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. 302-307

<http://www.numdam.org/item?id=NAM_1870_2_9__302_1>

MÉMOIRE SUR CERTAINES PROPRIÉTÉS DES RÉSIDUS NUMÉRIQUES

(suite, voir 2e série, t. IX, p. 221 et 271);

PAR MM. A. LAISANT ET ÉTIENNE BEAUJEUX.

16. Soit donc une progression géométrique

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

dont les termes, divisés par D, donnent lieu à une simple période de n restes

$$r_1, \quad r_2, \ldots, \quad r_n, \ldots.$$

De sorte que $r_n = r_0 = A$, $r_{n+1} = r_1$, $r_{n+2} = r_2, \ldots$, en général $r_{kn+p} = r_p$. On voit que dans toute relation établissant un caractère de divisibilité par D, on pourra remplacer un reste quelconque r_p par Aq^p, puis ajouter à p ou en retrancher un multiple quelconque de n. Nous aurons en premier lieu le théorème suivant :

Le produit $r_1 r_2 \ldots r_n$ de tous les restes de la période est égal à un multiple de D, + A^n *si n est impair, et à un multiple de* D, — A^n *si n est pair.*

En effet, remplaçant r_1 par Aq, r_2 par $Aq^2, \ldots,$ r_n par Aq^n, le produit est ramené à

$$A^n q^{1+2+\ldots+n} = A^n q^{\frac{n(n+1)}{2}}.$$

Soit d'abord n impair, on a (15)

$$q^n = m.D + 1;$$

donc

$$(q^n)^{\frac{n+1}{2}} = q^{\frac{n(n+1)}{2}} = m.D + 1,$$

et

$$A^n q^{\frac{n(n+1)}{2}} = m.D + A^n.$$

Si, au contraire, n est pair, il vient

$$q^{\frac{n}{2}} = m.D - 1,$$

et

$$q^{\frac{n(n+1)}{2}} = m.D - 1;$$

donc

$$A^n q^{\frac{n(n+1)}{2}} = m.D - A^n.$$

Corollaires. — 1° Si l'on était parti de la progression $q, q^2, \ldots,$ il suffirait de faire $A = 1$ dans les résultats ci-dessus, de sorte que le produit des restes eût été égal à un multiple de D, + ou — 1, selon que n est impair ou pair.

2° Il en serait de même si l'on avait $A^n - 1 = m.D$; ce qui aurait lieu, par exemple, si la fraction $\frac{1}{D}$, convertie dans le système de base A, conduisait aussi à une période de n chiffres.

3° Si $n = D - 1$, ce qui ne peut avoir lieu que lorsque

D est premier, il en sera encore de même, car

$$A^{D-1} - 1 = m.D,$$

d'après le théorème de Fermat.

4° Si $\frac{1}{D}$ convertie dans le système de base A donne Qn chiffres à la période, on a $A^n = m.D - 1$, et le produit sera un multiple de D + ou -1, selon que n sera pair ou impair

17. *La somme de tous les restes composant la période est égale à un multiple de* D.

Si nous remplaçons, en effet, $r_1, r_2, \ldots, r_n$ comme ci-dessus, il vient

$$Aq + Aq^2 + \ldots + Aq^n = Aq\left(\frac{q^n - 1}{q - 1}\right).$$

Cette expression représente un multiple de D, car D entre comme facteur dans $q^n - 1$, et ne saurait entrer dans $q - 1$.

18. *La somme des puissances semblables des restes composant la période est égale à un multiple de* D, *pourvu que l'exposant commun ne soit pas multiple du nombre des restes composant la période.*

Car si nous remplaçons encore $r_1, r_2, \ldots$ par $Aq, Aq^2, \ldots$,

$$r_1^p + r_2^p + r_3^p + \ldots + r_n^p$$

sera remplacé par

$$A^p q^p + A^p q^{2p} + \ldots + A^p q^{np} = A^p q^p \frac{q^{np} - 1}{q^p - 1}.$$

Or $q^{np} - 1 = m.D$ et $q^p - 1 \gtrless m.D$, puisque $p \gtrless m.D$.

Donc, etc.

Si p était multiple de n, la somme ci-dessus serait évidemment de la forme $m.D + n$, car chacun des termes $r_1^p, \ldots$ serait égal à un multiple de D, + 1, et il y en a n.

19. On pourrait voir d'une façon analogue que *la somme des produits* r_1r_2, r_2r_3, ..., r_nr_1 *est un multiple de* D; qu'il en est de même de *la somme de tous les produits deux à deux des restes*. Mais nous allons préférablement établir ce théorème général qui comprend les précédents comme cas très-particuliers :

Si l'on forme une fonction symétrique entière quelconque des restes $r_1r_2\ldots r_n$, *sa valeur numérique sera multiple de* D, *pourvu qu'il n'y ait aucun terme dans la fonction dont le degré soit multiple du nombre des termes de la période.*

Soit en effet $Br_i^l r_j^m \ldots r_k^p$ un des termes de cette fonction. Elle devra renfermer aussi tous ceux qu'on déduirait de ceux-là, en faisant passer respectivement les indices par les valeurs

$$\begin{aligned} &i+1,\ i+2,\ \ldots,\ i-1,\\ &j+1,\ j+2,\ \ldots,\ j-1,\\ &\ldots\ldots\ldots\ \ldots\ldots\ldots,\\ &k+1,\ k+2,\ \ldots,\ k+1. \end{aligned}$$

Mais si l'on se rappelle que, d'une façon générale, on a

$$r_k = r_{k+n},$$

on voit que les valeurs successives à donner aux indices s'obtiennent en augmentant successivement les premiers de $1, 2, \ldots, (n-1)$ unités. Ainsi le terme considéré $Br_i^l r_j^m \ldots r_k^p$, entraîne l'existence des suivantes :

$$\begin{aligned} &Br_{i+1}^l r_{j+1}\ldots r_{k+1}^p,\\ &Br_{i+2}^l r_{j+2}^m\ldots r_{k+2}^p,\\ &\ldots\ldots\ldots\ldots,\\ &Br_{i+n-1}^l r_{j+n-1}^m\ldots r_{k+n-1}^p. \end{aligned}$$

Mais, en appelant N le degré commun $l+m+\ldots+p$

des termes ci-dessus, on voit qu'ils peuvent être remplacés respectivement par

$$\begin{array}{l} BA^N q^{li+mj+\ldots+pk}, \\ BA^N q^{l(i+1)+m(j+1)+\ldots+p(k+1)}, \\ BA^N q^{l(i+2)+m(j+2)+\ldots+p(k+2)}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ BA^N q^{l(i+n-1)+m(j+n-1)+\ldots+p(k+n-1)}. \end{array}$$

La somme est donc

$$\begin{aligned} & BA^N q^{li+mj+\ldots+pk}\left[1 + q^N + q^{2N} + \ldots + q^{(n-1)N}\right] \\ & = BA^N q^{li+mj+\ldots+pk}\left(\frac{q^{nN}-1}{q^N-1}\right). \end{aligned}$$

Cette somme est multiple de D; le dénominateur ne l'étant pas en raison de l'hypothèse, tandis que $q^{nN}-1$ l'est au contraire. Il en sera de même de toutes celles qui proviendront d'un autre terme non encore considéré. Donc la valeur numérique de la fonction sera aussi un multiple du diviseur.

Remarquons, en raison même de la démonstration précédente, que la fonction pourrait n'être pas complétement symétrique sans que le théorème cessât d'avoir lieu. Il suffirait qu'elle se composât de groupes de n termes, tels qu'on pût de l'un déduire les autres en faisant successivement passer les indices par toutes les valeurs comprises entre 1 et n, inclusivement, en suivant l'ordre circulaire.

20. Le théorème précédent nous montre que la somme des n restes, la somme de leurs produits 2 à 2, de leurs produits 3 à 3,..., de leurs produits $n-1$ à $n-1$, sont autant de multiples du diviseur D. Si nous considérons en particulier le cas où $A=1$, nous avons vu en outre (16) que le produit des n restes est un mul-

tiple de D, + ou — 1, selon que n est pair ou impair. Il y a là un lien curieux entre les racines de l'équation indéterminée

$$(a) \qquad x^n - 1 = m.\mathrm{D},$$

et celles de l'équation algébrique

$$(b) \qquad x^n - 1 = 0.$$

On voit, en effet, qu'en appelant $r_1, r_2, \ldots, r_n$ comme nous l'avons fait, les racines de la première, et $\rho_1, \rho_2, \ldots, \rho_n$ celles de la seconde, on a

$$\begin{aligned}
&\Sigma r_1 = m.\mathrm{D}, && \Sigma \rho_1 = 0,\\
&\Sigma r_1 r_2 = m.\mathrm{D}, && \Sigma \rho_1 \rho_2 = 0,\\
&\Sigma r_1 r_2 r_3 = m.\mathrm{D}, && \Sigma \rho_1 \rho_2 \rho_3 = 0,\\
&\ldots\ldots\ldots\ldots, && \ldots\ldots\ldots,\\
&\Sigma r_1 \ldots r_{n-1} = m.\mathrm{D}, && \Sigma \rho_1 \ldots \rho_{n-1} = 0,\\
&r_1 r_2 \ldots r_n = m.\mathrm{D} \pm 1, && \rho_1 \rho_2 \ldots \rho_n = \pm 1.
\end{aligned}$$

Si n est impair, 1 est racine de l'équation (b), et toutes les autres racines sont imaginaires. Si n est pair, cette équation admet au contraire les racines + 1 et — 1. Dans ces deux cas respectivement, l'équation (a) a pour racine $r_n = 1$, ou $r_n = 1$ et $r_{\frac{n}{2}} = \mathrm{D} - 1$. De toute façon, on voit qu'il existe entre les racines de l'équation (b), d'une part, et entre celles de l'équation (a), de l'autre, des relations exactement semblables à des multiples près de D. Cette remarque nous paraît pouvoir être ajoutée aux lumineuses considérations développées par Poinsot dans son *Mémoire sur l'application de l'algèbre à la théorie des nombres*, et dans ses *Réflexions sur les principes fondamentaux de la théorie des nombres*.

(*La suite prochainement.*)
