

LÉON POMEY

Trois démonstrations des théorèmes de Fermat et de Wilson

Nouvelles annales de mathématiques 4^e série, tome 19
(1919), p. 373-380

http://www.numdam.org/item?id=NAM_1919_4_19__373_1

© Nouvelles annales de mathématiques, 1919, 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/>

[13b]

**TROIS DÉMONSTRATIONS DES THÉORÈMES DE FERMAT
ET DE WILSON;**

PAR M. LÉON POMEY,
Ingénieur des Manufactures de l'État.

Chacune de ces démonstrations établit *simultanément* ces deux théorèmes classiques, qu'on voit ainsi découler d'une même source :

Si p est un nombre premier et a un entier non divisible par lui, p divise $a^{p-1} - 1$ (Fermat) et $(p-1)! + 1$ (Wilson).

PREMIÈRE DÉMONSTRATION.

Le nombre a , étant premier avec p , a pour reste, par rapport au module premier p , un des nombres 1, 2, 3, ..., $p-1$; autrement dit, p divise un des $(p-1)$ nombres $(a-1)$, $(a-2)$, ..., $(a-p+1)$ et par suite leur produit. Ordonnons celui-ci par rapport aux puissances décroissantes de a ; en désignant par Σ_1 la somme des $(p-1)$ premiers entiers, par Σ_2 celle de leurs produits deux à deux, etc., on a la congruence

$$(1) \quad a^{p-1} - \Sigma_1 a^{p-2} + \Sigma_2 a^{p-3} - \dots \\ - \Sigma_{p-2} a + 1.2.3 \dots (p-1) \equiv 0 \pmod{p}.$$

On en obtient d'ailleurs une analogue en remplaçant a par le produit $k.a$, où k est un entier quelconque

non divisible par p ; d'où

$$(2) \quad k^{p-1}a^{p-1} - \Sigma_1 k^{p-2}a^{p-2} + \Sigma_2 k^{p-3}a^{p-3} - \dots \\ - \Sigma_{p-2} ka + (p-1)! \equiv 0 \pmod{p}.$$

Retranchons membre à membre (1) et (2); le terme $(p-1)!$ disparaît, et l'on peut diviser le résultat par a . Il reste alors une congruence de degré $(p-2)$ en a , laquelle est satisfaite pour $(p-1)$ valeurs incongrues deux à deux $\pmod{p}$, savoir $a = 1, 2, \dots, (p-1)$.

Or, d'après un théorème bien connu, le nombre des racines d'une congruence à module premier ne peut être supérieur à son degré, sinon la congruence doit être une identité. Il en résulte que les $(p-1)$ coefficients de la congruence considérée doivent être tous divisibles par p . D'où

$$(3) \quad k^{p-1} - 1 \equiv 0 \pmod{p}; \\ (4) \quad (k^{p-1-n} - 1)\Sigma_n \equiv 0 \pmod{p}, \quad (n = 1, 2, \dots, p-2).$$

La congruence (3) donne le *théorème de Fermat* (il suffit d'y faire $k = a$ pour retomber sur les notations de l'énoncé).

Les congruences (4) montrent que les $(p-2)$ coefficients $\Sigma_1, \Sigma_2, \dots, \Sigma_{p-2}$ sont divisibles par p ; en effet, si l'un d'eux Σ_n ne l'était pas, il en résulterait que la congruence $k^{p-1-n} - 1 \equiv 0$, qui est de degré $(p-1-n)$, aurait les $(p-1)$ racines $k = 1, 2, \dots, (p-1)$, ce qui, d'après le théorème rappelé plus haut, est impossible. En tenant compte de ces divers résultats, la congruence (1) se réduit à

$$1 + (p-1)! \equiv 0 \pmod{p},$$

ce qui est le *théorème de Wilson* (dont la réciproque est évidente) (1).

C. Q. F. D.

(1) Par cette méthode, les deux théorèmes (Fermat-Wilson) sont

REMARQUE. — Nous avons, en outre, obtenu incidemment ce théorème bien connu :

THÉOREME A. — *Les fonctions symétriques simples $\Sigma_1, \Sigma_2, \dots, \Sigma_{p-2}$ des $(p-1)$ premiers nombres entiers sont divisibles par p , quand ce nombre est premier.*

On en déduit immédiatement une *proposition analogue pour les sommes de puissances semblables $S_1, S_2, \dots, S_{p-2}$* au moyen des formules de Newton :

$$S_n - \Sigma_1 S_{n-1} + \Sigma_2 S_{n-2} - \dots + (-1)^n n \Sigma_n = 0 \\ (n = 1, 2, \dots, p-2).$$

DEUXIÈME DÉMONSTRATION.

LEMME. — *Les sommes S_n des puissances d'exposant n des $(p-1)$ premiers entiers sont divisibles par le nombre premier p pour $n=1, 2, \dots, p-2$.*

En effet, on a

$$(x+1)^n - x^n = C_n^1 x^{n-1} + C_n^2 x^{n-2} + \dots + C_n^{n-1} x + 1.$$

En remplaçant x successivement par $1, 2, \dots, (p-1)$ et ajoutant membre à membre, il vient

$$p^n - 1 = C_n^1 S_{n-1} + C_n^2 S_{n-2} + \dots + C_n^{n-1} S_1 + (p-1)$$

ou

$$C_n^1 S_{n-1} + C_n^2 S_{n-2} + \dots + C_n^{n-1} S_1 \equiv 0 \pmod{p}.$$

Puisque $S_1 = p \cdot \frac{p-1}{2}$ est divisible par p , on voit (en

démontrés *simultanément* en prenant pour base le théorème, rappelé dans le texte, sur les congruences. Au contraire (à ma connaissance) les démonstrations qu'on donne du théorème de Wilson en se fondant sur l'emploi du théorème en question supposent toujours en outre le théorème de Fermat démontré au préalable par une autre voie.

faisant ensuite $n = 2, 3, \dots$) qu'il en est de même pour $S_2, S_3, \dots, S_{p-2}$.

DÉMONSTRATION. — Ayant obtenu comme ci-dessus la congruence fondamentale (2), remplaçons-y successivement k par $1, 2, \dots, (p-1)$, et ajoutons membre à membre; d'où

$$(5) \quad S_{p-1} a^{p-1} - \Sigma_1 S_{p-2} a^{p-2} + \Sigma_2 S_{p-3} a^{p-3} - \dots \\ - \Sigma_{p-2} S_1 a + (p-1)1.2\dots(p-1) \equiv 0.$$

En vertu du lemme, cette congruence se réduit à

$$(6) \quad S_{p-1} a^{p-1} - (p-1)! \equiv 0;$$

d'où, pour $a \equiv 1$,

$$(7) \quad S_{p-1} - (p-1)! \equiv 0.$$

En vertu de (7), la congruence (6) devient

$$(8) \quad a^{p-1} - 1 \equiv 0 \pmod{p},$$

ce qui est le *théorème de Fermat*. Inversement, en vertu de (8), les $(p-1)$, termes dont S_{p-1} représente la somme, sont congrus à 1; d'où

$$S_{p-1} \equiv p-1$$

ou

$$(9) \quad S_{p-1} \equiv -1.$$

Donc (7) devient

$$1 + (p-1)! \equiv 0,$$

ce qui est le *théorème de Wilson*.

REMARQUE 1. — On déduit également de là sans peine le *théorème A*.

En effet, en combinant les congruences (6) et (9), on trouve

$$(10) \quad a^{p-1} + (p-1)! \equiv 0.$$

Par suite (1) devient une congruence de degré $(p-2)$ en a , qui a $(p-1)$ racines; c'est donc une identité; d'où

$$\Sigma_1 \equiv \Sigma_2 \equiv \dots \equiv \Sigma_{p-2} \equiv 0 \pmod{p}.$$

REMARQUE II. — Ce théorème A pourrait aussi être déduit directement du lemme (par exemple au moyen des formules de Newton). Alors, en vertu de ce théorème ainsi démontré, la congruence (1) se réduit à la congruence (10); celle-ci, pour $a=1$, donne le *théorème de Wilson*, lequel, inversement, combiné avec (10), fournit le *théorème de Fermat*.

C'est là encore une autre démonstration des deux théorèmes, mais déjà connue, comme je l'ai vu après coup. Elle est moins simple que les précédentes, puisque, contrairement à celles-ci, elle s'appuie à la fois sur le lemme et sur le théorème A.

THROISIÈME DÉMONSTRATION.

La congruence (2), obtenue comme ci-dessus, peut s'écrire

$$(E_k) \quad k^{p-1} a^{p-1} - \Sigma_1 k^{p-2} a^{p-2} + \Sigma_2 k^{p-3} a^{p-3} - \dots \\ - \Sigma_{p-2} k a + \varpi = m_k p,$$

en désignant par ϖ la factorielle $(p-1)!$ et par m_k un certain entier.

En faisant successivement $k=1, 2, \dots, (p-1)$, nous obtenons $(p-1)$ relations $E_1, E_2, \dots, E_{p-1}$, que nous considérerons comme des équations linéaires fournissant (par la règle de Cramer) les valeurs des $(p-1)$ quantités $a^{p-1}, a^{p-2}, \dots, a$. Le déterminant D_0 des coefficients de ces quantités peut s'écrire abrégativement :

$$D(k^{p-1}, -\Sigma_1 k^{p-2}, \Sigma_2 k^{p-3}, \dots, -\Sigma_{p-2} k),$$

en convenant que les éléments figurant dans la paren-

thèse représentent les éléments de la $k^{\text{ième}}$ ligne du déterminant, et que les $1^{\text{re}}, 2^{\text{e}}, \dots, (p-1)^{\text{ième}}$ lignes se déduisent de celle-là en y faisant $k=1, 2, \dots, p-1$. On peut mettre en facteur $-\Sigma_1, \Sigma_2, \dots, -\Sigma_{p-2}$, ainsi que le nombre 1 dans la 1^{re} ligne, 2 dans la $2^{\text{e}}, \dots, k$ dans la $k^{\text{ième}}$, etc...; donc, en tout, le produit $(p-1)!$. Posons

$$(-\Sigma_1)\Sigma_2\dots(-\Sigma_{p-2}) = S \quad \text{ou} \quad (-1)^{\frac{p-1}{2}} (\Sigma_1\Sigma_2\dots\Sigma_{p-3}) = S.$$

On a

$$D_0 = S \pi V,$$

en désignant par V un déterminant de Vandermonde qu'on peut écrire, suivant notre convention :

$$V = D(k^{p-2}, k^{p-3}, \dots, 1).$$

Quand on remplace dans D_0 les éléments de la première colonne par les seconds membres $(m_k p - \pi)$ des équations (E_k) , on obtient le déterminant

$$D_1 = D(m_k p - \pi, -\Sigma_1 k^{p-2}, \Sigma_2 k^{p-3}, \dots, -\Sigma_{p-2} k),$$

et l'on a

$$a^{p-1} = \frac{D_1}{D_0}.$$

Or, D_1 est évidemment une somme, savoir :

$$\begin{aligned} D_1 &= D(m_k p, -\Sigma_1 k^{p-2}, \dots, -\Sigma_{p-2} k) \\ &\quad + D(-\pi, -\Sigma_1 k^{p-2}, \dots, -\Sigma_{p-2} k). \end{aligned}$$

Le premier terme est le produit de (pS) par un certain déterminant D'_1

$$D'_1 = D(m_k, k^{p-2}, \dots, k).$$

Dans le second terme de D_1 , faisons passer la première colonne à la droite, ce qui ne fait que multiplier le

déterminant par $(-1)^{p-2}$, et mettons-y encore $(-\varpi S)$ en facteur. Puisque $(-1)^{p-2} = -1$, ce second terme devient finalement $= S \varpi V = D_0$. On a donc

$$D_1 = p S D'_1 + D_0;$$

d'où

$$a^{p-1} = 1 + p \frac{S D'_1}{D_0} = 1 + p \frac{D'_1}{\varpi V}.$$

Or, le premier membre est un entier; il en est donc de même du dernier terme; mais ϖ et V sont évidemment premiers avec p ; donc D'_1 est divisible par ϖV , ce qui donne le *théorème de Fermat*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Supposons maintenant que les inconnues des $(p-1)$ équations linéaires (E_k) soient les quantités a^{p-2} , a^{p-3} , ..., a , ϖ . Le déterminant Δ_0 de leurs coefficients est

$$\Delta_0 = D(-\Sigma_1 k^{p-2}, -\Sigma_2 k^{p-3}, \dots, -\Sigma_{p-2} k, 1),$$

ou visiblement $\Delta_0 = SV$.

Remplaçons-y les éléments de la dernière colonne de droite par les termes supposés connus des équations (E_k) , savoir $(m_k p - k^{p-1} a^{p-1})$. En tenant compte du théorème de Fermat, ceux-ci deviennent $(m'_k p - 1)$, où m'_k désigne un nouvel entier. On a donc

$$\begin{aligned} \Delta_1 &= D(-\Sigma_1 k^{p-2}, \dots, -\Sigma_{p-2} k, m'_k p - 1) \\ &= p S D(k^{p-2}, \dots, k, m'_k) - SV, \end{aligned}$$

et ϖ a pour expression

$$\varpi = \frac{\Delta_1}{\Delta_0} = \frac{p}{V} D(k^{p-2}, \dots, k, m'_k) - 1.$$

On voit comme ci-dessus que V , premier avec p , doit diviser $D(k^{p-2}, \dots, m'_k)$.

D'où le *théorème de Wilson*

$$(p-1)! \equiv -1 \pmod{p}. \quad \text{C. Q. F. D.}$$

REMARQUE. — En tenant compte des deux théorèmes de Fermat et de Wilson, et faisant $a=1$, (E_k) se réduit à

$$-\Sigma_1 k^{p-2} + \Sigma_2 k^{p-3} - \dots - \Sigma_{p-2} k = M_k p,$$

où M_k désigne un nouvel entier. Ne donnons à k que les valeurs de 1 à $(p-2)$ inclusivement.

Résolvons ce système de $(p-2)$ équations linéaires par rapport à $\Sigma_1, \Sigma_2, \dots, \Sigma_{p-2}$.

Le déterminant de leurs coefficients est

$$T_0 = D(-k^{p-2}, k^{p-3}, \dots, -k) = (-1)^{\frac{p-1}{2}} D(k^{p-3}, \dots, 1);$$

ce dernier déterminant est un déterminant de Vandermonde, dont évidemment aucun facteur n'est divisible par p .

On aura alors

$$\Sigma_n = \frac{T_n}{T_0},$$

en désignant par T_n le déterminant obtenu en remplaçant dans T_0 les coefficients de Σ_n par les seconds $M_k p$. On peut donc mettre p en facteur dans T_n . Puisque T_0 n'est pas divisible par p , on a $\Sigma_n \equiv 0 \pmod{p}$, pour $n=1, 2, \dots, p-2$. Nous retrouvons ainsi le théorème A.