Arithmétique (1)

L'arithmétique, c'est à dire la partie des mathématiques s'intéressant aux propriétés des nombres entiers positifs, a souvent laissé place à l'algèbre à partir du XVI^e siècle. Cependant, sous le nom de théorie des nombres, elle a repris un bel essor lorsque des méthodes analytiques ont permis de démontrer de nouvelle propriétés. De nos jours, on utilise des propriétés arithmétiques sur les nombres premiers pour envoyer des messages cryptés.

L'ensemble $\mathbb{Z}$ muni de l'addition et la multiplication est ce que l'on appelle un anneau unitaire, commutatif et intègre :

- unitaire car il existe un élément neutre pour la multiplication : 1
- commutatif car la multiplication d'entiers relatifs est commutative
- intègre signifie (avec la condition de commutativité) qu'un produit est nul si l'un de ses facteurs est nul.

I Divisibilité

Définition

On dit que l'entier relatif a est divisible par l'entier relatif d, ou que a est un multiple de d, s'il existe un entier relatif q tel que $a = qd$. On note d/a.

Remarque

- Les entiers 1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1.
- L'entier 0 est multiple de tous les entiers, mais ne divise que lui-même.

La relation de divisibilité est une relation d'ordre non totale sur $\mathbb{N}$, c'est à dire qu'elle est :

- **réflexive** : pour tout $a \in \mathbb{N}$, a/a ;
- **anti-symétrique** : si a/b et b/a dans $\mathbb{N}$ alors $a = b$;
- **transitive** : si a/b et b/c dans $\mathbb{N}$ alors a/c.

En revanche elle n'est pas totale car deux éléments de $\mathbb{N}$ ne sont pas toujours comparable au sens de la divisibilité : 3 et 5 par exemple (il n'existe aucune relation de divisibilité entre ses deux éléments).

⚠ Sur $\mathbb{Z}$, la relation de divisiblité n'est pas anti-symétrique : $6/-6$ et $-6/6$ pourtant $6 \neq -6$!
Sur $\mathbb{Z}$ la relation de divisibilité est seulement réflexive et transitive, ce n'est donc pas une relation d'ordre.

Démonstration

Soit a, b et c trois entiers relatifs. Montrons que sur $\mathbb{Z}$, la relation de divisibilité est réflexive et transitive :

- réflexive : $a = a \times 1$ donc a/a
- transitive : si a/b alors il existe $q \in \mathbb{Z}$ tel que $b = aq$. Si b/c alors il existe $q' \in \mathbb{Z}$ tel que $c = bq' = aqq' = a(qq')$.
  Or $qq' \in \mathbb{Z}$, donc a/c.

Exemple

Démontrer que pour tout entier relatif n, le nombre $6n + 5$ n'est pas divisible par 3.

Propriété

Stabilité des multiples d'un nombre par combinaison linéaire :
Si a et b sont deux multiples de d, alors quel que soit $(\lambda; \mu) \in \mathbb{Z}^2$, $\lambda a + \mu b$ est un multiple de d.
Pour tout entier relatif d, on note $d\mathbb{Z} = \{d \cdot q \mid q \in \mathbb{Z}\}$ l'ensemble des multiples de d.
On note $\mathcal{D}_n = \{q \in \mathbb{Z} \mid q \text{ divise } n\}$ l'ensemble de tous les diviseurs de n.

Démonstration

Nous allons démontrer la stabilité des multiples par combinaison linéaire : Soit a et b deux entiers relatifs multiples de d entier relatif :

- $\exists k \in \mathbb{Z},\ a = kd$
- $\exists k' \in \mathbb{Z},\ b = k'd$

Soit λ et μ deux entiers relatifs quelconques : $\lambda a + \mu b = \lambda kd + \mu k'd = (\lambda k + \mu k')d$
Or $\lambda k + \mu k' \in \mathbb{Z}$ car $(\mathbb{Z}, +, \cdot)$ est un anneau.
D'où $\lambda a + \mu b$ est également un multiple de d.

La réciproque de cette propriété est fausse !

Exemple

Déterminer les entiers relatifs n, tels que $2n + 5$ divise $n-1$.

II Division Euclidienne dans $\mathbb{Z}$

Propriété

- Toute partie non vide majorée de $\mathbb{Z}$ admet un plus grand élément.
- Toute partie non vide minorée de $\mathbb{Z}$ admet un plus petit élément.

Remarque

Soit A une partie de $\mathbb{Z}$.

$$A \text{ est majorée ssi } \exists M \in \mathbb{Z} \mid \forall a \in A,\ a \leq M$$

$$A \text{ est minorée ssi } \exists m \in \mathbb{Z} \mid \forall a \in A,\ a \geq m$$

Théorème

Division Euclidienne dans $\mathbb{Z}$: soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Il existe un unique couple d'entiers relatifs (q,r) tel que $a = bq + r$ avec $0 \leq r < b$

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

Unicité :

Supposons qu'il existe deux couples $(q;r)$ et $(q';r')$ vérifiant $a = bq + r$ et $a = bq' + r'$.
Alors $bq + r = bq' + r'$ donc $b(q - q') = r' - r$ or $q - q'$ est un entier, donc b divise $r' - r$.
Cependant $0 \leq r < b$ et $0 \leq r' < b$ donc $-b < r - r' < b$ donc $r - r' = 0$ car 0 est le seul multiple de b compris entre $-b$ et b.
D'où $r = r'$ et finalement, $q = q'$.

Existence :

$b \geq 1$ par hypothèse.
On pose $E = \{n \in \mathbb{Z} \mid nb \leq a\}$.
E est un ensemble de $\mathbb{Z}$ non vide (il contient 0 si $a \geq 0$, ou a si $a < 0$) et est majorée (par 0 si $a < 0$ ou a si $a \geq 0$), il admet donc un plus grand élément q.
q vérifie deux condition $\begin{cases} qb \leq a \text{ car } q \in A \\ (q+1)b > a \text{ car } (q+1) \notin A \end{cases}$
On pose alors $r = a - bq$.
Alors $a = bq + r$ et $0 \leq r < (q+1)b - bq = b$.

Démonstration

On définit de la même façon la division euclidienne d'un entier relatif a par un entier relatif b non nul.
On a alors $0 \leq r \leq |b|$.

Remarque

Exemple

Déterminer le quotient et le reste de la division euclidienne de -5000 par 17.

III Congruences dans $\mathbb{Z}$

Soit n un entier naturel non nul, a et b deux entiers relatifs.
On dit que a est congru à b modulo n, et on note $a \equiv b \pmod{n}$ ou $a \equiv b\ [n]$, lorsque n divise $a - b$. Donc,

$$a \equiv b\ [n] \iff n|a - b$$

Définition

- a est congru à b modulo n lorsqu'il existe un $k \in \mathbb{Z}$ tel que $a = b + kn$.
- L'égalité modulo n est aussi appelée *relation de congruence* modulo n.

Remarque

Exemple

- $32 \equiv 27\ [5]$ car $32 - 27 = 5$ divisible par 5.
- $32 \equiv -3\ [5]$ car $32 - (-3) = 35$ divisible par 5.

Soit n un entier naturel non nul. Deux entiers a et b sont congrus modulo n, si et seulement si, la division euclidienne de a par n a le même reste que la division euclidienne de b par n.

Propriété

Démonstration

Soit a et b deux entiers relatifs et n un entier naturel avec $a \equiv b\ [n]$. Il existe donc $k \in \mathbb{Z}$ tel que $a - b = kn$.
Soit $(q, r) \in \mathbb{Z} \times \mathbb{N}$ respectivement le quotient et le reste dans la division euclidienne de a par n.
Soit $(q', r') \in \mathbb{Z} \times \mathbb{N}$ respectivement le quotient et le reste dans la division euclidienne de b par n.
On a donc $a = nq + r$ et $b = nq' + r'$ d'une part, et $a - b = nk$ d'autre part.
D'où $a - b = n(q - q') + r - r' = nk$ donc $n(q - q' - k) = r' - r$
Ceci revient donc à dire que $r' - r$ est un multiple de n. Or $-n < r' - r < n$ donc le seul multiple possible est 0.
D'où $r' - r = 0$ et donc $r' = r$.

Exemple

a. Compléter :
   (a) $13 \equiv ....\ [5]$
   (b) $45 \equiv ....\ [3]$
   (c) $-8 \equiv ....\ [12]$

b. Démontrer que : $214 \equiv 25\ [9]$

Propriété

Soit n un entier naturel non nul, $a,\ b$ et c des entiers relatifs. La relation de congruence est une relation d'équivalence, donc

- $a \equiv a\ [n]$ **(réflexivité)**
- $a \equiv b\ [n]$ ssi $b \equiv a\ [n]$ **(symétrie)**
- $(a \equiv b\ [n]$ et $b \equiv c\ [n]) \Longrightarrow a \equiv c\ [n]$ **(transitivité)**

Démonstration

Soit $n \in \mathbb{N}$ et $a,\ b$ et c des entiers relatifs.

- $a - a = 0 \times n$ donc $a \equiv a\ [n]$.
- $a \equiv b\ [n]$ ssi $\exists k \in \mathbb{Z}$, $a - b = nk$ ssi $b - a = k'n$ avec $k' = -k$. Donc $b \equiv a\ [n]$
- $(a \equiv b\ [n]$ et $b \equiv c\ [n])$ ssi $(\exists k \in \mathbb{Z}$, $a - b = nk$ et $\exists k' \in \mathbb{Z}$, $b - c = nk')$
  donc par addition $a - c = n(k' + k)$ donc $a \equiv c\ [n]$

Propriété

Soit n entier naturel non nul, $a,\ b,\ c$ et d des entiers relatifs.

- La relation de congruence est compatible avec l'addition (et la soustraction), c'est à dire

$$(a \equiv b\ [n] \text{ et } c \equiv d\ [n]) \Longrightarrow a + c \equiv b + d\ [n]$$

- La relation de congruence est compatible avec la multiplication, c'est à dire

$$(a \equiv b\ [n] \text{ et } c \equiv d\ [n]) \Longrightarrow a \times c \equiv b \times d\ [n]$$

Démonstration

Soit n un entier naturel non nul, $a,\ b,\ c$ et d des entiers relatifs.

- $a \equiv b\ [n]$ donc il existe $k \in \mathbb{Z}$ tel que $a - b = nk$.
  $c \equiv d\ [n]$ donc il existe $k' \in \mathbb{Z}$ tel que $c - d = nk'$.
  Par addition,
  $a - b + c - d = nk + nk' = n(k + k') = nk''$ En posant $k'' = k + k' \in \mathbb{Z}$.
  Donc $a + c \equiv b + d\ [n]$
- On procède de même et par produit
  $(a - b) \times c + (c - d) \times b = nkc + nk'b = n(kc + k'b) = nk''$
  Donc $a \times c \equiv b \times d\ [n]$.

La division n'est pas compatible avec les congruences !
$5 \times 6 \equiv 5 \times 4\ [10]$ mais $4 \not\equiv 6\ [10]$.

Propriété

Soit n un entier naturel non nul, $a,\ b$ et c des entiers relatifs.

- $a \equiv b\ [n]$ ssi $a + c \equiv b + c\ [n]$
- $a \equiv b\ [n] \implies ac \equiv bc\ [n]$

Démonstration

- Soit n un entier naturel non nul, $a,\ b$ et c des entiers relatifs.
  $a + c \equiv b + c\ [n]$ ssi $a + c - (b + c) \equiv 0\ [n]$ ssi $a - b \equiv 0\ [n]$ ssi $a \equiv b\ [n]$
- $(a \equiv b\ [n]$ et $c \equiv c\ [n]) \implies a \times c \equiv b \times c\ [n]$.

Propriété

Soit n un entier naturel non nul, a et b des entiers relatifs et p un entier naturel.
La relation de congruence est compatible avec les puissances, c'est à dire

$$a \equiv b[n] \implies a^p \equiv b^p\ [n]$$

Démonstration

Cette démonstration s'effectue par récurrence : Soit $a \equiv b\ [n]$.
Pour tout entier naturel non nul p, on note la proposition $\mathcal{P}(p)$ suivante : $a^p \equiv b^p\ [n]$.

Initialisation :

rang $p = 1$.
$a \equiv b\ [n]$.
La propriété est donc vraie au rang $p = 1$.

Hérédité :

Supposons $\mathcal{P}(p)$ vraie pour un certain rang p et montrons que cela implique $\mathcal{P}(p+1)$ vrai.

$$\begin{aligned} \mathcal{P}(n) \text{ vraie} &\iff a^p \equiv b^p\ [n] \\ &\implies a \times a^p \equiv b \times b^p\ [n] \\ &\iff a^{p+1} \equiv b^{p+1}\ [n] \end{aligned}$$

Conclusion :

$\mathcal{P}(p)$ vraie $\implies \mathcal{P}(p+1)$ vraie. La propriété est donc héréditaire à partir du rang $p = 1$.
D'après le principe de récurrence : $\forall p > 0,\ \mathcal{P}(p)$ est vraie.
La propriété est ainsi démontrée.

Exemple

Compléter le tableau :

a	$\equiv 1\ [4]$	$\equiv -1\ [7]$	$\equiv 1\ [10]$
b	$\equiv 2\ [4]$	$\equiv 4\ [7]$	$\equiv -5\ [10]$
$a+b$	$\equiv ....\ [4]$	$\equiv ....\ [7]$	$\equiv ....\ [10]$
$a-b$	$\equiv ....\ [4]$	$\equiv ....\ [7]$	$\equiv ....\ [10]$
a^2	$\equiv ....\ [4]$	$\equiv ....\ [7]$	$\equiv ....\ [10]$
$4b$	$\equiv ....\ [4]$	$\equiv ....\ [7]$	$\equiv ....\ [10]$
a^2+4b-6	$\equiv ....\ [4]$	$\equiv ....\ [7]$	$\equiv ....\ [10]$

Exemple

a. Déterminer les entiers x tels que $6+x \equiv 5\ [3]$.
b. Déterminer les entiers x tels que $3x \equiv 5\ [4]$.

Exemple

Démontrer que pour tout entier naturel n, $n(n+5)(n-5)$ est divisible par 3.

Exemple

a. Déterminer le reste de la division de 2^{456} par 5.
b. Déterminer le reste de la division de 2^{437} par 7.

Définition

Soit a un entier relatif et n un entier naturel non nul.
On dit que a est **inversible modulo** n lorsqu'il existe un entier relatif b tel que $a \times b \equiv 1\ [n]$.

Exemple

- 8 est inversible modulo 3 d'inverse 2 car $8 \times 2 \equiv 1\ [3]$.
- 7 est inversible modulo 4 d'inverse 3 car $7 \times 3 \equiv 1\ [4]$.