3 Arithmétique

3.1 Principes fondamentaux

Définition 3.1 *Soit $a, b \in \mathbb{Z}$. On dit que* _____ *et on note* ____ _____

_____

On dit également que a est un multiple de b.

Exemples

- $7|21, -6|24$
- Pour tout $a \in \mathbb{Z}$ on a $a|0$ et $1|a$
- Pour tout $a \in \mathbb{Z}$ on a $a|a$ (Réflexivité)
- Si $a|b$ et $b|a$ alors _____ (pas antisymétrique dans $\mathbb{Z}$ mais antisymétrique dans $\mathbb{N}^*$)
- Si $a|b$ et $b|c$ alors ____ (transitivité)

Théorème de la division euclidienne dans $\mathbb{Z}$

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

_____

Les entiers q et r sont appelés, respectivement, le _____ et le ____ de la division euclidienne de a par b.

Cas particulier de la division euclidienne dans $\mathbb{N}$

Soit $a \in \mathbb{N}$, $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que :

_____

On va apporter la preuve de cette deuxième version. La preuve de la première s'obtenant ensuite en considérant des disjonctions de cas notamment suivant le signe de b.

Preuve de l'existence : Soit $E = \{n \in \mathbb{N} | bn \leq a\}$. C'est un ensemble non vide car $n = 0 \in E$. De plus pour $n \in E$ comme on a $b \geq 1$, on en déduit que $n \leq nb \leq a$. Il y a donc un nombre fini d'éléments dans E. Notons $q = max(E)$ le plus grand élément.

Alors $qb \leq a$ car $q \in E$, et $(q+1)b > a$ car $q + 1 \notin E$, donc :

$$qb \leq a < (q+1)b = qb + b$$

On définit alors $r = a - bq$ qui vérifie bien : $0 \leq r = a - bq < b$.

Preuve de l'unicité :

Supposons que (q, r) et $(q^{'}, r^{'})$ soient deux couples d'entiers qui vérifient les conditions du théorème et montrons que ces couples sont alors nécessairement égaux.

Tout d'abord $a = bq + r = bq' + r'$ et donc $b(q - q') = r' - r$. D'autre part $0 \leq r' < b$ et $0 \leq r < b$ (ou encore $-b < -r \leq 0$) et on en déduit que $-b < r' - r < b$ soit $-b < b(q - q') < b$. On peut diviser par b (car $b > 0$) et on obtient $-1 < q - q' < 1$. Comme $q - q'$ est entier, la seule possibilité est que $q - q' = 0$ soit $q = q'$. En exploitant encore la relation $b(q - q') = r' - r$, on obtient finalement $r = r'$.

Définition 3.2 (PGCD, PPCM) *Le plus grand commun diviseur de deux entiers a et b non nuls est le plus grand entier qui les divise simultanément. On le note $PGCD(a, b)$ ou $a \wedge b$.*

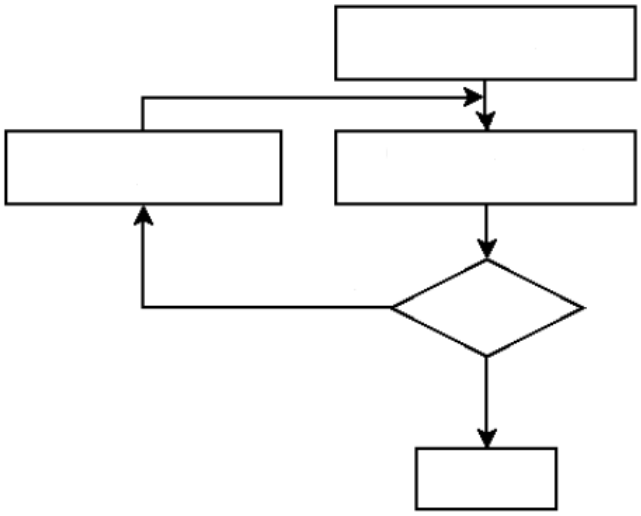
Le plus petit commun multiple de deux entiers a et b est le plus petit entier naturel qui soit multiple de ces deux nombres. On le note $PPCM(a, b)$ ou $a \vee b$.

Exemples

- $PGCD(90, 12) =$ et $PPCM(90, 12) =$
- Si $b|a$, alors $PGCD(a, b) =$

Algorithme d'Euclide dans $\mathbb{N}$

Pour deux entiers naturels a et b non nuls avec $a > b$, en écrivant la division euclidienne de a par b : $a = bq + r$, on obtient aisément que . En exploitant ceci on obtient par l'algorithme, décrit schématiquement ci-après, le PGCD de a et b.



Identité de Bézout dans $\mathbb{N}$

> Soient a, b deux entiers naturels non nuls. Soit d le PGCD de a et b.
> Alors il existe au moins un couple d'entiers relatifs (u, v) tel que _____.

Les entiers u et v sont des coefficients de Bézout. Ils peuvent s'obtenir en "remontant" l'algorithme d'Euclide ou, comme c'est illustré ci-après, en mettant en place l'algorithme d'Euclide étendu où chaque reste est exprimé comme combinaison linéaire de a et b

Algorithme d'Euclide étendu pour $(a, b) = (210, 55)$

_____ $\rightarrow$ _____

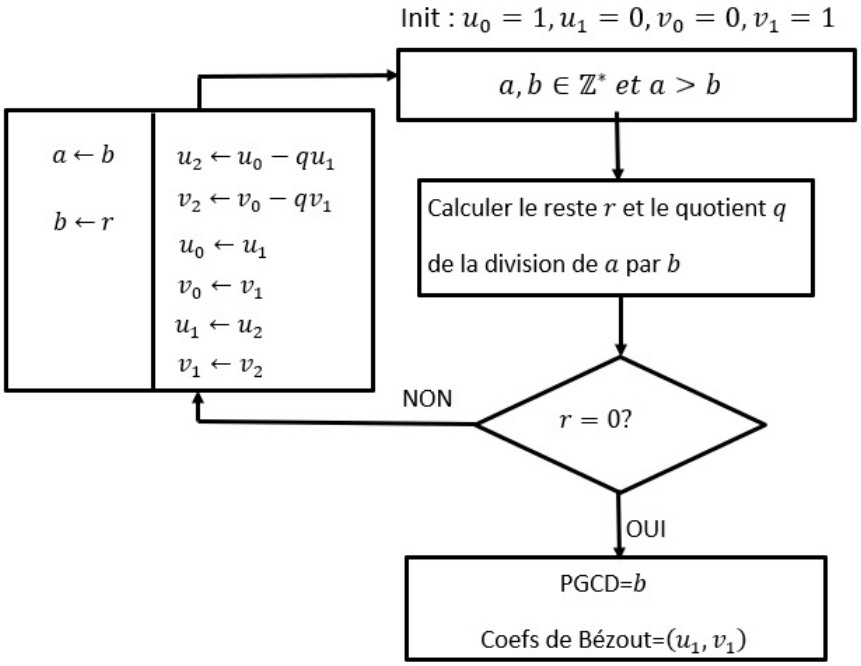
_____ $\rightarrow$ { _____ ; _____ ; _____ }

_____ $\rightarrow$ { _____ ; _____ ; _____ }

_____

On obtient donc le fait que le PGCD de 210 et 55 _____ (grâce à l'algorithme d'Euclide sur la partie gauche) et on obtient les coefficients de Bézout _____ sur la partie droite.

On remarque par ailleurs que pour exprimer un reste à une étape quelconque ($i = 2$) comme combinaison linéaire de a et b il nous faut pouvoir faire appel aux deux expressions précédentes ($i = 0$ et $i = 1$) pour les restes apparaissant dans l'algorithme d'Euclide. En posant les notations suivantes $r_i = a \times u_i + b \times v_i$, on obtient l'algorithme d'Euclide étendu :



Théorème de Bézout

Soient $a, b \in \mathbb{N}$. Les assertions suivantes sont équivalentes :

- _____
- _____

Un corollaire : Théorème de Gauss

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

Si __ et _____ alors __

Définition 3.3 *Soit $n \in \mathbb{N}^*, (a, b) \in \mathbb{Z}^2$; on dit que a est* _____ *, et on note* _____ *si et seulement si* _____

Propriété

Pour tout $n \in \mathbb{N}^*$, la relation $\equiv [n]$ est _____

Notation

Pour tout $n \in \mathbb{N}^*$, on note $\mathbb{Z}_{/n\mathbb{Z}}$ _____

____

Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe de x dans $\mathbb{Z}_{/n\mathbb{Z}}$: _____

Propriété

Soit $n \in \mathbb{N}^*$. On a, pour tout $(a, b, c, d) \in \mathbb{Z}^4$:

$$\left.\begin{array}{l} a \equiv b[n] \\ c \equiv d[n] \end{array}\right\} \Rightarrow \text{- - - - - - - - - - -}$$

et :

$$\left.\begin{array}{l} a \equiv b[n] \\ c \equiv d[n] \end{array}\right\} \Rightarrow \text{- - - - - - - - - - -}$$

En particulier si $a \equiv b[n]$, alors -

Exemples d'exploitation

- La preuve par neuf
  Principe : chaque nombre en écriture décimale étant congru modulo 9 à la somme des chiffres le composant, on peut montrer que le résultat d'un calcul est faux si les règles de compatibilité modulo 9 ne sont pas respectées. L'assertion suivante $137 \times 55 + 58^3 = 202647$ est peut-être vraie car :
  — $137 \times 55 + 58^3 \equiv$ -
  — $202647 \equiv$ - - - - - -
- L'arithmétique de l'horloge
  Principe : Une horloge avec aiguilles s'est arrêtée 50 heures plus tôt. Pour évaluer le déplacement à effectuer sur la petite aiguille on évalue - - - - - - - - - -
- Montrer que $2^{345} + 5^{432}$ est divisible par 3.
  Démonstration : $2^{345} + 5^{432} \equiv$ - .

Théorème des restes chinois

Soient $n_1, n_2, \cdots, n_k$ des entiers deux à deux premiers entre eux (ie $\forall i, j$ tels que $i \neq j$ on a $n_i \wedge n_j = 1$).
Alors pour tout k-uplet d'entiers $(a_1, a_2, \cdots, a_k)$, il existe un entier x unique modulo $n = \prod_{i=1}^{k} n_i$, tel que :

$$\left\{\begin{array}{l} \text{- - - - - - -} \\ \quad \cdots \\ \text{- - - - - - -} \end{array}\right.$$

Une solution algorithmique

Pour tout $i \in [\![1;k]\!]$, on définit $\hat{n_i} = \frac{n}{n_i} = \prod_{\substack{1 \leq l \leq k \\ l \neq i}} n_l$. Avec l'algorithme d'Euclide étendu on obtient les (u_i, v_i) tels que $u_i n_i + v_i \hat{n_i} = 1$. En posant $e_i = v_i \hat{n_i}$, on a alors : $e_i \equiv 1[n_i]$ et $e_i \equiv 0[n_j]$ pour $j \neq i$

Une solution du système est alors : $x = \sum_{i=1}^{k} a_i e_i$.

Définition 3.4 (Elément générateur) *Un élément $\overline{x}$ est dit* _____ *(ou* _____ *) si pour toute classe c de $\mathbb{Z}_{/n\mathbb{Z}}$, il existe $k \in \mathbb{N}$ tel que* _____

Propriété

Soit $x \in \mathbb{N}$ tel que $0 \leq x \leq n-1$. Les affirmations suivantes sont équivalentes :

- _____
- _____
- _____

Théorème fondamental de l'arithmétique

Tout entier strictement positif peut être écrit (on dira aussi décomposé) comme un unique produit fini de nombre premiers. Ainsi pour tout $m \in \mathbb{N}^*$, il existe un seul n-uplet $(v_i)_{1 \leq i \leq n}$ représentant des exposants associés à n nombre premiers distincts p_i (unicité à l'ordre près) :

$$m = \prod_{1 \leq i \leq n} p_i^{v_i}$$

Exemple

- $924 =$ _____
- $630 =$ _____

Petit théorème de Fermat

Soit p un nombre premier et $a \in \mathbb{Z}$.

Alors $a^p \equiv a[p]$

Et si a est un nombre premier avec p (c'est-à-dire tel que $PGCD(a,p) = 1$), alors $a^{p-1} \equiv 1[p]$

Démonstration :

Si a est multiple de p alors a^p l'est aussi (nullité modulo p), donc $a^p \equiv a[p]$

Supposons à présent que a ne soit pas un multiple de p.

L'application, qui au nombre n compris entre 0 et $p-1$, fait correspondre le produit $na[p]$, est une application de $[\![0; p-1]\!]$ dans lui-même.

Si deux nombres sont différents modulo p, alors leurs images par l'application sont aussi différentes (raisonnement par l'absurde en s'appuyant sur l'existence d'un inverse pour a). L'ensemble des $p-1$ images $a[p]; 2a[p]; \ldots; (p-1)a[p]$ coïncide donc avec les $p-1$ valeurs de l'ensemble d'arrivée $1; 2; \ldots; p-1$ (non nécessairement dans le même ordre). On a donc en faisant les produits modulo p :

$$1 \times 2 \times \cdots \times (p-1) \equiv a \times 2a \times \cdots \times (p-1)a[p]$$

Chaque élément de $[\![0; p-1]\!]$, étant premier avec p, possède un inverse modulo p et en multipliant successivement par ces inverses on obtient :

$$1 \equiv a^{p-1}[p]$$

3.2 Numération

Un **système de numération** se définit par deux éléments :

- La base du système
- Les symboles du système

Pour des applications en informatique, les systèmes les plus utilisés sont les suivants :

Système	Base	Symboles	Nb de symboles
Décimal	10	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	10
Binaire	2	0, 1	2
Octal	8	0, 1, 2, 3, 4, 5, 6, 7	8
Hexadécimal	16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F	16

Notation et signification

Soit N un entier quelconque exprimé dans une base b avec comme ensemble de symboles les éléments a_i pour i allant de 0 à $n-1$ et avec chaque $a_i < b$. N sera alors noté comme suit :

$$N = \overline{a_{n-1}a_{n-2}\cdots a_0}_b$$

On peut alors retrouver la valeur de N avec la relation suivante :

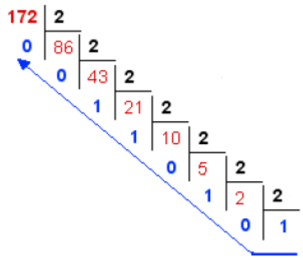
- - - - - - - - -

où la suite des coefficients $(c_i)_{0\leq i\leq n-1}$ correspond aux valeurs associées aux symboles a_i. Il y a unicité d'écriture d'un nombre dans une base.

Exemples

- $\overline{1011}_2 =$ -
- $\overline{A3F}_{16} =$ -

Conversion d'un nombre décimal en binaire On va ici utiliser la méthode par divisions euclidiennes successives avec $N = 172$. On divise par 2 sur les quotients obtenus successivement :



On peut traduire ceci par les égalités suivantes :

- - - - - - - - - - - - - - = - - - - - - - - - - - - - - - - - - -

= -

= -

= - - - - - - - -

On obtient donc bien la conversion en binaire en « remontant » les divisions successives.