

Arithmétique dans \mathbb{Z}

I) Division dans \mathbb{Z}

1) Relation de divisibilité

- **Définition** : Soit $a, b \in \mathbb{Z}$. On dit que a divise b , a est un diviseur de b ou que b est un multiple de a lorsqu'il existe un entier relatif k tel que $b = ka$. On le note $a \mid b$.
- **Théorème** : Soit $a, b, c \in \mathbb{Z}$.
 - 1) La relation divise est réflexive et transitive mais elle n'est pas antisymétrique dans \mathbb{Z} . (mais elle l'est dans \mathbb{N})

$$2) \quad \forall (u, v) \in \mathbb{Z}^2, (a \mid b \text{ et } a \mid c) \Rightarrow a \mid ub + vc$$

$$3) \quad \begin{array}{l} \text{Si } a \mid b \text{ et } c \mid d \Rightarrow ac \mid bd \\ \forall k \in \mathbb{N}, a \mid b \Rightarrow a^k \mid b^k \end{array}$$

$$4) \quad \text{Si } d \neq 0 \text{ alors } a \mid b \Leftrightarrow ad \mid bd$$

2) Relation de congruence

- **Définition** : On dit que a est congru à b modulo n lorsque n divise $(b - a)$, c'est-à-dire s'il existe un k relatif tel que $b = a + kn$. On le note $a \equiv b[n]$ ou $a \equiv b \pmod{n}$.
- **Théorème** : Soit $a, b, a', b' \in \mathbb{Z}$ et $m, n \in \mathbb{N}^*$
 - 1) La relation « être congru à » est une relation d'équivalence, c'est-à-dire qu'elle est réflexive, symétrique et transitive.

$$2) \boxed{\text{Si } a \equiv b[n] \text{ et } a' \equiv b'[n] \text{ alors } a + a' \equiv b + b'[n]}$$

$$3) \boxed{\text{Si } a \equiv b[n] \text{ et } a' \equiv b'[n] \text{ alors } aa' \equiv bb'[n]}$$

$$4) \boxed{a \equiv b[n] \Leftrightarrow am \equiv bm[nm]}$$

3) Division euclidienne

- **Théorème** : Soit $a \in \mathbb{Z}$ et b un entier non nul. Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

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

II) Diviseurs et multiples communs

- **Définition** : Soit $a, b \in \mathbb{Z}$. On dit que d est un diviseur commun de a et b lorsque $d \mid a$ et $d \mid b$. On dit que m est un multiple commun de a et b lorsque $a \mid m$ et $b \mid m$.

1) Plus Grand Diviseur Commun (PGCD)

- **Définition** : On appelle PGCD de deux entiers relatifs a et b tout nombre entier relatif d vérifiant :
 - 1) d est un diviseur commun de a et b .
 - 2) pour tout diviseur commun y de a et b , $y \mid d$.
- **Lemme** : Soit $a, b \in \mathbb{Z}$ et $a = bq + r$ la division euclidienne de a par b alors :
 - 1) Si a et b possède un PGCD y alors y est aussi PGCD de b et de r .
 - 2) Si b et r possède un PGCD y alors y est aussi PGCD de a et b .

- **Théorème** : Soit $a, b \in \mathbb{Z}$. Il existe un unique PGCD positif de a et b noté $\text{pgcd}(a, b)$. On l'appellera le PGCD de a et b .
- **Théorème** : Soit $a, b \in \mathbb{Z}$.

$$1) \quad \forall k \in \mathbb{Z}, \text{pgcd}(ka, kb) = |k| \text{pgcd}(a, b)$$

$$2) \quad \forall d \in \mathbb{Z}^*, \text{ si } d \mid a \text{ et } d \mid b \text{ alors } \text{pgcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{pgcd}(a, b)}{|d|}$$

- **Théorème** : Soit $a, b \in \mathbb{Z}$. Alors il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = \text{pgcd}(a, b)$$

Un tel couple n'est pas unique et est appelé couple de coefficient de Bézout.

2) Nombre premier entre eux

- **Définition** : Soit $a, b \in \mathbb{Z}$.
On dit que a et b sont premiers entre eux lorsque $\text{pgcd}(a, b) = 1$.
- **Théorème de Bézout** : Soit $a, b \in \mathbb{Z}$ alors a et b sont premiers entre eux si et seulement si $au + bv = 1$.

$$a \text{ et } b \text{ premiers entre eux} \Leftrightarrow au + bv = 1$$

- **Théorème de Gauss** : Soit $a, b, c \in \mathbb{Z}$.
Si $a \mid bc$ et si $\text{pgcd}(a, b) = 1$ alors $a \mid c$.

$$\begin{cases} a \mid bc \\ \text{pgcd}(a, b) = 1 \end{cases} \Rightarrow a \mid c$$

3) Plus Petit Multiple Commun (PPCM)

- **Définition** : On appelle PPCM de deux entiers relatifs a et b tout nombre entier relatif m vérifiant :
 - 1) m est un multiple commun de a et b .
 - 2) pour tout y : ($a \mid y$ et $b \mid y$) $\rightarrow m \mid y$
- **Théorème** : Soit $a, b \in \mathbb{Z}$ alors il existe un unique PPCM de a et b positif noté $\text{ppcm}(a, b)$. On l'appellera le PPCM de a et b .

$$\text{Et, } |ab| = \text{pgcd}(a, b) \times \text{ppcm}(a, b)$$

- **Théorème** : Soit $a, b \in \mathbb{Z}$.

$$1) \forall k \in \mathbb{Z}, \text{ppcm}(ka, kb) = |k| \text{ppcm}(a, b)$$

$$2) \forall d \in \mathbb{Z}^*, \text{ si } d \mid a \text{ et } d \mid b \text{ alors } \text{ppcm}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{ppcm}(a, b)}{|d|}$$

III) Nombres premiers

- **Définition** : Soit p un entier différent de 1. On dit que p est premier si ses seuls diviseurs sont 1 et p .

Attention : 1 n'est pas premier !

- **Théorème** : Soit r un entier non nul, (p_1, \dots, p_r) une famille de nombres premiers distincts et (a_1, \dots, a_r) des entiers non nuls alors tout diviseur premier de

$$\prod_{i=1}^r p_i^{a_i} \text{ est l'un des } P_i.$$

- **Théorème** : Soit $n > 1$ un entier.
Il existe un unique r entier non nul, une unique famille $(p_i)_{0 < i < r}$ d'entiers premiers vérifiant $p_1 < p_2 < \dots < p_r$ et une unique famille $(a_i)_{0 < i < r}$ d'entiers naturels non nuls tels que :

$$n = \prod_{i=1}^r p_i^{a_i}$$

- **Théorème** : L'ensemble P des nombres premiers est infini !
- **Théorème** : Soit a, b deux entiers non nuls et les uniques familles presque nulles $(u_p)_{p \text{ premier}}$ et $(v_p)_{p \text{ premier}}$ telles que :

$$a = \prod_{p \in P} p^{u_p} \quad \text{et} \quad b = \prod_{p \in P} p^{v_p} . \text{ Alors :}$$

$$\text{pgcd}(a, b) = \prod_{p \in P} p^{\min(u_p, v_p)} \quad \text{et} \quad \text{ppcm}(a, b) = \prod_{p \in P} p^{\max(u_p, v_p)}$$