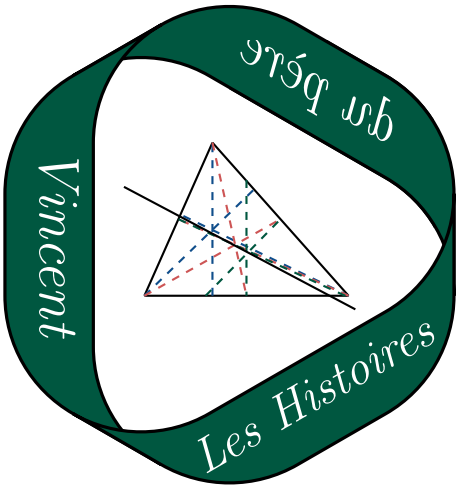
**Lycée Lucie Aubrac - Terminale**




# Chapitre 4
# Arithmétique
# Divisibilité dans $\mathbb{Z}$

## Table des matières

**Histoire – Arithmétique**

L'arithmétique est la science des nombres. Étymologiquement, *arithémtique* vient en effet du grec *arithmos* qui signifie nombre. On distingue en général l'arithmétique, basée sur des méthodes relativement élémentaires comme les congruences, et la théorie des nombres faisant intervenir des méthodes plus avancées. Au sein de la théorie des nombres, on distingue également la théorie analytique des nombres (basée sur l'analyse réelle et complexe) et la théorie algébrique des nombres (basée sur l'étude des ensembles de nombres et des structures abstraites). Pour ce qui est de ce dernier domaine, **Emmy Nœther** (1882-1935) a travaillé sur les corps de nombre et les invariants algébriques au début du XX$^{e}$ siècle. Elle était considérée par Einstein lui même comme « le génie mathématique créatif le plus considérable produit depuis que les femmes ont eu accès aux études supérieures ». Cela est d'autant plus remarquable qu'en tant que femme juive, elle a dû doublement faire face aux préjugés et aux discriminations de la société allemande de l'époque. En 1933, après l'arrivée d'Hitler au pouvoir, elle se vera d'ailleurs retirer son statut de Professeur et sera exclue de l'Université de Göttingen.

Emmy Nœther

# 1 Relation de divisibilité dans $\mathbb{Z}$

## 1.1 Définition et premières propriétés

**Définition 1**

Soient $a$, $b \in \mathbb{Z}$. On dit que $a$ **divise** $b$ lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On dit aussi que $a$ est un **diviseur** de $b$ et que $b$ est un **multiple** de $a$. On note $a|b$.

**Exemple.**
$3|15$ car $15 = 3 \times 5$.

**Proposition 1**

Soit $b$ un entier non nul.
- Si $a|b$ alors $|a| \leqslant |b|$.
- L'entier $b$ admet donc un nombre fini de diviseurs.

**Proposition 2**

Soient $a$, $b \in \mathbb{Z}$. Alors,

$$a|b \iff -a|b \iff a|-b \iff -a|-b.$$

*Démonstration.*
Montrons que si $a|b$ alors $-a|b$.

Supposons que $a|b$. Par définition, il existe $k \in \mathbb{Z}$ tel que $b = ak$.
Ainsi, $b = (-a) \times (-k)$ et on en déduit donc que $-a|b$.
La réciproque et les autres équivalences se montrent d'une manière similaire. □

## 1.2 Propriétés de la divisibilité

**Proposition 3 – Transitivité**

Soient $a$, $b$, $c \in \mathbb{Z}$.
Si $a|b$ et $b|c$, alors $a|c$.

*Démonstration.*
Supposons que $a|b$ et $b|c$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $b = ak$. De même, il existe $k' \in \mathbb{Z}$ tel que $c = bk'$.
Finalement, on en déduit que $c = akk'$ et donc que $a|c$. □

**Exemple.**
3|9 et 9|45 donc 3|45.

**Proposition 4**

Soient $a$, $b$, $c \in \mathbb{Z}$ tels que $a|b$ et $a|c$.
- Pour tous $m$, $n \in Z$, $a|(mb + nc)$.
- En particulier, $a|(b + c)$ et $a|(b - c)$.

*Démonstration.*
$a|b$ et $a|c$ donc il existe $k \in \mathbb{Z}$ tel que $b = ak$ et il existe $k' \in \mathbb{Z}$ tel que $c = ak'$. Ainsi,

$$mb + nc = mak + nak' = a(mk + nk')$$

et on en déduit donc que $a|(mb + nc)$. □

**Exemple.**
3|60 et 3|27 donc 3|87

**Remarque.**
Attention ! La proprosition « Si $a|c$ et si $b|c$ alors $a + b|c$ » est fausse.
Par exemple 2|6 et 3|6 mais 5 ne divise pas 6.

**Méthode – Déterminer l'ensemble des entiers vérifiant une relation de divisibilité de la forme $(an + b)|(cn + d)$**

1. On cherche une combinaison linéaire de $(an + b)$ et $(cn + d)$ de manière à éliminer l'inconnu $n$.
2. On en déduit que $an + b$ est un diviseur de la combinaison linéaire.
3. On en déduit finalement les valeurs possibles de $an + b$ puis de $n$.
4. On vérifie réciproquement que les entiers trouvés conviennent.

**Exemple.**
Déterminer les entiers relatifs $n$ tels que $(2n+7)|(3n+5)$.

Solution :
Soit $n \in \mathbb{Z}$ tel que $(2n+7)|(3n+5)$.
On a $3 \times (2n+7) - 2 \times (3n+5) = 11$.
Ainsi, comme $2n+7|2n+7$ et $2n+7|3n+5$, on en déduit que $2n+7|11$.
Par conséquent : $2n+7 = 11$ ou $2n+7 = 1$ ou $2n+7 = -11$ ou $2n+7 = -1$.
Finalement, on obtient donc $n = 2$ ou $n = -3$ ou $n = -9$ ou $n = 5$.
Réciproquement, on vérifie que 2, $-3$, $-9$ et 5 sont bien des solutions.
En conclusion,

$$\mathcal{S} = \{2\,;-3\,;-9\,;5\}.$$

## 1.3 Division euclidienne

**Proposition 5 – Division euclidienne dans $\mathbb{N}$**

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$.
Il existe un unique couple $(q,r) \in \mathbb{N} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < b$. L'entier $q$ est appelé le quotient de la division de $a$ par $b$ et $r$ le reste.

**Remarque.**
Pour démontrer cette proposition, on utilisera le fait que tout ensemble $A$ inclus dans $\mathbb{N}$ et non vide admet un minimum (c'est-à-dire qu'il existe $m \in A$ tel que pour tout $n \in A$, $m \leqslant n$).

*Démonstration.*
Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$.

- Montrons tout d'abord l'existence des entiers $q$ et $r$.
  On définit l'ensemble $A = \{a - bn,\ n \in \mathbb{N}\} \bigcap \mathbb{N}$. Alors $A$ est inclus dans $\mathbb{N}$ et est non vide (pour $n = 0$, on voit que $a \in A$).
  Ainsi, on en déduit que $A$ admet un élément minimum que l'on note $r$.
  Comme $r \in A$, par définition de $A$, il existe $q \in \mathbb{N}$ tel que $a - bq = r$.
  Finalement, on a prouvé qu'il existe des entiers $a$ et $r$ tels que $a = bq + r$. De plus, suppsoons par l'absurde que $r \geqslant b$. En posant $q' = q + 1$, on aurait $a = bq' + r - b$ et par conséquent, $r - b \in A$. Cela est absurde car $r$ est l'élément minimum de $A$.
- Montrons l'unicité du couple $(q,r)$.
  On suppose qu'il existe deux couples $(q_1,r_1)$ et $(q_2,r_2)$ vérifiant les conditions de la propriété.
  Ainsi, $a = bq_1 + r_1 = bq_2 + r_2$.
  On en déduit que $b(q_1 - q_2) = r_2 - r_1$ et donc que $b|r_2 - r_1$. Par ailleurs, on sait que $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$. Par conséquent, $-b < r_2 - r_1 < b$. Comme on a montré par ailleurs que $b|r_2 - r_1$, on en déduit que $r_2 - r_1 = 0$, c'est-à-dire que $r_2 = r_1$. Par suite, on obtient aussi que $q_2 = q_1$ ce qui prouve l'unicté.

□

**Proposition 6 – Division euclidienne dans $\mathbb{Z}$ (admise)**

Soient $a, \in \mathbb{Z}$ et $b, \in \mathbb{Z} \setminus \{0\}$.
Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < |b|$.

**Exemples.**

- La division euclidienne de 35 par 6 est $35 = 6 \times 4 + 3$.
- La division euclidienne de $-15$ par 4 est $-15 = 4 \times (-4) + 1$.

**Histoire – Division euclidienne**

On parle de « division euclidienne » en référence au mathématicien grec **Euclide (300 av. J.C.)**. La division était néanmoins connue bien avant lui et utilisée par exemple par les égyptiens. Le nom « euclidien » s'explique plutôt par le fait qu'Euclide a utilisé un algorithme basé sur la division euclidienne (voir chapitre suivant). Il le présente dans un ouvrage célèbre intitulé *Les Éléments*. Avec plus de mille éditions différentes depuis l'antiquité, il s'agit, juste après la Bible, de l'ouvrage le plus imprimé dans l'histoire de l'humanité.

Euclide

# 2 Congruences

## 2.1 Définition

**Définition 2**

Soit $m \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.
On dit que $a$ et $b$ sont **congrus modulo m** s'ils ont le même reste dans la division euclidienne par $m$.
On note $a \equiv b\,[m]$ ou $a \equiv b \mod m$.

**Exemple.**
Le reste de la division de 16 par 5 est 1. De même, le reste de la division de 31 par 5 est 1. Ainsi, $16 \equiv 31[5]$.

**Proposition 7**

Soit $m \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.

$$a \equiv b\,[m] \iff m|(b-a)$$

*Démonstration.*
Soit $m \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.

- Supposons que $a \equiv b\,[m]$. Cela signifie que $a$ et $b$ ont le même reste dans la division euclidienne par $m$. Autrement dit, il existe $p, q, r \in \mathbb{Z}$ tels que $a = mp + r$ et $b = mq + r$ avec $0 \leqslant r < |m|$.
  Ainsi, $b - a = (mq + r) - (mp + r) = m \times (q - p)$.
  Cela montre bien que $m$ divise $b - a$.

- Réciproquement, supposons que $m|(b - a)$.
  On effectue alors les divisions euclidiennes de $a$ et $b$ par $m$.
  D'une part, il existe $q, r \in \mathbb{Z}$ tels que $a = mq + r$ avec $0 \leqslant r < |m|$.
  D'autre part, il existe $q', r' \in Z$ tels que $b = mq' + r'$ avec $0 \leqslant r' < |m|$.
  L'objectif est de démontrer alors que $r = r'$.
  En fait, $b - a = (mq' + r') - (mq + r) = m(q' - q) + (r' - r)$.
  Or, les inégalités vérifiées par $r$ et $r'$ impliquent nécessairement que $(r' - r) \leqslant |m|$.
  Ainsi, si $r' - r \geqslant 0$, l'égalité 1 correspond à la division euclidienne de $b - a$ par $m$.
  Mais comme on sait que $m|(b - a)$, on en déduit que le reste $r' - r$ est nul, c'est-à-dire, $r' = r$.
  Autrement dit, $a$ et $b$ ont même reste dans la division par $m$ et sont donc congrus modulo $m$.
  Dans le cas où $r' - r < 0$, il suffit de raisonner de même avec $a - b$ au lieu de $b - a$.

□

**Histoire – Congruences**

**Carl Friedrich Gauß** (1777-1855) est originaire d'une famille pauvre de la principauté de Brunswick. Dès l'école primaire, l'instituteur et son assistant décèlent ses talents et lui transmettent leur passion pour les mathématiques. Gauß publie ses premiers résultats à 19 ans et à 24 ans, il introduit la notion de congruences dans un ouvrage célèbre intitulé *Disquisitiones Arithmeticae*. Dès 28 ans, il dirigea l'observatoire astronomique de Göttingen. Alors qu'il n'aimait pas vraiment enseigner, cela lui permettait justement de se consacrer à ses recherches mathématiques.

Carl Friedrich Gauß

## 2.2 Congruences et opérations

**Proposition 8 – Transitivité**

Soit $m \in \mathbb{N}^*$ et $a, b, c \in \mathbb{Z}$.

$$\text{Si } a \equiv b\,[m] \text{ et } b \equiv c\,[m] \text{ alors } a \equiv c\,[m]$$

*Démonstration.*
Évident en revenant à la définition d'une congruence. □

**Proposition 9**

Soit $m \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$.

- **Compatibilité avec l'addition :**
  Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a + c \equiv b + d\,[m]$
- **Compatibilité avec la multiplication :**
  Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a \times c \equiv b \times d\,[m]$
- **Compatibilité avec les puissances :**
  Si $a \equiv b\,[m]$, alors pour tout $p \in \mathbb{N}^*$, $a^p \equiv b^p\,[m]$

*Démonstration.*
Soient $a \equiv b\,[m]$ et $c \equiv d\ [m]$.
Cela signifie qu'il existe $k \in \mathbb{Z}$ tel que $a - b = mk$ et il existe $k' \in \mathbb{Z}$ tel que $c - d = mk'$.
Autrement dit, $a = b + mk$ et $c = d + mk'$.
En sommant les deux égalités, on obtient : $a + c = b + d + m(k + k')$, ce qui signifie exactement que $a + c \equiv b + d\,[m]$.
De la même manière, en multipliant les deux égalités, $a \times c = (b + mk) \times (d + mk') = b \times d + m(dk + bk')$.
On en déduit que $a \equiv b\,[m]$ et $c \equiv d\,[m]$, alors $a \times c \equiv b \times d\,[m]$.
Finalement, la dernière propriété s'obtient par récurrence comme conséquence de la seconde. □

**Méthode – Montrer une relation de divisibilité**

1. On travaille modulo le diviseur (3 dans l'exemple ci-dessous).
2. On distingue les cas grâce à un tableau en montrant utilisant le fait qu'être divisible par $n$ est équivalent au fait d'être égal à 0 modulo $n$.

**Exemple.**
Montrer que pour tout entier $n \in \mathbb{Z}$, $2n(n + 1)(n + 5)$ est divisible par 3.

Solution :
On distingue les cas modulo 3 :

| $n$ | 0 | 1 | 2 |
|---|---|---|---|
| $2n$ | 0 | 2 | 1 |
| $n + 1$ | 1 | 2 | 0 |
| $n + 5$ | 2 | 0 | 1 |
| $2n(n + 1)(n + 5)$ | 0 | 0 | 0 |

Ainsi, dans tous les cas, $2n(n+1)(n+5) \equiv 0\,[3]$ ce qui signifie exactement que $2n(n+1)(n+5)$ est divisible par 3.

## 2.3 Inverse modulo $m$

**Définition 3**

Soient $m \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$.
On dit que $a$ est **inversible** modulo $m$ lorsqu'il existe un entier $b$ tel que $a \times b \equiv 1\,[m]$.
De plus, l'entier $b$ est appelé **inverse de $a$ modulo $m$** .

**Exemple.**
8 est inversible modulo 3 car $8 \times 2 \equiv 1[3]$. Son inverse est 2 modulo 3.

**Proposition 10 – Unicité de l'inverse**

Soient $m \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$.
Si $a$ est inversible modulo $m$ alors l'inverse est unique modulo $m$.

*Démonstration.*
Supposons qu'il existe deux inverse de $a$, notés $b_1$ et $b_2$. On va montrer que $b_1 \equiv b_2\,[m]$.
En fait, $a \times b_1 \equiv 1\,[m]$ (car $b_1$ est un inverse).
Ainsi, en multipliant par $b_2$, il vient :
$b_2 \times a \times b_1 \equiv b_2 \times 1\,[m]$
donc $1 \times b_1 \equiv b_2\,[m]$
donc $b_1 \equiv b_2\,[m]$
Cela prouve donc l'unicité, modulo $m$ de l'inverse. □

**Méthode – Déterminer si un entier est inversible ou non**

On établit un tableau de congruences afin de distinguer tous les cas.

**Exemple.**

1. Montrer que 7 est inversible modulo 9.
2. Montrer que 4 n'est pas inversible modulo 6.

Solution :

1.

| $n \equiv \ldots\,[9]$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $7n \equiv \ldots\,[9]$ | 0 | 7 | 5 | 3 | 1 | … | … | … | … |

Ainsi, $7 \times 4 \equiv 1\,[9]$ donc 7 est inversible modulo 9.

2.

| $n \equiv \ldots\,[6]$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $4n \equiv \ldots\,[6]$ | 0 | 4 | 2 | 0 | 4 | 2 |

Ainsi, pour tout entier $n$, $4n \not\equiv 1\,[6]$, ce qui signifie que 4 n'est pas inversible modulo 6.

## 2.4 Application à l'étude des règles de divisibilité

Dans cette partie, on se servira du fait que tout nombre entier $N$ peut s'écrire sous la forme $N = \sum_{k=0}^{n} a_k 10^k$, où pour tout $k \in \{1, \ldots, n\}$, $0 \leqslant a_k \leqslant 9$ et $a_n \neq 0$.

**Proposition 11**

Un nombre entier $N$ est divisible par 10 si, et seulement si, son chiffre des unités est 0.

*Démonstration.*
En écrivant $N = \sum_{k=0}^{n} a_k 10^k$, cela revient à prouver que $N$ est divisible par 10 si, et seulement si, $a_0 = 0$.
En fait, comme pour tout $k \geqslant 1$, $10^k \equiv 0[10]$, on a : $N \equiv a_0[10]$, d'où le résultat. □

**Proposition 12**

Un nombre entier $N = \sum_{k=0}^{n} a_k 10^k$ est divisible par 3 si, et seulement si, $a_0 + a_1 + \ldots + a_n$ est divisible par 3.

*Démonstration.*
Comme $10 \equiv 1[3]$, on en déduit que $10^k \equiv 1[3]$ (d'après la compatibilité des congruences avec les puissances).
Finalement, par compatibilité des congruences avec la multiplication, on en déduit que :

$$N \equiv \sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k \times 1 \equiv \sum_{k=0}^{n} a_k [3].$$

□

**Savoir-faire du chapitre**

- Déterminer l'ensemble des diviseurs d'un entier.
- Déterminer l'inverse (lorsqu'il existe) d'un nombre entier modulo $n$.
- Déterminer l'ensemble des entiers vérifiant une relation de divisibilité de la forme $(an + b)|(cn + d)$
- Utiliser les congruences pour établir une relation de divisibilité.
- Utiliser un raisonnement par disjonction de cas (pour établir une divisibilité par exemple).

**QCM d'entrainement**