

# Maths : Arithmetic

## Contents

<b>1</b>	<b>Divisibilité</b>	<b>2</b>
1.1	Définitions . . . . .	2
1.2	Propriétés . . . . .	2
1.3	Division euclidienne . . . . .	2
<b>2</b>	<b>Congruences</b>	<b>2</b>
2.1	Définition . . . . .	2
2.2	Propriétés . . . . .	2
<b>3</b>	<b>PGCD</b>	<b>3</b>
3.1	Définition . . . . .	3
3.2	Propriétés . . . . .	3
3.3	Algorithme d'Euclide . . . . .	3
<b>4</b>	<b>PPCM</b>	<b>4</b>
4.1	Définition . . . . .	4
4.2	Propriétés . . . . .	4
<b>5</b>	<b>Bézout, Gauss</b>	<b>4</b>
5.1	Relation de Bézout . . . . .	4
5.2	Théorème de Bézout . . . . .	4
5.3	Lemme de Gauss . . . . .	4
<b>6</b>	<b>Nombres premiers</b>	<b>4</b>
6.1	Définition . . . . .	4
6.2	Propriétés . . . . .	5
6.3	Petit théorème de Fermat . . . . .	5

# 1 Divisibilité

## 1.1 Définitions

Divisibilité :  $\forall a, b \in \mathbb{Z}, a|b \Leftrightarrow \exists k \in \mathbb{Z} \mid b = ak$

Ensemble des diviseurs :  $\forall a \in \mathbb{Z}, \mathcal{D}(a) = \{x \in \mathbb{Z}, x|a\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \mid a = kx\}$

Multiples :  $\forall a \in \mathbb{Z}, a\mathbb{Z} = \{na, n \in \mathbb{Z}\}$

## 1.2 Propriétés

$$\forall (a, b) \in \mathbb{Z}^2, \begin{cases} a|b \\ b|a \end{cases} \Leftrightarrow |a| = |b|$$

$$\forall (a, b, c) \in \mathbb{Z}^3, \begin{cases} c|a \\ c|b \end{cases} \Rightarrow \forall (u, v) \in \mathbb{Z}, c|(au + bv)$$

$$\forall (a, b, c) \in \mathbb{Z}^3, \begin{cases} c \neq 0 \\ ac|bc \end{cases} \Rightarrow a|b$$

## 1.3 Division euclidienne

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, \exists!(q, r) \in \mathbb{Z} \times \mathbb{N} \mid \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

# 2 Congruences

## 2.1 Définition

$$\forall (a, b, n) \in \mathbb{Z}^3, a \equiv b [n] \Leftrightarrow \exists k \in \mathbb{Z} \mid a - b = kn$$

## 2.2 Propriétés

$$\forall a, a', b, b', \alpha \in \mathbb{Z} \mid \begin{cases} a \equiv b [\alpha] \\ a' \equiv b' [\alpha] \end{cases}, \text{ on a :}$$

$$a + a' \equiv b + b' [\alpha]$$

$$aa' \equiv bb' [\alpha]$$



### 3 PGCD

#### 3.1 Définition

$$\forall (a, b) \in \mathbb{N}^2, \text{ avec } a \neq 0 \text{ ou } b \neq 0, \quad a \wedge b = \max(\mathcal{D}(a) \cap \mathcal{D}(b))$$

$$\forall (a, b) \in \mathbb{Z}^2, \quad a \wedge b = |a| \wedge |b|$$

#### 3.2 Propriétés

$$\forall (a, b) \in \mathbb{N}^* \times \mathbb{N}, \quad a|b \Leftrightarrow a \wedge b = a$$

$$\forall (a, b, q, r) \in \mathbb{N}^4 \mid a = bq + r, \text{ on a :}$$

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(r)$$

$$\text{si } a \neq 0 \text{ ou } b \neq 0, \quad a \wedge b = b \wedge r$$

$$\forall (a, b, d) \in \mathbb{N}^2 \times \mathbb{N}^* \mid a \neq 0 \text{ ou } b \neq 0, \text{ on a :}$$

$$d = a \wedge b \Leftrightarrow \mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b)$$

$$\Leftrightarrow \begin{cases} d|a \\ d|b \\ \forall n \in \mathbb{N}, \begin{cases} n|a \\ n|b \end{cases} \Rightarrow n|d \end{cases}$$

$$\forall (a, b) \in \mathbb{Z}^2, \exists (a_1, b_1) \in \mathbb{Z}^2, \begin{cases} a_1 \wedge b_1 = 1 \\ a = a_1(a \wedge b) \\ b = b_1(a \wedge b) \end{cases}$$

#### 3.3 Algorithme d'Euclide

Soient  $a, b \in \mathbb{N}^*$ . On construit tant que possible une suite  $(r_n)_{n \geq -1} \subset \mathbb{N}$  par récurrence :

- On pose  $r_{-1} = a$  et  $r_0 = b$  ;
- Si  $r_n \neq 0$ , on pose  $r_{n+1} \equiv r_{n-1} [r_n]$ , avec  $0 \leq r_{n+1} < r_n$  ;
- Sinon,  $r_{n+1}$  n'est pas défini.

Alors :

- $\exists p \in \mathbb{N} \mid \forall n \leq p, r_n \neq 0$  et est bien défini, et  $r_{p+1} = 0$  ;
- $r_p = a \wedge b$ .

## 4 PPCM

### 4.1 Définition

$$\forall (a, b) \in \mathbb{N}^*, a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*)$$

$$\forall (a, b) \in (\mathbb{Z}^*)^2, a \vee b = |a| \vee |b|$$

### 4.2 Propriétés

$\forall a, b, m \in \mathbb{N}^*$ , on a :

$$\begin{aligned} m = a \vee b &\Leftrightarrow m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \\ &\Leftrightarrow \begin{cases} a|m \\ b|m \\ \forall n \in \mathbb{N}, \begin{cases} a|n \\ b|n \end{cases} \Rightarrow m|n \end{cases} \end{aligned}$$

$$\forall (a, b) \in \mathbb{Z}^2 \mid a \wedge b = 1, a \vee b = |ab|$$

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

## 5 Bézout, Gauss

### 5.1 Relation de Bézout

$$\forall (a, b) \in \mathbb{Z}^2, \exists (u, v) \in \mathbb{Z}^2 \mid au + bv = a \wedge b$$

### 5.2 Théorème de Bézout

$$\forall (a, b) \in \mathbb{Z}^2, a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2 \mid au + bv = 1$$

### 5.3 Lemme de Gauss

$$\forall (a, b, c) \in \mathbb{Z}^3, \begin{cases} a|bc \\ a \wedge b = 1 \end{cases} \Rightarrow a|c$$

## 6 Nombres premiers

### 6.1 Définition

$$\forall p \in \mathbb{N}^*, p \in \mathbb{P} \Leftrightarrow \exists! (a, b) \in \mathbb{N}^2, a \neq b \mid p = ab \text{ ou } p = ba.$$



Un entier naturel est premier si et seulement si il admet exactement deux diviseurs entiers distincts (qui sont alors 1 et lui même).

## 6.2 Propriétés

$\forall p \in \mathbb{P}$ , on a :

$$\forall k \in \llbracket 1 ; p-1 \rrbracket, p \mid \binom{p}{k}$$

$$\forall (a, b, n) \in \mathbb{Z}^2 \times \mathbb{N}, (a+b)^n \equiv a+b \pmod{p}$$

$\forall (a, b, c) \in \mathbb{Z}^3$ , on a :

$$a \wedge bc = 1 \Leftrightarrow \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases}$$

$$\begin{cases} a|c \\ b|c \\ a \wedge b = 1 \end{cases} \Rightarrow ab|c$$

## 6.3 Petit théorème de Fermat

$\forall (p, a) \in \mathbb{P} \times \mathbb{Z}, a^p \equiv a \pmod{p}$

Et si  $a \wedge p = 1$ , alors  $a^{p-1} \equiv 1 \pmod{p}$