Arithmétique
Terminale Maths Expertes
Partie 2. PGCD et théorèmes fondamentaux

Lycée Pierre Mendes France - Tunis

Table des matières

1 PGCD de deux entiers

1.1 Diviseurs communs à deux entiers

Définition 1 (*Notation*)

Pour tous les entiers relatifs a et b, on note $D(a;b)$ l'ensemble des diviseurs communs à a et b. On a donc $D(a;b) = D(b;a) = D(a) \cap D(b)$.

Exemple

Déterminer $D(12;18)$.

....

....

....

Propriété 1 (*conséquences immédiates*)

Soient a et b deux entiers relatifs.

- $D(a;b) \subset D(b)$
- $D(a;0) = \ldots\ldots$
- $D(1;a) = \ldots\ldots$
- $D(a;b) = D(\mid a \mid ; \mid b \mid)$
- *Si* $b \mid a$, *alors* $D(a;b) = \ldots\ldots$

Propriété 2

Soient a et b deux entiers relatifs.

1. *Pour tout entier k, $D(a;b) = D(a - kb; b)$*
   En particulier, $D(a;b) = D(a - b; b)$.
2. *Si $b \in \mathbb{N}^*$ et si r est le reste de la division euclidienne de a par b, alors $D(a;b) = D(b;r)$.*

Démonstration 1

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

1.2 Définition et propriétés

Propriété 3

Étant donnés deux entiers relatifs a et b non simultanément nuls, l'ensemble $D(a;b)$ admet un plus grand élément.

Démonstration 2

....
....
....

Définition 2

Étant donnés deux entiers relatifs a et b non simultanément nuls, le plus grand élément de l'ensemble $D(a;b)$ est appelé plus grand diviseur commun de a et b. On le note indifféremment $pgcd(a;b)$ ou $PGCD(a;b)$.

Exemple

$D(12;18) = \{-6;-3;-2;-1;1;2;3;6\}$ donc $\text{pgcd}(12;18) = \ldots$

Propriété 4 (*conséquences immédiates*)

Soient a et b deux entiers relatifs avec $b \neq 0$.

- *$pgcd(b;0) = \ldots\ldots$*
- *$pgcd(a;1) = \ldots\ldots$*
- *$pgcd(a;b) = pgcd(\mid a \mid ; \mid b \mid)$*
- *Si $b \mid a$, alors $pgcd(a;b) = \ldots\ldots$*
- *$pgcd(a;b) = pgcd(b;a)$ (on parle de .... du pgcd).*

Propriété 5

Soient a et b deux entiers relatifs avec $b \neq 0$.
Pour tout $k \in \mathbb{Z}$, $pgcd(a;b) = pgcd(a - kb;b)$.
En partculier : $pgcd(a;b) = pgcd(a - b;b)$

Démonstration 3

....
....
....

Propriété 6 (*lemme d'Euclide*)

Soient a un entier relatif et b un entier naturel non nul. Si r est le reste de la division euclidienne de a par b, alors $pgcd(a;b) = pgcd(b;r)$.

Démonstration 4

....
....
....

Exercice

Soient a et b deux entiers naturels non nuls. Montrer que $\text{pgcd}(4a + 9b; 3a + 7b) = \text{pgcd}(a;b)$
....
....

1.3 Algorithme d'Euclide

Propriété 7 (*Algorithme d'Euclide*)

Soient a et b deux entiers naturels tels que $0 < b \leq a$.
L'algorithme suivant permet en un nombre fini d'étapes de calculer le pgcd de a et b :

1. *Calculer le reste r de la division euclidienne de a par b.*
2. *Si $r = 0$, alors $pgcd(a;b) = b$ sinon remplacer a par b et b par r et revenir en 1.*

Le pgcd de a et b est le dernier reste non nul.

Démonstration 5

1.4 Conséquences

Propriété 8

Soient a et b deux entiers naturels tels que $b \neq 0$. Alors :

$$D(a;b) = D(pgcd(a;b))$$

Démonstration 6

Propriété 9 (*homogénéité du pgcd*)

Soient a et b deux entiers relatifs tels que $b \neq 0$. Pour tout entier relatif k,

$$pgcd(ka; kb) = \dots\dots\dots\dots\dots\dots$$

Démonstration 7

....
....
....
....
....
....
....
....
....

2 Entiers premiers entre eux

Définition 3

On dit que deux entiers relatifs non nuls sont premiers entre eux lorsque leur pgcd est égal à 1, ce qui est équivalent à dire que leurs seuls diviseurs communs sont 1 et -1.

Exemple

14 et 39 sont premiers entre eux.

Propriété 10

Soient a et b deux entiers relatifs non nuls.
$d = pgcd(a; b)$ si, et seulement si, il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = da'$ et $b = db'$

Démonstration 8

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

Remarque

Conséquence très pratique et déjà bien connue : tout nombre rationnel s'écrit sous forme irréductible $\frac{a}{b}$, où a et b sont des entiers premiers entre eux.

3 Le théorème de Bézout

3.1 Coefficients de Bézout

Propriété 11

Soient a et b deux entiers relatifs non nul et soit δ leur pgcd.
Alors il existe un couple d'entiers relatifs (u, v) tel que $\delta = au + bv$.

Démonstration 9

....
....
....
....
....
....
....
....
....
....
....
....

Exemple

$\text{pgcd}(6; 15) = 3$ et $3 = 6 \times 3 - 15 \times 1$ ou encore $3 = 15 \times 3 - 6 \times 7$.

Remarques

- Souvent, pour déterminer les coefficients de Bézout, on procède par tâtonnement. Mais il existe des algorithmes.
- La réciproque de la propriété est fausse ! En effet, $15 \times 30 + 22 \times (-20) = 10$, mais $\text{pgcd}(15; 22) \neq 10$.

3.2 Identité de Bézout

Théorème 1 (*théorème de Bézout*)

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 $au + bv = 1$

Démonstration 10

....
....
....
....
....
....
....
....
....

Exercice

n est un entier naturel. Montrer que $a = 3n + 7$ et $b = 2n + 5$ sont premiers entre eux.

....
....
....

Exercice
Soient a, b et c des entiers relatifs. Montrer que si a est premier avec b et c, alors a est premier avec leur produit bc.

. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .

4 Le théorème de Gauss

Théorème 2 (*théorème de Gauss*)

Soient a, b et c trois entiers relatifs non nuls.
Si $a \mid bc$ et a est premier avec b, alors $a \mid c$.

Démonstration 11

. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .

Remarque
L'hypothèse « a et b sont premiers entre eux » est indispensable ! Par exemple, $6 \mid 14 \times 15$ pourtant 6 ne divise ni 14 ni 15.

Propriété 12 (*conséquence du théorème de Gauss*)

Soient a, b et c trois entiers relatifs non nuls. Si les deux entiers a et b divisent c et sont premiers entre eux alors leur produit ab divise c.

Démonstration 12

. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .
. . . .

Remarque
L'hypothèse « a et b sont premiers entre eux » est indispensable ! Par exemple, 60 est divisible par 6 et 4 mais n'est pas divisible par $6 \times 4 = 24$.

5 Équations diophantiennes

Une équation diophantienne est une équation du type $ax + by = c$ d'inconnue le couple $(x; y)$ et où a, b, c sont trois entiers relatifs. Voici trois exemples de résolutions d'équations diophantiennes. Nous nous en servirons comme modèle.

Énoncé 1. Déterminer les entiers x et y tels que $5x = 3y$.

Énoncé 2. Déterminer les entiers x et y tels que $2x + 3y = 1$.

Énoncé 3. Déterminer les entiers x et y tels que $2x + 3y = 5$.