Equation de Fermat-Pell.

I) Cette équation joue un rôle important en arithmétique. Elle s'écrit :

$$(1) \qquad x^2 - Ky^2 = 1 \qquad (x,y) \in \mathbb{N}^2 \qquad K \text{ naturel non carré parfait.}$$

On peut aussi bien la résoudre dans $\mathbb{Z}^2$ mais (x,y) étant une solution dans $\mathbb{N}^2$ on obtient les solutions dans $\mathbb{Z}^2$ en prenant les couples $(\pm x , \pm y)$.

On remarque immédiatement qu'elle admet une solution simple $(1,0)$ mais le but de la résolution sera justement de trouver les autres solutions si elles existent. Jusqu'à nouvel ordre, chaque fois qu'il sera question de solution, il s'agira donc d'une solution autre que la solution triviale $(1,0)$. Nous adopterons le plan suivant basé sur l'établissement des trois propriétés.

a) Toute solution en engendre une infinité d'autres.

b) S'il existe une solution dite minimale elle engendre <u>toutes</u> les autres.

c) Il existe une solution minimale ; les développements en fraction continue nous permettent de la trouver.

Procédons donc à la démonstration de ces différents points.

---

a) <u>SUPPOSONS QU'IL EXISTE UNE SOLUTION (x_1, y_1)</u>.

Nous pouvons donc écrire l'égalité :

$$x_1^2 - K y_1^2 = 1 \qquad \text{c'est-à-dire}$$

$$(x_1 - \sqrt{K}\, y_1)(x_1 + \sqrt{K}\, y_1) = 1 \qquad \text{et en élevant à la puissance } n .$$

$$(x_1 - \sqrt{K}\, y_1)^n (x_1 + \sqrt{K}\, y_1)^n = 1$$

Les deux facteurs du premier membre ont respectivement pour formule :

$$(x_1 - \sqrt{K}\, y_1)^n = x_n - \sqrt{K}\, y_n$$

$$(x_1 + \sqrt{K}\, y_1)^n = x_n + \sqrt{K}\, y_n$$

où x_n et y_n sont des polynômes en x_1 et y_1 constituant respectivement la partie entière et le coefficient de K du développement de $(x_1 + \sqrt{K}\, y_1)^n$.

Nous avons donc l'implication :

$$x_1^2 - K y_1^2 = 1 \quad \Longrightarrow \quad x_n^2 - K y_n^2 = 1$$

Donc si (x_1,y_1) est une solution il en existe une infinité (x_n,y_n) où (x_n,y_n) est donné par les relations :

$$\begin{cases} x_n = \dfrac{(x_1 + K\, y_1)^n + (x_1 - K\, y_1)^n}{2} \\[2ex] y_n = \dfrac{(x_1 + K\, y_1)^n - (x_1 - K\, y_1)^n}{2\sqrt{K}} \end{cases} \quad (n \in \mathbb{N}) \quad (2)$$

Nous dirons que (x_1,y_1) engendre les solutions (x_n,y_n).

---

b) SOLUTION MINIMALE.

Considérons la fonction définie sur $\mathbb{N}^2$:

$$f(x,y) = x + \sqrt{K}\, y .$$

C'est une fonction croissante en x et en y. D'autre part on s'aperçoit que, si (x',y') et (x'',y'') sont deux solutions de (1), l'on a l'équivalence :

$$x' < x'' \iff y' < y''$$

Si donc (x_1,y_1) est une solution de (1) il n'y a qu'un nombre fini de solutions de (1) pour lesquelles :

$$f(x,y) \leqslant f(x_1,y_1)$$

Soit (x_o,y_o) celle pour laquelle $f(x_o,y_o)$ prend la plus petite valeur possible. Nous l'appellerons solution minimale de (1).

Proposition 1 : La solution minimale est unique.

$$\left.\begin{array}{l}(x_o,y_o) \text{ solution minimale} \\ (x'_o,y'_o) \text{ solution minimale}\end{array}\right\} \Longrightarrow f(x_o,y_o) = f(x'_o,y'_o)$$

$$\Longrightarrow x_o + \sqrt{K}\, y_o = x'_o + \sqrt{K}\, y'_o \Longrightarrow x_o - x'_o = \sqrt{K}\,(y_o - y'_o)$$

$$\Longrightarrow \begin{cases} x_o = x'_o \\ y_o = y'_o \end{cases} \quad \text{puisque } \sqrt{K} \text{ est irrationnel.}$$

Nous constatons d'ailleurs d'après les remarques faites plus haut que (x_o,y_o) ne donne pas seulement parmi tous les couples solutions la plus petite valeur à $f(x,y)$ mais qu'elle vérifie aussi par rapport à tout autre solution (x_1,y_1) :

$$\begin{cases} x_o < x_1 \\ y_o < y_1 \end{cases}$$

Proposition 2 : La solution (x_o,y_o) si elle existe, engendre toutes les solutions de (1).

Supposons qu'il existe une solution (x',y') non engendrée par (x_o,y_o). Comme la suite des $(x_o + \sqrt{K}\, y_o)^n$ est croissante et non bornée et que (x_o, y_o) est solution minimale, il existe $n \geqslant 1$ tel que :

$$(x_o + \sqrt{K}\, y_o)^n < x' + \sqrt{K}\, y' < (x_o + \sqrt{K}\, y_o)^{n+1} \qquad (3)$$

Or $x_o - \sqrt{K}\, y_o > 0$ puisque $x_o + \sqrt{K}\, y_o > 0$ et $x_o^2 - Ky_o^2 = 1$

Multiplions les trois membres de (3) par $(x_o - \sqrt{K}\, y_o)^n$:

$$(x_o + \sqrt{K}\, y_o)^n (x_o - \sqrt{K}\, y_o)^n < (x' + \sqrt{K}\, y')(x_o - \sqrt{K}\, y_o)^n < (x_o + \sqrt{K}\, y_o)^{n+1}(x_o - \sqrt{K}\, y_o)^n$$

donc $$1 < (x' + \sqrt{K}\, y')(x_o - \sqrt{K}\, y_o)^n < x_o + \sqrt{K}\, y_o$$

Ecrivons $(x' + \sqrt{K}y')(x_o - \sqrt{K}\, y_o)^n$ sous la forme $u + \sqrt{K}\, v$ $\quad (u,v) \quad \mathbb{N}^2$

donc $$1 < u + \sqrt{K}\, v < x_o + \sqrt{K}\, y_o \qquad (4)$$

- Montrons que (u,v) est une solution de (1)

$$(x' + \sqrt{K}\, y')(x_o - \sqrt{K}\, y_o)^n = u + \sqrt{K}\, v$$

$$(x' - \sqrt{K}\, y')(x_o + \sqrt{K}\, y_o)^n = u - \sqrt{K}\, v$$

$$u^2 - K v^2 = (x' + \sqrt{K}\, y')(x_o - \sqrt{K}\, y_o)^n (x' - \sqrt{K}\, y')(x_o + \sqrt{K}\, y_o)^n$$

$$= (x'^2 - K\, y'^2)(x_o^2 - K\, y_o^2)^n = 1$$ puisque (x',y'), (x_o,y_o) sont solutions de (1).

$\Longrightarrow \quad u^2 - K\, v^2 = 1$

Il suffit encore de montrer que u et v sont tous les deux positifs.

$\boxed{u \neq 0}$ $\quad u = 0 \Longrightarrow -Kv^2 = 1$ impossible car $K > 0$

$\boxed{v \neq 0}$ $\quad v = 0 \Longrightarrow u > 1$ et $u^2 = 1$ impossible

$\boxed{sg(u) = sg(v)}$ $\quad sg(u) = -\, sg(v) \Longrightarrow |u - \sqrt{K}\, v| \geqslant |u + \sqrt{K}\, v|$

$\Longrightarrow |u + \sqrt{K}\, v| \cdot |u - \sqrt{K}\, v| = |u^2 - K\, v^2| > 1$

puisque $u + \sqrt{K}\, v > 1$ et c'est impossible car $|u^2 - K\, v^2| = 1$

Comme u et v sont de même signe ils sont positifs d'après (4).

Conclusion : $(u,v) \in \mathbb{N}^2$ vérifiant $u^2 - K\, v^2 = 1$ $\quad (u,v) \neq (1,0)$

(u,v) est donc une solution qui d'après (4) vérifie de plus

$$u + \sqrt{K}\, v < x_o + \sqrt{K}\, y_o$$

Ceci est impossible puisque (x_o, y_o) est minimale et il n'existe donc pas de solution (x',y') non engendrée par (x_o,y_o).

---

c) RECHERCHE DE LA SOLUTION MINIMALE ET RESULTATS DEFINITIFS.

D'après l'étude précédente, toute la résolution de l'équation (1) dépend donc de l'existence et de la recherche de la solution minimale.

Pour démontrer l'existence de la solution minimale, nous allons utiliser un résultat de la théorie générale des fractions continues que voici : si p est la période du développement de $\sqrt{K}$ et si $\delta_p = N_p / D_p$ est la réduite d'ordre p (*), alors :

$$\left(\delta_p - \sqrt{K}\right)\left(\delta_p + \sqrt{K}\right) = \frac{(-1)^p}{D_p^2} \qquad (5)$$

D'autre part il n'existe pas de fraction a/b plus simple que δ_p c'est-à-dire

$$(a < N_p \quad \text{et} \quad b < D_p) \quad \text{et} \quad \left(\frac{a}{b} - \sqrt{K}\right)\left(\frac{a}{b} + \sqrt{K}\right) = \frac{\pm 1}{b^2}$$

Si p pair :

Comme (5) s'écrit alors $\left(\frac{N_p}{D_p} - \sqrt{K}\right)\left(\frac{N_p}{D_p} + \sqrt{K}\right) = \frac{1}{D_p^2}$

c'est-à-dire $(N_p - \sqrt{K}\, D_p)(N_p + \sqrt{K}\, D_p) = 1$

on en déduit que (N_p, D_p) est non seulement solution de (1) mais aussi que c'est la solution minimale.

Si p impair :

En élevant les deux membres de (5) au carré on obtient :

$$(N_p - \sqrt{K}\, D_p)^2 (N_p + \sqrt{K}\, D_p)^2 = 1 \quad \Longleftrightarrow$$

$$(N_p^2 + K D_p^2)^2 - K\,(2N_pD_p)^2 = 1 \quad \Longleftrightarrow$$

$(N_p^2 + K D_p^2 \;;\; 2 N_p D_p)$ est solution de (1)

Mais cette solution est aussi la solution minimale sinon il existerait (x'_0, y'_0) et n 2 tel que :

$$(x'_0 + \sqrt{K}\, y'_0)^n = N_p^2 + K D_p^2 + k\,(2N_pD_p)$$

et (x'_0, y'_0) vérifierait
$$\begin{cases} x'_0 < N_p \\ y'_0 < D_p \\ \left(\frac{x'_0}{y'_0} - K\right)\left(\frac{x'_0}{y'_0} + K\right) = \left(\frac{1}{y'_0}\right)^2 \end{cases}$$

(*) On démontre que tout nombre irrationnel, solution d'une équation du second degré à coefficients entiers admet un développement en fraction continue périodique.

En résumé :

Chaque solution de l'équation

$$(x,y) \in \mathbb{N}^2 \qquad x^2 - K y^2 = 1$$

est de la forme (x_n , y_n) , x_n et y_n étant donnés par :

$$x_n = \frac{(x_o + \sqrt{K}\, y_o)^n + (x_o - \sqrt{K}\, y_o)^n}{2}$$

$$y_n = \frac{(x_o + \sqrt{K}\, y_o)^n - (x_o - \sqrt{K}\, y_o)^n}{2\sqrt{K}} \qquad n \in \mathbb{N}$$

où (x_o , y_o) est la solution minimale.

Le nombre $\sqrt{K}$ étant développé en fraction continue périodique de période p et la $p^{\text{ième}}$ réduite étant a/b la solution minimale sera donné par :

$$\begin{cases} x_o = a \\ y_o = b \end{cases} \quad \text{si } p \text{ est pair}$$

$$\begin{cases} x_o = a^2 + K b^2 \\ y_o = 2ab \end{cases} \quad \text{si } p \text{ est impair}$$

<u>Remarque</u> : On peut remarquer que pour $n = 0$ on retrouve la solution triviale $(1,0)$

Par ailleurs deux solutions consécutives (x_n , y_n) et (x_{n+1} , y_{n+1}) sont liées par :

$$\begin{aligned} x_{n+1} + \sqrt{K}\, y_{n+1} &= (x_n + \sqrt{K}\, y_n)(x_o + \sqrt{K}\, y_o) \\ &= x_o x_n + K\, y_o y_n + \sqrt{K}\,(y_o x_n + x_o y_n) \end{aligned}$$

Ce qui donne :

$$\begin{cases} x_{n+1} = x_o x_n + K\, y_o y_n \\ y_{n+1} = y_o x_n + x_o y_n \end{cases} \iff \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_o & Ky_o \\ y_o & x_o \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

si p est pair $\begin{pmatrix} x_o & Ky_o \\ y_o & x_o \end{pmatrix} = \begin{pmatrix} a & Kb \\ b & a \end{pmatrix} = A$

si p impair $\begin{pmatrix} x_o & Ky_o \\ y_o & x_o \end{pmatrix} = \begin{pmatrix} a^2 + Kb^2 & 2Kab \\ 2ab & a^2 + K b^2 \end{pmatrix} = A^2$

Il est donc possible de donner le résultat sous une forme un peu plus concise en utilisant l'écriture vectorielle :

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{si } p \text{ est pair}$$

$$A = \begin{pmatrix} a & kb \\ b & a \end{pmatrix}$$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A^{2n} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{si } p \text{ impair}$$

$A = \begin{pmatrix} a & Kb \\ b & a \end{pmatrix}$. a/b étant la p-ième réduite du développement en fraction continue de $\sqrt{K}$.

II) EXERCICES

a) Résoudre $(x,y) \in \mathbb{N}^2$ $\quad x^2 - 7y^2 = 1$

Dans beaucoup de cas on peut trouver la solution minimale par tâtonnements. Ici en remplaçant successivement y par 1 , 2 , 3 , ... on trouve la solution minimale très rapidement : c'est $(8, 3)$.

La matrice A s'écrit :
$$A = \begin{pmatrix} 8 & 21 \\ 3 & 8 \end{pmatrix}$$

On obtient les solutions par :

$$\begin{pmatrix} x \\ y \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$(1,0)$ $\quad (8,3)$ $\quad (127,48)$ $\quad (2024, 765)$ $\quad \ldots\ldots\ldots$

b) Résoudre $(x,y) \in \mathbb{N}^2$ $\quad x^2 - 19\,y^2 = 1$

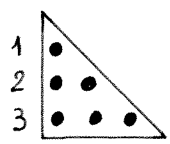
La solution minimale est moins simple que précédemment :

$$\sqrt{19} = (4)(\overline{2\ ,\ 1\ ,\ 3\ ,\ 1\ ,\ 2\ ,\ 8}) \quad p = 6 \qquad \delta_6 = 170/39$$

$$A = \begin{pmatrix} 170 & 741 \\ 39 & 170 \end{pmatrix} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$(1,0)$ $\quad (170\ ,\ 39)$ $\quad (57799\ ,\ 13260)$ $\quad \ldots\ldots\ldots$

c) Quels sont les nombres à la fois carrés et triangulaires ?



On appelle nombre triangulaire un nombre de la forme

$$1 + 2 + 3 + \ldots.. + n$$

exemple $6 = 1 + 2 + 3$ est un nombre triangulaire

Le problème conduit à l'équation :

$$1 + 2 + 3 + \ldots + n = m^2 \iff \frac{n(n+1)}{2} = m^2$$

$$\iff n^2 + n - 2m^2 = 0 \quad \text{résolvons en } n :$$

$$n = \frac{-1 + \sqrt{8m^2 + 1}}{2} \quad n \text{ et } m \text{ entiers positifs}$$

Toute valeur entière positive de m pour laquelle $8m^2 + 1$ est un carré parfait convient puisque $\sqrt{8\,m^2 + 1}$ sera alors entier positif impair. Il suffit donc de trouver les entiers positifs x et y pour lesquels : $8\,y^2 + 1 = x^2$

$$\iff x^2 - 8\,y^2 = 1$$

La solution minimale est $(3,\ 1)$. Les nombres y_n seront donnés par :

$$y_n = \frac{(3 + \sqrt{8})^n - (3 - \sqrt{8})^n}{2\sqrt{8}}$$

Les nombres cherchés seront (enécrivant $8 = 2\sqrt{2}$) :

$$X_n = y_n^2 = \frac{(3 + 2\sqrt{2})^{2n} + (3 - 2\sqrt{2})^{2n} - 2(3 + 2\sqrt{2})(3 - 2\sqrt{2})}{32}$$

$$\boxed{X_n = \frac{(3 + 2\sqrt{2})^{2n} + (3 - 2\sqrt{2})^{2n} - 2}{32}}$$

Pour trouver les premiers nombres X_n il est peut-être plus simple d'utiliser la matrice $A = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$

On trouve : 1 , 36 , 1225 , 41 616 , ...

d) Un problème de Sam Loyd : La bataille de Hastings. (14 - 10 - 1066)

On trouvera l'enoncé e ce problème dans le tome 1 des "cassestête mathématiques de Sam Loyd" de martin Gardner. En résumé voici l'énoncé du problème :

"... je vis les hommes de Harold groupés en 13 grands carrés tous égaux. Harold se porta alors au milieu de ses hommes et à son signal ils se réunirent en un seul et énorme carré ..."

Quels était le nombre des hommes de Harold ?

Soit x^2 le nombre des hommes, Harold compris, puisque ensemble il formaient un carré. On a donc pour équation :

$$x^2 = 13\,y^2 + 1 \quad \text{ou encore :}$$

$$x^2 - 13\,y^2 = 1$$

$\sqrt{13} = (3)(\overline{1\,,1\,,\,1\,,\,1\,,\,6}\,)$ $p = 5$ $\delta_5 = 18/5$

Mais comme p est impair la solution minimale est donnée par :

$$\begin{cases} x = 18^2 + 13 \times 5^2 = 649 \\ y = 2 \times 18 \times 5 \quad = 130 \end{cases}$$

Le nombre des hommes de Harold a donc été :

$$x^2 - 1 = 421\ 200$$

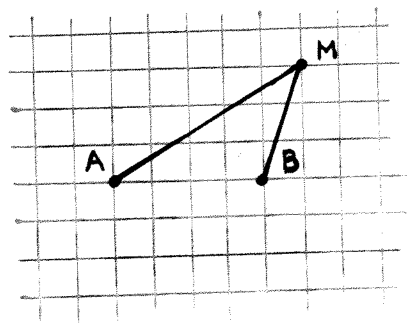
La solution suivante est en effet beaucoup trop grande pour être acceptable.

Le talent proprement diabolique de Sam Loyd réside non seulement dans le choix d'une équation peu classique mais surtout dans celui de $K = 13$ car, parmi les premières valeurs entières, $K = 13$ est certainement la valeur pour laquelle la solution minimale est la moins évidente.

e) Un des problèmes en rapport avec l'équation de Fermat-Pell est la recherche des points de coordonnées entières sur une hyperbole.

Soient A et B deux points situés sur une même droite d'un réseau carré et distants de 4 unités (unité = côté du petit carré). Trouver l'ensemble des points M du réseau tels que :

$$\left| d(M,A) - d(M,B) \right| = 2$$



Prenons pour axes Ox et Oy respectivement les droites AB et la médiatrice de AB. Nous trouvons pour équation de $\left\{ M \ / \ d(M,A) - d(M,B) = 2 \right\}$

$$\left| \sqrt{(x+2)^2 + y^2} - \sqrt{(x-2)^2 + y^2} \right| = 2$$

ce qui équivaut à : $3\,x^2 - y^2 = 3$ (1)

si (x_o, y_o) est une solution de (1), $(x_o, y_o) \in \mathbb{Z}^2$, y_o est nécessairement un multiple de 3. Posons $y = 3z$.

Il nous faut résoudre l'équation :

$$x^2 - 3\,z^2 = 1 \qquad (2)$$

(2,1) est la solution minimale et en tenant compte de $y = 3z$ on trouve les solution de (1) : les couples $(\pm x_n, \pm y_n)$ sont donnés par :

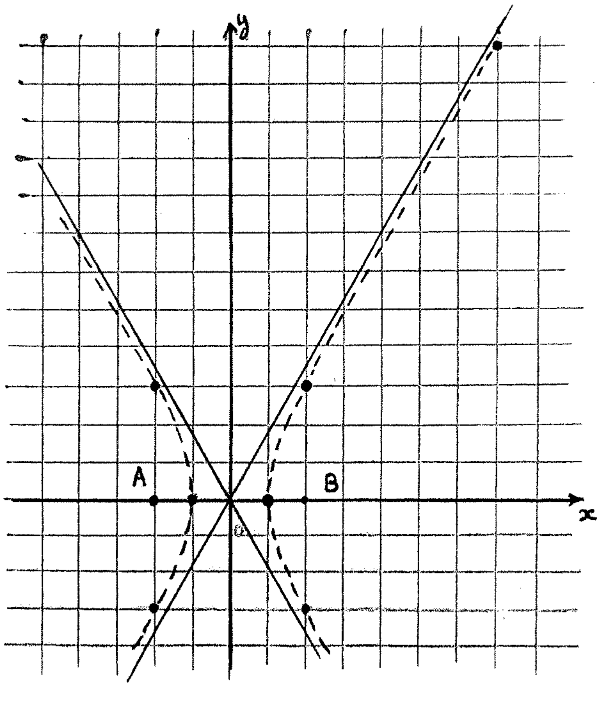
$$x_n = \frac{(2 + \ 3)^n + (2 - \ 3)^n}{2}$$

$$y_n = \frac{(2 + \ 3)^n - (2 - \ 3)^n}{2 \quad 3}$$

Les premières solutions sont :

$(\pm 1 , 0)$ $(\pm 2 , \pm 3)$

$(\pm 7 , \pm 12)$ $(\pm 26 , \pm 45)$



Pour terminer, voici un tableau donnant la solution minimale de l'équation $x^2 - K y^2 = 1$, pour les premières valeurs de K ;

K	x	y	K	x	y	K	x	y	K	x	y
2	3	2	15	4	1	28	127	24	40	19	3
3	2	1	17	33	8	29	9801	1820	41	2049	320
5	9	4	18	17	4	30	11	2	42	13	2
6	5	2	19	170	39	31	1520	273	43	3482	531
7	8	3	20	9	2	32	17	3	44	199	30
8	3	1	21	55	12	33	23	4	45	161	24
10	19	6	22	197	42	34	35	6	46	24335	3588
11	10	3	23	24	5	35	6	1	47	48	7
12	7	2	24	5	1	37	73	12	48	7	1
13	649	180	26	51	10	38	37	6	50	99	14
14	15	4	27	26	5	39	25	4	51	50	7

Stoltz
