DÉMONSTRATION ARITHMÉTIQUE DE L'EXISTENCE D'UNE INFINITÉ DE NOMBRES PREMIERS DE LA FORME nk + 1

Autor(en): **Rotkiewicz, A.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **7 (1961)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **15.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-37138

DÉMONSTRATION ARITHMÉTIQUE DE L'EXISTENCE D'UNE INFINITÉ DE NOMBRES PREMIERS DE LA FORME $nk + 1$

par A. Rotkiewicz (Varsovie)

Le but de cette Note est de donner une démonstration purement arithmétique du théorème suivant:

Théorème. — *Quel que soit le nombre naturel* n, *il existe une infinité de nombres premiers de la forme* nk + 1, *où* k *est un nombre naturel.*

Pour démontrer ce théorème, il suffira évidemment de prouver qu'il existe, pour tout nombre naturel n, au moins un nombre premier de la forme $nk + 1$, où k est un nombre naturel, puisque alors il existe pour tous les nombres naturels n et m au moins un nombre premier de la forme $nmt + 1$, où t est un nombre naturel, et ce nombre premier est évidemment plus grand que m et de la forme $nk + 1$ (pour $k = mt$).

Il est aussi évident que nous pouvons supposer que n est un nombre naturel > 2. Soit donc n un tel nombre, $n = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ — son développement en facteurs premiers, où $q_1 < q_2 < \dots < q_s$. Soit a un nombre naturel tel que $n \mid a$: on aura donc $a > 2$ (puisque $n > 2$). Supposons que pour tout facteur premier p du nombre $a^n - 1$ le nombre a appartient pour le module p à un exposant $< n$. Soit

$$f_n(a) = \prod_{d \mid n} (a^d - 1)^{\mu(n/d)} \tag{1}$$

où $\mu(k)$ est la fonction bien connue de Möbius, et où le produit $\prod_{d \mid n}$ s'étend à tous les diviseurs naturels du nombre n. Si l'on décompose en facteurs premiers chacun des nombres $a^d - 1$, où $d \mid n$, le nombre (1) sera un produit dont les facteurs seront des puissances de nombres premiers aux exposants entiers positifs, négatifs ou nuls. Soit p un de ces facteurs: il existe donc un

nombre naturel $d \mid n$ tel que $p \mid a^d - 1$ et (vu que $d \mid n$) à plus forte raison $p \mid a^n - 1$, donc $(a, p) = 1$ et, comme $n \mid a$, $(n, p) = 1$. Soit δ l'exposant auquel appartient a pour le module p: d'après notre hypothèse, nous aurons donc $\delta < n$. D'après les propriétés connues des exposants auxquels appartiennent les nombres modulo p, des nombres $a^d - 1$, où $d \mid n$ ces et seulement ces sont divisibles par p, pour lesquels $\delta \mid d$, c'est-à-dire seulement ces qui ont la forme δk, où k est un nombre naturel tel que $\delta k \mid n$, donc tel que $k \mid \frac{n}{\delta}$. Vu que $p \mid a^n - 1$, on a $\delta \mid n$ et le nombre $\frac{n}{\delta}$ est naturel, plus grand que 1, puisque $\delta < n$.

Soit p^λ la plus grande puissance du nombre p qui divise $a^\delta - 1$: on aura donc $p^\lambda \mid a^\delta - 1$ et $p^{\lambda+1} \nmid a^\delta - 1$. Si pour un nombre naturel $k \mid \frac{n}{\delta}$ il était $p^{\lambda+1} \mid a^{\delta k} - 1$, alors, vu l'identité

$$\frac{a^{\delta k} - 1}{a^\delta - 1} = ((a^\delta)^{k-1} - 1) + ((a^\delta)^{k-2} - 1) + \ldots + (a^\delta - 1) + k$$

on aurait $p \mid k$, ce qui est impossible, vu que $k \mid n$ et $(n, p) = 1$. Donc, pour tout nombre naturel $k \mid \frac{n}{\delta}$, la plus grande puissance du nombre p qui divise $a^{\delta k} - 1$ est p^λ. Il en résulte que dans le développement du nombre (1) le nombre p figure avec l'exposant

$$\sum_{k \mid \frac{n}{\delta}} \lambda \mu\left(\tfrac{n}{\delta k}\right)$$

Or, comme $\frac{n}{\delta}$ est un nombre naturel > 1, on conclut d'après la propriété connue de la fonction μ que

$$\sum_{k \mid \frac{n}{\delta}} \mu\left(\tfrac{n}{\delta k}\right) = \sum_{k \mid \frac{n}{\delta}} \mu(k) = 0.$$

Cela étant pour tout facteur premier p de (1), il en résulte que $f_n(a) = 1$.

Or on a, d'après (1):

$$f_n(a) = \prod_{d \mid n} (a^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d \mid q_1 q_2 \ldots q_s} (a^{\frac{n}{d}} - 1)^{\mu(d)}, \tag{2}$$

puisque, comme on sait, $\mu(d) = 0$ lorsque d est divisible par un carré d'un entier > 1. Soit $b = a^{q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \dots q_s^{\alpha_s - 1}}$: ce sera donc un nombre naturel $\geqslant a > 2$ et on aura $b^{q_1 q_2 \dots q_s} = a^n$, donc, d'après (2):

$$f_n(a) = \prod_{d \mid q_1 q_2 \dots q_s} (b^{q_1 q_2 \dots q_s / d} - 1)^{\mu(d)}.$$

Donc $f_n(a)$ est un quotient de deux polynômes en b aux coefficients entiers. Examinons quelles sont les plus petites puissances de b (aux exposants naturels) qui figurent dans le numérateur et dans le dénominateur de ce quotient. Distinguons deux cas: s pair et s impair. Si s est pair, alors on obtient dans le numérateur la plus petite puissance de b évidemment pour $d = q_1 q_2 \dots q_s$: ce sera la puissance b^1, et, comme on le voit sans peine, le reste de la division du numérateur par b^2 sera $b - 1$ ou bien $b^2 - b + 1$. Or, dans le dénominateur (d'après $q_1 < q_2 < \dots < q_s$) on obtient la plus petite puissance de b à l'exposant naturel pour $d = q_2 q_3 \dots q_s$: ce sera donc la puissance b^{q_1} et le reste de la division du dénominateur par b^2 sera 1 ou bien $b^2 - 1$. D'après $f_n(a) = 1$ on a donc une contradiction, puisque, comme $b > 2$, les nombres $b - 1$ et $b^2 - b + 1$ sont distincts des nombres 1 et $b^2 - 1$. Si s est impair, on obtient dans le numérateur la plus petite puissance de b à l'exposant naturel pour $d = q_2 q_3 \dots q_s$, et dans le dénominateur pour $d = q_1 q_2 \dots q_s$ et, comme plus haut, on en aboutit à une contradiction.

L'hypothèse que pour tout facteur premier p du nombre $a^n - 1$ le nombre a appartient pour le module p à un exposant $< n$ implique donc une contradiction. Nous avons ainsi démontré que le nombre $a^n - 1$ a au moins un diviseur premier p tel que a appartient pour le module p à l'exposant n. Or, comme $(a, p) = 1$ (puisque $p \mid a^n - 1$), on a (d'après le théorème de Fermat) $p \mid a^{p-1} - 1$ et il en résulte, comme on sait, que $n \mid p - 1$, donc que $p = nk + 1$, où k est un nombre naturel.

Nous avons ainsi démontré qu'il existe pour tout nombre naturel $n > 1$ au moins un nombre premier p de la forme $nk + 1$, où k est un nombre naturel, et il en résulte, comme nous savons, notre théorème.

NOTE BIBLIOGRAPHIQUE DE LA RÉDACTION

P.-G. LEJEUNE DIRICHLET [1]) a démontré le résultat général suivant: dans toute progression arithmétique (ensemble des entiers $a + bn$, où n décrit l'ensemble de tous les entiers rationnels) dont le premier terme a et la raison b sont premiers entre eux, il existe une infinité de nombres premiers. La démonstration de DIRICHLET utilise les propriétés des séries analytiques $L(s, \chi)$, qui généralisent la fonction $\zeta(s)$ de RIEMANN.

Atle SELBERG [2] a donné récemment une démonstration « arithmétique » de ce résultat, c'est-à-dire une démonstration qui n'utilise pas les propriétés des fonctions de variables complexes et de leurs intégrales. Mais cette démonstration, longue et difficile, utilise des approximations asymptotiques de fonctions arithmétiques. H. ZASSENHAUS [3]) a donné une démonstration qui utilise les propriétés des nombres algébriques.

Au cours des XIX^{e} et XX^{e} siècles, plusieurs auteurs ont donné des démonstrations élémentaires pour des valeurs particulières du premier terme a et de la raison b.

La démonstration ci-dessus de A. ROTKIEWICZ est élémentaire et valable pour des valeurs de a et b plus étendues que les valeurs considérées antérieurement.

---

1) LEJEUNE DIRICHLET, *Œuvres*. Berlin, 1889. Tome 1, p. 315.

2) Atle SELBERG, *Annals of mathematics*. Tome 50, pp. 297-304 (1949) et *Canadian journal of mathematics*. Tome 2, pp. 66-78 (1950).

3) Hans ZASSENHAUS, *Commentarii mathematici helvetici*. Tome 22, pp. 232-259 (1949).