Arithmétique

Aubin SIONVILLE

MPI Clemenceau - 2021-2023

Définitions

Nombres associés

$(a, b) \in \mathbb{Z}$ associés si $a = b$ ou $a = -b$

Division euclidienne

Hypothèse : $a \in \mathbb{Z}, b \in \mathbb{Z}^*$

$$\boxed{\exists!(q, r) \in \mathbb{Z}^2, \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}}$$

$$\begin{array}{ccc} r = 0 & \iff & a \mid b \\ a \equiv b \pmod{c} & \iff & c \mid (b - a) \end{array}$$

PGCD et PPCM

PGCD

Le plus grand diviseur commun à $a, b \in \mathbb{Z}^2$:

$\boxed{\text{PGCD}(a, b) \text{ ou } a \wedge b}$

PPCM

Le plus petit élément de $\{k \in \mathbb{N} |\ \ a \mid k \text{ et } b \mid k\}$:

$\boxed{\text{PPCM}(a, b) \text{ ou } a \vee b}$

Diviseurs

Hypothèses : $d = a \wedge b$ et $D = \{k \in \mathbb{Z}\ \ |k \mid a \text{ et } k \mid b\}$

$$\boxed{\forall k \in \mathbb{Z}, k \in D \iff k \mid d}$$

PGCD et PPCM

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

Théorèmes d'arithmétique

Théorème d'Euclide

Hypothèse : r est le reste de a/b

$$\boxed{a \wedge b = b \wedge r}$$

Théorème de Gauss

Hypothèse : $a \wedge b = 1$ et $a \mid bc$

$$\boxed{a \mid c}$$

Théorème de Bézout

Hypothèse : $d = a \wedge b$

$$\boxed{\exists (u, v) \in \mathbb{Z}^2, d = au + bv}$$

Petit théorème de Fermat

Hypothèse : p est premier

$$\boxed{a^p \equiv a \pmod{p}}$$

Nombres premiers

Si $a = \prod_{p \in \mathbb{P}} p^{\alpha(p)}$ et $b = \prod_{p \in \mathbb{P}} p^{\beta(p)}$:

$$\boxed{a \mid b \iff \forall p \in \mathbb{P}, \alpha(p) \geq \beta(p)}$$

$$\boxed{a \wedge b = \prod_{p \in \mathbb{P}} p^{\min(\alpha(p), \beta(p))}}$$

$$\boxed{a \vee b = \prod_{p \in \mathbb{P}} p^{\max(\alpha(p), \beta(p))}}$$