Divisibilité, division euclidienne et congruence

I) Divisibilité dans $\mathbb{Z}$

Généralités

Définitions : L'arithmétique est l'étude des entiers naturels ou relatifs et de leur rapport.
$\mathbb{N}$ est l'ensemble des entiers naturels : $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$ est l'ensemble des entiers relatifs : $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Quelques axiomes dans $\mathbb{N}$:

- Principe du bon ordre : toute partie de $\mathbb{N}$ non vide admet un plus petit élément.
- Principe de la descente infinie : toute suite dans $\mathbb{N}$ strictement décroissante est finie.
- Principe des tiroirs : si l'on range $n+1$ éléments dans n tiroirs, alors un des tiroirs contiendra au moins deux éléments.

Divisibilité dans $\mathbb{Z}$

Définitions : Soient a et b deux entiers relatifs.
a **divise** b s'il existe un entier relatif k tel que $b = ka$. On note $a|b$.
On dit également : a est un **diviseur** de b ; b est **divisible** par a ; b est un **multiple** de a.

Remarques :

- Tout diviseur de $n \in \mathbb{N}$ est compris entre $-|n|$ et $|n|$.
- Tout entier relatif non nul n a donc un nombre fini de diviseurs.

Exemples :

- 56 est un multiple de -8 car $56 = -7 \times (-8)$
- L'ensemble des multiples de 5 est $\{\dots ; -15; -10; -5; 0; 5; 10; \dots\}$. On note cet ensemble $5\mathbb{Z}$.
- 0 est multiple de tout entier a car $0 = 0 \times a$.
- 1 divise tout entier a car $a = 1 \times a$.

Quelques propriétés

Propriété : Transitivité : Soient a, b et c trois entiers relatifs.
Si a divise b et b divise c alors a divise c. C'est-à-dire $\left\{ \begin{array}{l} a|b \\ b|c \end{array} \right. \Rightarrow a|c$

Démonstration : Si a divise b et b divise c alors il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = k'b$.
D'où $c = kk'a$. Posons $k'' = kk' \in \mathbb{Z}$. il existe donc un entier relatif k'' tel que $c = k''a$. Ainsi a divise c.

Propriété : Combinaison linéaire : Soient a, b et c trois entiers relatifs.
Si c divise a et b, alors c divise toute combinaison linéaire de a et b.
C'est-à-dire : Si c divise a et b, alors c divise $ua + vb$ où u et v sont deux entiers relatifs.
En particulier si c divise a et b, alors c divise $a + b$ et $a - b$.

Démonstration : Si c divise a et c divise b alors il existe deux entiers relatifs k et k' tels que $a = kc$ et $b = k'c$.
Ainsi $ua + bv = ukc + vk'c = (ku + k'v)c = k''c$ avec $k'' = ku + k'v \in \mathbb{Z}$. CQFD.
Exemples :

a. Soit $n \in \mathbb{N}$. Déterminer un entier relatif N qui divise les entiers relatifs n et $n+1$.

b. Soit $k \in \mathbb{N}$. On pose $a = 9k + 2$ et $b = 12k + 1$. Déterminer une condition sur les diviseurs positifs communs à a et b.

Piste correction : a. N divise $n + 1 - n = 1$ d'où $N = 1$ ou -1.
b. On cherche une combinaison linéaire de a et b qui élimine les k. $4a - 3b = 5$. Donc les diviseurs positifs communs à a et b ne peuvent être que 1 ou 5.

II) Division euclidienne

Propriété : Soit a un entier naturel et b un entier naturel non nul.
On appelle division euclidienne de a par b l'opération qui, au couple $(a;b)$, associe l'unique couple d'entiers naturels $(q;r)$ tel que : $\boxed{a = bq + r \text{ avec } 0 \leqslant r < b}$.

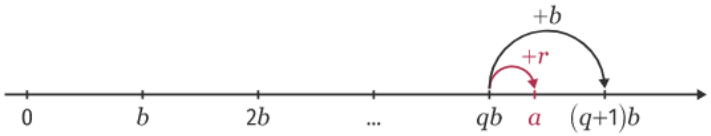
Définitions : Dans la division euclidienne de a par b :

- a est le dividende
- b est le diviseur
- q est le quotient
- r est le reste

Démonstration :
• **Existence :** Soit E l'ensemble des entiers e tels que $be > a$. $E = \{e \in \mathbb{N}, be > a\}$.
E est non vide car $(a+1) \in E$. Preuve : $b \geqslant 1 \Rightarrow b(a+1) \geqslant a+1 > a$.
E est une partie de $\mathbb{N}$ non vide donc admet un plus petit élément. Notons m ce plus petit élément.
Ainsi $\begin{cases} m \in E \\ (m-1) \notin E \end{cases} \iff \begin{cases} mb > a \\ (m-1)b \leqslant a \end{cases}$ d'où $(m-1)b \leqslant a < mb$.
Posons $q = m-1$. On a $bq \leqslant a < b(q+1) \Rightarrow 0 \leqslant a - bq < b$.
Posons $r = a - bq$. On a finalement $a = bq + r$ et $0 \leqslant r < b$.
Il existe donc un couple d'entiers naturels $(q;r)$ tel que : $a = bq + r$ avec $0 \leqslant r < b$.
• **Unicité :** Supposons qu'il existe deux couples $(q;r)$ et $(q;r')$ distincts tels que : $\begin{cases} a = bq + r \text{ avec } 0 \leqslant r < b \\ a = bq' + r' \text{ avec } 0 \leqslant r' < b \end{cases}$
On obtient $0 = b(q-q') + r - r' \iff b(q-q') = r' - r$. De plus $-b < r' - r < b$.
Ainsi b divise $r' - r$ et $-b < r' - r < b$. D'où $r - r' = 0$ puis $r = r'$ et ensuite $q = q'$. Ce qui contredit notre hypothèse.
Finalement $(q;r)$ est unique.

Interprétation graphique

On encadre a entre deux multiples consécutifs de b :



Remarques :

a. La condition $0 \leqslant r < b$ assure l'unicité du couple $(q;r)$.

b. Par exemple : Les restes possibles dans la division par 7 sont alors : 0, 1, 2, 3, 4, 5, 6.

Exemple : Division euclidienne de 412 par 15 : $412 = 15 \times 27 + 7$. Avec potence :

4 1 2	1 5
1 1 2	2 7
7	

Propriété : On peut étendre la propriété précédente au cas où a est un entier relatif.

Démonstration : : Admise.
Exemple : Déterminer le quotient et le reste de la division de -5000 par 17.
On obtient pour 5000 et 17 : $5000 = 17 \times 294 + 2$.
D'où $-5000 = -17 \times 294 - 2$. Or $-2 \notin [\![0 : 17]\!]$ (Point notation)
On en déduit $-5000 = -17 \times 295 + 15$ (on ajoute et enlève 17)
Doù $q = -295; r = 15$

5 0 0 0	1 7
1 6 0	2 9 4
7 0	
2	

Propriété : Soit b un entier naturel tel que $b \geqslant 2$.
Tout entier a s'écrit sous une, et une seule, des formes $bq, bq+1, bq+2, \ldots, bq+(b-1)$, où q est un entier.

Démonstration : Soit a un entier.
En effectuant la division euclidienne de a par b non nul, il existe deux entiers naturels q et r tels que $a = bq + r$ avec $0 \leqslant r < b$.
Par unicité du quotient et du reste $a = bq$ ou $a = bq + 1$ ou $a = bq + 2$ ... ou $a = bq + (b-1)$.

Remarque : Ainsi, dans la division par 2, le reste est 0 ou 1. Tout entier s'écrit sous la forme $2k$ ou $2k+1$.
On retrouve donc qu'un entier est pair ou impair.

Exemple : Soit n un entier naturel. Posons $A = n(n-2)(n+2)$. Démontrer que A est un multiple de 3.
Méthode : D'après le résultat du cours sur la division euclidienne, on sait que tout entier n s'écrit sous une des trois formes suivantes : $n = 3k$; $n = 3k+1$ ou $n = 3k+2$ avec $k \in \mathbb{N}$.
On raisonne par disjonction de cas en distinguant les trois cas possibles et en démontrant le résultat dans chacun des cas.

III) Congruence dans $\mathbb{Z}$

Définition : Soit n un entier naturel non nul.
Deux entiers a et b sont congrus modulo n lorsque $a-b$ est divisible par n.
On note $a \equiv b\ [n]$

Exemple : Deux nombres de la liste : 1 ;6 ;11 ;16 ;21 ;26 ;31 ;36 sont congrus modulo 5.
Par exemple pour 21 et 6 : 21-6=15 qui est divisible par 5. On a $21 \equiv 6\ [5]$

Propriété : 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.

Démonstration :
• Sens direct : Soient a et b sont congrus modulo n.
Par divisions euclidiennes par n on a il existe $(q;r) \in \mathbb{Z}^2$ et $(q',r') \in \mathbb{Z}^2$ tels que $a = nq + r$ et $b = nq' + r'$ avec $0 \leqslant r < n$ et $0 \leqslant r' < n$.
On sait qu'il existe $k \in \mathbb{Z}$ tel que $a - b = kn$. ainsi $n(q-q') + r - r' = kn \iff r - r' = n(q - q' - k)$.
Or $-n < r - r' < n$ et $r - r'$ divise n donc $r - r' = 0 \iff r = r'$
• Sens indirect : Notons r le même reste que la division euclidienne de a par nn et b par n.
Par divisions euclidiennes par n on a il existe q et q' tels que $a = nq + r$ et $b = nq' + r$ avec $0 \leqslant r < n$.
D'où $a - b = n(q - q') = nk$ en posant $k = q - q'$ avec $k \in \mathbb{Z}$. CQFD

Exemple : On a vu $21 \equiv 6\ [5]$ et $21 = 4 \times 5 + 1; 6 = 1 \times 5 + 1$.

Remarques :

- n pair $\iff n \equiv 0\ [2]$; n impair $\iff n \equiv 1\ [2]$
- n est un diviseur de $a \iff a \equiv 0\ [n]$

Propriétés : La congruence est une **relation d'équivalence** c'est-à-dire on a pour tous entiers a, b, c et n :

- (Réflexivité) $a \equiv a\ [n]$
- (Symétrie) $a \equiv b\ [n] \Rightarrow b \equiv a\ [n]$
- (Transitivité) $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$

Démonstration : Découle directement de ce qui précède.

Théorème : Soit n un entier naturel ($n \geqslant 2$), a et b deux entiers relatifs : $a \equiv b\ [n] \iff a - b \equiv 0\ [n]$.

Démonstration :
• Sens direct : $a \equiv b\ [n]$ d'où il existe q, q' et r entiers tels que $a = nq + r$ et $b = nq' + r$ avec $0 \leqslant r < n$.
D'où $a - b = n(q - q') \iff a - b \equiv 0\ [n]$.
• Sens indirect : $a - b \equiv 0\ [n] \iff a - b = kn$ avec k entier.
La division euclidienne de a par nn donne $a = nq + r$ avec $0 \leqslant r < n$.
D'où par substitution $nq + r - b = kn \iff b = (q - n) + r$. Ainsi a et b ont même reste dans la division euclidienne par n.

Propriétés : Compatibilité avec certaines opérations :
Soient n un entier naturel non nul et a, b, a', b' des nombres relatifs tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors on a :

- Addition : $a + a' \equiv b + b'\ [n]$
- Soustraction : $a - a' \equiv b - b'\ [n]$
- Produit : $a \times a' \equiv b \times b'\ [n]$
- Puissance : $a^p \equiv b^p\ [n]$

Démonstration :
• Addition : $\begin{cases} a \equiv b\ [n] \\ a' \equiv b'\ [n] \end{cases} \iff \begin{cases} a - b \equiv 0\ [n] \\ a' - b' \equiv 0\ [n] \end{cases} \iff \begin{cases} a - b = kn \\ a' - b' = k'n \end{cases}$ avec k, k' entiers.
$(a-b) + (a'-b') = kn + k'n \iff (a + a') - (b - b') = (k + k')n \iff a + a' \equiv b + b'\ [n]$.
• Multiplication : $\begin{cases} a \equiv b\ [n] \\ a' \equiv b'\ [n] \end{cases} \iff \begin{cases} a = b + kn \\ a' = b' + k'n \end{cases}$
$aa' = bb' + nK$ avec $K = bk' + b'k + kk'n \in \mathbb{Z}$ i.e. $aa' \equiv bb'\ [n]$

• Puissance : Par récurrence.
Initialisation : trivial pour $p = 0$ ou $p = 1$.
Hérédité : Supposons qu'il existe un entier k tel que la propriété $P(k) : a^p \equiv b^p \ [n]$ soit vraie.
Alors $a^{k+1} \equiv a^k \times a \equiv b^k \times b \equiv b^{k+1} \ [n]$.
Conclusion : La propriété est vraie pour $p = 0$ et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel p.
Exemples :

a. On a $7 \equiv 4 \ [3]$ et $11 \equiv 20 \ [3]$ d'où
$7 + 11 \equiv 4 + 20 \ [3] \iff 18 \equiv 24 \ [3]$
$7 \times 11 \equiv 4 \times 20 \ [3] \iff 77 \equiv 80 \ [3] \iff 77 \equiv 2 \ [3]$

b. $22 \equiv 1 \ [7]$ d'où $22^{50} \equiv 1 \ [7]$
$59 \equiv 3 \ [7]$ d'où $59^3 \equiv 2^3 \ [7] \iff 59^3 \equiv 1 \ [7]$.

Exemple : Déterminer le reste de la division de 2^{437} par 7.
Méthode :
On cherche une puissance de 2 congrue à 1 modulo 7. on trouve $2^3 \equiv 1 \ [7]$.
On décompose 497 avec la division euclidienne par 3 : $497 = 3 \times 145 + 2$.
Ainsi $2^{437} \equiv 2^{3\times145+2} \equiv \left(2^3\right)^{145} \times 2^2 \equiv 1^{145} \times 4 \equiv 4[7]$

Exemple : Résoudre une équation avec des congruences

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

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

a. $6 + x \equiv 5 \ [3] \iff x \equiv -1 \ [3] \iff x \equiv 2 \ [3]$.
Les entiers x solutions sont les entiers de la forme $2 + 3k$ avec $k \in \mathbb{Z}$.
b. $3x \equiv 5 \ [4] \iff 3x \equiv 1 \ [4]$.
x est nécessairement congru soit à 0,1,2 ou 3 modulo 4.
Par disjonction de cas on obtient :

x modulo 4	0	1	2	3
$3x$ modulo 4	0	3	2	1

Seul $x \equiv 3 \ [4]$ convient ainsi les entiers x solutions sont les entiers de la forme $3 + 4k$ avec $k \in \mathbb{Z}$.