§ Problem Statement

For every pair of integers $a, b \in \mathbb{Z}^+$ and function $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$, let $\Delta f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ denote the function $n \mapsto f(n+1) - f(n)$. In terms of a and b, determine the number of functions $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ for which $\Delta^N f = f$ for some $N \in \mathbb{Z}^+$.

§ Solution

The answer is

$$b^a \prod_{i=1}^{k} p_i^{-e_i p_i^{\nu_{p_i}(a)}}$$

where $b = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of b.

For every prime p, pair of integers $a, k \in \mathbb{Z}^+$, and function $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$, let $\pi f : \mathbb{Z}/p^{\nu_p(a)}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ denote the function

$$n \mapsto \sum_{\substack{x \in \mathbb{Z}/a\mathbb{Z} \\ x \equiv n \bmod p^{\nu_p(a)}}} f(x).$$

Lemma 1. *Let p be a prime, and let $a, k \in \mathbb{Z}^+$. Then a function $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ satisfies $\Delta^N f = f$ for some $N \in \mathbb{Z}^+$ if and only if $\pi f = 0$.*

Proof.

$\Longrightarrow$ It suffices to show that $\Delta^M \pi f = 0$ for some $M \in \mathbb{Z}_{\geq 0}$, since this would imply

$$\pi f = \pi \Delta^N f = \pi \left(\Delta^N\right)^M f = \pi \left(\Delta^M\right)^N f = \left(\Delta^M\right)^N \pi f = 0.$$

Indeed, choosing $M = kp^{\nu_p(a)}$ suffices, because Kummer's theorem on

$$\begin{aligned}(\Delta^{p^{\nu_p(a)}} \pi f)(x) &= \sum_{i=0}^{p^{\nu_p(a)}} (-1)^i \binom{p^{\nu_p(a)}}{i} (\pi f)(x + p^{\nu_p(a)} - i) \\ &= \sum_{i=1}^{p^{\nu_p(a)}-1} (-1)^i \binom{p^{\nu_p(a)}}{i} (\pi f)(x - i) + \begin{cases} 2(\pi f)(x) & p = 2 \\ 0 & p \text{ odd} \end{cases}\end{aligned}$$

implies $\operatorname{im} \Delta^{p^{\nu_p(a)}} \pi f \subseteq p(\mathbb{Z}/p^k\mathbb{Z})$, so $\operatorname{im} \Delta^{kp^{\nu_p(a)}} \pi f \subseteq p^k(\mathbb{Z}/p^k\mathbb{Z}) = \{0\}$.

$\Longleftarrow$ It suffices to show that for every function $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ satisfying $\pi f = 0$, there is a function $\Sigma f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ satisfying $\pi \Sigma f = 0$ and $\Delta \Sigma f = f$. This is because the pigeonhole principle implies $\Sigma^A f = \Sigma^B f$ for some nonnegative integers $A < B$, so

$$f = \Delta^B \Sigma^B f = \Delta^B \Sigma^A f = \Delta^{B-A} f.$$

Indeed, $g(x) = \sum_{i=0}^{x-1} f(i)$ is well-defined because

$$\sum_{i \in \mathbb{Z}/a\mathbb{Z}} f(i) = \sum_{i \in \mathbb{Z}/p^{\nu_p(a)}\mathbb{Z}} (\pi f)(i) = 0,$$

and πg is some constant function c because $\Delta\pi g = \pi\Delta g = \pi f = 0$. Choosing $\Sigma f = g - d^{-1}c$, where d^{-1} is the inverse of $d = \frac{a}{p^{\nu_p(a)}}$ modulo p^k, works because

$$\Delta\Sigma f = \Delta(g - d^{-1}c) = \Delta g - d^{-1}\Delta c = f - d^{-1}0 = f$$

and

$$\pi\Sigma f = \pi(g - d^{-1}c) = \pi g - d^{-1}\pi c = c - d^{-1}dc = 0. \qquad \square$$

Since a function $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ satisfying $\pi f = 0$ is a unique extension of its first $a - p^{\nu_p(a)}$ inputs, the number of functions $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ for which $\Delta^N f = 0$ for some $N \in \mathbb{Z}^+$ is exactly $(p^k)^{a-p^{\nu_p(a)}}$. By the Chinese remainder theorem, the number of functions $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ for which $\Delta^N f = 0$ for some $N \in \mathbb{Z}^+$ is exactly

$$\prod_{i=1}^{k} (p_i^{e_i})^{a-{p_i}^{\nu_{p_i}(a)}} = b^a \prod_{i=1}^{k} p_i^{-e_i p_i^{\nu_{p_i}(a)}},$$

where $b = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of b.

§ Variants

Variant A. For every pair of integers $a, b \in \mathbb{Z}^+$ and function $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$, let $\Delta f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ denote the function $n \mapsto f(n) + f(n+1)$. In terms of a and b, determine the number of functions $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ for which $\Delta^N f = f$ for some $N \in \mathbb{Z}^+$.

Solution sketch. I am not sure what the answer is.

§ Comments

This problem was inspired by 21M.361, Fall 2022.

§ Metadata

This problem was selected as Problem 3 of the 2023 USA TSTST.

- Title: Iterated Difference Modulo N
- Author: Holden Mui
- Subject: number theory
- Description: count the number of functions that become itself after iterating its finite differences
- Keywords: finite differences, iteration, modular arithmetic
- Difficulty: TSTST 3/6
- Collaborators: Reagan Choi, Rishabh Das, Luke Robitaille, Kevin Zhao
- Date written: November 2022
- Submission history: 2023 TSTST
- Other credits: none