

Alexandre Junod

Lycée Denis-de-Rougemont (Neuchâtel), alexandre.junod@rpn.ch

Les équations de Pell-Fermat généralisées

L'équation diophantienne $x^2 - ny^2 = 1$, où n est un entier positif non carré, a suscité l'intérêt des mathématiciens depuis l'Antiquité. En Inde, Brahmagupta (598-668) a montré comment générer une infinité de solutions à partir d'une solution non triviale $(x; y) \neq (\pm 1; 0)$, tandis que Bhāskara II (1114-1185) a développé un algorithme (appelé méthode *chakravala*) permettant de trouver une telle solution initiale. En Europe, ce problème attira également l'attention et fut progressivement relié aux fractions continues, notamment par Pierre de Fermat (1601-1665), William Brouncker (1620-1684), John Wallis (1616-1703), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813), Évariste Galois (1811-1832) et Adrien-Marie Legendre (1752-1833). Une introduction est donnée dans [2] et nous améliorons ici l'algorithme présenté dans [1] afin de traiter l'équation plus générale $mx^2 - ny^2 = m$, où $m < n$ sont des entiers positifs dont le produit n'est pas un carré parfait.

1 Algorithme

On considère deux entiers positifs $m < n$ dont le produit n'est pas un carré parfait et un algorithme :

Initialisation :

$$\begin{array}{ccc|ccc} a_{i-1} & b_{i-1} & c_{i-1} & = & 0 & 1 & n \\ a_i & b_i & c_i & & 1 & 0 & m \end{array} \quad \text{pour } i = 0.$$

Itération :

$$\begin{array}{ccc|ccc} a_{i+1} = q_i a_i + a_{i-1} & b_{i+1} = q_i b_i + b_{i-1} & & & & & \\ c_{i+1} = 2q_i \sqrt{mn - c_{i-1}c_i} + c_{i-1} - q_i^2 c_i & & & & & & \end{array} \quad \text{avec } q_i = \left\lfloor \frac{\sqrt{mn - c_{i-1}c_i} + \sqrt{mn}}{c_i} \right\rfloor$$

Nous allons établir les faits suivants.

- Il existe un indice s tel que $q_s = 2q_0$. On a alors $c_s = m$ et la fraction continue périodique

$$\sqrt{\frac{n}{m}} = [q_0; q_1, q_2, \dots] = [q_0; \overline{q_1, \dots, q_s}] = [q_0; \underbrace{q_1, \dots, q_1}_{\text{palindrome}}, 2q_0].$$

- Pour chaque indice $i \geq 0$, on a $ma_i^2 - nb_i^2 = (-1)^i c_i$ ainsi que $\frac{a_{i+1}}{b_{i+1}} = [q_0; q_1, \dots, q_i]$.

Exemple. Trouver deux nombres impairs consécutifs dont le produit est 23 fois un carré parfait. Ce problème conduit à l'équation de Pell-Fermat classique $x^2 - 23y^2 = 1$, où x est un nombre pair (les deux nombres impairs étant alors $x \pm 1$). Avec $m = 1$ et $n = 23$, l'algorithme fournit la fraction continue $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$ et la première solution $(x; y) = (24; 5)$. Les nombres 23 et 25 répondent donc au problème (la prochaine solution sera 55'223 et 55'225). Notons encore que $\frac{24}{5} = [4; 1, 4] = [4; \overline{1, 3, 1}]$.

i	a_i	b_i	c_i	q_i
-1	0	1	23	← initialisation
0	1	0	1	$q_0 = \lfloor (0 + \sqrt{23})/1 \rfloor = 4$
1	4	1	7	$q_1 = \lfloor (4 + \sqrt{23})/7 \rfloor = 1$
2	5	1	2	$q_2 = \lfloor (3 + \sqrt{23})/2 \rfloor = 3$
3	19	4	7	$q_3 = \lfloor (3 + \sqrt{23})/7 \rfloor = 1$
4	24	5	1	$q_4 = \lfloor (4 + \sqrt{23})/1 \rfloor = 8$
⋮	⋮	⋮	⋮	⋮

Raccourci. Pour résoudre une équation classique $x^2 - ny^2 = 1$, on peut arrêter l'algorithme dès que c_i divise $2a_i$: la relation $a_i^2 - nb_i^2 = (-1)^i c_i$ implique la solution $x = \frac{2a_i^2}{c_i} + (-1)^{i+1}$ et $y = \frac{2a_i b_i}{c_i}$.

Remarque. Pour visualiser une matrice identité, on peut initialiser l'algorithme comme ci-contre. On a alors $q_{-1} = 0$ (car $m < n$) et la suite est la même.

$$\begin{bmatrix} a_{-2} & b_{-2} & c_{-2} \\ a_{-1} & b_{-1} & c_{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & m \\ 0 & 1 & n \end{bmatrix}$$

2 Pertinence

Proposition 1. Les nombres c_{i-1} , c_i , q_i sont des entiers strictement positifs et $\sqrt{mn - c_{i-1}c_i}$ est aussi un entier (autrement dit $mn - c_{i-1}c_i$ est un carré parfait).

Preuve. L'assertion est vraie pour $i = 0$ et on procède par récurrence : on suppose qu'elle est vraie pour un indice i et on prouve sa validité pour l'indice $i + 1$.

- $\sqrt{mn - c_i c_{i+1}}$ est un entier

Le polynôme $P(x) = c_i x^2 - 2\sqrt{mn - c_{i-1}c_i}x + c_{i+1} - c_{i-1}$ s'annule au moins une fois (lorsque $x = q_i$). Son discriminant $\Delta = 4(mn - c_{i-1}c_i) - 4c_i(c_{i+1} - c_{i-1}) = 4(mn - c_i c_{i+1})$ est donc positif ou nul et $\sqrt{mn - c_i c_{i+1}}$ est bien défini. On peut vérifier que $|c_i q_i - \sqrt{mn - c_{i-1}c_i}| = \sqrt{mn - c_i c_{i+1}}$ car les deux membres de l'égalité ont le même carré. On en déduit que $\sqrt{mn - c_i c_{i+1}}$ est un entier.

- c_{i+1} est un entier strictement positif

La relation évidente $0 < \frac{\sqrt{mn - c_{i-1}c_i} + \sqrt{mn}}{c_i} - q_i < 1$ peut s'écrire sous la forme

$$-\sqrt{mn} < \underbrace{\sqrt{mn - c_{i-1}c_i} - c_i q_i}_{\pm \sqrt{mn - c_i c_{i+1}}} < c_i - \sqrt{mn} \quad (*)$$

car $c_i > 0$. Comme $q_i \geq 1$ et $c_i c_{i-1} > 0$, on a $c_i \leq c_i q_i < \sqrt{mn - c_{i-1}c_i} + \sqrt{mn} < 2\sqrt{mn}$ et l'encadrement $(*)$ implique $\sqrt{mn - c_i c_{i+1}} < \sqrt{mn}$. Il s'ensuit que $c_i c_{i+1} > 0$ et que le nombre c_{i+1} est un entier strictement positif.

- q_{i+1} est un entier strictement positif

La fonction $x \mapsto x^2 - c_i x - mn$ est décroissante sur l'intervalle $]-\infty; \frac{1}{2}c_i]$. On peut l'appliquer à $(*)$ en inversant les inégalités (car $c_i - \sqrt{mn} < c_i - \frac{1}{2}c_i = \frac{1}{2}c_i$). On obtient

$$c_i \sqrt{mn} > -c_i c_{i+1} + c_i^2 q_i - c_i \sqrt{mn - c_{i-1}c_i} > -c_i \sqrt{mn},$$

c'est-à-dire $|c_{i+1} + \sqrt{mn - c_{i-1}c_i} - c_i q_i| < \sqrt{mn}$. En utilisant l'inégalité triangulaire, on en déduit

$$c_{i+1} = |c_{i+1}| \leq |c_{i+1} + \sqrt{mn - c_{i-1}c_i} - c_i q_i| + |c_i q_i - \sqrt{mn - c_{i-1}c_i}| < \sqrt{mn} + \sqrt{mn - c_i c_{i+1}},$$

donc l'entier évident q_{i+1} est strictement positif. $\square$

On a remarqué que les entiers $c_i q_i - \sqrt{mn - c_{i-1}c_i}$ et $\sqrt{mn - c_i c_{i+1}}$ sont égaux ou opposés. On peut maintenant montrer qu'ils sont réellement les mêmes :

- si $c_i > \sqrt{mn}$, alors $c_i q_i - \sqrt{mn - c_{i-1}c_i} > \sqrt{mn} - \sqrt{mn - c_i c_{i+1}} > 0$;
- si $c_i < \sqrt{mn}$, alors $(*)$ montre que $c_i q_i - \sqrt{mn - c_{i-1}c_i} > \sqrt{mn} - c_i > 0$.

Comme mn n'est pas un carré parfait, le cas $c_i = \sqrt{mn}$ ne se pose pas.

3 Fraction continue de $\sqrt{n/m}$

Théorème 1. *Il existe un indice s tel que $q_s = 2q_0$. La suite $(q_i)_{i \geq 1}$ est alors s -périodique et on a la fraction continue périodique*

$$\sqrt{\frac{n}{m}} = [q_0; q_1, q_2, \dots] = [q_0; \overline{q_1, \dots, q_s}] = [q_0; \underbrace{q_1, \dots, q_1}_{\text{palindrome}}, 2q_0].$$

Preuve. Considérons le nombre réel positif $\theta_i = \frac{\sqrt{mn - c_{i-1}c_i} + \sqrt{mn}}{c_i}$ présent dans la définition de q_i . Comme $\sqrt{mn - c_{i-1}c_i} = c_i q_i - \sqrt{mn - c_i c_{i+1}}$, on a

$$\theta_i = \frac{c_i q_i - \sqrt{mn - c_i c_{i+1}} + \sqrt{mn}}{c_i} = q_i + \frac{\sqrt{mn} - \sqrt{mn - c_i c_{i+1}}}{c_i}$$

et en amplifiant la dernière fraction par $\sqrt{mn} + \sqrt{mn - c_i c_{i+1}}$, on obtient

$$\theta_i = q_i + \frac{c_i c_{i+1}}{c_i(\sqrt{mn} + \sqrt{mn - c_i c_{i+1}})} = q_i + \frac{c_{i+1}}{\sqrt{mn} + \sqrt{mn - c_i c_{i+1}}} = q_i + \frac{1}{\theta_{i+1}}$$

Comme tous les q_i sont des entiers strictement positifs, on a alors $\theta_i = [q_i; q_{i+1}, q_{i+2}, \dots]$.

De la même manière, les nombres $\theta'_i = \frac{\sqrt{mn - c_{i-1}c_i} + \sqrt{mn}}{c_{i-1}}$ satisfont

$$\theta'_{i+1} = \frac{\sqrt{mn - c_i c_{i+1}} + \sqrt{mn}}{c_i} = q_i + \frac{\sqrt{mn} - \sqrt{mn - c_{i-1}c_i}}{c_i} = q_i + \frac{1}{\theta'_i}$$

donc $\theta'_{i+1} = [q_i, q_{i-1}, \dots, q_0, \theta'_0]$ avec $\theta'_0 = \sqrt{mn}$. On peut aussi en déduire que $q_i = \lfloor \theta'_{i+1} \rfloor$.

- *Périodicité*

Comme la suite $(c_i)_{i \geq 0}$ d'entiers est bornée, on peut trouver deux indices $s > i \geq 0$ avec i minimal, tels que $c_s = c_i$ et $c_{s+1} = c_{i+1}$. On a alors les égalités $\theta'_{s+1} = \theta'_{i+1}$, $q_s = \lfloor \theta'_{s+1} \rfloor = \lfloor \theta'_{i+1} \rfloor = q_i$ et $c_{s-1} = q_s^2 c_s - 2q_s \sqrt{mn - c_s c_{s+1}} + c_{s+1}$ coïncide avec c_{i-1} . Pour respecter la minimalité de i , on en déduit que $i = 0$, donc $c_s = c_0 = m$ et $c_{s+1} = c_1 = n - m q_0^2$. On a aussi la fraction continue

$$\theta_{s+1} = \theta_1 = [q_1, q_2, \dots, q_s, \theta_{s+1}] = [\overline{q_1, q_2, \dots, q_s}].$$

- *Palindromie*

On peut vérifier que $\theta'_1 = \sqrt{n/m} + q_0$ et que $\theta_1 = \frac{\sqrt{m}(\sqrt{n} + \sqrt{m}q_0)}{n - m q_0^2} = \frac{\sqrt{m}}{\sqrt{n} - \sqrt{m}q_0} = \frac{1}{\theta'_1 - 2q_0}$.

Avec la fraction continue ci-dessus, on a $\theta'_1 - 2q_0 = [0, \overline{q_1, q_2, \dots, q_s}]$, donc $\theta'_1 = [2q_0, \overline{q_1, q_2, \dots, q_s}]$.

En comparant avec

$$\theta'_1 = \theta'_{s+1} = [q_s, q_{s-1}, \dots, q_1, \theta'_1] = [\overline{q_s, q_{s-1}, \dots, q_1}],$$

on obtient $q_s = 2q_0$, $q_{s-1} = q_1$, $q_{s-2} = q_2$, et ainsi de suite. $\square$

4 Equation de Pell généralisée

Théorème 2. *Pour chaque indice $i \geq 0$, on a $ma_i^2 - nb_i^2 = (-1)^i c_i$ et $\frac{a_{i+1}}{b_{i+1}} = [q_0; q_1, \dots, q_i]$.*

Preuve. Avec les relations $a_{i+1} = q_i a_i + a_{i-1}$ et $\theta_{i+1} = \frac{1}{\theta_i - q_i}$, on obtient

$$a_{i+1}\theta_{i+1} + a_i = \theta_{i+1}(q_i a_i + a_{i-1} + a_i(\theta_i - q_i)) = \theta_{i+1}(a_i \theta_i + a_{i-1})$$

et une relation similaire est valable pour les nombres b_i . En itérant le raisonnement et en utilisant les valeurs initiales $a_0 \theta_0 + a_{-1} = \theta_0 = \sqrt{n/m}$, respectivement $b_0 \theta_0 + b_{-1} = 1$, on peut écrire

$$a_{i+1}\theta_{i+1} + a_i = \theta_{i+1}\theta_i \cdots \theta_2 \theta_1 \sqrt{n/m} \quad \text{et} \quad b_{i+1}\theta_{i+1} + b_i = \theta_{i+1}\theta_i \cdots \theta_2 \theta_1$$

On a donc $(a_i \theta_i + a_{i-1}) = (b_i \theta_i + b_{i-1}) \sqrt{n/m}$. Explicitons θ_i et multiplions cette relation par mc_i :

$$(a_i \sqrt{mn - c_{i-1}c_i} + c_i a_{i-1})m + ma_i \sqrt{mn} = (b_i \sqrt{mn - c_{i-1}c_i} + c_i b_{i-1})\sqrt{mn} + mnb_i.$$

Comparons maintenant les parties purement irrationnelles et les parties purement entières :

$$ma_i = b_i \sqrt{mn - c_{i-1}c_i} + c_i b_{i-1} \quad \text{et} \quad nb_i = a_i \sqrt{mn - c_{i-1}c_i} + c_i a_{i-1}.$$

En multipliant la première équation par a_i , la seconde par b_i et en soustrayant les relations obtenues, on trouve $ma_i^2 - nb_i^2 = c_i(a_i b_{i-1} - a_{i-1} b_i)$. En considérant le déterminant dans la relation matricielle

$$\begin{pmatrix} a_{i+1} & a_i \\ b_{i+1} & b_i \end{pmatrix} = \begin{pmatrix} a_i & a_{i-1} \\ b_i & b_{i-1} \end{pmatrix} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} = \cdots = \underbrace{\begin{pmatrix} a_0 & a_{-1} \\ b_0 & b_{-1} \end{pmatrix}}_{\text{Matrice identité}} \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix},$$

on voit que $a_{i+1}b_i - a_i b_{i+1} = (-1)^{i+1}$ et la première partie du théorème est démontrée.

Étant donné une matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et un nombre x , on définit $M * x = \frac{ax + b}{cx + d}$. On a par exemple

$\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} * x = q + \frac{1}{x}$ et on peut vérifier que $M_1 * (M_2 * x) = M_1 M_2 * x$. En appliquant $M \mapsto M * x$

à la relation matricielle ci-dessus, on trouve $\frac{a_{i+1}x + a_i}{b_{i+1}x + b_i} = [q_0; q_1, \dots, q_i, x]$. La deuxième partie du théorème est démontrée en prenant la limite lorsque x tend vers l'infini. $\square$

Corollaire. Soit s la longueur de la période de la fraction continue de $\sqrt{n/m}$ comme définie dans le théorème 1. On a alors $c_{ks} = c_0 = m$ et $ma_{ks}^2 - nb_{ks}^2 = (-1)^{ks}m$ pour tout entier $k \geq 0$.

Pour résumer, lorsque $n > m \geq 1$, l'équation $mx^2 - ny^2 = c$

- est toujours résoluble pour $c = m$ (en choisissant des valeurs paires de k si s est impair),
- est résoluble pour $c = -m$ lorsque s est impair (en considérant des valeurs impaires de k).

Remarque 1. Supposons que l'équation $mx^2 - ny^2 = c$ admette une solution $(x; y)$ avec $x > y > 0$. On a alors

$$\left| \frac{x}{y} - \sqrt{\frac{n}{m}} \right| = \left| \frac{\sqrt{m}x - \sqrt{n}y}{\sqrt{m}y} \right| = \left| \frac{c}{(\sqrt{m}x + \sqrt{n}y)\sqrt{m}y} \right| < \frac{|c|}{(\sqrt{m} + \sqrt{n})\sqrt{m}y^2} \stackrel{(*)}{<} \frac{1}{2y^2}$$

l'inégalité $(*)$ étant valable lorsque $2|c| < m + \sqrt{mn}$. Ceci implique alors (par un résultat bien connu en théorie des fractions continues) que x/y est une réduite de $\sqrt{n/m}$. On en déduit que si $|c| < \frac{m + \sqrt{mn}}{2}$ (en particulier si $c = \pm m$), l'algorithme pourra trouver toute solution éventuelle. Si $|c| > 2\sqrt{mn}$, il n'en trouvera aucune car on a montré que $c_i < 2\sqrt{mn}$ dans la section 2. Pour les autres valeurs de c , rien ne garantit qu'il trouvera des solutions, même s'il en existe.

Remarque 2. Lorsque $m > n \geq 1$, l'équation se réécrit $ny^2 - mx^2 = -c$ et on peut échanger les rôles de m et n , ainsi que ceux de x et y , tout en considérant la constante opposée. On obtient donc la règle suivante : si $m > n \geq 1$, l'équation $mx^2 - ny^2 = c$ est toujours résoluble pour $c = -n$, et est résoluble pour $c = n$ lorsque la période de la fraction continue de $\sqrt{m/n}$ est de longueur impaire.

Exemple. L'équation diophantienne $7X - 11Y = 7$ admet la solution générale $X = 1 + 11k$ et $Y = 7k$ avec $k \in \mathbb{Z}$. Trouver des valeurs $k > 0$ pour lesquelles ces deux nombres sont des carrés parfaits.

Le problème revient à résoudre l'équation $7x^2 - 11y^2 = 7$ (on pourrait également s'intéresser à $x^2 - 77y^2 = 1$). En considérant $m = 7$ et $n = 11$ dans l'algorithme (voir ci-contre), on trouve la solution non triviale $(x; y) = (351; 280)$. Elle correspond à $X = x^2 = 123'201$ et $Y = y^2 = 78'400$, donc à $k = 11'200$. La prochaine valeur possible sera $k = 5'519'404'800$.

On voit que l'algorithme peut résoudre l'équation $7x^2 - 11y^2 = c$ pour $c \in \{7, -4, 13, -1\}$ mais pas pour $c = -7$: la fraction continue $\sqrt{11/7} = [1; \mathbf{3}, \mathbf{1}, \mathbf{16}, \mathbf{1}, \mathbf{3}, \mathbf{2}]$ a une période de longueur paire.

i	a_i	b_i	c_i	q_i
-1	0	1	11	
0	1	0	7	1
1	1	1	4	3
2	4	3	13	1
3	5	4	1	16
4	84	67	13	1
5	89	71	4	3
6	351	280	7	2
7	791	631	4	3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Le programme suivant, écrit en Python, indique les premières éventuelles solutions $(x; y)$ d'une équation $mx^2 - ny^2 = c$ que l'algorithme permet de trouver en moins de 100 itérations.

```
def Pell(m,n,c) :
    print(f"Equation {m}x^2 - {n}y^2 = {c}")
    nbIter = nbSol = 0
    if c*c < 4*m*n :
        a0, b0, c0, a1, b1, c1 = 0, 1, n, 1, 0, m
        while (nbSol != 5 and nbIter != 100) :
            if (1-2*(nbIter%2))*c1 == c :
                print(f"x = {a1} et y = {b1}")
                nbSol += 1
            nbIter += 1
            q1 = int((m*n - c0*c1)**(1/2) + (m*n)**(1/2)) // c1
            a2 = q1*a1 + a0
            b2 = q1*b1 + b0
            c2 = 2*q1*int((m*n - c0*c1)**(1/2)) + c0 - q1*q1*c1
            a0, b0, c0, a1, b1, c1 = a1, b1, c1, a2, b2, c2
        if nbSol == 0: print("Aucune solution trouvée")
```

Pell(1,29,1) : $x^2 - 29y^2 = 1$ pour (1;0), (9'801;1'820), (192'119'201;35'675'640), etc.

Pell(1,29,-1) : $x^2 - 29y^2 = -1$ pour (70;13), (137'2210;254'813), etc.

Pell(7,11,7) : $7x^2 - 11y^2 = 7$ pour (1;0), (351;280), (246'401;196'560), etc.

Pell(7,11,-7) : $7x^2 - 11y^2 = -7$, Aucune solution trouvée

Références (articles personnels)

- [1] "An Algorithm to Solve a Pell Equation", General Mathematics Notes, Vol. 28, No. 2, Juin 2015
www.emis.de/journals/GMN/volumes/all_volumes-page1_2015.html
- [2] "Initiation aux équations de Pell-Fermat", Bulletin de la SSPMP n° 138, septembre 2018
www.vsmf.ch/bulletin/suche/Artikel/138/138_Junod.pdf

