Bézout, Fermat revisités

M.Gouy, G.Huvent, A.Ladureau

23 mars 2003

1 Le Théorème de Bézout

1.1 Introduction

Le théorème de Bézout[1] est un des premiers résultats que l'on établit dans un cours d'arithmétique élémentaire. Rappelons ici son énoncé

Théorème 1 *Soient* a *et* b *deux entiers non nuls et premiers entre eux, alors il existe deux entiers* u *et* v *tels que*

$$au + bv = 1$$

De ce théorème, on déduit facilement l'équivalence entre "premiers entre eux" et "vérifient une relation de Bézout". Traditionnellement, ce théorème est démontré comme conséquence de l'algorithme d'Euclide[2]. Cette présentation présente l'avantage d'être constructiviste, elle permet de récupérer les coefficients de Bézout par "remontée". En pratique la méthode de remontée est inadaptée à une programmation effective sur calculatrice ou sur un ordinateur. On résout ce problème avec l'algorithme d'Euclide étendu (voir l'article du groupe calculatrice).
Il est cependant possible de démontrer le théorème de Bézout par une autre approche : le principe de Dirichlet ou des tiroirs[3]

1.2 Le principe des tiroirs

On dispose de p objets (par exemple des colliers de perles) que l'on désire ranger dans n tiroirs différents (d'une petite commode par exemple)
Le principe des tiroirs[4] affirme que si $n < p$, i.e. si le nombre de tiroirs est inférieur au nombre de colliers, alors un des tiroirs contient au moins deux colliers.

Enoncé ainsi ce principe relève du sens commun. La démonstration se fait immédiatement par l'absurde.
L'efficacité de ce principe va nous apparaître sur quelques exemples simples.

Exercice 2 *On se donne* 2003 *entiers* $a_1, \cdots, a_{2003},$, *alors on peut en trouver* n *consécutifs dont la somme est divisible par* 2003

Exercice 3 *Montrer que parmi quatre nombres réels deux à deux distincts, il en existe deux* a *et* b *tels que* $0 \leq \dfrac{a-b}{1+ab} \leq 1$

On pourra consulter également l'article [1] "De l'ordre dans le désordre" publié par l'IREM de Lille.
Comment peut-on prouver le théorème de Bézout à l'aide du principe des tiroirs ?

[1] Le théorème de Bezout pour les entiers a été établi par Bachet de Meziriac en 1624. Bezout a démontré ensuite celui concernant les polynômes.
[2] Ou dans l'enseignement supérieur à l'aide des idéaux. On signale alors que l'algorithme d'Euclide permet le calcul effectif des coefficients de Bezout.
[3] "Pigeon Hole " dans la littérature anglophone.
[4] Dit aussi principe de Dirichlet

1.3 Bézout par l'approximation de Dirichlet

Considérons un réel, par exemple $\pi = 3,\ 141\,592\,654....$ On cherche à approcher ce réel par une fraction $\frac{p}{q}$ dont le dénominateur est inférieur à 10. Considérons alors la suite $\pi_i = i \times \pi$ pour $i = 0,1,2,3,4,5,6,7,8,9,10$. La fraction cherchée est telle que $q\pi \simeq p$. Cela incite à considérer la suite des parties entières de π_i et à observer les parties fractionnaires. On définit ainsi α_i

$$\alpha_i = \{\pi_i\} = \pi_i - E(\pi_i)$$

où

$$E(\pi_i) \text{ est la partie entière de } \pi_i$$

Les $(\alpha_i)_i$ sont 11 réels de l'intervalle $[0,1[$.

$$\begin{aligned}
\alpha_0 &= 0, \alpha_1 = 0.14159265,\ \alpha_2 = 0.28318530,\\
\alpha_3 &= 0.42477796,\ \alpha_4 = 0.56637062,\ \alpha_5 = 0.70796327,\\
\alpha_6 &= 0.84955592,\ \alpha_7 = 0.99114858,\ \alpha_8 = 0.13274123,\\
\alpha_9 &= 0.27433389, \alpha_{10} = 0.41592654
\end{aligned}$$

On va les placer dans les tiroirs formés par les 10 intervalles $\left[0, \frac{1}{10}\right[$, $\left[\frac{1}{10}, \frac{2}{10}\right[$, $\left[\frac{2}{10}, \frac{3}{10}\right[$, $\cdots$, $\left[\frac{9}{10}, 1\right[$.
($\alpha_i \neq 1$ car $E(\pi_i) \leq \pi_i < E(\pi_i) + 1$ par définition de la partie entière)
Par le principe de Dirichlet, deux des α_i sont dans le même tiroirs.
Ici on constate que

$$\begin{aligned}
\alpha_1 \text{ et } \alpha_8 \text{ sont dans } &\left[\frac{1}{10}, \frac{2}{10}\right[\\
\alpha_2 \text{ et } \alpha_9 \text{ sont dans } &\left[\frac{2}{10}, \frac{3}{10}\right[\\
\alpha_3 \text{ et } \alpha_{10} \text{ sont dans } &\left[\frac{4}{10}, \frac{5}{10}\right[
\end{aligned}$$

On s'intéresse, par exemple au cas de α_2 et α_9. On a

$$\begin{aligned}
\frac{2}{10} &\leq 9\pi - E(9\pi) < \frac{3}{10}\\
\frac{2}{10} &\leq 2\pi - E(2\pi) < \frac{3}{10}
\end{aligned}$$

Par soustraction, il vient

$$\frac{-1}{10} < 7\pi - (E(9\pi) - E(2\pi)) < \frac{1}{10}$$

Posons

$$q = 7,\ p = E(9\pi) - E(2\pi) = 22$$

On obtient

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{7 \times 10}$$

Si on considère les autres cas, on a obtient la même approximation

Remarque 4 *On peut tout a fait obtenir d'autres approximations. Avec* $x = \sqrt{3}$, *si l'on cherche les fractions de dénominateurs inférieurs à* 5, *on obtient*

$$\begin{aligned}
\alpha_0 \text{ et } \alpha_3 \in \left[0, \frac{1}{5}\right[&\text{ donne l'approximation } \left|\sqrt{3} - \frac{5}{3}\right| \leq \frac{1}{3 \times 5}\\
\alpha_1 \text{ et } \alpha_5 \in \left[\frac{3}{5}, \frac{4}{5}\right[&\text{ donne l'approximation } \left|\sqrt{3} - \frac{7}{4}\right| \leq \frac{1}{4 \times 5}
\end{aligned}$$

Dans ce cas, afin d'avoir la meilleure approximation possible, on peut chercher les entiers i *et* j *tels que* α_i *et* α_j *soient dans le même tiroir et* $|i-j|$ *soit maximal. Dans l'exemple précédent, la seconde approximation donne l'erreur la plus petite.*

La méthode, que l'on vient d'expérimenter donne le résultat suivant.

Proposition 5 (Approximation de Dirichlet) *Soit* $x \in \mathbb{R}$ *et* $N \in \mathbb{N}^*$, *il existe* $(p,q) \in \mathbb{N}^2$ *tels que*

$$1 \leq q \leq N$$

et

$$\left|x - \frac{p}{q}\right| < \frac{1}{q \times N}$$

En particulier

$$|qx - p| < \frac{1}{N}$$

Preuve. *Posons* $\alpha_k = kx - E(kx)$, *et* $I_k = \left[\frac{k-1}{N}, \frac{k}{N}\right[$ *pour* $k = 0, 2, \cdots, N$. *On a* $N+1$ *réels de* $[0,1[$ *à placer dans les* N *tiroirs* $I_1, I_2, \cdots, I_n$. *L'un des tiroirs contient deux éléments. Soit par exemple* α_i *et* α_j, *avec* $j > i$ *qui sont tous deux dans le tiroir* I_m. *On a donc les inégalités*

$$\frac{m-1}{N} \leq \alpha_j < \frac{m}{N}$$
$$\frac{m-1}{N} \leq \alpha_i < \frac{m}{N}$$

Par soustraction,

$$|\alpha_j - \alpha_i| = |(i-j)x - (E(jx) - E(ix))| < \frac{1}{N}$$

Posons alors

$$q = (j-i)$$
$$p = E(jx) - E(ix)$$

Alors

$$1 \leq q \leq N-1$$

et

$$|qx - p| < \frac{1}{N}$$

■

Comment exploiter ce résultat pour en déduire le théorème de Bézout ? Rien n'est plus simple. On considère a et b deux entiers non nuls premiers entre eux avec $b \geq 2$. On pose alors $x = \frac{a}{b}$ qui est une fraction irréductible. On applique le théorème précédent avec $N = b-1$. Cela assure l'existence de p et q tels que

$$\left|q\frac{a}{b} - p\right| < \frac{1}{N} = \frac{1}{b-1}$$

ce qui équivaut à

$$|qa - pb| < \frac{b}{N} = \frac{b}{b-1} = 1 + \frac{1}{b-1} \leq 2$$

Pour conclure, il suffit de remarquer que $|qa - pb|$ est un entier non nul (car sinon $\frac{a}{b} = \frac{p}{q}$ et $q < b$ n'est pas irréductible), il est donc égal à ± 1.
Quitte à changer les signes de p et q,on a trouvé $(u,v) \in \mathbb{N}^2$ tels que

$$au - bv = 1$$

Cette méthode peut se programmer sur une calculatrice ou avec un logiciel de calcul Formel comme Maple. Quelques essais (à la main, ou après programmation) montre que l'on trouve toujours deux réels α_i et α_j dans le premier tiroirs $\left[0, \frac{1}{b-1}\right[$.

1.4 Programmation effective

1.4.1 Coefficients de Bézout optimums

Soient a et b deux entiers premiers entre eux, on vient de prouver l'existence de u et v tels que

$$au - bv = 1$$

Le couple (u, v) est dit un couple de Bézout de (a, b). Il est alors facile d'en fabriquer d'autres.
En effet $\forall k \in \mathbb{Z}$, $(u + kb, v + ka)$ est un couple de Bézout. Si l'on cherche maintenant un couple (u_0, v_0) tel que

$$0 < u_0 < b$$

on est ramené au problème de l'existence de $k \in \mathbb{Z}$ tel que

$$0 < u + kb < b \iff -\frac{u}{b} < k < 1 - \frac{u}{b}$$

Cette inéquation admet une solution (unique), en effet $-\frac{u}{b} \notin \mathbb{Z}$ (car sinon b divise u et ainsi b divise $au - bv = 1$), on a donc

$$E\left(-\frac{u}{b}\right) < -\frac{u}{b} < E\left(-\frac{u}{b}\right) + 1 < -\frac{u}{b} + 1$$

ce qui prouve que

$$k = E\left(-\frac{u}{b}\right) + 1 \text{ convient}$$

Remarque 6 *On peut aussi remarquer que l'intervalle* $\left[-\frac{u}{b}, 1 - \frac{u}{b}\right]$ *est de largeur* 1, *d'extrémités non entières donc contient un entier dans son intérieur.*

Remarque 7 *On a trouvé* u_0 *tel que* $0 < u_0 < b$, *on en déduit que*

$$-\frac{1}{b} < v_0 = \frac{au_0 - 1}{b} < a - \frac{1}{b}$$

et puisque v_0 *est entier*

$$0 < v_0 < b$$

1.4.2 Localisation des α_i égaux de la suite $(\alpha_0, \cdots, \alpha_{b-1})$

On a donc trouvé $(u_0, v_0) \in \mathbb{N}^2$ tels que

$$\begin{aligned} au_0 - bv_0 &= 1 \\ 0 < u_0 &< b \end{aligned}$$

On en déduit que

$$u_0\frac{a}{b} = v_0 + \frac{1}{b} \Longrightarrow E\left(u_0\frac{a}{b}\right) = v_0$$

et ainsi

$$\alpha_{u_0} = u_0\frac{a}{b} - E\left(u_0\frac{a}{b}\right) = \frac{1}{b} < \frac{1}{b-1}$$

En conséquence

$$\alpha_0 \text{ et } \alpha_{u_0} \text{ sont dans l'intervalle } \left[0, \frac{1}{b-1}\right[$$

Ceci permet une programmation effective de la recherche des couples de Bézout par l'approximation diophantienne. On calcule de proche en proche les α_i (pour $i \leq b - 1$), dès que l'on en trouve un inférieur à $\frac{1}{b-1}$, l'entier u est son

indice et $v = \dfrac{au-1}{b}$.
Afin d'améliorer un peu la méthode, il est souhaitable de procéder ainsi. On se donne deux entiers a et b premiers entre eux avec $a > b$. On calcule $f = \left\{\dfrac{a}{b}\right\} = \dfrac{a}{b} - E\left(\dfrac{a}{b}\right)$. On a alors $\alpha_0 = 0,\ \alpha_1 = f,\ \alpha_2 = 2f - E(2f)$ ...

L'algorithme est donc le suivant :

Entrée : a et b avec $a > b$
$f \longleftarrow \dfrac{a}{b} - E\left(\dfrac{a}{b}\right)$
$x \longleftarrow f$
Pour i de 1 tant que $x \geq \dfrac{1}{b-1}$ faire $x \longleftarrow i \times f - E(i \times f)$
$u \longleftarrow i - 1,\ v \longleftarrow \dfrac{au-1}{b}$
Sortie : u, v

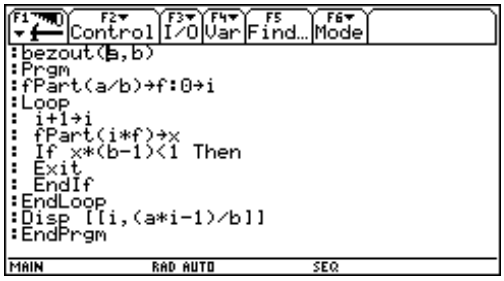
Ce qui donne les programmes suivant en Maple et pour les calculatrices TI 89, 92 et Voyage 200

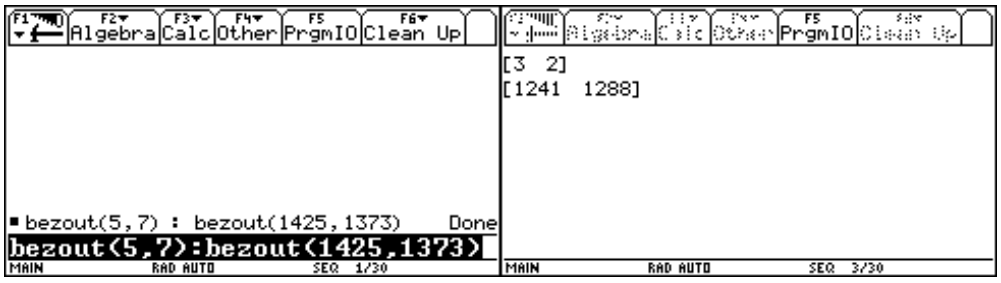
Programme Maple

```
> bezout :=proc(a,b) local f,x,i,u ; f :=frac(a/b) ;
x :=f ;
for i from 1 while x>1/(b-1)
do
x :=frac(i*f)
od ;
u :=i-1 ;
(u,(a*u-1)/b)
end :
> bezout(5,7) ;
                    3, 2

> bezout(1425,1288) ;
                  1241, 1373
```

Programme Texas-Instruments





Remarque 8 *Pourquoi supposer* $a > b$ *? On sait que l'on va faire au plus* $b-1$ *essais avant de trouver* u_0*, il est alors clair qu'il faut mieux avoir* $b < a$*.*

1.5 Bézout et la fonction "totient"

On rappelle que la fonction totient d'Euler (ou indicatrice d'Euler) est définie par :

$$\varphi(n) \text{ est le nombre d'entier compris entre } 1 \text{ et } n-1 \text{ et premiers avec } n.$$

On dispose alors du théorème suivant (cf article sur Fermat)

Théorème 9 (Euler 1760) *Si* a *et* n *sont premiers entre eux alors* $a^{\varphi(n)} \equiv 1 \ (n)$

Ainsi si a et b sont premiers entre eux, on a

$$\frac{a^{\varphi(b)}-1}{b} \in \mathbb{N}$$

on en déduit que

$$a \times a^{\varphi(b)-1} + b \times \left(\frac{1-a^{\varphi(b)}}{b}\right) = 1$$

Formule qui donne un couple de Bézout

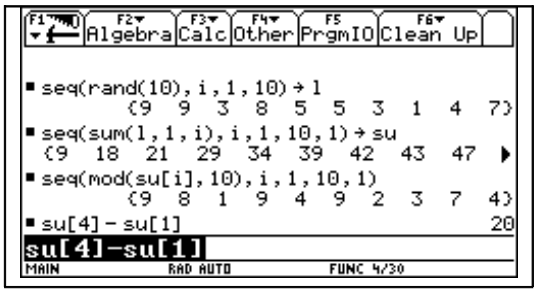
$$\begin{aligned} u &= a^{\varphi(b)-1} \\ v &= \left(\frac{1-a^{\varphi(b)}}{b}\right) \end{aligned}$$

Par exemple pour $a = 2$ et $b = 3$, on trouve $u = 2$ et $v = -1$ (ce qui est raisonnable). Avec $a = 5$ et $b = 7$, on a $u = 3125$ et $v = -2232$ (ce qui est vraiment déraisonnable). Cette formule est très belle mais complètement inutile....

2 Solutions des exercices

Exercice 1.

On considère les 2003 sommes $S_1 = a_1, S_2 = a_1 + a_2, \cdots, S_{2003} = a_1 + a_2 + \cdots + a_{2003}$ dont on prend les restes modulo 2003. Ces restes sont dans $\{0, 1, \cdots, 2002\}$. Si l'un d'entre eux est nul, c'est terminé. Sinon ces restes sont dans l'ensemble $\{1, 2, \cdots, 2002\}$ qui a 2002 éléments (tiroirs). Deux des restes sont égaux, par exemple $S_i = S_j \ (2003)$ avec $i > j$. Mais alors $S_i - S_j = a_{j+1} + \cdots + a_i$ est divisible par 2003.
Par exemple avec 10 au lieu de 2003, on utilise le générateur aléatoire le la Voyage 200 pour obtenir



On crée un suite d'entiers entre 1 et 10
On crée la suite des sommes
puis celle modulo 10
On constate que $S_1 = S_4$

Remarque : On choisit des entiers entre 0 et 9 car le problème reste le même (n'oubliez pas que l'on cherche une somme divisible par 10)

Exercice 2.

Notons x_1, x_2, x_3, x_4 et x_5 ces cinq réels et $\alpha_1, \cdots, \alpha_5$ les réels de $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ tels que $x_i = \tan \alpha_i$. On découpe l'intervalle

$\left]-\frac{\pi}{2},\frac{\pi}{2}\right[$, de largeur π, en 4 intervalles de largeur $\frac{\pi}{4}$: $I_1=\left]-\frac{\pi}{2},-\frac{\pi}{4}\right[$, $I_2=\left]-\frac{\pi}{4},0\right]$, $I_3=\left]0,\frac{\pi}{4}\right]$ et $I_4=\left]\frac{\pi}{4},\frac{\pi}{2}\right[$. On a quatre tiroirs et cinq éléments. Deux au moins, α etβ, sont dans le même intervalle et vérifient (si $\alpha>\beta$)

$$\begin{aligned} 0 &\leq \alpha-\beta\leq\frac{\pi}{4}\Longrightarrow\tan 0\leq\tan(\alpha-\beta)=\frac{a-b}{1+ab}\leq 1\\ \text{où } a &= \tan\alpha, b=\tan\beta \end{aligned}$$

Références

[1] *De l'ordre dans le désordre*, M.Gouy, G.Huvent, A.Ladureau, Publication de l'Irem de Lille.
`http://perso.wanadoo.fr/gery.huvent`

[2] Le théorème de Fermat revisité, M.Gouy, G.Huvent, A.Ladureau, Publication de l'Irem de Lille.
`http://perso.wanadoo.fr/gery.huvent`