Arithmétique

Maths Expertes

sullyvan.fr

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple (q, r) tel que $a = bq + r$ avec $0 \leq r < b$

Vocabulaire : a est le dividende ; b le diviseur ; q le quotient et r le reste

Divisibilité dans $\mathbb{Z}$

a divise b

$\iff$ b multiple de a

$\iff$ il existe $k \in \mathbb{Z}$ tel que $b = ka$

✧ Notation : a/b

✧ Réflexivité : a/a

✧ Transitivité : $\begin{cases} a/b \\ b/c \end{cases} \Longrightarrow a/c$

✧ Linéarité : $\begin{cases} a/b \\ a/c \end{cases} \Longrightarrow a/bu + cv$

✧ Lien avec les congruences : $a/b \iff b \equiv 0(a)$

✧ Lien avec le PGCD : $a/b \iff PGCD(a, b) = a$

Congruence dans $\mathbb{Z}$

a et b ont même reste dans la division euclidienne par n

$\iff$ a est congru à b modulo n

$\iff$ $a - b$ est multiple de n

✧ Notation : $a \equiv b\,(n)$

✧ Réflexivité : $a \equiv a\,(n)$

✧ Symétrie : $a \equiv b\,(n) \Longrightarrow b \equiv a\,(n)$

✧ Transitivité : $\begin{cases} a \equiv b\,(n) \\ b \equiv c\,(n) \end{cases} \Longrightarrow a \equiv c\,(n)$

✧ Addition : $\begin{cases} a \equiv b\,(n) \\ a' \equiv b'\,(n) \end{cases} \Longrightarrow a + a' \equiv b + b'\,(n)$

✧ Multiplication : $\begin{cases} a \equiv b\,(n) \\ a' \equiv b'\,(n) \end{cases} \Longrightarrow aa' \equiv bb'\,(n)$

✧ Puissance : $a \equiv b\,(n) \Longrightarrow a^k \equiv b^k\,(n)$

Nombres premiers

Un entier p supérieur ou égal à 2 est premier si et seulement si il admet exactement deux diviseurs : 1 et lui-même

Théorème fondamental de lâarithmétique : tout entier naturel supérieur ou égal à 2 se décompose de manière unique à lâordre des facteurs près en produit de facteurs premiers : on note $p = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$

Critère d'arrêt : si n n'admet pas de diviseur premier p tel que $2 \leq p \leq \sqrt{n}$ alors n est premier

PGCD, PPCM

L'ensemble des diviseurs communs à a et b admet un plus grand élément noté PGCD(a, b)

L'ensemble des multiples communs à a et b admet un plus petit élément noté PPCM(a, b)

✧ Si $\begin{cases} a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} \end{cases}$ alors $\begin{cases} \text{PGCD}(a, b) = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} \\ \text{PPCM}(a, b) = p_1^{M_1} p_2^{M_2} \dots p_n^{M_n} \end{cases}$ oàź $m_i = \min(\alpha_i, \beta_i)$ et $M_i = \max(\alpha_i, \beta_i)$

✧ PGCD$(ka, kb) = k$PGCD(a, b)

✧ Si $a = bq + r$, alors PGCD$(a, b) =$ PGCD(b, r)

✧ Le PGCD de deux nombres non nuls est le dernier reste non nul de la suite des divisions de l'algorithme d'Euclide

Théorème de Bézout

✧ PGCD$(a, b) = 1$

$\iff$ a et b sont premiers entre eux

$\iff$ il existe deux entiers u et v tels que $au + bv = 1$

✧ Identité de Bézout : PGCD$(a, b) = d$

$\Longrightarrow$ il existe deux entiers u et v tels que $au + bv = d$

✧ Corollaire de Bézout : l'équation $ax + by = c$ admet des solutions entiers $\iff$ c est multiple de PGCD(a, b)

Théorème de Gauss

$\begin{cases} a/bc \\ \text{PGCD}(a, b) = 1 \end{cases} \Longrightarrow a/c$

Corollaires :

✧ $\begin{cases} a/c \text{ et } b/c \\ \text{PGCD}(a, b) = 1 \end{cases} \Longrightarrow ab/c$

✧ $\begin{cases} p \text{ premier} \\ p/ab \end{cases} \Longrightarrow p/a \text{ ou } p/b$