Arithmétique

Multiples, diviseurs

$b/a \Leftrightarrow \exists k \in \mathbb{Z}\ tq\ a = kb$

Congruence

A$\equiv b[n] \Leftrightarrow n/b - a \Leftrightarrow b - a = kn$ $/k \in \mathbb{N}$

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

Division euclidienne

Division de a par b , q est le quotient et r est le reste

$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z}^*)(\exists!\,(q,r) \in \mathbb{Z} \times \mathbb{N}) tq$a = bq+r et $0 \leq r < |b|$

L'équation ax+by =c /a,b,c $\in \mathbb{Z}$

L'équation admet des solutions ssi a$\wedge b\ /\ c$

PGCD	PPCM
• a$\wedge b = \|a\| \wedge \|b\|$ • a$\wedge (b \wedge c) = (a \wedge b) \wedge c$ • ab$\wedge ac = \|a\|(b \wedge c)$ • a$\wedge b/a$ $et\ a \wedge b\ /\ b$ • $a/b\ et\ a/c \Rightarrow a\ /\ b \wedge c$ • $a/b \Leftrightarrow a \wedge b = \|a\|$ • a$\wedge b = d \Leftrightarrow (\exists \alpha, \beta \in \mathbb{Z})\ d = \alpha a + \beta b$	• a$\vee b = \|a\| \vee \|b\|$ • a $\vee$ (b$\vee$c)=(a$\vee$b) $\vee$c • $a/a \vee b\ et\ b/a \vee b$ • $a/b \Leftrightarrow a \vee b = \|b\|$ • ab$\vee ac = \|a\|(b \vee c)$
• a $\wedge b/a \vee b$ • (a $\vee b) \times (a \wedge b) = \|ab\|$	

Nombres premiers

a$\wedge b = 1 \Leftrightarrow a\ et\ b\ premiers\ entre\ eux$
$\Leftrightarrow D_n = \{-n, -1, 1, n\}$

A$\wedge b = d \Leftrightarrow (\exists a', b' \in \mathbb{Z}) a = da', b = db'\ et\ a' \wedge b' = 1$

Propriétés

- Le plus petit diviseur positif de a différent de 1 est un nombre premier $a \in \mathbb{Z}^*$
- L'ensemble des nombres premiers est infini
- n n'est pas premier $\Rightarrow$ $(\exists p\ premier), p\ /\ n\ et\ p^2 \leq n$
- $(\forall p\ premier)\ p \times n\ et\ p^2 > n$

systèmes de numérotation à base b, $\boldsymbol{b} \in \mathbb{N}^* \setminus \{\mathbf{1}\}$

Soit $n \in \mathbb{N}^*\ et\ b \in \mathbb{N}^* \setminus \{1\}$

$(\exists!\ q_0 q_1 \dots q_k)\ n = q_k b^k + q_{k-1} b^{k-1} + \dots + q_1 b^1 + q_0 b^0$

avec $0 < q_k < b\ et\ 0 \leq q_i < b$, $i \in \{0,1,2,\dots,k-1\}$

Rappel

0 ! =1

n !=1$\times 2 \times 3 \times 4 \times \dots \times n$

$\mathrm{C_n^k} = \frac{n!}{k! \times (n-k)!}$

$(\mathrm{a+b})^{\mathrm{n}} = \sum_{k=0}^{n} \mathrm{C_n^k} a^k b^{n-k}$

Nombres premiers et divisibilité

- p premier et $a \in \mathbb{Z}, p\ /\ a\ ou\ p \wedge a = 1$
- p et a deux nombres premiers, $p \neq q \implies p \wedge q = 1$
- $\begin{cases} p\ premier \\ p\ /\ ab \\ a, b \in \mathbb{Z} \end{cases} \implies p\ /\ a\ ou\ p\ /\ b$
- $\begin{cases} p\ premier \\ p\ /\ ab \\ p \wedge a = 1 \end{cases} \implies p\ /\ b$
- $\begin{cases} p\ premier \\ p\ /\ a_1 a_2 \dots a_n \end{cases} \implies (\exists i \in \{1,2,\dots,n\}), p\ /\ a_i$

La décomposition en facteurs premiers

$(\forall n \in \mathbb{Z}^* \setminus \{-1,1\})(\exists p_1, p_2, \dots, p_k premiers\ et\ positifs), n = \mathcal{E} {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$

$\alpha_i \in \mathbb{N}\ et\ i \in \{1,2,\dots,k\}, \begin{cases} \mathcal{E} = 1\ si\ n \in \mathbb{N}^* \setminus \{1\} \\ \mathcal{E} = -1\ si\ n \in \mathbb{Z}^{-*} \setminus \{-1\} \end{cases}$

Le nombre de diviseurs de n est : (1+$\alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$

Soient $a = \mathcal{E} \prod_{i=1}^{k} p_i^{\alpha_i}\ et\ b = \mathcal{E} \prod_{i=1}^{k} p_i^{\beta_i}$

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

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

Critères de divisibilités

$N \equiv 0[3] \Leftrightarrow \sum_{i=0}^{n} b_i \equiv 0[3]$

$N \equiv 0[9] \Leftrightarrow \sum_{i=0}^{n} b_i \equiv 0[9]$

$N \equiv 0[5] \Leftrightarrow b_0 \equiv 0[5]$

$N \equiv 0[11] \Leftrightarrow \sum_{i=0}^{n} (-1)^i \times b_i \equiv 0[11]$

$N \equiv 0[4] \Leftrightarrow b_1 b_0 \equiv 0[4]$

$N \equiv 0[25] \Leftrightarrow b_1 b_0 \in \{00,25,50,75\}$

Théorème de BEZOUT a$\wedge b = 1 \Leftrightarrow (\exists U, V \in \mathbb{Z})\ aU + bV = 1$	**Théorème de Gauss** $\begin{cases} a/bc \\ a \wedge b = 1 \end{cases} \implies a\ /\ c$
Grand théorème de Fermat $\begin{cases} p\ premier \\ a \in \mathbb{Z} \end{cases} \implies a^p \equiv a[p]$	**Conséquences** $a/c,\ b\ /\ c\ et\ a \wedge b = 1 \implies ab\ /\ c$ $a \wedge b = 1\ et\ a \wedge c = 1 \Leftrightarrow a \wedge bc$ a$\wedge b = 1 \Leftrightarrow a^n \wedge b^m = 1, pour\ n, m \in \mathbb{N}^*$ ac $\equiv bc[n] \Leftrightarrow a \equiv b\left[\frac{n}{d}\right]\ avec\ c \wedge n = d$ ac $\equiv bc[n] \Leftrightarrow a \equiv b[n]\ avec\ c \wedge n = 1$
Petit théorème de Fermat $\begin{cases} p\ premier \\ a \in \mathbb{Z} \\ p \wedge a = 1 \end{cases} \implies a^{p-1} \equiv 1[p]$	