

On semi-special permutations on $[2p^\alpha]$.

By K. R. YACOUB in Alexandria, Egypt.

In an earlier paper [1] on general products of two finite cyclic groups, certain permutations called "semi-special", played a certain role: The permutation π of the numbers $1, 2, \dots, n$ is semi-special¹⁾ 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 .

Examples of semi-special permutations are the linear permutations defined by $\pi x \equiv tx \pmod{n}$, where t is prime to n . As I have shown [2], the linear permutations do not by any mean furnish all the semi-special permutations. If n is a prime number, then all semi-special permutations on $[n]$ are linear ([1], Corollary 4.13); if n is composite, this is not always true.

However, it is of particular interest, though not always possible, to determine those permutations which are not linear. For this purpose, I made a general survey for the theory of semi-special permutations [1], [2].

As an application to the results in [2], § 3, I obtained the non-linear semi-special permutations on $[n]$ when n is the product of two (equal or distinct) prime factors ([2], § 4). Further, in [3], I dealt with the case $n = p^\alpha$ when p is an odd prime and $\alpha > 1$.

In the present note, I obtain the non-linear semi-special permutations on $[2p^\alpha]$ where p is an odd prime and $\alpha \geq 1$. In order that the paper may be self contained, I collect in § 1 the results that will be required here.

§ 1.

We start with the following theorem:

To every semi-special permutation π on $[n]$ which is not linear, there corresponds a number s ($1 < s < n$) dividing n , such that $\pi_s = \pi$ and the permutation induced mod s is linear ([2], Conclusion 2.3).

¹⁾ We write permutations as left hand operators and denote the set of numbers $1, 2, \dots, n$ by $[n]$.

We remark that, with this value of s , $\pi_{s'} = \pi$ for every multiple s' of s ([1], Theorem 4.4) but π is not necessarily linear mod s' . This suggested to me the following definition.

Definition. The maximal divisor s of n for which $\pi_s = \pi$ and π is linear mod s is called the principal number of π ([2], Definition 2.4).

We require further the following two theorems.

Theorem 1. *If there is a non-linear semi-special permutation π on $[n]$, with principal number s , and if π induces mod s the identity permutation, then π can be written in the form*

$$(1) \quad \pi x \equiv x + s\lambda(1 + \omega + \dots + \omega^{x-1}) \pmod{n},$$

where λ is a number prime to N , $N = \frac{n}{s}$, and where

$$(2) \quad \omega^s - 1 \equiv 0 \pmod{N}, \quad \omega - 1 \not\equiv 0 \pmod{N}.$$

Conversely, if λ is prime to N and if ω satisfies (2), then (1) defines a non-linear semi-special permutation of the desired type ([2], Theorem 3.1).

Theorem 2. *If there is a non-linear semi-special permutation π on $[n]$, with principal number s , if π induces mod s a linear permutation other than the identity and if $\pi 1 = t$, then t is prime to n and π can be written in the form*

$$(3) \quad \pi x \equiv tx + s\psi(x) \pmod{n}$$

with

$$(4) \quad \psi(1) \equiv 0 \pmod{N}, \quad \psi(x) \equiv R \sum_{i=1}^{x-1} (x-i)\theta^{i-1} \pmod{N}, \quad x \geq 2,$$

where R is prime to N , $N = \frac{n}{s}$, and

$$(5) \quad 1 + \theta + \dots + \theta^{s-1} \equiv 0 \pmod{N}.$$

Moreover, if h is the order of t mod s , and u is defined mod N by $t^h \equiv 1 + us \pmod{n}$, then

$$(6) \quad u + \sum_{i=0}^{h-1} t^{h-i-1} \psi(t^i) \text{ is prime to } N;$$

$$(7) \quad u(\theta - 1) \equiv \sum_{i=0}^{h-1} t^{h-i-1} \{\psi(2t^i) - (\theta + 1)\psi(t^i)\} \pmod{N};$$

$$(8) \quad \sum_{i=0}^{h-1} t^{h-i-1} (1 + \theta + \dots + \theta^{s-1})^2 (\theta^{t^i} - \theta^r) \equiv 0 \pmod{N}, \quad r = 1, \dots, s.$$

Conversely, if t is prime to n , R is prime to N , and if θ, t, R are chosen such that (5)–(8) are satisfied, then (3) defines a non-linear semi-special permutation of the desired type ([2], Theorem 3.10).

§ 2.

In this section we describe briefly our problem. Let p be an odd prime, α be a positive integer and let π denote, if any, a non-linear semi-special permutation on $[2p^\alpha]$. If s is the principal number of π , then by the definition, given in § 1, s is a proper divisor of $2p^\alpha$; therefore s may have the values $2, p^\beta$ with $1 \leq \beta \leq \alpha$ and $2p^\beta$ with $1 \leq \beta < \alpha$. We have thus three cases to consider. In the following sections, we put $N = \frac{2p^\alpha}{s}$.

§ 3. The case $s = 2, N = p^\alpha$.

In this case, π induces mod 2 the identity permutation and by Theorem 1 a number ω exists such that

$$\omega^2 - 1 \equiv 0 \pmod{p^\alpha}, \quad \omega - 1 \not\equiv 0 \pmod{p^\alpha},$$

i. e. such that $\omega \equiv -1 \pmod{p^\alpha}$. Thus if λ is prime to p , then by Theorem 1, π can be written in the form

$$\pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p^\alpha}.$$

We now have

Theorem 3. *If π is a non-linear semi-special permutation on $[2p^\alpha]$ with principal number 2, then it is of the form*

$$\pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p^\alpha},$$

where λ is prime to p .

§ 4. The case $s = p^\beta, N = 2p^{\alpha-\beta}$ ($1 \leq \beta \leq \alpha$).

We have two possibilities:

(i) If π induces mod p^β the identity permutation, then by Theorem 1 there exists a number ω such that

$$\omega^{p^\beta} - 1 \equiv 0 \pmod{2p^{\alpha-\beta}}, \quad \omega - 1 \not\equiv 0 \pmod{2p^{\alpha-\beta}}.$$

These congruences cannot be satisfied simultaneously unless $\alpha - \beta > 1$, i. e. unless $\beta < \alpha - 1$; in this case, it is not difficult to see that

$$(9) \quad \omega \equiv 1 + 2\Omega p^\gamma \pmod{2p^{\alpha-\beta}},$$

where Ω is prime to p ; $\gamma = 1, \dots, \alpha - \beta - 1$ if $2\beta \geq \alpha$ and $\gamma = \alpha - 2\beta, \dots, \alpha - \beta - 1$ if $2\beta < \alpha$. Thus if $\beta < \alpha - 1$ and ω is given by (9), then by Theorem 1 π has the form

$$\pi x \equiv x + \lambda p^\beta (1 + \omega + \dots + \omega^{x-1}) \pmod{2p^\alpha},$$

where λ is prime to $2p$. On substitution for ω , we find that

$$\pi x \equiv x + \lambda p^\beta \sum_{i=1}^x \binom{x}{i} (2\Omega p^\gamma)^{i-1} \pmod{2p^\alpha}.$$

(ii) Next, we show that π cannot induce mod p^β a linear permutation other than the identity. This is easily seen because equation (5), in our case, reduces to

$$1 + \theta + \dots + \theta^{p^\beta-1} \equiv 0 \pmod{2p^{\alpha-\beta}},$$

which has no solution.

We have thus shown

Theorem 4. *There is no semi-special permutation on $[2p^\alpha]$ with principal number p^β for $\beta = \alpha - 1, \alpha$. Further, if π is such a permutation with $1 \leq \beta \leq \alpha - 2$, then it is of the form*

$$\pi x \equiv x + \lambda p^\beta \sum_{i=1}^x \binom{x}{i} (2\Omega p^\gamma)^{i-1} \pmod{2p^\alpha},$$

where λ is prime to $2p$, Ω is prime to p ; $\gamma = 1, \dots, \alpha - \beta - 1$ if $2\beta \geq \alpha$ and $\gamma = \alpha - 2\beta, \dots, \alpha - \beta - 1$ if $2\beta < \alpha$.

§ 5. The case $s = 2p^\beta$, $N = p^{\alpha-\beta}$ ($1 \leq \beta < \alpha$).

(i) Suppose first that π induces mod $2p^\beta$ the identity permutation, then by Theorem 1 a number ω exists such that

$$(10) \quad \omega^{2p^\beta} - 1 \equiv 0 \pmod{p^{\alpha-\beta}}, \quad \omega - 1 \not\equiv 0 \pmod{p^{\alpha-\beta}}.$$

Now since $\beta < \alpha$, then by the first of (10) $\omega^2 \equiv 1 \pmod{p}$, i. e. $\omega \equiv \pm 1 \pmod{p}$. Let $\omega \equiv 1 \pmod{p}$ or precisely $\omega \equiv 1 + \Omega p^\gamma \pmod{p^{\alpha-\beta}}$ where Ω is prime to p and $\gamma \geq 1$. The second of (10) requires $\gamma < \alpha - \beta$ i. e. $\alpha - \beta > 1$, and by the first of (10) we see that $\gamma = 1, \dots, \alpha - \beta - 1$ if $2\beta \geq \alpha$ and $\gamma = \alpha - 2\beta, \dots, \alpha - \beta - 1$ if $2\beta < \alpha$. Thus, provided that $\beta < \alpha - 1$, if λ is prime to p , then by Theorem 1, π can be written in the form

$$\pi x \equiv x + 2p^\beta \lambda \sum_{i=1}^x \binom{x}{i} (\Omega p^\gamma)^{i-1} \pmod{2p^\alpha}.$$

Next, let $\omega \equiv -1 \pmod{p}$, or precisely $\omega \equiv -1 + \Omega p^\delta \pmod{p^{\alpha-\beta}}$ with Ω prime to p . By the first of (10), we see that $\delta = 1, \dots, \alpha - \beta$ if $2\beta \geq \alpha$ and $\delta = \alpha - 2\beta, \dots, \alpha - \beta$ if $2\beta < \alpha$. In this case $\omega^2 \equiv 1 + \Delta p^\delta \pmod{p^{\alpha-\beta}}$ say,

where $\Delta \equiv -2\Omega + \Omega^2 p^\delta \pmod{p^{\alpha-\beta-\delta}}$. Then

$$(11) \quad \left\{ \begin{array}{l} 1 + \omega + \dots + \omega^{2x-1} = (1 + \omega)(1 + \omega^2 + \dots + (\omega^2)^{x-1}) \\ \equiv \Omega p^\delta \sum_{i=1}^x \binom{x}{i} (\Delta p^\delta)^{i-1} \pmod{p^{\alpha-\beta}} \\ \text{and } 1 + \omega + \dots + \omega^{2x} \equiv \Omega p^\delta \sum_{i=1}^x \binom{x}{i} (\Delta p^\delta)^{i-1} + (1 + \Delta p^\delta)^x \pmod{p^{\alpha-\beta}}. \end{array} \right.$$

Thus if λ is prime to p , then by Theorem 1 and by using (11), we see that π is of the form

$$\pi(2x) \equiv 2x + 2\lambda\Omega p^{\beta+\delta} \sum_{i=1}^x \binom{x}{i} (\Delta p^\delta)^{i-1} \pmod{2p^\alpha},$$

$$\pi(2x+1) \equiv 2x+1 + 2\lambda\Omega p^{\beta+\delta} \sum_{i=1}^x \binom{x}{i} (\Delta p^\delta)^{i-1} + 2\lambda p^\beta (1 + \Delta p^\delta)^x \pmod{2p^\alpha}.$$

We have thus shown

Theorem 5. *If π is a non-linear semi-special permutation on $[2p^\alpha]$ with principal number $2p^\beta$ ($1 \leq \beta < \alpha$) and if π induces mod $2p^\beta$ the identity permutation, then it is of the form*

$$\pi x \equiv x + 2p^\beta \lambda \sum_{i=1}^x \binom{x}{i} (\Omega p^\gamma)^{i-1} \pmod{2p^\alpha}, \text{ provided } \beta < \alpha - 1;$$

or

$$\pi(2x) \equiv 2x + 2\lambda\Omega p^{\beta+\delta} \sum_{i=1}^x \binom{x}{i} (\Delta p^\delta)^{i-1} \pmod{2p^\alpha},$$

$$\pi(2x+1) \equiv 2x+1 + 2\lambda\Omega p^{\beta+\delta} \sum_{i=1}^x \binom{x}{i} (\Delta p^\delta)^{i-1} + 2\lambda p^\beta (1 + \Delta p^\delta)^x \pmod{2p^\alpha},$$

where λ and Ω are any numbers prime to p , $\Delta \equiv -2\Omega + \Omega^2 p^\delta \pmod{p^{\alpha-\beta-\delta}}$, and where

$$\begin{array}{ll} \gamma = 1, \dots, \alpha - \beta - 1; \delta = 1, \dots, \alpha - \beta, & \text{if } 2\beta \geq \alpha; \\ \text{and} & \\ \gamma = \alpha - 2\beta, \dots, \alpha - \beta - 1; \delta = \alpha - 2\beta, \dots, \alpha - \beta & \text{if } 2\beta < \alpha. \end{array}$$

(ii) Next, suppose that π induces mod $2p^\beta$ a linear permutation other than the identity. Then, by Theorem 2, there exists a number θ such that

$$(12) \quad 1 + \theta + \dots + \theta^{2p^\beta-1} \equiv 0 \pmod{p^{\alpha-\beta}},$$

i. e. such that $\theta^{2p^\beta} - 1 \equiv 0 \pmod{p^{\alpha-\beta}}$ and so $\theta \equiv \pm 1 \pmod{p}$.

If $\theta \equiv -1 \pmod{p}$, we show that conditions (6) and (7) (of Theorem 2) contradict each other. This can be easily shown if²⁾ we take $\psi(x) \pmod{p}$

²⁾ This is available since N is a power of p .

in (6) and each term mod p in (7). In this case (see Theorem 2, (4))

$$\psi(x) \equiv R \sum_{i=1}^{x-1} (x-i)(-1)^{i-1} \pmod{p},$$

and thus

$$(13) \quad \psi(2x) \equiv Rx \pmod{p}, \quad \psi(2x+1) \equiv Rx \pmod{p}.$$

It is convenient, here, to remind the reader that, in the case under consideration, t is prime to $2p$, $t \not\equiv 1 \pmod{2p^\beta}$ and that h is the order of t mod $2p^\beta$, and accordingly $\frac{t^h-1}{t-1} \equiv 0 \pmod{p}$.

Now by using (13) and remembering that t is odd, we have

$$\begin{aligned} u + \sum_{i=0}^{h-1} t^{h-i-1} \psi(t^i) &\equiv u + \frac{1}{2} R \sum_{i=0}^{h-1} t^{h-i-1} (t^i - 1) \pmod{p}, \\ &\equiv u + \frac{1}{2} R \left\{ h t^{h-1} - \frac{t^h - 1}{t - 1} \right\} \pmod{p}, \\ &\equiv u + \frac{1}{2} R h t^{h-1} \pmod{p}, \end{aligned}$$

because $\frac{t^h-1}{t-1} \equiv 0 \pmod{p}$. Hence (6) is secured if $u + \frac{1}{2} R h t^{h-1}$ is prime to p . Furthermore (7), with each term reduced mod p , gives

$$-2u \equiv R \sum_{i=0}^{h-1} t^{h-i-1} t^i \pmod{p}, \quad \text{i. e.} \quad 2u + R h t^{h-1} \equiv 0 \pmod{p};$$

this contradicts (6). Thus $\theta \not\equiv -1 \pmod{p}$.

Now, it remains to discuss the case $\theta \equiv 1 \pmod{p}$. Let $\theta \equiv 1 + \Theta p^\gamma \pmod{p^{\alpha-\beta}}$, where Θ is prime to p and $\gamma \geq 1$. This value of θ satisfies (12) provided that $2\beta \geq \alpha$ and $\gamma = 1, \dots, \alpha - \beta$. In this case (see Theorem 2, (4)), if we substitute for θ , $\psi(x)$ can be written in the form

$$(14) \quad \psi(x) \equiv R \sum_{i=0}^{x-2} a_{x,i} (\Theta p^\gamma)^i \pmod{p^{\alpha-\beta}}, \quad x \geq 2.$$

Moreover, from (4), we deduce

$$(15) \quad \psi(x+1) - \psi(x) \equiv R(1 + \theta + \dots + \theta^{x-1}) \pmod{p^{\alpha-\beta}}.$$

In (15), if we put $\theta \equiv 1 + \Theta p^\gamma \pmod{p^{\alpha-\beta}}$, substitute from (14) for $\psi(x)$ and $\psi(x+1)$ and compare the coefficients of $(\Theta p^\gamma)^i$ on both sides we obtain

$$(16) \quad a_{x+1,i} - a_{x,i} = \binom{x}{i+1}, \quad i = 0, 1, \dots, x-2;$$

and

$$(17) \quad a_{x+1,x-1} = 1.$$

Now, if we write down (16) for $x=i+2, \dots, y$ then add together and use (17) with $x=i+1$, we obtain

$$a_{y+1,i} = 1 + \binom{i+2}{i+1} + \dots + \binom{y}{i+1} = \binom{y+1}{i+2}, \quad \text{i. e. } a_{x,i} = \binom{x}{i+2},$$

and thus

$$(18) \quad \psi(x) \equiv R \sum_{i=0}^{x-2} \binom{x}{i+2} (\Theta p^\gamma)^i \pmod{p^{\alpha-\beta}}, \quad x \geq 2.$$

Now, we turn to the conditions of Theorem 2. Since N is a power of p , (6) will be secured if $\psi(x)$ is taken mod p . From (18), we see that

$$\psi(x) \equiv \frac{1}{2} R x(x-1) \pmod{p},$$

and, as we have done before, (6) is thus secured if

$$(19) \quad u - \frac{1}{2} R h t^{h-1} \text{ is prime to } p.$$

Further (7) may be written

$$(20) \quad \left\{ u + \sum_{i=0}^{h-1} t^{h-i-1} \psi(t^i) \right\} (\theta - 1) \equiv \sum_{i=0}^{h-1} t^{h-i-1} \{ \psi(2t^i) - 2\psi(t^i) \} \pmod{p^{\alpha-\beta}}.$$

Using (4) and substituting for θ , we get

$$(21) \quad \begin{aligned} \psi(2x) - 2\psi(x) &\equiv R(1 + \theta + \dots + \theta^{x-1})^2 \\ &\equiv R \left\{ \sum_{j=0}^{x-1} \binom{x}{j+1} (\Theta p^\gamma)^j \right\}^2 \pmod{p^{\alpha-\beta}}. \end{aligned}$$

Then by substituting for $\psi(t^i)$ from (18), for $\psi(2t^i) - 2\psi(t^i)$ from (21); putting $\theta \equiv 1 + \Theta p^\gamma \pmod{p^{\alpha-\beta}}$ and remembering that $\psi(1) \equiv 0$, $\psi(2) \equiv R \pmod{p^{\alpha-\beta}}$ (see Theorem 2, (4)), (20) will become

$$(22) \quad \begin{aligned} u \Theta p^\gamma + R \sum_{i=1}^{h-1} t^{h-i-1} \sum_{j=0}^{t^i-2} \binom{t^i}{j+2} (\Theta p^\gamma)^{j+1} \\ \equiv R t^{h-1} + R \sum_{i=1}^{h-1} t^{h-i-1} \left\{ \sum_{j=0}^{t^i-1} \binom{t^i}{j+1} (\Theta p^\gamma)^j \right\}^2 \pmod{p^{\alpha-\beta}}. \end{aligned}$$

Lastly, (8) on substitution for θ , requires that

$$(23) \quad \sum_{i=0}^{h-1} t^{h-i-1} \left\{ \sum_{j=0}^{t^i-1} \binom{t^i}{j+1} (\Theta p^\gamma)^j \right\}^2 \sum_{s=1}^{r t^i} \left\{ \binom{r t^i}{s} - \binom{r}{s} \right\} (\Theta p^\gamma)^s \equiv 0 \pmod{p^{\alpha-\beta}},$$

$r = 1, \dots, 2p^\beta,$

where $\binom{r}{s}$ is the usual binomial coefficient when $s \leq r$ and is zero otherwise.

Thus, by Theorem 2, if t is prime to $2p$, $t \not\equiv 1 \pmod{2p^\beta}$; R , Θ are both prime to p and are chosen such that (19), (22) and (23) are satisfied, then π will be of the form

$$\pi 1 \equiv t, \quad \pi x \equiv tx + 2p^\beta R \sum_{i=0}^{x-2} \binom{x}{i+2} (\Theta p^\gamma)^i \pmod{2p^\alpha}, \quad x \geq 2.$$

We have thus shown

Theorem 6. *If there is a non-linear semi-special permutation π on $[2p^a]$, with principal number $2p^\beta$, and if π induces mod $2p^\beta$ a linear permutation other than the identity, then $\frac{\alpha}{2} \leq \beta < \alpha$, and π is of the form*

$$\pi 1 \equiv t, \quad \pi x \equiv tx + 2p^\beta R \sum_{i=0}^{x-2} \binom{x}{i+2} (\Theta p^\gamma)^i \pmod{2p^\alpha}, \quad x \geq 2,$$

with $\gamma = 1, \dots, \alpha - \beta$; where t is prime to $2p$, $t \not\equiv 1 \pmod{2p^\beta}$ and Θ , R are both prime to p and are chosen such that (19), (22) and (23) are satisfied, h being the order of $t \pmod{2p^\beta}$ and u being defined mod $p^{\alpha-\beta}$ by $t^h \equiv 1 + 2p^\beta u \pmod{2p^\alpha}$.

Conclusion: Theorems 3, 4, 5 and 6 supply us with all the non-linear semi-special permutations on $[2p^a]$.

We remark that Theorem 4 does not furnish such permutations unless $\alpha \geq 3$; Theorems 5 and 6 unless $\alpha \geq 2$.

We conclude by describing the non-linear semi-special permutations on $[2p^a]$ when $\alpha = 1, 2, 3$.

By the above note, if $\alpha = 1$, the non-linear semi-special permutations on $[2p]$ are described in Theorem 3. We now have

Theorem 7. *The non-linear semi-special permutations on $[2p]$ are of the form*

$$\pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p},$$

where λ is prime to p .

Next let $\alpha = 2$. Then (see the above note) the non-linear semi-special permutations are described in Theorems 3, 5 and 6.

By Theorem 5, there is one value for β , namely $\beta = 1$; this yields $\delta = 1$ but no γ and the corresponding permutation is of the form

$$\pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2p\lambda \pmod{2p^2},$$

where λ is prime to p .

Further, by Theorem 6, we have $\beta = 1$, $\gamma = 1$, and the induced permutation is given by

$$\pi 1 \equiv t, \quad \pi x \equiv tx + 2pR \cdot \frac{1}{2} x(x-1) \pmod{2p^2}, \quad x \geq 2,$$

i. e. by

$$\pi x \equiv tx + pRx(x-1) \pmod{2p^2},$$

where t is prime to $2p$, and R is prime to p and are chosen such that (19), (22) and (23) are satisfied. Since $\gamma=1$, $\alpha-\beta=1$, then (23) is satisfied identically. Further, (22) reduces, in this case, to

$$0 \equiv R t^{h-1} \frac{t^h - 1}{t - 1} \pmod{p},$$

which is also satisfied since h is the order of $t \pmod{2p}$ and $t \not\equiv 1 \pmod{p}$.

We now have

Theorem 8. *The non-linear semi-special permutations on $[2p^2]$ are:*

$$\pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p^2};$$

$$\pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2p\lambda \pmod{2p^2};$$

and

$$\pi x \equiv tx + pRx(x-1) \pmod{2p^2},$$

where λ is prime to p , t is prime to $2p$ ($t \not\equiv 1 \pmod{2p}$), R is prime to p and are chosen such that $u - \frac{1}{2} R h t^{h-1}$ is prime to p , h being the order of $t \pmod{2p}$ and u being defined $\pmod{p}$ by $t^h \equiv 1 + 2pu \pmod{2p^2}$.

Lastly, let $\alpha=3$. Theorem 3 supplies us with the permutations

$$(24) \quad \pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p^2},$$

where λ is prime to p .

Further, Theorem 4 gives $\beta=1$, $\gamma=1$ and the corresponding permutations are

$$(25) \quad \pi x \equiv x + \lambda p \left\{ x + \frac{1}{2} x(x-1) \cdot 2\Omega p \right\} \pmod{2p^3},$$

where λ is prime to $2p$, and Ω is prime to p .

Also, Theorem 5 gives $\beta=1, 2$. If $\beta=1$, we have $\gamma=1$, $\delta=1, 2$; while if $\beta=2$, we have $\delta=1$, but no γ . Then the permutations described in Theorem 5 will be

$$(26) \quad \pi x \equiv x + 2p\lambda \left\{ x + \frac{1}{2} x(x-1)\Omega p \right\} \pmod{2p^3};$$

$$(27) \quad \begin{cases} \pi(2x) \equiv 2x + 2\lambda\Omega p^2 x \pmod{2p^3}, \\ \pi(2x+1) \equiv 2x+1+2\lambda\Omega p^2 x + 2\lambda p(1+x\Delta p) \pmod{2p^3} \\ \quad \equiv 2x+1+2\lambda p - 2\lambda\Omega p^2 x \pmod{2p^3}; \end{cases}$$

because $\Delta \equiv -2\Omega \pmod{p}$;

$$(28) \quad \pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda p \pmod{2p^3};$$

$$(29) \quad \pi(2x) \equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda p^2 \pmod{2p^3};$$

where in (26), (27), (28) and (29), λ and Ω are both prime to p .

Moreover, Theorem 6 gives $\beta=2$, $\gamma=1$, and the induced permutations will be

$$(30) \quad \pi 1 \equiv t, \quad \pi x \equiv tx + 2p^2 R \cdot \frac{1}{2} x(x-1) \pmod{2p^3}, \quad x \geq 2,$$

where t is prime to $2p$ (with $t \not\equiv 1 \pmod{2p^2}$) and R is prime to p , and are chosen such that (19), (22) and (23) are satisfied. Now, since $\alpha-\beta=1$ and $\gamma=1$, then (23) is satisfied identically. Furthermore, (22) in this case reduces to

$$0 \equiv R t^{h-1} \frac{t^h - 1}{t - 1} \pmod{p}$$

which is also satisfied since h is the order of $t \pmod{2p^2}$ and $t \not\equiv 1 \pmod{p}$ (note that t is odd). Thus t and R must be chosen such that $u - \frac{1}{2} R h t^{h-1}$ is prime to p .

To sum up, we observe that the permutations given by (26) can be obtained from (25) if we put 2λ instead of λ and Ω instead of 2Ω . Moreover the permutations given by (28) and (29) can be obtained from (24) if λ takes all possible values which are less than p^3 . We now have

Theorem 9. *The non-linear semi-special permutations on $[2p^3]$ are*

$$\begin{aligned} \pi(2x) &\equiv 2x, \quad \pi(2x+1) \equiv 2x+1+2\lambda \pmod{2p^3}, & 1 \leq \lambda < p^3; \\ \pi x &\equiv x + p\lambda x + x(x-1)p^2\lambda\Omega \pmod{2p^3}, & \lambda \text{ and } \Omega \text{ being prime to } p; \\ \pi(2x) &\equiv 2x + 2\lambda\Omega p^2 x \pmod{2p^3}, \\ \pi(2x+1) &\equiv 2x+1+2\lambda p - 2\lambda\Omega p^2 x \pmod{2p^3} \end{aligned} \quad \left\{ \begin{array}{l} \lambda \text{ and } \Omega \text{ being prime to } p; \end{array} \right.$$

and

$$\pi x \equiv tx + p^2 R x(x-1) \pmod{2p^3},$$

where t is prime to $2p$ ($t \not\equiv 1 \pmod{2p^2}$) and R is prime to p and are chosen such that $u - \frac{1}{2} R h t^{h-1}$ is prime to p , h being the order of $t \pmod{2p^2}$ and u being defined mod p by $t^h \equiv 1 + 2p^2 u \pmod{2p^3}$.

Bibliography.

- [1] K. R. YACOUB, General products of two finite cyclic groups, *Proc. Glasgow Math. Assoc.* **2** (1955), 116–123.
- [2] K. R. YACOUB, On semi-special permutations I., *Proc. Glasgow Math. Assoc.* **3** (1956), 18–35.
- [3] K. R. YACOUB, Semi-special permutations II., *Duke Math. J.* **24** (1957), 455–465.

(Received July 30, 1957.)