

R. BRICARD

**Pruvo simpla de la Fermat'a teoremo.
Démonstration simple du théorème
de Fermat**

Nouvelles annales de mathématiques 4^e série, tome 3
(1903), p. 340-342

http://www.numdam.org/item?id=NAM_1903_4_3__340_0

© Nouvelles annales de mathématiques, 1903, 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/>

PRUVO SIMPLA DÉMONSTRATION SIMPLE
DE LA FERMAT'A TEOREMO; DU THÉORÈME DE FERMAT;

DE S^o R. BRICARD.

PAR M. R. BRICARD.

Se p estas primo, m entjero iu, la nombro $m^p - m$ estas oblo de p .

Soient p un nombre premier, m un entier quelconque : le nombre $m^p - m$ est multiple de p .

Ni skribu, per la sistemo de nombrofarado m -uma ĉiujn entjerojn p -ciferajn, kies nombro (enhavante la nulon) estas m^p .

Écrivons, dans le système de numération de base m , tous les entiers de p chiffres : leur nombre (y compris zéro) est m^p .

El ĉi tiuj nombroj, la m jenaj :

Parmi ces nombres les m suivants :

$$\begin{aligned} & (0 \ 0 \ \dots \ 0), \\ & (1 \ 1 \ \dots \ 1), \\ & \dots\dots\dots, \\ & (\overline{m-1} \ \overline{m-1} \ \dots \ \overline{m-1}) \end{aligned}$$

konsistas ĉia el unu cifero p -foje ripetita.

sont constitués chacun d'un chiffre répété p fois.

Estu

Soit

$$A_1 = (a \ b \ \dots \ l)$$

unu el la $m^p - m$ aliaj l'un des ' $m^p - m$ autres

numeroj. Mi pretendas *ke* nombros. Je dis *que les*
la p nombroj *p nombres*

$$A_1 = (a \ b \ \dots \ l),$$

$$A_2 = (b \ \dots \ l \ a),$$

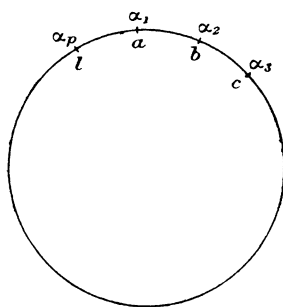
$$\dots\dots\dots,$$

$$A_p = (l \ a \ b \ \dots)$$

kiuj devenas de A₁, per *qui proviennent de A₁, par*
cirkla ŝanĝado, ĉiuj dife- *permutation circulaire,*
rencas unu de la alia. *sont tous différents les uns*
des autres.

Supozinte efektive ke
 (ekzemple) A_1 identas A_h ,
 ni p -onigu cirklon, kaj je
 la dividpunktoj $\alpha_1, \alpha_2, \dots,$
 α_p , ni apudigu la ciferojn
 de A_1 , kiel montras la jena
 figuro.

Supposons en effet que,
 par exemple, A_1 soit iden-
 tique à A_h ; divisons un
 cercle en p parties égales,
 et, à côté des points de divi-
 sion $\alpha_1, \alpha_2, \dots, \alpha_p$, écrivons
 les chiffres de A_1 , comme
 sur la figure suivante.



Se A_h identas A_1 , la
 unua cifero de A_h estas la
 unua cifero de A_1 , t. e. : a .
 Sed la unua cifero de A_h
 estas la h^a cifero de A_1 .
 Sekve, la h^a cifero de A_1 ,

Si A_h est identique à A_1 ,
 le premier chiffre de A_h est
 le premier chiffre de A_1 ,
 c'est-à-dire a . Mais le pre-
 mier chiffre de A_h est le
 $h^{\text{ième}}$ chiffre de A_1 . Par

kiu estas la h^a cifero de A_h , estas a . Sed la h^a cifero de A_h estas la $2h^a$ cifero de A_1 , k. t. p.

Videble, oni povas geometrie esprimi ĉi-tion, dirante :

Se oni alkondukas rektajn de la punkto α_1 al la punkto α_h , de la punkto α_h al la punkto α_{2h} , k. t. p., la ciferoj, apudaj je la vertikoj de la formita regula stelmultangulo, estas samaj.

Sed, ĉar p estas primo, tiu multangulo estas necesse p -angulo. Sekve, la nombro A_1 konsistas el identaj ciferoj, kaj ne povas esti unu el la $m^p - m$ nombroj nun konsiderataj.

De tio rezultas tuj ke tiaj $m^p - m$ nombroj estas p -opigeblaj.

Ĉi tio povas nur okazi, se $m^p - m$ estas entjero dividebla per p .

K. O. D. P.

suite, le h^i ème chiffre de A_1 , c'est-à-dire le h^i ème chiffre de A_h , est a . Mais le h^i ème chiffre de A_h est le $2h^i$ ème chiffre de A_1 , etc.

On voit que l'on peut exprimer géométriquement ce fait, et dire :

Joignons par des droites le point α_1 au point α_h , le point α_h au point α_{2h} , etc. : les chiffres, inscrits à côté des sommets du polygone régulier étoilé ainsi formé, sont identiques.

Mais, comme p est un nombre premier, ce polygone a nécessairement p sommets. Par conséquent le nombre A_1 se compose de chiffres identiques et ne peut être l'un des $m^p - m$ nombres actuellement considérés.

De là résulte immédiatement que ces $m^p - m$ nombres peuvent être répartis par groupes de p .

Cela ne peut avoir lieu que si $m^p - m$ est un nombre entier divisible par p . C. Q. F. D.