SEMI-SPECIAL PERMUTATIONS II: SEMI-SPECIAL PERMUTATIONS ON $[p^\alpha]$

By K. R. Yacoub

In my paper [1], on semi-special permutations I, I have obtained necessary and sufficient conditions for the existence of non-linear semi-special permutations on $[n]$. (The symbol $[n]$ is used to denote the set of numbers $1, 2, \cdots, n$.)I have also obtained such permutations on $[2p]$, $[p^2]$ and $[pq]$ when p and q are odd primes.

In the present note, I proceed further to obtain the non-linear semi-special permutations on $[p^\alpha]$ when p is an odd prime and $\alpha > 1$. (If p is an odd prime, the semi-special permutations on $[p]$ are all linear [2, Corollary 4.13].) The note is self contained, since I shall state explicitly the requisite definitions and theorems. These are discussed in greater detail in [1] and [2].

1. Definitions and general results.

Definition 1. A permutation π defined on $[n]$ is said to be semi-special if $\pi n = n$ and if, for every $y \in [n]$

$$\pi_y x \equiv \pi(x + y) - \pi y \pmod{n}$$

is again a permutation, namely a power (depending on y) of π.

Definition 2. The permutation π defined by $\pi x \equiv tx \pmod{n}$, where t is some number prime to n, is called a linear permutation.

From this definition, it follows that every linear permutation is semi-special, but the converse is not true. It is, however, interesting to determine the semi-special permutations on $[n]$ which are not linear. This is the main object of the present note when $n = p^\alpha$ and p is an odd prime.

Theorem 1. *Let $n > 2$; then to every semi-special permutation defined on $[n]$ there exists an integer r which divides n such that $1 \leq r < n$ and $\pi_r = \pi$* [2, *Theorem* 4.12].

Theorem 2. *To every semi-special permutation defined on $[n]$, there corresponds a number s which divides n such that the permutation induced mod s is linear* [1, *Theorem* 2.1].

The above two theorems combine to give the principal result.

Conclusion. *The totality of semi-special permutations on $[n]$ (for a given n) which are not linear can be obtained in the following manner:*

(i) *choose a proper divisor of n, call this r, say;*

Received December 21, 1956.