ON SEMI-SPECIAL PERMUTATIONS I

by K. R. YACOUB

(Received 30th May, 1955)

In an earlier paper [1] on groups which are the products of two finite cyclic groups with trivial intersection, certain permutations, called " semi-special ", played a certain role. The permutation π of the numbers 1, 2, ... , n is 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.

Examples of semi-special permutations are the linear permutations defined by $\pi x \equiv rx \pmod{n}$, where r is prime to n. If n is a prime number, then all semi-special permutations on $[n]$ are linear (see [1], Corollary 4.13). If n is composite, the determination of all semi-special permutations is much more difficult.

The aim of the present paper is to advance their study far enough to permit their determination when n is the product of two (equal or distinct) prime factors.

Although the motivation of this investigation is group theoretical, the present paper is only concerned with arithmetical properties of permutations, and no group theory occurs in it. In order that it may be self-contained we put together in § 1 those notations and results of [1] that will be required here.

Throughout this paper, congruences that occur with no modulus stated are to be understood to be modulo n. An expression like $\dfrac{d^x - 1}{d-1}$ is to be interpreted as an abbreviation for $1 + d + \ldots + d^{x-1}$.

1. Notations and preliminary results.

1.1 LEMMA : *If* $\pi 1 \equiv 1$, *then* $\pi = \iota$ ([1], Lemma 3.1).

1.2 LEMMA : $(\pi^r)_u$ *is a power of* π *for all* r *and* u ([1], Lemma 3.3).

We denote $(\pi^r)_u$ by $\pi^{\tau(r,u)}$, where $\tau(r, u)$ is determined modulo k, the order of π.

1.3 LEMMA : *With the above notation*

$$\tau(r, u+v) \equiv \tau(\tau(r, u), v) \pmod{k}, \quad \ldots\ldots(1.4)$$

$$\tau(r+s, u) \equiv \tau(r, \pi^s u) + \tau(s, u) \pmod{k} \quad \ldots\ldots(1.5)$$

([1], Lemma 3.4).

1.6 LEMMA : *With the same notation*

(i) *if* $\tau(r, u) \equiv \tau(r, v) \pmod{k}$, *then*

$$\tau(r, v-u) \equiv r \pmod{k}; \quad \ldots\ldots(1.7)$$

(ii) *if* $\tau(r, u) \equiv r \pmod{k}$, *then, for all* y *and* z,

$$\tau(r, uy+z) \equiv \tau(r, z) \pmod{k} \quad \ldots\ldots(1.8)$$

([1], Lemma 3.7).

1.9 THEOREM : *Let* π *be a permutation (which is not necessarily semi-special). If* $\pi_u = \pi$ *for some number* u, *then, for all* y *and* z,

$$\pi y u = y \pi u,$$

$$\pi_{yu+z} = \pi_z, \quad \pi_{yu} = \pi.$$

([1], Theorem 4.4).

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

1.10 COROLLARY : *If π is semi-special on $[n]$ and if u is some divisor of n such that $\pi_u = \pi$, then $\pi u \equiv ud$, where $(ud, n) = u$. Moreover, π permutes multiples of u among themselves* ([1], Corollary 4.8).

1.11 LEMMA : *Let π be a semi-special permutation defined on $[n]$. If u is some divisor of n such that $\pi_u = \pi$, then π defines modulo u a semi-special permutation ρ by $\rho x \equiv \pi x \pmod{u}$* ([1], Lemma 4.9).

1.12 THEOREM : *Let π be a permutation (which is not necessarily semi-special) defined on the range $[n]$. If $\pi_u = \pi$ for some number u which is prime to n, then π is a linear permutation.*

Conversely, if π is a linear permutation, then $\pi_u = \pi$ for every u; therefore a linear permutation is semi-special ([1], Theorem 4.10).

1.13 THEOREM : *Let $n > 2$; then to every semi-special permutation defined on $[n]$ there exists an integer r which divides n, such that*

$$1 \leqslant r < n \quad \text{and} \quad \pi_r = \pi.$$

([1], THEOREM 4.12).

1.14 COROLLARY: *If p is an odd prime number, the semi-special permutations on $[p]$ are all linear* ([1], Corollary 4.13).

2. Some constructive properties of semi-special permutations.

2.1 THEOREM : *To every semi-special permutation defined on a given range $[n]$, there corresponds a number s which divides n such that the permutation induced modulo s is linear.*

Proof : If π is linear, the theorem is obvious with $s = n$. If π is not linear, then $\pi_1 \neq \pi$, by Theorem 1.12. In this case there exists a proper divisor n_1 of n such that $\pi_{n_1} = \pi$ (Theorem 1.13). Moreover, by Lemma 1.11, the permutation $\pi^{(1)}$ defined on $[n_1]$ by

$$\pi^{(1)} x \equiv \pi x \pmod{n_1}$$

is semi-special. If $\pi^{(1)}$ is linear, the theorem is proved with $s = n_1$; otherwise we repeat the same process. In this way we obtain a sequence of integers $n_0 = n, n_1, n_2, \ldots, n_i, \ldots$ together with a sequence of permutations $\pi^{(0)} = \pi, \pi^{(1)}, \pi^{(2)}, \ldots, \pi^{(i)}, \ldots$ defined by

$$\pi^{(i+1)} x \equiv \pi^{(i)} x \pmod{n_{i+1}},$$

where $\pi^{(i)}_{n_{i+1}} = \pi^{(i)}$, $1 < n_{i+1} < n_i$, $n_{i+1} \mid n_i$.

Observing that the sequence $n_0, n_1, n_2, \ldots, n_i, \ldots$ decreases monotonically, we see that the process may be repeated until we arrive at a linear permutation $\pi^{(t)}$; this happens at the latest when n_t is a prime. The theorem then follows if we take $s = n_t$, and remark that $\pi^{(t)} x \equiv \pi x \pmod{n_t}$.

The above theorem and Theorem 1.13 together imply the following :

2.2 CONCLUSION : *The totality of semi-special permutations on a given range $[n]$ which are not linear can be obtained in the following manner:*

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

(ii) *determine all the semi-special permutations π for which $\pi_r = \pi$ and the permutations induced modulo r are linear;*

(iii) *make r take all its possible values.*

From the above conclusion, we deduce the following

2.3 CONCLUSION : *To every semi-special permutation 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 modulo s is linear.*

If s is such a number, then by Theorem 1.9 it follows that $\pi_{s'} = \pi$ for every multiple s' of s, but π is not necessarily linear modulo s'.

2.4 DEFINITION : *The maximal divisor s of n for which $\pi_s = \pi$ and π is linear modulo s is called the principal number of π.*

If π is linear on $[n]$, its principal number is n.

2.5 LEMMA : *If π is a non-linear semi-special permutation on $[n]$, then it is of the form*

$$\pi x \equiv tx + sf(x)$$

for suitable s, t; and there is at most one π with given values of s, t (mod n), $f(1)$, $f(2)$, ..., $f(s)$ (mod n/s).

Proof: Let the principal number of π be s. By hypothesis π is non-linear; therefore $s<n$. Moreover, π is linear modulo s ; *i.e.*, $\pi x \equiv tx$ (mod s), where t is prime to s. Thus we can write

$$\pi x \equiv tx + sf(x), \quad \text{.....(2.6)}$$

where $f(x)$ is to be determined modulo n/s.

There is at most one π with given values of s, t (mod n), $f(1)$, $f(2)$, ..., $f(s)$ (mod n/s). This is obvious ; for, by the definition of s, $\pi_s = \pi$, and, by Theorem 1.9, it follows that

$$\pi ys \equiv y\pi s, \quad \pi(x+ys) \equiv \pi x + \pi ys. \quad \text{.....(2.7)}$$

Then (2.6) and (2.7), taken together, define π uniquely in terms of the given values s, t (mod n), $f(1), f(2), \ldots, f(s)$ (mod n/s). This proves the lemma.

For convenience of notation, we write $N = n/s$, $d \equiv t + f(s)$ (mod N) ; then† $\pi s \equiv sd$, and (2.7) can be written

$$\pi ys \equiv ysd, \quad \pi(x+ys) \equiv \pi x + ysd. \quad \text{.....(2.8)}$$

With the notation of Lemma 2.5, we prove the following results :

2.9 LEMMA : (i) *If $t \not\equiv 1$ (mod s) and if h is the order of t modulo s, then*

$$\pi^{ih+j}x \equiv t^j x + s\left\{F(x,j) + d^j \frac{d^{ih}-1}{d^h-1} g(x)\right\}, \quad \text{.....(2.10)}$$

where $F(x,j) \equiv \sum_{i=0}^{j-1} d^{j-i-1} f(t^i x)$, $g(x) \equiv ux + F(x,h)$ (mod N), u being defined modulo N by $t^h \equiv 1 + us$.‡

(ii) *If $t \equiv 1$ (mod s), then*

$$\pi^j x \equiv x + s\frac{d^j - 1}{d-1} f(x). \quad \text{.....(2.11)}$$

Proof: (i) Let $t \not\equiv 1$ (mod s). Then, by using (2.6) and (2.8), we have

$$\pi^2 x \equiv \pi(\pi x) \equiv \pi(tx + sf(x)) \equiv \pi tx + sdf(x) \equiv t^2 x + s\{f(tx) + df(x)\}$$

By induction we find that

$$\pi^j x \equiv t^j x + s\sum_{i=0}^{j-1} d^{j-i-1} f(t^i x),$$

and, by using the notation of the lemma,

$$\pi^j x \equiv t^j x + sF(x,j). \quad \text{.....(2.12)}$$

Thus $\pi^h x \equiv t^h x + sF(x,h) \equiv x(1+us) + sF(x,h)$,

i.e., $\pi^h x \equiv x + sg(x)$. $\quad \text{.....(2.13)}$

Moreover, a repeated application of the second formula of (2.8) gives

† It should be noted that $(d, N) = 1$ (Corollary 1.10).

‡ Such a number u always exists, because $t^h \equiv 1$ (mod s) and s divides n.

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

$$\pi^j(x+ys) \equiv \pi^j x + ysd^j. \quad \text{.....(2.14)}$$

For $j=h$, we have

$$\pi^h(x+ys) \equiv \pi^h x + ysd^h. \quad \text{.....(2.15)}$$

Hence $\pi^{2h}x \equiv \pi^h(\pi^h x) \equiv \pi^h(x+sg(x))$, by (2.13),

$\equiv \pi^h x + sg(x)d^h$, by (2.15),

i.e., $\pi^{2h}x \equiv x + sg(x)\ (1+d^h)$.

By induction over multiples of h, we obtain

$$\pi^{ih}x \equiv x + sg(x)\frac{d^{ih}-1}{d^h-1}. \quad \text{.....(2.16)}$$

Then, combining together (2.14) and (2.16), we get

$$\pi^{ih+j}x \equiv \pi^j(\pi^{ih}x) \equiv \pi^j\left(x + sg(x)\frac{d^{ih}-1}{d^h-1}\right)$$

$$\equiv \pi^j x + sg(x)\frac{d^{ih}-1}{d^h-1}d^j,$$

which, by using (2.12), proves the first part of the lemma.

(ii) If $t \equiv 1 \pmod{s}$, the proof is obvious and will be omitted.

2.17 LEMMA : (i) *If* $t \not\equiv 1 \pmod{s}$ *and if* h *is the order of* t *modulo* s, *then the quantities* $\tau(h,1)$ *and* $\tau(1,y)-1$, *for all* y, *are multiples of* h. *If* k *is the order of* π *and if* $\tau(h,1) \equiv \theta h \pmod{k}$ *and* $\tau(1,1) \equiv 1+\phi h \pmod{k}$, *then*

$$\tau(1,y) \equiv 1 + \phi h(1+\theta+\theta^2+\ldots+\theta^{v-1}) \pmod{k},$$

$$\phi(1+\theta+\theta^2+\ldots+\theta^{s-1}) \equiv 0 \pmod{k/h}. \quad \text{.....(2.18)}$$

(ii) *If* $t \equiv 1 \pmod{s}$ *and if* $\tau(1,1) \equiv \omega \pmod{k}$, *then*

$$\tau(1,y) \equiv \omega^v, \quad \omega^s \equiv 1 \pmod{k}.$$

Proof: (i) Let $t \not\equiv 1 \pmod{s}$. Then, by (2.13),

$$\pi^{\tau(h,1)}x \equiv \pi^h(x+1) - \pi^h 1 \equiv x + s\{g(x+1) - g(1)\};$$

and, by (2.6),

$$\pi^{\tau(1,v)}x \equiv \pi_v x \equiv \pi(x+y) - \pi y \equiv tx + s\{f(x+y) - f(y)\};$$

hence, by (2.10), it follows that $\tau(h,1) \equiv 0 \pmod{h}$ and $\tau(1,y) \equiv 1 \pmod{h}$. Thus we can write $\tau(h,1) \equiv \theta h$, $\tau(1,1) \equiv 1+\phi h \pmod{k}$.

Now, by putting $y=1$ in (2.15), we get

$$\pi^h(x+s) \equiv \pi^h x + sd^h \equiv \pi^h x + \pi^h s;$$

thus $\pi^h(x+s) - \pi^h s \equiv \pi^h x$,

showing that $\tau(h,s) \equiv h \pmod{k}$. Hence, using lemma 1.6 (ii) with $r=h$, $u=s$, and $z=1$, we obtain, from (1.8),

$$\tau(h, sy+1) \equiv \tau(h,1) \pmod{k}. \quad \text{.....(2.19)}$$

Similarly, since $\tau(1,s) \equiv 1 \pmod{k}$, we have, by (1.8),

$$\tau(1, sy+1) \equiv \tau(1,1) \pmod{k}. \quad \text{.....(2.20)}$$

Next, by (1.5), we have

$$\tau(2h,1) \equiv \tau(h, \pi^h 1) + \tau(h,1) \pmod{k}$$

$$\equiv \tau(h, 1+sg(1)) + \tau(h,1) \pmod{k}, \text{ by (2.13)},$$

i.e., $\tau(2h,1) \equiv \tau(h,1) + \tau(h,1) \equiv 2\tau(h,1) \pmod{k}$, by (2.19).

By induction, we obtain

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

$$\tau(ih, 1) \equiv i\tau(h, 1) \pmod{k}. \quad \text{.....(2.21)}$$

Moreover, by (1.4) and (1.5), we have

$$\begin{aligned}\tau(1, 2) &\equiv \tau(\tau(1, 1), 1) \equiv \tau(1 + \phi h, 1) \pmod{k}\\ &\equiv \tau(\phi h, 1) + \tau(1, \pi^{\phi h}1) \pmod{k}\\ &\equiv \tau(\phi h, 1) + \tau\left(1, 1 + sg(1)\frac{d^{\phi h} - 1}{d^h - 1}\right) \pmod{k}, \text{ by (2.16)},\\ &\equiv \phi\tau(h, 1) + \tau(1, 1) \pmod{k}, \text{ by (2.21) and (2.20)},\\ &\equiv \phi\theta h + 1 + \phi h \equiv 1 + \phi h(1 + \theta) \pmod{k}.\end{aligned}$$

By induction, we find that

$$\tau(1, y) \equiv 1 + \phi h(1 + \theta + \theta^2 + \ldots + \theta^{y-1}) \pmod{k}.$$

Then (2.18) follows if we remark that $\tau(1, s) \equiv 1 \pmod{k}$.

This completes the proof of part (i) of the lemma.

(ii) Now let $t \equiv 1 \pmod{s}$. In this case (2.6) may be written

$$\pi x \equiv x + sf(x). \quad \text{.....(2.22)}$$

Now $\tau(2, 1) \equiv \tau(1, \pi 1) + \tau(1, 1) \pmod{k}$, by (1.5),

$\equiv \tau(1, 1 + sf(1)) + \tau(1, 1) \pmod{k}$, by (2.22),

$\equiv \tau(1, 1) + \tau(1, 1) \pmod{k}$, by (2.20) ;†

thus $\tau(2, 1) \equiv 2\tau(1, 1) \equiv 2\omega \pmod{k}$.

By induction, we obtain

$$\tau(y, 1) \equiv y\omega \pmod{k}. \quad \text{.....(2.23)}$$

Then, by (1.4), we have

$$\tau(1, 2) \equiv \tau(\tau(1, 1), 1) \equiv \tau(\omega, 1) \equiv \omega^2 \pmod{k}, \text{ by (2.23)}.$$

By induction, $\tau(1, y) \equiv \omega^y \pmod{k}$.

Moreover, $\tau(1, s) \equiv 1 \pmod{k}$ and therefore $\omega^s \equiv 1 \pmod{k}$. This proves part (ii) of the lemma.

2.24 LEMMA : (i) *If* $t \not\equiv 1 \pmod{s}$ *and if*

$$\alpha(y) \equiv \phi(1 + \theta + \theta^2 + \ldots + \theta^{y-1}) \pmod{k/h},$$

then, with the notation of the previous lemmas,

$$f(x + y) \equiv f(x) + f(y) + d\frac{d^{h\alpha(y)} - 1}{d^h - 1} g(x) \pmod{N}, \quad \text{.....(2.25)}$$

$$d^{h\alpha(y)} - 1 \equiv 0 \pmod{N}. \quad \text{.....(2.26)}$$

(ii) *If* $t \equiv 1 \pmod{s}$ *and if* r *is the order of* d *modulo* N, *then*

$$f(x + y) \equiv f(x) + f(y) + d(\omega^y - 1)\frac{d^r - 1}{d - 1} f(x) \pmod{N}. \quad \text{.....(2.27)}$$

Proof: (i) Let $t \not\equiv 1 \pmod{s}$. By the preceding lemma, $\tau(1, y) \equiv 1 + h\alpha(y) \pmod{k}$ and therefore

$$\pi^{1+h\alpha(y)}x \equiv \pi^{\tau(1, y)}x \equiv \pi_y x \equiv \pi(x + y) - \pi y,$$

which, by using (2.10) and (2.6), gives

$$tx + s\left\{F(x, 1) + d\frac{d^{h\alpha(y)} - 1}{d^h - 1} g(x)\right\} \equiv tx + s\{f(x + y) - f(y)\};$$

† It should be noted that the proof of (2.20) depends on the fact that $\tau(1, s) \equiv 1 \pmod{k}$ and therefore (2.20) is still true when $t \equiv 1 \pmod{s}$.

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

thus $$f(x+y)-f(y)\equiv F(x,1)+d\frac{d^{h\alpha(y)}-1}{d^h-1}g(x) \pmod N$$

and (2.25) then follows if we remark that $F(x,1)\equiv f(x) \pmod N$.

Moreover, $$\pi^{1+h\alpha(y)}s\equiv\pi^{\tau(1,y)}s\equiv\pi(s+y)-\pi y\equiv\pi s\ ;$$

therefore $sd^{1+h\alpha(y)}\equiv sd$, which proves (2.26) if we remember that $(d,N)=1$.

(ii) Next, let $t\equiv 1 \pmod s$. Then $\tau(1,y)\equiv\omega^y \pmod k$, by Lemma 2.17, and therefore

$$\pi^{\tau(1,y)}x=\pi^{\omega^y}x\equiv x+s\frac{d^{\omega^y}-1}{d-1}f(x), \quad \text{by (2.11)}\ ;$$

on the other hand

$$\pi^{\tau(1,y)}x\equiv\pi(x+y)-\pi y\equiv x+s\{f(x+y)-f(y)\}, \text{ by (2.22)}\ ;$$

thus $$f(x+y)-f(y)\equiv\frac{d^{\omega^y}-1}{d-1}f(x) \pmod N.$$

Moreover,

$$\pi^{\omega^y}s\equiv\pi^{\tau(1,y)}s\equiv\pi(s+y)-\pi y\equiv\pi s\ ;$$

therefore $sd^{\omega^y}\equiv sd$. This shows that $\omega^y\equiv 1 \pmod r$, r being the order of d modulo N. Then we have

$$\frac{d^{\omega^y}-1}{d-1}=1+d\frac{d^{\omega^y-1}-1}{d-1}=1+d\frac{d^{\omega^y-1}-1}{d^r-1}\cdot\frac{d^r-1}{d-1}$$

$$\equiv 1+d(\omega^y-1)\frac{d^r-1}{d-1} \pmod N,$$

because ω^y-1 is a multiple of r, and $d^r\equiv 1 \pmod N$. Therefore

$$f(x+y)\equiv f(x)+f(y)+d(\omega^y-1)\frac{d^r-1}{d-1}f(x) \pmod N.$$

This proves part (ii) of the lemma.

2.28 THEOREM : *Let π be a non-linear semi-special permutation whose principal number is s. Let π be written in the form.*

$$\pi x\equiv tx+sf(x)$$

and let $d\equiv t+f(s) \pmod N$, where $N=n/s$.

(i) *If $t\equiv 1 \pmod s$, then the order of d modulo N divides the order of t modulo s.*

(ii) *If $t\equiv 1 \pmod s$, then $d\equiv 1 \pmod N$.*

Proof: (i) Let $t\not\equiv 1 \pmod s$ and let h be, as before, the order of t modulo s. We have to show that $d^h\equiv 1 \pmod N$, *i.e.*, that $(d^h-1,N)=N$. Let $(d^h-1,N)=N'$.

We first show that $N'>1$. Suppose that $N'=1$. Then, from (2.26),

$$\frac{d^{h\alpha(y)}-1}{d^h-1}\equiv 0 \pmod N$$

and therefore, from (2.25),

$$f(x+y)=f(x)+f(y) \pmod N\ ;$$

thus π is linear, contrary to the hypothesis of the theorem. Hence $N'>1$.

We now show that $N'=N$. Let $N'=N'N''$ and suppose that $N''>1$. Then, from (2.26) and (2.25),

$$\frac{d^{h\alpha(y)}-1}{d^h-1}\equiv 0, \quad f(x+y)\equiv f(x)+f(y) \pmod{N''}.$$

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

From the latter it follows that $f(x) \equiv xf(1) \pmod{N''}$, *i.e.*, that $f(x) \equiv xf(1) + N''F(x) \pmod{N}$, say ; hence π may be written in the form

$$\pi x \equiv t'x + s'F(x),$$

where $t' \equiv t + sf(1)$ and $s' = sN''$. Moreover, since $\pi_s = \pi$, it follows from Theorem 1.9 that $\pi_{s'} = \pi$. Hence the principal number of π is s', a multiple of s. This contradicts the hypothesis of the present theorem. Hence $N'' = 1$, *i.e.*, $N' = N$.

This completes the proof of part (i) of the theorem.

(ii) Let $t \equiv 1 \pmod{s}$. We have to show that $(d-1, N) = N$. Let $(d-1, N) = N'$.

We first show that $N' > 1$. Suppose that $N' = 1$; then

$$\frac{d^r - 1}{d-1} \equiv 0 \pmod{N},$$

r being the order of d modulo N; hence, by (2.27),

$$f(x+y) = f(x) + f(y) \pmod{N},$$

showing that π is linear, contrary to hypothesis. Thus $N' > 1$.

By following the method used in part (i), we can show that $N' = N$. This completes the proof of part (ii).

2.29 COROLLARY : (i) *If* $t \not\equiv 1 \pmod{s}$ *and if* h *is the order of* t *modulo* s, *then* $\pi^h s \equiv s$, *and*

$$\phi(1 + \theta + \theta^2 + \ldots + \theta^{s-1}) \equiv 0 \quad \left(\mathrm{mod}\ \frac{N}{(N, g(1))}\right), \quad \ldots\ldots(2.30)$$

$$f(x+y) \equiv f(x) + f(y) + dg(1)\phi(1 + \theta + \theta^2 + \ldots + \theta^{x-1})(1 + \theta + \theta^2 + \ldots + \theta^{y-1}) \pmod{N}. \quad \ldots(2.31)$$

(ii) *If* $t \equiv 1 \pmod{s}$, *then* $\pi s \equiv s$, *and*

$$f(x+y) \equiv f(y) + \omega^y f(x) \pmod{N}. \quad \ldots\ldots(2.32)$$

(*N.B.*: The symbols that appear here have the same significance as before.)

Proof: (i) If $t \not\equiv 1 \pmod{s}$, then, by Theorem 2.28, $d^h \equiv 1 \pmod{N}$; moreover, $\pi s \equiv sd$, $\pi ys \equiv ysd$ and therefore $\pi^h s \equiv sd^h \equiv s$. Furthermore, since $d^h \equiv 1 \pmod{N}$, (2.16) may be written

$$\pi^{ih} x \equiv x + sig(x). \quad \ldots\ldots(2.33)$$

Thus $\pi^{ih} 1 \equiv 1 + sig(1) \equiv 1$, if $i = \dfrac{N}{(N, g(1))}$; hence, by Lemma 1.1, it follows that $\pi^{ih} 1 \equiv 1$ for this value of i, and the order of π is therefore $k = \dfrac{Nh}{(N, g(1))}$. Then (2.30) follows directly from (2.18).

Again, since $d^h \equiv 1 \pmod{N}$, then

$$\frac{d^{h\alpha(y)} - 1}{d^h - 1} \equiv \alpha(y) \equiv \phi(1 + \theta + \theta^2 + \ldots + \theta^{y-1}) \quad \left(\mathrm{mod}\ \frac{N}{(N, g(1))}\right). \quad \ldots\ldots(2.34)$$

Next

$$\pi^h(x+1) - \pi^h 1 \equiv \pi^{\theta^h x},$$

which, by using (2.13) and (2.33), implies that

$$g(x+1) - g(1) \equiv \theta g(x) \pmod{N}. \quad \ldots\ldots(2.35)$$

This obviously gives

$$g(x) \equiv g(1)(1 + \theta + \theta^2 + \ldots + \theta^{x-1}) \pmod{N}. \quad \ldots\ldots(2.36)$$

Then (2.31) follows from (2.25), if we use (2.34) and (2.36).

(ii) If $t \equiv 1 \pmod{s}$, then $d \equiv 1 \pmod{N}$, by the theorem, and therefore $\pi s \equiv s$. Moreover, as $d \equiv 1 \pmod{N}$, then $r = 1$, r being the order of d modulo N ; (2.32) then follows from (2.27).

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

3. Existence criteria of non-linear semi-special permutations. In this paragraph, we obtain necessary and sufficient conditions for the existence of non-linear semi-special permutations.

3.1 THEOREM : (i) *If there is a non-linear semi-special permutation π on $[n]$ with principal number s and if π induces modulo s the identity permutation, then π can be written in the form*

$$\pi x \equiv x + s\lambda(1 + \omega + \omega^2 + \ldots + \omega^{x-1}),\dagger \quad \ldots\ldots(3.2)$$

where λ is a number prime to N, $N = n/s$, and where

$$\omega^s - 1 \equiv 0 \pmod{N}, \quad \omega - 1 \not\equiv 0 \pmod{N}. \quad \ldots\ldots(3.3)$$

(ii) *Conversely, if λ is prime to N, and if ω satisfies* (3.3), *then* (3.2) *defines a non-linear semi-special permutation of the desired type.*

Proof: Assume the existence of π. By hypothesis π can be written in the form

$$\pi x \equiv x + sf(x), \quad \ldots\ldots(3.4)$$

where, by Corollary 2.29, $\pi s \equiv s$.

Let ω denote $\tau(1, 1)$ modulo k, the order of π ; then, by (2.32),

$$f(x+y) \equiv f(y) + \omega^y f(x) \pmod{N}.$$

For $y = 1$, we have

$$f(x+1) \equiv f(1) + \omega f(x) \pmod{N},$$

which by repeated application shows that

$$f(x) \equiv f(1)(1 + \omega + \omega^2 + \ldots + \omega^{x-1}) \pmod{N}.$$

Then (3.4) can be written

$$\pi x \equiv x + sf(1)(1 + \omega + \omega^2 + \ldots + \omega^{x-1}), \quad \ldots\ldots(3.5)$$

where $f(1)$ is prime to N, since otherwise the principal number of π would be greater than s. Moreover, since $\pi s \equiv s$,

$$f(1)(1 + \omega + \omega^2 + \ldots + \omega^{s-1}) \equiv 0 \pmod{N},$$

where $f(1)$ is prime to N, and therefore

$$1 + \omega + \omega^2 + \ldots + \omega^{s-1} \equiv 0 \pmod{N}. \quad \ldots\ldots(3.6)$$

We now prove the second of the conditions (3.3). Suppose that $\omega \equiv 1 \pmod{N}$; then by (3.5),

$$\pi x \equiv x + sf(1)(x + tN)$$

for some integer t, and therefore

$$\pi x \equiv \{1 + sf(1)\}x = rx,$$

say. Let $(r, n) = \delta$; then

$$\pi\left(\frac{n}{\delta}\right) = r\left(\frac{n}{\delta}\right) = \frac{r}{\delta} n \equiv 0.$$

Hence $\pi\left(\frac{n}{\delta}\right) = n$. But $\pi(n) \equiv rn \equiv 0$, and therefore $\pi n = n$. Hence $\pi\left(\frac{n}{\delta}\right) = \pi n$; since π is a permutation it follows that $n/\delta = n$, *i.e.*, that $\delta = 1$, *i.e.*, that r is prime to n. Thus if $\omega \equiv 1 \pmod{N}$, $\pi x \equiv rx$ with r prime to n, *i.e.*, π is linear. But π is non-linear, so $\omega \not\equiv 1 \pmod{N}$. This establishes the second of the conditions (3.3) ; the first follows from (3.6).

For the converse, we start by showing that π is in fact a permutation. For if

$$x' + s\lambda(1 + \omega + \omega^2 + \ldots + \omega^{x'-1}) \equiv x + s\lambda(1 + \omega + \omega^2 + \ldots + \omega^{x-1}), \quad \ldots\ldots(3.7)$$

then $x' \equiv x \pmod{s}$. Writing $x' \equiv x + sX$, (3.7) becomes

† Such permutations were first discovered by Douglas [2]. He calls them exponential substitutions.

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

$$X+\lambda(1+\omega+\omega^2+\ldots+\omega^{x+sX-1})\equiv\lambda(1+\omega+\omega^2+\ldots+\omega^{x-1}) \pmod N,$$

i.e.,
$$X+\lambda\omega^x(1+\omega+\omega^2+\ldots+\omega^{sX-1})\equiv 0 \pmod N.$$

But
$$1+\omega+\omega^2+\ldots+\omega^{sX-1}\equiv(1+\omega+\omega^2+\ldots+\omega^{s-1})(1+\omega^s+\omega^{2s}+\ldots+\omega^{(X-1)s})$$
$$\equiv 0 \pmod N, \text{ in virtue of (3.3)};$$

thus $X\equiv 0 \pmod N$, and $x'\equiv x$. This implies that π is a permutation.

Next, we proceed to show that π is semi-special. In virtue of (3.3), we can show that

$$\pi s\equiv s, \quad \pi(x+ys)\equiv\pi x+ys. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.8)$$

Then, by direct calculation, we find that

$$\pi^2x\equiv\pi(\pi x)\equiv\pi(x+s\lambda(1+\omega+\omega^2+\ldots+\omega^{x-1}))$$
$$\equiv x+2s\lambda(1+\omega+\omega^2+\ldots+\omega^{x-1}), \text{ by (3.8)}.$$

By induction, we obtain

$$\pi^yx\equiv x+ys\lambda(1+\omega+\omega^2+\ldots+\omega^{x-1}). \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.9)$$

Moreover,
$$\pi_yx\equiv\pi(x+y)-\pi y\equiv x+s\omega^y\lambda(1+\omega+\omega^2+\ldots+\omega^{x-1});$$

hence by (3.9) it is evident that $\pi_y x=\pi^{\omega^y}x$. Thus π_y is, for every y, a power of π, and therefore π is semi-special. Furthermore, the second of the conditions (3.3) ensures that π is non-linear. To show this, suppose that π is linear. Then $\pi x\equiv rx$, where r is an integer prime to n. Hence, by (3.2),

$$rx\equiv x+s\lambda(1+\omega+\ldots+\omega^{x-1}), \quad \text{for all } x,$$

i.e.,
$$(r-1)x\equiv s\lambda(1+\omega+\ldots+\omega^{x-1}), \quad \text{for all } x,$$

showing that s divides $r-1$. Let $r-1=Ls$; then

$$Lx\equiv\lambda(1+\omega+\ldots+\omega^{x-1}) \pmod N.$$

Putting $x=1$, 2 in succession, we obtain

$$L\equiv\lambda \text{ and } 2L\equiv\lambda(1+\omega) \pmod N;$$

therefore $\lambda(\omega-1)\equiv 0 \pmod N$ and hence $\omega\equiv 1 \pmod N$. Thus if π is linear, $\omega-1\equiv 0 \pmod N$ and hence if $\omega-1\not\equiv 0 \pmod N$, π is non-linear. Moreover, the principal number of π is s; this is obvious because λ is prime to N. Lastly it is clear that π induces modulo s the identity permutation. Hence π is the desired permutation. This completes the proof of the theorem.

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

$$\pi x\equiv tx+s\psi(x), \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.11)$$

with $\psi(1)\equiv 0$, $\psi(x)\equiv R\sum_{i=1}^{x-1}(x-i)\theta^{i-1} \pmod N$, $x\geqslant 2$, *where R is prime to N, $N=n/s$, and*

$$1+\theta+\theta^2+\ldots+\theta^{s-1}\equiv 0 \pmod N. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.12)$$

Moreover, if h is the order of t modulo s, and u is defined modulo N by $t^h\equiv 1+us$, then

$$\kappa\equiv u+\sum_{i=0}^{h-1}t^{h-i-1}\psi(t^i) \pmod N \text{ is prime to } N; \quad \ldots\ldots\ldots\ldots\ldots\ldots(3.13)$$

$$u(\theta-1)\equiv\sum_{i=0}^{h-1}t^{h-i-1}\{\psi(2t^i)-(\theta+1)\psi(t^i)\} \pmod N; \quad \ldots\ldots\ldots\ldots\ldots\ldots(3.14)$$

$$\sum_{i=0}^{h-1}t^{h-i-1}(1+\theta+\theta^2+\ldots+\theta^{t^i-1})^2(\theta^{rt^i}-\theta^r)\equiv 0 \pmod N, \ r=1, 2, \ldots, s. \quad \ldots\ldots\ldots\ldots\ldots(3.15)$$

Conversely, if t is prime to n and R and κ are both prime to N, and if θ, t and R satisfy (3.12), (3.14) *and* (3.15), *then* (3.11) *defines a non-linear semi-special permutation of the desired type.*

The proof of this theorem is somewhat long and it will be effected by means of a number of lemmas.

First, assume the existence of π. By hypothesis, π can be written in the form

$$\pi x \equiv tx + sf(x), \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.16)$$

where t is some number prime to s. Let k be the order of π; then, by Lemma 2.17,

$$\tau(h, 1) \equiv \theta h \pmod{k}, \quad \tau(1, 1) \equiv 1 + \phi h \pmod{k}.$$

Moreover, by (2.13),

$$\pi^h x \equiv x + sg(x), \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.17)$$

where $$g(x) \equiv ux + \sum_{i=0}^{h-1} d^{h-i-1} f(t^i x), \quad d \equiv t + f(s) \pmod{N}.$$

Furthermore, by (2.31),

$$f(x+y) \equiv f(x) + f(y) + dg(1)\phi(1+\theta+\theta^2+\ldots+\theta^{x-1})(1+\theta+\theta^2+\ldots+\theta^{y-1}) \pmod{N}. \quad \ldots(3.18)$$

For $y = 1, 2$ we have respectively

$$f(x+1) \equiv f(x) + f(1) + dg(1)\phi(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod{N},$$
$$f(x+2) \equiv f(x) + f(2) + dg(1)\phi(1+\theta+\theta^2+\ldots+\theta^{x-1})(1+\theta) \pmod{N};$$

from which we deduce that

$$f(x+2) - f(x+1) \equiv f(2) - f(1) + \theta\{f(x+1) - f(x) - f(1)\} \pmod{N}.$$

Replacing x by $x-1$, then putting

$$\Delta(x) \equiv f(x+1) - f(x), \quad c \equiv f(2) - f(1) - \theta f(1) \pmod{N},$$

we find that $\Delta(x) \equiv c + \theta\Delta(x-1) \pmod{N}$, which, by repeated application, gives

$$\Delta(x) \equiv c(1+\theta+\theta^2+\ldots+\theta^{x-2}) + \theta^{x-1}\Delta(1) \pmod{N}.$$

Then, by putting $R \equiv f(2) - 2f(1) \pmod{N}$ and accordingly

$$c \equiv R - (\theta - 1)f(1), \quad \Delta(1) \equiv R + f(1) \pmod{N},$$

we have $$\Delta(x) \equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1}) + f(1) \pmod{N},$$

i.e., $$f(x+1) - f(x) \equiv f(1) + R(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod{N}. \quad \ldots\ldots\ldots\ldots\ldots(3.19)$$

Defining $\psi(x)$ by $\psi(x) \equiv f(x) - xf(1) \pmod{N}$, (3.19) can be written

$$\psi(x+1) - \psi(x) \equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod{N}. \quad \ldots\ldots\ldots\ldots\ldots(3.20)$$

Writing (3.20) for $x = 1, 2, \ldots, y-1$, then adding together and remembering that $\psi(1) \equiv 0 \pmod{N}$, we obtain

$$\psi(y) \equiv R \sum_{i=1}^{y-1} (y-i)\theta^{i-1} \pmod{N}, \text{ for } y \geqslant 2.$$

Now, using the function $\psi(x)$, (3.16) can be written

$$\pi x \equiv (t + sf(1))x + s\psi(x).$$

Since t is prime to s, then so is $t + sf(1)$; moreover t and $t + sf(1)$ have the same order h modulo s. Hence, without loss of generality, we can replace $t + sf(1)$ by t, and π can be simply written as

$$\pi x \equiv tx + s\psi(x). \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3.21)$$

Now the principal number of π being s, R must be prime to N. This confirms (3.11), where t will be shown prime to n (Corollary 3.26).

Next, by putting $x=y=1$ in (3.18), we get $f(2)-2f(1)\equiv dg(1)\phi \pmod N$, *i.e.*, $R\equiv dg(1)\phi \pmod N$. But since R is prime to N, then d, $g(1)$ and ϕ must be all prime to N.

To confirm (3.12), we have, by (2.30),

$$\phi(1+\theta+\theta^2+\ldots+\theta^{s-1})\equiv 0 \quad \left(\mathrm{mod}\ \frac{N}{(N, g(1))}\right),$$

where ϕ and $g(1)$ were shown to be prime to N, and therefore

$$1+\theta+\theta^2+\ldots+\theta^{s-1}\equiv 0 \pmod N.$$

This shows that (3.12) is necessary.

It remains to show that (3.13–3.15) are necessary. For this purpose we prove the two following lemmas.

3.22 LEMMA : *The function $\psi(x)$ satisfies the following relations:*

$$\psi(x+y)-\psi(x)-\psi(y)\equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1})(1+\theta+\theta^2+\ldots+\theta^{y-1}) \pmod N, \quad \ldots(3.23)$$

$$\psi(rx)-r\psi(x)\equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1})^2(r-1+(r-2)\theta^x+\ldots+\theta^{(r-2)x}) \pmod N,\ r\geqslant 2, \quad \ldots(3.24)$$

Moreover, if θ satisfies (3.12), *then*

$$\psi(ys)\equiv 0,\ \psi(x+ys)\equiv\psi(x) \pmod N. \quad \ldots\ldots\ldots\ldots\ldots\ldots(3.25)$$

Proof: Since $\psi(1)\equiv 0 \pmod N$, (3.20) may be written

$$\psi(x+1)-\psi(x)-\psi(1)\equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod N.$$

This relation shows that (3.23) is true for all x and for $y=1$. We complete the proof by induction over y. Assume that (3.23) is true for a certain value of y. Then

$$\psi(x+y+1)-\psi(x)-\psi(y+1)$$
$$\equiv\{\psi(x+y+1)-\psi(x+1)-\psi(y)\}+\{\psi(x+1)-\psi(x)\}-\{\psi(y+1)-\psi(y)\} \pmod N,$$

which, by assumption for the first bracket and by using (3.20) for the last two brackets, implies

$$\psi(x+y+1)-\psi(x)-\psi(y+1)$$
$$\equiv R(1+\theta+\theta^2+\ldots+\theta^x)(1+\theta+\theta^2+\ldots+\theta^{y-1})+R(1+\theta+\theta^2+\ldots+\theta^{x-1})-R(1+\theta+\theta^2+\ldots+\theta^{y-1})$$
$$\equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1})(1+\theta+\theta^2+\ldots\theta^y) \pmod N;$$

the proof of (3.23) then follows by induction.

Next, for (3.24), we get, on putting $x=y$ in (3.23),

$$\psi(2x)-2\psi(x)\equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1})^2 \pmod N.$$

This shows that (3.24) is true for all x, and for $r=2$. The proof may be completed by induction over r, and we omit it.

Lastly, if θ satisfies (3.12), then $\theta^s\equiv 1 \pmod N$ and

$$\psi(s)\equiv R\sum_{i=1}^{s-1}(s-i)\theta^{i-1}\equiv -R\sum_{i=1}^{s} i\theta^{i-1} \pmod N$$
$$\equiv -R\frac{d}{d\theta}(\theta+\theta^2+\ldots+\theta^s) \pmod N$$
$$\equiv -R\frac{d}{d\theta}(1+\theta+\theta^2+\ldots+\theta^{s-1})\equiv 0 \pmod N, \text{ by (3.12).}$$

By putting $x=s$, $r=y$ in (3.24) and using (3.12), we deduce that

$$\psi(ys)\equiv y\psi(s)\equiv 0 \pmod N;$$

moreover, by putting $y=s$ in (3.23) and using (3.12), we get

$$\psi(x+s)\equiv\psi(x)+\psi(s)\equiv\psi(x) \pmod N,$$

and inductively

$$\psi(x+ys)\equiv\psi(x) \pmod N.$$

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

This completes the proof of the lemma.

3.26 COROLLARY : *If* $\pi 1 \equiv t$, *then* t *is prime to* n.

Proof: By (3.21), $\pi s \equiv st + s\psi(s) \equiv st$, by (3.25) ; hence t is prime to N, by Corollary 1.10. But t is known to be prime to s ; therefore t is prime to n.

3.27 LEMMA : *With the same notation, if* θ *satisfies* (3.12) *and if the relation*

$$g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod{N}$$

is satisfied for $x = 1, 2, \ldots, s$, *then it is satisfied for all* x.

Proof: Let $1 \leqslant x \leqslant s$; then by hypothesis

$$g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod{N}, \quad \ldots\ldots\ldots\ldots (3.28)$$

which, for $x = s$, gives, on using (3.12) and (3.25),

$$us \equiv 0 \pmod{N}. \quad \ldots\ldots\ldots\ldots (3.29)$$

Now, let $X = x + ys$; then

$$\begin{aligned} g(1)(1+\theta+\theta^2+\ldots+\theta^{X-1}) &= g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) + g(1)\,\theta^x(1+\theta+\theta^2+\ldots+\theta^{ys-1}) \\ &\equiv g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod{N}, \text{ by (3.12)}, \\ &\equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod{N}, \text{ by (3.28)}. \end{aligned}$$

On the other hand,

$$\begin{aligned} uX + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i X) &\equiv u(x+ys) + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x + t^i ys) \pmod{N} \\ &\equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod{N}, \end{aligned}$$

by (3.29) and (3.25) ; thus

$$g(1)(1+\theta+\theta^2+\ldots+\theta^{X-1}) \equiv uX + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i X) \pmod{N},$$

which proves the lemma.

We now proceed to show the necessity of (3.14) and (3.15). Following the procedure of Lemma 2.9 and using the second formula of (3.25), we obtain

$$\pi^h x \equiv x + sg(x),$$

where

$$g(x) \equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod{N}.$$

Moreover, by (2.36),

$$g(x) \equiv g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod{N} ;$$

hence, by comparing the two expressions for $g(x)$, we have

$$g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod{N}, \text{ for all } x. \quad \ldots\ldots (3.30)$$

Moreover, by Lemma 3.27, we have shown, in virtue of (3.12), that the validity of (3.30) for $x = 1, 2, \ldots, s$ implies its validity for all x. Hence it is sufficient to consider the values $1, 2, \ldots, s$ of x. For $x = 1$, y, $y+1$ we have in succession

$$g(1) \equiv u + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i) \pmod{N}, \quad \ldots\ldots\ldots\ldots (3.31)$$

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

$$g(1)(1+\theta+\theta^2+\ldots+\theta^{y-1}) \equiv uy + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i y) \pmod N, \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.32)$$

$$g(1)(1+\theta+\theta^2+\ldots+\theta^{y}) \equiv u(y+1) + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i(y+1)) \pmod N,$$

where $y = 1, 2, \ldots, s$.

From these relations, if we eliminate u, we obtain

$$g(1)(\theta^y - 1) \equiv \sum_{i=0}^{h-1} t^{h-i-1}\{\psi(t^i(y+1)) - \psi(t^i) - \psi(t^i y)\} \pmod N,$$

i.e.,
$$g(1)(\theta^y - 1) \equiv R \sum_{i=0}^{h-1} t^{h-i-1}(1+\theta+\theta^2+\ldots+\theta^{t^i-1})^2(1+\theta^{t^i}+\theta^{2t^i}+\ldots+\theta^{(y-1)t^i}) \pmod N,$$

by (3.23). Writing this relation for $y = 1, 2, \ldots, s$ and then eliminating $g(1)$ from each pair of consecutive relations and remarking that R is prime to N, we get

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

This confirms (3.15). [Note that (3.15), with $r = s$, is obvious in virtue of (3.12).] Next, to confirm (3.14), eliminate $g(1)$ from (3.31) and (3.32) with $y = 2$, obtaining

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

this confirms (3.14).

Moreover, since $g(1)$ is prime to N, then so is κ; this confirms (3.13).

We have thus shown the necessity of all the conditions.

For the converse, we show that if (i) t is prime to n, (ii) R and κ are prime to N and (iii) (3.12–3.15) are satisfied, then (3.11) defines a non-linear semi-special permutation of the type required.

We show first that π is in fact a permutation. For if

$$tx' + s\psi(x') \equiv tx + s\psi(x), \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.33)$$

then $tx' \equiv tx \pmod s$ and therefore $x' \equiv x \pmod s$, because t is prime to s. If $x' = x + sX$, then (3.33) becomes

$$tX + \psi(x + sX) \equiv \psi(x) \pmod N.$$

But in virtue of (3.12), it was shown (Lemma 3.22, (3.25)) that

$$\psi(x + sX) \equiv \psi(x) \pmod N;$$

thus $tX \equiv 0 \pmod N$. Since t is prime to N, this implies that $X \equiv 0 \pmod N$; hence $x' \equiv x$. This shows that π is a permutation.

Next we show that π is semi-special. By direct calculation and by using the relation $\psi(x + ys) \equiv \psi(x) \pmod N$, we obtain

$$\pi^y x \equiv t^y x + s \sum_{i=0}^{y-1} t^{y-i-1}\psi(t^i x) \pmod N.$$

Therefore
$$\pi^h x \equiv x + sg(x), \quad \ldots\ldots\ldots\ldots\ldots\ldots (3.34)$$

where $g(x) \equiv ux + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i x) \pmod N$, u being defined modulo N by $t^h \equiv 1 + us$.

We now show that, in virtue of (3.14) and (3.15),

$$g(x) - g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \equiv 0 \pmod N.$$

Denoting the left hand side of this relation by $r(x)$, we have

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

$$r(x) \equiv -u\{(\theta-1)+(\theta^2-1)+\ldots+(\theta^{x-1}-1)\} + \sum_{i=0}^{h-1} t^{h-i-1}\{\psi(t^i x)-\psi(t^i)(1+\theta+\theta^2+\ldots+\theta^{x-1})\} \pmod N$$

$$\equiv -\{1+(1+\theta)+\ldots+(1+\theta+\theta^2+\ldots+\theta^{x-2})\}\sum_{i=0}^{h-1} t^{h-i-1}\{\psi(2t^i)-(\theta+1)\psi(t^i)\} + \sum_{i=0}^{h-1} t^{h-i-1}\{\psi(t^i x)-\psi(t^i)(1+\theta+\theta^2+\ldots+\theta^{x-1})\} \pmod N,$$

by substituting for $u(\theta-1)$ from (3.14),

$$\equiv -\{1+(1+\theta)+\ldots+(1+\theta+\theta^2+\ldots+\theta^{x-2})\}\sum_{i=0}^{h-1} t^{h-i-1}\{\psi(2t^i)-2\psi(t^i)\} + \sum_{i=0}^{h-1} t^{h-i-1}\{\psi(t^i x)-x\psi(t^i)\} \pmod N,$$

which, by (3.24), implies

$$r(x) \equiv -R\{1+(1+\theta)+\ldots+(1+\theta+\theta^2+\ldots+\theta^{x-2})\}\sum_{i=0}^{h-1} t^{h-i-1}(1+\theta+\theta^2+\ldots+\theta^{t^i-1})^2 + R\sum_{i=0}^{h-1} t^{h-i-1}(1+\theta+\theta^2+\ldots+\theta^{t^i-1})^2(x-1+(x-2)\theta^{t^i}+\ldots+\theta^{(x-2)t^i}) \pmod N$$

$$\equiv R\sum_{i=0}^{h-1} t^{h-i-1}(1+\theta+\theta^2+\ldots+\theta^{t^i-1})^2\{(x-2)(\theta^{t^i}-\theta)+(x-3)(\theta^{2t^i}-\theta^2)+\ldots + (\theta^{(x-2)t^i}-\theta^{x-2})\} \pmod N$$

$$\equiv 0 \pmod N,$$

by (3.15), which can be shown true for all r by means of (3.12). Thus

$$g(x) \equiv g(1)(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod N \quad \ldots\ldots\ldots\ldots(3.35)$$

and, by (3.12), one can show that

$$g(x+ys) \equiv g(x) \pmod N. \quad \ldots\ldots\ldots\ldots(3.36)$$

Hence, by (3.34), we have

$$\pi^{2h}x \equiv \pi^h(\pi^h x) \equiv \pi^h(x+sg(x)) \equiv x+sg(x)+sg(x+sg(x)) \equiv x+2sg(x), \text{ by (3.36)};$$

and inductively

$$\pi^{ih}x \equiv x+isg(x).$$

Furthermore,

$$\pi^{ih+1}x \equiv \pi(\pi^{ih}x) \equiv \pi(x+isg(x)) \equiv t(x+isg(x))+s\psi(x+isg(x)), \text{ by (3.11)}, \equiv tx+s\{\psi(x)+itg(x)\};$$

thus

$$\pi^{ih+1}x \equiv tx+s\{\psi(x)+itg(1)(1+\theta+\theta^2+\ldots\theta^{x-1})\}. \quad \ldots\ldots\ldots\ldots(3.37)$$

Next, by direct calculation,

$$\pi_y x \equiv \pi(x+y)-\pi y \equiv tx+s\{\psi(x+y)-\psi(y)\}$$

which, by (3.23), gives at once

$$\pi_y x \equiv tx+s\{\psi(x)+R(1+\theta+\theta^2+\ldots+\theta^{x-1})(1+\theta+\theta^2+\ldots+\theta^{y-1})\}. \quad \ldots\ldots\ldots(3.38)$$

Comparing (3.37) and (3.38), we see that $\pi_y = \pi^{i(y)h+1}$, where

$$i(y) \equiv R\rho(1+\theta+\theta^2+\ldots+\theta^{y-1}) \pmod N, \quad \rho t g(1) \equiv 1 \pmod N;\dagger$$

thus π is semi-special.

† Such ρ exists because both t and $g(1)$ are prime to N.

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

Furthermore, it is obvious that the principal number of π is s, and that π induces modulo s a linear permutation other than the identity permutation.

Finally, we show that π is non-linear. For if π is linear, then $\pi x \equiv t'x$, where t' is prime to n, and therefore

$$t'x \equiv tx + s\psi(x), \quad \text{for all } x;$$

thus
$$(t'-t)x \equiv s\psi(x), \quad \text{for all } x. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.39)$$

For $x=1$, this implies that $t'-t \equiv s\psi(1) \equiv 0$, because $\psi(1) \equiv 0 \pmod N$; hence, by (3.39), $\psi(x) \equiv 0 \pmod N$, for all x. But, by (3.20), we have

$$\psi(x+1) - \psi(x) \equiv R(1+\theta+\theta^2+\ldots+\theta^{x-1}) \pmod N;$$

therefore
$$R(1+\theta+\theta^2+\ldots+\theta^{x-1}) \equiv 0 \pmod N, \quad \text{for all } x.$$

But this cannot be satisfied since R is prime to N; hence π is not linear.

This completes the proof of the theorem.

3.40 COROLLARY: *If N divides s and if $(\theta-1, N) = N$ and $(t-1, N) = 1$, then π can be written in the form*

$$\pi x \equiv tx + s\mu x(x-1),$$

where t is prime to s, and μ is prime to N and is chosen so that $u - \mu h t^{h-1}$ is prime to N, h being the order of t modulo s and u being defined modulo N by $t^h = 1 + us$.

Proof: By hypothesis, $\theta \equiv 1 \pmod N$; this obviously satisfies (3.15). Also (3.12) is satisfied, because N divides s. Furthermore,

$$\psi(x) \equiv R \sum_{i=1}^{x-1} (x-i) \equiv \tfrac{1}{2} Rx(x-1) \pmod N.$$

But as t is prime to N (being prime to n) and as $(t-1, N) = 1$, N must be odd; moreover, since R is prime to N, there exists a number μ, prime to N, such that $2\mu \equiv R \pmod N$, and we have

$$\psi(x) \equiv \mu x(x-1) \pmod N. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.41)$$

Next, $t^h - 1 \equiv 0 \pmod N$, because h is the order of t modulo s, and s is a multiple of N. Moreover, $(t-1, N) = 1$ by hypothesis and therefore $\dfrac{t^h-1}{t-1} \equiv 0 \pmod N$; this shows that $\theta \equiv 1 \pmod N$ satisfies (3.14). Then, by (3.11) and (3.41),

$$\pi x \equiv tx + s\mu x(x-1),$$

where $\kappa \equiv u + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i) \equiv u - \mu h t^{h-1} \pmod N$ is prime to N.

This completes the proof of the corollary.

3.42 COROLLARY: *If $(\theta-1, N) = 1$, then (3.14) becomes*

$$u(\theta-1) \equiv R\left\{\sum_{i=0}^{h-1} t^{h-i-1}(\theta^{t^i}-1)(\theta^{t^i}-\theta) + (\theta-1)^2 t^{h-1} h\right\} \pmod N, \qquad \ldots\ldots\ldots\ldots (3.43)$$

and π can be defined by

$$\pi x \equiv (t - sR(\theta-1))x + sR(\theta^x - 1), \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.44)$$

where t is prime to n, and R is prime to N and is chosen so that

$$u + R\left\{\sum_{i=0}^{h-1} t^{h-i-1}(\theta^{t^i}-1) - (\theta-1)t^{h-1}h\right\}$$

is prime to N, h being the order of t modulo s and u being defined modulo N by $t^h \equiv 1 + us$.

Proof: By hypothesis, there exists a number λ prime to N such that $\lambda(\theta-1) \equiv 1 \pmod N$.

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

For this λ,

$$\lambda(\theta^i - 1) \equiv 1 + \theta + \theta^2 + \ldots + \theta^{i-1} \pmod{N}.$$

But $$\psi(i+1) - \psi(i) \equiv R(1 + \theta + \theta^2 + \ldots + \theta^{i-1}) \pmod{N}, \text{ by (3.20)};$$

therefore $$\psi(i+1) - \psi(i) \equiv R\lambda(\theta^i - 1) \pmod{N}.$$

By writing this relation for $i = 1, 2, \ldots, x$ and then adding together, we obtain

$$\psi(x+1) - \psi(1) \equiv R\lambda(\theta + \theta^2 + \ldots + \theta^x - x) \pmod{N}.$$

But $\psi(1) \equiv 0 \pmod{N}$ and therefore

$$\psi(x+1) \equiv R\lambda(1 + \theta + \theta^2 + \ldots + \theta^x - (x+1)) \pmod{N},$$

$$\equiv R\lambda^2(\theta^{x+1} - 1) - R\lambda(x+1) \pmod{N};$$

thus $$\psi(x) \equiv R\lambda^2(\theta^x - 1) - R\lambda x \pmod{N}.$$

Since R and λ are prime to N, we can replace $R\lambda^2$ by R. Hence

$$\psi(x) \equiv R(\theta^x - 1) - R(\theta - 1)x \pmod{N}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.45)$$

and, by (3.11), π can be written in the form

$$\pi x \equiv (t - sR(\theta - 1))x + sR(\theta^x - 1),$$

where t is prime to n, and R prime to N. Moreover

$$\kappa \equiv u + \sum_{i=0}^{h-1} t^{h-i-1}\psi(t^i) \pmod{N}$$

$$\equiv u + R\left\{\sum_{i=0}^{h-1} t^{h-i-1}(\theta^{t^i} - 1) - (\theta - 1)t^{h-1}h\right\} \pmod{N}$$

is prime to N.

Finally, (3.43) follows at once if in (3.14) we substitute for $\psi(t^i)$ and $\psi(2t^i)$ from (3.45).

This completes the proof of the corollary.

3.46 CONCLUSION: *Theorems* 3.1 *and* 3.10 *supply necessary and sufficient conditions for the existence of non-linear semi-special permutations.*

Examples of such permutations will be given in the following section.

4. Examples of non-linear semi-special permutations. We conclude by constructing the non-linear semi-special permutations when n is the product of two (equal or distinct) prime factors. We consider the following three cases where p, q are distinct prime numbers.

I. $n = 2p$. The proper divisors of n are $2, p$. There are two cases to be considered.

(i) $s = 2$, $N = p$. In this case π induces modulo 2 the identity permutation. By Theorem 3.1, there exists a number ω such that

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

and therefore such that $\omega \equiv -1 \pmod{p}$. Hence, by (3.2), π is defined by

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

where λ is prime to p.

(ii) $s = p$, $N = 2$. We show that this is impossible.

If π induces modulo p the identity permutation, then, by (3.3), there is a number ω such that $\omega^p - 1 \equiv 0 \pmod{2}$, $\omega - 1 \not\equiv 0 \pmod{2}$. These congruences cannot be satisfied simultaneously.

If π induces modulo p a linear permutation other than the identity one, then, by Theorem 3.10, there exists a number θ satisfying

$$1+\theta+\theta^2+\ldots+\theta^{p-1}\equiv 0 \pmod 2,$$

which is impossible.

Hence there is no semi-special permutation on $[2p]$ with principal number p.

Thus we have shown the following

4.1 THEOREM : *The non-linear semi-special permutations on* $[2p]$, *where* p *is an odd prime number, are defined by*

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

where λ *is prime to* p.

II. $n=p^2$. There is just one case to be considered, namely, $s=p$, $N=p$. It is evident (Theorem 3.1, (3.3)) that

$$\omega^p-1\equiv 0 \pmod p, \qquad \omega-1\not\equiv 0 \pmod p$$

cannot be satisfied simultaneously. Hence, if $n=p^2$, there is no semi-special permutation with principal number p which induces modulo p the identity permutation.

Next, if π induces modulo p a linear permutation other than the identity, then, by Theorem 3.10, there must be a number θ such that

$$1+\theta+\theta^2+\ldots+\theta^{p-1}\equiv 0 \pmod p\,;$$

this implies that $\theta\equiv 1 \pmod p$. Hence the conditions of Corollary 3.40 will be satisfied and therefore π may be defined by

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

where t and μ are both prime to p and are chosen so that $u-\mu ht^{h-1}$ is prime to p, u being defined modulo p by $t^h\equiv 1+up \pmod{p^2}$, and h is the order of t modulo p. Thus we have shown the following

4.2 THEOREM : *The non-linear semi-special permutations on* $[p^2]$ *can be written in the form*

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

where t *and* μ *are chosen arbitrarily prime to* p *in such a way that* $u-\mu ht^{h-1}$ *is also prime to* p, h *being the order of* t *modulo* p, *and* u *is defined modulo* p *by* $t^h\equiv 1+up \pmod{p^2}$.

III. $n=pq$. The proper divisors of n are p and q and so we have two cases to consider.

(i) $s=p$, $N=q$. If π induces modulo p the identity permutation, then, by Theorem 3.1, there exists a number ω such that

$$\omega^p-1\equiv 0 \pmod q, \qquad \omega-1\not\equiv 0 \pmod q.$$

These congruences cannot be simultaneously satisfied unless p divides $q-1$, in which case ω may be any number prime to q whose order modulo q is p, and π is defined by

$$\pi x\equiv x+p\lambda(1+\omega+\omega^2+\ldots+\omega^{x-1}) \pmod{pq},$$

where λ may be any number prime to q. Since $\omega-1$ and λ are prime to q, there exists a number prime to q such that $\mu(\omega-1)\equiv\lambda \pmod q$, and π is defined by

$$\pi x\equiv x+p\mu(\omega^x-1) \pmod{pq}.$$

Next, if π induces modulo p a linear permutation other than the identity one, then, by Theorem 3.10, there exists a number θ such that

$$1+\theta+\theta^2+\ldots+\theta^{p-1}\equiv 0 \pmod q\,;$$

thus $\theta^p-1\equiv 0 \pmod q$, and $\theta\not\equiv 1 \pmod q$. These can only be satisfied if p divides $q-1$, and

https://doi.org/10.1017/S2040618500033396 Published online by Cambridge University Press

then θ may be any number prime to q whose order modulo q is p. Moreover, $(\theta-1, q)=1$. Hence, by Corollary 3.42, π may be defined by

$$\pi x \equiv (t - pR(\theta-1))x + pR(\theta^x - 1) \pmod{pq},$$

where t is prime to pq and R prime to q, and where t, R, θ are chosen so that

$$u + R\left\{\sum_{i=0}^{h-1} t^{h-i-1}(\theta^{t^i}-1) - (\theta-1)t^{h-1}h\right\} \text{ is prime to } q, \quad \ldots\ldots\ldots\ldots\ldots\ldots(4.3)$$

$$u(\theta-1) \equiv R\left\{\sum_{i=0}^{h-1} t^{h-i-1}(\theta^{t^i}-1)(\theta^{t^i}-\theta) + (\theta-1)^2 t^{h-1}h\right\} \pmod{q}, \quad \ldots\ldots\ldots\ldots(4.4)$$

$$\sum_{i=0}^{h-1} t^{h-i-1}(1+\theta+\theta^2+\ldots+\theta^{t^i-1})^2(\theta^{rt^i}-\theta^r) \equiv 0 \pmod{q}, \quad r=1, 2, \ldots, p-1. \quad \ldots\ldots(4.5)$$

(ii) $s=q$, $N=p$. In this case the procedure is exactly the same as in (i), and we omit it.

Assuming, without loss of generality, that $p<q$, we have shown the following

4.6 THEOREM: (i) *If p is not a divisor of $q-1$, the semi-special permutations on $[pq]$ are all linear.*

(ii) *If p divides $q-1$, and ω and θ are any numbers prime to q having p as their order modulo q, then the non-linear semi-special permutations on $[pq]$ may be defined by*

$$\pi x \equiv x + p\mu(\omega^x - 1) \pmod{pq}$$

and

$$\pi x \equiv (t - pR(\theta-1))x + pR(\theta^x - 1) \pmod{pq},$$

where t is prime to pq, and μ and R are prime to q, and where t, R, θ are chosen so that (4.3–4.5) *are satisfied.*

REFERENCES

1. K. R. Yacoub, General products of two finite cyclic groups, *Proc. Glasgow Math. Assoc.*, **2** (1955), 116–123.

2. J. Douglas, On finite groups with two independent generators. Exponential substitutions, *Proc. Nat. Acad. Sci., U.S.A.*, **37** (1951), 749–760.

FACULTY OF SCIENCE
UNIVERSITY OF ALEXANDRIA
EGYPT