Chapitre 12 : Arithmétique dans $\mathbb{Z}$

I. Division euclidienne, diviseurs, multiples

Définition I.1. Soit $a, b \in \mathbb{Z}$. On dit que b **divise** a et on note $b \mid a$ s'il existe $k \in \mathbb{Z}$ tel que $a = bk$.
Alors, b est un **diviseur** de a et a un **multiple** de a.

Proposition I.1. *Soient $a, b, c, d \in \mathbb{Z}$. On a :*

- $a \mid a$
- $a \mid b$ *et* $b \mid c \Rightarrow a \mid c$
- $a \mid b$ *et* $b \mid a \iff a = \pm b$
- $a \mid b \Rightarrow a \mid bc$
- $a \mid b$ *et* $a \mid c \Rightarrow a \mid b + c$
- $a \mid c$ *et* $b \mid d \Rightarrow ab \mid cd$.

Si $a \neq 0$ et $b \mid a$ alors $|b| \leq |a|$. En particulier, un entier non nul n'a qu'un nombre fini de diviseurs.

Théorème I.2 (Division euclidienne dans $\mathbb{Z}$)

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

$$a = bq + r \quad et \quad 0 \leq r < |b|$$

Remarque I.1. Si on omet la condition $0 \leq r < |b|$, le couple n'est plus unique !

Définition I.2. Soit $a = bq + r$ la division euclidienne de a par b. On dit que :

- a est le **dividende** ;
- b est le **diviseur** ;
- q est le **quotient** ;
- r est le **reste**.

Proposition I.3. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Alors $b \mid a$ si et seulement si le reste de la division euclidienne de a par b vaut* 0.

II. PGCD et PPCM

Proposition II.1. *Soient $a, b \in \mathbb{Z}$ avec $(a, b) \neq (0, 0)$. Alors l'ensemble des diviseurs communs à a et à b est une partie de $\mathbb{Z}$ bornée et admet donc un plus grand élément.*
*On appelle cet élément le **plus grand diviseur commun** à a et b, et on le note* $\mathrm{PGCD}(a, b)$.

Lemme II.1. *Soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ et $a = bq + r$ la division euclidienne de a par b.*
Alors a et b ont les mêmes diviseurs communs que b et r. En particulier, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$.

Méthode. Pour calculer le PGCD de deux entiers a et $b \neq 0$, on dispose de l'**algorithme d'Euclide** : on définit des entiers $r_0, r_1, r_2 \ldots$ par récurrence par

- $r_0 = a$ et $r_1 = b$;
- si $r_k \neq 0$, on pose r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k.

On s'arrête lorsqu'on obtient un entier nul. On a donc $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(r_0, r_1) = \mathrm{PGCD}(r_1, r_2) = \ldots$.

Théorème II.2

Il existe $N \in \mathbb{N}$ tel que $r_N \neq 0$ et $r_{N+1} = 0$. Ainsi, $\text{PGCD}(a,b) = \text{PGCD}(r_N, 0) = r_N$.

Proposition II.3. *Soient $a, b \in \mathbb{Z}$ avec $(a,b) \neq (0,0)$. Alors l'ensemble des multiples strictement positifs communs à a et à b admet un plus petit élément.*
*On appelle cet élément le **plus petit commun multiple** à a et b, et on le note* $\text{PPCM}(a,b)$.
De plus, $\text{PPCM}(a,b) = \dfrac{ab}{\text{PGCD}(a,b)}$.

III. Nombres premiers

Définition III.1. Un entier naturel $n \geq 2$ est dit **premier** si il a exactement deux diviseurs positifs.

Lemme III.1 (Lemme d'Euclide). *Soit a et b deux entiers relatifs et p un nombre premier. Si p divise ab alors p divise a ou p divise b.*

Théorème III.1 (Décomposition en facteurs premiers)

Soit $n \geq 2$ un entier naturel. Il existe un entier $r \geq 1$ et des nombres premiers $p_1, p_2, \ldots, p_r$ et des entiers non nuls $v_1, v_2, \ldots, v_r$ tels que

$$n = \prod_{k=1}^{r} p_k^{v_k}.$$

De plus, cette décomposition est unique à l'ordre des facteurs près.

Proposition III.2. *Soit $a = \prod_{k=1}^{r} p_i^{\alpha_i}$ et $b = \prod_{k=1}^{r} p_i^{\beta_i}$, les décompositions en facteurs premiers de a et b. Alors* $\text{PGCD}(a,b) = \prod_{k=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$ *et* $\text{PPCM}(a,b) = \prod_{k=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$.

Théorème III.3

L'ensemble des nombres premiers est infini.