ARITHMÉTIQUES DANS $\mathbb{Z}$

Notation.

$$(\forall a \in \mathbb{Z}),\quad \begin{cases} \mathscr{D}(a) \text{ désigne l'ensemble des diviseurs de } a \\ a\mathbb{Z} \text{ désigne l'ensemble des multiples de } a \end{cases}$$

Remarques

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

- b divise $a \iff \mathscr{D}(b) \subset \mathscr{D}(a) \iff a\mathbb{Z} \subset b\mathbb{Z}$
- $\mathscr{D}(a) = \mathscr{D}(-a) = \mathscr{D}(|a|)$

1. Division euclidienne

Théorème

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$,

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

- q : Le quotient. (En python : $a//b$)
- r : Le reste. (En python : $a\%b$)

NB : $b \mid a \iff r = 0$

Preuve

.....

.....

.....

.....

.....

.....

Propriétés

Soient $a,b,c,d \in \mathbb{Z}$

- $(\forall (u,v) \in \mathbb{Z}^2),\quad a \mid b$ et $a \mid c \Longrightarrow a \mid bu+cv$
  - $a \mid b$ et $a \mid c \Longrightarrow a \mid b+c$
  - $a \mid c$ et $b \mid d \Longrightarrow ab \mid cd$
  - $a \mid b \Longrightarrow |a| \leq |b|$
  - $b \mid a$ et $a \mid b \Longleftrightarrow |a| = |b|$
- La relation de divisibilité est une relation d'ordre dans $\mathbb{N}$.

Exercice

Soient $n, p \in \mathbb{N}^*$ tels que $p > n$,effectuer la division euclidienne de 2^p-1 par 2^n-1.

.....

.....

.....

2. PGCD

Définitions

Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

L'ensemble $\mathscr{D}(a) \cap \mathscr{D}(b)$ possède un plus grand élément, noté $a \wedge b$.

$$a \wedge b \overset{\text{déf}}{=} max(\mathscr{D}(a) \cap \mathscr{D}(b)) = max\{d \in \mathbb{Z} / \quad d|a \text{ et } d|b\} \in \mathbb{N}^*$$

Par convention : $0 \wedge 0 = 0$.

NB : $a \wedge b \geq 0$

Remarques

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

- $a \wedge 0 = |a|$
- $a \wedge 1 = 1$
- $a \wedge b = |a| \wedge |b|$
- a divise $b \Longleftrightarrow a \wedge b = |a|$
- $\forall d \in \mathbb{Z},\quad [(d \mid a \text{ et } d \mid b) \Rightarrow d \leq a \wedge b]$

Théorème

Soient $a, b, q, r \in \mathbb{Z}$,

$$a = bq + r \implies a \wedge b = b \wedge r$$

Preuve

.....

.....

.....

.....

Application : Algorithme d'Euclide

Principe : On effectue des divisions euclidiennes successives tant que le reste est non nul.
Soit $(a, b) \in \mathbb{Z}^2 / \{(0,0)\}$. On cherche $d = a \wedge b$. On note $r_0 = |a|$, $r_1 = |b|$.

$$\begin{cases} r_0 = r_1 q_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & 0 < r_3 < r_2 \\ r_2 = r_3 q_3 + r_4 & 0 < r_4 < r_3 \\ \vdots & \\ r_{n-2} = r_{n-1} q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_n + 0 & r_{n+1} = 0 \end{cases}$$

- Le pgcd de a et b est le dernier reste non nul obtenu par l'algorithme d'Euclide.

$a \wedge b =$ .....

- $\mathscr{D}(a) \cap \mathscr{D}(b) =$ .....

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$$

Exercice

Soient $n, p \in \mathbb{N}^*$ tels que $p > n$,on écrit $p = qn + r$ avec $0 \leq r < n$.

1. Montrer que $\exists b \in \mathbb{N}$, $2^p - 1 = \left(2^n - 1\right) b + 2^r - 1$.
2. En déduire que $\left(2^p - 1\right) \wedge \left(2^n - 1\right) = 2^{p \wedge n} - 1$.
3. Montrer que $\left(2^n - 1\right)$ divise $\left(2^p - 1\right) \iff n$ divise p

Solution

.....

.....

.....

.....

.....

.....

.....

.....

Caractérisation de PGCD

Soient $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}, d \in \mathbb{N}$.

$$d = a \wedge b \iff \begin{cases} d \mid a \text{ et } d \mid b \\ \forall \delta \in \mathbb{Z}, \quad \delta \mid a \text{ et } \delta \mid b \Longrightarrow \delta \mid d \end{cases}$$

- $a \wedge b$ est le plus grand diviseur commun au sens de divisibilité aussi.

Preuve

.....

.....

.....

.....

Résultat

Soit $(a,b) \in \mathbb{Z}^2$

$$\boxed{\forall d \in \mathbb{Z}, \quad (d \mid a \quad \text{et} \quad d \mid b) \quad \Rightarrow \quad d \mid (a \wedge b)}$$

- Tout diviseur commun de a et b divise $a \wedge b$.

Autre caractérisation de PGCD

Soient $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Preuve

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Corollaire

Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$

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

Preuve

.....

.....

.....

.....

Relation de Bezout

Soient $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, $d \in \mathbb{N}$

$$a \wedge b = d \implies \exists (u,v) \in \mathbb{Z}^2 \quad \text{tels que} \quad au + bv = d$$

Preuve

.....

.....

.....

.....

Remarque

S'il existe $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = d$, alors $(a \wedge b) \mid d$

Exemple

Déterminer le PGCD et les coefficients de Bezout de $a = 600$ et $b = 124$

.....

.....

.....

.....

.....

.....

.....

.....

.....

PGCD de plusieurs entiers

Soien $a_1, a_2, \ldots, a_n$ des entiers relatifs non nuls.

$\bigwedge_{i=1}^{n} a_i \overset{\text{déf}}{=}$ Le plus grand des diviseurs positifs communs de $a_1, a_2, \ldots, a_n$.

$$\boxed{\bigwedge_{i=1}^{n} a_i \overset{\text{déf}}{=} max\left(\mathrm{D}(a_1) \cap \mathrm{D}(a_2) \cap \ldots \cap \mathrm{D}(a_n)\right)}$$

- $a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_n\mathbb{Z} = \bigwedge_{i=1}^{n} a_i\mathbb{Z}$
- $\exists (u_1, \ldots, u_n) \in \mathbb{Z}^n, \quad \sum_{i=1}^{n} u_i a_i = \bigwedge_{i=1}^{n} a_i$
- $ka_1 \wedge ka_2 \wedge \ldots \wedge ka_n = |k| \bigwedge_{i=1}^{n} a_i$

Preuve

.....

.....

.....

.....

.....

3. Entiers premiers entre eux

Définition

Soit $(a, b) \in \mathbb{Z}^2$

Les entiers a et b sont premiers entre eux si : $a \wedge b = 1$

Théorème de Bézout

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$

$$\boxed{a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \quad \text{tels que} \quad au + bv = 1}$$

Preuve

.....

.....

.....

.....

Corollaire

Soient $a, b_1, \ldots, b_n \in \mathbb{Z}$. Alors :

$$\forall i \in [|1, n|], a \wedge b_i = 1 \iff a \wedge \left(\prod_{i=1}^{n} b_i \right) = 1$$

■ **En particulier :** Pour tous $n, m \in \mathrm{N}^*$

$$a \wedge b = 1 \iff a \wedge b^n = 1$$

$$a \wedge b = 1 \iff a^m \wedge b^n = 1$$

Preuve

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Une décomposition utile

Soient $a, b \in \mathbb{Z}^*$ et $d = a \wedge b$, alors

$$\exists \alpha, \beta \in \mathbb{Z}, \quad \begin{cases} a = d\alpha \\ b = d\beta \end{cases} \quad \text{avec } \alpha \wedge \beta = 1$$

$$\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b} = 1$$

Preuve

.....

.....

.....

Lemme de Gauss

Soit $(a, b, c) \in \mathbb{Z}^3$.

$$a \mid bc \text{ et } a \wedge c = 1 \implies a \mid b$$

Preuve

.....

.....

.....

.....

Lemme d'Euclide

Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge c = 1$

$$a|b \text{ et } c|b \implies ac|b$$

■ **En général :** Si $a_1, \ldots, a_n \in \mathbb{Z}$ deux à deux premiers entre eux . Alors :

$$\forall i \in [|1, n|], a_i \mid b \quad \Longleftrightarrow \prod_{i=1}^{n} a_i \mid b$$

Preuve

.....

.....

.....

4. Plus petit commun multiple (PPCM)

Définition

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

$a \vee b \overset{\text{déf}}{=}$ Le plus petit des multiples strictement positifs communs à a et b.

$$a \vee b \overset{\text{déf}}{=} min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*) = min\{m \in \mathbb{N}^* / \quad a|m \text{ et } b|m\}$$

Par convention : $a \vee 0 = 0$.

NB : $a \vee b \geq 0$

Remarques

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

- $a \vee 1 = |a|$
- $\forall m \in \mathbb{Z}, \quad (a \mid m \text{ et } b \mid m) \Rightarrow a \vee b \leq |m|$
- $a \vee b = |a| \vee |b|$
- b divise $a \Longleftrightarrow a \vee b = |a|$

Théorème

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

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

Preuve

.....

.....

.....

.....

.....

Conséquence

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

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

Preuve

.....

.....

.....

.....

Caractérisation de PPCM

Soient $a, b \in \mathbb{Z}^*, m \in \mathbb{N}$.

$$m = a \vee b \iff \begin{cases} a \mid m \text{ et } b \mid m \\ \forall m' \in \mathbb{Z}, \quad a \mid m' \text{ et } b \mid m' \Longrightarrow m \mid m' \end{cases}$$

- $a \vee b$ est le plus petit multiple commun au sens de divisibilité également.

Preuve

.....

.....

.....

.....

.....

Remarque

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

$$\boxed{\forall m \in \mathbb{Z}, \quad (a \mid m \quad \text{et} \quad b \mid m) \quad \Rightarrow \quad (a \vee b) \mid m}$$

- Tout multiple commun de a et b est un multiple $a \vee b$.

Lien avec le pgcd

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

- **En particulier :** $a\wedge b=1\Longrightarrow a\vee b=ab$

Preuve

.....

.....

.....

.....

.....

.....

PPCM de plusieurs entiers

Soient $a_1,a_2,\dots,a_n$ des entiers relatifs non nuls.

$\bigvee_{i=1}^{n} a_i \overset{\text{déf}}{=}$ Le plus petit des multiples strictement positifs communs de $a_1,a_2,\dots,a_n$.

$$\boxed{\bigvee_{i=1}^{n} a_i \overset{\text{déf}}{=} min\left(a_1\mathbb{Z}\cap a_2\mathbb{Z}\cap\ldots\cap a_n\mathbb{Z}\cap\mathbb{N}^*\right)}$$

- $a_1\mathbb{Z}\cap a_2\mathbb{Z}\cap\ldots\cap a_n\mathbb{Z}=\bigvee_{i=1}^{n} a_i\mathbb{Z}$
- $\forall i\in[|1,n|],\quad a_i|m\Longrightarrow\bigvee_{i=1}^{n} a_i|m$
- $\forall(a_1,\dots,a_n)\in\mathbb{Z}^n,\forall k\in\mathbb{Z},\quad (ka_1)\vee\ldots\vee(ka_n)=|k|(a_1\vee\ldots\vee a_n)$
- $a_1,\dots,a_n$ premier entre eux 2à 2 $\Longrightarrow\bigvee_{i=1}^{n} a_i=|\prod_{i=1}^{i=n} a_i|$

Preuve

.....

.....

5. Nombres premiers

Définition

Un nombre premier est entier naturel $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p

- On note $\mathscr{P}$ l'ensemble des nombres premiers.

Remarque

Soit $p \in \mathbb{N}^* / \{1\}$.

$$p \text{ est un nombre } \textbf{premier} \iff \mathscr{D}(p) = \{-1, 1, -p, p\}.$$

Exemples

- 1 n'est pas un nombre premier.
- 2 est le seul nombre premier pair.
- $3, 5, 7, \ldots$ sont des nombres premiers.

Propriétés

Soit p un nombre premier.

- $\forall d \in \mathbb{N},\quad d|p \implies d = 1 \ \ ou \ \ d = p.$
- $\forall n \in \mathbb{Z},\quad p|n \ \text{ ou } \ p \wedge n = 1.$

Preuve

.....

.....

.....

.....

.....

Remarques

- $\forall p, q \in \mathscr{P},\quad p \neq q \implies p \wedge q = 1.$
- $\forall p, q \in \mathscr{P},\quad p \neq q \implies \forall \alpha, \beta \in \mathbb{N},\quad p^\alpha \wedge p^\beta = 1.$

Proposition

- p est premier $\overset{p\geq 3}{\iff}$ $\forall k \in [\![2, p-1]\!],\ p \wedge k = 1.$

$\iff$ $p \wedge (p-1)! = 1.$

Propriétés

Soit p un nombre premier.

- $p \mid ab \implies p|a$ ou $p|b.$
- $p \mid \prod_{i=1}^{n} a_i \iff \exists i \in [|1, n|],\ p \mid a_i$

Preuve

.....

.....

.....

.....

.....

Théorème

Tout entier $n \geq 2$ admet au moins un diviseur premier.

En particulier : Si $n \geq 2$ n'est pas premier, il admet un diviseur premier $p \leq \sqrt{n}$.

Preuve

.....

.....

.....

.....

Théorème

L'ensemble $\mathscr{P}$ des nombres premiers est infini.

Preuve

.....

.....

.....

.....

Définition :Valuation p-adique

Soient $p \in \mathscr{P}$, $n \geq 2$.

valuation p-adique de n est notée $v_p(n)$.

$$v_p(n) \overset{\text{déf}}{=} max\left\{k \in \mathbb{N},\ p^k \mid n\right\}$$

Exemple

.....

Remarques

Soient $p \in \mathscr{P}$, $n \geq 2$.

- $v_p(n) = 0 \iff p \nmid n$
- $v_p(n) = 1 \iff p \mid n$ et $p^2 \nmid n$
- $v_p(n) = \alpha \iff p^\alpha \mid n$ et $p^{\alpha+1} \nmid n$

Théorème de décomposition en facteurs premiers

Tout entier $n \in \mathbb{N}^*/\{1\}$ se décompose de façon unique de la forme :

$$\boxed{n = {p_1}^{\alpha_1} \dots {p_k}^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}}$$

où $p_1, \dots, p_k$ sont premiers et $p_1 < p_2 < \dots < p_k$ et $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.

- Cette formule s'écrit sous la forme :

$$n = {p_1}^{v_{p_1}(n)} \cdots {p_k}^{v_{p_k}(n)} = \prod_{p \in \mathscr{P}} p^{v_p(n)}$$

Preuve

.....

.....

.....

.....

.....

.....

.....

.....

Propriétés

Soit $n, m \in \mathbb{Z}^*$

- $\forall p \in \mathscr{P},\ v_p(mn) = v_p(m) + v_p(n)$
- $n \mid m \iff \forall p \in \mathscr{P},\ v_p(n) \leqslant v_p(m)$

Preuve

.....

.....

.....

.....

.....

.....

L'expression de PGCD , PPCM

Soit $m, n \in \mathbb{N}^* \setminus \{1\}$, alors :

$$n \wedge m = \prod_{p \in \mathscr{P}} p^{min\{v_p(n), v_p(m)\}} \quad ; \quad m \vee n = \prod_{p \in \mathscr{P}} p^{max\{v_p(n), v_p(m)\}}$$

Preuve

.....

.....

.....

.....

.....

.....

Exemples

1. Soient $a \in \mathbb{Z}, n \in \mathbb{N}^*$ et $p \in \mathscr{P}$. p divise a si et seulement si p divise a^n.
2. Montrer que $\sqrt[5]{\frac{4}{3}}$ est irrationnel.

Solution

.....

.....

.....

.....

.....

.....

6. Congruences

Définition

La relation de congruence modulo $n \in \mathbb{N}^*$:

$$\forall a, b \in \mathbb{Z}, \quad a \equiv b[n] \overset{\text{déf}}{\iff} n \mid b - a$$

$$\iff \exists k \in \mathbb{Z} \ / \ b = a + kn$$

Congruence modulo n

Soit $n \in \mathbb{N}^*$.

- La **relation de congruence** modulo n est une **relation d'équivalence** sur $\mathbb{Z}$.
  - **Réflexive :** $\forall a \in \mathbb{Z},\ a \equiv a[n]$.
  - **Symétrique :** $\forall (a,b) \in \mathbb{Z}^2,\ a \equiv b[n] \Longrightarrow b \equiv a[n]$.
  - **Transitive :** $\forall (a,b,c) \in \mathbb{Z}^3,\ (a \equiv b[n] \text{ et } b \equiv c[n]) \Longrightarrow a \equiv c[n]$
- **La classe d'équivalence** de a modulo n : $\overline{a} = \{x \in \mathbb{Z},\ x \equiv a[n]\}$

$$\forall a,b \in \mathbb{Z},\quad \overline{a} = \overline{b} \Longleftrightarrow a \equiv b[n]$$

On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n}\}$ l'ensemble des classes modulo n

Régles de calcul

Soit $n \in \mathbb{N}^*$ et $a,b,c,d \in \mathbb{Z}$. Alors :

$$a \equiv b[n] \text{ et } c \equiv d[n] \Longrightarrow a+c \equiv b+d[n] \text{ et } ac \equiv bd[n].$$

$$a \equiv b[n] \overset{k\in\mathbb{Z}}{\Longrightarrow} ka \equiv kb[n].$$

$$a \equiv b[n] \overset{p\in\mathbb{N}}{\Longrightarrow} a^p \equiv b^p[n].$$

$$a = b[n] \Longleftrightarrow a\%n = b\%n \quad \text{même reste .}$$

Petit théorème de FERMAT

Soit p un nombre premier.

- $\forall a \in \mathbb{Z},\ a^p \equiv a[p]$
- Si de plus $a \wedge p = 1,\ a^{p-1} \equiv 1[p]$

Preuve

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Exercice

Soient p, q deux npmbres premiers distincts .

1. Montrer que $p^{q-1} + q^{p-1} \equiv 1[pq]$.
2. Soient $n \in \mathbb{N}^*$, tel que $n \wedge p = 1$,
   (a) Si p est impair ,montrer que $n^{\frac{p-1}{2}} \equiv 1[p]$ ou $n^{\frac{p-1}{2}} \equiv -1[p]$.
   (b) Montrer que $n^{p(p-1)} \equiv 1[p^2]$.

Solution

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Structure de $(\mathbb{Z}/n\mathbb{Z},+,\times)$

- $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un anneau commutatif d'éléments neutres $\overline{0}$ pour $+$ et $\overline{1}$ pour $\times$.

$$\overline{x}+\overline{y}=\overline{x+y} \qquad \overline{x}\times\overline{y}=\overline{x\times y}$$

- $\overline{a}\in \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ est inversible $\iff$ $a\wedge n=1$.
- $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps $\iff$ p est premier.

Preuve

.....

.....

.....

.....

.....

.....

.....

.....

Exercice

1. Résoudre dans $\mathbb{Z}/7\mathbb{Z}$, l'équation suivante $3x\equiv 5[7]$
2. Résoudre dans $\mathbb{Z}/13\mathbb{Z}$, le systeme suivant :

$$\begin{cases} 3x+4y\equiv 5[13] \\ 2x+5y\equiv 7[13] \end{cases}$$

Solution

.....

.....

.....

.....

.....