Mohammed El Amrani

# Arithmétique dans **Z** et dans **K**[*X*]

## Cours complet avec exercices et problèmes corrigés

ellipses

# Chapitre 1

# Divisibilité dans Z

Dans cet ouvrage, le mot "*entier*" (sans précision supplémentaire) désigne un élément de $\mathbf{Z}$.

## 1 Diviseurs. Multiples

**1.1. Définition** Soient $a$ et $b$ deux entiers. On dit que $a$ *divise* $b$, ou que $b$ est *divisible* par $a$, s'il existe un entier $k$ tel que $b = ka$. On dit encore que $a$ est un *diviseur* de $b$, ou que $b$ est un *multiple* de $a$.

**Notations**

– Si $a$ divise $b$, on note $a|b$, sinon, on note $a \not| b$.

– L'ensemble des diviseurs de $b$ est noté $\mathcal{D}(b)$.

– L'ensemble des multiples de $a$ est noté $\mathcal{M}(a)$ ou $a\mathbf{Z}$.

**1.2. Exemples** 1) 1 et $-1$ divisent tous les entiers mais ne sont divisibles que par 1 et $-1$.

2) 0 est un multiple de tous les entiers, mais n'est diviseur que de lui-même.

3) $\mathcal{D}(6) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$.

4) $\mathcal{M}(1) = \mathbf{Z}$, et $\mathcal{M}(2) = 2\mathbf{Z} = \{2k,\ k \in \mathbf{Z}\}$.

**1.3. Remarques** 1) On a bien sûr $a|a$ puisque $a = 1 \times a$.

2) Si $a|b$ et $b|c$ alors $a|c$. En effet, il existe $k, k' \in \mathbf{Z}$ tels que $b = ka$ et $c = k'b$. Donc $c = kk'a$, et comme $kk' \in \mathbf{Z}$, on a bien $a|c$.

**1.4. Proposition** *1) Soient $a$ et $b$ dans $\mathbf{Z}^*$. Si $a|b$, alors $|a| \leq |b|$.*

*2) Tout entier non nul admet un nombre fini de diviseurs.*

*Démonstration.* 1) Si $a|b$, alors il existe $k$ dans $\mathbf{Z}$ tel que $b = ka$. On a donc $|b| = |ka| = |k| \times |a|$.

Comme $b \neq 0$, on a $|k| \geq 1$, et par suite $|a| \leq |a| \times |k|$, c'est-à-dire $|a| \leq |b|$.
2) Soit $a$ un diviseur d'un entier non nul $b$. On a alors $|a| \leq |b|$, et par suite $-|b| \leq a \leq |b|$. L'entier $a$ prend donc au maximum $2\,|b| + 1$ valeurs. D'où le résultat annoncé. □

**1.5. Remarque** De la proposition ci-dessus, on déduit que

$$\big(a|b \quad \text{et} \quad b|a\big) \iff |a| = |b|.$$

En effet, $a|b$ et $b|a$ entraînent que $|a| \leq |b|$ et $|b| \leq |a|$, donc $|a| = |b|$.
Réciproquement, l'égalité $|a| = |b|$ implique $a = b$ ou $a = -b$, et par suite on a bien $a|b$ et $b|a$.

**1.6. Proposition** *Soient $a$ et $b$ dans* **Z**.
*1) Si $(u, v) \in \mathbf{Z}^2$, alors*

$$\big(d|a \ \text{ et } \ d|b\big) \ \Rightarrow \ d|(au + bv).$$

*2) Si $x$ est un entier non nul, alors*

$$a|b \iff ax|bx.$$

*Démonstration.* 1) Puisque $d|a$ et $d|b$, il existe $k$ et $k'$ dans **Z** tels que $a = kd$ et $b = k'd$. On a alors $au + bv = kdu + k'dv = d\,(ku + k'v)$, et comme $ku + k'v \in \mathbf{Z}$, on conclut que $d$ divise $au + bv$.
2) Si $a|b$ alors il existe $k \in \mathbf{Z}$ tel que $b = ka$, donc $bx = kax$, d'où $ax|bx$.
Réciproquement, si $ax|bx$, on a $bx = kax$ avec $k \in \mathbf{Z}$, et comme $x \neq 0$ il s'ensuit que $b = ka$, et donc $a|b$. □

**1.7. Remarque** Dans la première assertion de la proposition ci-dessus, l'implication "$\Leftarrow$" n'est pas vraie en général. Par exemple, 3 divise $2 + 4$ mais 3 ne divise pas 2.

## 2 Division euclidienne dans Z

Le résultat suivant est fondamental.

**2.1. Théorème** *Soient $a$ un entier et $b$ un entier naturel non nul. Il existe un unique couple $(q, r)$ d'entiers vérifiant :*

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b. \tag{1.1}$$

∗ *$q$ est appelé le quotient de la division euclidienne de $a$ par $b$,*
∗ *$r$ est appelé le reste de la division euclidienne de $a$ par $b$.*

*Démonstration.* – *Existence.*

Supposons d'abord que $a \in \mathbf{N}$ et considérons $A = \{n \in \mathbf{N}\ ,\ nb \leq a\}$.

L'ensemble $A$ est une partie non vide de $\mathbf{N}$ puisque $0 \in A$. De plus, $A$ est majorée par $a$ puisque si $n \in A$, alors $n \leq nb \leq a$ ($b$ est non nul donc $b \geq 1$). D'après la proposition 2.2 du chapitre 7, l'ensemble $A$ admet un plus grand élément, disons $q$, qui vérifie alors :

$*$ $qb \leq a$ puisque $q \in A$,

$*$ $(q+1)b > a$ puisque $q+1 \notin A$.

En prenant $r = a - bq$, on a alors $a = bq + r$ et $0 \leq r < (q+1)b - bq$, c'est-à-dire $0 \leq r < b$.

– Cas général où $a \in \mathbf{Z}$.

Comme $b \geq 1$, on a $|a|b \geq |a|$ et donc $a + |a|b \in \mathbf{N}$. En notant $q'$ et $r$ respectivement le quotient et le reste de la division euclidienne de $a + |a|b$ par $b$, on obtient

$$a = bq' + r - |a|b = bq + r$$

où l'on a posé $q = q' - |a|$.

– *Unicité.*

Soient $(q, r)$ et $(q', r')$ deux couples d'entiers vérifiant (1.1), et montrons que $q = q'$ et $r = r'$.

Puisque $0 \leq r < b$ et $0 \leq r' < b$, on a

$$0 \leq b\,|q - q'| = |r' - r| < b,$$

ce qui implique $|q - q'| = 0$. On en déduit que $q - q' = 0$, donc $q' = q$, et par suite $r' = r = 0$. □

**2.2. Remarque** Dans le théorème 2.1, on peut considérer $b$ dans $\mathbf{Z}^*$, mais alors la condition (1.1) devient

$$a = bq + r \quad \text{avec} \quad 0 \leq r < |b|. \tag{1.2}$$

Pour la démonstration, on traite le cas $b < 0$ en considérant l'entier naturel $-b$. Le théorème 2.1 donne alors l'existence de $(q', r')$ vérifiant

$$a = -bq' + r' \quad \text{avec} \quad 0 \leq r' < -b. \tag{1.3}$$

Il suffit alors de prendre $q = -q'$ et $r = r'$ pour déduire (1.2).

Pour prouver l'unicité, supposons que deux couples d'entiers $(q, r)$ et $(q', r')$ vérifient (1.2). On a alors

$$|r - r'| = |b\,(q - q')| \leq |b|$$

avec $r$ et $r'$ dans $[0, |b|[$, ce qui est impossible. Donc $q = q'$ et $r = r'$.

**2.3. Proposition** *Soient $a \in \mathbf{Z}$ et $b \in \mathbf{Z}^*$. Alors*

$$b|a \iff r = 0$$

*où $r$ désigne le reste de la division euclidienne de $a$ par $b$.*

*Démonstration.* D'après le théorème 2.1 et la remarque ci-dessus, il existe un unique couple $(q, r)$ d'entiers tels que

$$a = bq + r \quad \text{avec} \quad 0 \leq r < |b|.$$

– Si $r = 0$, alors $a = bq$, et donc $b$ divise $a$.
– Réciproquement, si $b$ divise $a$, alors $a = kb + 0$ avec $k \in \mathbf{Z}$ et $0 \leq 0 < |b|$. L'unicité fournie par le théorème 2.1 implique alors $k = q$ et $r = 0$. □

## 3 Numération des entiers naturels

### 3.1. Écriture en base $a$

La *numération* des entiers naturels est une des applications directes et importantes de la division euclidienne dans **Z**.
Précisons d'abord une notation que l'on gardera tout le long de l'ouvrage.
Si $a$ et $b$ sont deux entiers, avec $a \leq b$, on notera $[\![a, b]\!]$ l'ensemble des entiers $k$ vérifiant $a \leq k \leq b$.

**3.2. Définition** Soient $E$ un ensemble à $n$ éléments et $p \in [\![1, n]\!]$. On appelle *$p$-liste* de $E$ toute suite $(x_1, \ldots, x_p)$ de $p$ éléments de $E$.

**3.3. Proposition** *Soit $a \in \mathbf{N}$, $a \geq 2$. Pour $m \in \mathbf{N}^*$, il existe un unique entier naturel $p$ et une unique $(p+1)$-liste $(x_0, x_1, \ldots, x_p)$ d'éléments de $[\![0, a-1]\!]$ tels que*

$$m = x_p\, a^p + \cdots + x_1 a + x_0 \quad \text{avec} \quad x_p \neq 0.$$

*Démonstration.* – *Existence.* Raisonnons par récurrence forte sur $m \geq 1$.
Le résultat est vrai si $1 \leq m < a$, car il suffit alors de prendre $p = 0$ et $x_0 = m$.
Pour $m \geq a$, supposons le résultat vrai jusqu'au rang $m - 1$ et montrons-le au rang $m$.
Soient $q$ et $r$ le quotient et le reste de la division euclidienne de $m$ par $a$. Alors, $0 \leq r < a$ et $q \geq 1$ car $m \geq a$, et on a $q < m$ puisque $a > 1$.

Par hypothèse de récurrence, il existe $p \in \mathbf{N}^*$ et $(x_1, x_2, \ldots, x_p)$ une $p$-liste d'éléments de $[\![0, a-1]\!]$ telle que

$$q = \sum_{k=1}^{p} x_k \, a^{k-1} \quad \text{et} \quad x_p \neq 0.$$

En posant $x_0 = r$, la $(p+1)$-liste $(x_0, x_1, \ldots, x_p)$ est à éléments dans $[\![0, a-1]\!]$ et on a bien

$$m = r + qa = \sum_{k=0}^{p} x_k \, a^k \quad \text{avec} \quad x_p \neq 0.$$

– *Unicité.* Soient

$$(x_0, x_1, \ldots, x_p) \in [\![0, a-1]\!]^{p+1} \quad \text{et} \quad (y_0, y_1, \ldots, y_q) \in [\![0, a-1]\!]^{q+1}$$

deux listes telles que $x_p \neq 0$ et $y_q \neq 0$. Posons

$$m = \sum_{k=0}^{p} x_k \, a^k \quad \text{et} \quad n = \sum_{k=0}^{q} y_k \, a^k.$$

Si $p < q$, alors $p + 1 \leq q$, et comme $a \geq 2$, on a

$$m \leq \sum_{k=0}^{p} (a-1) \, a^k = a^{p+1} - 1 < a^q$$

ainsi que

$$n \geq y_q \, a^q \geq a^q$$

puisque $y_q \neq 0$. Donc $m < n$.

Si $p = q$ et $x_p < y_p$, alors le calcul ci-dessus où l'on remplace $p$ par $p-1$ et $q$ par $p$ montre que

$$\sum_{k=0}^{p-1} x_k \, a^k < a^p,$$

donc

$$m < (x_p + 1) \, a^p \leq y_p \, a^p \leq n.$$

Si $p = q$, alors $(x_p, x_{p+1}, \ldots, x_r) = (y_p, y_{p+1}, \ldots, y_r)$ et $x_{r-1} < y_{r-1}$ avec $r \in [\![1, p]\!]$ ; donc on a encore $m < n$ puisqu'en retranchant à $n$ et $m$ la quantité $\sum_{k=r}^{p} x_k \, a^k$ on se ramène au cas précédent.

On en déduit que si les listes $(x_0, x_1, \ldots, x_p)$ et $(y_0, y_1, \ldots, y_q)$ sont distinctes, alors $m \neq n$, ce qui prouve bien l'unicité annoncée. □

**3.4. Définition** Les entiers $x_p, \ldots, x_1, x_0$ sont appelés *chiffres*, et la formule

$$m = x_p\, a^p + \cdots + x_1\, a + x_0$$

est dite *écriture dans le système de numération en base a* de l'entier naturel $m$ considéré. On note alors

$$m = \overline{x_p \ldots x_1 x_0}^a,$$

ou simplement

$$m = \overline{x_p \ldots x_1 x_0}$$

lorsqu'aucun risque de confusion n'est à craindre.

**3.5. Exemples** Pour $a = 10$, on obtient l'écriture habituelle dite *décimale* dont les chiffres sont $0, 1, \ldots, 9$.

Pour $a = 2$, on obtient l'écriture dite *binaire* dont les chiffres sont 0 et 1.

Pour $a = 8$ on obtient l'écriture dite *octale*.

Pour $a = 16$ on obtient l'écriture dite *hexadécimale*...

**Méthode pratique :**

$*$ Pour obtenir l'écriture en base $a$ d'un entier naturel non nul $m$, il suffit de diviser $m$ par $a$, puis diviser le quotient obtenu par $a$, et ainsi de suite jusqu'à l'obtention d'un quotient nul. Les restes successifs nous donnent, de droite à gauche, les chiffres de l'écriture de l'entier naturel $m$ dans le système de numération en base $a$.

$*$ Réciproquement, pour retrouver l'entier naturel $m$ connaissant son écriture $\overline{x_p \ldots x_1 x_0}^a$, il suffit d'observer que

$$m = x_p \times a^p + \cdots + x_1 \times a + x_0$$

**3.6. Exemples** 1) Pour représenter le nombre 56 dans le système binaire, on a d'abord

$56 = 2 \times 28 + 0$ , $28 = 2 \times 14 + 0$ , $14 = 2 \times 7 + 0$ , $7 = 2 \times 3 + 1$,
$3 = 2 \times 1 + 1$, et enfin $1 = 2 \times 0 + 1$.

Les restes successifs (jusqu'à l'obtention d'un quotient nul) sont donc :
$0, 0, 0, 1, 1, 1$. En les écrivant de gauche à droite, on obtient $56 = \overline{111000}^2$.

2) Dans le système en base 12, si l'on convient de représenter par les symboles $A$ et $B$ les nombres 10 et 11 du système décimal, alors l'écriture $\overline{5A0B1}^{12}$ représente le nombre donné en base 10 par

$$5 \times 12^4 + 10 \times 12^3 + 0 \times 12^2 + 11 \times 12 + 1,$$

c'est-à-dire 9636.

### 3.7. Opérations en base $a$

**– Addition en base $a$ :**

L'opération d'addition en base 10 se généralise en base quelconque.

Soient $m = \overline{x_p \dots x_1 x_0}$ et $n = \overline{y_q \dots y_1 y_0}$ deux entiers naturels non nuls écrits en base $a$. Si l'on suppose par exemple que $q \leq p$, alors on peut poser $y_{q+1} = \dots = y_p = 0$, et on a

$$m = \sum_{k=0}^{p} x_k\, a^k \quad \text{et} \quad n = \sum_{k=0}^{p} y_k\, a^k,$$

d'où

$$m + n = \sum_{k=0}^{p} (x_k + y_k)\, a^k.$$

Cela n'est pas en général l'écriture en base $a$ de $m + n$ puisque $x_k + y_k$ (qui est inférieur à $2a - 2$) peut être plus grand que $a$. Dans ce cas, il faut *diminuer* $x_k + y_k$ de $a$ et propager une retenue sur les chiffres d'ordre $k + 1$.

**3.8. Exemple** En base 2, on a

$$\begin{array}{cccccc} & {\scriptstyle 1} & {\scriptstyle 1}1 & {\scriptstyle 1}0 & 1 & 0 \\ + & & & 1 & 1 & 1 \\ \hline & 1 & 0 & 0 & 0 & 1 \end{array}$$

ce qui correspond, en base 10, à l'opération : $10 + 7 = 17$.

**– Soustraction en base $a$ :**

Avec les notations ci-dessus, on a maintenant

$$m - n = \sum_{k=0}^{p} (x_k - y_k)\, a^k,$$

et ici aussi cette écriture n'est pas en général l'écriture en base $a$ de $m - n$ puisque $x_k - y_k$ peut être strictement négatif. Dans ce cas, il faut *ajouter* $a$ à $x_k$ et propager une retenue sur le chiffre $y_{k+1}$.

**3.9. Exemple** En base 5, on a

$$\begin{array}{cccccc} & & 4 & {\scriptstyle +5}3 & {\scriptstyle +5}1 & {\scriptstyle +5}2 \\ - & & {\scriptstyle 1}2 & {\scriptstyle 1}3 & {\scriptstyle 1}2 & 3 \\ \hline & & 1 & 4 & 3 & 4 \end{array}$$

**– Multiplication en base $a$ :**

L'opération de multiplication «à la main» en base 10 se généralise en base quelconque.

Soient $m = \overline{x_p \dots x_1 x_0}$ et $n = \overline{y_q \dots y_1 y_0}$ deux entiers naturels non nuls écrits en base $a$. Le produit $m \times n$ vaut $m \sum_{k=0}^{q} y_k\, a^k$. Il suffit donc de savoir multiplier un nombre par un chiffre et par une puissance de $a$, cette dernière multiplication étant très simple puisque :

$$m\, a^k \;=\; \overline{x_p \dots x_1 x_0 \underbrace{0 \dots 0}_{k \text{ fois}}}^{a}.$$

**3.10. Exemple** En base 2, on a

$$\begin{array}{cccccccc}
 & & & & 1 & 1 & 1 & 1 \\
 & & \times & & & 1 & 0 & 1 \\
\hline
 & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1}1 & 1 & 1 & 1 \\
+ & & 1 & 1 & 1 & 1 & . & \\
\hline
 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}$$

## 4 PGCD et PPCM dans Z

### 4.1. L'algorithme d'Euclide [1]

Soient $a$ et $b$ deux entiers.

– Si $(a, b) \neq (0, 0)$, l'ensemble des diviseurs communs à $a$ et $b$ est une partie non vide de **Z** puisqu'elle contient 1, et elle est majorée par $\max(|a|, |b|)$. D'après la proposition 2.2 du chapitre 7, cette partie possède un plus grand élément, qui est ici supérieur ou égal à 1.

– Si $ab \neq 0$, l'ensemble des multiples strictement positifs communs à $a$ et $b$ est une partie non vide de **N** car elle contient $|ab|$. D'après la proposition 2.2 de l'Annexe, cette partie possède un plus petit élément.

**4.2. Définition** $*$ Le PGCD de $a$ et $b$, noté $\mathrm{PGCD}(a, b)$ ou $a \wedge b$ est :

– le plus grand des diviseurs communs à $a$ et $b$ lorsque $(a, b) \neq (0, 0)$,

– 0 lorsque $a = b = 0$.

$*$ Le PPCM de $a$ et $b$, noté $\mathrm{PPCM}(a, b)$ ou $a \vee b$ est :

– le plus petit des multiples strictement positifs communs à $a$ et $b$ lorsque $a$ et $b$ sont non nuls.

– 0 lorsque $a = 0$ ou $b = 0$.

1. EUCLIDE, un des plus grands mathématiciens de la Grèce antique, souvent désigné comme «le père de la géométrie» car il est l'auteur des *Éléments de mathématiques* qui sont considérés comme l'un des textes fondateurs des mathématiques en Occident.