SUR L'ÉQUATION
$x^2 + 7 = 2^n$

Maurice MIGNOTTE

RAMANUJAN avait noté que l'équation

$$x^2 + 7 = 2^n$$

possède les solutions $n = 3, 4, 5, 7, 15$, sans trouver d'autres solutions. En 1948, NAGELL, le premier, montra que ce sont les seules solutions. D'autres preuves ont été données par BROWKIN et SCHINZEL, SKOLEM, CHOWLA et LEWIS, CHOWLA, DUNTON et LEWIS, MORDELL, ... HASSE a écrit un article présentant ces diverses solutions. La preuve qui suit a été publiée par l'auteur en 1984.

• Si n est pair :

Dans ce cas on peut écrire l'équation :

$$(x - 2^{n/2})(x + 2^{n/2}) = -7.$$

Puisque les seules décompositions en facteurs premiers de -7 sont $1 \times (-7)$ et $(-1) \times (7)$, l'un des facteurs est négatif et l'autre positif. En cherchant x positif on a nécessairement

$$\left.\begin{aligned} x - 2^{n/2} &= -1 \\ x + 2^{n/2} &= 7 \end{aligned}\right\}$$

dont la résolution conduit à $n = 4$ (puis $x = 3$) qui est alors la seule solution paire.

• Si n est impair :

Nous posons $n = 2m + 1$ et $y = 2^m$, ce qui permet d'écrire l'équation sous la forme :

$$x^2 - 2y^2 = -7, \text{ avec } y > 0.$$

L'idée est de travailler dans l'anneau $\mathbb{Z}[\sqrt{2}]$, ensemble des nombres de la forme $a + b\sqrt{2}$ avec a et b dans $\mathbb{Z}$. Cet **anneau est principal**, c'est-à-dire qu'entre autre il y a unicité de la décomposition en facteurs premiers (aux unités près). Les **unités ou éléments inversibles** sont de la forme $\pm\varepsilon^s$, avec $s \in \mathbb{Z}$ et $\varepsilon = 1 + \sqrt{2}$. Dans cet anneau, -7 admet la factorisation en éléments premiers $(1 + 2\sqrt{2})(1 - 2\sqrt{2})$. L'équation s'écrit alors

$$\begin{aligned}(x + y\sqrt{2})(x - y\sqrt{2}) &= (1 + 2\sqrt{2})(1 - 2\sqrt{2}) \\ &= \delta\varepsilon^s(1 + 2\sqrt{2})\delta\varepsilon^{-s}(1 - 2\sqrt{2}) \text{ avec } \delta = \pm 1.\end{aligned}$$

Par identification, nous obtenons les deux cas :

$$\begin{cases} x + y\sqrt{2} = \delta\varepsilon^s(1+2\sqrt{2}) \\ x - y\sqrt{2} = \delta\varepsilon^{-s}(1-2\sqrt{2}) \end{cases} \text{ ou } \begin{cases} x + y\sqrt{2} = \delta\varepsilon^s(1-2\sqrt{2}) \\ x - y\sqrt{2} = \delta\varepsilon^{-s}(1+2\sqrt{2}). \end{cases}$$

D'autre part, comme dans chacun des cas les premiers membres sont conjugués, les deuxièmes membres doivent l'être aussi, ce qui n'est possible que si s est pair car le conjugué de ε est $(-\varepsilon)^{-1}$.

Enfin, comme nous pouvons toujours nous limiter à $x > 0$, nous voyons que dans le premier cas $\delta = +1$ et $s > 0$ et dans le deuxième $\delta = -1$ et $s > 0$. Les deux cas peuvent alors s'écrire :

$$\begin{cases} x + y\sqrt{2} = \varepsilon^s(1+2\sqrt{2}) \\ x - y\sqrt{2} = (-\varepsilon)^{-s}(1-2\sqrt{2}) \\ s \text{ pair} \end{cases} \text{ ou } \begin{cases} x + y\sqrt{2} = -\varepsilon^s(1-2\sqrt{2}) \\ x - y\sqrt{2} = -(-\varepsilon)^{-s}(1+2\sqrt{2}) \\ s \text{ pair} \end{cases}$$

et en tirant y nous obtenons (toujours avec s pair) :

$$y = \frac{1}{2\sqrt{2}}\left(\varepsilon^s - (-\varepsilon)^{-s}\right) + \left(\varepsilon^s + (-\varepsilon)^{-s}\right) \text{ ou } y = \frac{-1}{2\sqrt{2}}\left(\varepsilon^s - (-\varepsilon)^{-s}\right) + \left(\varepsilon^s + (-\varepsilon)^{-s}\right)$$

et nous remarquons que l'on passe d'un cas à l'autre en remplaçant s par $-s$. Notons $y_s = \frac{1}{2\sqrt{2}}\left(\varepsilon^s - (-\varepsilon)^{-s}\right) + \left(\varepsilon^s + (-\varepsilon)^{-s}\right)$.

Il est facile de vérifier que la suite y_s est donnée par :

$$y_0 = 2 \ ; \ y_1 = 3 \ ; \ y_{s+2} = 2y_{s+1} + y_s \qquad s \in \mathbb{Z}$$

(il suffit de vérifier la récurrence pour ε^s et $(-\varepsilon)^{-s}$). Les solutions de l'équation initiale sont à rechercher parmi les y_s correspondant à s pair.

• La question est de savoir si y_s peut être une puissance de 2. L'exploration pour les petites valeurs de s donne les solutions indiquées au début de l'article pour $s = -6, -2, 0, 2$ correspondant respectivement à $n = 15, 5, 7, 3$ ($m = 7, 2, 3, 1$). Or, si y_s est une puissance de 2, il est divisible par 2^p (et le quotient vaut 2^q), d'où l'idée d'étudier les valeurs de la suite y_s modulo 2^p pour p pas trop grand. Les petites solutions ayant été trouvées, plaçons-nous dans le cas $m \geq 8$, soit $2^m \geq 256 = 8 \times 32$.

L'étude de la suite y_s modulo 8 donne : $y_0 \equiv 2, y_1 \equiv 3, y_2 \equiv 0, y_3 \equiv 3, y_4 \equiv 6, y_5 \equiv 7, y_6 \equiv 4, y_7 \equiv 7, y_8 \equiv 2, y_9 \equiv 3$ et par conséquent

$$y_s \equiv 0 \pmod 8 \Longleftrightarrow s \equiv 2 \pmod 8.$$

On peut donc, pour limiter un peu les calculs, se contenter d'étudier la suite $u_t = \frac{1}{8}y_{8t-6}$, qui est définie par $u_0 = 16, u_1 = 1, u_{t+2} = 1154u_{t+1} - u_t$ (ici encore

il suffit de vérifier la récurrence pour ε^{8t-6} et $(-\varepsilon)^{-(8t-6)}$ après avoir calculé les deux premiers termes).

L'étude de la suite u_s modulo 32 se simplifie en : $u_0 \equiv 16, u_1 \equiv 1, u_{t+2} \equiv 2u_{t+1} - u_t$. Il en résulte que l'on a $u_t \equiv t \pmod{32}$ lorsque t est impair et $u_t \equiv 16 + t \pmod{32}$ quand t est pair, comme le montre une récurrence immédiate. Par conséquent, si $y = 2^m$ avec $m \geq 8$, alors $y = 8u_t$ pour un certain $t \equiv 16$ modulo 32.

• Nous allons maintenant revenir à la suite u_t, l'étudier modulo un autre nombre, et montrer que pour $t \equiv 16 \pmod{32}$ u_t ne peut pas être une puissance de 2. Pour cela, nous allons choisir un nombre premier p tel que dans $\mathbb{Z}/p\mathbb{Z}$, 2 soit un carré parfait. On dit alors que **2 est résidu quadratique modulo p**. Cela a lieu pour $p = 8k \pm 1$. Si nous montrons que, pour $t \equiv 16 \pmod{32}$, u_t n'est pas résidu quadratique modulo p, il ne pourra pas être une puissance de 2 et par conséquent le problème n'aura pas d'autres solutions que celles trouvées par RAMANUJAN.

Il nous faut choisir ce nombre premier p de façon que, modulo p, la suite u_t ait une période pas trop longue et multiple de 32 pour qu'il n'y ait qu'un petit nombre de termes u_t différents avec $t \equiv 16 \pmod{32}$. De plus, ces termes ne doivent pas être résidus quadratiques modulo p. Quelques tâtonnements conduisent à prendre $p = 7681 = 8(2^6 \times 3 \times 5) + 1$, en prenant pour k des petits facteurs.

Modulo 7681, on vérifie que la suite u_t a une période égale à 64 et que $u_{16} \equiv 4214$ et $u_{48} \equiv -4214$. Pour montrer qu'aucun de ces deux nombres n'est résidu quadratique nous utiliserons le **symbole de Legendre** et **la loi de réciprocité quadratique**. Rappelons que le symbole de LEGENDRE $(\frac{a}{p})$ note la quantité $a^{\frac{p-1}{2}}$ modulo p (premier impair). Cette quantité vaut +1 ou -1 selon que a est ou n'est pas résidu quadratique modulo p. On a évidemment $(\frac{a}{p}) \times (\frac{b}{p}) = (\frac{ab}{p})$ mais surtout, la loi de réciprocité quadratique, pour p et q premiers impairs :

$$(\frac{q}{p}) = (-1)^{\frac{p-1}{2}} \times \frac{q-1}{2}(\frac{p}{q}).$$

Or, pour $p = 7681$, -1 et 2 sont résidus quadratiques et par suite :

$$(\frac{\pm 4214}{p}) = (\frac{\pm 1}{p})(\frac{2}{p})(\frac{49}{p})(\frac{43}{p}) = (\frac{p}{43}) = (\frac{27}{43}) = (\frac{3}{43}) = -(\frac{43}{3}) = -1.$$

ce qui achève la démonstration.

• En regardant cette démonstration d'un peu plus près, on constate que l'on a même prouvé le résultat suivant :

Théorème : Les équations $x^2 - 2^{17}y^4 = -7$ et $x^2 - 2^{19}y^4 = -7$ n'ont pas de solutions en nombres entiers.

Références

H. HASSE.— *Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung, Nagoya Math. J.*, **27**, 1966, p. 77–102.