Article
Sur le théorème de fermat.
Mansion, Paul
in: Nouvelle correspondance mathématique | Nouvelle correspondance mathématique - 4 | Sur la théorie des fonctions numériques simplement périodiques. Sur le t...

Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library. Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept there Terms and Conditions. Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:

Niedersächsische Staats- und Universitätsbibliothek
Digitalisierungszentrum
37070 Goettingen
Germany
Email: gdz@sub.uni-goettingen.de

Purchase a CD-ROM

The Goettingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:
Niedersaechisische Staats- und Universitaetsbibliothek Goettingen - Digitalisierungszentrum
37070 Goettingen, Germany, Email: gdz@sub.uni-goettingen.de

SUR LE THÉORÈME DE FERMAT;

par M. Paul Mansion.

---

1. *Démonstration du théorème de Fermat, généralisé, considéré comme identique au principe fondamental de la théorie des fractions périodiques.* Dans ce qui suit, les symboles 10, 100, 1000, ... représentent les puissances B, B^2, B^3,... d'un nombre B, base d'un système quelconque de numération; mais, à une première lecture, on peut supposer qu'ils ont la signification ordinaire.

Premier cas. Si l'on divise 1000... par N, nombre premier à 10, le quotient $q_1q_2\ldots q_nq_1q_2\ldots q_n\ldots$ se composera de n chiffres qui se reproduisent périodiquement; n, nombre de chiffres de chaque période, sera $< N$; aux chiffres $q_1, q_2, \ldots, q_n$, correspondront n restes $r_1 = 1, r_2, \ldots, r_n$, tous différents les uns des autres, et premiers à 10 et à N. Nous aurons

$$\frac{1}{N} = \frac{q_1q_2\ldots q_n}{100\ldots 0} + \frac{1}{N \times 100\ldots 0}, \quad \ldots \quad (1)$$

ou

$$\frac{10^n - 1}{N} = q_1q_2\ldots q_n. \quad \ldots \quad (2)$$

Si $r_1, r_2, \ldots r_n$ sont les $\varphi(N)$ *nombres premiers à* N *et non supérieurs à* N, l'équation (2) peut s'écrire :

$$\frac{10^{\varphi(N)} - 1}{N} = \textit{entier},$$

ou

$$\frac{B^{\varphi(N)} - 1}{N} = \textit{entier};$$

ce qui est le théorème de Fermat, généralisé.

Second cas. Si n n'est pas égal à φ (N), je dis qu'il en est un sous-multiple. En effet, soit s l'un des φ (N) nombres premiers et inférieurs à N, non compris dans la suite $r_1, r_2, \ldots, r_n$. La fraction $(s_1 : \mathrm{N})$ donnera naissance, comme $(1 : \mathrm{N})$, à une fraction périodique, où la période aura n chiffres et où les restes successifs, $s_1, s_2, \ldots, s_n$, seront tous différents de $r_1, r_2, \ldots, r_n$.

Ce dernier point est évident : si l'un des nombres $s_1, s_2, \ldots, s_n$ était égal à l'un des nombres $r_1, r_2, \ldots, r_n$, il en serait de même de tous les autres, contrairement à l'hypothèse. Quant au premier point, observons d'abord que l'équation (1) donne

$$\frac{s_1}{\mathrm{N}} = \frac{s_1 \times q_1 q_2 \ldots q_n}{100 \ldots 0} + \frac{s_1}{\mathrm{N} \times 100 \ldots 0};$$

donc $(s_1 : \mathrm{N})$ est égale à une fraction périodique, où la période a n chiffres au plus. Il est aisé de voir qu'elle ne peut en avoir moins. Si l'on avait

$$\frac{s_1}{\mathrm{N}} = \frac{q'_1 q'_2 \ldots q'_{n'}}{100 \ldots 0} + \frac{s_1}{\mathrm{N} \times 100 \ldots 0}, \quad (n' < n),$$

il en résulterait

$$s_1 (10^{n'} - 1) = q'_1 q'_2 \ldots q'_{n'} \times \mathrm{N}.$$

Par conséquent, $q'_1 q'_2 \ldots q'_n$ serait divisible par s_1, et égal à $s_1 \times q''_1 q''_2 \ldots q''_{n'}$. De l'équation (3) on déduirait

$$\frac{1}{\mathrm{N}} = \frac{q''_1 q''_2 \ldots q''_{n'}}{100 \ldots 0} + \frac{1}{\mathrm{N} \times 100 \ldots 0};$$

c'est-à-dire que, contrairement à l'hypothèse, la période de la fraction égale à $(1 : \mathrm{N})$ aurait n' chiffres et non n.

Il y a donc n restes $s_1, s_2, \ldots, s_n$, différents de $r_1, r_2, \ldots, r_n$, et inférieurs à N. S'il n'y en a pas d'autres premiers à N, $\varphi(\mathrm{N}) = 2n$. S'il y en a d'autres, de l'un d'eux, t_1, on en déduira, comme ci-dessus, une série $t_1, t_2, \ldots, t_n$ S'il n'y en a pas d'autres premiers à N, $\varphi(\mathrm{N}) = 3n$. Et ainsi de suite. Donc enfin, en général, $\varphi(\mathrm{N}) = mn$.

D'après l'équation (2), $10^n - 1$ est un multiple de N. Mais $10^n - 1$ est un sous-multiple de $10^{mn} - 1$ ou de $10^{\varphi(N)} - 1$. Donc $10^{\varphi(N)} - 1$ ou $B^{\varphi(N)} - 1$ *est un multiple de* N, *si* B *est premier à* N (théorème de Fermat, généralisé).

Si N est premier, $\varphi(N) = N - 1$; l'on a alors $B^{N-1} - 1 =$ *multiple de* N : cette proposition est appelée, aujourd'hui, *théorème de Fermat.* Fermat l'a signalée, mais comme simple corollaire de la proposition plus générale : $B^n - 1 =$ *multiple de* N, *n étant un sous-multiple convenable de* $N - 1$.

2. Notions historiques. « Le théorème de Fermat, dit Gauss (n° 50 des *Disquisitiones*), publié, sans démonstration, dans les OEuvres de ce géomètre (*Fermatii Opera mathematica*, Tolosae, 1679, p. 163, ou *Précis des Œuvres de Fermat*, par M. Brassinne, p. 143), a été démontré d'abord par Euler (*Comm. Act. Petrop.*, t. VIII) de la manière suivante : Si p est premier, le développement de $(a+1)^p$ permet de voir que $(a+1)^p - (a+1)$ est divisible par p, si $a^p - a$ est divisible par p. Or $1^p - 1 = 0$, est divisible par p; il en est donc de même de $2^p - 2$, $3^p - 3$, etc., et enfin de $B^p - B = B(B^{p-1} - 1)$, B étant un entier quelconque. Donc, *si* p *est un nombre premier qui ne divise pas* $B, B^{p-1} - 1$ *est divisible par* p. »

Euler a tiré de là le théorème général :

$$B^{\varphi(N)} - 1 = \mathfrak{M}N,$$

N étant premier à B, comme il suit.

Soit d'abord $N = p^\pi$. Élevons, à la puissance p,

$$B^{p-1} = 1 + \mathfrak{M}p;$$

le résultat à la puissance p, et ainsi de suite. On trouve

$$B^{\varphi(p^\pi)} = 1 + \mathfrak{M}p^\pi.$$

Soit ensuite $N = a^\alpha b^\beta \ldots l^\lambda$, $a, b, \ldots, l$ étant premiers entre eux. On aura

$$B^{\varphi(a^\alpha)} = 1 + \mathfrak{M}a^\alpha;$$

et, à cause de $\varphi(N) = \varphi(a^\alpha)\varphi(b^\beta)\dots\varphi(l^\lambda)$, en élevant à la puissance $\varphi(b^\beta)\dots\varphi(l^\lambda)$:

$$B^{\varphi(N)} = 1 + \mathfrak{M}a^\alpha.$$

De même :

$$B^{\varphi(N)} = 1 + \mathfrak{M}b^\beta, \quad \dots, \quad B^{\varphi(N)} = 1 + \mathfrak{M}l^\lambda.$$

Donc enfin, $B^{\varphi(N)} - 1$, divisible par $a^\alpha, b^\beta, \dots, l^\lambda$, nombres premiers entre eux, est divisible par leur produit, ou par N.

« Comme le développement du binôme, dit Gauss, semble assez étranger à la théorie des nombres, Euler a publié plus tard une autre démonstration (*Comm. nov. Petrop.*, t. VII, p. 70), fondée sur la considération des restes de la division, par N, des termes de la progression géométrique 1, B, B^2, B^3, ... » Reproduite dans les *Disquisitiones*, nos 45-49, elle est, au fond, absolument identique à celle que nous avons exposée au n° 1. Poinsot l'a revêtue d'une forme géométrique, sans y rien changer (*). Cette seconde démonstration d'Euler est la plus naturelle de toutes celles que l'on a données du théorème de Fermat; de plus, elle a l'avantage de prouver, du même coup, la proposition plus générale :

$$B^n - 1 = \mathfrak{M}N,$$

n étant un diviseur convenable de $\varphi(N)$.

Il y en a une qui conduit simplement à la relation

$$B^{\varphi(N)} - 1 = \mathfrak{M}N,$$

mais qui est beaucoup plus courte. Elle est insérée dans plusieurs traités élémentaires d'Arithmétique (**), parfois sous le nom de Poinsot, parce que celui-ci se l'est attribuée, sans aucun droit, dans son Mémoire trop vanté (c. II, n° 1). En réalité, trois

---

(*) *Réflexions sur les principes fondamentaux de la Théorie des Nombres* (Journal de Liouville, 1845, t. X, pp. 1-101), c. III. n° 11.

(**) Cirodde, *Arithmétique*, 15e édition, p. 309 ; Serret, *Arithmétique*, 6e édition, p. 303.

ans avant Poinsot, M. Catalan, alors à ses débuts, a donné cette démonstration ingénieuse, dans un Recueil que Poinsot devait connaître (*). D'ailleurs, un célèbre lemme de Gauss,

$$B^{\frac{p-1}{2}} = \pm 1 + \mathfrak{M}p, \quad (p \text{ premier})$$

dont le théorème de Fermat est un corollaire évident, a été démontré, en 1808, par l'illustre Géomètre de Gœttingue, au moyen du même artifice de calcul, qui a servi à M. Catalan, en 1842, à Poinsot, en 1845, pour établir le théorème de Fermat (**). Ce lemme, avec la démonstration de Gauss, a été reproduit dans les deux dernières éditions de la *Théorie des nombres*, de Legendre (***). Poinsot l'a donc nécessairement eu sous les yeux; et l'on peut s'étonner qu'il ne l'ait pas cité, non plus que l'article de M. Catalan.

Note du Rédacteur. — I. Le petit travail publié dans le tome I des *Nouvelles Annales* avait été rédigé, en 1836, quand j'étais *Régent* de Mathématiques, au collége de Châlons-sur-Marne. A cette époque, je ne connaissais pas le *théorème d'Euler;* et, on le comprend, je fus tout heureux d'avoir *généralisé le théorème de Fermat* (IV).

II. La démonstration de la formule

$$\varphi(a^\alpha b^\beta c^\gamma \cdots) = a^\alpha b^\beta c^\gamma \cdots \left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\cdots,$$

(*) *Sur les fractions décimales périodiques* (Nouv. Ann. de Math., 1842, t. I, pp. 457-470), nos VI-IX. M. Catalan dit qu'il a emprunté plusieurs des démonstrations contenues dans son article à un écrit intitulé : *De quelques propriétés des nombres et des fractions périodiques*, par M. E. Midy. Paris, Bachelier, 1835, in-4° de 21 pages.

(**) Gauss, OEuvres, t. II, pp. 4-5; *Theorematis arithmetici demonstratio nova*, n° 3 (Anciens Mémoires de Gœttingue, t. XVI, 1808).

(***) IIe édition, 1808, IVe partie, § VII, p. 408; IIIe édition, 1830, t. I, p. 197.

(IV) *Nouvelles Annales*, tome I, p. 464.

exposée dans la *Théorie des nombres*, de Legendre (*), est très-peu satisfaisante. Dans l'intérêt de mon enseignement, j'en cherchai donc une autre. Celle-ci, qu'on peut lire dans les *Nouvelles Annales* (**), a, me semble-t-il, toute la clarté désirable.

III. *Les réflexions sur les principes fondamentaux*..., publiées en 1845, avaient été annoncées, par l'auteur, *trente-quatre ans à l'avance!* Non-seulement, comme le fait observer M. Mansion, Poinsot ne citait ni Gauss ni Legendre; mais il donnait, comme *nouveaux*, de *petits* théorèmes enseignés dans toutes les Écoles préparatoires (***)! Le célèbre Géomètre s'est même cru obligé, paraît-il, de démontrer la formule

$$N = \frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\cdot\frac{c^{\gamma+1}-1}{c-1}\cdots$$

La croyait-il *nouvelle?*

IV. Dans une remarquable Note *sur la théorie des nombres*, que M. Mansion vient de faire paraître, et sur laquelle nous reviendrons, notre honorable Collaborateur signale une *erreur de Poinsot*, relative à cette proposition : *Si l'on a* N *points rangés en cercle, et qu'on les joigne de* h *en* h, h *étant premier à* N, *on passe nécessairement par tous les* N *points, avant de retomber sur le point de départ; et l'on fait nécessairement* h *fois le tour entier de la circonférence.*

Vers 1840, si mes souvenirs sont exacts, je proposais à mes élèves l'*exercice* suivant :

Étant donné le système

$$\begin{aligned} x_1 + x_2 + \cdots + x_p &= a_1, \\ x_2 + x_3 + \cdots + x_{p+1} &= a_2, \\ \cdots\cdots&\cdots\cdots \\ x_n + x_1 + \cdots + x_{p-1} &= a_n; \end{aligned}$$

(*) Troisième édition (1830), tome I, p. 8.

(**) Tome I, p. 466.

(***) En particulier, la démonstration relative à $\varphi(n)$, dont il a été question ci-dessus, se retrouve, presque mot à mot, dans le Mémoire de Poinsot.

trouver dans quel cas il est déterminé, indéterminé, ou impossible.

Or, si l'on écrit ainsi ces équations :

$$x_1 + x_2 \quad + \cdots + x_p = a_1,$$
$$x_{p+1} + x_{p+2} + \cdots + x_{2p} = a_{p+1},$$
$$x_{2p+1} + x_{2p+2} + \cdots + x_{3p} = a_{2p+1},$$
$$\cdots\cdots\cdots\cdots\cdots$$

on trouve (*) que *le système est déterminé si* n *et* p *sont premiers entre eux; et réciproquement.* Cette proposition ne diffère pas du théorème de Poinsot. En outre, elle démontre cette propriété :

Le déterminant des n^2 *nombres*

1,	1,	1,	1,	1,	0,	0,	0,	0,
0,	1,	1,	1,	1,	1,	0,	0,	0,
0,	0,	1,	1,	1,	1,	1,	0,	0,
0,	0,	0,	1,	1,	1,	1,	1,	0,
0,	0,	0,	0,	1,	1,	1,	1,	1,
1,	0,	0,	0,	0,	1,	1,	1,	1,
1,	1,	0,	0,	0,	0,	1,	1,	1,
1,	1,	1,	0,	0,	0,	0,	1,	1,
1,	1,	1,	1,	0,	0,	0,	0,	1

est égal au nombre p *des unités contenues dans chaque ligne, quand* p *est premier avec* n. *Dans le cas contraire, ce déterminant est nul* (**).

(*) *Recherches sur les déterminants*, p. 14 (*Bulletins de l'Académie*, 1846).

(**) Pour fixer les idées, et rendre la figure claire, nous avons supposé $n = 9$, $p = 5$.