Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 46 (1) (2023), 1 − 5

Original Article

Sums of Powers of Cyclically Consecutive Integers

Nathan P. Jones*[1]

[1] *University of Kentucky, Lexington, KY 40506*

Abstract

The study in [1] of divisibility properties of sums of k^{th} powers of k-many consecutive non-negative integers inspires an analogous study in the rings $\mathbb{Z}_n$. Inquiry into this new context uncovers interesting behavior.

Mathematics Subject Classification (2020). 16D60,

Keywords. Finite Rings, Power Sums, Modular Arithmetic

1. Introduction

It is a well-known fact that the sum of cubes of three consecutive integers is always divisible by 9. The divisibility of sums of k^{th} powers of k-many consecutive integers has been well-studied by Ho, Mellblom, and Frodyma [1]. However, properties of sums over the ring of integers modulo n have not; these sums will be the primary focus of this paper.

Throughout the paper, $\mathbb{Z}^+$ will denote the set of positive integers, and $\mathbb{Z}_n$ will denote the ring of integers modulo n for $n \in \mathbb{Z}^+$

Definition 1.1. For $n, k \in \mathbb{Z}^+$, define

$$A_{n,k} := \{(\alpha, ..., \alpha + k - 1) \mid \alpha \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n^k.$$

$A_{n,k}$ is the *set of cyclically consecutive sequences of length k in $\mathbb{Z}_n$.*

With fixed k, each element in $A_{n,k}$ is uniquely determined by the first element α. Since $|\mathbb{Z}_n| = n$, this immediately implies that $|A_{n,k}| = n$, regardless of the choice of k. A more interesting object, however, is a type of sum action over the elements in $A_{n,k}$.

Definition 1.2. For $n, k \in \mathbb{Z}^+$, define

$$S_{n,k} := \left\{ \sum_{i=0}^{k-1} (\alpha + i)^k \mod n \mid \alpha \in \mathbb{Z}_n \right\}.$$

$S_{n,k}$ is the k^{th} *sum set of $\mathbb{Z}_n$.*

*Corresponding Author.
Email addresses: nathan.jonesviolin@uky.edu
Received: January 2, 2023; Accepted: March 1, 2023

The k^{th} sum set of $\mathbb{Z}_n$ will be the primary focus of this paper. There are a few propositions that follow immediately: $|S_{1,k}| = 1$ for all $k \in \mathbb{Z}$, and $|S_{n,1}| = n$ for all $n \in \mathbb{Z}$ since, clearly, $S_{n,1} = \mathbb{Z}_n$. Instances where $|S_{n,k}| = n$ are of particular interest, as regardless of choice of both n and k, we have $|S_{n,k}| = n \iff S_{n,k} = \mathbb{Z}_n$.

To begin analyzing properties of these sum sets, we will first build some theory on sums in $\mathbb{Z}_n$.

Lemma 1.3. *For $\alpha, \beta \in \mathbb{Z}_n$ and $k \in \mathbb{Z}^+$,*

$$\sum_{i=0}^{n-1} (\alpha + i)^k \equiv \sum_{i=0}^{n-1} (\beta + i)^k \mod n$$

Proof. For $\alpha \in \mathbb{Z}_n$,

$$\{\alpha + i \mod n \mid 0 \le i \le n-1\} = \mathbb{Z}_n,$$

which immediately implies

$$\sum_{i=0}^{n-1} (\alpha + i)^k \equiv \sum_{i=0}^{n-1} (\beta + i)^k \mod n$$

□

This result provides a simple description of $S_{n,n}$ for $n \in \mathbb{Z}^+$, and will produce a description of $S_{n,k}$ when $n \mid k$.

Proof. Suppose $\alpha, \beta \in \mathbb{Z}_n$. Since $\alpha \equiv \alpha + n \mod n$, we have

$$|\{\alpha + i \mod n \mid 0 \le i \le n-1\}| = n \quad \forall \alpha \in \mathbb{Z}_n.$$

Since $|\mathbb{Z}_n| = n$, this also implies

$$\{\alpha + i \mod n \mid 0 \le i \le n-1\} = \{\beta + i \mod n \mid 0 \le i \le n-1\},$$

which further implies

$$\{(\alpha + i)^k \mod n \mid 0 \le i \le n-1\}$$
$$= \{(\beta + i)^k \mod n \mid 0 \le i \le n-1\} \text{ for } k \in \mathbb{Z}^+.$$

Since both sets are equivalent, the sum over their respective elements will also be equivalent. Thus,

$$\sum_{i=0}^{n-1} (\alpha + i)^k \equiv \sum_{i=0}^{n-1} (\beta + i)^k \mod n$$

□

Proposition 1.4. *For $n, k \in \mathbb{Z}^+$ where $n > 1$, if $n \mid k$, then $|S_{n,k}| = 1$.*

Proof. Suppose $n|k$. Then $k = m \cdot n$ for some $m \in \mathbb{Z}^+$. Now, consider

$$S_{n,k} = \left\{ \sum_{i=0}^{mn-1} (\alpha + i)^{mn} \mod n \mid \alpha \in \mathbb{Z}_n \right\}.$$

For $\alpha \in \mathbb{Z}_n$, we have

$$\begin{aligned}\sum_{i=0}^{mn-1}(\alpha+i)^{mn} &= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(\alpha+i\cdot n+j)^{mn}\\ &\equiv \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(\alpha+j)^{mn} \mod n\\ &= m\sum_{i=0}^{n-1}(\alpha+i)^{mn} \mod n.\end{aligned}$$

However, by applying Lemma 1, for all $\beta \in \mathbb{Z}_n$,

$$m\sum_{i=0}^{n-1}(\alpha+i)^{mn} \equiv m\sum_{i=0}^{n-1}(\beta+i)^{mn} \mod n.$$

Thus, $|S_{n,k}| = 1$. □

2. Results

Now that some preliminary results have been established, we can begin to examine specific values of n to find values of k such that $|S_{n,k}| = n$.

Proposition 2.1. *For $k \in \mathbb{Z}^+, |S_{3,k}| = 3$ if and only if*

$$k = \begin{cases} 3t+1, & t \text{ is even} \\ 3t+2, & t \text{ is odd.} \end{cases}$$

Proof. Either $k = 3t, k = 3t+1$ or $k = 3t+2$. If $k = 3t$, by Proposition 1, $|S_{3,3t}| = 1$. Before we consider the remaining cases, note that in $\mathbb{Z}_3$,

$$0^m + 1^m + 2^m \equiv \begin{cases} 2 \mod 3, & m \text{ is even} \\ 0 \mod 3, & m \text{ is odd.} \end{cases}$$

First, let $k = 3t+1$. Then there are three such general instances: first, the sequence starts at 0, ends at 0 **(1)**, second, starts at 1, ends at 1 **(2)**, and third, starts at 2, ends at 2 **(3)**. For **(1)**, we have

$$0^k + 1^k + 2^k + 0^k + ... + 1^k + 2^k + 0^k \equiv \begin{cases} 2t \mod 3, & k \text{ is even} \\ 0 \mod 3, & k \text{ is odd.} \end{cases}$$

For **(2)**, we have

$$1^k + 2^k + 0^k + 1^k + ... + 2^k + 0^k + 1^k \equiv \begin{cases} 2t+1 \mod 3, & k \text{ is even} \\ 1 \mod 3, & k \text{ is odd.} \end{cases}$$

For **(3)**, we have

$$2^k + 0^k + 1^k + 2^k + ... + 0^k + 1^k + 2^k \equiv \begin{cases} 2t+1 \mod 3, & k \text{ is even} \\ 2 \mod 3, & k \text{ is odd.} \end{cases}$$

Clearly, if $k = 3t+1$, then $|S_{3,k}| = 3$ if and only if k is odd, which implies that t is even.

Next, let $k = 3t+2$. Then there are again three general instances: first, the sequence starts at 0, ends at 1 **(1)**, second, starts at 1, ends at 2 **(2)**, and third, starts at 2, ends at 0 **(3)**. For **(1)**, we have

$$0^k + 1^k + 2^k + 0^k + 1^k + ... + 2^k + 0^k + 1^k \equiv \begin{cases} 2t+1 \mod 3, & k \text{ is even} \\ 1 \mod 3, & k \text{ is odd.} \end{cases}$$

For **(2)**, we have

$$1^k + 2^k + 0^k + 1^k + 2^k + ... + 0^k + 1^k + 2^k \equiv \begin{cases} 2(t+1) \mod 3, & k \text{ is even} \\ 0 \mod 3, & k \text{ is odd.} \end{cases}$$

For **(3)**, we have

$$2^k + 0^k + 1^k + 2^k + 0^k + ... + 1^k + 2^k + 0^k \equiv \begin{cases} (2t+1) \mod 3, & k \text{ is even} \\ 2 \mod 3, & k \text{ is odd.} \end{cases}$$

Clearly, if $k = 3t + 2$, then $|S_{3,k}| = 3$ if and only if k is odd, which implies t is odd. □

It is of interest to find some criterion by which $|S_{n,k}| = n$ is immediate. From the above result, it is evident that no even value of k satisfies $|S_{3,k}| = 3$, which is a special case of our next result.

Proposition 2.2. *For $n, k \in \mathbb{Z}^+$ where $n > 1$, if $2 \mid k$, then $|S_{n,k}| < n$.*

Proof. For $k \in \mathbb{Z}^+$, suppose $2 \mid k$. First, note that since k is even,

$$(\alpha)^k \equiv (-\alpha)^k \mod n \quad \forall\, \alpha \in \mathbb{Z}_n, \tag{2.1}$$

It suffices to show that $\exists\, \alpha, \beta \in \mathbb{Z}_n$ distinct such that

$$\sum_{i=0}^{k-1} (\alpha + i)^k \equiv \sum_{i=0}^{k-1} (\beta + i)^k \mod n. \tag{2.2}$$

First, suppose $1 \not\equiv (-k) \mod n$. Then by (1), we have

$$(1)^k + ... + (k)^k = (-k)^k + ... + (-1)^k.$$

Using $\overline{-k} \equiv -k \mod n$ where $\overline{-k} \in \{0, ..., n-1\}$, we have

$$\sum_{i=0}^{k-1} (1 + i)^k \equiv \sum_{i=0}^{k-1} (\overline{-k} + i)^k \mod n,$$

meaning 1 and $\overline{-k}$ satisfy (2). But $1 \not\equiv \overline{-k} \mod n$, so we are done.

Next, suppose $1 \equiv (-k) \mod n$. Then

$$1 + k \equiv 0 \mod n \Rightarrow n \text{ is odd and } k \equiv n - 1 \mod n.$$

This also means $n > 2$, so consider distinct elements $0, 2 \in \mathbb{Z}_n$. We have

$$\sum_{i=0}^{k-1} (i)^k = (0)^k + (1)^k + (2)^k + ... + (k-1)^k$$

and

$$\begin{aligned} \sum_{i=0}^{k-1} (2 + i)^k &= (2)^k + ... + (k-1)^k + (k)^k + (k+1)^k \\ &\equiv (2)^k + ... + (k)^k + (0)^k \mod n. \end{aligned}$$

However, since $(1)^k \equiv (-k)^k \equiv (k)^k \mod n$, we have

$$\sum_{i=0}^{k-1} (i)^k \equiv \sum_{i=0}^{k-1} (2 + i)^k \mod n,$$

or that $0, 2 \in \mathbb{Z}_n$ satisfy (2). But $0 \not\equiv 2 \mod n$, meaning we can conclude that if $2 \mid k$, then $|S_{n,k}| < n$ for $n > 1$. □

Next, we will prove a result for k^{th} sum sets of $\mathbb{Z}_p$ where $p \in \mathbb{Z}^+$ is prime

Proposition 2.3. *If $p, t \in \mathbb{Z}^+$ where p is prime, $k = pt-(t-1)$, and $p \nmid k$, then $|S_{p,k}| = p$.*

Proof. For $\alpha \in \mathbb{Z}_p \setminus \{0\}$, since $\alpha^p \equiv \alpha \mod p$, we have

$$\begin{aligned}\alpha^{pt-(t-1)} &\equiv \alpha^{pt} \cdot \alpha^{1-t} \\ &\equiv \alpha^{t} \cdot \alpha^{1-t} \\ &\equiv \alpha \mod p.\end{aligned}$$

Since $(0)^{pt-(t-1)} = 0$, we have that $\alpha^{pt-(t-1)} \equiv \alpha \mod p$ for all $\alpha \in \mathbb{Z}_p$.

Therefore, for $\alpha \in \mathbb{Z}_p$, we have

$$\sum_{i=0}^{t(p-1)} (\alpha+i)^{t(p-1)+1} \equiv \sum_{i=0}^{t(p-1)} \alpha + i \mod p = \sum_{i=0}^{t(p-1)} \alpha + \sum_{i=0}^{t(p-1)} i.$$

The second term is constant, meaning we need only consider the first term. We have

$$\sum_{i=0}^{t(p-1)} \alpha = \alpha(t(p-1)+1).$$

Since $k = t(p-1)+1 \not\equiv 0 \mod p$ and $\mathbb{Z}_p$ is a field, we obtain that $|\{\alpha k \mid \alpha \in \mathbb{Z}_p\}| = p$. Thus,

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

□

3. Conclusion

Note that this does not provide every k such that $|S_{p,k}| = p$ for some prime p. Experimental data suggests that for most primes p, the smallest non-trivial k such that $|S_{p,k}| = p$ is of the form $k = 2p-1$, or the $t = 2$ instance of the above proposition. However, this is not true for all primes. For instance, we have that $|S_{23,5}| = 23$ and $|S_{37,7}| = 37$, meaning that $k = 2p-1$ is not the smallest non-trivial value to have that property. This leads to an interesting open question: for $n \in \mathbb{Z}^+$, what is the smallest non-trivial $k \in \mathbb{Z}^+$ such that $|S_{n,k}| = n$?

Another open problem that has not been resolved is that of the instance when $4 \mid n$. The following has been conjectured through experimental data:

Conjecture 3.1. *For $n, k \in \mathbb{Z}^+$, if $4 \mid n$, then $|S_{n,k}| < n$ for $k > 1$.*

Again through experimental data, the following conjecture suggests the strongest characterization yet of our main problem:

Conjecture 3.2. *For $n, k \in \mathbb{Z}^+$, if $|S_{n,k}| = n$ and $t = n(n-1)+k$, then $|S_{n,t}| = n$.*

This conjecture is immediately true for $S_{p,k}$ where p is prime by using similar techniques from the proof of Proposition 4. However, the general case has not yet been proven. This conjecture would immediately imply that, given $n \in \mathbb{Z}^+$, every instance where $|S_{n,k}| = n$ can be determined by testing finitely many $k \in \mathbb{Z}^+$.

Acknowledgement. This research was supported by NSF Grant No. 1950563.

References

[1] Chungwu Ho, Gregory Mellblom, & Marc Frodyma, *On the sum of powers of consecutive integers*, The College Mathematics Journal, 2020, **51**(4), 295-301.