Chapitre 6
Arithmétique dans $\mathbb{N}$, Dénombrement

Table des matières

Vidal AGNIEL

Introduction

L'Arithmétique est la branche des mathématiques qui porte sur l'étude des propriétés des nombres entiers. Une notion fondamentale de ce domaine est celle de **diviseur**.
Une question classique d'arithmétique est par exemple de déterminer une condition nécessaire et suffisante sur un entier pour savoir s'il est divisible par 9.
Nous répondrons à cette question dans le chapitre.

Nous terminons cette partie par l'étude des nombres premiers qui sont les "briques" fondamentales avec lesquels tous les nombres entiers sont construits. En effet, tout nombre entier se décompose de manière unique comme produit de nombres premiers.

1 Rudiments d'arithmétique dans $\mathbb{N}$

1.1 Multiples et diviseurs

Définition 1 (**Multiple et diviseurs**)
Soient $a, b, d, m \in \mathbb{N}$ des entiers. Alors :

- *L'entier d est un **diviseur** de a s'il existe $k \in \mathbb{N}$ tel que $a = d \times k$.*
  On le note $d|a$ (d divise a).
- *L'entier m est un **multiple** de a, si a est un diviseur de m.*
- *Si d divise à la fois a et b, on dit que d est **un diviseur commun de** a **et** b.*
- *On note $Div(a)$ l'ensemble des diviseurs positifs de a.*
  On note $Div(a, b) = Div(a) \cap Div(b)$, l'ensemble des diviseurs communs à a et b.

Exemple 2 —

- *2 est un diviseur de 128.*
- *51 est un multiple de 17.*
- *0 est un multiple de 5.*
- *L'ensemble des diviseurs de 12 est $\{1, 2, 3, 4, 6, 12\}$.*

Proposition 3
Soient $a, b, d \in \mathbb{N}$ des entiers naturels. Alors :

1. *Si d divise b et b divise a, alors d divise a.*
2. *Si $d \mid a$ et $d \mid b$, alors pour tous $m, n \in \mathbb{Z}$, d divise $(a \times m + b \times n)$.*

Démonstration — *On utilise la définition de la divisibilité : $a = da'$, $b = db'$.*

Exercice 1 — *Réécrire l'énoncé de la proposition précédente uniquement en utilisant des multiples.*

Définition 4 (**Nombres premiers entre eux**)
Soient $a, b \in \mathbb{N}$ deux entiers.
*On dit que a et b sont **premiers entre eux** si leur seul diviseur commun dans $\mathbb{N}$ est 1.*
On le note parfois $a \wedge b$.

Exemple 5 — *Les entiers 14 et 9 sont premiers entre eux.*

Quand des entiers a et b ne sont pas premiers entre eux, il est naturel de se demander quel entier parmi leurs diviseurs communs est le plus grand.
Du point de vue des multiples, on peut se poser une question similaire : parmi les multiples communs à a et b, lequel est le plus petit ?

Définition 6 (**PGCD et PPCM**)
Soient $a, b \in \mathbb{N}$ deux entiers.

- *On apelle **plus grand diviseur commun** de a et b, noté $pgcd(a, b)$, le maximum de l'ensemble $Div(a, b) = \{d \in \mathbb{N} \mid d|a \text{ et } d|b\}$.*
  C'est le plus grand diviseur commun à a et à b.
- *On appelle **plus petit multiple commun** de a et b, noté $ppcm(a, b)$, le minimum de l'ensemble $Mul(a, b) = \{m \in \mathbb{N} \mid a|m \text{ et } b|m\}$.*
  C'est le plus petit multiple commun à a et à b.

Exemple 7 — *Soient $a = 189 = 3^3 \times 7$ et $b = 114 = 2 \times 3 \times 19$. On a alors :*

- *$pgcd(a, b) = 3$ car $Div(a, b) = \{1, 3\}$.*
- *$ppcm(a, b) = 2 \times 19 \times 9 \times 7 = 2394$*

Remarque 8 — *Deux entiers a, b sont premiers entre eux si et seulement si on a $pgcd(a, b) = 1$. En général, pour déterminer si a et b sont premiers entre eux, on détermine $pgcd(a, b)$ (ou bien on regarde les facteurs premiers de a et de b).*

Exercice 2 — *Montrer que :*

1. *$pgcd(n, 1) = 1$.*
2. *$pgcd(a, a + b) = pgcd(a, b)$.*
3. *$pgcd(n, 0) = n$.*
4. *$pgcd(n - 1, n + 1) = 1$ ou 2, pour $n \geq 1$.*

1.2 PGCD et algorithme d'Euclide

Comment calculer le PGCD de deux entiers a et b ? La question est simple à résoudre lorsque l'on connaît les diviseurs de a et de b. En pratique on possède rarement cette information (demande trop de calculs). On calcule le *PGCD* de deux nombres d'une façon bien plus efficace, grâce à la division euclidienne et à *l'algorithme d'Euclide*.

Proposition-Définition 9 (**Division euclidienne**)
Soient $a, b \in \mathbb{N}$.
Alors il existe des uniques entiers $q, r \in \mathbb{N}$ tel que :

$$a = b \times q + r, \text{ et } 0 \leq r < b.$$

*Ce résultat est appelé la **division euclidienne** de a par b (div. eucl.).*
*L'entier q est appelé le **quotient** de la division euclidienne.*
*L'entier r est appelé le **reste** de la division euclidienne.*
Démonstration — *Sur feuille. Il faut démontrer l'existence, et l'unicité.*

Exemple 10 — *Effectuons la division euclidienne de 23 par 4.*

1. *On détermine l'entier q tel que $23 - 4q$ soit positif et strictement inférieur à 4.*
   On a $23 - 4 = 19$, $23 - 2.4 = 15$, ...,$0 \leq 23 - 5 \times 4 = 3 < 4$.
   Cela revient à calculer $\lfloor \frac{23}{4} \rfloor$, la partie entière de $\frac{23}{4}$.
   On trouve $q = 5$.
2. *On en déduit alors que le reste r vaut 3.*
3. *La division euclidienne de 23 par 4 est donc $23 = 5 \times 4 + 3$.*

Remarque 11 — *La division euclidienne de a par b est constituée de deux conditions : $a = bq + r$, et $0 \leq r < b$.*
Sans la deuxième condition, les entiers q et r ne sont pas uniques. Attention à ne pas l'oublier.

Exercice 3 — *Déterminer la division euclidienne de 52 par 7.*

La division euclidienne est la division que vous avez probablement apprise en primaire (un quotient, un reste). Elle est très simple et rapide à effectuer.
Cependant, elle est le coeur central de l'arithmétique sur $\mathbb{N}$. On l'utilise pour obtenir des résultats plus poussés.

PROPOSITION 12
Soient $a, b \in \mathbb{N}$ deux entiers. Soit r le reste de la div. eucl. de a par b.
Alors, on a $Div(a,b) = Div(b,r)$.
Les diviseurs communs à a et b sont les diviseurs communs à b et r.
En particulier, on a $pgcd(a,b) = pgcd(b,r)$.
Démonstration — *On utilise le fait que $a = bq + r$, $r = bq - a$, et les propriétés de la divisibilité.*

L'algorithme d'Euclide est construit à partir de cette Proposition. Pour déterminer $d = pgcd(a,b)$, au lieu de chercher le maximum de l'ensemble $Div(a,b)$, on effectue une suite de divisions euclidiennes jusqu'à arriver à des entiers assez petits pour lesquels le *pgcd* s'obtient facilement. En général, on s'arrête lorsque le reste des divisions euclidiennes devient 0.

PROPOSITION 13 (**Algorithme d'Euclide**)
Soient $a, b \in \mathbb{N}$ deux entiers, avec $a \geq b$.
Soient q, r le quotient et le reste de la div. eucl. de a par b.
On pose $a_0 = a$, $b_0 = b$, $q_0 = q$, $r_0 = r$. On définit les d'entiers naturels $(a_n)_n$, $(b_n)_n$, $(q_n)_n$ et $(r_n)_n$ par récurrence comme suit :
Pour tout $n \geq 0$, on pose $a_{n+1} = b_n$ et $b_{n+1} = r_n$. q_{n+1} et r_{n+1} sont le quotient et le reste de la division euclidienne de a_{n+1} par b_{n+1}.
Alors, la suite $(r_n)_n$ n'a qu'un nombre fini de termes non-nuls.
L'agorithme d'Euclide, qui s'arrête quand on obtient $r_n = 0$, a toujours un nombre fini d'étapes.
Argument sur feuille.

THÉORÈME 14 (**Calcul du PGCD par l'algorithme d'Euclide**)
Soient $a, b \in \mathbb{N}$ deux entiers naturels.
Soient $(a_n)_n$, $(b_n)_n$, $(q_n)_n$ et $(r_n)_n$ les suites de l'algorithme d'Euclide. Soit m le premier entier tel que $r_m = 0$.
Alors, on a $r_{m-1} = pgcd(a,b)$.
Le pgcd de a et de b est le dernier reste non-nul obtenu dans l'algorithme d'Euclide.
Démonstration — *On utilise les propriétés liant pgcd et division euclidienne.*

EXEMPLE 15 — *Déterminons à l'aide de cet algorithme le PGCD de 41 et 12.*
- $41 = 12 \times 3 + 5$
- $12 = 5 \times 2 + 2$
- $5 = 2 \times 2 + 1$
- $2 = 1 \times 2 + 0$

On obtient, d'après l'algorithme d'Euclide, que $pgcd(41, 12) = 1$.

EXERCICE 4 — *À l'aide de l'algorithme d'Euclide, déterminer le pgcd de 135 et 15.*

Une autre application de l'algorithme d'Euclide est la proposition suivante.

THÉORÈME 16 (**Théorème de Bézout** (HP))
Soient a et b deux entiers naturels.
Alors, il existe $u, v \in \mathbb{Z}$ tels que $pgcd(a,b) = au + bv$.
En particulier, si a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.
Pour démontrer ce résultat, on effectue l'algorithme d'Euclide entre a et b, puis on utilise chaque ligne de l'algorithme pour exprimer les restes r_n en fonction de a et de b. On appelle cette méthode l'algorithme d'Euclide étendu. (Hors Programme)

EXEMPLE 17 — *Calculer $d = pgcd(26, 133)$. Déterminer $u, v \in \mathbb{Z}$ tels que $26.u + 133.v = d$.*

• *On commence par l'algorithme d'Euclide :*
$133 = 26.5 + 3$
$26 = 3.8 + 2$
$3 = 2.1 + 1$
$2 = 2.1 + 0$
Ainsi, on a $pgcd(26, 133) = 1$.
• *Trouvons alors* u *et* v. *On a :*
$26 = 133.0 + 26.1$
$3 = 133.1 - 26.5$
$2 = 26.1 - 3.8 = 133.(-8) + 26.41$
$1 = 3.1 - 2.1 = 133.(1 - (-8)) + 26.(-5 - 41) = 133.9 - 46.26.$
Ainsi, $u = -46$ *et* $v = 9$ *conviennent.*

La maîtrise de l'algorithme d'Euclide étendu n'est pas exigée au programme (mais celle de l'algorithme d'Euclide si !).

1.3 Congruence modulo n

Définition 18 (**Congruence modulo** n)
Soient $a, b, n\mathbb{N}$ *des entiers.*
On dit que a *et* b *sont congrus modulo* n, *noté* $a \equiv b\, mod(n)$, *si* $n \mid b - a$.

Exemple 19 —
- 21 *est congru à* 0 *modulo* 3.
- 151 *est congru à* 1 *modulo* 2.
- 151 *est congru à* 6 *modulo* 9.

Proposition 20
Soient $a, b, c, n \in \mathbb{N}$. *Alors :*
- *On a* $a \equiv a\, mod(n)$ *(réflexivité)*
- *Si* $a \equiv b\, mod(n)$ *alors* $b \equiv a\, mod(n)$ *(symétrie)*
- *Si* $a \equiv b\, mod(n)$ *et* $b \equiv c\, mod(n)$ *alors* $a \equiv c\, mod(n)$ *(transitivité)*

On dit que la congruence modulo n *est une relation d'équivalence sur* N.
Démonstration — *On a* $a - a = 0$ *et* $n \mid 0$.
Si $n \mid b - a$ *et* $n \mid c - b$ *alors* $n \mid (c - b) + (b - a) = c - a$, *donc* $a \equiv c\, mod(n)$. □

Proposition 21
Soient $a, b, n \in \mathbb{N}$.
On a $a \equiv b\, mod(n)$ *ssi* a *et* b *ont le même reste dans la division euclidienne par* n.
Démonstration — *On a* $q, q', r, r' \in \mathbb{N}$ *tq* $a = nq + r$, $b = nq' + r'$ *et* $r < n$, $r' < n$. *Alors* $b - a = n(q' - q) + (r' - r)$, *donc* n *divise* $b - a$ *ssi* n *divise* $r' - r$. *Or,* $r' - r \in \{-n + 1, \dots, 0, \dots, n - 1\}$, *donc* n *divise* $r' - r$ *ssi* $r' - r = 0$ *ssi* $r' = r$. □

Proposition 22
Soient $a, n \in \mathbb{N}$. *Alors :*
- *Il existe* $k \in \{0, \dots, n - 1\}$ *tel que* $a \equiv k\, mod(n)$
- *On a* $a \equiv 0\, mod(n)$ *ssi* $n \mid a$.

Proposition 23
Soient $a, b, c, d, n \in \mathbb{N}$ *tels que* $a \equiv b\, mod(n)$ *et* $c \equiv d\, mod(n)$. *Alors :*
- $a + c \equiv b + c\, mod(n)$ *et* $a + c \equiv b + d\, mod(n)$
- $ac \equiv bc\, mod(n)$ *et* $ac \equiv bd\, mod(n)$
- *pour tout* $k \geq 0$, $a^k \equiv b^k\, mod(n)$.

Démonstration — *On a* $n \mid b - a$ *et* $(b + c) - (a + c) = b - a$, *donc* $n \mid (b + c) - (a + c)$, *donc* $a + c \equiv b + c\, mod(n)$.
Par transitivité, on a $a + c \equiv b + c\, mod(n)$ *et* $b + c \equiv b + c\, mod(n)$, *d'où* $a + c \equiv b + d\, mod(n)$.
On a $n \mid b - a$, *donc* $n \mid c(b - a) = cb - ca$, *donc* $ac \equiv bc\, mod(n)$.

Par transitivité, on a $ac \equiv bc \, mod(n)$ *et* $bc \equiv bd \, mod(n)$ *donc* $ac \equiv bd \, mod(n)$.
Enfin, on démontre par récurrence sur $k \geq 0$ *que :* $\forall k \geq 0$, $a^k \equiv b^k \, mod(n)$. □

1.4 Nombres premiers

Définition 24 (**Nombre premier**)
Soit $n \in \mathbb{N}$.
On dit que n *est un nombre* ***premier*** *si* $Div(n) = \{1, n\}$, *avec* $n \neq 1$.
*Un nombre premier est un nombre entier qui possède exactement deux diviseurs (*1 *et lui-même).*
On note $\mathcal{P}$ ***l'ensemble des nombres premiers.***

Proposition 25
Soit $p \in \mathcal{P}$ *un nombre premier. Soit* $n \in \mathbb{N}$ *qui n'est pas un multiple de* p.
Alors, p *est premier avec* n.
En particulier, pour tout $1 \leq k \leq p-1$ *on a* $pgcd(p, k) = 1$.
Démonstration — *On utilise la définition de nombre premier.*

Proposition 26
Soit $n \in \mathbb{N}$ *avec* $n > 1$.
Alors, n *possède un diviseur qui est un nombre premier.*
Démonstration — *On procède par disjonction de cas (soit* n *premier, soit* n *non premier).*

Théorème 27 (**Infinité des nombres premiers**)
Il existe une infinité de nombres premiers.
L'ensemble $\mathcal{P}$ *est infini.*
Démonstration — *On démontre ce résultat par l'absurde.*

Méthode 28
Pour montrer qu'un entier n $(n \geq 2)$ *est premier, il suffit de montrer que pour tout nombre premier* p *tel que* $2 \leq p \leq \sqrt{n}$ *on a* $p \nmid n$.

Exemple 29 — *Les entiers* $2; 3; 5; 7; 9; 11; 13$ *sont les premiers nombres premiers.*

Exercice 5 — *À l'aide de la méthode précédente, montrer que* 97 *est un nombre premier.*

Le théorème fondamental concernant les nombres premiers est le fait qu'ils sont les "briques de base" qui permettent de construire et d'identifier tous les nombres entiers.

Théorème 30 (**Décomposition en produit de facteurs premiers**)
Soit $n \in \mathbb{N}$ *un entier naturel, avec* $n \geq 2$.
Alors n *se décompose en produit de la forme :*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_N^{\alpha_N}.$$

Les $p_1, \ldots, p_r$ *sont des nombres premiers deux à deux distincts, et les* α_i *sont des entiers naturels non nuls.*
De plus, cette décomposition est unique, à l'ordre près des termes $p_i^{\alpha_i}$. *Les nombres premiers* $p_1, \ldots, p_r$ *sont appelés les* ***facteurs premiers*** *de* n.
Démonstration —*Admise.*

Exemple 31 — $7007 = 7 \times 7 \times 11 \times 13$

L'existence et l'unicité de cette décomposition en produit de facteurs premiers est un résultat central en arithmétique. Cela explique que tout nombre entier n est un produit de certains nombre premiers.

Si on connaît les facteurs premiers de a et de b, on peut facilement en déduire des quantités comme $pgcd(a,b)$, $ppcm(a,b)$, et donc dire si a, b sont premiers entre eux (ou si a ou b est premier).

Exemple 32 — *Pour $a = 12 = 4.3 = 2^2.3$ et $b = 20 = 4.5 = 2^2.5$, on a $pgcd(a,b) = 2^2 = 4$ et $ppcm(a,b) = 2^2.3.5 = 60$.*

Avec les nombres premiers et la notion de "premiers entre eux", viennent plusieurs théorèmes qui aident beaucoup à résoudre des questions de divisibilité.
Nous utiliserons l'un d'entre eux, le théorème de Gauss.

Proposition 33 (Théorème de Gauss)
Soient $a, b \in \mathbb{N}$ qui sont premiers entre eux. Soit $c \in \mathbb{N}$.
Si $a \mid bc$, alors $a \mid c$.

Nous terminons avec une proposition qui relie *pgcd* et *ppcm* entre eux.

Proposition 34
Soient $a, b \in \mathbb{N}$. On a :

$$a \times b = pgcd(a,b) \times ppcm(a,b).$$

Démonstration —*Admise. (Utilise le théorème de décomposition en produit de facteurs premiers)*

Ainsi, pour calculer $ppcm(a,b)$, il suffit de déterminer $pgcd(a,b)$, puis de calculer $\frac{ab}{pgcd(a,b)}$.

2 Ensembles, dénombrement

2.1 Un peu de théorie des ensembles

Intuitivement, un ensemble est une collection d'objets, ces objets étant les éléments de l'ensemble. Cette définition pose un un problème théorique car la "collection" de tous les ensembles n'est pas un ensemble.
Cependant, nous ne rencontrerons pas d'ensembles posant des problèmes de ce type (la théorie des ensmbles est hors-programme), donc cette structure d'ensemble nous conviendra.

Le symbole principal pour les ensembles est $\in$, l'appartenance d'un élément à un ensemble. Les autres symboles ensemblistes découlent de celui-ci.

Définition 35 (**Appartenance**)
Soient A, B deux ensembles. On dit que A est inclus dans B, noté $A \subset B$, si "$\forall x \in A$ on a $x \in B$."

Axiome 36 (**Ensemble vide**)
Il existe un ensemble ne contenant aucun élément, et que cet ensemble est unique.
*On le note $\emptyset$, et on l'appelle **ensemble vide**.*

Axiome 37 (**Egalité d'ensembles**)
Soient A, B deux ensembles. A et B sont égaux si et seulement s'ils ont les mêmes éléments.
Autrement dit, on a $A = B$ ssi ($A \subset B$ et $B \subset A$).

Les preuves d'égalité d'ensembles par double-inclusion sont ainsi relativement courantes.

Remarque 38 —
- *Dans un ensemble, l'ordre des éléments ne compte pas. Ainsi, $\{1,5\} = \{5,1\}$.*
- *Un ensemble est décrit par les éléments qu'il contient. On a $\{1,1\} = \{1\}$.*
- *Certains ensembles usuels ont plusieurs écritures. Pour $n \in \mathbb{N}^*$, on a $\{1,2,\dots,n\} = [\![1,n]\!]$.*

Théorème 39
Soient E un ensemble, et pour tout $x \in E$ soit $P(x)$ une phrase mathématique.

Il existe un unique ensemble contenant tous les éléments $x \in E$ tels que $P(x)$ est vraie.
On le note $\{x \in E |\, P(x)\}$ ou $\{x \in E$ t.q. $P(x)$ est vraie$\}$.

Exemple 40 — *On a $\{0, 2, 4\} = \{k \in \mathbb{N}$ t.q. $k \leq 5$ et k pair$\}$.*

Définition 41 (**Union, intersection**)
Soient E un ensemble et A, B deux sous-ensembles de E.
*On définit l'ensemble A **union** B par $A \cup B = \{x \in E$ t.q. $x \in A$ ou $x \in B\}$.*
*On définit l'ensemble A **inter** B par $A \cap B = \{x \in E$ t.q. $x \in A$ et $x \in B\}$.*
*On définit l'ensemble **complémentaire de** A dans E par $E \setminus A = \{x \in E$ t.q. $x \notin A\}$.*
On le note aussi $\overline{A}$.

Proposition 42
Soient E un ensemble et A, B, C trois sous-ensembles de E. On a :

$A \cup A = A$	$A \cup B = B \cup A$	$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap A = A$	$A \cap B = B \cap A$	$A \cap (B \cap C) = (A \cap B) \cap C$
$\bar{\bar{A}} = A$	$A \cup \bar{A} = E$	$A \cap \bar{A} = \emptyset$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$		$A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$
$\overline{A \cup B} = \overline{A} \cap \overline{B}$		$\overline{A \cap B} = \overline{A} \cup \overline{B}$

Définition 43
*Soient E un ensemble et A, B deux sous-ensembles de E. On définit l'ensemble A **privé de** B par $A \setminus B = \{x \in E$ t.q. $x \in A$ et $x \notin B\} = A \cap \overline{B}$.*

2.2 Dénombrement

Le dénombrement (aussi appelé la cardinalité) est le fait de compter les éléments d'un ensemble. Cela est facile sur des exemples, mais comment décrire formellement cette notion ? On utilise pour cela les bijections.

Définition 44 (**Ensemble fini, ensemble infini**)
Soit E un ensemble.
- *On dit que E est un **ensemble fini** s'il existe $n \geq 0$ et f une bijection de $\{1, \ldots, n\}$ vers E.*
- *On dit que E est **l'ensemble vide** s'il ne contient aucun élément. On le note $\emptyset$.*
- *Sinon, on dit que E est un **ensemble infini**.*

Autrement dit, un ensemble fini est un ensemble pour lequel on peut numéroter les éléments, avec une quantité finie de numéros.
On écrira alors $E = \{x_1, \ldots, x_n\}$ (un numérotage des éléments de E).
Un ensemble infini est au contraire un ensemble *qui n'est pas fini*.

Remarque 45 — *En mathématiques on définit les ensembles **infinis dénombrables** comme les ensembles E qui sont en bijection avec $\mathbb{N}$. Ce sont les ensembles pour lesquels on peut numéroter les éléments avec tous les entiers. (ex : $\mathbb{Z}, \mathbb{N}^2, \mathbb{Q}$ sont dénombrables)*
*Et on appelle ensembles infinis **non-dénombrables** ceux qui ne sont pas dénombrables (ex : $\mathbb{R}, [0, 1]$ sont non-dénombrables).*

Définition 46 (**Cardinal d'un ensemble**)
Soit E un ensemble.
*Si E est fini, en bijection avec $\{1, \ldots, n\}$, on définit le **cardinal de** E par $Card(E) = n$.*
Si $E = \emptyset$ (l'ensemble vide), on pose $Card(E) = 0$.
Sinon, E est infini, et on pose $Card(E) = +\infty$.

Le cardinal d'un ensemble E, parfois noté $|E|$ ou $\sharp(E)$, désigne le nombre d'éléments de E. Le dénombrement consiste à déterminer le cardinal de E, à compter le nombre d'éléments de E.

2.3 Cardinalité pour les ensembles finis

PROPOSITION 47 (**Opérations ensemblistes et cardinal**)
Soient E un ensemble fini, et $A, B \subset E$ des parties de E. Alors on a :

1. *$A, A \cap B$, $A \cup B$, A^C sont des ensembles finis.*
2. *$Card(A) \leq Card(E)$. On a $Card(A) = Card(E)$ ssi $A = E$.*
3. *$Card(A^C) = Card(E) - Card(A)$.*
4. *$Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$.*
5. *Si $A_1, \ldots, A_n$ sont disjoints, alors $Card(A_1 \cup \ldots \cup A_n) = Card(A_1) + \ldots + Card(A_n)$.*

Démonstration — On fait du comptage d'élements dans E. □

DÉFINITION 48 (**Produit cartésien d'ensembles**)
Soient E, F des ensembles.
*On définit le **produit cartésien de E et F**, noté $E \times F$, par :*

$$E \times F = \{(x, y),\ x \in E, y \in F\}.$$

PROPOSITION 49
Soient E, F deux ensembles finis.
Alors on a $Card(E \times F) = Card(E)Card(F)$.

Démonstration — (Idée) Pour $E = \{e_1, \ldots, e_n\}$ et $F = \{f_1, \ldots, f_p\}$, on peut représenter les éléments de $E \times F$ dans un tableau :

$F \setminus E$	e_1	e_2	$\ldots$	e_n
f_1	(e_1, f_1)	(e_2, f_1)	$\ldots$	(e_n, f_1)
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
f_p	(e_1, f_p)	(e_2, f_p)	$\ldots$	(e_n, f_p)

.

Ce tableau est rectangulaire, avec p lignes et n colonnes, donc $n \times p$ éléments. □

DÉFINITION 50 (k-**uplet**)
Soient E un ensemble, et $k \geq 1$ un entier.
*Un **k-uplet** d'éléments de E est un élément de $E^k = E \times E \times \ldots \times E$ (k fois).*
On a $E^k = \{(a_1, \ldots, a_k),\ a_k \in E\}$.

EXEMPLE 51 — *Le pavé délimité par $(0,0), (1,0), (1,1), (0,1)$ est égal à $[0,1]^2$.*
Le plan $\mathbb{R}^2$ est l'ensemble des paires de réels, et l'espace $\mathbb{R}^3$ est l'ensemble des triplets de réels.

REMARQUE 52 — *Dans un k-uplet, on peut trouver plusieurs fois le même élément. De plus, l'ordre compte. Ne pas confondre le k-uplet $(a_1, \ldots, a_k)$ avec l'ensemble $\{a_1, \ldots, a_k\}$.*
Dans des situations où l'on prend des éléments de E sans remise (tirage dans une urne) ou que l'ordre ne compte pas (une main au poker), les ensembles de choix possibles seront différents de E^k (et leurs cardinaux aussi).

PROPOSITION 53
Soient E un ensemble fini de cardinal n, et $k \geq 1$.
Il existe $Card(E)^k = n^k$ k-uplets d'éléments de E.

Démonstration — *Le nombre de k-uplets est $Card(E^k)$. On montre par récurrence sur k que ce cardinal vaut $Card(E)^k$.* □

DÉFINITION 54 (**Ensemble des parties**)
Soit E un ensemble.
*On appelle **ensemble des parties de E**, noté $\mathcal{P}(E)$, la collection de toutes les parties de E. On a : $\mathcal{P}(E) = \{A,\ A \subset E\}$.*

Exemple 55 — *Pour $E = \{0, 1\}$ on a $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.*

Quand E est un ensemble fini, on peut expliciter tous les éléments de $\mathcal{P}(E)$. Quand E est infini cela devient beaucoup trop difficile.

Proposition 56
Soit E un ensemble fini de cardinal n.
Alors $\mathcal{P}(E)$ est un ensemble fini. On a $Card(\mathcal{P}(E)) = 2^{Card(E)} = 2^n$.

Démonstration — *Voir Ch 1. Pour $E = \{x_1, \dots, x_n\}$, choisir une partie A de E revient exactement à choisir pour tout $1 \leq k \leq n$ si $x_k \in A$ ou si $x_k \notin A$.*
On a 2 choix possibles, à refaire n fois de façon distincte, donc $2 \times 2 \times \dots \times 2 = 2^n$ choix possibles au total. □

Exemple 57 — *Un ensemble E à 4 éléments a $2^4 = 16$ parties possibles, càd $Card(P(E)) = 16$.*

Proposition 58
Soient E, F des ensembles finis, à n et p éléments. L'ensemble des fonctions de E vers F, $\mathcal{F}(E, F)$, est fini, et $Card(\mathcal{F}(E, F)) = Card(F)^{Card(E)} = p^n$.

Démonstration — *On pose $E = \{x_1, \dots, x_n\}$. Définir $f : E \to F$, c'est choisir pour tout $1 \leq k \leq n$ la valeur de x_k. On a $Card(F)$ valeurs possibles pour $f(x_k)$, il faut faire ce choix $Card(E)$ fois, et tous les choix sont indépendants. D'où $Card(F)^{Card(E)}$ choix possibles au total.* □

Exercice 6 — *Pour $Card(E) = n$, $Card(F) = p$, déterminer $a_{n,p}$ le nombre de fonctions injectives de E vers F.*
Déterminer $b_{n,p}$ le nombre de fonctions surjectives de E vers F. (plus difficile)

Proposition 59
Soit E un ensemble fini à n éléments. On note $Bij(E)$ l'ensemble des bijections $f : E \to E$.
Alors, on a $Card(Bij(E)) = n!$.

Démonstration — *On pose $E = \{x_1, \dots, x_n\}$. Comptons d'abord le nombre de fonctions injectives. Pour que f soit injective il faut que chaque $f(x_k)$ soit différent. On a ainsi n choix pour $f(x_1)$, puis $(n-1)$ choix pour $f(x_2)$, puis $(n-2)$ choix pour $f(x_3)$, ...,puis 2 choix pour $f(x_{n-1})$ et 1 choix pour $f(x_n)$. Cela donne $n(n-1)(n-2)\dots 2.1 = n!$ fonctions injectives possibles de E dans E. Et comme f est injective, l'ensemble $f(E) = \{f(x_1), \dots, f(x_n)\}$ contient exactement n éléments. Vu que $Card(f(E)) = Card(E)$ et $f(E) \subset E$, on a donc $f(E) = E$. Donc f est surjective, donc f est bijective.* □

Définition 60 (**Parties**)
Soient E un ensemble et $k \geq 0$.
*Une **partie de E à k éléments** est un ensemble A tel que $A \subset E$ et $Card(A) = k$.*

Les parties à k éléments représentent les façons de choisir k éléments de E distincts (sans remise), et non ordonnés.

Définition 61
Soient $n, p \in \mathbb{N}$.
*On définit le **coefficient binomial** $\binom{n}{p}$ par : $\binom{n}{p} = Card(\{A \subset \{1, \dots, n\} \text{ t.q. } Card(A) = p\}$.*

Le coefficient binomial $\binom{n}{k}$ est le nombre de parties à k éléments dans un ensemble à n éléments.

Exemple 62 — *Dans un jeu de 52 cartes, on a $\binom{52}{5}$ tirages de 5 cartes possibles (cartes toutes distinctes, l'ordre ne compte pas).*
Dans une urne contenant 10 boules numérotées, si on tire 4 boules simultanément, il y a $\binom{10}{4}$ tirages possibles.

Proposition 63

Soient $n, k \in \mathbb{N}$. On a :

1. $\binom{n}{0} = 1$, $\binom{n}{1} = n$
2. $\binom{n}{k} = 0$ *si* $k > n$
3. $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$
4. *Si* $0 \leq k \leq n$, $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}$
5. *Si* $0 \leq k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$
6. *Si* $1 \leq k \leq n$, $k\binom{n}{k} = n\binom{n-1}{k-1}$

Définition 64 (**Arrangements**)
Soient E un ensemble et $1 \leq k \leq n$.
*Un k-**arrangement** de E est un k-uplet d'éléments de E qui sont tous différents.*

Comme E ne contient que n éléments, il n'existe pas de k-arrangements de E pour $k > n$. Un k-arrangement représente une partie de E à k éléments que l'on a ordonnée. Ici les éléments sont distincts et l'ordre compte. (ex : On tire une à une 4 boules sans remise dans une urne de 10 boules numérotées)

Proposition 65
Soient E un ensemble fini de cardinal n et $1 \leq k \leq n$.
Alors le nombre de k-arrangements de E est $\frac{n!}{(n-k)!} = n(n-1)\dots(n-k+1) = \binom{n}{k}.k!$.

Démonstration — Un k-arrangement est un k-uplet $(a_1, \dots, a_k)$ tel que $\forall 1 \leq i < j \leq k$ on a $a_i \neq a_j$.
On peut le construire en choisissant a_1 d'abord (n choix), puis a_2 ($n-1$ choix), puis a_3 ($n-2$ choix),..., puis a_k ($n-k+1$ choix). Au total, cela fait $n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}$ constructions possibles. □

2.4 Tirages

Remarque 66 — *Soit E un ensemble fini, avec $Card(E) = n$. Pour $k \in \mathbb{N}$, on a 4 façons usuelles de tirer k éléments dans l'ensemble E :*

1. *[Avec remise, avec ordre] Les k-uplets de E. On en a n^k.*
   Cela correspond à l'ensemble des combinaisons d'un cadenas (k numéros avec n valeurs chacun).
2. *[Sans remise, sans ordre] Les parties à k éléments. On en a $\binom{n}{k}$.*
   Cela corredpond à l'ensemble des tirages au loto (k boules avec n valeurs possibles).
3. *[Sans remise, avec ordre] Les k-arrangements. On en a $k!\binom{n}{k}$.*
   Cela corredpond à l'ensemble des tirages au tiercé (k premiers chevaux, n participants).
4. *[Sans remise, sans ordre] Les parties à k éléments avec répétitions. On en a $\binom{n+k-1}{n-1}$.*
   Cela correspond à l'ensemble des coupes de boules de glace possibles (k boules de glace, n parfums).

Exemple 67 — *Dans une classe à 21 élèves, le nombre de choix possibles pour leurs dates de naissances est 365^{21} (en négligeant le 29 Février).*
Le nombre de choix de dates de naissances qui sont toutes différentes (sans répétition) est $\frac{365!}{344!}$.
Ainsi, en prenant 21 éléèves au hasard uniforme, la probabilité que leurs dates d'anniversaires soient toutes différentes est de $\frac{\frac{365!}{344!}}{365^{21}} \sim 0.55$.
La probabilité qu'au moins deux élèves aient la même date d'anniversaire est donc environ de $1 - 0.55 = 0.45$. Il y a à peu près 1 chance sur 2 pour que cela arrive.

Exemple 68 — *Dans une classe à 21 élèves, combien de répartitions en groupes de colles sont possibles ?*
Il y aura 7 groupes de colles de 3 personnes chacun. On peut constituer les groupes de colles les uns après les autres en prenant 3 élèves parmi ceux de la classe, sans remise. L'ordre des élèves ne compte pas. L'ordre de ces 7 groupes de colle n'importe pas.
Ainsi, le nombre de répartitions possibles est $\binom{21}{3}\binom{18}{3}\binom{15}{3}\binom{12}{3}\binom{9}{3}\binom{6}{3}\binom{3}{3}\frac{1}{7!}$.
Ce nombre se simplifie en $\frac{21!}{(3!)^7.7!}$.

PROPOSITION 69 (**Lemme des tiroirs**)
Soient E un ensemble fini de cardinal n, $1 \leq k \leq n$, et $f : E \to \{1, \dots, k\}$.
Alors il existe $r \in \{1, \dots, k\}$ tel que $Card(\{x \in E \text{ t.q. } f(x) = r\}) \geq \lfloor \frac{n}{k} \rfloor$.

PROPOSITION 70 (**Lemme des tiroirs (cas infini)**)
Soient E un ensemble infini, $k \in \mathbb{N}^*$, et $f : E \to \{1, \dots, k\}$.
Alors il existe $r \in \{1, \dots, k\}$ tel que $Card(\{x \in E \text{ t.q. } f(x) = r\}) = +\infty$.

EXEMPLE 71 — *Si l'on range 15 livres dans 3 tiroirs, alors il y a forcément un tiroir qui contient au moins 5 livres. Sinon tous les tiroirs contiendraient au plus 4 livres, ce qui n'est pas possible.*

Bilan du contenu <u>nécessaire</u> à maîtriser :

- *Notion de diviseur et de multiple chez les entiers. Notation $a \mid b$.*
  Si $a \mid b$ et $a \mid c$ alors pour $d, e \in \mathbb{Z}$, $a \mid bd + ce$.
- *Ensemble $Div(a)$ des diviseurs de a. Ensemble $Div(a, b)$ des diviseurs communs à a et b. Définition de $pgcd(a, b)$ et $ppcm(a, b)$.*
- *Nombres premiers p. Ensemble $\mathcal{P}$. L'ensemble des nombres premiers $\mathcal{P}$ est infini.*
- *Théorème de décomposition en produit de facteurs premiers : $n = p_1^{a_1} \dots p_r^{a_r}$, unicité à l'ordre près des termes.*
- *Relation $a \times b = pgcd(a, b).ppcm(a, b)$.*
- *Théorème de division euclidienne de a par b : Il existe un unique couple (q, r) tel que $a = bq + r$ et $0 \leq r < b$.*
  Corollaire : On a $a \mid b$ ssi $r = 0$.
  Corollaire : On a $pgcd(a, b) = pgcd(r, b)$.
- *Algorithme d'Euclide pour calculer $pgcd(a, b)$, par divisions euclidiennes successives.*
- *Nombres entiers premiers entre eux. Deux nombres premiers entre eux n'ont aucun facteur premier en commun.*
  Théorème de Gauss : Si a et b sont premiers entre eux et si $a \mid bc$, alors $a \mid c$.
- *Fondements de théorie des ensembles. Inclusion, double-inclusion, ensemble vide, sous-ensembles. Opérations : union, intersection, complémentaire. Propriétés de ces opérations. Lien avec la logique booléenne (vrai/faux, et, ou, non).*
- *Fonctions injectives, surjectives, bijectives (les différentes caractérisations).*
- *Ensembles finis, cardinal. Lien entre $A \subset E$, $A \cap B$, $A \cup B$, $E \times F$ et cardinal.*
- *k-uplets d'un ensemble E, on en a n^k. Parties de E, on en a 2^n. Parties à k éléments de E, on en a $\binom{n}{k}$. k-arrangements de E, on en a $k!\binom{n}{k}$. Tirages sans ordre avec remise, on en a $\binom{n+k-1}{n-1}$. Exemples simples à maîtriser. (tiercé, loto, combinaison de cadenas, coupe de boules de glace)*
- *Savoir compter le nombre d'éléments dans un ensemble en découpant la construction de ces éléments (répétitions possibles ou non, l'ordre compte ou non).*