

# COURS : ARITHMÉTIQUE

## Table des matières

<b>1 Relation de divisibilité, division euclidienne</b>	
1.1 Relation de divisibilité . . . . .	1
1.2 Congruence, division euclidienne . . . . .	1
<b>2 Pgcd, ppcm</b>	
2.1 Plus grand commun diviseur . . . . .	2
2.2 Algorithme d'Euclide . . . . .	2
2.3 Relation de Bézout . . . . .	3
2.4 Lemme de Gauss . . . . .	3
2.5 Plus petit commun multiple . . . . .	4
<b>3 Nombres premiers</b>	
3.1 Nombres premiers . . . . .	4
3.2 Décomposition en facteurs premiers . . . . .	4
<b>4 Pour briller en société</b>	

## 1 Relation de divisibilité, division euclidienne

### 1.1 Relation de divisibilité

**Définition 1.** Soit  $a, b \in \mathbb{Z}$ . On dit que  $a$  divise  $b$  lorsqu'il existe  $k \in \mathbb{Z}$  tel que  $b = ka$ .

#### Remarques :

- ⇒ Soit  $a, b \in \mathbb{Z}$  tels que  $a|b$ . Alors  $-a|b$ ,  $a|-b$  et  $-a|-b$ . Autrement dit, lorsqu'on parle de divisibilité, le signe n'est pas significatif.
- ⇒ Soit  $a \in \mathbb{Z}$ . Alors  $a|1$  si et seulement si  $a = \pm 1$ .
- ⇒ Soit  $a, b, c \in \mathbb{Z}$ . Si  $ac|bc$  et  $c \neq 0$ , alors  $a|b$

**Proposition 1.** La relation de divisibilité :

- est réflexive :  $\forall a \in \mathbb{Z} \quad a|a$
- est transitive :  $\forall a, b, c \in \mathbb{Z} \quad [a|b \text{ et } b|c] \implies a|c$
- n'est pas antisymétrique. Cependant :

$$\forall a, b \in \mathbb{Z} \quad [a|b \text{ et } b|a] \iff a = \pm b$$

#### Remarques :

- ⇒ La relation de divisibilité n'étant pas antisymétrique sur  $\mathbb{Z}$ , ce n'est pas une relation d'ordre. Cependant, si  $a, b \in \mathbb{N}$ , on a

$$[a|b \text{ et } b|a] \iff a = b$$

En particulier, la relation de divisibilité est une relation d'ordre sur  $\mathbb{N}$ .

- 2** ⇒ Quel que soit  $n \in \mathbb{Z}$ ,  $1|n$  et  $n|0$ . Sur  $\mathbb{N}$ , pour la relation d'ordre de divisibilité,  $\mathbb{N}$  admet donc 1 pour plus petit élément et 0 pour plus grand élément.
- 3** ⇒ Soit  $a, b \in \mathbb{Z}$ . Si  $a|b$  et  $b \neq 0$ , alors  $|a| \leq |b|$ .

**Proposition 2.** Soit  $a, b, c \in \mathbb{Z}$  et  $k_1, k_2 \in \mathbb{Z}$ . Alors :

$$[a|b \text{ et } a|c] \implies a|(k_1b + k_2c)$$

#### Exercices :

- 5** ⇒ Soit  $a, b, c \in \mathbb{Z}$ . Les assertions suivantes sont-elles vraies ?
- 5** — Si  $a$  divise  $b + c$ , alors  $a$  divise  $b$  et  $c$ .
- 6** — Si  $a$  et  $b$  divisent  $c$ , alors  $ab$  divise  $c$ .
- 6** ⇒ Déterminer les entiers  $n \in \mathbb{N}$  tels que  $n|n + 8$ .

### 1.2 Congruence, division euclidienne

**Définition 2.** Soit  $a, b \in \mathbb{Z}$  et  $m \in \mathbb{N}^*$ . On dit que  $a$  est congru à  $b$  modulo  $m$  et on note

$$a \equiv b \pmod{m}$$

lorsque  $m|(a - b)$ , c'est-à-dire lorsqu'il existe  $k \in \mathbb{Z}$  tel que  $a = b + km$ .

#### Remarques :

- ⇒ Si  $m \in \mathbb{N}^*$ , la relation binaire  $\mathcal{R}$  définie sur  $\mathbb{Z}$  par

$$\forall a, b \in \mathbb{Z} \quad a \mathcal{R} b \iff a \equiv b \pmod{m}$$

est une relation d'équivalence.

- ⇒ Soit  $m, n \in \mathbb{N}^*$  et  $a, b \in \mathbb{Z}$ . Alors  $a \equiv b \pmod{m} \iff an \equiv bn \pmod{mn}$ .

**Proposition 3.** Soit  $a_1, a_2, b_1, b_2 \in \mathbb{Z}$  et  $m \in \mathbb{N}^*$  tels que :

$$a_1 \equiv b_1 \pmod{m} \text{ et } a_2 \equiv b_2 \pmod{m}$$

Alors, si  $k_1, k_2 \in \mathbb{Z}$  et  $k \in \mathbb{N}$  :

$$k_1a_1 + k_2a_2 \equiv k_1b_1 + k_2b_2 \pmod{m} \quad a_1a_2 \equiv b_1b_2 \pmod{m} \quad \text{et} \quad a_1^k \equiv b_1^k \pmod{m}$$

## Exercices :

- ⇒ Montrer que pour tout  $n \in \mathbb{N}$ , 11 divise  $3^{n+3} - 4^{4n+2}$ .
- ⇒ Trouver les  $n \in \mathbb{N}$  tels que  $10^n + 5^n + 1$  est un multiple de 3.
- ⇒ Montrer qu'un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3. De même, montrer qu'un entier est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. Enfin, montrer qu'un nombre est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

**Proposition 4.** Soit  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ . Alors il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que :

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

$q$  est appelé quotient de la division euclidienne de  $a$  par  $b$ ,  $r$  son reste.

## Remarques :

- ⇒ Si  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ , le reste de la division euclidienne de  $a$  par  $b$  est l'unique élément  $r$  de  $\llbracket 0, b-1 \rrbracket$  tel que  $a \equiv r \pmod{b}$ .
- ⇒ Si  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}^*$ , on montre qu'il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que  $a = qb + r$  et  $0 \leq r < |b|$ . On peut donc ainsi étendre la définition de la division euclidienne au cas où  $b \in \mathbb{Z}^*$ . Mais en pratique, on effectuera toujours des divisions euclidiennes par des entiers strictement positifs.
- ⇒ Les langages Python et OCaml possèdent tous les deux une division entière et un opérateur « modulo ». Si  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}^*$ , la division entière s'obtient avec `a // b` en Python et avec `a / b` en OCaml. L'opérateur « modulo » s'obtient quant à lui avec `a % b` en Python et `a mod b` en OCaml. Si on note  $q$  la division entière de  $a$  par  $b$  et  $r$  le résultat de l'opérateur modulo, on aura toujours  $a = qb + r$ . Cependant,  $q$  et  $r$  ne sont pas toujours le quotient et le reste de la division euclidienne de  $a$  par  $b$ . En pratique, on ne s'intéressera qu'au cas où  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ , car aucun programmeur sensé ne va tenter de faire une division entière par un nombre  $b$  strictement négatif. Cependant, Python et OCaml n'ont pas le même comportement, même lorsque  $b > 0$ .
  - En Python, si  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}^*$ ,  $q$  et  $r$  sont respectivement le quotient et le reste de la division euclidienne de  $a$  par  $b$ .
  - En OCaml, si  $a \in \mathbb{N}$  et  $b \in \mathbb{N}^*$ ,  $q$  et  $r$  sont respectivement le quotient et le reste de la division euclidienne de  $a$  par  $b$ . Mais, si  $a < 0$  et  $b > 0$ , ce n'est plus le cas. Dans ce cas, le résultat renvoyé par `a / b` est  $-((-a) / b)$ . Par exemple, si  $a = -5$  et  $b = 2$ , alors les quotient et reste de la division euclidienne de  $a$  par  $b$  sont respectivement  $-3$  et  $1$ , mais `a / b` renvoie  $2$  et `a mod b` renvoie  $-1$ .

## Exercice :

- ⇒ Déterminer le reste de la division euclidienne de  $4852^{203}$  par  $5$ .

## 2 Pgcd, ppcm

### 2.1 Plus grand commun diviseur

**Définition 3.** Soit  $a, b \in \mathbb{Z}$ . Il existe un unique entier positif  $p$  tel que :

- $p|a$  et  $p|b$
- $\forall q \in \mathbb{Z} \quad [q|a \text{ et } q|b] \implies q|p$

On l'appelle pgcd (plus grand commun diviseur) de  $a$  et de  $b$  et on le note  $\text{pgcd}(a, b)$  ou  $a \wedge b$ .

## Remarques :

- ⇒ Si  $a, b \in \mathbb{Z}$ , les diviseurs de  $a$  et de  $b$  sont les diviseurs de  $a \wedge b$ .
- ⇒ Soit  $a, b \in \mathbb{N}$ . Pour la relation d'ordre de divisibilité sur  $\mathbb{N}$ , l'ensemble des diviseurs de  $a$  et de  $b$  n'est rien d'autre que l'ensemble des minorants de  $\{a, b\}$ . La définition précédente montre donc que cet ensemble admet un plus grand élément (au sens de la divisibilité) qui est  $a \wedge b$ . Autrement dit, au sens de la divisibilité, l'ensemble  $\{a, b\}$  admet une borne inférieure qui est  $a \wedge b$ .
- ⇒ Soit  $a, b \in \mathbb{N}$ . Si l'un des deux entiers est non nul, le pgcd de  $a$  et de  $b$  est le plus grand (au sens de l'ordre) diviseur commun de  $a$  et  $b$ .

**Proposition 5.** On a :

$$\forall a \in \mathbb{Z} \quad a \wedge 0 = |a|$$

$$\forall a \in \mathbb{Z} \quad a \wedge 1 = 1$$

$$\forall a, b \in \mathbb{Z} \quad a \wedge b = 0 \iff [a = 0 \text{ et } b = 0]$$

**Proposition 6.** On a :

$$\forall a, b \in \mathbb{Z} \quad a \wedge b = b \wedge a$$

$$\forall a, b \in \mathbb{Z} \quad a \wedge b = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b) = |a| \wedge |b|$$

$$\forall a, b, k \in \mathbb{Z} \quad (ka) \wedge (kb) = |k| (a \wedge b)$$

**Définition 4.** Soit  $a_1, \dots, a_n \in \mathbb{Z}$ . Il existe un unique entier positif  $p$  tel que :

- $\forall i \in \llbracket 1, n \rrbracket \quad p|a_i$
- $\forall q \in \mathbb{Z} \quad [\forall i \in \llbracket 1, n \rrbracket \quad q|a_i] \implies q|p$

On l'appelle pgcd (plus grand commun diviseur) de la famille  $(a_1, \dots, a_n)$  et on le note  $\text{pgcd}(a_1, \dots, a_n)$  ou  $a_1 \wedge \dots \wedge a_n$ .

## Remarque :

- ⇒ Le pgcd d'une famille d'entiers  $(a_1, \dots, a_n)$  ne dépend pas de l'ordre de ces derniers.

**Proposition 7.** Soit  $a_1, \dots, a_n \in \mathbb{Z}$  et  $p \in \llbracket 1, n-1 \rrbracket$ . Alors

$$a_1 \wedge \dots \wedge a_n = (a_1 \wedge \dots \wedge a_p) \wedge (a_{p+1} \wedge \dots \wedge a_n)$$

## 2.2 Algorithme d'Euclide

**Proposition 8.** Soit  $a, b, k \in \mathbb{Z}$ . Alors :

$$a \wedge b = a \wedge (b + ka) = (a + kb) \wedge b$$

En particulier, si  $b \in \mathbb{N}^*$  et  $r$  est le reste de la division euclidienne de  $a$  par  $b$ , on a :

$$a \wedge b = b \wedge r$$

Soit  $a, b \in \mathbb{N}$ , pour calculer  $a \wedge b$ , on utilise l'algorithme suivant, appelé **algorithme d'Euclide**.

- On pose  $r_0 = a$  et  $r_1 = b$ .
- Si  $r_1 = 0$ , la réponse est  $r_0$ . Sinon, on effectue la division euclidienne de  $r_0$  par  $r_1$ . Il existe donc  $q_1 \in \mathbb{N}$  et  $r_2 \in \llbracket 0, r_1 - 1 \rrbracket$  tels que  $r_0 = q_1 r_1 + r_2$ .
- Si  $r_2 = 0$ , la réponse est  $r_1$ . Sinon, on effectue la division euclidienne de  $r_1$  par  $r_2$ . Il existe donc  $q_2 \in \mathbb{N}$  et  $r_3 \in \llbracket 0, r_2 - 1 \rrbracket$  tels que  $r_1 = q_2 r_2 + r_3$ .
- Si  $r_3 = 0$ , etc.
- Supposons que  $r_{n+1}$  soit défini. Si  $r_{n+1} = 0$ , la réponse est  $r_n$ . Sinon, on effectue la division euclidienne de  $r_n$  par  $r_{n+1}$ . Il existe donc  $q_{n+1} \in \mathbb{N}$  et  $r_{n+2} \in \llbracket 0, r_{n+1} - 1 \rrbracket$  tels que  $r_n = q_{n+1} r_{n+1} + r_{n+2}$ .

Démontrons la validité de cet algorithme :

- **L'algorithme s'arrête :**  
En effet, si tel n'était pas le cas, on aurait ainsi construit une suite  $(r_n)_{n \in \mathbb{N}}$  strictement décroissante (à partir du rang 1) d'entiers naturels, ce qui n'existe pas.
- **L'algorithme donne la bonne réponse :**  
En effet, comme  $r_n = q_{n+1} r_{n+1} + r_{n+2}$ , on en déduit que

$$\begin{aligned} r_n \wedge r_{n+1} &= (q_{n+1} r_{n+1} + r_{n+2}) \wedge r_{n+1} \\ &= r_{n+2} \wedge r_{n+1} \quad (\text{lemme d'Euclide}) \\ &= r_{n+1} \wedge r_{n+2} \end{aligned}$$

On en déduit facilement par récurrence finie que, pour tout entier  $n$ ,  $r_n \wedge r_{n+1} = r_0 \wedge r_1 (= a \wedge b)$ . Lorsque l'algorithme s'arrête,  $r_{n+1} = 0$  donc  $a \wedge b = r_n \wedge r_{n+1} = r_n \wedge 0 = r_n$ . L'algorithme donne donc la bonne réponse.

**Remarque :**

- ⇨ Remarquons qu'il est inutile de supposer que  $b$  soit inférieur à  $a$  pour que l'algorithme fonctionne. En effet, si  $a < b$ , alors la division euclidienne de  $a$  par  $b$  donne  $a = 0 \cdot b + a$  donc  $r_2 = a$ . On a ainsi  $r_1 = b$  et  $r_2 = a$ . La première étape de l'algorithme échange donc  $a$  et  $b$ .

**Exercices :**

- ⇨ Calculer  $105 \wedge 147$ .
- ⇨ Soit  $n \in \mathbb{N}$ . Calculer  $(3n + 1) \wedge (2n)$ , puis  $(n^4 - 1) \wedge (n^6 - 1)$ .
- ⇨ Soit  $(F_n)$  la suite, appelée suite de Fibonacci, définie par

$$F_0 = 0 \quad F_1 = 1 \quad \text{et} \quad \forall n \in \mathbb{N} \quad F_{n+2} = F_{n+1} + F_n$$

Montrer que pour tout  $n \in \mathbb{N}$ ,  $F_n \wedge F_{n+1} = 1$ .

## 2.3 Relation de Bézout

**Proposition 9.** Si  $a, b \in \mathbb{Z}$ , il existe  $u, v \in \mathbb{Z}$  tels que :

$$ua + vb = a \wedge b$$

**Exercices :**

- ⇨ Trouver une relation de Bézout pour 105 et 147.
- ⇨ Soit  $n, m \in \mathbb{N}^*$ . Montrer que

$$\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$$

**Définition 5.** Soit  $a, b \in \mathbb{Z}$ . On dit que  $a$  et  $b$  sont premiers entre eux lorsque  $a \wedge b = 1$ .

**Remarque :**

- ⇨ Soit  $a, b \in \mathbb{Z}$ . Puisque  $a \wedge b$  est un diviseur commun à  $a$  et  $b$ , il existe  $a', b' \in \mathbb{Z}$  tels que  $a = a'(a \wedge b)$  et  $b = b'(a \wedge b)$ . Si  $(a, b) \neq (0, 0)$ , alors  $a'$  et  $b'$  sont premiers entre eux.

**Exercice :**

- ⇨ Soit  $a, b \in \mathbb{Z}$  deux entiers premiers entre eux. Calculer  $(a - b) \wedge (a + b)$ .

**Proposition 10.** Soit  $a, b \in \mathbb{Z}$ . Alors  $a$  et  $b$  sont premiers entre eux si et seulement si il existe  $u, v \in \mathbb{Z}$  tels que :

$$ua + vb = 1$$

**Exercice :**

- ⇨ Résoudre sur  $\mathbb{Z}$  l'équation  $2n \equiv 7 \pmod{9}$ .

**Proposition 11.**

- Soit  $a, b, c \in \mathbb{Z}$  tels que  $a \wedge b = 1$  et  $a \wedge c = 1$ . Alors  $a \wedge (bc) = 1$ .
- Plus généralement, si  $a \in \mathbb{Z}$  est premier avec chaque élément d'une famille d'entiers  $b_1, \dots, b_n \in \mathbb{Z}$ , alors  $a$  est premier avec leur produit.
- Soit  $a, b \in \mathbb{Z}$  deux entiers premiers entre eux et  $m, n \in \mathbb{N}$ . Alors  $a^m \wedge b^n = 1$ .

**Exercice :**

- ⇨ Soit  $a, b \in \mathbb{Z}$  deux entiers premiers entre eux. Montrer que  $a + b$  et  $ab$  sont premiers entre eux.

**Définition 6.** Soit  $a_1, \dots, a_n \in \mathbb{K}[X]$ .

- On dit que  $a_1, \dots, a_n$  sont deux à deux premiers entre eux lorsque

$$\forall i, j \in \llbracket 1, n \rrbracket \quad i \neq j \implies a_i \wedge a_j = 1$$

- On dit que  $a_1, \dots, a_n$  sont premiers entre eux dans leur ensemble lorsque

$$a_1 \wedge \dots \wedge a_n = 1$$

Remarques :

⇒ Si les entiers  $a_1, \dots, a_n$  sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. Cependant, la réciproque est fausse. Par exemple,  $a_1 = 2$ ,  $a_2 = 3$  et  $a_3 = 6$  sont premiers entre eux dans leur ensemble mais ne sont pas deux à deux premiers entre eux.

**Proposition 12.** Soit  $a_1, \dots, a_n \in \mathbb{Z}$ . Alors  $a_1, \dots, a_n$  sont premiers entre eux dans leur ensemble si et seulement si il existe  $u_1, \dots, u_n \in \mathbb{Z}$  tels que

$$u_1 a_1 + \dots + u_n a_n = 1$$

Exercice :

⇒ Trouver les solutions entières de l'équation :

$$a^2 + b^2 = 3c^2$$

2.4 Lemme de Gauss

**Théorème 1.** Soit  $a, b, c \in \mathbb{Z}$ . Alors :

$$[a|bc \quad \text{et} \quad a \wedge b = 1] \implies a|c$$

Exercices :

- ⇒ Résoudre l'équation  $105u + 147v = 21$  dans  $\mathbb{Z}$ .
- ⇒ Trois comètes passent régulièrement dans le ciel Shadok. La première, la comète Gabu, passe tous les 10 jours depuis le deuxième jour d'existence de leur planète. La seconde, la comète Zomeu passe tous les 21 jours depuis le cinquième jour d'existence de leur planète. Enfin, la comète Gibi passe tous les 6 jours depuis le troisième jour d'existence de leur planète. Est-il possible d'admirer les comètes Gabu et Zomeu le même jour dans le ciel Shadok ? Si oui, lesquels ? Même question pour les comètes Gabu et Gibi.

Remarque :

⇒ Soit  $a, b, c \in \mathbb{Z}$  tels que  $(a, b) \neq (0, 0)$ . On cherche les solutions entières de l'équation

$$(E) \quad ua + vb = c$$

- Si  $a \wedge b$  ne divise pas  $c$ , il n'y a aucune solution.
- Sinon, il existe  $c' \in \mathbb{Z}$  tel que  $c = c'(a \wedge b)$ . En utilisant l'algorithme d'Euclide, on trouve  $u'_0, v'_0 \in \mathbb{Z}$  tels que  $u'_0 a + v'_0 b = a \wedge b$ . On a donc  $(c' u'_0) a + (c' v'_0) b = c$  ce qui nous donne une solution particulière à l'équation (E). Soit  $a', b' \in \mathbb{Z}$  tels que  $a = a'(a \wedge b)$  et  $b = b'(a \wedge b)$ . Alors  $a'$  et  $b'$  sont premiers entre eux. On a alors :

$$\begin{aligned} \forall u, v \in \mathbb{Z} \quad ua + vb = c &\iff ua + vb = (c' u'_0) a + (c' v'_0) b \\ &\iff (u - c' u'_0) a = (c' v'_0 - v) b \\ &\iff (u - c' u'_0) a' = (c' v'_0 - v) b' \quad (E') \end{aligned}$$

Si le couple  $(u, v)$  est solution de  $(E')$ , on en déduit que  $b'$  divise  $(u - c' u'_0) a'$ . Or  $a'$  et  $b'$  sont premiers entre eux, donc d'après le lemme de Gauss,  $b'$  divise  $u - c' u'_0$ . Il

existe donc  $k \in \mathbb{Z}$  tel que  $u = c' u'_0 + k b'$ . En reportant cette égalité dans  $(E')$ , on trouve  $v = c' v'_0 - k a'$ . Réciproquement, on vérifie que de tels  $u$  et  $v$  sont bien solution de  $(E')$ . L'ensemble des solutions de  $(E)$  est donc

$$\mathcal{S} = \{(c' u'_0 + k b', c' v'_0 - k a') : k \in \mathbb{Z}\}$$

**Proposition 13.** Soit  $r \in \mathbb{Q}$ .

— Alors, il existe un unique couple  $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$  tel que :

$$r = \frac{a}{b} \quad \text{et} \quad a \wedge b = 1$$

Cette écriture est appelée forme irréductible de  $r$ .

— De plus, si  $p \in \mathbb{Z}$  et  $q \in \mathbb{Z}^*$ ,  $r = p/q$  si et seulement si il existe  $k \in \mathbb{Z}^*$  tel que  $p = k a$  et  $q = k b$ .

Remarque :

⇒ Si  $P(x) = a_n x^n + \dots + a_1 x + a_0$  est un polynôme à coefficients entiers et  $r = p/q$  est une racine rationnelle de  $P$ , mise sous forme irréductible, alors  $q|a_n$  et  $p|a_0$ . On a ainsi un moyen de trouver toutes les racines rationnelles d'un polynôme à coefficients entiers.

Exercices :

- ⇒ Rechercher les racines rationnelles de  $P(x) = 2x^3 + x^2 + x - 1$ . En déduire une factorisation de ce polynôme.
- ⇒ Soit  $n \in \mathbb{N}$ . Montrer que  $\sqrt{n}$  est soit entier, soit irrationnel.
- ⇒ Déterminer les triplets  $(a, b, c) \in \mathbb{N}^{*3}$  tels que

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$$

**Proposition 14.**

- Soit  $a, b, c \in \mathbb{Z}$ . On suppose que  $a|c$ ,  $b|c$  et  $a \wedge b = 1$ . Alors  $ab|c$ .
- Plus généralement si  $a \in \mathbb{Z}$  est divisé par chaque élément d'une famille  $b_1, \dots, b_n \in \mathbb{Z}$  d'entiers deux à deux premiers entre eux, alors il est divisé par leur produit.

2.5 Plus petit commun multiple

**Définition 7.** Soit  $a, b \in \mathbb{Z}$ . Il existe un unique entier positif  $p$  tel que :

- $a|p$  et  $b|p$
- $\forall q \in \mathbb{Z} \quad [a|q \quad \text{et} \quad b|q] \implies p|q$

On l'appelle ppcm (plus petit commun multiple) de  $a$  et de  $b$  et on le note  $\text{ppcm}(a, b)$  ou  $a \vee b$ .

**Proposition 15.** On a :

$$\begin{aligned} \forall a \in \mathbb{Z} \quad a \vee 0 &= 0 \\ \forall a \in \mathbb{Z} \quad a \vee 1 &= |a| \\ \forall a, b \in \mathbb{Z} \quad a \vee b = 0 &\iff [a = 0 \quad \text{ou} \quad b = 0] \end{aligned}$$

**Proposition 16.** On a :

$$\begin{aligned}\forall a, b \in \mathbb{Z} \quad a \vee b &= b \vee a \\ \forall a, b \in \mathbb{Z} \quad a \vee b &= (-a) \vee b = a \vee (-b) = (-a) \vee (-b) = |a| \vee |b| \\ \forall a, b, k \in \mathbb{Z} \quad (ka) \vee (kb) &= |k| (a \vee b)\end{aligned}$$

**Proposition 17.** Soit  $a, b \in \mathbb{Z}$ .

— Si  $a \wedge b = 1$ , alors :

$$a \vee b = |ab|$$

— De manière générale :

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

**Exercice :**

⇒ Résoudre dans  $\mathbb{Z}$  l'équation  $a \vee b = a + b - 1$ .

## 3 Nombres premiers

### 3.1 Nombres premiers

**Définition 8.** On dit qu'un entier  $p \geq 2$  est premier lorsque ses seuls diviseurs positifs sont 1 et  $p$ . On note  $\mathcal{P}$  l'ensemble des nombres premiers.

**Remarque :**

⇒ Soit  $p$  un entier supérieur ou égal à 2. Pour montrer que  $p$  est premier, il suffit de montrer que  $k$  ne divise pas  $p$  pour tout entier  $k$  compris (au sens large) entre 2 et  $\sqrt{p}$ .

**Exercices :**

⇒ Pour tout  $n \in \mathbb{N}$ , on définit le  $n$ -ième nombre de Mersenne comme  $M_n = 2^n - 1$ . Montrer que si  $M_n$  est premier, alors  $n$  est premier. La réciproque est-elle vraie ?

⇒ Soit  $p$  un nombre premier supérieur ou égal à 5. Montrer que  $24|p^2 - 1$ .

⇒ Soit  $n \in \mathbb{N}^*$ . Montrer qu'il existe  $n$  nombres consécutifs non premiers

**Proposition 18.** Soit  $p$  un nombre premier et  $n \in \mathbb{Z}$ . Alors  $p|n$  ou  $p \wedge n = 1$ .

**Exercice :**

⇒ Soit  $p$  un nombre premier et  $k \in \llbracket 1, p-1 \rrbracket$ . Montrer que  $p$  divise  $\binom{p}{k}$ .

**Proposition 19.** Soit  $p$  un nombre premier et  $m \in \mathbb{Z}$  un entier qui n'est pas un multiple de  $p$ . Alors

$$m^{p-1} \equiv 1 [p]$$

**Remarque :**

⇒ Cette proposition porte le nom de « petit théorème de Fermat ».

**Proposition 20.** Soit  $p$  un nombre premier.

— Si  $a, b \in \mathbb{Z}$  :

$$p|ab \iff [p|a \text{ ou } p|b]$$

— Plus généralement,  $p$  divise un produit si et seulement si il divise un de ses facteurs.

**Proposition 21.** Tout entier supérieur ou égal à 2 admet un diviseur premier.

**Remarque :**

⇒ Soit  $n \geq 2$ . On cherche l'ensemble des nombres premiers inférieurs ou égaux à  $n$ . Pour cela, on utilise le crible d'Ératosthène :

— On forme une table avec tous les entiers compris entre 2 et  $n$ .

— On raye tous les multiples de 2.

— On cherche le plus petit entier qui n'est pas rayé : c'est 3 et il est premier. On raye alors tous les multiples de 3.

— On cherche ensuite le plus petit entier qui n'est pas rayé (c'est 5). Il est forcément premier car on a trouvé tous les nombres premiers strictement inférieurs à celui-ci et on a rayé tous leurs multiples. On raye alors tous les multiples de 5.

— On continue ainsi jusqu'à ce qu'on trouve un nombre premier dont le carré est strictement supérieur à  $n$ . Les nombres qui ne sont pas rayés sont les nombres premiers compris entre 2 et  $n$ .

Par exemple, si on cherche les nombres premiers inférieurs à 99, on trouve :

		2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

**Proposition 22.** L'ensemble  $\mathcal{P}$  des nombres premiers est infini.

**Remarque :**

⇒ Cette démonstration est due à Euclide (325–265 avant J.C.).

3.2 Décomposition en facteurs premiers

**Proposition 23.** Soit  $n \in \mathbb{Z}^*$ . Alors, il existe  $u \in \{-1, 1\}$ ,  $p_1, \dots, p_r$  des nombres premiers deux à deux distincts et  $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$  tels que :

$$n = u \prod_{k=1}^r p_k^{\alpha_k}$$

De plus, à permutation près des  $p_k$ , cette décomposition est unique.

**Définition 9.** Lorsque  $n \in \mathbb{Z}^*$  et  $p$  est nombre premier, on appelle valuation de  $p$  relativement à  $n$  et on note  $\text{Val}_p(n)$  le plus grand  $\alpha \in \mathbb{N}$  tel que  $p^\alpha | n$ .

Remarques :

- ⇒ Si  $n \in \mathbb{Z}^*$ , il n'existe qu'un nombre fini de nombres premiers  $p$  tels que  $\text{Val}_p(n) \neq 0$ . Ce sont les nombres premiers apparaissant dans la décomposition de  $n$  en facteurs premiers.
- ⇒ Si  $u \in \{1, -1\}$  est le signe de  $n$ , la décomposition de  $n$  en facteurs premiers s'écrit

$$n = u \prod_{p \in \mathcal{P}} p^{\text{Val}_p(n)}$$

**Proposition 24.** Soit  $n_1, n_2 \in \mathbb{Z}^*$ . Alors

- $n_1 | n_2$  si et seulement si

$$\forall p \in \mathcal{P} \quad \text{Val}_p(n_1) \leq \text{Val}_p(n_2)$$

- Le pgcd et le ppcm de  $n_1$  et  $n_2$  est donné par les relations

$$\begin{aligned} \forall p \in \mathcal{P} \quad \text{Val}_p(n_1 \wedge n_2) &= \min(\text{Val}_p(n_1), \text{Val}_p(n_2)) \\ \text{Val}_p(n_1 \vee n_2) &= \max(\text{Val}_p(n_1), \text{Val}_p(n_2)) \end{aligned}$$

Exercices :

- ⇒ Soient  $a, b \in \mathbb{N}$  tels que  $a \wedge b = 1$  et  $ab$  est un carré parfait ( $ab$  est le carré d'un entier). Montrer que  $a$  et  $b$  sont des carrés parfaits.
- ⇒ Si  $n \in \mathbb{N}$  et  $p$  est un nombre premier, montrer que

$$\text{Val}_p(n!) = \sum_{k=1}^{+\infty} E\left(\frac{n}{p^k}\right)$$

En déduire le nombre de zéros à la fin de l'écriture décimale de 2007!.

4 Pour briller en société

— Postulat de Bertrand :

Le postulat de Bertrand affirme que si  $n \in \mathbb{N}^*$ , alors il existe un nombre premier  $p$  tel que  $n < p \leq 2n$ . Cette conjecture fut énoncée par Joseph Bertrand en 1845 et démontrée par Tchebychev en 1848. Bien que ce résultat est aujourd'hui un théorème, le nom de postulat lui est resté associé.

— Théorème de la progression arithmétique :

Ce théorème affirme que si  $a$  et  $b$  sont premiers entre eux, alors il existe une infinité de nombres premiers  $p$  tels que  $p \equiv a \pmod{b}$ . On le doit à Dirichlet (1805–1859).

— Théorème des nombres premiers :

Pour tout  $n \in \mathbb{N}^*$ , on définit  $\pi_n$  comme le cardinal de l'ensemble des nombres premiers inférieurs ou égaux à  $n$ . Le théorème des nombres premiers affirme que

$$\pi_n \underset{n \rightarrow +\infty}{\sim} \frac{n}{\ln n}$$

Autrement dit, si l'on choisit au hasard un entier entre 1 et  $n$ , la probabilité pour qu'il soit premier est de l'ordre de  $1/(\ln n)$ . Remarquons que cette quantité tend vers 0 lorsque  $n$  tend vers  $+\infty$ , c'est-à-dire que les nombres premiers deviennent « de plus en plus rares » lorsqu'on avance parmi les entiers naturels. Ce théorème fut conjecturé de manière indépendante par Gauss et Legendre vers 1800. Il fut démontré par Hadamard et de la Vallée Poussin en 1896.

— Grand (ou dernier) théorème de Fermat :

Il s'énonce ainsi :

$$\text{« Pour tout entier } n \geq 3, \text{ il n'existe pas de triplet } (a, b, c) \in \mathbb{N}^{*3} \text{ tel que } a^n + b^n = c^n. \text{ »}$$

Contrairement au petit théorème, il s'agit d'un résultat extrêmement difficile, dont Fermat n'a pas publié de démonstration. Fermat n'a même jamais affirmé publiquement l'avoir démontré. Il a cependant écrit dans une marge de livre II des Oeuvres de Diophante : « J'ai découvert une démonstration merveilleuse, mais je n'ai pas la place de la mettre dans la marge ». Le livre et cette annotation ont été publiés après sa mort, par son fils. De nombreux mathématiciens ont tenté de le prouver et sont arrivés à des résultats partiels, notamment :

- Fermat (1601–1665) le démontre pour  $n = 4$ .
- Euler (1707–1783) le démontre pour  $n = 3$ .
- Sophie Germain (1776–1831) apporte un résultat majeur ouvrant la porte à la démonstration du cas  $n = 5$ , démontré quelques années plus tard par Legendre (1752–1833).
- Kummer (1810–1893) le prouve pour tout  $n \in \llbracket 3, 99 \rrbracket$ .

En 1993, Andrew Wiles prouve un résultat sur les courbes elliptiques, résultat qui admet le grand théorème de Fermat pour corollaire. La démonstration initiale possède une erreur mais elle sera vite réparée. La conjecture de Fermat devient alors le théorème de Fermat-Wiles.

— Nombres premiers jumeaux :

On dit qu'un couple  $(p, q) \in \mathbb{N}$  est un couple de nombres premiers jumeaux lorsque  $q = p + 2$ . Par exemple (3, 5), (5, 7), (11, 13) sont des couples de nombres premiers jumeaux. Bien que l'on pense que cette conjecture soit vraie, elle n'a jamais été démontrée. Depuis janvier 2016, le plus grand couple de nombres premiers jumeaux connu est  $2\,996\,863\,034\,895 \times 2^{1\,290\,000} \pm 1$ .

— Conjecture de Goldbach :

En 1742, Goldbach (1690–1764) et Euler (1707–1783) énoncent :

$$\text{« Tout entier pair supérieur ou égal à 4 peut s'écrire comme la somme de deux nombres premiers. »}$$

On pense que cette conjecture est vraie, mais aucune démonstration n'a jamais été faite.