Exposé 9 : Division Euclidienne dans $\mathbb{Z}$. Unicité du quotient et du reste. Applications.

Prérequis[1] :
-Majorants, minorants, plus petit élément, plus grand élément
-Théorème : toute partie non vide de $\mathbb{Z}$ majorée (repect. minorée) admet un plus grand élément (resp. un plus petit élément).
-Diviseurs
-Sous groupes

Introduction : lorsque l'on effectue une division de deux entiers relatifs à la calculatrice, elle affiche très souvent un nombre à virgule. Ici, on étudie une division particulière où n'interviennent que des entiers.

1 Division Euclidienne

1.1 Division Euclidienne dans $\mathbb{Z}$

Théorème : Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tq. $a = bq + r$, avec $0 \leqslant r < |b|$

preuve : -Existence : supposons $b > 0$ et posons $\mathcal{B} = \{k \in \mathbb{Z}$, tel que $kb \leqslant a\}$
$\mathcal{B}$ est une partie non vide de $\mathbb{Z}$ (car si $a \geqslant 0$, alors $0 \in \mathcal{B}$, et si $a < 0$, alors $a \in \mathcal{B}$).
$\mathcal{B}$ est majorée par $max(0, a)$ donc $\mathcal{B}$ admet un plus grand élément q qui vérifie $qb \leqslant a < (q + 1)b$ (donc $qb \leqslant a < bq + b$ donc $\exists r \in \mathbb{N}$ tq. $a = bq + r$ pour le q précédemment déterminé)
Lorsque $b < 0$ on se ramène au cas précédent avec $(-b)q + r = b(-q) + r$. Dans tous les cas, on a prouvé l'existence de $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que $r = a - bq$, d'où $0 \leqslant r < |b|$.
-Unicité : soient (q, r), $(q', r') \in (\mathbb{Z} \times \mathbb{N})$ tels que $a = bq + r$ et $a = bq' + r'$ avec $0 \leqslant r < |b|$ et $0 \leqslant r' < |b|$.
On a : $b(q - q') = r - r'$ donc $|b|.|q - q'| = |r - r'|$ or $|r - r'| < |b|$, d'où $0 \leqslant |q - q'| < 1$ (car $b \neq 0$), d'où $q = q'$ et $r = r'$. □

Définition : 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.

Remarque : si $r = 0$, on dit que b divise a, que b est un diviseur de a, que a est un multiple de b, et on note $b|a$

1.2 Division Euclidienne dans $\mathbb{N}$

Théorème : Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tq. $a = bq + r$, avec $0 < r \leqslant b$

preuve :
-Existence : posons $\mathcal{B} = \{k \in \mathbb{N}$, tel que $kb \leqslant a\}$ après idem.
-Unicité : idem.

[1] L'exposé a été tapé et présenté à Bordeaux(4) le 19/10/2005 par Gwendal Haudebourg. Mis à jour le 31/07/2007.

2 Applications

2.1 Algorithme d'Euclide

Théorème : soient $a, b \in (\mathbb{Z}^*)^2$. L'ensemble des diviseurs communs à a et b admet un plus grand élément.

Définition : soient $a, b \in (\mathbb{Z}^*)^2$. Le plus grand diviseur commun à a et b est appelé $pgcd$ de (a, b), et on note le note $pgcd(a, b)$ ou $a \wedge b$.

Théorème (d'Euclide) : soient a, b, q, r non nuls. Alors $a = bq + r \Rightarrow pgcd(a, b) = pgcd(b, r)$.

preuve : (du théorème d'Euclide)
$pgcd(a, b)|b$ donc $pgcd(a, b)|bq$, $pgcd(a, b)|a$ et $r = a - bq$ donc $pgcd(a, b)|r$ d'où $pgcd(a, b)|pgcd(r, b)$ car $pgcd(r, b)$ est le plus grand diviseur commun à r et b.
De même $pgcd(b, r)|b$, $pgcd(b, r)|r$ donc $pgcd(b, r)|bq$ or $a = bq + r$ donc $pgcd(b, r)|a$, $pgcd(b, r)|b$ donc $pgcd(b, r)|pgcd(a, b)$ d'où l'égalité. □

On en déduit l'algorithme d'Euclide dans $\mathbb{N}$ pour la recherche du $pgcd(a, b)$ où a, b sont des entiers non nuls :
Soient $(a, b) \in (\mathbb{N}^*)^2$. $\exists!(q_1, r_1) \in \mathbb{N}^2$ tq. $a = bq_1 + r_1$, $0 \leqslant r_1 < b$ (division Euclidienne)
-si $r_1 = 0$ alors $pgcd(a, b) = b$
-si $r_1 \neq 0$ alors $pgcd(a, b) = pgcd(b, r_1)$ (théorème d'Euclide). $\exists!(q_2, r_2) \in (\mathbb{Z}^*)^2$ tq. $b = r_1 q_2 + r_2$, $0 \leqslant r_2 < r_1$
...
On construit ainsi une suite $(r_n)_n$ de $\mathbb{N}$ strictement décroissante et minorée (par 0), donc $\exists k \in \mathbb{N}$ tq. $r_k \neq 0$ et $r_{k+1} = 0$.
De plus, on a (théorème d'Euclide) $pgcd(a, b) = pgcd(b, r_1) = pgcd(r_1, r_2) = ... = pgcd(r_k, r_{k+1}) = r_k$ (ie dernier reste non nul).

Exemple : $a = 93$ et $b = 66$ $93 = 66 \times 1 + 27$ d'où $pgcd(93, 66) = pgcd(66, 27)$

$66 = 27 \times 2 + 12$ d'où $pgcd(66, 27) = pgcd(27, 12)$
$27 = 12 \times 2 + 3$ d'où $pgcd(27, 12) = pgcd(12, 3) = 3$
$12 = 3 \times 4 + 0$ d'où $pgcd(93, 66) = 3$

2.2 Numération en base $b \in \mathbb{N} - \{0, 1\}$

Théorème : pour tout x entier naturel non nul, il existe un unique $n \in \mathbb{N}$ et un unique $n + 1$-uplets $x_0, ..., x_n \in \mathbb{N}$ tel que :

1. $x_n \neq 0$
2. $\forall i = 0...n$, $0 \leqslant x_i < b$ et $x = x_0 + bx_1 + ... + b^n x_n$

Définition : on notera $x = \overline{x_n x_{n-1} ... x_0}^b$, c'est l'écriture en base b de x

preuve (Théorème) : Soit $x = bq_0 + r_0$, $0 \leqslant r_0 < b$ (division euclidienne de x par b)

On a $q_0 \leqslant \dfrac{x}{b} < x$ car $b > 1$, donc $q_0 b \leqslant x < bx$
$q_0 = bq_1 + r_1$ où $0 \leqslant r_1 < b$ (division Euclidienne de q_0 par b)
De même $q_1 < bq_1 \leqslant q_0$ car $b > 1$ et $r \geqslant 0$ (car $q_2 b \leqslant q_1 < q_1 < q_1 b$ et $q_1 b \leqslant q_0 < q_0 b$)
...
$q_p b = bq_{p+1} + r_p$ où $0 \leqslant r_p < b$
D'où $q_{p+1} < bq_{p+1} \leqslant q_p < q_{p-1} < ... < q_1 < q_0$

On définit ainsi une suite $(q_n)_n$ strictement décroissante d'entiers positifs (car on effectue des divisions Euclidiennes dans $\mathbb{N}$ de q_i par b). Donc il existe $n \in \mathbb{N}$ tq. $q_n = 0$
$x = bq_0 + r_0 = b(q_1 b + r_1) + r_0 = b^2 q_1 + br_1 + r_0 = b^2(bq_2 + r_2) + br_1 + r_0 = b^3 q_2 + b^2 r_2 + br_1 + r_0$
$= ...$
$= b^n q_{n-1} + b^{n-1} r_{n-1} + ... + br_1 + r_0$
or $q_{n-1} = bq_n + r_n$ et $q_n = 0$, $q_{n-1} \neq 0$ (sinon on s'arrête avant) donc $r_n \neq 0$ et $q_n = r_n$
d'où $x = b^n r_n + b^{n-1} r_{n-1} + ... + br_1 + r_0$
d'où $x_i = r_i \forall i \in \{0, ..., n\}$ or $0 \leqslant r_i < b$ (division Euclidienne) et $x_n \neq 0$, donc on a bien le résultat souhaité. □

Exemples :

Ecriture en base 3 de 85 (que l'on note aussi $\overline{85}^{10}$)
$85 = 28 \times 3 + 1$ ($q_0 = 28$)
$28 = 9 \times 3 + 1$ ($q_1 = 9$)
$9 = 3 \times 3 + 0$ ($q_2 = 3$)
$3 = 1 \times 3 + 0$ ($q_3 = 1$)
$1 = 0 \times 3 + 1$ ($q_4 = 0$, on s'arrête)
donc 85 = 10011 en base 3 ie $\overline{85}^{10} = \overline{10011}^{3}$. On a bien : $85 = 3^4 \times 1 + 3^3 \times 0 + 3^2 \times 0 + 3^1 \times 1 + 3^0 \times 1$.
Ecriture en base 4 de $\overline{16}^{16}$
$\overline{16}^{16} = 1 \times 16^1 + 6 \times 16^0 = 22 = 1 \times 4^2 + 1 \times 4^1 + 2 \times 4^0 = \overline{112}^{4}$

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

Théorème : tous les sous groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$, $n \in \mathbb{N}$

3 Compléments

3.1 Preuves

Théorème : soient $a, b \in (\mathbb{Z}^*)^2$. L'ensemble des diviseurs communs à a et b admet un plus grand élément, noté $pgcd(a, b)$.

preuve : soit $\mathcal{D}$ cet ensemble. $\mathcal{D}$ est non vide car $1|a$ et $1|b$, donc $1 \in \mathcal{D}$.
$|a|$ est le plus grand diviseur de a donc tout élément de $\mathcal{D}$ est inférieur à $|a|$.
$\mathcal{D}$ est donc une partie non vide et majorée de $\mathbb{Z}$. Elle admet donc un plus grand élément. □

Théorème : tous les sous groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$, $n \in \mathbb{N}$

preuve : Soit H sous-groupe de $\mathbb{Z}$
Si $H = \{0\}$, on a $H = 0.\mathbb{Z}$
Si $H \neq \{0\}$, $\exists c \neq 0$ tel que $c \in H$ et $-c \in H$ (car H groupe), donc H contient au moins un élément strictement positif.
Si on considère l'ensemble $H^+ := \{x \in H, x > 0\}$, cet ensemble est non vide car contient c ou $-c$, et est un sous ensemble de $\mathbb{N}$. Donc H^+ est un sous ensemble non vide de $\mathbb{N}$, donc contient un plus petit élément n (car $\mathbb{N}$ minorée par 0). On a donc $n > 0$.
$\forall x \in H, \exists (q, r) \in \mathbb{Z} \times \mathbb{N}$, $x = nq + r$, $0 \leqslant r < n$ (division Euclidienne de x par n), donc $r = x - nq$ or $x \in H$, $nq \in H$ donc $r \in H$. Si $r > 0$, alors $r \in H^+$ et $r < n$ absurde !
Donc $r = 0$ et $x = nq$, donc $H^+ \subset a\mathbb{Z}$, $a \in \mathbb{N}$ donc $H \subset a\mathbb{Z}$.
Réciproquement, si on considère un élément de $a\mathbb{Z}$, il est clairement dans H (puisque H sous groupe de $\mathbb{Z}$), donc $H = a\mathbb{Z}$. □

3.2 Remarques

Dans la division Euclidienne "classique", bq n'est pas forcément le multiple de b le plus proche de a (ex : $a = 5, b = 3, q = 1, r = 2, bq = 3$ moins proche de 5 que $6 = 3 \times 2$).

Dans la division Euclidienne "classique", si on remplace la condition $0 \leqslant |b|$ par $|r| < |b|$ (donc avec $r \in \mathbb{Z}$ ie peut être négatif), il n'y a plus unicité du couple (q, r) (ex : $10 = 3 * 3 + 1 = 4 * 3 - 2$). Par ailleurs, on a le corollaire suivant :

Corollaire : pour tout couple $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, il existe un couple (q,r) tel que $a = bq + r$ et $|r| \leqslant \frac{|b|}{2}$

remarque : on obtient ainsi le multiple de b le plus proche de a, mais on perd l'unicité (quand $|r| = \frac{|b|}{2}$ ex : $10 = 4 \times 2 + 1 = 4 \times 3 - 2$)
Si on effectue les divisions Euclidiennes successives de cette manière, on obtient un algorithme d'Euclide "amélioré" (ie tend plus vite vers le $pgcd$).

On définit le $pgcd(a, b)$ lorsque $(\mathbb{Z}^*)^2$ car $(0, 0)$ n'a pas de plus grand diviseur. Comme convention, on pose $pgcd(0, 0) = 1$ (?)

Méthode de détermination des quotients et du reste : (la descente de Fermat)
Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$
-si $a < b$, alors le couple $(0, a)$ est le couple (quotient, reste) cherché
-si $a \geqslant b$, soit $q_1 \in \mathbb{N}^*$ tel que $bq_1 \leqslant a$. On pose $r_1 = a - bq_1$. Si $r_1 < b$, (q_1, r_1) est le couple recherché.
Si $r_1 \geqslant b$, soit $q_2 \in \mathbb{N}^*$ tel que $bq_2 \leqslant r_1$ et on pose $r_2 = r_1 - bq_2$.
Si $r_2 < b$, le couple $(q_1 + q_2, r_2)$ convient, sinon, on recommence...
On construit ainsi deux suites $(q_n)_n$ et $(r_n)_n$ tq. si $r_n \geqslant b$ alors q_{n+1} est tele que $bq_{n+1} \leqslant r_n$, et $r_{n+1} = r_n - bq_{n+1}$
La suite $(r_n)_n$ est strictement décroissante dans $\mathbb{N}$, donc il existe un rang n pour lequel $r_n < b$, donc $(r_n)_n$ est une suite finie, et $(q_1 + ... + q_n, r_n)$ est le couple recherché.

3.3 Comentaires-compléments du professeur Z.

On peut dans cette leçon étudier d'abord les sous groupes de $(\mathbb{Z}, +)$, puis définir le $pgcd(a, b)$ et le $ppcm(a, b)$ par :
$\forall a, b \in \mathbb{N} \times \mathbb{N}^*, \exists! d \in \mathbb{Z}$ tq. $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. d s'appelle le $pgcd$ de a et b
$\forall a, b \in \mathbb{N} \times \mathbb{N}^*, \exists! m \in \mathbb{Z}$ tq. $a\mathbb{Z} \bigcap b\mathbb{Z} = m\mathbb{Z}$. m s'appelle le $ppcm$ de a et b

Autre définition possible :
d est appelé $pgcd(a, b)$ si(si) $d|a, d|b$ et si $d'|a, d'|b$ alors $d'|d$
m est appelé $ppcm(a, b)$ si(si) m multiple de a et de b, et si m' multiple de a et b alors m' multiple de m

On peut définir voir la division Euclidienne dans $\mathbb{Z}$ comme :
Théorème : Soient $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tq. $a = bq + r$, avec $0 < r \leqslant b$