Exposé 9 :

Division Euclidienne de $\mathbb{Z}$. Unicité du quotient et du reste. Applications.

0 - Pré-Requis :

- Majorants, Minorants, plus petit elt, plus gd elt.
- Thm : Toute partie non vide de $\mathbb{Z}$ majorée (resp minorée) admet un plus grand elt (resp plus petit elt).
- Diviseurs
- Sous groupes.

I Division Euclidienne.

1) Dans $\mathbb{Z}$

Thm : Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tq $a = bq + r$ $0 \leq r < |b|$

[Existence : Supposons $b > 0$ et posons $B = \{k \in \mathbb{Z} \text{ tq } kb \leq a\}$

B est une partie non vide de $\mathbb{Z}$ (car si $a \geq 0$, alors $0 \in B$
si $a < 0$, alors $a \in B$)

B est majorée par $\max(0,a)$ donc B admet un plus gd élt q qui vérifie
$qb \leq a < (q+1)b$

lorsque $b < 0$ on se ramène au cas précédent avec $(-b)q + r = b(-q) + r$

Ds tous les cas, on a prouvé l'existence de $q \in \mathbb{Z}$
et $r \in \mathbb{N}$ tq $r = a - bq$ et donc a bien $0 \leq r < |b|$

Unicité :
(q,r) et $(q',r') \in \mathbb{Z} \times \mathbb{N}$
tq $a = bq + r$ et $a = bq' + r'$
$0 \leq r < |b|$ $\quad$ $0 \leq r' < |b|$
$b(q - q') = r' - r$
or $|r' - r| < |b|$ et $b \mid r' - r$ $\Rightarrow r' - r = 0$ dc $r = r'$ et $q = q'$]

Def : L'opération ainsi définie, associant au couple (a,b) le couple (q,r) est appelée division euclidienne de a par b.
a est appelé le dividende, b le diviseur, q le quotient et r le reste.

2) Dans $\mathbb{N}$

Def. Soit $(a,b) \in \mathbb{N} \times \mathbb{N}^*$ il existe un unique couple $(q,r) \in \mathbb{N} \times \mathbb{N}$ tq $a = bq + r$ et $0 \leq r < b$

[Existence : considérer $B = \{k \in \mathbb{N} \text{ tq } kb \leq a\}$ après m̂ chose.
Unicité : m̂ chose.]

Rq : Si $r = 0$, on dit que b divise a, que b est est diviseur de a, que a est un multiple de b, et on note $b \mid a$

II Applications :

1) Algorithme d'Euclide :

Thm : Soit $a, b \in \mathbb{Z}^*$ l'ensemble des diviseurs communs à a et b admet un plus grand élément d et on note $d = pgcd(a,b)$

[$D = \{$ensemble des diviseurs communs à a et b$\}$. Il suffit de montrer que D est une partie non vide et majorée de $\mathbb{Z}$.
$\Rightarrow$ Elle admet donc un plus grand elt].

Thm d'Euclide : Soit a, b, q, r non nuls $a = bq + r \Rightarrow pgcd(a,b) = pgcd(b,r)$

[$a \wedge b \mid a$, $a \wedge b \mid b \Rightarrow a \wedge b \mid bq$ or $r = a - bq$ dc $a \wedge b \mid r$ et $a \wedge b \mid b$ $\Rightarrow a \wedge b \mid r \wedge b$ car $r \wedge b$ est le plus gd div commun à r et b.

De même $b \wedge r \mid b$, $b \wedge r \mid r \Rightarrow b \wedge r \mid bq$ or $a = bq + r$ dc $b \wedge r \mid a$, $b \wedge r \mid b$ $\Rightarrow b \wedge r \mid a \wedge b$ d'où l'égalité]

On en déduit l'algorithme d'euclide pour la recherche du $pgcd(a,b)$ où a, b sont des entiers non nuls.

Soit $a, b \in \mathbb{N}^*$, $\exists! (q_1, r_1) \in \mathbb{N}^2$ $a = bq_1 + r_1$ $0 \leq r_1 < b$ (div euclidienne)

- si $r_1 = 0$ alors $pgcd(a,b) = b$
- si $r_1 \neq 0$ $pgcd(a,b) = pgcd(b, r_1)$ (Thm d'Euclide)

$$\exists! (q_2, r_2) \in \mathbb{N}^2 \quad b = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

...

Donc on construit une suite (r_n) strict décroissante et minorée de $\mathbb{N}$ donc $\exists k \in \mathbb{N}$ tq $r_k \neq 0$ et $r_{k+1} = 0$

De plus on a (Thm euclide) $pgcd(a,b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \dots = pgcd(r_k, r_{k+1}) = r_k$
(ie dernier reste non nul).

Exemple : $a = 93$ et $b = 66$

$93 = 66 \times 1 + 27$	$93 \wedge 66 = 66 \wedge 27$
$66 = 27 \times 2 + 12$	$66 \wedge 27 = 27 \wedge 12$
$27 = 12 \times 2 + \boxed{3}$	$27 \wedge 12 = 12 \wedge 3 = 3$
$12 = 3 \times 4 + 0$	Donc $\boxed{93 \wedge 66 = 3}$

2) Numération en base $b \in \mathbb{N} \setminus \{0, 1\}$

Thm et Def : Pour tout x entier naturel non nul, il existe un unique $m \in \mathbb{N}$ et $x_0, \dots, x_m \in \mathbb{N}$ tq i) $x_m \neq 0$
ii) $\forall i \in [0, m]$, $0 \leq x_i < b$ et $x = x_0 + bx_1 + \dots + b^m x_m$

On notera $x = \overline{x_m x_{m-1} \dots x_0}^{\,b}$, c'est l'écriture en base b de x.

[$x = bq_0 + r_0$ $0 \leq r_0 < b$ (Div euclidienne de x par b.)

On a $q_0 \leq \frac{x}{b} < x$ car $b > 1$

$q_0 = bq_1 + r_1 \quad 0 \leq r_1 < b$ (div eucl de q_0 par b).

De même $q_1 < bq_1 \leq q_0$ car $b > 1$ et $r_1 \geq 0$

...

$q_p = bq_{p+1} + r_p \quad 0 \leq r_p < b$

De $\hat{m}$ $q_{p+1} < bq_{p+1} \leq q_p < q_{p-1} < \cdots < q_1 < q_0$

Donc on définit une suite $(q_n)_n$ strict décroissante d'entiers positifs (car on effectue des divisions euclidiennes de $\mathbb{N}$ de q_i par b).

Donc $\exists m \in \mathbb{N}$ tq $q_m = 0$

$x = bq_0 + r_0$

$= b(q_1 b + r_1) + r_0 = b^2 q_1 + br_1 + r_0$

$= b^2(bq_2 + r_2) + br_1 + r_0 = b^3 q_2 + b^2 r_2 + br_1 + r_0$

$= b^m q_{m-1} + b^{m-1} r_{m-1} + \cdots + br_1 + r_0$

or $q_{m-1} = b\underset{0}{\underset{\shortparallel}{q_m}} + \underset{\neq 0}{r_m}$ car $q_{m-1} \neq 0$ Sinon on aurait arrêter.

$x = b^m r_m + b^{m-1} r_{m-1} + \cdots + br_1 + r_0$

D'ou $x_i = r_i \; \forall i \in \{0, .., m\}$ or $0 \leq r_i < b$ (car div eucl)

et $x_m \neq 0$ Donc on a bien le résultat souhaité $\rrbracket$.

3) Sous groupes de $(\mathbb{Z}, +)$

Thm: Tout les sous groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$.

Thm: soit $(a,b) \in \mathbb{Z}^*$. l'ensemble des diviseurs commun à a et b admet un plus grand élément d'elt on note $d = pgcd(a,b)$

[Soit D cet ensemble
* D non vide car $1|a$ et $1|b$ dc $1 \in D$
* $|a|$ est le plus grand diviseur de a donc tout élt de D est inférieur à $|a|$
D est donc une partie non vide et majorée de $\mathbb{Z}$ elle admet donc un plus grand élément]

Thm: Tout les sous groupe de $\mathbb{Z}$ st de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

[H ss groupe de $\mathbb{Z}$

_ $H = \{0\}$ on a $H = 0.\mathbb{Z}$

- Si $H \neq \{0\}$, $\exists c \neq 0$ tq $c \in H$ et $-c \in H$ (car H ss groupe)

$\Rightarrow$ H contient au moins un elt strict positif.

Si on considère l'ensemble $\{x \in H, x > 0\}$, c'est ensemble est non vide car il contient c ou -c et est un sous ensemble de $\mathbb{N}$

$\Rightarrow$ H sous ensemble non vide de $\mathbb{N}$, H contient un plus petit élément m.

On a donc $m > 0$.

$\forall x \in H, \exists ! (q,r) \in \mathbb{Z} \times \mathbb{N}, x = mq + r \quad 0 \leq r < m$ (div euc de x par m)

$$r = \underbrace{\underbrace{x}_{\in H} - \underbrace{mq}_{\in H}}_{\in H} \text{ et } r > 0 \text{ donc } r \in \{x \in H, x > 0\}$$

et $r < m$ Absurde !

Donc $r = 0$ et $x = mq$

Donc $H \subset a\mathbb{Z}$

Réciproquement si on considère un elt de $a\mathbb{Z}$ il est clairement dans H (puisque H ss groupe de $\mathbb{Z}$)

Donc $H = a\mathbb{Z}$]