COMPOSITIO MATHEMATICA

PAUL LÉVY

Sur quelques classes de permutations

Compositio Mathematica, tome 8 (1951), p. 1-48

<http://www.numdam.org/item?id=CM_1951__8__1_0>

Sur quelques classes de permutations

par

M. Paul Lévy.

Le chapitre I du présent travail a pour objet l'étude de la décomposition en cycles d'une classe simple de permutations. Quelques généralisations seront indiquées au chapitre II. Le chapitre III est consacré à l'étude, au même point de vue, d'une classe un peu moins simple de permutations [1]).

Chapitre I — *Les permutations* P_n.

1. *Définition de* P_n. — Nous désignerons par x un quelconque des entiers 1, 2, . . ., n, et par P_n la permutation des n premiers nombres entiers définie par les formules

$$(a) \qquad y = P_n x = 2x - 1 \qquad (2x - 1 \leqq n),$$

$$(b) \qquad y = P_n x = 2(n + 1 - x) \qquad (2x - 1 > n),$$

qu'on peut remplacer par la formule unique:

$$(1) \qquad \varepsilon(y - 1) \equiv 2(x - 1) \qquad [\mathrm{mod}\ (2n - 1)],$$

où $\varepsilon = \pm 1$. Il en résulte immédiatement que la $\sigma^{\text{ième}}$ itérée $x_\sigma = P_n^\sigma x$ est définie par la formule:

$$(2) \qquad \varepsilon(x_\sigma - 1) = \varepsilon(P_n^\sigma x - 1) \equiv 2^\sigma(x - 1) \quad [\mathrm{mod}\ (2n - 1)],$$

où $\varepsilon = \pm 1 = (-1)^\beta$, β désignant le nombre des opérations b qu'il faut employer pour former successivement les σ premiers transformés de x; comme les opérations a et b donnent respectivement des nombres impairs et des nombres pairs, c'est aussi le nombre des entiers pairs de la suite, $x_1, x_2, \ldots, x_\sigma$. C'est aussi le nombre des termes supérieurs à $\frac{n+1}{2}$ dans la suite $x_0, x_1, \ldots, x_{\sigma-1}$ (l'opération b s'applique en effet à ces nombres, et à eux seuls).

---

[1]) Les principaux résultats du présent travail ont été énoncés dans deux Notes présentées à l'Académie des Sciences le 9 août et le 20 septembre 1948 (C. R. Acad. Sc., t. 227, p. 422—423 et 578—579).

Il faut bien remarquer que la formule (2) définit à la fois ε et x_σ, sauf dans le seul cas où $x = 1$, cas où la valeur de ε est indifférente. Les valeurs possibles de ε $(x_\sigma - 1)$ sont en effet $0, \pm 1, \pm 2, \ldots, \pm (n-1)$; un de ces nombres et un seul est congru à $2^\sigma (x-1)$, et on en déduit sans ambiguité x_σ (ainsi que ε si $x \neq 1$).

2. *Eléments invariants.* — Quel que soit n, 1 est un élément invariant, se reproduisant par l'opération a. D'autre part, en écrivant que x se reproduit par l'opération b, il vient

$$x = \tfrac{2}{3}(n+1). \tag{3}$$

Si donc n est de la forme $2 + 3k$ $(k = 0, 1, 2, \ldots)$, il y a un autre élément invariant, donné par la formule (3). Dans le cas contraire 1 est le seul élément invariant.

Remarquons que, si x n'est pas un élément invariant, le cycle qui contient x, contient nécessairement des opérations des deux types a et b. Cela résulte immédiatement de ce que les transformés successifs de x par l'opération a sont donnés par

$$x_\sigma - 1 = 2^\sigma (x-1) \qquad (\sigma = 1, 2, \ldots),$$

et ne peuvent jamais coïncider avec x, sauf si $x = 1$. De même ses transformés par l'opération b sont donnés par

$$x_\sigma - \tfrac{2}{3}(n+1) = (-2)^\sigma \left[x - \tfrac{2}{3}(n+1)\right],$$

et ne peuvent coïncider avec x que si x a la valeur (3).

3. *Le théorème fondamental. — Le p.p.c.m. des ordres des cycles de* P_n (c'est-à-dire l'ordre du groupe des puissances de P_n ou, par abréviation, *l'ordre de* P_n) *est l'ordre du cycle qui contient* 2.

D'après la formule (2), l'ordre $\sigma = \omega(n)$ du cycle qui contient 2 est le plus petit nombre σ tel que

$$2^\sigma \equiv \varepsilon = \pm 1 \qquad [\mathrm{mod}\ (2n-1)]. \tag{4}$$

En multipliant les deux membres par $(x-1)$, il vient

$$2^\sigma (x-1) \equiv \varepsilon (x-1) \equiv \pm (x-1) \quad [\mathrm{mod}\ (2n-1)], \tag{5}$$

de sorte que $x_\sigma = x$. Tous les nombres x considérés, $1, 2, \ldots, n$, se reproduisent donc par l'opération P_n. Il en résulte que chacun d'eux appartient à un cycle d'ordre égal à σ ou sous-multiple de σ. Ce nombre σ, égal à l'ordre d'un ou plusieurs cycles et multiple de ceux des autres cycles, est bien le p.p.c.m. de tous ces ordres, c.q.f.d.

Remarquons de plus que, si un nombre x appartient à un cycle d'ordre σ', on a

$$2^{\sigma'}(x-1) \equiv \pm (x-1)$$

(nous ne répétons pas le module, qui est toujours $2n-1$).

Si $x-1$ est premier avec le module $2n-1$, cette formule entraîne

$$2^{\sigma'} \equiv \pm 1,$$

de sorte que σ' est à la fois multiple et sous-multiple de σ. Donc $\sigma' = \sigma$. Donc: *tous les nombres x tels que $x-1$ soit premier avec $2n-1$ appartiennent à des cycles d'ordre σ.*

Nous verrons que la réciproque n'est pas exacte. Si donc, suivant l'usage, on désigne par $\varphi(n)$ le nombre des entiers au plus égaux à n qui sont premiers avec n, et par suite par $\frac{1}{2}\varphi(2n-1)$ le nombre de ceux qui sont premiers avec $2n-1$, on peut seulement affirmer que l'ensemble des cycles d'ordre σ comprend au moins $\frac{1}{2}\varphi(2n-1)$ éléments.

4. *Types pairs et impairs, primitifs et non primitifs.* — Nous appellerons *type* d'un cycle l'expression telle que

$$a^{\alpha_1}b^{\beta_1}a^{\alpha_2}b^{\beta_2}\ldots a^{\alpha_\nu}b^{\beta_\nu} \tag{6}$$

qui définit la succession des opérations a et b qu'il faut effectuer pour retrouver l'élément initial x. Si on a pris pour x le plus petit élément du cycle, nécessairement pair et $\leqq \frac{n+1}{2}$ (sauf si le cycle se réduit à un élément invariant), cette expression commence par une opération a et finit par une opération b. Changer l'élément initial équivaut à effectuer une permutation circulaire sur les opérations considérées. Si le cycle est d'ordre σ, on a ainsi σ représentations distinctes du même type.

Nous poserons

$$\alpha = \Sigma\,\alpha_i, \quad \beta = \Sigma\,\beta_i.$$

On a donc $\sigma = \alpha + \beta$. Nous dirons que le type est *pair* si β est pair, *impair* si β est impair.

Si $\sigma = \lambda\sigma'$ (λ entier > 1), il peut arriver qu'un type soit de la forme A^λ, A désignant une succession déterminée de σ' opérations a et b. Nous dirons dans ce cas que c'est un type *non primitif* d'ordre σ. Les autres types seront dits *primitifs*.

Nous verrons au n° 5 que, pour une valeur donnée de n, il ne peut y avoir qu'un seul cycle de type donné; l'élément initial x est bien déterminé si on connaît la succession des opérations

du cycle. Si alors un cycle est d'un type de la forme A^λ, x et son transformé $x' = Ax$ par l'opération A, qui ont tous les deux la propriété de se reproduire par l'opération A^λ, sont égaux, et le cycle considéré est un cycle d'ordre σ' répété λ fois. Il peut être commode de considérer σ comme un *ordre apparent*; mais *l'ordre réel*, c'est-à-dire le nombre des éléments distincts du cycle, est σ' (à condition bien entendu que A ne soit pas lui-même de la forme B^μ, avec $\mu > 1$).

Au point de vue de la parité, il importe de distinguer A et A^λ. Ils définissent un même cycle, et on peut dire qu'ils constituent un même type. Mais, si on le représente par A, son ordre est σ', et sa parité est celle du nombre β' des opérations b que comprend A. Si on le représente par A^λ, c'est un type non primitif d'ordre $\sigma = \lambda\sigma'$, *et sa parité est celle de* $\beta = \lambda\beta'$.

Si alors on se reporte à la démonstration du théorème fondamental, on voit que, dans la formule (5), ε est, comme σ, indépendant de x. Tous les cycles sont donc des cycles, primitifs ou non, du même ordre σ, et la parité, *rapportée à cet ordre* (c'est-à-dire, si $\sigma = \lambda\sigma'$ et s'il s'agit d'un cycle d'ordre reél σ', définie par $\beta = \lambda\beta'$), est la même pour tous.

5. *Recherche des cycles de type donné.* — Le transformé de x par la succession d'opérations a et b définie par la formule (6) est

$$x_\sigma = \varepsilon(2^\sigma x - \lambda n - \mu) \qquad [\varepsilon = (-1)^\beta],$$

λ et μ étant des coefficients entiers, indépendants de n et de x, mais qui dépendent de la succession d'opérations considérée. Il en résulte que, si x est l'élément initial d'un cycle de ce type, on a

$$(2^\sigma - \varepsilon)x = \lambda n + \mu. \tag{7}$$

Pour $\sigma > 1$, le coefficient de x est toujours positif; x n'est donc jamais indéterminé. Comme nous l'avons annoncé au n° 5, pour une valeur donnée de n, il ne peut jamais y avoir qu'un seul cycle de type donné. Pour que ce type existe, il faut et il suffit que la valeur de x déduite de la formule (7) soit acceptable, c'est-à-dire, d'une part, qu'elle soit entière, d'autre part, qu'elle soit positive et $\leqq n$, ainsi que ses transformés successifs par les opérations du type considéré.

Cette dernière condition est nécessairement vérifiée. Si en effet x ou un de ses transformés n'appartenait pas à l'intervalle $(1, n)$, par les opérations a et b effectuées dans un ordre quelconque on s'éloignerait de plus en plus de cet intervalle, et on ne pourrait

ni y revenir, ni revenir à la valeur initiale (qu'elle soit ou non dans cet intervalle). Il n'y a donc qu'à écrire que x est entier.

A première vue, trois circonstances sont possibles:

1°. Les coefficients $2^\sigma - \varepsilon$ et λ sont premiers entre aux. Alors l'ensemble des valeurs de n pour lesquelles x est entier, ensemble que nous désignerons par e_σ, est une progression arithmétique de raison $2^\sigma - \varepsilon$. En désignant son plus petit élément par n_0, il est donc défini par la formule

$$n = n_0 + (2^\sigma - \varepsilon)k \qquad (k = 0, 1, 2, \ldots). \tag{8}$$

2°. $2^\sigma - \varepsilon$ et λ ont un p.g.c.d. $\delta > 1$, qui divise μ. Alors e_σ est défini par

$$n = n_0 + k\varrho \qquad \left(\varrho = \frac{2^\sigma - \varepsilon}{\delta};\ k = 0, 1, 2, \ldots\right).$$

3°. δ ne divise pas μ. Alors x et n ne sont jamais entiers en même temps. Nous verrons au n° 6 que cette dernière circonstance n'est en fait pas réalisée. Tous les types que l'on peut définir par une succession quelconque d'opérations a et b en nombre σ sont tous réalisés pour $n = 2^{2\sigma-1}$, et aussi, suivant la parité du type, par $2^{\sigma-1}$ ou par $2^{\sigma-1} + 1$.

Donc: *chaque ensemble e_σ est une progression arithmétique de raison ϱ égale à $2^\sigma - \varepsilon$ ou sous-multiple de ce nombre.*

Rappelons que σ est l'ordre, et que $\varepsilon = \pm 1$ dépend de la parité du type. La notation impropre e_σ ne doit pas faire oublier que l'ensemble ainsi désigné, pour une même valeur de σ, varie avec le type considéré. Il peut arriver que plusieurs types conduisent au même ensemble e_σ. Mais un ensemble e_σ correspondant à un type impair et un ensemble e_σ correspondant à un type pair sont nécessairement différents, puisque les raisons ϱ' et ϱ'' qui leur correspondent divisent respectivement $2^\sigma + 1$ et $2^\sigma - 1$, qui sont premiers entre eux.

6. *Cas où $n = 2^q + \delta$ ($\delta = 0$ ou 1).* — Dans ce cas, en posant $\varepsilon = 1 - 2\delta$ (donc $= \pm 1$), on a

$$2^{q+1} = 2n - 2\delta \equiv \varepsilon \qquad [\mathrm{mod}\ (2n - 1)],$$

de sorte que la formule (4) est vérifiée pour $\sigma = q + 1$. Elle ne l'est manifestement pour aucune valeur plus petite de σ. Donc: *pour $n = 2^q$, tous les cycles de P_n sont des cycles, primitifs ou non, d'ordre $q+1$, et pairs* (relativement à cet ordre); pour $n = 2^q + 1$ *tous les cycles de P_n sont des cycles, primitifs ou non, d'ordre $q + 1$, et impairs* (relativement à cet ordre). Il y a seulement

exception pour le type a (ou a^σ), qui correspond à l'élément invariant 1 et existe quel que soit n; cette exception s'explique parce que, comme nous l'avons vu, si $x = 1$, et dans ce cas seulement, la formule (2) cesse de déterminer ε. Il n'y a pas d'autre exception.

Montrons maintenant que: *tous les types possibles, primitifs ou non, d'ordre* $q + 1$, *sont réalisés une fois et une seule, soit pour* $n = 2^q$, *soit pour* $n = 2^q + 1$, *à la seule exception du type* a (*ou* a^{q+1}) *qui est réalisé pour ces deux valeurs de* n.

Nous savons déjà qu'aucun autre type que a ne peut être réalisé deux fois (cela résulte des considérations sur la parité; on peut aussi observer que, si un même type d'ordre est réalisé pour deux valeurs consécutives de n, cela implique que la progression arithmétique e_σ qui lui correspond comprend tous les nombres entiers; il ne peut donc s'agir que du type a, qui existe seul pour $n = 1$).

Il suffit donc, pour montrer que tous les types possibles d'ordre $\sigma = q + 1$, primitifs ou non, sont réalisés, de montrer qu'il les faut tous, chacun une fois et une seule, pour obtenir en tout

$$2^q + (2^q + 1) - 1 = 2^\sigma$$

éléments. Or, cela est bien évident. Chaque type a un nombre de représentations différentes égal à son ordre réel, c'est-à-dire au nombre de ses éléments distincts, et on obtient toutes les représentations de tous ces types en formant une suite de σ lettres dont chacune est a ou b.

D'une manière plus précise, comme on change la parité en changeant la dernière lettre, il y a $2^{\sigma-1}$ représentations distinctes pour l'ensemble des types de chaque parité; il faut donc exactement $2^{\sigma-1}$ éléments pour obtenir une fois et une seule tous les types distincts d'une même parité.

Donc: *tous les types, primitifs ou non, d'ordre* σ, *et pairs par rapport à cet ordre, sont réalisés pour* $n = 2^{\sigma-1}$; *tous ceux d'ordres impairs, et en plus le type pair* a^σ, *sont réalisés pour* $n = 2^{\sigma-1} + 1$. Tous les types de cycles d'ordre σ sont donc réalisés pour l'une ou l'autre de ces valeurs. Le résultat annoncé au n° 5 est ainsi établi.

On remarque que tous ces types sont des types non primitifs d'ordre 2σ, et pairs relativement à cet ordre. Donc: *tous existent pour* $n = 2^{2\sigma-1}$. Bien entendu, on n'obtient pas ainsi tous les éléments de P_n, pour $n = 2^{2\sigma-1}$.

On peut d'ailleurs déduire ce résultat des précédents, ou inversement en observant que

$$2^{2\sigma-1} - 2^{\sigma-1} \text{ et } 2^{2\sigma-1} - (2^{\sigma-1} + 1)$$

sont respectivement multiples de $2^\sigma - 1$ et de $2^\sigma + 1$, donc des raisons des progressions arithmétiques e_σ qui correspondent respectivement aux types pairs et aux types impairs.

7. *Deuxième méthode pour l'étude des cas précédents* [2]).

Considérons d'abord le cycle contenant 2. Les transformés successifs de 2 sont d'abord

$$2 + 1,\ 4 + 1,\ \ldots,\ 2^\nu + 1,\ \ldots,$$

et, si $n = 2^q + 1$, on peut aller ainsi jusqu'à $2^q + 1 = n$; on a ainsi une *séquence* de $q + 1$ nombres, obtenus par la seule opération a. L'opération b, appliquée à n, redonne 2. On a ainsi un cycle d'ordre $q + 1$, et du type impair $a^q b$. Si $n = 2^q$, il faut limiter à $2^{q-1} + 1$ la séquence issue de 2. Deux opérations b successives donnent alors n, puis 2. On obtient donc encore un cycle d'ordre $q + 1$; il est du type pair $a^{q-1}b^2$.

On peut faire un calcul analogue en partant de 4, ou 6, ou 8, etc. Indiquons encore un exemple numérique. En partant par exemple de 14, on trouve d'abord la séquence des $q - 3$ éléments

$$14 = 13 + 1,\ 26 + 1,\ 52 + 1,\ \ldots,\ 13 \cdot 2^{q-4} + 1.$$

Ensuite, en indiquant les opérations a par des virgules et les opérations b par des points et virgules; on trouve, pour $n = 2^q$,

$$\tfrac{3}{8}2^q,\ \tfrac{3}{4}2^q - 1;\ \tfrac{1}{2}2^q + 4;\ 2^q - 6;$$

puis on revient à 14. De même, pour $n = 2^q + 1$, on trouve

$$\tfrac{3}{8}2^q + 2,\ \tfrac{3}{4}2^q + 3;\ \tfrac{1}{2}2^q - 2,\ 2^q - 5;$$

puis on revient à 14. Dans les deux cas, le cycle est d'ordre $q + 1$. Dans le premier, il est du type pair $a^{q-4}bab^3$; dans le second il est du type impair $a^{q-4}bababab$.

Proposons-nous maintenant de montrer que, d'une manière générale: *pour* $n = 2^q$ *ou* $2^q + 1$, *le* $(q + 1)^{\text{ième}}$ *transformé d'un nombre quelconque* x *n'est autre que* x. En d'autres termes: *le cycle de* x *est d'ordre égal à* $q + 1$ *ou sous-multiple de* $q + 1$.

Comme cela est évident pour $x = 1$, et que, sauf pour le cycle réduit à l'élément invariant 1, le plus petit élément d'un cycle est toujours pair, nous pouvons supposer x pair ($x = 2\xi$). Comme cela est vrai pour $x = 2$, nous pouvons procéder par récurrence

---

[2]) La lecture de ce paragraphe n'est pas nécessaire pour la suite.

et supposer le théorème démontré pour 4, 6, ..., 2^{r-1}. Il s'agit de le démontrer dans l'hypothèse

$$2^{r-1} + 2 \leqq x = 2\xi \leqq 2^r. \tag{9}$$

Comme x doit être au plus égal à n, il faut que q soit au moins égal à r. Le cycle de x commence alors par la séquence

$$x,\ x_1 = 2x - 1,\ \ldots,\ x_{q-r} = 2^{q-r}(x-1) + 1;$$

qui contient $q + 1 - r$ éléments (donc, si $q = r$, elle se réduit à l'élément initial x). Quelles que soient les successions des opérations a et b que l'on a à appliquer ensuite, les transformés suivants de x sont de la forme

$$x_{q-r+k} = \lambda_k 2^{-r} + \mu_k \qquad (k = 1, 2, \ldots), \tag{10}$$

les entiers λ_k et μ_k, pour chacun des deux cas considérés ($n - 2^q = 0$ ou 1), dépendant de la succession des opérations a et b effectuées, mais non de q. On le vérifie par récurrence. On vérifie de même que, pour $k \leqq r$, λ_k est un multiple impair de 2^k. Quant à μ_k, si $n = 2^q$, on trouve successivement

$$\mu_1 = 0,\ \mu_2 = -1 \text{ ou } 2,\ -3 \leqq \mu_3 \leqq 4,$$

et d'une manière générale

$$-2^{k-1} + 1 \leqq \mu_k \leqq 2^{k-1}.$$

De même, pour $n = 2^q + 1$, on trouve

$$\mu_1 = 2,\ \mu_2 = 0 \text{ ou } 3,\ -2 \leqq \mu_3 \leqq 5,$$

et d'une manière générale

$$-2^{k-1} + 2 \leqq \mu_k \leqq 2^{k-1} + 1.$$

Dans les deux cas, pour $k = r$, on peut écrire

$$-2^{r-1} + 1 \leqq \mu_r - \delta \leqq 2^{r-1} \qquad (\delta = n - 2^q = 0 \text{ ou } 1). \tag{11}$$

Supposons d'abord $q = r$. Alors, ou bien x est invariant, et le théorème est exact dans ce cas; ou bien le plus petit élément x_0 du cycle qui contient x est un nombre pair au plus égal à $2^{r-1} + 1$, donc à 2^{r-1}, et le théorème a été supposé vrai dans ce cas. Le cycle de x, qui est celui de x_0, est donc d'ordre $r + 1$ ou sous-multiple de $r + 1$, et

$$x_r = \lambda_r 2^{q-r} + \mu_r = \lambda_r + \mu_r$$

est l'antécédent de x. Donc

$$\lambda_r + \mu_r = 2^r + 1 + \delta - \xi.$$

Or λ_r est un multiple impair de 2^r. Il résulte alors des inégalités (9) et (11) qu'on a nécessairement

$$\lambda_r = 2^r, \ \mu_r = 1 + \delta - \xi. \tag{12}$$

Supposons maintenant $q > r$, et transformons x par la même succession d'opérations que dans le cas où $q = r$. La formule (10) s'applique, λ_k et μ_k étant indépendants de q, de sorte que λ_r et μ_r ont encore les valeurs (12).

Or les opérations ainsi effectuées sont bien, même si $q > r$, celles qu'il faut effectuer pour avoir le cycle de x. Si en effet, à un moment quelconque, on n'avait pas appliqué celle des deux opérations qui convient, on obtiendrait un nombre extérieur à l'intervalle $(1, n)$, et ses transformés successifs seraient de plus en plus éloignés de cet intervalle. Il n'en est pas ainsi, puisqu'on arrive à

$$x_q = \lambda_r 2^{q-r} = \mu_r = 2^q + 1 + \delta - \xi = n + 1 - \xi.$$

Ce nombre est donc bien le $(q+1)^{\text{ième}}$ élément du cycle dont le premier est x, et le cycle se ferme ensuite par l'opération b qui redonne $2\xi = x$. Donc $x_{q+1} = x$, c.q.f.d.

Nous avons ainsi, pour $n = 2^q + \delta$, obtenu une démonstration du théorème fondamental indépendante de la formule (5) qui détermine à la fois σ et ε. Il est facile aussi, toujours sans utiliser la formule (5), de retrouver les résultats du n° 3 concernant la parité des types des cycles obtenus.

D'abord, d'après un raisonnement utilisé plus haut (n° 6), nous savons qu'un ensemble de cycles d'ordre $\sigma = q + 1$ *et de parité donnée* doit avoir 2^q éléments pour qu'il y ait un cycle et un seul de chaque type possible, primitif ou non. Considérons alors un type impair. D'après le n° 5, l'ensemble e_σ correspondant à ce type est une progression arithmétique dont la raison ϱ, au moins égale à 3, divise $2^q - 1$ et par suite

$$D = 2^{2q+1} - (2^q + 1) = (2 \cdot 2^q + 1)(2^q - 1).$$

Or, il faut (d'après le n° 6) que ce cycle soit réalisé, d'une part pour l'un des nombres 2^q et $2^q + 1$, d'autre part pour l'un des nombres 2^{2q+1} et $2^{2q+1}+1$. Comme, des quatre différences d'un de ces derniers nombres avec un des deux premiers, égales respectivement à D, $D+1$, $D+1$, $D+2$, la seule qui soit mutiple de ϱ est D, il faut bien que le cycle considéré soit réalisé pour $n=2^{q+1}$ et pour $n = 2^{2q+1}$. Donc, n'importe quel cycle, primitif ou non, d'ordre $\sigma = q + 1$, et de type impair (par rapport à cet ordre

σ) est réalisé pour $n = 2^q + 1$; ces cycles comprennent alors les nombres 2, 3, . . ., n (l'élément 1 constituant, quel que soit n, un cycle de type pair).

Il en résulte que les cycles d'ordre $\sigma = q + 1$ et de types pairs (par rapport à σ) sont tous réalisés pour $n = 2^q$.

8. *Etude des ensembles e_σ. Types naissants et types anciens.* — 1°. — Les équations (a) et (b) peuvent s'écrire

$$y - 1 = 2(x - 1) \qquad [2(x - 1) < n - \tfrac{1}{2}],$$
$$y - 1 = (2n - 1) - 2(x - 1) \qquad [2(x - 1) > n - \tfrac{1}{2}].$$

Elles sont homogènes en $2n - 1$, $x - 1$ et $y - 1$. Si donc, k désignant un entier positif, on pose

$$2n_k - 1 = (1 + 2k)(2n_0 - 1), \tag{13}$$

$$x_k - 1 = (1 + 2k)(x_0 - 1), \tag{14}$$
$$y_k - 1 = (1 + 2k)(y_0 - 1),$$

et si elles sont vérifiées pour les valeurs n_0, x_0, y_0 de n, x, y, elles le sont aussi pour les valeurs n_k, x_k, y_k. Donc: *la transformation*

$$x_k = x_0 + 2k(x_0 - 1) \qquad (k = 1, 2, \ldots). \tag{15}$$

fait correspondre à tout cycle de P_{n_0} un cycle du même type de la permutation P_n d'indice

$$n = n_k = n_0 + k(2n_0 - 1). \tag{16}$$

Ce cycle est donc réalisé pour tous les nombres de la progression arithmétique (16); les cycles de chaque permutation P_n que l'on obtient ainsi ne contiennent naturellement qu'une partie des éléments x de cette permutation, ceux pour lesquels $x - 1$ est multiple de $1 + 2k$.

2°. — Nous dirons qu'un type de cycle est *naissant* pour $n = n_0$ si, étant réalisé pour $n = n_0$, il ne l'est pour aucune valeur plus petite de n; en d'autres termes, si n_0 est le plus petit élément de l'ensemble e_σ relatif à ce type. Pour les autres nombre n de cet ensemble, c'est un *type ancien*.

Soit alors un cycle d'ordre σ et de type naissant pour $n = n_0$. Nous allons montrer que: *l'ensemble e_σ relatif à ce type est défini par la formule* (16), *où* $k = 0, 1, 2, \ldots$

D'après le 1°, il contient en effet tous ces nombres n_k. D'après le n° 5, c'est une progression arithmétique. Comme il contient celle définie par la formule (16), sa raison ϱ est égale, soit à $2n_0 - 1$, soit à un sous-multiple de ce nombre. Mais ce dernier

cas est exclu, puisqu'il impliquerait $\varrho < n_0$; e_σ contiendrait donc l'élément positif $n_0 - \varrho$, et n_0 ne serait pas son plus petit élément. Donc $\varrho = 2n_0 - 1$, c.q.f.d.

Donc: *un ensemble e_σ est bien défini par la donnée de son plus petit élément n_0; c'est une progression arithmétique de raison $2n_0$—1.*

3°. — *Corollaire. — Tous les types naissants pour une valeur donnée n' de η sont des cycles du même ordre réel σ et de la même parité. Les autres types ont un ordre réel égal à σ ou sous-multiple de σ.*

En effet, d'après le 2°, l'ensemble e_σ est le même pour tous les types naissants pour $n = n'$; σ est alors le plus petit entier tel que l'un des deux nombres $2^{\sigma-1} + \delta$ ($\delta = 0$ ou 1) appartienne à e_σ. Tous les types des cycles de $P_{n'}$ sont réalisés pour tous les P_n d'indices appartenant à e_σ, donc pour $n = 2^{q-1} + \delta$. Donc, d'après le n° 6, ce sont des types, primitifs ou non, d'ordre σ; ils sont tous pairs si $\delta = 0$, et, sauf le type a qui est toujours pair, ils sont tous impairs si $\delta = 1$.

Soit σ_0 l'ordre réel d'un de ces types. Si $\sigma_0 < \sigma$, ce type est réalisé pour $n = 2^{\sigma_0-1} + \delta_0$ ($\delta_0 = 0$ ou 1); d'après la définition de σ, ce nombre n n'appartient pas à e_σ, et le type considéré n'est pas naissant pour $n = n'$. Donc inversement, tous les types naissants pour $n = n'$ ont le même ordre réel $\sigma = \omega(n')$, ce qui achève la démonstration du corollaire énoncé.

La réciproque de ce dernier résultat n'est évidemment pas exacte: si n_0 n'est pas de la forme 2^q ou $2^q + 1$, P_{n_0} comprend au moins un cycle d'ordre $\sigma = \omega(n_0)$ et d'un type naissant qui, pour $n = 2^{\sigma-1} + \delta$ ($\delta = 0$ ou 1 suivant la parité de ce type) se retrouve comme type ancien en même temps que d'autres types nouveaux du même ordre. Donc: *un cycle de P_n de type ancien peut être d'ordre réel $\sigma = \omega(n)$.*

On remarque que, si l'on suppose les résultats relatifs au cas où $n = 2^q + \delta$ établis par la méthode du n° 7, les raisonnements qui précèdent sont indépendants du n° 3.

4°. — *Recherche des types anciens pour $n = n'$.* — Un tel type est naissant pour $n = n_0 < n'$, et n' peut être identifié au nombre n_k de la formule (13), k étant positif. Donc $p_0 = 2n_0 - 1$ est sous-multiple de $p' = 2n' - 1$. On obtient donc tous les types anciens pour $n = n'$ en prenant successivement pour p_0 tous les sous-multiples de $p' = 2n' - 1$, et en formant les types naissants pour les valeurs de $n_0 = \dfrac{p_0 + 1}{2}$ qui s'en déduisent.

Naturellement, on peut aussi ne considérer que les sous-

multiples p de p' obtenus en divisant successivement p' par tous ses diviseurs premiers; pour les nombres $n = \frac{p+1}{2}$ qui s'en déduisent, on formera alors tous les types de P_n, naissants ou anciens; ils seront tous des types anciens de P_n; mais, si p' n'est pas premier, certains types anciens de $P_{n'}$ seront obtenus plusieurs fois, tandis que par la première méthode chacun était obtenu une fois et une seule.

Pour $n' > 1$, donc $p' \geqq 3$, le diviseur $p_0 = 1$ de p' donne toujours le type ancien a, qui est nouveau pour $n_0 = 1$.

5°. — *L'ensemble des cycles de types naissants pour $n = n'$.*

Si un nombre x' appartient à un cycle de type ancien pour $n = n'$, il peut être identifié au nombre x_k de la formule (14). Donc $x_k - 1$ est multiple de $2k + 1$ qui, d'après ce qui précède, est un diviseur de p, supérieur à 1, à cela près quelconque. Inversement, n'importe quel multiple de $2k + 1$, inférieur à n', peut être identifié à $x_k - 1$. L'ensemble des éléments x' appartenant à des cycles de types anciens pour $n = n'$ est donc l'ensemble de ceux pour lesquels $x' - 1$ et $2n' - 1$ ont un diviseur commun autre que 1.

Donc inversement: *l'ensemble des éléments x' appartenant à des cycles de types naissants pour $n = n'$ est l'ensemble des éléments pour lesquels $x' - 1$ est premier avec $2n' - 1$.*

6°. *Corollaire. — Le nombre des éléments de P_n qui appartiennent à des cycles de types naissants est* $\frac{1}{2}\varphi(2n-1)$, $\varphi(n)$ étant la fonction arithmétique déjà considérée au n° 3. Pour $n > 1$, ν et $2n - 1 - \nu$ étant en même temps premiers avec $2n - 1$, le nombre des éléments de la suite $1, 2, \ldots, n - 1$, qui sont premiers avec $2n - 1$ est en effet $\frac{1}{2}\varphi(2n-1)$.

L'ordre σ des types naissants est donc nécessairement un diviseur de $\frac{1}{2}\varphi(2n-1)$.

7°. *Pour que, sauf le cycle réduit à l'élément invariant* 1, *tous les cycles de P_n soient de types naissants, il faut et il suffit que $p = 2n - 1$ soit premier.*

Cet énoncé est un corollaire du précédent. En effet $\frac{1}{2}\varphi(2n-1) = n - 1$, c'est-à-dire $\varphi(p) = p - 1$, signifie que p est premier.

8°. Nous avons vu que tous les types naissants, pour une valeur donnée de n, ont le même ordre réel $\sigma = \omega(n)$. Compte tenu du 6°, il en résulte que σ divise $\frac{1}{2}\varphi(2n-1)$ et que l'ensemble des cycles d'ordre réel $\sigma = \omega(n)$ comprend au moins $\frac{1}{2}\varphi(2n-1)$ éléments. Si $2n - 1$ est premier, il en résulte que σ divise $n - 1$:

pour que σ *divise* $n-1$, *il suffit que* $p = 2n-1$ *soit premier.*

Cette condition n'est d'ailleurs pas nécessaire. Ainsi, pour $n = 1024 = 2^{10}$, on a $p = 2047 = 23 \cdot 89$; ce nombre n'est pas premier. Pourtant $\sigma = 11$ divise $n-1 = 1023$; d'après le premier théorème de Fermat, il en est toujours de même lorsque, n étant de la forme $2^{\sigma-1}$, σ est premier. On le voit aussi en observant que, si σ est un nombre premier impair, $n \equiv 1 \pmod 3$, et P_n ne comprend pas d'autre élément invariant que 1; donc les cycles d'ordre réel σ comprennent $n-1$ éléments, et σ divise $n-1$.

Dans le cas qui nous occupe, $\sigma = 11$, et P_n comprend nécessairement 93 cycles d'ordre réel 11. Le nombre p n'étant pas premier, ces cycles ne sont pas tous de types naissants; les cycles de types naissants comprennent $\frac{1}{2}\varphi(p) = 11 \cdot 88$ éléments; leur nombre est donc 88, et il y a 5 types anciens. Ils sont naissants pour les valeurs 12 et 45 de n_0, obtenues en prenant successivement pour $p_0 = 2n_0 - 1$ les deux diviseurs de p; donc un de ces types est naissant pour $n_0 = 12$; les quatre autres le sont pour $n_0 = 45$.

Des circonstances analogues se retrouvent pour tous les nombres σ ayant la double propriété d'être premiers et que $2^\sigma - 1$ ne le soit pas. Des considérations simples de calcul des probabilités conduisent à penser qu'il y a une infinité de ces nombres, mais que leur fréquence dans la suite des nombres premiers tend vers zéro; 11 est le plus petit de ces nombres [3]).

9°. Du résultat énoncé au début du 8° résulte évidemment que: *pour que* $\sigma = n-1$, *il suffit que* $n-1$ *et* $2n-1$ *soient premiers* (en effet, si $n > 2$, σ divise $n-1$ et est > 1; si $n = 2$, $\sigma = 1$).

La condition que $p = 2n-1$ soit premier est nécessaire, puisque $\sigma = n-1$ implique que cet unique cycle de type naissant comprenne $n-1$ éléments; alors, d'après le 7°, p est premier.

La condition que $n-1$ soit premier n'est pas nécessaire. On a en effet $\sigma = n-1$ pour les valeurs

6, 9, 14, 18, 26, 30, 33, 35, 39, 50, 51, 65, 69, . . .,

de $n-1$.

En utilisant encore des considérations simples de calcul des

[3]) V. P. Lévy, Communic. à la Soc. Math. de France (10 février 1937). Sans se reporter à cette communication, le lecteur verra au 9° ci-dessous quelle est la nature des considérations de calcul des probabilités qui, sans donner de démonstrations, semblent permettre de prévoir certains théorèmes de théorie des nombres.

probabilités, on est conduit à penser que les nombres $\sigma = n - 1$ qui sont premiers en même temps que $2\sigma + 1 = 2n - 1$ forment une suite infinie dont la densité tend vers zéro comme

$$\frac{2}{(\log n)^2} \Pi' \left[1 - \frac{1}{(q-1)^2}\right],$$

Π' désignant un produit étendu à tous les nombres premiers impairs. En effet, la probabilité pour que σ et $2\sigma + 1$ soient tous les deux premiers avec un nombre premier impair q est

$$1 - \frac{2}{q} = \left(1 - \frac{1}{q}\right)^2 \left[1 - \frac{1}{(q-1)^2}\right].$$

On est ainsi conduit à multiplier par le second facteur une probabilité calculée comme si, au lieu de $2\sigma + 1$, il s'agissait d'un nombre choisi au hasard au voisinage de $2n$ (par exemple entre $\frac{3}{2}n$ et $\frac{5}{2}n$), et admettre que les probabilités ainsi calculées deviennent des fréquences. En tenant compte en outre du rôle spécial du nombre premier 2 ($2\sigma + 1$ étant sûrement impair), on obtient le résultat énoncé.

S'il est exact, il donne une borne inférieure pour la fréquence des nombres n pour lesquels $\omega(n) = n - 1$.

10°. Une question en rapport avec celles que nous venons de traiter est celle du nombre total $\psi(n)$ des éléments de P_n qui appartiennent à des cycles d'ordres sous-multiples de $\sigma = \omega(n)$. Ces cycles étant nécessairement de types anciens, nous savons que ce nombre est au plus $n - \frac{1}{2}\varphi(2n - 1)$. Comme $\varphi(2n - 1)$ peut être très petit par rapport à n, cela ne donne qu'une limite supérieure élevée, qui en fait n'est pas la véritable borne supérieure de $\psi(n)$.

A ce sujet, indiquons d'abord un résultat vérifié empiriquement pour les faibles valeurs de n, et qui semble général. Il peut arriver que $\sigma = \omega(n)$ soit égal à $\frac{n+h}{2}$ ($h = 0$, ou 1, ou 2); ainsi $\omega(8) = 4$, $\omega(23) = 12$, $\omega(38) = 20$. Dans les cas de ce genre, il n'y a qu'un cycle d'ordre σ, et $\psi(n) = \frac{n-h}{2}$. Il semble probable que les grandes valeurs de $\psi(n)$ sont réalisées dans ces conditions; on aurait toujours $2\psi(n) \leqq n$, peut-être même $2\psi(n) < n$ sauf pour $n = 8$, et il existerait une suite infinie de valeurs de n pour lesquelles $\frac{\psi(n)}{n}$ tende vers $\frac{1}{2}$, ou même pour lesquelles $n - 2\psi(n)$ soit borné (ou même égal à 1).

On peut obtenir une borne supérieure beaucoup plus étroite pour $\psi(n)$ dans le cas où $n = 2^q + \delta$ (δ désignant toujours 0 ou 1). Dans ce cas, $\sigma = q + 1$, et, si l'ordre σ' d'un cycle de P_n est inférieur à σ, il divise σ.

Sa plus grande valeur possible est donc $\frac{\sigma}{2}$; elle n'est réalisée que si σ est pair (donc q impair), et pour $\delta = 0$, puisqu'un type de cycle d'ordre $\sigma' = \frac{\sigma}{2}$, considéré comme type non primitif d'ordre σ, est toujours pair. Dans ce cas, les cycles d'ordre égal à σ' ou sous-multiple de σ' comprennent $2^{\sigma'} = \sqrt{2n}$ éléments. Ce nombre donne une borne inférieure de $\psi(n)$, et les autres sous-multiples de σ étant $\leqq \frac{\sigma}{3}$, on a pour n très grand, $\psi(n) = \sqrt{2n} + O(n^{\frac{1}{3}})$.

Dans les autres cas, la plus grande valeur possible pour σ' est $\frac{\sigma}{3}$. Si σ est multiple de 3, les cycles, primitifs ou non, d'ordre $\sigma' = \frac{\sigma}{3}$ et de types pairs comprennent $2^{\sigma'-1}$ éléments, et sont réalisés pour $n = 2^q$; ceux de types impairs sont réalisés pour $n = 2^q + 1$. Dans chacun de ces deux cas, on a un ensemble de

$$\tfrac{1}{2}\sqrt[3]{2(n-\delta)}$$

éléments appartenant à des types, primitifs ou non, d'ordre σ', et on a

$$\psi(n) \geqq \tfrac{1}{2}\sqrt[3]{2(n-\delta)} + \delta \text{ et } \psi(n) = \tfrac{1}{2}\sqrt[3]{2n} + O(n^{\alpha}),$$

α désignant un exposant au plus égal à $\frac{1}{5}$ (si σ est multiple de 12, le diviseur $\frac{\sigma}{4}$ n'intervient pas si $\delta = 1$; le cas où σ est pair et $\delta = 0$ a déjà été considéré; il en résulte que la valeur $\alpha = \frac{1}{4}$ est exclue).

D'une manière générale, sauf dans le cas considéré d'abord où $\delta = 0$ et où $\sigma = q + 1$ est pair, on a pour $n = 2^q + \delta$,

$$\psi(n) = \tfrac{1}{2}(2n)^{\frac{1}{r}} + O(n^{\frac{1}{r'}}),$$

r et r' ($r' > r$) désignant les deux plus petits diviseurs premiers et impairs de $q + 1$.

On remarque que si, pour $n = 2^q + \delta$, $\psi(n)$ est ainsi petit par rapport à n, il est grand par rapport à σ, sauf bien entendu

si $\sigma = q + 1$ est premier, cas où $\psi(n) = 1 + \delta$. Le maximum de $\psi(n)$, pour $\sigma = \omega(n) \leqq 2\sigma'$, est réalisé pour $\sigma = 2\sigma'$, $n = 2^{\sigma-1} + 1$, et est, d'après ce qui précède, à la fois $\geqq 2^{\sigma'} + 1$, et équivalent à cette valeur, pour n infini.

Désignons maintenant par $\lambda = \lambda(n)$ le nombre des cycles de P_n dont l'ordre est $\sigma = \omega(n)$. Nous avons indiqué que, si $\lambda = 1$, on a probablement $\psi(n) \leqq \sigma$ (et même peut-être $< \sigma$, sauf pour $n = 8$). Ce résultat, et celui que nous venons d'établir pour les cas où λ (en fonction de n, ou de σ) est aussi grand que possible, suggèrent qu'il doit être possible de trouver pour $\psi(n)$ une borne supérieure de la forme $f(\lambda, \sigma)$, cette fonction se réduisant à σ si $\lambda = 1$, et étant de l'ordre de grandeur de $2^{\sigma'}$ $\left(\sigma' = \frac{\sigma}{2}\right)$ quand λ atteint sa borne supérieure qui est infiniment grande et équivalente à $\frac{2^{\sigma-1}}{\sigma}$.

9. *Intersection de deux ensembles e_σ.* — Désignons par e' et e'' deux ensembles de la classe des e_σ, correspondant respectivement à des valeurs σ' et σ'' de σ, et définis respectivement par les formules

$$n'_k = n'_0 + (2n'_0 - 1)k, \quad n''_k = n''_0 + (2n''_0 - 1)k$$

($k = 0, 1, 2, \ldots$). Le p.g.c.d. des deux raisons $\varrho' = 2n'_0 - 1$ et $\varrho'' = 2n''_0 - 1$ est impair, et divise leur différence $2(n'_0 - n''_0)$; il divise donc $n'_0 - n''_0$, qui est représentable par la forme

$$\lambda'(2n'_0 - 1) + \lambda''(2n''_0 - 1)$$

(λ' et λ'' entiers, de signes quelconques). L'intersection e de e' et e'' existe donc, et est une progression arithmétique dont la raison ϱ est le p.p.c.m. de ϱ' et ϱ'' [4]).

Posons $\varrho = 2n_0 - 1 = \lambda'\varrho' = \lambda''\varrho''$ (ϱ' et ϱ'' étant impairs, ϱ, λ' et λ'' le sont aussi). On a

$$n_0 - n'_0 = \frac{\varrho - \varrho'}{2} = \frac{\lambda' - 1}{2}\varrho',$$

de sorte que n_0 appartient à e'; il appartient de même à e'', donc à e. Cet ensemble e est donc défini par

$$n_k = n_0 + (2n_0 - 1)k \qquad (k = 0, 1, \ldots).$$

C'est donc un ensemble e_σ.

---

[4]) Pour exclure l'hypothèse que e' et e'' soient sans éléments communs, on peut observer aussi que, si μ est le p.p.c.m. de σ' et σ'', tous les deux contiennent $2^{2\mu}$.

Le théorème fondamental nous apprend que σ est multiple de σ' et σ''. Le résultat précédent précise ce théorème en nous apprenant qu'à deux types donnés A' et A'', d'ordres réels σ' et σ'', on peut toujours associer au moins un troisième type A, d'ordre multiple à la fois de A' et A'', tel que la présence simultanée des types A' et A'' entraîne celle de A.

On peut d'ailleurs aisément définir σ en fonction de σ', σ'', et des nombres ε' et ε'' qui définissent les parités des types A' et A''. On remarquera que, compte tenu du n° 7, on a ainsi une nouvelle démonstration du théorème fondamental.

L'ordre cherché σ est en effet le plus petit nombre tel que $2^{\sigma-1} + \delta$ ($\delta = 0$ ou 1) appartienne à la fois à e' et e'', donc à e. Or, pour qu'il appartienne à e', il faut et il suffit que $\sigma = \nu'\sigma'$ (ν' étant entier) et que $\varepsilon = 1 - 2\delta = (\varepsilon')^{\nu'}$ (ce nombre définissant la parité du cycle A' considéré comme étant d'ordre σ; en d'autres termes, si A' contient β' opérations b, $\varepsilon = (-1)^{\beta'\nu'}$). Il faut qu'on ait de même $\sigma = \nu''\sigma''$ et $\varepsilon = (\varepsilon'')^{\nu''} = (-1)^{\beta''\nu''}$.

Le nombre σ est donc multiple à la fois de σ' et σ'', donc de leur p.p.c.m., μ. Si alors $\frac{\mu}{\sigma'}\beta'$ et $\frac{\mu}{\sigma''}\beta''$ ont la même parité, les conditions

$$\varepsilon = (-1)^{\beta'\nu'} \text{ et } \varepsilon = (-1)^{\beta''\nu''}$$

sont compatibles pour $\sigma = \mu$ (donc $\frac{\mu}{\sigma'} = \nu'$, $\frac{\mu}{\sigma''} = \nu''$) et μ est bien la valeur cherchée. Dans le cas contraire, μ ne convient pas, et on a $\sigma = 2\mu$; en effet ν' et ν'' sont alors pairs, et les deux conditions imposées à ε sont identiques; on a $\varepsilon = 1$, donc $\delta = 0$.

Remarquons que, si $\sigma' = 2$, et σ'' impair, le type A' ne peut être que ab; il est impair. Dans ce cas $\mu = 2\sigma''$, et la valeur $\sigma = \mu$ ne convient pas, $\beta'\nu' = \beta'\sigma''$ étant impair, tandis que $\beta''\nu'' = 2\beta''$ est pair. Donc $\sigma = 2\mu = 4\sigma''$.

Ainsi l'intersection d'un e_2 et d'un e_3 est toujours un e_{12}; celle d'un e_2 et d'un e_5 est toujours un e_{20}; et ainsi de suite.

Si, au contraire $\sigma'' \geqq \sigma' > 2$, les deux parités sont possibles pour A' et pour A'', et $\frac{\mu}{\sigma'}$ et $\frac{\mu}{\sigma''}$, premiers entre eux, ne peuvent pas être tous les deux pairs. Alors la valeur de σ(μ ou 2μ) n'est pas déterminée par σ' et σ''; elle dépend aussi de la parité des types choisis. Ainsi l'intersection d'un e_3 et d'un e_5 est un e_{15} si A' et A'' sont de la même parité, et un e_{30} dans le cas contraire.

Quant à la parité du type résultant, lié à e_σ, remarquons que

ce sera généralement un type pair. Pour que ce soit un type impair, il faut en effet que $\beta'\nu'$ et $\beta''\nu''$ soient impairs, ce qui implique: 1° que A' et A'' soient tous les deux de types impairs: 2° que σ' et σ'' soient tous les deux impairs ou tous les deux multiples impairs d'une même puissance de 2. L'ensemble de ces conditions, réalisé avec une probabilité voisine de $\frac{1}{12}$ (si l'on choisit au hasard σ', puis σ'', puis un type d'ordre σ' et un type d'ordre σ''), est suffisant.

10. *Résultats numériques.* — Nous donnerons en annexe un tableau (tableau I) indiquant la décomposition de P_n en cycles pour $n = 2, 3, \ldots, 45$, et pour certaines valeurs plus grandes, notamment pour tous les $n \leqq 75$ et tels que $2n - 1$ soit premier et pour tous ceux de la forme $2^q + \delta$ ($q \leqq 11$, $\delta = 0$ ou 1).

Nous allons indiquer ci-dessous les e_σ qui correspondent aux valeurs de σ au plus égales à 8. Comme chaque e_σ est défini par son plus petit élément n_0, il suffit d'indiquer la valeur de n_0. Comme, d'autre part, tous les e_σ contiennent la valeur $2^{\sigma-1} + \delta$ de n (δ=0 ou 1 suivant la parité du type considéré), il suffit d'indiquer les valeurs de n_0 inférieures à cette valeur qui correspondent à ce qu'on peut appeler les types *fréquents* pour lesquels la raison ϱ est sous-multiple de $2^\sigma - \varepsilon$. On les obtient par la méthode, indiquée au n° 8, 4°, et appliquée déjà au 8° à $n = 1024$, pour chercher les $n_0 < n$ et qui correspondent aux types anciens de P_n; parmi ceux-là, il ne faut naturellement retenir que ceux pour lesquels $\omega(n_0) = \omega(n) = \sigma$. Rappelons que, si $2n - 1$ est premier, il n'y en a pas: tous les cycles de P_n, sauf ceux qui sont réduits à un élément invariant, sont dans ce cas d'ordre σ et de types naissants pour la valeur n considérée.

Les résultats sont les suivants: pour $\sigma < 5$, on n'a jamais $n_0 < n$. Pour $\sigma = 5$, 31 étant premier, les types pairs d'ordre 5 sont tous naissants pour $n = 16$; le type impair a^2b^3 est naissant pour $n_0 = 6$; les deux autres types impairs sont naissants pour $n = 17$. Pour $\sigma = 6$, le type impair a^2b^2ab est naissant pour $n_0 = 7$; le type pair a^3bab est naissant pour $n_0 = 11$; les autres types sont naissants pour $n = 32$ ou 33. Pour $\sigma = 7$, 127 étant premier, tous les types pairs sont naissants pour $n = 64$; trois types impairs sont naissants pour $n_0 = 22$, les six autres pour $n = 65$. Pour $\sigma = 8$, 257 étant premier, tous les types impairs sont naissants pour $n = 129$; deux types pairs sont naissants pour $n = 22$, quatre autres pour $n = 43$, les huit autres pour $n = 128$.

CHAPITRE II — *Généralisations.*

11. *Remarques préliminaires.* — La permutation P_n que nous venons d'étudier est une des huit permutations des n nombres 1, 2, . . ., n qu'on peut définir de la manière suivante: on pose $n = 2n' + \delta$ ($\delta = 0$ ou 1); les nombres pairs 2, 4, . . ., $2n'$ sont les transformés, soit des nombres 1, 2, . . ., n', soit des nombres n, $n - 1$, $n - n' + 1$, tandis que les nombres impairs sont les transformés des $n' + \delta$ nombres restants. Dans chacun des deux cas, chacune des transformations partielles est définie par une formule linéaire, de la forme

$$y = \pm 2x + h.$$

Il y a alors trois classes de permutations. Pour chaque valeur de n, la classe C_0 obtenue en prenant deux signes +, comprend deux permutations. La classe C_1, obtenue en prenant deux signes différents, en comprend quatre, dont P_n. La classe C_2, obtenue en prenant deux signes —, en comprend deux (l'indice est toujours le nombre des signes —).

Dans chaque classe, une réduction triviale permet de ne considérer qu'une des permutations. Ainsi, en partant de P_{n+1}, en supprimant l'élément invariant 1, et remplaçant x et y par $x + 1$ et $y + 1$, il vient

$$\begin{aligned} y &= 2x && (x = 1, 2, \ldots, n') \\ y &= 2(n - x) + 1 && (x = n' + 1, \ldots, n). \end{aligned}$$

C'est la seconde permutation de la classe C_1. Les deux autres se déduisent des deux premières par le changement de x et y en $n + 1 - x$ et $n + 1 - y$.

Il en résulte que, pour deux des quatre substitutions considérées, les ordres des différents cycles sont ceux de P_n; pour les deux autres, ce sont ceux de P_{n+1}, à cela près qu'un élément invariant a été supprimé.

Une réduction analogue nous permettra, pour chacune des deux autres classes, de n'étudier qu'un seul de ses deux types de substitutions.

12. *La classe C_0.* — Nous poserons $n = 2n' - \delta$ ($\delta = 0$ ou 1), et considèrerons la substitution $P_n^{(0)}$ définie par les formules

$$\begin{aligned} &(a) && y = 2x - 1 && (x = 1, 2, \ldots, n') \\ &(a') && y = 2(x - n') && (x = n' + 1, n' + 2, \ldots, n). \end{aligned}$$

Les formules sont les mêmes pour $n = 2n'$ et pour $n = 2n' - 1$; on passe simplement du premier cas au second en supprimant

l'élément invariant $2n'$. Les cycles sont les mêmes dans les deux cas, sauf le cycle du type a', constitué par cet élément invariant, qui n'existe que dans le premier cas. On passe d'une manière analogue de $P_n^{(0)}$ à la seconde substitution de la classe C_0 et d'ordre $n-1$ en supprimant l'élément invariant 1 et en remplaçant 2, 3, ..., n par 1, 2, ..., $n-1$.

Si $n = 2n' - 1$, les formules (a) et (a') peuvent être remplacées par la formule unique

$$y \equiv 2x - 1 \qquad [\mathrm{mod}\ (2n' - 1)], \tag{17}$$

formule exacte aussi pour $n = 2n'$, mais qui dans ce cas ne permet pas, pour $x \equiv 1$, de savoir si y a la valeur 1 ou la valeur n.

La formule (17) conduit immédiatement, pour le $\sigma^{\text{ième}}$ itéré x_σ de x, à la formule

$$x_\sigma - 1 \equiv 2^\sigma (x - 1) \qquad [\mathrm{mod}\ (2n' - 1)], \tag{18}$$

qui joue ici le même rôle que la formule (2) pour la transformation P_n. On en déduit immédiatement que le théorème fondamental subsiste sans modification: *l'ordre* $\sigma = \omega(n)$ *du cycle qui contient 2 est le p.p.c.m. des ordres de tous les cycles.*

Mais on remarque deux différences importantes pour le reste de la théorie. D'une part, le coefficient de x dans la formule (2) était ± 2; ici le double signe a disparu. Il n'y aura pas à distinguer des types pairs et des types impairs; tous les types sont pairs, et $\varepsilon = 1$. D'autre part $\sigma = \omega(n)$ est ici le plus petit exposant pour lequel $2^\sigma \equiv 1$ (et non ± 1), le module étant $2n' - 1$, et non $2n - 1$.

Dans l'ensemble, la théorie que nous avons exposée au chapitre I s'applique à $P_n^{(0)}$. Il semble suffisant de signaler les principales différences, conséquences de celles que nous venons d'indiquer.

Pour $n = 2^\sigma$, tous les types, primitifs ou non, d'ordre σ sont réalisés une fois et une seule, sans qu'il y ait à distinguer les types pairs et les types impairs. Donc, pour $n = 2^\sigma - 1$, ils le sont tous, sauf le type a'.

Les équations (a) et (a') subsistent si on y remplace $x - 1$, $y - 1$ et $2n' - 1$ par $(2k+1)(x-1)$, $(2k+1)(y-1)$, $(2k+1)(2n'-1)$. Il en résulte que les principaux résultats du n° 8 subsistent, pour n impair, avec quelques changement provenant, d'une part de ce que tous les types sont pairs, d'autre part de ce que n et $p = 2n - 1$ doivent être remplacés par n' et $n = 2n' - 1$. Ainsi l'ensemble $e_\sigma^{(0)}$ des valeurs impaires de n pour lesquelles un type donné d'ordre σ est réalisé est l'ensemble des multiples impairs de son plus petit élément n_0.

Notons que, toutefois, la condition $x \leqq n$ reste inchangée, n ne devant pas être remplacé par n'. Il en résulte que le nombre des éléments appartenant à des cycles de types naissants, pour n impair, est $\varphi(n)$, et non $\frac{1}{2}\varphi(n)$; si n est premier, ces cycles comprennent tous les éléments autres que 1. Si alors $n = 2n' - 1$ et $n' - 1$ sont premiers à la fois, σ peut être égal, soit à $n' - 1$, soit à $n - 1$. Ces circonstances sont effectivement réalisées, la première pour $n = 7, 23; \ldots$, la seconde pour $n = 3, 5, 11$.

Remarquons d'autre part que, pour n pair, la permutation $P_n^{(0)}$ ne change pas si on change x et y en $2n'+1-x$ et $2n'+1-y$; il y a symétrie par rapport à $n'+\frac{1}{2}$. C'est pour cela que la classe C_0 ne comprend que deux substitutions, et non quatre, comme la classe C_1, pour laquelle la symétrie par rapport à $\frac{n+1}{2}$ donne une substitution nouvelle. Donc la permutation $P_n^{(0)}$ ne peut comprendre que des cycles symétriques, ou bien des couples de deux cycles symétriques l'un de l'autre, sauf, si n est impair, le cycle réduit à l'élément 1, dont le symétrique est alors $2n' > n$. Ainsi, pour $n = 15$, $\sigma = 4$, et les 14 éléments autres que 1 se répartissent en deux cycles d'ordre 4, symétriques l'un de l'autre, et un cycle d'ordre 4 et un d'ordre 2 dont chacun est son propre symétrique.

13. *La classe C_2.* — Nous désignerons par P'_n celle des permutations d'ordre n et de la classe C_2 pour laquelle n est le transformé de 1, et l'autre par P''_n. En posant $n = 2n' + \delta$ ($\delta = 0$ ou 1), les équations qui définissent P'_n sont

$$(b') \quad y = n + 2 - 2x \qquad (x = 1, 2, \ldots, n' + \delta),$$

$$(b'') \quad y = 2n + 1 + \delta - 2x \qquad (n = n, n-1, \ldots, n' + \delta + 1).$$

Si n est impair, en changeant x et y en $n + 1 - x$ et $n + 1 - y$, on permute P'_n et P''_n. Si, au contraire, n est pair, chacune de ces permutations est invariante par cette opération, de sorte que la décomposition en cycles présente la symétrie déjà signalée pour $P_n^{(0)}$. Dans ce cas, les éléments 1 et n, se correspondant l'un à l'autre, constituent, pour P'_n, un cycle d'ordre 2. En faisant abstraction, et diminuant d'une unité les éléments restants 2, 3, ..., $n - 1$, on obtient la permutation P''_{n-2}. Donc, quelle que soit la parité de n, une réduction triviale nous ramène à l'étude des permutations P'_n (ou, si l'on préfère, à celle de P''_n).

Les équations de P'_n se ramènent à l'équation unique

$$(19) \qquad y + 2x \equiv 3 - \delta \qquad [\text{mod } (n + \delta - 1)]$$

qui définit y, à cela près que, dans le cas où $\delta = 0$, elle ne permet pas de distinguer les valeurs 1 et n de x et y; nous venons de voir que ces valeurs, qui pour $P^{(0)}_{2n'}$ étaient invariantes, s'échangent ici.

Les éléments invariants ne peuvent être que de l'une des formes

$$\frac{n.+2}{3}, \quad \frac{2n+\delta+1}{3}.$$

Si n est pair, $\delta = 0$, et ces deux valeurs sont entières si $n \equiv 1$ (mod 3), donc $n = 4$ (mod. 6). Si n est impair et multiple de 3, aucune des deux n'est entière; si enfin n est impair et $\equiv \pm 1$ (mod 3), donc aussi $\equiv \pm 1$ (mod 6), une seule de ces deux valeurs est entière.

De toute façon, l'équation (19) peut s'écrire

$$y - 1 + \frac{\delta}{3} + 2\left(x - 1 + \frac{\delta}{3}\right) \equiv 0,$$

et la condition pour que x appartienne à un cycle, primitif ou non, d'ordre σ, est

$$[(-2)^\sigma - 1]\left(x - 1 + \frac{\delta}{3}\right) \equiv 0, \tag{20}$$

le module étant toujours $n + \delta - 1$.

Si alors n est pair, $\delta = 0$, et l'ordre du cycle contenant 2 est le plus petit exposant pour lequel $(-2)^\sigma \equiv 1$ [mod $(n-1)$]. Pour cet ordre, l'équation (20) est vérifiée quel que soit x. Donc: *sauf peut-être le cycle d'ordre 2 constitué par les éléments 1 et n, tous les cycles de la substitution P'_n ont des ordres égaux à l'ordre σ du cycle qui contient 2, ou sous-multiples de σ.*

Donc: *pour n pair, le théorème fondamental s'applique à P'_n ou non, suivant que σ est pair ou impair.* Les deux cas sont effectivement possibles; en effet, pour $n = 4, 6, \ldots, 32$, les valeurs de σ sont

1, 4, 6, 3, 5, 12, 4, 8, 9, 6, 22, 20, 9, 28, 10.

Quand σ est impair, c'est 2σ, et non σ, qui est l'ordre de P'_n; sauf pour $n = 4$, cas où $\sigma = 1$, cet ordre n'est réalisé pour aucun des cycles. Il est d'ailleurs toujours inférieur à n, car, n étant pair, un cycle d'ordre impair n'est pas son propre symétrique, et il y a au moins deux cycles d'ordre σ et un cycle d'ordre 2; donc $n \geqq 2(\sigma + 1)$.

Pour la permutation P''_n, déduite (pour n pair) de P'_{n+2} par suppression des éléments 1 et $n + 2$, les éléments restants étant

diminués d'une unité, on obtient le résultat suivant: *σ étant l'ordre du cycle qui contient* 1 (ou de celui qui contient n), *tous les cycles sont d'ordres égaux à σ ou sous-multiples de σ.*

Supposons maintenant n impair et non multiple de 3. Qu'il s'agisse de P'_n ou de P''_n, il y a un élément invariant x_0, et l'équation qui exprime que le $\sigma^{\text{ième}}$ transformé de x est x s'écrit

$$[(-2)^\sigma - 1](x - x_0) \equiv 0 \pmod{n}. \tag{21}$$

L'ordre σ du cycle contenant $x_0 + 1$ (et de celui qui contient $x_0 - 1$) est alors le plus petit nombre σ tel que $(-2)^\sigma \equiv 1 \pmod{n}$, et, pour cette valeur de σ, l'équation (21) est vérifiée quel que soit x. Dans ce cas encore, le théorème fondamental est vérifié.

Supposons enfin n impair et multiple de 3, donc de la forme $3^h k$ ($h > 0$, k impair et non multiple de 3). L'équation (20) relative à P'_n s'écrit

$$\frac{(1-3)^\sigma - 1}{3}(3x - 2) \equiv 0 \pmod{n}. \tag{22}$$

Le premier facteur est entier. Cette condition se décompose en

$$(-2)^\sigma \equiv 1 \pmod{3^{h+1}} \tag{23}$$

$$\frac{(-2)^\sigma - 1}{3}(3x - 2) \equiv 0 \pmod{k}. \tag{24}$$

L'ordre du cycle auquel appartient le nombre 1 est alors le plus petit nombre σ tel que

$$\frac{(-2)^\sigma - 1}{3} \equiv 0 \pmod{n},$$

et, pour cette valeur de σ, l'équation (22) est vérifiée *quel que soit x.* Donc, finalement: *pour n impair, tous les ordres des cycles de P'_n sont, soit égaux à σ, soit sous-multiples de σ, σ étant, si n est multiple de* 3, *l'ordre du cycle qui contient* 1 *et n* (n étant le transformé de 1), *et, dans le cas contraire, celui du cycle qui contient $x_0 + 1$* (ou $x_0 - 1$).

Cet énoncé s'applique aussi à P''_n (c'est alors 1 qui est le transformé de n).

14. *Autres propriétés de P'_n et P''_n.* — Remarquons d'abord que la parité d'un type de cycle est ici définie par $\varepsilon = (-1)^\sigma$, sans qu'il y ait lieu de distinguer les deux opérations qui interviennent dans la définition de P'_n (ou de P''_n).

Supposons d'abord n pair; σ est le plus petit exposant pour lequel $2^\sigma - \varepsilon$ soit multiple de $n-1$. Donc, pour une valeur donnée de σ, la plus grande valeur possible de n est $2^\sigma + 1 - \varepsilon$, c'est-à-dire 2^σ si σ est pair et $2^\sigma + 2$ si σ est impair. Dans les deux cas, les cycles d'ordres égaux à σ ou sous-multiples de σ comprennent en tout 2^σ éléments.

Or, comme pour P_n, un type donné ne peut être réalisé qu'une fois, et il faut tous les types d'ordres égaux à σ ou sous-multiples de σ pour obtenir 2^σ éléments. Donc: *tous les types possibles, primitifs ou non, d'ordre σ, sont réalisés pour P'_n, si σ est pair, pour $n = 2^\sigma$, et si σ est impair, pour $n = 2^\sigma + 2$* (dans ce dernier cas, il y a en outre le cycle 1, n, du type $b'b''$).

La conséquence relative à P''_n est immédiate; *si σ est impair, tous les types, primitifs ou non, d'ordre σ, sont réalisés pour $n = 2^\sigma$; si σ est pair, ils le sont, sauf le type $b'b''$, pour $n = 2^\sigma - 2$.*

Supposons maintenant n impair et non multiple de 3; $2^\sigma - \varepsilon$ est toujours multiple de 3, et, d'après les résultats du n° 13, pour une valeur donnée de σ, la plus grande valeur possible de n est $\dfrac{2^\sigma - \varepsilon}{3}$ et, même en réunissant les cycles de P'_n et ceux de P''_n, on n'a en tout que $2n \leqq \frac{2}{3}(2^\sigma - \varepsilon)$ éléments. Il est donc impossible que, pour une même valeur impaire de n, tous les types de cycles d'ordre σ soient réalisés pour P'_n ou pour P''_n. On voit même aisément qu'il n'y a pas assez d'éléments pour que tous les types primitifs d'ordre σ soient réalisés.

Naturellement, le raisonnement précédent, et le résultat, supposent que $\sigma = \sigma(n)$ soit le nombre défini au n° 13. Mais, même pour un exposant $\sigma' < \sigma$, il est impossible que tous les types primitifs ou non d'ordre σ' soient réalisés à la fois pour P'_n, si n est impair; il y a en effet au plus un élément invariant, et les deux types b' et b'' ne peuvent pas être tous les deux réalisés.

Occupons-nous maintenant de l'ensemble e_σ des valeurs de n pour lesquelles P'_n (ou P''_n) contient un cycle d'ordre σ et de type donné. Les méthodes développées au chapitre I s'appliquent encore, à cela près qu'il faut toujours distinguer le cas où n est pair et celui où n est impair. Les formules ne sont pas les mêmes dans les deux cas, et e_σ comprend deux progressions arithmétiques différentes.

Considérons d'abord le cas où n est pair, donc $\delta = 0$. L'équation (19) est homogène en $x-1$, $y-1$, et $n-1$, ce dernier nombre étant nécessairement impair. Il en résulte que, si l'équation (19)

est vérifiée pour les valeurs x_0, y_0, n_0 de x, y, n (n_0 étant pair), elle l'est aussi pour les valeurs x_k, y_k, n_k définies par

$$\begin{aligned} x_k - 1 &= (2k+1)(x_0 - 1) \\ y_k - 1 &= (2k+1)(y_0 - 1) \\ n_k - 1 &= (2k+1)(n_0 - 1) \qquad (k = 0, 1, \ldots). \end{aligned}$$

Toute la théorie développée au Chapitre I subsiste alors, $2n - 1$ étant seulement remplacé par $n - 1$. Notamment: *si un type est naissant pour une valeur paire n_0 de n* (nous entendons par là qu'il n'est réalisé pour aucune valeur paire plus petite), *il est réalisé pour les valeurs*

$$n_k = n_0 + 2k(n_0 - 1)$$

et ne l'est pour aucune autre valeur paire.

Si n est impair, les équations de P'_n et celles de P''_n sont respectivement

$$\begin{aligned} y - \tfrac{2}{3} + 2(x - \tfrac{2}{3}) &\equiv 0 \pmod{n}, \\ y + \tfrac{2}{3} + 2(x + \tfrac{2}{3}) &\equiv 0 \pmod{n}. \end{aligned}$$

Le module étant encore impair, les multiplicateurs impairs $K = 2k + 1$ conviennent seuls, et on est conduit à poser, pour P'_n

$$x_k = x_0 + 2k(x_0 - \tfrac{2}{3}),$$

et, x_k devant être entier en même temps que x_0, il faut que k soit multiple de 3, donc que K soit de la forme $6k' + 1$.

D'autre part, si $k = 3k' - 1$, donc $K = 6k' - 1$, à des valeurs x_0, y_0 et n_0 vérifiant l'équation de P'_{n_0} correspondent par les formules

$$x'_k + \tfrac{2}{3} = (2k+1)(x_0 - \tfrac{2}{3}), \quad y'_k + \tfrac{2}{3} = (2k+1)(y_0 - \tfrac{2}{3})$$

des valeurs entières de x'_k et y'_k qui vérifient l'équation de P''_n pour $n = n_k$.

Donc, si un type est réalisé pour P'_n pour $n = n_0$, il est réalisé aussi

pour P'_n, pour $n_k = n_0 + 6k'(n_0 - 1)$
pour P''_n, pour $n_k = n_0 + 2(3k' - 1)(n_0 - 1)$, $(k' = 1, 2, \ldots)$.

Cet énoncé subsiste en échangeant P'_n et P''_n. Si alors on prend pour n_0 la plus petite valeur de n pour laquelle un type est réalisé soit pour P'_n soit pour P''_n, la formule précédente donne toutes les valeurs de n pour lesquelles il est réalisé, soit pour P'_n, soit pour P''_n. Le type symétrique, obtenu en échangeant les opérations b' et b'', est alors réalisé pour les mêmes valeurs de n, les rôles de P'_n et P''_n étant seulement intervertis.

Il semble inutile d'insister davantage sur ces questions. Le lecteur verra aisément que les considérations du Chapitre I relatives à l'ensemble des éléments appartenant, pour chaque n, à des cycles de types naissants se généralisent en grande partie, avec des modifications analogues à celles indiquées dans ce qui précède pour l'étude des ensembles e_σ; il faut toujours distinguer deux cas, suivant la parité de n.

15. *Remarque.* — En partant de P'_n, pour n pair, et en ne distinguant pas 1 et n, on obtient une permutation à $m = n - 1$ éléments définie par

$$y - 1 + 2(x - 1) \equiv 0 \pmod{m} \tag{25}$$

qui se rattache étroitement à la classe C_2, mais qui ne rentre pas dans notre définition initiale de cette classe, parce que, pour $x = 1, 2, \ldots, m$, $y + 2x - 3$ a successivement les trois valeurs 0, m et $2m$. Si donc on n'utilise pas les congruences, il faut trois formules et non deux, pour la définir. Naturellement, pour cette permutation, le théorème fondamental s'applique: l'ordre du cycle contenant 2 est multiple des ordres de tous les cycles.

On peut naturellement remplacer $x - 1$, $y - 1$ et 2 par $x - x_0$, $y - x_0$, $1 + x_0$.

Pour n impair, donc m pair, la permutation des nombres $1, 2, \ldots, m$ définie par la formule (25) est P''_m.

16. *Généralisations.* — Les permutations étudiées jusqu'ici sont des cas particuliers d'une classe plus générale de permutations définies de la manière suivante: on se donne un entier; soit r le reste de la division de n par q (donc $n = kq + r$). On répartit les nombres $1, 2, \ldots, n$ en q progressions arithmétiques correspondant aux valeurs $0, 1, 2, \ldots, q - 1$ du reste. On range ces q progressions dans un ordre quelconque, et, pour chacune d'elles, on range ses termes, soit dans l'ordre des grandeurs croissantes, soit dans l'ordre des grandeurs décroissantes. L'ordre ainsi obtenu est le résultat de la permutation qu'il s'agit d'étudier.

Pour des valeurs données de q et $n \geqq 2q$, on obtient ainsi une famille de $2^q q!$ permutations; si $q \leqq n < 2q$, la définition s'applique encore, mais le nombre des permutations n'est que $2^{n-q} q!$ [5]).

[5]) Les permutations considérées peuvent être réalisées de la manière suivante, avec un jeu de n cartes. On constitue q paquets en prenant les n cartes l'une après l'autre, et en les plaçant successivement sur les paquets. On prend ensuite ces paquets dans un ordre quelconque; à l'intérieur de chaque paquet, on peut, soit conserver l'ordre initial, soit prendre les cartes dans l'ordre inverse.

Cette famille est beaucoup trop générale pour qu'on puisse lui étendre notre théorème fondamental. Si en effet il s'appliquait, cela devrait être vrai en particulier pour $n = q$, et, comme dans ce cas il s'agit d'une permutation quelconque de q éléments, le théorème est forcément faux pour $n = q > 4$.

Je dois à Mademoiselle Sophie Piccard la remarque qu'il est déjà faux pour $q = 3$, et $n = 8$. En effet, la substitution

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 8 & 5 & 2 & 7 & 4 & 1 \end{pmatrix}$$

comprend un cycle d'ordre 3 (1, 3, 8) et un cycle d'ordre 5. Non seulement le théorème fondamental est en défaut, mais le p.p.c.m. de ces ordres est supérieur à n, ce qui n'avait pas lieu pour le cas d'exception déjà rencontré au n° 12.

Un autre exemple de Mademoiselle Piccard montre que, pour $q = 6$, $n = 14$, le p.p.c.m. en question peut atteindre la valeur 40; il peut donc déjà dépasser $2n$.

Ces remarques conduisent à ne considérer que des classes plus restreintes de permutations et notamment la classe de celles qui peuvent être définies par une formule de la forme

$$\varepsilon y \equiv qx + \lambda \pmod{m} \tag{26}$$

q étant premier avec m et ε désignant ± 1. Supposons d'abord ε indépendant de x, et $m = n$.

Il y a alors deux cas à distinguer, suivant qu'il existe un élément invariant x_0, ou non. Dans le premier cas, la formule (26) s'écrit

$$y - x_0 \equiv \varepsilon q(x - x_0) \pmod{n} \tag{27}$$

et la condition pour que x appartienne à un cycle, primitif ou non, d'ordre σ, est

$$(q^\sigma - \varepsilon^\sigma)(x - x_0) \equiv 0 \pmod{n} \tag{28}$$

Si elle est vérifiée pour $x = x_0 \pm 1$, elle l'est pour x quelconque; l'ordre de la permutation étudiée est donc celui du cycle (ou des cycles) contenant $x_0 - 1$ et $x_0 + 1$. Le théorème fondamental du chapitre I s'applique (2 étant remplacé par $x_0 + 1$).

Dans le second cas, celui où le p.g.c.d. de $q - \varepsilon$ et n ne divise pas λ, on peut encore écrire la formule (27), mais en prenant pour x_0 la valeur non entière $\dfrac{-\lambda}{q - \varepsilon}$, et la formule (28) prend la forme

$$\frac{q^\sigma - \varepsilon^\sigma}{q - \varepsilon}[(q - \varepsilon)x + \lambda] \equiv 0 \pmod{n} \tag{29}$$

Soit δ le p.g.c.d. de $q - \varepsilon$, λ, et n. Posons

$$q - \varepsilon = q'\delta, \quad \lambda = \lambda'\delta, \quad n = n'\delta.$$

L'équation (29) équivaut à

$$\frac{q^\sigma - \varepsilon^\sigma}{q - \varepsilon}(q'x + \lambda') \equiv 0 \pmod{n'}.$$

Si q' et λ' ne sont pas premiers entre eux, leur p.g.c.d., δ', est premier avec n', et, en posant $q' = \delta' q''$, $\lambda' = \delta'\lambda''$, la formule précédente s'écrit

$$\frac{q^\sigma - \varepsilon^\sigma}{q - \varepsilon}(q''x + \lambda'') \equiv 0 \pmod{n'}.$$

Comme q'' et λ'' sont premiers entre eux, on peut choisir $x_1 \leqq n' \leqq n$ de manière que $q''x_1 + \lambda''$ soit premier avec n'. Alors, si l'équation considérée est vérifiée pour x_1, elle l'est quel que soit x, ce qui prouve que le thorème fondamental s'applique encore (2 étant remplacé par x_1).

Comme dans le cas où $q = 2$, nous pouvons étudier, par les mêmes méthodes, les cas où $n = m \pm 1$.

L'hypothèse $n = m - 1$ implique évidemment que la valeur $m \equiv 0$ de x soit invariante par la formule (26), donc que $\lambda \equiv 0 \pmod{m}$; autrement, en effet, l'ensemble 1, 2, . . ., n ne serait pas invariant. Alors la permutation considérée se déduit de la précédente par la suppression d'un élément invariant, et le théorème fondamental s'applique.

L'hypothèse $n = m + 1$ implique que l'ensemble des éléments 1 et n soit invariant; ces deux valeurs de x doivent en effet se transformer en deux valeurs y_1 et y_2 de y, telles que $y_1 \equiv y_2$. Il faut donc que $\lambda \equiv 1 - q\varepsilon$. Dans ce cas, la formule (26) ne suffisant pas à définir la permutation, il faut convenir, soit que 1 et n sont invariants, soit que ces valeurs s'échangent. Dans le premier cas, le théorème fondamental s'applique encore; dans le second, on ajoute un cycle d'ordre deux à une permutation à laquelle le théorème fondamental s'applique; il ne s'applique donc que si la valeur σ relative à cette permutation auxiliaire est paire, ou (cas exceptionnel) égale à un.

Ces cas ne comprennent pas encore la généralisation de la permutation P_n étudiée au chapitre I. On peut la généraliser par la permutation définie par la formule

$$\varepsilon(y - 1) \equiv q(x - 1) \quad [\text{mod } (2n - 1)], \tag{30}$$

où la valeur de ε, égale à ± 1, peut dépendre de x, et où q est premier avec $2n - 1$. Cette formule définit parfaitement y dans tous les cas. Le théorème fondamental subsiste, sans changement.

On peut naturellement faire abstraction de l'élément invariant 1, puis remplacer 2, 3, . . ., n par 1, 2, . . ., $n - 1$; en désignant par $n' = n - 1$ le nombre des éléments, le module sera $2n' + 1$, et le théorème fondamental subsiste. Mais on ne peut pas remplacer $x - 1$ et $y - 1$ par $x - x_0$ et $y - y_0$ étant un entier quelconque; dans ce cas $y - y_0$ ne déterminerait pas y.

Remarquons enfin que l'équation

$$q'x - \varepsilon q''y + \lambda' \equiv 0 \pmod{n}, \tag{31}$$

où q'' est premier avec n, ne constitue qu'une généralisation apparente de l'équation (26). Elle se ramène en effet à la forme (26), où q et λ sont définis par les conditions $q' \equiv qq''$, $\lambda' \equiv \lambda q''$. Le théorème fondamental s'applique donc dans les mêmes conditions que pour l'équation (26). Il peut d'ailleurs être utile d'étudier l'équation (31) sans la réduire à la forme (26); ainsi, pour $q' = 2$, $q'' = 3$, q peut être arbitrairement grand, et l'équation (31), avec de faibles valeurs de q' et q'' peut être plus commode à étudier que l'équation (31) avec une grande valeur de q; pour $q' - \varepsilon q'' = \pm 1$, la forme (31) met en évidence l'existence certaine d'un élément invariant, quel que soit λ', et la réduction à la forme (26) ne peut pas mettre ce fait plus en évidence.

Chapitre III — *La permutation* Q_n.

17. *Définition de* Q_n. — Considérons un jeu de n cartes, rangées initialement dans un certain ordre, la première étant sur le dessus du jeu. Plaçons la première sur la table, la seconde sous le jeu, la suivante sur la table, la suivante sous le jeu, et ainsi de suite, en alternant les deux gestes, jusqu'à ce que le jeu soit réduit à une carte, que nous placerons sur la table à la suite des autres. Le passage de l'ordre initial à l'ordre final est l'opération Q_n [6]).

[6]) Il peut être utile de préciser le point suivant: les *cartes* et les *cases* où elles sont placées étant numérotées, et chaque carte étant initialement dans la case de même numéro, la carte $y = f(x)$ est finalement dans la case x. L'ordre final des cartes étant $f(1), f(2), \ldots, f(n,)$ la substitution ainsi définie est celle qui fait passer de x à y. Si on observe une case déterminée, elle fait passer de la carte qui y était initialement à celle qui est finalement. Si au contraire on observe une carte déterminée, la substitution fait passer de son rang final à son rang initial.

L'opération inverse Q_n^{-1} peut être réalisée de la manière suivante: préparons n cases, numérotées 1, 2, . . ., n, et disposées circulairement, de manière que la case n soit suivie par la case 1. Plaçons successivement les cartes dans les cases 1, 3, 5, et ainsi de suite, en tournant toujours dans le même sens et en passant chaque fois une case vide. Aux tours suivant le premier, nous ne tiendrons bien entendu compte que des cases non encore occupées. Au $k^{\text{ième}}$ tour, les numéros des cases successivement remplies, et ceux des cases laissées encore vides, formeront ainsi deux progressions arithmétiques de raison 2^k.

Dans ces conditions, entre la carte x (c'est-à-dire celle de rang initial x) et la carte $x + 1$, pourvu que $x + 1 < n$, il y aura toujours une place laissée vide au moment où on place la carte $x + 1$, et qui, finalement, sera occupée par une carte de numéro plus élevé. C'est là une propriété de l'ordre final qui reste invariante aussi bien par une permutation circulaire que par l'enlèvement successif des cartes 1, 2, . . . Il en résulte que si, après avoir ramassé les cartes dans l'ordre où elles se trouvent, en commençant par celle qui occupe la case 1, on effectue l'opération Q_n, on retrouve bien l'ordre initial: après avoir placé la carte x sur la table, on place sous le jeu la carte de numéro plus élevé qui la séparait de la carte $x + 1$, qui se présente ensuite pour être placée à son tour sur la table.

Le tableau ci-dessous indique le résultat de cette opération pour $n = 17$; les valeurs de x sont inscrites au-dessous des valeurs 1, 2, . . ., 17 de $y = Q_{17}x$. Les lettres α, β, γ inscrites dans la troisième ligne indiquent les cycles mis en évidence par ce tableau.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	17	2	10	3	14	4	11	5	16	6	12	7	15	8	13	9
	α	α	β	α	γ	β	γ	α	β	γ		β	γ	γ	β	α

On voit que, indépendamment des éléments invariants 1 et 12, il y a trois cycles d'ordre 5.

Pour n quelconque, Q_n peut être défini par une succession de formules

$$(a_k) \qquad y = 2^k(x - x_k) + c_k$$

correspondant aux différents tours considérés dans la définition de Q_n^{-1}, et dont la première coïncide avec la formule (a) du chapitre I. La formule (a_k) s'applique pour la valeur x_k de x, et donne pour y la valeur c_k.

Nous verrons au n° 20 que, d'une manière plus précise, la

relation entre x et y peut s'écrire

$$2n - y = 2^{k-1}(2n - 2x + 1). \tag{32}$$

$2n - 2x + 1$ est donc le plus grand diviseur impair de $2n - y$, ce qui définit x quand y est donné. Quand inversement x est donné, la formule (32) et la condition $0 < y \leqq n$ déterminent y.

Il faut remarquer que, q désignant le nombre entier défini par $2^{q-1} < n \leqq 2^q$, la formule a_{q+1} s'applique toujours, et donne $y = 2n - 2^q$ qui est le transformé de $x = n$. Si alors $n > 3.2^{q-2}$, la formule a_q s'applique, et donne le transformé $2n - 3.2^{q-1}$ de $n - 1$; dans le cas contraire, c'est la formule a_{q-1} qui donne le transformé de $n - 1$, égal dans ce cas à $2n - 3.2^{q-2}$.

18. *Enoncés des principaux résultats.* — Nous donnons en annexe un tableau (tableau II) indiquant la décomposition en cycles de Q_n, pour les valeurs 3, 4, 5, . . ., 45 de n, et pour quelques valeurs plus grandes. A la suite de chaque formule, la valeur de $\sigma = \Omega(n)$, ordre de Q_n, est indiquée entre parenthèses (nous conserverons la notation $\omega(n)$ pour désigner l'ordre de P_n).

Pour les valeurs quelconques de n, aucune loi générale ne se dégage de ce tableau. La fonction $\Omega(n)$ est une fonction arithmétique très irrégulière. Ainsi on a

$$\Omega(127) = 52.780, \quad \Omega(128) = 420, \quad \Omega(129) = 8.$$

Il ne semble exister aucune règle simple en relation avec la décomposition de n en facteurs premiers. On pourrait penser qu'il y en a une en relation avec la représentation dyadique de n; il n'en est ainsi que dans les cas où n est de la forme $2^q + \delta$ ($\delta = 0$ ou 1); même pour les valeurs -1 ou 2 de δ, il n'existe aucune règle simple.

Les règles que nous avons ainsi d'abord découvertes empiriquement, et qui seront démontrées aux n^{os} 17 à 19, sont les suivantes:

A. — Pour $n = 2^q$, les ordres des cycles sont 1, 2, . . ., q. La fonction $\Omega(n)$ est donc le p.p.c.m. des nombres 1, 2, . . ., q, de sorte que $\dfrac{\Omega(2^q)}{\Omega(2^{q-1})}$ est égal à p si q est une puissance d'un nombre premier p, et à 1 dans le cas contraire.

B. — Pour $n = 2^q + 1$, les cycles de Q_n sont exactement ceux de P_n; donc $\Omega(n) = q + 1$, et tous les cycles sont d'ordres égaux à $q + 1$ ou sous-multiples de $q + 1$.

Précisons bien que, par l'énoncé précédent, nous ne voulons pas seulement dire qu'on a la même formule de décomposition

que pour P_n, mais que les cycles sont exactement les mêmes. Naturellement, à l'intérieur de chaque cycle, l'ordre des éléments n'est pas en général le même.

D'ailleurs les séquences formées à l'aide de la seule opération a sont les mêmes pour P_n et pour Q_n; aussi: si un cycle de P_n ne comprend qu'une ou deux opérations b, il se retrouve dans P_n exactement avec le même ordre. Mais l'ordre peut changer s'il y a au moins trois opérations b (donc trois séquences comprenant chacune un ou plusieurs termes) et il semble qu'il change toujours effectivement.

Ainsi, pour $n=17$, le cycle 2, 3, 5, 9, 17 est exactement le même, avec le même ordre, pour P_n et pour Q_n. Mais pour les deux autres cycles, on a les ordres

4, 7, 13; 10; 16; et 6,11; 14; 8,15; pour P_n,
4, 7, 13; 16; 10; et 6,11; 8 ; 15,14; pour Q_n.

Dans le cas général, nous avons récemment obtenu les résultats suivants, qui seront démontrés et complétés au n° 20.

C. — Nous désignerons par E_1 l'ensemble des entiers positifs n pour lesquels $p = 2n - 1$ admet un multiple de la forme $2^\sigma + 1$, et par E_0 l'ensemble complémentaire.

Si $n \in E_0$, tous les cycles de Q_n sont d'ordres inférieurs à l'ordre $\varphi(n)$ de P_n. Mais, sauf de rares exceptions (4 et 11 sont sans doute les seules), il n'existe pas de cycle d'ordre $\Omega(n)$, et $\Omega(n)$ est supérieur, non seulement à l'ordre du plus grand cycle, mais à $\omega(n)$, et même, le plus souvent, à n (comme exceptions à cette dernière règle, indépendamment de 4 et 11, citons 16, 39 et 64).

Si $n \in E_1$, les cycles de Q_n sont exactement ceux de P_n. Donc $\Omega(n) = \omega(n)$. La valeur commune de ces deux ordres est le plus petit nombre σ tel que $2^\sigma + 1$ soit multiple de p.

19. — *Premières remarques sur les cas où* $n = 2^q + \delta$ ($\delta = 0$ ou 1). —

1°) Dans le cas où $n = 2^q$, la formule a_k relative à un indice k donné est valable pour

$$n - 2^{q+1-k} < x \leqq n - 2^{q-k},$$

et prend la forme

$$y = 2^k(x - n + 2^{q+1-k}) - 2^{k-1}, \tag{33}$$

de sorte que les valeurs de y ainsi obtenues sont les multiples impairs de 2^{k-1}. Il en est bien ainsi pour $k = 1$. On voit alors par récurrence qu'il en sera ainsi pour toutes les valeurs de k.

Si en effet il en est ainsi pour 1, 2, . . ., k, les cases dont les rangs sont multiples de 2^k seront restées vides jusqu'au $(k+1)^{\text{ième}}$ tour. Comme on aura terminé le $k^{\text{ième}}$ tour en passant la case vide de rang 2^q, il faudra au $(k+1)^{\text{ième}}$ tour remplir les cases vides de deux en deux, en commençant par la première; on remplira ainsi les cases dont les rangs sont les multiples impairs de 2^k. La formule (33) reste donc valable pour l'indice $k+1$.

Il en est ainsi jusqu'au $q^{\text{ième}}$ tour, qui donne $y = 2^{q-1}$ pour $x = n-1$. Enfin la seule valeur restante, $y = n$, correspond à $x = n$.

Il y a ainsi toujours les deux éléments invariants 1 et n. Nous verrons qu'il peut y en avoir d'autres.

2°) Dans le cas où $n = 2^q + 1$, la formule a_1 s'applique pour $x = 1, 2, \ldots, 2^{q-1}+1$, et donne pour y les valeurs 1, 3, . . ., n. A chacun des tours suivants, jusqu'à celui de rang q, le nombre des valeurs de x à considérer sera 2^{q-k}, et, à l'inverse de ce qui a lieu pour $n = 2^q$, il faudra laisser vide la première case vide, et remplir celles de rangs pairs. La case $y = 2$ sera donc toujours laissée vide, et sera finalement occupée par la carte $x = n$.

Ce résultat s'exprime par la règle suivante: la formule a_k $(k = 2, 3, \ldots, q)$ est valable pour

$$n - 2^{q+1-k} < x \leqq n - 2^{q-k}$$

et s'écrit

$$y = 2^k(x - n + 2^{q+1-k}) - 2^{k-1} + 2. \tag{34}$$

3°) Dans ce cas, le cycle qui contient 2 est constitué par la séquence

$$2, 3, 5, 9, \ldots, 2^q + 1 = n;$$

d'après ce qui précède, le transformé de n est 2. On a donc un cycle d'ordre $q+1$, exactement le même que pour P_n.

Au contraire, pour $n = 2^q$, le cycle qui contient 2 est

$$2, 3, 5, \ldots, \frac{n}{2} + 1,$$

et $\frac{n}{2} + 1$, étant la première valeur de x du second tour (celui qui correspond à $k = 2$), a pour transformé 2. Le résultat n'est donc pas le même que pour P_n; le cycle considéré est d'ordre q, et non $q+1$.

On peut étudier de la même manière le cycle contenant n'importe quel nombre donné x. Pour permettre la comparaison

avec P_n, considérons encore, comme au n° 7, le cas où $x = 14$. Le cycle qui contient 14 comprend d'abord, comme pour P_n, la séquence

$$(35) \qquad 14 = 13 + 1,\ 26 + 1,\ 52 + 1,\ \ldots,\ 13 \cdot 2^{q-4} + 1.$$

Ensuite, si $n = 2^q + 1$, on trouve

$$(36) \qquad \tfrac{1}{2}2^q - 2,\ 2^q - 5;\ \tfrac{3}{8}2^q + 2,\ \tfrac{3}{4}2^q + 3,$$

et on revient à 14 (les formules utilisées successivement étant a_3, a, a_{q-2}, a, a_3). On obtient bien ainsi, conformément à l'énoncé B du n° 16, le même cycle que pour P_n; mais l'ordre des deux dernières séquences est changé.

Supposons maintenant $n = 2^q$. Après la séquence (35), on trouve $\frac{1}{2}2^q + 4$, et on revient à 14 (les opérations effectuées étant successivement a_3 et a_2). Conformément à l'énoncé A, on obtient ainsi un cycle d'ordre $q - 2 < q + 1$.

Il faut remarquer que les ordres $q + 1$ ou $q - 2$ ainsi obtenus sont nécessairement des ordres réels s'ils sont premiers, et aussi dans le cas où q est assez grand. En effet, l'hypothèse contraire implique une périodicité, qui est exclue à partir du moment où la séquence initiale comprend plus de termes que les autres. Mais, pour $q = 5$ et $\delta = 1$ (donc $n = 33$), le cycle constitué par les suites (35) et (36) se réduit au cycle (14, 27) répété 3 fois.

Ces remarques s'étendent au cas d'un élément initial x quelconque, et il ne serait pas impossible d'arriver de cette manière à la démonstration complète des énoncés A et B. Mais nous arriverons plus simplement au résultat par une autre méthode, qui utilise la représentation dyadique du nombre $x - 1 - \delta$.

20. *Etude du cas où $n = 2^q$.* — Dans ce cas, nous représenterons $x - 1$ par la formule

$$x - 1 = 2^{q-1}\delta_1 + 2^{q-2}\delta_2 + \ldots + 2\delta_{q-1} + \delta_q,$$

tous les δ_k étant égaux à 0 ou 1, et nous désignerons par

$$(37) \qquad S = (\delta_1, \delta_2, \ldots, \delta_q) = 1^\alpha \cdot 0^{\alpha'} \cdot 1^\beta \cdot 0^{\beta'} \ldots 1^\lambda \cdot 0^{\lambda'-1}$$

la suite des coefficients δ_k qui correspond ainsi à x; 1^μ et 0^μ représentent respectivement une suite de μ chiffres égaux à 1, et une suite de μ zéros. Les exposants α et $\lambda' - 1$ sont des entiers positifs ou nuls; les autres exposants sont positifs.

Si $\alpha = 0$, $x \leqq 2^{q-1}$, et la formule à appliquer est a_1. D'une manière générale, chacune des formules a_k, qui ont ici la forme

(33), s'applique à 2^{n-k} valeurs consécutives de x, celles obtenus en prenant $\alpha = k - 1$, et les chiffres de la suite S qui suivent les k premiers indiquent le rang

$$1 + 2^{q-k-1}\,\delta_{k+1} + \ldots + 2\delta_{q-1} + \delta_q$$

de x dans la suite des nombres auxquels cette formule s'applique. Elle donne alors

$$y - 1 = 2^{q-1}\delta_{k+1} + 2^{q-2}\,\delta_{k+2} + \ldots + 2^k\delta_q + 2^{k-1} - 1,$$

c'est-à-dire (puisque $k = \alpha + 1$) que l'opération Q_n équivaut à une substitution T qui transforme la suite S en

$$TS = 0^{\alpha'-1} \cdot 1^{\beta} \cdot 0^{\beta'-1} \ldots 1^{\lambda} \cdot 0^{\lambda'} \cdot 1^{\alpha} \quad [7]). \tag{38}$$

On remarque que, si $\alpha = 0$, donc $y - 1 = 2$ $(x - 1)$, cette formule indique bien qu'il faut enlever un zéro au commencement de la suite S et le mettre à la fin. Donc $\alpha' - 1$ nouvelles applications de cette règle donnent

$$T^{\alpha'}S = 1^{\beta} \cdot 0^{\beta'} \cdot 1^{\gamma} \ldots 1^{\lambda} \cdot 0^{\lambda'} \cdot 1^{\alpha} \cdot 0^{\alpha'-1}. \tag{39}$$

Le résultat de α' opérations T est donc une permutation circulaire des groupes (α, α'), (β, β'), . . ., (λ, λ'). Donc, en posant

$$\alpha' + \beta' + \ldots + \lambda' = \sigma', \tag{40}$$

c'est-à-dire en désignant par $\sigma' - 1$ le nombre des zéros, on a

$$T^{\sigma'}S = S. \tag{41}$$

L'ordre du cycle de la substitution T qui contient S, c'est-à-dire l'ordre du cycle de Q_n qui contient x, est donc égal à σ' ou sous-multiple de ce nombre.

Les valeurs possibles de σ' sont 1, 2, . . ., $q + 1$. Mais $\sigma' = q+1$ implique $S = 0^q$, $x = 1$; dans ce cas, le cycle considéré se réduit à un élément invariant. Les ordres possibles des cycles sont donc 1, 2, . . ., q.

Nous avons déjà vu que le cycle qui contient l'élément $x = 2$ est d'ordre réel q. Il est d'ailleurs évident que toutes les autres valeurs possibles de σ' sont effectivement des ordres réels pos-

---

[7]) On peut hésiter sur la signification de cette formule dans le cas où $S = 1^q$. Nous savons que l'élément $x = n$ auquel correspond cette suite est invariant dans Q_n. Donc $T\,1^q = 1^q$. C'est bien ce que donne la formule du texte, en observant que $\alpha' = \gamma' - 1 = 0$. Le facteur $0^{\alpha'-1}$ est alors dépourvu de signification; mais il faut considérer que les facteurs $0^{\alpha'-1} = 0^{-1}$ et $0^{\lambda'} = 0^1$ se détruisent, et il reste bien $TS = 1^q$.

sibles. Pour que l'ordre réel soit réduit, c'est-à-dire soit sous-multiple de σ', il est en effet, d'après la formule (38), nécessaire et suffisant que la suite α, α', β, β', ..., λ, λ' soit de la forme A^{μ}, A comprenant un nombre pair de termes, et μ étant > 1. C'est une circonstance évidemment exceptionelle. Ces cas de réduction de l'ordre sont d'ailleurs analogues à ceux que nous avons étudiés au n° 6 pour les types de cycles d'ordre σ. Il n'y a pas identité entre les deux problèmes, parce qu'à cet endroit la permutation circulaire portait sur tous les éléments, de sorte qu'un même type avait σ représentations, en général distinctes. Ici les chiffres 1 et 0 ne jouent pas le même rôle; il y a toujours un zéro, accompagné ou non d'un groupe 1^{α}, qui passe de gauche à droite dans l'opération T, et le nombre de termes du cycle est σ' (c'est-à-dire le nombre des zéros, augmenté d'une unité), et non le nombre total q des termes de la suite S. Malgré cette différence, on peut, comme au Chapitre I, conclure que parmi les $n = 2^q$ suites S possibles, le nombre de celles qui appartiennent à des cycles d'ordres réduits est $O(\sqrt{n})$.

On en déduit d'abord que les valeurs possibles 1, 2, ..., q sont toutes réalisées pour les ordres réels. La fonction $\sigma = \Omega(n)$ est donc le p.p.c.m. des q premiers nombres entiers, ce qui termine la démonstration de l'énoncé A du n° 16.

D'autre part, le coefficient du binôme $N' = C_q^{\sigma'-1}$, qui est le nombre des suites S ayant q termes dont $\sigma' - 1$ zéros, donne (sauf pour $\sigma' = q + 1$) une valeur approchée du nombre N de celles qui appartiennent à des cycles d'ordre σ'. Il en donne évidemment une borne supérieure si $2\sigma' > q$ (puisque dans ce cas il n'est pas possible que le nombre des zéros soit $k\sigma' - 1$, sauf si $k = 2$, $2\sigma' - 1 = q$, cas où l'ordre réel est 1). Au contraire, si σ' est premier, $N' - 1$ borne supérieurement N (car dans ce cas il y a au plus un élément appartenant à un cycle d'ordre sous-multiple de σ', c'est-à-dire un élément invariant).

Ainsi, pour $q = 7$, les valeurs de N et N' sont données par le tableau suivant

σ'	8	7	6	5	4	3	2	1
N'	1	7	21	35	35	21	7	1
N	0	7	18	35	32	24	8	4

Pour $\sigma' = 4, 5, 6, 7$, on a bien $N \leqq N'$. On remarque que N,

nécessairement multiple de σ', est en fait le plus grand multiple de σ' qui soit $\leqq N'$. Mais cette circonstance cesse d'être vérifiée pour des valeurs plus grandes de q. Pour $\sigma' = 5$ et 7, $N = N'$. Pour les valeurs 4 et 6 de σ', il y a des restes $N' - N$, tous les deux égaux à 3. L'ordre réel devant, pour ces restes, être sous-multiple de σ', on voit que le reste correspondant à $\sigma' = 6$ donne nécessairement un cycle d'ordre 3, le huitième; celui qui correspond à $\sigma' = 4$ donne un cycle d'ordre 2, le quatrième, et un élément invariant $S = (1 \,.\, 0)^3 \,.\, 1$, donc $x = 86$. Pour $\sigma' = 2$, on a à la fois un élément invariant ($S = 1^3 \,.\, 0 \,.\, 1^3$, donc $x = 120$), et un cycle provenant d'un reste antérieur (formé des suites $1^2 \,.\, 0^2 \,.\, 1^2 \,.\, 0$ et $0 \,.\, 1^2 \,.\, 0^2 \,.\, 1^2$, c'est-à-dire des valeurs 52 et 103 de x). Les quatre éléments invariants sont donc 1, 86, 120, 128 [8]).

21. *Le cas* $n = 2^q + 1$.

1° — Dans ce cas, en laissant de côté l'élément invariant 1, on peut représenter $x - 2$ (et non $x - 1$) par une suite S. Changeant en outre légèrement la forme adoptée pour S, nous poserons

$$x - 2 = 2^{q-1}\delta_1 + 2^{q-2}\delta_2 + \ldots + 2\delta_{q-1} + \delta^q, \tag{42}$$

$$S = (\delta_1, \delta_2, \ldots, \delta_q) = 1^\alpha \,.\, 0^{\alpha'} \,.\, 1^\beta \,.\, 0^{\beta'} \ldots 1^\lambda \,.\, 0^{\lambda'}, \tag{43}$$

α et λ' étant positifs ou nuls; tous les autres exposants sont positifs.

La formule de transformation à appliquer est ici la formule (34), l'indice k ayant encore la valeur $k + 1$. Un calcul analogue à celui qui nous a conduit à la formule (38) donne ici, pour la suite $S' = TS$ qui représente $y - 2$

$$TS = 0^{\alpha'-1} \,.\, 1^\beta \,.\, 0^{\beta'} \ldots 1^\lambda \,.\, 0^{\lambda'} \,.\, 1 \,.\, 0^\alpha, \tag{44}$$

formule qui est seulement en défaut pour la suite $S = 1^q$ dont la transformée est 0^q. Les valeurs correspondantes de x sont n et 2, et nous savons déjà qu'elles appartiennent à un cycle d'ordre réel $q + 1$.

De la formule (44), on déduit aisément le théorème fondamental, identique à celui relatif à P_n, mais seulement valable ici pour des valeurs particulières de n: *pour* $n = 2^q + 1$, *le cycle de* 2 *est*

---

[8]) D'une manière générale, si $q = 2r - 1$, la suite $(1.0)^{r-1}$ est invariante. L'élément $x = \dfrac{2(n+1)}{3}$ est donc invariant. On obtient un résultat analogue chaque fois que q est de la forme $kr - 1$; aux valeurs de k données par cette formule, correspond toujours une suite invariante $(1^{k-1} \,.\, 0)^{r-1} \,.\, 1^{k-1}$ pour laquelle $\sigma' = r$, l'ordre réel étant 1.

d'ordre $q+1$; *les ordres de tous les autres cycles sont égaux à* $q+1$ *ou sous-multiples de* $q+1$. *Donc* $\Omega(n) = q+1$.

La formule (44), dans le cas où $\alpha = 0$, indique que, pour passer de S à TS, il faut remplacer un zéro à gauche par un 1 à droite. Son itération donne donc

$$T^{\alpha'}S = 1^{\beta} \cdot 0^{\beta'} \cdot 1^{\gamma} \ldots 1^{\lambda} \cdot 0^{\lambda'} \cdot 1 \cdot 0^{\alpha} \cdot 1^{\alpha'-1}, \tag{45}$$

$$T^{\alpha'+\beta'}S = 1^{\gamma} \cdot 0^{\gamma'} \ldots 1^{\lambda} \cdot 0^{\lambda'} \cdot 1 \cdot 0^{\alpha} \cdot 1^{\alpha'} \cdot 0^{\beta} \cdot 1^{\beta'-1},$$

et ainsi de suite, jusqu'à

$$T^{s'}S = 1 \cdot 0^{\alpha} \cdot 1^{\alpha'} \cdot 0^{\beta} \cdot 1^{\beta'} \ldots 0^{\lambda} \cdot 1^{\lambda'-1} \tag{46}$$

(nous posons $\alpha' + \beta' + \ldots + \lambda' = s'$, $\alpha + \beta + \ldots + \lambda = s$, donc $s + s' = q$). Il vient ensuite

$$T^{s'+\alpha}S = 1^{\alpha'} \cdot 0^{\beta} \cdot 1^{\beta'} \ldots 0^{\lambda} \cdot 1^{\lambda'} \cdot 0 \cdot 1^{\alpha-1}$$

$$T^{s'+\alpha+\beta}S = 1^{\beta'} \cdot 0^{\gamma} \ldots 0^{\lambda} \cdot 1^{\lambda'} \cdot 0 \cdot 1^{\alpha} \cdot 0^{\alpha'} \cdot 1^{\beta-1},$$

et ainsi de suite, jusqu'à

$$T^{q}S = 1^{\lambda'} \cdot 0 \cdot 1^{\alpha} \cdot 0^{\alpha'} \cdot 1^{\beta} \cdot 0^{\beta'} \ldots 1^{\lambda-1}$$

et enfin

$$T^{q+1}S = 1^{\alpha} \cdot 0^{\alpha'} \cdot 1^{\beta} \cdot 0^{\beta'} \ldots 1^{\lambda} \cdot 0^{\lambda'} = S, \tag{47}$$

ce qui démontre le théorème énoncé.

2°. *Relation entre* P_n *et* Q_n (toujours pour $n = 2^q + 1$). — Pour mettre cette relation en évidence, il faut d'abord transformer P_n en une substitution U opérant sur S. En posant $x - 2 = \xi$, $y - 2 = \eta$, les équations de P_n, pour $n = 2^q + 1$, deviennent

$$\eta = \begin{cases} 2\xi + 1 & (\xi < 2^{q-1}) \\ 2(2^n - 1 - \xi) & (\xi \geqq 2^{q-1}), \end{cases}$$

ce qui conduit pour U aux formules

$$US = \begin{cases} 0^{\alpha'-1} \cdot 1^{\beta} \cdot 0^{\beta'} \ldots 1^{\lambda} \cdot 0^{\lambda'} \cdot 1 & (\alpha = 0) \\ 0^{\alpha-1} \cdot 1^{\alpha'} \cdot 0^{\beta} \cdot 1^{\beta'} \ldots 0^{\lambda} \cdot 1^{\lambda'} \cdot 0 & (\alpha > 0). \end{cases} \tag{48}$$

On a alors

$$U^{\alpha}S = 1^{\alpha'} \cdot 0^{\beta} \cdot 1^{\beta'} \ldots 0^{\lambda} \cdot 1^{\lambda'} \cdot 0 \cdot 1^{\alpha-1} \qquad (\alpha > 0),$$

et, comme $\alpha' > 0$, une nouvelle application de la formule (48) donne en tout cas

$$U^{\alpha+1}S = 0^{\alpha'-1} \cdot 1^{\beta} \cdot 0^{\beta'} \ldots 1^{\lambda} \cdot 0^{\lambda'} \cdot 1 \cdot 0^{\alpha},$$

c'est-à-dire, compte tenu de (44),

$$U^{\alpha+1}S = TS. \tag{49}$$

D'autre part, on déduit de (46)

$$T^{s'+1}S = 0^{\alpha-1} \cdot 1^{\alpha'} \cdot 0^{\beta} \cdot 1^{\beta'} \ldots 0^{\lambda} \cdot 1^{\lambda'} \cdot 0 \qquad (\alpha > 0),$$

c'est-à-dire

$$T^{s'+1}S = US \qquad (\alpha > 0), \tag{50}$$

tandis que, pour $\alpha = 0$, on a évidemment

$$TS = US \qquad (\alpha = 0). \tag{51}$$

D'après les formules (49) et (51), on obtient TS en effectuant $\alpha + 1$ fois l'opération U; on obtient US, suivant que α est nul ou positif, en considérant l'opération TU elle-même ou sa $(s'+1)^{\text{ième}}$ puissance.

Il faut remarquer que les exposants varient avec la suite considérée. On ne peut, ni identifier d'une manière générale T à une puissance déterminée de U, ni identifier U à une puissance de T. Cela n'empêche pas de conclure que, pour chaque suite S, l'ensemble des $T^{\nu}S$ $(\nu = 0, 1, \ldots, q)$ coïncide avec l'ensemble des $U^{\nu}S$.

Donc, si nous revenons à P_n et Q_n: *le cycle contenant un élément donné x est le même pour P_n et pour Q_n.* L'ordre seul de la permutation circulaire effectuée entre les éléments du cycle peut varier.

D'ailleurs, l'opération a (ou a_1) est la même pour P_n et pour Q_n. Les séquences sont donc les mêmes; mais, si un cycle comprend plus de deux séquences, la permutation circulaire effectuée sur ces séquences ne sera en général pas la même pour P_n et pour Q_n (il le faut bien, puisque, pour $n > 3$, les opérations P_n et Q_n sont différentes).

La démonstration de l'énoncé A du n° 16 est ainsi terminée. Il en résulte évidemment que les résultats du Chapitre I, dans la mesure où l'ordre des éléments d'un cycle ne jouent pas un rôle essentiel, s'appliquent à Q_n aussi bien qu'à P_n. Ainsi la parité d'un cycle étant la parité du nombre de ses éléments pairs, les énoncés relatifs à la parité des cycles subsistent sans changement, c'est-à-dire que, puisqu'il ne s'agit ici que du cas où $n = 2^q + 1$: les cycles de Q_n sont tous de types impairs, et, si leur ordre est sous-multiple de $q + 1$, le rapport $\frac{q+1}{\sigma}$ est impair; il n'y a exception que pour le cycle constitué par l'élément invarient 1.

22. *Etude du cas général.* — 1°. Il nous faut d'abord revenir sur la formule (32), indiquée sans démonstration au n° 15. Désignons à cet effet par z un nombre impair, positif et $< n$, à cela près quelconque. Posons

$$z_\nu = 2^\nu z \qquad (\nu = 0,\ 1,\ 2,\ \ldots).$$

Parmi les nombres z_ν, il y en a un et un seul qui soit à la fois $\geqq n$ et $< 2n$; nous le désignerons par $2n - y$, et poserons

$$2n - y = 2^{k-1} z. \tag{52}$$

Comme inversement, si y est donné, z est bien défini comme étant le plus grand diviseur impair de $2n - y$, la relation ainsi établie entre y et z est biunivoque, et k est une fonction bien déterminée de y aussi bien que de z.

Considérons maintenant $2n$ cases, préparées pour recevoir des cartes, et considérons toutes celles de rangs $2n - 2^\nu z$ (z fixe, $\nu = k - 1,\ k - 2,\ \ldots,\ 1,\ 0$) comme des images successives de la première, celle dont le rang est y. Plaçons successivement les cartes $x = 1,\ 2,\ \ldots,\ n$, dans les cases de rangs $y \leqq n$ ayant pour images celles de rangs $2n - z = 1,\ 3,\ \ldots,\ 2n - 1$. Cela revient à établir entre x et z la relation

$$2n - z = 2x - 1, \tag{53}$$

donc entre x et y la relation annoncée

$$2n - y = 2^k(n - x) + 2^{k-1}. \tag{32}$$

Désignons par Q'_n la permutation ainsi obtenue (les cartes se trouvant rangées dans l'ordre des y croissants). Il s'agit de montrer qu'elle coïncide avec Q_n^{-1}, c'est-à-dire qu'en effectuant l'opération Q_n définie au n° 15, on retrouve l'ordre initial.

Or, pour effectuer l'opération Q_n, on enlève d'abord la carte $x = 1$ placée dans la case $y = 1$, et on déplace la carte suivante, située dans la case $y = 2$, pour la mettre à la suite du jeu dans la case de rang $n + 1$, qui est la première image de la case $y = 2$. En répétant alternativement ces deux gestes, on enlèvera ainsi successivement les cartes $x = 1,\ 2,\ 3,\ \ldots$, trouvées aux cases $y = 1,\ 3,\ 5,\ \ldots$, tandis que les cartes trouvées dans les cases de rangs pairs seront transportées de ces cases à leurs images. Chacune de ces cartes sera ainsi déplacée une ou plusieurs fois, jusqu'à ce qu'elle arrive à la case de rang impair $2n - z$, dernière image de la case initiale y. Elle sera donc bien la $x^{\text{ième}}$ carte

enlevée, x étant défini par la formule (53), étant donc le numéro inscrit sur cette carte, c.q.f.d.

Si l'on préfère, on peut raisonner par récurrence. Les deux premiers gestes amènent les cartes 2, 3, ..., n à un ordre qui est celui résultant de l'opération Q'_{n-1} effectuée en partant de leur ordre naturel. Si donc Q'_{n-1} est bien l'opération inverse de Q_{n-1}, la suite de l'opération Q_n, qui coïncide évidemment avec l'opération Q_{n-1}, ramène ces cartes à l'ordre naturel, c.q.f.d.

2°. La formule (32), étant homogène en $2n-1$, $x-1$ et $y-1$, toutes les conséquences de cette circonstance qui ont été développées au n° 8 à propos de P_n s'appliquent à Q_n. Il en résulte d'abord que, si

$$n_h = n_0 + (2n_0 - 1)h \qquad (h = 0, 1, 2, \ldots), \tag{54}$$

la relation

$$x_h = x_0 + 2(x_0 - 1)h \tag{55}$$

établit entre les éléments de Q_{n_0} et certains éléments de Q_{n_k} (ceux pour lesquels $x-1$ est multiple de $2h+1$) une relation telle qu'à un cycle de Q_{n_0} corresponde un cycle de Q_{n_h} du même ordre et du même *type*. Le type est ici défini par la succession des formules a_k employées (a_k désignant la formule (32) où k est fixé), ou, plus simplement, par la succession des valeurs de k. Sa *parité* est celle du nombre des termes > 1 dans la suite des k; a_k donnant un nombre pair si $k > 1$ et seulement dans ce cas, c'est aussi la parité de la somme $\Sigma(x-1)$ étendue aux éléments du cycle.

D'ailleurs le transformé de x par la suite des opérations d'un type donné est une fonction linéaire de x où le coefficient de x est > 1. On en déduit, comme nous l'avons vu au n° 5 pour P_n, que, pour un n donné, il ne peut y avoir dans Q_n qu'un cycle de type donné. Il n'est pas tout à fait évident que tous les types théoriquement possibles soient réalisés. Mais, comme pour P_n, tout type qui est réalisé l'est pour un ensemble e de valeurs n_k de n déduit par la formule (54) de son premier élément n_0. Cet ensemble est donc exactement le même que pour les types de P_n qui sont naissants pour $n = n_0$. Mais, pour Q_n, il peut arriver (par exemple pour $n_0 = 12$) qu'à un même ensemble e soient associés plusieurs types *d'ordres différents, tous inférieurs à* $\omega(n_0)$, tandis que pour P_n, tous les types associés à un tel ensemble ont *le même ordre* $\sigma = \omega(n_0)$.

Comme pour P_n, les éléments x des cycles de types naissants

sont, pour chaque n, ceux pour lesquels $x - 1$ est premier avec $2n - 1$ (condition toujours vérifiée pour $x = 2$). Leur nombre est $\frac{1}{2}\varphi(2n-1)$; il est donc $n - 1$ si $2n - 1$ est premier. Mais, les ordres de ces cycles n'étant pas nécessairement égaux, on ne peut pas ici affirmer qu'ils divisent $\frac{1}{2}\varphi(2n-1)$ (ou $n - 1$, si $2n - 1$ est premier).

3°. On a vu le rôle joué dans l'étude de P_n par le nombre $\sigma = \omega(n)$ défini comme étant le plus petit exposant entier pour lequel on ait

$$2^\sigma \equiv \varepsilon = \pm 1 \qquad (\text{mod } p = 2n - 1),$$

et par la valeur de ε qui lui est associée. Tous les types naissants de P_n sont d'ordre σ, et pairs si $\varepsilon = 1$, impairs si $\varepsilon = -1$. Nous désignerons par E_0 l'ensemble des n pour lesquels $\varepsilon = 1$, et par E_1 l'ensemble complémentaire, pour lequel $\varepsilon = -1$.

Les éléments de E_1 sont évidemment caractérisés par la condition que p admette des multiples de la forme $2^\nu + 1$. Or la formule (54') peut s'écrire

$$p_h = (2h+1)p_0 \qquad (p_h = 2n_h - 1).$$

Il en résulte évidemment que, si un ensemble e contient un n_h élément de E_1, son premier élément n_0 appartient aussi à E_1; en effet p_0 est un diviseur de p_h, qui admet des multiples de la forme $2^\nu + 1$; il admet donc aussi ces multiples. Donc inversement, si $n_0 \in E_0$, tous les n_h sont aussi des éléments de E_0. La réciproque n'est évidemment pas vraie. Quel que soit n_0, l'ensemble des n_h contient le nombre $2^{2\sigma_0 - 1}$ $[\sigma_0 = \omega(n_0)]$, qui est un élément de E_0.

Les remarques qui précèdent ne sont d'ailleurs qu'un nouvel aspect de la remarque déjà faite au chapitre I: un cycle de type pair, répété un nombre quelconque de fois, reste toujours de type pair; un cycle de type impair, répété un nombre pair de fois, devient de type pair et peut être réalisé en même temps qu'un type primitif pair; il est alors naissant pour un $n_0 \in E_1$, et réalisé pour des $n_h \in E_0$.

Montrons encore que: *tous les multiples de 4 sont des éléments de* E_0. Si en effet on avait $n = 4n' \in E_1$, on aurait

$$2^\sigma \equiv -1, \quad 2^{\sigma+1} \equiv -2 \qquad (\text{mod } p),$$

et, comme un des nombres 2^σ et $2^{\sigma+1}$ est carré parfait, un des nombres -1 et -2 serait résidu quadratique pour le module $p = 2n - 1 = 8n' - 1$. D'après deux théorèmes connus de Gauss [9]), cela n'est pas possible.

[9]) Gauss. Recherches arithmétiques, n^{os} 108 et 113 (trad. francaise, édit. Hermann 1910, p. 79 et 83).

4°. Revenons maintenant à Q_n, et montrons les conséquences du fait que les formules (54) et (55) jouent exactement le même rôle que dans l'étude de l'opération P_n. Il en résulte évidemment que: si un cycle est commun à P_{n_0} et Q_{n_0}, on en déduit par la formule (55) un cycle commun à P_{n_h} et Q_{n_h}. Si un cycle de P_{n_0} n'est pas un cycle de Q_{n_0}, on en déduit par la même formule un cycle de P_{n_h} qui n'est pas un cycle de Q_{n_h}.

On en déduit immédiatement que:

Théorème. — Si $n \in E_1$, la décomposition en cycles est la même pour P_n et pour Q_n.

En effet, dans ce cas, le nombre $2^{\sigma-1}+1$ est un des n_h de l'ensemble e dont le premier élément est $n_0 = n$. Si, pour $n = n_0$, on pouvait trouver un cycle de P_n qui ne soit pas un cycle de Q_n, il en serait de même pour $n = 2^{\sigma-1}+1$. D'après le n° 19, 2°, cette hypothèse est exclue.

Théorème. — Si $n \in E_0$, tous les cycles de Q_n sont d'ordres inférieurs à $\sigma = \omega(n)$. La décomposition en cycles n'est donc pas la même que pour P_n.

En effet, dans ce cas, c'est $N = 2^{\sigma-1}$ qui appartient à l'ensemble e dont le premier élément est n. A tout cycle de Q_n correspond un cycle de Q_N ayant le même ordre, et, d'après le n° 18, cet ordre est au plus égal à $\sigma - 1$.

5°. *Remarques.* — On peut préciser le théorème précédent en remarquant que les éléments de P_n peuvent se décomposer en ensembles invariants à la fois pour P_n et pour Q_n. L'un d'eux est celui qui contient tous les éléments des cycles de types naissants. D'autre part, pour un élément x quelconque, le cycle auquel il appartient est d'un type qui est naissant pour une valeur n_0 qu'on obtient par la formule

$$2n - 1 = (2n_0 - 1)\delta,$$

δ étant le plus grand commun diviseur de $x - 1$ et $2n - 1$. Cette valeur de n_0 est la même, qu'il s'agisse de P_n ou de Q_n. Il en résulte évidemment que l'ensemble des x correspondant à une valeur déterminée de δ est invariant à la fois pour P_n et pour Q_n. Il en est de même de l'ensemble des x pour lesquels $x - 1$ est multiple d'un certain diviseur q de $2n - 1$, puisque c'est l'ensemble des x pour lesquels δ est égal à q ou multiple de q.

Les éléments de chacun de ces ensembles appartiennent, pour P_n, à des cycles de types naissants pour n_0, donc du même ordre $\sigma_0 = \omega(n_0)$, et pairs si $n_0 \in E_0$, impairs si $n_0 \in E_1$. Ils appartiennent, pour Q_n, à des cycles d'ordres $< \sigma_0$ si $n_0 \in E_0$, et coïncidant avec

ceux de P_n si $n_0 \in E_1$. Cette propriété, vraie pour $n = n_0$, subsiste en effet pour tout $n = n_h$ déduit de n_0 par la formule (54).

Si $n \in E_1$, n_0 est aussi un élément de E_1, et nous ne faisons que retrouver un résultat contenu dans le premier théorème du 4°. Mais, si $n \in E_0$, nous obtenons dans ce cas un résultat nouveau: *il peut, même dans ce cas, exister des cycles de P_n d'ordres $\sigma_0 < \sigma$, et de types impairs* (cela revient à dire qu'ils sont naissants pour un n_0 qui appartient à E_1; il faut pour cela que $\lambda = \frac{\sigma}{\sigma_1}$ soit un entier pair; en effet, le type du cycle répété λ fois doit devenir pair). *Les cycles de P_n ainsi obtenus sont aussi des cycles de Q_n. Chacun des autres éléments appartient à un cycle de P_n d'ordre σ_0 et de type pair, et à un cycle de Q_n d'ordre $< \sigma_0$* (dont le type peut être aussi bien pair qu'impair).

6°. Désignons respectivement par $\mathcal{S}$ et par $\mathcal{S}'$ les suites des n pour lesquels P_n et Q_n comprennent, en dehors de l'élément invariant 1, un cycle unique d'ordre $n - 1$. D'après les propriétés connues de P_n, $n \in \mathcal{S}$ équivaut à $\omega(n) = n - 1$. D'autre part $n \in \mathcal{S}'$ entraîne $\Omega(n) = n - 1$; la réciproque, peut-être exacte, n'est pas évidente.

Nous venons de voir que, si $n \in E_1$, P_n et Q_n ont les mêmes cycles. Donc, pour les éléments de E_1, $n \in \mathcal{S}$ équivaut à $n \in \mathcal{S}'$. Si au contraire $n \in E_0$, tous les cycles de Q_n sont d'ordres $< \sigma = \omega(n) \leqq n - 1$, et n n'appartient pas à $\mathcal{S}'$. Donc: *$\mathcal{S}'$ est l'intersection de $\mathcal{S}$ et de E_1.*

Or, si $n \in \mathcal{S}$, le cycle de P_n qui comprend les éléments 2, 3, ..., n est de type impair si $n \equiv 2$ ou 3 (mod. 4), et dans ce cas seulement. Donc, dans ce cas et dans ce cas seulement, $n \in E_1$. Donc: *pour que $n \in \mathcal{S}'$, il faut et il suffit que $n \in \mathcal{S}$ et que $n \equiv 2$ ou 3 (mod 4).*

D'ailleurs $\mathcal{S}$ ne contient aucun nombre de la forme $4n' + 1$. En effet $n = 4n' + 1 \in \mathcal{S}$ entraîne, d'une part (d'après le n° 8) que $p = 2n - 1$ soit premier, d'autre part, comme nous venons de le voir, $n \in E_0$. Donc $\sigma = \omega(n) = n - 1 = 4n'$, et $2^{4n'} \equiv 1$ (mod p). Le module étant premier, on en déduit $2^{2n'} \equiv \pm 1$, ce qui est en contradiction avec $\sigma = 4n'$ (puisque σ est le plus petit exposant tel que $2^\sigma \equiv \pm 1$).

Donc: *on obtient la suite $\mathcal{S}'$ en enlevant de la suite $\mathcal{S}$ tous les multiples de 4.*

Compte tenu des résultats du n° 8 (8° et 9°), on peut alors observer que: *pour que $n \in \mathcal{S}'$, il faut que $2n - 1$ soit premier et que $n \equiv 2$ ou 3 (mod 4); il suffit que $n - 1$ et $2n - 1$ soient premiers en même temps et que $4n$ ne soit pas multiple de 4.*

23. *Structure de l'ensemble* E_1 [10]). — 1°. Nous avons indiqué au n° 20, 3°, une condition nécessaire pour que le nombre n_h défini par la formule (54) appartienne à E_1. Nous allons maintenant indiquer la condition nécessaire et suffisante.

Le problème se simplifie si on substitue à chaque entier n le $n^{\text{ième}}$ nombre impair, $p = 2n - 1$. Aux $n \in E_1$ correspondent ainsi les éléments d'un ensemble F, et $p \in F$ signifie que p admet des multiples de la forme $2^\nu + 1$ [11]). Le plus petit étant $2^\sigma + 1$, avec $\sigma = \omega(n)$, tous les autres s'obtiennent en prenant pour ν les multiples impairs de σ. Nous poserons pour la suite $\omega(n) = \zeta(p)$. Si p, p' et P sont les nombres impairs ainsi substitués à n_0, $h + 1$ et n_h, la relation (54) prend la forme $pp' = P$, et il est évident que: *pour que* $P \in F$, *il faut que* p *et* p' *soient des éléments de* F.

2°. Désignons par $k = \lambda(p)$ le plus grand entier tel que $\zeta(p)$ soit divisible par 2^k, et par f_k l'ensemble des éléments de F pour lesquels $\lambda(p) = k$. Tous ces ensembles existent, puisque $2^\nu + 1 \in f_k$ ($k = 0, 1, 2, \ldots$) si ν est multiple impair de 2^k; F est leur réunion.

Théorème. — *Si un nombre premier* p *est un élément de* f_k, *il en est de même de toutes ses puissances.*

Pour démontrer ce théorème pour $p^{\alpha+1}$, nous pouvons évidemment le supposer vrai pour p^α. On a alors

$$2^\sigma = hp^\alpha - 1 \qquad (\sigma = \zeta(p^\alpha),\ h \text{ entier}),$$

et par suite

$$2^{p\sigma} = (hp^\alpha - 1)^p = Hp^{\alpha+1} - 1 \qquad (H \text{ entier}).$$

Donc, pour la valeur $\nu = p\sigma$ qui est un multiple impair de 2^k; $2^\nu + 1$ est multiple de $p^{\alpha+1}$. Donc $p^{\alpha+1} \in f_k$, c.q.f.d.

On remarque de plus que $\zeta(p^{\alpha+1})$ ne peut être que $\zeta(p^\alpha)$ ou $p\zeta(p^\alpha)$. Donc $\zeta(p^\alpha) = p^\beta \zeta(p)$, β s'annulant pour $\alpha = 1$, et β et $\alpha - \beta$ étant non décroissants.

3°. *Théorème.* — *Pour qu'un produit* P *appartienne à* F, *il faut*

---

[10]) Ce n°, comme le 3° du n° 20, dont il est la suite, se rattache au Chapitre I autant qu'au Chapitre III.

[11]) La propriété caractéristique de F équivaut á la suivante: si $p \in F$, et dans ce cas seulement, la période du développement dyadique de $\frac{1}{p}$ comprend un nombre pair 2ν de termes, et se décompose en deux demi-périodes complémentaires, c'est-à-dire que les termes correspondants des deux demi-périodes out pour somme 1. En effet cette propriété équivaut à: la partie fractionnaire de $\frac{2^\nu}{p}$ est $1 - \frac{1}{p}$; c'est-à-dire: $2^\nu + 1$ est multiple de p.

et il suffit que tous ses facteurs appartiennent à un même sous-ensemble f_k. Alors P appartient aussi à f_k.

Il suffit de démontrer ce théorème pour la décomposition de P en facteurs premiers; l'extension est ensuite immédiate. Posons donc

$$P = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h},$$

les p_ν étant premiers. Nous supprimerons les indices, en désignant par p un quelconque des p_ν et par α l'exposant correspondant.

Supposons d'abord $P \in f_k$. Alors, pour $\sigma = \zeta(P)$, $2^\sigma + 1$ est multiple de P, donc de p. Cela implique, d'une part que $p \in F$, d'autre part (d'après le 1°) que σ soit multiple impair de $\zeta(p)$, donc que p soit multiple impair de 2^k. Donc $p \in f_k$.

Pour démontrer la réciproque, supposons que tous les p, donc (d'après le 2°) tous les p^α, appartiennent à un même f_k. Soit μ le p.p.c.m. de tous les $\sigma = \zeta(p^\alpha)$; c'est un multiple impair de tous les σ. Donc, d'une part c'est un multiple impair de 2^k, d'autre part $2^\mu + 1$ est multiple de tous les $2^\sigma + 1$, donc de tous les p^α, donc de P. Donc $P \in f_k$, c.q.f.d.

On remarque de plus que $\mu = \zeta(P)$. En effet $2^\nu + 1$ n'est multiple de tous les p^α que si ν est multiple de tous les σ; la plus petite valeur possible pour ν est égale à la fois à μ et à $\zeta(P)$.

4°. *Conclusion. — F est la réunion d'ensembles disjoints f_k. Chacun des f_k est défini par la suite des nombres premiers qui lui appartiennent, et comprend tous les nombres qui n'ont pas d'autres facteurs premiers que ceux de cette suite.*

5°. Voici quelques résultats numériques: les nombres premiers 23, 31, 47, 71, 73, 79, 89 n'appartiennent pas à F. 3, 7, 11, 19, 43, 59, 67, 83 appartiennent à f_0. 5, 13, 29, 37, 41, 53, 61 appartiennent à f_1. 17, 241 (diviseur de 4097) appartiennent à f_2. 97 et 257 appartiennent à f_3.

D'une manière générale, les nombres premiers de la forme $4q + 3$, pour lesquels -1 n'est pas résidu quadratique (Gauss, loc. cit.), ne peuvent pas appartenir à des f_k autres que f_0. En posant $2^{2^k} = a_k$, il y a lieu de chercher les plus petits éléments de chaque f_k parmi les nombres $a_k + 1$, $a_k^3 + 1$, $a_k^5 + 1$, etc., et leurs diviseurs. On peut remarquer que $a_0 + 1$, $a_1 + 1$, ..., $a_4 + 1$ sont premiers. Pour $k = 3$, on a

$$a_3^3 + 1 = (256)^3 + 1 = 257 \cdot 97 \cdot 673,$$

de sorte que $a_3 + 1 = 257$ n'est pas le plus petit élément de f_3.

Il semble néanmoins probable qu'il arrive souvent que $a_k + 1$ soit premier et soit le plus petit élément de f_k [12]).

(Reçu le 28 septembre 1948, le n°. 21 le 7 octobre 1948, les notes [11]) et [12]) le 20 janvier 1949).

[12]) On remarque que, pour que $a_k + 1$ soit le plus petit élément de f_k, il faut, non seulement que ce nombre soit premier, mais que $b_k = a_k^2 - a_k + 1$, diviseur de $a_k^3 + 1$, donc élément de f_k, le soit aussi. Si en effet il ne l'était pas, son plus petit diviseur (autre que 1) serait un élément de f_k inférieur à a_k; c'est ce qui a lieu pour $k = 3$.

ANNEXES.

TABLEAU I.

Décomposition de P_n en cycles pour diverses valeurs de n. ($n = \lambda_1\sigma_1 + \lambda_2\sigma_2 + \ldots$ signifie que P_n comprend λ_1 cycles d'ordre σ_1, λ_2 cycles d'ordre σ_2, et ainsi de suite).

4 = 3+1	18 = 12+3+2+1	32 = 4.6 + 2.3 + 2.1
5 = 3+2.1	19 = 18+1	33 = 5.6 + 2 + 1
6 = 5+1	20 = 12+6+2.1	34 = 33 +1
7 = 6+1	21 = 2.10+1	35 = 22+11+2.1
8 = 4+2+2.1	22 = 3.7+1	36 = 35+1
9 = 2.4+1	23 = 12+4+3+2+2.1	37 = 4.9+1
10 = 9+1	24 = 23+1	38 = 20+10+4+2+2.1
11 = 6+3+2.1	25 = 21+3+1	39 = 30+5+3+1
12 = 11+1	26 = 2.8+2.4+2.1	40 = 39+1
13 = 10+2+1	27 = 26+1	41 = 27+9+3+2.1
14 = 9+3+2.1	28 = 20+5+2+1	42 = 41+1
15 = 14+1	29 = 3.9+2.1	43 = 4.8+2.4+2+1
16 = 3.5+1	30 = 29+1	44 = 28+14+2.1
17 = 3.5+2.1	31 = 30+1	45 = 4.11+1

49 = 2.24+1	78 = 3.20+3.5+2+1
51 = 50+1	83 = 3.20+3.5+4+2+2.1
52 = 51+1	127 = 110+11+5+1
53 = 3.12+6+4+3+2+2.1	128 = 14.8+3.4+2+2.1
54 = 53+1	129 = 16.8+1
55 = 3.18 + 1	130 = 3.36+18+3+1
57 = 4.14+1	256 = 28.9+3+1
63 = 50+10+2+1	257 = 28.9+3+2.1
64 = 9.7+1	512 = 48.10+6.5+2.1
65 = 9.7+2.1	513 = 51.10+2+1
66 = 65+1	1024 = 93.11+1
69 = 2.34+1	1025 = 93.11+2.1
70 = 69+1	2048 = 165.12+9.6+4+2.3+2+2.1
75 = 74+1	2049 = 170.12+2.4+1

TABLEAU II.

Décomposition de Q_n en cycles pour diverses valeurs de n. (Le nombre entre parenthèses suivant chaque formule est l'ordre du groupe des puissances de Q_n).

$4 = 2+2.1$ (2)	$25 = 11+10+2+2.1$ (110)
$5 = 3+2.1$ (3)	$26 = 6+5+2.4+3+2+2.1$ (60)
$6 = 5+1$ (5)	$27 = 26+1$ (26)
$7 = 6+1$ (6)	$28 = 12+8+5+2+1$ (120)
$8 = 3+2+3.1$ (6)	$29 = 3.9+2.1$ (9)
$9 = 2.4+1$ (4)	$30 = 29+1$ (29)
$10 = 9+1$ (9)	$31 = 30+1$ (30)
$11 = 4+2.2+3.1$ (4)	$32 = 5+2.4+3.3+3.2+4.1$ (60)
$12 = 7+4+1$ (28)	$33 = 5.6+2+1$ (6)
$13 = 10+2+1$ (10)	$34 = 33+1$ (33)
$14 = 9+3+2.1$ (9)	$35 = 2.11+7+4+2.1$ (308)
$15 = 14+1$ (14)	$36 = 21+14+1$ (42)
$16 = 4+2.3+2.2+2.1$ (12)	$37 = 3.6+5+4+3.3+1$ (60)
$17 = 3.5+2.1$ (5)	$38 = 11+10+9+3+2+3.1$ (990)
$18 = 7+5+2.2+2.1$ (70)	$39 = 2.15+5+2+2.1$ (30)
$19 = 18+1$ (18)	$40 = 18+14+7+1$ (126)
$20 = 8+6+4+2.1$ (24)	$41 = 27+9+3+2.1$ (27)
$21 = 2.10+1$ (10)	$42 = 41+1$ (41)
$22 = 3.7+1$ (7)	$43 = 2.6+5+4.4+3+3.2+1$ (60)
$23 = 7+5+2.3+2+3.1$ (210)	$44 = 19+18+5+2.1$ (1710)
$24 = 14+9+1$ (126)	$45 = 8+7+2.6+2.5+4+3+1$ (840)

$48 = 22+14+9+2+1$ (1386)
$52 = 28+23+1$ (644)
$53 = 8+7+2.6+5+2.4+3+3.2+4.1$ (840)
$64 = 6+3.5+5.4+5.3+4.2+4.1$ (60)
$127 = 58+52+7+5+4+1$ (52780)
$128 = 7+3.6+7.5+8.4+8.3+4.2+4.1$ (420)

En outre, pour toutes les valeurs de la forme $2^q + 1$ (donc $n = 65, 129, 257, \ldots$), et pour $n = 51, 54, 63, 66, 75, \ldots$, on a la même formule de décomposition que pour P_n (tableau I).