PGCD, Théorème de Bézout, Théorème de Gauss

Algorithme d'Euclide

Soit $a, b \in \mathbb{N}^*$, b ne divise pas a :

- Si $a = bq + r$ alors $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.
  On démontre cette égalité par une double inégalité.
- Les divisions successives du diviseur par le reste finissent par s'arrêter. Le dernier reste non nul est alors $\text{pgcd}(a,b)$.
  C'est le principe de la descente infinie dans $\mathbb{N}$.
- **Exemple** : Calculer $\text{pgcd}(4\,539, 1\,958)$.

$$4\,539 = 1\,958 \times 2 + 623$$
$$1\,958 = 623 \times 3 + 89$$
$$623 = 89 \times 7 + 0$$

Conclusion : $\text{pgcd}(4\,539, 1\,958) = 89$.

PGCD

Soit a et b deux entiers relatifs non nuls.
L'ensemble des diviseurs communs à a et b admet un plus grand élément D, appelé **plus grand commun diviseur**.
On note : $D = \text{pgcd}(a,b)$

Propriétés

- $\text{pgcd}(ka, kb) = k\text{pgcd}(a,b)$
- Si b divise a alors $\text{pgcd}(a,b) = |b|$

a et b sont premiers entre eux ssi $\text{pgcd}(a,b) = 1$

⚠ Ne pas confondre des nombres premiers entre eux comme 15 et 8 et des nombres premiers comme 7 et 13.

Exemple de résolution

Résoudre dans $\mathbb{Z}^2$, (E) : $2x - 3y = 5$

- L'équation admet des solutions car $\text{pgcd}(2,3) = 1$ et 5 multiple de 1.
- On cherche une solution particulière, ici (4,1).
- On soustrait termes à termes la solution particulière et la solution générale, on trouve alors
  (E') : $2(x-4) = 3(y-1)$.
- 3 divise $2(x-4)$, comme $\text{pgcd}(2,3) = 1$, d'après le théorème de Gauss, 3 divise $(x-4)$. On a alors $x - 4 = 3k$, $k \in \mathbb{Z}$.
- On remplace dans (E') , on trouve alors $y - 1 = 2k$
- L'ensemble des couples (x,y) solution de (E) est alors :

$$\begin{cases} x = 4 + 3k \\ y = 1 + 2k \end{cases}, \quad k \in \mathbb{Z}$$

Bézout

- **Identité de Bézout** : Soit $\text{pgcd}(a,b) = D$ alors il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = D$
- **Théorème de Bézout** : a et b sont premiers entre eux ssi il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$
- **Corollaire de Bézout** : L'équation $ax + by = c$ admet des solutions entières ssi c est un multiple de $\text{pgcd}(a,b)$

Gauss - ROC

- **Théorème de Gauss** : Si a divise bc et si a et b sont premiers entre eux alors a divise c.
- **Corollaire de Gauss** : Si b et c divise a et si b et c sont premiers entre eux alors bc divise a.

Utilisation du théorème de Bézout

- Soit $n \in \mathbb{N}$, on donne $a = 2n + 1$ et $b = 3n + 2$. Montrer $\forall n \in \mathbb{N}$, que a et b sont 1er entre eux.

  Il faut trouver une combinaison linéaire qui supprime le nombre n et dont le résultat donne 1 :

  $$-3a + 2b = -6n - 3 + 6n + 4 = 1$$

  D'après le théorème de Bézout, il existe un couple $(-3\ ;\ 2) \in \mathbb{Z}^2$ tel que $-3a + 2b = 1$, les nombres a et b sont premiers entre eux.

Utilisation de corollaire du théorème de Bézout

L'équation (E) : $221x + 338y = 26$ admet-elle des solutions entières ?

$\text{pgcd}(221, 338) = 13$ et $26 = 2 \times 13$, donc d'après le corollaire du théorème de Bézout, l'équation (E) admet des solutions entières.

Pour trouver une solution particulière, on divise par 13 : $17x + 26y = 2$, puis l'on cherche une solution évidente, ici $x = -6$ et $y = 4$

Équation diophantienne

Ce sont les équations de la forme : $ax + by = c$.
Pour résoudre, si $c = k \times \text{pgcd}(a,b)$

- On divise l'équation par $\text{pgcd}(a,b)$.
- On cherche une solution particulière.
- Puis une solution générale en soustrayant termes à termes la solution particulière et la solution générale. On applique le théorème de Gauss et on conclut sur l'ensemble des couples solutions.

PPCM

(Notion maintenant hors programme)

L'ensemble des multiples strictement positifs de deux entiers a et b admet un plus petit élément appelé **p**lus **p**etit **c**ommun **m**ultiple. Il se note $\text{ppcm}(a,b)$.

Le ppcm sert entre autre à déterminer le dénominateur commun de deux fractions.
$\text{ppcm}(6,15)=30$, on a alors $\dfrac{7}{6}+\dfrac{11}{15}=\dfrac{35+22}{30}=\dfrac{57}{30}=\dfrac{19}{10}$

Propriétés : On pose : $D=\text{pgcd}(a,b)$ et $M=\text{ppcm}(a,b)$. À l'aide des théorèmes de Bézout et Gauss, on peut montrer les relations suivantes.

- Il existe deux entiers a' et b' premiers entre eux tels que : $\begin{cases} a=Da' \\ b=Db' \end{cases}$
- $M=Da'b'$ et $ab=MD$

Théorème chinois

Dans les annales du bac, on trouve des exercices qui ont pour but de résoudre le système suivant :

$$\begin{cases} x\equiv a\ (n_1) \\ x\equiv b\ (n_2) \end{cases},\quad \text{pgcd}(n_1,n_2)=1$$

Il n'y a pas de méthode particulière à savoir en terminale. Vous n'aurez qu'à vous laisser guider par l'énoncé où interviendront les théorèmes de Bézout et Gauss.
Ce type de problème peut intervenir dans la conjonction d'astres célestes.

Le théorème chinois permet sa résolution dont le nom vient de l'énoncé :

« Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ? »

$$\begin{cases} n\equiv 3 \mod 17 \\ n\equiv 4 \mod 11 \\ n\equiv 5 \mod 6 \end{cases} \Rightarrow$$

La plus petite valeur possible est 785 pièce d'or

Chiffrement

Afin de coder un message on assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le chiffrement ou cryptage consiste à coder un message. Le déchiffrement consiste à décoder une message codé.

Etienne Bézout (1730-1783)

Carl Friedrich Gauss (1777-1855)

Application

Un chiffrement élémentaire est le chiffrage affine. On se donne une fonction de codage affine f, par exemple : $f(x)=11x+8$.
À une lettre du message :

- on lui associe un entier x entre 0 et 25 suivant le tableau ci-dessus
- on calcule $f(x)=11x+8$ et l'on détermine le reste y de la division euclidienne de $f(x)$ par 26
- On traduit y par une lettre d'après le tableau ci-dessus

Exemple : Si l'on veut coder par exemple la lettre G par la fonction $f(x)=11x+8$

G $\Rightarrow$ $x=6$ $\Rightarrow$ $11\times 6+8=74$ $\Rightarrow$ $74\equiv 22\ (26)$ $\Rightarrow$ $y=22$ $\Rightarrow$ W

La lettre G est donc codée par la lettre W.

Remarques

- Pour la fonction de déchiffrage f^{-1}, vous n'aurez qu'à vous laisser guider par l'énoncé. Dans l'exemple $f^{-1}(y)=19y+4$.
- D'autres chiffrements existent comme le chiffrement de Hill où l'on prend les lettres par paquet de 2. Là encore laissez-vous guider par l'énoncé.