PELL-FERMAT toujours d'actualité

Christian Jeanbrau (Orsay)
Charles Notari (Montaut)

Fermat avait déjà posé la question à FRENICLE DE BESSY, en signalant qu'elle était "de grande difficulté" : *«Tout nombre non carré est de telle nature qu'il y a infinis carrés qui, multipliant ledit nombre, font un carré moins 1»*. Euler l'a appelé par erreur "Equation de Pell", nous la connaissons aujourd'hui sous la forme $a^2 - b^2d = \varepsilon$, où $\varepsilon = 1$ ou -1, et nous l'appelons "Equation de Pell-Fermat". d est un entier naturel sans facteur carré, au moins égal à 2. Les inconnues sont a et b. Cette équation est d'ailleurs une équation diophantienne (Diophante : grec, 325 - 409), $P(a, b) = 0$, où P est un polynôme à coefficients dans $\mathbb{Z}$ mais son étude systématique date de Fermat (1601 - 1665).

L'équation de Pell-Fermat, nous l'avons rencontrée

Qui ne connaît pas, au moins de nom, le problème des *"Bœufs du soleil"* posé et résolu par Archimède (287 - 212 avant J.C.) ?

> Ami, si tu as la sagesse en partage, apporte un grand soin à calculer à combien s'élevait la multitude des bœufs du Soleil qui, jadis, dans les plaines de l'île de la Sicile thrinacienne, paissaient, répartis en quatre troupeaux de couleurs différentes, l'un blanc de lait, l'autre d'un noir luisant, le troisième brun et le quatrième tavelé. Il y avait dans chaque troupeau un

nombre considérable de taureaux répartis dans les proportions suivantes: imagine, mon ami, que les blancs étaient en nombre égal à la moitié augmentée du tiers des taureaux noirs, et augmentée de tous les bruns, tandis que les noirs étaient en nombre égal aux quatrième et cinquième parties des tavelés, accrues de tous les bruns. Considère, d'autre part, que les tavelés restants, étaient en nombre égal aux sixième et septième parties des blancs, accrues de tous les bruns. Les vaches étaient réparties de la manière suivante: les blanches étaient en nombre précisément égal aux troisième et quatrième parties de tout le troupeau noir, tandis que les noires étaient de nouveau en nombre égal aux quatrième et cinquième parties des tavelées qui étaient toutes venues paître en compagnie des taureaux. Les tavelées étaient, d'autre part, en nombre égal aux cinquième et sixième parties de tout le troupeau brun, tandis que les brunes étaient en nombre égal à la moitié de la troisième partie accrue de la septième partie du troupeau blanc.

Ami, si tu me dis exactement combien il y avait de bœufs du Soleil, quel était en particulier le nombre des taureaux gras et en particulier le nombre des vaches pour chacune des couleurs, on ne te qualifiera ni d'ignorant ni de malhabile en matière de nombres; mais tu ne pourras cependant pas encore compter parmi les savants. Dès lors, observe encore les diverses manières dont les bœufs du Soleil étaient disposés: lorsque les taureaux blancs joignaient leur multitude aux noirs, ils se maintenaient en un groupe compact, ayant la même mesure en profondeur qu'en largeur et ce carré remplissait entièrement les immenses plaines de la Thrinacie. D'autre part, les bruns et les tavelés réunis, sans que les taureaux d'autres couleurs fussent présents ou sans qu'ils manquassent, étaient groupés de telle sorte que, le premier rang étant constitué par un seul, ils formaient graduellement une figure triangulaire.

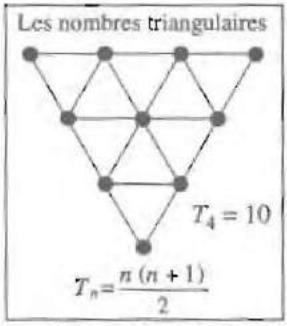
Ami, si tu trouves toutes ces choses de pair , et si, en un mot, concentrant tes esprits, tu exprimes toutes les mesures de ces multitudes, va, te glorifiant d'avoir remporté la victoire, et persuadé que l'on te juge complètement consommé dans cette science.

(cité dans *«Arithmétique et théorie des nombres"* de J. Itard, Collection Que sais-je?)

Si W, X, Y, Z (resp. w, x, y, z) désignent le nombre des bœufs (resp. vache) blancs, noirs, tavelés et bruns, mettre l'énoncé en équations conduit à :

$W = 10\,366\,482k$, $X = 7\,460\,514k$, $Y = 7\,358\,060k$, $Z = 4\,149\,387k$, $w = 7\,206\,360k$, $x = 4\,893\,246k$, $y = 3\,515\,820k$, $z = 5\,439\,213k$ (k entier)

conditions auxquelles il faut ajouter que $W + X$ soit un carré, et $Y + Z$ un



nombre triangulaire. La première de ces contraintes donne $k = 957 \times 4657n^2$ (n entier), la seconde $Y + Z = p(p + 1)/2$, soit $8(Y + Z)^2 + 1 = 2p^2(p + 1) + 1$, carré d'un nombre impair $(2t + 1)$. Ainsi, $(2t + 1)^2 = 8(Y + Z)^2 + 1$, ou encore :

$$(2t + 1)^2 = 4102864232784 24n^2 + 1$$

C'est une équation de Pell-Fermat du type $x^2 - Ay^2 = 1$, et on démontre que le problème est toujours possible.

Euler (1707-1783), lui aussi, posa dans son "Algèbre", deux problèmes élémentaires relevant de la même équation :

- *«Trouver tous les nombres triangulaires qui sont en même temps des carrés»*.

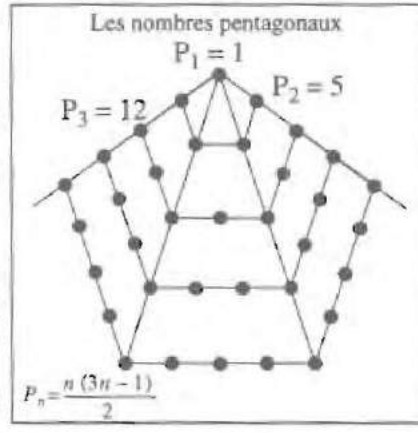
On est ramené à $n(n + 1)/2 = m^2$, qui se transforme en $8m^2 + 1 = (2n + 1)^2$, ou $(2n + 1)^2 - 8m^2 = 1$, autre équation de Pell-Fermat.

- *«Trouver tous les nombres triangulaires qui sont en même temps pentagones»*.

On arrive à $n(n + 1) = m(3m - 1)$ soit, en introduisant :

$x = 2n + 1$ et $y = 6m - 1$

$3(2n + 1)^2 - 3 = (6m - 1)^2 - 1$, ou $y^2 - 3x^2 = -2$, équation que Fermat dit savoir résoudre dès lors qu'on connaît la solution (1, 1).



Un dernier exemple de tel problème :

- *«Trouver deux entiers différant de 2 dont le produit soit le triple du produit de deux entiers consécutifs»*. Celui-ci donne : $m(m + 2) = 3p(p + 1)$, qui se transforme en :

$$(2(m + 1))^2 - 3(2p + 1)^2 = 1.$$

Les exemples, historiques ou non, ne manquent pas, et leur résolution, au cours des âges, n'a pas toujours été simple. Nous donnerons ici, en essayant d'en simplifier l'exposé, quelques principes de résolution.

Etude générale de l'équation de Pell-Fermat.

Remarquons d'abord que l'équation de Pell-Fermat correspondant à $\varepsilon = -1$ n'a pas toujours de solution. En effet, $a^2 - 3b^2 = -1$ donne, modulo 3 $a^2 \equiv 2$, ce qui est impossible. Il n'y a possibilité de solution que si (-1) est résidu quadratique de d, c'est-à-dire si (-1) est un carré dans $\mathbf{Z}/d\mathbf{Z}$.

Par contre, l'équation de Pell-Fermat correspondant à $\varepsilon = 1$, au-delà de la solution triviale $(1, 0)$, a toujours une solution. Une démonstration de ce résultat est indiquée par Jean ITARD ("Que sais-je", n°1093 : *"Arithmétique et théorie des nombres"*), à partir des travaux de DIRICHLET (allemand, 1805-1859).

La solution fondamentale :

Le couple (A, b) étant une solution de l'équation de Pell-Fermat, il en est de même de $(a, -b)$, $(-a, b)$ et $(-a,-b)$. On peut donc se restreindre au cas où a et b sont positifs.

On appellera *solution fondamentale* le plus petit couple (a, b) de $\mathbb{N} \times \mathbb{N}^*$ vérifiant cette équation. La recherche de ce couple se met théoriquement en place à partir du développement en fraction continue de $\sqrt{d}$. On trouve quelques indications sur ce type de développement dans J. Itard. Plus élémentairement, pour de "petites" valeurs de d, on peut procéder par tâtonnements :

b décrivant $\mathbb{N}^*$, un test sur le couple $(d.b^2 - 1, d.b^2 + 1)$ permet de déterminer le cas où l'une de ces quantités est un carré. Le premier couple (a_1, b_1) ainsi déterminé est solution fondamentale soit de $a^2 - d.b^2 = -1$, soit de $a^2 - d.b^2 = 1$.

Dans ce premier cas, on peut écrire :

$$a_1^2 - d.b_1^2 = -1 \Rightarrow \left(a_1^2 - d.b_1^2\right)^2 = 1 \Rightarrow \left(a_1^2 + d.b_1^2\right)^2 - \left(2a_1b_1\right)^2 = 1$$

On peut démontrer alors (ici, admis) que le couple $\left(a_1^* = a_1^2 + d.b_1^2,\ b_1^* = 2a_1b_1\right)$ constitue la solution fondamentale de l'équation : $a^2 - d.b^2 = 1$. La démarche par tâtonnements fournit donc, outre la solution fondamentale de l'une des deux équations (P-F), une réponse théorique : si elle fournit directement la solution associée à $\varepsilon = 1$, c'est que l'équation est impossible pour $\varepsilon = -1$. La justification est immédiate : si $a^2 - d.b^2 = 1$., alors pour tout entier naturel n $\left(a_1^2 - d.b_1^2\right)^n = 1$, et l'équation

$a^2 - d.b^2 = -1$ ne peut pas avoir de solution.

Algorithme de détermination élémentaire de la solution fondamentale.

En italique : *les commentaires*. Le symbole ← est le symbole d'affectation).

```
DEBUT
Sasir d
a ← 0; b ← 0 ;    initialisation de a et b
Faire
      b ← b + 1 ;
      a ← √(db² - 1)
      si non (a entier) alors a ← √(db² + 1) ;
Jusqu'à (a entier) ;
Afficher ('Solution fondamentale : (', a,
                                    ',',b,')') ;
FIN.
```

Donnons une traduction de cet algorithme adaptée par exemple à un sous-ensemble "Pascal" disponible sur calculatrice programmable (ici : Texas Instrument TI 74). Les commentaires sont en italique.

```
Program PF ;
Var   b,d : integer ;
      a : real ; pour pouvoir affecter √(...)
BEGIN

{$w-}
Write('d= ') ;
Readln(d) ;
{$w+}

Writeln('Etude pour d= ',d) ;
a:=sqrt(2) ; valeur arbitraire non entière de a en
             vue condition while...
b:=0 ;
While ((Round(a) - a)<>0 do
      begin
```

```
        b:=b+1 ;
        a:=sqrt(d*sqrt(b)-1) ;
        If((Round(a)-a)<>0) thena:=sqrt(d*sqrt(b)+1);
        end ;
Writeln('Resultat _ Solution_Fondamentale :');
Writeln('a= 'round(a),' ;b= ',b);

END.
```

A l'aide de ce programme, on obtient, pour d non carré de 2 à 21

d	2	3	5	6	7	8	10	11	12	13
a	1	2	2	5	8	3	3	10	7	18
b	1	1	1	2	3	1	1	3	2	5

d	14	15	17	18	19	20	21
a	15	4	4	17	170	9	55
b	4	1	1	4	39	2	12

Solution générale de l'équation (P-F)

La solution fondamentale étant supposée obtenue, il reste à déterminer la forme générale des solutions. On va présenter le problème en dégageant une suite de solutions dont on montrera ensuite qu'elles répondent entièrement à la question.

Cas $\varepsilon = 1$

On dispose du couple (a_1 , b_1) : $a_1^2 - d.b_1^2 = 1$

Trivialement, on en déduit, pour tout n de IN* :

$$\left(a_1 - b_1.\sqrt{d}\right)^n.\left(a_1 + b_1.\sqrt{d}\right)^n = 1$$

par simple utilisation du binome et identification, on met en évidence (a_n , b_n), couple d'entiers naturels tels que : $a_n^2 - d.b_n^2 = 1$.

Il suffit de poser $\left(a_1 + b_1.\sqrt{d}\right)^n = a_n + b_n.\sqrt{d}$ d'où $\left(a_1 - b_1.\sqrt{d}\right)^n = a_n - b_n.\sqrt{d}$

La suite (a_n , b_n) est solution de l'équation (P-F).

Cas $\varepsilon = -1$

On dispose du couple (a_1 , b_1) : $a_1^2 - d.b_1^2 = -1$.

On en déduit (même type d'approche que $\varepsilon = 1$; binome et identifi-

cation) une suite de solutions de l'équation de Pell-Fermat, $(\alpha_n\ \beta_n)$, $n \geq 0$, par

$(a_1 + b_1\sqrt{d})^{2n+1} = \alpha_n + \beta_n\sqrt{d}$ d'où $(a_1 - b_1\sqrt{d})^{2n+1} = \alpha_n - \beta_n\sqrt{d}$

A-t-on dans les deux cas dégagé toutes les solutions dans $\mathbb{N} \times \mathbb{N}^*$ de l'équation (P-F)? Il est assez clair que cette question est la seule à examiner, les solutions dans $\mathbf{Z} \times \mathbf{Z}$ se déduisant immédiatement de celles dans $\mathbb{N} \times \mathbb{N}^*$.

J. Itard propose une démonstration simple à ce sujet, fondée sur une détermination récurrente de la suite $(a_n\ ,\ b_n)$ [resp. $(\alpha_n\ \beta_n)$,]. On peut s'en inspirer.

Les formules de résolution

$\varepsilon = 1$

$$a_{n+1} + b_{n+1}\sqrt{d} = (a_n + b_n\sqrt{d})(a_1 + b_1\sqrt{d})$$
$$= (a_1a_n + db_1b_n) + ((a_1b_n + b_1a_n)\sqrt{d})$$

d'où : (a_1, b_1) solution fondamentale et, pour $n \geq 1$:

$$a_{n+1} = a_1a_n + db_1b_n \ ;\ b_{n+1} = a_1b_n + b_1a_n$$

$\varepsilon = -1$

$$\alpha_{n+1} + \beta_{n+1}\sqrt{d} = (\alpha_n + \beta_n\sqrt{d})(a_1 + b_1\sqrt{d})^2$$
$$= (\alpha_n + \beta_n\sqrt{d})\left[(a_1^2 + db_1^2) + (2a_1b_1)\sqrt{d}\right]$$

d'où : (a_1, b_1) solution fondamentale

$$a_1^* = a_1^2 + db_1^2 \ ;\ b_1^* = 2a_1b_1$$

$\alpha_0 = a_1$; $\beta_0 = b_1$ et, pour $n \geq 0$:

$$\alpha_{n+1} = a_1^*\alpha_n + db_1^*\beta_n \ ;\ \beta_{n+1} = b_1^*\alpha_n + a_1^*\beta_n$$

Remarque : On notera que ces récurrences sont de programmation immédiate. On notera aussi que l'expression explicite directe en fonction de n des suites ainsi mises en évidence s'obtient par :

$\varepsilon = 1$ $\quad a_n = \dfrac{1}{2} \cdot \left\{(a_1 + b_1\sqrt{d})^n + (a_1 - b_1\sqrt{d})^n\right\}$

$$b_n = \left(\frac{1}{2}\sqrt{d}\right) \cdot \left\{(a_1 + b_1\sqrt{d})^n - (a_1 - b_1\sqrt{d})^n\right\}$$

$\underline{\varepsilon = -1}$ $\alpha_n = \frac{1}{2} \cdot \left\{ \left(a_1 + b_1\sqrt{d}\right)^{2n+1} + \left(a_1 - b_1\sqrt{d}\right)^{2n+1} \right\}$

$$\beta_n = \left(\frac{1}{2}\sqrt{d}\right) \cdot \left\{ \left(a_1 + b_1\sqrt{d}\right)^{2n+1} - \left(a_1 - b_1\sqrt{d}\right)^{2n+1} \right\}$$

La démonstration

Les suites (a_n), (b_n), (α_n), (β_n) sont trivialement (cf. les récurrences) strictement croissantes dans $\mathbb{N}$, par $b_1 \neq 0$, $a_1 = 1$. Si donc un couple (x, y) de $\mathbb{N} \times \mathbb{N}^*$ est solution, on peut déterminer n tel que :

$$a_n \leq x < a_{n+1} \qquad (\text{resp. } \alpha_n \leq x < \alpha_{n+1})$$

On en déduit immédiatement en relisant l'équation (P-F):

$$b_n \leq y < b_{n+1} \qquad (\text{resp. } \beta_n \leq y < \beta_{n+1})$$

d'où :

$\underline{\varepsilon = 1}$ $a_n + b_n\sqrt{d} \leq x + y\sqrt{d} < a_{n+1} + b_{n+1}\sqrt{d}$

$\underline{\varepsilon = -1}$ $\alpha_n + \beta_n\sqrt{d} \leq x + y\sqrt{d} < \alpha_{n+1} + \beta_{n+1}\sqrt{d}$

En multipliant par $\left(a_n - b_n\sqrt{d} > 0\right)$ $\left[\text{resp. } \beta_n\sqrt{d} - \alpha_n > 0\right]$, il vient :

$\underline{\varepsilon = 1}$ $1 \leq \left(x + y\sqrt{d}\right)\left(a_n - b_n\sqrt{d}\right) < a_1 + b_1\sqrt{d}$

$\underline{\varepsilon = -1}$ $1 \leq \left(x + y\sqrt{d}\right)\left(\beta_n\sqrt{d} - \alpha_n\right) < a_1^* + b_1^*\sqrt{d}$

On définit alors, $\ddot{a}_1$, $\breve{b}_1$, $\ddot{a}_1^*$, $\breve{b}_1^*$ par :

$$\left(x + y\sqrt{d}\right)\left(a_n - b_n\sqrt{d}\right) = \left(xa_n - ydb_n\right) + \left(ya_n - xb_n\right)\sqrt{d} = \ddot{a}_1 + \breve{b}_1\sqrt{d}$$

$$\left(x + y\sqrt{d}\right)\left(\beta_n\sqrt{d} - \alpha_n\right) = \left(yd\beta_n - x\alpha_n\right) + \left(x\beta_n - y\alpha_n\right)\sqrt{d} = \ddot{a}_1^* + \breve{b}_1^*\sqrt{d}$$

Soit :

$$\ddot{a}_1 = xa_n - ydb_n \;\; ; \;\; \ddot{a}_1^* = yd\beta_n - x\alpha_n$$

$$\breve{b}_1 = ya_n - xb_n \;\; ; \;\; \breve{b}_1^* = x\beta_n - y\alpha_n$$

En notant que :

$$\ddot{a}_1 - \breve{b}_1\sqrt{d} = \left(y - x\sqrt{d}\right)\left(a_n + b_n\sqrt{d}\right) \text{ et } \ddot{a}_1^* - \breve{b}_1^*\sqrt{d} = -\left(x - y\sqrt{d}\right)\left(\beta_n\sqrt{d} + \alpha_n\right)$$

on peut écrire : $\ddot{a}_1^2 - d\breve{b}_1^2 = 1$; $\ddot{a}_1^{*2} - d\breve{b}_1^{*2} = -1$.

On voit ainsi que les couples $(\ddot{a}_1, \breve{b}_1)$ et $(\ddot{a}_1^*, \breve{b}_1^*)$ sont solution de

l'équation (P-F) dans $\mathbb{N} \times \mathbb{N}$ (le contrôle de leur appartenance à $\mathbb{N} \times \mathbb{N}$ est immédiat).

Or, on a : $\quad 1 \leq \ddot{a}_1 + \bar{b}_1\sqrt{d} < a_1 + b_1\sqrt{d}$

$$1 \leq \ddot{a}_1^* + \bar{b}_1^*\sqrt{d} < a_1^* + b_1^*\sqrt{d}$$

Si $\bar{b}_1$ (resp. $\bar{b}_1^*$) est non nul, alors (a_1, b_1) (resp. (a_1^*, b_1^*)) n'est pas la solution fondamentale annoncée. On en déduit donc $\bar{b}_1 = 0$ (resp. $\bar{b}_1^* = 0$) d'où l'on tire sans difficulté : $(x, y) = (a_n, b_n)$ (resp. $(x, y) = (\alpha_n, \beta_n)$)

Bilan :

Toute solution dans $\mathbb{N} \times \mathbb{N}^*$ de l'équation de Pell-Fermat est bien une solution $\{(a_n, b_n) ; n \geq 1\}$ (resp. $\{(\alpha_n, \beta_n) ; n \geq 0\}$).

En conclusion :

On dispose au terme de ce qui précède, d'une démarche globale permettant d'étudier complètement l'équation (P-F) : $a^2 - db^2 = \varepsilon$, où $\varepsilon = 1$ ou -1.

➡ Si $\varepsilon = 1$, l'équation a toujours une solution. On commence par déterminer sa solution fondamentale (a_1, b_1), et la suite (a_n, b_n) telle que $\left(a_1 + b_1\sqrt{d}\right)^n = a_n + b_n\sqrt{d}$.

➡ Si $\varepsilon = -1$, l'équation n'a de solution que si ε est résidu quadratique de d dans $\mathbb{Z}/d\mathbb{Z}$ et la suite des solutions est alors (α_n, β_n) telle que $\left(a_1 + b_1\sqrt{d}\right)^n = \alpha_n + \beta_n\sqrt{d}$ est solution.

Application à la résolution du problème cité au début :

Trouver deux entiers différant de 2 dont le produit soit le triple de celui de deux entiers consécutifs.

Il s'agissait de résoudre en (m, p) élément de $\mathbb{N} \times \mathbb{N}$:

$$[2(m + 1)]^2 - 3(2p + 1)^2 = 1$$

(P-F) $\quad a^2 - db^2 = \varepsilon$; $\varepsilon = 1$ et $d = 3 \Rightarrow a_1 = 2$ et $b_1 = 1$

D'où la suite (a_n, b_n) des solutions dans $\mathbb{N} \times \mathbb{N}$ de cette équation (P-F) déterminée soit par la récurrence :

$$a_{n+1} = 2a_n + 3b_n \qquad b_{n+1} = a_n + 2b_n$$

soit explicitement par :

$$a_n = \frac{1}{2} \cdot \left[(2+\sqrt{3})^n + (2-\sqrt{3})^n\right] \text{ et } b_n = \frac{1}{2}\sqrt{3} \cdot \left[(2+\sqrt{3})^n - (2-\sqrt{3})^n\right]$$

Par $2(m+1) = a_n$ et $2p+1 = b_n$, il vient explicitement, sous réserve de discussion sur n (a_n pair et b_n impair ?) :

$$m = \frac{1}{4} \cdot \left[(2+\sqrt{3})^n + (2-\sqrt{3})^n\right] - 1$$

$$p = \frac{1}{2} \cdot \left(\frac{\left[(2+\sqrt{3})^n - (2-\sqrt{3})^n\right]}{2\sqrt{3}} - 1 \right)$$

On constate que, pour $n = 1$, a_n est pair et b_n est impair.

On contrôle immédiatement par la récurrence :

$(a_n, b_n) = (\text{pair, impair}) \Rightarrow (a_{n+1}, b_{n+1}) = (\text{impair, pair})$

$(a_n, b_n) = (\text{impair, pair}) \Rightarrow (a_{n+1}, b_{n+1}) = (\text{pair, impair})$

L'ensemble cherché dans $\mathbb{N}^* \times \mathbb{N}^*$ des solutions en (m, p) à la question est donc explicitement défini par le formulaire :

k décrivant $\mathbb{N}$:

$$m = \frac{1}{4} \cdot \left[(2+\sqrt{3})^{2k+1} + (2-\sqrt{3})^{2k+1}\right] - 1$$

$$p = \frac{1}{2} \cdot \left(\frac{\left[(2+\sqrt{3})^{2k+1} - (2-\sqrt{3})^{2k+1}\right]}{2\sqrt{3}} - 1 \right)$$