

# Autour des équations de Pell-Fermat (Brahmagupta)

## Quel est le nombre d'animaux du troupeau d'Hélios ?

- I. Introduction aux équations de Pell-Fermat
    - A. Problème des bœufs d'Hélios : Système linéaire
    - B. Mise en équation de la seconde partie
  
  - II. Réduction de l'équation de Pell-Fermat
    - A. Fractions continues et réduites
    - B. Solution fondamentale
  
  - III. Résolution informatique de l'équation de Pell-Fermat : Solution du problème
    - A. Recherche de la solution fondamentale
    - B. Application au problème des bœufs d'Hélios
- Conclusion

## I. Introduction aux équations de Pell-Fermat

Dénombrer, Ami, les troupeaux du Soleil qui couvraient jadis les plaines de la Sicile, divisés en quatre groupes selon leurs couleurs, les blancs, les noirs, les marrons et les tachetés. Il y avait plus de taureaux que de vaches, et les relations entre leurs nombres étaient les suivantes :

A. Problème des bœufs d'Hélios : Système linéaire

Tableau des Symboles	Blanc : $B=W+w$	Noir : $N=X+x$	Marron : $M=Y+y$	Tacheté : $T=Z+z$
Taureau	$W$	$X$	$Y$	$Z$
Vache	$w$	$x$	$y$	$z$

$$\left\{ \begin{array}{l}
 W = \left(\frac{1}{2} + \frac{1}{3}\right) X + Y \\
 X = \left(\frac{1}{4} + \frac{1}{5}\right) Z + Y \\
 Z = \left(\frac{1}{6} + \frac{1}{7}\right) W + Y \\
 w = \left(\frac{1}{3} + \frac{1}{4}\right) N \\
 x = \left(\frac{1}{4} + \frac{1}{5}\right) T \\
 y = \left(\frac{1}{5} + \frac{1}{6}\right) M \\
 z = \left(\frac{1}{6} + \frac{1}{7}\right) B
 \end{array} \right. \quad \text{MAPLE SOL1} \quad \left\{ \begin{array}{l}
 z = PPCM * k = 3515820k, \\
 W = 10366482 * k, X = 7460514 * k, \\
 Y = 4149387 * k, Z = 7358060 * k, \\
 w = 7206360 * k, x = 4893246 * k, y = 5439213 * k
 \end{array} \right.$$

Si tu peux donner, Ami, le nombre de chaque sorte de vaches et de taureaux, tu n'es pas un novice en matière de nombres, mais on ne peut encore te considérer comme ayant un talent supérieur. Apprends, cependant, qu'il y avait aussi d'autres relations entre les taureaux du Soleil.

Si tu peux calculer également ces nombres, Ami, et trouver ainsi la taille totale du troupeau, exulte, car par ta conquête, tu as montré que tu as atteint le degré suprême dans la science des nombres.

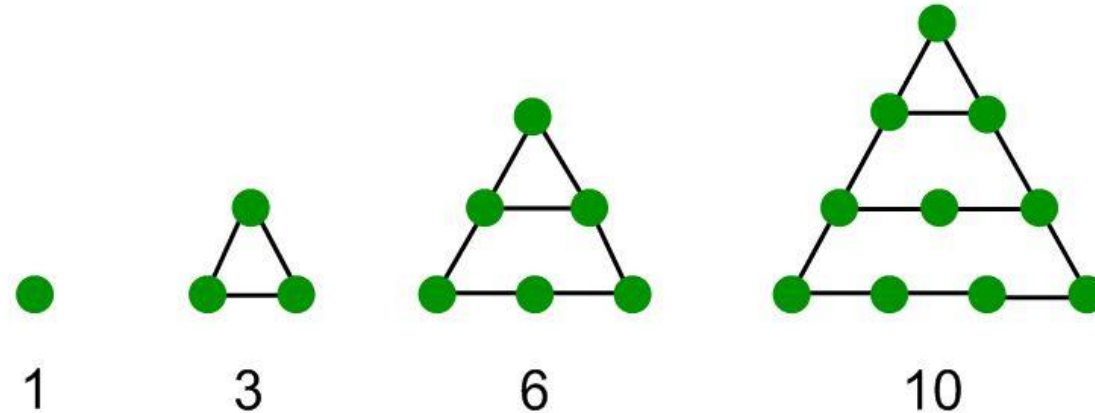
**B.** Mise en équation de la seconde partie

$$\begin{aligned} \blacksquare \text{ Carré Parfait } W + X &= \lambda^2 \\ &= 17826996 * k \\ &= 2^2 * 3 * 11 * 29 * 4657 * k \end{aligned}$$

$$\text{DONC } z = \text{PPCM} * 3 * 11 * 29 * 4657 * m^2$$

$$\text{SOL2} \left\{ \begin{array}{l} z = 15669127269180 * m^2, W = 46200808287018 * m^2, \\ X = 33249638308986 * m^2, Y = 18492776362863 * m^2, \\ Z = 32793026546940 * m^2, w = 32116937723640 * m^2, \\ x = 21807969217254 * m^2, y = 24241207098537 * m^2 \end{array} \right\}$$

- Nombre triangulaire :  $Y + Z = \frac{\mu^2 + \mu}{2}$



Crédits: Google image

CONDITION : Discriminant carré parfait => Équation de PELL

$$\Delta = 410286423278424 m^2 + 1$$

$$p^2 - 410286423278424 m^2 = 1$$

## II.

### A. Fractions continues et réduites

Écrire  $\alpha \in \mathbb{R}$  comme fraction continue :

- Si  $\alpha$  entier : ☺
- Sinon écrire  $\alpha = [\alpha] + (\alpha - [\alpha])$
- ...
- ☺

« *On appelle Réduite de rang  $n$  du nombre  $\alpha$  le rationnel*

$$\frac{P_n}{Q_n} = [a_0, a_1, \dots, a_n] \text{ »}$$

$$p^2 - m^2 d = (p - m\sqrt{d})(p + m\sqrt{d})$$

Donc une solution de l'équation de Pell est une réduite de  $\sqrt{d}$

Démo (réduite) :

$$(p - m\sqrt{d})(p + m\sqrt{d}) = 1$$

$$(p - m\sqrt{d}) = \frac{1}{p + m\sqrt{d}}$$

$$\text{Ainsi } (p - m\sqrt{d}) > 0$$

$$p > m\sqrt{d}$$

$$\text{Or, } \left| \sqrt{d} - \frac{p}{m} \right| = \frac{p - m\sqrt{d}}{m} = \frac{1}{m(p + m\sqrt{d})} < \frac{1}{m(m\sqrt{d} + m\sqrt{d})}$$

$$\left| \sqrt{d} - \frac{p}{m} \right| < \frac{1}{2m^2\sqrt{d}}$$

$$\text{Donc } \left| \sqrt{d} - \frac{p}{m} \right| < \frac{1}{2m^2}$$

*Condition pour que  $\frac{p}{m}$  soit une réduite de  $\sqrt{d}$  d'après le théorème de la meilleure approximation :* « La réduite s'écrit  $p/m$ , si et seulement si l'écart entre ce nombre rationnel et le nombre irrationnel qu'elle représente est inférieur à  $1/m^2$  »



## B. Solution fondamentale

$(\mathbb{Q}[\sqrt{d}], +, \cdot)$  est un corps commutatif

Norme  $N(\alpha) = \alpha\bar{\alpha}$  donc éléments inversible de  $\mathbb{Q}[\sqrt{d}]$  de norme  $\pm 1$

- $(p, m)$  solution d'une équation de Pell

- $u_1 = p, v_1 = m, u_n + \sqrt{d}v_n = (u_1 + \sqrt{d}v_1)^n$

- $(u_n, v_n)$  solution  $\overset{ssi}{\Leftrightarrow} (u_1, v_1)$  solution

En effet par l'identité de Brahmagoupta :

$$(a^2 - nb^2)(c^2 - nd^2) = (ac \pm nbd)^2 - n(ad \pm bc)^2$$

- Donc toutes les solutions sont caractérisées par une puissance n-ième de la solution fondamentale (On résonne sur la norme des éléments inversibles)

### III.

#### A. Recherche de la solution fondamentale

#Définir s et q pour distinguer les cas

```
def valeurSetQ(D):  
if D%4==1:  
s=2  
q=1  
elif D%4==0:  
s=2  
q=0  
else:  
s=1  
q=0  
return(s,q)
```

#Une solution des équations de Pell est une réduite  
#Algorithme pour trouver les réduites

```
def recurrence_GB(D):  
s=valeurSetQ(D)[0]  
q=valeurSetQ(D)[1]  
P=q  
Q=s  
q0=int((sqrt(D)+q)/s)  
i=0  
G_1=s  
B_1=0  
G_0=int((sqrt(D)+q)/s)*s-q  
B_0=1  
while (abs(Q-s)>0) or i==0:  
P=q0*Q-P  
Q=(D-P**2)/Q  
q0=int((P+sqrt(D))/Q)  
G_1,G_0=G_0,q0*G_0+G_1  
B_1,B_0=B_0,q0*B_0+B_1  
i=i+1  
return([i,s,G_1,B_1])
```

## Annexe 1

```
def table(D):
a=recurrence_GB(D)
x=a[2]
y=a[3]
S=a[1]
sig=(-1)**a[0]
if S==1:
k=1
elif x%2==0 and y%2==0 and sig==1:
k=1
elif x%2==0 and y%2==1 and sig==1:
k=2
elif x%2==0 and sig==-1:
k=2
elif x%2==1 and sig==1:
k=3
elif x%2==1 and sig==-1:
k=6
return(k)

def donnees(D):
K=table(D)
a=recurrence_GB(D)
return(D,a[2],a[3],a[1],K)
```

### #Multiplication de la forme voulue

```
def mult(D,(a,b),(c,d)):
return((a*c+(b*d)*D,a*d+c*b))
```

```
def puissance(D,(a,b),n):
c=(a,b)
for i in range (n-1):
c=mult(D,(a,b),c)
return(c)
```

### #Donner les diviseurs d'un nombre

```
def diviseurs(n):
L=[]
for i in range(1,n/2+1):
if n%i==0:
L.append(i)
else:
L=L
L.append(n)
return(L)
```

## Annexe 2

```
def puissance_chgt_var(D,p):  
A=diviseurs((p+1)/2)  
e=fondamental(D)  
i=0  
while puissance(D,e,A[i])[1]%p>0 or i<len(A)-1:  
i=i+1  
return(2*A[i])
```

#Donner les parités des moitiés successives d'un nombre

```
def liste(n):  
L=[]  
while(n>1):  
if n%2==0:  
L.append(0)  
n=n/2  
else:  
L.append(1)  
n=n-1  
L.reverse()  
return(L)
```

### #Donner la solution fondamentale

**def** fondamental(D):

l=donnees(D)

e=puissance(D,(l[1]/l[3],l[2]/l[3]),l[4])

return(e)

### #Puissances des solutions

**def** solutions(D,n):

L=[fondamental(D)]

for i in range(1,n):

L=L+[mult(D,L[i-1],L[0])]

return(L)

### #Donner les autres solutions à partir de la fondamentale

**def** pui2(D,(a,b),P):

L=liste(P)

e=(a,b)

E=(a,b)

if L[0]==1:

E=E

for i in range(1,len(L)):

if L[i]==0:

E=mult(D,E,E)

else:

E=mult(D,E,e)

else:

for i in range(len(L)):

if L[i]==0:

E=mult(D,E,E)

else:

E=mult(D,E,e)

return(E)

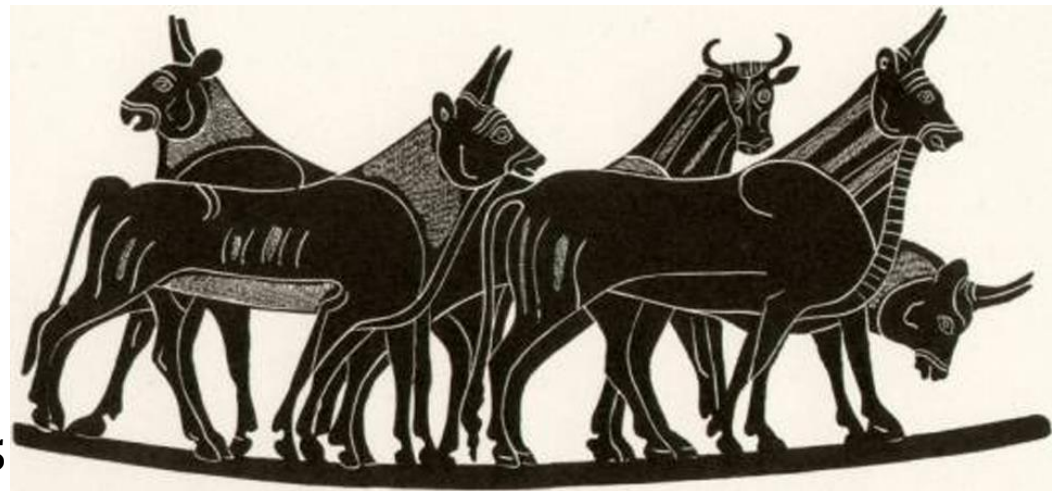
## B. Application au problème des bœufs d'Hélios

#Résultat bœufs Hélios.

D=410286423278424 et P=2

```
def resultat(D,P):  
    e=fondamental(D)  
    fichier=open("resultat.txt",'w')  
    fichier.write(str((int((pui2(D,e,P)[0]-1))*25194541)/92059576))
```

Écriture ~10sec



Troupeau :  $7,76 \cdot 10^{206545}$

## • Conclusion

776027140648681826953023283321388666423232240592337610315061922690321593061406953194348955323833033238580023195089004703344094211982833508953446  
157558874364918967966655125464772584546510461602748276908192273273239624708376752171812383319307106205947089778102846151371929989868111868841692  
72785696573474267596983337408630132757251813990392952408675358975110163303819959522862248989774767949347758862273723746255675090116296340679382  
452054261676932371219380212606631852813266328345233258182216126279820675226279382553204835331774536078819419510012902535378907943077080222390477  
002712323982680054751070633312406401842494106264559135633570932873950709846825186508464899773410357848770231421207023187305429219598310950037546  
619359116492266575520991844006671059444489935414661474017880964784212568417686213811881736706649486939349427478388044733984371799656338216395615  
067290682140459765856258954380106549596389432316812462043510835506874178802215370487620735578787317123762036035001543668020475611971279587979515  
354611992021622996696816931387575159627207593603605773271221152829620797794193624267440392635935320573979912232151674560564545791492924456171830  
301813667384589167056522577623089709143598292275630551090992443744816361683463507051783329274098023993328211302957737063485656678442873441890779  
376036197673182179631315403585193210105443103293624652486177725908896596831135843667028911733111185491846594977587665039791677109215889382268067  
519946239720594300361698612324170432810168312071503448140574573971379173734887941315310023769828368113313780683053636451507250550342600937411864  
830010550157963495114816583555475876795909042784483106585324414267249623707115372654601907558190199832272382845825509194548808552246369616821866  
714195657247590577717959340130295805375  
642869131042241359302693638651079384343  
257283706135422773378817030599492560088  
690970227387146943593774022242727905534  
848849221768729079022303105014329675931  
713365514125146616821713246052804253580  
983421187829875948093811480148364866938  
625181770918885962860179616995497679567  
631530075412865391722210014546268189028  
879533507808931006202760224408823846524  
987408060435680476832971622382499245596  
613341290875259928046880740588571000851  
331492495671702737508884265990900006524  
932570315140927669468984482767036354380  
298376714081869978272602947368085520109  
634877845953631430484254087161726921107  
828876930951258618268534576626447747593  
238055326093798580010551095407701998427  
882538007053459930080903500366024493378  
123474294014063238790463120673939944762025678623603660177149305634180217481135858331756787486669728961927180923753804369650828406141949670470589  
15884662557818772661023208875566175666466213830863266430737080531164872657028058775410864084307813446855614568083326230234784104

Statistiques

Statistiques :

Pages	18
Mots	1
Caractères (espaces non compris)	206 545
Caractères (espaces compris)	206 545
Paragrophes	1
Lignes	1 435

Inclure les zones de texte, les notes de bas de page et les notes de fin

Fermer

## • Bibliographie:

- Ilan Vardi, Archimedes' Cattle Problem, New York University, Mathematics Department Occidental College.
- Michael J. Jacobson, Jr., Hugh C. Williams, Solving the Pell Equation