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. 221-229

<http://www.numdam.org/item?id=NAM_1870_2_9__221_1>

MÉMOIRE SUR CERTAINES PROPRIÉTÉS DES RÉSIDUS NUMÉRIQUES;

PAR MM. A. LAISANT ET ÉTIENNE BEAUJEUX.

1. Soient $r_1, r_2, \ldots, r_n, \ldots$ les *restes* ou *résidus* qu'on obtient, en divisant par un même diviseur entier et positif D, les termes de la progression géométrique

$$Aq,\ Aq^2, \ldots,\ Aq^n, \ldots$$

où A et q sont entiers et positifs. On aura

$$Aq = m.D + r_1,\ Aq^2 = m.D + r_2, \ldots,\ Aq^n = m.D + r_n, \ldots.$$

Donc, dans toute relation établissant un caractère de divisibilité par D, on pourra remplacer respectivement Aq, $Aq^2, \ldots, Aq^n, \ldots$ par $r_1, r_2, \ldots, r_n, \ldots$ et inversement.

2. Si l'on a

$$(I) \qquad \alpha_0 + \alpha_1 q + \alpha_2 q^2 + \ldots + \alpha_p q^p = m.D,$$

il viendra, en multipliant par Aq^n,

$$\alpha_0 Aq^n + \alpha_1 Aq^{n+1} + \ldots + \alpha_p Aq^{n+p} = m.D,$$

et, par suite, d'après la remarque précédente,

$$(II) \qquad \alpha_0 r_n + \alpha_1 r_{n+1} + \ldots + \alpha_p r_{n+p} = m.D.$$

Ainsi, toutes les fois qu'on aura la relation (I), on pourra en conclure la relation (II), qui aura lieu quel que soit n; et réciproquement, lorsque cette dernière existera pour une certaine valeur de n, pourvu que Aq^n soit premier avec D, il en sera de même pour toute autre valeur, et on pourra en déduire la relation (I).

Dans ces relations, il est clair qu'on peut remplacer D par un quelconque d de ses diviseurs, car tout multiple de D le sera aussi de d.

Ces remarques permettent déjà de trouver des lois en grand nombre, auxquelles satisfont les restes provenant d'un diviseur donné, et réciproquement de trouver les diviseurs qui peuvent fournir des restes satisfaisant à une loi déterminée, analogue à la relation (II) ci-dessus.

Ainsi, supposons $q = 10$. Soit $D = 17$: on a

$$2.10 - 3 = m.17,\ 5\ 10 + 1 = m.17,\ 10^2 + 2.10 - 1 = m.17.$$

Donc aussi

$$2r_{n+1} - 3r_n = m.17, \quad 5r_{n+1} + r_n = m.17,$$
$$r_{n+2} + 2r_{n+1} - r_n = m.17,$$

résultats qu'on vérifierait sans peine.

De même, si l'on demande les diviseurs, tels que l'on ait

$$r_{n+3} - r_{n+2} - r_n = m.D,$$

il suffit de former le nombre $10^3 - 10^2 - 1 = 899$ et ses diviseurs 29 et 31. Ces trois nombres satisfont à la question.

Enfin, ces remarques permettent de former immédiatement des multiples d'un nombre donné, et réciproquement de vérifier si un nombre est divisible par un autre. Ainsi, dans l'exemple précédent, on trouve les trois restes consécutifs 4, 6, 9, qui satisfont à la relation

$$2.9 + 2.6 + 1.4 = 34 = m.17.$$

Donc

$$2.10^2 + 2.10 + 1 = 221 = m.17.$$

En outre, supposons qu'on veuille savoir si 153 est ou non multiple de 17. Je prends trois restes consécutifs, les mêmes que ci-dessus, par exemple, et je forme l'expression

$$1.9 + 5.6 + 3.4 = 51 = m.17.$$

Donc

$$153 = m.17.$$

3. Si la relation qu'on se donne est $r_{n+p} - r_n = 0$, c'est-à-dire si les restes doivent se reproduire périodiquement de p en p, on voit que $q^p - 1$ doit être un multiple du diviseur, résultat connu auquel on est directement amené ici. Nous aurons occasion plus loin d'étudier particulièrement ces restes périodiques.

4. Si le diviseur D s'écrit $\alpha_p \alpha_{p-1} \ldots \alpha_1 \alpha_0$ dans le système de numération dont la base est q, on a

$$D = \alpha_p q^p + \alpha_{p-1} q^{p-1} + \ldots + \alpha_1 q + \alpha_0,$$

et par suite (2)

$$\text{(III)} \quad \alpha_p r_{n+p} + \alpha_{p-1} r_{n+p-1} + \ldots + \alpha_1 r_{n+1} + \alpha_0 r_n = m.D.$$

Ainsi, *écrivant un nombre de restes consécutifs quelconques, égal à celui des chiffres du diviseur, plaçant respectivement au-dessous les chiffres du diviseur dans leur ordre inverse et effectuant les produits indiqués, la somme de ces produits sera un multiple du diviseur.*

Par exemple, 134, appliqué comme diviseur aux puissances successives de 10, donne lieu aux trois restes consécutifs

	62	84	36	
J'écris au-dessous	4	3	1	
et	248	$+ 252$	$+ 36 = 536 = m.134.$	

Il est évident, d'après ce qui précède, que la même propriété subsisterait en désignant par $\alpha_p, \ldots, \alpha_1, \alpha_0$ les chiffres d'un multiple quelconque de D.

Enfin, comme rien ne suppose dans notre raisonnement que les coefficients $\alpha_0, \alpha_1, \ldots$ soient plus petits que la base q, on voit que, dans le cas pris ci-dessus pour exemple, on peut écrire

$$134 = 1.10^2 + 34.10^0,$$

ou

$$134 = 13.10 + 4.10^0,$$

d'où résulte que les chiffres du diviseur peuvent être disposés au-dessous des restes des deux manières suivantes, écrites, pour plus de commodité, dans l'ordre inverse du

précédent, qui est l'ordre direct des chiffres du diviseur :

$$(1)\quad \begin{cases} 36 & 84 & 62 \\ 1 & 0 & 34 \end{cases}$$

$$36 + 0 + 2108 = 2144 = m.134$$

$$(2)\quad \begin{cases} 36 & 84 & 62 \\ 0 & 13 & 4 \end{cases}$$

$$0 + 1072 + 248 = 1340 = m.134$$

Par suite, *ayant écrit les restes par ordre d'indices décroissants de gauche à droite et les chiffres d'un multiple quelconque du diviseur au-dessous, comme on l'a vu précédemment, on peut déplacer ceux-ci de manière à les masser* SUR LA DROITE, *à volonté, sans que la propriété cesse d'être vraie.*

5. *Si la base du système de numération est* B, *différent de* q, *et qu'on divise successivement* Aq, $Aq^2, \ldots$ *par un diviseur quelconque* D *de* $q - B$, *la même propriété aura lieu.* Car soit

$$D = \frac{q - B}{N},$$

d'où

$$q = N.D + B,$$

et

$$q^2 = m.D + B^2, \ldots, q^n = m.D + B^n, \ldots.$$

De là

$$Aq^n = m.D + AB^n, \quad \text{et} \quad r_n = m.D + AB^n,$$
$$Aq^{n+1} = m.D + AB^{n+1}, \quad r_{n+1} = m.D + AB^{n+1},$$
$$\ldots\ldots\ldots\ldots\ldots \quad \ldots\ldots\ldots\ldots\ldots$$
$$Aq^{n+p} = m.D + AB^{n+p}, \quad r_{n+p} = m.D + AB^{n+p}.$$

Multipliant respectivement par $\alpha_0, \alpha_1, \ldots, \alpha_p$, et ajoutant, on tombe sur la relation (III).

On verrait, d'une manière semblable, *que les divisions successives* Aq, Aq^2, ... *par un diviseur de* $q + B$ *conduisent à une loi analogue, dans laquelle il faudrait seulement* ALTERNER LES SIGNES DES TERMES, *ou, ce qui revient au même,* PRENDRE ALTERNATIVEMENT LES RESTES PAR DÉFAUT ET PAR EXCÈS, *en leur conservant le signe* +.

On pourrait ici encore masser les chiffres sur la droite, ou en général du côté des puissances les plus faibles de la base, à la condition de conserver à chaque emplacement de chiffres dont on se sert le signe + ou — dont il était primitivement affecté. Ainsi, en divisant par $10 + 7 = 17$, les puissances successives de 7, on obtient les restes successifs 7, 15, 3,.... Si je prends un multiple quelconque de 17, tel que 153, et que j'écrive

+	−	+
3	15	7

puis

1	5	3

j'aurais un multiple de 17 en faisant la somme des produits indiqués avec leurs signes. Je pourrais aussi bien écrire

+	−	+
3	15	7
1	0	53

ou bien

+	−	+
3	15	7
0	15	3

et encore, en prenant les restes par excès et par défaut,

3	2	7
1	5	3
3	2	7
1	0	53
3	2	7
0	15	3

on arriverait toujours ainsi à des multiples de 17. Nous ne nous arrêterons pas à la démonstration de cette règle, qui résulte de ce que rien ne suppose les chiffres employés inférieurs à la base du système de numération. Elle est d'ailleurs applicable aux propriétés analogues que nous allons étudier maintenant.

6. Soit toujours la progression Aq, Aq^2, Aq^3, ... *Si l'on en divise les termes successifs par un diviseur quelconque* D *de* $Bq - 1$, B *étant la base du système de numération employée, et qu'on écrive sous des restes consécutifs quelconques les divers chiffres de* D DANS LEUR ORDRE NATUREL, *la somme des produits indiqués sera un multiple de* D.

Soit, en effet,

$$D = \frac{Bq - 1}{N};$$

de là

$$B = \frac{ND + 1}{q}.$$

Soient, en outre, α_0, α_1, α_2, ..., α_n les divers chiffres de D, de telle sorte qu'on ait

$$D = \alpha_n B^n + \alpha_{n-1} B^{n-1} + \ldots + \alpha_1 B + \alpha_0.$$

Si nous substituons à B sa valeur précédente, il vient

$$D = \alpha_n \frac{(ND+1)^n}{q^n} + \alpha_{n-1} \frac{(ND+1)^{n-1}}{q^{n-1}} + \ldots + \alpha_1 \frac{(ND+1)}{q} + \alpha_0,$$

$$q^n D = \alpha_n (ND+1)^n + \alpha_{n-1} (ND+1)^{n-1} + \ldots + \alpha_1 (ND+1) q^{n-1} + \alpha_0 q^n.$$

Réunissant, dans le second membre, tous les multiples de D, après qu'on a effectué tous les développements,

$$\alpha_n + \alpha_{n-1} q + \ldots + \alpha_1 q^{n-1} + \alpha_0 q^n = m.D.$$

D'où multipliant par $A q^p$, p étant quelconque,

$$\alpha_n A q^p + \alpha_{n-1} A q^{p+1} + \ldots + \alpha_1 A q^{p+n-1} + \alpha_0 A q^{p+n} = m . D.$$

Si l'on remplace à présent $A q^p \ldots$ par $r_p, \ldots$, suivant la remarque faite au n° 1, il vient

$$\alpha_n r_p + \alpha_{n-1} r_{p+1} + \ldots + \alpha_1 r_{p+n-1} + \alpha_0 r_{p+n} = m . D;$$

c'est présisément l'égalité en démonstration.

Un calcul semblable ferait voir qu'*en prenant pour* D *un diviseur quelconque de* $Bq + 1$, *on aurait une propriété analogue à la condition de* PRENDRE ALTERNATIVEMENT LES RESTES AVEC LES SIGNES + OU —, OU PAR EXCÈS ET PAR DÉFAUT SUCCESSIVEMENT, *comme plus haut.*

De plus, on verrait facilement que les mêmes propriétés subsisteraient en écrivant à la place des chiffres de D ceux d'un multiple quelconque de D.

7. *Si* B *étant toujours la base du système de numération, on prend comme diviseur un sous-multiple quelconque de* $q^p - B$, *on aura une propriété analogue à celle du n° 5; seulement, au lieu de prendre des restes consécutifs, on devra écrire des restes* SE SUIVANT DE p EN p. En effet, soient

$$D = \frac{q^p - B}{N}$$

et en outre

$$D = \alpha_n B^n + \ldots + \alpha_1 B + \alpha_0,$$

on aura

$$q^p = ND + B.$$

De là

$$q^{2p} = m . D + B^2,$$
$$q^{3p} = m . D + B^3,$$
$$\ldots\ldots\ldots\ldots,$$
$$q^{np} = m . D + B^n.$$

Multipliant toutes ces égalités respectivement par $\alpha_1 \mathrm{A}q^m$, $\alpha_2 \mathrm{A}q^m, \ldots, \alpha_n \mathrm{A}q^m$, et les ajoutant entre elles et avec l'identité $\alpha_0 \mathrm{A}q^m = \mathrm{A}q^m \alpha_0$, il vient

$$\alpha_0 \mathrm{A}q^m + \alpha_1 \mathrm{A}q^{m+p} + \alpha_2 \mathrm{A}q^{m+2p} + \ldots + \alpha_n \mathrm{A}q^{m+np} = m.\mathrm{D}.$$

Remplaçant maintenant $\mathrm{A}q^m$, $\mathrm{A}q^{m+p}$,... par r_m, r_{m+p},..., on a la relation en démonstration

$$\alpha_0 r_m + \alpha_1 r_{m+p} + \alpha_2 r_{m+2p} + \ldots + \alpha_n r_{m+np} = m.\mathrm{D}.$$

La division par $\dfrac{q^p + \mathrm{B}}{\mathrm{N}}$ *donnerait lieu à une propriété analogue*, EN PRENANT SUCCESSIVEMENT LES RESTES PAR EXCÈS ET PAR DÉFAUT.

Enfin, en prenant pour diviseur $\dfrac{\mathrm{B}q^p - 1}{\mathrm{N}}$ *ou* $\dfrac{\mathrm{B}q^p + 1}{\mathrm{N}}$, *on aurait deux propriétés analogues à celles du n° 6, avec cette même restriction que* LES RESTES DEVRAIENT ÊTRE PRIS DE p EN p *et non pas consécutifs.*

(*La suite prochainement.*)