

# Chapitre I

## Arithmétique

### 1 Divisibilité

**Remarque :** dans ce chapitre, on désignera par **entier** un élément de  $\mathbb{Z}$ . Les éléments de  $\mathbb{N}$  seront appelés **entiers positifs**.

#### 1.2 Généralités

##### Définition

Soient  $a, b \in \mathbb{Z}$ , on dit que  $a$  **divise**  $b$  ou que  $a$  est un **diviseur** de  $b$  ou encore que  $b$  est un **multiple** de  $a$  si et seulement si il existe  $q \in \mathbb{Z}$  tel que  $b = aq$ .

##### Quelques rappels de propriétés bien connues, à montrer à titre d'exercice

Soient  $a, b$  et  $c$  des entiers.

- 1) Si  $a$  divise  $b$  et  $b$  divise  $c$  alors  $a$  divise  $c$ .
- 2) Si  $a$  divise  $b$  et  $b$  divise  $a$  alors  $a = \pm b$ .
- 3) Si  $a$  divise  $b$  et  $c$  alors  $a$  divise  $b + c$ .
- 4) Si  $a$  divise  $b$  alors  $a$  divise  $bc$ .
- 5) Si  $a$  divise  $b$  alors  $ac$  divise  $bc$ .

#### 1.3 Division euclidienne

##### Propriété

Soit  $a$  un entier et  $b$  un entier **positif non nul**.

Il existe un unique couple d'entier  $(q, r)$  tel que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < b$$

On dit que  $q$  est le **quotient** et  $r$  est le **reste** de la **division euclidienne** de  $a$  par  $b$ .

##### Propriété

Soit  $a$  un entier et  $b$  un entier **positif non nul**.

$a$  est divisible par  $b$  si et seulement si le reste de la division euclidienne de  $a$  par  $b$  est nul.

## 1.4 Congruence

### Définition

Soient  $a, b$  et  $n$  des entiers, on dit que  $a$  **est congru à  $b$  modulo  $n$**  et on note  $a \equiv b[n]$  si et seulement si  $a - b$  est un multiple de  $n$ .

### Règles de calcul à montrer à titre d'exercice

Soient  $n, m$  et  $a, b, c, d$  des entiers :

- Si  $a \equiv b[n]$  alors  $b \equiv a[n]$ .
- Si  $a \equiv b[n]$  et  $b \equiv c[n]$  alors  $a \equiv c[n]$ .
- Si  $a \equiv c[n]$  et  $b \equiv d[n]$  alors  $a + b \equiv c + d[n]$ .
- Si  $a \equiv c[n]$  et  $b \equiv d[n]$  alors  $ab \equiv cd[n]$ .
- Si  $a \equiv b[n]$  alors  $ma \equiv mb[mn]$ .

## 2 Plus grand commun diviseur (PGCD)

### Définition

Soient  $a, b \in \mathbb{Z}$  non tous deux nuls (c.a.d.  $a \neq 0$  ou  $b \neq 0$ ).

Le plus grand entier qui divise  $a$  et  $b$  s'appelle le **plus grand diviseur commun** de  $a$  et  $b$  et se note  $\text{pgcd}(a, b)$ .

*Justification :*

Cette définition a un sens car l'ensemble  $D$  des diviseurs communs à  $a$  et  $b$  est fini et non vide (il contient au moins le nombre 1), il en découle que  $D$  admet un plus grand élément.

### Propriété fondamentale pour l'algorithme d'Euclide

Soient  $a$  et  $b$  des entiers **positifs** avec  $b$  **non nul**.

Si  $r$  est le reste de la division euclidienne de  $a$  par  $b$  alors  $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ .

### Algorithme d'Euclide

entrées :  $a, b$  positifs,  $b \neq 0$

sortie :  $\text{pgcd}(a, b)$

```

1  Tant que  $b \neq 0$  faire
2       $q, r \leftarrow$  quotient, reste de la division euclidienne de  $a$  par  $b$ 
3       $a \leftarrow b$ 
4       $b \leftarrow r$ 
5  retourner  $a$ 
```

### Propriété

Soit  $a$  et  $b$  des entiers **positifs** avec  $b$  **non nul**.

La valeur de retour de l'algorithme d'Euclide est le  $\text{pgcd}$  de  $a$  et  $b$ .

## 3 Nombres premiers entre eux

### 3.2 Définition et propriétés

#### Définition

Soient  $a$  et  $b$  des entiers **non tous deux nuls**, on dit que  $a$  et  $b$  sont premiers entre eux si  $\text{pgcd}(a, b) = 1$ .

### Propriété

Soient  $a$  et  $b$  des entiers **non nuls**, les quotients de  $a$  et  $b$  par  $\text{pgcd}(a, b)$  sont des nombres premiers entre eux.

### Théorème de Bezout

Soient  $a$  et  $b$  des entiers **positifs non nuls**, alors il existe des entiers  $u$  et  $v$  tels que  $\text{pgcd}(a, b) = a u + b v$ .

Cette existence est montrée dans la preuve de l'algorithme d'Euclide étendu.

### Algorithme d'Euclide étendu

Soient  $a$  et  $b$  des entiers **positifs non nuls**. L'algorithme d'Euclide étendu est :

entrées :  $a, b$  positifs non nuls

sortie :  $r = \text{pgcd}(a, b)$  et  $u, v$  entiers tels que  $r = a u + b v$

```

1   Initialisation :  $(r, u, v, r', u', v') \leftarrow (a, 1, 0, b, 0, 1)$ 
2   Tant que  $r' \neq 0$  faire
3        $q \leftarrow$  quotient de la division euclidienne de  $r$  par  $r'$ 
4        $(r, u, v, r', u', v') \leftarrow (r', u', v', r - q r', u - q u', v - q v')$ 
5   retourner  $(r, u, v)$ 
```

### Propriété

Soient  $a$  et  $b$  des entiers **positifs non nuls**, l'algorithme d'Euclide étendu retourne  $\text{pgcd}(a, b)$  et  $u, v$  tels que  $\text{pgcd}(a, b) = a u + b v$ .

### Propriété

Soient  $a$  et  $b$  des entiers **positifs non nuls**, alors  $a$  et  $b$  sont premiers entre eux si et seulement si il existe des entiers  $u$  et  $v$  tels que  $a u + b v = 1$ .

### Attention

Cette propriété est une réciproque au théorème de Bezout **uniquement pour des nombres premiers entre eux**. Il n'y a pas de réciproque au théorème de Bezout dans le cas général.

### Propriété

Soient  $a$  et  $b$  des entiers **positifs non nuls** :

- 1) Tout diviseur commun à  $a$  et  $b$  divise  $\text{pgcd}(a, b)$ .
- 2) Pour tout entier  $m$  positif non nul,  $\text{pgcd}(ma, mb) = m \text{pgcd}(a, b)$ .

### Théorème de Gauss

Soient  $a, b$  et  $c$  des entiers **positifs non nuls**. Si  $a$  divise  $b c$  et si  $a$  est premier avec  $b$ , alors  $a$  divise  $c$ .

## 4 Plus petit commun multiple

### Propriété et définition

Soient  $a$  et  $b$  des entiers non nuls, il existe un plus petit commun multiple positif et non nul de  $a$  et  $b$  qui est noté  $\text{ppcm}(a, b)$ .

*Justification* : l'ensemble des multiples strictement positifs communs à  $a$  et  $b$  est non vide car il contient

$|ab|$ . Or toute partie non vide de  $\mathbb{N}$  admet un plus petit élément. Donc l'ensemble des multiples strictement positifs communs à  $a$  et  $b$  admet un plus petit élément.

#### Propriété - ADMISE

Soient  $a$  et  $b$  des entiers **positifs non nuls**,  $ab = \text{pgcd}(a, b) \text{ ppcm}(a, b)$ .

#### Propriété immédiate

Soient  $a$  et  $b$  des entiers **non nuls**,  $a$  et  $b$  sont premiers entre eux si et seulement si  $\text{ppcm}(a, b) = ab$ .

## 5 Équation diophantienne

### 5.1.1 Problème

Soient  $a$ ,  $b$  et  $c$  des entiers avec  $a$  et  $b$  **non nuls**.  
Résoudre dans  $\mathbb{Z}$  l'équation (E)  $ax + by = c$  d'inconnues  $x$  et  $y$ .  
Une telle équation est appelée équation diophantienne.

### 5.1.2 Méthode

La résolution d'une telle équation utilise les théorèmes de Bezout et Gauss. On l'effectue en trois étapes.

**Étape 1 : calculer  $\text{pgcd}(a, b)$ .**

Si  $c$  n'est pas un multiple de  $\text{pgcd}(a, b)$ , l'équation  $ax + by = c$  n'a pas de solution.

**Étape 2 : si  $c$  est un multiple de  $\text{pgcd}(a, b)$ , l'équation  $ax + by = c$  admet des solutions et on recherche une solution particulière.**

On note  $d := \text{pgcd}(a, b)$ . On calcule le quotient de  $c$  par  $d$  que l'on note  $m$ .  
L'algorithme d'Euclide étendu appliqué à  $a$  et  $b$  fournit des entiers  $u$  et  $v$  tels que  $au + bv = d$ .  
Une solution particulière de l'équation  $ax + by = c$  est  $(x_0, y_0) = (mu, mv)$ .

**Étape 3 : si  $c$  est un multiple de  $\text{pgcd}(a, b)$ , on recherche toutes les solutions de l'équation  $ax + by = c$ .**

On note  $d := \text{pgcd}(a, b)$  et  $(x_0, y_0)$  la solution particulière déterminée à l'étape 2.  
On calcule  $a'$  et  $b'$  les quotients respectifs de  $a$  et  $b$  par  $d$ .  
L'ensemble des solutions est  $S = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}$ .

### 5.1.3 Problème dérivé

Soient  $a$ ,  $b$  et  $c$  des entiers avec  $a$  et  $b$  **non nuls**.  
Résoudre dans  $\mathbb{Z}$  l'équation  $ax \equiv c[b]$ .

On remarque que l'entier  $x$  est solution de  $ax \equiv c[b]$  si et seulement il existe un entier  $y$  tel que  $ax = c - by$ , c.a.d.  $ax + by = c$ .

La méthode de résolution en découle directement.

### 5.1.4 Méthode

**Etape 1 : calculer  $\text{pgcd}(a, b)$ .**

Si  $c$  n'est pas un multiple de  $\text{pgcd}(a, b)$ , l'équation  $ax \equiv c[b]$  n'a pas de solution.

**Etape 2 :** si  $c$  est un multiple de  $\text{pgcd}(a, b)$ , l'équation  $ax \equiv c[b]$  admet des solutions et on recherche une solution particulière.

On note  $d := \text{pgcd}(a, b)$ . On calcule le quotient de  $c$  par  $d$  que l'on note  $m$ .

L'algorithme d'Euclide étendu appliqué à  $a$  et  $b$  fournit des entiers  $u$  et  $v$  tels que  $au + bv = d$ .

Une solution particulière de l'équation  $ax \equiv c[b]$  est  $x_0 = mu$ .

**Etape 3 :** si  $c$  est un multiple de  $\text{pgcd}(a, b)$ , on recherche toutes les solutions de l'équation  $ax \equiv c[b]$ .

On note  $d := \text{pgcd}(a, b)$  et  $x_0$  la solution particulière déterminée à l'étape 2.

On calcule  $b'$  le quotient de  $b$  par  $d$ .

L'ensemble des solutions est  $S = \{x_0 + kb' \mid k \in \mathbb{Z}\}$ .

## 6 Décomposition en facteurs premiers

### 6.2 Nombres premiers

#### Définition

On appelle nombre premier tout entier  $p \geq 2$  dont les seuls diviseurs positifs sont 1 et  $p$ .

*Exemples :* Les nombres premiers inférieurs à 100 sont :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

#### Propriété

Soient  $n$  un entier et  $p$  un nombre premier, alors ou bien  $p$  divise  $n$  ou bien  $p$  et  $n$  sont premiers entre eux.

#### Lemme d'Euclide : une conséquence immédiate du théorème de Gauss

Soient  $a$  et  $b$  des entiers et  $p$  un nombre premier.

Si  $p$  divise  $ab$ , alors  $p$  divise  $a$  ou  $p$  divise  $b$ .

### 6.3 Décomposition en facteurs premiers

#### Propriété (ADMISE)

Tout entier  $n \geq 2$  a au moins un facteur premier.

#### Décomposition en facteurs premiers (ADMISE)

Soit  $n \geq 2$  un entier, il existe un unique entier  $r \geq 1$  et des nombres premiers  $p_1 \leq \dots \leq p_r$  uniques tels que  $n = p_1 \dots p_r$ .