Arithmétique : à retenir (J-Y D)

Définition

Soient $p, q \in \mathbb{Z}$.

(a) On note $\quad p\mathbb{Z} := \{pk \ ; \ k \in \mathbb{Z}\}$.

(b) On dit que p *divise* q (ou que q *est multiple de* p), et note $p|q$, si : $\ q \in p\mathbb{Z}$.

Théorème

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$.

Il existe $\ q, r \in \mathbb{Z}$ uniques tels que : $\quad a = bq + r \ \text{ et } \ 0 \leq r < b$.

Définition-Proposition

Soient $a, b \in \mathbb{Z}$.

(a) Il existe $d \in \mathbb{N}$ unique qui divise a et b, et tel que tout diviseur commun dans $\mathbb{Z}$ de a et b divise d. Il est caractérisé par : $\quad a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On le note : $\ d := \text{pgcd}(a, b)$.

(b) Il existe $m \in \mathbb{N}$ unique qui est multiple de a et b, et tel que tout multiple commun dans $\mathbb{Z}$ de a et b est multiple de m. Il est caractérisé par : $\quad a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On le note : $\ m := \text{ppcm}(a, b)$.

(c) On a : $\ |ab| = md$.

Définition

On dit que $a, b \in \mathbb{Z}$ sont *premiers entre eux* si : $\ \text{pgcd}(a, b) = 1$.

Théorème (« th. de Bézout »)

Des éléments a et b de $\mathbb{Z}$ sont premiers entre eux si et seulement si :

il existe $u, v \in \mathbb{Z}$ tels que $\ au + bv = 1$.

Proposition (« algorithme d'Euclide »)

Soient $a, b \in \mathbb{Z} \setminus \{0\}$.

On effectue les divisions euclidiennes successives de a par $|b|$ (reste $r_1 \neq 0$), $|b|$ par r_1 (reste $r_2 \neq 0$), r_1 par r_2 (reste $r_3 \neq 0$), ..., , r_{n-1} par r_n (reste 0 pour la $1^{\text{ère}}$ fois).

Alors : $\boxed{\text{pgcd}(a, b) = r_n}$.

Définition

Un *nombre premier* est un élément p de $\mathbb{N} \setminus \{0\}$ différent de 1 tel que les éléments de $\mathbb{N} \setminus \{0\}$ qui divisent p sont 1 et p.

Proposition

(a) Soient $a, b \in \mathbb{Z}$ et p un nombre premier.

Si $\ p|ab$, alors $\ p|a \ $ ou $\ p|b$.

(b) Soient $a, b, c \in \mathbb{Z}$.

Si $\ a|bc \ $ et $\ \text{pgcd}(a, b) = 1$, alors $\ a|c \ $ (« th. de Gauss »).

Théorème (« th. de décomposition en facteurs premiers »)

Soit $n \in \mathbb{N}\setminus\{0\}$. Il existe $k \in \mathbb{N}$, des nombres premiers $p_1 < ... < p_k$ et $\alpha_1, ...\alpha_k \in \mathbb{N}\setminus\{0\}$ uniques, tels que : $n = \underbrace{p_1^{\alpha_1} ... p_k^{\alpha_k}}_{1 \text{ quand } k=0}$.

Dans ce cas, les éléments de $\mathbb{N}\setminus\{0\}$ qui divisent n sont les nombres :

$$p_1^{\beta_1} ... p_k^{\beta_k} \text{ avec } 0 \leq \beta_1 \leq \alpha_1, ..., 0 \leq \beta_k \leq \alpha_k.$$

Corollaire

Soient $a, b \in \mathbb{N}\setminus\{0\}$ de la forme :
$a = p_1^{\alpha_1} ... p_k^{\alpha_k}$ et $b = p_1^{\beta_1} ... p_k^{\beta_k}$ avec $p_1 < ... < p_k$ premiers et $\alpha_1, ...\alpha_k, \beta_1, ...\beta_k \in \underbrace{\mathbb{N}}_{\text{on accepte } 0}$.

On a : $\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} ... p_k^{\min(\alpha_k,\beta_k)}$ et $\text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} ... p_k^{\max(\alpha_k,\beta_k)}$.

Dans la suite, on se donne $n \in \mathbb{N}\setminus\{0\}$.

Définition

Soient $a, b \in \mathbb{Z}$.

On dit que a est congru à b modulo n, et note $a \equiv b\,[n]$, si $a - b$ est multiple de n.

Proposition

(a) Soient $a, b, a', b' \in \mathbb{Z}$. Si $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$, alors $a + a' \equiv b + b'\,[n]$ et $aa' \equiv bb'\,[n]$.

(b) Soit $a \in \mathbb{Z}$. Il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1\,[n]$ si et seulement si a et n sont premiers entre eux.

Théorème (« petit th. de Fermat »)

Soit p un nombre premier.

On a : $a^{p-1} \equiv 1\,[p]$ quand $a \in \mathbb{Z}$ n'est pas multiple de p, donc $a^p \equiv a\,[p]$ pour tout $a \in \mathbb{Z}$.

Définition-Proposition

(a) Pour tout $a \in \mathbb{Z}$, on note : $\overline{a} := \{a + b\ ;\ b \in n\mathbb{Z}\}$.

On peut munir — et on munit — l'ensemble $\mathbb{Z}/n\mathbb{Z} := \{\overline{a}\ ;\ a \in \mathbb{Z}\}$ des lois $+$ et $\cdot$ suivantes :

$$\overline{a} + \overline{a'} := \overline{a + a'} \quad \text{et} \quad \overline{a} \cdot \overline{a'} := \overline{aa'} \quad \text{pour } a, a' \in \mathbb{Z}.$$

(b) L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a pour éléments distincts $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$.

(c) On a : $\mathbb{Z}/n\mathbb{Z} \neq \{\overline{0}\}$ et $\left(\forall \overline{a} \in \mathbb{Z}/n\mathbb{Z} \quad \exists \overline{a'} \in \mathbb{Z}/n\mathbb{Z} \quad \overline{a} \cdot \overline{a'} = \overline{1}\right)$ si et seulement si n est premier