On the transformation and classification of Permutations.

By T. B. Sprague, M.A.

Let $(a_1, a_2, a_3, \ldots\ldots\ldots\ldots a_n)$ represent any permutation of the first n natural numbers. If we take the first number, a_1, and put it last, we get a new permutation; and if we perform this operation $(n-1)$ times, we get the $(n-1)$ permutations

$$\begin{aligned}
&(a_2, a_3, \ldots\ldots\ldots\ldots a_n, a_1)\\
&(a_3, a_4, \ldots\ldots\ldots\ldots a_n, a_1, a_2)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&(a_n, a_1, a_2, \ldots\ldots\ldots\ldots\ldots a_{n-1}).
\end{aligned}$$

These, together with the original permutation, make n in all. All these n permutations are evidently different from each other, but they all belong to the same cyclical series, $a_1, a_2, a_3, \ldots\ldots\ldots a_n, a_1, a_2, \ldots$, which for brevity we will call a "cycle". It is clearly immaterial with what number in a cycle we begin, but it will be convenient to begin always with 1. Let the process of deriving one of our permutations from the preceding one, be denoted by t, so that

$$t(a_m, a_{m+1}, \ldots\ldots\ldots a_{m-1}) = (a_{m+1}, \ldots\ldots\ldots a_{m-1}, a_m);$$

then, if we put P for our original permutation, the n permutations will be denoted by

$$\mathrm{P}, t\mathrm{P}, t^2\mathrm{P}, \ldots\ldots\ldots t^{n-1}\mathrm{P}.$$

It is obvious that, by repeating the process n times, we get the original permutation over again, so that $t^n\mathrm{P} = \mathrm{P}$; or we may say $t^n = 1$. We see also that any permutations which differ only by a power of t, belong to the same cycle.

Again, if 1 is subtracted from each of the numbers in our permutation, and the 0 in the result is replaced by n, we shall get a new permutation. For instance, from the permutation 123456, we get in this way 612345; and from 124653, we get 613542. In the former of these cases, but not in the latter, the new permutation belongs to the same cycle as the old one. By performing this process $(n-1$ times we get $(n-1)$ fresh permutations, or n in all.

Let s denote this operation, so that

$$s\mathrm{P} = (a_1 - 1, a_2 - 1, \ldots\ldots\ldots a_n - 1)$$

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

where, in accordance with what was said above, the constituent 0 is to be replaced by n; then the n permutations will be denoted by

$$\mathrm{P},\ s\mathrm{P},\ s^2\mathrm{P}.....s^{n-1}\mathrm{P}.$$

These will all be different from each other, but the above example shows that they may all belong to the same cycle. If we perform the operation n times, we evidently get the original permutation again, so that $s^n = 1$.

If now we combine the two kinds of operations in all possible ways, we have n^2 permutations, as follows :—

$$\left.\begin{array}{llll} \mathrm{P}, & t\mathrm{P}, & t^2\mathrm{P}, & \ldots\ldots\ldots t^{n-1}\mathrm{P}\,; \\ s\mathrm{P}, & st\mathrm{P}, & st^2\mathrm{P}, & \ldots\ldots\ldots st^{n-1}\mathrm{P}\,; \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ s^{n-1}\mathrm{P}, & s^{n-1}t\mathrm{P}, & s^{n-1}t^2\mathrm{P}, & \ldots\ldots s^{n-1}t^{n-1}\mathrm{P}. \end{array}\right\} \quad \mathrm{A}.$$

The n^2 permutations thus related I call a "set". It is to be observed that the permutations are not necessarily all different. In fact, the example taken above has shown that the set may contain only n different permutations, all belonging to the same cycle.

If $\mathrm{P} = (12435)$, we obtain in this way the following set of 25 permutations :—

12435	24351	43512	35124	51243
51324	13245	32451	24513	45132
45213	52134	21345	13452	34521
34152	41523	15234	52341	23415
23541	35412	54123	41235	12354.

Instead of writing down the 25 permutations in full, as above, we may represent them briefly as follows :—

124351243
513245132
452134521
341523415
235412354.

Here any five consecutive members constitute one of our 25 permutations; and this arrangement enables us to write down with very great ease the symbolical representation of any permutation. Thus, from $\mathrm{P} = (12435)$, we get

$$(13245) = st\mathrm{P}\,;\ (13452) = s^2t^3\mathrm{P}\,;\ (15234) = s^3t^2\mathrm{P}\,;\ (12354) = s^4t^4\mathrm{P}$$

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

A little consideration shows that our s and t operations, being entirely independent of each other, may be combined like ordinary algebraical quantities, and groupt and transposed in any way we please; thus $st = ts$; $sts = s^2t = ts^2$; $(st)^2 = s^2t^2 = t^2s^2$; $s^ht^k = t^ks^h$; also $s^hs^k = s^{h+k}$; $t^ht^k = t^{h+k}$.

There is no difficulty in interpreting negative indices; thus t^{-1} denotes the operation of taking the last number in a permutation, and putting it first, or

$$t^{-1}\mathrm{P} = (a_n, a_1, a_2, \ldots\ldots a_{n-1}).$$

The permutation thus got is the same thing as $t^{n-1}\mathrm{P}$, and this follows at once from the equation $t^n = 1$; for $t^{-1}\mathrm{P} = t^nt^{-1}\mathrm{P} = t^{n-1}\mathrm{P}$.

Again, s^{-1} denotes the operation of adding 1 to each number in a permutation, substituting, however, 1 for $(n+1)$; thus

$$s^{-1}\mathrm{P} = (a_1 + 1, a_2 + 1, \ldots\ldots a_n + 1),$$

where the constituent $(n+1)$ is to be replaced by 1. We see, in fact, that n must be added (or subtracted) at each operation, as may be found necessary; and this is to be understood in future, as I shall not mention it again.

We have also $s^{-1}\mathrm{P} = s^ns^{-1}\mathrm{P} = s^{n-1}\mathrm{P}$.

We may perform the s operation on a cycle; thus,

$$s(1245312\ldots) = (5134251\ldots) = (1342513\ldots),$$

and

$$s(1234512\ldots) = (5123451\ldots) = (1234512\ldots).$$

In the latter case the s operation reproduces the original cycle, and this relation may be represented by $s(\mathrm{C}) = \mathrm{C}$; and such a cycle may be called a self-repeating cycle.

In the example given above, of the set of 25 permutations derived from (12435), it is obvious that, whichever of the 25 permutations we take as our original one, we shall get by the process the same 25, but differently arranged; and the same is clearly true whatever the value of n. In other words, the set remains the same, whichever of the permutations in it is taken as the original one. In this example the 25 permutations are all different; but if we had started with the permutation (12345), or with (15432), we should have got a set containing only five different permutations, which all belong to the same cycle. Thus, putting P for (12345), we have $s\mathrm{P} = (51234)$; $t\mathrm{P} = (23451)$; $ts\mathrm{P} = st\mathrm{P} = (12345) = \mathrm{P}$. In general, since all the permutations in each column of our scheme (A) are

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

different, and all the permutations in each row are different, a set must contain at least n different permutations; and the above example shows that it may contain n^2.

It is clear that no permutation can belong to two different sets; for if a permutation in one set is the same as a permutation in another set, it follows that all the permutations in the one set are the same as all the permutations in the other, or the two sets differ only in the arrangement of the permutations. We thus see that the $n!$ permutations of n numbers, admit of being groupt in sets containing n^2 each, so that no permutation shall occur in two of the sets. But, when n is prime, $n!$ is not divisible by n^2, and it follows that one, at least, of the sets must be such that the same permutation occurs more than once in it.

If one permutation in a set is repeated, then every permutation in it must be repeated. For instance, let the original permutation, P, be equal to $s^h t^k \mathrm{P}$, and let $s^p t^q \mathrm{P}$ be any other permutation in the set; then since $\mathrm{P} = s^h t^k \mathrm{P}$, operating on both sides with $s^p t^q$, we have

$$s^p t^q \mathrm{P} = s^p t^q (s^h t^k \mathrm{P}) = s^{p+h} t^{q+k} \mathrm{P} = s^h t^k (s^p t^q \mathrm{P}) :$$

and this shows that $s^p t^q \mathrm{P}$ is repeated in the set. Each permutation in the set must, of course, be repeated the same number of times; and it follows that the number of different permutations in a set must be a divisor of n^2, and the number of different cycles in a set must be a divisor of n. If n is prime, the set must therefore contain either n permutations belonging to 1 cycle, or n^2 permutations belonging to n cycles; and such sets may be conveniently called 1-cycle sets and n-cycle sets, respectively; the permutations contained in them being similarly called 1-cycle permutations and n-cycle permutations.

It thus appears that sets, cycles, and permutations, may each be divided into two classes. We may have (1) sets in which each permutation is repeated a certain number of times; and these sets may be called "repeating sets". The permutations contained in them, and the cycles to which they belong, may be called "recurring". We may have (2) sets which contain n^2 different permutations, which belong to n different cycles; and these sets, which we have called n-cycle sets, may be also called "full sets", or "non-repeating sets". The permutations contained in these sets, which we have called n-cycle permutations, and the cycles to which they belong, may be also called "non-recurring".

I propose now to investigate the conditions that must be satisfied, in order that a permutation may belong to the one class or to the other; and I begin with ascertaining the condition that $s\mathrm{P}$ may belong to the same cycle as P, or that we may have $s(\mathrm{C}) = \mathrm{C}$. In this case, P and $s\mathrm{P}$, since they belong to the same cycle, can only differ by a power of t, so that we must have $st^f\mathrm{P} = \mathrm{P}$, where f is an integer. We then get $s^2t^{2f}\mathrm{P} = st^f(st^f\mathrm{P}) = st^f\mathrm{P} = \mathrm{P}$; and, similarly, $\mathrm{P} = st^f\mathrm{P} = s^2t^{2f}\mathrm{P} = \ldots\ldots\ldots\ldots = s^{n-1}t^{(n-1)f}\mathrm{P}$. This shows that all the n^2 permutations in the set belong to the same cycle.

We next notice that f must be prime to n; for suppose that they are not prime, but have a common factor x, so that $f = \mathrm{F}x$, $n = \mathrm{N}x$, then, since $\mathrm{N} < n$, we have $s^{\mathrm{N}}t^{\mathrm{N}f} = \mathrm{P}$.

Also $$s^{\mathrm{N}}t^{\mathrm{N}f}\mathrm{P} = s^{\mathrm{N}}t^{\mathrm{N}x\mathrm{F}}\mathrm{P} = s^{\mathrm{N}}t^{n\mathrm{F}}\mathrm{P} = s^{\mathrm{N}}\mathrm{P}, \text{ since } t^n = 1.$$

But since $s^{\mathrm{N}}t^{\mathrm{N}f}\mathrm{P} = \mathrm{P}$, it follows that $s^{\mathrm{N}}\mathrm{P} = \mathrm{P}$; and this being impossible, f and n cannot have any common factor, or they are prime to each other.

Again, since f is prime to n, it is well known that the products, f, $2f$, $3f$,....., $(n-1)f$, when divided by n, give remainders which form a permutation of $1,2,3,\ldots\ldots(n-1)$; hence there is one of the products, gf, such that $gf = qn + 1$, q being an integer, and both q and g being $< n$; and this equation shows that g, as well as f, is prime to n. Then $s^gt^{gf}\mathrm{P} = s^gt^{qn+1}\mathrm{P} = s^gt\mathrm{P}$; and consequently $s^gt\mathrm{P} = \mathrm{P}$ or $t\mathrm{P} = s^{-g}\mathrm{P}$.

Hence $$(a_2, a_3, \ldots\ldots a_n, a_1) = (a_1 + g, a_2 + g \ldots\ldots a_n + g),$$

and $$a_2 = a_1 + g,\ a_3 = a_2 + g, \ldots\ldots, a_1 = a_n + g;$$

or each constituent in P is got by adding g to the preceding one, or subtracting $(n-g)$ from it; and

$$\mathrm{P} = \{a_1,\ a_1 + g,\ a_1 + 2g, \ldots\ldots a_1 + (n-1)g\}.$$

Conversely, if we take any number a not $> n$, and g any number $< n$ and prime to it, since the numbers a, $a+g$, $a+2g$,..... $a+(n-1)g$, all give different remainders when divided by n, the above formula for P will give a permutation of the numbers 123 .....n. It is obvious from the formula, that $s^gt\mathrm{P} = \mathrm{P}$; and, by reversing the above demonstration, we may show that

$$\mathrm{P} = st^f\mathrm{P} = s^2t^{2f}\mathrm{P} = \ldots\ldots\ldots = s^{n-1}t^{(n-1)f}\mathrm{P};$$

whence P is a 1-cycle permutation.

When n is prime, we may give g any one of the values 1,2,3, ...$(n-1)$, and there are therefore $(n-1)$ 1-cycle sets, and $(n-1)$ self-repeating cycles, which may be obtained from the $(n-1)$ permutations.

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

$$\{1,\quad 1+1,\qquad 1+2,\qquad \ldots\ldots\ldots\quad 1+(n-1)\}$$
$$\{1,\quad 1+2,\qquad 1+4,\qquad \ldots\ldots\ldots\quad 1+2(n-1)\}$$
$$\{1,\quad 1+3,\qquad 1+6,\qquad \ldots\ldots\ldots\quad 1+3(n-1)\}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\{1,\quad 1+(n-1),\quad 1+2(n-1),\quad \ldots\ldots\ldots\quad 1+(n-1)^2\}.$$

When n is a composite number, the number of such sets is $\phi(n)$, or the number of numbers $<n$ and prime to it.

Next take the more general case, and suppose that $s^h t^k \mathrm{P} = \mathrm{P}$; then we can prove that, either h and k are both prime to n; or, if x is the G. C. M. of h, k, n, and $h = x\mathrm{H}$, $k = x\mathrm{K}$, $n = x\mathrm{N}$, then H and K are both prime to N. If h and k are not both prime to n, suppose that h and n contain a common factor x, so that $h = x\mathrm{H}$, $n = x\mathrm{N}$; then $s^h t^k = s^{x\mathrm{H}} t^k$, and $(s^h t^k)^{\mathrm{N}} = s^{\mathrm{N}x\mathrm{H}} t^{\mathrm{N}k} = s^{n\mathrm{H}} t^{\mathrm{N}k} = t^{\mathrm{N}k}$. Hence $s^h t^k \mathrm{P} = \mathrm{P}$ leads to $t^{\mathrm{N}k}\mathrm{P} = \mathrm{P}$; but this cannot be the case unless $\mathrm{N}k$ is a multiple of n or of $\mathrm{N}x$, and therefore k must be a multiple of x. Hence every common factor which h and n contain, must be also a factor of k; and it may be proved similarly that every common factor which k and n contain, must be also a factor of h. Hence, if we divide by the G. C. M. of h, k, n, suppose x, the quotients, H and K, must both be prime to N; for, if this were not the case, but H and N, for instance, contained a common factor y, then h and n would have the common factor xy, which is not a factor of k. Since h and k are both $<$than n, H and K are both $<\mathrm{N}$. It follows that, if $h = 1$, or $st^k\mathrm{P} = \mathrm{P}$, then k must be prime to n; and if $k = 1$, or $s^h t \mathrm{P} = \mathrm{P}$, then h must be prime to n.

We will first consider the case where h and k are both prime to n. We have

$$\mathrm{P} = s^h t^k \mathrm{P} = s^{2h} t^{2k} \mathrm{P} = \ldots\ldots\ldots\ldots = s^{(n-1)h} t^{(n-1)k} \mathrm{P},$$

and we have therefore to consider the operations

$$s^h t^k,\ s^{2h} t^{2k},\ s^{3h} t^{3k} \ldots\ldots\ldots\ldots\ldots\ldots s^{(n-1)h} t^{(n-1)k},$$

and to suppress the multiples of n that occur in the indices. Now, h being prime to n, if we divide n into the numbers, h, $2h$, $3h$..... $(n-1)h$, we shall have $(n-1)$ different remainders, one of which must therefore be 1; and the same is true of k; therefore the above operations contain two which are equivalent to st^l, $s^g t$, so that we have $\mathrm{P} = st^l\mathrm{P} = s^g t \mathrm{P}$. Hence, by what was proved above, both f and g must be prime to n, and P must be a 1-cycle permutation, or must be of the form

$$\{a,\ a+g,\ a+2g, \ldots\ldots\ldots\ldots\ldots a+(n-1)g\}.$$

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

It is to be observed that, if $s^h t^k P = P$, and P is of the above form, it does not follow that h and k are prime to n; and it is easy to see that this will not always be the case. For instance, if $n = 6$, and $st P = P$, so that P is of the form $(a, a+1, a+2, \ldots\ldots\ldots\ldots a+5)$, we shall have $s^2t^2P = P$, $s^3t^3P = P$, $s^4t^4P = P$.

When n is prime, h and k are necessarily prime to it; and, whatever values we give to h and k, we shall get by the above process a value of g. Since we may give h any of the $(n-1)$ values $1,2,3\ldots\ldots\ldots(n-1)$, and the same is true of k, the total number of pairs of values of h and k is $(n-1)^2$; and as there can only be $(n-1)$ values of g, or $(n-1)$ self-repeating cycles, it follows that $(n-1)$ of the pairs belong to each cycle.

We are now in a position to determine, in the case when n is prime, how many permutations and sets there are of each class. We have seen that there are $(n-1)$ 1-cycle sets, and these contain $n(n-1)$ recurring permutations. Also, the total number of permutations being $n!$, the number of non-recurring permutations is $n! - n(n-1) = n(n-1)\{(n-2)! - 1\}$.

Each of these, as we have seen, belongs to a set which contains n^2 different permutations; hence the number of these sets is

$$n(n-1)\{(n-2)! - 1\} \div n^2 = \frac{n-1}{n}\{(n-2)! - 1\}.$$

This number is always integral; for by Wilson's Theorem, $(n-1)! + 1$ is divisible by n. Suppose the quotient to be Q, so that $(n-1)! + 1 = Qn$; then $(n-1) \times (n-2)! + 1 = Qn$, and $(n-2)! - 1 = n\{(n-2)! - Q\}$.

We thus see that, when n is prime, there are $n(n-1)\{(n-2)! - 1\}$ n-cycle permutations, which can be arranged in n-cycle sets; and $n(n-1)$ 1-cycle permutations, which belong to $(n-1)$ 1-cycle sets. And since each cycle gives n permutations, we see that the total number of cycles is $(n-1)!$; also that $(n-1)$ of these are self-repeating, and the remaining $(n-1)\{(n-2)! - 1\}$ are non-recurring, or are such that the s operation gives a new cycle in every case.

When $n = 5$, and we give g the values 1, 2, 3, 4, we get the four following self-repeating cycles :—

1234512.....; 1352413.....; 1425314.....; 1543215.....;

It will be found by actual trial that the 20 non-recurring cycles are :—

C	1235412.....	1245312.....	1254312.....	1354213.....
s C	1243512.....	1342513.....	1432514.....	1524315.....
s^2C	1324513.....	1452314.....	1453214.....	1325413.....
s^3C	1345213.....	1253412.....	1534215	1435214.....
s^4C	1523415.....	1423514.....	1542315.....	1532415.....

These results may be otherwise stated by saying that, when we form all the possible permutations by means of the s and t operations, the following are 1-cycle permutations, and give rise to 5 permutations each, or 20 in all :—

12345, 13524, 14253, 15432;

and the following are 5-cycle permutations, and give rise to 25 each, or 100 in all :—

12354, 12453, 12543, 13542.

It will be convenient now to show how to find f and g when we know h, k, and n; h and k being both prime to n. We have seen that there exists some number g less than n, such that $s^g t$ is equivalent to $s^{mh}t^{mk}$, where $m<n$. It follows that $mk=qn+1$, where q is some integer which must be less than n, because both m and k are less than n; also $mh=q'n+g$. If for any value of n we form a table of the following form, we shall be able by inspection to determine the value of m when we know k.

Table showing the values of $(qn+1)$, and its resolution into two factors, each less than n.

q	$n=11$	$n=12$
	$11q+1$	$12q+1$
0	$1=1\times1$	$1=1\times1$
1	$12=2\times6=3\times4$	13
2	23	$25=5\times5$
3	34	37
4	$45=5\times9$	$49=7\times7$
5	$56=7\times8$	61
6	67	73
7	78	85
8	89	97
9	$100=10\times10$	109
10	111	$121=11\times11$
11		133

We see from this table that, when $n=11$ and 12 respectively,

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

and $q<n$, the numbers $(qn+1)$ can in certain cases be resolved into pairs of factors, each $<n$; and that these factors include all the numbers $<n$ and prime to it. It is easy to prove that this will always be the case. If k is any number $<n$ and prime to it, and we divide n into the $(n-1)$ numbers $k, 2k, 3k, \ldots\ldots\ldots (n-1)k$, we shall get $(n-1)$ different remainders, one of which must therefore be 1 : hence there is some number $m<n$, such that mk is of the form $(qn+1)$. This proves the proposition.

If n is a largeish number, the table is easily formed with the help of a table of the prime factors of numbers. In this way I have got the following results for $n=101$ and 120.

q	$n=101$		q	$n=120$	
	$qn+1$	Factors.		$qn+1$	Factors.
0	1	1×1	0	1	1×1
1	102	2×51, 3×34, 6×17	1	121	11×11
2	203	7×29	3	361	19×19
3	304	4×76, 8×38, 16×19	4	481	13×37
4	405	5×81, 9×45, 15×27	6	721	7×103
5	506	11×46, 22×23	7	841	29×29
7	708	12×59	8	961	31×31
9	910	10×91, 13×70, 14×65, 26×35	9	1081	23×47
13	1314	18×73	14	1681	41×41
16	1617	21×77, 33×49	16	1921	17×113
19	1920	20×96, 24×80, 30×64, 32×60, 40×48	20	2401	49×49
20	2021	43×47	24	2881	43×67
22	2223	39×57	29	3481	59×59
23	2324	28×83	31	3721	61×61
24	2425	25×97	34	4081	53×77
26	2627	37×71	42	5041	71×71
27	2728	31×88, 44×62	52	6241	79×79
28	2829	41×69	59	7081	73×97
31	3132	36×87, 54×58	66	7921	89×89
32	3233	53×61	69	8281	91×91
35	3536	52×68	74	8881	83×107
37	3738	42×89	85	10201	101×101
49	4950	50×99, 55×90, 66×75	99	11881	109×109
51	5152	56×92	118	14161	119×119
58	5859	63×93			
61	6162	78×79			
63	6364	74×86			
65	6566	67×98			
67	6768	72×94			
69	6970	82×85			
79	7980	84×95			
99	10000	100×100			

The same table will enable us to find f when we know g, or to find g when we know f; for the relation between f and g is exactly the same as that between k and m.

The table shows (1) the values of $(qn+1)$ for all values of $q<n$;

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

and (2) the factors of $(qn+1)$ when it is the product of two numbers each $<n$. Thus, when $n=11$, the table shows us that

if	k (or f)	=	1, 2, 3, 4, 5, 6, 7, 8, 9, 10;
then	m (or g)	=	1, 6, 4, 3, 9, 2, 8, 7, 5, 10.

Again, when $n=12$,

if	k (or f)	=	1, 5, 7, 11;
then	m (or g)	=	1, 5, 7, 11.

Having got m, the equation $mh=q'n+g$, shows that g is the remainder we get when mh is divided by n. Suppose, for example, that $n=11$, and $h=2$, $k=3$; so that $s^2t^3\mathrm{P}=\mathrm{P}$. Then, from above, $m=4$, $mh=8$; so that $g=8$; and then $f=7$, or $st^7\mathrm{P}=s^8t\mathrm{P}=\mathrm{P}$. Hence P must be a permutation belonging to the cycle 1,9,6,3,11,8,5,2,10,7,4,1,9.....where each constituent is got from the preceding by adding 8 or subtracting 3; and a little consideration shows that P may be any such permutation.

The positions in the scheme (A) of the 10 permutations which are identical with the original one, are given by the following values of the indices of s and t, which correspond to st^7, s^2t^{14}, s^3t^{21}, etc.

1,7 ; **2,3;** 3,10 ; 4,6 ; 5,2 ; 6,9 ; 7,5 ; 8,1 ; 9,8 ; 10,4 ;

or they may be otherwise arranged, so as to correspond with s^8t, $s^{16}t^2$, etc.

8,1 ; 5,2 ; **2,3;** 10,4 ; 7,5 ; 4,6 ; 1,7 ; 9,8 ; 6,9 ; 3,10.

But their relation to each other will be better understood by observing the positions of the identical numbers in a series of permutations where each is got from the one above it by the s operation. Retaining the value $g=8$, let us take 8 as the initial constituent of the permutation; then the 11 permutations in question are :—

8	5	2	10	7	4	1	9	6	3	11
7	4	1	9	6	3	11	**8**	5	2	10
6	3	11	**8**	5	2	10	7	4	1	9
5	2	10	7	4	1	9	6	3	11	**8**
4	1	9	6	3	11	**8**	5	2	10	7
3	11	**8**	5	2	10	7	4	1	9	6
2	10	7	4	1	9	6	3	11	**8**	5
1	9	6	3	11	**8**	5	2	10	7	4
11	**8**	5	2	10	7	4	1	9	6	3
10	7	4	1	9	6	3	11	**8**	5	2
9	6	3	11	**8**	5	2	10	7	4	1

If, instead of taking $s^2t^3P = P$, we had taken values of h and k corresponding to any other of the identical permutations, we should have got the same result; for instance, if $s^5t^2P = P$; or $h = 5$, $k = 2$; we have $m = 6$, $mh = 30 = 2 \times 11 + 8$; and $g = 8$, as before.

As mentioned above, there are $(n-1)^2$, or 100, pairs of values of h and k, to each of which corresponds a value of g; and in the adjoining diagram each of the squares with a number in it, represents one of these pairs of values, and the number in it is the value of g for that pair.

$k=10$		10	9	8	7	6	5	4	3	2	1
9		5	10	4	9	3	8	2	7	1	6
8		7	3	10	6	2	9	5	1	8	4
7		8	5	2	10	7	4	1	9	6	3
6		2	4	6	8	10	1	3	5	7	9
5		9	7	5	3	1	10	8	6	4	2
4		3	6	9	1	4	7	10	2	5	8
3		4	8	1	5	9	2	6	10	3	7
2		6	1	7	2	8	3	9	4	10	5
1		1	2	3	4	5	6	7	8	9	10
0											
$h=0$	1	2	3	4	5	6	7	8	9	10	

Next take $n = 12$, and $h = 5$, $k = 11$; then from above $m = 11$, $mh = 55 = 4 \times 12 + 7$, or $g = 7$; whence, again, $f = 7$. Therefore P belongs to the cycle

1,8,3,10,5,12,7,2,9,4,11,6,1,8.....

Also the positions of the 11 permutations that are identical with the original one, are indicated by

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

1,7 ; 2,2 ; 3,9 ; 4,4 ; **5,11** ; 6,6 ; 7,1 ; 8,8 ; 9,3 ; 10,10 ; 11,5.

Here the following pairs of values of h and k are prime to $n(=12)$; namely, 1,7 ; 5,11 ; 7,1 ; 11,5 ; and taking any one of these pairs, we should by the same process find the same values of f and g. In the remaining pairs, 2,2 ; 3,9 ; 4,4 ; 6,6 ; 8,8 ; 9,3 ; 10,10 ; we see that, consistently with what was said above, both numbers in each pair contain a factor which is also a factor of 12 ; and dividing by the G.C.M.'s, 2, 3, 4, 6, 4, 3, 2 respectively, the quotients are both prime to the quotient of 12 ; for instance, taking 3,9, and dividing by the G.C.M., 3, we get 1,3, each of which is prime to the quotient of 12 by 3, namely 4.

This example shows us that, although when h,k, are both prime to n, the relation $s^h t^k \mathrm{P} = \mathrm{P}$, cannot be satisfied unless P is a 1-cycle permutation, yet when P is such a permutation, and $s^h t^k \mathrm{P} = \mathrm{P}$, it is not necessary that h, k, should be prime to n, but only that, when all three numbers are divided by their G.C.M., the quotients of h,k, should be prime to the quotient of n.

When $n = 12$, and h,k, are both prime to it, the only possible pairs of values of h and k are the following 16 :—

1,1 ; 1,5 ; 1,7 ; 1,11 ;	5,1 ; 5,5 ; 5,7 ; 5,11 ;
7,1 ; 7,5 ; 7,7 ; 7,11 ;	11,1 ; 11,5 ; 11,7 ; 11,11.

Each of these belongs to a 1-cycle permutation ; and, taking any pair, we can, by the process above described, find the value of g. Since g must be prime to 12, it can only have the 4 values 1, 5, 7, 11 ; so that there can be only 4 1-cycle permutations, and 4 of the pairs of values of h,k, belong to each of these. The pairs that belong to each value of g are shown in the adjoining diagram.

k	0	1	2	3	4	5	6	7	8	9	10	11
11		11				7		5				1
10			11, 5								1, 7	
9				11, 7						1, 5		
8					11, 5				1, 7			
7		7				11		1				5
6							11, 7 1, 5					
5		5				1		11				7
4					1, 7				11, 5			
3				1, 5						11, 7		
2			1, 7								11, 5	
1		1				5		7				11
0												

For the sake of completeness I have inserted the values of g that belong to pairs of values of h and k that are not prime to 12; and it will be noticed that every one of such pairs belongs to more than one cycle. We shall see later on how the values of g may be determined in these cases. The squares which are left blank in the diagram, are those which correspond to values of h and k which cannot coexist.

Having thus fully considered the case where h and k are prime to n, we have now to consider the case where all 3 numbers have a common factor. Suppose that x is the G.C.M., and $h = x\mathrm{H}$, $k = x\mathrm{K}$, $n = x\mathrm{N}$; then, as we have seen, H, K, are both prime to N, and, of course, $< \mathrm{N}$. Hence among the numbers H, 2H, 3H.....$(\mathrm{N}-1)\mathrm{H}$, there is one which gives the remainder 1 when divided by N; and the same is true of the numbers K, 2K, 3K,.....$(\mathrm{N}-1)\mathrm{K}$.
Hence the operations

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

$$(s^{\mathrm{H}}t^{\mathrm{K}})^{x},\ (s^{\mathrm{H}}t^{\mathrm{K}})^{2x},\ (s^{\mathrm{H}}t^{\mathrm{K}})^{3x}\ldots\ldots(s^{\mathrm{H}}t^{\mathrm{K}})^{(\mathrm{N}-1)x}$$

contain two which are equivalent to $(s^{m\mathrm{N}+1}t^{\mathrm{F}})^{x}$ and $(s^{\mathrm{G}}t^{m\,\mathrm{N}+1})^{x}$, or to $(st^{\mathrm{F}})^{x}$ and $(s^{\mathrm{G}}t)^{x}$, since $\mathrm{N}x=n$, and $t^{n}=1$. Here F and G must both be $<\mathrm{N}$, and prime to it; and they are to be found from H, K, in the same way that f, g, were found from h, k.

We next observe that $\mathrm{P}=(st^{\mathrm{F}})^{x}\mathrm{P}$ leads to $\mathrm{P}=s^{x}t^{\mathrm{F}x}\mathrm{P}=s^{2x}t^{2\mathrm{F}x}\mathrm{P}=\ldots\ldots=s^{(\mathrm{N}-1)x}t^{(\mathrm{N}-1)\mathrm{F}x}\mathrm{P}$. This shows that these N permutations all belong to the same cycle, and it follows that there cannot be more than x different cycles in the set to which they belong. We shall presently see that there may be fewer.

Resuming now the relation $(s^{\mathrm{G}}t)^{x}\mathrm{P}=\mathrm{P}$, or $t^{x}\mathrm{P}=s^{-\mathrm{G}x}\mathrm{P}$, we have

$$t^{x}\mathrm{P}=(a_{x+1},a_{x+2},\ldots\ldots a_{n},a_{1},a_{2},\ldots\ldots a_{x})$$

and

$$s^{-\mathrm{G}x}\mathrm{P}=(a_{1}+\mathrm{G}x,a_{2}+\mathrm{G}x,a_{3}+\mathrm{G}x\ldots\ldots a_{n}+\mathrm{G}x)$$

and it follows from the identity of these that

$$a_{x+1}=a_{1}+\mathrm{G}x,\ a_{2x+1}=a_{x+1}+\mathrm{G}x,\ldots\ldots$$
$$a_{x+2}=a_{2}+\mathrm{G}x,\ a_{2x+2}=a_{x+2}+\mathrm{G}x,\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{2x}=a_{x}+\mathrm{G}x,\ a_{3x}=a_{2x}+\mathrm{G}x,\ldots\ldots\ldots$$

whence $a_{2x+1}=a_{1}+2\mathrm{G}x,\ a_{2x+2}=a_{2}+2\mathrm{G}x,\ldots\ldots\ldots\ldots$

and generally $a_{mx+1}=a_{1}+m\mathrm{G}x,\ a_{mx+2}=a_{2}+m\mathrm{G}x,\ldots\ldots\ldots\ldots$

Hence we get

$$\mathrm{P}=\{a_{1},a_{2},a_{3}\ldots\ldots a_{x},a_{1}+\mathrm{G}x,a_{2}+\mathrm{G}x\ldots\ldots a_{x}+\mathrm{G}x,a_{1}+2\mathrm{G}x\ldots\ldots$$
$$a_{x}+2\mathrm{G}x,\ldots\ldots\ldots\ldots a_{1}+(\mathrm{N}-1)\mathrm{G}x,\ldots\ldots\ldots\ldots a_{x}+(\mathrm{N}-1)\mathrm{G}x\}$$

Here we know G, which has been found from H and K; and our next step will be to show how many permutations of this form can be got from any known value of G. We first observe that, if a_{1}, a_{2}, $\ldots\ldots a_{x}$, are x consecutive numbers, all less than n, then all the numbers in the above expression for P will give different remainders when divided by n. For any two of these numbers may be represented by $a_{u}+m\mathrm{G}x$, $a_{v}+m'\mathrm{G}x$, where a_{u} and a_{v} are two of the numbers, $a_{1},a_{2},\ldots\ldots a_{x}$ and therefore $v-u<x$. Suppose these two numbers, if possible, to give the same remainder, R, so that

$$a_{u}+m\,\mathrm{G}x=qn+\mathrm{R}=q\,\mathrm{N}x+\mathrm{R},$$
$$a_{v}+m'\mathrm{G}x=q'n+\mathrm{R}=q'\mathrm{N}x+\mathrm{R};$$

then

$$a_{u}-a_{v}+(m-m')\mathrm{G}x=(q-q')\mathrm{N}x.$$

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

In order that this equation may subsist, $a_u - a_v$ must be divisible by x; but this is impossible, because the difference between a_u and a_v is $< x$, these being two of x consecutive numbers. Hence no two of the n numbers can give the same remainder, or they all give different remainders. If, then, we take any x consecutive numbers, $< n$, and form P according to the above formula, we shall get a permutation of $1,2,3,\ldots\ldots n$. It is not necessary, however, that $a_1, a_2 \ldots\ldots a_x$ should be consecutive numbers; but if, in place of any one of them, a_u, we set any one of the numbers $a_u + Gx$, $a_u + 2Gx, \ldots\ldots$ $a_u + (N-1)Gx$, and form P by the same formula, we shall get another permutation satisfying the same condition. In this way from any one permutation we get $(N-1)$ others, or N in all. But each of the x numbers $a_1, a_2, \ldots\ldots a_x$, may be separately dealt with in the same way; and thus we get in all N^x different permutations satisfying the condition. Lastly, the x numbers $a_1, a_2 \ldots\ldots a_x$, may be permuted in $x!$ ways; and for each of these arrangements we get, as we have seen, N^x different permutations, so that, finally, we have $x! \times N^x$ different permutations of $1,2,3,\ldots\ldots n$, which satisfy the required condition.

This result may also be arrived at as follows:—

Having assumed a_1 at pleasure, we must have $a_{x+1} = a_1 + Gx$, $a_{2x+1} = a_1 + 2Gx, \ldots\ldots a_{(N-1)x+1} = a_1 + (N-1)Gx$; so that N of the numbers in the required permutation are determined. This leaves $n - N = N(x-1)$ numbers, any one of which may he taken for a_2, and thus N more of the numbers in the permutation are determined. This leaves $n - 2N = N(x-2)$ numbers, any one of which may be taken for a_3, and so on. Hence, bearing in mind that we may take any one of the n (or Nx) numbers for a_1, the total number of permutations for a known value of G is

$$Nx.N(x-1).N(x-2)\ldots\ldots N(1) = N^x \times x!$$

As an example, let us take $n = 12$, $h = 3$, $k = 9$, so that $x = 3$, $N = 4$, $H = 1$, $K = 3$: then we have the auxiliary table annexed. This shows that $m = 3$; then $mH = 3$, and $G = 3$, and P must be of the form, (suppressing multiples of 12)

N = 4	
q	$4q+1$
0	$1 = 1^2$
1	5
2	$9 = 3^2$
3	13

$$(a_1, a_2, a_3, a_1+9, a_2+9, a_3+9, a_1+6, a_2+6, a_3+6, a_1+3, a_2+3, a_3+3).$$

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

Giving a_1, a_2, a_3, the values 1,2,3, we may conveniently represent P in the following way :

$$\left|\begin{array}{l} 1.10.7.4 \\ 2.11.8.5 \\ 3.12.9.6 \end{array}\right|$$

where it is to be understood that the figures in each line may be cyclically transposed, independently of those in the other lines, and the order of the lines may also be altered as we please. All the permutations thus got will satisfy the condition $s^3t^9P = P$, or $s^3P = t^3P$; and the total number of such permutations is $4^3 \times 3! = 384$, belonging to 32 cycles.

If we take, for instance 1,9,11, as the first 3 numbers, we have the permutation

$$1,\ 9, 11, 10,\ 6,\ 8,\ 7,\ 3,\ 5,\ 4, 12,\ 2;$$

and then performing the s operation 3 times, we get

$$\begin{array}{l} 12,\ 8, 10,\ 9,\ 5,\ 7,\ 6,\ 2,\ 4,\ 3, 11,\ 1, \\ 11,\ 7,\ 9,\ 8,\ 4,\ 6,\ 5,\ 1,\ 3,\ 2, 10, 12, \\ 10,\ 6,\ 8,\ 7,\ 3,\ 5,\ 4, 12,\ 2,\ 1,\ 9, 11; \end{array}$$

whence we see that the permutation satisfies the condition $s^3t^9P = P$, or $s^3P = t^3P$; also that it is a 3-cycle permutation.

All the 384 will not be 3-cycle permutations ; for the following are 1-cycle permutations, corresponding to the values of g, 7 and 11,

$$\begin{array}{l} 1,\ 8,\ 3, 10,\ 5, 12,\ 7,\ 2,\ 9,\ 4, 11,\ 6; \\ 1, 12, 11, 10,\ 9,\ 8,\ 7,\ 6,\ 5,\ 4,\ 3,\ 2. \end{array}$$

The 1-cycle permutations which satisfy the condition $(s^Gt)^xP = P$, may be determined as follows :—

This condition will be satisfied by $s^Gt P = P$ if this is a possible condition, that is to say, if G is prime to n, or prime to x as well as N. In the above example, $G = 3$, and is not prime to n, which is 12. But, since $s^n = s^{xN} = 1$, the condition $P = (s^Gt)^x P$ leads to

$$P = (s^Gt)^xP = (s^{G+N}t)^xP = (s^{G+2N}t)^xP = \ldots\ldots\ldots = \{s^{G+(x-1)N}t\}^xP ;$$

and from this we see that the condition will be satisfied if the index of s, which may as usual be denoted by g, has any one of the values $G, G+N, G+2N, \ldots\ldots G+(x-1)N$, provided it is prime to n, or prime to x as well as N. If x is prime to N, one of these x numbers is divisible by x, and the others give different remainders when divided by x ; and if x is a prime, these $(x-1)$ remainders will all

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

be prime to it, so that in the latter case we have $(x-1)$ different self-repeating cycles to which P may belong.

In the example we have been considering, $x=3$, $N=4$, $G=3$; and g may have the values $G+N, G+2N$, or 7 and 11; and we get the 2 self-repeating cycles given above.

In the case of these self-repeating cycles, the first x constituents of the cycle become

$a, a_1+G,$ $a_1+2G, \ldots\ldots\ldots\ldots a_1+(x-1)G$
or $a_1, a_1+G+N,$ $a_1+2(G+N)\ldots\ldots a_1+(x-1)(G+N)$
or $a_1, a_1+G+2N,$ $a_1+2(G+2N)\ldots\ldots a_1+(x-1)(G+2N)$
or etc. $\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$
or
$a_1, a_1+G+(x-1)N, a_1+2\{G+(x-1)N\}, \ldots a_1+(x-1)\{G+(x-1)N\}$

We have thus seen that the permutations which satisfy the condition $(s^G t)^x P = P$ may be either x-cycle permutations or 1-cycle permutations. But if x is a composite number, $=yz$ suppose, there may be also y-cycle and z-cycle permutations. In order that they may be y-cycle permutations, we must give $a_{1+y}, a_{1+2y}, \ldots\ldots a_{1+(z-1)y}$ the same values as they have in the 1-cycle permutations, as shown in the following scheme :—

	either	or	etc., etc.
a_{1+y}	a_1+yG	$a_1+y(G+N)$	
a_{1+2y}	a_1+2yG	$a_1+2y(G+N)$	
....	.....	.....	
$a_{1+(z-1)y}$	$a_1+(z-1)yG$	$a_1+(z-1)y(G+N)$	

For instance, if $n=12$, $x=4$, $N=3$, suppose we have found $G=4$; then the permutations will be represented by

1.5. 9
2.6.10
3.7.11
4.8.12

Here g may have the values 1,7; and we have 1-cycle permutations, belonging to the cycles :—

1,2,3, 4,5, 6,8,9,10,11,12,1.....
1,8,3,10,5,12,7,2, 4,11, 6,1.....

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

We have also 2-cycle permutations, which may be represented by

$$\left|\begin{array}{l} 1.3.5.7.\ 9.11 \\ 2.4.6.8.10.12 \end{array}\right|$$

Thus the permutation 1,4,3,6,5,8,7,10,9,12,11,2, is a 2-cycle permutation.

If, instead of supposing h and k to be known, and therefore H and K, we simply suppose n to be a composite number $= x\mathrm{N}$, it may be proved by a similar process that, if G be any number $< \mathrm{N}$ and prime to it, the permutations given by the formula on p. 72 all satisfy the condition $(s^{\mathrm{G}}t)^x\mathrm{P} = \mathrm{P}$.

Resuming our example, $n = 12$, $x = 3$, $\mathrm{N} = 4$, we may give G the values 1 and 3, and the permutations that satisfy the conditions $(st)^3\mathrm{P} = \mathrm{P}$, and $(s^3t)^3\mathrm{P} = \mathrm{P}$ respectively, are represented by

$$\left|\begin{array}{l} 1.4.7.10 \\ 2.5.8.11 \\ 3.6.9.12 \end{array}\right| \text{ and } \left|\begin{array}{l} 1.10.7.4 \\ 2.11.8.5 \\ 3.12.9.6 \end{array}\right|$$

When $\mathrm{G} = 1$, we may give g the values 5 and 1; and when $\mathrm{G} = 3$, we may give g the values 7 and 11.

Next putting $n = 12$, $x = 4$, $\mathrm{N} = 3$, we may give G the values 1 and 2, and the permutations that satisfy the conditions $(st)^4\mathrm{P} = \mathrm{P}$, and $(s^2t)^4\mathrm{P} = \mathrm{P}$ respectively are represented by

$$\left|\begin{array}{l} 1.5.\ 9 \\ 2.6.10 \\ 3.7.11 \\ 4.8.12 \end{array}\right| \text{ and } \left|\begin{array}{l} 1.\ 9.5 \\ 2.10.6 \\ 3.11.7 \\ 4.12.8 \end{array}\right|$$

When $\mathrm{G} = 1$, we may give g the values 1 and 7; and when $\mathrm{G} = 2$, we may give g the values 5 and 11.

Again, putting $n = 12$, $x = 2$, $\mathrm{N} = 6$, we may give G the values 1 and 5; and the permutations that satisfy the conditions $(st)^2\mathrm{P} = \mathrm{P}$, and $(s^5t)^2\mathrm{P} = \mathrm{P}$ respectively, are represented by

$$\left|\begin{array}{l} 1.3.5.7.\ 9.11 \\ 2.4.6.8.10.12 \end{array}\right| \text{ and } \left|\begin{array}{l} 1.11.\ 9.7.5.3 \\ 2.12.10.8.6.4 \end{array}\right|$$

When $\mathrm{G} = 1$, g may be 1 or 7; and when $\mathrm{G} = 5$, g may be 5 or 11.

Lastly, putting $n = 12$, $x = 6$, $\mathrm{N} = 2$, we can only give G the value 1; and g may be 1, 5, 7, or 11.

These results agree with those that we obtained before, see p. 70.

We have seen that when $s^ht^k\mathrm{P} = \mathrm{P}$, we always have $s^{mh}t^{mk}\mathrm{P} = \mathrm{P}$, and we are now able to answer the question whether the latter condition necessarily implies the former. This will always be the case

when m is prime to n; for then one of the numbers, $m, 2m, 3m, \ldots\ldots$ $(n-1)m$ must give a remainder 1 when divided by n. For instance, when $n=11$, if we have $s^6t^6\mathrm{P}=\mathrm{P}$, we must also have $s^3t^4\mathrm{P}=\mathrm{P}$; and when $n=12$, if $s^5t^5\mathrm{P}=\mathrm{P}$, we must have $st\mathrm{P}=\mathrm{P}$. In both these cases, P must be a 1-cycle permutation. It is not necessary that h and k should be prime to n; thus, if $n=12$, $h=k=2$, $m=5$, so that $s^{10}t^{10}\mathrm{P}=\mathrm{P}$, we must have $s^2t^2\mathrm{P}=\mathrm{P}$, and we may have also $st\mathrm{P}=\mathrm{P}$. In the latter case, P is a 1-cycle permutation for which $g=1$; but when $s^2t^2\mathrm{P}=\mathrm{P}$, P may either be one of the 1-cycle permutations for which $g=1$ or 7; or one of many 2-cycle permutations.

When m is not prime to n, it does not necessarily follow that $s^ht^k\mathrm{P}=\mathrm{P}$; but this may be the case if h and k are both prime to n, or if, on dividing all 3 numbers by their G.C.M., the quotients of h and k are both prime to the quotient of n. If h and n have a common factor which is not a factor of k, or if k and n have such a factor which is not a factor of h, the relation $s^ht^k\mathrm{P}=\mathrm{P}$ cannot subsist.

Let us now suppose that both x and N are primes; then, as we have seen, there are $(\mathrm{N}-1)$ admissible values of G; and for each of these, there are $(x-1)$ admissible values of g. There are, therefore, $(\mathrm{N}-1)(x-1)$ self-repeating cycles, and $n(x-1)(\mathrm{N}-1)$ 1-cycle permutations which satisfy the condition $(s^{\mathrm{G}}t)^x\mathrm{P}=\mathrm{P}$. Now we have seen that the total number of permutations which satisfy that condition for a given value of G, is $\mathrm{N}^x\times x!$; and the total number, for all values of G, is therefore $(\mathrm{N}-1)\mathrm{N}^x\times x!$ Now, since both x and N are prime, all of these must be either 1-cycle permutations or x-cycle permutations. Subtracting, then, the number of 1-cycle permutations, as found above, we get the number of x-cycle permutations:

$$\begin{aligned}&(\mathrm{N}-1)\mathrm{N}^x\times x!-n(\mathrm{N}-1)(x-1)\\&=n(x-1)(\mathrm{N}-1)\{\mathrm{N}^{x-1}\times(x-2)!-1\}\end{aligned}$$

Similarly, the number of N-cycle permutations is

$$n(x-1)(\mathrm{N}-1)\{x^{\mathrm{N}-1}\times(\mathrm{N}-2)!-1\}$$

But the total number of permutations of the n numbers is $n!$, and all of these must be either 1-cycle, x-cycle, N-cycle, or n-cycle permutations. Hence, by subtraction, the number of n-cycle permutations is

$$n!-n(x-1)(\mathrm{N}-1)\{\mathrm{N}^{x-1}\times(x-2)!+x^{\mathrm{N}-1}\times(\mathrm{N}-2)!-1\}$$

Since these can be arranged in sets containing n^2 each, this number must be divisible by n^2. Now, since $n=x\mathrm{N}$, $(n-1)!$ is clearly

divisible by n, and therefore $n!$ by n^2; and we thus see that the number will be divisible by n^2 if

$$N^{x-1} \times (x-2)! + x^{N-1} \times (N-2)! - 1 \ldots\ldots\ldots Z$$

is divisible by n. We will first prove that it is divisible by x. Since x is prime, and N prime to it, N^{x-1} is of the form $Mx+1$ (Fermat's Theorem): also $(x-2)!$ is of the form $M'x+1$ (Wilson's Theorem): hence $N^{x-1} \times (x-2)!$ is of the form $mx+1$, and $N^{x-1} \times (x-2)! - 1$ is divisible by x. And, since the other term in Z, namely, $x^{N-1} \times (N-2)!$ is divisible by x, Z itself is so divisible. Similarly Z is divisible by N, and therefore by xN or n.

These results may be otherwise stated as follows :—

Suppose that $n = xy$, where x and y are both prime, then the number of 1-cycle sets is $(x-1)(y-1)$; and this is also the number of the self-repeating cycles, while the number of the 1-cycle permutations is n times as many.

The number of the x-cycle sets is found by dividing the number of the x-cycle permutations, as above found, by nx, and is therefore

$$(x-1)(y-1)\{y^{x-1}(x-2)! - 1\} \div x$$

The number of y-cycle sets is

$$(x-1)(y-1)\{x^{y-1}(y-2)! - 1\} \div y\,;$$

and the number of n-cycle sets is

$$[(n-1)! - (x-1)(y-1)\{y^{x-1}(x-2)! + x^{y-1}(y-2)! - 1\}] \div n.$$

As an example we will take the case of $n = 6$. Here the only possible values of g are 1 and 5; and these give us the two self-repeating cycles :— 12345612....., 16543216.....

Next, putting $x = 2$, $y = 3$, we may have G = 1 or 2, and each of these values gives us $3^2 \times 2! = 18$ permutations. Those given by G = 1 may be symbolized by $\left|\begin{matrix} 1.3.5 \\ 2.4.6 \end{matrix}\right|$ These belong to 3 cycles, one of which, namely, 12345612..... is self-repeating; and excluding this, and writing down the other two, and performing the s operation on them, we have

143652.....	163254.....
632541.....	652143.....
521436.....	541632.....
416325.....	436521.....
365214.....	325416.....
254163.....	214365.....

https://doi.org/10.1017/S0013091500030856 Published online by Cambridge University Press

from which we see that the two cycles belong to a 2 cycle set.

Next, taking G = 2, we have $\left|\begin{matrix}1.5.3\\2.6.4\end{matrix}\right|$, which gives us the self-repeating cycle 16543216....., and two other cycles,

12563412..... 16543216.....

which belong to another 2-cycle set.

Again, if we take $x=3$, $y=2$, the only admissible value of G is 1, and we get $2^3 \times 3!$ or 48 permutations symbolized by $\left|\begin{matrix}1.4\\2.5\\3.6\end{matrix}\right|$. These belong to 8 cycles, 2 of which are the self-repeating cycles we have already had, and the other 6 are

126453....., 132465....., 135462.....,
153426....., 156423....., 162435..... ;

and these belong to two 3-cycle sets, as follows :—

126453.....	132465.....
615342.....	621354.....
564231.....	516243.....
453126.....	465132.....
342615...	354621.....
231564.....	243516.....

We have thus got

2 cycles belonging to 1-cycle sets
4 „ „ „ 2-cycle „
6 „ „ „ 3-cycle „

or 12 cycles in all ; and the total number of cycles being 5! or 120, the number of cycles which belong to 6-cycle sets is 108, and the number of such sets is 18. By actual trial I have found that the following 18 permutations give rise to these sets :—

123465	124653	126543
123564	125364	132654
123645	125463	135264
123654	125643	136254
124365	126354	136542
124635	126435	142653