

# COMPOSITIO MATHEMATICA

ANDRÉ SCHINZEL

## Démonstration d'une conséquence de l'hypothèse de Goldbach

*Compositio Mathematica*, tome 14 (1959-1960), p. 74-76

[http://www.numdam.org/item?id=CM\\_1959-1960\\_\\_14\\_\\_74\\_0](http://www.numdam.org/item?id=CM_1959-1960__14__74_0)

© Foundation Compositio Mathematica, 1959-1960, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) 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/>

## Démonstration d'une conséquence de l'hypothèse de Goldbach.

par

André Schinzel

M. W. Sierpinski a déduit récemment (d'une façon élémentaire) de l'hypothèse connue de Goldbach la proposition suivante:

**THÉORÈME 1.** *k et m étant deux nombres naturels donnés quelconques, il existe des nombres premiers p et q aussi grands que l'on veut et tels que*

$$(1) \quad 2k \equiv p + q \pmod{m}^1).$$

M. Sierpinski m'a posé la question si l'on pourrait démontrer le théorème 1 sans faire appel à l'hypothèse de Goldbach. La même question il a posé pour le théorème 2 qu'on obtient en remplaçant dans le théorème 1 la formule (1) par la formule

$$(2) \quad 2k \equiv p - q \pmod{m}.$$

Je donnerai ici une démonstration tout à fait élémentaire des théorèmes 1 et 2, en utilisant le théorème de Lejeune-Dirichlet sur la progression arithmétique (dont les démonstrations élémentaires sont connues).

**LEMME.** *Si f(x) est un polynôme en x aux coefficients entiers, tel qu'il n'existe aucun nombre naturel d > 1 qui divise f(x) quel que soit l'entier x, et si m est un nombre naturel, il existe un entier x<sub>0</sub> tel que*

$$(3) \quad (f(x_0), m) = 1.$$

Démonstration du lemme. Pour  $m = 1$  le lemme est évident. Soit donc  $m > 1$  et soit  $m = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$  le développement de  $m$  en facteurs premiers. Soit  $i$  un des nombres  $1, 2, \dots, s$ . D'après l'hypothèse sur le polynôme  $f(x)$ , le nombre  $q_i$  ne peut pas être un diviseur de  $f(x)$  quel que soit l'entier  $x$ . Il en résulte qu'il existe un entier  $x_i$  tel que  $f(x_i) \not\equiv 0 \pmod{q_i}$ . D'après un théorème connu sur

---

<sup>1)</sup> Voir l'article de W. Sierpinski *Sur une conséquence de l'hypothèse de Goldbach* qui paraîtra (en polonais) dans le journal *Wiadomosci Matematyczne*.

les restes, il existe un nombre  $x_0$  tel que  $x_0 \equiv x_i \pmod{q_i}$  pour  $i = 1, 2, \dots, s$ , ce qui donne

$$f(x_0) \equiv f(x_i) \not\equiv 0 \pmod{q_i} \quad \text{pour } i = 1, 2, \dots, s,$$

d'où  $(f(x_0), q_i) = 1$  pour  $i = 1, 2, \dots, s$ , ce qui donne l'égalité (3) et notre lemme se trouve démontré.

Soit maintenant  $k$  un entier donné et soit  $f(x) = x(x+2k)$ . On aura  $f(1) = 2k+1$  et  $f(-1) = -(2k-1)$  et, comme évidemment  $(2k-1, 2k+1) = 1$ , il en résulte qu'il n'existe aucun nombre naturel  $> 1$  qui divise  $f(x)$  quel que soit l'entier  $x$ . Le polynôme  $f(x)$  satisfait donc aux conditions de notre lemme, d'après lequel on conclut que,  $m$  étant un nombre naturel donné, il existe un entier  $x_0$  tel que  $(x_0(x_0+2k), m) = 1$ , d'où  $(x_0, m) = (x_0+2k, m) = 1$  et aussi  $(-x_0, m) = 1$ . D'après le théorème de Dirichlet il existe donc des nombres premiers  $p, p_1$  et  $q$  aussi grands que l'on veut et des entiers  $t, t_1$  et  $u$  tels que  $p = mt+x_0$ ,  $p_1 = mt_1-x_0$  et  $q = mu+x_0+2k$ , d'où  $p-q \equiv 2k \pmod{m}$  et  $p_1+q \equiv 2k \pmod{m}$ . Les théorèmes 1 et 2 se trouvent ainsi démontrés.

Il est à remarquer que, dans le même ordre d'idées, M. W. Sierpinski a récemment démontré les deux théorèmes suivants:

**THÉORÈME 3.**  *$m$  étant un nombre naturel donné, il existe pour tout nombre premier  $p$  suffisamment grand, un nombre premier  $q$  aussi grand que l'on veut et tel que  $2^p-1 \equiv q \pmod{m}$ .*

**THÉORÈME 4.**  *$m$  étant un nombre naturel donné et  $n$  un nombre naturel suffisamment grand, il existe une infinité de nombres premiers  $p$  tels que  $2^{2^n}+1 \equiv p \pmod{m}$ .*

Démonstration du théorème 3. Comme on sait, si  $p$  et  $p'$  sont des nombres premiers distincts, on a  $(2^p-1, 2^{p'}-1) = 1$ . Il en résulte tout de suite que pour tout nombre naturel  $m$  il existe un nombre  $\mu_m$  tel que pour tout nombre premier  $p > \mu_m$  on a  $(2^p-1, m) = 1$ . Donc, si  $p$  est un nombre premier  $> \mu_m$ , il résulte du théorème de Dirichlet l'existence des nombres premiers  $q$  aussi grands que l'on veut qui sont termes de la progression arithmétique  $mk+2^p-1$  ( $k = 1, 2, \dots$ ), donc tels que  $2^p-1 \equiv q \pmod{m}$ . Le théorème 3 est ainsi démontré.

Démonstration du théorème 4. Comme on sait, si  $k$  et  $n$  sont des nombres naturels distincts, on a  $(2^{2^k}+1, 2^{2^n}+1) = 1$ . Il en résulte tout de suite que,  $m$  étant un nombre naturel donné, on a

pour  $n$  naturels suffisamment grands:  $(2^{2^n} + 1, m) = 1$ . D'après le théorème de Dirichlet il en résulte l'existence d'une infinité de nombres premiers  $p$  tels que  $2^{2^n} + 1 \equiv p \pmod{m}$ . Le théorème 4 est ainsi démontré.

(Oblatum 25-7-58).

Sandomierz (Pologne).