

I. Division euclidienne/ divisibilité /congruence

Division euclidienne

Quels que soit le nombre entier relatif a , quel que soit l'entier naturel non nul b , il existe deux entiers uniques q et r tels que :

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

Divisibilité

a et b sont deux entiers relatifs, on dit que b divise a (a est multiple de b) si et seulement si, il existe un entier k tel que :

$$a = b.k$$

congruence

n est un entier naturel non nul donné. a et b sont deux entiers relatifs. On dit que a est congrus à b modulo n si et seulement si, il existe k dans $\mathbb{Z}$ tel que : $a - b = k.n$
On écrit : $a \equiv b [\text{modulo } n]$

II. Propriétés de la divisibilité et de la congruence

Divisibilité

$$(a \mid b \text{ et } b \mid a) \Rightarrow |a| = |b|$$

$$(\delta \mid a \text{ et } \delta \mid b) \Rightarrow (\forall (\alpha, \beta) \in \mathbb{Z}^2) ; \delta \mid \alpha.a + \beta.b$$

$$a^n \mid b \Rightarrow a \mid b$$

congruence

$$a \equiv b [n] \Leftrightarrow a - b = k.n \Leftrightarrow n \mid a - b$$

$$\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d [n] \\ a.c \equiv b.d [n] \end{cases}$$

III. PGDC et PPMC

Plus grand diviseur commun

on le note : $d = \text{pgcd}(a, b) = a \wedge b$

Le pgcd vérifie les propriétés suivantes :

$$(d = a \wedge b) \Leftrightarrow (\exists (a', b') \in \mathbb{Z}^2) ; \begin{cases} a = d.a' \\ b = d.b' \end{cases} \text{ et } a' \wedge b' = 1$$

$$\begin{cases} d' \mid a \\ d' \mid b \end{cases} \Rightarrow d' \mid a \wedge b$$

Plus petit multiple commun

on le note : $m = \text{ppmc}(a, b) = a \vee b$

Le ppmc vérifie les propriétés suivantes :

$$(m = a \vee b) \Rightarrow \begin{cases} a \mid m \\ b \mid m \end{cases}$$

$$\begin{cases} a \mid c \\ b \mid c \end{cases} \Rightarrow a \wedge b \mid c$$

Propriété commune

$$\forall (a, b) \in \mathbb{Z}^2 ; (a \vee b).(a \wedge b) = |a.b|$$

IV. Nombres premiers entre eux / Bezzout / Gauss/Propriétés

Nombres premiers entre eux

On dit que les entiers a et b sont premiers entre eux si et seulement si $\text{pgcd}(a, b) = 1$.

Identité de Bezzout

$$(a \wedge b = 1) \Leftrightarrow (\exists (u, v) \in \mathbb{Z}^2 ; a.u + b.v = 1)$$

Conséquence :

$$(a \wedge b = d) \Leftrightarrow (\exists (u, v) \in \mathbb{Z}^2 ; a.u + b.v = d)$$

Théorème de Gauss : $(c \mid a.b \text{ et } c \wedge a = 1) \Rightarrow (c \mid b)$

Autres propriétés :

$$(a \mid c \text{ et } b \mid c \text{ et } a \wedge b = 1) \Rightarrow (a.b \mid c)$$

$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \Rightarrow (a \wedge b.c) = 1$$

$$(a \wedge b = 1) \Leftrightarrow \forall (m, n) \in \mathbb{N}^* \times \mathbb{N}^* ; (a^m \wedge b^n = 1)$$

$$(a = b.q + r \text{ et } 0 \leq r < b) \Rightarrow (a \wedge b = r \wedge b)$$

V. Nombres premiers / Propriétés

Un nombre entier est premier s'il a exactement deux diviseurs positifs : 2, 3, 5, 7 etc.... 1 et -1 ne sont pas premiers...

L'ensemble des nombres premiers est infini.

Propriétés : soit p premier on a :

$$(p \mid a.b) \Rightarrow (p \mid a \text{ ou } p \mid b)$$

$$(p \mid a^n) \Rightarrow (p \mid a)$$

$$(p \mid a_1.a_2...a_n) \Leftrightarrow \exists i \in \{1, 2, \dots, n\} ; (p \mid a_i)$$

$$(p \mid a) \Rightarrow p \wedge a = p \text{ et } (p \text{ ne divise pas } a) \Rightarrow p \wedge a = 1$$

VI. Algorithme d'Euclide

Soient deux entiers naturels a et b tels que $a > b$:

On divise a (le plus grand) par b , on obtient :

$$(1): \quad a = b \cdot q_0 + r_0 \quad \text{et} \quad 0 \leq r_0 < b$$

Si $r_0 = 0$ alors b divise a et $\text{pgcd}(a, b) = b$

Si $r_0 \neq 0$ On divise b par r_0 , on obtient :

$$(2): \quad b = r_0 \cdot q_1 + r_1 \quad \text{et} \quad 0 \leq r_1 < r_0 < b$$

Si $r_1 = 0$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = r_0$

Si $r_i \neq 0$ On divise r_0 par r_1 , on obtient :

etc

Après un certain nombre d'opération, on obtient un reste nul (en effet la suite des restes est une suite décroissante de nombres entiers), soit r_n , le dernier reste non nul de cette suite, on alors :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$$

VII. Décomposition d'un entier en un produit de facteurs premiers

Tout nombre entier naturel non nul et différent de 1, se décompose d'une manière unique sous la forme :

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$$

Où les nombres p_i sont des nombres premiers et les α_i sont des entiers naturels non nuls.

VIII. L'ensemble des classes d'équivalence $\mathbb{Z}/n\mathbb{Z}$

La relation de congruence :

$$a \equiv b [n] \Leftrightarrow a - b = k \cdot n \Leftrightarrow n \mid a - b$$

Est une relation d'équivalence dans $\mathbb{Z}$, compatible avec la somme et le produit:

$$\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d [n] \\ a \cdot c \equiv b \cdot d [n] \end{cases}$$

La classe d'équivalence d'un entier relatif x est l'ensemble défini par :

$$\alpha = \bar{x} = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\}$$

L'ensemble qui contient toutes les classes

d'équivalence modulo n est noté : $\mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-2}, \overline{n-1} \}$$

Dans $\mathbb{Z}/n\mathbb{Z}$, on définit la somme et le produit des classes, de la façon suivante :

$$\begin{cases} \overline{a+b} \equiv \overline{a} + \overline{b} \\ \overline{a \cdot b} \equiv \overline{a} \cdot \overline{b} \end{cases}$$

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire, en général non intègre.

Si n est premier, alors $\mathbb{Z}/n\mathbb{Z}$ est un corps.

$$(\bar{a} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z}) \Leftrightarrow (a \wedge n = 1)$$

IX. La numération

Soit x un entier naturel supérieur ou égal à 2. Tout entier b de $\mathbb{N}$ peut s'écrire sous la forme :

$$b = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0$$

Où

$$a_n \neq 0 \quad \text{et} \quad (\forall i \in [0, n]) ; \quad a_i \in [0, x-1]$$

On écrit :

$$(1): \quad b = \overline{a_n a_{n-1} \dots a_1 a_0}^{(x)}$$

Et on dit que l'écriture (1) est l'écriture du nombre b dans le système de numération de base x .

X. Détermination du $\text{pgcd}(a, b)$ et du $\text{ppmc}(a, b)$

Soient :

$$a = \prod_{i=1}^n p_i^{\alpha_i} \quad \text{et} \quad b = \prod_{i=1}^n p_i^{\beta_i}$$

La décomposition en facteurs premiers de a et b , on obtient :

$$a \wedge b = \prod_{i=1}^n p_i^{\inf(\alpha_i, \beta_i)}$$

$$a \vee b = \prod_{i=1}^n p_i^{\sup(\alpha_i, \beta_i)}$$