Cours & méthodes

PGCD et théorèmes de Bézout et Gauss

5
ARITHMETIQUE

1 Diviseurs communs et PGCD

1.1 Diviseurs, diviseurs communs d'un entier

Vidéo de cours

Notations 1 : Ensemble des diviseurs

Soit $a \in Z$. On note D_a l'ensemble des diviseurs de a.

Méthode 1 : Déterminer les diviseurs d'un entier

Déterminer l'ensemble des diviseurs de 48.

Correction

Propriété 1 : Propriété de D_a

Pour tout $a \in \mathbb{Z}^*$, D_a est un ensemble fini non vide.

Propriété 2 : Diviseurs communs

L'ensemble des diviseurs communs à deux entiers non nuls est nécessairement fini et non vide.

Méthode 2 : Déterminer les diviseurs communs

Déterminer l'ensemble des diviseurs de 48 et 18.

1.2 PGCD de deux entiers relatifs

Définition 1

Soient a et b deux entiers relatifs dont l'un au moins est non nul.
On appelle plus grand commun diviseur de a et b, et on note PGCD $(a\,;b)$ ou $a \wedge b$, le plus grand élément de l'ensemble des diviseurs communs de a et b.

Notations 2

$$\text{PGCD}(a\,;b) = \max\left(D_a \cap D_b\right)$$

Démonstration

L'ensemble des diviseurs communs à a et b est un ensemble fini car intersection de deux ensembles finis.
De plus 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide.
Tout ensemble fini non vide admet un plus grand élément donc PGCD existe.

Méthode 3 : Déterminer le plus grand commun diviseur de deux entiers

Déterminer le plus grand commun diviseur de 48 et 18.

Correction

Propriété 3 : Propriétés élémentaires du PGCD de deux entiers

Pour tous entiers relatifs a et b non nuls :

$$\text{PGCD}(a\,;b) = \text{PGCD}(|a|\,;|b|), \qquad \text{PGCD}(a\,;b) = \text{PGCD}(b\,;a)$$
$$\text{PGCD}(a\,;1) = 1, \qquad \text{PGCD}(a\,;0) = |a|$$

Vidéo de cours

Propriété 4

Soient a et b deux entiers naturels avec b non nul.
Alors :

a divise b si, et seulement si, $\text{PGCD}(a\,;b) = a$

Démonstration

Méthode 4 : Déterminer les diviseurs communs

Soit un entier $n \geq 2$.
Déterminer $\text{PGCD}\left(n^3 - n, n + 1\right)$

Correction

1.3 Algorithme d'Euclide

Propriété 5 : Lemme d'Euclide

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
Si $a = bq + r$ est la division euclidienne de a par b, alors $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$.

Démonstration

Remarque 1

Le résultat reste vrai si r ne vérifie pas $0 \leqslant r < b$.

Remarque 2

Le lemme d'Euclide est un résultat important car il permet de traiter la plupart des questions au sujet du PGCD. C'est la "pierre angulaire" de la mise en place de l'algorithme d'Euclide.
Nous illustrons cette dernière remarque par les exemples qui suivent.

Exemple 1

Déterminons PGCD(230, 22) :
En effectuant la division de 230 par 22, il vient

$$230 = 22 \times 10 + 10$$

ce qui donne, en appliquant le lemme d'Euclide,

$$\text{PGCD}(230, 22) = \text{PGCD}(22, 10)$$

En réitérant ce lemme pour le PGCD(22, 10), nous obtenons

$$22 = 10 \times 2 + 2, \text{ c'est-à-dire } \text{PGCD}(22, 10) = \text{PGCD}(10, 2).$$

Puisque 2 divise 10 , il vient

$$\text{PGCD}(10, 2) = 2$$

Nous en concluons

$$\text{PGCD}(230, 22) = \text{PGCD}(22, 10) = \text{PGCD}(10, 2) = 2.$$

Cette itération du lemme d'Euclide est un premier exemple qui illustre **l'algorithme d'Euclide**.

Méthode 5 : Algorithme d'Euclide

Soit a et b deux entiers naturels tels que $0 < b \leqslant a$.
L'algorithme d'Euclide permet de calculer en un nombre fini d'étapes le PGCD de a et b : il consiste à remplacer $(a\,;b)$ par des couples de nombres de plus en plus petits qui ont le même PGCD :

1) Calculer le reste r de la division euclidienne de a par b ;

2) Si $r = 0$, alors $\text{PGCD}(a\,;b) = b$, sinon, remplacer a par b et b par r et revenir en 1.

$\text{PGCD}(a\,;b)$ est donc **le dernier reste non nul** dans la liste des restes successifs obtenus par l'algorithme d'Euclide.

Déterminer PGCD (455 ; 312) et PGCD (1542 ; 58).

Correction

Méthode 6 : Algorithme d'Euclide en Python (spécial pour les NSI)

Compléter l'algorithme d'Euclide ci-dessous où a et b sont deux entiers naturels tels que $a > b > 0$.

```
def Euclide(a,b):
  while ... :
    r=...
    a=...
    b=...
  return ...
```

Correction

Méthode 7 : Algorithme d'Euclide niveau Maths Expert !

Soit n un entier relatif. Démontrer que $\text{PGCD}(2n+1 ; n+3) = \begin{cases} 5 & \text{si } n \equiv 2 \ [5] \\ 1 & \text{sinon} \end{cases}$

Correction

Propriété 6

Pour tout entier naturel non nul k, et pour a et b entiers relatifs, $\text{PGCD}(ka ; kb) = k \times \text{PGCD}(a ; b)$.

Méthode 8 : Calcul d'un PGCD Niveau collège !!

Calculer à l'aide du corollaire précédent, PGCD (2400 ; 210).

Méthode 9 : Calcul d'un PGCD niveau Maths Expert !

Soient n et p deux entiers naturels non nuls. Calculer $\text{PGCD}(np, n(2p+1))$

Propriété 7 : Caractérisation du PGCD

Soient a et b deux entiers relatifs non nuls. Quel que soit $d \in \mathbb{N}^*$,

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

si et seulement s'il existe deux entiers relatifs non nuls a' et b', premiers entre eux, tels que

$$a = da' \text{ et } b = db'.$$

Démonstration

Méthode 10 : Équation diophantienne

Résoudre dans $\mathbb{N}^2$:

$$\begin{cases} x + y = 144 \\ \text{PGCD}(x, y) = 18 \end{cases}$$

Correction

1.4 Relation de Bézout

Propriété 8 : Relation de Bézout pour deux entiers

Soit a et b deux entiers relatifs. Il existe deux entiers relatifs u et v tels que

$$\text{PGCD}\,(a\,;b) = au + bv.$$

Démonstration

Remarque 3

- Le couple $(u\,;v)$ n'est pas unique !
  Par exemple $\text{PGCD}\,(4\,;6) = 2$ et on a à la fois $2 = 4 \times (-1) + 6 \times 1$ et $2 = 4 \times 2 + 6 \times (-1)$.
- La réciproque de l'identité de Bézout est fausse : $4 \times 5 - 3 \times 6 = 2$ et pourtant, 2 n'est pas le PGCD de 4 et 3.

Méthode 11 : Détermination de la relation de Bézout

On donne $a = 3080$ et $b = 525$.

a) Déterminer PGCD $(a\,;b)$ avec l'algorithme d'Euclide.

b) En exprimant de proche en proche chaque reste en fonction des restes précédents, déterminer un couple $(u\,;v)$ de nombres entiers relatifs tels que $au + bv = \text{PGCD}\,(a\,;b)$.

c) Reprendre les deux questions précédentes avec $a = 155$ et $b = 55$.

Correction

2 Nombres premiers entre eux et théorème de Bézout

2.1 Nombres premiers entre eux

Définition 2

Soit a et b deux entiers relatifs non nuls. On dit que a et b sont **premiers entre eux** si PGCD $(a\,;b) = 1$.

Méthode 12 : Démontrer que deux entiers sont premiers : Niveau 3ème (programme DNB avant la réforme)

Justifier que 35 et 26 sont premiers entre eux.

Correction

Propriété 9 : Fraction irréductible

Soit a un entier relatif et b un entier relatif non nul.
La fraction $\dfrac{a}{b}$ est irréductible si les entiers a et b sont premiers entre eux.

Méthode 13 : Nombre premiers entre-eux : Niveau Maths Expert !!

a) Démontrer que deux entiers naturels consécutifs sont premiers entre eux.

b) Démontrer que la fraction $\dfrac{2n+1}{3n+2}$ est irréductible pour tout entier naturel n.

Correction

2.2 Théorème de Bézout

Propriété 10 : Théorème de Bézout

Soient 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 $au + bv = 1$.

Méthode 14 : Utilisation du théorème de Bézout.

- On commence par justifier qu'il existe bien un couple d'entiers (u, v) tel que $29u + 12v = 1$.
- On applique l'algorithme d'Euclide pour calculer les restes successifs jusqu'à obtenir le reste égal à 1.
- On utilise les équations obtenues en "remontant" l'algorithme d'Euclide .

Déterminer deux entiers u et v tels que $29u + 12v = 1$

Correction

Méthode 15 : Résolution d'équation dans $\mathbb{Z}$

On dit qu'un entier relatif a admet un inverse modulo n ($n \in \mathbb{N}$ et $n \geqslant 2$)
ou encore qu'il est inversible modulo n lorsqu'il existe un entier relatif b tel que $ab \equiv 1\ [n]$.

a) Justifier que 7 est inversible modulo 23.

b) Résoudre alors dans $\mathbb{Z}$ l'équation $7x \equiv 8\ [23]$.

Correction

Propriété 11 : Théorème de Gauss

Soient a, b et c trois entiers relatifs non nuls.
Si $a \mid bc$ et $\text{PGCD}(a\,;b) = 1$, alors $a \mid c$.

Démonstration

Remarque 4

- Si a et b ne sont pas premiers entre eux, alors le théorème de Gauss est inexact.
  Contre-exemple : Soit : $a = 6, b = 2$ et $c = 9$.
  Nous avons $\text{PGCD}(6, 2) = 3 \neq 1$, donc a et b ne sont pas premiers entre eux. $6 \mid 2 \times 9$ mais 6 ne divise pas 9.
- La réciproque du théorème de Gauss est fausse.
  Contre-exemple : Soit : $a = 5, b = 10$ et $c = 15$. $5 \mid 15$ donc $a \mid c$, on a bien $5 \mid 10 \times 15$ mais $\text{PGCD}(5, 10) \neq 1$

Méthode 16 : Résolution diophantienne

Trouver tous les couples d'entiers naturels $(x\,;y)$ tels que

$$4x - 3y + 9 = 0.$$

Propriété 12

Soient a, b et c trois entiers relatifs non nuls. Si $a \mid c$, $b \mid c$ et $\text{PGCD}(a\,;b) = 1$ alors $ab \mid c$.

Exemple

Pour prouver, qu'un nombre est divisible par 6, il suffit de prouver qu'il est divisible par 2 et par 3.

Méthode 17 : Prouver une divisibilité

Démontrer que, pour tout entier naturel n, $5n^2(n^2+11)$ est divisible par 30.

2.3 Équations diophantienne $ax + by = c$

Définition 3

Soient a, b et c trois entiers relatifs non nuls. Une équation du type $ax + by = c$, où l'inconnue est le couple d'entiers relatifs $(x\,;y)$, est appelée **équation diophantienne linéaire**.

Propriété 13

Soient a, b et c trois entiers relatifs non nuls.
L'équation $ax + by = c$ possède au moins admet au moins un couple solution si, et seulement si, PGCD $(a\,;b)$ divise c.

Méthode 18 : Résolution d'une équation diophantienne

On note (E) l'équation $2x + 5y = 4$ où x et y sont des entiers relatifs.

a) Justifier que (E) admet au moins couple d'entiers relatifs solution.

b) Déterminer un couple $(u\,;v)$ d'entiers relatifs tels que $2u + 5v = 1$.
En déduire un couple $(x_0\,;y_0)$ solution de (E).

Correction

Méthode 19 : Résolution d'une équation diophantienne

Soit (E) l'équation $9x - 14y = 3$ où x et y sont des entiers relatifs.

a) Justifier que le couple $(x_0\,;y_0) = (5\,;3)$ est solution de (E).

b) Démontrer qu'un couple $(x\,;y)$ est solution de (E) si, et seulement si, $9(x - x_0) = 14(y - y_0)$.

c) Résoudre l'équation (E).

Correction