

Arithmétique dans  $\mathbb{Z}$ 

## I Divisibilité et division euclidienne

### 1 Multiples et diviseurs

#### Définition 1

Si  $a, b \in \mathbb{Z}$ , on dit que  $b$  **divise**  $a$  ou que  $a$  **est un multiple de**  $b$ , et on note  $b|a$  lorsque l'on a  $k \in \mathbb{Z}$  tel que  $a = kb$ .

L'ensemble des multiples de  $b$  est noté  $b\mathbb{Z}$ .

Si  $a|b$  et  $b|a$ ,  $a$  et  $b$  sont dit **associés**.

#### Propriétés 1

Soient  $a, b, c, d, k, \ell \in \mathbb{Z}$ .

- (i) La relation  $|$  est transitive et réflexive sur  $\mathbb{Z}$ .
- (ii)  $a$  et  $b$  sont associés si et seulement si  $|a| = |b|$  si et seulement si  $a = \pm b$ .
- (iii)  $b|a \implies b|ac$
- (iv)  $b|a$  et  $b|c \implies b|(ka + \ell c)$
- (v)  $b|a$  et  $d|c \implies bd|ac$
- (vi)  $b|a \implies \forall n \in \mathbb{N}, b^n | a^n$

### 2 Division euclidienne

#### Théorème 1 : Division euclidienne dans $\mathbb{Z}$

Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

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

#### Propriété 1 : caractérisation de la divisibilité par le reste

Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ .  $b|a$  si et seulement si le reste de la division euclidienne de  $a$  par  $b$  est nul.

## II Diviseurs communs

### 1 Définition

#### Définition – Propriété 1 : PGCD

Soient  $a, b \in \mathbb{N}$  dont l'un au moins est non nul. Alors l'ensemble des diviseurs (positifs) communs à  $a$  et  $b$  admet un plus grand élément, appelé **pgcd** de  $a$  et de  $b$ , noté  $a \wedge b$ .

Par convention, on pose  $0 \wedge 0 = 0$ .

### 2 Algorithme d'Euclide

#### Propriété 2 : Propriété d'Euclide

Si  $(a, b) \in \mathbb{N}^2$ ,  $k \in \mathbb{N}$ , alors les diviseurs communs à  $a$  et  $b$  sont les diviseurs communs à  $a - bk$  et  $b$ , et en particulier  $a \wedge b = (a - bq) \wedge b$ .

#### Propriété 3 : Algorithme d'Euclide

Soient  $(a, b) \in \mathbb{N}^2 \setminus \{(0, 0)\}$ .

On effectue les divisions euclidiennes successives

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

$\vdots$

$$\forall k, r_{k-1} = r_kq_{k+1} + r_{k+1}$$

$$\text{avec } 0 \leq r_{k+1} < r_k$$

(en notant  $a = r_{-1}$  et  $b = r_0$ ).

Le procédé s'arrête et le dernier reste non nul vaut  $a \wedge b$ .

Implémentations itérative et récursive en Python et Ocaml

```

1 def pgcd_rec(a, b):
2     """renvoie le pgcd des entiers naturels
3     a et b"""
4     if b == 0:
5         return a
6     else:
7         return pgcd_rec(b, a % b)

```



```

1 let rec pgcd a b =
2   match b with
3   | 0 -> a
4   | _ -> pgcd b (a mod b)
5 ;;
6 pgcd : int -> int -> int = <fun>

```

Algorithme récursif efficace (terminal) car par de retour nécessaire sur la pile d'évaluation!

```

1 def pgcd(a, b):
2     """renvoie le pgcd des entiers naturels
3     a et b"""
4     while b != 0:
5         a, b = b, a % b
6     return b

```

```

1 let pgcd a b =
2   let r = ref a in
3   let r1 = ref b in
4   while !r1 <> 0 do
5     let temp = !r in
6     r := !r1;
7     r1 := temp mod !r
8   done;
9   !r;;
10 pgcd : int -> int -> int = <fun>

```

Invariant de sortie du  $k^{\text{e}}$  tour de boucle,  $a$  contient  $r_{k-1}$  et  $b$  contient  $r_k$ .

### 3 Relation de Bézout

#### Propriété 4 : Relation de Bézout

Si  $(a, b) \in \mathbb{N}^2$ , on peut trouver  $(u, v) \in \mathbb{Z}^2$  tels que  $au + bv = a \wedge b$ .

Algorithme d'Euclide étendu en Python et OCaml :

```

1 def euclide_rec(a, b):
2     """renvoie un triplet (d, u, v) où
3     d = pgcd(a, b) et au + bv = d"""
4     if b == 0:
5         return a, 1, 0
6     else:
7         q, r = divmod(a, b)
8         d, u, v = euclide_rec(b, r)
9         return d, v, u - q * v

```

```

1 let rec euclide a b =
2   match b with
3   | 0 -> a, 1, 0
4   | _ ->
5     let q = a / b in
6     let r = a mod b in
7     let d, u, v = euclide b r in
8     d, v, u - q * v
9 ;;
10 euclide:
11 int -> int -> int * int * int = <fun>

```

### 4 Caractérisation du pgcd

#### Propriété 5 : Caractérisation du pgcd

Soient  $(a, b) \in \mathbb{N}^2$ ,  $d \in \mathbb{Z}$ .

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall d' \in \mathbb{Z}, d'|a \text{ et } d'|b \implies d'|d \end{cases}$$

Ainsi,  $a \wedge b$  est le plus grand diviseur commun au sens de l'ordre  $|$  également.

#### Corollaire 1

Les diviseurs communs à  $a$  et  $b$  sont les diviseurs de  $a \wedge b$ .

#### Propriété 6 : Factorisation dans un pgcd

Soient  $(a, b) \in \mathbb{N}^2$ ,  $c \in \mathbb{N}$ , alors

$$(ca) \wedge (cb) = c(a \wedge b).$$

### 5 Extension aux entiers relatifs

#### Définition 2 : pgcd dans $\mathbb{Z}$

Si  $(a, b) \in \mathbb{Z}^2$ , alors on pose  $a \wedge b = |a| \wedge |b|$ .  
Il s'agit du **plus grand diviseur commun** à  $a$  et à  $b$ .

#### Propriété 7

- (i) Les diviseurs communs à  $a$  et  $b$  sont les diviseurs de  $a \wedge b$ .
- (ii) Si  $a = bq + r$  (pas nécessairement une division euclidienne),  $a \wedge b = b \wedge r$ .
- (iii) On a  $u, v \in \mathbb{Z}$  tels que  $au + bv = a \wedge b$ .
- (iv) Si  $c \in \mathbb{Z}$ ,  $\triangleleft$   $(ca) \wedge (cb) = |c|(a \wedge b)$ .

## 6 Extension à plus de deux entiers

### Définition 3 : pgcd de plus de deux entiers

Soient  $(a_1, \dots, a_n) \in \mathbb{Z}^n$ . On note  $a_1 \wedge a_2 \wedge \dots \wedge a_n = \bigwedge_{k=1}^n a_k$  le **plus grand diviseur commun** à  $a_1, a_2, \dots, a_n$  s'il sont non tous nuls, 0 sinon.

### Propriété 8 : Associativité du pgcd

Si  $a, b, c \in \mathbb{Z}$ ,

$$a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c).$$

Plus généralement, les diviseurs communs à  $a_1, \dots, a_n$  sont les diviseurs de  $\bigwedge_{k=1}^n a_k$  et

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = (a_1 \wedge a_2 \wedge \dots \wedge a_{n-1}) \wedge a_n.$$

### Propriété 9 : Relation de Bézout

On a  $u_1, \dots, u_n \in \mathbb{Z}$  tels que

$$a_1 u_1 + \dots + a_n u_n = \bigwedge_{k=1}^n a_k.$$

## III Nombres premiers entre eux

### 1 Définition

#### Définition 4 : Nombres premiers entre eux

$(a, b) \in \mathbb{Z}^2$  sont dits **premiers entre eux** lorsque

$$a \wedge b = 1,$$

c'est-à-dire lorsque le seul diviseur positif commun à  $a$  et  $b$  est 1.

### 2 Propriétés

#### Théorème 2 : Théorème de Bézout

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}, au + bv = 1$$

### Propriété 10

Si  $(a, b) \in \mathbb{Z}^2$ ,  $d = a \wedge b$ . On a  $(a', b') \in \mathbb{Z}^2$  tel que

$$\begin{cases} d \in \mathbb{N} \\ a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases}$$

### Propriété 11

$$a \wedge bc = 1 \iff a \wedge b = 1 \text{ et } a \wedge c = 1$$

## 3 Lemme de Gauß et applications

### Théorème 3 : Lemme de Gauß

Si  $a|bc$  et  $a \wedge b = 1$ , alors  $a|c$ .

### Corollaire 2

Si  $a \wedge b = 1$  tels que  $a|c$  et  $b|c$ , alors  $ab|c$ .

### Corollaire 3 : Fractions irréductibles

Tout nombre rationnel  $r \in \mathbb{Q}$  s'écrit de manière unique sous la forme  $\frac{p}{q}$  avec  $p \in \mathbb{Z}$ ,  $q \in \mathbb{N}^*$  et  $p \wedge q = 1$ .



### Méthode : résolution des équations diophantiennes $ax + by = c$

où  $a, b, c \in \mathbb{Z}^*$  sont fixés, on cherche les solutions entières.

On a facilement qu'il y a des solutions si et seulement si  $d = a \wedge b | c$ .

Lorsque  $c$  est le cas, on peut trouver une solution particulière  $(x_0, y_0)$  avec l'algorithme d'Euclide par exemple.

Alors, si  $(x, y)$  solution,  $ax + by = ax_0 + by_0$  puis  $a(x - x_0) = b(y_0 - y)$  donc  $a'(x - x_0) = b'(y_0 - y)$  avec  $a' \wedge b' = 1$  en divisant par  $d$ .

Par lemme de Gauß, on a  $k \in \mathbb{Z}$  tel que  $x = x_0 + b'k$  puis en réinjectant  $y = y_0 - a'k$ .

On vérifie enfin que la réciproque étant vraie. Ensemble des solutions :

$$\{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\}.$$



## 4 Généralisation à plus de deux entiers

### Définition 5

$a_1, \dots, a_n$  sont dits premiers entre eux dans leur ensemble lorsque  $\prod_{k=1}^n a_k = 1$ , c'est-à-dire que le seul diviseur positif commun à tous les  $a_k$  est 1.  
 $a_1, \dots, a_n$  sont dits premiers entre eux deux à deux lorsque  $\forall i \neq j, a_i \wedge a_j = 1$ .

### Propriété 12

Premiers entre eux deux à deux  $\implies$  premiers entre eux dans leur ensemble, mais la réciproque est fautive pour plus de deux entiers.

### Propriété 13 : Théorème de Bézout

$a_1, \dots, a_n$  sont premiers entre eux dans leur ensemble si et seulement si on a  $u_1, \dots, u_n \in \mathbb{Z}$  tels que  $a_1 u_1 + \dots + a_n u_n = 1$ .

### Propriété 14

Si  $a_1, \dots, a_n$  sont premiers entre eux deux à deux et divisent  $c$ , alors  $a_1 \dots a_n | c$ .

### Propriété 15 : Caractérisation du ppcm

Soient  $(a, b) \in (\mathbb{N})^2, m \in \mathbb{Z}$ .

$$m = a \vee b \iff \begin{cases} m \in \mathbb{N} \\ a|m \text{ et } b|m \\ \forall m' \in \mathbb{Z}, a|m' \text{ et } b|m' \implies m|m' \end{cases}$$

Ainsi,  $a \vee b$  est le plus petit multiple commun  $> 0$  au sens de l'ordre | également.

### Corollaire 4

Les multiples communs à  $a$  et  $b$  sont les multiples de  $a \vee b$ .

### Propriété 16

Si  $a, b, c \in \mathbb{N}, (ca) \vee (cb) = c(a \vee b)$ .

## 2 Lien avec le pgcd

### Propriété 17

Si  $a, b \in \mathbb{N}$ ,

$$(a \wedge b)(a \vee b) = ab.$$

En particulier, si  $a \wedge b = 1$ ,

$$a \vee b = ab.$$

## 3 Extension aux entiers relatifs

### Définition 6

Si  $(a, b) \in \mathbb{Z}^2$ , alors on pose  $a \vee b = |a| \vee |b|$ .  
 Il s'agit du plus petit multiple commun  $> 0$  de  $a$  et  $b$  s'ils sont non nuls.

### Propriété 18

- (i) Si  $c \in \mathbb{Z}, \triangleleft (ca) \vee (cb) = |c|(a \vee b)$ .
- (ii)  $\triangleleft (a \wedge b)(a \vee b) = |ab|$ .

# IV Multiples communs

## 1 Définition et caractérisation du ppcm

### Définition – Propriété 2 : PPCM

Soient  $a, b \in \mathbb{N}^*$ . Alors l'ensemble des multiples **strictement positifs** communs à  $a$  et  $b$  admet un plus petit élément, appelé **ppcm** de  $a$  et de  $b$ , noté  $a \vee b$ .  
 On pose, de plus,  $a \vee 0 = 0 \vee b = 0 \vee 0 = 0$ .

# V Nombres premiers

## 1 Définition

### Définition 7 : Nombre premier

Un **nombre premier** est un entier naturel  $p \geq 2$  dont les seuls diviseurs positifs sont 1 et  $p$ .  
On notera  $\mathcal{P}$  l'ensemble des nombres premiers.

## 2 Propriétés

### Propriété 19

Tout entier  $\notin \{0, \pm 1\}$  possède un diviseur premier.

### Propriété 20

L'ensemble des nombres premiers est infini.

### Propriété 21

Si  $p \in \mathcal{P}$  et  $n \in \mathbb{Z}$ , soit  $p|n$ , soit  $p \wedge n = 1$ .

### Propriété 22

Soient  $p \in \mathcal{P}$  et  $a_1, \dots, a_n \in \mathbb{Z}$ .  
 $p|(a_1 \times \dots \times a_n)$  si et seulement si  $p$  divise l'un des  $a_k$ .

## 3 Décomposition primaire et valuations $p$ -adiques

### Théorème 4 : Décomposition primaire

Soit  $n \in \mathbb{Z}^*$ . On peut trouver  $k \in \mathbb{N}$ ,  $p_1, \dots, p_k$  premiers deux à deux distincts,  $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$  tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

appelée décomposition primaire de  $n$ .  
De plus, cette écriture est unique à l'ordre des facteurs près.  
 $p_1, \dots, p_k$  sont les diviseurs premiers de  $n$ .

### Propriété 23

Soient  $n, m \in \mathbb{Z}^*$ ,  $p \in \mathcal{P}$ .

- (i)  $v_p(n) \neq 0 \iff p|n$
- (ii)  $v_p(n \times m) = v_p(n) + v_p(m)$
- (iii)  $n|m \iff \forall p \in \mathcal{P}, v_p(n) \leq v_p(m)$
- (iv)  $v_p(n \wedge m) = \min(v_p(n), v_p(m))$  et  $v_p(n \vee m) = \max(v_p(n), v_p(m))$

### Propriété 24

Si  $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  et  $b = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$  avec des exposants éventuellement nuls et chaque  $p_i$  premier, alors

$$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_k^{\min(\alpha_k, \beta_k)}$$

et

$$a \vee b = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

# VI Congruences

## 1 Définition (rappel)

### Définition 8 : Congruence

Soit  $n \in \mathbb{N}^*$ . On dit que  $a, b \in \mathbb{Z}$  sont **congrus modulo  $n$**  et on note  $a \equiv b [n]$  lorsque

$$n|(a - b)$$

ie lorsqu'il existe  $k \in \mathbb{Z}$  tel que  $a = b + kn$ .

## 2 Propriétés

### Propriété 25

$\forall a \in \mathbb{Z}, \exists! r \in [0, n-1], a \equiv r [n]$ .  
 $r$  est le reste de la division euclidienne de  $a$  par  $n$ .  
Il y a donc exactement  $n$  classes d'équivalences :  $\overline{0}, \overline{1}, \dots, \overline{n-1}$ .

### Propriété 26

$$n|k \iff k \equiv 0 [n]$$



### Propriété 27 : Compatibilité de + et ×

Soient  $n \in \mathbb{N}^*$  et  $a, b, c, d \in \mathbb{Z}$  tels que  $a \equiv b [n]$  et  $c \equiv d [n]$ .

alors

$$a + c \equiv b + d [n]$$

et

$$a \times c \equiv b \times d [n].$$

Plus généralement, si  $m \in \mathbb{N}$ ,

$$a^m \equiv b^m [n].$$

### Propriété 28

Soit  $c \neq 0$ .

(i)  $ac \equiv bc [nc] \Rightarrow a \equiv b [n].$

(ii) Si  $c \wedge n = 1$  alors  $ac \equiv bc [n] \Rightarrow a \equiv b [n].$

## 3 Petit théorème de Fermat

### Lemme 1

Soit  $p$  un nombre premier et  $k \in \llbracket 1, p-1 \rrbracket$ . Alors  $p \mid \binom{p}{k}$ .

### Théorème 5 : Petit théorème de Fermat

Soit  $p$  un nombre premier et  $a \in \mathbb{Z}$ .

$$a^p \equiv a [p].$$

En particulier, si  $p \nmid a$ , alors  $a^{p-1} \equiv 1 [p]$ .

## 4 Critères de divisibilité

Si  $a_0, \dots, a_k$  sont les chiffres de  $n$  en base 10,

$$n = a_0 + a_1 \times 10 + \dots + a_k \times 10^k,$$

$$\forall i \in \llbracket 0, k \rrbracket, a_i \in \llbracket 0, 9 \rrbracket.$$

**Divisibilité par 2 :**  $10^i \equiv 0 [2]$  donc

$$2|n \iff 2|a_0 \iff a_0 \in \{0, 2, 4, 6, 8\}$$

**Divisibilité par 3 :**  $10^i \equiv 1 [3]$  donc

$$3|n \iff 3 \mid \sum_{i=0}^k a_i$$

**Divisibilité par 4 :**  $10^i = 10^{i-2} \times 100 \equiv 10^{i-2} \times 0 \equiv 0 [4]$  si  $i \geq 2$  donc

$$4|n \iff 4 \mid \overline{a_1 a_0}^{10}$$

**Divisibilité par 5 :**  $10^i \equiv 0 [5]$  si  $i \geq 1$  donc

$$5|n \iff 5|a_0 \iff a_0 \in \{0, 5\}$$

**Divisibilité par 8 :**  $10^i = 10^{i-3} \times 1000 \equiv 10^{i-3} \times 0 \equiv 0 [8]$  si  $i \geq 3$  donc

$$8|n \iff 8 \mid \overline{a_2 a_1 a_0}^{10}$$

**Divisibilité par 9 :**  $10^i \equiv 1 [9]$  donc

$$9|n \iff 9 \mid \sum_{i=0}^k a_i$$

**Divisibilité par 11 :**  $10^i \equiv -1 [11]$  donc

$$11|n \iff 11 \mid (a_0 - a_1 + a_2 - \dots)$$