

SUR L'ÉQUATION DIOPHANTINNE $2^x - xy = 2$

A. Rotkiewicz et W. Sierpiński

(Présenté le 9 mars 1964)

Le but de cette Note est de démontrer d'une façon élémentaire les cinq théorèmes suivants:

Théorème 1. *L'équation*

$$(1) \quad 2^x - xy = 2$$

a une seule solution en nombres premiers x et y notamment $x=3$, $y=2$.

Démonstration. Pour $x=2$ on trouve de (1) $y=1$, ce qui n'est pas un nombre premier. Or, si x est un nombre premier > 2 , y est pair, donc, s'il est premier, $y=2$ et (1) donne $2^{x-1} = x+1$, ce qui est vrai pour $x=3$. Si x est un nombre premier > 3 , on a $x \geq 5$, d'où $2^{x-1} > x+1$ (ce qu'on démontre sans peine par l'induction). L'équation (1) a donc en nombres premiers x et y seulement la solution $x=3$, $y=2$, c. q. f. d.

Théorème 2. *L'équation (1) a une infinité de solutions en nombres composés x et y .*

Démonstration. Les nombres naturels composés n tels que $n \mid 2^n - 2$ sont appelés pseudopremiers. Comme on sait, il existe une infinité de nombres pseudopremiers impairs (ce qui est démontré d'une façon élémentaire dans [1]). Si x est un tel nombre, le nombre $y = \frac{2^x - 2}{x}$ est évidemment pair > 2 , puisque $2^{x-1} > x+1$ pour x composés. Les nombres x et y sont donc composés.

Théorème 3. *Il existe une infinité de solutions de l'équation (1), où x est un nombre premier et y un nombre naturel composé.*

Démonstration. Soit x un nombre premier > 3 . D'après le théorème de Fermat, le nombre $y = \frac{2^x - 2}{x} > 2$ est naturel et pair (vu que x est impair), donc composé.

Théorème 4. *Il n'existe aucune solution de l'équation (1), où x est un nombre composé et y un nombre premier.*

Démonstration. Supposons qu'il existe une solution de l'équation (1), où x est un nombre composé et y un nombre premier. Il résulte de (1) que $y = \frac{2^x - 2}{2}$ et x étant composé, on a ici $x > 3$. Si x était impair, y serait un

nombre pair > 2 , donc composé, contrairement à l'hypothèse. Le nombre x est donc pair, soit $x = 2n$, où n est un nombre naturel > 1 .

Soit δ l'exposant auquel appartient le nombre 2 modulo n . Comme $n > 1$, on a $\delta > 1$. D'autre part, comme on sait, $\delta \mid \varphi(n)$ donc $\delta \leq \varphi(n)$. Vu que $n \mid 2^{2n-1} - 1$, on a $\delta \mid 2n - 1$, donc $2n - 1 = \delta r$, où r est un nombre naturel et, vu que $\delta \leq \varphi(n) < n$ (puisque $n > 1$) et que $2n - 1 > n$ (puisque $n > 1$), on a $r > 1$. Distinguons maintenant deux cas:

1) $n \neq 2^\delta - 1$. Alors, vu que $n \mid 2^\delta - 1$, on a

$$(2) \quad n < 2^\delta - 1.$$

Or, $y = \frac{2^{2n-1} - 1}{n} = \frac{2^{\delta r} - 1}{n} = \frac{2^{\delta r} - 1}{2^\delta - 1} \cdot \frac{2^\delta - 1}{n}$ et, vu que $r > 1$ et, vu l'inégalité (2), chacun de deux facteurs de y est > 1 , donc y est un nombre composé, contrairement à l'hypothèse.

2) $n = 2^\delta - 1$. Nous prouverons d'abord que $r > \delta$.

En effet, vu que $n = 2^\delta - 1$, $2n - 1 = \delta r$, on a $2(2^\delta - 1) - 1 = \delta r$, d'où $r = \frac{2^{\delta+1} - 3}{\delta} > \delta$ (puisque, comme on le démontre facilement par l'induction, $2^{\delta+1} - 3 > \delta^2$ pour $\delta > 1$).

Or, comme $2^\delta - 1 \mid 2^{\delta r} - 1$, $2^r - 1 \mid 2^{\delta r} - 1$, on a

$$\frac{(2^\delta - 1)(2^r - 1)}{2^{(\delta, r)} - 1} = \frac{(2^\delta - 1)(2^r - 1)}{(2^\delta - 1, 2^r - 1)} \mid 2^{\delta r} - 1,$$

d'où

$$(3) \quad (2^\delta - 1)(2^r - 1) \mid (2^{(\delta, r)} - 1)(2^{\delta r} - 1).$$

D'autre part, on a

$$y = \frac{2^{2n-1} - 1}{n} = \frac{2^{\delta r} - 1}{2^\delta - 1} = \frac{(2^{(\delta, r)} - 1)(2^{\delta r} - 1)}{(2^\delta - 1)(2^r - 1)} \cdot \frac{2^r - 1}{(2^{(\delta, r)} - 1)},$$

où, d'après (3), chacun de deux facteurs pour y est naturel.

Comme $r > \delta$, on a

$$\frac{2^r - 1}{(2^{(\delta, r)} - 1)} > \frac{2^r - 1}{2^\delta - 1} > 1.$$

Pareillement, vu que $\delta \geq 2$:

$$\frac{2^{\delta r} - 1}{(2^\delta - 1)(2^r - 1)} > \frac{2^{2r} - 1}{(2^\delta - 1)(2^r - 1)} > \frac{2^{2r} - 1}{(2^r - 1)(2^r - 1)} = \frac{2^r + 1}{2^r - 1} > 1.$$

Les deux facteurs du nombre y sont donc > 1 et le nombre y est composé, contrairement à l'hypothèse. Le théorème 4 se trouve ainsi démontré.

De nos quatre théorèmes résulte sans peine ce

Corollaire. *Toutes les solutions de l'équation (1) en nombres naturels x et y sont celles, où x est un nombre premier ou pseudo-premier quelconque et $y = \frac{2^x - 2}{x}$. Si $x > 3$, y est toujours un nombre composé.*

Or, nous ne savons pas s'il existe des solutions de l'équation (1), où x et y sont des nombres pseudopremiers.

Dans le travail [2] il est démontré (d'une façon élémentaire) qu'il existe une infinité de nombres triangulaires impairs x , tels que $x \mid 2^x - 2$. Il en résulte tout de suite le

Théorème 5. *L'équation (1) a une infinité de solutions où x est un nombre triangulaire et y un nombre naturel pair.*

Or, le problème reste ouvert s'il existe une infinité de solutions de l'équation (1), où x est un nombre naturel et y un nombre triangulaire.

TRAVAUX CITÉS

[1] W. Sierpiński, *Remarque sur une hypothèse des Chinois concernant les nombres $(2^n - 2)/n$* , Colloquium Math., Vol. 1 (1947), p. 9.

[2] A. Rotkiewicz, *Sur les nombres pseudopremiers triangulaires*, Elemente der Mathematik (sous presse).