Arithmétique et congruence

A. Division euclidienne:

1. Définition:

Propriété:

Si b appartient à $\mathbb{N}^*$, alors, quel que soit a entier positif, il existe un entier n dans $\mathbb{N}$ tel que $a<n\cdot b$.

On dit que $\mathbb{N}$ est **archimédien**.

Remarque:

$\mathbb{R}$ est aussi archimédien.

Exemple:

Les ensembles suivants possèdent un plus petit élément:

- $\{3\,;5\ 12\,;21\}$
- $\{k \mid k\in\mathbb{N}\ ;\ 3\cdot k\geqslant 50\}$

Tous les sous-ensembles de $\mathbb{R}$ ne possèdent pas un plus petit élément: $]0\,;1]$ ne possède pas de plus petit élément.

Propriété: *(admise)*

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Exemple: *(d'utilisation)*

Considérons l'ensemble $\mathcal{E}=\{n\in\mathbb{N} \mid 12\cdot n\geqslant 236\}$ est non vide car il contient la valeur 20:

$12\times 100=1200\geqslant 236$

Le fait que $\mathbb{N}$ est archimédien nous assure également que $\mathcal{E}$ est non-vide.

La propriété précédente nous assure l'existence d'un plus petit élément de $\mathcal{E}$. Mais dans ce cas, nous pouvons le déterminer facilement:

- $20\in\mathbb{E}$: car $12\times 20=240\geqslant 236$
- $19\notin\mathbb{E}$: car $12\times 19=228<236$

On vient donc de montrer que le nombre 12 rentre au maximum 19 fois dans le nombre 236.

Théorème:

Soit a un nombre entier relatif et b un entier naturel non nul.
Il existe un unique couple $(q\,;r)$ d'entiers relatifs tels que $a=b\cdot q+r$ et $0\leqslant r<b$.

Démonstration

L'énoncé de l'exercice affirme deux certitudes: l'existence du couple $(q\,;r)$ et son unicité; notre démonstration reprend séparemment ces deux points:

- **Existence:**

  Effectuons un raisonnement par dijonction de cas:

  ➪ Supposon que $a\in\mathbb{N}$; considérons l'ensemble A défini par:

  $$A=\{n\in\mathbb{N} \mid n\cdot b>a\}$$

  L'ensemble $\mathbb{N}$ est archimédien ce qui nous assure que A est non vide; or, nous savons que toute partie non-vide de $\mathbb{N}$ possède un plus petit élément.

  Notons n_0 le plus petit élément l'ensemble A; puisque n_0 est le plus petit élément de A, cela signifie que son prédécesseur n'y appartient pas:

  $$(n_0-1)\notin A \implies n_0\cdot b\leqslant a$$

  Les propriétés de n_0 et de (n_0-1) permetttent d'écrire:

  $$\left.\begin{array}{l}(n_0-1)\notin A\\ n_0\in A\end{array}\right\}\implies (n_0-1)\cdot b\leqslant a<n_0\cdot b$$

  Ainsi, on a les encadrements suivants:

  $$\begin{array}{rcl}(n_0-1)\cdot b\leqslant & a & <n_0\cdot b\\ (n_0-1)\cdot b-(n_0-1)\cdot b\leqslant & a-(n_0-1)\cdot b & <n_0\cdot b-(n_0-1)\cdot b\\ 0\leqslant & a-(n_0-1)\cdot b & <b\end{array}$$

  Posons: $r=a-(n_0-1)\cdot b$

  $$0\leqslant r<b$$

  Posons maintenant $q=(n_0-1)$, on a:

  $$\begin{array}{rcl}q\cdot b+r &=& (n_0-1)\cdot b+[a-(n_0-1)\cdot b]\\ &=& a\end{array}$$

  Ainsi le couple $(n_0-1\,;a-(n_0-1)\cdot b)$ est une solution à notre théorème.

  ➪ Supposons maintenant que a est strictement négatif: Ainsi, $-a$ est positif; d'après le travail effectué précédemment, on a l'existente d'un couple $(q\,;r)$ tel que:

  $$(-a)=q\cdot b+r \quad \text{où } 0\leqslant r<b$$

  Ainsi, on obtient l'égalité:

  $$a=(-q)\cdot b+(-r) \quad \text{où } -b<-r\leqslant 0$$

  Raisonnons de nouveau par disjonction de cas:

  - si $r=0$, alors le couple $(-q\,;0)$ est une solution.
  - Supposons que $r>0$, ainsi, on a l'encadrement:

    $$-b<-r<0$$

    Modifions l'égalité précédente:

    $$\begin{array}{rcl}a &=& (-q)\cdot b+(-r)\\ a &=& [(-q)\cdot b-b]+[(-r)+b]\\ a &=& (-q-1)\cdot b+(b-r)\end{array}$$

    Effectuons un encadrement de $(b-r)$:

    $$\begin{array}{rcl}-b< & -r & <0\\ -b+b< & b-r & <b\\ 0< & b-r & <b\end{array}$$

    Ainsi, le couple $(-b-1\,;b-r)$ est une solution de notre problème:

    $$a=(-b-1)\cdot q+(b-r) \quad \text{où } 0\leqslant b-r<b.$$

  On vient donc de montrer l'existence d'un tel couple

- **Unicité:**

  Pour montrer l'unicité, supposons l'existence de deux couples $(q_1\,;n_1)$ et $(q_2\,;n_2)$ vérifiant conjointement les propriétés citées:

  $$\left\{\begin{array}{l}a=q_1\cdot b+r_1\\ 0\leqslant r_1<b\end{array}\right. ;\ \left\{\begin{array}{l}a=q_2\cdot b+r_2\\ 0\leqslant r_2<b\end{array}\right.$$

  Etudions de deux manières la différence (r_1-r_2):

  ➪ On a: $0\leqslant r_1<b$; $0\leqslant r_2<b$

  On en déduit: $-b<-r_2\leqslant 0$

  En additionnant ces deux encadrements, on obtient:

  $$\begin{array}{rcl}0+(-b) &<& r_1+(-r_2)<b+0\\ -b< & r_1-r_2 & <b\end{array}$$

  ➪ On a les égalités suivantes:

  $$r_1=a-q_1\cdot b \ ;\ r_2=a-q_2\cdot b$$

  On en déduit:

$$\begin{aligned} r_1 - r_2 &= \big(a - q_1{\cdot}b\big) - \big(a - q_2{\cdot}b\big) \\ &= a - q_1{\cdot}b - a + q_2{\cdot}b \\ &= -q_1{\cdot}b + q_2{\cdot}b \\ &= \big(q_2 - q_1\big){\cdot}b \end{aligned}$$

Ainsi, le nombre $\big(r_1 - r_2\big)$ est un multiple de b.

Or, le seul multiple de b compris dans l'intervalle $\left]-b\,;b\right[$ est 0 ; ainsi, on en déduit :

$r_1 - r_2 = 0 \quad\Longrightarrow\quad r_1 = r_2$

Des égalités : $a = q_1{\cdot}b + r_1$; $a = q_2{\cdot}b + r_2$

On en déduit l'égalité suivante :

$$\begin{aligned} q_1{\cdot}b + r_1 &= q_2{\cdot}b + r_2 \\ q_1{\cdot}b &= q_2{\cdot}b + \big(r_2 - r_1\big) \\ q_1{\cdot}b &= q_2{\cdot}b \\ q_1 &= q_2 \end{aligned}$$

Les deux couples sont donc égaux : ceci montre l'unicité de la solution.

2. Utilisation :

Proposition : *(Quelques résultats d'arithmétique)*

- Soit n un entier pair, alors il existe un entier n tel que : $n = 2{\cdot}n$
- Soit n un entier impair alors il existe un entier n tel que : $n = 2{\cdot}n + 1$
- Le carré d'un entier impair est impair.

Remarque :

La division euclidienne est à la base de la détermination du "*Plus Grand Commun Diviseur*" à l'aide de l'algorithme d'Euclide :

Dividende	Diviseur	Reste	
240	36	24	$240 = 6 \times 36 + 24$
36	1	12	$36 = 24 \times 1 + 12$
24	12	0	$24 = 2 \times 12 + 0$

1. Exemples :

Exemple :

Voici un exemple de codage d'un message à l'aide de la division euclidienne :

- $y = 4x + 5$ Exemple de codage : SALADE XFWFRV

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Reste de la division de y par 27	5	9	13	17	21	25	2	6	10	14	18	22	26	3	7	11	15	19	23	0	4	8	12	16	20	24	1
Lettre	F	J	N	R	V	Z	C	G	K	O	S	W	_	D	H	L	P	T	X	A	E	I	M	Q	U	Y	B

- $y = 6x + 4$ Exemple de codage : SALADE EEQEWB

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Reste de la division de y par 27	4	10	16	22	1	7	13	19	25	4	10	16	22	1	7	13	19	25	4	10	16	22	1	7	13	19	25
Lettre	E	K	Q	W	B	H	N	T	Z	E	K	Q	W	B	H	N	T	Z	E	K	Q	W	B	H	N	T	Z

- $y = 3x^2 + 5x + 2$ Exemple de codage : SALADE OCSCUT

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Reste de la division de y par 27	2	13	0	20	19	24	8	25	21	23	4	18	11	10	15	26	16	12	14	22	9	2	1	6	17	7	3
Lettre	C	N	A	U	T	Y	I	Z	V	X	E	S	L	K	P	_	Q	M	O	W	J	C	B	G	R	H	D

- $y = 3x^2 + 4x + 6$ Exemple de codage : SALADE WGGGQO

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Reste de la division de y par 27	6	11	24	16	14	18	1	17	12	13	20	6	25	23	0	10	26	21	22	2	15	7	5	9	19	8	3
Lettre	G	L	Y	Q	O	S	B	R	M	N	U	G	Z	X	A	K	_	V	W	C	P	H	F	J	T	I	D

Remarque : deux de ces codages ne sont pas efficient car, on ne pourra pas déchiffrer un message codé.

A. Congruence :

Définition :

On dit que deux entiers a et b relatifs sont **congrus modulo** c si ils ont le même reste par la division euclidienne par c.

Proposition :

Deux entiers sont congrus entre eux modulo c si, et seulement, si leur différence est un multiple de c.

Corollaire :

Deux entiers a et b sont congrus modulo $c$si, et seulement si, il existe un entier relatif k vérifiant :

$$a = b + k\cdot c$$

Preuve :

La division euclidienne des entiers b et a permettent d'obtenir les couples $(q\,;r)$ et $\big(q'\,;r'\big)$ tels que :

$$a = q\cdot c + r \text{ où } 0 \leqslant r \leqslant |c| \quad ; \quad b = q'\cdot c + r' \text{ où } 0 \leqslant r' \leqslant |c|$$

- $\Longrightarrow$:

  Supposons que le nombre $(a-b)$ est un multiple de c : il existe un entier k vérifiant :

  $$a - b = k\cdot c$$

  Le nombre $(a-b)$ peut s'écrire :

  $$a - b = \big(q - q'\big)\cdot c + \big(r - r'\big)$$

  $$k\cdot c = \big(q - q'\big)\cdot c + \big(r - r'\big)$$

  $$k\cdot c - \big(q - q'\big)\cdot c = \big(r - r'\big)$$

  $$r - r' = \big[k - \big(q - q'\big)\big]\cdot c$$

  On vient de montrer que le nombre $(r-r')$ est un multiple de c.

  Des propriétés des restes, on écrit :

  $$\begin{cases} 0 \leqslant r \leqslant |c| \\ 0 \leqslant r' < |c| \end{cases} \Longrightarrow \begin{cases} 0 \leqslant r \leqslant |c| \\ -|c| < r' \leqslant 0 \end{cases}$$

  On en déduit l'encadrement suivant :

  $$-|c| < r - r' < |c|$$

  Dans l'intervalle $\big]-|c|\,;|c|\big[$, le seul multiple de c est 0 :

  $$r - r' = 0 \quad \Longrightarrow \quad r = r'$$

- $\Longleftarrow$:

  Supposons que les deux entiers a et b, on le même reste par la division euclidienne par r ; on en déduit :

  $$a - b = \big(q\cdot c + r\big) - \big(q'\cdot c + r\big)$$

  $$= \big(q\cdot c + r\big) - \big(q'\cdot c + r\big) = \big(q - q'\big)\cdot c$$

  On vient de montrer que $(a-b)$ est un multiple de c.

Proposition :

Soit a, a', b et b' quatre entiers relatives vérifiant les relations suivantes :

$$a \equiv a' \pmod{c} \quad ; \quad b \equiv b' \pmod{c}$$

On a les propriétés algébriques suivantes :

1. $a + b \equiv a' + b' \pmod{c}$
2. $a - b \equiv a' - b' \pmod{c}$
3. $a \cdot b \equiv a' \cdot b' \pmod{c}$
4. $a^n \equiv a'^n \pmod{c}$

Preuve :

Puisque $a \equiv a' \pmod{c}$, il existe un entier k vérifiant :

$$a = a' + k\cdot c$$

De même, il existe un entier k' tel que :

$$b' = b' + k'\cdot c$$

1. Ainsi, on a :

   $$a + b = \big(a' + k\cdot c\big) + \big(b' + k'\cdot c\big)$$

   $$= a' + b' + k\cdot c + k'\cdot c = a' + b' + \big(k + k'\big)\cdot c$$

   Ainsi, on a : $a+b \equiv a'+b' \pmod{c}$

2. Ainsi, on a :

   $$a - b = \big(a' + k\cdot c\big) - \big(b' + k'\cdot c\big)$$

   $$= a' - b' + k\cdot c - k'\cdot c = a' - b' + \big(k - k'\big)\cdot c$$

   Ainsi, on a : $a-a' \equiv b-b' \pmod{c}$

3. De même, on a :

   $$a \cdot b = \big(a' + k\cdot c\big)\cdot\big(b' + k'\cdot c\big)$$

   $$= a'\cdot b' + a'\cdot k'\cdot c + k\cdot c\cdot b' + k\cdot k'\cdot c^2$$

   $$= a'\cdot b' + c\cdot\big(b\cdot k' + k\cdot b' + k\cdot k'\cdot c\big)$$

   On en déduit : $a\cdot b \equiv a'\cdot b' \pmod{c}$

4. Considérons la propriété $\mathcal{P}_n$ définie pour tout entier naturel n définie par :

   $\mathcal{P}_n$: "$a^n \equiv a'^n \pmod{c}$"

   Montrons, à l'aide d'un raisonnement par récurrence, que pour tout entier naturel n la propriété $\mathcal{P}_n$ est vraie :

   - **Initialisation :**

     $$a^0 = 1 \equiv 1 \pmod{c} \quad ; \quad a'^0 = 1 \equiv 1 \pmod{c}$$

     On vient d'établir que $\mathcal{P}_0$ est vraie.

   - **Hérédité :**

     Supposons la propriété $\mathcal{P}_n$ réalisée pour un entier naturel n quelconque. C'est à dire qu'on a l'hypothèse par récurrence :

     $$a^n \equiv a'^n \pmod{c}$$

     Les entiers a et a' vérifient également :

     $$a \equiv a' \pmod{c}$$

     Par multiplication de ces deux équivalences, on obtient :

     $$a^n \cdot a \equiv a'^n \cdot a' \pmod{c} \Longrightarrow a^{n+1} \equiv a'^{n+1} \pmod{c}$$

     On vient d'établir la propriété $\mathcal{P}_{n+1}$.

   - **Conclusion :**

     On vient d'établir que la propriété $\mathcal{P}_n$ est initialisée pour $n=0$ et vérifie la propriété d'hérédité. A l'aide d'un raisonnement par récurrence, on vient d'établir que la propriété $\mathcal{P}_n$ est réalisée pour tout entier naturel n.