

Kit de survie du cours

Diviseur, multiple, division euclidienne

Définition 14.1 (Diviseur, multiple). Soit $a, b \in \mathbf{Z}$. On dit que a est un **diviseur** de b , ou que a **divise** b ou encore que b est un **multiple** de a , s'il existe $k \in \mathbf{Z}$ tel que $b = ka$.
Le cas échéant, on note $a \mid b$.

Théorème 14.2 - Division euclidienne dans $\mathbf{Z}$.

Soit $a \in \mathbf{Z}$ et $b \in \mathbf{N}^*$. Il existe un unique couple $(q, r) \in \mathbf{Z} \times \mathbf{N}$ tel que

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

- q est appelé **quotient** de la division euclidienne de a par b .
- r est appelé **reste** de la division euclidienne de a par b .
- Dans ce contexte, b est le **diviseur** et a le **dividende**.

Proposition 14.3 - Lien entre reste de la division euclidienne et divisibilité.

Soit $a \in \mathbf{Z}$ et $b \in \mathbf{N}^*$. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Proposition 14.4 - Lien entre reste de la division euclidienne et congruences.

Soit $a \in \mathbf{Z}$, $b \in \mathbf{N}^*$ et $r \in \llbracket 0, b-1 \rrbracket$. $a \equiv r [b]$ si et seulement si r est le reste de la division euclidienne de a par b .

Plus grand commun diviseur, plus petit commun multiple

Définition 14.5 (Plus grand commun diviseur). Soit $(a, b) \in \mathbf{Z}^2 \setminus \{(0, 0)\}$. Soit A l'ensemble des diviseurs qui sont communs à a et b . On appelle **plus grand commun diviseur** de a et b , et on note $\text{PGCD}(a, b)$, le plus grand élément de A .

Lemme 14.6 - « Simplification » du PGCD pour l'algorithme d'Euclide.

Soit $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$. On note r le reste de division euclidienne de a par b . On a

$$\text{PGCD}(a, b) = \text{PGCD}(b, r).$$

Définition 14.7 (Nombres premiers entre eux). Soit $a, b \in \mathbf{Z}^*$. On dit que a et b sont **premiers entre eux** lorsque $\text{PGCD}(a, b) = 1$.

Définition 14.8 (Plus petit commun multiple). Soit $a, b \in \mathbf{Z}^*$. Soit M l'ensemble des multiples strictement positifs qui sont communs à a et b . On appelle **plus petit commun multiple** de a et b , et on note $\text{PPCM}(a, b)$ le plus petit élément de M .

Nombres premiers

Définition 14.9 (Nombre premier). On appelle **nombre premier** tout entier naturel non nul admettant exactement 2 diviseurs entiers naturels distincts : 1 et lui-même.

Théorème 14.10 - Décomposition d'un nombre en produit de nombres premiers.

Tout entier naturel n supérieur ou égal à 2 admet une décomposition en facteurs premiers de la forme $n = q_1 q_2 \dots q_k$ où $q_1, \dots, q_k$ sont des nombres premiers. Cette décomposition est unique à l'ordre près des facteurs.

On peut également écrire cette décomposition sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où $p_1, \dots, p_r$ sont des nombres premiers distincts deux à deux et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls.

Proposition 14.11 - PGCD, PPCM à partir de la décomposition en facteurs premiers.

Soit $(a, b) \in (\mathbf{N} \setminus \{0, 1\})^2$, dont on écrit $a = \prod_{i=1}^n p_i^{\alpha_i}$ et $b = \prod_{i=1}^n p_i^{\beta_i}$ les décompositions en facteurs premiers (quitte à choisir $\alpha_i = 0$ ou $\beta_i = 0$ pour que les mêmes nombres premiers apparaissent dans les deux décompositions). On a :

$$\text{PGCD}(a, b) = \prod_{i=1}^n p_i^{\min(\alpha_i, \beta_i)} \quad \text{et} \quad \text{PPCM}(a, b) = \prod_{i=1}^n p_i^{\max(\alpha_i, \beta_i)}.$$

Corollaire 14.12 - Lien entre PGCD et PPCM.

Pour tout $(a, b) \in \mathbf{N}^2$, $\text{PGCD}(a, b) \times \text{PPCM}(a, b) = a \times b$.

Méthodes et exercices à connaître

Démontrer qu'un entier est divisible par un autre

On peut revenir à la définition ou utiliser des congruences.

- Résultats du cours : Définition 14.1, Proposition 14.3, Proposition 14.4.
- Exercices  : 14.1, 14.2, 14.3
- Exercices  : 14.4, 14.14
- Exercices  :

Utiliser le théorème de division euclidienne

L'énoncé du théorème est à parfaitement connaître. Il faut savoir l'utiliser sur un exemple pratique ! Pour les exercices plus difficile, il faut revenir à l'énoncé du théorème.

- Résultats du cours : Théorème 14.2.
- Exercices  :
- Exercices  : 14.6, 14.7, 14.8
- Exercices  :

Trouver le PGCD de deux entiers avec l'algorithme d'Euclide

- Résultats du cours : Définition 14.5, algorithme d'Euclide (basé sur le Lemme 14.6).
- Exercices  : 14.15
- Exercices  : 14.16
- Exercices  : 14.17, 14.18, 14.19