Chapitre 3

Nombres premiers entre eux

I Exercices

3.1 Chiffrement affine

Exercice 3.1

Le chiffrement affine est une méthode pour écrire un message codé.

- On associe un nombre x à chaque lettre de l'alphabet comme l'indique le tableau de la figure 3.1 ;
- on choisit deux entiers naturels a et b comme clef ;
- on détermine y tel que $ax + b \equiv y\ [26]$;
- enfin on associe une lettre à y d'après le tableau de la figure 3.1.

1. On choisit $a = 15$ et $b = 6$.

a) Coder le mot `MOT`.

b) Décoder le mot `KPO`.

2. On choisit $a = 21$ et $b = 4$. Améliorons le procédé de décodage.

a) Démontrer que $21x + 4 \equiv y\ [26] \iff x \equiv 5y + 6\ [26]$
Indication : déterminer d'abord le reste de la division euclidienne de 5×21 par 26.

b) Décoder le mot `UMPK`.

3. On choisit $a = 2$ et $b = 3$. Dans ce cas, on obtient un mauvais système de codage parce que deux lettres différentes peuvent être codées par la même lettre. Par exemple, déterminer les deux lettres dont le codage donne la lettre H.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fig. 3.1

Remarques

L'exercice 3.1 est une première approche du chiffrement affine et nous y reviendrons ultérieurement.

La 3e question de cet exercice montre que pour certains choix de a et de b, on obtient un système de chiffrement non satisfaisant, mais alors, les deux choix précédents de a et de b donnent-ils des systèmes de chiffrement satisfaisants ? La réponse est oui, mais nous ne l'avons pas démontré, comme nous n'avons pas démontré pourquoi le système de chiffrement de la 3e question est incorrect.

Pour étudier la validité d'un sytème de chiffrement affine, nous devons d'abord revoir le PGCD et les nombres premiers entre eux, étudiés en troisième, puis étudier deux théorèmes importants en arithmétique : le théorème de Bézout et le théorème de Gauss.

3.2 PGCD

Exercice 3.2

1. Écrire la liste des diviseurs de 18, et la liste des diviseurs de 66.
2. Écrire la liste des diviseurs communs à 18 et à 66.
3. Quel est le PGCD de 18 et 66, c'est à dire leur plus grand diviseur commun ?
4. Écrire la liste des diviseurs du PGCD. Que constate-t-on ?
5. Retrouver le PGCD de 18 et 66 en effectuant l'algorithme d'Euclide. Pour se remémorer cet algorithme, on pourra lire l'exemple du paragraphe 3.1.a du cours.

Exercice 3.3

Déterminer chaque fois le PGCD des deux nombres indiqués en détaillant l'algorithme d'Euclide.

1. 204 et 84 **2.** 777 et 357 **3.** 69 696 et 9 339

3.3 PGCD et Identité de Bézout

Lire dans le cours la propriété 3.3 (Identité de Bézout), puis faire l'exercice ci-dessous.

Exercice 3.4

Le PGCD de 10 et 6 est 2. D'après l'identité de Bézout, il existe deux entiers u et v tels que $10 \times u + 6 \times v = 2$. Déterminer deux nombres u et v qui vérifient cette égalité.

Exercice 3.5

1. Vérifier l'égalité $10 \times 3 + 7 \times (-4) = 2$.
2. Le PGCD de 10 et 7 est-il égal à 2 ?
3. Que signifie cet exemple pour la propriété 3.3 du cours (Identité de Bézout) ?

Exercice 3.6

Le PGCD de 306 et 90 est 18, et l'algorithme d'Euclide est détaillé ci-dessous.

$$\begin{array}{rcrcrcl} 306 & = & 90 & \times & 3 & + & 36 \quad (1) \\ 90 & = & 36 & \times & 2 & + & 18 \quad (2) \\ 36 & = & 18 & \times & 2 & + & 0 \quad (3) \end{array}$$

On peut déterminer u et v tels que $306\,u + 90\,v = 18$ à l'aide de l'algorithme d'Euclide.

1. D'après la ligne (2), écrire 18 comme combinaison linéaire de 54 et de 36 :

   $18 =$ .....

2. D'après la ligne (1), écrire 36 comme combinaison linéaire de 198 et 54 :

   $36 =$ .....

3. Dans la combinaison linéaire du **1.** ci-dessus, remplacer 36 par la combinaison linéaire du **2.** ci-dessus.

   $18 =$ .....

   $18 =$ .....

   $18 =$ .....

Exercice 3.7

1. Déterminer d le PGCD de 240 et 56 avec l'algorithme d'Euclide.
2. Déterminer deux entiers u et v tels que $128\,u + 56\,v = d$.

Exercice 3.8

1. Déterminer d le PGCD de 532 et 434 avec l'algorithme d'Euclide.
2. Déterminer deux entiers u et v tels que $532\,u + 434\,v = d$.

Exercice 3.9

Dans chaque cas, déterminer une solution de l'équation.

1. $6x \equiv 2\ [8]$ **2.** $15x \equiv 5\ [35]$ **3.** $30x \equiv 10\ [50]$

3.4 Nombres premiers entre eux

3.4.a Théorème de Bézout

Lire dans le cours la définition 3.3. (Nombres premiers entre eux) et la propriété 3.8 (Théorème de Bézout) puis faire l'exercice ci-dessous.

Exercice 3.10

1. Justifier que les nombres 131 et 21 sont premiers entre eux avec l'algorithme d'Euclide.
2. Déterminer deux entiers u et v tels que $131\,u + 21\,v = 1$.

Exercice 3.11

1. Calculer $5 \times 45 - 16 \times 14$.
2. En déduire 4 paires de nombres premiers entre eux.

3.4.b Théorème de Gauss

Exercice 3.12

1. Déterminer un entier non nul x tel que 6 divise $15x$ et 6 ne divise pas x.
2. Déterminer un entier non nul x tel que 6 divise $11x$ et 6 ne divise pas x.
3. Un des deux problèmes ci-dessus n'a pas de solution. L'explication est donnée par la propriété 3.9 (théorème de Gauss).

3.4.c Équations diophantiennes

Les couples solutions $(x\ ;\ y)$ des équations qui suivent doivent être des couples de nombres entiers.

Exercice 3.13

1. Sans justifier, indiquer si les entiers 7 et 10 sont premiers entre eux.
2. Résoudre l'équation $7x = 10y$, c'est à dire déterminer tous les couples d'entiers $(x\ ;\ y)$ solutions de cette équation.

Exercice 3.14

Résoudre l'équation $7(x-1) = 10(y+2)$, c'est à dire déterminer tous les couples d'entiers $(x\ ;\ y)$ solutions de cette équation.

Exercice 3.15

1. Justifier pourquoi l'équation $7x + 10y = 1$ a des solutions.
2. Résoudre l'équation $7x + 10y = 1$.
   Indications :
   - Déterminer un couple solution $(x_0\ ;\ y_0)$ de cette équation.
   - Justifier qu'on peut alors écrire l'équation de départ sous la forme $7(x-x_0)+10(y-y_0) = 0$, puis sous la forme $7(x-x_0) = -10(y-y_0)$.
   - Achever la résolution de l'équation.

Exercice 3.16

Résoudre les équations diophantiennes ci-dessous.

1. $8x - 5y = 1$ **2.** $3x + 11y = 1$ **3.** $9x - 7y = 1$

Exercice 3.17

1. Donner sans justifier le PGCD de 6 et de 9.
2. L'équation $6x + 9y = 1$ a-t-elle des solutions ? Justifier.

Exercice 3.18

Le but de cet exercice est de résoudre l'équation diophantienne $11x - 8y = 7$.

1. Déterminer un couple $(u\ ;\ v)$ solution de l'équation $11u - 8v = 1$.
2. En déduire un un couple $(x\ ;\ y)$ solution de $11x - 8y = 7$.
3. Résoudre l'équation $11x - 8y = 7$.

Exercice 3.19

Résoudre les équations diophantiennes ci-dessous.

1. $10x - 3y = 4$ **2.** $13x + 6y = 5$

3.4.d Conséquence du théorème de Gauss

Exercice 3.20

1. Déterminer un entier non nul x tel que 4 et 10 divisent x et 4×10 ne divise pas x.
2. Déterminer un entier non nul x tel que 4 et 7 divisent x et 4×7 ne divise pas x.
3. Un des deux problèmes ci-dessus n'a pas de solution. L'explication est donnée par la propriété 3.10 (conséquence du théorème de Gauss).

Exercice 3.21

1. Si 6 et 15 divisent un même nombre entier n, peut-on dire qu'alors 6×15 divise n. Justifier.
2. Si 8 et 15 divisent un même nombre entier n, peut-on dire qu'alors 8×15 divise n. Justifier.

Exercice 3.22

Démontrer que pour tout entier naturel n, le nombre $3n(n+1)$ est mutiple de 6.

3.5 Chiffrement affine (2)

Exercice 3.23

Le chiffrement affine a été décrit et étudié dans l'exercice 3.1. Un cas a été étudié où deux lettres différentes étaient codées par la même lettre, ce qui pose problème.

On rappelle qu'on associe un nombre x entre 0 et 25 à une lettre, puis on lui associe un autre nombre y entre 0 et 25 tel que $ax + b \equiv y\ [26]$ et on associe une lettre à y.

Comment choisir a et b pour que deux lettres associées à x_1 et x_2 soient codées par deux lettres différentes associées à y_1 et y_2 ?

Nous allons raisonner par la contraposée, en prouvant que si $y_1 \equiv y_2\ [26]$ et si a est un nombre premier avec 26, alors $x_1 \equiv x_2\ [26]$.

On a donc $\begin{cases} ax_1 + b \equiv y_1\ [26] \\ ax_2 + b \equiv y_2\ [26] \end{cases}$ et $y_1 \equiv y_2\ [26]$ et on suppose que a et 26 sont premiers entre eux.

1. Démontrer qu'il existe un entier k tel que $a(x_1 - x_2) = 26k$.
2. Que peut-on en déduire pour a et k ?
3. En déduire qu'il existe un entier k' tel que $x_2 - x_1 = 26k'$.
4. Que peut-on en déduire pour x_1 et x_2 ?

Exercice 3.24

En français les deux lettres les plus fréquentes sont le E (17,8 %) et le S (8,2 %).
Cela permet de décrypter un chiffrement affine, en effet, dans un chiffrement affine défini par une égalité $ax + b \equiv y\ [26]$, où a est premier avec 26, chaque lettre est codée par une lettre unique et on peut ainsi déterminer par quelles lettres sont codées le E et le S.

Un message est codé par un chiffrement affine tel que a est premier avec 26, et on remarque que les lettres D et X apparaissent avec des fréquences respectives proches de 17,8 % et 8,2 %, on suppose donc que E et S sont codés D et X.

Déterminer a et b d'après ces informations.

Indications :

- écrire un système d'équations d'inconnues a et b modulo 26 ;
- en déduire qu'il existe un entier k tel que $7a - 13k = 10$;
- résoudre cette équation et justifier qu'une seule valeur de a est possible entre 0 et 25 ;
- déterminer b.

3.6 Chiffrement de Vigenère

L'exercice 3.24 montre comment, s'il on connaît le codage de deux lettres, on peut décrypter une message codé par un chiffrage affine. Cela est dû au fait qu'avec un chiffrage affine, une lettre donnée, comme le E, est toujours codée par la même lettre qui est alors repérée dans le message codé par sa fréquence d'apparition.

Étudions maintenant le chiffrement, de Vigenère, qui évite qu'une lettre donnée soit toujours codée par la même lettre, sans que cela pose de problème de décodage.

Exercice 3.25

Le chiffrement de Vigenère utilise une clef de codage sous la forme d'un mot. Utilisons par exemple le mot `CLE` pour coder le mot `SUITE`, puis on répète la clef de codage autant de fois qu'il faut sous le message comme on le voit dans le tableau ci-dessous.

On associe un nombre entre 0 et 25 à chaque lettre (le tableau de correspondance est rappelé plus bas) : pour `S` $\rightarrow x = 18$ et pour `C` $\rightarrow y = 2$.

On calcule la somme modulo 26 : $x + y = 18 + 2 \equiv 20$ [26] et 20 correspond à `U`.

Lettre non codée	S	U	I	T	E	S
Lettre de la clef de codage	C	L	E	C	L	E
x	18					
y	2					
$x + y \equiv z$[26]	20					
Lettre codée	U					

1. Finir de coder le mot `SUITE`.
2. Décoder le mot codé : `DLG`

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Remarque

- Le codage du mot `SUITES` dans l'exercice 3.25 montre bien que le premier et le deuxième `S` ne sont pas codés par la même lettre, ce qui empêche le décryptage par l'étude de la fréquence des lettres du message codé.
- Malgré cela, vers 1854, le mathématicien britannique Charles Babbage a trouvé une méthode de décryptage du chiffrement de Vigenère.

3.7 Chiffrement de Hill

Exercice 3.26

Le chiffrement de Hill s'effectue de la manière suivante.

- On groupe les lettres du message deux par deux
- On associe un nombre entre 0 et 26 à chaque lettre, et on obtient ainsi des couples de nombres $(x_1 \ ; \ x_2)$
- On associe en suite ce couple $(x_1 \ ; \ x_2)$ à un couple $(y_1 \ ; \ y_2)$ de la manière suivante :
  $\begin{cases} ax_1 + bx_2 \equiv y_1 \ [26] \\ cx_1 + dx_2 \equiv y_2 \ [26] \end{cases}$

1. **Procédure de codage**

   Un chiffrement de Hill est effectué d'après le système ci-dessous.
   $\begin{cases} 3x_1 + 4x_2 \equiv y_1 \ [26] \\ 2x_1 + 3x_2 \equiv y_2 \ [26] \end{cases}$

   On veut coder le mot MATH.

   a) Associer un couple $(x_1 \ ; \ x_2)$ aux lettres M-A

   b) Calculer un couple $(y_1 \ ; \ y_2)$ d'après le système ci-dessus.

   c) Associer deux lettres au couple $(y_1 \ ; \ y_2)$

   d) Procéder de la même façon pour T-H.

   e) Donner le codage du mot MATH.

2. **Procédure de décodage**

   Le codage consistait à calculer $(y_1 \ ; \ y_2)$ d'après $(x_1 \ ; \ x_2)$, le décodage consiste à calculer $(x_1 \ ; \ x_2)$ d'après $(y_1 \ ; \ y_2)$.

a) D'après le système donné au **1.**, écrire x_1 en fonction de y_1 et y_2, puis x_2 en fonction de y_1 et y_2. Pour cela, faire une combinaison linéaire qui élimine x_2, et une autre qui élimine x_1. On obtient ainsi un nouveau système

$$\begin{cases} x_1 \equiv py_1 + qy_2 \ [26] \\ x_2 \equiv ry_1 + sy_2 \ [26] \end{cases}$$

b) Utiliser ce système pour décoder Z-C

Exercice 3.27

x et y sont deux entiers qui vérifient l'égalité : $3x \equiv y \ [10]$. Écrire x en fonction de y.

Indication : déterminer un entier a tel que $3a \equiv 1 \ [10]$, puis multiplier les deux membres de l'égalité précédente par a.

Exercice 3.28

Pour chaque égalité ci-dessous, écrire x en fonction de y.

1. $8x \equiv y \ [15]$ **2.** $6x \equiv y \ [11]$ **3.** $9x \equiv y \ [26]$ **4.** $5x \equiv y \ [26]$

Exercice 3.29

Un chiffrement de Hill est effectué d'après le système ci-dessous.

$$\begin{cases} 2x_1 + 5x_2 \equiv y_1 \ [26] \\ x_1 + 4x_2 \equiv y_2 \ [26] \end{cases}$$

1. **Procédure de codage :** coder les lettres O-K.
2. **Procédure de décodage**

a) À partir du système précédent, justifier qu'on obtient le système ci-dessous.

$$\begin{cases} 3x_1 \equiv 4y_1 - 5y_2 \ [26] \\ 3x_2 \equiv -y_1 + 2y_2 \ [26] \end{cases}$$

b) Justifier ensuite qu'on obtient le système ci-dessous.

$$\begin{cases} x_1 \equiv 10y_1 + 7y_2 \ [26] \\ x_2 \equiv 17y_1 + 18y_2 \ [26] \end{cases}$$

c) Utiliser ce système pour décoder A-B.

3.8 Pour réviser

Chapitre du livre n° 2 – Théorème de Bézout, Théorème de Gauss, page 35

Les exercices résolus

- ex 1 p 41 : PGCD, algorithme d'Euclide, combinaison linéaire des deux nombres égale au PGCD
- ex 2 p 41 : démontrer que $2n + 1$ et $3n + 2$ sont premiers entre eux
- ex 9 p 47 : divisibilité d'une expression par 6
- ex 10 p 47 : équation diophantienne $(ax + by = c)$

Rubrique *Pour s'exercer*, corrigés page 156-157

- ex 3 p 41 : PGCD, algorithme d'Euclide, combinaison linéaire des deux nombres égale au PGCD.
- ex 7 p 41 : démontrer que deux expressions en fonction de n sont premiers entre eux
- ex 11 p 47 : divisibilité d'une expression par 6
- ex 15 p 47 : équation diophantienne $(ax + by = c)$

Rubrique *Objectif bac*, corrigés page 158

- ex 74 p 54 : QCM
- ex 75 p 54 : Vrai-Faux
- ex 76 p 54 : Vrai-Faux
- ex 77 p 55 : exercice de type bac, système de congruences

II Cours

3.1 PGCD

3.1.a Exemple

Étudions les diviseurs commun à 12 et à 20.

Liste des diviseurs de 12 :

$12 = 1 \times 12 = 2 \times 6 = 3 \times 4$

$\{-12\ ;\ -6\ ;\ -4\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 6\ ;\ 12\}$

Liste des diviseurs de 20 :

$12 = 1 \times 20 = 2 \times 10 = 4 \times 5$

$\{-20\ ;\ -10\ ;\ -5\ ;\ -4\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 4\ ;\ 5\ ;\ 10\ ;\ 20\}$

Liste des diviseurs communs à 12 et à 20 :

$\{-4\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 4\}$

Le PGCD de 12 et 20 est 4.

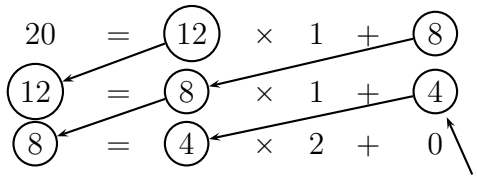
Écrivons maintenant la liste des diviseurs de 4 :

$4 = 1 \times 4 = 2 \times 2$

$\{-4\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 4\}$

Il s'avère donc que la liste des diviseurs communs à 12 et à 20 est la liste des diviseurs de leur PGCD.

On peut aussi obtenir le PGCD à l'aide de l'algorithme d'Euclide.



On effectue la division euclidienne de 20 par 12.

On recommence avec le dernier diviseur par le dernier reste.

Le PGCD est le dernier reste non nul dans l'algorithme d'Euclide, et on retrouve bien le nombre 4.

3.1.b Définition et propriété

Un nombre entier a un ensemble de diviseurs qui contient au moins 1 et lui même.

Deux nombres entiers non nuls a et b ont donc un ensemble de diviseurs communs qui contient au moins 1.

Définition 3.1

Pour deux nombres entiers non nuls a et b, on note PGCD le plus grand diviseur commun à ces deux nombres a et b.

Remarque

On dit « Plus Grand Diviseur Commun », on pourrait donc écrire PGDC au lieu de PGCD. Peut être s'agit-il d'un anglicisme, puisqu'en anglais le PGCD est appelé *Greatest Common Divisor* et se note GCD. Il se pourrait aussi que cela vienne de l'ancien français où l'on plaçait l'adjectif avant le nom, comme en anglais.

Propriété 3.1

Le PGCD de deux nombre est strictement positif.

Démonstration

L'ensemble des diviseurs communs contient des nombres strictement négatifs et des nombres strictement positif donc le plus grand d'entre eux est strictemnt positif.

Propriété 3.2 (PGCD d'un nombre et un de ses diviseurs)

Pour deux nombres entiers non nuls a et b tels que b divise a, le PGCD de a et b est b si b est positif et $-b$ si b est négatif.

Démonstration

Appelons d le PGCD de a et b.

Si b divise a, alors b et $-b$ font partie des diviseurs communs à a et à b, puisque b divise a et lui même, donc $b \leqslant d$ et $-b \leqslant d$, or le PGCD de a et b divise a et b donc d divise b et $-b$.

Si $b > 0$, alors d divise b implique que $d \leqslant b$, or $b \leqslant d$, donc $b = d$.

Si $b < 0$ alors d divise $-b$ implique que $d \leqslant -b$, or $-b \leqslant d$, donc $-b = d$, donc $d = -b$.

Propriété 3.3 (Identité de Bézout)

Si d est le PGCD de deux nombres entiers non nuls a et b, il existe des entiers u et v tels que $d = au + bv$.

Propriété 3.4

Si d est le PGCD de deux nombres entiers non nuls a et b, l'ensemble des diviseurs commun à a et à b est l'ensemble des diviseurs de d.

Remarque

La réciproque de l'identité de Bézout est fausse, par exemple $2 \times 7 + (-4) \times 3 = 2$ et pourtant le nombre 2 n'est pas le PGCD de 7 et 3, puisque 7 et 3 sont impairs.

Démonstration de ces deux propriétés.

On appelle E l'ensemble des combinaisons linéaires de a et b à coefficients entiers, c'est à dire l'ensemble des nombres de la forme $ua + vb$ où u et v sont des entiers.

- **Étudions d'abord cet ensemble E.**
  Remarquons d'abord que E est un ensemble d'entiers puisque si a, b, u, v sont des entiers $ua + vb$ est un entier.
  On peut remarquer aussi que cet ensemble contient a et b et zéro, puisque : $a = 1a + 0b$ et $b = 0a + 1b$ et $a = 1a + 0b$ et $0 = 0a + 0b$, et qu'il n'est donc pas vide.
  Cet ensemble E contient aussi des entiers naturels strictement positifs. C'est bien sûr le cas si a ou b est strictement positif, mais, même si a et b sont strictement négatifs, E contient $-a$ qui est strictement positif.
  L'ensemble des entiers naturels strictement positifs de E admet un plus petit élément qu'on appelle d'.

- **Démontrons que $d' = d$, c'est à dire que ce nombre d' est le PGCD de a et b.**
  Puisque d' appartient à E, il existe des entiers u' et v' tels que $u'a + v'b = d'$.
  Or, d'après la propriété 3.3 tout diviseur commun à a et à b divise toute combinaison linéaire de a et b.
  Donc, en particulier d, le PGCD, divise d', donc $d \leqslant d'$ puisque d et d' sont strictement positifs.

  Démontrons que d' est un diviseur commun à a et à b.
  Écrivons d'abord la division euclidienne de a par d' : $a = d'q + r$ et $0 \leqslant r < d'$.

On a donc : $r = a - d'q = a - (u'a + v'b) \times q = a - qu'a - qv'b = (1 - qu')a - qv'b$
c'est à dire que r est une combinaison linéaire de a et b.
Donc $r \in$ E, or $r \geqslant 0$, mais comme $r < d$ et d' est le plus petit élément de E, il est impossible d'avoir $0 < r < d'$, donc $r = 0$ et d' est un diviseur de a.
On démontre de même que d' est un diviseur de b.
Donc d' est un diviseur commun à a et à b, donc $d' \leqslant d$.

Donc $d = d' = u'a + v'b$, ce qui démontre la propriété 3.3.

- **Démontrons la propriété 3.4**
  Nous avons mentionné plus haut que tout diviseur commun à a et à b est un diviseur de d le PGCD de a et b, mais la réciproque est vraie, en effet, si un nombre entier est un diviseur de d qui est lui même un diviseur de a et b, ce nombre est un diviseur commun à a et à b.
  Nous venons donc aussi de prouver que l'ensemble des diviseurs commun à a et à b est l'ensemble des diviseurs de d, leur PGCD.

3.1.c L'algorithme d'Euclide

Propriété 3.5

Pour deux nombres entiers naturels non nuls a et b tels que $a > b$ et b ne divise pas a si r est le reste de la division euclidienne de a par b, alors PGCD$(a\ ;\ b)$ = PGCD$(b\ ;\ r)$

Remarque

Pour deux nombres entiers naturels non nuls a et b, la propriété 3.5 ci-dessus concerne le cas où $a > b$ et b ne divise pas a. Rappelons que d'après la propriété 3.2, si b divise a, alors leur PGCD est b.

Démonstration

$a = bq + r$ or le PGCD de b et r divise b et r donc d'après l'égalité précédente il divise a, ainsi le PGCD de b et r divise a et b, donc le PGCD de b et r divise le PGCD de a et b.

Réciproquement, $a = bq + r \iff r = a - bq$ or le PGCD de a et b divise a et b, donc d'après l'égalité précédente il divise r, ainsi le PGCD de a et b divise b et r, donc le PGCD de a et b divise le PGCD de b et r.

Par conséquent les deux PGCD sont égaux, puisqu'ils sont strictement positifs.

Définition 3.2 (Algorithme d'Euclide)

L'algorithme d'Euclide pour deux nombres entiers naturels non nuls a et b tels que $a > b$ et b ne divise pas a est décrit ci-dessous.

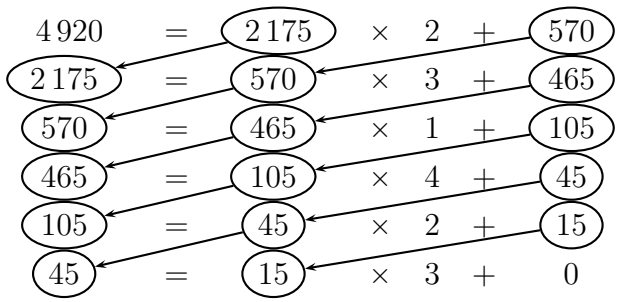
- **Entrées :** les nombres entiers a et b.
- **Initialisation :** on effectue la division euclidienne de a par b.
- À chaque étape suivante, on effectue la division euclidienne du dernier diviseur par le dernier reste, tant que le reste n'est pas nul.
- **Sortie :** le dernier reste non nul.

Propriété 3.6

Pour deux nombres entiers naturels non nuls, le dernier reste non nul de l'algorithme d'Euclide est le PGCD de ces deux nombres.

Exemple

Appliquons l'algorithme d'Euclide aux nombres 4 920 et 2 175.



On effectue la division euclidienne de 4 920 par 2 175
À chaque étape suivante, on effectue la division euclidienne du dernier diviseur par le dernier reste.

Le dernier reste non nul est le PGCD des 2 nombres.

Donc le PGCD de 4 920 et 2 175 est $\boxed{15}$.

Justifions cela d'après les calculs ci-dessus et à l'aide de la propriété 3.5.

$\text{PGCD}(4\,920\,;\,2\,175) = \text{PGCD}(2\,175\,;\,570) = \text{PGCD}(570\,;\,465) = \text{PGCD}(465\,;\,105) = \text{PGCD}(105\,;\,45) = \text{PGCD}(45\,;\,15)$

or 45 est multiple de 15, donc le PGCD de 45 et 15 est 15, donc 15 est bien le PGCD de 4 920 et 2 175.

3.1.d Obtenir le PGCD avec la calculatrice

Exemple : le PGCD de 6 et 8 est 2.

Avec la TI 82

math → (NUM), descendre jusqu'à `pgcd`, puis compléter ainsi : `pgcd(6,8)` et appuyer sur entrer.

Avec la CASIO

MENU choisir RUN-MAT OPTN F6 (→) F4 (NUM) F6 (→) F2 (GCD)
puis compléter ainsi : `GCD(6,8)` et appuyer sur EXE.

3.1.e Méthode : comment déterminer le PGCD de deux entiers ?

- On peut, comme dans l'exemple du paragraphe 3.1.a, écrire les listes des diviseurs des deux nombres, puis écrire la liste de leurs diviseurs communs, et le PGCD est alors le plus grand nombre de cette liste.
  Cette méthode ne peut être utilisée que pour des petits nombres.
- On peut aussi utiliser l'algorithme d'Euclide : voir paragraphe 3.1.c.
- Si l'énoncé ne demande ni justification ni calcul, on peut utiliser la calculatrice : voir paragraphe 3.1.d.
- On peut enfin utiliser la décomposition d'un entier en produit de puissances de nombres premiers, ce qui sera étudié au chapitre 5 *Nombres premiers*.

3.2 Nombres premiers entre eux

3.2.a Définition et propriété

Définition 3.3

Dire que deux nombres entiers non nuls a et b sont premiers entre eux signifie que leur PGCD est 1.

Exemple

35 et 6 sont premiers entre eux, puisque leur PGCD est 1, d'après l'algorithme d'Euclide ci-dessous.

$35 = 6 \times 5 + 5$
$6 = 5 \times 1 + 1$
$5 = 1 \times 5 + 0$

Propriété 3.7

Lorsque deux nombres entiers non nuls a et b sont premiers entre eux, les nombres a et $-b$, $-a$ et b, $-a$ et $-b$, sont aussi premiers entre eux.

3.2.b Théorème de Bézout

Propriété 3.8 (Théorème de Bézout)

Deux nombres entiers non nuls a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que $au + bv = 1$

Démonstration

D'après la propriété 3.3, si d est le PGCD de deux nombres entiers non nuls a et b, il existe des entiers u et v tels que $d = au + bv$, et comme ici nous avons $d = 1$, nous pouvons affirmer qu'il existe des entiers u et v tels que $au + bv = 1$.

Réciproquement, s'il existe des entiers u et v tels que $au + bv = 1$, alors le PGCD de a et b divise aussi 1, donc le PGCD de a et b est égal à 1.

3.2.c Théorème de Gauss et conséquence

Propriété 3.9 (Théorème de Gauss)

Pour trois nombres entiers a, b, et c,
si a et b sont premiers entre eux et si a divise bc,
alors a divise c.

Démonstration

Considérons trois nombres entiers a, b, et c, tels que a et b sont premiers entre eux et tels que a divise bc.

Puisque a et b sont premiers entre eux, il existe des entiers u et v tels que $au + bv = 1$.

$au + bv = 1 \Rightarrow (au + bv)c = c \Rightarrow auc + bvc = c$

or a divise bc donc il existe un entier k tel que $bc = ka$.

Donc : $auc + vbc = c \Rightarrow auc + vka = c \Rightarrow a(uc + vk) = c$

Donc a divise c.

Propriété 3.10 (Conséquence du théorème de Gauss)

Pour trois nombres entiers a, b, et c,
si b et c sont premiers entre eux et si b et c divisent a,
alors bc divise a.

Démonstration

Puisque b divise a, il existe un entier k tel que $a = bk$.

Or, c divise aussi a, autrement dit c divise bk, or c est premier avec b, donc d'après le théorème de Gauss, c divise k.

Par conséquent il existe un entier k' tel que $k = ck'$.

On a donc : $a = bck'$, donc bc divise a.