Terminale Maths Expertes – Chapitre 05

LES THÉORÈMES DE BÉZOUT ET DE GAUSS

.

Table des matières

I Théorème de Bézout

1) L'identité de Bézout

PROPRIÉTÉ

Soient a et b deux entiers naturels non nuls.
Il existe deux entiers relatifs u et v tels que $\boldsymbol{au + bv = \text{PGCD}(a\,;b)}$

DÉMONSTRATION

Soit E l'ensemble des combinaisons linéaires strictement positives de a et b :
$E = \{am + bm \in \mathbb{N}^*,\ \text{avec } m \in \mathbb{Z} \text{ et } n \in \mathbb{Z}\}$
E est non vide car il contient a et b donc E admet un plus petit élément noté d. Il existe donc deux entiers relatifs u et v tels que $au + bv = d$.
Montrons que $d = \text{PGCD}(a;b)$. Pour cela, on va montrer que $\text{PGCD}(a;b) \leqslant d$ et que $d \leqslant \text{PGCD}(a;b)$.

1) **$\text{PGCD}(a;b) \leqslant d$** :
Comme le PGCD de a et b divise a et b, il divise toute combinaison linéaire de ces entiers.
En particulier, il divise d. On en déduit que $\text{PGCD}(a;b) \leqslant d$.

2) **$d \leqslant \text{PGCD}(a;b)$** :
On effectue la division euclidienne de a par d : il existe des entiers q et r tels que $a = dq + r$ avec $0 \leqslant r < d$.
Or $r = a - dq = a - (au + bv)q = a - auq - bvq = a(1 - uq) - bvq$ est une combinaison linéaire de a et b positive ou nulle.
Si r n'était pas nul, on aurait alors construit un élément de E strictement inférieur à d, ce qui est absurde. On en déduit que r est nul et par suite que d divise a.
On montre de même que d divise b.
d est donc un diviseur commun à a et b, et par définition du PGCD, on a donc $d \leqslant \text{PGCD}(a;b)$.

3) **Conclusion** :
$d = \text{PGCD}(a;b)$ et il existe donc bien une combinaison linéaire de a et b telle que $au + bv = \text{PGCD}(a;b)$.

EXEMPLE

$\text{PGCD}(18;60) = 6$. On peut trouver un couple $(u;v)$ tel que $18u + 60v = 6$, par exemple le couple $(-3\,;1)$.

REMARQUES

1) Il n'y a pas d'unicité du couple $(u;v)$ trouvé. Dans l'exemple précédent, le couple $(7\,;-2)$ convient aussi. Pour déterminer l'ensemble de ces couples, il faut résoudre une équation diophantienne. (Voir plus loin)

2) La réciproque de cette propriété est **fausse** ! En effet, si $d = au + bv$, alors d n'est pas nécessairement le PGCD des entiers a et b.
Contre-exemple : $2 = 1 + 1$ et pourtant 2 n'est pas le PGCD du couple $(1;1)$.

2) Le théorème de Bézout

THÉORÈME

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

DÉMONSTRATION

-Si a et b sont premiers entre eux, alors $\text{PGCD}(a;b)=1$, et d'après l'identité de Bézout, il existe alors deux entiers relatifs u et v tels que $au+bv=1$.
- Réciproquement, si il existe deux entiers relatifs u et v tels que $au+bv=1$, alors tout diviseur commun à a et b divise $au+bv$, donc 1. Donc $\text{PGCD}(a;b)=1$ et donc a et b sont premiers entre eux.

EXEMPLES

1) Démontrer que, pour tout entier naturel n, $5n+7$ et $3n+4$ sont premiers entre eux.

2) **a)** Justifier qu'il existe deux entiers u et v tels que $29u+12v=1$.

b) En utilisant l'algorithme d'Euclide, déterminer un couple $(u\,;v)$ possible.

Correction :

1) $3(5n+7)-5(3n+4)=1$ donc $PGCD(5n+7\,;3n+4)=1$...

2) **a)** 29 et 12 sont premiers entre eux, donc d'après le théorème de Bézout, il existe bien deux entiers u et v tels que $29u+12v=1$.

b) D'après l'algorithme d'Euclide, on a :
$29=12\times2+5$;
$12=5\times2+2$;
$5=2\times2+1$.
En remontant l'algorithme d'Euclide, on a alors :
$1=5-2\times2=5-2\times(12-5\times2)=5\times5-2\times12$.
Et ainsi, $1=5\times(29-12\times2)-2\times12=29\times5+12\times(-12)$
Ainsi, le couple $(u\,;v)=(5\,;-12)$ convient.

EXERCICE

Après avoir justifié son existence, déterminer un entier a tel que $30a\equiv1\,[23]$.

Correction :
30 et 23 sont premiers entre eux donc, d'après le théorème de Bézout, il existe un couple d'entiers relatifs $(a\,;b)$ tel que $30a+23b=1$, donc il existe un entier a tel que $30a\equiv1\,[23]$.
D'après l'algorithme d'Euclide, on a :
$30=23\times1+7$
$23=7\times3+2$
$7=3\times2+1$
En remontant l'algorithme d'Euclide, on a alors :
$1=7-3\times2=7-3\times(23-7\times3)=7\times10-3\times23=(30-23\times1)\times10-3\times23=30\times10-13\times23$.
On en déduit que $30\times10-1=-23\times13$, donc que $30\times10-1$ est un multiple de 23, autrement dit, $30\times10\equiv1\,[23]$.
Ainsi, l'entier $a=10$ convient.

II Le théorème de Gauss

1) Le théorème

THÉORÈME

Soient a, b et c trois entiers naturels non nuls.
Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

DÉMONSTRATION

a divise bc, donc il existe un entier k tel que $bc = ka$.
a et b sont premiers entre eux. D'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $au + bv = 1$.
En multipliant cette égalité par c, on obtient $auc + bvc = c$ et par suite, comme $bc = ka$, l'égalité devient $auc + kav = c$, soit en factorisant $a(uc + kv) = c$.
Ainsi, a divise c.

EXEMPLE

Si 4 divise $3^{10} \times n$, comme 4 et 3^{10} sont premiers entre eux, on sait alors que 4 divise n.

2) Le corollaire

PROPRIÉTÉ

Soient a, b et c trois entiers naturels non nuls.
Si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.

DÉMONSTRATION

Si a et b divisent c, alors il existe deux entiers k et k' tels que $c = ka = k'b$. On en déduit que a divise $k'b$; or a et b sont premier entre eux, donc d'après le théorème de Gauss, a divise k'. Il existe donc un entier k'' tel que $k' = k''a$. On obtient alors $c = k'b = k''ab$, d'où ab divise c.

EXEMPLE

Comme 4 et 7 divisent 700 et que 4 et 7 sont premiers entre eux, alors $4 \times 7 = 28$ divise 700.

REMARQUE

La condition « a et b premiers entre eux » est essentielle dans le théorème et la propriété qui en découle.
On peut proposer deux contre-exemples :
- 6 divise $8 \times 9 = 72$ mais 6 ne divise ni 8 ni 9.
- 4 et 6 divisent 12 mais 4×6 ne divise pas 12.

III Applications

1) Résoudre une équation diophantienne

Résoudre dans $\mathbb{Z}^2$ l'équation $14x - 17y = 4$.

• Vérifions que l'équation admet des solutions :
14 et 17 sont premiers entre eux (évident, ou calcul du PGCD), et 4 est un multiple de 1, donc d'après l'identité de Bézout, l'équation $14x - 17y = 4$ admet des solutions.
(14 et 17 étant premiers entre eux, l'équation n'est pas simplifiable)

• Déterminons une solution particulière en remontant l'algorithme d'Euclide :
$17 = 14 \times 1 + 3$ donc $3 = 17 - 14$
$14 = 3 \times 4 + 2$ donc $2 = 14 - 3 \times 4$
$3 = 2 \times 1 + 1$ donc $1 = 3 - 2$.

Ainsi, on a :
$1 = 3 - 2$
donc $1 = 3 - (14 - 3 \times 4) = 3 \times 5 - 14$
donc $1 = (17 - 14) \times 5 - 14 = 14 \times (-6) + 17 \times 5$
On multiplie chaque membre de l'égalité par 4 :
$4 = 14 \times (-24) + 17 \times 20$ soit $14 \times (-24) - 17 \times (-20) = 4$.
Ainsi, une solution particulière de l'équation $14x - 17y = 4$ est $\boxed{(-24\,;-20)}$

• On modifie l'équation en utilisant cette solution particulière :
$$\begin{aligned} 14x - 17y = 4 &\iff 14x - 17y = 14 \times (-24) - 17 \times (-20) \\ &\iff 14x + 14 \times 24 = 17y + 17 \times 20 \\ &\iff \boxed{14(x+24) = 17(y+20)} \end{aligned}$$

• On termine la résolution de l'équation en déterminant toutes ses solutions :
$14(x + 24) = 17(y + 20)$ donc 14 divise $17(y + 20)$, or 14 et 17 sont premiers entre eux, donc d'après le théorème de Gauss, 14 divise $y + 20$, donc il existe $k \in \mathbb{Z}$ tel que $y + 20 = 14k$, d'où $\boxed{y = -20 + 14k}$
Or $14(x + 24) = 17(y + 20)$, donc $14(x + 24) = 17 \times 14k$, d'où $x + 24 = 17k$ donc $\boxed{x = -24 + 17k}$

• Réciproquement :
Pour **tout** $k \in \mathbb{Z}$, si $x = -24 + 17k$ et $y = -20 + 14k$, alors :
$14x - 17y = 14(-24 + 17k) - 17(-20 + 14k) = -14 \times 24 + 14 \times 17k + 17 \times 20 - 17 \times 14k = -336 + 340 = 4$
Donc $(x\,;y)$ est bien une solution de l'équation $14x - 17y = 4$.

• Conclusion :
Les solutions de l'équation $14x - 17y = 4$ dans $\mathbb{Z}^2$ sont tous les couples d'entiers relatifs de la forme

$$\boxed{(-24 + 17k\,;-20 + 14k), \text{ pour tout } k \in \mathbb{Z}.}$$

EXERCICE

- Résoudre dans $\mathbb{Z}^2$ l'équation $5x - 4y = 2$.
- Résoudre dans $\mathbb{Z}^2$ l'équation $9x - 12y = 6$.

2) Inverse modulo n

DÉFINITION

Soit a un entier relatif et soit n entier naturel supérieur ou égal à 2.
a admet un inverse modulo $n \iff$ il existe un entier b tel que $ab \equiv 1\,[n]$.
On dit que b est un inverse de a modulo n.

EXEMPLE

$4 \times 3 = 12 = 11 + 1$, donc $4 \times 3 - 1 = 12$, donc $4 \times 3 \equiv 1\,[12]$. Donc 4 est un inverse de 3 modulo 11.

PROPRIÉTÉ

Soit a un entier relatif et soit n entier naturel supérieur ou égal à 2.
a admet un inverse modulo $n \iff a$ et n sont premiers entre eux.

DÉMONSTRATION

a admet un inverse modulo $n \iff$ il existe un entier b tel que $ab \equiv 1\,[n]$
$\iff$ il existe deux entiers b et k tels que $ab - 1 = kn$
$\iff$ il existe deux entiers b et k tels que $ab + (-k)n = 1$
$\iff a$ et n sont premiers entre eux (d'après le théorème de Bézout)

REMARQUE

Si a est inversible alors il possède un inverse unique entre 1 et $n - 1$, et une infinité d'inverses car ils sont tous définis modulo n.

EXEMPLES

- Montrer que 7 possède un inverse modulo 22 puis donner celui compris entre 1 et 21.
- Résoudre dans $\mathbb{Z}$: $7x \equiv 5\,[22]$.

Correction :

- 7 et 22 sont premiers entre eux donc d'après la propriété précédente, 7 possède un inverse modulo 22. On cherche alors l'entier a compris entre 0 et 22 tel que $7a \equiv 1\,[22]$.
$22 = 7 \times 3 + 1$, donc $7 \times 3 \equiv -1\,[22]$ donc $7 \times (-3) \equiv 1\,[22]$, donc -3 est un inverse de 7 modulo 22, donc $-3 + 22 = 19$ aussi.
- $7x \equiv 5\,[22] \iff -3 \times 7x \equiv 5 \times (-3)\,[22]$ (il y a bien équivalence grâce à l'inverse modulo).
Or $-3 \times 7 \equiv 1\,[22]$, donc $7x \equiv 5\,[22] \iff x \equiv -15\,[22] \iff x \equiv 7\,[22]$.
Les solutions de l'équation $7x \equiv 5\,[22]$ sont donc les entiers $x = 7 + 22k$, avec $k \in \mathbb{Z}$.

EXERCICE

L'équation $4x \equiv 5\,[2]$ a-t-elle des solutions ?
Correction : ici, 4 et 2 ne sont pas premiers entre eux donc on ne peut pas utiliser la méthode ci-dessus avec l'inverse. Il faut revenir à une équation diophantienne : $4x \equiv 5\,[2] \iff \exists k \in \mathbb{Z} / 4x - 2k = 5$...

REMARQUE

En fait, l'équation $ax \equiv b\,[n]$ admet des solutions si PGCD$(a\,;n)$ divise b.