NOUVELLES ANNALES DE MATHÉMATIQUES

ELIE CARTAN

Sur certains cycles arithmétiques

Nouvelles annales de mathématiques 6^e *série*, tome 2 (1927), p. 33-45

<http://www.numdam.org/item?id=NAM_1927_6_2__33_0>

SUR CERTAINS CYCLES ARITHMÉTIQUES ;

PAR ELIE CARTAN.

Le problème de Mathématiques élémentaires proposé au dernier concours d'agrégation contenait une intéressante question d'Arithmétique (¹) sur les cycles de nombres entiers obtenus en partant d'un nombre de n chiffres et en effectuant sur ces chiffres successivement $1, 2, \ldots, n-1$ permutations circulaires. Il peut arriver que les n nombres ainsi obtenus forment une progression arithmétique, et l'on demandait aux candidats de trouver tous les cycles de 3 et de 6 chiffres jouissant de cette propriété.

Ce problème, qui semble n'avoir fait jusqu'ici l'objet d'aucune recherche, est susceptible d'une solution complète, non seulement dans le système de numération décimale, mais encore dans le système de numération le plus général. C'est cette solution que je me propose d'exposer dans les pages qui suivent. Comme on le verra, les cycles cherchés rentrent dans deux catégories nettement distinctes.

I. — Remarques préliminaires.

1. Considérons, dans le système de numération à base a, un nombre de n chiffres

$$\mathcal{N} = \alpha_1 \alpha_2 \ldots \alpha_n,$$

ainsi que les $n-1$ nombres obtenus par permutation circulaire des chiffres

$$\mathcal{N}_1 = \alpha_2 \alpha_3 \ldots \alpha_n \alpha_1,$$
$$\mathcal{N}_2 = \alpha_3 \alpha_4 \ldots \alpha_1 \alpha_2,$$
$$\ldots\ldots\ldots\ldots\ldots$$

Nous supposerons dans ce qui suit que $\mathcal{N}$ est le plus petit des nombres du cycle formé par les n nombres considérés. Nous nous proposons de trouver tous les cas dans lesquels les nombres du cycle forment, à l'ordre près, une progression arithmétique. Il est clair que la question ne se pose que pour $n \geq 3$.

(¹) L'énoncé et la solution ont paru dans le numéro de novembre 1926, p 366.

Nous pouvons regarder le nombre $\mathcal{N}$ comme la période d'une fraction pseudo-décimale périodique simple, résultant de la conversion d'une certaine fraction irréductible $\frac{N}{D}$:

$$\frac{N}{D} = \frac{\alpha_1}{a} + \frac{\alpha_2}{a^2} + \ldots + \frac{\alpha_n}{a^n} + \frac{\alpha_1}{a^{n+1}} + \ldots = \frac{\mathcal{N}}{a^n} + \frac{\mathcal{N}}{a^{2n}} + \ldots = \frac{\mathcal{N}}{a^n - 1}.$$

On aura $N < D$; de plus D sera un diviseur de $a^n - 1$; en particulier D sera premier avec a.

Il est facile de voir quelles sont les fractions ordinaires qui donnent naissance aux périodes $\mathcal{N}_1, \ldots, \mathcal{N}_{n-1}$. On a en effet

$$\begin{aligned} \frac{aN}{D} - \alpha_1 &= \frac{\alpha_2}{a} + \ldots = \frac{\mathcal{N}_1}{a^n - 1}, \\ \frac{a^2 N}{D} - (\alpha_1 a + \alpha_2) &= \frac{\mathcal{N}_2}{a^n - 1}, \\ \ldots\ldots\ldots\ldots & \quad \ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Les fractions

$$\frac{aN - \alpha_1 D}{D}, \quad \frac{a^2 N - (\alpha_1 a + \alpha_2) D}{D}, \quad \ldots$$

sont irréductibles, car tout diviseur commun au numérateur et au dénominateur de la $i^{\text{ième}}$ fraction diviserait $a^i N$; étant premier avec a, il diviserait N, contrairement à la propriété d'irréductibilité de la fraction $\frac{N}{D}$.

Par suite *les n nombres* $\mathcal{N}, \mathcal{N}_1, \ldots, \mathcal{N}_{n-1}$ *du cycle sont les périodes des fractions périodiques résultant de la conversion de n fractions irréductibles* $\frac{N}{D}, \frac{N_1}{D}, \ldots, \frac{N_{n-1}}{D}$, *où* N_i *est le reste de la division de* $a^i N$ *par* D.

Si les nombres $\mathcal{N}_i$ forment une progression arithmétique, il en est de même des nombres N_i : ces derniers nombres seront donc tous distincts. Par suite n est l'exposant de la plus petite puissance de a qui soit congrue à 1 (mod D) ; autrement dit, *a appartient à l'exposant n* (mod D).

2. Nous pouvons adopter une représentation géométrique commode. Considérons une circonférence divisée en D parties égales à partir d'un point origine O. Tout entier N_i sera représenté par un des points de subdivision de la circonférence, à savoir celui qu'on

obtient en portant, à partir de O, dans un sens fixé une fois pour toutes, N_t divisions ; nous désignerons ce point par (N_t). Deux nombres congrus entre eux (mod D) sont représentés par le même point.

Nous avons alors à chercher tous les cas dans lesquels les points de la suite illimitée (N), (aN), (a^2N), ... *se réduisent à n distincts et forment les sommets d'une ligne brisée polygonale régulière convexe* $\mathcal{L}$; il faut du reste qu'en partant de O, on rencontre tous les sommets de cette ligne avant de revenir au point O.

3. D'après ce qui précède, la suite des points

$$(aN),\quad (aN_1),\quad \ldots,\quad (aN_{n-1}) \tag{1}$$

coincide, à l'ordre près, avec la suite des points

$$(N),\quad (N_1),\quad \ldots,\quad (N_{n-1}). \tag{2}$$

Soit d'autre part R la raison de la progression arithmétique formée par les nombres N_t ; la suite des points

$$(N+R),\quad (N_1+R),\quad \ldots,\quad (N_{n-1}+R) \tag{3}$$

a $n-1$ points communs avec la suite (2). De là résulte que la suite des points

$$(aN+aR),\quad (aN_1+aR),\quad \ldots,\quad (aN_{n-1}+aR)$$

a également $n-1$ points communs avec la suite (2) ; il en est de même de la suite

$$(N+aR),\quad (N_1+aR),\quad \ldots,\quad (N_{n-1}+aR).$$

Donc *si l'on fait tourner de* aR *divisions la ligne brisée polygonale régulière* $\mathcal{L}$, *la nouvelle ligne* $\mathcal{L}'$ *obtenue a au moins* $n-1$ *sommets communs avec* $\mathcal{L}$.

4. Remarquons que la rotation de aR divisions est une rotation effective ; sinon en effet aR serait un multiple de D, et aussi par suite R, ce qui est absurde.

Si les deux lignes $\mathcal{L}$ et $\mathcal{L}'$ ont tous leurs sommets communs, c'est qu'en allant dans le sens positif du dernier sommet $[N+(n-1)R]$

au premier (N) on s'avance exactement de R divisions, autrement dit qu'on a

$$D = nR. \tag{4}$$

Si $\mathcal{L}$ et $\mathcal{L}'$ n'ont pas tous leurs sommets communs, on peut supposer que le sommet de $\mathcal{L}$ qui n'appartient pas à $\mathcal{L}'$ est soit le premier sommet (N), soit le dernier $[N + (n-1)R]$, soit un sommet intermédiaire.

Si le point (N) ne fait pas partie de $\mathcal{L}'$, la ligne $\mathcal{L}'$ se déduit de $\mathcal{L}$ par une rotation de R divisions dans le sens positif ; on a donc

$$aR \equiv R \pmod{D}$$

ou

$$(a-1)R \equiv 0 \pmod{D}. \tag{5}$$

Si c'est le point $[N + (n-1)R]$ qui ne fait pas partie de $\mathcal{L}'$, on obtient de même $\mathcal{L}'$ par une rotation de $\mathcal{L}$ de R divisions dans le sens négatif ; on a donc

$$(a+1)R \equiv 0 \pmod{D}. \tag{6}$$

Si enfin c'est un sommet intermédiaire de $\mathcal{L}$ qui ne fait pas partie de $\mathcal{L}'$, les deux points $(N - R)$ et $(N + nR)$ doivent faire partie de $\mathcal{L}'$, et comme aucun d'eux ne fait partie de $\mathcal{L}$, c'est qu'ils sont identiques ; par suite

$$(n+1)R \equiv 0 \pmod{D}.$$

Cela n'est possible que si l'on a

$$D = (n+1)R. \tag{7}$$

En définitive on a l'une des quatre relations (4), (5), (6), (7).

5. Ajoutons enfin un dernier théorème. Soit Δ le plus grand commun diviseur de R et de D. On a

$$(a-1)N = N_1 - N + \alpha_1 D = hR + \alpha_1 D \qquad (1 \leq h \leq n-1).$$

Par suite Δ divise $(a-1)N$; mais Δ est premier avec N, puisque la fraction $\frac{N}{D}$ est irréductible ; donc Δ divise $a-1$.

THÉORÈME. — *Le plus grand commun diviseur de* R *et de* D *divise* $a-1$.

Le cas où R et D sont premiers entre eux n'est naturellement pas exclu.

II. — Les cycles de la première catégorie.

6. *Nous allons*, après ces préliminaires, *supposer d'abord que le dénominateur* D *de la fraction irréductible* $\frac{N}{D}$ *contient au moins un facteur premier* p *ne figurant pas dans* $a-1$.

Supposons que p figure dans D avec l'exposant α. Il ne figure certainement pas dans R, à cause du théorème du n° 5.

Il résulte immédiatement de là l'inégalité

$$p > n. \tag{8}$$

En effet l'un des p termes de la progression arithmétique

$$N,\quad N+R,\quad \ldots,\quad N+(p-1)R,$$

dont la raison est première avec p, est divisible par p ; si p était inférieur ou égal à n, ce terme serait le numérateur d'une des fractions $\frac{N_i}{D}$, qui ne serait donc pas irréductible, ses deux termes étant divisibles par p.

En second lieu, la base a appartient à l'exposant $n \pmod p$. En effet si a appartenait à l'exposant $\nu < n$, on aurait

$$a^{\nu}N - N \equiv 0 \pmod p.$$

Or

$$(a^{\nu}-1)N = qD + hR \qquad (1 \leqq h \leqq n-1);$$

le nombre premier p divisant le premier membre, ainsi que le terme qD du second membre, devrait diviser hR, ce qui n'est pas, puisque p ne divise ni R, ni $h \leqq n-1 < p$.

Si nous revenons maintenant aux quatre cas possibles indiqués au n° 4, nous voyons que les congruences (5) et (6) sont exclues, puisqu'elles entraîneraient $a^2 \equiv 1 \pmod p$; l'égalité (4) est également exclue, puisque p est premier avec nR. On a donc nécessairement

$$D = (n+1)R. \tag{7}$$

Il résulte de cette dernière égalité que p^α est un diviseur de $n+1$, et comme p est au moins égal à $n+1$, cela n'est possible que si l'on a

$$p = n+1, \qquad \alpha = 1. \tag{9}$$

Cela prouve en particulier qu'il ne peut entrer dans D qu'un seul facteur premier diviseur de $a-1$, et que ce facteur premier est $n+1$, entrant avec l'exposant 1. Il en résulte aussi que a est une *racine primitive* de p, puisque a appartient à l'exposant

$$n = p-1.$$

Enfin des p termes de la progression arithmétique

$$N-R, \quad N, \quad N+R, \quad \ldots, \quad N+(n-1)R,$$

dont la raison est première avec p, un est divisible par p ; ce ne peut être que le premier : on a donc

$$\begin{gathered} N-R \equiv 0 \pmod p, \\ N = R \mp kp. \end{gathered} \tag{10}$$

L'entier k, s'il est précédé du signe —, doit satisfaire à l'inégalité

$$kp < R; \tag{11}$$

s'il est précédé du signe +, le nombre $N+(n-1)R = nR+kp$ doit être plus petit que $D = (n+1)R$; on a donc encore la même inégalité (11).

Le théorème du n° 5 montre enfin, d'après (7), que R est un diviseur de $a-1$.

7. De l'analyse précédente résulte le théorème suivant :

THÉORÈME. — *Si la fraction irréductible* $\frac{N}{D}$ *jouit de la propriété que son dénominateur contienne un facteur premier p ne figurant pas dans* $a-1$, *elle est de la forme*

$$\frac{N}{D} = \frac{R \mp kp}{pR}, \tag{12}$$

où R *est un diviseur de* $a-1$, *a une racine primitive de p, et* $k < \frac{R}{p}$.

Réciproquement, supposons ces conditions réalisées. On a

$$a^i\mathrm{N} = a^i\mathrm{R} \mp a^i kp \equiv a^i\mathrm{R} \mp kp \qquad (\mathrm{mod}\, p\mathrm{R})$$

Or les $p-1$ nombres $a^i\mathrm{R}$ sont, à l'ordre près, congrus aux nombres

$$\mathrm{R},\quad 2\mathrm{R},\quad \ldots,\quad (p-1)\,\mathrm{R} \qquad (\mathrm{mod}\, p\mathrm{R}).$$

Les points $(a^i\mathrm{N})$ sont donc identiques aux points représentatifs des nombres

$$\mathrm{R} \mp kp,\quad 2\mathrm{R} \mp kp,\quad \ldots.\quad (p-1)\mathrm{R} \mp kp,$$

lesquels sont tous inférieurs à $\mathrm{D} = p\mathrm{R}$ et forment une progression arithmétique de raison R. Le cycle de $n = p-1$ nombres définis par la fraction considérée $\frac{\mathrm{N}}{\mathrm{D}}$ fournit donc bien une progression arithmétique de raison R.

8. On peut poser

$$\frac{\mathrm{N}}{\mathrm{D}} = \frac{1}{p} \mp \frac{k}{\mathrm{R}} = \frac{1}{p} \mp \frac{k'}{a-1}. \tag{13}$$

La fraction $\frac{k'}{a-1}$ se développe suivant une fraction illimitée dont tous les chiffres sont égaux à k'. D'autre part tous les chiffres du developpement de $\frac{1}{p}$ sont d'une part supérieurs ou égaux à k', d'autre part inférieurs ou égaux à $a-k'$. En effet le plus petit chiffre de la période de $\frac{1}{p}$ est évidemment son premier chiffre, c'est donc le quotient de a par p. Or

$$k' < \frac{a-1}{p} < \frac{a}{p}.$$

De même le plus grand chiffre de la période de $\frac{1}{p}$ est le quotient de $(p-1)\,a$ par p. Or on a

$$a - k' > a - \frac{a-1}{p} = \frac{a(p-1)}{p} + \frac{1}{p} > \frac{a(p-1)}{p}.$$

Il résulte de là le théorème suivant

Théoreme. — *Pour avoir toutes les solutions du problème*

pour lesquelles D *admet un diviseur premier non contenu dans* $a-1$, *on cherche les différents nombres premiers* p *dont* a *est racine primitive. Si* p *est un de ces nombres, la période de la fraction illimitée à laquelle donne naissance* $\frac{1}{p}$ *définit un cycle d'ordre* $p-1$, *dont les* $p-1$ *nombres forment une progression arithmétique; on déduira de ce cycle un certain nombre d'autres cycles jouissant de la même propriété en augmentant ou en diminuant tous les chiffres d'une même valeur, tant que cela sera possible.*

9. Le cas $n=2$ étant exclu, nous n'avons à considérer que les nombres premiers $p \geqq 5$:

Si $p=5$, $n=4$.....	$a \equiv \pm 2$	(mod 5);
si $p=7$, $n=6$.....	$a \equiv 3$ ou 5	(mod 7);
si $p=11$, $n=10$.....	$a \equiv 2$, 5, 7 ou 8	(mod 11);
si $p=13$, $n=12$.....	$a \equiv 2$, 6, 7 ou 11	(mod 13);
.....	.....	

Dans le cas particulier $a=10$, on peut avoir

$$p = 7,\ 17,\ 19,\ 23,\ 29,\ 47,\ \ldots.$$

On a 3 cycles d'ordre 6 définis respectivement par les nombres

$$142857,\ 031746,\ 253968,$$

qui sont respectivement les périodes des fractions

$$\frac{1}{7},\qquad \frac{1}{7}-\frac{1}{9}=\frac{2}{63},\qquad \frac{1}{7}+\frac{1}{9}=\frac{16}{63}.$$

On a un cycle d'ordre 16 défini par le nombre

$$0588235294117647,$$

période de la fraction $\frac{1}{17}$.

On a un cycle d'ordre 18 défini par le nombre

$$052631578947368421,$$

période de la fraction $\frac{1}{19}$.

Enfin si $a = 2$ (système de numération binaire), on peut avoir

$$p = 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ 53,\ 59,\ 61,\ \ldots;$$

tous ces nombres sont des multiples de 8, plus ou moins 3.

Si $p = 5$, $n = 4$, on a le cycle défini par le nombre

0011 ;

si $p = 11$, $n = 10$, on a le cycle défini par le nombre

0001011101 ;

si $p = 13$, $n = 12$, on a le cycle défini par le nombre

000100111011 ;

si $p = 19$, $n = 18$, on a le cycle défini par le nombre

000011010111100101.

III. — Les cycles de la seconde catégorie.

10. Supposons maintenant que les facteurs premiers de D entrent tous dans $a - 1$. Soit

$$a - 1 = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_h^{\alpha_h},$$
$$D = p_1^{\lambda_1}\, p_2^{\lambda_2} \ldots p_h^{\lambda_h}.$$

Nous allons d'abord chercher l'exposant n auquel appartient a (mod D).

Nous nous appuierons sur la remarque suivante :

Si a appartient respectivement aux exposants n_1 et n_2 par rapport aux modules D_1 et D_2 premiers entre eux, l'exposant n auquel appartient a (mod $D_1 D_2$) *est égal au plus petit commun multiple de n_1 et de n_2.*

En effet la congruence

$$a^n \equiv 1 \pmod{D}$$

entraîne

$$a^n \equiv 1 \pmod{D_1};$$

donc n est un multiple de n_1. De même n est un multiple de n_2.

Réciproquement si n est un multiple commun de n_1 et de n_2, $a^n - 1$ est divisible à la fois par D_1 et par D_2, et par suite par D.

Il résulte de là qu'il suffit de connaître l'exposant auquel appartient a par rapport à chacun des nombres $p_1^{\lambda_1}$, $p_2^{\lambda_2}$, ..., $p_h^{\lambda_h}$.

11. Prenons l'un des nombres premiers p qui entrent dans $a - 1$; soit α son exposant. On peut poser

$$a = 1 + kp^\alpha,$$

k étant premier avec p. On en déduit

$$a^p = (1 + kp^\alpha)^p = 1 + kp^{\alpha+1} + \ldots + k^p p^{p\alpha},$$

$$a^p - 1 = kp^{\alpha+1} + \ldots + k^p p^{p\alpha}. \tag{14}$$

Les coefficients des termes non extrêmes du binome $(x+y)^p$ sont tous divisibles par p, si p est un nombre premier. Les différents termes du second membre de (14) contiennent donc p avec les exposants

$$\alpha + 1, \quad 2\alpha + 1, \quad \ldots, \quad (p-1)\alpha + 1, \quad p\alpha.$$

Par suite $a^p - 1$ est divisible par $p^{\alpha+1}$. Il ne pourrait être divisible par $p^{\alpha+2}$ que si l'on avait

$$\alpha + 1 = p\alpha,$$

c'est-à-dire

$$p = 2, \qquad \alpha = 1.$$

Si nous écartons ce cas, nous voyons que *si p entre avec l'exposant α dans $a - 1$, il entre avec l'exposant $\alpha + 1$ dans $a^p - 1$*. Le même raisonnement appliqué au nombre a^p, au lieu du nombre a, montre que p entre avec l'exposant $\alpha + 2$ dans $a^{p^2} - 1$, $\alpha + 3$ dans $a^{p^3} - 1$, et ainsi de suite. Il en résulte que l'exposant auquel appartient $a \pmod{p^{\alpha+k}}$ est égal à p^k ou a un diviseur de p^k; mais ce ne peut être un diviseur de p^k, car ce serait p^{k-1} ou un de ses diviseurs, et l'on aurait

$$a^{p^{k-1}} - 1 \equiv 0 \pmod{p^{\alpha+k}},$$

tandis que p n'entre qu'avec l'exposant $\alpha + k - 1$ dans $a^{p^{k-1}} - 1$.

En conséquence *l'exposant auquel appartient $a \pmod{p^\lambda}$ est égal à 1 si $\lambda \leq \alpha$, à $p^{\lambda-\alpha}$ si $\lambda > \alpha$.*

12. Il y a un cas d'exception, c'est celui où $p = 2, \alpha = 1$; $a - 1$ est alors le double d'un nombre impair. Dans ce cas, en effet, $a^2 - 1$ est divisible au moins par 8 et, par suite, contient le facteur premier $p = 2$ plus de $\alpha + 1 = 2$ fois. Mais si $a^2 - 1$ contient β fois le facteur 2, le raisonnement du numéro précédent est valable; $a^1 - 1$ contient $\beta + 1$ fois le facteur 2, $a^8 - 1$ le contient $\beta + 2$ fois et ainsi de suite.

13. Si nous excluons le cas où $a - 1$ est le double d'un nombre impair, nous voyons que n est le plus petit multiple commun de h nombres qui sont égaux soit à 1, soit à des puissances des facteurs premiers $p_1, \ldots, p_h$; si donc $\lambda_i \leqq \alpha_i$, n ne contient pas le facteur premier p_i ; si $\lambda_i > \alpha_i$, n contient le facteur premier p_i avec l'exposant $\lambda_i - \alpha_i$. Autrement dit, *n est le quotient de* D *par le plus grand commun diviseur* δ *de* D *et de* $a - 1$.

Ce résultat est encore valable si $a - 1$ est le double d'un nombre impair, à condition que D soit impair ou contienne le facteur premier 2 à un des exposants 1 ou 2. Si D est impair ou le double d'un nombre impair, n est impair ; si D est divisible par 4 (et non par 8), n est le double d'un nombre impair.

14. Nous allons montrer que, réciproquement, si l'on a

$$D = n\delta,$$

δ étant le plus grand commun diviseur de D et de $a - 1$, la période du développement de la fraction irréductible $\frac{N}{D}$ donne naissance à un cycle dont les n nombres forment une progression arithmétique.

Prenons en effet sur la circonférence le point (N) et considérons le polygone régulier de n côtés dont ce point est un des sommets ; deux sommets consécutifs du polygone sont séparés par δ divisions.

On a

$$a^i N - N = (a^i - 1) N \equiv 0 \pmod{\delta};$$

par suite le point $(a^i N)$ coïncide avec l'un des sommets du polygone régulier qui vient d'être construit. Et comme tous ces points sont au nombre de n distincts, on obtient bien tous les sommets du polygone. Le théorème est donc démontré, et l'on a $R = \delta$. On est dans le cas de la formule (4) prévue au n° 4.

Remarquons qu'ici on peut écrire

$$\frac{N}{D} = \frac{N}{n\delta} = \frac{N'}{n(a-1)},$$

N′ étant premier avec n, et $a-1$ étant divisible par chacun des facteurs premiers qui entrent dans n, avec la restriction qu'il doit être divisible par 4 si n est lui-même divisible par 4.

Si l'on veut que la période de $\frac{N}{D}$ fournisse le plus petit nombre du cycle, il faut que N soit inférieur à δ, c'est-à-dire $N' < a-1$.

15. Reste le cas où D serait divisible par 8, $a-1$ étant simplement divisible par 2. Nous allons voir que les n nombres du cycle ne peuvent pas dans ce cas former une progression arithmétique.

En effet remarquons d'abord que si i est impair, a^i-1 est divisible par 2 et non par 4, car on a

$$a^i - 1 = (a-1)(a^{i-1} + a^{i-2} + \ldots + a + 1);$$

le nombre premier 2 entre une fois dans le premier facteur du second membre, et il n'entre pas dans le second facteur, qui est la somme d'un nombre impair de nombres impairs.

Au contraire si i est pair, a^i-1 est divisible par a^2-1 et par suite par 8.

Cela posé, le nombre D de divisions de la circonférence étant un multiple de 8, on passe du point (N) au point (a^iN) en portant un nombre de divisions égal au double d'un nombre impair si i est impair, à un multiple de 8 si i est pair. Si les résidus de a^iN formaient une progression arithmétique, la raison de cette progression serait donc le double d'un nombre impair; le double de cette raison, qui serait congru à l'un des nombres $(a^i-1)\,N \pmod{\delta}$, serait divisible par 4, sans l'être par 8, ce qui est impossible.

16. En résumé, on voit qu'*on peut former tous les cycles de la seconde catégorie en partant d'un nombre n quelconque; on prend une base a telle que a — 1 soit divisible par chacun des facteurs premiers de n (avec la restriction que a — 1 doit être divisible par 4 si n est divisible par 4). La période de la fraction illimitée résultant du développement de* $\frac{N'}{n(a-1)}$, *où* $N' < a-1$

est premier avec n, donne naissance à un cycle de la seconde catégorie.

Si $n = 3$ on prendra $a = \text{mult.}\, 3 + 1$,
si $n = 4$ » $a = \text{mult.}\, 4 + 1$,
si $n = 5$ » $a = \text{mult.}\, 5 + 1$,
si $n = 6$ » $a = \text{mult.}\, 6 + 1$,
si $n = 7$ » $a = \text{mult.}\, 7 + 1$,
si $n = 8$ » $a = \text{mult.}\, 4 + 1$,
si $n = 9$ » $a = \text{mult.}\, 3 + 1$,
....

Dans le cas $a = 10$, n sera une puissance quelconque de 3 :

$$n = 3^h, \qquad \frac{N}{D} = \frac{N'}{3^{h+2}} \qquad (N' = 1, 2, 4, 5, 7, 8).$$

Pour $h = 1$, on aura 6 cycles d'ordre 3 définis respectivement par leurs plus petits nombres

037, 074, 148, 185, 259, 296.

Pour $h = 2$, on aura 6 cycles d'ordre 9 définis respectivement par les nombres

012345679, 024691358, 049382716,
061728395, 086419753, 098765432.

Pour $h = 3$, on aura de même 6 cycles d'ordre 27, et ainsi de suite.

Dans le cas $a = 12$, n serait une puissance quelconque de 11 et l'on aurait 10 cycles d'ordre 11, 10 cycles d'ordre 121, etc.

Les cycles de la seconde catégorie ne peuvent se présenter si $a = 2$ ou 3.

Au contraire, les cycles de la première catégorie ne peuvent se présenter si a est un carré parfait.