THEOREME DE BEZOUT - THEOREME DE GAUSS

1) THEOREME DE BEZOUT

Théorème de Bézout :

Soit a et b deux entiers relatifs non nuls.
a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Preuve :

- Supposons qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.
  Soit D le PGCD de a et b, alors D divise a et D divise b, donc D divise $au + bv$. Donc D divise 1. Donc $D = 1$.
  On en déduit alors que a et b sont premiers entre eux.

- Supposons que a et b sont premiers entre eux.
  Considérons l'ensemble E des entiers naturels non nuls de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.
  E n'est pas vide (E contient a ou $-a$, E contient b ou $-b$, E contient $2a + 3b$ ou $-2a - 3b$ ...), donc E a un plus petit élément m.
  On peut écrire $m = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

  Écrivons la division euclidienne de a par m : $a = mq + r$ avec $r \in \mathbb{N}$ et $0 \leq r < m$.
  On a alors : $a = (au_1 + bv_1)\, q + r \Rightarrow r = a - (au_1 + bv_1)q \Rightarrow r = a\,(1 - u_1\, q) + b\,(-v_1\, q)$

  Donc r est un entier naturel de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ et d'autre part $r < m$.
  Comme m est le plus petit élément de E, on en déduit que $r = 0$, c'est-à-dire que a est divisible par m.

  De même on démontrerait que b est divisible par m.
  Donc m est un diviseur commun à a et b.
  Comme a et b sont premiers entre eux, on en déduit que $m = 1$.
  On a donc $1 = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

Remarque : Le théorème de Bézout est particulièrement intéressant pour travailler sur des expressions littérales ou sur des grands nombres.

Exemple :

En utilisant l'algorithme d'Euclide démontrons que 383 et 127 sont premiers entre eux et déterminons des entiers relatifs u et v tels que $383u + 127v = 1$
On peut écrire $383 = 127 \times 3 + 2$ (1)
et $127 = 2 \times 63 + 1$ (2)
Donc PGCD(383 ; 127) = 1 c'est-à-dire que 383 et 127 sont premiers entre eux.
Pour déterminer u et v, l'idée est d'exprimer le 1 qui apparaît comme reste de la dernière division en fonction des nombres 383 et 127.
D'après l'égalité (2), on peut écrire $1 = 127 - 2 \times 63$ (3)
D'après l'égalité (1), on peut écrire $2 = 383 - 127 \times 3$
En remplaçant 2 par $383 - 127 \times 3$ dans l'égalité (3), on obtient :
$1 = 127 - [383 - 127 \times 3] \times 63 = 127 - 383 \times 63 + 127 \times 3 \times 63 = 127(1 + 3 \times 63) - 383 \times 63$
On obtient alors $383 \times (-63) + 127 \times (190) = 1$. On peut donc prendre $u = -63$ et $v = 190$.

Le couple $(u\ ;\ v)$ d'entiers relatifs n'est pas unique, on peut vérifier que les couples (64 ; -293) et (-317 ; 956) répondent aussi à la question.

Propriété :

Soit a , b des entiers relatifs non nuls et D un entier naturel non nul . Les propositions si-dessous sont équivalentes :

- $D = PGCD(a\ ;\ b)$
- $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
- $a = Da'$ et $b = Db'$ a' et b' étant deux entiers relatifs non nuls premiers entre eux.

Preuve :

Soit a , b des entiers relatifs non nuls et D un entier naturel non nul.

- On a déjà vu que Si $D = PGCD(a\ ;\ b)$, alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.

- Supposons que $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.

  Puisque $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers, D divise a et D divise b .

  Soit $g = PGCD(a\ ;\ b)$.
  D divise a et b, donc D divise g et donc $D \leq g$.
  D'autre part $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux, donc il existe des entiers relatifs u et v tels que $\frac{a}{D}u + \frac{b}{D}v = 1.$, c'est-à-dire $D = au + bv$.
  Mais g étant le PGCD de a et de b, g divise a et b , donc g divise $au + bv$ donc g divise D, donc $g \leq D$.
  On a donc finalement $g = D$, c'est-à-dire $D = PGCD(a\ ;\ b)$

  On a donc démontré l'équivalence des deux premières propositions.

- L'équivalence des deux dernières propositions est immédiate.

Remarque : (Identité de Bézout)
Soit a et b deux entiers relatifs non nuls.
Si $D = PGCD(a\ ;\ b)$, alors il existe deux entiers relatifs u et v tels que $au + bv = D$.

2) THEOREME DE GAUSS

Théorème de Gauss :

Soit a et b deux entiers relatifs non nuls et c un entier relatif.
Si a divise bc et si a est premier avec b, alors a divise c.

Preuve :
Soit a et b deux entiers relatifs non nuls et c un entier relatif tels que a divise bc et a est premier avec b.
a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que $au + bv = 1$.
On a alors $acu + bcv = c$.
On sait que a divise bc, donc a divise bcv
D'autre part a divise acu
Donc a divise $acu + bcv$ c'est-à-dire a divise c .

Propriété : (parfois appelé théorème d'Euclide)

Soit a et b deux entiers relatifs et p un nombre premier.
Si p divise le produit ab, alors p divise a ou p divise b.

Preuve :
Soit a et b deux entiers relatifs. On suppose que p est un nombre premier divisant le produit ab.
Supposons que p ne divise pas a, alors $a \neq 0$ et a et p sont premiers entre eux (puisque p est premier)
Donc p divise ab et p est premier avec a, donc p divise b. (Théorème de Gauss)

Propriété :

Soit a et b deux entiers relatifs non nuls premiers entre eux et soit n un entier naturel.
Si n est divisible par a et par b, alors n est divisible par le produit ab.

Preuve :
Soit a et b deux entiers relatifs non nuls premiers entre eux, et n un entier naturel tel que n est divisible par a et par b.
a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que $au + bv = 1$.
On a alors $nau + nbv = n$.
On sait que a divise n, donc $n = aq$ avec $q \in \mathbb{Z}$ et b divise n, donc $n = bq'$ avec $q' \in \mathbb{Z}$.
L'égalité $nau + nbv = n$ peut alors s'écrire $bq'au + aqbv = n$
Alors ab divise $bq'au$ et ab divise $aqbv$ donc ab divise $bq'au + aqbv$ c'est-à-dire ab divise n.

Exemple :
Si un nombre est divisible par 5 et par 6, alors il est divisible par 30. (puisque 5 et 6 sont premiers entre eux)

3) APPLICATION : PETIT THEOREME DE FERMAT

Petit théorème de Fermat :

Si p un nombre premier et a un entier naturel non divisible par p, alors $a^{p-1} - 1$ est divisible par p. ou encore $a^{p-1} \equiv 1\ (p)$

Preuve :
Soit p un nombre premier et a un entier naturel non multiple de p.
Les entiers p et a sont donc premiers entre eux.

- Considérons l'ensemble des multiples de a : A = { a , $2a$, … , $(p - 1)\ a$ }
  Ce sont p - 1 multiples non nuls de a . L'entier p ne divise aucun d'entre eux.
  En effet, si p divisait ka (avec k entier, $1 \leq k \leq p - 1$) , puisque p est premier avec a, il diviserait k d'après le théorème de Gauss, ce qui est impossible puisque $k < p$.
  Donc leurs restes dans la division euclidienne par p sont non nuls et sont donc des éléments de {1 , 2 ,…, p - 1}
- Ces restes sont tous distincts : en effet si deux entiers k et k' appartenant à {1 , 2 ,…, p - 1}, avec $k > k$', étaient tels que $ka \equiv ka'\ (p)$ alors p diviserait $(k - k')\ a$.
  Or $1 \leq k - k' \leq p - 2$, donc $(k - k')\ a$ est élément de A et aucun élément de A n'est divisible par p.
  On a donc p - 1 multiples de a dont les restes dans la division euclidienne par p sont exactement, à l'ordre près, les entiers 1 , 2,…, p - 1.
- Considérons maintenant P le produit de ces multiples de a.
  On a donc $P \equiv 1 \times 2 \times \ldots \times (p - 1)\ \ (p)$, c'est-à-dire $P \equiv (p - 1)!\ \ (p)$. Ainsi p divise (P - (p - 1) !).
  Or en réordonnant les facteurs de P, on obtient $P = (p - 1)! \times a^{p-1}$.
  Donc $P - (p - 1)! = (p - 1)! \times a^{p-1} - (p - 1)! = (p - 1)! \times (a^{p-1} - 1)$.
  p divise donc $(p - 1)! \times (a^{p-1} - 1)$.
  Or p est premier et ne divise aucun des facteurs de $(p - 1)!$. Il est donc premier avec $(p - 1)!$
  Donc d'après le théorème de Gauss, p divise $a^{p-1} - 1$.

Propriété :

Si p un nombre premier et a un entier naturel, alors $a^p - a$ est divisible par p. ou encore $a^p \equiv a\ (p)$

Preuve :

- Si a est nul, le résultat est clairement vrai.
- Si a est non nul, a divise $a^p - a$.
  D'autre part $a^p - a = a \times (a^{p-1} - 1)$.
  On en déduit que $a^{p-1} - 1$ divise $a^p - a$.
  - Si a n'est pas un multiple de p, alors p divise $a^{p-1} - 1$ (d' après le petit théorème de Fermat) et $a^{p-1} - 1$ divise $a^p - a$.
    Par transitivité, on en déduit que p divise $a^p - a$.
  - Si a est un multiple non nul de p, alors p divise a et a divise $a^p - a$.
    Par transitivité, on en déduit que p divise $a^p - a$.