Chapitre 5
Divisibilité dans $\mathbb{Z}$

1 Introduction et notations

On note $\mathbb{N}$ l'ensemble de tous les entiers naturels : $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$,
$\mathbb{N}^* = \mathbb{N} - \{0\}$ l'ensemble de tous les entiers naturels non nuls et
$\mathbb{Z}$ l'ensemble de tous les entiers relatifs : $\mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$. Ainsi, $\mathbb{N}^* \subset \mathbb{N} \subset \mathbb{Z}$.

Sauf mention explicite du contraire, un entier désignera toujours un entier relatif.

On rappelle que la *valeur absolue* d'un nombre réel x est le nombre réel positif ou nul noté $|x|$ défini par

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}.$$

La valeur absolue du réel x est égale à la distance de x à 0.

Exemples 1.1. $|3| = 3 = |-3|$, $\quad |0| = 0$, $\quad |-1,4| = 1,4 = |1,4|$.
Deux nombres opposés ont la même valeur absolue.

2 Division euclidienne dans $\mathbb{Z}$

Théorème 2.1 (Théorème de la division euclidienne)**.** *Soient a et b des entiers avec $b \neq 0$. Alors il existe un unique couple d'entiers (q, r) tel que*

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

Définition 1. L'opération permettant de passer du couple (a, b) au couple (q, r) s'appelle la *division euclidienne* de a par b. L'entier q est alors appelé le *quotient* et l'entier r le *reste* de cette division euclidienne.

Exemples 2.2.

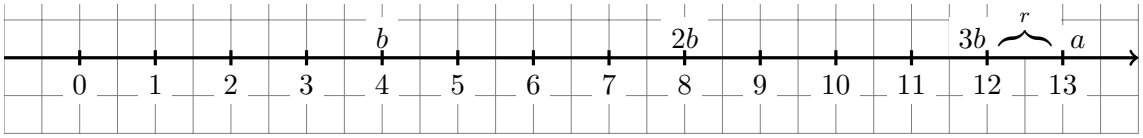
1. *Soient $a = 125$ et $b = 11$.*

2. *Soient $a = -35$ et $b = 12$.*

3. *Soient $a = 35$ et $b = -12$.*

4. *Soient $a = 12$ et $b = 35$*

Représentation graphique de la division euclidienne : cas où $a > b > 0$



L'entier bq est le multiple de b situé le plus près à gauche de a ; le reste r est alors la distance séparant bq de a, c'est-à-dire $r = a - bq$.

3 Divisibilité dans $\mathbb{Z}$

Définition 2. Soient a et b deux entiers. On dit que b *divise* a s' il existe un entier k tel que $a = kb$. On note alors $b \mid a$ (ce qui se lit donc "b divise a").

Ainsi, b divise a si et seulement si a est divisible par b.

Dans ce cas on dit que a est un multiple de b, mais aussi que b est un diviseur de a.

Attention : Ne pas confondre la relation de divisibilité avec l'opération division.
Ne pas écrire b/a au lieu de $b \mid a$.

Notation : Lorsque b ne divise pas a, on écrit $b \nmid a$.

Exemples 3.1.

1. 3 divise 21 (puisque $21 = 3 \times \mathbf{7}$) donc on note $3 \mid 21$.
2. 6 ne divise pas 21 donc on note $6 \nmid 21$

Proposition 1. *Un entier b non nul divise un entier a si et seulement si le reste de la division euclidienne de a par b est nul.*

Exemple 3.2. *966 est-il divisible par 23 ?*
Posons la division euclidienne de 966 par 23 pour en déterminer le quotient et le reste.

	$\overset{\frown}{966}$	23
-	92	42
	46	
-	46	
	0	

Ainsi 966=23× 42+0. Le reste est nul dans cette division euclidienne donc 23 divise 966.
On remarquera que 42 divise aussi 966.

Notations : Si a est un entier, on note $\mathcal{D}(a)$ l'ensemble de tous les diviseurs de a et $\mathcal{D}_{\mathbb{N}}(a)$ l'ensemble de tous les diviseurs positifs de a.

Exemples 3.3.

1. Soit $a = 182$. 182 est divisible par 1 et par lui-même.

   Alors $\mathcal{D}_{\mathbb{N}}(182) = \{1, \quad , \quad , \quad , \quad , \quad , \quad , 182\}$
2. On a aussi $\mathcal{D}_{\mathbb{Z}}(182) = \{ \qquad \}$.

Proposition 2.

1. *L'entier* 0 *ne divise que lui-même :* $0 \mid n \iff n = 0$.
2. *Soient* a *et* b *deux entiers tels que* $b \mid a$ *et* $a \neq 0$. *Alors* $1 \leq |b| \leq |a|$.

Attention au fait que $b \mid a$ n'implique pas nécessairement $b \leq a$; considérer par exemple $b = 1$ et $a = -1$ (on a $b \mid a$ mais $b > a$).

Démonstration :

1.

2.

Théorème 3.4. *Soient* a, b, c *et* n *des entiers.*

1. $1 \mid n$ *(l'entier* 1 *est diviseur universel).*
2. $n \mid 0$ *(l'entier* 0 *est multiple universel).*
3. $n \mid n$ *(réflexivité).*
4. *Si* $a \mid b$ *et* $b \mid a$, *alors* $|a| = |b|$, *c'est-à-dire* $a = b$ *ou* $a = -b$.
5. *Si* $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$ *(transitivité).*
6. *Si* $a \mid b$, *alors* $ac \mid bc$ *pour tout entier* c *; en particulier,* $a \mid bc$.
7. *Si* $ac \mid bc$ *pour un entier* c non nul, *alors* $a \mid b$.
8. *Si* $a \mid b$ *et* $a \mid c$, *alors* $a \mid xb + yc$ *pour tous* $x, y \in \mathbb{Z}$ *(linéarité de la divisibilité).*

Remarque.

1. La divisibilité ne satisfait pas la propriété d'antisymétrie suivante : "si $a \mid b$ et $b \mid a$, alors $a = b$". Par exemple, $1 \mid -1$ et $-1 \mid 1$, mais $1 \neq -1$. Bien faire attention aux valeurs absolues dans la propriété 4.
2. L'hypothèse $c \neq 0$ est essentielle dans la propriété 7 : en effet, si par exemple $a = 3$ et $b = 2$, alors on a bien $a \times 0 \mid b \times 0$ (puisque $0 \mid 0$) mais bien sûr $a \nmid b$.
3. Puisque $|n| = n$ pour tout $n \in \mathbb{N}$, les propriétés 3, 4 et 5 du théorème 3.4 impliquent que la relation de divisibilité est une *relation d'ordre* dans $\mathbb{N}$ (mais pas dans $\mathbb{Z}$).

4 Décomposition d'un nombre entier en produit de facteurs premiers

4.1 Nombres premiers

Définition 3. Un nombre entier naturel est dit **premier** s'il admet **exactement deux diviseurs** dans $\mathbb{N}$: 1 et lui-même.

Remarque. : L'expression "exactement deux diviseurs" signifie "deux diviseurs distincts".

1 n'est donc pas premier puisqu'il n'admet qu'un seul diviseur dans $\mathbb{N}$: lui-même.

Exemples 4.1. *:*

i) 0 n'est pas premier (il admet une infinité de diviseurs).

ii) 2, 3, 5, 7,11, 13, 17, 19, 23, 29, 31,... sont premiers.

iii) 6 n'est pas premier car il admet 4 diviseurs dans $\mathbb{N}$ *: 1, 2, 3 et 6.*

Théorème 4.2. *Tout entier naturel distinct de* 1 *admet au moins un diviseur premier.*

Théorème 4.3. *L'ensemble des nombres premiers est infini.*

4.2 Décomposition d'un nombre entier en produit de facteurs premiers

Exemples 4.4. *i) Soit $n = 26$. On cherche un facteur premier de 26.*
2 est premier et 2 divise 26 alors on écrit $26 = 2 \times 13$. Comme 13 est premier, 2×13 est la factorisation de 26 en produit de facteurs premiers.

ii) Soit $n = 24$. On a : $n = 2 \times 12$ et 12 n'est pas premier mais $12 = 2 \times 6$
donc $n = 2 \times 2 \times 6 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$.

iii) Soit $n = -24$. On a $n = -2^3 \times 3$.

On ne s'intéressera par la suite qu'à la décomposition en produit de facteurs premiers d'un entier naturel distinct de 0 et 1.

Disposition pratique de décomposition d'un nombre entier en produit de facteurs premiers :

38 808	2	38 808	$= 2 \times 19\,404$
19 404	2		$= 2 \times 2 \times 9\,702$
9 702	2		$= 2 \times 2 \times 2 \times 4\,851$
4 851	3		$= 2 \times 2 \times 2 \times 3 \times 1\,617$
1 617	3		$= 2 \times 2 \times 2 \times 3 \times 3 \times 539$
539	7		$= 2 \times 2 \times 2 \times 3 \times 3 \times 7 \times 77$
77	7		$= 2 \times 2 \times 2 \times 3 \times 3 \times 7 \times 7 \times 11$
11	11		
1			

Donc $38\,808 = 2^3 \times 3^2 \times 7^2 \times 11$.

Théorème 4.5. *Tout entier naturel n non nul et distinct de 1 peut s'écrire de **façon unique** sous la forme :*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$\text{où } \begin{cases} p_1, p_2, \cdots, p_r & \text{sont des nombres premiers tels que } p_1 < p_2 \cdots < p_r \\ \alpha_1, \alpha_2, \cdots, \alpha_r & \text{sont des entiers naturels non nuls.} \end{cases}$$

Cette égalité s'appelle **la décomposition en produit de facteurs premiers** de n.

Exemples 4.6. *Un autre exemple :*

983 125	5
196 625	5
39 325	5
7 865	5
1 573	11
143	11
13	13
1	

Donc $983\,125 =$.

5 Recherche des diviseurs et des multiples d'un entier naturel

5.1 Décomposition d'un diviseur de n. Nombre de diviseurs d'un entier.

Exemple introductif : on a $24 = 2^3 \times 3$. Soit d un diviseur positif de 24. Il existe un entier naturel q tel que $24 = qd$, c'est-à-dire tel que

$$2^3 \times 3 = qd$$

Par unicité de la décomposition en produit de facteurs premiers indiquée dans le théorème 4.5., la décomposition de d en produit de facteurs premiers ne peut contenir que les nombres premiers 2 et 3, avec des exposants inférieurs ou égaux à 3 et 1 respectivement.

Ainsi d est de la forme

$$d = 2^{\delta_1} \times 3^{\delta_2} \quad \text{où} \quad 0 \leq \delta_1 \leq 3 \text{ et } 0 \leq \delta_2 \leq 1$$

On notera qu'ici les exposants δ_1 et δ_2 peuvent prendre la valeur 0. On pourrait construire un arbre, ou un tableau, pour représenter tous les cas possibles et trouver ainsi tous les diviseurs positifs de 24.

δ_1	δ_2	$2^{\delta_1} \times 3^{\delta_2}$	$= d$
0	0	$2^0 \times 3^0$	$= 1$
0	1	$2^0 \times 3^1$	$= 3$
1	0	$2^1 \times 3^0$	$= 2$
1	1	$2^1 \times 3^1$	$= 6$
2	0	$2^2 \times 3^0$	$= 4$
2	1	$2^2 \times 3^1$	$= 12$
3	0	$2^3 \times 3^0$	$= 8$
3	1	$2^3 \times 3^1$	$= 24$

Ainsi l'ensemble des diviseurs positifs de 24 est

$$\mathcal{D}_{\mathbb{N}}(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}.$$

Le nombre de ces diviseurs est facilement calculable de la façon suivante :

(nombre de valeurs possibles pour δ_1)$\times$(nombre de valeurs possibles pour δ_2)
soit $(3 + 1) \times (1 + 1) = 8$

On remarque alors que la décomposition de 24 en produit de facteurs premiers est suffisante pour calculer ce nombre.

Théorème 5.1. *Soit n un entier naturel décomposé en produit de facteurs premiers comme dans le théorème :* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, *et d un entier naturel diviseur de n .*
Il existe donc un entier naturel q tel que $n = qd$.

i) Comme la décomposition d'un entier en produit de facteurs premiers est unique, d est de la forme :

$$d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r}$$

$$\textit{avec} \quad 0 \leq \delta_i \leq \alpha_i \quad \textit{pour tout } i \textit{ tel que } 1 \leq i \leq r.$$

ii) Le nombre d' entiers naturels diviseurs de n est donc :

$$card(\mathcal{D}_{\mathbb{N}}(n)) = (1 + \alpha_1)(1 + \alpha_2).....(1 + \alpha_r)$$

où $(1 + \alpha_i)$ est le nombre de choix possibles pour l'exposant du facteur p_i.

On pourrait construire ces nombres grâce à un arbre.

5.2 Autre méthode pour déterminer tous les diviseurs positifs d'un entier

Une astuce va permettre de déterminer sans effort la liste de tous les diviseurs de n dans $\mathbb{N}$. Considérons le produit :

$$(p_1^0 + p_1^1 + \cdots + p_1^{\alpha_1})(p_2^0 + p_2^1 + \cdots + p_2^{\alpha_2}) \cdots (p_n^0 + p_r^1 + \cdots + p_r^{\alpha_r}).$$

Chaque terme de son développement s'obtient en choisissant un terme dans chaque parenthèse et en faisant le produit de ces termes. Ceci prouve que chaque terme du produit est de la forme :

$$d' = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

avec $0 \leq \beta_i \leq \alpha_i$, pour tout i tel que $1 \leq i \leq r$.

d' est donc un diviseur de n et tous les diviseurs de n dans $\mathbb{N}$ s'obtiennent par ce procédé.

Exemple 5.2. *:*
$n = 120 = 2^3 \times 3 \times 5$.
n *admet* $(1+3) \times (1+1) \times (1+1) = 16$ *diviseurs positifs.*

Développons (sans réduire !) le produit P *suivant :*

$$P = (1 + 2 + 2^2 + 2^3)(1 + 3)(1 + 5) = \begin{cases} \quad 1 + 2 + 2^2 + 2^3 \\ +3 + 2.3 + 2^2.3 + 2^3.3 \\ +5 + 2.5 + 2^2.5 + 2^3.5 \\ +3.5 + 2.3.5 + 2^2.3.5 + 2^3.3.5 \end{cases}$$

Les termes de cette somme sont les diviseurs de 120 *dans* $\mathbb{N}$ *donc :*

$\mathcal{D}_{\mathbb{N}}(120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$.

Remarque. : le produit P a peu d'intérêt en lui-même. C'est ... la somme des diviseurs de n dans $\mathbb{N}$.

5.3 Décomposition d'un multiple de n

Soit m un multiple de n. Il existe un entier k tel que $m = nk$, c'est-à-dire :

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\ k.$$

Il se peut que la décomposition de k contienne certains des facteurs $p_1, \cdots, p_r$ donc la décomposition de m en facteurs premiers contient tous ces facteurs $p_i (1 \leq i \leq r)$ avec un exposant $\alpha_i \leq \mu_i$. On a donc :

$$m = p_1^{\mu_1} p_2^{\mu_2} \cdots p_r^{\mu_r} k'$$

où $k' \in \mathbb{N}$, tel que k' est premier avec n, et pour tout i tel que $1 \leq i \leq r$ on a : $\alpha_i \leq \mu_i$.

Exemples 5.3. *Soit m=*8 400 *un multiple de n=*120*. On a en effet* $8\,400 = 120 \times 70$.
On a $120 = 2^3 \times 3 \times 5$ *donc* $8\,400 = 2^3 \times 3 \times 5 \times 70$
$= 2^3 \times 3 \times 5 \times 2 \times 5 \times 7 = (2^4 \times 3 \times 5^2) \times 7$.
Ici on a $k' = 7$.

Annexes

Démonstration de la transitivité de la divisibilité : Soient a, b et c des entiers.
Hypothèse : $a \mid b$ et $b \mid c$

Montrons que $a \mid c$.

$a \mid b \iff$ il existe un entier k_1 tel que $b = k_1 \times a$.
$b \mid c \iff$ il existe un entier k_2 tel que $c = k_2 \times b$.

Il s'agit de trouver un entier k vérifiant $c = k \times a$.

Or $c = k_2 \times b = k_2 \times (k_1 \times a) = (k_2 \times k_1) \times a$.
Posons alors $k = k_2 \times k_1$.

Conclusion : $a \mid c$

Démonstration des autres assertions du théorème 3.4 :

1. $n = n \times 1$ donc $1 \mid n$.
2. $0 = n \times 0$ donc $n \mid 0$.
3. $n = 1 \times n$ donc $n \mid n$.
4. **Hypothèse :** $a \mid b$ et $b \mid a$
   Montrons qu'alors $a = b$ ou $a = -b$.
   $a \mid b \iff \exists k_1$ tel que $b = k_1 a$ et $b \mid a \iff \exists k_2$ tel que $a = k_2 b$.
   Ainsi $a = k_1 b = k_1 k_2 a$.

   Premier cas : $a = 0$. Les hypothèses sont alors $0 \mid b$ et $b \mid 0$, ce qui implique que $b = 0$. On a alors $a = b$.

   Deuxième cas : $a \neq 0$. Alors $k_1 k_2 = 1 \iff (k_1 = k_2 = 1)$ ou $(k_1 = k_2 = -1)$.

   On a alors $a = b$ ou $a = -b$
5. Transitivité : voir ci-dessus.
6. **Hypothèse :** $a \mid b$.
   Il existe donc un entier k telque $a = kb$. Soit un entier c quelconque. $a = kb \Rightarrow ac = k(bc)$, et donc $ac \mid bc$.
7. **Hypothèse :** $ac \mid bc$, avec $c \neq 0$.
   Il existe donc un entier k telque $ac = k(bc)$. Puisque $c \neq 0$, on peut diviser les deux membres de cette égalité par c, et on obtient $a = kb$.
   Alors $a \mid b$.
8. **Hypothèse :** $a \mid b$ et $a \mid c$.
   $a \mid b \iff \exists k_1$ tel que $b = k_1 a$ et $a \mid c \iff \exists k_2$ tel que $c = k_2 a$.
   Soit x et y deux entiers quelconques.
   Alors $xb + yc = x(k_1 a) + y(k_2 a) = (k_1 x + k_2 y)a$, ce qui prouve que $a \mid xb + yc$.