

## ◆ Chapitre 12. — Arithmétique dans $\mathbb{Z}$

*Rappels.* On note  $\mathbb{N}$  l'ensemble des entiers naturels c'est-à-dire l'ensemble des entiers positifs ou nuls. Ainsi,  $\mathbb{N} = \{0; 1; 2; 3; 4; \dots\}$ .

On note  $\mathbb{Z}$  l'ensemble des entiers relatifs c'est-à-dire l'ensemble des entiers positifs, négatifs ou nuls. Ainsi,  $\mathbb{Z} = \{\dots; -4; -3; -2; -1; 0; 1; 2; 3; 4; \dots\}$

Dans tout ce chapitre, lorsqu'on ne précise pas, le mot « entier » signifie « entier relatif ».

### I. — Notion de divisibilité

#### Définition 1

Soit  $a$  et  $b$  deux nombres entiers relatifs. On dit que  $b$  divise  $a$  s'il existe un entier relatif  $k$  tel que  $a = k \times b$ .

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

#### Exemple 2.

1. 4 divise 12 car  $12 = 3 \times 4$  (ici,  $k = 4$ ).
2. 30 est un multiple de  $-6$  car  $30 = (-5) \times (-6)$  (ici,  $k = -5$ ).
3. 1 divise n'importe quel entier  $a$  car  $a = a \times 1$  (ici,  $k = a$ ).
4. Tout entier  $b$  divise 0 car  $0 = 0 \times b$  (ici,  $k = 0$ ).
5. Si  $b$  est un diviseur de  $a$  alors  $-b$  est aussi un diviseur de  $a$ . En effet, dans ce cas, il existe un entier  $k$  tel que  $a = k \times b$  donc  $a = (-k) \times (-b)$  et  $-k$  est un entier car  $k$  est un entier donc  $-b$  est un diviseur de  $a$ .

*Remarque 3.* ATTENTION! Le mot « divise » ne fait pas référence ici à une division. Ainsi, si on ne peut pas diviser par 0, on peut en revanche dire que 0 divise 0 car  $0 = 2 \times 0$ .

*Remarque 4.* On remarque que les diviseurs fonctionnent par paire. En effet, 4 divise 12 car  $12 = 3 \times 4$  mais on a donc aussi  $12 = 4 \times 3$  ce qui signifie que 3 divise aussi 12. On dit que 3 et 4 forment une paire de diviseurs associés de 12. Il se peut cependant que deux diviseurs associés d'un entier  $a$  soient égaux : par exemple,  $36 = 6 \times 6$  donc 6 divise 36 et son diviseur associé est lui-même. Cela signifie en fait que  $a$  est le carré d'un entier. C'est ce qu'on appelle un carré parfait.

#### Définition 5

De manière plus générale, si  $x$  et  $y$  sont des réels quelconques (pas nécessairement entiers), on dit que  $y$  est un multiple de  $x$  s'il existe un entier relatif  $k$  tel que  $y = k \times x$ .

**Exemple 6.** Ainsi, 7 est un multiple de 3,5 car  $7 = 2 \times 3,5$  et  $\sqrt{18}$  est un multiple de  $\sqrt{2}$  car  $\sqrt{18} = \sqrt{9 \times 2} = \sqrt{9} \times \sqrt{2} = 3 \times \sqrt{2}$ .

ATTENTION, on ne peut pas dire en revanche que 7 est un multiple de 2 car 3,5 n'est pas un entier. Ainsi, dans le cas des réels, les diviseurs ne fonctionnent pas forcément par paire.

### Propriété 7

Soit  $x$  un réel. On suppose que  $y$  et  $z$  sont des multiples de  $x$ . Alors,  $y + z$  est un multiple de  $x$ .

*Démonstration.* Comme  $y$  est un multiple de  $x$ , il existe un entier  $k$  tel que  $y = kx$ . De même, comme  $z$  est un multiple de  $x$ , il existe un entier  $k'$  tel que  $z = k'x$ . (Attention, il n'y a aucune raison que  $k = k'$  donc il faut choisir deux noms différents pour ces entiers). Dès lors,  $y + z = kx + k'x = (k + k')x$ . Or, comme  $k$  et  $k'$  sont des entiers,  $k + k'$  est un entier donc  $y + z$  est un multiple de  $x$ .  $\square$

**Exemple 8.** Les nombres  $6\pi$  et  $-14\pi$  sont des multiples de  $2\pi$  car  $6\pi = 3 \times 2\pi$ ,  $-14\pi = -7 \times 2\pi$  et 3 et  $-7$  sont des entiers. On en déduit que  $6\pi + (-14\pi)$  est un multiple de  $2\pi$ . (Et, en effet,  $6\pi + (-14\pi) = 6\pi - 14\pi = -8\pi = -4 \times 2\pi$ .)

## II. — Nombres pairs et nombres impairs

### Définition 9

Soit  $n$  un entier relatif. On dit que :

1.  $n$  est pair si  $n$  est un multiple de 2 ;
2.  $n$  est impair si  $n - 1$  est pair.

**Exemple 10.**

1. Le nombre 6 est pair car  $6 = 3 \times 2$  donc 6 est un multiple de 2.
2. Le nombre 0 est pair car  $0 = 0 \times 2$  donc 0 est un multiple de 2.
3. Le nombre  $-198$  est pair car  $-198 = (-99) \times 2$  donc  $-198$  est un multiple de 2.
4. Le nombre 1 est impair car  $1 - 1 = 0$  est pair.
5. Le nombre 7 est impair car  $7 - 1 = 6$  est pair.
6. Le nombre  $-19$  est impair car  $-19 - 1 = -20 = (-10) \times 2$  est pair.

### Propriété 11

1. Un nombre entier  $n$  est pair si et seulement s'il existe un entier  $k$  tel que  $n = 2k$ .
2. Un nombre entier  $n$  est impair si et seulement s'il existe un entier  $k$  tel que  $n = 2k + 1$ .

*Démonstration.*

1. Un entier  $n$  est pair si et seulement si  $n$  est un multiple de 2 ce qui, par définition, équivaut à l'existence d'un entier  $k$  tel que  $n = 2k$ .
2. Un entier  $n$  est impair si et seulement si  $n - 1$  est pair ce qui équivaut, d'après ce qui précède, à l'existence d'un entier  $k$  tel que  $n - 1 = 2k$ . On conclut donc que  $n$  est impair si et seulement s'il existe un entier  $k$  tel que  $n = 2k + 1$ .  $\square$

**Exemple 12.** Si  $m$  est un entier alors le nombre entier  $4m + 3$  est impair. En effet, on peut écrire  $4m + 3 = 2 \times 2m + 2 + 1 = 2(2m + 1) + 1$  donc, en posant  $k = 2m + 1$  qui est bien un entier car  $m$  est entier, on a  $4m + 3 = 2k + 1$ . Ainsi,  $4m + 3$  est impair.

*Remarque 13.* On peut montrer que tout entier  $n$  est soit pair soit impair : c'est ce qu'on appelle la parité de  $n$ .

#### Propriété 14

Soit  $n$  un entier. Alors,  $n$  et  $n^2$  ont la même parité.

*Démonstration.* Supposons que  $n$  est pair. Alors, il existe un entier  $k$  tel que  $n = 2k$ . Dès lors,  $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ . En posant  $K = 2k^2$  qui est un entier car  $k$  est entier, on a  $n^2 = 2K$  donc  $n^2$  est pair.

Supposons que  $n$  est impair. Alors, il existe un entier  $k$  tel que  $n = 2k + 1$ . Dès lors, grâce aux identités remarquables,  $n^2 = (2k + 1)^2 = (2k)^2 + 2 \times 2k \times 1 + 1^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ . En posant  $K = 2k^2 + 2k$  qui est un entier car  $k$  est entier, on a  $n^2 = 2K + 1$  donc  $n^2$  est impair.

Ainsi, on a bien montré que  $n$  et  $n^2$  ont la même parité.  $\square$

### III. — Nombres premiers

#### Définition 15

Un entier naturel  $p$  est un nombre premier si  $p$  admet exactement deux diviseurs positifs : 1 et lui-même.

**Exemple 16.** Les nombres premiers inférieurs ou égaux à 20 sont 2, 3, 5, 7, 11, 13, 17 et 19.

*Remarque 17.* 0 n'est pas premier car il admet une infinité de diviseurs positifs (on a vu que tout entier divise 0) et 1 n'est pas premier car 1 possède un seul diviseur positif : lui-même. Ainsi, le plus petit nombre premier est 2. C'est par ailleurs le seul nombre premier pair. En effet, si  $n$  est un entier pair strictement supérieur à 2 alors  $n$  possède au moins 3 diviseurs : 1, 2 et  $n$ .

#### Théorème 18. — (Admis)

Tout entier naturel  $n \geq 2$  est soit un nombre premier soit un produit de nombres premiers. De plus, si  $n$  n'est pas premier, il existe une seule façon d'écrire  $n$  comme un produit de nombres premiers. Cette écriture est appelée la décomposition de  $n$  en produit de facteurs premiers.

**Exemple 19.**

1. La décomposition de 6 en produit de facteurs premiers est  $6 = 2 \times 3$ .
2. La décomposition de 100 en produit de facteurs premiers est  $100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$ .
3. La décomposition de 77 en produit de facteurs premiers est  $77 = 7 \times 11$ .

#### Méthode 20

Pour déterminer la décomposition en produit de facteurs premiers d'un entier  $n \geq 2$ , on teste tous les diviseurs premiers successivement et autant de fois que possible.

**Exemple 21.** Décomposons 4312 en produit de facteurs premiers. Pour cela, Une présentation pratique est la suivante :

|      |    |
|------|----|
| 4312 | 2  |
| 2156 | 2  |
| 1078 | 2  |
| 539  | 7  |
| 77   | 7  |
| 11   | 11 |
| 1    |    |

À droite, on met les diviseurs premiers successifs et à gauche les quotients obtenus. La colonne de droite contient la décomposition produit de facteurs premiers :  $4312 = 2^3 \times 7^2 \times 11$ .

## IV. — Forme irréductible d'un nombre rationnel

*Rappels.* Un nombre rationnel est un nombre  $r$  qui peut s'écrire sous la forme  $r = \frac{a}{b}$  où  $a$  est un entier relatif et  $b$  est un entier naturel non nul.

Dans la pratique, si  $r$  est négatif, on écrira souvent  $r = -\frac{a}{b}$  avec  $a$  et  $b$  entiers naturels. Ainsi, on écrira  $-\frac{17}{25}$  au lieu de  $\frac{-17}{25}$  (qui correspond à l'application stricte de la définition).

### Définition 22

Soit  $a$ ,  $b$  et  $d$  des entiers. On dit que  $d$  est un diviseur commun de  $a$  et  $b$  si  $d$  divise  $a$  et  $d$  divise  $b$ .

**Exemple 23.** Le nombre 5 est un diviseur commun de 10 et 35 car  $10 = 2 \times 5$  et  $35 = 7 \times 5$  donc 5 divise 10 et 35.

### Définition 24

Soit  $a$  un entier relatif et  $b$  un entier naturel non nul. On dit que la fraction  $\frac{a}{b}$  est irréductible si  $a$  et  $b$  n'ont pas d'autre diviseur commun positif que 1.

**Exemple 25.** La fraction  $\frac{5}{7}$  est irréductible mais la fraction  $\frac{14}{77}$  n'est pas irréductible car 14 et 77 sont tous les deux divisibles par 7.

### Théorème 26. — (Admis)

Tout rationnel peut s'écrire de manière unique sous la forme d'une fraction irréductible.

**Exemple 27.** Le rationnel  $\frac{14}{77}$  n'est pas écrit sous forme irréductible mais on peut l'écrire  $\frac{2}{11}$  qui est une forme irréductible.

### Méthode 28

Pour obtenir la forme irréductible d'un rationnel (positif), on peut utiliser les décompositions en produits de facteurs premiers du numérateur et du dénominateur.

**Exemple 29.** Considérons le rationnel  $r = \frac{140}{4312}$ . Pour obtenir l'écriture sous forme de fraction irréductible de  $r$ , on peut décomposer 140 et 4312 en produits de facteurs premiers. On a vu, dans l'exemple 21, que  $4312 = 2^3 \times 7^2 \times 11$ . De plus,  $140 = 2^2 \times 5 \times 7$  donc

$$r = \frac{140}{4312} = \frac{2^2 \times 5 \times 7}{2^3 \times 7^2 \times 11} = \frac{5}{2 \times 7 \times 11} = \frac{5}{154}.$$

### Propriété 30

Le nombre  $\sqrt{2}$  est irrationnel.

*Démonstration.* On donne ici une nouvelle démonstration de cette propriété.

Supposons que  $\sqrt{2}$  soit rationnel. Alors, on peut écrire  $\sqrt{2} = \frac{a}{b}$  sous la forme d'une fraction irréductible. En élevant au carré, on en déduit que  $2 = \frac{a^2}{b^2}$  donc  $a^2 = 2b^2$ . Ainsi,  $a^2$  est pair et donc, par la propriété 14,  $a$  est pair. Il existe donc un entier  $k$  tel que  $a = 2k$ . Dès lors,  $a^2 = (2k)^2 = 4k^2$  donc, puisque  $a^2 = 2b^2$ ,  $4k^2 = 2b^2$ . En simplifiant par 2, on en déduit que  $2k^2 = b^2$  donc  $b^2$  est pair. Toujours d'après la propriété 14, on en déduit que  $b$  est pair. Ainsi,  $a$  et  $b$  sont tous les deux pairs donc 2 est un diviseur commun de  $a$  et  $b$ . C'est absurde car on a supposé que la fraction  $\frac{a}{b}$  est irréductible.

On conclut donc que  $\sqrt{2}$  est irrationnel. □