

E. PROUHET

Mémoire sur la théorie des résidus dans les proportions géométriques

Nouvelles annales de mathématiques 1^{re} série, tome 5 (1846), p. 652-662

[<http://www.numdam.org/item?id=NAM_1846_1_5_652_0>](http://www.numdam.org/item?id=NAM_1846_1_5_652_0)

© 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 proportions géométriques.

(Voir p. 175.)

PAR M. E. PROUHET,

Professeur au collège royal d'Auch.

17. Nous devons à M. Poinsoi une méthode directe pour trouver les racines primitives, progrès immense sous le point de vue théorique. Mais on jugera souvent plus commode dans la pratique d'avoir recours à des essais.

Pour diminuer le nombre des essais , on ne devra prendre pour générateur de période , aucun carré ou résidu de carré Car si a est un résidu de carré en sorte que $b^2 = \dot{p} + a$, on aura $a^{\frac{n-1}{2}} = \dot{p} + b^{n-1} = \dot{p} + 1$, et par conséquent la période de a aura au plus $\frac{n-1}{2}$ termes.

Un nombre faisant partie d'une période incomplète , ne pourra pas non plus être racine primitive.

Enfin , si g est une racine primitive , on devra avoir

$$g^{\frac{p-1}{2}} = \dot{p} - 1.$$

Le théorème suivant indique , sans beaucoup de calcul , les nombres qui satisfont ou ne satisfont pas à cette condition , et pourra , par conséquent , servir à diminuer de beaucoup le nombre des essais.

18. THÉORÈME. Si on divise par p les termes de la progression

$$(A) \quad a, 2a, 3a, \dots \dots \dots \frac{p-1}{2} a,$$

si on désigne par :

$$(1) \quad a', a'', a''', \dots \dots \dots a^{(\gamma)};$$

les restes moindres que $\frac{p-1}{2}$ et par :

$$(2) \quad b', b'', b''', \dots \dots \dots b^{(\mu)};$$

les restes plus grands que $\frac{p-1}{2}$; $a^{\frac{p-1}{2}}$ sera $\dot{p} + 1$ ou $\dot{p} - 1$, suivant que μ sera pair ou impair ; c'est-à-dire qu'on aura toujours

$$a^{\frac{p-1}{2}} = \dot{p} + (-1)^{\mu}. \quad (*)$$

Si on prolongeait la progression (A) jusqu'au terme $(p-1)a$, on sait que tous les résidus qu'elle fournirait, seraient différents entre eux, et que ceux de la seconde moitié seraient les compléments à p des résidus de la première. Il suit de là qu'aucun des nombres

$$p-b', p-b'', p-b''', \dots \dots \dots p-b^{(\mu)},$$

ne peut faire partie de la suite (1). Par conséquent tous les $\frac{p-1}{2}$ nombres suivants

$$a', a'', a''', \dots \dots a^{(\gamma)}, \quad p-b', p-b'', p-b''', \dots \dots p-b^{(\mu)},$$

tous différents entre eux, tous moindres que $\frac{p-1}{2}$, doivent comprendre dans un ordre différent de l'ordre naturel, les $\frac{p-1}{2}$ entiers, inférieurs à $\frac{p-1}{2}$.

On aura donc :

$$\begin{aligned} & a' a'' a''' \dots a^{(\gamma)} (p-b') (p-b'') \dots (p-b^{(\mu)}) = \\ & = \dot{p} + a' a'' a''' \dots b' b'' b''' \dots (-1)^{\mu} = 1.2.3. \dots \frac{p-1}{2}; \end{aligned}$$

(*) M. Gauss a fait de ce théorème la base de sa démonstration de la loi de réciprocité entre les nombres premiers.

et par suite :

$$a'a''a''' \dots b'b''b''' \dots = p + 1.2.3 \dots \frac{p-1}{2} (-1)^\mu;$$

d'un autre côté on a évidemment :

$$1.2.3 \dots \frac{p-1}{2} a^{\frac{p-1}{2}} = p + a'a''a''' \dots b'b'' \dots b^{(\mu)};$$

donc :

$$1.2.3 \dots \frac{p-1}{2} a^{\frac{p-1}{2}} = p + 1.2.3 \dots \frac{p-1}{2} (-1)^\mu$$

d'où :

$$1.2.3 \dots \frac{p-1}{2} \left\{ a^{\frac{p-1}{2}} - (-1)^\mu \right\} = p;$$

p ne peut pas diviser le produit $1.2.3 \dots \frac{p-1}{2}$. Donc

$$a^{\frac{p-1}{2}} - (-1)^\mu = p;$$

ce qu'il fallait démontrer.

19. PROBLÈME. a étant un diviseur de $p-1$, trouver le résidu de $a^{\frac{p-1}{2}}$ par rapport à p .

Désignons par b le quotient de $p-1$ par a , en sorte que

$$ab = p-1.$$

Nous allons distinguer plusieurs cas.

1^{er} Cas. $a=2$, $b=2$. Les résidus de la progression (A) forment $\frac{a}{2}$ progressions arithmétiques, contenant chacune b termes, comme il suit :

$$(1) \quad a, 2a, 3a, \dots, \frac{b}{2}a, \left(\frac{b}{2}+1\right)a, \dots, ab.$$

$$(2) \quad a-1, 2a-1, 3a-1, \dots, \frac{b}{2}a-1, \left(\frac{b}{2}+1\right)a-1, \dots, ab-1.$$

$$(3) \quad \dots \dots \dots$$

$$(n) \quad a-n+1, 2a-n+1, 3a-n+1, \dots, \frac{b}{2}a-n+1,$$

$$\left(\frac{b}{2}+1\right)a-n+1, \dots, ab-n+1$$

.....

$$\left(\frac{a}{2}\right). a-\frac{a}{2}+1, 2a-\frac{a}{2}+1, 3a-\frac{a}{2}+1, -\frac{b}{2}a-\frac{a}{2}+1,$$

$$\left(\frac{b}{2}+1\right)a-\frac{a}{2}+1, \dots, ab-\frac{a}{2}+1.$$

Dans la n^e ligne, tous les termes sont moindres que $\frac{ab}{2}$, jusqu'au terme $\frac{b}{2}a-n+1$ inclusivement; mais le suivant $\frac{ab}{2}+a-(n-1)$ est évidemment supérieur à $\frac{ab}{2}$, puisque n est plus petit que $\frac{a}{2}$. Tous les résidus suivants sont à plus forte raison $> \frac{ab}{2}$. Ainsi chaque ligne renferme $\frac{b}{2}$ résidus plus grands que $\frac{ab}{2}$ ou $\frac{p-1}{2}$, donc

$$\mu = \frac{a}{2} \cdot \frac{b}{2}.$$

2^e Cas. $a=\dot{2}$, $b=\dot{2}+1$. En procédant comme dans le premier cas, on décomposerait la suite des résidus en $\frac{a}{2}$ progressions dont chacune renfermera $\frac{b+1}{2}$ résidus $> \frac{p-1}{2}$. Donc, ici,

$$\mu = \frac{a}{2} \cdot \frac{b+1}{2}.$$

3^e Cas. $a=\dot{2}+1$, $b=\dot{2}$. Les résidus de la progression (A) forment $\frac{a-1}{2}$ progressions de b termes, et une de $\frac{b}{2}$ termes comme il suit :

$$(1) \quad a, 2a, 3a, \dots, \frac{b}{2}a, \dots, \left(\frac{b}{2}+1\right)a, \dots, ab.$$

$$(2) \quad a-1, 2a-1, 3a-1, \dots, \frac{b}{2}a-1, \dots, \left(\frac{b}{2}+1\right)a-1, \dots, ab-1.$$

.

$$(n) \quad a-n+1, 2a-n+1, 3a-n+1, \dots, \frac{b}{2}a-n+1, \dots$$

$$\left(\frac{b}{2}+1\right)a-n+1, \dots, ab-n+1.$$

.

$$\left(\frac{a-1}{2}\right), a-\frac{a-1}{2}+1, 2a-\frac{a-1}{2}+1, 3a-\frac{a-1}{2}+1, \dots$$

$$\frac{b}{2}a-\frac{a-1}{2}+1, \dots, \left(\frac{b}{2}+1\right)a-\frac{a-1}{2}+1, \dots, ab-\frac{n+1}{2}+1.$$

$$\frac{a+1}{2}, a-\frac{a+1}{2}+1, 2a-\frac{a+1}{2}+1, \dots, \frac{b}{2}a-\frac{a+1}{2}+1.$$

La dernière ligne ne renferme aucun résidu plus grand que $\frac{ab}{2}$. Dans chacune des autres il y en a $\frac{b}{2}$. Donc

$$\mu = \frac{b}{2} \cdot \frac{a-1}{2}.$$

20. PROBLÈME. a étant un diviseur de $p+1$, trouver le résidu de $a^{\frac{p-1}{2}}$ par rapport à p .

Par des raisonnements qui diffèrent très-peu de ceux que nous venons de faire on trouvera :

$$\mu = \frac{a}{2} \cdot \frac{b}{2} \quad \text{si} \quad a = 2, \quad b = \frac{p+1}{a} = 2$$

$$\mu = \frac{a}{2} \cdot \frac{b-1}{2} \quad \text{si} \quad a = 2, \quad b = 2+1$$

$$\mu = \frac{a-1}{2} \cdot \frac{b}{2} \quad \text{si} \quad a = 2+1, \quad b = 2.$$

21. Les formules précédentes conduisent très-simplement aux relations des nombres 2 et 3 avec tous les autres nombres premiers.

Si dans la première formule du n° 19 on fait $\alpha=2$, on a :

$$\mu = \frac{b}{2} = \frac{\frac{p-1}{2}}{2} = \frac{p-1}{4},$$

et par suite,

$$2^{\frac{p-1}{2}} = p + (-1)^{\frac{p-1}{4}}.$$

Donc $2^{\frac{p-1}{4}}$ sera $p+1$ ou $p-1$, suivant que $\frac{p-1}{4}$ sera pair ou impair; ou suivant que $p-1$ sera $8+1$ ou $8-3$.

Si dans la deuxième formule on fait $\alpha=2$, on a :

$$\mu = \frac{b+1}{2} = \frac{\frac{p-1}{2}+1}{2} = \frac{p+1}{4},$$

et par suite,

$$2^{\frac{p-1}{2}} = p + (-1)^{\frac{p+1}{4}}.$$

et $2^{\frac{p-1}{4}}$ sera $p+1$ ou $p-1$, suivant que $\frac{p+1}{4}$ sera pair

ou impair : c'est-à-dire suivant que p sera $8-1$ ou $8+3$.

Ainsi en résumé :

$$2^{\frac{p-1}{2}} = p + 1 \quad \text{lorsque } p = 8 \pm 1$$

$$2^{\frac{p-1}{2}} = p - 1 \quad \text{lorsque } p = 8 \pm 3.$$

Ces relations permettent de trouver directement une racine primitive dans tout système dont la base $p=2q+1$, q étant un nombre premier. Le nombre des termes d'une

période dans ce système ne peut-être que 1, 2, q , ou $2q$, et on aura :

$$2^q = p \pm 1,$$

suivant que p sera $8-1$ ou $8-3$. Or, dans le premier cas, d'après le théorème du n° 9, $\frac{p-1}{2}$ ou q aura une période de $2q$ termes et sera racine primitive. Dans le second cas le nombre des termes de la période de 2 sera nécessairement pair, et ne pourra être que $2q$. 2 sera donc alors racine primitive.

22. Cherchons maintenant les relations du nombre 3 avec les autres nombres premiers.

p étant un nombre premier plus grand que 3, l'un des deux quotients,

$$\frac{p-1}{3}, \quad \frac{p+1}{3},$$

est entier.

Dans le premier cas la troisième formule du n° 19 donnera :

$$\mu = \frac{b}{2} = \frac{p-1}{6}.$$

Dans le deuxième, la troisième formule du n° 20 donnera :

$$\mu = \frac{b}{2} = \frac{p+1}{6}.$$

Ainsi

$$\frac{p-1}{3} = p + (-1)^{\frac{p+1}{6}}.$$

M. Cauchy, dans ses exercices de mathématiques, a donné le moyen de trouver une équation satisfaite exclusivement par toutes les racines primitives d'un système. Un exemple fera comprendre la marche suivie par l'illustre géomètre.

Supposons qu'il s'agisse de trouver les racines primitives

du système dont la base est 37. Cela revient évidemment à chercher les nombres qui satisfont à l'équation

$$(1) \quad x^{36} - 1 = 37,$$

sans satisfaire à aucune équation analogue dans laquelle l'exposant de x serait moindre. Or cette équation se ramène aux deux suivantes :

$$(2) \quad x^{18} - 1 = 37,$$

$$(3) \quad x^{18} + 1 = 37.$$

Les solutions de (2) doivent être rejetées, puisque tout nombre qui satisfait à cette équation a au plus 18 termes à sa période. Quant à l'équation (3) son premier membre est divisible par $x^6 + 1$, et elle se ramène aux deux suivantes :

$$(4) \quad x^6 + 1 = 37,$$

$$(5) \quad x^{12} - x^6 + 1 = 37.$$

Tout nombre qui satisfait à l'équation (4) doit être rejeté, car il ne peut avoir à sa période plus de 6 termes. Donc, en définitive les 12 racines primitives du système ne sont autres que les 12 solutions entières et moindres que p de l'équation

$$x^{12} - x^6 + 1 = 37 \quad (*).$$

Mais cette méthode est de peu d'utilité dans la recherche qui nous occupe. Car l'équation finale à laquelle on arrive est

(*) Le même raisonnement fait voir que dans tout système dont la base est $37 + 1$, les racines primitives de p par rapport à 37 s'obtiennent en résolvant l'équation

$$x^{12} - x^6 + 1 = p.$$

souvent très-compiquée et ne peut d'ailleurs être résolue que par tâtonnement. C'est ainsi que pour trouver les racines primitives du système dont la base est 23, on aurait à résoudre l'équation

$$x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 = 23,$$

ce qui est bien moins simple que de rechercher un nombre qui ne satisfasse à aucune des trois équations

$$x - 1 = 23, \quad x^2 - 1 = 23, \quad x^{11} - 1 = 23.$$

§ III.

Des systèmes de périodes dont la base est une puissance d'un nombre premier.

24. Nous allons maintenant supposer que la base du système est p^h , p étant un nombre premier plus grand que 2. Le nombre des périodes du système ou l'indicateur de P sera $p^{h-1}(p-1)$, et toute période complète, s'il en existe, devra présenter $p^{h-1}(p-1)$ termes.

25. THÉORÈME. *Si la période de a comprend n termes dans le système p^h , la période de ce nombre en comprendra n ou p dans le système p^{h+1} .*

Soit m le nombre des termes de la période de a dans le système p^{h+1} , on aura :

$$a^m = p^{h+1} + 1,$$

et par conséquent aussi,

$$a^n = p^h + 1.$$

Donc m ne peut être que n ou $\dot{n}$. Posons donc $m = nx$. On a par hypothèse :

$$a^n = Ap^h + 1;$$

d'où l'on tire :

$$a^{nx} = p^{h+1} + Axp^h + 1.$$

Or la plus petite valeur à donner à x pour que le second nombre soit p^{r+1} est 1 si A est p , et p dans le cas contraire. Donc $x = 1$ ou p . Donc $m = n$ ou pn , c. q. f. d.

Corollaire. Si n est le nombre des termes de la période de a dans le système p et dans le système p^2, p^3, p^4 , etc., jusqu'à p^{r+1} exclusivement, le nombre des termes de la période de a dans le système $p^{r+\alpha}$ sera np^α (*).

D'après l'hypothèse on a :

$$(1) \quad a^n = Ap^r + 1,$$

A étant premier avec p . La période de a ne pouvant être de n termes dans le système p^{r+1} , sera nécessairement de np termes ; posons donc :

$$(2) \quad a^{np} = A'p^{r+1} + 1.$$

Je dis que A' est aussi premier avec p . En effet, élevons les deux membres de (1) à la puissance p , nous aurons :

$$\begin{aligned} a^{np} &= 1 + pAp^r + \frac{p(p-1)}{1 \cdot 2} A^2 p^{2r} + \dots \\ &= 1 + p^{r+1} A(1+p); \end{aligned}$$

donc

$$A' = A(\dot{p} + 1).$$

A' est donc premier avec p . Il résulte de là que le nombre des termes de la période de a dans le système p^{r+2} ne peut être np ; ce nombre sera donc np^2 , conformément à l'énoncé.

On prouverait de même que la période de a est de np^2 termes par rapport à p^{r+3} , de np^4 par rapport à p^{r+4} , et ainsi de suite. Donc, etc.

26. THÉORÈME. Il existe des racines primitives dans tout

(*) V. t. II, p. 84, un article de M. Thibaut.

système, dont la base est une puissance d'un nombre premier impair.

Soit a une racine primitive de p ; si la période de a par rapport à p^2 n'est pas de $p - 1$ termes, la période de a par rapport à p^h sera, d'après le corollaire précédent, de $p^{h-1} (p - 1)$ termes. Donc a sera racine primitive de p^h , quel que soit h .

Si la période de a dans le système p^2 est de $p - 1$ termes, comme dans le système p , en sorte que l'on ait :

$$a^{p-1} = Ap^2 + 1.$$

Posons :

$$a' = p + a,$$

nous aurons :

$$\begin{aligned} a'^{p-1} &= p^2 + (p-1)pa^{p-2} + a^{p-1} \\ &= p^2 + (p-1)pa^{p-2} + 1. \end{aligned}$$

On voit par là que a'^{p-1} n'est pas $\dot{p} + 1$. Donc la période de a' n'a pas le même nombre de termes dans les systèmes p et p^2 . Donc la période de a' par rapport à p^h sera de $p^{h-1} (p - 1)$ termes, et a' sera racine primitive de p^h .

(La fin prochainement).