa = 2$) and thus $\sum_{i = b_y + 1}^{b_y + 1} \Lambda(i - 1) = \sum_{i = b_y + 1}^{b_y + 1} (\Lambda(i) - 1) - 0$, implying that $\delta(b_y + 1) = \delta(y) + \sum_{i = b_y + 1}^{b_y + 1} (\Lambda(i) - 1) = \delta(y) = 0$, as desired. So we may now assume $\delta(b_y) \neq 0$.

Observe that $g(y) \geq 2 + \varepsilon_y \geq 2$ ensures that $\Lambda'(b_y) = \Lambda(b_y) \geq 2$ (the first equality holds as $\delta(b_y) \neq 0 = \delta(\frac{n + 1}{2})$) so that $-1 \leq \delta(b_y - 1) < \delta(b_y)$, showing that $\delta(b_y) = -1$ is not possible. Thus we may assume $\delta(b_y) = 1$. Since $y \in Y$ with $y < x_2 - 1$, we have $\varsigma(y + 1) = \varsigma(y) + 2$, which implies that $\sum_{i = b_y + 1}^{b_y + 1} \Lambda(i - 1) = -2$. Thus, $1_{X_2}(b_y + 1) = 1$, we have $\sum_{i = b_y + 1}^{b_y + 1} \Lambda(i - 1) \geq 1$ with equality possible only if $X_3 \cap [b_y + 1, b_y + 1] = \emptyset$. Consequently, since $\delta(b_y + 1) = \delta(b_y) + \sum_{i = b_y + 1}^{b_y + 1} (\Lambda(i) - 1) = 1 + \sum_{i = b_y + 1}^{b_y + 1} (\Lambda(i) - 1) = 1 + \sum_{i = b_y + 1}^{b_y + 1} (\Lambda'(i) - 1) = 1 + \sum_{i = b_y + 1}^{b_y + 1} (\Lambda'(i) - 1)$, we see that $\delta(b_y + 1) = -1$ is only possible if $X_4 \cap [b_y + 1, b_y + 1] = \emptyset$ but $X_3 \cap [b_y + 1, b_y + 1] = \emptyset$. However, in such a case, we have $\Lambda(i) \leq 1$ for all $i \in [b_y + 1, b_y + 1] - 1$ and $\delta(b_y + 1) = -1$, which implies to the contrary that $X_4 \cap [b_y + 1, b_y + 1] = \emptyset$ (as $\Lambda(\frac{n + 1}{2}) = 2$ and $\delta(\frac{n + 1}{2}) = 0$ when $\kappa = 2$). Therefore we conclude that $\delta(b_y + 1) \geq 0$. As a result, if the claim fails, then $\delta(b_y + 1) = 1$. Since $\varsigma(y + 1) = \varsigma(y) + 2$, we must have $g(y + 1) \leq 1$ as noted after Inequality (15). Since $|I_{(y + 1)}| - 2 \geq d - 2 = 2$, it follows that $\Lambda(b_y + 1), \Lambda(b_y + 1 + 2) \geq 1$, ensuring that $1 = \delta(b_y + 1) \leq \delta(b_y + 1 + 1) \leq \delta(b_y + 1 + 2)$, contrary to Claim 5, which completes Subclaim 9.1. ☐

Subclaim 9.2: If $\delta(b_y) = 0$ and $\delta(b_y + 1) \neq 0$, for some $y \in [1, x_2 - 2]$, then $\omega = 2$, $\delta(b_y + 1) = 1$, and there is some $v \in X_3 \cap [b_y, b_y + 1]$ with $v$ congruent to an element from $\{3, 4, -3, -2\}$ mod $q$.

Proof. Since $\delta(b_y + 1) \neq 0$, Subclaim 9.1 ensures that $y \notin Y \setminus \{x_2 - 1\}$. Thus, since $y < x_2 - 1$, we have $y \notin Y$ and $\varsigma(y + 1) = \varsigma(y) + 1$ per definition of $Y$. Consequently, $\sum_{i = b_y + 1}^{b_y + 1} 1_{X_2}(i - 1) = -1$ while $\sum_{i = b_y + 1}^{b_y + 1} 1_{X_2}(i - 1) = 1$ by definition of the $b_i$. Thus $\delta(b_y + 1) = \delta(b_y) + \sum_{i = b_y + 1}^{b_y + 1} (\Lambda(i - 1) \geq \delta(b_y) = 0$ follows by the same reasoning used at the end of Subclaim 9.1. Hence the hypothesis $\delta(b_y + 1) \neq 0$ forces $\delta(b_y + 1) = 1$. This means either $X_3 \cap [b_y + 1, b_y + 1] \cap X_4 = \emptyset$.

Let us first handle the second case. As the difference between consecutive elements in $X_3$ is either $d_3$ or $d_3 + 1$ with $d_3 \geq d_2 = 5$ and $b_y + 1 - b_y \in \{d_2, d_2 + 1\} = \{5, 6\}$, we see that the only way $X_3 \cap [b_y + 1, b_y + 1]$ can contain two elements is if $b_y + 1 = b_y + 6$, with $b_y + 1, b_y + 1 \in X_3$. Now $\delta(b_y + 1) = 1$ and $\Lambda(u) \leq 1$ for $u \in [b_y + 2, b_y + 1 - 1]$. As a result, since $[b_y + 1, b_y + 1] \cap X_4 \neq \emptyset$, we conclude that $b_y + 1 = \frac{w + 1}{2}$, whence
$b_y - 1$ is relatively prime to $n$, implying $\delta(b_y - 1) = 0$. As $\delta(b_y) = 0$, this forces $\Lambda(b_y) = \Lambda'(b_y) = 1$, whence $\varrho(y) = 0$ and $b_y = a'_y$. Thus $b_y + 4$ or $b_y + 5$ must equal $a'_{y+1}$. In either case, we have $b_{y+1} = b_y + 6 \in X_1$, whence $\Lambda(b_{y+1}) = 3$. But this forces $\delta(b_y + 5) = \delta(b_{y+1} - 1) = -1$, contradicting that $\delta(\frac{n + 9}{2}) = 0$ must hold in view of $\gcd(\frac{n + 9}{2}, n) = 1$. So we see that the second case cannot hold and instead assume the first case does.

It remains to determine the possible locations of $v$ and the corresponding values modulo $q$ (and show that $\omega = 2$), for which we will freely use the assumption that $[b_y + 1, b_y + 1] \subseteq [2, n - 1] \setminus X_4$ and (13). Also recall that $p = 5$. Since $\delta(b_{y+1}) = 1$, Claims 5 and 6 ensure that $\varrho(y + 1) \geq 2$ with equality only possible when $I_{\varrho(y)+1}$ is short. If $b_y \notin X_4$ (which we will soon establish), then $\delta(b_y) = 0$ and Claim 6 ensure that $\varrho(y) \leq 2$.

Suppose $b_y \in X_4$. Then Equation (7) ensures that $\varrho(b_y) \geq 1$. Thus $b_y \in X_1 \cap X_2$, ensuring that $\frac{n + 1}{2} = b_y \notin X_3$ (as $\Lambda(\frac{n + 1}{2}) = 2$ when $\kappa = 2$), whence $x_3$ is odd. If $X_3 \cap [\frac{n + 3}{2}, \frac{n + 5}{2}]$ is nonempty, then $\frac{n + 5}{2} \geq \left[ \frac{x_3 + 1}{x_3} \right] \geq \frac{(x_3 + 1)n}{x_3}$, implying $\frac{n}{x_3} \leq 5$, so that $5 = d_2 \leq d_3 = \left[ \frac{n}{x_3} \right] - 1 \leq 4$, which is not possible. Therefore $X_3 \cap [\frac{n + 3}{2}, \frac{n + 5}{2}] = \emptyset$, implying $v \geq b_y + 3$. Now $\delta(b_{y+1}) = 1$ with $b_{y+1} = b_y + 5 = \frac{n + 11}{2}$ or $b_{y+1} = b_y + 6 = \frac{n + 13}{2}$, forcing $q \mid b_{y+1}$ with $q \in \{11, 13\}$. In particular, all elements of $[b_y + 1, b_{y+1} - 1]$ are relatively prime to $n$ except for $b_y + 2 = \frac{n + 5}{2}$, and thus have $\delta$ value $0$. Quickly scanning all possible cases (depending on the value of $\varrho(y) \geq 1$ and whether $I_{\varrho(y)}$ is short or long), we see this is only possible if $v \in [b_y + 1, b_y + 3]$ or else $v = b_y + 4$ with $\varrho(y) = 1$ and $I_{\varrho(y)}$ long in this latter case, we have $\varrho(y + 1) \leq 2$, whence $\varrho(y + 1) = 2$ with $I_{\varrho(y)+1}$ short (see the previous paragraph). In this case, $b_{y+1} = b_y + 6$ as noted above. If $\varrho(y + 1) = 1$, $I_{\varrho(y)}$ is long, and $\varrho(y + 1) = 2$ with $q \mid b_{y+1}$, ensuring that $v = b_y + 4$ is congruent to $-2$ modulo $q$, as desired. In the former case, since we already established that $v \geq b_y + 3$, we conclude that $v = b_y + 3$. Then, since $q \mid b_{y+1}$ with $b_{y+1} = b_y + 5$ or $b_y + 6$, we find $v$ is congruent to $-2$ or $-3$ modulo $q$, also as desired. So we now assume $b_y \notin X_4$, and thus $\varrho(y) \leq 2$ as noted above.

Suppose $\varrho(y + 1) = 2$. Then $I_{\varrho(y)+1}$ is short (as noted above) with $1 = \delta(b_{y+1}) \leq \delta(b_{y+1} + 1)$. In consequence, since $\delta(u) = 0$ when $\gcd(u, n) = 1$, it follows that $\omega = 2$ and either $p$ divides $b_{y+1}$ and $q$ divides $b_{y+1} + 1$ or else $q$ divides $b_{y+1}$ and $p$ divides $b_{y+1} + 1$. In either case, the elements $b_{y+1} - 1$, $b_{y+1} - 2$ and $b_{y+1} - 3$ must all be relatively prime to $n$ (in view of $q \geq p = 5$), whence $\delta(u) = 0$ for each $u \in [b_{y+1} - 3, b_{y+1} - 1]$. Now $\delta(b_{y+1} - 3) = \delta(b_{y+1} - 2) = 0$ forces $\Lambda(b_{y+1} - 2) \geq 1$. Hence, since $b_{y+1} - 2 = a'_{\varrho(y)+1} \notin X_1$ and $b_{y+1} - 2 \notin X_2$ (as the difference of consecutive elements in $X_2$ is at least $d_2 = 5$), we conclude that $v = b_{y+1} - 2 \in X_3$. Since either $b_{y+1} \mid b_{y+1} + 1$ is congruent to $0$ modulo $q$, it follows that $v$ is congruent to either $-2$ or $-3$ modulo $q$, as desired. So we may now assume $\varrho(y + 1) \geq 3$ instead (we noted $\varrho(y + 1) \geq 2$ above). Since $\varrho(y + 1) \in \varrho(y) + \{0, 1, 2\}$, this ensures that $\varrho(y) \in [1, 2]$ (as we already noted $\varrho(y) \leq 2$ earlier in the subclaim).

Suppose $\varrho(y) = 1$. Then $b_{y+1} - b_y = d + 2 = 6$, for otherwise $b_{y+1} - b_y = d + 1$ would ensure that $\varrho(y + 1) \leq \varrho(y) + 1 \leq 2$, contrary to our current assumption. Thus either $\varrho(y + 1) = \varrho(y) + 2 = 3$ with $I_{\varrho(y)}$ short or else $\varrho(y + 1) = \varrho(y) + 1 = 2$ with $I_{\varrho(y)}$ long. Since $\varrho(y + 1) \geq 3$, the latter is not possible, whence we assume $\varrho(y + 1) = 3$ with $I_{\varrho(y)}$ short. Since $\varrho(y) = 1$ and $b_y \notin X_4$, we have $\Lambda'(b_y) = \Lambda(b_y) \geq 2$, implying $\delta(b_y - 1) < \delta(b_y) = 0$. Since $\delta(b_y - 1) = -1 \neq 0$ and $\delta(b_{y+1}) = 1 \neq 0$, it follows that both $b_y - 1$ and $b_{y+1}$ are not relatively prime to $n$. Hence, as $p = 5$ and $b_{y+1} - (b_y - 1) = 7$, it follows that either $b_{y+1}$ or $b_y - 1$ is congruent to $0$ modulo $q$ with $\omega = 2$. Moreover, as $q \geq 7$, there can be no element in $[b_y, b_{y+1} - 1] = [a'_{\varrho(y)+1} - 3, a'_{\varrho(y)+1} + 2]$ congruent to $0$ modulo $q$ (note that the equality
of intervals follows from $I_{x(y)}$ being short with $\varrho(y + 1) = 3$ and $\varrho(y) = 1$. If $v = b_y + 1 = a'_{c(y)+1} - 2$, then $\delta(b_y + 1) = \delta(b_y + 2) = 1$, in which case both $b_y + 1$ and $b_y + 2$ must be non-relatively prime to $n$, which is not possible as neither is congruent to 0 modulo $q$. If $v \geq b_{y+1} - 1 = a'_{c(y)+1} + 2$, then $\delta(a'_{c(y)+1} + 1) = \delta(a'_{c(y)+1}) = -1$, in which case both $a'_{c(y)+1} + 1$ and $a'_{c(y)+1}$ must be non-relatively prime to $n$, contradicting that neither of them is 0 modulo $q$. Therefore we conclude that $v \in [b_y + 2, b_y + 4] = [b_{y+1} - 4, b_{y+1} - 2]$.

Recall that $q$ must divide either $b_{y+1}$ or $b_y - 1$. If $q$ divides $b_{y+1}$, then $v$ will be congruent to $-2$, $-3$ or $-4$ modulo $q$ with $-4$ only possible if $v = b_{y+1} - 4 = a'_{c(y+1)} - 1$. Note that $-4 \equiv 3 \pmod{7}$, so this gives the desired conclusion unless $q > 7$, in which case $p = 5$ must divide $b_y - 1$ (as both $b_{y+1}$ are $b_y - 1$ and non-relatively prime to $n$ with their difference being 7). However, in this case $\delta(v) = \delta(b_y + 2) = 1$, forcing $b_y + 2$ to also be non-relatively prime to $n$. It cannot be 0 modulo $q$ as noted above and is congruent to 3 modulo 5 (as 5 divides $b_y - 1$), so this is a contradiction. On the other hand, if $q$ instead divides $b_y - 1$, then $v$ will be congruent to 3, 4 or 5 modulo $q$ with 5 only possible if $v = b_{y+1} - 2$. Note that $5 \equiv -2 \pmod{7}$, so this gives the desired conclusion unless $q > 7$, in which case $p = 5$ must divide $b_{y+1}$ (as both $b_{y+1}$ are $b_y - 1$ and non-relatively prime to $n$ with their difference being 7). However, in this case $\delta(v - 1) = \delta(b_{y+1} - 3) = -1$, forcing $b_{y+1} - 3$ to also be non-relatively prime to $n$. It cannot be 0 modulo $q$ as noted above and is congruent to $-3$ modulo 5 (as 5 divides $b_{y+1}$), so this is a contradiction. It remains to handle the case when $\varrho(y) = 2$.

Suppose $\varrho(y) = 2$. Since $\varrho(y) = 2$ and $b_y \notin X_4$, we have $\Lambda'(b_y) = \Lambda(b_y) \geq 2$ and $\Lambda(b_y - 1) \geq 1$, whence $\delta(b_y - 2) \leq \delta(b_y - 1) < \delta(b_y) = 0$. Thus both $b_y - 2$ and $b_y - 1$ must be non-relatively prime to $n$, forcing $\omega = 2$ with $p = 5$ dividing one of them and $q$ dividing the other.

If $I_{x(y)}$ is long, then $\varrho(y) = 2$ and $\varrho(y + 1) \geq 3$ force $b_{y+1} - b_y = d_2 + 1 = d + 2 = 6$. Since $\delta(b_{y+1}) = 1$, we have $b_{y+1}$ non-relatively prime to $n$. Since $b_y - 2$ and $b_y - 1$ are also non-relatively prime, it follows that either both $b_{y+1}$ and $b_y - 2$ are congruent to 0 modulo $p = 5$ or $q \geq 7$, which in view of $b_{y+1} - (b_y - 2) = 8$ is not possible, or else $b_{y+1}$ and $b_y - 1$ are both 0 modulo $p = 5$ or $q \geq 7$, which in view of $b_{y+1} - (b_y - 1) = 7$ is only possible if they are both congruent to 0 modulo $q = 7$. In this case, $p = 5$ must then divide $b_y - 2$, resulting in $b_y + 3 = a'_{c(y)+1}$ being the only element in $[b_y, b_{y+1} - 1]$ non-relatively prime to $n$. Thus $\delta(u) = 0$ for all $u \in [b_y, b_{y+1} - 1] \setminus \{a'_{c(y)+1}\}$. If $v > a'_{c(y)+1} + 1$, then $\delta(a'_{c(y)+1} + 1) = -1$, and if $v < a'_{c(y)+1}$, then $\delta(a'_{c(y)+1} - 1) = 1$ (recall that $v \geq b_y + 1$). Both cases contradict what we just showed, so we instead conclude that $v \in [a'_{c(y)+1}, a'_{c(y)+1} + 1] = [b_y + 3, b_y + 4]$. But now, since $b_y - 1 \equiv 0 \pmod{q}$ with $q = 7$, it follows that $v$ is either congruent to 0 or 5 modulo $q = 7$, as desired.

If $I_{x(y)}$ is short, then, since $q \geq p = 5$ with one of $\{p, q\}$ dividing $b_y - 2$ and the other dividing $b_y - 1$, it follows that the elements $b_y$, $b_y + 1$, $b_y + 2 = a'_{c(y)+1}$ are all relatively prime to $n$ (the equality follows in view of $\varrho(y) = 2$ with $I_{x(y)}$ short). If $v > a'_{c(y)+1}$, then $\delta(a'_{c(y)+1}) = -1$ will follow, forcing $a'_{c(y)+1}$ to be non-relatively prime to $n$, contrary to what we just noted. Therefore $v \in [b_y + 1, a'_{c(y)+1}] = [b_y + 1, b_y + 2]$. If $v = b_y + 1$, then $\delta(v) = \delta(b_y + 1) = 1$ follows, forcing $b_y + 1$ to be non-relatively prime to $n$, contrary to what we just noted. Therefore $v = b_y + 2$. But now, since either $b_y - 2$ or $b_y - 1$ is congruent to 0 modulo $q$, it follows that $v$ is congruent to either 3 or 4 modulo $q$, as desired. □
Subclaim 9.3: \( \omega = 2 \) and there are at most two elements of \( X_3 \) not congruent to some number from \( \{3, 4, -3, -2\} \) modulo \( q \geq 7 \). Moreover, if there is at least one such element, then \( \kappa = 2 \), and if there are two such elements of \( X_3 \), then one of them must lie in the interval \( \left[ \frac{n+3}{2}, \frac{n+9}{2} \right] \).

Proof. From Equation (16), we know \( |Y| = x_3 - \kappa \in \{ |X_3|, |X_3| - 1 \} \). Set \( Y' = \{ y \} \cup \{ x_2 - 1 \} \) and observe that \( |Y'| = |Y| \) (as \( x_2 - 1 \in Y \)). Let \( y_1 < \ldots < y_\ell = x_2 - 1 \) be the elements of \( Y \) and let \( 1 = y'_1 < \ldots < y'_\ell \) be the elements of \( Y' \), where \( \ell = |Y'| \). Then the nonempty intervals \( J_\nu = [y'_\nu, y_\nu] \), for \( \nu = 1, \ldots, \ell \), give a disjoint partition of \([1, x_2 - 1] \).

Let \( \nu \in [1, \ell] \) be arbitrary. If \( y_\nu \in X_4 \) with \( \delta(y_\nu) = 0 \), then \( b_\nu = \frac{n-1}{2} \) and Subclaim 9.1 implies that there is some \( v \in X_3 \) with \( v \in \left[ \frac{n-1}{2}, \frac{n+1}{2} \right] = [b_\nu + 2, b_\nu + 4] \subseteq (b_\nu, b_\nu + 1) \). If this is not the case, then we will instead show that there exists some \( j \in J_\nu \) with \( x_2 - 1 = j \) and some \( v \in X_3 \cap (b_j, b_{j+1}) \) such that \( v \) is congruent to some number from \( \{3, 4, -3, -2\} \) modulo \( q \geq 7 \). This will then show that there are at least \( |Y| - 1 \) distinct elements of \( X_3 \) satisfying the conclusion of Subclaim 9.3 (indeed, \( |Y| \) such elements with \( \kappa = 1 \), with equality only possible if there is an additional \( v \in X_3 \cap \left[ \frac{n+3}{2}, \frac{n+9}{2} \right] \). Since \( |Y'| = x_3 - \kappa \in \{ |X_3|, |X_3| - 1 \} \), this will mean that all but at most two elements of \( X_3 \) satisfy the desired congruence conditions (and that all elements of \( X_3 \) satisfy the desired congruence conditions when \( \kappa = 1 \)), and the rest of the subclaim will quickly follow (that \( \omega = 2 \) will also be shown below).

By Subclaim 9.1, we have \( \delta(y_\nu) = 0 \) for all \( y' \in Y' \) with \( y' > 1 \), while \( \delta(b_\nu) = \delta(d_\nu + 1) = \delta(6) = 0 \) since \( \gcd(6, n) = 1 \). Note \( b_{x_2 - 1} = n - d - 1 = n - 5 \neq \frac{n+1}{2} \) as \( p = 5 \). Thus, since \( g(x_2 - 1) = d - 1 + \varepsilon_{x_2 - 1} \geq 3 \) (as noted at the start of the claim), it follows from Claim 6 (as remarked above Condition (17)) that \( \delta(b_{x_2 - 1}) = 1 \).

If \( \delta(b_i) = 0 \) for all \( i \in J_\nu = [y'_\nu, y_\nu] \), then \( \nu < \ell \) (as the interval \( J_\ell \) contains \( x_2 - 1 \) with \( \delta(b_{x_2 - 1}) = 1 \)). In this case, \( y_\nu < y_\ell = x_2 - 1 \) and Subclaim 9.1 ensures (given our assumption \( b_\nu \notin X_4 \)) that there is some \( v \in X_3 \cap (b_\nu, b_\nu + 1) \) with \( v \) congruent to 3 or 4 modulo \( q \) and that \( \omega = 2 \). Taking \( j = y_\nu \) then gives the desired element.

Next suppose that \( \delta(b_{j+1}) \neq 0 \) for some \( j + 1 \in J_\nu = [y'_\nu, y_\nu] \). Since \( \delta(b'_\nu) = 0 \) as shown above, we must have \( j \geq y_\nu \), and we can assume \( j + 1 \in J_\nu \) is the minimal index with \( \delta(b_{j+1}) \neq 0 \). Thus \( \delta(b_j) = 0 \) with \( j \in J_\nu \) and \( j < j + 1 \leq y_\nu \leq y_\ell = x_2 - 1 \). In this case, Subclaim 9.2 implies \( \omega = 2 \) and that there is some \( v \in X_3 \cap (b_j, b_{j+1}) \) with \( v \) congruent to some element from \( \{3, 4, -3, -2\} \) modulo \( q \), as desired.

If \( \kappa = 1 \), then \( |Y'| = x_3 - 1 \geq 1 \) ensures that the hypotheses of one of the previous paragraphs holds.

If \( \kappa = 2 \), then Claim 3 implies that \( |Y'| = x_3 - 2 = x_3 - 2 \geq 3 > 1 \), and again, one of the hypotheses of the previous paragraphs must hold with \( b_\nu \notin X_4 \). In either case, it follows that \( \omega = 2 \) as shown in these paragraphs, and the proof of Subclaim 9.3 is now complete. \( \square \)

Subclaim 9.4: \( d_3 \) is congruent modulo \( q \geq 7 \) to some element from \( \{2, 3, -4, -3\} \).

Proof. Since \( d_3 + 1 = \min X_3 \leq \frac{n+1}{2} \), the desired conclusion follows from Subclaim 9.3 unless \( \kappa = 2 = \omega \) and \( d_3 + 1 = \min X_3 < \frac{n+5}{2} \) is one of the at most two elements of \( X_3 \) failing to satisfy the congruence conditions given in Subclaim 9.3. By Claim 3, we have \( x_3 = z_3 \geq 5 \), implying \( d_3 < \frac{n}{z_3} \leq \frac{n}{5} \). Hence, since \( \omega = 2 \) implies that \( n \geq 35 \), it follows that \( n - d_3 = \max X_3 > \frac{n+9}{2} \). Thus Subclaim 9.3 and Lemma 2.4.3 imply that \( \max X_3 = n - d_3 \equiv -d_3 \) must be congruent modulo \( q \) to some element from \( \{3, 4, -3, -2\} \), implying \( d_3 \) is congruent modulo \( q \) to some element from \( \{2, 3, -4, -3\} \), as desired. \( \square \)
Subclaim 9.5: $x_3 \geq 4$.

Proof. If $\kappa = 2$, then $x_3 = z_3 \geq 5$ follows by Claim 3. Therefore we may assume $\kappa = 1$, so $x_1 + x_2 + x_3 = n + 1$. By Subclaim 9.3, $\omega = 2$, implying that $n \geq 35$. Since $4 = d = \lfloor \frac{n}{x_1} \rfloor$ with $x_1' = n - x_1$, we have $4 \leq \frac{n}{x_1'} < 5$ and $\frac{3}{2}n \leq x_1 < \frac{5}{2}n$, which in view of $5 = p \mid n$ implies that $x_1 \leq \frac{4}{5}n - 1$. Likewise, $6 = d_2 + 1 = \lfloor \frac{n}{x_2'} \rfloor$ implies that $5 < \frac{n}{x_2'} \leq 6$ and $\frac{3}{2}n \leq x_2 < \frac{5}{2}n$. Again, as $5 = p \mid n$, this implies $x_2 \leq \frac{5}{2}n - 1$. Hence $x_1 + x_2 \leq n - 2$, implying $x_3 = n + 1 - (x_1 + x_2) \geq 3$. Thus, if the subclaim fails, then we must have

$$x_3 = 3, \quad x_1 = \frac{4}{5}n - 1, \quad \text{and} \quad x_2 = \frac{1}{5}n - 1.$$

Suppose $n \equiv -1 \pmod{3}$, whence $n \equiv 5 \pmod{15}$. Consider $u = \frac{2n+2}{3}$. Note $\gcd(u, n) = 1$ and $ux_2 = \frac{2(n-5)}{15} (n + 1)$, which is congruent to $\frac{2(n-5)}{15}$ modulo $n$ in view of $n \equiv 5 \pmod{15}$. Likewise, $ux_1 = \frac{2(4n-5)}{15}(n + 1)$, which is congruent to $\frac{2(4n-5)}{15}$ modulo $n$ in view of $n \equiv 5 \pmod{15}$. Thus $(ux_1)_n + (ux_2)_n + (ux_3)_n = \frac{2(4n-5)}{15} + \frac{2(n-5)}{15} + 2 = \frac{2n+2}{3} < n$, showing that the theorem is true for $S$, contrary to assumption. So instead assume $n \equiv 1 \pmod{3}$.

In this case, we have $n \equiv 10 \pmod{15}$. If $q > 7$, consider $u = \frac{2n+7}{3}$, and if $q = 7$, instead consider $u = \frac{2n+13}{3}$. As before, we readily check that $\gcd(u, n) = 1$. If $q > 7$, then $ux_2 = \frac{2n-5}{15}n + \frac{2n-35}{15}$ and $ux_1 = \frac{8n+10}{15}n + \frac{8n-35}{15}$, whence $(ux_1)_n + (ux_2)_n + (ux_3)_n = \frac{8n-35}{15} + \frac{2n-35}{15} + 7 = \frac{2n+7}{3} < n$, showing the theorem is true. If $q = 7$, then $ux_2 = \frac{2n-5}{15}n + \frac{8n-65}{15}$ and $ux_1 = \frac{8n+40}{15}n + \frac{2n-65}{15}$, whence $(ux_1)_n + (ux_2)_n + (ux_3)_n = \frac{2n-65}{15} + \frac{8n-65}{15} + 13 = \frac{2n+13}{3} < n$, showing the theorem is again true.

By Subclaim 9.3, $\omega = 2$ and all but at most two elements of $X_3$ are congruent to some element from

$$\{3, 4, -3, -2\} \pmod{q} \geq 7.$$  

Let us show there cannot be three consecutive elements of $X_3$ satisfying these congruence conditions. To this end, suppose $c_i$, $c_{i+1}$ and $c_{i+2}$ are three consecutive elements of $X_3$ each congruent to some number from $\{3, 4, -3, -2\}$ modulo $q$. By Subclaim 9.4, there are four possible values for $d_3$ modulo $q$, and in what follows, we use that the difference of consecutive elements in $X_3$ is either $d_3$ or $d_3 + 1$ (by Lemma 2.4.1) in order to determine the possible congruence values of $c_i$, $c_{i+1}$ and $c_{i+2}$.

If $d_3 \equiv 2 \pmod{q}$, then $c_{i+1}$ must be congruent modulo $q \geq 7$ to some number from $\{3, 4, -3, -2\} + \{2, 3\} = \{5, 6, 7, -1, 0, 1\}$ as well as some number from $\{3, 4, -3, -2\}$, which is only possible if $q = 7$ and $c_{i+1} \equiv 5 \pmod{7}$. But then $c_{i+2}$ must be congruent to some number from $5 + \{2, 3\} = \{7, 8\}$ as well as some number from $\{3, 4, -3, -2\}$ modulo $q = 7$, which is not possible.

If $d_3 \equiv 3 \pmod{q}$, then $c_{i+1}$ must be congruent modulo $q \geq 7$ to some number from $\{3, 4, -3, -2\} + \{3, 4\} = \{6, 7, 8, 0, 1, 2\}$ as well as some number from $\{3, 4, -3, -2\}$, which is only possible if $q = 11$ and $c_{i+1} \equiv 8 \pmod{11}$. But then $c_{i+2}$ must be congruent to some number from $8 + \{3, 4\} = \{11, 12\}$ as well as some number from $\{3, 4, -3, -2\}$ modulo $q = 11$, which is not possible.

If $d_3 \equiv -4 \pmod{q}$, then $c_{i+1}$ must be congruent modulo $q \geq 7$ to some number from $\{3, 4, -3, -2\} + \{-4, -3\} = \{-1, 0, 1, -7, -6, -5\}$ as well as some number from $\{3, 4, -3, -2\}$, which is only possible if $q = 11$ and $c_{i+1} \equiv -7 \pmod{11}$. But then $c_{i+2}$ must be congruent to some number from $-7 + \{-4, -3\} = \{-11, -10\}$ as well as some number from $\{3, 4, -3, -2\}$ modulo $q = 11$, which is not possible.
If \( d_3 \equiv -3 \pmod{q} \), then \( c_{i+1} \) must be congruent modulo \( q \) to some number from \( \{3, 4, -3, -2\} + \{-3, -2\} = \{0, 1, 2, -6, -5, -4\} \) as well as some number from \( \{3, 4, -3, -2\} \), which is only possible if \( q = 7 \) and \( c_{i+1} \equiv -4 \pmod{11} \). But then \( c_{i+2} \) must be congruent to some number from \(-4 + \{-3, -2\} = \{-7, -6\} \) as well as some number from \( \{3, 4, -3, -2\} \) modulo \( q = 7 \), which is not possible.

As the above exhausts all four cases, we now conclude that there cannot be three consecutive elements of \( X_3 \) satisfying the stated congruence conditions. If \( \kappa = 1 \), then all elements of \( X_3 \) satisfy these congruence conditions, whence \( x_3 - 1 = |X_3| \leq 2 \) follows, contrary to Subclaim 9.5. Therefore we may now assume \( \kappa = 2 \). In particular, \( \omega = 2 \) by Condition (4). If \( |X_3| \geq 9 \), then Subclaim 9.3 ensures that there will be three consecutive elements of \( X_3 \) satisfying the stated congruence conditions. Therefore, we can assume \( z_1 - 1 = |X_3| \leq 8 \).

Suppose at most one element of \( X_3 \) fails to satisfy the congruence conditions. Then we must have \( z_3 - 1 = |X_3| \leq 5 \) (else three consecutive elements will satisfy the congruence condition), whence Claim 3 implies that \( z_3 = 5 \). However, since \( p = 5 \mid n \), this contradicts that \( \gcd(x_3, n) = 1 \) when \( \omega = 2 \) (by hypothesis). So we may instead assume that exactly two elements of \( X_3 \) fail to satisfy the congruence conditions, say \( v_1, v_2 \in X_3 \). Moreover, Subclaim 9.3 ensures that w.l.o.g. \( v_2 \in \{(\frac{n+1}{2}, \frac{n+9}{2}) \} \).

Since \( \omega = 2 \), the theorem’s hypotheses ensure that \( \gcd(z_3, n) = 1 \), which in view of \( p = 5 \mid n \) and Claim 3 forces \( z_3 \geq 7 \). As shown above, we also have \( z_3 \leq 9 \). This gives three possible values for \( z_3 \).

If \( z_3 = 8 \), then \( \frac{n+1}{2} = \left[ \frac{4n}{7} \right] \in X_3 \), whence \( \frac{5n+1}{8} \leq \left[ \frac{4n}{7} \right] \leq \frac{n+9}{2} \), implying \( n = 35 \). But \( \omega = 2 \) ensures that \( n \geq 35 \), meaning we must have \( n = 35 \) with \( p = 5 \) and \( q = 7 \), in which case \( X_3 = \{5, 9, 14, 18, 22, 27, 31\} \), which does not satisfy Subclaim 9.3. Thus \( z_3 = 8 \) is not possible.

Suppose \( z_3 = 9 \). For each \( k \in [1, z_3 - 1] = [1, 8] \), we have \( c_k = \left[ \frac{kn}{73} \right] = \frac{kn + 4k}{73} \) for some \( c_k \in [0, 8] \). Since \( \gcd(9, n) = 1 \), it follows that the elements \( \epsilon_k \in [0, 8] \) are distinct modulo 9, and thus distinct elements. Consequently, if \( q > 7 \), then the elements of \( X_3 \) represent at least 8 different residue classes modulo \( q \), contradicting that Subclaim 9.3 ensures there can be at most 6 such residue classes. On the other hand, if \( q = 7 \), then \( X_3 \) instead represents at least 6 different residue classes modulo \( q = 7 \). However, for \( q = 7 \), Subclaim 9.3 ensures that there can be at most 5 such residue classes (as \(-3 \equiv 4 \pmod{7}\)). Thus, in all cases, we obtain a contradiction.

Finally, it remains to consider the case when \( z_3 = 7 \). Hence, since \( \gcd(z_3, n) = 1 \) in view of \( \omega = 2 \), we conclude that \( q \geq 11 \) and \( n \geq 55 \). In this case, we have \( \frac{4n+1}{7} \leq \left[ \frac{4n}{7} \right] \leq \frac{n+9}{2} \), implying \( n \leq 61 \), forcing \( n = 55 \). Hence \( X_3 = \{8, 16, 24, 32, 40, 48\} \), which does not satisfy Subclaim 9.3. Thus \( z_3 = 7 \) is also not possible, completing Claim 9.

In view of Claim 9, we have \( d_2 = d \). In this case, \( X'_1 = \min X_2 = d + 1 \), and the difference between consecutive element in \( X'_1 \), as well as between consecutive elements in \( X_2 \cup \{n\} \), is either \( d \) or \( d + 1 \) by Lemma 2.4.2. This means that \( \zeta(i+1) \in \zeta(i) \cup \{0, 1, 2\} \) for \( i \in [1, x_2 - 2] \), with \( \zeta(i+1) = \zeta(i) \) only possible when \( g(i) = 0 \) and \( g(i+1) = d \) with \( I_{(i)} \) long, and \( \zeta(i+1) = \zeta(i) + 2 \) only possible when \( g(i) = d - 1 + \varepsilon_i \) and \( g(i+1) = 0 \) with \( I_{(i+1)} \) short. Moreover, when \( \zeta(i+1) = \zeta(i) + 1 \), we have \( g(i+1) \in \{d, 0\} \). From Claim 6, we find that

\[
\delta(b_i) = 0 \quad \text{when} \quad 1 \leq g(i) \leq d + \varepsilon_i - 3, \quad \text{and} \quad \delta(b_i) = 1 \quad \text{when} \quad g(i) \geq 3 \quad \text{and} \quad b_i \notin X_4 \quad (18)
\]
By Lemma 2.4.3, we have $b_{x_2-1} = n - d_2 = n - d$ when $x_2 \nmid n$, and $b_{x_2-1} = n - d_2 - 1 = n - d - 1$ when $x_2 \mid n$. Likewise, $a'_{x'-1} = n - d$ when $x'_1 \mid n$, and $a'_{x'-1} = n - d + 1$ when $x'_1 \nmid n$. Thus, when $\omega = 2$, we must have $b_{x_2-1} = a'_{x'-1} = n - d$ (recall $x'_1 = n - x_1$ with $\gcd(x_1, n) = 1$ for all $i$ when $\omega = 2$). On the other hand, when $\omega = 1$, then $x_2 \mid n$ and $x'_1 \mid n$ would imply $d = \frac{n}{x_1'} = \frac{n}{x'_1}$ and $d + 1 = \frac{n}{x_2} - \frac{n}{x'_2}$ are both congruent to 0 modulo $p$, which is not possible. Therefore, when $\omega = 1$, we have $a'_{x'-1} \geq b_{x_2-1} \geq a'_{x'-1} - 1$. In particular, if $\varsigma(x_2 - 1) < |X'_1|$, then $\varsigma(x_2 - 1) = |X'_1| - 1$ and $\varrho(x_2 - 1) = d - 1 + \varepsilon_{x_2-1}$.

For $i \in [1, |X_2|]$, let $f(i) = \varsigma(i) - i$. Observe that $\varsigma(1) = 1$ since $b_1 = d_2 + 1 = d + 1 = a'_1$. By the work of the previous paragraph, we have $\varsigma(|X_2|) \geq |X'_1| + \omega - 2$. Thus $f(1) = 0$ and $f(|X_2|) \geq |X'_1| + \omega - 2 - |X_2| = n - x_1 - x_2 - 2 + \omega = x_3 - \kappa - 2 + \omega$, with the final equality from Claim 1. Hence, if $\omega = 2$, then Claim 3 implies $f(|X_2|) \geq \kappa$, while if $\omega = 1$, then Claim 3 instead implies $f(|X_2|) \geq x_3 - 2 \geq 0$. In this case, we also have $f(|X_2|) \geq \kappa$ unless equality holds in the estimates used to show $f(|X_2|) \geq 0$. In particular, this is only possible when $x_3 = 2$ and $\varrho(x_2 - 1) = d - 1 + \varepsilon_{x_2-1}$.

Let $t = \max\{f(i) : i \in [1, x_2 - 1]\} \geq f(|X_2|) \geq 0$ by $f(1)$. Since $\varsigma(i+1) \in \varsigma(i) + \{0, 1, 2\}$ for all $i \in [1, x_2 - 2]$, it follows that $f(i + 1) - f(i) \in \{1, 0, 1\}$. Consequently, the function $f$ must achieve all integer values between $f(1) = 0$ and $t$ at some point on the interval $[1, x_2 - 1]$. For $i \in [0, t]$, let $j_i + 1 \in [1, x_2 - 1]$ be the first index such that $f(j_i + 1) = i$. Observe that $0 < j_0 < j_1 < j_2 \ldots < j_t$ in view of $f(i + 1) - f(i) \in \{1, 0, 1\}$. The minimality of $j_i + 1$ together with $f(i + 1) - f(i) \in \{1, 0, 1\}$ ensures that $f(j_i + 1) = f(j_i + 1) + 1$ for $i \in [1, t]$, which implies that $1 = f(j_i + 1) - f(j_i) = \varsigma(j_i + 1) - \varsigma(j_i)$, so that $\varsigma(j_i + 1) - \varsigma(j_i) = 2$. As observed above, this implies $g(j_i + 1) = 0$ and $g(j_i) = d - 1 + \varepsilon_{j_i}$ with $I_{\varsigma(j_i)+1}$ short. Since we also have $g(j_0 + 1) = g(1) = 0$, this shows that $g(j_i + 1) = 0$ for all $i \in [0, t]$ and that $g(j_i) = d - 1 + \varepsilon_{j_i}$ for all $i \in [1, t]$. Now, if $t = 0$, define $j_1 = x_2 - 1$ and $t' = t + 1 = 1$. Set $t' = t$ when $t \geq 1$. Note $t = 0$ is only possible if $f(|X_2|) = 0$, in which case $\varrho(x_2 - 1) = d - 1 + \varepsilon_{x_2-1}$ and $\omega = 1$. Thus

$$g(j_i) = d - 1 + \varepsilon_{j_i} > 0 \quad \text{and} \quad g(j_i + 1) = 0 \quad \text{for all} \quad i \in [1, t'].$$ 

In particular, $j_{i-1} + 1 < j_i$ for each $i \in [1, t']$. Moreover, since $g(i + 1) \in g(i) + \{1, 0, 1\}$ when $f(i + 1) = f(i)$ (as this ensures $\varsigma(i + 1) = \varsigma(i) + 1$), and since $g(i + 1) = 0$ when $f(i + 1) = f(i) + 1$ (as this ensures $\varsigma(i + 1) = \varsigma(i) + 2$), it follows from the minimality of $j_i$ and the definition of $t$ that the function $g$ achieves all integer values between $g(j_i + 1) = 0$ and $g(j_i) = d - 1 + \varepsilon_{j_i}$ at some point on the interval $[j_i - 1 + 1, j_i]$, for each $i \in [1, t']$. Noting that $t' \geq \kappa$, we can find some $i \in [1, t']$ such that

$$[b_{j_i-1+1}, b_{j_i}] \cap X_4 = \emptyset.$$ 

(19)

If $d \geq 6$, then there must be some $j \in [j_i - 1 + 1, j_i]$ with $g(j) = 3 \leq d + \varepsilon_j - 3$ (as $g$ achieves all values between $0$ and $d - 1 + \varepsilon_{j_i} \geq 3$ on this interval). But now $\delta(b_j) = 0$ as $g(j) \leq d + \varepsilon_j - 3$, and $\delta(b_j) = 1$ as $g(j) \geq 3$ and $b_j \notin X_4$ (both in view of (18)), which is clearly absurd. This shows that $d \leq 5$.

If $d = 5$, then, arguing as above, we again obtain a contradiction unless there is some $j \in [j_i - 1 + 1, j_i]$ with $g(j) = 2 \leq d - 3 + \varepsilon_j$ and $g(j + 1) = 3 \geq 2 - 2 + \varepsilon_{j+1} = 3 + \varepsilon_{j+1}$. We cannot have $j = j_i$ as $g(j_i) = d - 1 + \varepsilon_{j_i} \geq 4$, and we cannot have $j = j_i + 1$ as $g(j_i + 1) = 0$, so $j \in [j_i - 1 + 2, j_i - 1]$. Since $g(j + 1) = g(j) + 1$, we must have

$$b_{j+1} - b_j = d_2 + 1 = d + 1 = 6.$$
with $I_{d(j)}$ short. Since $[b_j, b_{j+1}] \cap X_4 = \emptyset$ (in view of Equation (19) and $j_{i-1} + 1 < j < j_i$), Claims 6 implies that $\delta(b_j - 2) \leq \delta(b_j - 1) < \delta(b_j) = 0$ and $\delta(b_{j+1} + 1) \geq \delta(b_{j+1}) = 1$, so that $b_j - 1, b_j - 2, b_{j+1}$ and $b_{j+1} + 1$ must all be non-relatively prime to $n$. This is only possible if either $b_{j+1} - (b_j - 1) = 7$ is divisible by one of the primes $p$ or $q$ with $(b_{j+1} + 1) - (b_j - 2) = 9$ divisible by the other or else $(b_{j+1} + 1) - (b_j - 1) = 8$ is divisible by both of the primes $p$ and $q$. However, since $p, q \geq 5$, neither is possible. This shows that $d \leq 4$. We divide the remainder of the proof into cases based on the remaining sizes for $d \geq 2$ (by Claim 4). In all such cases, recall that $\delta(v) \neq 0$ implies $\gcd(v, n) \neq 1$, further implying $5 \leq p \leq v \leq n - p \leq n - 5$, which guarantees that $v \pm \epsilon \in [1, n - 1]$ for $\epsilon \in [0, 4]$. It also guarantees that $X_4 \cap [v - 1, v + 2] = \emptyset$ by (13).

Case A. $d = 4$.

We begin by showing the following subclaim.

Subclaim A.1: If $5 \mid n$, then each $u \in X_3$ is congruent to 3 modulo 5 when $\kappa = 1$ while each $u \in X_3$ with $\kappa = 2$ and $u < \frac{n+1}{2} - 4$ is congruent to 3 modulo 5 when $\kappa = 2$. If $5 \nmid n$, then $7 \mid n$ and each $u \in X_3$ is congruent to 4 modulo 7 when $\kappa = 1$ while each $u \in X_3$ with $\kappa = 2$. Furthermore, $x_3 \geq 3$.

Proof. Recall that $|X_3| = x_3 - 1 \geq 1$ by Claim 3. Let $u \in X_3 \setminus X_4$ be arbitrary.

Suppose $u \in X_2$. If we also have $u \in X_1$, then $\delta(u) = \delta(u - 1) + 2 \geq 1$, which is only possible (by Claim 5) if $\Lambda(u - 1) = -1$ with $u - 1 \notin X'_1$. But then, as the difference between consecutive elements in $X'_1$ is $d = 4$ or $d + 1 = 5$, we find that $u + 1 \in X_1$, so that $\Lambda(u + 1) \geq 1$ and $\delta(u + 1) \geq \delta(u) = 1$. Hence $\delta$ is non-zero on $[u - 1, u + 1]$, contrary to Claim 5. Therefore, we instead conclude that $u \notin X_1$, whence $u \in X'_1$. Since $\Lambda'(u) = \Lambda(u) = 2$ and $\Lambda(i) \geq 1$ for $i \in [u - 3, u - 1]$ (since $u \in X'_1$ with the difference of consecutive elements in $X'_1$ being $d = 4$ or $d + 1 = 5$), we have $\delta(u - 1) = \delta(u + 1) \geq \delta(u - 2) \geq \delta(u - 3)$, which forces $\delta(u) = 1$ in view of Claim 5. But we also have $\Lambda(i) \geq 1$ for $i \in [u + 1, u + 2]$ by similar reasoning, which forces $1 = \delta(u) \leq \delta(u + 1) \leq \delta(u + 2)$, contrary to Claim 5. So we instead conclude that $u \notin X_2$, i.e., that $X_3 \cap X_2 \subseteq X_4$, which, in view of Equation (7) and $\Lambda(v) = 2$ for $v \in X_4$, ensures $X_3 \cap X_2 = \emptyset$. Now additionally assume that $u < \frac{n+1}{2} - 4$ when $\kappa = 2$. By Lemma 2.4.3, we have $\max X_3 = n - d_3$ or $n - d_3 - 1$, with the latter occurring when $x_3 \mid n$, and $\max X_2 = n - d_2$ or $n - d_2 - 1$, with the latter occurring when $x_2 \mid n$. Thus $\max X_3 \leq \max X_2$ unless $d_3 = d_2 = d = 4$ with $\omega = 1$. However, this would imply $x_2, x_3 \geq \frac{n}{2}$ and $x_1 > \frac{3n}{4}$, yielding $n + 1 = x_1 + x_2 + x_3 > \frac{3}{2}n + \frac{3}{4}n$, contradicting that $n \geq 11$ by Claim 3. Therefore $\max X_3 \leq \max X_2$. Thus, as $\min X_3 = x_3 + 1 \geq \min X_2$ and $X_3 \cap X_2 = \emptyset$, let $j \in [1, x_2 - 2]$ be the index such that $b_j < u < b_{j+1}$. Combining this with $b_{j+1} + b_j \leq d_2 + 1 = d + 1 = 5$ and $u < \frac{n+1}{2} - 4$ (when $\kappa = 2$) yields $[1, b_{j+1}] \cap X_4 = \emptyset$.

We must have $X_3 \cap [b_j, b_{j+1}] = \{u\}$, for if $u' \in X_3 \cap [b_j, b_{j+1}]$ is an element distinct from $u$, then $|u - u'| \geq d_3 \geq d_2 = d \geq b_{j+1} - b_j - 1$, meaning either $u' = b_j$ or $u' = b_{j+1}$, both contradicting that $X_3 \cap X_2 = \emptyset$. Observe that

$$\sum_{i = b_{j+1}}^{b_{j+1} + 1} (1X_3(i) + 1X_2(i) - 1) = 1 - t,$$

where $\varsigma(j + 1) = \varsigma(j) + t$ with $t \in \{0, 1, 2\}$.

In particular, $\delta(b_{j+1}) = \delta(b_j) + 2 - t$ as $X_3 \cap [b_j + 1, b_{j+1}] = \{u\}$ and $[1, b_{j+1}] \cap X_4 = \emptyset$. 

Suppose $t = 2$. Then $\varsigma(j + 1) = \varsigma(j) + 2$, which is only possible if $\rho(j) = d - 1 + \varepsilon_j$ and $\rho(j + 1) = 0$ with $I_{\varsigma(j) + 1}$ short. Since $\rho(j) = d - 1 + \varepsilon_j \geq 3$ and $b_j \not\in X_4$, we have $\delta(b_j) = 1$ (by Claim 6). If $u = b_j + 1$, then $\Lambda(u) \geq 1$ for all $v \in [b_j + 1, b_j + 7]$, implying $1 = \delta(b_j) \leq \delta(b_j + 1) \leq \delta(b_j + 2)$, contrary to Claim 5. If $u > b_j + 1$, then $\delta(b_j + 1) = 0$ and $\Lambda'(u) = \Lambda(u) \geq 2$ (as $u \not\in X_4$), implying $0 = \delta(b_j + 1) - \delta(u) \leq \delta(u + 1) \leq \delta(u + 2)$ (in view of $u < b_j + 1 = b_j + 5$), also contradicting Claim 5.

Suppose $t = 0$. Then $\varsigma(j + 1) = \varsigma(j)$, which is only possible if $\rho(j) = 0$ and $\rho(j + 1) = d$ with $I_{\varsigma(j)}$ long. Since $\rho(j) = 0$, we must have $\delta(b_j) \geq 0$, for if $\delta(b_j) = -1$, then $\delta(b_j - 2) \leq \delta(b_j - 1) \leq \delta(b_j) = -1$ (as $\Lambda(b_j - i) \geq 1$ for $i \in [0, d - 1]$ in view of $\rho(j) = 0$), contrary to Claim 5. But then $\delta(b_{j+1}) = \delta(b_j) + 2 - t \geq 2$, which is impossible. It remains to consider the case $t = 1$, for which $\delta(b_{j+1}) = \delta(b_j) + 2 - t = \delta(b_j) + 1$.

If $\delta(b_{j+1}) = 0$, then $\delta(b_j) = 1$. Since $\Lambda(b_j) \geq 1$, we have $\delta(b_j - 1) \leq \delta(b_j) = 1$. Furthermore, if $\Lambda(b_j) \geq 2$, then $\delta(b_j - 1) \leq \delta(b_j) - 1 = -2$, which is not possible. Thus $\Lambda(b_j) = 1$, which is only possible if $\rho(j) = 0$, so that $\Lambda(b_j - i) \geq 1$ for $i \in [0, d - 1]$. Thus $\delta(b_j - 2) \leq \delta(b_j - 1) \leq \delta(b_j) = 1$, contrary to Claim 5. So we instead conclude that $\delta(b_{j+1}) = 1$ and $\delta(b_j) = 0$.

Since $\delta(b_{j+1}) = 1$, Claim 5 ensures that $\rho(j + 1) \geq d - 2 + \varepsilon_{j+1} = 2 + \varepsilon_{j+1}$, else we obtain the contradiction $1 = \delta(b_{j+1}) \leq \delta(b_{j+1} + 1) = \delta(b_{j+1} + 2)$. Since $\rho(j) = 0$, we must have $\rho(j + 2)$, else we obtain $\delta(b_j - 3) \leq \delta(b_j - 2) \leq \delta(b_j) - \delta(b_j) = 0$, contrary to Claim 5.

Suppose $b_{j+1} - b_j = d = 4$. Then $2 \geq \rho(j) \geq \rho(j + 1) \geq 2 + \varepsilon_{j+1}$, whence $\rho(j) = (j + 1) = 2$ with $I_{\varsigma(j)}$ short (else $\rho(j) > \rho(j + 1)$ would hold in view of $b_{j+1} - b_j = d$ and $I_{\varsigma(j)}$ short (as $\varepsilon_{j+1} = 0$). Since $\rho(j) = 2$, we have $\Lambda(b_j) \geq 2$ and $\Lambda(b_j - 1) \geq 1$, whence $\delta(b_j - 2) \leq \delta(b_j - 1) \leq \delta(b_j) = 0$. Thus $b_j - 1$ and $b_j - 2$ are both non-relatively prime to $n$. Since $\delta(b_{j+1}) = 1$ and $\Lambda(b_{j+1} + 1) \geq 1$, we also have $b_{j+1} = (b_{j+1} + 1)$ and $b_{j+1} + 1 = (b_{j+1} + 1) \geq 6$ non-relatively prime to $n$. As $n$ has at most two prime divisors $\Lambda(b_{j+1} - (b_j - 2)) = 6$ relatively prime to $n$, it follows that every $n$ with $b_j - 1$ and $b_{j+1}$ congruent to $0$ modulo $5$ and $b_j - 2$ and $b_{j+1}$ relatively prime to $n$ and $7$. Thus $\omega = 2, p = 5$ and $q = 7$. Moreover, all number in the interval $[b_{j+1} - b_j = 1]$ are relatively prime to $n$ and thus must have $\delta(b_j) = 0$, the only way this is possible is if the element $u \in X_3$ that lies between $b_j$ and $b_{j+1}$ coincides with $\alpha_j = b_{j+1} + 2$. Thus $u = (b_j - 1) + 3 \equiv 3 \pmod{5}$, as desired. It remains to show $x_3 \geq 3$ in this case, so assume instead that $\kappa = 1$ (as $x_3 \geq 5$ by Claim 3 when $\kappa = 2$) and $x_3 = 2$, so that $X_3 = \{\frac{n+1}{2}\}$. Then $u = b_j + 2 = \frac{n+1}{2}$ is the unique element of $X_3$.

Now $\rho(j + 1) = 2 > 0$, so $b_{j+1}$ cannot be the last element of $X_2$ (in view of $\omega = 2$ and Lemma 2.4.3), so $b_{j+2}$ is either equal to $b_{j+1} + 4$ or $b_{j+1} + 5$. In either case, $\Lambda(b_{j+2}) = 2$, implying $\delta(b_{j+2}) \geq \delta(b_j) = 1$. However, only $b_{j+1} + 5 = \frac{n+15}{2}$ is non-relatively prime to $n$, so we must have $b_{j+2} = b_{j+1} + 5$ with $\rho(j) = 2$. If $I_{\varsigma(j) + 5}$ is long, then $\Lambda(b_{j+2} + 1) = 1$ and $\delta(b_{j+2} + 1) = 1$, contradicting that $b_{j+2} + 1 = \frac{n+17}{2}$ is relatively prime to $n$. Therefore we must have $I_{\varsigma(j) + 2}$ short. Again, $\rho(j + 2) = 3 > 0$, so $b_{j+2}$ cannot be the last element of $X_2$, so $b_{j+3}$ is either equal to $b_{j+1} + 4$ or $b_{j+1} + 5$. If $b_{j+3} = b_{j+2} + 4$, then $\Lambda(b_{j+3}) = 2$ and $\delta(b_{j+3}) = 1$, contradicting that $b_{j+3} = \frac{n+23}{2}$ is relatively prime to $n$. Therefore we must have $b_{j+3} = b_{j+2} + 5$. Thus there are two consecutive differences in $X_2$ equal to $5 = d_2 + 1$, whence Lemma 2.4.6 implies that $x_2 < \frac{n}{5\sqrt{2} + 1} = \frac{2}{5} n$. As $\rho(j) = 2 > 0$, we see that $b_j$ cannot be the first element of $X_2$. Thus $b_{j-1} = b_{j-4} \text{ or } b_{j-5}$. In either case, if $I_{\varsigma(j) - 1}$ is long, then $\Lambda(b_{j-1}) = 2$ and $\Lambda(b_{j-1} - 1) = 1$, implying $\delta(b_{j-1} - 1) = \delta(b_{j-1} - 2) = -1$. However, if $b_{j-1} = b_{j-4}$, then $b_{j-1} - 1 = b_{j-5} = \frac{n-13}{2}$ is relatively prime to $n$, while if $b_{j-1} = b_{j-5}$, then $b_{j-1} - 2 = b_{j-7} = \frac{n-15}{2}$ is relatively prime to $n$, implying the $\delta$ value of these numbers must be 0, not -1, a contradiction. Therefore it must be that
$I_{c(j)-1}$ is short, so that we have 4 consecutive short intervals in $X'_1$. Thus Lemma 2.4.6 implies that $n - x_1 = x'_1 > \frac{n}{4\ell+2} = 4\ell / 17$. Hence $x_1 < \frac{13}{17} n$. But now $n - 1 = n + 1 - x_3 = x_1 + x_2 < \left(\frac{13}{17} + \frac{3}{2}\right)n$, which implies $n < \frac{152}{2}$. As $35 \mid n$ with $n$ only divisible by the primes 5 and 7, this forces $n = 35$. Finally, in this case, since $d = 4$, we have $x'_1 \leq \left\lceil \frac{n}{4}\right\rceil = 8$, contradicting that $x'_1 \geq \left\lceil \frac{4}{17}n\right\rceil = 9$. So we now assume $b_{j+1} - b_j = d + 1 = 5$.

Suppose $g(\ell) \leq 1$. Then $g(\ell + 1) \leq 2$. However, since we know $g(\ell + 1) \geq 2 + \varepsilon_{j+1}$, this forces $g(\ell) = 1$ and $g(\ell + 1) = 2$ with $I_{c(j)}$ and $I_{c(j)+1}$ both short. But now $\delta(b_j) = 1 < \delta(b_j - 1)$, forcing $b_j - 1$ to be non-relatively prime to $n$. Likewise, $\delta(b_{j+1}) \geq \delta(b_{j+1}) = 1$, forcing $b_{j+1}$ and $b_{j+1}$ to also be non-relatively prime to $n$. Since $b_{j+1} - (b_j - 1) = 6$ and $(b_{j+1} + 1) - (b_j - 1) = 7$, this is only possible if $7 \mid n$ with $b_{j+1} + 1$ and $b_j - 1$ both congruent to 0 modulo 7. Furthermore, $\omega = 2$, and if $5 \mid n$, then we must also have $b_{j+1}$ congruent to 0 modulo 5. Regardless, all numbers in the interval $[b_j + 1, b_{j+1} - 1]$ are now relatively prime to $n$, thus having $\delta$ value 0. Since $\delta(b_j) = 0$, the only way this is possible is if the element $u \in X_3$ that lies between $b_j$ and $b_{j+1}$ coincides with $a'_{c(j)+1} = b_j + 3$. If $5 \mid n$, this means $u = b_j + 3 = b_{j+1} - 2 \equiv -2 \equiv 3 \pmod{5}$, as desired. Otherwise, $u = (b_j - 1) + 4 \equiv 4 \pmod{7}$. Both cases yield the desired congruence conclusion. It remains to show $x_3 \geq 3$ in this case, so assume instead that $\kappa = 1$ and $x_3 = 2$, so that $X_3 = \{\frac{n+1}{2}\}$. Then $u = \frac{n+1}{2}$ is the unique element of $X_3$. In this case, we must have $x_2$ odd (since $\frac{n+1}{2} \notin X_2$) with $\frac{n+1}{2} = b_j = \left\lfloor \frac{x_2 - 1}{x_2} \right\rfloor > \frac{x_2 - 1}{x_2}$ (the strict inequality follows as gcd$(x_2, n) = 1$ when $\omega = 2$), implying $\frac{n}{x_2} > 5$, so that $d_2 = \left\lceil \frac{n}{x_2} \right\rceil - 1 \geq 5$, contradicting that $d_2 = d = 4$. So we now consider the remaining case when $g(\ell) = 2$.

In this case, we have $\delta(b_j - 2) \leq \delta(b_j - 1) < \delta(b_j)$, forcing $b_j - 2$ and $b_j - 1$ to both be non-relatively prime to $n$. We also have $\delta(b_{j+1}) = 1$, so that $b_{j+1} = 5$ is also non-relatively prime to $n$. Since $b_{j+1} - (b_j - 1) = 6$ and $b_{j+1} - (b_j - 2) = 7$, this is only possible if $7 \mid n$ with $b_{j+1}$ and $b_j - 2$ both congruent to 0 modulo 7. Furthermore, $\omega = 2$, and if $5 \mid n$, then $b_j - 1$ must be congruent to 0 modulo 5. As in previous cases, all integers in the interval $[b_j, b_{j+1} - 2]$ must then be relatively prime to $n$, thus having $\delta$ value 0. This is only possible if $u = a'_{c(j)+1}$.

If $I_{c(j)}$ is long, then $g(j+1) = g(j) = 2$, in which case $\delta(b_{j+1} + 1) \geq \delta(b_{j+1}) = 1$. Thus $b_{j+1} + 1$ is also non-relatively prime to $n$, along with $b_{j+1} + 1$, $b_j - 2$ and $b_j - 1$. However, since $b_{j+1}$ and $b_j - 2$ are both congruent to 0 modulo 7 with $n$ only having two prime divisors, this is only possible if both $b_{j+1} + 1$ and $b_j - 1$ are congruent to zero modulo the other prime dividing $n$ (as clearly they cannot both be congruent to 0 modulo 7 in view of $b_j - 2 \equiv 0 \pmod{7}$). However, since $(b_{j+1} + 1) - (b_j - 1) = 7$, this is impossible. Therefore we must have $I_{c(j)}$ short.

In this case, $u = a'_{c(j)+1} = (b_j - 1) + 3 = (b_j - 2) + 4$, yielding the desired congruences conditions for $u$. It remains to show $x_3 \geq 3$, so assume instead $\kappa = 1$ and $x_3 = 2$, so that $X_3 = \{\frac{n+1}{2}\}$. Then $u = \frac{n+1}{2}$ is the unique element of $X_3$. In this case, we must have $x_2$ odd (since $\frac{n+1}{2} \notin X_2$) with $\frac{n+7}{2} = b_{j+1} = \left\lfloor \frac{x_2 + 1}{x_2} \right\rfloor < \frac{x_2 + 1}{x_2} + 1$, implying $\frac{n}{x_2} > 5$, so that $d_2 = \left\lceil \frac{n}{x_2} \right\rceil - 1 \geq 5$, contradicting that $d_2 = d = 4$ and completely the last case for Subclaim A.1. \hfill \Box

By Subclaim A.1, we have $x_3 \geq 3$, implying $|X_3| = x_3 - 1 \geq 2$. Thus, if $\kappa = 1$, then the first two consecutive elements of $X_3$ satisfy the congruence conditions given in Subclaim A.1. On the other hand, if $\kappa = 2$, then $\omega = 2$, $n \geq 35$ and $x_3 \geq 5$ (by Claim 3). If the first two elements of $X_3$ do not satisfy the congruence conditions given in Subclaim A.1 in this case, then we must have $\left\lceil \frac{4n}{17} \right\rceil > \frac{n-7}{2}$.
Hence \( \frac{n}{5} \geq \frac{n}{x_3} > \frac{n-9}{4} \), which is only possible if \( n = 35 \) and \( x_3 = 5 \) (in view of \( \omega = 2 \)). But this contradicts the hypothesis \( \gcd(x_3, n) = 1 \). So we conclude that, for both \( \kappa = 1 \) and \( \kappa = 2 \), the first two elements of \( X_3 \) satisfy the congruence conditions given in Subclaim A.1.

Suppose \( 5 \mid n \). Then \( c_1 = d_3 + 1 \equiv 3 \pmod{5} \), implying \( d_3 \equiv 2 \pmod{5} \), whence \( c_2 \) is either congruent to \( 3 + d_3 \equiv 0 \pmod{5} \) or \( 3 + d_3 + 1 \equiv 1 \pmod{5} \), both contradicting that this element should be congruent to 3. So we instead assume \( 5 \notmid n \).

In this case, \( c_1 = d_3 + 1 \equiv 4 \pmod{7} \), implying \( d_3 \equiv 3 \pmod{7} \), whence \( c_2 \) is either congruent to \( 4 + d_3 \equiv 0 \pmod{7} \) or \( 4 + d_3 + 1 \equiv 1 \pmod{7} \), both contradicting that this element should be congruent to 4. This completes Case A.

**Case B.** \( d = 3 \).

We begin by showing the following subclaim.

**Subclaim B.1:** If \( 5 \mid n \), then each \( u \in X_3 \), with \( u \notin [\frac{n-3}{2}, \frac{n+7}{2}] \) if \( \kappa = 2 \), is either congruent to 2 modulo 5 and 0 modulo \( q \) or is congruent to 4 modulo 5 and 1 modulo \( q \) or is congruent to 3 modulo 5, with the first two possibilities only possible if \( \omega = 2 \). If \( 5 \notmid n \), then each \( u \in X_3 \), with \( u \notin [\frac{n-5}{2}, \frac{n+7}{2}] \) if \( \kappa = 2 \), is either congruent to 3 or \(-2 \pmod{p} \). Furthermore, \( x_3 \geq 4 \).

**Proof.** Let \( u \in X_3 \) be arbitrary. We break the claim into four scenarios depending on whether \( u \in X_2 \) and \( u \in X_1 \).

If \( u \in X_2 \) and \( u \in X_1 \), then \( \Lambda(u) = \Lambda'(u) = 3, \delta(u) = 1 \) and \( \delta(u-1) = -1 \), forcing \( \delta(u+1) = 0 \) and \( \delta(u-2) = 0 \) by Claim 5, which is only possible if \( \Lambda(u+1) = 0 \) and \( \Lambda(u-1) = 0 \). Thus \( u+1, u-1 \in X'_1 \).

But \( (u+1) - (u-1) = 2 < d \), contradicting that the difference between consecutive elements in \( X'_1 \) is \( d \) or \( d+1 \).

If \( u \in X_2 \) and \( u \in X'_1 = [2, n-1] \setminus X_1 \), then \( \Lambda(u) = \Lambda'(u) = 2 \) (in view of Equation (7)), whence Claim 6 ensures that \( \Lambda(v) = 0 \) for some \( v \) with \( |u - v| \leq 2 \). But then, \( u, v \in X'_1 \) with \( |u - v| \leq 2 < d \), contradicting that the difference between consecutive element in \( X'_1 \) is either \( d \) or \( d+1 \). So we now conclude that \( u \notin X_2 \), i.e., that \( X_2 \cap X_3 = \emptyset \). We now further assume that \( u \notin [\frac{n-5}{2}, \frac{n+7}{2}] \) if \( \kappa = 2 \), which ensures \( |u - 3, u + 3] \cap X_4 = \emptyset \).

Suppose \( u \notin X_2 \) and \( u \in X_1 \). Then, in view of Claim 6, there must be some \( \epsilon \in [1, 2] \) so that

\[
\delta(u) = \frac{1}{2} \pm \frac{1}{2}, \quad \Lambda(u \pm \epsilon) = 0, \quad \text{and} \quad \delta(u - \frac{1}{2} \pm \frac{1}{2}) = \delta(u - \frac{1}{2} \pm \frac{1}{2} \pm \epsilon) = \pm 1,
\]

where the \( \pm \) is either always + or always − above.

If \( \pm = + \) and \( \epsilon = 2 \), then \( \delta(u) = 1, \delta(u+1) = 1 \) and \( \delta(u+2) = \delta(u+3) = 0 \) (by Claim 5). Also, \( u \notin X_2 \) by assumption, \( u+1 \notin X_2 \) (else \( \Lambda'(u+1) = \Lambda(u+1) \geq 2 \) implying \( \delta(u+1) > \delta(u) = 1 \), which is not possible) and \( u+2 \notin X_2 \) (as \( \Lambda(u+2) = 0 \)). Consequently, since the difference between consecutive elements in \( X_2 \) is either \( d = 3 \) or \( d+1 = 4 \), we conclude that \( u-1, u+3 \in X_2 \). Since \( \Lambda(u+2) = 0 \), we also have \( u+3 \in X_1 \), whence \( \Lambda'(u+3) = \Lambda(u+3) \geq 2 \), implying \( \delta(u+3) > \delta(u+2) = 0 \), contradicting that \( \delta(u+3) = 0 \).

If \( \pm = - \) and \( \epsilon = 2 \), then \( \delta(u) = 0, \delta(u-1) = \delta(u-2) = -1 \) and \( \delta(u-3) = \delta(u-4) = 0 \) (by Claim 5). Also, \( u \notin X_2 \) by assumption, \( u-1 \notin X_2 \) (else \( \Lambda'(u-1) = \Lambda(u-1) \geq 2 \) implying \( -1 = \delta(u-1) > \delta(u-2) = -1 \), which is not possible) and \( u-2 \notin X_2 \) (as \( \Lambda(u-2) = 0 \)). Consequently, since the difference between consecutive elements in \( X_2 \) is either \( d = 3 \) or \( d+1 = 4 \), we conclude that
u + 1, u − 3 ∈ \(X_2\). Since \(\Lambda(u - 2) = 0\), we also have \(u - 3 ∈ X_1\), whence \(\Lambda' (u - 3) = \Lambda (u - 3) ≥ 2\), implying \(0 = \delta(u - 3) > \delta(u - 4)\), contradicting that \(\delta(u - 4) = 0\).

If \(± = +\) and \(e = 1\), then \(\delta(u) = 1, \Lambda(u + 1) = 0\) and \(\delta(u + 1) = 0\). Thus \(u + 1 \in X_1\), implying \(u + 2, u + 3, u, u - 1 \in X_1\). Moreover, \(1 = \delta(u) = \delta(u - 1) + \Lambda'(u - 1) = \delta(u - 1) + \Lambda(u) - 1 = \delta(u - 1) + 1\), implying that \(\delta(u - 1) = 0\). We have \(u \not∈ X_2\) and \(u + 1 \not∈ X_2\) (by assumption). Consequently, since the difference between consecutive elements in \(X_2\) is \(d = 3\) or \(d + 1 = 4\), we conclude that either \(u + 2 \in X_2\) or \(u + 3 \in X_2\). If \(u + 2 \in X_2\), then \(\Lambda'(u + 2) = \Lambda(u + 2) ≥ 2\) and \(\Lambda(u + 3) ≥ 1\) (as \(u + 1, u + 2 ∈ X_1\) also holds), implying \(\delta(u + 3) ≥ \delta(u + 2) > \delta(u + 1) = 0\). Hence \(u + 3, u + 2\) and \(u\) must all be non-relatively prime to \(n\), which contradicts that \(n\) has only two prime divisors each at least 5.

Therefore we instead conclude that \(u + 3 ∈ X_2\) and \(u + 2 \not∈ X_2\). In this case, \(u + 2, u + 1, u \not∈ X_2\), forcing \(u - 1 \in X_1\). Since we also have \(u - 1 \in X_1\), it follows that \(\Lambda'(u - 1) = \Lambda(u - 1) ≥ 2\), implying \(0 = \delta(u - 1) > \delta(u - 2)\). Since \(u + 3 ∈ X_2\) and \(u + 3 ∈ X_1\), we have \(\Lambda'(u + 3) = \Lambda(u + 3) ≥ 2\), implying \(\delta(u + 3) > \delta(u + 2) ≥ \delta(u + 1) = 0\) (where \(\delta(u + 2) ≥ \delta(u + 1)\) follows in view of \(u + 2 ∈ X_1\)). But now \(u - 2, u - 3\) and \(u - 1\) are all non-relatively prime to \(n\). As \(n\) has only two prime divisors, each at least 5, this is only possible if \(ω = 2\) and \(p = 5\) with \(u - 2\) and \(u + 3\) congruent to 0 modulo 5 and \(u\) congruent to 0 modulo \(q\). It remains to show \(x_3 ≥ 4\) in this case, so assume instead that \(κ = 1\) and \(x_3 ∈ \{2, 3\}\), so that \(X_3 = \{\frac{n + 1}{3}, \frac{2n + 2}{3}\} or \{\frac{2n + 2}{3}, \frac{2n + 1}{3}\}\). However, none of the possible elements of these potential sets is congruent to zero modulo \(q ≥ 7\), contradicting what we just established. Therefore we must have \(x_3 ≥ 4\) in this case, as desired.

If \(± = -\) and \(e = 1\), then \(\delta(u) = 0, \Lambda(u - 1) = 0\) and \(\delta(u - 1) = -1\). Thus \(u - 1 \in X_1\), implying \(u, u + 1, u - 2, u - 3 \in X_1\). Moreover, \(-1 = \delta(u - 1) = \delta(u - 2) + \Lambda'(u - 1) = \delta(u - 2) + \Lambda(u) - 1 = \delta(u - 2) - 1\), implying that \(\delta(u - 2) = 0\). We have \(u \not∈ X_2\) (by assumption) and \(u - 1 \not∈ X_2\) (as \(\Lambda(u - 1) = 0\)). Consequently, since the difference between consecutive elements in \(X_2\) is \(d = 3\) or \(d + 1 = 4\), we conclude that either \(u - 2 \in X_2\) or \(u - 3 \in X_2\). If \(u - 2 \in X_2\), then \(\Lambda'(u - 2) = \Lambda(u - 2) ≥ 2\) and \(\Lambda(u - 3) ≥ 1\) (as \(u - 2, u - 3 \in X_1\) also holds), implying \(0 = \delta(u - 2) > \delta(u - 3) ≥ \delta(u - 4)\). Hence \(u - 4, u - 3\) and \(u - 1\) must all be non-relatively prime to \(n\), which contradicts that \(n\) has only two prime divisors each at least 5.

Therefore we instead conclude that \(u - 3 ∈ X_2\) and \(u - 2 \not∈ X_2\). In this case, \(u - 2, u - 1, u \not∈ X_2\), forcing \(u + 1 \in X_1\). Since we also have \(u + 1 \in X_1\), it follows that \(\Lambda'(u + 1) = \Lambda(u + 1) ≥ 2\), implying \(\delta(u + 1) > \delta(u) = 0\). Since \(u - 3 ∈ X_2\) and \(u - 3 ∈ X_1\), we have \(\Lambda'(u - 3) = \Lambda(u - 3) ≥ 2\), implying \(0 = \delta(u - 2) ≥ \delta(u - 3) > \delta(u - 4)\) (where \(\delta(u - 2) ≥ \delta(u - 3)\) follows in view of \(u - 2 ∈ X_1\)). But now \(u - 4, u - 1\) and \(u + 1\) are all non-relatively prime to \(n\). As \(n\) has only two prime divisors, each at least 5, this is only possible if \(ω = 2\) and \(p = 5\) with \(u - 4\) and \(u + 1\) congruent to 0 modulo 5 and \(u - 1\) congruent to 0 modulo \(q\). It remains to show \(x_3 ≥ 4\) in this case, so assume instead that \(κ = 1\) and \(x_3 ∈ \{2, 3\}\), so that \(X_3 = \{\frac{n + 1}{3}, \frac{2n + 2}{3}\} or \{\frac{2n + 2}{3}, \frac{2n + 1}{3}\}\). However, none of the possible elements from \(X_3\) are congruent to 1 modulo \(q ≥ 7\) (as \(ω = 2\)), contradicting what we just established for \(u\). Therefore we must have \(x_3 ≥ 4\) in this case, as desired. So we may now instead assume \(u \not∈ X_2\) and \(u \not∈ X_1\).

In this case, we have \(u ∈ X_1\) so that \(u + 1, u + 2, u - 1, u - 2 ∈ X_1\). Thus \(\Lambda(v) ≥ 1\) for all \(v ∈ \{u - 2, u + 2\}\) (as \(v ∈ X_3\)). Consequently, if \(\delta(u) = 1\), then \(1 = \delta(u) ≤ \delta(u + 1) ≤ \delta(u + 2)\), contrary to Claim 5. On the other hand, if \(\delta(u - 1)\), then \(-1 = \delta(u) ≥ \delta(u - 1) ≥ \delta(u - 2) ≥ \delta(u - 3)\), also contrary to Claim 5. Therefore \(\delta(u) = 0\). The latter argument also shows that \(\delta(u - 1) = 0\).
Suppose $u + 1, u - 1 \notin X_2$. Then, since the difference between consecutive elements in $X_2$ is either $d = 3$ or $d + 1 = 4$, we conclude that $u + 2, u - 2 \in X_2$. But then $\Lambda'(u + 2) = \Lambda(u + 2) \geq 2$ and $\Lambda'(u - 2) = \Lambda(u - 2) \geq 2$ (as $u + 2, u - 2 \in X_1$), implying $\delta(u + 2) > \delta(u + 1) \geq \delta(u) = 0$ and $0 = \delta(u - 1) \geq \delta(u - 2) > \delta(u - 3)$. Thus $u - 3$ and $u + 2$ are both non-relatively prime to $n$. If $5 \mid n$, then this implies $u - 3$ and $u + 2$ are congruent to 0 modulo 5, as desired. If $5 \nmid n$, then $\omega = 2$ and $p$ must divide one of $u - 3$ or $u + 2$ with $q$ dividing the other, also as desired. It remains to show $x_3 \geq 4$ in these cases as well, so assume instead that $\kappa = 1$ and $x_3 \in \{2, 3\}$, so that $X_3 = \{\frac{n+1}{2}\}$ or $\{\frac{n+1}{3}, \frac{2n+2}{3}\}$ or $\{\frac{n+1}{3}, \frac{2n+1}{3}\}$. If $5 \nmid n$, then $q \geq 11$ but none of the possible elements from $X_3$ are congruent to either 3 or -2 modulo $q$, contrary to what we just established. On the other hand, if $p = 5$, then neither $\frac{n+1}{3}, \frac{n+2}{3}, \frac{2n+1}{3}$ nor $\frac{n+2}{3}$ is congruent to 3 modulo $p = 5$, contrary to what was established. So we must have $x_3 = 2$ with $X_3 = \{\frac{n+1}{2}\}$. Thus $u = \frac{n+1}{2}$ is the unique element from $X_3$. Let $b_j = u - 2 \in X_2$.

If $I_{(j)+1}$ is long, then $u + 3 \in X_1, u + 4 \in X'_1$ and $u + 5, u + 6 \in X_1$. Moreover, as the difference of consecutive elements in $X_2$ is either 3 or 4, we have $b_{j+2} = u + 5$ or $u + 6$. In either case, $\Lambda(b_{j+2}) = 2$ and $\delta(b_{j+2}) = 1$. Now $\Lambda(u + 3) = 1$ ensures that $\delta(u + 3) = \delta(u + 2) = 1$, so we must have $\omega = 2$ with $u + 3 = \frac{n+2}{3}$ non-relatively prime to $n$, which forces $q = 7$. Since $q = 7$ divides $u + 3$ and $p = 5$ divides $u + 2$, it follows that the integers in $[u + 4, u + 6]$ are all relatively prime to $n$. But this contradicts that $\delta(b_{j+2}) = 1$ with $b_{j+2} \in \{u + 5, u + 6\}$. Therefore we instead conclude that $I_{(j)+1}$ is short, meaning $u + 1, u + 2, u + 4, u + 5 \in X_1$ and $u + 3 \in X'_1$.

If $I_{(j)}$ is long, then $u - 4 \in X'_1$ will be the element of $X'_1$ preceding $u = \frac{n+1}{2} \in X'_1$, in which case $u - 1, u - 2, u - 3, u - 5, u - 6 \in X_1$. Since $\delta(u - 3) = -1$ with $u - 3 \in X_1$, we also have $\delta(u - 4) = -1$, implying that $u - 4 = \frac{n+2}{2}$ is non-relatively prime to $n$. Hence $q = 7$ with $7$ dividing $u - 4$ and $p = 5$ dividing $u - 3$. It follows that the integers in $[u - 7, u - 5]$ must all be relatively prime to $n$, and thus each have $\delta$ value 0. Now, $b_{j-1}$ will either equal $b_3 - 3 = u - 5$ or $b_3 - 4 = u - 6$. In either case, $\Lambda(b_{j-1}) = 2$, ensuring that $\delta(b_{j-1}) > \delta(b_{j-1} - 1)$, which contradicts that $b_{j-1} \in \{u - 5, u - 6\}$ with $\delta(v) = 0$ for all $v \in [u - 7, u - 5]$. Therefore we instead conclude that $I_{(j)}$ is short, meaning $u - 1, u - 2, u - 4, u - 5 \in X_1$ and $u + 3 \in X'_1$.

If $I_{(j)+2}$ and $I_{(j)-1}$ are both long, then $u + 5, u + 6, u - 5, u - 6 \in X_1$. If $b_{j+2} = b_{j+1} + 3 = u + 5$, then $\Lambda(u + 5) = 2$ and $\Lambda(u + 6) = 1$, implying $\delta(u + 5) = \delta(u + 6) = 1$. Thus $u + 5 = \frac{n+11}{2}$ and $u + 6 = \frac{n+13}{2}$ must both be non-relatively prime to $n$, forcing 11 and 13 to divide $n$. Since 5 also divides $n$, this contradicts that $n$ has at most 2 distinct prime divisors. Therefore we instead conclude that $b_{j+2} = b_{j+1} + 4 = u + 6$. Additionally, $\Lambda(u + 6) = 2$ forcing $\delta(u + 6) = 1$, so that $u + 6 = \frac{n+13}{2}$ must be non-relatively prime to $n$, implying $q = 13$. Likewise, if $b_{j-1} = b_{j-2} = u - 5$, then $\Lambda(u - 5) = 2$ and $\Lambda(u - 6) = 1$, implying $\delta(u - 6) = \delta(u - 7) = -1$. Thus $u - 6 = \frac{n-11}{2}$ and $u - 7 = \frac{n-13}{2}$ must both be non-relatively prime to $n$, forcing 11 and 13 to divide $n$. Since 5 also divides $n$, this contradicts that $n$ has at most 2 distinct prime divisors. Therefore we instead conclude that $b_{j-1} = b_j - 4 = u - 6$. Since we also have $b_{j+1} = b_j + 4$, Lemma 2.4.6 implies that $x_2 < \frac{n}{\frac{n+1}{2}} = \frac{3}{4}n$. Since $I_{(j)}$ and $I_{(j)+1}$ are both short, Lemma 2.4.6 also implies that $x'_1 > \frac{n}{\frac{n+1}{2}} = \frac{2}{3}n$, whence $x_1 = n - x'_1 < \frac{5}{7}n$. Hence $n - 1 = n + 1 - x_3 = x_2 + x_1 < \frac{3}{4}n + \frac{5}{7}n = \frac{26}{21}n$, implying $n < 77$. As 5 and 13 both divide $n$, this is only possible if $n = 65$. In this case, we have $x_2 \leq \lfloor \frac{3}{11}n \rfloor = 17$, while $3 = d = d_2 = \lfloor \frac{n}{17} \rfloor - 1$ implies $\frac{n}{x_2} \leq 4$, and thus $x_2 \geq \lfloor \frac{n}{4} \rfloor = 17$. Hence $x_3 = 2, x_2 = 17$ and $x_1 = 47$ with $n = 65$. However, letting
Since $u+5 = \frac{n+11}{2}$ must be non-relatively prime to $n$, forcing $q = 11$, while $u+8 = \frac{n+17}{2}$ must also be non-relatively prime, forcing $q = 17$. Since $q$ cannot both be 11 and 17, we obtain a contradiction. Therefore we may assume either $b_{j+2} > b_{j+1} + 3$ or $b_{j+3} > b_{j+2} + 3$. In either case, it follows that $b_{j+3} \geq u + 9$. Since $b_j = u - 2$, we now have $11 \leq b_{j+3} - b_j = \left\lfloor \frac{(j+3)n}{x_2} \right\rfloor - \left\lfloor \frac{jn}{x_2} \right\rfloor < \frac{3n}{x_2} + 1$, implying $x_2 < \frac{3n}{10}$.

If $b_{j+2} > b_{j+1} + 3$, then we have $b_{j+2} = b_{j+1} + 4 = u + 6$, so that $8 \leq b_{j+2} - b_j = \left\lfloor \frac{(j+2)n}{x_2} \right\rfloor - \left\lfloor \frac{jn}{x_2} \right\rfloor < \frac{2n}{x_2} + 1$, implying $x_2 < \frac{3n}{10}$. Thus, as the argument of previous paragraph shows, we must have $x_2 < \frac{3n}{10}$ unless $b_{j+2} = b_{j+1} + 3 = u + 5 = \frac{n+11}{2}$ is non-relatively prime to $n$ with $\delta(b_{j+1}) = 1$ and $q = 11$.

The above work shows that $n - 1 = n - x_3 + 1 = x_1 + x_2 < \frac{7n}{10} + \frac{3}{10}n = n$. Thus, in order to avoid a contradiction, we must have $x_1 = \left\lfloor \frac{7n}{10} \right\rfloor = \frac{7n-5}{10}$ and $x_2 = \left\lfloor \frac{3n}{10} \right\rfloor = \frac{3n-5}{10}$ (since $n \equiv 5 \pmod{10}$) in view of $n$ being odd with $5 | n$. Since $x_2 = \frac{3n-5}{10} \geq \frac{3}{7}n$, it follows as noted above that $q = 11$.

We must have $n \equiv 5 \pmod{15}$ or $15$ modulo $20$. If $n \equiv 5 \pmod{20}$, then let $u = \frac{n+1}{2}$ and observe that $ux_2 = \frac{n(3n-5)+3n-5}{20}$ and $ux_1 = \frac{n(7n-5)+7n-5}{20}$, so that $(ux_1)n + (ux_2)n + (x_3)n = \frac{7n-5}{20} + \frac{3n-5}{20} + 1 < n$. Thus the theorem holds for this sequence. On the other hand, if $n \equiv 5 \pmod{20}$, then let $u = \frac{n+13}{2}$ and observe that $ux_2 = \frac{n(3n+25)+9n-65}{20}$ and $ux_1 = \frac{n(7n+85)+n-65}{20}$, so that, provided $n \geq 65$, we have $(ux_1)n + (ux_2)n + (x_3)n = \frac{n-65}{20} + \frac{9n-65}{20} + 13 < n$, showing the theorem holds for the sequence $S$ when $n \geq 65$. However, as 5 and 11 divide $n$ with $n \equiv 5 \pmod{20}$, it follow that $n \geq 65$ does hold, completing this case. So we may now assume that either $u+1 \in X_2$ or $u-1 \in X_2$.

Suppose $b_{j+1} = u + 1 \in X_2$. Then $\Lambda'(u+1) = \Lambda(u+1) \geq 2$ (as $u+1 \in X_1$ also), whence $0 = \delta(u) < \delta(u+1) \leq \delta(u+2)$ (with $\delta(u+2) \geq \delta(u+1)$) in view of $u+2 \in X_1$. We must have $\Lambda(u+3) = 0$, else $\delta(u+3) \geq \delta(u+2) = 1$ follows, contrary to Claim 5. Hence $u+3 \in X'_1$ implying $u+4, u+5 \in X_1$. Since $\delta(u+1) = \delta(u+2) = 1$ with $n$ divisible by at most two prime divisors, each at least 5, it follows that $\delta(u+3) = \delta(u+4) = \delta(u+5) = 0$. Since the difference of consecutive elements in $X_2$ is 3 or 4, we have $b_{j+2} = u+1+3 = u+4$ or $u+1+4 = u+5$. Hence $\Lambda(b_{j+2}) = 2$, whence $\delta(b_{j+2}) = 1$ follows provided $b_{j+2} \notin X_4$. Since $\delta(u+4) = \delta(u+5) = 0$ with $b_{j+2} \in \{u+4, u+5\}$, we conclude that $b_{j+2} \notin X_4$, which is only possible in view of $\delta(u+2) = 1$ and (13) if $\kappa = 2$ and $b_{j+2} = u+5 = \frac{3n+1}{2}$ with $u+1 = \frac{n-7}{2}$ and $u+2 = \frac{n-5}{2}$ both non-relatively prime to $n$, forcing $p = 5$ and $q = 7$ with $\omega = 2$. Hence $u$ is congruent to 3 modulo 5, as desired. Moreover, $x_3 \geq 5$ by Claim 3 since $\kappa = 2$. So we now conclude that $u+1 \notin X_2$ and $b_j = u-1 \in X_2$.

Since $u-1 \in X_2$ and $u-1 \in X_1$, ensuring $\Lambda'(u-1) = \Lambda(u-1) \geq 2$, we have $0 = \delta(u-1) > \delta(u-2) \geq \delta(u-3)$ (with $\delta(u-2) \geq \delta(u-3)$ in view of $u-2 \in X_1$). We must have $\Lambda'(u-3) = \Lambda(u-3) = 0$, else $-1 = \delta(u-3) \geq \delta(u-4)$ follows, contrary to Claim 5. Hence $u-3 \in X'_1$ implying $u-4, u-5 \in X_1$. Since $\delta(u-2) = \delta(u-3) = 1$ with $n$ divisible by at most two prime divisors, each at least 5, it follows that $\delta(u-4) = \delta(u-5) = \delta(u-6) = 0$. Since the difference of consecutive elements in $X_2$ is 3 or 4, we have $b_{j-1} = u-1-3 = u-4$ or $u-1-4 = u-5$. Hence $\Lambda(b_{j-1}) = 2$, whence $\delta(b_{j-1} - 1) = -1$.
follows provided \( b_{j-1} \notin X_4 \). Since \( \delta(u-5) = \delta(u-6) = 0 \) with \( b_{j-1} - 1 \in \{u-5, u-6\} \), we conclude that \( b_{j-1} \in X_4 \), which is only possible in view of \( \delta(u-3) = 1 \) and (13) if \( \kappa = 2 \) and \( b_{j-1} = u-5 = \frac{n+1}{2} \) with \( u-2 = \frac{n+7}{2} \) and \( u-3 = \frac{n+5}{2} \) both non-relatively prime to \( n \), forcing \( p = 5 \) and \( q = 7 \) with \( \omega = 2 \). Hence \( u \) is congruent to 3 modulo 5, as desired. Moreover, \( x_3 \geq 5 \) by Claim 3 since \( \kappa = 2 \), completing the proof of Subclaim B.1.

If \( \kappa = 1 \), then Subclaim B.1 ensures that \( |X_3| = x_3 - 1 \geq 3 \), so that the first three elements of \( X_3 \) satisfy one of the congruences condition from Subclaim B.1. If \( \kappa = 2 \), then \( \omega = 2 \), \( n \geq 35 \) and Claim 3 implies that \( |X_3| = x_3 - 1 \geq 4 \) with \( x_3 \neq 6 \). Thus, since \( \left\lfloor \frac{2n}{x_3} \right\rfloor < \frac{n-5}{2} \) (in view of \( x_3 \geq 5 \) and \( n \geq 35 \)), we see that the first two elements of \( X_3 \) must satisfy one of the congruence conditions from Subclaim B.1. If the third element of \( X_3 \) does not, then \( \frac{n-5}{2} < \left\lfloor \frac{3n}{x_3} \right\rfloor < \frac{n+7}{2} \). However, this would imply \( \frac{6n}{n+7} < x_3 < \frac{6n}{n-7} \); the first inequality is strict because \( \gcd(x_3, n) = 1 \) by hypothesis when \( \omega = 2 \). If \( x_3 = 5 \), then \( \frac{6n}{n+7} < x_3 = 5 \) implies \( n < 35 \), which is not possible for \( \omega = 2 \). If \( x_3 \geq 7 \), then \( 7 \leq x_3 < \frac{6n}{n+7} \) implies \( n < 49 \), so that \( n = 35 \). Moreover, if \( x_3 \geq 8 \), the previous calculation leads directly to contradiction, so we must also have \( x_3 = 7 \) in this case, contradicting that \( \gcd(x_3, n) = 1 \) for \( \omega = 2 \). So we see that, in all cases, the first three elements of \( X_3 \) satisfy one of the congruence conditions given in Subclaim B.1. If, for \( \kappa = 2 \), the fourth element of \( X_3 \) does not satisfy one of the congruence conditions from Subclaim B.1, then \( \frac{2n}{x_3} \leq \left\lfloor \frac{4n}{x_3} \right\rfloor < \frac{n+7}{2} \), implying \( \frac{8n}{n+7} < x_3 < \frac{8n}{n-7} \). If \( x_3 = 5 \), then \( \frac{8n}{n+7} < x_3 = 5 \) implies \( 3n < 35 \), contradicting that \( n \geq 35 \). If \( x_3 = 7 \), then \( \frac{8n}{n+7} < x_3 = 7 \) implies \( n < 49 \), forcing \( n = 35 \). But this contradicts that \( \gcd(x_3, n) = 1 \) for \( \omega = 2 \). If \( x_3 = 9 \), then \( 9 = x_3 < \frac{8n}{n+7} \) implies \( n < 63 \), forcing \( n = 35 \) or \( 55 \). If \( x_3 \geq 10 \), then \( 10 \leq x_3 < \frac{8n}{n+7} \), implies \( n < 35 \), which is not possible. In summary, if \( \kappa = 2 \) and the fourth element of \( X_3 \) fails to satisfy one of the congruence conditions from Subclaim B.1, then we must have \( x_3 = 8 \) or \( x_3 = 9 \), with the latter only possible when \( n = 35 \) or \( 55 \).

Suppose \( 5 \nmid n \). Then, in view of Subclaim B.1 and the previous paragraph, \( c_1, c_2 \) and \( c_3 \) are each congruent to some element from \( \{3, -2\} \) modulo \( p \geq 7 \). Since \( c_1 = d_3 + 1 \), this implies \( d_3 \) is congruent to some element from \( \{2, -3\} \) modulo \( p \). If \( d_3 \equiv 2 \) (mod \( p \)), then \( c_1 \equiv 3 \) and \( c_2 \equiv 5 \) or \( 6 \) modulo \( p \), which is only possible if \( c_2 \equiv 5 \) (mod \( p \)) with \( p = 7 \). But then \( c_2 \equiv 0 \) or \( 1 \) modulo \( p = 7 \), neither of which is equal to \( 3 \) or \( -2 \) modulo \( 7 \). On the other hand, if \( d_3 \equiv -3 \) (mod \( p \)), then \( c_1 \equiv -2 \) (mod \( p \)) and \( c_2 \equiv -5 \) or \( -4 \) modulo \( p \), which is only possible if \( c_2 \equiv -4 \) (mod \( p \)) with \( p = 7 \). But then \( c_3 \equiv 0 \) or \( 1 \) modulo \( p = 7 \), neither of which is congruent to \( 3 \) or \( -2 \) modulo \( p = 7 \). So it remains to consider the case when \( p = 5 \mid n \).

In this case, Subclaim B.1 implies that \( c_1, c_2 \) and \( c_3 \) are each either congruent to \( 2 \) modulo \( 5 \) and \( 0 \) modulo \( q \) or congruent to \( 4 \) modulo \( 5 \) and \( 1 \) modulo \( q \) or congruent to \( 3 \) modulo \( 5 \), with the first two possibilities only possible if \( \omega = 2 \), i.e., if \( q \mid n \). Since \( c_1 = d_3 + 1 \), this means \( d_3 \) is either congruent to \( 1 \) modulo \( 5 \) and \( -1 \) modulo \( q \) or is congruent to \( 3 \) modulo \( 5 \) and \( 0 \) modulo \( q \) or is congruent to \( 2 \) modulo \( 5 \), with the first two possibilities only possible if \( \omega = 2 \).

If \( d_3 \equiv 2 \) (mod \( 5 \)), then \( c_1 \equiv 3 \) (mod \( 5 \)) and \( c_2 \equiv 0 \) or \( 1 \) modulo \( 5 \), neither of which is congruent to \( 4, 2 \) or \( 3 \) modulo \( 5 \). Therefore we must have \( \omega = 2 \).

If \( d_3 \equiv 3 \) (mod \( 5 \)) and \( d_3 \equiv 0 \) (mod \( q \)), then \( c_1 \equiv 4 \) (mod \( 5 \)), \( c_2 \equiv 2 \) or \( 3 \) modulo \( 5 \), and \( c_3 \equiv 0, 1 \) or \( 2 \) modulo \( 5 \). Thus we must have \( c_3 = c_2 + d_3 + 1 \equiv 2 \) (mod \( 5 \)) and \( c_2 = c_1 + d_3 + 1 \equiv 3 \) (mod \( 5 \)). If \( |X_3| \geq 4 \), then we must also have \( c_4 \equiv 0 \) or \( 1 \) modulo \( 5 \). If \( \kappa = 1 \) and \( |X_3| \geq 4 \), then \( c_4 \) must
satisfy one of the congruence conditions from Subclaim B.1, implying $c_4$ is congruent to 2, 3 or 4 modulo 5, contrary to what was just noted. If $\kappa = 1$ and $|X_3| = 3$, then $c_3 = \max X_3 = n - d_3$ (in view of Lemma 2.4.3 and \(\gcd(x_3,n) = 1\) when $\omega = 2$), with $c_3 \equiv -d_3 \equiv 0 \pmod{q}$. But $c_3 = c_2 + d_3 + 1 = c_1 + 2d_3 + 2 = 3d_3 + 3 \equiv 3 \pmod{q}$, which contradicts that $q > 4$. If $\kappa = 2$ and the fourth element of $X_3$ satisfies one of the congruence conditions from Subclaim B.1, then we obtain a contradiction as before. Therefore we must have $x_3 = 8$ or $x_3 = 9$, with the latter only possible if $n = 35$ or $n = 55$. However, if $x_3 = 9$ and $n = 35$, then $d_3 = \lceil \frac{n}{9} \rceil - 1 = 3$, and if $x_3 = 9$ and $n = 55$, then $d_3 = \lceil \frac{n}{9} \rceil - 1 = 6$, neither of which is congruent to 0 modulo $q \geq 7$. On the other hand, if $x_3 = 8$, then $c_4 = \frac{n+1}{2}$, which is not congruent to 0 or 1 modulo 5, contrary to what we showed above.

If $d_3 \equiv 1 \pmod{5}$ and $d_3 \equiv -1 \pmod{q}$, then $c_1 \equiv 2 \pmod{5}$, $c_2 \equiv 3$ or 4 modulo 5, and $c_3 \equiv 4, 0$ or 1 modulo 5. Thus we must have $c_3 = c_2 + d_3 \equiv 4 \pmod{5}$ and $c_2 = c_1 + d_3 \equiv 3 \pmod{5}$. If $|X_3| \geq 4$, then we must also have $c_4 \equiv 0$ or 1 modulo 5. If $\kappa = 1$ and $|X_3| \geq 4$, then $c_4$ must satisfy one of the congruence conditions from Subclaim B.1, implying $c_4$ is congruent to 2, 3 or 4 modulo 5, contrary to what was just noted. If $\kappa = 1$ and $|X_3| = 3$, then $c_3 = \max X_3 = n - d_3$ (in view of Lemma 2.4.3 and \(\gcd(x_3,n) = 1\) when $\omega = 2$), with $c_3 \equiv -d_3 \equiv 1 \pmod{q}$. But $c_3 = c_2 + d_3 = c_1 + 2d_3 = 3d_3 + 1 \equiv -2 \pmod{q}$, which contradicts $q > 3$. If $\kappa = 2$ and the fourth element of $X_3$ satisfies one of the congruence conditions from Subclaim B.1, then we obtain a contradiction as before. Therefore $x_3 = 8$ or $x_3 = 9$, with the latter only possible if $n = 35$ or $n = 55$. However, if $x_3 = 9$ and $n = 35$, then $d_3 = \lceil \frac{n}{9} \rceil - 1 = 3$, which is not congruent to 1 modulo 5, and if $x_3 = 9$ and $n = 55$, then $d_3 = \lceil \frac{n}{9} \rceil - 1 = 6$, which is not congruent to $-1$ modulo $q = 11$. On the other hand, if $x_3 = 8$, then $c_4 = \frac{n+1}{2}$, which is not congruent to 0 or 1 modulo 5, contrary to what we showed above, completing Case B.

**Case C.** $d = 2$ and $x_3 \leq 3$.

**Proof.** If $\kappa = 2$, then Claim 3 gives $x_3 \geq 5$, so we may assume $\kappa = 1$. Since $2 = d = d_2 = \lceil \frac{n}{x_2} \rceil - 1 = \lceil \frac{n}{x_3} \rceil - 1$, we have $\frac{n}{3} < x_2 < \frac{n}{2}$ and $\frac{n}{2} < x_1 = n - x'_1 < 2n/3$.

Suppose $x_3 = 2$. Then $x_2 = \frac{n+1}{2} - x$ and $x_1 = \frac{x_2}{2} + x$ for some integer $x \in [1, \frac{n-4}{6}]$. If $n + 2x \equiv 1 \pmod{4}$, then let $u = \frac{n+1}{2}$ and observe that $ux_2 = \frac{n(n-2x-1)+n-1-2x}{4}$ and $ux_1 = \frac{n(n-2x+1)+n-1+2x}{4}$, whence $(ux_1)_n + (ux_2)_n + (ux_3)_n = \frac{n+2}{4} + \frac{n+2}{4} + 1 = \frac{n+1}{2} < n$, showing that the theorem holds for $S$. On the other hand, if $n + 2x \equiv -1 \pmod{4}$, then let $u = \frac{n+3}{2}$ and observe that $ux_2 = \frac{n(n-2x+1)+n-3-6x}{4}$ and $ux_1 = \frac{n(n+2x+1)+n-3+6x}{4}$, whence $(ux_1)_n + (ux_2)_n + (ux_3)_n = \frac{n+3}{4} + \frac{n+3}{4} < n$, showing that the theorem holds for $S$. So instead assume that $x_3 = 3$, implying that $X_3 = \{ \frac{n+2}{2}, \frac{2n+2}{3} \}$ or $X_3 = \{ \frac{n+2}{3}, \frac{2n+2}{3} \}$.

Let $u \in X_3$ be the element $u = \frac{cn+2}{3}$, where $c \in \{1, 2\}$. Then $u = \frac{cn+2}{3}$, $u - 1 = \frac{cn-1}{3}$ and $u - 2 = \frac{cn-4}{3}$, implying \(\gcd(v,n) = 1\) for $v \in [u-2, u]$, whence $\delta(v) = 0$ for $v \in [u-2, u]$. If $\Lambda(u) \geq 2$, then $\delta(u-1) < \delta(u)$, contradicting that $\delta(u-1) = \delta(u) = 0$. Therefore $\Lambda(u) = 1$, implying $u - 1, u + 1 \subseteq X_1$. Hence, if $u - 1 \notin X_2$, then $\Lambda(u-1) > 2$, implying $\delta(u-2) < \delta(u-1)$, contradicting that $\delta(u-2) = \delta(u-1) = 0$. Therefore $u - 1 \notin X_2$, implying $u - 2, u + 1 \subseteq X_2$ (as the difference between consecutive elements in $X_2$ is either $d_2 = 2$ or $d_2 = 1$). Thus $u - 3, u + 2 \notin X_2$ and $\Lambda(u+1) \geq 2$, implying $\delta(u+1) > \delta(u) = 0$, so that $\delta(u+1) = 1$. Thus $\gcd(u+1, n) \neq 1$, which in view of $u + 1 = \frac{cn+2}{3}$, forces $p = 5$ and thus also $n \geq 25$ (as $n \geq 11$ by Claim 3). Since $u + 2 = \frac{cn+4}{3}$ is relatively prime to $n$, we have $\delta(u+2) = 0$. Hence, since $\delta(u+1) = 1$, we conclude that $\Lambda(u+2) = 0$, implying $u + 3 \in X_1$. 


Suppose $u + 3 \in X_2$. Then $\Lambda(u + 3) \geq 2$, implying $\delta(u + 3) > \delta(u + 2) = 0$. Thus $\delta(u + 3) = 1$, implying $q = 11$ and $\omega = 2$ since $u + 3 = \frac{\omega + 1}{3}$. Hence

$$\delta(v) = 0 \quad \text{for all } v \in [u - 7, u + 10] \setminus \{u - 4, u + 1, u + 6, u + 3\}.$$ 

Since $\delta(u + 4) = 0$ and $\delta(u + 3) = 1$, we must have $\Lambda(u + 4) = 0$. Since $\delta(u - 3) = 0$ and $u - 2 \notin X_2$, we have $u - 2 \notin X_1$, whence $u - 3 \in X_1$ and $u - 3 \notin X_2$. Moreover, $u - 3 \notin X_3$ since $\frac{2u + 2}{2} - 3 > \frac{u + 5}{3}$. Thus, $\delta(u - 4) = \delta(u - 3) = 0$. Consequently, since $\delta(u - 5) = 0$, we must have $\Lambda(u - 4) = 1$, meaning either $u - 4 \notin X_2$ or $u - 4 \notin X_1$. Since $\Lambda(u + 4) = 0$, we have $u + 5 \in X_1$. Hence, since $\delta(u + 5) = 0$ and $\delta(u + 4) = 0$, we must have $u + 5 \notin X_2$, implying $u + 6 \in X_2$ (as the difference between consecutive elements in $X_2$ is 2 or 3). Summarizing what we know, we have $X_2 \cap [u - 3, u + 6] = \{u - 2, u + 1, u + 3, u + 6\}$, $X_1' \cap [u - 3, u + 5] = \{u - 2, u, u + 2, u + 4\}$ and either $u - 4 \notin X_2$ or $u - 4 \notin X_1$.

If $u - 4 \notin X_2$, then $u - 5 \in X_2$ so that $u - 5, u - 2$ and $u + 1$ are consecutive elements of $X_2$ with the difference $d_2 + 1 = 3$ occurring twice in a row. Thus Lemma 2.4.6 implies that $x_2 < \frac{n}{3^{1/2}} = \frac{2}{5} n$. Since $X_1' \cap [u - 3, u + 5] = \{u - 2, u, u + 2, u + 4\}$, we see that there are three short intervals in a row in $X_1'$, whence Lemma 2.4.6 implies that $n - x_1 = x_1' > \frac{n}{2^{1/3}} = \frac{2}{5} n$, so that $x_1 < \frac{3}{5} n$. Hence $n - 2 = x_1 + x_2 < \frac{2}{5} n + \frac{3}{5} n$, implying $n < 70$, which is only possible if $n = 55$ (as $p = 5$ and $q = 11$ with $\omega = 2$). In this case, $53 = n - 2 = x_1 + x_2 \leq \left[\frac{5n-1}{7}\right] + \left[\frac{4n-1}{5}\right] = 52$, which is a contradiction.

If $u - 4 \notin X_1$. Then there will be four short intervals in a row in $X_1'$, whence Lemma 2.4.6 implies that $n - x_1 = x_1' > \frac{2n}{2^{1/3}} = \frac{2}{5} n$, so that $x_1 < \frac{3}{5} n$. Since $X_2 \cap [u - 3, u + 6] = \{u - 2, u + 1, u + 3, u + 6\}$, we have $b_j = u - 2$ and $b_{j+3} = u + 6$ for some $j$, whence $8 = (u + 6) - (u - 2) = b_{j+3} - b_j < \frac{3n}{x_2} + 1$, implying $x_2 < \frac{3}{5} n$. Hence $n - 2 = x_1 + x_2 < \frac{2}{5} n + \frac{3}{5} n$, implying $n < 126$, forcing $n = 55$ (as $p = 5$ and $q = 11$ with $\omega = 2$). In this case, $53 = n - 2 = x_1 + x_2 \leq \left[\frac{5n-1}{7}\right] + \left[\frac{4n-1}{5}\right] = 30 + 23 = 53$, forcing $x_1 = 30$ and $x_2 = 23$. But then $\gcd(x_1, n) \neq 1$, contrary to hypothesis. So we instead conclude that $u + 3 \notin X_2$, whence $u + 4 \in X_2$ (as the difference between consecutive elements of $X_2$ is either 2 or 3) and $u + 5 \notin X_2$.

Suppose $u + 4 \notin X_1$. Then $u + 5 \in X_1$ and $u + 2$ and $u + 4$ are consecutive elements of $X_1'$, implying that there are two short intervals in a row in $X_1'$. Hence Lemma 2.4.6 implies that $n - x_1 = x_1' > \frac{n}{2^{1/2}} = \frac{2}{5} n$, so that $x_1 < \frac{3}{5} n$. If $u + 6 \notin X_2$, then $u - 2, u + 1, u + 4$ and $u + 7$ will be consecutive elements of $X_2$ with the difference $d_2 + 1$ occurring three times in a row, whence Lemma 2.4.6 implies that $x_2 < \frac{n}{3^{1/2}} = \frac{2}{5} n$. Hence $n - 2 = x_1 + x_2 \leq \left[\frac{3n-1}{5}\right] + \left[\frac{2n-1}{5}\right]$, implying $n \leq 35$ (recall that $p = 5$). Thus $n = 25$ or 35. If $n = 35$, then this calculation instead forces $x_1 = 20$ and $x_2 = 13$, contradicting that $\gcd(x_1, n) = 1$ for $\omega = 2$. If $n = 25$, then $x_1 = 14, x_2 = 9$ and $x_3 = 3$, so that $(9x_1)_n + (9x_2)_n + (9x_3)_n = 1 + 6 + 2 = 9$, implying the theorem holds for $S$. Therefore, we instead conclude that $u + 6 \in X_2$. The same argument also shows that $u - 4 \notin X_2$. Since we nonetheless have $u - 2, u + 1$ and $u + 4$ being consecutive elements of $X_2$, Lemma 2.4.6 gives $x_2 < \frac{n}{3^{1/2}} = \frac{2}{5} n$. We have $X_1' \cap [u - 1, u + 5] = \{u, u + 2, u + 4\}$.

If $u + 6 \in X_1'$ or $u - 2 \in X_1'$, then Lemma 2.4.6 gives $n - x_1 = x_1' > \frac{n}{2^{1/3}} = \frac{2}{5} n$. In this case, $n - 2 = x_1 + x_2 \leq \left[\frac{4n-1}{5}\right] + \left[\frac{2n-1}{5}\right]$, implying $n = 25$ (recall that $p = 5, \gcd(n, 6) = 1$ and $n \geq 25$), in which case $x_1 = 14, x_2 = 9$ and $x_3 = 3$, a case which we showed the theorem held for in the previous paragraph. Therefore, we must have $u + 6 \in X_1$ and $u - 2 \in X_1$ instead.
Since $\delta(u - 2) = 0$ and $u - 2 \in X_1 \cap X_2$, it follows that $\delta(u - 3) = -1$. Thus $u - 3 = \frac{cn-7}{3}$ is non-relatively prime to $n$, implying $\omega = 2$ and $q = 7$. As a result, $\delta(v) = 0$ for $v \in [u - 6, u - 5]$ (recall that $u + 1 \equiv 0 \pmod{5}$). Since $u - 2, u - 1 \in X_1$, we must have $u - 3 \notin X_1$ and $u - 4 \in X_1$. Since $u - 3 \notin X_2$ also, and as $\frac{2n+2}{3} - 3 > \frac{n+1}{3}$, it follows that $\Lambda(u - 3) = 0$, implying $\delta(u - 4) = \delta(u - 3) + 1 = 0$. Since $u - 4 \in X_2 \cap X_1$, it follows that $\delta(u - 5) < \delta(u - 4) = 0$, implying $\delta(u - 5) = -1$, contradicting that $\delta(v) = 0$ for $v \in [u - 6, u - 5]$. So we may now instead assume $u - 4 \in X_1$, whence $u + 5 \notin X_1$ (as $u + 3, u + 4 \in X_1$).

Since $\delta(u + 2) = 0$, $u + 3 \in X_1$ and $u + 4 \in X_1 \cap X_2$, we have $\Lambda(u + 3) \geq 1$ and $\Lambda(u + 4) \geq 2$, whence $\delta(u + 4) > \delta(u + 3) \geq \delta(u + 2) = 0$. Thus $\delta(u + 4) = 1$, implying $u + 4 = \frac{cn+14}{3}$ is non-relatively prime to $n$, implying $\omega = 2$ and $q = 7$. Thus $\delta(u + 5) = 0$, which together with $\delta(u + 4) = 1$ implies that $\Lambda(u + 5) = 0$. Hence $u + 5 \notin X_2$ and $u + 5 \notin X_1$, implying $u + 6 \in X_1$.

Suppose $u - 2 \in X_1'$, in which case $u - 3 \in X_1$. Since $u - 2, u$ and $u + 2$ are consecutive elements of $X_1'$ with difference $2 = d$, it follows from Lemma 2.4.6 that $n - x_1 = x_1' > \frac{n}{2+1/2}$, implying $x_1 < \frac{3}{8} n$. We also have $u - 2, u + 1$ and $u + 4$ as consecutive elements of $X_2$. If $u - 4 \notin X_2$, then $u - 5 \in X_2$ and the difference $3 = d_2 + 1$ will occur three times in a row in $X_2$, whence Lemma 2.4.6 implies that $x_2 < \frac{n}{3-1/3} = \frac{3}{8} n$, in which case $n - 2 = x_1 + x_2 < \frac{3}{8} n + \frac{3}{8} n$, implying $n < 80$, so that $n = 35$ (in view of $p = 5, q = 7$ and $\omega = 2$). But then $33 = n - 2 \leq \left\lfloor \frac{3n-1}{5} \right\rfloor + \left\lfloor \frac{2n-1}{5} \right\rfloor = 20 + 13$, forcing $x_1 = 20$ and $x_2 = 13$, which contradicts that $\gcd(x_1, n) = 1$ for $\omega = 2$. Therefore, we must have $u - 4 \notin X_2$, whence $u - 5 \notin X_2$. If $u - 4 \notin X_1$, then $u - 4, u - 2, u$ and $u + 2$ will be consecutive elements of $X_1'$, whence Lemma 2.4.6 implies $x_1 < \frac{3}{8} n$. Since $u - 2, u + 1$ and $u + 4$ are consecutive elements of $X_2$, Lemma 2.4.6 gives $x_2 < \frac{n}{3-1/7} = \frac{3}{8} n$, whence $n - 2 = x_1 + x_2 \leq \left\lfloor \frac{4n-1}{7} \right\rfloor + \left\lfloor \frac{2n-1}{5} \right\rfloor$, which is not possible for $p = 5, q = 7$ and $\omega = 2$. Therefore we must have $u - 4 \in X_1$ too. But now $u - 4 \in X_1 \cap X_2$, whence $\delta(u - 4) > \delta(u - 5) = 0$ (since $u - 5 = \frac{cn-13}{2}$ with $p = 5$ and $q = 7$, we must have $\gcd(u - 5, n) = 1$). Thus $\delta(u - 4) = 1$. But since $u - 3 \in X_1$ and $u - 2 \in X_2$, implying $\Lambda(u - 3), \Lambda(u - 2) \geq 1$, we have $\delta(u - 2) \geq \delta(u - 3) \geq \delta(u - 4) = 1$, contradicting that $\delta(u - 2) = 0$ as already established. So we instead conclude that $u - 2 \in X_1$.

Since $u - 1, u - 2 \in X_1$, it follows that $u - 3 \notin X_1$ and $u - 4 \in X_1$. Since $\delta(u - 2) = 0$ and $u - 2 \in X_2 \cap X_1$, we have $\delta(u - 3) = -1$. Since $p = 5$ and $q = 7$ with $u + 1 \equiv 0 \pmod{5}$ and $u + 4 \equiv 0 \pmod{7}$, we have $\delta(v) = 0$ for $v \in [u - 8, u - 5]$. Since $\delta(u - 3) = -1, \delta(u - 5) = 0$ and $u - 4 \in X_1$, this forces $u - 4 \notin X_2$. Since $u - 4, u - 3 \notin X_2$, it follows that $u - 5 \in X_2$, whence $u - 6 \notin X_2$. Since $u - 5 \in X_2$ and $\delta(u - 6) = \delta(u - 5) = 0$, it follows that $u - 5 \notin X_1$, whence $u - 6 \in X_1$.

If $u - 7 \notin X_2$, then $u - 8 \in X_2$ (as $u - 6 \notin X_2$ as well), whence $u - 8, u - 5, u - 2, u + 1$ and $u + 4$ are consecutive elements of $X_1$ with the difference $3 = d_2 + 1$ occurring 4 times in a row in $X_2$. Thus Lemma 2.4.6 implies that $x_2 < \frac{n}{3-1/7} = \frac{4}{11} n$. We also have $X_1 \cap [u - 6, u + 3] = \{u - 6, u - 4, u - 2, u - 1, u + 1, u + 3\}$. Thus $a_j = u - 6$ and $a_j + 5 = u + 3$ for some $j$, where $a_1 < a_2 < \ldots < a_{x_1 - 1}$ are the elements of $X_1$, whence $9 = (u + 3) - (u - 6) = a_j + 5 - a_j < \frac{5n}{x_1} + 1$, implying $x_1 < \frac{5}{8} n$. Hence $n - 2 = x_1 + x_2 \leq \left\lfloor \frac{5n-1}{8} \right\rfloor + \left\lfloor \frac{4n-1}{11} \right\rfloor$, implying $n = 35$ with $x_2 = 12$ and $x_1 = 21$ (in view of $p = 5, q = 7$ and $\omega = 2$), contradicting that $\gcd(x_1, n) = 1$ when $\omega = 2$. Therefore we instead conclude that $u - 7 \in X_2$.

Since $u - 7 \in X_2$ and $\delta(u - 7) = \delta(u - 8) = 0$, it follows that $u - 7 \notin X_1$, whence $u - 8 \in X_1$. But now $X_1 \cap [u - 8, u + 3] = \{u - 8, u - 6, u - 4, u - 2, u - 1, u + 1, u + 3\}$. Thus $a_j = u - 8$ and $a_j + 6 = u + 3$ for some $j$,
where $a_1 < a_2 < \ldots < a_{x_1-1}$ are the elements of $X_1$, whence $11 = (u+3) - (u-8) = a_{j+6} - a_j < \frac{6n}{21} + 1$, implying $x_1 < \frac{3}{7}n$. Since $u-5$, $u-2$, $u+1$ and $u+4$ are consecutive elements of $X_2$, the difference $3 = d_2 + 1$ occurs three times in a row in $X_2$, whence Lemma 2.4.6 implies that $x_2 < \frac{3}{10}n$. Hence $n - 2 = x_1 + x_2 < \left\lfloor \frac{30}{7} - 1 \right\rfloor + \left\lfloor \frac{30}{8} - 1 \right\rfloor$, implying $n = 35$, $x_2 = 13$ and $x_1 = 20$ (in view of $p = 5$, $q = 7$ and $\omega = 2$), contradicting that $\gcd(x_1, n) = 1$ when $\omega = 2$, which at last completes the case. \hfill $\square$

Case D. \quad $d = 2$ and $\omega = 1$.

Proof. Suppose $\omega = 1$, hence $\kappa = 1$ also, and let $u \in X_3$ be arbitrary.

If $u \in X_2$ and $u \in X_1$, then $\Lambda(u) = 3$, $\delta(u) = 1$ and $\delta(u-1) = -1$, contrary to Claim 5.

If $u \in X_2$ and $u \in X'_1 = [2, n - 1] \setminus X_1$, then $\Lambda(u) = 2$, whence Claim 6 ensures that $\Lambda(u + 1) = 0$ or $\Lambda(u - 1) = 0$. Thus either $u$, $u - 1 \in X'_1$ or $u$, $u + 1 \in X'_1$, both contradicting that the difference of consecutive elements in $X'_1$ is at least $d = 2$ by Lemma 2.4.2.

If $u \not\in X_2$ and $u \in X_1$, then, by Claim 6,

$\delta(u) = 0$ implies $\Lambda(u - 1) = 0$ with $\delta(u - 1) = -1$, and

$\delta(u) = 1$ implies $\Lambda(u + 1) = 0$ with $\delta(u + 1) = 0$.

First consider the case when $\delta(u) = 0$. Then $\Lambda(u - 1) = 0$ and $\delta(u - 1) = -1$, whence $\delta(v) = 0$ for $v \in [u - 5, u + 3] \setminus \{u - 1\}$ in view of $\omega = 1$ and $p \geq 5$. Since $\Lambda(u - 1) = 0$, we have $u - 2 \in X_1$.

We have $u \not\in X_2$ and $u - 1 \not\in X_2$ (as $\Lambda(u - 1) = 0$) whence $u - 2, u + 1 \in X_2$ (as the difference of consecutive elements in $X_2$ is either $d_2 = d = 2$ or $d_2 + 1 = 3$). Hence $\Lambda(u - 2) \geq 2$ with $\delta(u - 2) = 0$, implying $\delta(u - 3) = -1$, contrary to what we showed above. Next consider the case when $\delta(u) = 1$.

Then $\Lambda(u + 1) = 0$, $\delta(u + 1) = 0$, and $\delta(v) = 0$ for $v \in [u - 4, u + 4] \setminus \{u\}$ in view of $\omega = 1$ and $p \geq 5$.

Since $\Lambda(u + 1) = 0$, we have $u + 2 \in X_1$. We have $u \not\in X_2$ and $u + 1 \not\in X_2$ (as $\Lambda(u + 1) = 0$) whence $u - 1, u + 2 \in X_2$ (as the difference of consecutive elements in $X_2$ is either $d_2 = d = 2$ or $d_2 + 1 = 3$). Hence $\Lambda(u + 2) \geq 2$ with $\delta(u + 1) = 0$, implying $\delta(u + 2) = 1$, contrary to what we showed above.

It remains to consider the case when $u \not\in X_2$ and $u \in X'_1$. Since $u \in X'_1$, it follows that $u + 1, u - 1 \in X_1$. Thus $\delta(u) = 0$, as otherwise $\delta(u) = \delta(u + 1) = 1$ or $\delta(u) = \delta(u - 1) = -1$, both contrary to Claim 5. Since $u \not\in X_2$ and the difference of elements in $X_2$ is either $d_2 = d = 2$ or $d_2 + 1 = 3$, we must have $u - 1 \in X_2$ or $u + 1 \in X_2$. If $u + 1 \in X_2$, then $\delta(u + 1) = 1$, implying $u \equiv -1 \pmod{p}$; and if $u - 1 \in X_2$, then $\delta(u - 1) = 0$ and $\delta(u - 2) = -1$, implying $u \equiv 2 \pmod{p}$.

In summary, the above shows that an arbitrary element $u \in X_3$ must be congruent to $-1$ or $2$ modulo $p \geq 5$. In view of Case C, we may assume $|X_3| = x_3 - 1 \geq 3$, whence $c_1$, $c_2$ and $c_3$ are each congruent to $-1$ or $2$ modulo $p$. Since $c_1 = d_3 + 1$, this implies that $d_3$ is either $-2$ or $1$ modulo $p$.

If $d_3 \equiv -2 \pmod{p}$, then $c_1 \equiv -1 \pmod{p}$ and $c_2 \equiv -3$ or $-2$ modulo $p \geq 5$, forcing $c_2 \equiv -3 \equiv 2 \pmod{p}$ with $p = 5$, in which case $c_3 \equiv 0$ or $1$ modulo $p$, neither of which is equal to $-1$ or $2$ modulo $p = 5$, contrary to what we showed above.

If $d_3 \equiv 1 \pmod{p}$, then $c_1 \equiv 2 \pmod{p}$ and $c_2 \equiv 3$ or $4$ modulo $p$, forcing $c_2 \equiv 4 \equiv -1 \pmod{p}$ with $p = 5$, in which case $c_3 \equiv 0$ or $1$ modulo $p$, neither of which is equal to $-1$ or $2$ modulo $p = 5$, contrary to what we showed above, completing the case. \hfill $\square$

In view of the above work, the theorem is established when $\omega = 1$, so we now assume $\omega = 2$. The above claims nearly complete the proof. Indeed, if we use the $y_i$ in all the above arguments, then the theorem follows except in the case $d = d_2 = 2$ and $y_3 \geq 4$, implying $\frac{n}{\omega} < y_2 < \frac{n}{2} < y_1 < \frac{2}{3}n$. 

Thus $y_1 + y_2 \geq \frac{n+1}{3} + \frac{n+1}{2} = \frac{5n+5}{6}$, implying that $y_3 = n + 1 - y_1 - y_2 \leq \frac{n+1}{6}$. Thus Condition (4) holds. Moreover, Condition (4) must hold no matter which $y_j$ is re-indexed to equal $y_4$, else the sequence $S$ will be transformable into a case with $\kappa = 1$ already handled above. But these are precisely the conditions under which we instead use the $z_i$ in the above arguments. Observe that $\frac{2}{3}n < (2y_2)_n = 2y_2 < n$, that $0 < (2y_1)_n = 2y_1 - n < \frac{n}{3}$, and that $8 \leq (2y_3)_n = 2y_3 \leq \frac{n+1}{3}$. Thus, when we use the $z_i$, we have $z_1 = (2y_2)_n$ with $\frac{2}{3}n < z_1 < n$, implying $0 < x_1' = z_1' = n - z_1 < \frac{n}{3}$, whence $d = \lfloor \frac{n}{x_1'} \rfloor \geq 3$. But that means we do not need to consider the case when $d = 2$ and $\kappa = 2$, meaning the cases already handled above exhaust all possibilities, and the proof is complete. \hfill \Box

References


E-mail address: diambri@hotmail.com

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA

E-mail address: vishne@math.biu.ac.il

Department of Mathematics, Bar Ilan University, Ramat Gan 5290002, Israel