Arithmétique

Fiche d'Axel Chambily

Ecriture en base q q étant un entier supérieur ou égal à 2, x étant un entier quelconque, il existe une unique suite d'entiers $a_0, a_1, \cdots, a_n$ tels que : $x = a_0 + a_1 q + a_2 q^2 + \cdots + a_n q^n$ avec $\forall i \in [0, n] \quad 0 \leq a_i < q$. On écrit alors : $x = \overline{a_n a_{n-1} \cdots a_2 a_1 a_0}^q$

Passage de la base q à la base 10 On écrit bêtement la définition. Par exemple : $\overline{110111}^2 = 1 + (1 \times 2) + (1 \times 2^2) + (0 \times 2^3) + (1 \times 2^4) + (1 \times 2^5) = 1 + 2 + 4 + 16 + 32 = 55$.

Passage de la base 10 à la base q On effectue les divisions :

$$x = qx_1 + a_0, \quad x_1 = qx_2 + a_1, \quad x_2 = qx_3 + a_2, \quad \cdots, \quad x_n = q \times 0 + a_n$$

$$\begin{array}{c|l} x & q \\ \hline a_0 & x_p \end{array} \quad \begin{array}{c|l} x_p & q \\ \hline a_1 & x_2 \end{array} \quad \begin{array}{c|l} x_2 & q \\ \hline a_2 & x_3 \end{array} \quad \ddots \quad \begin{array}{c|l} x_n & q \\ \hline a_n & 0 \end{array}$$

et on obtient : $x = \overline{a_n \cdots a_1 a_0}^q$

Critères de divisibilité

- par $q-1$: $\overline{a_n \cdots a_0}^q \equiv 0(q-1) \Leftrightarrow a_n + \cdots + a_0 \equiv 0(q-1)$
- par $q+1$: $\overline{a_n \cdots 0}^q \equiv 0(q+1) \Leftrightarrow a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n \equiv 0(q+1)$
- en base 10 :
  - par 9 : $\sum_{p=0}^{n} a_p \equiv 0(9)$
  - par 11 : $\sum_{p=0}^{n} a_{2p} - \sum_{p=0}^{n} a_{2p+1} \equiv 0(11)$
  - par 3 : $\sum_{p=0}^{n} a_p \equiv 0(3)$
  - par 5 : $a_0 \equiv 0(5)$
  - par 2 : $a_0 \equiv 0(2)$

Congruences

$$a \equiv b(n) \Leftrightarrow \ a - b \text{ est un multiple de } n \ \Leftrightarrow \exists k \in \mathbb{Z} \quad a - b = kn$$

$a \equiv a'(n)$ et $b \equiv b'(n) \Rightarrow a+b \equiv a'+b'(n), \quad ab \equiv a'b'(n), \quad ka \equiv ka'(kn), \quad a^p \equiv a'^p(n)$

Division euclidienne $\forall a \in \mathbb{Z} \quad \forall b \in \mathbb{N}^* \quad \exists! q \in \mathbb{Z} \quad \exists! r \in \mathbb{N} \quad : \quad a = bq + r$ et $0 \leq r < b$

Relation "divise" $a|b \Leftrightarrow \exists k \in \mathbb{Z} \ : \ b = ka$ (b est un multiple de a)

pgcd

$$d = pgcd(a,b) \Leftrightarrow (\forall x \in \mathbb{Z} \ x|a \text{ et } x|b \Leftrightarrow x|d)$$

$$pgcd(ka, kb) = kpgcd(a,b)$$

$$pgcd\,[a, pgcd(b,c)] = pgcd\,[pgcd(a,b), c] = pgcd(a,b,c)$$

$$\text{a et b premiers entre eux} \Leftrightarrow pgcd(a,b) = 1$$

$$d = pgcd(a,b) \Leftrightarrow a = da' \text{ et } b = db' \text{ et } pgcd(a',b') = 1$$

Algorithme d'Euclide On effectue les divisions $a = bq_1 + r, \quad b = rq_1 + r_1, \quad r = r_1q_2 + r_2, \cdots$ pgcd(a,b) est le dernier reste non nul.

Théorème de Bezout a, b premiers entre eux $\Leftrightarrow \exists (u,v) \in \mathbb{Z}^2 \ : \ au + bv = 1$

Théorème de Gauss

$$a|bc \text{ et } a \text{ premier avec } b \Rightarrow a|c$$

$$k|ab \text{ et k premier } \Rightarrow k|a \text{ ou } k|b$$

$$a \text{ premier avec } b \text{ et } c \Rightarrow a \text{ premier avec } bc$$

$$b|a, \ c|a \text{ et } b \text{ et } c \text{ premiers entre eux} \Rightarrow bc|a$$

ppcm

$$m = ppcm(a,b) \Leftrightarrow \forall x \in \mathbb{Z} \quad (a|x \text{ et } b|x \Leftrightarrow m|x)$$

$$ppcm(ka, kb) = kppcm(a,b)$$

$$pgcd(a,b) \times ppcm(a,b) = ab$$

$$a \text{ et } b \text{ premiers entre eux } \Leftrightarrow ppcm(a,b) = ab$$

Nombres premiers

Entiers naturels ayant pour seuls diviseurs 1 et eux-mêmes

Il existe une infinité de nombres premiers

$$p \text{ premier et } p|a \Rightarrow \exists n \in \mathbb{N} \quad a = p^n b$$

$$p|a^n \Rightarrow p|a$$

Tout entier n s'écrit de façon unique $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Le nombre de diviseurs de n est alors $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.