Méthode indienne pour résoudre l'équation de Pell

1) Rappel sur l'équation de Pell

L'équation dite de Pell[1] est de la forme $x^2 - d\,y^2 = n$, avec d et n entiers donnés, et dont on cherche les solutions entières supérieures ou égales à 0. [2]

Voyons d'abord les cas les moins intéressants.

- d est un nombre négatif, soit $d' = -d > 0$, et l'équation s'écrit
$x^2 + d'y^2 = n$, et l'on a un nombre fini de solutions, voire aucune.
Si d et n ne sont pas trop grands, on procède par essais et en se ramenant modulo d.

Exemples :

1) Résoudre $x^2 + 5\,y^2 = 68$.
En se ramenant modulo 5, l'équation devient $x^2 = 3$ [5]. Quant x décrit $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$, x^2 décrit $\{0, 1, 4\}$ et ne donne jamais 3. L'équation n'a pas de solution.

2) Résoudre $x^2 + 5\,y^2 = 69$.
En cas de solutions, on a comme condition nécessaire : $x^2 = 4$ [5], ce qui impose $x = 2$ ou $x = 3$ [5]. Par essais, en faisant $x = 2, 3, 7, 8$, on trouve finalement deux solutions (7, 2), (8, 1).

2) Résoudre $x^2 + 5\,y^2 = 74$.
La condition nécessaire : $x^2 = 4$ [5] impose $x = 2$ ou $x = 3$ [5]. Mais en faisant $x = 2, 3, 7, 8$, aucun essai n'est concluant. Il n'y a aucune solution.

- d est un carré parfait, soit $d = d'^2$, et l'équation $x^2 - (d'y)^2 = n$ peut s'écrire :
$(x - d'y)(x + d'y) = n$. L'équation a un nombre fini de solutions, voire aucune.

Exemple : Résoudre $x^2 - 25\,y^2 = 21$.

$(x - 5y)(x + 5y) = 21$, avec $21 = 1 \times 21$ ou $21 = 3 \times 7$, ce qui revient à résoudre deux systèmes :

$$\begin{cases} x - 5y = 1 \\ x + 5y = 21 \end{cases} \text{ ou } \begin{cases} x - 5y = 3 \\ x + 5y = 7 \end{cases}$$

Le premier système donne la solution unique $x = 11$ et $y = 2$, le deuxième système n'a pas de solution entière.

Il reste le cas le plus intéressant, celui où d est positif et n'est pas un carré parfait. Dans ce cas, l'équation $x^2 - d\,y^2 = n$ peut n'avoir aucune solution, mais si elle en a une, elle en possède une infinité, comme cela a été démontré. Ce résultat est lié au fait que l'équation de Pell la plus emblématique, à savoir $x^2 - d\,y^2 = 1$, a toujours une infinité de solutions. Le traitement complet de ce type d'équation date du 19è siècle, notamment grâce aux fractions continuées, mais bien avant les savants indiens avaient trouvé des méthodes expérimentales particulièrement performantes.

---

[1] Le nom d'équation de Pell est seulement un point de repère. Il semble que J. Pell (années 1600) ne soit pas pour grand chose dans la résolution de cette équation. Mieux vaudrait parler d'équation de Brahmagupta (années 600), ce savant indien ayant fait dès cette époque une étude approfondie à ce sujet.

[2] Si (x, y) est une solution positive, ou a aussi $(-x, y)$, $(x, -y)$, $(-x, -y)$ qui sont solutions.

Exercice 1 : Cas où l'équation de Pell n'a pas de solution

1) Montrer que l'équation $x^2 - 3y^2 = 2$ n'a pas de solutions en entiers.

Supposons qu'il existe une solution (a, b), soit $a^2 - 3\,b^2 = 2$. Alors ramenons l'égalité modulo 3, ce qui donne $(a_{[3]})^2 = 2$. Maintenant a ne peut être que 0, 1 ou 2, et a^2 ne peut être autre que 0 ou 1, sans jamais être égal à 2. On tombe sur une contradiction. L'équation initiale n'a pas de solution.

2) Montrer que l'équation $x^2 - dy^2 = -1$ n'a pas de solution si $d = 3$ [4].

S'il y avait une solution (a, b), on aurait $a^2 - d\,b^2 = -1$. En ramenant cette égalité modulo 4, elle devient $a^2 - 3\,b^2 = -1$ [4] ou encore $a^2 + b^2 = 3$. Donnons à a les valeurs 0, 1, 2, 3, alors a^2 vaut 0 ou 1 [4], et de même b^2. L'addition de a^2 et b^2 vaut 0, 1 ou 2, mais jamais 3. Contradiction.

Passons maintenant aux méthodes indiennes, qui ont été trouvées en deux temps, d'abord la méthode *samasabhavana*, puis la méthode *chakravala*.

2) La méthode *samasabhavana* de Brahmagupta

Prenons l'équation $x^2 - dy^2 = n$, et si elle admet une solution (a, b), notons $(a, b\,;\, n)$ le triplet correspondant, tel que $a^2 - db^2 = n$. Brahmagupta a découvert comment composer (*samasabhavana*) deux de ses triplets :

Si l'on a $(a, b\,;\, n)$ et $(a', b'; n')$ alors on a aussi $(aa' + bb'd, ab' + ba'; nn')$

Cela signifie que si l'on a une solution (a, b) de l'équation $x^2 - dy^2 = n$ et une solution (a', b') de l'équation $x^2 - dy^2 = n'$, alors $(aa' + bb'd, ab' + ba')$ est une solution de l'équation $x^2 - dy^2 = nn'$.

Pour le vérifier, il suffit de faire le calcul, mais on peut le vérifier aussi en utilisant une terminologie plus moderne.

Considérons l'anneau[3] des nombres de la forme $\alpha = a + b\sqrt{d}$ avec a et b entiers, où d est un nombre positif qui n'est pas un carré parfait. Le conjugué de α est $\bar{\alpha} = a - b\sqrt{d}$, et l'on dispose des règles de conjugaison classiques :

$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$

$\overline{\alpha\beta} = \bar{\alpha}\ \bar{\beta}$

$\bar{\bar{\alpha}} = \alpha$

On appelle norme[4] de α, ou encore de (a, b) le nombre entier positif ou négatif :

$N(\alpha)$ ou $N(a,b) = \alpha\bar{\alpha} = a^2 - db^2$.

[3] Cela signifie que l'on peut faire les additions et les multiplications habituelles mais tous les éléments ne sont pas inversibles.

[4] Attention à cette notion de « norme ». Lorsque l'on prend les nombres complexes de la forme $z = a + ib$, on définit le module du nombre comme la longueur de son vecteur image **v**, celle-ci étant appelée la norme du vecteur, soit $\|\mathbf{v}\| = \sqrt{z\,\bar{z}}$. Mais dans le cas des nombres de la forme $\alpha = a + b\sqrt{d}$, la norme est $\alpha\bar{\alpha}$ (et non pas la racine carrée). Cette norme est elle aussi liée à la taille du nombre, et si l'on choisit $\alpha\bar{\alpha}$, c'est parce que ce nombre peut être négatif, auquel cas la racine carrée n'aurait pas de sens.

Dans ce contexte le triplet de Brahmagupta n'est autre que (a, b ; $N(a, b)$). On obtient alors la formule :

$N(\alpha\beta) = N(\alpha)\,N(\beta)$ avec $\alpha = a + b\sqrt{d}$ et $\beta = a' + b'\sqrt{d}$

En effet $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\,\bar{\beta} = \alpha\bar{\alpha}\,\beta\bar{\beta} = N(\alpha)\,N(\beta)$.

Or $\alpha\beta = (a + b\sqrt{d})(a' + b'\sqrt{d}) = aa' + bb'd + (ab' + ba')\sqrt{d}$
Avec $N(\alpha) = n$ et $N(\beta) = n'$, on retrouve bien la formule de Brahmagupta, soit
$(aa' + bb'd, ab' + ba'; nn')$ ou encore $(aa' + bb'd)^2 - d(ab' + ba')^2 = nn'$.

Cela va nous aider pour traiter l'équation la plus importante : $x^2 - dy^2 = 1$, et trouver d'autres solutions que la solution évidente (1, 0) sans intérêt. Prenons un exemple simple :

$x^2 - 3y^2 = 1$

On trouve aussitôt une solution $(a, b) = (2, 1)$.
En posant $\alpha = a + b\sqrt{d}$, avec $N(\alpha) = 1$, on a aussi $N(\alpha^n) = 1$, ce qui donne une infinité de solutions. En composant (2, 1 ; 1) avec lui-même, comme l'a fait Brahmagupta, on trouve (7, 4 ; 1), d'où la solution (7, 4) avec $7^2 - 3\times4^2 = 1$. Puis on compose ce résultat avec (2, 1 ; 1), et l'on obtient (26, 15; 1), d'où la solution (26, 15). On peut continuer ainsi indéfiniment. C'est ainsi que Brahmagupta trouva que l'équation admettait une infinité de solutions, à partir de l'une d'elles.[5] On en sait un peu plus aujourd'hui : il y a toujours une plus petite solution positive, comme (2, 1) dans notre exemple, et en prenant les puissances α^n, on les obtient toutes. Il n'y en a pas d'autres.

Quitte à procéder par tâtonnements, Brahmagupta a aussi résolu l'équation

$x^2 - 92y^2 = 1$

Aucune solution simple n'apparaissant, on choisit x^2 le plus proche possible de 92, soit $x = 10$. On obtient alors le triplet (10, 1 ; 8) avec $10^2 - 92\times1^2 = 8$. Puis composons ce triplet avec lui-même, ce qui donne (192, 20, 64), soit $192^2 - 92\times20^2 = 64$. Divisons tout par 64, quitte à obtenir une fraction :
$24^2 - 92\times(5/2)^2 = 1$, ce qui donne le triplet (24, 5/2; 1).

Enfin composons ce triplet avec lui-même, la fraction va disparaître (car 92 est divisible par 4), et l'on trouve le triplet (1151, 120; 1), d'où la solution (1151, 120).

Brahmagupta est allé plus loin. Il a montré que si l'on a une solution de l'équation $x^2 - dy^2 = k$, avec $k = -1$ ou $k = \pm2$ ou $k = \pm4$, on peut en déduire une solution pour $x^2 - dy^2 = 1$.

- Cas où l'on connaît une solution (a, b) de $x^2 - dy^2 = -1$. En composant $(a, b ; 1)$ avec lui-même, on trouve le triplet $(a^2 + b^2d, 2ab ; 1)$ et le couple $(a^2 + b^2d, 2ab)$ est une solution de $x^2 - dy^2 = 1$.

Exemple : $x^2 - 5y^2 = 1$. Comme l'équation $x^2 - 5y^2 = -1$ admet la solution évidente (2, 1), on en déduit la solution (9, 4) pour $x^2 - 5y^2 = 1$.

- Cas où l'on connaît une solution (a, b) de $x^2 - dy^2 = \pm2$. En composant $(a, b, \pm2)$ avec lui-même, on obtient $(a^2 + d\,b^2, 2ab ; 4)$, soit $(a^2 + d\,b^2)^2 - (2ab)^2 = 4$. Mais $a^2 + d\,b^2 = a^2 - d\,b^2 + 2\,d\,b^2$

[5] En appelant (a_1, b_1) le premier couple solution, on obtient ensuite le couple (a_2, b_2), puis (a_3, b_3), etc. On constate grâce aux formules que $a_1 < a_2 < a_3 < \ldots$, et aussi $b_1 < b_2 < b_3 < \ldots$. Les solutions sont toutes différentes, il y en a bien une infinité. Autrement dit, si l'on avait $\alpha^k = \alpha^{k'}$, soit $\alpha^{k-k'} = 1$, cela impose que $k - k' = 0$ et $k = k'$, puisque l'on ne prend pas $\alpha = 1$.

$= \pm 2 + 2\ d\ b^2$, soit un multiple de 2. On peut diviser par 4 les deux membres de l'égalité précédente, ce qui donne

$(\frac{a^2+db^2}{2})^2-(ab)^2=1$, et la solution $(\frac{a^2+db^2}{2}, ab)$ pour $x^2 - dy^2 = 1$. Cette solution correspond à $\alpha^2/2$ pour $\alpha = a+b\sqrt{d}$.

Exemples :

1) $\boldsymbol{x^2 - 98y^2 = 1}$.

On constate que l'équation $x^2 - 98y^2 = 2$ admet la solution évidente. (10, 1). On en déduit (en prenant $\alpha^2/2$) que ((100+98)/2, 20/2), soit (99, 10) est solution de $x^2 - 98y^2 = 1$.

2) $\boldsymbol{x^2 - 83y^2 = 1}$.

On constate que l'équation $x^2 - 83y^2 = -2$ admet la solution évidente. (9, 1). On en déduit (en prenant $\alpha^2/2$) que ((81+83)/2, 18/2), soit (82, 9) est solution de $x^2 - 83y^2 = 1$.

- Cas où l'on connaît une solution (a, b) de $x^2 - dy^2 = \pm 4$.

On verra, dans la méthode *chakravala* qui suit, que a et b sont toujours premiers entre eux. Ils ne peuvent pas être pairs tous les deux. D'ailleurs s'ils l'étaient, on pourrait diviser x et y par 2 et l'on retomberait sur l'équation $x^2 - d\,y^2 = \pm 1$. On distingue alors deux cas.

- Premier cas : a et b ne sont pas tous les deux pairs. Supposons en plus que non seulement d n'est pas un carré parfait, mais n'est pas un multiple de 4. Montrons que cela impose que d soit impair.

Si d était pair, avec $a^2 - db^2 = \pm 4$, alors a^2 serait un nombre pair, et a le serait aussi. Dont a^2 serait multiple de 4, $db^2 = a^2 \mp 4$ serait multiple de 4. Comme d n'est pas multiple de 4, 2 doit diviser b^2 et par suite b. Alors a et b seraient pairs tous les deux, ce qui est contraire à notre hypothèse.

Dans ce contexte, b doit être impair. En effet, si b était pair, db^2 serait multiple de 4 et $a^2 = db^2 \pm 4$ serait multiple de 4, a serait pair. Mais a et b ne sont pas tous les deux pairs en même temps. Donc b ne peut être qu'impair.

Maintenant, avec $\alpha = a+b\sqrt{d}$, formons $\alpha^3 = (a+b\sqrt{d})^3 = a^3+3dab^2+(3a^2b+db^3)\sqrt{d}$ et l'on obtient le triplet $(a^3+3dab^2, 3a^2b+db^3; \pm 64)$, soit

$(a^3+3dab^2)^2 - d\,(3a^2b+db^3)^2 = \pm 64$. On constate que :

$a^3+3dab^2 = a(a^2+3db^2) = a(a^2-db^2+4db^2) = a(\pm 4+4db^2) = 4a(\pm 1+db^2)$.

Avec d et b impairs comme on l'a vu, db^2 est impair, et $db^2 \pm 1$ est pair. Ainsi a^3+3ab^2 est divisible par 8, $(a^3+3ab^2)/8$ est un entier.

De même, $3a^2b+db^3 = b(3a^2+db^2) = b(3a^2-3db^2+4db^2) = b(3\times\pm 4+4db^2) = 4b(\pm 3+db^2)$ avec ici aussi $\pm 3+db^2$ pair, donc $(3a^2b+db^3)/8$ est un entier.

En divisant l'égalité précédemment trouvée par 64, il reste :

$(\frac{a^3+3dab^2}{8})^2 - d\,(\frac{3a^2b+b^3d}{8})^2 = \pm 1$

Si c'est +1, on a la solution $((a^3+3dab^2)/8,\ (3a^2b+b^3d)/8)$ pour $x^2 - dy^2 = 1$.

Si c'est – 1, on compose la solution précédente avec elle-même, ce qui correspond à $\alpha^6/64$, pour avoir $x^2 - dy^2 = 1$.

Exemple : $x^2 - 61y^2 = 1$

Brahmagupta remarqua que l'on avait le triplet (39, 5, –4), soit $39^2 - 61\times5^2 = -4$. Avec 39 et 5 tous deux impairs, on a alors, grâce au résultat précédent :

$(a^3 + 3dab^2)/8 = 29718$, et $(3a^2b + b^3d)/8 = 3805$. Il reste à composer (29728, 3805 ; –1) avec lui-même, ce qui donne :

$29728^2 + 61\times3805^2 = 1\,766\,319\,049$,

$2\times29718\times3805 = 226\,153\,980$.

C'est le couple solution pour $x^2 - 61y^2 = 1$.

- Deuxième cas : avec a et b non pairs tous les deux, d n'est pas un carré parfait mais est un multiple de 4, ce qui impose que a soit pair et b impair, comme on va le vérifier.

En effet, avec $a^2 - db^2 = \pm 4$, et $d = 4d'$, $a^2 = db^2 \pm 4 = a^2 = 4d'b^2 \pm 4$, a^2 est multiple de 4, et a est pair, et b est impair.

Partons du triplet (a, b ; ± 4). En divisant par 4, on obtient le triplet ($a/2$, $b/2$, ± 1), où $a/2$ est entier, mais $b/2$ ne l'est pas. Mais la formule de composition fonctionne encore. Composons le triplet avec lui-même, ce qui donne ($(a^2 + db^2)/4$, $ab/2$; 1). Avec $a/2$ entier et $a^2/4$ entiers, on a aussi $db^2/4$ entier puisque 4 divise d. On a trouvé la solution entière $((a^2 + db^2)/4, ab/2)$. C'est justement ce qu'a fait Brahmagupta pour traiter $x^2 - 92y^2 = 1$, comme on l'a vu ci-dessus.

A ce stade, si l'on est capable de trouver une solution de $x^2 - dy^2 = n$ avec $n = \pm 1$ ou ± 2 ou ± 4, on est assuré d'avoir une solution de $x^2 - dy^2 = 1$, et ensuite d'en trouver une infinité. Mais cela peut demander beaucoup de tâtonnements, comme par exemple lorsque Brahmagupta trouva la solution (39, 5) vérifiant $x^2 - 61y^2 = -4$, ce qui lui a ensuite permis de résoudre $x^2 - 61y^2 = 1$. Mais prenons par exemple $x^2 - 13y^2 = 1$. En choisissant a tel que $|a^2 - d|$ soit le plus petit possible, on trouve $a = 4$, et l'on a le triplet (4, 1 ; 3) qui ne nous est d'aucun secours. Il faudrait de nombreux tâtonnements pour arriver au triplet (18, 5 ; –1) qui nous permettrait de conclure. Pour avoir une méthode générale de résolution, un nouveau procédé était requis, et c'est ce que découvrit le savant indien Bhaskara II vers 1150, avec la méthode *chakravala*.

3) La méthode *chakravala* de Bhaskara II

L'objectif est toujours de trouver une solution (a, b) entière positive pour $x^2 - dy^2 = 1$, avec d positif qui n'est pas un carré parfait. Un moyen de s'approcher du résultat consiste à prendre un nombre a_1 tel que a_1^2 soit le plus proche de d possible, soit $m_1 = a_1^2 - d$ le plus proche de 0 possible en valeur absolue [6], et de prendre $b_1 = 1$, de façon que l'on ait le triplet (a_1, b_1 ; m_1) où (a_1, b_1) est solution de $x^2 - dy^2 = m_1$ avec m_1 petit. Si par chance $m_1 = 1$ c'est fini. Et même si $m_1 = -1$ ou ± 2 ou ± 4, on peut appliquer les formules de Brahmagupta pour en finir, mais nous ne le ferons pas ici de façon à rester dans le cas général. L'idée de Bhaskara II consiste à enclencher un processus répétitif à partir de cette première étape où l'on a le triplet (a_1, b_1 ; m_1) ainsi qu'un quatrième nombre $c_1 = a_1$.

Lors de la deuxième étape, on commence par prendre $c_2 = -c_1$ [m_1], soit $c_2 = -c_1 + q_1 m_1$ en choisissant c_2^2 le plus proche de d possible, ou $|c_2^2 - d|$ le plus proche de 0 possible. Puis on compose le triplet précédent (a_1, b_1 ; m_1) avec le triplet (c_2, 1, $c_2^2 - d$), ce qui donne le triplet :

---

[6] Posons $A = [\sqrt{d}]$, $\sqrt{d}$ est strictement compris entre A et $A + 1$, et d entre A^2 et $(A + 1)^2$.. Or a_1 est soit A soit $A + 1$. Comme $m_1 = a_1^2 - d$ est le plus proche de 0 possible, on a $|m_1| \le ((A+1)^2 - A^2)/2$, $m_1 \le A + 1/2$ ou encore $|m_1| \le A$.

$(a_1 c_2 + b_1 d, a_1 + b_1 c_2 ; m_1 (c_2^2 - d))$.

Puis divisons les deux premiers éléments par $|m_1|$ pour garder des nombres positifs), alors la norme $m_1 (c_2^2 - d)$ est divisée par $|m_1|^2$ ou m_1^2. On obtient le nouveau triplet :

$$(\frac{a_1 c_2 + b_1 d}{|m_1|}, \frac{a_1 + b_1 c_2}{|m_1|}; \frac{c_2^2 - d}{m_1})$$

Les fractions obtenues sont en fait des nombres entiers, grâce au choix de c_2. [7]

Posons $a_2 = \frac{a_1 c_2 + b_1 d}{|m_1|}$, $b_2 = \frac{a_1 + b_1 c_2}{|m_1|}$, $m_2 = \frac{c_2^2 - d}{m_1}$. Dans ce nouveau triplet, où $c_2^2 - d$ est relativement proche de 0 en étant positif ou négatif, m_2 est aussi un nombre petit. Avec un peu de chance, on peut avoir $m_2 = 1$ et c'est fini. Sinon on recommence, en procédant par récurrence.

Il s'agit de montrer que $a_i = \frac{a_{i-1} c_i + b_{i-1} d}{|m_{i-1}|}$, $b_i = \frac{a_{i-1} + b_{i-1} c_i}{|m_{i-1}|}$, $m_i = \frac{c_i^2 - d}{m_{i-1}}$ pour tout i.

Supposons que l'on soit arrivé à l'étape i, avec le triplet $(a_i, b_i ; m_i)$ obéissant aux formules précédentes, et passons à l'étape $i + 1$ en prenant $c_{i+1} = - c_i$ $[m_i] = -c_i + q_i m_i$ de façon que c_{i+1}^2 soit le plus proche de d possible. Puis composons le triplet $(a_i, b_i ; m_i)$ avec le triplet $(c_{i+1}, 1, c_{i+1}^2 - d)$, soit

$(a_i c_{i+1} + b_i d, a_i + b_i c_{i+1} ; m_i (c_{i+1}^2 - d))$,

et divisons par $|m_i|$ les deux premiers éléments, ce qui donne le nouveau triplet :

$$(\frac{a_i c_{i+1} + b_i d}{|m_i|}, \frac{a_i + b_i c_{i+1}}{|m_i|}; \frac{c_{i+1}^2 - d}{m_i})$$

Montrons que ces trois nombres sont des entiers obéissant aux formules.

- $a_i + b_i c_{i+1} = a_i - b_i c_i$ $[m_i] = \frac{a_{i-1} c_i + b_{i-1} d}{|m_i|} - \frac{a_{i-1} + b_{i-1} c_i}{|m_i|} c_i$ $[m_i]$

  $= \frac{b_{i-1}(d - c_i^2)}{|m_{i-1}|}$ $[m_i] = b_{i-1} m_i$ $[m_i] = 0$ $[m_i]$. Ainsi $b_{i+1} = \frac{a_i + b_i c_{i+1}}{|m_i|}$ est bien entier.

- $a_i c_{i+1} + b_i d = -a_i c_i + b_i d$ $[m_i] = -\frac{a_{i-1} c_i + b_{i-1} d}{|m_{i-1}|} c_i + \frac{a_{i-1} + b_{i-1} c_i}{|m_{i-1}|} d$ $[m_i]$

  $= \frac{a_{i-1}(d - c_i^2)}{|m_{i-1}|}$ $[m_i] = -a_{i-1} m_i = 0$ $[m_i]$, et $a_{i+1} = \frac{a_i c_{i+1} + b_i d}{|m_i|}$ est entier.

- $c_{i+1}^2 - d = c_i^2 - d$ $[m_i] = m_i m_{i-1}$ $[mi]$ par hypothèse de récurrence

  $= 0$ $[m_i]$, et $m_{i+1} = \frac{c_{i+1}^2 - d}{m_i}$ est entier.

Cela étant fait, on constate que la suite des (m_i) est bornée, plus précisément $|m_i| \leq 2\sqrt{d}$.[8] On constate aussi que a_i et b_i sont premiers entre eux.[9]

---

[7] En effet :

- $a_1 + b_1 c_2 = a_1 + b_1(- c_1 + q_1 m_1) = q_1 m_1$ puisque $b_1 = 1$ et $c_1 = a_1$. Ainsi m_1 divise $a_1 + b_1 c_2$.
- $a_1 c_2 + b_1 d = a_1 (- c_1 + q_1 m_1) + b_1 d = - a_1^2 + d + a_1 q_1 m_1 = - m_1 + a_1 q_1 m_1 = 0$ $[m_1]$ et m_1 divise $a_1 c_2 + b_1 d$.
- $c_2^2 - d = (- c_1 + q_1 m_1)^2 - d = (- a_1 + q_1 m_1)^2 - d = a_1^2 - d - 2 q_1 a_1 m_1 + q_1^2 m_1^2$ avec $m_1 = a_1^2 - d$, et m_1 divise $c_2^2 - d$.

Tandis que les (a_i) et les (b_i) croissent, les normes m_i restent bornées. Cela ne prouve pas que l'on va finir par tomber sur une norme égale à 1, mais cela se démontre.[10]

En fait, on assiste à un phénomène cyclique (d'ailleurs avec une allure de palindrome comme on le constatera dans quelques exemples). Au lieu de commencer par le triplet (a_1, b_1 ; m_1) avec $c_1 = a_1$, on aurait pu commencer par (a_0, b_0 ; m_0) avec $a_0 = 1$, $b_0 = 0$, $m_0 = 1$, ce qui correspond à la solution évidente, et $c_0 = 0$. En appliquant les formules précédentes, on retrouve l'étape 1, en prenant c_1^2 le plus proche de d possible, ce qui donne $a_1 = c_1$, $b_1 = 1$ et $m_1 = a_1^2 - d$. En partant ainsi de $m_0 = 1$, on itère le processus jusqu'à retomber sur 1, et l'on peut continuer ainsi indéfiniment. C'est ce phénomène cyclique que traduit le mot *chakravala*. Vérifiions-le sur quelques exemples.

Exemple 1 : $x^2 - 13y^2 = 1$.
On commence à l'étape 1 par le triplet (4, 1, 3) avec $c_1 = 4$. En appliquant les formules, on trouve :
-étape 2 : $c_2 = 2$, et le triplet (7, 2 ; –3)
-étape 3 : $c_3 = 4$, et le triplet (18, 5 ; –1)
-étape 4 : $c_4 = 4$, et le triplet (127, 38 ; –3)
-étape 5 : $c_5 = 2$, et le triplet (256, 71 ; 3)
-étape 6 : $c_6 = 4$, et le triplet (649,180 ; 1), d'où la solution (a, b) = (649,180).
Si l'on continue sur les six étapes suivantes, on retrouve le même cycle –3, –1, –3, 3, 1, ce qui donne une deuxième solution (a, b) = (842 401, 133640).

Exemple 2 : $x^2 - 106y^2 = 1$.

On trouve comme succession des m_i à partir du rang 0 :
1, –6, 7, 9, – 9, –7, 6, –1, 6, –7, –9, 9, 7, –6, 1, et l'on aboutit à la solution :
a = 32 080 051, b = 3 115 890.

4) Programme pour avoir une solution de $x^2 - dy^2 = 1$

Il suffit de faire la récurrence précédente jusqu'à ce que l'on tombe sur ± 1, $\pm$ ou ± 2 ou ± 4, auxquels cas on applique les résultats de Brahmagupta. Le programme en découle.

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>

int N(int a,int b);
void resultat(int a,int b);
int d,norme;

int main()
```

---

[8] Toujours avec $A = [\sqrt{d}]$, on a $A^2 < d < (A + m_{i-1})^2$, et par définition, c_i est soit A soit $A + m_{i-1}$. Il en découle que $|c_i^2 - d| \leq ((A + m_{i-1})^2 - A)/2$ et $|m_i| = |c_i^2 - d| / |m_{i-1}| \leq |(2A\, m_{i-1} + m_{i-1}^2) / 2m_{i-1}|$.
$|m_i| \leq A + m_{i-1}/2$. Avec m_{i-1} supposé inférieur au égal à $2\sqrt{d}$ par hypothèse de récurrence (et c'était vrai au départ), on trouve bien que $|m_i| \leq 2\sqrt{d}$

[9] Lors du passage de l'étape i à i +1, on a la relation
$|m_i|(a_{i+1} + b_{i+1}\sqrt{d}) = (a_i + b_i\sqrt{d})(c_{i+1} + \sqrt{d})$ avec $m_i = (a_i + b_i\sqrt{d})(a_i - b_i\sqrt{d})$, d'où
$c_{i+1} + \sqrt{d} = (a_i - b_i\sqrt{d})(a_{i+1} + b_{i+1}\sqrt{d})$ au signe près. Tout diviseur commun à a_{i+1} et b_{i+1} doit diviser c_{i+1} et 1, ce ne peut être que ± 1, a_{i+1} et b_{i+1} sont premiers entre eux.

[10] On trouvera quelques indications dans le document *wikipédia* sur la *méthode chakravala*. Précisons aussi que cette méthode donne la plus petite solution entière positive.

```
{ int a,b,c,i,newa,newb;
  for(d=2;d<100;d++)  /* ici on a pris d de 2 à 99, en laissant tomber les cas où d est un carré */
   { printf(" \n  d = %3.d", d);
     a=1; b=1; i=1;  /* étape 1 avec le premier terme de la suite */
     while(N(a,b)<0) a++;
     if (a*a==d) continue;
     if (-N(a-1,b)<N(a,b)) a=a-1;
     norme=N(a,b);
     if (abs(norme)==4 || abs(norme)==2  || abs(norme)==1)  /* c'est fini */
       { resultat(a,b);     continue;  }
     c=a;
     for(;;)  /* boucle des étapes à partir de l'étape 2 */
       { i++;
         c=-c;
         while(c<sqrt(d))  c+=abs(norme);
         if (d-(c-abs(norme))*(c-abs(norme)) < c*c-d) c=c-abs(norme);
         newa=(a*c+d*b)/abs(norme);
         newb=(a+c*b)/abs(norme);
         a=newa; b=newb; norme=N(a,b);
         if  (abs(norme)==4 || abs(norme)==2  || abs(norme)==1) break;
        }
     resultat(a,b);
   }
getchar();return 0;
}

int N(int a,int b)   /* norme */
{ return (a*a-d*b*b);
}

void resultat(int a, int b)
{ int X,Y,XX,YY,XXX,YYY;
   if (abs(norme)==2)
     { X=(a*a+d*b*b)/2;
       Y=a*b;
       printf("  X = %d   Y= %d",X,Y);

     }
   else if (norme==-1)
     { X=a*a+d*b*b;
       Y=2*a*b;
       printf("  X = %d   Y= %d",X,Y);

     }
    else if (norme==1)
     { X=a;
       Y=b;
       printf("  X = %d   Y= %d",X,Y);

     }
   else if (abs(norme)==4)
     { if (d%4!=0)
           { X=(a*a+d*b*b)/2;Y=a*b;
             XX=(a*X+b*Y*d)/4; YY=(b*X+a*Y)/4;
             if (N(XX,YY)==1)
                { printf("  X = %d   Y= %d",XX,YY);
                 }
             else if (N(XX,YY)==-1)
                 { XXX=XX*XX+YY*YY*d;  YYY= 2*XX*YY;
                    printf("  X = %d   Y= %d",XXX,YYY);
```

```
                }
            }
          else
            {  X=(a*a+d*b*b)/4;Y=a*b/2;
               printf("  X = %d   Y= %d",X,Y);
             }
       }
}
```

Quelques résultats pour *d* de 50 à 99 :

```
d =  50  X = 99    Y= 14
d =  51  X = 50    Y= 7
d =  52  X = 649    Y= 90
d =  53  X = 66249    Y= 9100
d =  54  X = 485    Y= 66
d =  55  X = 89    Y= 12
d =  56  X = 15    Y= 2
d =  57  X = 151    Y= 20
d =  58  X = 19603    Y= 2574
d =  59  X = 530    Y= 69
d =  60  X = 31    Y= 4
d =  61  X = 1766319049    Y= 226153980
d =  62  X = 63    Y= 8
d =  63  X = 8    Y= 1
d =  64
d =  65  X = 129    Y= 16
d =  66  X = 65    Y= 8
d =  67  X = 48842    Y= 5967
d =  68  X = 33    Y= 4
d =  69  X = 7775    Y= 936
d =  70  X = 251    Y= 30
d =  71  X = 3480    Y= 413
d =  72  X = 17    Y= 2
d =  73  X = 2281249    Y= 267000
d =  74  X = 3699    Y= 430
d =  75  X = 26    Y= 3
d =  76  X = 57799    Y= 6630
d =  77  X = 351    Y= 40
d =  78  X = 53    Y= 6
d =  79  X = 80    Y= 9
d =  80  X = 9    Y= 1
d =  81
d =  82  X = 163    Y= 18
d =  83  X = 82    Y= 9
d =  84  X = 55    Y= 6
d =  85  X = 285769    Y= 30996
d =  86  X = 10405    Y= 1122
d =  87  X = 28    Y= 3
d =  88  X = 197    Y= 21
d =  89  X = 500001    Y= 53000
d =  90  X = 19    Y= 2
d =  91  X = 1574    Y= 165
d =  92  X = 1151    Y= 120
d =  93  X = 12151    Y= 1260
d =  94  X = 2143295    Y= 221064
d =  95  X = 39    Y= 4
d =  96  X = 49    Y= 5
d =  97  X = 62809633    Y= 6377352
d =  98  X = 99    Y= 10
d =  99  X = 10    Y= 1
```

Le seul écueil de ce programme est de travailler dans la limite des nombres entiers, d'où des possibilités de débordement lorsque l'on fait des élévations au carré. La plus petite valeur de *d* pour laquelle un débordement a lieu est *d* = 109.[11]

[11] En remplaçant les nombres entiers par des flottants (*float* ou *double*) dans le programme précédent, ce qu'il convient de faire avec beaucoup de circonspection, on trouve pour *d* = 109 : *a* = 158 070 671 986 249 et *b* = 15 140 424 455 100. Un des autres exemples où les entiers sont « débordés » est pour *d* = 193, avec *a* = 6 224 323 426 849 et *b* = 448 036 604 040. Mais les flottants peuvent aussi être dépassés, à cause de leur propre flottement.

P.S. En 2017, j'ai repris le traitement de l'équation de Pell de façon plus approfondie, dans l'article consacré plus largement aux *mathématiques de l'Inde ancienne, des années 500 à 1600*. On le trouvera sur mon site *pierreaudibert.fr* dans la rubrique *Travaux complémentaires, algorithmes sur les nombres*.