

E. PROUHET

Mémoire sur la théorie des résidus dans les progressions géométriques

Nouvelles annales de mathématiques 1^{re} série, tome 5 (1846), p. 175-187

http://www.numdam.org/item?id=NAM_1846_1_5__175_1

© Nouvelles annales de mathématiques, 1846, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). 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/>

MÉMOIRE

sur la théorie des résidus dans les progressions géométriques.

PAR M. E. PROUHET,

Professeur au collège royal d'Auch.

1. Pour bien faire comprendre l'objet de ce mémoire, nous allons rappeler quelques théorèmes, et définir quelques locutions dont nous ferons un continuel usage.

Soit :

$$a, a', a^3, a^4, \dots a^n, a^{n+1}, \dots$$

une progression indéfinie comprenant les puissances entières.

et positives de l'entier a ; si on divise tous ses termes par le nombre P premier avec a , on obtiendra une certaine suite de résidus, dont l'unité fera nécessairement partie. Si a^n est le premier terme de la progression qui donne le résidu 1, tous les résidus précédents seront différents entre eux ; au delà, ils se reproduiront dans le même ordre. On sait d'ailleurs que n sera un diviseur de l'indicateur de P , c'est-à-dire du nombre qui indique combien il y a d'entiers inférieurs et premiers à P .

2. Nous appellerons *période de a par rapport à P* , l'ensemble des résidus fournis par les termes $a, a^2, a^3, \dots, a^n$; *système de périodes*, l'ensemble des périodes de tous les nombres inférieurs et premiers à P ; le nombre P sera dit la *base* du système.

Voici par exemple, toutes les périodes du système dont la base est 13.

1,
 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1.
 3, 9, 1.
 4, 3, 12, 9, 10, 1.
 5, 12, 8, 1.
 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1.
 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1.
 8, 12, 5, 1.
 9, 3, 1.
 10, 9, 12, 3, 4, 1.
 11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1.
 12, 1.

3. La formation d'un pareil tableau n'offre pas de difficulté. On obtient chaque résidu en multipliant le précédent par le nombre qui engendre la période, et supprimant tous les multiples de la base contenus au produit. On peut cepen-

dant n'employer que l'addition, en procédant de la manière suivante :

Soit proposé par exemple, de trouver la période de 3 dans le système dont la base est 25. A cet effet j'écris ces deux lignes :

Coefficients

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24.

Résidus

3, 6, 9, 12, 15, 18, 21, 24, 2, 5, 8, 11, 14, 17, 20, 23, 1, 4, 7, 10, 13, 16, 19, 22.

La première renferme tous les nombres inférieurs à 25 ; la seconde se forme en ajoutant successivement 3 à lui-même, et retranchant 25 de la somme s'il y a lieu. Cela fait, le second terme de la période sera le résidu 9 correspondant au coefficient 3 ; le deuxième terme sera le résidu 2 correspondant au coefficient 9 ; le troisième terme sera le résidu 6 correspondant au coefficient 2, et ainsi de suite. De cette manière on obtient pour la période de 3 par rapport à 25, les nombres :

3, 9, 2, 6, 18, 4, 12, 11, 8, 24, 22, 16, 23, 19, 7, 21, 13, 14, 17, 1.

Au reste, on n'aura besoin de former directement que la moitié des périodes du système ; car si la somme de deux nombres est égale à la base, il est facile de voir que les termes de même rang de leurs périodes sont égaux si ce rang est pair ; et donnent une somme égale à la base, si ce rang est impair.

Nous verrons plus loin d'autres moyens de simplifier la formation d'un système de périodes.

4. Nous appellerons *racine primitive de P par rapport à n*, tout nombre qui, dans le système P engendrera une période de n termes.

Nous appellerons plus simplement *racine primitive du système* ou *de la base P*, la racine primitive de P par rapport

à (P), c'est-à-dire tout nombre dont la période comprendra tous les entiers inférieurs et premiers à la base.

Ces définitions comprennent comme cas particulier la définition d'Euler, et concordent avec celle de M. Poinso, sauf le point de vue spécial auquel nous nous plaçons.

Enfin, une période sera dite *complète*, quand elle renfermera tous les nombres inférieurs et premiers à la base.

5. Cela posé, l'objet de ce mémoire est l'étude détaillée et complète autant que possible des différents systèmes de périodes. Les théorèmes que nous démontrerons ne sont pas nouveaux; à quelques développements près, ils se trouvent dans l'ouvrage de Legendre, mais séparés et déduits de théories différentes. Nous avons cru utile de les réunir et de les déduire les uns des autres d'une manière uniforme. Ce travail aura en outre l'avantage de faciliter aux jeunes lecteurs de ce journal, l'accès de la théorie des nombres, partie difficile et encore peu cultivée des mathématiques, et sur laquelle paraît aujourd'hui reposer l'avenir de la science.

N. B. — Dans tout ce qui va suivre P désignera constamment la base d'un système de périodes, et p un nombre premier.

§ I. Propriétés générales des systèmes de périodes (*).

6. *Théorème.* Dans toute période (l'unité non comprise), les termes à égale distance des extrêmes sont associés par rapport à la base.

Soit n le nombre des termes de la période de a , en sorte que l'on ait

$$a^n = P + 1,$$

deux termes également éloignés de a et de a^{n-1} , seront (m étant $< n$)

$$a^m \qquad a^{n-m}.$$

(*) Cette théorie des résidus a été créée par Euler (Voir N. comm. Pétersb., t. V).

Le produit de ces deux puissances étant a^n et par conséquent $\dot{P} + 1$, le produit de leurs résidus sera aussi $\dot{P} + 1$. Donc ces résidus sont associés. C. Q. F. D.

Corollaire 1^{er}. Dans toute période d'un nombre impair de termes (l'unité comprise), le produit de tous les résidus est $\dot{P} + 1$.

Car si on laisse de côté le résidu 1, il reste un nombre pair de termes associés deux à deux. Le produit des résidus pouvant se décomposer en $\frac{n-1}{2}$ facteurs de la forme $\dot{P} + 1$, sera aussi $\dot{P} + 1$.

Corollaire 2. Le produit des résidus d'une période d'un nombre pair de termes est $\dot{P} - 1$, quand la base est une puissance ou le double d'une puissance d'un nombre premier impair.

Car, si on néglige l'unité, il reste un nombre impair de termes associés deux à deux, à l'exception de celui du milieu qui doit être un associé double. Or, d'après l'hypothèse, P ne peut avoir que deux associés doubles 1 et $P - 1$. Le terme du milieu ne peut être 1; autrement la période commencerait plus tôt qu'on ne l'a supposé. Donc ce terme sera $P - 1$. Donc le produit des résidus sera $(\dot{P} + 1)(\dot{P} - 1) = \dot{P} - 1$, C. Q. F. D.

Corollaire 3. Quand la base est une puissance ou le double d'une puissance d'un nombre premier impair, dans toute période d'un nombre pair de termes, les résidus qui occupent le même rang dans chaque demi-période, donnent une somme égale à la base.

En effet on a, comme nous venons de le voir,

$$a^{\frac{n}{2}} = \dot{P} - 1$$

D'où l'on réduit aisément

$$a^{\frac{n+1}{2}} + a = \dot{P}$$

$$a^{\frac{n+2}{2}} + a^2 = \dot{P}$$

$$a^{\frac{n+3}{2}} + a^3 = \dot{P}$$

.

C. Q. F. D.

Corollaire 4°. Un associé double ne peut pas faire partie d'une période d'un nombre impair de termes.

7. Théorème. Deux associés par rapport à la base ont des périodes inverses l'une de l'autre.

Si on désigne par a' l'associé de a par rapport à P , on doit avoir d'après le théorème précédent

$$a^{n-1} = \dot{P} + a'$$

en élevant les deux membres de cette égalité aux puissances 1, 2, 3... n , et supprimant dans l'exposant de a tous les multiples de n , on aura

$$a^{n-1} = \dot{P} + a'$$

$$a^{n-2} = \dot{P} + a'^2$$

$$.$$

$$a^0 = \dot{P} + a'^n$$

Donc les résidus formés par

$$a^{n-1}, a^{n-2}, a^{n-3}, \dots$$

Sont respectivement ceux fournis par

$$a', a'^2, a'^3, \dots \quad \text{C. Q. F. D.}$$

Ce théorème simplifie la construction d'un système de périodes, puisque la période d'un nombre se déduit sans calcul de celle de son associé.

Théorème. Lorsque la somme de deux nombres est un multiple de la base, leurs périodes renferment le même nom-

bre de termes ou bien la période de l'une renferme deux fois plus de termes que la période de l'autre.

Soient a et a' les deux nombres proposés ; n et n' les nombres de termes de leurs périodes, n n'étant pas plus grand que n' . On aura d'après l'hypothèse :

$$a' = \dot{P} - a$$

$$\text{d'où} \quad a^n = \dot{P} + (-1) a^n$$

$$\text{et comme} \quad a^n = \dot{P} + 1$$

$$a^n = \dot{P} + (-1)^n$$

Par conséquent si n est pair, on aura $n'=n$; et si n est impair, $n'=2n$. C. Q. F. D.

On voit par là que n et n' ne peuvent pas être tous les deux impairs et que c'est seulement dans le cas de n pair que les deux périodes peuvent avoir le même nombre de termes.

9. *Théorème. Lorsque le produit de deux nombres augmenté de l'unité est un multiple de la base, leurs périodes se composent d'un même nombre de termes ou bien la période de l'un renferme deux fois plus de termes que la période de l'autre.*

Soient a et a' les deux nombres proposés et a'' l'associé de a par rapport à P . On aura

$$aa' + 1 = \dot{P}$$

$$aa'' - 1 = P$$

$$\text{d'où on tire} \quad a(a' + a'') = \dot{P}$$

et comme a est premier avec P il en résulte

$$a' + a'' = \dot{P}$$

Le théorème précédent est donc applicable à a' et a'' . Mais a et a'' ont même nombre de termes à leurs périodes (7). Donc, etc.

10. *Problème. Une période étant donnée, trouver la période engendrée par chacun de ses résidus.*

Soit b le résidu de rang m dans la période de a , en sorte que

$$a^m = \dot{P} + b$$

Soit x l'exposant de la puissance à laquelle on doit élever b pour obtenir le résidu 1. On aura

$$a^{mx} = \dot{P} + 1$$

Il faut donc que $mx = n$ et par conséquent la plus petite valeur de x propre à satisfaire à la relation

$$b^x = \dot{P} + 1$$

s'obtiendra en cherchant la plus petite valeur de x propre à satisfaire à la relation

$$m^x = n$$

Pour trouver ce nombre désignons par d le p. g. c. d. entre m et n et posons

$$m = dm', n = dn';$$

$m n'$ sera divisible par n et ce sera évidemment le plus petit multiple de m jouissant de cette propriété. Donc le nombre des termes de la période de b sera n' . On pourra donc énoncer la règle suivante :

Un résidu de rang m dans une période de n termes engendre une période dont le nombre des termes s'obtient en divisant n par le p. g. c. d. de m et n .

Reste maintenant à obtenir les termes mêmes de la période de b : il suffira pour cela de prendre les résidus de la période de a de m en m comme si ces nombres étaient écrits circulairement, car on a $b^1 = \dot{0} + a^m$; $b^2 = \dot{P} + a^{2m}$, etc.

Corollaire. Si m est premier avec n , $d=1$; $n'=n$. Donc :

Dans toute période de n termes un résidu dont le rang est indiqué par un nombre premier avec n , engendre une période de n termes : ou suivant une autre manière de s'exprimer, est racine primitive de P par rapport à n .

Remarque 1^{re}. Si dans un système il existe une période n , il en existera au moins $i(n)$.

Remarque 2^e. Une période complète suffit pour obtenir sans calcul toutes les autres périodes du système.

11. Théorème. Si m est premier avec $i(P)$, les résidus obtenus en divisant par P tous les nombres inférieurs et premiers à P élevés à la même puissance m ? sont différents.

Supposons que a^m et b^m donnent le même résidu, on aura

$$a^m - b^m = P$$

soit b' l'associé de b par rapport à P .

Multiplions les deux membres de l'équation par b'^m , nous aurons :

$$(ab')^m - 1 = P$$

Puisque m est premier avec $i(P)$, cette égalité ne peut subsister à moins que

$$ab' - 1 = P$$

mais on a

$$bb' - 1 = P$$

il en résulterait

$$(a-b)b' = P$$

égalité impossible puisque b' est premier avec P et $a-b$ moindre que P .

§ II. Des systèmes de périodes dont la base est un nombre premier.

12. Théorème. Lorsque la base est un nombre premier p , la somme des m^{es} puissances des résidus d'une période de n termes est divisible par la base quand m n'est pas un multiple de n . Soit a un nombre qui dans le système p engendre une période de n termes. Les résidus de la période élevés à la m^{e} puissance donnent les mêmes restes que les termes de la progression

$$a^m, a^{2m}, a^{3m}, \dots, a^{nm}$$

dont la somme

$$a^m \frac{a^{mn} - 1}{a^m - 1}$$

est divisible par p , puisque $a^{mn} - 1 = \dot{p}$ et que $a^m - 1$ ne peut être $\dot{p}$ quand m n'est pas $\dot{n}$. Donc la somme S_m des m^{es} puissances des résidus est aussi divisible par p . C. Q. F. D.

Quand $m = n$, la somme n'est plus divisible par p ; mais comme alors chaque terme est $\dot{p} + 1$, on a

$$S_n = \dot{p} + n.$$

13. *Corollaire. Les sommes de produits 2 à 2, 3 à 3, ... (n-1) à (n-1) des résidus d'une période de n termes sont divisibles par p.*

En effet, si $P_1, P_2, \dots, P_{n-1}$, désignent ces sommes de produits, on aura, k étant $\leq n-1$

$$S_k - P_1 S_{k-1} + P_2 S_{k-2} - \dots \pm P_{k-1} S_1 \mp k P_k = 0$$

De cette égalité et du théorème précédent, on déduit $k P_k = \dot{p}$. Mais k est inférieur à n et par conséquent premier à p : donc

$$P_k = \dot{p}.$$

Cette relation cesse d'avoir lieu si on fait $k = n$, mais il résulte du n° 6 (corol. 1^{er} et 2^e) qu'on a dans ce cas

$$P_n = \dot{p} + (-1)^n.$$

14 *Théorème. Si a produit une période de n termes et si le nombre des termes de la période de b est n ou un diviseur de n, b sera un des termes de la période de a.*

Retranchons de b tous les termes de la période de a et multiplions toutes ces différences entre elles: leur produit B est un polynome en b dont le premier terme b^n est $\dot{p} + 1$ et dont le dernier $(-1)^n P_n = (-1)^n \left\{ \dot{p} - (-1)^n \right\}$ est $\dot{p} - 1$.

Les termes intermédiaires ayant pour coefficients $-P_1, +P_2, \dots \pm P_{n-1}$ sont $\dot{p}$ d'après le corollaire précédent. Donc

$$B = \dot{p} + b^n + (-1) P_n = \dot{p}.$$

Ainsi, p divise B et par conséquent un des facteurs de B ; mais tous ces facteurs sont $< p$. Donc, l'égalité précédente ne peut subsister à moins que l'un de ces facteurs ne soit nul, ou que b ne soit égal à l'un des termes de la période de a . C. Q. F. D.

Corollaire 1^{er}. *Quand la base est un nombre premier, toutes les périodes d'un même nombre de termes renferment les mêmes nombres dans un ordre différent.*

Car si a et b engendrent tous deux une période de n termes, b sera un résidu de la période de a et n'aura à sa période que des termes faisant partie de la période de a . (10)

Corol. 2^o. *Quand la base est un nombre premier, il ne peut pas y avoir plus de $i(n)$ périodes de n termes.*

Car tout générateur d'une période de n termes ne pourra être qu'un résidu occupant dans la période de a un rang marqué par un nombre premier avec n ... (10, corol.). Il n'y aura donc pas plus de périodes de n termes qu'il n'y a d'entiers inférieurs et premiers à n .

15. Théorème. *Quand la base est un nombre premier p , si n est un diviseur de $p-1$, le nombre des périodes de n termes est $i(n)$.*

On sait que le nombre des termes d'une période ne peut être qu'un diviseur de $p-1$ et que si $n, n', n'', \dots$ désignent les diviseurs de ce nombre on a

$$i(n) + i(n') + i(n'') + \dots = p-1.$$

Comme le nombre total des périodes doit être égal à $p-1$, s'il n'y avait pas $i(n)$ périodes de n termes il faudrait qu'il y eût plus de $i(n')$ périodes de n' termes, ou plus de $i(n'')$ périodes de n'' termes, etc., ce qui est contraire au théorème précédent.

Corollaire 1^{er}. Dans tout système dont la base est un nombre premier p , le nombre des racines primitives est $i(p-1)$.

Corollaire 2^o. Si a est une racine primitive, les termes de sa période seront dans un ordre différent de l'ordre naturel, les nombres $1, 2, 3, \dots, p-1$. De là et du n° 12 on déduit ce théorème :

La somme des m^{es} puissances des termes de la progression $1, 2, 3, \dots, (p-1)$, est $\dot{p}$, quand p est premier et que m n'est pas $\frac{p-1}{2}$ ().*

Corollaire 3^o.

$1, 2, 3, \dots, (p-2)(p-1) + 1 = \dot{p}$ (n° 6, corol.).

C'est dans cette égalité que consiste le théorème de Wilson.

16. Nous avons vu qu'on pouvait déduire d'une période complète, toutes les autres périodes d'un système. Le tableau suivant renfermant les demi-périodes complètes des systèmes dont la base est un nombre premier inférieur à 29, pourra donc, entre ces limites, tenir lieu de tableau analogue à celui du n° 2.

base.	demi-période complète.
5	2, 4,
7	3, 2, 6,
11	2, 4, 8, 5, 10,
13	2, 4, 8, 3, 6, 12,
17	3, 9, 10, 13, 5, 15, 11, 16,
19	2, 4, 8, 16, 13, 7, 14, 9, 18,
23	5, 2, 10, 4, 20, 8, 17, 16, 9, 22.

(*) Voir t. I, p. 176. Ce théorème est encore une conséquence fort simple de celui établi au n° 11. En effet, d'après ce dernier les puissances $1, 2^m, 3^m, \dots, (p-1)^m$ divisées par p donnent pour restes dans un ordre différent de l'ordre naturel tous les nombres inférieurs à p . On a donc

$$S_m = \dot{p} + S_1.$$

et comme
$$S_1 = \frac{p(p-1)}{2} = \dot{p}, \text{ on en conclut } S_m = \dot{p}$$

La seconde partie de chacune de ces périodes s'obtiendra en retranchant de la base les termes de la première. (6, cor. 3.)

Note. Nous ajouterons ici, comme sujet d'exercice, les énoncés de quelques théorèmes d'Euler, et dont la démonstration ne présente pas de difficulté sérieuse.

Théorème. Si dans la période des résidus on trouve γ et γs premiers avec p , on y trouve aussi s .

Théorème. Si α est un résidu et a un non-résidu, $a\alpha$ est aussi un non-résidu. Tm.