Chapitre 3

Théorème de Bezout et conséquences

1°) Le théorème de Bezout.

Théorème : Soit $(a,b) \in \mathbb{Z}^2$ et $d \in \mathbb{N}$,

on a :

$$d = \text{pgcd}(a,b)$$

ssi $\begin{cases} i) & d \mid a \text{ et } d \mid b \\ ii) & \exists (u,v) \in \mathbb{Z}^2, \quad au + bv = d. \end{cases}$

Preuve :

$\Rightarrow$ Soit $d = \text{pgcd}(a,b)$.

Le i) est vrai par définition.

Puisque d est le générateur de $a\mathbb{Z} + b\mathbb{Z}$, $d \in a\mathbb{Z} + b\mathbb{Z}$, il existe donc $u, v \in \mathbb{Z}$ tels que

$$d = au + bv.$$

($\Leftarrow$) Considérons un autre diviseur commun à a et b, que l'on note d'. Puisque d' divise a et b, d' divise $au + bv$, donc d' divise d. Ceci montre que $d = pgcd(a, b)$.

$\square$

Remarques :

i) Si $d \geqslant 2$, la condition i), $d \mid a$ et $d \mid b$, est essentielle.

Par exemple, si $a = 3$, $b = 1$ et $d = 2$

On a bien :

$$1 \times 3 + (-1) \times 1 = 2$$

$$1 \times a + (-1) \times b = d$$

Mais $d \neq pgcd(a, b)$.

ii) En revanche, si $d = 1$, la condition i) est automatique. On obtient alors le

Corollaire : Soit $(a, b) \in \mathbb{Z}^2$

$\operatorname{pgcd}(a, b) = 1$

$\Longleftrightarrow \exists (u, v) \in \mathbb{Z}^2 ; \quad au + bv = 1.$

Donnons quelques premières applications du théorème de Bezout :

Propriété : Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ et $d = a \wedge b$.
Soit $(a', b') \in \mathbb{Z}^2$ tels que

$$a = da' , \quad b = d b'.$$

Alors $\operatorname{pgcd}(a', b') = 1.$

Preuve :

D'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$$au + bv = d$$

$$\Longrightarrow \quad da'u + d b'v = d.$$

Puisque a et b ne sont pas tous deux nuls, $d \neq 0$ et on peut diviser par d pour obtenir :

$$a'u + b'v = 1.$$

D'après le corollaire de Bezout
$$\mathrm{pgcd}(a', b') = 1. \qquad \square$$

Propriété : Soit $(a, b) \in \mathbb{Z}^2$ et $k \in \mathbb{N}$,
$$\mathrm{pgcd}(ka, kb) = k \cdot \mathrm{pgcd}(a, b)$$

Preuve : Soit $d = \mathrm{pgcd}(a, b)$. Montrons que kd vérifie le critère de théorème de Bezout :

i) $d \mid a$ donc kd divise ka.

De même kd divise kb.

ii) Soit $(u, v) \in \mathbb{Z}^2$ tel que
$$au + bv = d.$$

Alors $(ka)u + (kb)v = kd$.

Ceci montre que
$$kd = \mathrm{pgcd}(ka, kb). \qquad \square$$

2°) Calcul de coefficients de Bezout.

Soit $(a, b) \in \mathbb{Z}^2$ et $d = a \wedge b$.
Les couples d'entiers $(u, v) \in \mathbb{Z}^2$ tels que

$$au + bv = d$$

Sont appelés des coefficients de Bezout.

Ces coefficients ne sont pas uniques : si $au + bv = d$, alors $a(u + kb) + b(v - ka)$ vaut aussi d pour tout entier k.
Il y a donc une infinité de coefficients de Bezout possibles.

Il sera souvent utile de trouver un couple de coefficients. S'il n'y a pas de couple évident, on utilisera l'algorithme d'Euclide augmenté.

Principe de l'algorithme d'Euclide augmenté (ou étendu):

On cherche à trouver les coefficients de Bezout pour les entiers a et b.

- On effectue l'algorithme d'Euclide pour a et b, en conservant bien la liste des différentes divisions euclidiennes.
- Pour chacune de ces équations, on exprime le reste comme une combinaison linéaire entière du dividende et du diviseur.

- Partant du dernier reste non nul, qui est le pgcd, on remonte les équations de l'algorithme d'Euclide, en remplaçant successivement chaque reste en fonction du diviseur et du dividende.

- À la fois, le pgcd s'écrit comme une combinaison linéaire entière de a et b.

Exemple : $a = 358$, $b = 42$

$$358 = 8 \times 42 + 22 \implies 22 = 358 - 8 \times 42 \quad (1)$$
$$42 = 1 \times 22 + 20 \implies 20 = 42 - 22 \quad (2)$$
$$22 = 1 \times 20 + 2 \implies 2 = 22 - 20 \quad (3)$$
$$20 = 10 \times 2 + 0$$

pgcd.

On part de l'équation (3) :
$$2 = 22 - 20.$$
On remplace 20 à l'aide de (2) :
$$2 = 22 - (42 - 22)$$
$$= -42 + 2 \times 22$$
On remplace 22 à l'aide de (1) :

$$2 = -42 + 2 \times (358 - 8 \times 42)$$
$$2 = 2 \times 358 - 17 \times 42$$
$$= ua + vb$$

où $u = 2$, $v = -17$.

3°) Lemme de Gauss.

Le résultat suivant est un corollaire essentiel du théorème de Bezout :

Proposition (Lemme de Gauss)

Soient a, b, c trois entiers.
Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Preuve :

Puisque $a \wedge b = 1$, il existe $u, v \in \mathbb{Z}^2$ tels que :

$$au + bv = 1$$
$$\Longrightarrow \quad bv = 1 - au \qquad (1)$$

Par ailleurs, puisque $a \mid bc$, il existe $k \in \mathbb{Z}$ tel que

$$bc = ka$$

$\Longrightarrow$ $vbc = vka$ (après multi. par v)

$\Longrightarrow$ $(1 - au)c = vka$ (en utilisant (1)).

$\Longrightarrow$ $c = a(uc + kv)$

$\Longrightarrow$ $a \mid c$. $\square$

Remarque :

Ce résultat est évidemment faux si $a \wedge b \neq 1$.

Par exemple, si $a = 4$, $b = 2$ et $c = 2$ on a bien $4 \mid 2 \times 2$, mais $4 \nmid 2$.

Voici quelques conséquences du lemme de Gauss.

Corollaire (Lemme d'Euclide) :

Soit $(a, b, c) \in \mathbb{Z}^3$.
Si $a | c$, $b | c$ et $a \wedge b = 1$,
alors $ab | c$.

Preuve : Puisque $a | c$, il existe $k \in \mathbb{Z}$ tel que $c = ka$.

On a aussi, $b | c$, donc $b | ka$.
Puisque $b \wedge a = 1$, $b | k$ d'après le lemme de Gauss.

Il existe donc $k' \in \mathbb{Z}$ tel que $k = bk'$.

On en déduit : $c = ka = k'ab$. $\square$

Corollaire 2 :

Soit p un nombre premier.
Soit $q \in \mathbb{N}$ tel que $0 < q < p$.
Le coefficient binomial $\binom{p}{q}$ est divisible par p.

Preuve : Posons $N = \binom{p}{q}$.

Puisque $N = \dfrac{p!}{q!(p-q)!}$, on a :

$$p! = N\, q!\,(p-q)!$$

Donc p divise $N q!\,(p-q)!$.

Puisque p ne divise pas q, $p \wedge q = 1$.
le lemme de Gauss permet alors de dire que

$$p \text{ divise } N \times (q-1)!\,(p-q)!$$

On réapplique q fois le lemme de Gauss pour obtenir :

$p \mid N\,(p-q)!$

On recommence ensuite avec $(p-q)!$ pour obtenir $p \mid N$. $\square$

4°) Equations diophantiennes de la forme $ax + by = c$.

Soit $(a, b, c) \in \mathbb{Z}^3$.
On cherche l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ solutions de l'équation

$$ax + by = c.$$

Etape 1 : On calcule $d = \mathrm{pgcd}(a, b)$.

* Si d ne divise pas c, il n'y a pas de solution (car d divise $ax + by$). C'est terminé.
* Si d divise c, on divise toute l'équation par d pour obtenir une équation équivalente :

$a'x + b'y = c'$ $(a = da', b = db', c = dc')$.

avec en plus : $\text{pgcd}(a', b') = 1$.

Etape 2 : On suppose maintenant que l'équation s'écrit :

$$ax + by = c, \quad \text{avec } a \wedge b = 1.$$

On cherche une solution particulière à partir de coefficients de Bezout pour a et b (que l'on peut trouver avec l'algo. d'Euclide augmenté).

$$au + bv = 1$$

$$\Rightarrow a(uc) + b(vc) = c$$

(multiplication par c).

Posons $x_0 = uc$ et $y_0 = vc$.

Le couple (x_0, y_0) est donc une solution particulière.

Etape 3 : Solutions générales.

Soit (x, y) une solution. On a :

$$\begin{cases} ax + by = c \\ ax_0 + by_0 = c \end{cases}$$

$\Rightarrow \quad a(x - x_0) + b(y - y_0) = 0 \quad (*)$

$\Rightarrow \quad a \mid b(y - y_0).$

Puisque $a \wedge b$, le lemme de Gauss nous assure que $a \mid (y - y_0)$.

Il existe donc $k \in \mathbb{Z}$ tel que

$$y - y_0 = ka$$

et $y = y_0 + ka$.

Remplaçons $(y - y_0)$ par ka dans l'équation ci-dessus. On obtient :

$$a(x - x_0) = -bka$$

$\Rightarrow x - x_0 = -kb$

$\Rightarrow \quad x = x_0 - kb.$

Le couple (x, y) peut donc s'écrire $(x_0 - kb, y_0 + ka)$ avec $k \in \mathbb{Z}$.

Réciproquement, on vérifie que tout couple de cette forme est une solution.

L'ensemble des solution est donc :

$$S = \{ (x_0 - kb, y_0 + ka) ; k \in \mathbb{Z} \}.$$