# Chapitre I

## Divisibilité dans Z

# Table des matières

# 1 Diviseurs et multiples

L'ensemble **Z** des entiers relatifs est stable par addition, soustraction et multiplication, c'est à dire que chacune de ces opérations, appliquée à deux entiers relatifs, donne un entier relatif. Ce n'est pas le cas pour la division. On trouve sans difficulté des exemples de divisions d'entiers donnant des résultats non entiers. Les divisions restant dans le cadre de l'ensemble **Z** ont de ce fait un intérêt particulier.

**Définition 1** Diviseur – Multiple

Soient $a$ et $b$ deux nombres entiers relatifs non nuls. On dit que $a$ est divisible par $b$ si il existe un entier relatif $c$ tel que $a = bc$. On dit alors que $b$ est un **diviseur** de $a$ et que $a$ est un **multiple** de $b$.

*Exemple :* 12 est divisible par 3 ; 3 est un diviseur de 12 ; 12 est un multiple de 3.

**Proposition 1**

Soient $a$ et $b$ deux entiers tels que $a$ est divisible par $b$. Alors,

1. L'entier $a$ est divisible par $-b$.
2. Les nombres $a$ et $b$ vérifient $|b| \leqslant |a|$.
3. Si d'autre part $b$ est divisible par $a$, alors $a = b$ ou $a = -b$.
4. Si $k$ est un entier quelconque non nul, alors $bk$ divise $ak$.
5. Si $d$ est un entier qui divise $b$, alors $d$ divise $a$. On dit que la relation de divisibilité est transitive.

**Preuve.** Par définition, le fait que $a$ soit divisible par $b$ signifie qu'il existe un entier relatif $c$ tel que $a = bc$.

1. Sachant que $a = bc$, il est clair que $a = (-b)(-c)$ donc $a$ est divisible par $-b$.
2. Par définition, $1 \leqslant |c|$ donc $|b| \leqslant |bc|$, c'est à dire $|b| \leqslant |a|$.
3. D'après la propriété démontrée précédemment, si $b$ divise $a$ et $a$ divise $b$ alors on a à la fois $|b| \leqslant |a|$ et $|a| \leqslant |b|$, donc $|a| = |b|$. Ceci signifie que soit $a = b$, soit $a = -b$.
4. On sait que $a = bc$, donc $ak = (bc)k = (bk)c$, ce qui prouve que $bk$ divise $ak$.
5. Si $d$ divise $b$, alors il existe un entier $c'$ tel que $b = dc'$. On en déduit que $a = bc = dc'c$ et donc que $d$ divise $a$.

**Proposition 2** Linéarité de la divisibilité

Si un entier $b$ divise deux entiers $a$ et $a'$, alors $b$ divise toute combinaison linéaire de $a$ et $a'$, c'est à dire tout entier de la forme $au + a'v$, où $u$ et $v$ sont deux entiers quelconques. En particulier, $b$ divise $a + a'$ et $a - a'$.

*Exemple :* 12 divise 24 et 36 donc, sans faire de calcul, on sait que 12 divise $5 * 24 + 2 * 36$.

**Preuve.** Par définition, si $b$ divise $a$ et $a'$, il existe deux entiers $c$ et $c'$ tels que $a = bc$ et $a' = bc'$. Ainsi, quels que soient les entiers $u$ et $v$, $au + a'v = (bc)u + (bc')v = b(cu + c'v)$, ce qui prouve que $b$ divise $au + a'v$.

# 2 P.G.C.D de deux entiers

**Définition 2**

Soit $a$ un entier positif. On note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de $a$. Cet ensemble est fini car tout diviseur positif $m$ de $a$ vérifie $m < a$.
Par convention, l'ensemble $\mathcal{D}(0)$ est l'ensemble des entiers naturels.

*Exemple :* $\mathcal{D}(12) = \{1; 2; 3; 4; 6; 12\}$.

**Définition 3** Plus grand diviseur commun

Soient $a$ et $b$ deux entiers naturels. L'ensemble de leurs diviseurs positifs communs est $\mathcal{D}(a, b) = \mathcal{D}(a) \cap \mathcal{D}(b)$. Cet ensemble est fini car majoré par $a$ et $b$. Il contient donc un plus grand élément unique $d$, le plus grand diviseur commun de $a$ et $b$. On le note **P.G.C.D** de $a$ et $b$ et on le note $\text{PGCD}(a, b)$ ou $a \wedge b$.

*Exemple :* $\mathcal{D}(12) = \{1; 2; 3; 4; 6; 12\}$ et $\mathcal{D}(16) = \{1; 2; 4; 8; 16\}$ donc $\text{PGCD}(12, 16) = 4$.

**Proposition 3**

Soient $a$ et $b$ deux entiers positifs.

1. $\mathcal{D}(a, 0) = \mathcal{D}(a)$, donc $\text{PGCD}(a, 0) = a$.
2. Si $b$ divise $a$ alors $\mathcal{D}(a, b) = \mathcal{D}(b)$ et donc $\text{PGCD}(a, b) = b$.
3. $\text{PGCD}(a, b) \geqslant 1$, car $1 \in \mathcal{D}(a, b)$.

**Preuve.**

1. Par définition $\mathcal{D}(a, 0) = \mathcal{D}(a) \cap \mathcal{D}(0) = \mathcal{D}(a) \cap \mathbf{N} = \mathcal{D}(a)$. Il est alors clair que $\text{PGCD}(a, 0) = a$.
2. Si $b$ divise $a$ il est clair que $\mathcal{D}(b) \subset \mathcal{D}(a)$ et donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b)$. Par conséquent $\text{PGCD}(a, b) = b$.
3. Il est clair que 1 divise $a$ et $b$, donc $1 \in \mathcal{D}(a)$ et $1 \in \mathcal{D}(b)$, ce qui prouve que $1 \in \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a, b)$. Par conséquent, $\text{PGCD}(a, b) \geqslant 1$.

**Définition 4**

Soient $a$ et $b$ deux entiers relatifs. Leur P.G.C.D est $PGCD(a; b) = PGCD(|a|; |b|)$.

# 3 Les nombres premiers

## a ) Définition

**Définition 5** Nombre premier

Un entier naturel $n$ est **premier** s'il admet exactement deux diviseurs positifs distincts, 1 et lui-même.

*Exemples :*

- L'entier 1 n'est pas premier car il n'a qu'un diviseur positif.
- Le plus petit nombre premier est 2, qui est divisible par 1 et 2.
- 3 est aussi premier.
- 4 n'est pas premier car il est divisible par 1, 2 et 4.
- Plus généralement, un nombre pair supérieur à 4 n'est pas premier, car il est divisible par 1, 2 et lui-même, soit au moins 3 diviseurs.

## b ) Reconnaître un nombre premier

### i ) Méthode directe

Soit $n$ un entier. Pour savoir si $n$ est premier, on effectue les divisions de $n$ par tous les entiers naturels inférieurs à $n$. Si aucune de ces divisions ne donne un résultat entier, alors $n$ est un nombre premier.

### ii ) Méthode directe optimisée

Elle est basée sur la propriété suivante :

**Proposition 4**

Si tous les nombres premiers inférieurs à $\sqrt{N}$ ne sont pas des diviseurs de N, alors N est un nombre premier.

*Exemple :* 53 est -il un nombre premier ?
$\sqrt{53}$ environ 7,28. Les nombres premiers inférieurs à 7,28 sont 2, 3, 5, 7. Comme aucun d'eux ne divisent 53, alors 53 est un nombre premier.

### iii ) Crible d'Erathostène

A proprement parler, le crible d'Erathostène ne détermine pas si un entier est premier. C'est une méthode pour dresser la liste de tous les nombres premiers inférieurs à un entier naturel $n$. Prenons l'exemple $n = 50$. Plaçons tous les entiers naturels inférieurs à 50 dans un tableau.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 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 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

Commençons par barrer le nombre 1, qui n'est pas premier par définition. Le nombre 2 est premier. On peut alors barrer tous les multiples de 2, puisqu'ils ne sont pas premiers. Le nombre non barré suivant est donc premier, il s'agit de 3. On barre maintenant tous les multiples de 3, qui ne peuvent pas être premiers et on passe au nombre non barré suivant. Une fois tout le tableau parcouru, les seuls entiers non barrés sont tous les nombres premiers inférieurs à 50.

## c ) Ensemble des nombres premiers

On a longtemps cherché une logique dans la répartition des nombres premiers. En vain. On est aujourd'hui persuadé que cette répartition est anarchique. Seuls quelques résultats concernant l'ensemble des nombres premiers sont connus à ce jour.

**Théorème 1** Théorème d'Euclide (Livre IX, proposition 20)

L'ensemble des nombres premiers est infini.

**Preuve.** Démontrons ce résultat par l'absurde, c'est à dire en supposant que l'ensemble des nombres premiers est fini.
Notons alors $\mathcal{P}$ le produit de tous les nombres premiers. Il est clair que $\mathcal{P}+1$ n'est divisible par aucun des nombres premiers (car $\mathcal{P}$ est divisible par chacun des nombres premiers mais 1 ne l'est pas). Il est donc premier, ce qui est impossible car il ne fait pas partie de l'ensemble des nombres premiers. Ceci contredit notre hypothèse. Par conséquent, l'ensemble des nombres premiers est infini.

*Remarque :* La demonstration s'appuie sur le fait que si $a$ et $b$ sont premiers alors $a \times b + 1$ l'est aussi.

La répartition des nombres premiers est donnée par la fonction $\pi$, où $\pi(x)$ est le nombre d'entiers premiers inférieurs à $x$. Le mathématicien Tchebychef a démontré en 1896 que $\pi(x)$ est équivalent, au voisinage de l'infini, à $\frac{x}{\ln x}$. Cela signifie globalement que la proportion de nombres premiers est décroissante

## d ) Décomposition en facteurs premiers

**Proposition 5**

Soit $a$ un entier naturel ($a > 1$). Alors :
- $a$ admet un diviseur premier.
- Si $a$ n'est pas premier, il admet un diviseur premier $p$ tel que $2 \leqslant p \leqslant \sqrt{a}$.

**Preuve.**
- Si $a$ est premier, comme $a$ divise $a$, la propriété est bien vérifiée.
- Si $a$ n'est pas premier alors il admet au moins un diviseur strictement supérieur à 1. Notons $p$ le plus petit d'entre ces diviseurs. $p$ est forcement premier car sinon, il admettrait un diviseur $d$ avec $1 < d < p$, qui serait alors un diviseur de $a$ strictement inférieur au plus petit d'entre eux : $p$ ; c'est impossible. Donc $p$ est pemier.

De plus, $a$ s'écrit $a = pq$ avec $p \leqslant q$ ; on en tire : $p^2 \leqslant pq = a$, donc $p \leqslant \sqrt{a}$. Finalement, on a bien

$$2 \leqslant p \leqslant \sqrt{a}.$$

**Théorème 2** Décomposition en facteurs premiers

Soit $n$ un entier supérieur ou égale à deux. Alors :
- $n$ se décompose en un produit de facteur premier.
- Cette décomposition est unique à l'ordre des facteurs près.
  On note alors $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ où $p_1, p_2, \cdots p_r$ sont des nombres premiers distincts et $\alpha_1, \alpha_2, \cdots \alpha_r$ sont des entiers naturels non nuls.

**Preuve.** On ne démontrera que l'existence de la décomposition. L'unicité est admise.
Démontrons cette propriété par récurrence.
- **Initialisation :** Pour $n = 2$, elle est vraie puisque 2 est lui-même premier.
- **Hérédité :** Supposons la propriété vérifiée pour tout entier $n \leqslant k$ et étudions le cas $n = k+1$.
  - Si $k+1$ est premier, la propriété est bien vérifiée.
  - Sinon, $k+1$ admet un diviseur premier $p$ et il existe $k'$ tel que $k+1 = pk'$ avec $k' < k+1$. Par récurrence, $k'$ est un produit de nombres premiers, et donc $k+1$ aussi.

**Preuve.** Voici une autre preuve moins formelle :
D'après la proposition 5, $n$ admet un diviseur premier $p_1$, alors $n = p_1 n_1$ avec $1 \leqslant n_1 < n$, puisque $p_1 \geqslant 2$.
Si $n_1 = 1$, c'est terminé.
Si $n_1 \geqslant 2$ on répète ce raisonnement avec $n_1$ : $n_1$ admet un diviseur premier $p_2$ et $n_1 = p_2 n_2$, avec $1 \leqslant n_2 < n_1 < n$.
On itère ce raisonnement tant que le quotient $n_i$ n'est pas égal à 1.
La suite de ces quotients étant strictement décroissante ($\cdots < n_i < \cdots < n_2 < n_1 < n$), le processus s'arrête à une certaine étape $k$. Alors $n = p_1 p_2 \cdots p_k$ et en regroupant les facteurs non distincts, on obtient :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

### Méthode de décomposition

Pour décomposer un entier naturel en facteurs premiers, on peut utiliser une méthode systématique qui consiste à tester un par un par les facteurs possibles, c'est à dire les nombres premiers inférieurs à $n$. L'exemple suivant, $n = 2184$ expose le procédé et sa présentation graphique conventionnelle :

| | | |
|---|---|---|
| 2184 est divisible par 2 et le quotient est 1092 | 2184 | 2 |
| 1092 est divisible par 2 et le quotient est 546 | 1092 | 2 |
| 546 est divisible par 2 et le quotient est 273 | 546 | 2 |
| 273 est divisible par 3 et le quotient est 91 | 273 | 3 |
| 91 est divisible par 7 et le quotient est 13 | 91 | 7 |
| 13 est un nombre premier | 13 | 13 |
| La décomposition est terminée | 1 | |

La décomposition en facteurs premiers de 2184 est donc $2184 = 2^3 \times 3 \times 7 \times 13$.

**Théorème 3**

Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition en nombres premiers d'un entier naturel $n$. Les diviseurs de $n$ sont les entiers dont les décompositions sont de la forme $p_1^{\beta_1} \cdots p_k^{\beta_k}$, où pour tout $i \in \{1, \cdots, k\}$, $\beta_i \leqslant \alpha_i$.

**Preuve.** Il est clair qu'un entier de la forme donnée dans le théorème divise bien $n$. Il reste à démontrer que tout diviseur de $n$ est de cette forme.
Soient $d$ un diviseur de $n$, $p$ un facteur premier de $d$ et $\beta$ tel que $d = p^\beta d'$, où $d'$ n'est pas divisible par $p$. Alors $p^\beta$ divise $n$ et donc $p$ doit être l'un des facteurs premiers de $n$, disons $p_i$. Il est alors clair que $\beta$ doit être inférieur à $\alpha_i$. Comme ceci est vrai pour tous ses diviseurs premiers, $d$ est bien de la forme donnée dans le théorème.

**Proposition 6**

Soit $n$ un entier supérieur ou égal à 2, admettant la décomposition en facteur premier :

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Le nombre de diviseurs de $n$ est :

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

**Preuve.** Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors d'après la proposition précédente, tout diviseur $d$ de $n$ s'écrit $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, où pour tout $i \in \{1, \cdots, k\}$, $\beta_i \leqslant \alpha_i$.
On a $\alpha_1 + 1$ choix pour la valeur de $\beta_1$, $\alpha_2 + 1$ choix pour la valeur de $\beta_2$, ...

# 4 P.P.C.M

**Définition 6**

Soient $a$ et $b$ deux entiers positifs. L'ensemble des multiples positifs non nuls communs à $a$ et $b$ n'est pas vide car il contient $ab$, et il est minoré par $a$ et $b$. Il contient donc un plus petit élément. Cet élément est appelé P.P.C.M de $a$ et $b$ et noté PPCM$(a, b)$ ou $a \vee b$.

**Proposition 7**

Tout multiple commun à $a$ et $b$ est un multiple de leur P.P.C.M $m$.

**Preuve.** Soit $n$ un multiple commun à $a$ et $b$ et $m$ leur P.P.C.M. Par définition de $m$, on a $m \leqslant n$. La division de $n$ par $m$ donnent deux nombres $q$ et $r$ tel que $n = mq + r$ avec $r < m$.
On a alors $r = n - mq$ qui est un multiple commun à $a$ et $b$ (car $n$ et $m$ le sont) et qui est inéfrieur à $m$. Par définition de $m$, on a donc $r = 0$. Ainsi $n$ est un multiple de $m$.

**Théorème 4**

Soient $a$ et $b$ deux entiers. Si $d$ et $m$ sont respectivement le P.G.C.D et le P.P.C.M de $a$ et $b$, alors $md = ab$.

**Preuve.**

- On considère l'entier $\frac{ab}{d}$. $d$ étant le pgcd, il existe $a'$ et $b'$ entiers tels que $\frac{ab}{d} = a'b = ab'$ ce qui signifie que $\frac{ab}{d}$ est un multiple commun à $a$ et $b$.
  C'est donc, d'après la propriété précédente, un multiple de $m$. Cela signifie qu'il existe $k$ dans $\mathbf{Z}$ tel $\frac{ab}{d} = km$, et donc $ab = kmd$.
- $m$ étant un multiple commun à $a$ et $b$, il existe $h$ et $h'$ dans $\mathbf{Z}$ tels que $m = ah$ et $m = bh'$. En remplaçant $m$ par la première de ces expressions, on obtient $ab = kahd$, et donc $b = kdh$. L'entier $b$ est donc divisible par $kd$. De manière analogue $kd$ divise aussi $a$. Par maximalité de $d$, on doit donc avoir $kd \leqslant d$. La seule valeur possible pour $k$ est 1, ce qui implique $ab = md$.

**Théorème 5**

Soient $a$ et $b$ deux entiers. Notons $\{p_1,\dots,p_k\}$ l'union des ensembles de leurs facteurs premiers. On peut noter $a = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ et $b = p_1^{\beta_1}\dots p_k^{\beta_k}$ où certains exposants $\alpha_i$ et $\beta_i$ sont éventuellement nuls. Notons $d$ et $m$ respectivement le P.G.C.D et le P.P.C.M de $a$ et $b$. Alors

$$d = p_1^{\text{Min}(\alpha_1,\beta_1)}\cdots p_k^{\text{Min}(\alpha_k,\beta_k)} \text{ et } m = p_1^{\text{Max}(\alpha_1,\beta_1)}\cdots p_k^{\text{Max}(\alpha_k,\beta_k)}.$$

**Preuve.** Soit $d'$ un diviseur commun de $a$ et $b$. D'après le théorème 3.3, $d'$ est de la forme $p_1^{\gamma_1}\dots p_k^{\gamma_k}$, où pour tout $i\in\{1,\dots,k\}$, $\gamma_i \leqslant \alpha_i$ et $\gamma_i \leqslant \beta_i$, c'est à dire $\gamma_i \leqslant \text{Min}(\alpha_i,\beta_i)$. Par conséquent tout diviseur commun à $a$ et $b$ $d'$ vérifie $d' \leqslant p_1^{\text{Min}(\alpha_1,\beta_1)}\dots p_k^{\text{Min}(\alpha_k,\beta_k)}$, et comme ce produit est bien un diviseur de $a$ et $b$, c'est leur P.G.C.D. D'autre part on sait que $ab = md$, c'est à dire $m = \frac{ab}{d}$, et donc

$$\begin{aligned} m &= \frac{p_1^{\alpha_1}\cdots p_k^{\alpha_k}\times p_1^{\beta_1}\cdots p_k^{\beta_k}}{p_1^{\text{Min}(\alpha_1,\beta_1)}\cdots p_k^{\text{Min}(\alpha_k,\beta_k)}} \\ m &= \frac{p_1^{\alpha_1+\beta_1}\cdots p_k^{\alpha_k+\beta_k}}{p_1^{\text{Min}(\alpha_1,\beta_1)}\cdots p_k^{\text{Min}(\alpha_k,\beta_k)}} \\ m &= p_1^{\text{Max}(\alpha_1,\beta_1)}\cdots p_k^{\text{Max}(\alpha_k,\beta_k)} \end{aligned}$$

*Exemple :* Prenons $a = 2184$ et $b = 1617$. Leurs décompositions en facteurs premiers sont $a = 2^3\times 3\times 7\times 13$ et $b = 3\times 7^2\times 11$. Donc

$$\begin{aligned} PGCD(a,b) &= 3\times 7 = 21 \\ PPCM(a,b) &= 2^3\times 3\times 7^2\times 11\times 13 \\ &= 168168. \end{aligned}$$