Division euclidienne dans $\mathbb{Z}$, unicité du quotient et du reste. Applications.

Pré-requis:
- $\mathbb{Z}$ est un anneau commutatif unitaire totalement ordonné et archimédien possédant la propriété que tout ensemble non vide majoré possède un plus grand élément.
- Notion de divisibilité.

0.1 Division euclidienne dans $\mathbb{Z}$.

Théorème 0.1.1.
(Division euclidienne dans $\mathbb{Z}$)
$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, $\exists ! (q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < |b|.$$

Démonstration. Soit $b > 0$, on considère $E = \{n \in \mathbb{Z} | nb \leq a\}$ E est non vide et majoré car $\mathbb{Z}$ est archimédien. Soit q le plus grand élément de E alors $qb \leq a < (q+1)b$ et si $r = 1 - bq$, le couple (q,r) convient.

Si $b < 0$, on travail avec $-b$ qui nous donne $a = (-b)q + r = b(-q) + r$ et $(-q, r)$ convient.

Si (q', r') est un autre couple satisfaisant à $a = bq' + r'$ avec $0 \leq r' < |b|$ alors par différence on obtient $|r - r'| = |b| \cdot |q - q'|$ et comme $|r - r'| < |b|$ alors $|q - q'| < 1$ donc $q = q'$ et $r = r'$ d'où l'unicité. ∎

Définition 0.1.2.
Avec les même notations que dans le théorème précédent, q est appelé le quotient de la division euclidienne de a par b et r le reste.
On notera $q = a \div b$.

Remarque: Dans le cas $r = 0$, cela équivaut à dire que b divise a que l'on pourra noter $b|a$.

Propriétés 0.1.3.

1. Si $c \in \mathbb{Z}^*$ divise a ou b on a:
$$(a + b) \div c = (a \div c) + (b \div c).$$
2. Pour tout couple (b, c) de $\mathbb{Z}^*$ on a, pour $b > 0$ et $b|a$:
$$a \div (bc) = (a \div b) \div c.$$

Démonstration.
1. Supposons par exemple que $c|a$, alors il existe q' dans $\mathbb{Z}$ tel que $a = cq'$ et il existe q'' dans $\mathbb{Z}$ tel que $b = cq'' + r''$ avec $0 \leq r'' < |c|$ alors $a + b = (q' + q'')c + r''$ avec $0 \leq r'' < |c|$.
2. $a = bcq + r$ avec $0 \leq r < |bc|$ et $a = bq'$, ainsi $q' = cq + \frac{r}{b}$ avec $0 \leq \frac{r}{b} < c$.

∎

0.2 Applications.

0.2.1 Congruences.

Définition 0.2.1.
On dit que a est congru à b modulo n lorsque n divise $(b-a)$, on note alors

$$a \equiv b[n].$$

Théorème 0.2.2.
$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}$, $a \equiv b[n]$ si, et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration. $\boxed{\Leftarrow}$ Si a et b ont le même reste dans la division euclidienne par n alors:

$$a = nq + r \quad \text{où} \quad 0 \leq r \leq n-1$$

et

$$b = nq' + r$$

donc $a - b = n(q - q')$ d'où $a \equiv b[n]$.
$\boxed{\Rightarrow}$ Si $a \equiv b[n]$ alors par hypothèse, il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ or $a - b = (q-q')n + r - r'$. Comme $n|(a-b)$, alors $n|(r-r')$ mais $1 - n \leq r - r' \leq n - 1$ et le seul multiple de n dans $[1-n, n-1]$ est 0 donc $r - r' = 0$.

■

0.2.2 Système de numération.

Théorème 0.2.3.
Soit $a \in \mathbb{N}$, $a \geq 2$. Pour tout $x \in \mathbb{N}^*$, il existe un unique entier n et un unique $(n+1)-$uplet d'entiers naturels $(x_0, x_1, \ldots, x_n)$ tels que:

$$\begin{cases} x_n \neq 0 \\ \forall i \in \{0, 1, \ldots, n\},\ x_i < a \end{cases}$$

et

$$x = x_n a^n + x_{n-1} a^{n-1} + \ldots + x_0.$$

Démonstration. Montrons l'existence par récurrence sur x:

- Si $x < a$ alors $x_0 = x$.
- Si $x \geq a$ alors supposons la propriété vraie pour tout $y < x$. On a $x = aq + r$ avec $r < a$ et $q < x$ donc par hypothèse de récurrence $q = q_n a^n + q_{n-1} a^{n-1} + \ldots + q_0$ et donc $x = q_n a^{n+1} + q_{n-1} a_n + \ldots + q_0 a + r$.

Montrons maintenant l'unicité de cette écriture:

Supposons que

$$\begin{aligned} x &= x_n a^n + x_{n-1}a^{n-1} + \ldots + x_1 a + x_0 \\ &= x'_{n'} a^{n'} + x'_{n'-1}a^{n'-1} + \ldots + x'_1 a + x'_0. \end{aligned}$$

Alors, x_0 et x'_0 apparaissent comme le reste de la division euclidienne de x par a et par unicité du reste, $x_0 = x'_0$. Ainsi

$$x_n a^{n-1} + x_{n-1}a^{n-2} + \ldots + x_1 = x'_{n'} a^{n'-1} + x'_{n'-1}a^{n'-2} + \ldots + x'_1.$$

Par récurrence sur k en supposant $x_i = x'_i$ pour tout $i < k$, on a:

$$X_k = x_n a^{n-k} + x_{n-1}a^{n-k-1} + \ldots + x_k = x'_{n'} a^{n'-k} + x'_{n'-1}a^{n'-k-1} + \ldots + x'_k$$

x_k et x'_k deviennent alors le reste de la division euclidienne de X_k par a d'où $x_k = x'_k$. ■

Convention: On désigne les nombres $\{0, 1, \ldots, a-1\}$ par des symboles conventionnels appelés chiffres.

Définition 0.2.4.

On appelle écriture de x en base a le symbole $\overline{x_n x_{n-1} \ldots x_0}$ qui représente le nombre x, les x_i étant des chiffres.

Algorithme: Pour obtenir l'écriture en base a de x on fait des divisions successives de x par a jusqu'à l'obtention d'un quotient nul.

Exercice: Critère de divisibilité en base a:

Soit $x \in \mathbb{N}^*$ et $\overline{x_n x_{n-1} \ldots x_0}$ sont écriture en base a, montrer que x est divisible par $(a-1)$ si, et seulement si $\sum_{i=0}^{n} x_i$ est divisible par $(a-1)$.

Démonstration. $x = a^n x_n + a^{n-1}x_{n-1} + \ldots + x_0$ et $a^k = (a^k - 1) + 1 = (a-1)\sum_{i=0}^{k-1} a^i + 1$. ■