Chapitre 6

Arithmétique

1. Divisibilité

1.1. Entiers naturels

On note $\mathbb{N}$ l'ensemble des *entiers naturels*.
Le raisonnement par récurrence s'applique aux propositions dont l'énoncé dépend d'un entier naturel n. Il est une conséquence de la construction de l'ensemble des entiers naturels $\mathbb{N}$ (basée sur les axiomes de Peano). Ce raisonnement a été vu dans le chapitre sur les démonstrations.

Voici deux autres propriétés des entiers naturels qui nous seront utiles :

- *Un ensemble non vide d'entiers naturels a un plus petit élément.*
  Soit B un sous-ensemble de $\mathbb{N}$, et supposons qu'il n'a pas de plus petit élément. Soit A l'ensemble des entiers naturels n tels qu'aucun entier naturel inférieur ou égal à n n'appartienne à B. Alors
  1) 0 appartient à A, sinon 0 serait le plus petit élément de B,
  2) si n appartient à A, alors $n+1$ appartient à A, sinon $n+1$ serait le plus petit élément de B.

  Donc A est égal à $\mathbb{N}$, et B est vide. Le raisonnement qu'on vient de faire est un raisonnement par récurrence.
- *Une suite strictement décroissante d'entiers naturels est toujours finie (il n'y a pas de suite infinie strictement décroissante).*
  Supposons qu'il y ait une suite (a_n) strictement décroissante d'entiers naturels. Alors, d'après la propriété précédente, l'ensemble des a_n, qui est non vide, a un plus petit élément, disons a_N. On devrait avoir $a_{N+1} < a_N$, ce qui contredit le fait que a_N est le plus petit élément.

1.2. Entiers relatifs

On note $\mathbb{Z}$ l'ensemble des *entiers relatifs*. On rappelle quelques propriétés algébriques de $\mathbb{Z}$, pour l'addition et la multiplication.
Addition

1) (*associativité*) Quels que soient les entiers relatifs m, n, p,
$$(m+n)+p = m+(n+p).$$
2) (*commutativité*) Quels que soient les entiers relatifs m, n,
$$m+n = n+m.$$
3) (0 est *élément neutre*) Quel que soit l'entier relatif m,
$$0+m = m+0 = m.$$
4) (*existence d'un opposé*) Quel que soit l'entier relatif m, il existe un entier relatif n tel que
$$m+n = n+m = 0.$$

Multiplication

5) (*associativité*) Quels que soient les entiers relatifs m, n, p,

$$(m\,n)\,p = m\,(n\,p).$$

6) (*commutativité*) Quels que soient les entiers relatifs m, n,

$$m\,n = n\,m.$$

7) (1 est *élément neutre*) Quel que soit l'entier relatif m,

$$1\,m = m\,1 = m.$$

8) (*distributivité* par rapport à l'addition) Quels que soient les entiers relatifs m, n, p,

$$m\,(n+p) = m\,n + m\,p \qquad (n+p)\,m = n\,m + p\,m.$$

Les quatre propriétés pour l'addition font de $\mathbb{Z}$ un *groupe commutatif*. Quelle propriété manque-t-il à $\mathbb{N}$, muni de l'addition, pour être un groupe commutatif ?
Les propriétés de groupe commutatif pour l'addition, plus les quatre propriétés pour la multiplication, font de $\mathbb{Z}$ un *anneau commutatif*.
En plus de ces propriétés d'anneau commutatif, on peut "faire des simplifications" dans $\mathbb{Z}$. Si $a \neq 0$ et $ab = 0$, alors $b = 0$. Aussi, si $a \neq 0$ et $ab = ac$, alors $b = c$; ceci est une conséquence de la propriété précédente, car $ab = ac$ peut se réécrire $a(b - c) = 0$, d'où il vient $b - c = 0$.
Tous les anneaux commutatifs n'ont pas cette propriété de simplification : nous verrons des exemples plus loin, à propos des congruences.

1.3. La division euclidienne, relation de divisibilité

La *division euclidienne* est la "division avec reste" des entiers naturels. On rappelle ce qui la caractérise.

Proposition 6.1 – *Soient a et b deux entiers naturels avec $b \neq 0$. Alors il existe deux entiers naturels q (quotient) et r (reste) tels que*

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

De plus il n'y a qu'un couple d'entiers (q, r) qui vérifie cette propriété.

Exemple - La division euclidienne de 223 par 12 est $223 = 12 \times 18 + 7$.
7 est le reste et 18 le quotient.

Remarque - La condition $0 \leq r < b$ est équivalente à $0 \leq r \leq b - 1$ car r et b sont des entiers naturels.
Démonstration : soit b un entier strictement positif, et soit A l'ensemble des entiers naturels n tels qu'il existe un entier naturel s vérifiant $n < bs$. Alors

- 0 appartient à A car $0 < b$,
- si n appartient à A, il existe s dans $\mathbb{N}$ tel que $n < bs$ et alors $n+1 < bs+b = b(s+1)$, donc $n + 1$ appartient à A.

On en déduit que $A = \mathbb{N}$. Si a est un entier naturel quelconque, il existe s dans $\mathbb{N}$ tel que $a < bs$. Soit t le plus petit de ces entiers. Forcément on a $t > 0$ car $b0 = 0 \leq a$. Posons $q = t - 1$ et $r = a - bq$; comme $bq \leq a < b(q + 1)$, on a bien $0 \leq r < b$ et $a = bq + r$.
S'il y a un autre couple (q_1, r_1) tel que $a = bq_1 + r_1$ et $0 \leq r_1 < b$, alors $0 = b(q - q_1) + (r - r_1)$, d'où $b\,|q - q_1| = |r - r_1| < b$, ce qui n'est possible que si $q_1 = q$, et alors $r_1 = r$. Le couple (q, r) est défini de manière unique. □

Nous aurons aussi besoin de la division euclidienne de a par b quand a est un entier relatif. Le quotient q est alors un entier relatif, et on demande toujours que le reste r vérifie $0 \leq r < b$. Il faut examiner le cas où $a < 0$. On a par la division euclidienne des entiers naturels

$$-a = bq_1 + r_1 \quad \text{avec} \quad 0 \leq r_1 < b.$$

Si $r_1 = 0$, alors $a = b(-q_1)$ convient. Sinon, on a

$$a = b(-q_1) - r_1 = b(-1 - q_1) + (b - r_1)$$

et on prend $q = -1 - q_1$, et $r = b - r_1$ qui vérifie $0 < r < b$. Le couple (q, r) est également défini de manière unique.

Soient a et b deux entiers naturels. Par définition, on dit que a *divise* b quand il existe un entier naturel q tel que $b = aq$ (la division "tombe juste", son reste est nul). On dit aussi que a est un *diviseur* de b, ou que b est un *multiple* de a. On notera $a \mid b$ pour "a divise b".

Remarque - Ne pas confondre $a \mid b$ qui signifie "a divise b" et a/b qui est la fraction de a par b.
Voici quelques propriétés de la relation de divisibilité sur l'ensemble des entiers naturels.

1) (*réflexivité*) Quel que soit l'entier naturel a,

$$a \mid a.$$

2) (*antisymétrie*) Quels que soient les entiers **naturels** a, b,

$$(a \mid b \text{ et } b \mid a) \quad \Longrightarrow \quad a = b.$$

3) (*transitivité*) Quels que soient les entiers naturels a, b, c,

$$(a \mid b \text{ et } b \mid c) \quad \Longrightarrow \quad a \mid c.$$

L'ordre usuel $\leq$ sur les entiers naturels est bien sûr une relation d'ordre sur $\mathbb{N}$. La divisibilité est aussi une relation d'ordre sur $\mathbb{N}$. L'ordre usuel est un *ordre total*, ce qui signifie que quels que soient les entiers naturels a et b, on a $a \leq b$ ou $b \leq a$. Cette propriété n'est pas vraie pour la divisibilité : 2 ne divise pas 3, et 3 ne divise pas 2. La relation de divisibilité n'est pas un ordre total.
On remarque que si $a \mid b$ et $b \neq 0$, alors $a \leq b$. Ceci montre qu'un entier naturel non nul a un nombre fini de diviseurs.
On étend la relation de divisibilité aux entiers relatifs : l'entier relatif a divise l'entier relatif b quand il existe un entier relatif q tel que $b = qa$ (on dit aussi que a est un diviseur de b, ou que b est un multiple de a). La relation de divisibilité n'est plus une relation d'ordre sur les entiers relatifs ; quelle est la propriété qui est prise en défaut dans ce cas ? Les questions de divisibilité sur les entiers relatifs se ramènent à celles sur les entiers naturels : l'entier relatif a divise l'entier relatif b si et seulement si l'entier naturel $|a|$ divise l'entier naturel $|b|$.
On remarque que 1 (et -1) divisent tous les entiers, et que tous les entiers divisent 0. Si a divise b et c, alors il divise $b + c$. Si a divise b, alors ac divise bc (et réciproquement pour $c \neq 0$).

2. Congruences

2.1. Relation de congruence. Classes de congruence

Définition 6.2 – *Soit n un entier supérieur ou égal à 2. On dit que deux entiers relatifs a et b sont congrus modulo n quand n divise $a-b$. On note* $a \equiv b \pmod{n}$.

Exemple - $12 \equiv 2 \pmod{5}$.

La relation de congruence modulo n vérifie les propriétés suivantes :

1) *réflexivité* Quel que soit l'entier relatif a,

$$a \equiv a \pmod{n}.$$

2) *symétrie* Quels que soient les entiers relatifs a et b,

$$a \equiv b \pmod{n} \iff b \equiv a \pmod{n}.$$

3) *transitivité* Quels que soient les entiers relatifs a, b et c,

$$(a \equiv b \pmod{n} \text{ et } b \equiv c \pmod{n}) \implies a \equiv c \pmod{n}.$$

La vérification de la réflexivité et de la symétrie est immédiate. Pour la transitivité, si n divise $(a-b)$ et n divise $(b-c)$, alors n divise $(a-b)+(b-c) = a-c$.

C'est une *relation d'équivalence sur A*.

Soit a un entier relatif, et r le reste de la division euclidienne de a par n. Alors $a \equiv r \pmod{n}$. Deux entiers relatifs sont congrus modulo n si et seulement si ils ont même reste dans la division euclidienne par n (vérifier !). La *classe de conguence modulo n* d'un entier relatif a est l'ensemble de tous les entiers relatifs qui sont congrus à a modulo n. Autrement dit, c'est l'ensemble des entiers relatifs de la forme $a+nq$ où q est un entier relatif quelconque. Cette description montre que la notation naturelle pour la classe de congruence de a modulo n serait $a + n\mathbb{Z}$. Cependant on utilisera la notation $\overline{a}$ qui est moins précise (car elle ne fait pas référence à n), mais qui a l'avantage d'être courte. Dire que la classe de congruence de a modulo n est égale à la classe de congruence de b modulo n revient à dire que a est congru à b modulo n. Voici par exemple la liste des classes de congruence modulo 5 : sur chaque ligne figure une classe de congruence.

$$\begin{array}{lcl}
\overline{0} & = & \{\ldots\ \text{-15}\ \text{-10}\ \text{-5}\ 0\ \ 5\ \ 10\ \ 15\ \ \ldots\} \\
\overline{1} & = & \{\ldots\ \text{-14}\ \ \text{-9}\ \ \text{-4}\ \ 1\ \ 6\ \ 11\ \ 16\ \ \ldots\} \\
\overline{2} & = & \{\ldots\ \text{-13}\ \ \text{-8}\ \ \text{-3}\ \ 2\ \ 7\ \ 12\ \ 17\ \ \ldots\} \\
\overline{3} & = & \{\ldots\ \text{-12}\ \ \text{-7}\ \ \text{-2}\ \ 3\ \ 8\ \ 13\ \ 18\ \ \ldots\} \\
\overline{4} & = & \{\ldots\ \text{-11}\ \ \text{-6}\ \ \text{-1}\ \ 4\ \ 9\ \ 14\ \ 19\ \ \ldots\}
\end{array}$$

Sur la troisième ligne, on a $\overline{2}$, qui est la même chose que $\overline{17}$, ou que $\overline{-13}$. Cet exemple est une illustration de la proposition suivante.

Proposition 6.3 – *Il y a n classes de congruence modulo n, qui sont* $\overline{0}$, $\overline{1}$,...,$\overline{n-1}$.

Démonstration : tout d'abord, ces classes de congruence sont bien distinctes. Si k et l sont deux entiers différents avec $0 \leq k < n$ et $0 \leq l < n$, alors n ne divise pas $k-l$ et donc les classes de congruence $\overline{k}$ et $\overline{l}$ sont différentes. Ensuite, on obtient bien ainsi toutes les classes de congruence. Si a est un entier relatif quelconque, sa classe de congruence modulo n est égale à celle de son reste dans la division euclidienne par n. Donc $\overline{a}$ est égale à l'une des classes $\overline{0}$, $\overline{1}$,...,$\overline{n-1}$. □

En fait, dans cette démonstration, on a répété ce qu'on a dit plus haut : a et b sont congrus modulo n si et seulement s'ils ont même reste dans la division par n. L'ensemble des n classes de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$.

2.2. Opérations sur les congruences

Théorème 6.4 – *Soient a, b, c et d quatre entiers relatifs qui vérifient $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors*

$$-a \equiv -b \pmod{n},$$
$$a + c \equiv b + d \pmod{n},$$
$$ac \equiv bd \pmod{n}.$$

Démonstration : par hypothèse, n divise $a - b$ et $c - d$. L'item 1 est très facile à démontrer. Vérifions l'item 2. On a $(a + c) - (b + d) = (a - b) + (c - d)$, donc n divise $(a + c) - (b + d)$. Vérifions l'item 3. On a $ac - bd = c(a - b) + b(c - d)$, donc n divise $ac - bd$. □

Les règles qui figurent dans le théorème permettent de faire rapidement des "calculs modulo n". Par exemple, calculons $1! + 2! + 3! + 4! + 5! + 6!$ modulo 7. On a (toutes les congruences sont modulo 7) :

$$4! \equiv 3 \quad 5! \equiv 3 \times 5 \equiv 1 \quad 6! \equiv 5! \times 6 \equiv 6,$$

d'où

$$1! + 2! + 3! + 4! + 5! + 6! \equiv 1 + 2 + 6 + 3 + 1 + 6 \equiv 5,$$

autrement dit le reste de la division euclidienne de $1! + 2! + 3! + 4! + 5! + 6!$ par 7 est 5.

Les résultats du théorème permettent de définir l'addition et la multiplication de classes de congruence modulo n. Le deuxième résultat nous dit par exemple que, pour $\overline{a} = \overline{b}$ et $\overline{c} = \overline{d}$, alors $\overline{a + b} = \overline{c + d}$. On peut donc poser

$$\overline{a} + \overline{c} = \overline{a + c}$$

sans risquer de problème : si on remplace a par b et c par d, on trouve bien le même résultat. Prenons l'exemple des classes de congruence modulo 5 que nous avons décrites ci-dessus. On pose $\overline{1} + \overline{2} = \overline{3}$. On pose aussi $\overline{-4} + \overline{12} = \overline{8}$. A gauche on a $\overline{1} = \overline{-4}$ et $\overline{2} = \overline{12}$, donc les deux résultats à droite doivent être égaux. C'est bien le cas, $\overline{3} = \overline{8}$. Dressons les tables d'addition et de multiplication dans $\mathbb{Z}/5\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Quelles sont les propriétés vérifiées par l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$? On a par exemple

$$\overline{a} \times \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \times \overline{a}$$

qui montre la commutativité de la multiplication des classes de congruence. Ainsi, on a des propriétés qui sont "héritées" de celles de l'addition et de la multiplication sur $\mathbb{Z}$. L'addition des classes de congruence modulo n est associative, commutative, a un élément neutre $\overline{0}$ et toute classe $\overline{a}$ a un opposé $\overline{-a}$. La multiplication est associative, commutative, a un élément neutre $\overline{1}$ et est distributive par rapport à l'addition. Au total, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.

⚠ Un élément de $\mathbb{Z}/n\mathbb{Z}$ n'admet pas toujours un inverse pour la multiplication. Ce fait oblige à changer ses habitudes de calcul, en particulier pour la simplification dans la multiplication des classes de congruence

$$\overline{a} \times \overline{b} = \overline{a} \times \overline{c} \text{ et } \overline{a} \neq \overline{0} \quad \text{n'entraînent pas toujours} \quad \overline{b} = \overline{c}.$$

Par exemple $\overline{9} \times \overline{1} = \overline{9} \times \overline{5}$ et $\overline{9} \neq \overline{0}$, mais $\overline{1} \neq \overline{5}$ dans $\mathbb{Z}/12\mathbb{Z}$.

⚠ De même, si $\overline{ac} = \overline{0}$, cela ne veut pas dire $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Par exemple, $\overline{2} \times \overline{3} = \overline{0}$ dans $\mathbb{Z}/6\mathbb{Z}$.

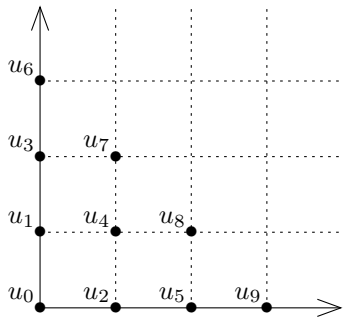
3. Ensembles finis ou dénombrables (pour votre culture générale)

Théorème et définitions 6.5 – *Un ensemble E non vide est fini s'il existe un entier $n \in \mathbb{N}^*$ et une bijection $f : \{1, 2, \ldots, n\} \longrightarrow E$. Le nombre n est alors unique et on l'appelle le cardinal ou le nombre d'éléments de E. On convient que $\emptyset$ est fini et de cardinal 0. Un ensemble qui n'est pas fini est dit infini.*

Définition 6.6 – *Un ensemble E est dénombrable s'il existe une surjection u de $\mathbb{N}$ sur E.*

Exemples - • L'ensemble $\mathbb{N}$ est infini et dénombrable.

• $\mathbb{N} \times \mathbb{N}$ est dénombrable : pour le voir, on numérote ses éléments comme sur le dessin ci-dessous :



• On peut montrer qu'un produit fini d'ensembles dénombrables est dénombrable, qu'un sous-ensemble d'un ensemble dénombrable est dénombrable et qu'une réunion finie d'ensembles dénombrables est dénombrable. On déduit de ce qui précède que $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.

• Mais $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable. Raisonnons par l'absurde. Si $\mathcal{P}(\mathbb{N})$ est dénombrable, il existe une surjecion de $\mathbb{N}$ sur $\mathcal{P}(\mathbb{N})$ Soit u une telle surjection. Alors $\forall n \in \mathbb{N}$, $u(n)$ est un sous-ensemble de $\mathbb{N}$. Soit $E = \{n \in \mathbb{N} \mid n \notin u(n)\}$. On a $E \subset \mathbb{N}$ donc $E \in \mathcal{P}(\mathbb{N})$; comme u est surjective, E a au moins un antécédent par u ; soit $n \in \mathbb{N}$ un antécédent de E ; on a donc $E = u(n)$. Pour un tel n, il y a deux possibilités : $n \in E$ ou $n \notin E$. Si $n \in E$, par définition $n \notin u(n)$, c'est-à-dire $n \notin E$ et on a une contradiction. De même, si $n \notin E$, on a $n \in u(n)$, c'est-à-dire $n \in E$ et on aboutit encore à une contradiction. L'hypothèse de départ est donc absurde et on en déduit le résultat.

• On en déduit que l'ensemble des suites d'entiers n'est pas dénombrable, non plus que $\mathbb{R}$

EXERCICES D'APPLICATION

Exercice n°1

Quel est le reste de la division par 7 de 247^{349}, de la division par 13 de 100^{1000} ?

Exercice n°2

Montrer que le produit de trois entiers consécutifs est divisible par 3.

Exercice n°3

Montrer que tout entier premier > 3 est de la forme $6k \pm 1$.

Exercice n°4

Résoudre dans $\mathbb{Z}$ le système suivant

$$\begin{cases} x \equiv 7 \bmod 10 \\ x \equiv 2 \bmod 15 \end{cases}$$

Exercice n°5

1) Calculer les carrés des éléments de $\mathbb{Z}/5\mathbb{Z}$.
2) Résoudre, dans $\mathbb{Z}/5\mathbb{Z}$, l'équation $\bar{x}^2 + \bar{2}\bar{y}^2 = \bar{0}$.

INDICATIONS ET SOLUTIONS SOMMAIRES

Exercice n°1

On obtient $247^{349} \equiv 2 \bmod 7$ en utilisant $247 \equiv 2 \bmod 7$ et $2^3 \equiv 1 \bmod 7$.
On obtient $100^{1000} \equiv 9 \bmod 13$ en utilisant $100 \equiv 9 \bmod 13$ et $9^6 \equiv 1 \bmod 13$.

Exercice n°2

Soit $n, n+1$ et $n+2$ trois entiers consécutifs. On a $n \equiv 0 \bmod 3$ ou $n \equiv 1 \bmod 3$ ou $n \equiv 2 \bmod 3$. Etudier chacun de ces cas.

Exercice n°3

Utiliser une congruence modulo 6.

Exercice n°4

On écrit : $x \equiv 7 \bmod 10 \iff (\exists k \in \mathbb{Z},\ x = 7 + 10k)$. On en déduit que

$$\begin{aligned} x \equiv 2 \bmod 15 &\iff 7 + 10k \equiv 2 \bmod 15 \iff 10k \equiv -5 \bmod 15 \\ &\iff 2k \equiv -1 \bmod 3 \iff 2k \equiv 2 \bmod 3 \\ &\iff k \equiv 1 \bmod 3 \text{ en multipliant par } \overline{2}. \end{aligned}$$

On en déduit qu'il existe $p \in \mathbb{Z}$ tel que $k = 1 + 3p$ et $x = 7 + 10(1 + 3p) = 17 + 30p$, donc $x \equiv 17 \bmod 30$.

Exercice n°5

1) $\overline{x}^2 \in \{\overline{0}, \overline{1}, \overline{4}\}$
2) Faire un tableau à deux entrées en utilisant la première question.