4

PGCD, théorèmes de Bézout et de Gauss

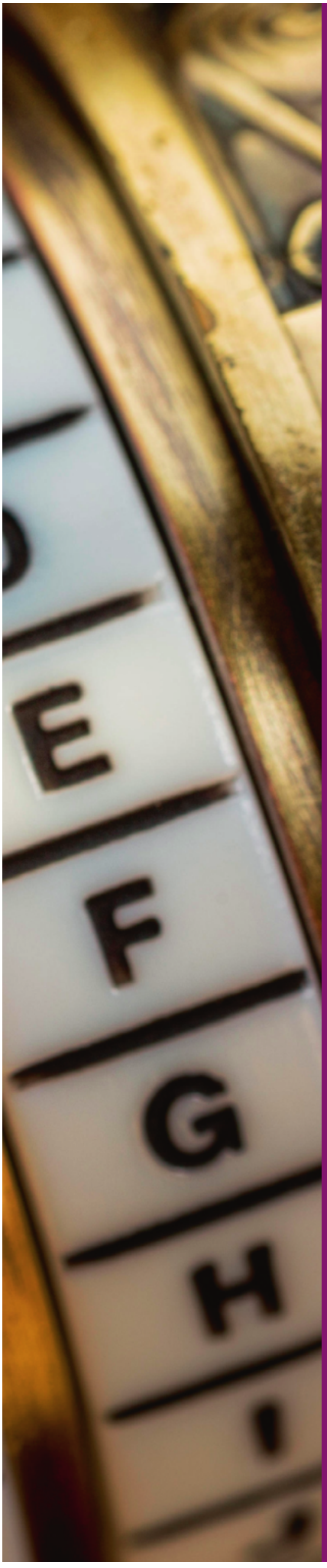
Pour coder un message, César décalait les lettres dans l'alphabet. Pour plus de sécurité, on peut aussi grouper les lettres par lot et appliquer à ces lots une fonction de codage.

Comment chiffrer un message en groupant les lettres par 2 ?

↪ **TP 2** p. 131

VIDÉO

Les codes secrets
lienmini.fr/maths-e04-01



Pour prendre un bon départ

EXOS Prérequis
lienmini.fr/maths-e04-02

Les rendez-vous Sésamath

1 Trouver le plus grand diviseur commun

Déterminer le plus grand diviseur commun des couples d'entiers suivants.

a) 28 et 77 **b)** 96 et 36 **c)** 88 et 132

d) 170 et 65 **e)** 66 et 180

2 Simplifier une fraction

Par quel nombre faut-il diviser numérateur et dénominateur pour obtenir une fraction irréductible des rationnels suivants ?

a) $\frac{26}{65}$ **b)** $\frac{72}{54}$ **c)** $\frac{255}{35}$ **d)** $\frac{693}{55}$

3 Déterminer si des nombres sont premiers entre eux

Deux nombres sont premiers entre eux si leur seul diviseur commun est 1.

Les couples d'entiers suivants sont-ils premiers entre eux ?

a) 9 et 16 **b)** 35 et 91 **c)** 31 et 67 **d)** 26 et 91

4 Diviser par un produit

Les phrases suivantes sont-elles vraies ou fausses ? Justifier

a) Si un entier a est divisible par 6 et 9 alors cet entier a est divisible par 54.

b) Si un entier a est divisible par 8 et 9 alors cet entier a est divisible par 72.

c) Si un entier a est divisible par 4 et 18 alors $a \equiv 0\ (36)$.

d) Si un entier a est divisible par 10 et 15 alors $a \equiv 0\ (150)$.

5 Résoudre une équation

Trouver un couple d'entiers $(x\,;y)$ solution des équations suivantes.

a) $7x - 10y = 1$ **b)** $4x + 5y = 1$

c) $3x + 4y = 3$ **d)** $7x - 12y = 3$

6 Traduire un problème en équation

1. Pierre a des jetons d'une valeur de 3 € et Lilya a des jetons d'une valeur de 7 €. Pierre doit donner 34 € à Lilya.

Comment Pierre et Lilya peuvent-ils procéder ?

2. a) Céline possède des jetons de 3 € et des jetons de 7 € pour une valeur totale de 34 €.

Combien de jetons de chaque sorte possède-t-elle ? Trouver toutes les solutions.

b) En déduire le nombre maximum de rectangles de 3 cm par 7 cm que l'on peut obtenir en découpant une plaques rectangulaire de 21 cm par 34 cm.

Proposer deux dispositions de découpage

7 Comprendre un algorithme en langage Python

Que retourne ce programme pour `f("L")` ?

```
def f(lettre):
    alphabet=["A","B","C","D","E","F","G","H","I","J","K","L",
    "M","N","O","P","Q","R","S","T","U","V","W","X","Y","Z"]
    x=alphabet.index(lettre)
    y=(11*x+8)%26
return alphabet[y]
```

Activités

15 min

1 Trouver le plus grand commun diviseur

A ▸ Méthode archaïque

1. Déterminer l'ensemble D_{84} des diviseurs positifs de 84.

2. Déterminer l'ensemble D_{147} des diviseurs positifs de 147.

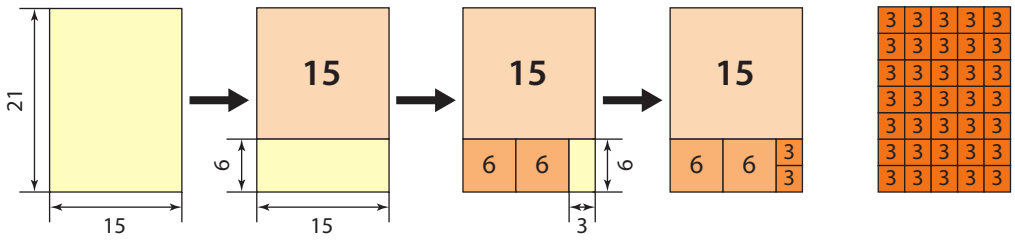
3. Déterminer l'ensemble $D_{84} \cap D_{147}$ des diviseurs communs, ou codiviseurs, de 84 et 147.

4. Cet ensemble admet un plus grand élément appelé plus grand commun diviseur et noté PGCD(84 , 147). Quel est-il ?

5. Utiliser la même procédure pour trouver le plus grand diviseur commun de 255 et 77. Que peut-on dire de 255 et 77 ?

B ▸ Méthode géométrique

On désire déterminer le plus grand commun diviseur par une construction géométrique.
Par exemple, pour PGCD(21 , 15) on propose la construction suivante.



1. Expliquer cette construction du PGCD(21 , 15) du point de vue géométrique.

2. Proposer une construction géométrique pour PGCD(91 , 52).

↪ Cours 1 p. 108

Histoire des maths 15 min

2 Déterminer le PGCD par divisions successives

Le procédé décrit ici était connu des Grecs sous le nom d'**anthyphérèse** (soustraire alternativement) car la division était obtenue par soustractions successives. Il est décrit dans le livre VII des *Éléments d'Euclide*.

Soit d un diviseur commun à 347 et 105.

1. a) Vérifier que le reste dans la division euclidienne de 347 par 105 est 42.

b) Pourquoi si d divise 347 et 105, d divise 105 et 42 ?

2. a) Vérifier que le reste dans la division euclidienne de 105 par 42 est 21.

b) Pourquoi si d divise 105 et 42, d divise 21 ?

3. Donner l'ensemble de tous les diviseurs positifs commun à 347 et 105. Quel est son plus grand élément ?

4. Appliquer cette méthode pour trouver le plus grand diviseur commun à 5 726 et 2 045.

↪ Cours 2 p. 110

50 min

3 Découvrir le chiffrement affine

Le chiffrement ou cryptage consiste à transformer un message en un message codé (ou chiffré).
Le déchiffrement est le procédé inverse, il consiste à décoder un message codé.

A ▸ Procédé de chiffrement

Afin de coder un message, on assimile chaque lettre de l'alphabet à un nombre entier entre 0 et 25 comme l'indique le tableau ci-dessous.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Un chiffrement affine utilise une fonction affine f, par exemple $f(x) = 11x + 8$.
Pour chaque lettre du message :
• on associe un entier x entre 0 et 25 comme indiqué sur le tableau ;
• on calcule $f(x)$ et on détermine le reste y de la division de $f(x)$ par 26 ;
• on traduit ensuite y par une lettre suivant le même tableau ci-dessus.
Codage de la lettre G :

$$\text{G} \longrightarrow 6 \longrightarrow f(6) = 11 \times 6 + 8 = 74 \longrightarrow 74 \equiv 22\ (26) \longrightarrow \text{W}.$$

1. Coder la lettre *W*.

2. Le but de cette question est de déterminer la fonction de décodage f^{-1}.
a) Montrer que pour tous entiers relatifs x et z, on a :

$$11x \equiv z\ (26) \Leftrightarrow x \equiv 19z\ (26).$$

b) En déduire que la fonction f^{-1} de décodage est :

$$f^{-1}(y) = 21y + 11.$$

B ▸ Casser un chiffrement affine

On peut facilement casser un chiffrement affine si l'on connaît la langue dans laquelle il est écrit car une lettre est toujours codée de la même façon.
On a reçu le message : « FMEYSEPGCB ».
Une étude statistique de la fréquence d'apparition des lettres sur un passage plus important, montre que la lettre E est chiffrée en E et que la lettre J est chiffrée en N.
Soit la fonction de chiffrage f définie par :

$$f(x) = ax + b \text{ où } a, b \in [0\,;25].$$

1. Montrer que a et b vérifient le système suivant :

$$\begin{cases} 4a + b \equiv 4\ (26) \\ 9a + b \equiv 13\ (26) \end{cases}$$

2. a) Montrer que : $5a \equiv 9\ (26)$, puis que $a \equiv 7\ (26)$.
b) En déduire que $b \equiv 2\ (26)$ et que f est définie par :

$$f(x) = 7x + 2.$$

c) Démontrer que pour tous entiers relatifs x et z, on a :

$$7x \equiv z\ (26) \Leftrightarrow x \equiv 15z\ (26).$$

d) En déduire que la fonction de décodage f^{-1} est définie par :

$$f^{-1}(y) = 15y + 22.$$

e) Décoder le message.

↪ Cours 3 p. 112 et 4 p. 114

Cours

1 PGCD : plus grand commun diviseur

Définition PGCD

Soit a et b deux entiers relatifs non tous nuls.

L'ensemble des diviseurs communs à a et b admet un plus grand élément d, appelé plus grand commun diviseur.

On le note PGCD(a , b).

Démonstration

Démontrons l'existence et l'unicité du PGCD.

L'ensemble des diviseurs communs à a et b est un ensemble fini car c'est l'intersection de deux ensembles dont l'un au moins est fini (non tous nuls).

1 divise a et b donc l'ensemble des diviseurs communs à a et b n'est pas vide.

Or tout ensemble fini non vide dans $\mathbb{Z}$ admet un plus grand élément, donc d existe.

Exemples

PGCD(24 , 18) = 6
PGCD(60 , 84) = 12
PGCD(150 , 240) = 30

Propriétés Propriétés du PGCD

① PGCD(a , b) = PGCD(b , a)

② PGCD(a , b) = PGCD($|a|$, $|b|$)

③ PGCD(a , 0) = a car 0 est multiple de tout entier.

④ Si b divise a, alors PGCD(a , b) = $|b|$.

⑤ Pour tout entier naturel k non nul, on a : PGCD(ka , kb) = k PGCD(a , b).

Exemples

① PGCD(30 , 75) = PGCD(75 , 30) = 15
② PGCD(– 24 , – 18) = PGCD(24 , 18) = 6
③ PGCD(82 , 0) = 82
④ PGCD(30 , 5) = 5 car 30 est un multiple de 5.
⑤ PGCD(240 , 180) = 10 PGCD(24 , 18) = 60

Définition Nombres premiers entre eux

Soit a, b deux entiers relatifs non tous nuls.

On dit que a et b sont premiers entre eux si, et seulement si, PGCD(a , b) = 1

Exemples

PGCD(15 , 8) = 1 donc 15 et 8 sont premiers entre eux.
PGCD(a , 1) = 1 donc l'entier 1 est premier avec tout entier.

Remarques

• Il ne faut pas confondre nombres premiers entre eux et nombres premiers.
Les nombres 15 et 8 sont premiers entre eux mais ni l'un ni l'autre ne sont premiers.
En revanche, deux nombres premiers sont premiers entre eux.

• Une fraction irréductible q s'écrit comme le rapport de deux entiers premiers entre eux :

$$q = \frac{a}{b} \text{ avec } a \in \mathbb{Z},\ b \in \mathbb{N}^* \text{ et PGCD}(a\ ,\ b) = 1$$

Exercices résolus

Méthode 1 Utiliser la définition et les propriétés du PGCD

Énoncé

1. Déterminer tous les entiers naturels n tels que : PGCD(n , 324) = 12.

2. En déduire parmi eux les entiers naturels n inférieurs à 100.

Solution

1. L'entier 12 divise n et 324. 1

$n = 12k$, $k \in \mathbb{N}$ et $324 = 12 \times 27$.

Le problème revient à résoudre : PGCD(k , 27) = 1. 2

k et $27 = 3^3$ sont premiers entre eux si 3 ne divise pas k. 3

On a donc : $k \equiv 1$ (3) ou $k \equiv 2$ (3). 4

Les valeurs de n qui conviennent sont les multiples de 12 non multiples de $12 \times 3 = 36$.

2. On veut : $n < 100 \Rightarrow 12k < 100 \Rightarrow k \leqslant 8$

k non multiple de 3 : $k \in \{1 , 2 , 4 , 5 , 7 , 8\}$. 5

Les valeurs de n qui conviennent sont : $n \in \{12 , 24 , 48 , 60 , 84 , 96\}$.

Conseils & Méthodes

1 Revenir à la définition du PGCD : diviseur commun.

2 Utiliser la linéarité du PGCD : PGCD(ka , kb) = kPGCD(a , b).

3 Si deux nombres sont premiers entre eux, 1 est leur seul diviseur commun.

4 Traduire la contrainte à l'aide des congruences.

5 Faire la liste des choix possibles pour k puis pour n dans l'intervalle [0 , 100].

À vous de jouer !

1 **1.** Déterminer les entiers naturels n tels que : PGCD(n , 378) = 54.

2. En déduire parmi eux les entiers naturels n inférieurs à 500.

2 **1.** Déterminer les entiers naturels n tels que : PGCD(n , 150) = 6.

2. En déduire parmi eux les entiers naturels n inférieurs à 400.

↪ Exercices 42 à 48 p. 120

Méthode 2 Résoudre un système d'équations

Énoncé

Trouver tous les entiers naturels a et b avec $a < b$ tels que : $ab = 432$ et PGCD(a , b) = 6.

Solution

PGCD(a , b) = 6, on peut alors écrire : $a = 6a'$ et $b = 6b$ avec a' et b' premiers entre eux. 1

On a alors :

$$ab = 432 \Leftrightarrow 6^2 a'b' = 432 \Leftrightarrow a'b' = \frac{432}{6^2} = 12.$$

Les diviseurs de 12 sont : {1 ; 2 , 3 ; 4 ; 6 ; 12}.

Comme 2 et 6 ne sont pas premiers entre eux 2,

les seuls décompositions possibles sont : 1×12 et 3×4.

Les couples solutions sont donc : (1 ; 12) et (3 ; 4).

Conseils & Méthodes

1 a' et b' sont premiers entre eux sinon 6 ne serait pas le plus grand diviseur commun.

2 PGCD(2 , 6) = 2.

À vous de jouer !

3 Trouver tous les entiers naturels a et b avec $a < b$ tels que : $ab = 7\,776$ et PGCD(a , b) = 18.

4 Déterminer les entiers naturels a et b avec $a < b$ tels que : $a + b = 24$ et PGCD(a , b) = 4.

↪ Exercices 42 à 48 p. 120

Cours

2 Algorithme d'Euclide

Théorème **Algorithme d'Euclide**

Soit a et b deux entiers naturels non nuls tels que b ne divise pas a.

La suite des divisions euclidiennes du diviseur par le reste de la division précédente finit par s'arrêter.

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

Division de a par b	$a = bq_0 + r_0$	**avec**	$b > r_0 \geqslant 0$
Division de b par r_0	$b = r_0 q_1 + r_1$	**avec**	$r_0 > r_1 \geqslant 0$
Division de r_0 par r_1	$r_0 = r_1 q_2 + r_2$	**avec**	$r_1 > r_2 \geqslant 0$
⋮	⋮		⋮
Division de r_{n-2} par r_{n-1}	$r_{n-2} = r_{n-1} q_n + r_n$	**avec**	$r_{n-1} > r_n \geqslant 0$
Division de r_{n-1} par r_n	$r_{n-1} = r_n q_{n+1} + 0$	**on a alors : PGCD$(a, b) = r_n$**	

Démonstration

• Montrons que PGCD(a, b) = PGCD(b, r_0) par une double inégalité.

Soit D = PGCD(a, b) et d = PGCD(b, r_0).

D divise a et b alors D divise toute combinaison de a et b donc D divise $a - bq_0 = r_0$.

D divise b et r_0. Par conséquent $D \leqslant d$.

d divise b et r_0, alors d divise toute combinaison de a et r_0 donc d divise $bq_0 + r_0 = a$.

d divise a et b. Par conséquent $d \leqslant D$.

De ces deux inégalités, on déduit que $D = d$ soit PGCD(a, b) = PGCD(b, r_0).

• La suite des restes : $r_0, r_1, r_2, \ldots, r_n$ est une suite strictement décroissante dans $\mathbb{N}$ car :

$$r_0 > r_1 > r_2 > \cdots > r_n.$$

D'après le principe de descente infinie (toute suite strictement décroissante dans $\mathbb{N}$ est finie), il existe n tel que $r_{n+1} = 0$.

• De proche en proche, on en déduit que :

PGCD(a, b) = PGCD(b, r_0) = … = PGCD(r_{n-2}, r_{n-1}) = PGCD(r_{n-1}, r_n).

Or r_n divise r_{n-1}, donc PGCD$(r_{n-1}, r_n) = r_n$.

• Conclusion : PGCD$(a, b) = r_n$.

Le dernier reste non nul est le PGCD.

Remarques

• Cette démonstration est celle qu'utilisait Euclide, aux notations près, au III^e^ siècle av. J.-C.

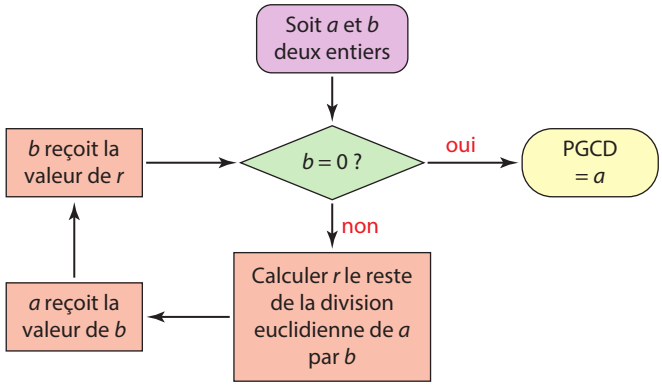
• Bien retenir que pour montrer que deux PGCD sont égaux, il est souvent préférable de procéder par double inégalités.

• Le petit nombre d'étapes pour trouver le PGCD fait de cet algorithme un procédé plus efficace que la décomposition en nombres premiers (chapitre 5).

• L'algorithme d'Euclide peut être présenté sous la forme d'un organigramme (ci-contre).

On pose la question « est-ce que $b = 0$? ». Si oui, le PGCD est égal à a. Si non, on part dans la boucle « non ».

On revient à la question avec les nouvelles valeurs de a et b.



Exercices résolus

Méthode 3 Appliquer l'algorithme d'Euclide

Algo

Énoncé

1. À l'aide de l'algorithme d'Euclide, déterminer PGCD(1 958 , 4 539).

2. Déterminer une fonction en Python calculant le PGCD de deux entiers à l'aide de l'algorithme d'Euclide. Vérifier le résultat trouvé à la question 1.

Solution

1. $4\,539 = 1\,958 \times 2 + 623$ 1

$1\,958 = 623 \times 3 + 89$ 2

$623 = 89 \times 7 + 0$

On obtient alors : PGCD(1 958 , 4 539) = 89 3

Remarque
Si l'on avait divisé le plus petit par le plus grand, cela aurait rajouté la ligne : $1\,958 = 4\,539 \times 0 + 1\,958$. Ensuite, on divise 4 539 par 1 958 retrouvant ainsi les divisions effectuées.

2. On crée la fonction **`pgcd(a,b)`** en initialisant le reste.

Par une boucle conditionnelle, tant que le reste est non nul, on divise.
On remarquera qu'à chaque étape, on réactualise les valeurs de a et b.

On obtient alors :

```
def pgcd(a,b):
    r=a%b 4
    while r!=0: 5
        a=b
        b=r
        r=a%b
    return b
```

```
>>> pgcd(4539 , 1958)
89
```

Conseils & Méthodes

1 Diviser le plus grand nombre par le plus petit.

2 Diviser ensuite le diviseur par le reste jusqu'à obtenir un reste nul.

3 Le dernier reste non nul est le PGCD.

4 a % b signifie le reste de la division de a par b.

5 $r!=0$ signifie $r \neq 0$

À vous de jouer !

5 À l'aide de l'algorithme d'Euclide, déterminer les PGCD des couples d'entiers suivants.
a) (144 ; 840) **b)** (202 ; 138)

6 À l'aide de l'algorithme d'Euclide, déterminer les PGCD des couples d'entiers suivants.
a) (441 ; 777) **b)** (2 004 ; 9 185)

7 À l'aide de l'algorithme d'Euclide, dire si les couples d'entiers suivants sont premiers entre eux.
a) (4 847 ; 5 633) **b)** (5 617 ; 813)

8 **1.** À l'aide de l'algorithme d'Euclide, déterminer PGCD(a , b) avec $a = 18\,440$ et $b = 9\,828$.
2. Que peut-on dire des nombres $\frac{a}{84}$ et $\frac{b}{84}$?

9 Écrire un programme en langage naturel permettant de calculer le PGCD(a , b) avec l'algorithme d'Euclide.
Tester ce programme avec $a = 1\,958$ et $b = 4\,539$ puis avec $a = 123\,456\,789$ et $b = 987\,654\,321$.

10 Compléter le programme en **Python** ci-dessous pour que la fonction récursive **`euclide`** donne le PGCD (a , b).

```
def euclide(a,b):
    if b==0:
        return …
    return euclide(… , …)
```

Tester ce programme avec $a = 1\,958$ et $b = 4\,539$ puis avec $a = 123\,456\,789$ et $b = 987\,654\,321$.

↪ Exercices 49 à 53 p. 120

Cours

3 Théorème de Bézout et son corollaire

Théorème Identité de Bézout

Soit deux entiers non nuls a et b tels que PGCD(a , b) = D.
Il existe un couple d'entiers relatifs (u ; v) tel que :

$$au + bv = D.$$

Démonstration

Soit G l'ensemble des combinaisons linéaires strictement positives de a et de b.

G n'est pas vide car il contient par exemple $|a|$.

D'après le principe du bon ordre, cet ensemble admet un plus petit élément $d = au + bv$ avec $d > 0$.

Notons D = PGCD(a , b) et montrons que $D = d$ par double inégalité.

- D divise a et b donc D divise toute combinaison linéaire de a et b donc D divise $au + bv = d$.

En conséquence $D \leqslant d$.

- Divisons a par d : $a = dq + r$ avec $0 \leqslant r < d$.

Isolons r et remplaçons d par $au + bv$:

$r = a - dq = a - (au + bv)q = a - auq - bvq = a(1 - uq) + b(-vq)$.

Si $r \neq 0$ alors r est un élément de G des combinaisons linéaires strictement positives. Comme d est le plus petit élément, on a alors $r \geqslant d$, ce qui est impossible car $r < d$.

Par conséquent $r = 0$ et donc d divise a.

- Par un raisonnement analogue, on montre que d divise b.
- d divise a et b donc $d \leqslant D$.
- Par double inégalité, on en déduit que $D = d$ et donc que $au + bv = D$.

VIDÉO
Démonstration
lienmini.fr/maths-e04-04
ØLJEN Les maths en finesse

Théorème Conséquence de l'identité de Bézout

Tout diviseur commun à a et b divise PGCD(a , b).

Démonstration

Soit d un diviseur commun à a et b, il existe donc $k, k' \in \mathbb{Z}$ tels que : $a = kd$ et $b = k'd$.
De l'identité de Bézout, on a :

$$au + bv = D \Leftrightarrow kdu + k'dv = D \Leftrightarrow d(ku + k'v) = D ;$$

d divise donc D = PGCD(a , b).

Théorème Théorème de Bézout

Les entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe un couple d'entier relatifs (u ; v) tels que : $au + bv = 1$.

Démonstration

Démontrons par double implications.

- Si PGCD(a , b) = 1, d'après l'identité de Bézout, il existe un couple d'entiers relatifs (u , v) tels que $au + bv = 1$.
- Réciproquement si $au + bv = 1$ alors si D = PGCD(a , b), D divise toute combinaison linéaire de a et de b donc D divise $au + bv$ donc D divise 1 et donc $D = 1$.

Théorème Corollaire du théorème de Bézout

L'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple du PGCD(a , b).

Démonstration

↪ **Exercice 66** p. 121

Méthode 4 Déterminer un couple d'entiers de Bézout

Énoncé

1. Montrer que les entiers 59 et 27 sont premiers entre eux.

2. Déterminer un couple d'entiers relatifs $(x\,;y)$ tel que : $59x + 27y = 1$. On parle d'un couple d'entiers de Bézout.

3. Montrer que pour tout entier relatif n, les entiers $(2n + 1)$ et $(3n + 2)$ sont premiers entre eux.

Solution

1. $59 = 27 \times 2 + 5 \quad (L_1)$ 1

$27 = 5 \times 5 + 2 \quad (L_2)$

$5 = 2 \times 2 + 1 \quad (L_3)$

Le dernier reste est 1 donc PGCD(59 , 27) = 1.

2. On remonte l'algorithme d'Euclide : 2

de (L_3) : $2 \times 2 = 5 - 1 \quad (L_4)$

de $(L_2) \times 2$ $27 \times 2 = 5 \times 10 + 2 \times 2$ 3

de (L_4) $27 \times 2 = 5 \times 10 + 5 - 1$

$27 \times 2 = 5 \times 11 - 1$

$5 \times 11 = 27 \times 2 + 1 \quad (L_5)$ 4

de $(L_1) \times 11$ $59 \times 11 = 27 \times 22 + 5 \times 11$

de (L_5) $59 \times 11 = 27 \times 22 + 27 \times 2 + 1$

$59 \times 11 = 27 \times 24 + 1$

On obtient alors : $59 \times 11 + 27 \times (-24) = 1$ 6

Un couple d'entiers de Bézout est $(11\,, -24)$

3. On cherche une combinaison linéaire de $(2n + 1)$ et $(3n + 2)$ égale à 1 : 7

$$-3(2n + 1) + 2(3n + 2) = -6n - 3 + 6n + 4 = 1$$

Il existe donc un couple $(u\,, v) = (-3, 2)$ tel que $(2n + 1)u + (3n + 2)v = 1$, d'après le théorème de Bézout, pour tout n les nombre $(2n + 1)$ et $(3n + 2)$ sont premiers entre eux.

Conseils & Méthodes

1. Pour montrer que deux nombres sont premiers entre eux, utiliser l'algorithme d'Euclide.
2. On reprend l'algorithme d'Euclide en partant de la ligne (L_3) jusqu'à la ligne (L_1).
3. Pour utiliser $2 \times 2 = 5 - 1$ il faut multiplier (L_2) par 2.
4. On isole 5×11 pour pouvoir utiliser (L_1).
5. On multiplie ensuite (L_1) par 11.
6. Réorganiser l'égalité pour trouver un couple d'entiers de Bézout.
7. Les coefficients doivent permettre « d'éliminer n ».

À vous de jouer !

11 **1.** Montrer que 87 et 31 sont premiers entre eux à l'aide de l'algorithme d'Euclide.

2. En remontant cet algorithme, déterminer un couple d'entiers relatifs $(x\,;y)$ tel que :

$$87x + 31y = 1.$$

12 **1.** Montrer que 38 et 45 sont premiers entre eux à l'aide de l'algorithme d'Euclide.

2. En remontant cet algorithme, déterminer un couple d'entiers relatifs $(x\,;y)$ tel que : $38x + 45y = 1$.

13 **1.** Montrer que deux entiers naturels consécutifs sont premiers entre eux.

2. Montrer que deux entiers naturels impairs consécutifs sont premiers entre eux.

14 **1.** Montrer que 41 et 25 sont premiers entre eux à l'aide de l'algorithme d'Euclide

2. En remontant cet algorithme, déterminer un couple d'entiers relatifs $(x\,;y)$ tel que :

$$41x - 25y = 1.$$

15 Montrer que la fraction $\dfrac{9n+1}{6n+1}$ est irréductible pour tout entier naturel n.

16 Montrer que la fraction $\dfrac{14n+3}{5n+1}$ est irréductible pour tout entier naturel n.

↪ Exercices 54 à 67 p. 120

Cours

4 Théorème de Gauss et son corollaire

Théorème **Théorème de Gauss**

Soit a, b et c trois entiers relatifs non nuls.

Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration

Démontrons à l'aide du théorème de Bézout.

- a divise bc donc il existe un entier relatif k tel que : $bc = ka$. (Éq. 1)
- a et b sont premiers entre eux donc d'après le théorème de Bézout, il existe un couple d'entiers relatifs $(u\,;v)$ tel que : $au + bv = 1$. (Éq. 2)
- (Éq. 2) $\times c$: $acu + bcv = c \overset{\text{(Éq. 1)}}{\Rightarrow} acu + kav = c \Rightarrow a(cu + kv) = 1$

  Donc a divise c.

Théorème **Corollaire du théorème de Gauss**

Soit a, b et c trois entiers relatifs non nuls.

Si b et c divise a et si b et c sont premiers entre eux, alors bc divise a.

Démonstration

Si b et c divise a, alors il existe deux entiers relatifs k et k' tels que : $a = kb$ et $a = k'c$.

On a alors $kb = k'c$ donc b divise $k'c$ comme b et c sont premiers entre eux, d'après le théorème de Gauss, b divise k'. Il existe alors un entier relatif k'' tel que $k' = k''b$.

Or $a = k'c$ donc $a = k''bc$ et donc bc divise a.

5 Équations diophantiennes

Définition **Équation diophantienne**

Une équation diophantienne est une équation polynomiale à coefficients entiers dont on cherche les solutions parmi les nombres entiers.

Une équation diophantienne du premier degré est une équation qui peut se mettre sous la forme :

$$ax + by = c.$$

D'après le corollaire du théorème de Bézout, une telle équation admet des solutions si c est un multiple de PGCD(a , b).

Une solution particulière et le théorème de Gauss permettent alors de trouver toutes les solutions de cette équation du premier degré.

Remarque

Ce type d'équation doit son nom à Diophante d'Alexandrie, mathématicien grec du III^e^ siècle.

Exemples

L'équation $17x - 33y = 2$ admet des solutions entières car 17 et 33 sont premiers entre eux et 2 est un mutiple de 1. Une solution particulière est (4 ; 2) car : $17 \times 4 - 33 \times 2 = 68 - 66 = 3$. Pour donner toutes les solutions ↪ Méthode 7 p. 116.

L'équation $15x + 27y = 2$ n'admet pas de solutions entières car PGCD(15 , 27) = 3 et 2 n'est pas un multiple de 3.

Exercices résolus

Méthode 5 Appliquer le théorème de Gauss

Énoncé

1. Trouver tous les couples d'entiers relatifs $(x\,;y)$ tels que : $5(x-1)=7y$.

2. En déduire les couples d'entiers relatifs $(x\,;y)$ tels que : $5x+7y=5$.

Solution

1. $5(x-1)=7y$ donc 7 divise $5(x-1)$.

Comme 7 et 5 sont premiers entre eux, d'après le théorème de Gauss, 7 divise $(x-1)$. 1

On a alors : $x-1=7k$ avec $k\in\mathbb{Z}$.

En remplaçant dans l'équation : $5\times 7k=7y$. 2

En divisant par 7 : $y=5k$.

Les solutions sont donc de la forme :

$$\begin{cases} x=1+7k \\ y=5k \end{cases}, k\in\mathbb{Z}$$

Les solutions trouvées sont bien solution de l'équation :

$5(1+7k-1)=7(5k)$. 3

2. $5x+7y=5 \Leftrightarrow 5x-5=-7y \Leftrightarrow 5(x-1)=7(-y)$

Il suffit alors de remplacer y par $(-y)$ dans les solutions précédentes :

$$\begin{cases} x=1+7k \\ y=-5k \end{cases}, k\in\mathbb{Z}$$

Conseils & Méthodes

1 Penser à utiliser le théorème de Gauss lorsque $ab=cd$ avec a et b premiers entre eux.

2 Il est indispensable de remplacer dans l'équation pour montrer qu'il s'agit du même k dans $y=5k$.

3 Comme on a raisonné par implication, il faut vérifier que les solutions trouvées sont bien solution de l'équation.

À vous de jouer !

17 **1.** Déterminer les couples d'entiers relatifs $(x\,;y)$ tels que : $33x-45y=0$.
2. En déduire les couples d'entiers relatifs $(x\,;y)$ tels que : $33x+45y=12$.

18 **1.** Déterminer les couples d'entiers relatifs $(x\,;y)$ tels que : $7(x-3)=5(y-2)$.
2. En déduire les entiers relatifs x tels que : $7x\equiv 1\ (5)$.

↪ Exercices 68 à 70 p. 121

Méthode 6 Appliquer le corollaire du théorème de Gauss

Énoncé

Soit x un entier relatif

Montrer que si $x\equiv 0\ (8)$ et $x\equiv 0\ (9)$, alors $x\equiv 0\ (72)$.

Solution

Si $x\equiv 0\ (8)$ et $x\equiv 0\ (9)$ alors 8 et 9 divise x. 1

Comme 8 et 9 sont premiers entre eux, d'après le corollaire du théorème de Gauss,

$8\times 9=72$ divise x donc $x\equiv 0\ (72)$.

Conseils & Méthodes

1 Traduire les congruences en termes de divisibilité pour pouvoir utiliser le théorème de Gauss.

À vous de jouer !

19 Montrer que si $x\equiv 0\ (3)$, $x\equiv 0\ (5)$ et $x\equiv 0\ (7)$ alors $x\equiv 0\ (105)$.

20 Soit n un entier naturel.
Montrer que $n(n+1)(n+2)$ est divisible par 6.

↪ Exercices 68 à 70 p. 121

Exercices résolus

EXOS Méthodes lienmini.fr/maths-e04-03 — Les rendez-vous Sésamath

Méthode 7 Résoudre une équation diophantienne

↪ Cours 5 p. 114

Énoncé

Soit l'équation (E) à valeurs dans $\mathbb{Z}$: $17x - 33y = 1$.

1. Démontrer que cette équation admet des solutions.

2. Déterminer une solution particulière de l'équation (E).

3. En utilisant le principe de superposition, déterminer l'ensemble des solutions de (E).

Solution

1. 17 et 33 sont premiers entre eux, donc d'après le théorème de Bézout, il existe un couple d'entiers relatifs $(x\,;y)$ tel que : $17x - 33y = 1$. 1

2. Le couple (2 ; 1) est solution de (E) car :

$$17 \times 2 - 33 \times 1 = 34 - 33 = 1.$$

3. Soit $(x\,;y)$ une solution quelconque de l'équation (E).

Comme le couple (2 ; 1) est aussi solution de (E), on a :

$17x - 33y = 17 \times 2 - 33 \times 1 \Leftrightarrow 17(x-2) = 33(y-1)$ (E').

33 divise $17(x-1)$, or 33 et 17 sont premiers entre eux, donc d'après le théorème de Gauss, 33 divise $(x-2)$. 2

Donc $x - 2 = 33k$ avec $k \in \mathbb{Z}$.

En remplaçant dans (E'), on a : $17 \times 33k = 33(y-1)$.

En divisant par 33, on a : $y - 1 = 17k$.

L'ensemble des couples solutions sont de la forme :

$$\begin{cases} x - 2 = 33k \\ y - 1 = 17k \end{cases} \Leftrightarrow \begin{cases} x = 2 + 33k \\ y = 1 + 17k \end{cases}, k \in \mathbb{Z}$$

Ces couples solutions vérifient l'équation (E) : 3

$$17(2 + 33k) - 33(1 + 17k) = 34 + 17 \times 33k - 33 + 33 \times 17k = 1.$$

Ces couples sont bien l'ensemble des solutions de (E).

Conseils & Méthodes

1 Penser au théorème de Bézout ou à son corollaire.

2 Utiliser le théorème de Gauss, pour sélectionner des solutions.

3 Vérifier que les solutions trouvées sont bien solution de l'équation.

À vous de jouer !

21 Soit l'équation

$$(E) : 4x + 3y = 2.$$

1. Dire pourquoi l'équation (E) admet des solutions entières.
2. Déterminer une solution particulière de (E).
3. Déterminer l'ensemble des couples d'entiers relatifs solutions de (E).

22 Soit l'équation

$$(E) : 15x + 8y = 5.$$

1. Déterminer une solution particulière de l'équation : $15x + 8y = 1$.
2. En déduire une solution particulière de (E).
3. Déterminer l'ensemble des couples d'entiers relatifs solutions de (E).

23 Soit l'équation

$$(E) : 51x - 26y = 1.$$

1. Dire pourquoi l'équation (E) admet des solutions entières.
2. Déterminer une solution particulière de (E).
3. Déterminer l'ensemble des couples d'entiers relatifs solutions de (E).

24 Soit l'équation

$$(E) : 29x - 13y = 6.$$

1. Dire pourquoi l'équation (E) admet des solutions entières.
2. Déterminer une solution particulière de (E).
3. Déterminer l'ensemble des couples d'entiers relatifs solutions de (E).

↪ Exercices 71 à 76 p. 121

Exercices résolus

Méthode 8 Montrer la rationalité d'un nombre

Cours 1 p. 108 et 2 p. 110

Énoncé

On considère le polynôme du second degré :

$$P(x) = x^2 + ax + b \text{ où } a, b \in \mathbb{Z}.$$

1. Montrer que si $P(x) = 0$ admet une solution rationnelle α, alors α est entier.

2. En déduire que $\sqrt{n}$, avec $n \in \mathbb{N}$, est soit un entier soit un irrationnel.

Solution

1. Supposons qu'il existe une solution α rationnelle à l'équation $P(x) = 0$. On pose $\alpha = \frac{p}{q}$ irréductible. 1

On a donc :

$$\left(\frac{p}{q}\right)^2 + a\left(\frac{p}{q}\right) + b = 0 \overset{\times q^2}{\Leftrightarrow} p^2 + apq + bq^2 = 0.$$

On isole p^2 : $p^2 = q(-ap - bq)$.

q divise p^2, or q et p sont premier entre eux donc, d'après le théorème de Gauss, q divise 1.

Comme $q \in \mathbb{N}^*$, on a $q = 1$.

Conclusion : si α est rationnel alors α est entier. 2

2. En prenant $a = 0$ et $b = n$, on a :

$$P(x) = x^2 - n \quad 3$$

$\sqrt{n}$ est une solution de $P(x) = 0$.

D'après la question 1, $\sqrt{n}$ est soit un entier soit un irrationnel. 4

Remarque

On a ainsi montré que $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, ... ainsi que les combinaisons avec des rationnels comme le nombre d'or $\frac{1+\sqrt{5}}{2}$ sont des irrationnels.

Conseils & Méthodes

1. Un nombre rationnel est un nombre qui peut s'écrire sous la forme $\frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $PGCD(p, q) = 1$.
2. Si $q = 1$ alors $\frac{p}{q}$ est un entier.
3. On cherche un polynôme où $\sqrt{n}$ est une racine.
4. Un nombre qui n'est pas un rationnel est un irrationnel.

À vous de jouer !

25 On considère le polynôme :

$$P(x) = x^3 + ax^2 + bx + c$$

où $a, b, c \in \mathbb{Z}$.

1. Montrer que si $P(x) = 0$ admet une solution rationnelle α, alors α est un entier.

2. En déduire que $\sqrt[3]{n}$, avec $n \in \mathbb{Z}$, est soit un entier soit un irrationnel.

26 **1.** Montrer que $\frac{\ln 2}{\ln 3} > 0$.

2. On suppose $\frac{\ln 2}{\ln 3} = \frac{p}{q}$ avec PGCD $(p, q) = 1$ et $p, q \in \mathbb{N}^*$.

Montrer alors que $2^q = 3^p$.

3. En déduire que $\frac{\ln 2}{\ln 3}$ n'est pas un nombre rationnel.

27 On pose $\alpha = \sqrt{2} + \sqrt{3}$.

1. Calculer α^2 puis $(\alpha^2 - 5)^2$.

2. Déterminer un polynôme du quatrième degré pour lequel α est une racine.

3. Prouver que α est irrationnel.

28 On considère le polynôme $P(x) = x^3 + x^2 - 2x - 1$.

On suppose que le polynôme P admet une racine rationnelle $r = \frac{p}{q}$ avec PGCD $(p, q) = 1$, $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.

1. Justifier que p divise q^3 puis que p divise q. En déduire que $p = \pm 1$.

2. Par un procédé identique, montrer que $q = 1$.

3. En déduire alors que le polynôme P n'admet pas de solution rationnelle.

Exercices 86 à 87 p. 122

Exercices apprendre à démontrer

VIDÉO
Démonstration
lienmini.fr/maths-e04-04

ØLJEN
Les maths en finesse

Le théorème à démontrer Identité de Bézout

Soit deux entiers non nuls a et b tels que PGCD(a , b) = D.
Il existe un couple d'entiers relatifs (u ; v) tel que : $au + bv = D$.

On montrera à l'aide de l'ensemble des combinaisons linéaires positives de a et b, que D est son plus petit élément.

Comprendre avant de rédiger

- PGCD(6 , 9) = 3, il existe un couple (u ; v) = (2 ; – 1) car $6 \times 2 + 9 \times (-1) = 3$.
Ce couple n'est pas unique car (– 1 , 1) donne aussi $6 \times (-1) + 9 \times 1 = 3$.
- Pour montrer que deux nombres x et y sont égaux, on peut procéder par double inégalité : $x \leqslant y$ et $y \leqslant x$.
- Pour montrer que x divise y, on effectue la division euclidienne de x par y et l'on montre que le reste est nul.

Rédiger

Étape 1
On crée l'ensemble des combinaisons linéaire de a et de b strictement positives.

Étape 2
Toute partie de $\mathbb{N}$ admet un plus petit élément.

Étape 3
D = PGCD(a , b)
D divise a et b donc divise toute combinaison linéaire de a et de b.

Étape 4
On divise a par d.

Étape 5
On exprime r comme une combinaison linéaire de a et de b

Étape 6
On montre que r est nul par impossibilité qu'il soit strictement positif.

Étape 7
d est un diviseur commun à a et b.

La démonstration rédigée

G = $\{ax + by , ax + by > 0\}$
$|a| \in$ G car $a \in$ G ou $-a \in$ G.

Soit d le plus petit élément de G,
il correspond à la combinaison : $d = au + bv$.

D divise d donc $D \leqslant d$.

$a = dq + r \Rightarrow r = a - dq$ avec $0 \leqslant r < d$.

$r = a - q\,(au + bv) = a(1 - qu) + (-bq)v$.

Si $r \neq 0$ alors $r \in$ G et donc d n'est pas le plus petit élément ce qui est contradictoire.
D'où $r = 0$ et donc d divise a.
Par un raisonnement similaire, on déduit que d divise b.

d divise a et b donc $d \leqslant D$

$D \leqslant d$ et $d \leqslant D$ donc $D = d$.

Pour s'entraîner

Soit a et b deux entiers realatifs non nuls. On pose A = $4a + 3b$ et B = $5a + 4b$.
Montrer que : PGCD(a , b) = PGCD(A , B).