Introduction : En arithmétique, on travaille dans l'ensemble des entiers naturels $\mathbb{N}$ et l'ensemble des entiers relatifs $\mathbb{Z}$, les raisonnements menés sont totalement différent de ce mener en analyse sur l'ensemble $\mathbb{R}$, nous utiliserons le raisonnement par récurrence que vous verrez dans le tronc commun.

I. Divisibilité dans $\mathbb{Z}$,

a. Multiple et Diviseurs

Définition : Soient a et b deux entiers relatifs. S'il existe un entier relatif k tel que $a = kb$, on dit que a est un multiple de b. De plus lorsque $b \neq 0$, on dit que

- b est un diviseur de a,
- a est divisible par b ou a est un multiple de b,
- b divise a.

On note $b|a$

Exemples :

b. Propriétés

Propriété (transitivité): Soient a, b, c 3 entiers relatifs avec $a \neq 0$ $b \neq 0$. Si a divise b et b divise c, alors a divise c.

Démo : Si a divise b alors il existe un entier relatif k tel que $b = ka$.
Si b divise c alors il existe un entier relatif k' tel que $c = k'b$.
Ainsi, $c = k'b = k'ka$ avec k et k' deux entiers relatifs donc a divise c.

Propriété 2 : Soit $a \neq 0$. Si a divise b, alors pour tout entier relatif k, a divise kb.

Démo : Si $a|b$ alors $\exists k' \in \mathbb{Z}$ tel que $b = k'a$ donc pour tout entier relatif k, $kb = kk'a$ avec $k'k' \in \mathbb{Z}$ donc $a|kb$

Propriété 3 : Soit $a \neq 0$. Si a divise b et c, alors pour tous entiers relatifs k et k, a divise $kb + k'c$.

Démo : Si a divise b et a divise c alors il existe un entier relatif u tel que $b = ua$ et il existe un entier relatif v tel que $c = v'a$.
Soient k, k' deux entiers relatifs, alors $kb + k'c = kua + k'va = a(ku + k'v)$ et comme $ku + k'v$ est un entier relatif alors $a|kb + k'c$

Exemples :

II. Division Euclidienne.

a. Division Euclidienne des entiers naturels

Théorème : Pour tout couple d'entier naturel $(a\,,b)$ avec $b \neq 0$,
il existe un unique couple d'entier naturel $(q\,,r)$ tel que $a = qb + r$, avec $0 \leq r < b$.

$$\begin{array}{c|c} a & b \\ r & q \end{array}$$
$$a = bq + r$$
$$0 \leq r < b$$

Démo : La propriété nous assure existence et unicité d'un couple, la démonstration se rédige donc en deux étapes.
Pour cette démonstration, nous aurons besoin d'admettre la propriété suivante :

Propriété[1] (admise) : Une partie non vide de $\mathbb{N}$ admet un plus petit élément.

Existence : Si $0 \leq a < b$, le couple $(q,r) = (0,a)$ convient.
Supposons maintenant que $b \leq a$. Les entiers naturels a et b sont alors strictement positifs.
Soit M l'ensemble des multiples de b inférieurs ou égaux à a, c'est-à-dire $M = \{k \in \mathbb{N}\,;\, bk \leq a\}$.
Cet ensemble M n'est pas vide car l'entier 0 appartient à celui-ci.
De plus, M est majoré par a car $ba \geq a$. Ainsi, M admet un plus grand élément.
Donc il existe un entier naturel q tel que $qb \leq a < (q+1)b$.
Comme $b \leq a$, on a $b \leq a < (q+1)b$. En particulier $b < (q+1)b$, donc $1 < q+1$ et d'où $0 < q$.
Posons alors $r = a - qb$. Comme a, b et q sont des entiers, r est aussi un entier.
De $qb \leq a < (q+1)b$, on déduit que $0 \leq r < b$. On a alors trouvé un couple (q,r) tel que $a = bq + r$ avec $0 \leq r < b$.
Unicité : supposons qu'il existe deux couples d'entiers $(q\,,r)$ et $(q_0\,,r_0)$ tels que $a = bq + r = bq_0 + r_0$ avec $0 \leq r < b$ et $0 \leq r_0 < b$.
De $bq + r = bq_0 + r_0$, on tire $b(q - q_0) = r_0 - r$.
Ainsi, $q - q_0$ étant entier, $r_0 - r$ est un multiple de b. $0 \leq r < b$ on déduit $-b < -r \leq 0$.
Par addition avec $0 \leq r_0 < b$, on obtient $-b < r_0 - r < b$. Donc $r_0 - r$ est un multiple de b strictement compris entre $-b$ et b : c'est donc 0.
Par suite, $b(q - q_0) = r_0 - r = 0$ et comme $b \neq 0$ on a $q = q_0$. Le couple $(q\,,r)$ est donc unique

Définition : Dans la division euclidienne de a par b

- a est appelé dividende,
- b le diviseur,
- q le quotient,
- r le reste.

Remarques : - Si $r = 0$ alors b divise a.
- Effectuer la division euclidienne de a par b, c'est déterminer q et r.

b. Algorithme de calcul (💻)

[1] Cette propriété découle des axiomes de Péano qui permettent de construire l'ensemble des entiers naturels en admettant un minimum de propriété.

III. Congruences.

Définition : Soient a et b deux entiers relatifs. On dit que a est CONGRU à b MODULO n si $a-b$ est un multiple de n. C'est-à-dire il existe un entier relatif k tel que $a-b=kn$.
Et on note $a \equiv b(n)$

Propriété : Soient a, b deux entiers relatifs et n un entier naturel non nul. $a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Démo : $\Rightarrow$) Si $a \equiv b\ [n]$, $a = nq + r$ avec $0 \leq r < n$ et $b = nq' + r'$ avec $0 \leq r' < n$.
Alors $b - a = n(q' - q) + (r - r')$.
Or $a \equiv b\ [n]$ donc il existe $k \in \mathbb{Z}$ tel que $b - a = kn$ ie $r' - r$ multiple de n et $1 - n \leq r' - r \leq n - 1$ donc $r' - r = 0$ et $r = r'$.
$\Leftarrow$) On suppose $a = nq + r$ et $b = nq' + r$ alors $b - a = n(q' - q) = nk$ avec $k \in \mathbb{Z}$ donc $a \equiv b\ [n]$

Propriété (transitivité) : Soient a, a', a'' trois entiers relatifs et n un entier naturel non nul. Si $a \equiv a'(n)$ et $a' \equiv a''(c)$, alors $a \equiv a''(c)$.

Propriété : Soient a, b, a', b' des entiers relatifs et n un entier naturel non nul. Si $a \equiv b(n)$ et $a' \equiv b'(n)$ alors :

- $a + a' \equiv b + b'(n)$ et $a - a' \equiv b - b'(n)$
- $aa' \equiv bb'(n)$ et pour tout entier naturel k non nul, $a^k \equiv b^k(n)$.

Démo : si $a \equiv b[n]$ et $a' \equiv b'[n]$ c'est-à-dire il existe $k, k' \in \mathbb{Z}$ tel que $b - a = kn$ et $b' - a' = k'n$. Alors $a + a' = b + kn + b' + k'n = b + b' + (k + k')n$ avec $k + k' \in \mathbb{Z}$ donc $(x + x') - (y + y')$ multiple de n ie $a + a' \equiv b + b'[n]$
De même $aa' = (b + kn)(b' + k'n) = bb' + n(bk' + kb' + kk'n)$ avec $bk' + kb' + kk'n \in \mathbb{Z}$ donc $aa' - bb'$ multiple de n et donc $a \times a' \equiv b \times b'[n]$

IV. Congruences.

Théorème : Soit $b \in \mathbb{N}$ tel que $b \geq 2$ et a un entier naturel non nul.. Il existe un entier naturel n, des entiers naturels $a_0, a_1, \ldots, a_n$ avec $a_n \neq 0$ et les a_i entiers naturels compris entre 0 et $b-1$ pour tout entier naturel i compris en 0 et n tels que a s'écrive de façon unique sous la forme :
$a = a_n b^n + a_{n-1}\ b^{n-1} + \cdots + a_1 b + a_0$.
Et on note $a = \overline{a_n a_{n-1} \ldots a_0}^{b}$

Exemple :