NOUVELLES ANNALES DE MATHÉMATIQUES

E. PROUHET

Mémoire sur la théorie des résidus dans les proportions géométriques (fin)

Nouvelles annales de mathématiques 1re série, tome 5 (1846), p. 675-683

<http://www.numdam.org/item?id=NAM_1846_1_5__675_1>

MÉMOIRE

sur la théorie des résidus dans les proportions géométriques (fin).

(*Voir* p. 175.)

PAR M. E. PROUHET,
Professeur au college royal d'Auch.

—

27. Théorème. *Dans tout système dont la base* P *est une puissance d'un nombre premier impair, si* n *est un diviseur de* i(P), *il y aura* i(n) *périodes de* n *termes.*

Soit a une racine primitive du système P; posons $i(\mathrm{P}) = mn$; si on prend dans la période de a un terme dont le rang soit mn', n' étant premier avec n, la période engen-

drée par ce terme sera de $\frac{i(P)}{m}$, ou n termes, d'après la règle du n° 10. Or, comme on peut prendre pour n' tous les nombres inférieurs et premiers à n, on voit qu'il y aura dans la période de a $i(n)$ nombres engendrant des périodes de n termes, c. q. f. d.

Remarque. Cette démonstration fait croire que le théorème a lieu dans tout système qui possède une période complète.

28. Théorème. *Lorsque la base* P *est une puissance d'un nombre premier impair, la* $m^{ème}$ *colonne du système contient tous les termes d'une période dont le nombre des termes est* $\frac{i(P)}{d}$, d *étant le plus grand commun diviseur de* m *et* i(P).

Soit a une racine primitive, et supposons

$$a^m = \dot{P} + \alpha.$$

La période de α relativement à P sera de $\frac{i(P)}{d}$ termes (10). Or de l'égalité précédente on tire :

$$(a^2)^m = \dot{P} + \alpha^2$$
$$(a^3)^m = \dot{P} + \alpha^3$$
$$(a^4)^m = \dot{P} + \alpha^4.$$
$$\cdots\cdots\cdots$$

Mais a, a^2, a^3 donnent pour résidus tous les nombres inférieurs et premiers à P. Donc ces nombres elevés à la $m^{ème}$ puissance donnent tous les termes de la période de α; donc la $m^{ème}$ colonne renfermera tous les résidus de cette période, c. q. f. d.

29. Théorème. *Toutes choses étant posées comme au théorème précédent, le même résidu se répétera* d *fois dans la* $m^{ème}$ *colonne.*

Soit

$$b_1,\ b_2,\ b_3,\ \ldots\ b_d$$

une période de d termes, on aura $b_1^d = \dot{P} + 1$, et par conséquent $b_1^m = \dot{P} + 1$, puisque m est $\dot{d}$. Il suit de là que $a^m b_1^m$ donne le même résidu que a^m. La même chose pouvant se dire de b_2, de b_3, etc., il en résulte que le nombre

$$ab_1, ab_2, \ldots . ab_d,$$

ou leurs résidus par rapport à P, élevés à la $m^{ème}$ puissance, sont tous $\dot{P} + a$. Donc le même résidu se répète au moins d fois, et comme il y a dans la $m^{ème}$ colonne $\frac{i(P)}{d}$ résidus différents, on ne doit pas trouver plus de d fois le même, autrement la $m^{ème}$ colonne renfermerait un nombre de termes supérieur à $i(P)$. Donc, etc.

30. Si l'on a bien suivi les raisonnements qui précèdent, on a dû voir qu'ils ne s'appliquent pas au cas où la base est une puissance de 2. Voyons ce qui doit se passer dans un pareil système.

Si $P = 2^m$, $i(P) = 2^{m-1}$; une période complète devrait avoir 2^{m-1} termes, mais il est facile de voir qu'aucune période ne peut avoir plus de 2^{m-2} termes. En effet, on a identiquement :

$$a^{2^{m-2}} - 1 = (a-1)(a+1)(a^2+1)(a^{2^2}+1)(a^{2^3}+1)\ldots.$$
$$\ldots.(a^{2^{m-3}}+1).$$

Le second membre renferme $m-1$ facteurs pairs, et est par conséquent divisible par 2^{m-1}; mais l'un des deux facteurs $a-1$, $a+1$ est divisible par 4; on aura donc toujours, a étant un nombre impair quelconque :

$$a^{2^{m-2}} - 1 = \dot{2}^m.$$

Ainsi il n'existe pas de racine primitive absolue dans le système 2^m.

31. Dans le système qui nous occupe, il est possible de

déterminer directement les racines primitives de 2^n par rapport à 2^m, n étant au plus égal à $m-2$.

Nous supposerons d'abord $n > 1$; a désignant l'une des racines cherchées, qui est nécessairement impaire, on a identiquement :

$$a^{2^n} - 1 = (a-1)(a+1)(a^2+1)(a^{2^2}+1)\ldots(a^{2^{n-1}}-1).$$

Les facteurs a^2+1, $a^{2^2}+1\ldots$ sont tous divisibles par 2 sans l'être par 4. La plus haute puissance de 2 qui divise leur produit est donc 2^{n-1}. Donc

$$a^{2^n} - 1 = (a-1)(a+1)\,\dot{2}^{n-1};$$

le second membre doit être divisible par 2^m sans l'être par 2^{m+1}. On doit donc avoir

$$(a-1)(a+1) = \dot{2}^{m-n+1}.$$

L'un des deux facteurs $a-1$, $a+1$, est divisible par 2 sans l'être par 4, l'autre devra donc être egal à 2^{m-n} multiplié par un nombre impair. Par conséquent, il y aura deux manières de satisfaire à l'egalité précédente, soit en posant

$$a - 1 = 2^{m-n}(2b+1),$$

ou bien :

$$a + 1 = 2^{m-n}(2b+1),$$

et alors a devra être de l'une des deux formes suivantes :

I. $\quad a = 2^{m-n}(2b+1)+1,$

II. $\quad a = 2^{m-n}(2b+1)-1.$

32. Voyons maintenant combien il y aura d'entiers inférieurs à 2^m et remplissant ces conditions.

Prenons d'abord les nombres de première espèce. On ne peut pas supposer $2b+1 = 2^n+1$, puisqu'on en tirerait $a > 2^m$; mais on peut faire $2b+1 = 2^n-1$, ou $b = 2^{n-1}-1$,

puisqu'on en tire $a = 2^m - 2^{m-n} + 1 < 2^m$. On pourra donc prendre pour b les valeurs suivantes

$$0,\ 1,\ 2,\ 3\ \ldots\ .\ 2^{n-1} - 1,$$

au nombre de 2^{n-1}. Donc a est susceptible de 2^{n-1} valeurs de première forme.

On verrait de même que les solutions de seconde forme sont aussi au nombre de 2^{n-1}, d'où l'on peut conclure ce théorème :

Dans le système 2^m, n *étant compris entre* 2 *et* 2^{m-2}, *il y a* 2^n périodes de 2^n *termes.*

33. Jusqu'à présent nous avons supposé $n > 1$. Si $n = 1$, on a à satisfaire à l'égalité

$$a^2 - 1 = 2^m,$$

laquelle est satisfaite par l'entier 1, générateur d'une période d'un terme et par les nombres

$$2^{m-1} - 1,\ 2^{m-1} + 1,\ 2^m - 1,$$

associés doubles par rapport à 2^m, et générateurs de périodes de 2 termes. Il y aura donc 3 périodes de 2 termes.

Indiquons maintenant une vérification des calculs précédents. Comme nous venons de le voir, il y aura :

1	période de	1 terme
$2+1$	—	2
2^2	—	2^2
. . . . .		
2^{m-2}	—	2^{m-2}.

Le nombre total des périodes sera donc :

$$1 + (1 + 2 + 2^2 + \ldots + 2^{m-2}) = 1 + (2^{m-1} - 1) = 2^{m-1}$$

ainsi qu'on devait s'y attendre.

§ IV.

Des systèmes de périodes dont la base est un nombre composé. — Des résidus dans les progressions géométriques quelconques.

34. Supposons que les lettres A, B, C... L représentent chacune ou un nombre premier ou une puissance d'un nombre premier impair différent, et posons :

$$P = ABC \ldots L ;$$

Soit N un entier premier avec P et générateur d'une période de α termes dans le système A, de β dans le système B, etc., et cherchons quel doit être le nombre des termes de la période dans le système P.

Il s'agit de trouver la plus petite valeur entière propre à satisfaire à l'équation

$$N^x - 1 = \dot{P}.$$

Or on y satisfera évidemment en prenant x à la fois $\dot{\alpha}$, $\dot{\beta}$, $\dot{\gamma}$, ... $\dot{\lambda}$. Donc la plus petite valeur que l'on pourra donner à x sera le plus multiple commun de α, β, γ, ... λ, ce que nous exprimons ainsi :

$$x = m(\alpha, \beta, \gamma, \ldots \lambda).$$

35. Cherchons maintenant quel est le plus grand nombre de termes dont une période puisse se composer.

Les nombres

$$\alpha, \quad \beta, \quad \gamma, \quad \ldots \lambda$$

doivent être respectivement des sous-multiples de

$$i(A), \ i(B), \ i(C), \ \ldots \ i(L).$$

Donc on aura :

$$m(\alpha, \beta, \gamma, \ldots \lambda) \underset{=}{<} m[i(A), i(B), i(C), \ldots i(L)];$$

mais $i(A)$, $i(B)$, ... $i(L)$ sont des nombres pairs, par conséquent non premiers entre eux. Leur plus petit multiple commun est donc inférieur à leur produit ou à $i(P)$. Donc on aura :

$$m(\alpha, \beta, \gamma, \ldots \lambda) < i(P).$$

Ainsi *il n'y a pas de racines primitives dans tout système dont la base est le produit de plusieurs nombres premiers impairs.*

36. Posons

$$k = m[i(A), i(B), i(C), \ldots i(L)],$$

et désignons par L un sous-multiple de K, je dis qu'il y aura dans le système P une période de L termes.

Pour le démontrer, supposons que les nombres

$$\alpha, \beta, \gamma, \ldots \lambda$$

soient respectivement des sous-multiples de

$$i(A), i(B), i(C), \ldots i(L);$$

et d'ailleurs choisis de telle sorte que

$$k = m(\alpha, \beta, \gamma, \ldots \lambda).$$

On trouvera nécessairement un système de nombres

$$a, b, c, \ldots l,$$

générateurs de périodes de

$$\alpha, \beta, \gamma, \ldots \lambda$$

termes, dans les systèmes

$$A, B, C, \ldots L.$$

D'un autre côté, on peut toujours trouver un nombre N moindre que P, et *un seul* satisfaisant aux conditions suivantes :

$$N = \dot{A} + a = \dot{B} + b = \dot{C} + c \ldots = \dot{L} + l.$$

Or N, d'après le n° 34, engendre dans le système P une période dont le nombre des termes est $m(\alpha, \beta, \gamma, \ldots \lambda)$ ou k. Donc notre proposition se trouve démontrée.

37. Cherchons maintenant combien il y aura de périodes de k termes.

Il y a $i(\alpha)$ nombres qui, dans le système A, engendrent, comme a, une période de α termes; $i(\beta)$ nombres qui, dans le système B, engendrent, comme b, une période de β termes, etc. Donc on pourra trouver $i(\alpha)\, i(\beta)\, i(\gamma) \ldots i(\lambda)$ systèmes analogues à

$$a, \quad b, \quad c, \quad \ldots \quad l,$$

et par conséquent pour chaque manière de satisfaire à la relation

$$k = m\ (\alpha, \beta, \gamma, \ldots \lambda);$$

le nombre de périodes de k termes sera

$$i(\alpha)\, i(\beta)\, i(\gamma) \ldots i(\lambda).$$

Donc le nombre total des périodes de k termes sera donné par la formule

$$\Sigma\, i(\alpha)\, i(\beta)\, i(\gamma) \ldots i(\lambda),$$

en prenant successivement pour $\alpha, \beta, \gamma, \ldots \lambda$ tous les nombres propres à satisfaire aux relations ci-dessus énoncées.

38. Ce que nous venons de dire s'applique, à peu de modifications près, aux systèmes dont la base est

$$2^m\text{A}, \text{B}, \text{C}, \text{D} \ldots \text{L},$$

m étant plus grand que 2. Seulement le maximum du nombre des termes d'une période est

$$k = m\,[2^{m-2},\ i(\text{A}),\ i(\text{B}),\ \ldots\ i(\text{L})],$$

ce qui tient à ce que dans le système 2^m il n'y a pas de périodes de plus de 2^{m-2} termes. Mais si $m = 1$ ou 2, on aura :

$$k = m\,[\,i(\text{A}),\ i(\text{B}),\ i(\text{C}),\ \ldots\ i(\text{L})\,].$$

Dans le cas où $m = 1$ et où P n'admet qu'un seul nombre premier impair, on a plus simplement :

$$k = i(\mathrm{A}) = i(2\mathrm{A}) = i(\mathrm{P}),$$

et par conséquent :

Il existe des racines primitives dans tout système dont la base est le double d'un nombre premier, ou le double d'une puissance d'un nombre premier impair (*).

Un pareil système jouirait donc de toutes les propriétés qui tiennent à l'existence des racines primitives.

Dans toutes les autres circonstances on aura évidemment $k < i(\mathrm{P})$, et par conséquent on a ce théorème général :

Il n'existe de racines primitives que dans tout système dont la base est ou une puissance ou le double d'une puissance d'un nombre premier impair.