Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 49 (1) (2026), 65 – 76

Original Paper

Settling Jones's Conjectures on Cyclically Consecutive Power Sums

Thi Son Thao Tran

Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam

Abstract

For fixed integers $n \geq 2$ and $k \geq 1$, let $S_{n,k}$ be the set of sums of kth powers of k cyclically consecutive residue classes modulo n. In 2023, Jones [1] posed two conjectures concerning when the maximal value $|S_{n,k}| = n$ is attained and how this equality behaves under shifts of the exponent k. We prove the first conjecture: $|S_{n,k}| < n$ whenever $4 \mid n$ and $k > 1$. We show that the second conjecture, which asserts that $|S_{n,k}| = n$ is preserved under the shift $k \mapsto k + n(n-1)$, does not hold in general, and establish the correct replacement: if T is a common multiple of n and the Carmichael function $\lambda(n)$, then $|S_{n,k+T}| = |S_{n,k}|$ for every $k \geq E(n)$, where $E(n)$ is the largest exponent appearing in the prime factorization of n. This periodicity makes the maximal cardinality problem finite for each fixed modulus, but it does not by itself construct exponents. We therefore study the complementary existence problem. For every odd prime p and every $e \geq 1$, the explicit exponent $k = p(p-1)+1$ gives $|S_{p^e,k}| = p^e$. A Chinese remainder synchronization argument extends the result beyond squarefree moduli under a simple nonentanglement condition on repeated prime factors, and a nonidentity construction settles an infinite family of entangled moduli $p^e q$.

Mathematics Subject Classification (2020). 11A07, 11B83, 11T06
Keywords. Power sums; Cyclically consecutive integers; Modular arithmetic; Carmichael function; Eventual periodicity; Chinese remainder theorem; Permutation polynomials.

1. Introduction

For $n, k \in \mathbb{Z}_{>0}$, Jones [1] studied the set

$$S_{n,k} = \left\{ \sum_{i=0}^{k-1} (\alpha + i)^k \pmod{n} : \alpha \in \mathbb{Z}/n\mathbb{Z} \right\}. \tag{1.1}$$

This is the set of all sums of kth powers of k cyclically consecutive elements of $\mathbb{Z}/n\mathbb{Z}$. The cyclic formulation in Jones [1] belongs to the broader elementary study of power sums of consecutive integers, including the work of Ho, Mellblom, and Frodyma [2]. Related divisibility variants for sums of powers of consecutive integers were studied by He and Shiue [3], using Girard–Waring identities. Since there are n possible starting points, one always has $|S_{n,k}| \leq n$. Thus the equality $|S_{n,k}| = n$ is the strongest possible noncollision property for the starting point map

$$a \longmapsto \sum_{i=0}^{k-1} (a + i)^k \pmod{n}.$$

Email addresses: tranthisonthao@tdtu.edu.vn

Writing

$$P_k(X) = \sum_{i=0}^{k-1} (X+i)^k \in \mathbb{Z}[X],$$

the condition $|S_{n,k}| = n$ is precisely that P_k induce a permutation of the residue ring $\mathbb{Z}/n\mathbb{Z}$. Thus the problem is a concrete family inside the classical theory of permutation polynomials over finite fields and residue class rings; see Lidl and Niederreiter [4, Chapter 7] for finite fields, and McDonald [5] or Frisch and Krenn [6, Fact 2.7] for polynomial permutations modulo prime powers.

Equivalently, the cyclically consecutive power sums attain every residue class modulo n. This is the reason Jones [1] singled out the equality case: it asks when a highly structured family of consecutive power sums is nevertheless as large as it can possibly be.

Jones [1] proved several elementary results, including that $|S_{n,k}| < n$ whenever k is even and $n > 1$ [1, Proposition 2.2]. The same paper proposed the following two conjectures.

Conjecture 1.1 (Jones, Conjecture 3.1 of [1]). *If $n, k \in \mathbb{Z}_{>0}$, $4 \mid n$, and $k > 1$, then $|S_{n,k}| < n$.*

Conjecture 1.2 (Jones, Conjecture 3.2 of [1]). *If $n, k \in \mathbb{Z}_{>0}$, $|S_{n,k}| = n$, and $t = n(n-1) + k$, then $|S_{n,t}| = n$.*

The first goal of this note is to settle the two conjectures from Jones [1] and to identify the correct periodicity principle behind the second one. We prove Conjecture 1.1, which is Conjecture 3.1 of [1]. We then show that Conjecture 1.2, which is Conjecture 3.2 of [1], does not hold in general. Its literal form already fails at the endpoint exponent $k = 1$, but the substantive counterexample is $(n, k) = (10, 13)$, for which $4 \nmid n$ and $k > 1$.

The shift in Conjecture 1.2 was proposed in Jones [1] not only as a formal recurrence, but also as a way to make the equality problem finite for each fixed modulus n: if the shift were valid, then one would only need to test finitely many exponents k. Although the proposed shift fails, the main periodicity theorem below recovers this intended finite decidability with the correct period.

The corrected periodicity uses the Carmichael function. Let $\lambda(n)$ denote the exponent of the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$; for standard background on this function, see Carmichael [7] and Hardy and Wright [8]. Let

$$T_n = \operatorname{lcm}(n, \lambda(n)).$$

If $E(n)$ is the largest exponent appearing in the prime factorization of n, then for every $k \geq E(n)$,

$$|S_{n,k+T_n}| = |S_{n,k}|.$$

This is not merely the ordinary Carmichael periodicity of the power map $x \mapsto x^k$. In (1.1), the same integer k controls both the exponent and the number of summands. Thus the period must simultaneously respect exponent periodicity, governed by $\lambda(n)$, and block length periodicity, governed by n. The shift proposed in Jones [1], namely $n(n-1)$, works when $\lambda(n) \mid n(n-1)$, but it fails in general. The period T_n restores the finite testing principle that motivated the shifted conjecture.

Finite testing, however, is not a structural existence theorem. Theorem 2.3 shows that $4 \nmid n$ is necessary for any nontrivial exponent with $|S_{n,k}| = n$, so the natural converse becomes the organizing problem of Section 5. We prove this converse locally for every prime power: for every odd prime p and every $e \geq 1$, the exponent $k = p(p-1)+1$ makes P_k a permutation polynomial of $\mathbb{Z}/p^e\mathbb{Z}$. We then use Chinese remainder synchronization to obtain full cardinality for all squarefree moduli, for broad nonsquarefree families, and for an infinite entangled family $p^e q$ by using a nonidentity permutation over $\mathbb{F}_q$. The remaining open cases become an explicit compatibility problem among local good congruence classes.

The same periodicity gives a finite procedure for the smallest witness problem raised in Jones [1]: after the finite initial range, only one complete Carmichael period must be tested. We return to this point in Remark 5.8.

The paper is organized according to this progression. Section 2 proves the obstruction at moduli divisible by 4. Section 3 records the endpoint and substantive counterexamples to the proposed shift. Section 4 replaces that shift by the Carmichael period theorem. Section 5 then uses the finite period viewpoint as a starting point for the constructive existence problem. Section 6 collects closing remarks.

2. The case $4 \mid n$

For $a \in \mathbb{Z}/n\mathbb{Z}$, define

$$F_{n,k}(a) = \sum_{i=0}^{k-1} (a+i)^k \pmod{n},$$

so that $S_{n,k} = \{F_{n,k}(a) : a \in \mathbb{Z}/n\mathbb{Z}\}$.

Lemma 2.1 (Jones [1], Proposition 2.2)**.** *If $n > 1$ and k is even, then $|S_{n,k}| < n$.*

Proof. We include a short reflection proof. For even k, the block

$$a, a+1, \ldots, a+k-1$$

has the same kth power sum as its reflected block

$$-a-k+1, -a-k+2, \ldots, -a.$$

Equivalently,

$$F_{n,k}(a) = F_{n,k}(1-k-a). \tag{2.1}$$

The map $a \mapsto 1-k-a$ is not the identity on $\mathbb{Z}/n\mathbb{Z}$ when $n > 1$ and k is even. Hence there is some $a \in \mathbb{Z}/n\mathbb{Z}$ such that $a \not\equiv 1-k-a \pmod{n}$. By (2.1), two distinct starting points give the same value, so the image cannot have size n. □

Lemma 2.2. *Let $k > 1$ be odd. Then*

$$F_{4,k}(a) \not\equiv 2 \pmod{4}$$

for every $a \in \mathbb{Z}/4\mathbb{Z}$.

Proof. For odd $k > 1$, the residues of x^k modulo 4 are

$$0^k \equiv 0, \qquad 1^k \equiv 1, \qquad 2^k \equiv 0, \qquad 3^k \equiv 3 \pmod{4}.$$

The sum over any complete block of four consecutive residues is therefore

$$0+1+0+3 \equiv 0 \pmod{4}.$$

Write $k = 4u + r$, where $r \in \{1, 3\}$. The u complete blocks of four contribute 0 modulo 4, so the remaining contribution consists of r consecutive terms of the periodic pattern

$$0, 1, 0, 3,$$

starting at the residue class of a. Thus $F_{4,k}(a)$ is congruent either to a single term of this pattern or to a sum of three consecutive terms in this pattern. The four possible sums of three consecutive terms are

$$0+1+0, \qquad 1+0+3, \qquad 0+3+0, \qquad 3+0+1,$$

which are congruent to $1, 0, 3, 0$ modulo 4, respectively. Hence in either case the possible values lie in $\{0, 1, 3\}$, never in $\{2\}$. □

Theorem 2.3. *If $4 \mid n$ and $k > 1$, then $|S_{n,k}| < n$.*

Proof. If k is even, this is Lemma 2.1. Suppose k is odd. Reducing $F_{n,k}(a)$ modulo 4 gives $F_{4,k}(\bar{a})$, where $\bar{a}$ is the image of a in $\mathbb{Z}/4\mathbb{Z}$. If $S_{n,k} = \mathbb{Z}/n\mathbb{Z}$, then reducing modulo 4 would give every residue in $\mathbb{Z}/4\mathbb{Z}$, since $4 \mid n$. But by Lemma 2.2, no reduced value is congruent to 2 modulo 4. Therefore $S_{n,k}$ cannot be all of $\mathbb{Z}/n\mathbb{Z}$, and $|S_{n,k}| < n$. □

Thus Conjecture 1.1 is true. The obstruction is genuinely 2-adic: odd powers modulo 4 miss the residue class 2 in the above cyclic sums. This explains why the condition $4 \mid n$ is special, rather than merely a symptom of nonsquarefree moduli.

3. Counterexamples to the shifted conjecture

There is a literal endpoint failure at the smallest modulus divisible by four. Since

$$F_{4,1}(a) = a,$$

one has $|S_{4,1}| = 4$. On the other hand, $13 = 4(4-1)+1 > 1$, so Theorem 2.3 gives $|S_{4,13}| < 4$; directly, $S_{4,13} = \{0, 1, 3\}$. This is only the endpoint case of Conjecture 1.2 as stated. The following example is the substantive counterexample: it has $4 \nmid n$ and $k > 1$, so it is not an artifact of either the endpoint exponent or the moduli excluded by Theorem 2.3.

Proposition 3.1. *The shifted preservation statement proposed in Jones [1] does not hold in general. In fact,*

$$|S_{10,13}| = 10, \qquad |S_{10,103}| = 6.$$

Here $103 = 13 + 10(10-1)$.

Proof. First consider $k = 13$. Modulo 2, since $x^{13} \equiv x \pmod 2$,

$$F_{10,13}(a) \equiv \sum_{i=0}^{12}(a+i) \equiv a \pmod 2.$$

Modulo 5, since $13 \equiv 1 \pmod 4$, one has $x^{13} \equiv x \pmod 5$ for every residue x. Hence

$$F_{10,13}(a) \equiv \sum_{i=0}^{12}(a+i) \equiv 13a + 78 \equiv 3a + 3 \pmod 5.$$

The map

$$a \longmapsto (a \bmod 2,\ 3a+3 \bmod 5)$$

is injective on $\mathbb{Z}/10\mathbb{Z}$. Therefore $|S_{10,13}| = 10$.

Now consider $k = 103$. Modulo 2, since 103 is odd, $x^{103} \equiv x \pmod 2$. Hence

$$F_{10,103}(a) \equiv \sum_{i=0}^{102}(a+i) = 103a + \frac{102 \cdot 103}{2} \equiv a + 1 \pmod 2.$$

Modulo 5, since $103 \equiv 3 \pmod 4$, we have $x^{103} \equiv x^3 \pmod 5$ for every residue x. Also $103 \equiv 3 \pmod 5$, and a complete block of five cubes has sum 0 modulo 5. Therefore

$$F_{10,103}(a) \equiv \sum_{i=0}^{2}(a+i)^3 \equiv 3a^3 + 4a^2 + 4 \pmod 5.$$

As a varies modulo 5, this polynomial assumes only the values

$$\{0, 1, 4\} \pmod 5.$$

Thus the image modulo 5 has at most three elements, so the image modulo 10 has at most six elements. Hence $|S_{10,103}| < 10$.

A direct evaluation gives

a	0	1	2	3	4	5	6	7	8	9
$F_{10,103}(a)$	9	6	9	6	5	4	1	4	1	0

so

$$S_{10,103} = \{0, 1, 4, 5, 6, 9\}$$

and $|S_{10,103}| = 6$. □

Proposition 3.1 is the essential counterexample: it reflects a failure of the proposed shift $n(n-1)$ to be an exponent period modulo the composite modulus 10.

4. A corrected periodicity theorem

The failure of Conjecture 1.2 comes from using the shift $n(n-1)$ as though it were always an exponent period modulo n. Jones [1] already observed that the proposed shift is immediately valid for prime moduli. This is explained by $\lambda(p) = p - 1$. For composite moduli, however, the same divisibility can fail. For instance,

$$\lambda(10) = 4, \qquad 4 \nmid 90 = 10(10-1).$$

The appropriate replacement is to use any common multiple of n and $\lambda(n)$. The point specific to the present problem is that k controls two different features at once: the exponent in each summand and the length of the consecutive block.

Write

$$n = \prod_{j=1}^{r} p_j^{e_j}, \qquad E(n) = \max_j e_j.$$

Lemma 4.1. *Let T be a multiple of $\lambda(n)$. If $m \geq E(n)$, then*

$$x^{m+T} \equiv x^m \pmod{n}$$

for every integer x.

Proof. We check the congruence modulo each prime power factor of n. Fix a prime power factor $p^e \| n$, meaning that $p^e \mid n$ and $p^{e+1} \nmid n$.

First suppose $p \nmid x$. Then x is a unit modulo p^e. Since $\lambda(p^e)$ divides $\lambda(n)$ and T is a multiple of $\lambda(n)$, we have

$$x^T \equiv 1 \pmod{p^e}.$$

Therefore $x^{m+T} \equiv x^m \pmod{p^e}$.

Now suppose $p \mid x$. This is the only point where the lower bound $m \geq E(n)$ is needed. Since $m \geq E(n) \geq e$, the integer x^m is divisible by p^e. Hence

$$x^m \equiv 0 \pmod{p^e} \qquad \text{and} \qquad x^{m+T} \equiv 0 \pmod{p^e}.$$

Thus the desired congruence holds modulo p^e in both the unit and nonunit cases. Since this is true for every prime power factor of n, the Chinese remainder theorem gives the congruence modulo n. □

Lemma 4.2. *If L is a multiple of n, then for every exponent $m \geq 1$ the sum*

$$\sum_{i=0}^{L-1} (a+i)^m \pmod{n}$$

is independent of a.

Proof. The interval of length L consists of L/n complete cycles modulo n. Each complete cycle contributes

$$\sum_{x \in \mathbb{Z}/n\mathbb{Z}} x^m,$$

which is independent of the starting point a. □

Lemma 4.2 generalizes Jones [1, Lemma 1.3], where the block length is n.

Theorem 4.3. *Let T be a common multiple of n and $\lambda(n)$. For every $k \geq E(n)$, one has*

$$F_{n,k+T}(a) \equiv F_{n,k}(a) + C_{n,k,T} \pmod{n}$$

for all $a \in \mathbb{Z}/n\mathbb{Z}$, where

$$C_{n,k,T} \equiv \frac{T}{n} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} x^k \pmod{n}.$$

Consequently,

$$|S_{n,k+T}| = |S_{n,k}|$$

for every $k \geq E(n)$.

Proof. Because T is a multiple of $\lambda(n)$ and $k \geq E(n)$, Lemma 4.1 gives

$$(a+i)^{k+T} \equiv (a+i)^k \pmod{n}$$

for all integers $a + i$. Therefore the first k terms of $F_{n,k+T}(a)$ satisfy

$$\sum_{i=0}^{k-1} (a+i)^{k+T} \equiv \sum_{i=0}^{k-1} (a+i)^k = F_{n,k}(a) \pmod{n}.$$

The remaining T terms are

$$\sum_{i=k}^{k+T-1} (a+i)^{k+T}.$$

Since T is divisible by n, these T consecutive residues contain exactly T/n complete residue systems modulo n. By Lemma 4.2, their contribution is independent of a; more explicitly, it is

$$\frac{T}{n} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} x^{k+T} \pmod{n}.$$

Applying Lemma 4.1 once more gives

$$\sum_{x \in \mathbb{Z}/n\mathbb{Z}} x^{k+T} \equiv \sum_{x \in \mathbb{Z}/n\mathbb{Z}} x^k \pmod{n}.$$

Since T/n is an integer, multiplying a congruence by the integer T/n preserves it. Thus

$$F_{n,k+T}(a) \equiv F_{n,k}(a) + C_{n,k,T} \pmod{n},$$

with

$$C_{n,k,T} \equiv \frac{T}{n} \sum_{x \in \mathbb{Z}/n\mathbb{Z}} x^k \pmod{n}.$$

The map $y \mapsto y + C_{n,k,T}$ is a translation of $\mathbb{Z}/n\mathbb{Z}$, so it preserves cardinality. Hence

$$|S_{n,k+T}| = |S_{n,k}|.$$

□

Taking $T = T_n = \operatorname{lcm}(n, \lambda(n))$ gives the convenient global period stated in the introduction. In particular, for each fixed n, the values of $|S_{n,k}|$ are eventually periodic and hence can be determined by finitely many tests. This recovers the decidability consequence that motivated the shifted conjecture in Jones [1], but with the correct period. This period need not be the minimal eventual period; for example, when $n = 12$ one has $T_n = 12$, while the cardinalities are already eventually periodic with period 6. The lower bound $k \geq E(n)$ is also not a cosmetic assumption: for $n = 9$, one has $E(9) = 2$ and $T_9 = 18$, but

$$|S_{9,1}| = 9 \qquad \text{whereas} \qquad |S_{9,19}| = 7.$$

Thus the asserted periodicity can fail below the threshold $E(n)$.

Corollary 4.4. *If n is squarefree, then*

$$|S_{n,k+T_n}| = |S_{n,k}|$$

for every $k \geq 1$.

Proof. If n is squarefree, then $E(n) = 1$. □

Corollary 4.5. *If $\lambda(n) \mid n(n-1)$, then*

$$|S_{n,k+n(n-1)}| = |S_{n,k}|$$

for every $k \geq E(n)$.

Proof. The integer $n(n-1)$ is always divisible by n. Under the additional hypothesis $\lambda(n) \mid n(n-1)$, it is also divisible by $\lambda(n)$. Theorem 4.3 therefore applies with $T = n(n-1)$. □

Remark 4.6. For a prime p, one has $\lambda(p) = p-1$ and $E(p) = 1$. Thus the observation in Jones [1] that the shift is valid for prime moduli is recovered as the special case $n = p$ of Corollary 4.5. More generally, Corollary 4.5 isolates the exact divisibility condition under which the proposed shift is covered by Theorem 4.3, namely $\lambda(n) \mid n(n-1)$. The counterexample $n = 10$ occurs because $\lambda(10) = 4$ does not divide $10(10-1) = 90$.

Remark 4.7 (When the shift $n(n-1)$ is an exponent period)**.** Corollary 4.5 applies exactly when

$$\lambda(n) \mid n(n-1).$$

Writing $n = \prod_j p_j^{e_j}$, the prime power part of $\lambda(n)$ coming from $p_j^{e_j}$ itself is never the obstruction: for odd p_j it contributes $p_j^{e_j-1}$, and for 2^{e_j} it contributes at most 2^{e_j-1}. Hence the possible obstructions come from prime divisors of the factors $q-1$ with $q \mid n$. Equivalently, for every prime divisor $q \mid n$ and every prime $p \mid (q-1)$, one must have

$$v_p(q-1) \leq v_p(n(n-1)),$$

where v_p is the usual p-adic valuation.

Two small failures illustrate the two possibilities. The modulus $n = 10$ fails internally, since both 2 and 5 divide 10 and

$$v_2(5-1) = 2 > v_2(10(10-1)) = v_2(90) = 1.$$

The modulus $n = 15$ fails externally, since $5 \mid 15$, $2 \mid 5-1$, and

$$v_2(5-1) = 2 > v_2(15(15-1)) = v_2(210) = 1.$$

Even when this divisibility fails, the shift $n(n-1)$ may preserve cardinality for some individual exponents. It is not a valid general period, however; for example, a direct computation gives

$$|S_{65,37}| = 65 \qquad \text{whereas} \qquad |S_{65,4197}| = 45,$$

with $4197 = 37 + 65(65-1)$. Since both 10 and 65 are squarefree, the failure of the proposed shift is not repaired merely by restricting to squarefree moduli. The corrected period $T_n = \operatorname{lcm}(n, \lambda(n))$ avoids these obstructions.

Theorem 4.3 turns $|S_{n,k}| = n$ into a finite computation for each fixed n, but it neither explains existence nor produces witnesses. A search over one eventual period can certify a particular modulus, but it gives little information about why a witness exists or how witnesses should be constructed.

The remaining structural problem is therefore different from the periodicity problem. One must understand how the permutation condition behaves under the prime power decomposition of n, and then decide whether the resulting local conditions can be imposed by a single exponent k. The Chinese remainder theorem supplies the reduction; the difficulty is synchronization. This is the role of the next section.

5. Local compatibility and maximal cardinality existence

Theorem 2.3 shows that no nontrivial exponent can give $|S_{n,k}| = n$ when $4 \mid n$. This leaves the natural converse question.

Question 5.1. For $n > 1$, does there exist $k > 1$ with $|S_{n,k}| = n$ if and only if $4 \nmid n$?

The forward direction is exactly Theorem 2.3. The reverse direction is the constructive part of the paper. The periodicity theorem says that it is decidable for each fixed n, but Question 5.1 asks for a uniform structural explanation.

The strategy has three layers. First, Proposition 5.2 separates the image into prime power components. Second, Theorem 5.4 closes the local prime power problem for every odd prime power by a uniform lifting argument. Third, Theorem 5.6 and Proposition 5.7 address the global synchronization problem. Thus the rest of this section is organized around the unobstructed direction of Question 5.1.

For prime moduli, Jones [1, Proposition 2.3] proved that if p is prime,

$$k = t(p-1) + 1, \qquad p \nmid k,$$

then $|S_{p,k}| = p$. For composite moduli, the issue is not only local existence but also compatibility of one exponent across different prime power factors. The Chinese remainder theorem separates the local images exactly.

Proposition 5.2. *Let $n = \prod_{j=1}^{r} q_j$ be the factorization of n into pairwise coprime prime powers. Then*

$$|S_{n,k}| = \prod_{j=1}^{r} |S_{q_j,k}|.$$

Consequently, $|S_{n,k}| = n$ if and only if $|S_{q_j,k}| = q_j$ for every j.

Proof. Under the Chinese remainder isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{j=1}^{r} \mathbb{Z}/q_j\mathbb{Z},$$

the function $a \mapsto F_{n,k}(a)$ decomposes componentwise as the product of the functions $a_j \mapsto F_{q_j,k}(a_j)$. Hence its image is the Cartesian product of the local images $S_{q_j,k}$. □

The prime field construction does not automatically lift to prime powers. If $e \geq 2$, a polynomial $f \in \mathbb{Z}[X]$ induces a permutation of $\mathbb{Z}/p^e\mathbb{Z}$ if and only if its reduction induces a permutation of $\mathbb{F}_p$ and

$$f'(z) \not\equiv 0 \pmod{p}$$

for every $z \in \mathbb{F}_p$; see McDonald [5], or Frisch and Krenn [6, Fact 2.7]. For

$$P_k(X) = \sum_{i=0}^{k-1} (X+i)^k, \qquad P_k'(X) = k \sum_{i=0}^{k-1} (X+i)^{k-1},$$

the derivative may vanish modulo p. For example, the Jones exponent $k = 5$ works modulo 3, but $P_5'(X) \equiv 0 \pmod 3$ at $X \equiv 0, 2 \pmod 3$, and indeed

$$|S_{9,5}| = 5 \neq 9.$$

Using Theorem 4.3, for a prime power $q = p^e$ set $T_q = \operatorname{lcm}(q, \lambda(q))$ and define

$$\mathcal{K}_q = \{c \in \mathbb{Z}/T_q\mathbb{Z} : |S_{q,k}| = q \text{ for some, equivalently every, } k \geq e \text{ with } k \equiv c \pmod{T_q}\}.$$

For $k \geq E(n)$, Proposition 5.2 says that $|S_{n,k}| = n$ exactly when $k \bmod T_q \in \mathcal{K}_q$ for each prime power factor q of n. Thus the local question is whether these sets are nonempty, and the global question is whether their classes can be synchronized. The following lemma gives a compact way to force both the reduction and the derivative condition.

Lemma 5.3. *Let p be an odd prime, and let $k > 1$ satisfy*

$$k \equiv 1 \pmod{p}, \qquad k \equiv 1 \pmod{p-1}.$$

Put $a = (k-1)/p$. Then $\overline{P_k}$ is the identity map on $\mathbb{F}_p$, and

$$P_k'(z) \equiv \begin{cases} k(1-a) \pmod{p}, & z \neq 0, \\ -ka \pmod{p}, & z = 0. \end{cases}$$

Thus P_k' has no zero on $\mathbb{F}_p$ exactly when $a \not\equiv 0, 1 \pmod{p}$.

Proof. Write $k = ap+1$. In the block $z, z+1, \ldots, z+k-1$, each residue modulo p occurs a times, and the class of z occurs once more. Hence

$$\overline{P_k}(z) \equiv a \sum_{x \in \mathbb{F}_p} x^k + z^k \pmod{p}.$$

Since $k \equiv 1 \pmod{p-1}$, the power sum is 0, and Fermat's theorem gives $z^k = z$. This proves $\overline{P_k} = \mathrm{id}$.

For the derivative, the same counting gives

$$P_k'(z) \equiv k \left(a \sum_{x \in \mathbb{F}_p} x^{k-1} + z^{k-1} \right) \pmod{p}.$$

Now $k-1 > 0$ and $k-1 \equiv 0 \pmod{p-1}$, so $\sum_x x^{k-1} = -1$, while $z^{k-1} = 1$ for $z \neq 0$ and 0 for $z = 0$. The displayed formula follows. Since $p \nmid k$, the derivative is nowhere zero exactly when $a \not\equiv 0, 1 \pmod{p}$. □

Theorem 5.4. *Let p be an odd prime and $e \geq 1$. For*

$$k_0 = p(p-1) + 1,$$

one has $|S_{p^e,k_0}| = p^e$. Equivalently, P_{k_0} is a permutation polynomial of $\mathbb{Z}/p^e\mathbb{Z}$. Moreover the eventual local good set $\mathcal{K}_{p^e}$ is nonempty for every odd prime power.

Proof. For $k_0 = p(p-1)+1$, Lemma 5.3 applies with $a = p-1$. Thus $\overline{P_{k_0}} = \mathrm{id}$ on $\mathbb{F}_p$, and $a \equiv -1 \not\equiv 0, 1 \pmod{p}$, so P_{k_0}' has no zero modulo p. The prime power criterion quoted above then gives that P_{k_0} permutes $\mathbb{Z}/p^e\mathbb{Z}$ for every $e \geq 1$.

If $k_0 \geq e$, this already gives a class in $\mathcal{K}_{p^e}$. If $k_0 < e$, choose m such that $k = k_0 + mT_{p^e} \geq e$. Since $T_{p^e} = p^e(p-1)$, the new exponent still satisfies $k \equiv 1 \pmod{p}$ and $k \equiv 1 \pmod{p-1}$, while $(k-1)/p \equiv p-1 \pmod{p}$. The same argument applies, so $\mathcal{K}_{p^e} \neq \varnothing$. □

This witness is uniform in e. It also explains why the first witnesses for $9, 27, 81, 729$ are all $7 = 3(3-1)+1$, whereas the prime modulus witness $2p-1$ need not lift.

Smaller local witnesses. The uniform witness in Theorem 5.4 is convenient for later synchronization, but it is not the smallest local construction. If $p \geq 5$, then $|S_{p^e,2p-1}| = p^e$ for every $e \geq 1$. Indeed, for $k = 2p-1$, the congruence $k \equiv 1 \pmod{p-1}$ gives

$$P_k(X) \equiv kX + \binom{k}{2} \equiv -X + 1 \pmod{p},$$

so the reduction is a permutation of $\mathbb{F}_p$. Also $k - 1 = 2(p-1)$. Hence, in

$$P_k'(X) = k \sum_{i=0}^{k-1} (X+i)^{k-1},$$

each nonzero term contributes 1 modulo p, while each zero term contributes 0. Among $2p-1$ consecutive residues, the zero class occurs $c(X) \in \{1, 2\}$ times, and therefore

$$P_k'(X) \equiv k(2p-1-c(X)) \equiv 1 + c(X) \in \{2, 3\} \pmod{p},$$

which is nonzero for $p \geq 5$. The prime power lifting criterion gives the claim. For $p = 3$, the exponent $2p - 1 = 5$ fails, but $k = 7$ works: its reduction is a permutation of $\mathbb{F}_3$, and since $k - 1 = 6$, the zero class occurs $c(X) \in \{2, 3\}$ times, giving

$$P_7'(X) \equiv 7(7 - c(X)) \equiv 1 - c(X) \in \{1, 2\} \pmod 3.$$

Thus P_7 permutes $\mathbb{Z}/3^e\mathbb{Z}$ for every $e \geq 1$.

Corollary 5.5. *For a prime power q, there exists $k > 1$ with $|S_{q,k}| = q$ if and only if $4 \nmid q$.*

Proof. If $4 \mid q$, Theorem 2.3 gives $|S_{q,k}| < q$ for all $k > 1$. If $q = 2$, take $k = 3$. If $q = p^e$ with p odd, use Theorem 5.4. □

We now synchronize the local construction across several prime power factors.

Theorem 5.6. *Let $n > 1$ with $4 \nmid n$, and write*

$$n = 2^{\varepsilon} \prod_{j=1}^{r} p_j^{e_j}, \qquad \varepsilon \in \{0, 1\},$$

where the p_j are distinct odd primes. Suppose that, whenever $e_j \geq 2$, one has

$$p_j^2 \nmid (p_i - 1) \qquad \text{for every } i \neq j.$$

Then there exists $k > 1$ such that $|S_{n,k}| = n$.

Proof. If $r = 0$, then $n = 2$ and $k = 3$ works. Assume $r \geq 1$, and set

$$M = \operatorname{lcm}(p_1, \ldots, p_r, p_1 - 1, \ldots, p_r - 1).$$

Let $k = M\mu + 1$. Then $k \equiv 1 \pmod{p_j}$ and $k \equiv 1 \pmod{p_j - 1}$ for every j, so Lemma 5.3 applies at each p_j. For indices with $e_j = 1$, the identity reduction already gives a permutation modulo p_j. For $e_j \geq 2$, we also need the derivative condition. The hypothesis gives $v_{p_j}(M) = 1$, so

$$\frac{k-1}{p_j} \equiv \frac{M}{p_j}\mu \pmod{p_j},$$

with $M/p_j \not\equiv 0 \pmod{p_j}$. Hence the forbidden values $(k-1)/p_j \equiv 0, 1 \pmod{p_j}$ exclude exactly two residue classes for μ modulo p_j. Since the repeated primes p_j are distinct and odd, there is at least one allowed class modulo each such p_j, and the Chinese remainder theorem gives a positive μ avoiding all forbidden classes. Then $|S_{p_j^{e_j},k}| = p_j^{e_j}$ for every j. Finally, M is even, so k is odd; if $\varepsilon = 1$, the local map modulo 2 is an affine permutation. Proposition 5.2 gives $|S_{n,k}| = n$. □

Theorem 5.6 recovers the squarefree case, since its hypothesis is then vacuous, and it covers many nonsquarefree moduli, such as $225 = 3^2 \cdot 5^2$ and $11025 = 3^2 \cdot 5^2 \cdot 7^2$. It does not cover entangled cases, where $p^2 \mid n$ and $p^2 \mid (q - 1)$ for some prime $q \mid n$; for instance $171 = 3^2 \cdot 19$. The local prime power obstruction is now removed, so the remaining issue is only global compatibility of the good local congruence classes.

Mechanism behind the entanglement. The proof of Theorem 5.6 uses a strategy based on the identity at every prime: it imposes $k \equiv 1 \pmod{p_j - 1}$ so that Lemma 5.3 gives $\overline{P_k} = \mathrm{id}$ over each $\mathbb{F}_{p_j}$. If $p^2 \mid n$, the derivative condition at p forbids $(k-1)/p \equiv 0, 1 \pmod p$, and in particular forbids $k \equiv 1 \pmod{p^2}$. If another prime $q \mid n$ satisfies $p^2 \mid (q - 1)$, then forcing the identity construction at q gives $k \equiv 1 \pmod{q - 1}$, hence the forbidden congruence $k \equiv 1 \pmod{p^2}$. Thus entanglement is not a local nonexistence obstruction; it is an obstruction to this synchronization strategy. The natural escape is to keep a good local class at p^e, but let P_k be a nonidentity permutation polynomial over the entangled field $\mathbb{F}_q$. The next proposition implements this escape for a whole entangled family.

Proposition 5.7 (An entangled prime power family)**.** *Let p and q be distinct odd primes, let $e \geq 2$, and suppose that*

$$q \equiv 1 \pmod{p^e(p-1)}.$$

Then there exists $k > 1$ such that

$$|S_{p^e q,k}| = p^e q.$$

Proof. Put

$$T_{p^e} = p^e(p-1), \qquad c_0 = p(p-1)+1.$$

By Theorem 5.4, the class $c_0 \pmod{T_{p^e}}$ is a good local class modulo p^e. Since $T_{p^e} \mid q-1$, we may choose a residue $r \pmod{q-1}$ such that

$$r \equiv c_0 \pmod{T_{p^e}}, \qquad \gcd(r, q-1) = 1.$$

Indeed, c_0 is a unit modulo T_{p^e}: it is congruent to 1 modulo both p and $p-1$. For each exact prime power divisor $\ell^\nu \| q-1$, choose $r \equiv c_0 \pmod{\ell^\nu}$ if $\ell \mid T_{p^e}$, and choose $r \equiv 1 \pmod{\ell^\nu}$ otherwise. The Chinese remainder theorem gives a class modulo $q-1$ satisfying the two required conditions.

Now choose a positive integer $k > 1$, large enough so that $k \geq e$, satisfying

$$k \equiv 1 \pmod{q}, \qquad k \equiv r \pmod{q-1}.$$

Since $r \equiv c_0 \pmod{T_{p^e}}$, Theorems 4.3 and 5.4 give

$$|S_{p^e,k}| = p^e.$$

It remains to check the prime modulus q. Write $k = aq+1$. Modulo q, the block of k consecutive terms consists of a complete residue cycles, together with one extra copy of the starting residue. Also $k \equiv r \pmod{q-1}$. Hence over $\mathbb{F}_q$,

$$P_k(X) \equiv a \sum_{y \in \mathbb{F}_q} y^r + X^r \equiv X^r \pmod{q},$$

because $q-1 \nmid r$. Since $\gcd(r, q-1) = 1$, the monomial X^r is a permutation of $\mathbb{F}_q$. Thus $|S_{q,k}| = q$. Proposition 5.2 gives

$$|S_{p^e q,k}| = |S_{p^e,k}|\,|S_{q,k}| = p^e q.$$

□

For $p = 3$ and $e = 2$, Proposition 5.7 gives the basic family $n = 9q$, with $q \equiv 1 \pmod 9$ prime, since this is equivalent to $18 \mid q-1$ for odd primes q. Thus the simplest entangled family is not left open. The condition $p^e(p-1) \mid q-1$ is only a clean sufficient condition; computations suggest that witnesses may exist under weaker congruence assumptions.

The results above give the present status of Question 5.1. It is known for all prime powers by Corollary 5.5; it is known for all squarefree moduli and for the nonentangled nonsquarefree moduli covered by Theorem 5.6; and Proposition 5.7 treats an infinite family where the strategy using the identity at every prime provably breaks down. The unresolved cases are the remaining entangled nonsquarefree moduli not divisible by 4. Question 5.1 is not used in the proof of the main conjectural results from Jones [1]; it records the structural existence problem left after the periodicity theorem.

Remark 5.8 (Computational evidence)**.** By Theorem 4.3, Question 5.1 is decidable for each fixed modulus by checking $2 \leq k < E(n)$ and one eventual period $E(n) \leq k < E(n)+T_n$. A complete check for $2 \leq n \leq 400$ was consistent with Question 5.1. A separate witness search for $2 \leq n \leq 1000$, $4 \nmid n$, tested $k = 2, 3, \ldots, 2n+200$. For $400 < n \leq 1000$, this was only a witness search, not a complete period check. The computations are not used in any proof.

In view of Theorem 5.6, the most relevant data are now the entangled nonsquarefree moduli. There are exactly nine such moduli $n \leq 1000$ with $4 \nmid n$, and their first witnesses are

n	171	333	342	513	657	666	855	981	999
k	43	7	43	43	439	7	151	115	7.

Of these, 171, 333, 657, and 981 are covered by Proposition 5.7, while 342, 513, 666, 855, and 999 lie outside the direct reach of Theorem 5.6 and Proposition 5.7, yet witnesses exist in every case. For even entangled moduli $n = 2m$, every odd k makes $F_{2,k}$ an affine bijection of $\mathbb{Z}/2\mathbb{Z}$, so by Proposition 5.2 the first witness of $2m$ coincides with that of m; this explains the pairs $(171, 342)$ and $(333, 666)$. We highlight $513 = 3^3 \cdot 19$: it is not of the form treated by Proposition 5.7, which would require $19 \equiv 1 \pmod{54}$, yet it has the small witness $k = 43$.

6. Closing remarks

We have proved the conjecture of Jones [1] for moduli divisible by 4 and shown that the shifted conjecture proposed there does not hold in general. The proposed shift $n(n-1)$ mixes two requirements: the length of the sum is periodic modulo n, while the exponent is eventually periodic modulo the Carmichael exponent of n. The common multiple $\operatorname{lcm}(n, \lambda(n))$ respects both effects and restores the finite decidability consequence that the original shift was meant to provide.

On the existence side, $k = p(p-1) + 1$ makes P_k a permutation polynomial modulo every odd prime power, so the local prime power core is closed. Theorem 5.6 recovers the squarefree case and many nonsquarefree moduli, while Proposition 5.7 treats an infinite family of entangled moduli $p^e q$. The remaining open cases are the other entangled nonsquarefree moduli not divisible by 4, where the issue is global compatibility of good local congruence classes.

References

[1] N.P.Jones. *Sums of powers of cyclically consecutive integers*, Alabama Journal of Mathematics. **46**(1) (2023) 1–5.

[2] C.Ho, G.Mellblom and M.Frodyma. *On the sum of powers of consecutive integers*, College Mathematics Journal. **51**(4) (2020) 295–301.

[3] T.-X.He and P.J.-S.Shiue. *Divisibility of the sums of the power of consecutive integers*, Notes on Number Theory and Discrete Mathematics. **30**(3) (2024) 557–574.

[4] R.Lidl and H.Niederreiter. *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press, 1997.

[5] B.R.McDonald. *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, New York, 1974.

[6] S.Frisch and D.Krenn. *Sylow p-groups of polynomial permutations on the integers modulo p^n*, Journal of Number Theory. **133**(12) (2013) 4188–4199.

[7] R.D.Carmichael. *Note on a new number theory function*, Bulletin of the American Mathematical Society. **16** (1910) 232–238.

[8] G.H.Hardy and E.M.Wright. *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, 2008.