NOUVELLES ANNALES DE MATHÉMATIQUES

A. LAISANT
ÉTIENNE BEAUJEUX

Mémoire sur certaines propriétés des résidus numériques

Nouvelles annales de mathématiques 2^e série, tome 9 (1870), p. 271-281

<http://www.numdam.org/item?id=NAM_1870_2_9__271_0>

MÉMOIRE SUR CERTAINES PROPRIÉTÉS DES RÉSIDUS NUMÉRIQUES

(suite, voir 2e série, t. IX, p. 221);

PAR MM. A. LAISANT ET ÉTIENNE BEAUJEUX.

8. La propriété établie au n° 4 donne lieu à quelques conséqnences dont voici un exemple. Supposons que le diviseur ait quatre chiffres, et qu'il s'écrive *abcd* dans le système de numération dont la base est q.

On pourra écrire les nombres suivants :

$$a,\ a+b,\ a+b+c,\ a+b+c+d,\ b+c+d,\ c+d,\ d,$$

sous sept restes consécutifs quelconques r_{p+7}, r_{p+6}, r_{p+5}, r_{p+4}, r_{p+3}, r_{p+2}, r_{p+1}, écrits dans l'ordre inverse de celui dans lequel ils ont été obtenus. La somme des produits respectifs sera encore un multiple du diviseur D. On a en effet (4)

$$\begin{aligned}
ar_{p+7} + br_{p+6} + cr_{p+5} + dr_{p+4} &= m.\mathrm{D},\\
ar_{p+6} + br_{p+5} + cr_{p+4} + dr_{p+3} &= m.\mathrm{D},\\
ar_{p+5} + br_{p+4} + cr_{p+3} + dr_{p+2} &= m.\mathrm{D},\\
ar_{p+4} + br_{p+3} + cr_{p+2} + dr_{p+1} &= m.\mathrm{D}.
\end{aligned}$$

Ajoutant

$$\begin{aligned}
ar_{p+7} + (a+b)r_{p+6} + (a+b+c)r_{p+5}\\
+ (a+b+c+d)r_{p+4} + (b+c+d)r_{p+3}\\
+ (c+d)r_{p+2} + dr_{p+1} = m.\mathrm{D}.
\end{aligned}$$

On aurait aussi bien pu écrire les nombres suivants au-dessous des restes considérés :

$$\begin{gathered}
a,\quad -a+b,\quad a-b+c,\quad -a+b-c+d,\\
-b+c-d,\quad -c+d,\quad -d,
\end{gathered}$$

et la propriété aurait toujours subsisté, comme on le verrait sans peine, en changeant de deux en deux les signes des égalités ci-dessus.

Il serait aisé d'étendre à un nombre quelconque de chiffres cette propriété que nous avons seulement énoncée ici pour un diviseur de quatre chiffres, pour plus de facilité dans la démonstration.

9. Soit encore un diviseur de quatre chiffres *abcd*. On aura toujours les quatre égalités du numéro précédent. En multipliant la première par a, la deuxième par $-b$, la troisième par c, la quatrième par $-d$, et ajoutant, on éliminera les termes en r_{p+2}, r_{p+4}, r_{p+6}, et il viendra

$$a^2 r_{p+7} - (b^2 - 2a \times c) r_{p+5} + (c^2 - 2b \times d) r_{p+3} - d^2 r_{p+1} = m.\mathrm{D}.$$

On étendrait aisément aussi cette propriété à un nombre quelconque de chiffres. Elle se réduit, comme on le voit, à

$$a^2 r_{p+3} - b^2 r_{p+1} = m.\mathrm{D},$$

dans le cas où le diviseur n'a que deux chiffres a et b.

10. Soit qu'en divisant les termes de la progression : A, AB, AB^2, . . . , où B est la base du système de numération, par un diviseur de p chiffres $a_p a_{p-1} \ldots a_2 a_1 = \mathrm{D}_1$, on ait trouvé les restes successifs

$$r_0, \quad r_1, \quad r_2, \ldots, r_p, \ldots,$$

r_0 étant un reste quelconque, et que les chiffres correspondants obtenus au quotient, en faisant la division d'une façon continue, comme pour les fractions décimales périodiques, soient

$$\mathrm{Q}_0, \ \mathrm{Q}_1, \ \mathrm{Q}_2, \ldots, \ \mathrm{Q}_p, \ldots.$$

Considérons les nombres

$$\begin{aligned}
&a_p a_{p-1} \ldots a_2 = D_2,\\
&a_p a_{p-1} \ldots a_3 = D_3,\\
&\ldots\ldots\ldots\ldots,\\
&a_p a_{p-1} = D_{p-1},\\
&a_p = D_p,
\end{aligned}$$

que nous nommerons *diviseurs tronqués*, et formons le tableau suivant :

Diviseurs tronqués.....	$D_p,\ D_{p-1},\ \ldots,\ D_2,\ D_1,$
Chiffres du quotient.....	$Q_p,\ Q_{p-1},\ \ldots,\ Q_2,\ Q_1,\ Q_0,$
Restes correspondants....	$r_p,\ r_{p-1},\ \ldots,\ r_2,\ r_1,\ r_0,$
Chiffres du diviseur.....	$a_p,\ a_{p-1},\ \ldots,\ a_2,\ a_1,$

on aura

$$\begin{aligned}
&a_p r_p + a_{p-1} r_{p-1} + a_1 r_1\\
&\quad = D_1 \times (r_1 - D_2 Q_2 - D_3 Q_3 - \ldots - D_p Q_p),
\end{aligned}$$

ou bien

$$= D_1 \times (B r_0 - D_1 Q_1 - D_2 Q_2 - \ldots - D_p Q_p).$$

L'identité de ces deux formules est évidente, car

$$B r_0 = D_1 Q_1 + r_1;$$

d'où

$$r_1 = B r_0 - D_1 Q_1.$$

Il suffit donc de démontrer l'une d'entre elles.

Or

$$\begin{aligned}
B r_0 &= Q_1 D_1 + r_1,\\
B r_1 &= Q_2 D_1 + r_2,\\
B r_2 &= Q_3 D_1 + r_3,\\
&\ldots\ldots\ldots\ldots,\\
B r_{p-1} &= Q_p D_1 + r_p.
\end{aligned}$$

De là

$$\begin{aligned}
Br_0 &= Q_1 D_1 + r_1,\\
B^2 r_0 &= (Q_1 B + Q_2) D_1 + r_2,\\
B^3 r_0 &= (Q_1 B^2 + Q_2 B + Q_3) D_1 + r_3,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
B^p r_0 &= (Q_1 B^{p-1} + \ldots + Q_p) D_1 + r_p.
\end{aligned}$$

Multipliant la première de ces égalités par a_1, la deuxième par a_2, et ainsi de suite, puis ajoutant, il vient

$$Br_0 \times D_1 = D_1 \times \left\{\begin{array}{ll}
Q_1(a_1 + a_2 B + \ldots + a_p B^{p-1}) & + a_1 r_1\\
+ Q_2(a_2 + a_3 B + \ldots + a_p B^{p-2}) & + a_2 r_2\\
+ \cdots\cdots\cdots\cdots\cdots\cdots & + \ldots\\
+ Q_p a_p & + a_p r_p.
\end{array}\right.$$

Donc

$$a_1 r_1 + \ldots + a_p r_p = D_1 (Br_0 - Q_1 D_1 - Q_2 D_2 - \ldots - Q_p D_p).$$

Cette relation donne, comme on le voit, l'expression du quotient de la quantité $a_1 r_1 + \ldots + a_p r_p$ par le diviseur, en fonction d'un reste (r_0 ou r_1), des chiffres successivement obtenus au quotient, et du diviseur lui-même. Ce quotient est

$$Br_0 - Q_1 D_1 - Q_2 D_2 - \ldots - Q_p D_p,$$

ou

$$r_1 - Q_2 D_2 - Q_3 D_3 - \ldots - Q_p D_p.$$

La propriété du n° 4 nous avait fait connaître que ce quotient est entier, mais sans fournir son expression.

Il ne sera pas sans intérêt de vérifier ce résultat sur un exemple numérique. Soit $\frac{2}{1271}$ que nous cherchons à convertir en décimales. On trouve, en particulier, au

quotient les chiffres successifs 5, 6, 4, 1, 2. Formons le même tableau que ci-dessus :

Diviseurs tronqués.....	1	12	127	1271	
Chiffres du quotient.....	2	1	4	6	5
Restes correspondants ...	348	289	156	524	815
Chiffres du diviseur.....	1	2	7	1	

On aura

$$(1\times 348)+(2\times 289)+(7\times 156)+(1\times 524)$$
$$=1271\times[8150-(6\times 1271)-(4\times 127)-(1\times 12)-(2\times 1)],$$
$$=1271\times[524-(4\times 127)-(1\times 12)-(2\times 1)].$$

Dans cet exemple, le nombre entre les crochets est égal à 2. On peut remarquer que, dans tous les cas, ce nombre sera plus petit que la somme des chiffres du diviseur. Car les restes 348, 289, 156, 524 étant tous inférieurs au diviseur 1271, on a

$$(1\times 348)+(2\times 289)+(7\times 156)+(1\times 524)$$
$$<(1+2+7+1)1271.$$

11. Soient r_{n+1}, r_{n+2}, r_{n+3} trois restes consécutifs quelconques, obtenus en divisant par un diviseur D les termes de la progression géométrique : Aq, Aq^2, ...

On a

$$Aq^{n+1}=m.D+r_{n+1},$$
$$Aq^{n+3}=m.D+r_{n+3};$$

d'où, par multiplication,

$$(\alpha)\qquad A^2q^{2n+4}=m.D+r_{n+1}\times r_{n+3};$$

d'autre part

$$Aq^{n+2}=m.D+r_{n+2};$$

élevant au carré

$$(\beta)\qquad A^2q^{2n+4}=m.D+r_{n+2}^2;$$

retranchant α de β,

$$r_{n+2}^2 - r_{n+1} \times r_{n+3} = m \cdot \mathrm{D}.$$

On verrait de même que quatre restes consécutifs satisfont toujours à la relation

$$r_{n+1} \times r_{n+4} - r_{n+2} \times r_{n+3} = m \cdot \mathrm{D}.$$

En général, *deux produits quelconques de restes, homogènes par rapport à la lettre r et tels, que les sommes des indices soient égales de part et d'autre, ne diffèrent entre eux que d'un multiple du diviseur.*

Car soient

$$r_i^m \times r_{i'}^{m'} \times r_{i''}^{m''} \times \ldots \quad \text{et} \quad r_j^n \times r_{j'}^{n'} \times r_{j''}^{n''} \times \ldots,$$

et supposons que

$$m + m' + m'' \ldots = n + n' + n'' + \ldots = \mathrm{M}$$
$$mi + m'i' + m''i'' \ldots = nj + n'j' + n''j'' + \ldots = \mathrm{I}.$$

En remplaçant r_i par $\mathrm{A}q^i$, $r_{i'}$ par $\mathrm{A}q^{i'}, \ldots$, et r_j par $\mathrm{A}q^j \ldots$, on ne pourra altérer l'un ou l'autre produit que d'un multiple de D. On aura ainsi

$$\mathrm{A}^m q^{mi} \times \mathrm{A}^{m'} q^{m'i'} \times \ldots = \mathrm{A}^{m+m'+\cdots} \times q^{mi+m'i'+\cdots} = \mathrm{A}^{\mathrm{M}} q^{\mathrm{I}},$$

et

$$\mathrm{A}^n q^{nj} \times \mathrm{A}^{n'} q^{n'j'} \times \ldots = \mathrm{A}^{n+n'+\cdots} \times q^{nj+n'j'+\cdots} = \mathrm{A}^{\mathrm{M}} q^{\mathrm{I}}.$$

Puisque les deux produits ainsi transformés deviennent identiques, leur différence ne pouvait donc être primitivement qu'un multiple de D.

Il est à remarquer qu'on doit faire la somme des indices en comptant ceux-ci dans tous les facteurs du premier degré. C'est ainsi que l'indice de

$$r_i^m = r_i \times r_i \times \ldots \times r_i,$$

a dû être considéré comme égal à *mi*.

Cette transformation de r_i^m en $A^m q^{mi}$, à un multiple près de D, peut conduire encore à d'autre résultats.

Ainsi $A^m q^{mi} = A^{m-1} \times A q^{mi}$, ce que nous pouvons remplacer par $A^{m-1} r_{mi}$. Donc r_i^m ne diffère de $A^{m-1} r_{mi}$ que d'un multiple de D.

12. Si dans la progression géométrique : Aq, Aq^2, ... que nous avons considérée jusqu'ici, nous supposons $A = 1$, c'est-à-dire s'il s'agit de la division des puissances successives d'un même nombre par un certain diviseur D, on voit qu'on pourra remplacer r_i par q^i à un multiple près de D. Mais r_1^i peut être aussi remplacé par q^i. Donc r_1^i et r_i ne diffèrent que d'un multiple de D. Par conséquent, r_i^n, r_1^{in}, r_{in} et r_n^i ne diffèrent aussi que par des multiples de D, c'est-à-dire que dans toute relation établissant un caractère de divisibilité par D, il sera permis de faire passer un indice quelconque en exposant, ou réciproquement; ainsi r_{12}, r_3^4, r_4^3, r_1^{12} ne diffèrent que par des multiples de D. Par conséquent aussi, dans tout calcul de ce genre, *on pourra opérer sur les indices comme on opère sur les exposants;* par exemple, on remplacera $r_2^3 \times r_5^4$ par $r_6 \times r_{20}$ ou par r_{26}. Cette remarque est capitale; elle sera fréquemment employée dans ce qui va suivre. Elle est d'une application bien facile, et s'étend même, dans certains cas, aux fonctions de formes fractionnaires qu'on sait devoir être entières, après les opérations effectuées. Ainsi, supposons que nous sachions que $\frac{aD + r_n}{bD + r_p}$ est un nombre entier, D étant premier. Cette expression ne pourra avoir qne la forme $C.D + r_{n-p}$. En effet, soit $\frac{aD + r_n}{bD + r_p} = C.D + x$. On tire de là : $r_n = m.D + r_p \times x$. Or on sait que $r_n = m.D + r_p \times r_{n-p}$. Donc $r_p \times x - r_p r_{n-p} = m.D$, ou $r_p(x - r_{n-p}) = m.D$;

ce qui nous montre, puisque D est premier et que r_p n'est pas divisible par D, que $x = m.\mathrm{D} + r_{n-p}$. Cette conclusion subsiste toujours lorsque D est simplement premier avec le nombre q qu'on a élevé aux diverses puissances.

Car, dans ce cas encore, r_p ne saurait avoir de facteur commun avec D ; on a, en effet

$$q^p = m.\mathrm{D} + r_p.$$

Donc si r_p et D avaient un facteur commun α, il appartiendrait aussi à q^p, ce qui serait contraire à l'hypothèse.

13. *Si l'on divise les puissances successives de deux nombres quelconques q et q' par un diviseur quelconque* D *de* $qq' - 1$, *deux restes correspondants* r_p *et* r'_p *donneront par leur produit un multiple du diviseur*, $+1$.

Car, soit

$$\mathrm{D} = \frac{qq' - 1}{\mathrm{N}};$$

de là

$$qq' = m.\mathrm{D} + 1,$$

$$q^p q'^p = m.\mathrm{D} + 1,$$

et

$$r_p r'_p = m.\mathrm{D} + 1.$$

On verrait d'une façon analogue que si D est un diviseur de $qq' + 1$, $r_p \times r'_p$ sera un multiple de D, $+1$, si p est pair, et un multiple de D, -1, si p est impair.

Si l'on considère plusieurs progressions : $q, q^2, \ldots$, $q', q'^2, \ldots$, $q'', q''^2, \ldots, \ldots$, et que le diviseur D soit un sous-multiple de $q \times q' \times q'' \times \ldots$, -1, le produit $r_p r'_p r''_p \ldots$ sera un multiple du diviseur, $+1$; on s'en assurerait de la même manière. Si, en particulier, on suppose $q = q' = q'' = \ldots$, on retombe sur ce résultat, que r_p^n ou r_{np} sera un multiple du diviseur, $+1$, si ce

diviseur est sous-multiple de $q^n - 1$. On verrait aussi sans plus de peine que, D étant pris de la forme $\frac{q^n+1}{N}$, on aura r_p^n ou $r_{np} = m.D \pm 1$, suivant que p sera pair ou impair.

14. Nous avons jusqu'à présent considéré les restes de Aq, $Aq^2, \ldots$, divisés par un même nombre D, indépendamment de toute loi à laquelle ils satisfassent nécessairement, et nous sommes arrivés néanmoins à établir certaines propriétés. Entrant maintenant dans un nouvel ordre d'idées, nous rappellerons que la suite indéfinie des restes qu'on obtient de la sorte prend un caractère périodique, soit dès l'origine des opérations, soit à partir d'un certain moment.

Remarquons d'abord qu'on peut supposer $A < D$; car si l'on a $A > D$ et $= m.D + A'$, la suite des restes dus à Aq, $Aq^2, \ldots$ sera la même que celle due à $A'q$, $A'q^2, \ldots$, où $A' < D$.

En second lieu, on peut supposer que A et D sont premiers entre eux. Soit en effet α leur plus grand commun diviseur, et $\frac{A}{\alpha} = A'$, $\frac{D}{\alpha} = D'$. A' et D' sont premiers entre eux. De plus, on a $Aq^m = m.D + r_m$; A et D étant divisibles par α, r_m le sera aussi, et on aura $r_m = r'_m \alpha$. Donc $A'\alpha q^m = m.\alpha D' + \alpha r'_m$, d'où $A'q^m = m.D' + r'_m$. En divisant les termes de la suite, $A'q$, $A'q^2, \ldots$ par D', on obtiendra donc la suite des restes r'_1, $r'_2, \ldots$, qui, étant multipliés par α, donneront les restes cherchés, r_1, $r_2, \ldots$.

15. Considérons maintenant la suite des restes dans le cas le plus général, celui où cette suite est périodique mixte. Supposons que le nombre des restes non pério-

diques soit $n+1$, en y comprenant comme premier reste $r_0 = A$, et que le nombre des termes de la période soit p. La suite générale sera

$$r_0 r_1 \ldots r_n r_{n+1} r_{n+2} \ldots r_{n+p} r_{n+p+1} \ldots .$$

On aura

$$r_{n+1} = r_{n+p+1}, \quad r_{n+2} = r_{n+p+2},$$

en général

$$r_{N+p} - r_N = 0,$$

pourvu que $N \geq n+1$. Donc

$$Aq^{N+p} - Aq^N = Aq^N(q^p - 1) = m.D.$$

Or D renferme des facteurs premiers appartenant à q et d'autres qui lui sont étrangers. Soit D′ l'ensemble des premiers, D″ l'ensemble des autres. Il faut, comme on le voit par ce qui précède, puisque A et D d'une part, q^N et $q^p - 1$ de l'autre sont premiers entre eux, que l'on ait $q^N = m.D'$, et $q^p - 1 = m.D''$.

La plus petite valeur de N satisfaisant à la première de ces deux relations fournit le nombre $n+1$ des chiffres de la partie non périodique; et la plus petite valeur de p satisfaisant à la seconde donne celui des chiffres de la période.

Si l'on considère un quelconque r_{n+1+k} des restes qui appartiennent à la partie périodique, on a

$$Aq^{n+1+k} = m.D + r_{n+1+k} = m.D'D'' + r_{n+1+k},$$

$$(\alpha) \qquad Aq^{n+1}.q^k = m.D'D'' + r_{n+1+k}.$$

Puisque q^{n+1} est divisible par D′, il en sera de même de r_{n+1+k}. Soit $D'r'_k = r_{n+1+k}$. Il viendra, en divisant par D′ l'égalité (α),

$$\frac{Aq^{n+1}}{D'} \times q^k = m.D'' + r'_k.$$

Si $\frac{Aq^{n+1}}{D'} = m.D'' + A'$, on voit que la suite des restes

périodiques s'obtiendra en divisant les termes de la suite A', $A'q$, $A'q^2$,... par D'' et en multipliant par D' tous les résultats ainsi obtenus. Nous ramenons ainsi l'étude des propriétés au cas où la période est simple. Aussi, dans les numéros suivants, supposerons-nous toujours qu'il en est ainsi.

Il n'est pas inutile de remarquer qu'on retrouve, par les raisonnements ci-dessus, les propriétés servant de point de départ à la théorie des fractions périodiques, et cela par la seule considération des restes. On voit, par exemple, que la période est simple, lorsque le dénominateur et la base q sont des nombres premiers entre eux ; que, dans le cas contraire, en débarrassant le dénominateur de tous ses facteurs communs avec q, et cherchant la période due au quotient, elle aura le même nombre de termes que celle de la fraction donnée. Enfin, on retombe sur les relations qui fournissent le nombre des chiffres de la période et le nombre des chiffres non périodiques.

(*La suite prochainement.*)