

M. BRINGER

**Sur un problème de R. Queneau**

*Mathématiques et sciences humaines*, tome 27 (1969), p. 13-20.

[http://www.numdam.org/item?id=MSH\\_1969\\_\\_27\\_\\_13\\_0](http://www.numdam.org/item?id=MSH_1969__27__13_0)

© Centre d'analyse et de mathématiques sociales de l'EHESS, 1969, tous droits réservés.

L'accès aux archives de la revue « Mathématiques et sciences humaines » (<http://msh.revues.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## SUR UN PROBLÈME DE R. QUENEAU

par

M. BRINGER

### INTRODUCTION.

$S_n$  étant le groupe des permutations de l'ensemble  $E = \{1, 2, \dots, n\}$  on appelle *permutation spirale*<sup>1</sup> ou *permutation de Queneau Daniel*, la permutation  $\delta_n$  définie par :

$$\delta_n(2p + 1) = n - p; \delta_n(2p) = p.$$

Le sous-groupe cyclique de  $S_n$  engendré par  $\delta_n$  s'appelle le groupe de Queneau-Daniel ; on le note  $G_n$ . Le problème à résoudre est le suivant : *trouver tous les entiers  $n$  tels que  $G_n$  soit d'ordre  $n$* . Si  $n$  est solution, la permutation  $\delta_n$  et l'entier  $n$  seront dits admissibles<sup>2</sup>.

### 0. — PRÉLIMINAIRES.

Le but de ce paragraphe est de rappeler les principales notions et les résultats qui seront utilisés dans la suite.

#### 0.1. — *Rappels concernant le groupe symétrique $S_n$ .*

Pour les démonstrations que nous ne referons pas ici, on pourra se reporter à : Marshall Hall, *The Theory of groups* (chapitre 5).

— On appelle *cycle* une permutation  $\Pi$  sur  $p$  lettres  $x_1, \dots, x_p$ , telle que :

$$\Pi(x_1) = x_2, \dots, \Pi(x_i) = x_{i+1}, \dots, \Pi(x_{p-1}) = x_p; \Pi(x_p) = x_1.$$

Nous noterons  $\Pi = (x_1, x_2, \dots, x_p)$  ;  $\Pi$  est un élément d'ordre  $p$  de  $S_n$ .

— Etant donnée une permutation  $\sigma$  de l'ensemble  $E = \{1, 2, \dots, n\}$ , on peut décomposer  $\sigma$  en un produit de cycles portant sur des sous-ensembles disjoints de  $E$ . L'ordre de  $\sigma$  est alors égal au ppcm des ordres de ces cycles, et  $n$  est égal à la somme des ordres de ces cycles.

— Un groupe de permutations  $G \subset S_n$  est dit transitif si pour tout couple  $p, q$  d'éléments de  $E$ , il existe  $\sigma$  élément de  $G$  tel que  $q = \sigma(p)$ . En particulier si  $G$  est le sous-groupe de  $S_n$  engendré par une permutation  $\sigma$ , le groupe  $G$  est transitif si et seulement si  $\sigma$  est un cycle portant sur les  $n$  nombres  $1, 2, \dots, n$ . On dira alors que  $\sigma$  est transitif.

---

1. L'expression « permutation en spirale » est due à M. E. Vinaver.

2. La première liste des  $n$ -ièmes possibles a été établie par M. Tavera.

0.2. — *Rappels concernant les congruences dans  $\mathbf{Z}$ , anneau des entiers relatifs.*

Pour les démonstrations on se reportera à : G. H. Hardy et E. M. Wright, *An introduction to the theory of numbers* (chapitre 6).

0.3. — Si  $p$  est un nombre entier,  $\mathbf{F}_p = \mathbf{Z}/p$  est un corps.

— Si  $p$  est un nombre entier de la forme  $8k \pm 1$ , il existe dans  $\mathbf{F}_p$  un élément  $x$  tel que  $x^2 = 2$ . On dit que « 2 est un carré dans  $\mathbf{F}_p$  ».

— Si  $p$  est un nombre premier de la forme  $8k \pm 3$ , 2 n'est pas un carré dans  $\mathbf{F}_p$ .

— Si  $p$  est un nombre premier de la forme  $4k + 3$ , une condition nécessaire et suffisante pour que  $2p + 1$  soit premier est que l'on ait :  $2^p \equiv 1 \pmod{2p + 1}$  soit  $2^p = 1$  dans  $\mathbf{F}_{2p+1}$ .

— Soit  $\mathbf{Z}_{2n+1}$  l'ensemble des entiers modulo  $2n + 1$  que nous représentons par  $\mathbf{A}_n = \{-n, \dots, -1, 0, 1, \dots, n\}$ ; on peut définir dans  $\mathbf{A}_n$  un produit. Si  $x, y$  sont des éléments de  $\mathbf{A}_n$ , le produit de  $x$  et  $y$  dans  $\mathbf{A}_n$  sera le représentant de  $xy$  (produit dans  $\mathbf{Z}$ ) modulo  $2n + 1$  appartenant à  $\mathbf{A}_n$ .

On peut définir dans  $\mathbf{A}_n$  une valeur absolue en posant :

$$|x| = x \text{ si } x = 0, 1, \dots, n; |x| = -x \text{ si } x = 0, -1, \dots, -n.$$

Cette valeur absolue vérifie :

$$|xy| = ||x||y||.$$

En effet si :

$$x, y > 0, \text{ on a } |x| = x, |y| = y,$$

donc :

$$xy = |x||y| \text{ et } |xy| = ||x||y||,$$

si :

$$x, y < 0 \text{ on a } |x| = -x, |y| = -y$$

donc :

$$xy = |x||y| \text{ et } |xy| = ||x||y||,$$

si :

$$x > 0, y < 0, \text{ on a } |x| = x, |y| = -y,$$

donc :

$$xy = -|x||y| \text{ et } |xy| = ||x||y||.$$

1. — ÉTUDE DE LA PERMUTATION INVERSE DE  $\delta_n$ .

1.1. —  $\delta_n$  étant une bijection de  $\mathbf{E} = \{1, 2, \dots, n\}$  sur lui-même possède un inverse  $d_n$ , qui sera défini par :

$$d_n(x) = 2x \text{ si } x \leq \frac{n}{2}$$

$$d_n(x) = 2n + 1 - 2x \text{ si } \frac{n}{2} < x \leq n.$$

Dans le premier cas  $x \leq \frac{n}{2}$ ,  $2x$  étant inférieur ou égal à  $n$  représente le produit de  $x$  par 2 dans  $A_n$  et ce produit est positif.

Si :  $\frac{n}{2} < x \leq n$  on a  $n + 1 \leq 2x \leq 2n$ ,

donc :  $n \leq 2x - (2n + 1) \leq -1$

et  $2x - (2n + 1)$

représente le produit de  $x$  par 2 dans  $A$  et ce produit est négatif ; or :

$$d_n(x) = 2n + 1 - 2x = -2x = |2x|.$$

Nous aurons donc :

$$d_n(x) = |2x|$$

et par récurrence :

$$d_n^p(x) = |2^p x|.$$

Nous raisonnerons désormais sur cette interprétation, car  $\delta_n$  est d'ordre  $n$  si et seulement si  $d_n$  est d'ordre  $n$ .

1.2. — *Théorème 1.* Pour que  $\delta_n$  soit d'ordre  $n$  il faut et il suffit que  $\delta_n$  soit transitive.

Considérons la décomposition de  $\delta_n$  en produit de cycles disjoints :  $\delta_n = C_1 C_2 \dots C_k$  (ce produit est indépendant de l'ordre des termes).

Soit  $C_1$  le cycle contenant 2, c'est-à-dire  $C_1 = (2, \delta_n(2), \dots, \delta_n^{p-1}(2))$  où  $p$  est le plus petit entier tel que  $\delta_n^p(2) = 2$ .

Pour démontrer le théorème démontrons d'abord le lemme suivant :

*Lemme 1.* L'ordre de  $C_i$  divise l'ordre de  $C_1$  pour tout  $i = 1, 2, \dots, k$ .

Si  $\delta_n = C_1, C_2, \dots, C_k$ , on aura  $d_n = C'_1, C'_2, \dots, C'_k$  où  $C'_i$  est le cycle inverse de  $C_i$ , il est équivalent de démontrer que l'ordre de  $C'_i$  divise l'ordre de  $C'_1$  :

$$C'_1 = (2, d_n(2), \dots, d_n^{p-1}(2)),$$

où  $p$  est le plus petit entier non nul tel que :

$$d_n^p(2) = 2 = d_n(1) \Leftrightarrow d_n^{p-1}(2) = 1 \Leftrightarrow |2^p| = 1,$$

$C'_1$  est alors un cycle d'ordre  $p$ .

Si  $x$  est un élément quelconque de  $E = \{1, 2, \dots, n\}$ , il existe un cycle  $C'_i$  tel que  $x$  figure dans  $C'_i$  et on a alors :

$$C'_i = (x, d_n(x), \dots, d_n^{q-1}(x))$$

où  $q$  est le plus petit entier tel que :

$$d_n^q(x) = |2^q x| = x.$$

$C'_i$  est un cycle d'ordre  $q$ .

Or :

$$|2^p x| = ||2^p|| |x| = |1 \cdot x| = |x| = x,$$

donc  $p \geq q$  d'après la définition de  $q$ . On peut alors diviser  $p$  par  $q$  :

$$p = \lambda q + r \quad \text{avec} \quad 0 \leq r < q.$$

Si  $r \neq 0$  on a :

$$x = |2^p x| = |2^{\lambda q} x 2^r| = ||2^{\lambda q} x|| |2^r||$$

Or :

$$|2^{\lambda q} x| = d_n^{\lambda q}(x) = (d_n^q)^\lambda(x) = x \quad \text{car} \quad d_n^q(x) = x,$$

donc on a :

$$x = |x| |2^r| = ||x|| |2^r| = |2^r x|$$

ce qui est incompatible avec la définition de  $q$  si  $r \neq 0$ .

On a nécessairement :  $r = 0$  donc  $p = \lambda q$ .

L'ordre de  $C'_i$  divise l'ordre de  $C'_1$ , donc l'ordre de  $C_i$  divise l'ordre de  $C_1$ . On en déduit le corollaire suivant :

*Corollaire.* L'ordre de  $\delta_n$  est égal à l'ordre de  $C_1$  ; en effet l'ordre de  $\delta_n$  étant le ppcm des ordres de  $C_i$ , est égal à l'ordre de  $C_1$ .

*Démonstration du théorème.*  $\delta_n$  d'ordre  $n$  est donc équivalent à  $C_1$  d'ordre  $n$ ,  $C_1$  est donc un cycle portant sur  $E$  tout entier. C'est le seul qui figure dans la décomposition de  $\delta_n$  en produit de cycles disjoints.  $C_1$  d'ordre  $n$  est donc équivalent à  $\delta_n = C_1$  (ce qui est équivalent comme nous l'avons rappelé à :  $\delta_n$  est transitive).

Donc  $\delta_n$  est d'ordre  $n$  si et seulement si  $\delta_n$  est transitive, c'est-à-dire si et seulement si :

$$\delta_n = (2, \delta_n(2), \dots, \delta_n^{n-1}(2)).$$

Nous pouvons obtenir un résultat plus précis.

*Lemme 2.* Si  $2n + 1$  est un nombre premier, tous les cycles  $C_i$  sont de même ordre et cet ordre est un diviseur de  $n$ .

Soit :  $p$  l'ordre de  $C'_1 = (2, d_n(2), \dots, d_n^{p-1}(2))$ ,

$q$  l'ordre de  $C'_i = (x, d_n(x), \dots, d_n^{q-1}(x))$ .

Nous savons que  $q$  divise  $p$ .

On a  $|2^q x| = x$ , ce qui est équivalent à  $2^q x = \pm x$  donc nous aurons dans  $A_n$ ,  $2^{2q} x^2 = x^2$ , ce qui veut dire que dans  $Z$ ,  $2n + 1$  divise  $(2^{2q} - 1) x^2 = (2^q - 1)(2^q + 1) x^2$ .

$x$  étant un élément de  $1, 2, \dots, n$ ,  $2n + 1$  ne peut diviser ni  $x$ , ni  $x^2$ .

Donc  $2n + 1$  divise  $2^q - 1$  ou  $2^q + 1$ . Nous aurons donc dans  $A_n$  :

$$2^q - 1 = 0 \quad \text{ou} \quad 2^q + 1 = 0, \quad \text{soit} \quad |2^q| = 1,$$

$p$  étant le plus petit entier tel que :  $2^p = 1$ , on a  $q \geq p$ .

Soit finalement  $q = p$ . Tous les cycles  $C'_i$  (donc tous les cycles  $C_i$ ) sont de même ordre que  $C'_1$ . Or  $n$  étant égal à la somme des ordres des cycles  $C_i$  et ces ordres étant tous égaux divisent nécessairement  $n$ .

## 2. — UNE CONDITION NÉCESSAIRE.

2.1. — *Théorème 2.* Une condition nécessaire pour que  $n$  soit admissible est que  $2n + 1$  soit un nombre premier.

Supposons  $\delta_n$  d'ordre  $n$  donc  $\delta_n = C_1$ .

Si  $2n + 1$  n'est pas premier, il a au moins un diviseur  $q \neq 1 \quad q \leq n$ .

Montrons alors que tous les nombres  $d_n^p(q) = |2^p q|$  sont tous divisibles par  $q$  : on a en effet dans  $\mathbb{Z}$ ,  $2^p q = (2n + 1)h + r$  avec  $-n \leq r \leq n$  et  $|2^p q| = |r|$  dans  $A_n$ .

Si  $q$  divise  $2n + 1$ , comme il divise  $2^p q$ , il divise  $r$  donc  $d_n^p(q)$ .

Le cycle  $C_i$  qui contient  $q$  contient tous les nombres  $d_n^p(q)$ , donc il ne comporte que des nombres divisibles par  $q$ . Or il existe dans  $E = \{1, 2, \dots, n\}$  des nombres non divisibles par  $q$  (par ex. :  $1, 2, \dots, q - 1$ ). Le cycle  $C_i$  n'est donc pas le seul dans la décomposition de  $\delta_n$  en produit de cycles ;  $\delta_n$  n'est donc pas transitive et par conséquent  $\delta_n$  n'est pas d'ordre  $n$ .

*Remarque 1.*

Cette condition est équivalente à la condition nécessaire due à R. Queneau : l'équation  $n = 2xy + x + y$  n'a pas de solutions entières.

Si  $2n + 1$  est premier, supposons que  $n = 2xy + x + y$  ait des solutions entières (différentes de  $x = -1, y = -(n + 1)$  qui est toujours solution pour tout  $n$ ) alors :

$$2n + 1 = 4xy + 2x + 2y + 1 = (2x + 1)(2y + 1).$$

Les deux nombres  $2x + 1$  et  $2y + 1$  sont différents de 1 et divisent  $2n + 1$  ce qui n'est pas possible ; l'équation n'a pas de solutions entières.

Si l'équation  $n = 2xy + x + y$  n'a pas de solutions entières ; supposons que  $2n + 1$  ne soit pas premier, alors on peut écrire  $2n + 1 = pq$  ;  $p$  et  $q \neq 1$  sont impairs,  $p = 2p' + 1$  ;  $q = 2q' + 1$ .

On en déduit alors  $n = 2p'q' + p' + q'$  ce qui est impossible, donc  $2n + 1$  est premier.

*Remarque 2.*

Cette condition n'est pas suffisante : par exemple,  $n = 20$  ;  $2n + 1 = 41$  est premier, et une étude directe montre que  $\delta_{20}$  est d'ordre 10.

2.2. — *Théorème 3.* Les nombres  $n$  de la forme  $2^p (p \neq 1)$  et  $2^p - 1 (p \neq 2)$  ne sont pas admissibles.

Si  $n = 2^p$ , nous avons :

$$\delta_n(2) = 1, \delta_n^2(2) = n = 2^p, \delta_n^3(2) = 2^{p-1}, \dots, \delta_n^{p+1}(2) = 2$$

le cycle  $C_1$  engendré par 2 est d'ordre  $p + 1 \neq 2^p$  si  $p \neq 1$  ; si  $p \neq 1$ ,  $2^p$  n'est pas admissible ; si  $p = 1$ ,  $C_1$  d'ordre  $2 = n$  donc 2 est admissible.

Si  $n = 2^p - 1$ , nous avons :

$$\delta_n(2) = 1 ; \delta_n^2(2) = n = 2^p - 1 ; \delta_n^3(2) = 2^{p-1} ; \dots, \delta_n^{p+1}(2) = 2$$

le cycle  $C_1$  engendré par 2 est d'ordre  $p + 1 \neq 2^p - 1$  si  $p \neq 2$  ; pour  $p \neq 2$ ,  $n = 2^p - 1$  n'est pas admissible ; pour  $p = 2$ ,  $C_1$  est d'ordre  $3 = n$ , 3 est donc admissible.

### 3. — UNE CONDITION SUFFISANTE.

3.1. — *Théorème 4.*  $2n + 1$  étant premier, pour que  $n$  soit admissible, il suffit que 2 engendre le groupe multiplicatif de  $F_{2n+1} = Z/2n + 1$ .

$2n + 1$  étant premier,  $F_{2n+1}$  est un corps. On peut donc parler du groupe multiplicatif de  $F_{2n+1}$  qui est d'ordre  $2n$ . Tous les éléments de  $F_{2n+1}$  ont des ordres qui divisent  $2n$ .

Si 2 engendre le groupe multiplicatif de  $F_{2n+1}$ , 2 est d'ordre  $2n$ .

On a donc :  $2^{2n} = 1$  et  $2^p \neq 1$  si  $p < 2n$ .

Alors les nombres  $d_n^p(2)$   $1 \leq p \leq n$  sont tous distincts : dans  $A_n$  nous avons :

$2^{2n} - 1 = 0 = (2^n - 1)(2^n + 1)$ , comme  $2^n \neq 1$  on a nécessairement  $2^n = -1$  et si  $2^p = -1$  on a  $2^{2p} = 1$  donc  $2p \geq 2n$  soit  $p \geq n$ .

Supposons qu'il existe  $p$  et  $q$  tels que  $1 \leq p < q \leq n$ , vérifiant :

$$d_n^p(2) = d_n^q(2) \quad \text{soit} \quad |2^{p+1}| = |2^{q+1}|.$$

Ceci entraîne :

$$2^{p+1} = 2^{q+1} \quad \text{d'où} \quad 2^{q-p} = 1 \quad \text{avec} \quad 1 \leq q - p \leq n,$$

ou bien :

$$2^{p+1} = -2^{q+1} \quad \text{d'où} \quad 2^{q-p} = -1 \quad \text{avec} \quad 1 \leq q - p \leq n.$$

Ceci n'est pas possible. Les nombres  $d_n^p(2)$ ,  $1 \leq p \leq n$  sont tous distincts ; le cycle  $C_1$  engendré par 2 est d'ordre  $n$  ;  $n$  est donc admissible.

*Remarque.*

Cette condition n'est pas nécessaire ; en effet si  $n = 11$ ,  $2n + 1 = 23$ . Une étude directe montre que  $n$  est admissible et que 2 est simplement d'ordre  $n$ .

Il est cependant nécessaire que 2 soit d'ordre  $k \geq n$  : si  $k < n$  les nombres  $d_n^p(2)$ ,  $1 \leq p \leq n$  prennent au plus  $k$  valeurs distinctes.  $C_1$  est donc d'ordre  $< n$  ;  $n$  n'est donc pas admissible.

Nous allons maintenant pouvoir, à l'aide des résultats obtenus précédemment, caractériser certaines familles de nombres  $n$  admissibles et certaines familles de nombres  $n$  non admissibles.

3.2. — *Théorème 5.* Si  $n$  et  $2n + 1$  sont tous les deux des nombres premiers, alors  $n$  est admissible.

Nous avons vu (lemme 2) que lorsque  $2n + 1$  est premier,  $\delta_n$  est un produit de  $k$  cycles tous de même ordre  $p$ , cet ordre divisant  $n$  ( $kp = n$ ) ; or, si  $n$  est premier, cet ordre commun ne peut être que 1 ou  $n$  ; ce ne peut être 1 ce qui voudrait dire que pour tout  $x$   $\delta_n(x) = x$ , ce qui n'est pas le cas. On a donc  $p = n$  et par suite  $k = 1$  ; donc  $\delta_n = C_1$  ce qui entraîne que  $n$  est admissible.

Nous pouvons aussi démontrer ce théorème en utilisant les propriétés des congruences modulo  $2n + 1$ , rappelées dans les préliminaires.

Si  $n$  est un nombre premier  $\neq 2$ ,  $n$  est impair et deux cas se présentent :

—  $n = 4p + 3$  ; alors  $2n + 1$  étant premier ceci entraîne que  $2^n = 1$  dans  $A_n$  ; l'ordre de 2 est donc un diviseur de  $n$  ; c'est donc  $n$ .

Alors tous les nombres  $|2^k|$   $1 \leq k \leq n$  sont tous distincts.

Si il existe  $k$  et  $k'$  tels que  $|2^k| = |2^{k'}|$  avec  $1 \leq k < k' \leq n$ , ceci entraîne  $2^k = 2^{k'}$  ou  $2^{k'-k} = 1$  avec  $k' - k < n$ , ce qui est impossible car l'ordre de 2 est  $n$  ou bien  $2^k = -2^{k'}$  soit  $2^{k'-k} = -1$  d'où  $2^{2(k'-k)} = 1$ , ce qui entraîne 2 ( $k' - k$ ) est un multiple de  $n$ ; comme  $n$  ne peut diviser 2,  $n$  qui est premier doit diviser  $k' - k$  ce qui est impossible car  $k' - k < n$ ; les nombres  $|2^k|$   $1 \leq k \leq n$  étant tous distincts, le cycle  $C_1$  est d'ordre  $n$ ; alors  $n$  est admissible.

—  $n = 4p + 1$ ; on sait alors que 2 n'est pas un carré dans  $F_{2n+1}$ . Or on a toujours :

$2^{2n} - 1 = (2^n - 1)(2^n + 1) = 0$ , si  $2^n - 1 = 0$  on a  $2^{n+1} = 2 = 2^{4p+2} = (2^{2p+1})^2$ , ce qui est impossible car 2 n'est pas un carré. On a donc nécessairement  $2^n = -1$ .  $2^{2n} = 1$  entraîne que l'ordre de 2 est un diviseur de  $2n$  : c'est donc  $2n$ ,  $n$  ou 2 (car  $n$  est premier); cet ordre n'est pas  $n$  puisque  $2^n = -1$ . Ce n'est pas 2 en général car on aurait  $2^2 - 1 = 0$ , soit  $2n + 1$  divise 3, ce qui implique  $n = 1$ . 2 est donc d'ordre  $2n$ , ce qui suffit pour que  $n$  soit admissible (théorème 4). En résumé, si  $n$  et  $2n + 1$  sont premiers,  $n$  est admissible.

3.3. — *Théorème 6.* Si  $n$  est de la forme  $n = 2p$ ,  $p$  et  $4p + 1$  étant premiers ( $p \neq 2$ ),  $n$  est admissible.

$p$  étant premier  $\neq 2$  est impair :  $p = 2k + 1$ , alors  $2n + 1 = 4p + 1 = 8k + 5 = 8k' - 3$ . On sait que 2 et  $-2$  ne sont pas des carrés dans  $F_{2p+1}$ . Or on a toujours :

$$2^{2n} - 1 = 2^{4p} - 1 = (2^{2p} + 1)(2^p + 1)(2^p - 1) = 0;$$

$$\text{si } 2^p = 1 \text{ on a } 2 = 2^{p+1} = 2^{2(k+1)}, 2 \text{ serait un carré;}$$

$$2^p = -1 \text{ on a } -2 = 2^{p+1} = 2^{2(k+1)}, -2 \text{ serait un carré.}$$

On a donc nécessairement :  $2^{2p} = -1 = 2^n$ .

$2^{4p} = 1$  entraîne que l'ordre de 2 est un diviseur de  $4p$  :  $4p$ ,  $2p$ ,  $p$ , 4 ou 2.

Nous avons vu que ce n'était ni  $p$  ni  $2p$ .

Si c'était 2 on aurait  $2^2 - 1 = 0$  ( $2n + 1$ ) ce qui entraîne  $n = 1$ .

Si c'était 4, on aurait  $2^4 - 1 = 0$  ( $2n + 1$ ),  $2n + 1$  (premier) doit diviser 15 donc  $2n + 1 = 3$ , soit  $n = 1$  ou  $2n + 1 = 5$  donc  $n = 2$ , qui sont admissibles.

En éliminant ces valeurs de  $n$  il reste : 2 est d'ordre  $4p = 2n$ . Ceci suffit pour que  $n$  soit admissible.

3.4. — *Théorème 7.* Si  $2n + 1$  est un nombre premier de la forme  $8p + 1$ , donc si  $n = 4p$ ,  $n$  n'est pas admissible.

$2n + 1$  étant premier de la forme  $8p + 1$ , 2 est un carré dans  $F_{2n+1}$ ; il existe donc  $x$  tel que  $x^2 = 2$ . Mais pour tout  $x$  on a :  $x^{2n} = 1$ , donc  $2^n = x^{2n} = 1 = 2^{4p}$ .

Soit  $(2^{2p} + 1)(2^p + 1)(2^p - 1) = 0$  entraîne  $2^{2p} = -1$  ou  $2^p = -1$  ou  $2^p = 1$ , ce qui entraîne dans tous les cas  $|2^{2p}| = 1 = d_n^2 p^{-1}(2)$ .

Le cycle  $C_1$  engendré par 2 est donc d'ordre  $\leq 2p = \frac{n}{2}$ ; l'ordre de  $\delta_n$  est donc  $< n$  et  $n$  n'est pas admissible.

Nous pouvons aussi obtenir ce résultat en étudiant la parité de  $\delta_n$ .

3.5. — *Théorème 8.* Si  $n \equiv 0, 1, 3 \pmod{4}$ ,  $\delta_n$  est paire; si  $n \equiv 2 \pmod{4}$ ,  $\delta_n$  est impaire.

La parité de  $\delta_n$  s'obtient en étudiant le signe de l'expression :

$$\Delta_n = \prod_{x < y} \frac{\delta_n(x) - \delta_n(y)}{x - y};$$

ce produit est égal à  $\pm 1$ .  $\delta_n$  est paire si  $\Delta_n = +1$ ; si  $\Delta_n = -1$ ,  $\delta_n$  est impaire.

Or nous avons entre  $\delta_n$  et  $\delta_{n+1}$  les relations suivantes :

$$\text{si } x \leq n \quad \begin{cases} x \text{ pair : } & \delta_{n+1}(x) = \delta_n(x) \\ x \text{ impair : } & \delta_{n+1}(x) = \delta_n(x) + 1, \end{cases}$$

$$\text{si } n \text{ est pair : } \quad \delta_{n+1}(n+1) = \delta_n(n) + 1,$$

$$\text{si } n \text{ est impair : } \quad \delta_{n+1}(n+1) = \delta_n(n),$$

et on a :

$$\Delta_{n+1} = \prod_{x < y \leq n} \frac{\delta_{n+1}(x) - \delta_{n+1}(y)}{x - y} \cdot \prod_{x \leq n} \frac{\delta_{n+1}(x) - \delta_{n+1}(n+1)}{x - (n+1)}.$$

Une étude simple des signes des différents rapports intervenant dans  $\Delta_{n+1}$  montre que si  $n \equiv 0, 3 \pmod{4}$   $\Delta_{n+1} = \Delta_n$  ; si  $n \equiv 1, 2 \pmod{4}$   $\Delta_{n+1} = -\Delta_n$ .

Ce qui entraîne dans tous les cas :  $\Delta_{n+4} = \Delta_n$  :  $\delta_{n+4}$  a même parité que  $\delta_n$ . Or, une étude directe montre que  $\delta_2$  est impaire,  $\delta_3, \delta_4, \delta_5$  sont paires d'où le résultat :  $n \equiv 0, 1, 3 \pmod{4}$   $\delta_n$  est paire ; si  $n \equiv 2 \pmod{4}$   $\delta_n$  est impaire.

*Corollaire.* Si  $n \equiv 0 \pmod{4}$ , ( $n = 4p$ )  $n$  n'est pas admissible.

En effet, si  $n$  était admissible,  $\delta_n$  serait un cycle de longueur  $n = 4p$  et  $\delta_n$  serait de la parité de  $n - 1$  donc impaire, ce qui n'est pas le cas.  $n$  n'est donc pas admissible.

Parmi les nombres,  $n \equiv 1, 2, 3 \pmod{4}$  il y en a qui sont admissibles, d'autres qui ne le sont pas ; par exemple  $5 \equiv 1 \pmod{4}$ ,  $6 \equiv 2 \pmod{4}$ ,  $23 \equiv 3 \pmod{4}$  sont admissibles, alors que  $13 \equiv 1 \pmod{4}$ ,  $22 \equiv 2 \pmod{4}$ ,  $27 \equiv 3 \pmod{4}$  ne le sont pas. On ne peut donc pas tirer d'autres conclusions du théorème 8.

#### 4. — RÉSUMÉ DES RÉSULTATS OBTENUS.

I. — Pour que  $n$  soit admissible, il est nécessaire que  $2n + 1$  soit premier.

II. —  $2n + 1$  étant premier, si 2 est d'ordre  $2n$  dans  $F_{2n+1}$ ,  $n$  est admissible :  $2n + 1$  étant premier, nous avons trouvé deux familles de nombres admissibles :

III. Les nombres  $n$  tels que  $n$  et  $2n + 1$  soient premiers.

IV. Les nombres  $n = 2p$  tels que  $p$  et  $4p + 1$  soient premiers ( $p \neq 2$ ).

Nous avons d'autre part, trouvé les nombres non admissibles suivants :

V.  $n = 2^p$  ( $p \neq 1$ ) (ces nombres sont aussi du type (VII).)

VI.  $n = 2^p - 1$  ( $p \neq 2$ ).

VII.  $n = 4p$ .