27.01.2021 RUNSER Laure

Chapitre 1 : Arithmétique

↑ étude des nb entiers

On note $\mathbb{N}$ les entiers naturels ($\geqslant 0$).
$\mathbb{Z}$ les entiers (relatifs).

Si $a \in \mathbb{Z}$, on note $|a|$ sa valeur absolue.

I/ Divisibilité

Déf Soient $a, b \in \mathbb{Z}$. Si il existe $k \in \mathbb{Z}$ tel que $b = ka$

Alors on dit que :

* a divise b
* a est un diviseur de b
* b est un multiple de a
* $a \mid b$

Ex : $4 \mid 8$ mais $5 \nmid 8$

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

1) $1 \mid a$
2) $a \mid 0$
3) $a \mid a$
4) Si $a \mid b$ et $b \mid c$ alors $a \mid c$ (transitivité)
5) Si $a \mid b$ et $b \mid a$ alors $|a| = |b| \Rightarrow a = \pm b$
6) Si $a \mid b$ et $a \mid c$, $\forall k, l \in \mathbb{Z}$ alors $a \mid (kb + lc)$

Déf : Un nombre premier est un entier naturel qui a exactement 2 diviseurs positifs (1 et lui-même).

⚠ 1 n'est PAS premier

Ex : 2, 3, 5 … sont premiers

24 n'est pas premier car $6 \mid 24$.

II/ Division euclidienne

Prop : Soient $a, b \in \mathbb{N}$, $b \neq 0$

Il existe un unique entier naturel q appelé quotient de a par b, et un unique entier naturel r appelé reste de la division de a par b, tels que :

1) $a = bq + r$

2) $0 \leq r < b$

Démonstration

* **Existence**

- **Si $b > a$**, on pose $q = 0$ et $r = a$. Alors $a = 0.b + a$ et $a < b$

- **Sinon**, on pose $q = \max\{k \in \mathbb{N}, kb \leq a\}$ ↖ ensemble fini

  et $r = a - bq$

  Par construction, $bq \leq a < b(q+1)$

* **Unicité :** Soient q', r' qui satisfont les mêmes conditions.

$$bq + r = bq' + r' = a$$

$$(bq + r) - (bq' + r') = 0$$

donc $b(q' - q) = r' - r$

On peut supposer $r \leq r'$

$$\left.\begin{array}{l} \text{donc on a } 0 \leq r' - r < b \\ \text{Or } b \mid r' - r \end{array}\right\} \Rightarrow r' - r = 0 \quad \text{donc } q' - q = 0 \text{ aussi}$$

Donc $(q, r) = (q', r')$

Remarque : On peut étendre la division euclidienne au cas où a et/ou b sont négatifs

⚠ Le reste doit tjrs être POSITIF sinon (q, r) n'est plus unique.

Ex :
$11 = 3 \times 3 + 2$
$-11 = -4 \times 3 + 1$

Remarque On a que $b \mid a$ ssi le reste de la division de a par b est 0.

III / Application : écriture en base $\mathbb{N}$

<u>Ex :</u> en base 10 $\longrightarrow$ $213 = 2 \times 10^2 + 1 \times 10^1 + 3 \times 10^0$

> <u>Théorème</u> : Soit $N \geq 2$ un entier.
>
> Alors tout entier naturel n s'écrit de façon unique
>
> $$n = i_0 + i_1 N + i_2 N^2 + \dots + i_k N^k$$
>
> avec $0 \leq i_0, i_1, \dots, i_k < N$ et $i_k \neq 0$

<u>Démonstration</u>

On fait la division de n par N : $n = Nq_0 + r_0$

On pose $i_0 = r_0$

Si $q_0 = 0$ on s'arrête

Sinon on divise q_0 par N : $q_0 = Nq_1 + r_1$

et on pose $i_1 = r_1$

Par construction :
$$\begin{aligned} n &= Nq_0 + i_0 \\ &= N(Nq_1 + i_1) + i_0 \\ &= i_0 + i_1 N + N^2 q_1 \end{aligned}$$

Si $q_1 = 0$ on arrête.

Sinon on divise q_1 par N ...

Comme $q_0, q_1, \dots$ sont positifs et sont de plus en plus petits, au bout d'un moment on arrive à 0.

On peut montrer que cette écriture est unique de la même manière que pour la division euclidienne.

<u>Ex :</u>
- Si $N = 10$, les $(i_0, i_1, \dots, i_k)$ sont juste les chiffres de l'écriture de n.

<u>Remarque</u>
En général, on appelle ça écriture de n en base N et on note $(i_k\, i_{k-1} \dots i_0)_N$

<u>Ex :</u> $N = 2$

$213 = 106.2 + \overset{i_0}{1}$
$106 = 53.2 + 1$
$53 = 26.2 + \underset{i_2}{1}$

$26 = 13.2 + 0$
$13 = 6.2 + 1$
$6 = 3.2 + \underset{i_5}{0}$

$3 = 1.2 + 1$
$1 = 0.2 + \underset{i_7}{1}$

$213 = (\overset{i_7}{1}1010 11\overset{i_0}{1})_2$

Ex : $N = 16 = 2^4$ On utilise comme chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

$213 = 13 . 16 + 5$ $\leftarrow i_0$

$16 = 0 . 16 + 13$ $\leftarrow i_1$

$213 = (\underset{=13}{D}\,5)_{16}$

IV/ PPCD, PPGM

Déf : Soient $a, b \in \mathbb{Z}$

On dit que $d \in \mathbb{Z}$ est un diviseur commun de a et de b ssi $d \mid a$ et $d \mid b$

——— $m \in \mathbb{Z}$ ——— multiple ——————— $a \mid m$ et $b \mid m$

Ex : Les diviseurs communs positifs de 90 et 60 sont 1, 2, 3, 5, 6, 10, 15 et 30.

Remarque : 1 et -1 sont tjrs des diviseurs communs de a et b.

$\pm a . b$ ——————— multiples ———————

Remarque : Si c est un diviseur commun de a et b, alors $|c| \leq |a|$ et $|c| \leq |b|$

donc l'ensemble des diviseurs communs de a et b est fini.

De même, l'ensemble des multiples communs de a et b est minoré, donc il a un plus petit élément.

Définition

- On appelle plus gd diviseur commun de a et b, noté PGCD (a, b) ou $a \wedge b$, le plus gd diviseur.
- ——— plus petit multiple commun ———, noté PPGM (a, b) ou $a \vee b$, le plus petit multiple > 0.

Remarque : PGCD (a, 0) = a

⚠ PGCD (0, 0) n'existe pas

Définition : Soient a et b non nuls.
On dit que a et b sont premiers entre eux si PGCD (a, b) = 1.

Lemme : Soient $a, b \in \mathbb{Z}$, $d = PGCD(a, b)$

Alors on pose $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ et donc a' et b' sont premiers entre eux.

Démonstration

Soit d' un diviseur commun positif de a' et b'.

Alors $d' | a'$ donc $d'd | \underbrace{a}_{= a'd}$. De même $d'd | b$.

Donc $d'd$ est un diviseur commun de a et b.

Comme $d' \geq 1$, $d'd \geq d$

Mais par hypothèse d est le plus gd diviseur commun.

Donc $d' = 1$.

Donc a' et b' sont premiers entre eux.

V/ Calcul du PGCD, théorème de Bézout

Lemme pratique pour calculer le PGCD :

Soient $a, b \in \mathbb{N}$ non nuls et r le reste de la division de a par b. Alors $PGCD(a, b) = PGCD(r, b)$.

Démonstration :

Soit (q, r) le résultat de la division euclidienne de a par b, et d un diviseur commun de a et b.

Donc $d | r = a - bq$

De même si $d | b$ et $d | q$ alors $d | a = bq + r$

Donc l'ensemble des diviseurs communs de a et b est égal à l'ensemble des diviseurs commun de b et r.