

Arithmetic progressions in a subset of $\mathbb{Z}/n\mathbb{Z}$ and its complement

Let $n > 3$ be an odd. Consider a subset $S \subseteq \mathbb{Z}/n\mathbb{Z}$. Define $A(S)$ to be the number of length 3 arithmetic progressions in S . That is,

$$A(S) = |\{a, b \in \mathbb{Z}/n\mathbb{Z} \mid b \neq 0; a, a+b, a+2b \in S\}|.$$

Note: this method of counting considers (x, y, z) and (z, y, x) to be different arithmetic progression, and does not consider (x, x, x) to be an arithmetic progression. However, the result still holds under every permutation of these settings.

Let $k = |S|$, and denote the complement of S in $\mathbb{Z}/n\mathbb{Z}$ as S^c , so $|S^c| = n - k$. The total number of arithmetic progressions $A(\mathbb{Z}/n\mathbb{Z})$ is $n(n-1)$. These arithmetic progressions can be split into four groups based on the locations of their elements: all in S , all in S^c , exactly one in S , and exactly one in S^c .

There are $A(S)$ progressions all in S and $A(S^c)$ all in S^c . The number of progressions with exactly one element in S is $3k(k-1) - 3A(S)$ since each ordered pair of elements of S is contained in 3 total progressions, but we need to subtract the contribution of the progressions entirely contained in S , each of which contains 3 ordered pairs. Similarly, the number of progressions with exactly one element in S^c is $3(n-k)(n-k-1) - 3A(S^c)$. Adding everything together, we get

$$n(n-1) = A(S) + (3k(k-1) - 3A(S)) + (3(n-k)(n-k-1) - 3A(S^c)) + A(S^c).$$

Simplifying,

$$A(S) + A(S^c) = \frac{1}{2} (3k(k-1) + 3(n-k)(n-k-1) - n(n-1)).$$

Surprisingly, this sum depends only on n and k .