Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

A. Rotkiewicz

Sur les polynómes en x qui pour une infinité de nombres naturels x donnent des nombres pseudopremiers

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **36** (1964), n.2, p. 136–140.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1964_8_36_2_136_0>

Teoria dei numeri. — *Sur les polynômes en x qui pour une infinité de nombres naturels x donnent des nombres pseudopremiers.* Nota di A. ROTKIEWICZ, presentata (*) dal Socio straniero W. SIERPIŃSKI.

On appelle *pseudopremiers* les nombres composés n, tels que $n \mid 2^n - 2$. Dans le travail [3] j'ai démontré que si a et b sont des nombres naturels premiers entre eux, il existe une infinité de nombres naturels x pour lesquels $ax + b$ est un nombre pseudopremier. Pour les polynômes du premier degré est donc vraie la proposition qui correspond au théorème de Dirichlet pour les nombres premiers. Or, on ne connait aucun polynôme du degré > 1 d'une variable x dont on pourrait démontrer qu'il donne des nombres premiers pour une infinité de nombres naturels x. Autrement est pour les nombres pseudopremiers, où l'on peut démontrer les théorèmes suivants.

THÉORÈME 1. – *Pour tout nombre naturel n il existe une infinité de polynômes en x du degré n aux coefficients entiers, irréductibles, qui donnent des nombres pseudopremiers pour une infinité de nombres naturels x.*

THÉORÈME 2. – *Pour tout nombre naturel* $n > 1$ *il existe un polynôme en x du degré n, réductible, qui donne des nombres pseudopremiers pour une infinité de nombres naturels x.*

LEMME 1. – *Si m et n sont des nombres naturels premiers entre eux, le polynôme* $2^m x^n - 1$ *donne, pour une infinité de nombres naturels x, des nombres pseudopremiers.*

Démonstration du lemme 1. – Soient m et n des nombres naturels premiers entre eux. D'après le théorème du travail [3], il existe une infinité de nombres naturels k tels que $nk + m$ est un nombre pseudopremier. Alors le nombre $2^{nk+m} - 1$ est aussi pseudopremier (voir [8]). Or $2^{nk+m} - 1 = 2^m (2^k)^n - 1$.

Le polynôme $f(x) = 2^m x^n - 1$ donne donc pour $x = 2^k$ (où k est un nombre naturel pour lequel $nk + m$ est un nombre pseudopremier) des nombres pseudopremiers.

Démonstration du théorème 1. – Vu qu'il existe pour tout nombre naturel n une infinité de nombres naturels m premiers avec n, il reste à démontrer que le polynôme $2^m x^n - 1$ est pour $(m, n) = 1$ irréductible. Pour le prouver nous profiterons du théorème de K. Th. Vahlen et A. Capelli d'après lequel le binôme $x^n - A$, où A est un nombre naturel, est réductible dans ce et seulement dans ce cas s'il existe un nombre premier p tel que $p \mid n$ et $A = b^p$, où b est nombre naturel.

Si le polynôme $2^m x^n - 1$ était réductible, il serait le même pour le polynôme $x^n - 2^m$ et, d'après le théorème de Th. Vahlen et A. Capelli, il exi-

(*) Nella seduta dell'8 febbraio 1964.

sterait un nombre premier $p \mid n$ et un nombre naturel b tels que $2^m = b^p$, ce qui est impossible, vu que $(m, n) = 1$.

Le théorème 1 se trouve ainsi démontré.

LEMME 2. – *Si n est un nombre naturel > 1 et p est un nombre premier de la forme $\varphi(n(2^n - 1))k + 1$ plus grand que $2^n - 1$, alors le nombre* $N = \frac{2^{np} - 1}{2^n - 1}$ *est pseudopremier.*

Démonstration du lemme 2. – Vu que $p > 2^n - 1 > n$, on a $(2^p - 1, 2^n - 1) = 2^{(n,p)} - 1 = 2^1 - 1 = 1$, donc $1 < 2^p - 1 \mid \frac{2^{np} - 1}{2^n - 1} = N$. Or, on a $N > 2^{n(p-1)} \geq 2^{2(p-1)} > 2^p - 1$ et le nombre N est composé. On a

$$N - 1 = \frac{2^{np} - 2^n}{2^n - 1} = \frac{2^n(2^{n(p-1)} - 1)}{2^n - 1}. \tag{1}$$

Soit $n = 2^\alpha m$, où $(m, 2) = 1$. Le nombre premier p étant de la forme $\varphi(n(2^n - 1))k + 1$, d'après $m \mid n$ on a $\varphi(m(2^n - 1)) \mid \varphi(n(2^n - 1)) \mid p - 1$, d'où :

$$m(2^n - 1) \mid 2^{\varphi(m(2^n-1))} - 1 \mid 2^{p-1} - 1 \mid 2^{n(p-1)} - 1,$$

donc, d'après (1),

$$m \mid N - 1. \tag{2}$$

Comme $2^n > n = 2^\alpha m$, on a $n > \alpha$ et $2^\alpha \mid 2^n$ et il résulte de (1) et (2) que

$$n \mid N - 1. \tag{3}$$

Comme $p \mid 2^{p-1} - 1$, $p > 2^n - 1 > n$, il résulte de (1) que $p \mid N - 1$ et, d'après (3) on a $np \mid N - 1$. Donc $N = \frac{2^{np} - 1}{2^n - 1} \mid 2^{np} - 1 \mid 2^{N-1} - 1$ et N est un nombre pseudopremier. Le lemme 2 est ainsi démontré.

Démonstration du théorème 2. – Soit $f(x) = \frac{x^n - 1}{2^n - 1}$. Il résulte du théorème de Dirichlet qu'il existe une infinité de nombres premiers p de la forme $\varphi(n(2^n - 1))k + 1$ (J'ai donné une démonstration élémentaire de la proposition qu'il existe pour tout nombre naturel m une infinité de nombres premiers de la forme $mx + 1$ dans le travail [5]). Vu que le nombre $f(2^p) = \frac{2^{np} - 1}{2^n - 1}$ est pseudopremier, il existe une infinité de nombres naturels x pour lesquels le nombre $f(x)$ est pseudopremier.

Comme l'a remarqué M. A. Schinzel, il en résulte que le polynôme

$$g(t) = f[(2^n - 1)t + 2] = \frac{[(2^n - 1)t + 2]^n - 1}{2^n - 1},$$

du degré n et aux coefficients entiers, donne pour une infinité de valeurs naturels t des nombres pseudopremiers. Le polynôme $g(t)$ est réductible, puisque $(2^n - 1)t + 1 \mid g(t)$.

Comme $2^n - 1 \mid 2^{\varphi(2^n-1)} - 1 \mid 2^{p-1} - p$, le nombre $\frac{2^p - 2}{2^n - 1}$ est entier et, d'après le lemme 2 le nombre $g\left(\frac{2^p - 2}{2^n - 1}\right) = \frac{2^{np} - 1}{2^n - 1}$ est pseudopremier. Le théorème 2 est ainsi démontré.

THÉORÈME 3. – *Les polynômes* $f(x) = x^p - 1$, *où* p *est un nombre premier, et* $g(x) = (x^{2^n} + 1)(x^{2^{n+1}} + 1)$, *où* $n = 0, 1, 2$, *donnent pour une infinité de nombres naturels* x *des nombres pseudopremiers.*

Démonstration du théorème 3. – D'après le théorème 2 du travail [4] il existe pour tout nombre premier p une infinité de nombres naturels n, tels que np est un nombre pseudopremier. Alors le nombre $f(2^n) = (2^n)^p - 1 = 2^{np} - 1$ est aussi pseudopremier et il existe une infinité des nombres naturels x, pour lesquels $f(x)$ est un nombre pseudopremier.

Or, soit $g(x) = (x^{2^n} + 1)(x^{2^{n+1}} + 1)$, où $n = 0, 1, 2, \cdots$ et soit $x = 2^{2^m}$, où $m = 2, 3, \cdots$ Or aura $g(2^{2^m}) = (2^{2^{n+m}} + 1)(2^{2^{n+m+1}} + 1)$, ce qui est un nombre pseudopremier, puisque les nombres $(2^{2^k} + 1)(2^{2^{k+1}} + 1)$ sont pour $k = 2, 3, \cdots$ pseudopremiers, ce qui a prouvé M. Cipolla dans le travail [2]. La démonstration du théorème 3 est ainsi achevée.

THÉORÈME 4. – *Il existe une infinité de nombres naturels impairs* x, *pour lesquels les nombres* $f_1(x) = x$, $f_2(x) = 2x - 1$, $f_3(x) = 3x - 2$, $f_4(x) = 2x^2 - x$, $f_5(x) = 3x^2 - 2x$, $f_6(x) = 6x^2 - 7x + 2$, $f_7(x) = 6x^3 - 7x^2 + 2x$ *sont à la fois pseudopremiers.*

Démonstration du théorème 4. – Dans le travail [6] j'ai démontré qu'il existe une infinité de nombres naturels x tels que les nombres x, $2x - 1$ et $3x - 2$ sont pseudopremiers. De la démonstration de cette proposition résulte qu'on a alors les formules $x \mid 2^{x-1} - 1$, $2x - 1 \mid 2^{x-1} - 1$, $3x - 2 \mid 2^{x-1} - 1$. (Dans le travail [6] j'ai démontré que si ces formules ont lieu pour un nombre naturel x, elles restes vraies lorsqu'on y remplace x par le nombre $\frac{2^{2x-1} + 1}{3} > x$, et qu'elles sont vraies pour le nombre $x = \frac{2^{37} + 1}{3}$). Les nombres x, $2x - 1$ et $3x - 2$ étant deux à deux premiers entre eux, et vu que $x - 1 \mid x(2x - 1) - 1$, $x - 1 \mid x(3x - 2) - 1$, $x - 1 \mid (2x - 1)(3x - 2) - 1$, $x - 1 \mid x(2x - 1)(3x - 2) - 1$ on a $f_4(x) = x(2x - 1) \mid 2^{x-1} - 1 \mid 2^{f_4(x)-1} - 1$, $f_5(x) = x(3x - 2) \mid 2^{x-1} - 1 \mid 2^{f_5(x)-1} - 1$, $f_6(x) = (2x - 1)(3x - 2) \mid 2^{x-1} - 1 \mid 2^{f_6(x)-1} - 1$, $f_7(x) = x(2x - 1)(3x - 2) \mid 2^{f_7(x)-1} - 1$ et les nombres $f_i(x)$ $(i = 1, 2, \cdots, 7)$ sont pseudopremiers. Le théorème 4 est ainsi démontré.

THÉORÈME 5. – *Il existe une infinité de nombres naturels* n *impairs, tels que les nombres* n, $2n + 1$ *et* $6n + 1$ *sont pseudopremiers.*

LEMME 3. – *Si les nombres* n, $2n + 1$ *et* $6n + 1$ *sont pseudopremiers et* $3n(2n + 1)$, *alors pour* $N = \frac{2^{2n} - 1}{3} > n$ *les nombres* N, $2N + 1$ *et* $6N + 1$ *sont pseudopremiers et* $3N(2N + 1)$.

Démonstration du lemme 3. – Soient n, $2n + 1$ et $6n + 1$ des nombres pseudopremiers, $N = \frac{2^{2n} - 1}{3}$ et $3n(2n + 1)$. Alors $2N + 1 =$

$= \frac{2^{2n+1}+1}{3}$, $6N+1 = 2^{2n+1}-1$ et, comme dans le travail [6] on démontre que ces nombre sont pseudopremiers et que $3N(2N+1)$.

Démonstration du théorème 5. – Vu le lemme 3 il reste à trouver un nombre impair n tel que n, $2n+1$ et $6n+1$ sont des nombres pseudopremiers et $3n(2n+1)$. Tel est le nombre $n = \frac{2^{2\cdot 41}-1}{3}$. En effet on a alors $2n+1 = \frac{2^{83}+1}{3}$, $6n+1 = 2^{83}-1$ et on vérifié que ces nombres sont composés. Comme $n-1 = \frac{4^{41}-4}{3}$, $2n = \frac{2^{83}-2}{3}$, $6n = 2^{83}-2$, on a $2\cdot 41 \mid n-1$, $2\cdot 83 \mid 2n$, $2\cdot 83 \mid 6n$, d'où $n \mid 2^{2\cdot 41}-1 \mid 2^{n-1}-1$, $2n+1 \mid 2^{2\cdot 83}-1 \mid 2^{2n}-1$, $6n+1 \mid 2^{83}-1 \mid 2^{6n}-1$, et on vérifie sans peine que $3n(2n+1)$. Le théorème 5 est ainsi démontré.

THÉORÈME 6. – *Il existe une infinité de nombres naturels impairs n, tels que les nombres n et $10n-3$ sont pseudopremiers.*

Démonstration du théorème 6. – D'après le théorème 5 il existe une infinité de nombres imparis n, tels que les nombres n et $2n+1$ sont pseudopremiers. Alors les nombres $N = \frac{2^{2n}+1}{5}$ et $10N-3 = 2^{2n+1}-1$ sont aussi pseudopremiers. En effet, le nombre $2n+1$ étant pseudopremier, le nombre $2^{2n+1}-1$ est aussi pseudopremier. Or, on a

$$N = \frac{\left(2^n+1+2^{\frac{n+1}{2}}\right)\left(2^n+1-2^{\frac{n+1}{2}}\right)}{5}$$

et, vu que $2^n+1-2^{\frac{n+1}{2}} > 5$ et $2^n+1+2^{\frac{n+1}{2}} > 5$ (puisque $n \geq 341$), le nombre N est composé. Comme $N-1 = \frac{(2^n-2)(2^n+2)}{5}$, on a $4n \mid N-1$, d'où : $N \mid 2^{4n}-1 \mid 2^{N-1}-1$ et N est un nombre pseudopremier. Le théorème 6 est ainsi démontré.

THÉORÈME 7. – *Il existe une infinité de nombres naturels x tels que*

a) *les nombres $2x^2-1$, $2x^4-1$ et $2x^6-1$ sont pseudopremiers,*

b) *les nombres $2x^2-1$, $8x^4-1$ et $128x^{12}-1$ sont pseudopremiers,*

c) *les nombres $2x^2-1$ et $128x^{20}-1$ sont pseudopremiers.*

Démonstration du théorème 7. – D'après le théorème 4 il existe une infinité de nombres naturels impairs n, tels que les nombres n, $2n-1$ et $3n-2$ sont pseudopremiers. Il en résulte qu'il existe une infinité de nombres naturels k tels que les nombres $2k+1$, $4k+1$ et $6k+1$ sont pseudopremiers. Alors les nombres

$$2^{2k+1}-1 = 2(2^k)^2-1 \quad , \quad 2^{4k+1}-1 = 2(2^k)^4-1 \quad \text{et} \quad 2^{6k+1}-1 = 2(2^k)^6-1$$

sont aussi pseudopremiers et les polynômes $2x^2-1$, $2x^4-1$ et $2x^6-1$ donnent des nombres pseudopremiers pour une infinité de nombres naturels x.

La démonstration des cas *b*) et *c*) est analogue, où il faut appliquer les théorèmes 5 et 6.

HYPOTHÈSE H_1 – *s étant un nombre naturel et* $f_1(x), f_2(x), \cdots, f_s(x)$ *des polynômes en x aux coefficients entiers, où le coefficient de la plus haute puissance de x est positif, deux à deux premiers entre eux et satisfaisant à la condition* S_1. *Il n'existe aucun entier* >1 *qui divise le produit* $f_1(x), f_2(x) \cdots f_s(x)$ *quel que soit l'entier x, alors il existe une infinité de nombres naturels x pour lesquels chacun des nombres* $f_1(x), f_2(x), \cdots, f_s(x)$ *est pseudopremiers.*

On obtient l'hypothèse H_1 de l'hypothèse H de M. A. Schinzel (voir [7]) en y remplaçant les nombres premiers par les nombres pseudopremiers et en remplaçant la condition que les polynômes $f_1(x), f_2(x), \cdots, f_s(x)$ soient irréductibles par celle qu'ils soient deux à deux premiers entre eux.

TRAVAUX CITÉS.

[1] A. CAPELLI, *Sulla irriducibilità della funzione* $x^n - A$ *in campo qualunque di razionalità*, «Math. Annalen», *54*, 602–603 (1901).

[2] M. CIPOLLA, *Sui numeri composti* P, *che verificano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$, «Annali di Matematica», *9*, 139–160 (1904).

[3] A. ROTKIEWICZ, *Sur les nombres pseudopremiers de la forme* $ax + b$, «Comptes rendus Acad. Sciences, Paris», *257*, 2601–2604 (1963).

[4] —, *Sur les nombres p et q tels que* $pq \mid 2^{pq} - 2$, «Rendiconti del Circolo Matematico di Palermo», *11*, 280–282 (1962).

[5] —, *Démonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme* $nk + 1$, «Enseignement Mathématique», *7*, 277–280 (1962).

[6] —, *Sur les progressions arithmétiques et géométriques formées de trois nombres pseudopremiers distincts*, sous presse dans les «Acta Arithmetica».

[7] A. SCHINZEL et W. SIERPIŃSKI, *Sur certaines hypothèses concernant les nombres premiers*, «Acta Arithmetica», 185–208, *4* (1958).

[8] W. SIERPIŃSKI, *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n - 2)/n$, «Colloquium Mathematicum», *1*, 9 (1947).

[9] K. H. VAHLEN, *Über reductible Binome*, «Acta Mathematica», *19* 195–198 (1895).