Chapitre 7

Nombres entiers, ensembles finis et dénombrement

Je n'ai jamais fait quoi que ce soit d'« utile ».

G. H. Hardy [1]

1. Rudiments d'arithmétique dans N

Proposition 1.

1. Toute partie non vide de **N** possède un plus petit élément (on dit que **N** est **bien ordonné**).
2. Toute partie non vide et majorée de **N** possède un plus grand élément.

Démonstration. 1. Soit A une partie non vide de **N**. Supposons que A ne possède pas de plus petit élément.
Posons pour tout $n \in \mathbf{N}$, H_n : « pour tout $x \in A$, $x \geqslant n$ ».
H_0 est vraie puisque $A \subset \mathbf{N}$.
Soit $n \in \mathbf{N}$ tel que H_n soit vraie, c'est-à-dire que n minore A. Or A ne possède pas de plus petit élément, donc pour tout $x \in A$, $x > n$. Ainsi pour tout $x \in A$, $x \geqslant n+1$, ce qui signifie que H_{n+1} est vraie.
Le principe de récurrence permet de conclure.
Ce résultat appliqué à $x \in A$ fixé et $n = x+1$ est contradictoire, et on conclut que A possède un plus petit élément.

1. Godfrey Harold HARDY - mathématicien britannique (1877-1947). La citation provient de son ouvrage *Apologie d'un Mathématicien*, dans lequel Hardy évoque son aversion pour les mathématiques appliquées et sa passion pour les mathématiques pures, « inutiles » et belles. Cette citation est d'autant plus savoureuse qu'un domaine de recherche de Hardy était l'arithmétique et que cette branche des mathématiques est l'une des plus appliquée aujourd'hui (dans le sens où tous les systèmes de chiffrement actuel, qui sont omniprésents de votre carte bancaire jusqu'à votre téléphone portable, sont basés sur les nombres premiers). La recherche mathématique n'a pas toujours vocation à être utile dans l'instant, mais qui sait ce qu'il en adviendra plus tard...

2. On cherche à démontrer que toute partie non vide et majorée de $\mathbf{N}$ possède un plus grand élément. Soit A une partie non vide et majorée de $\mathbf{N}$. Notons B l'ensemble des majorants de A.
   - Montrons que B possède un plus petit élément, que nous noterons m.
     A est majorée, donc B est non vide. Comme $\mathbf{N}$ est bien ordonné, B possède un plus petit élément.
   - Supposons $m = 0$. Pour tout $x \in A$, $x \leqslant m$, donc $A = \{0\}$, et $m = 0$ est le plus grand élément de A.
   - Supposons $m > 0$. Alors $m - 1$ n'appartient pas à B (puisque m est le plus petit élément de B), donc $m - 1$ ne majore pas A. Il existe donc $a \in A$ tel que $m - 1 < a \leqslant m$, d'où $a = m$ (l'inégalité ne concernant que des entiers). Comme m majore A, m est bien le plus grand élément de A. □

1.1. Diviseurs et multiples

Définition 2.

Soit a et b deux entiers naturels, on dit que a est un **diviseur** de b, ou que a **divise** b ou encore que b est un **multiple** de a, s'il existe un entier naturel k tel que $b = ka$.
Le cas échéant, on note $a \mid b$.
L'ensemble des multiples entiers naturels de a est l'ensemble

$$a\mathbf{N} = \{a \cdot n \ : \ n \in \mathbf{N}\}.$$

Exemple 3.
- 1 divise tous les entiers naturels mais n'est divisible que par 1.
- 0 est un multiple de tout entier naturel mais n'est le diviseur que de lui-même.
- L'ensemble des diviseurs entiers naturels de 6 est $\{1, 2, 3, 6\}$.

Exercice d'application 4. Montrer que pour tout entier positif impair n, $n^2 - 1$ est un multiple de 8.

↪ Soit $n \in \mathbf{N}$ impair. Il existe $k \in \mathbf{N}$ tel que $n = 2k + 1$. Alors $n^2 - 1 = 4q(q + 1)$ qui est un multiple de 8 car, comme les entiers q et $q + 1$ sont consécutifs, l'un deux est pair, et l'on a $n^2 - 1 = 8\frac{q(q+1)}{2}$, avec $\frac{q(q+1)}{2} \in \mathbf{N}$.

Proposition 5 - Quelques critères de divisibilité.

Soit n un entier naturel dont l'écriture décimale est $n = \overline{a_p \ldots a_1 a_0}$, ce qui signifie que

$$n = a_p 10^p + \cdots + a_1 10^1 + a_0 10^0,$$

avec $a_i \in [\![0, 9]\!]$ pour tout $i \in [\![0, p]\!]$.

(a) n est un multiple de 2 si et seulement si a_0 est un multiple de 2, *i.e.* $a_0 \in \{0; 2; 4; 6; 8\}$.

(b) n est un multiple de 3 si et seulement si $\sum_{k=0}^{p} a_k$ est un multiple de 3.

(c) n est un multiple de 5 si et seulement si a_0 est un multiple de 5, *i.e.* $a_0 \in \{0; 5\}$.

(d) n est un multiple de 9 si et seulement si $\sum_{k=0}^{p} a_k$ est un multiple de 9.

(e) n est un multiple de 10 si et seulement si a_0 est un multiple de 10, *i.e.* $a_0 = 0$.

(f) n est un multiple de 11 si et seulement si $\sum_{k=0}^{p} (-1)^k a_k$ est un multiple de 11.

Démonstration. (a) On a

$$n = \sum_{k=0}^{p} a_k 10^k = 2 \cdot 5 \cdot \sum_{k=0}^{p} a_k 10^{k-1} + a_0,$$

donc n est divisible par 2 si et seulement si a_0 est divisible par 2.

(b) Le binôme de Newton assure que, pour tout $k \in \mathbf{N}$, $10^k = (9+1)^k = \sum_{j=0}^{k} \binom{k}{j} 9^j$. Ainsi

$$n = \sum_{k=0}^{p} a_k \left(\sum_{j=0}^{k} \binom{k}{j} 9^k \right) = \sum_{k=0}^{p} a_k \left(1 + 9 \sum_{j=1}^{k} \binom{k}{j} 9^{j-1} \right) = \sum_{k=0}^{p} a_k + 3 \sum_{k=0}^{p} a_k \left(\sum_{j=1}^{k} \binom{k}{j} 3 \cdot 9^{j-1} \right)$$

L'entier n est donc multiple de 3 si et seulement si $\sum_{k=0}^{p} a_k$ est multiple de 3.

(c) Même preuve que (a), en factorisant la première somme par 5.

(d) Même preuve que (b), en factorisant la second somme par 9.

(e) Même preuve que (a), en factorisant la première somme par 10.

(f) Le binôme de Newton assure que, pour tout $k \in \mathbf{N}$, $10^k = (11-1)^k = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} 11^j$. Ainsi,

$$n = \sum_{k=0}^{p} a_k \left(\sum_{j=0}^{k} \binom{k}{j} (-1)^j 11^j \right) = \sum_{k=0}^{p} (-1)^k a_k + 11 \sum_{k=0}^{p} a_k \left(\sum_{j=1}^{k} \binom{k}{j} (-1)^{k-j} 11^{j-1} \right)$$

L'entier n est donc multiple de 11 si et seulement si $\sum_{k=0}^{p} (-1)^k a_k$ est multiple de 11. □

La relation « divise » est réflexive car pour tout entier naturel a, on a $a \mid a$. Elle est également transitive car si $a \mid b$ et $b \mid c$ alors $a \mid c$.

La relation « divise » n'est pas une relation d'équivalence car elle n'est pas symétrique : si $a \mid b$ alors on a pas nécessairement $b \mid a$ (exemple $a = 3$ et $b = 6$). Plus précisément, on a le résultat suivant :

Proposition 6.

Soit $(a, b) \in \mathbf{N}^2$. On a

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

Démonstration.
Sens direct. On suppose que $a \mid b$ et $b \mid a$. Il existe deux entiers naturels k et k' tels que $b = ka$ et $a = k'b$ ce qui donne $a = kk'a$. Si $a \neq 0$, alors $kk' = 1$. Comme k et k' sont des entiers naturels, on a nécessairement $k = k' = 1$ ce qui montre que $a = b$. Si $a = 0$, alors $b = k \times 0 = 0$ donc $a = b = 0$.
Sens réciproque. Si $a = b$ alors le résultat est évident. □

Remarque 7. La proposition précédente traduit l'antisymétrie de la relation |. Ainsi | est une relation d'ordre.

Proposition 8.

Soit $a, b, u, v \in \mathbf{N}$ et $x \in \mathbf{N}^\star$. On a

$$(d \mid a \text{ et } d \mid b) \implies d \mid (au + bv)$$

et

$$a \mid b \iff ax \mid bx.$$

Démonstration.
- Supposons que $d \mid a$ et $d \mid b$. Alors il existe deux entiers naturels k et k' tels que $a = dk$ et $b = dk'$. Avec deux tels entiers naturels k et k', on a donc $au + bv = dku + dk'v = d(ku + k'v)$. Puisque $ku + k'v$ est un entier naturel, on obtient que $d \mid (au + bv)$
- Supposons que $a \mid b$. Alors, il existe un entier naturel k tel que $b = ak$. Pour un tel k, on a donc $bx = akx = axk$ donc $ax \mid bx$.
  Réciproquement, supposons que $ax \mid bx$. Il existe donc un entier naturel k tel que $bx = axk$. Considérons un tel entier k. Comme $x \neq 0$, $b = ak$ donc $a|b$.

□

Proposition 9.

Soit a, b deux entiers naturels non nuls. Si b divise a alors $b \leqslant a$.

Démonstration.
Si b divise a, alors $a = bk$ où k est un entier naturel. Puisque $a \neq 0$, $k \neq 0$, donc $k \geqslant 1$ donc $bk \geqslant b$ donc $b \leqslant a$. □

1.2. Division euclidienne dans les entiers naturels

Théorème 10 - Division euclidienne.

Soit $a \in \mathbf{N}$ et $b \in \mathbf{N}^\star$. Il existe un unique couple d'entiers naturels (q, r) tel que

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

q est appelé **quotient** de la division euclidienne de a par b.
r est appelé **reste** de la division euclidienne de a par b.

Démonstration.
• Unicité de (q, r). Soit (q, r) et (q', r') deux couples d'entiers naturels vérifiant

$$a = qb + r, \quad 0 \leqslant r < b \qquad \text{et} \qquad a = q'b + r', \quad 0 \leqslant r' < b.$$

Montrons que $q = q'$ et que $r = r'$.

Comme $-b < -r' \leqslant 0$, on a $-b < r - r' < b$ c'est-à-dire $\mid r - r' \mid < b$. Or par définition de r et r', on a

$$\mid r - r' \mid = \mid (a - bq) - (a - bq') \mid = b \mid q' - q \mid .$$

On a donc $b \mid q' - q \mid < b$ donc $\mid q' - q \mid < 1$ ce qui implique que $\mid q' - q \mid = 0$ et donc que $q = q'$. Mais alors $\mid r - r' \mid = b \mid q' - q \mid = 0$ c'est-à-dire $r = r'$.

• Existence du couple (q, r). L'ensemble $A = \{n \in \mathbf{N} : nb \leqslant a\}$ est une partie non vide de $\mathbf{N}$ puisque $0 \in A$. De plus A est majoré par a car si $n \in A$ alors $nb \leqslant a$ et donc $n \leqslant a$ car $b \geqslant 1$. L'ensemble A possède donc un plus grand élément que l'on note q et qui vérifie

$$qb \leqslant a \ \ (\text{car } q \in A) \qquad \text{et} \qquad (q+1)b > a \ \ (\text{car } q + 1 \notin A).$$

En posant $r = a - qb$, on a $a = qb + r$ et $0 \leqslant r < (q+1)b - qb = b$. □

Exemple 11. Division euclidienne de 27 par 7. On a $27 = 3 \times 7 + 6$ et $0 \leqslant 6 < 7$. Le nombre 27 est appelé le **dividende** de cette division euclidienne, 7 le **diviseur**, 3 est le quotient et 6 le reste.

Remarque 12. Si q est le quotient de la division euclidienne de a par b, alors $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $\{n \in \mathbf{N},\ nb \leqslant a\} = [\![0, q]\!]$.

Proposition 13.

Soit $a \in \mathbf{N}$ et $b \in \mathbf{N}^\star$. On note r le reste de la division euclidienne de a par b. On a

$$b \mid a \iff r = 0.$$

Démonstration.
Notons q et r respectivement le quotient et le reste de la division euclidienne de a par b.
Si $r = 0$ alors on a $a = bq$ donc $b|a$.
Réciproquement, supposons que $b|a$. Alors il existe $k \in \mathbf{N}$ tel que $a = bk + 0$. Considérons un tel k. Comme $0 \in [0\,;\, b[$, par unicité du quotient et du reste dans la division euclidienne de a par b, $k = q$ et $r = 0$. □

1.3. Plus grand commun diviseur et plus petit commun multiple

Soit a et b deux entiers naturels non tous les deux nuls. Supposons que $a \neq 0$. Si un entier naturel n divise a alors $n \leqslant a$. Ainsi, l'ensemble des nombres entiers naturels qui divisent à la fois a et b est un ensemble fini de nombres (car il est inclus dans $[\![1, a]\!]$) et cet ensemble est non vide (car il contient 1). Cet ensemble possède donc un plus grand élément.

Définition 14.

Soit a et b deux entiers naturels. Si $(a, b) \neq (0, 0)$, on appelle **plus grand commun diviseur** de a et b, et on note $\text{PGCD}(a, b)$ (ou $a \wedge b$) le plus grand entier naturel qui divise a et b.
Par convention, $\text{PGCD}(0, 0) = 0$.

Remarque 15. Si a et b sont non nuls, $1 \leqslant \text{PGCD}(a, b) \leqslant \min(a, b)$. Pour tout entier naturel $a > 0$, $\text{PGCD}(a, 0) = a$.

Exemple 16. Les diviseurs de 15 sont 1, 3, 5, 15 et ceux de 12 sont 1, 3, 4, 6, 12 donc $\text{PGCD}(15, 12) = 3$.

Proposition 17.

Soit a et b deux entiers naturels non nuls. On note r le reste de division euclidienne de a par b. On a

$$\text{PGCD}(a, b) = \text{PGCD}(b, r).$$

Démonstration.
Notons q le quotient de cette division euclidienne.

- Par définition, $\text{PGCD}(a, b)$ divise a et b et comme $r = a - bq$, $\text{PGCD}(a, b)$ divise r. Ainsi $\text{PGCD}(a, b)$ divise b et r donc par définition de $\text{PGCD}(b, r)$, on a $\text{PGCD}(a, b) \leqslant \text{PGCD}(b, r)$.
- Par définition, $\text{PGCD}(b, r)$ divise b et r et comme $a = bq + r$, $\text{PGCD}(b, r)$ divise a. Ainsi $\text{PGCD}(b, r)$ divise a et b donc par définition de $\text{PGCD}(a, b)$, on a $\text{PGCD}(b, r) \leqslant \text{PGCD}(a, b)$.

N Finalement $\text{PGCD}(b, r) = \text{PGCD}(a, b)$. □

◇◇

Remarque technique 18. Cette proposition permet de construire un algorithme, appelé **algorithme d'Euclide**, pour déterminer le PGCD de deux nombres entiers a et b. L'algorithme ci-dessous prend en entrée deux entiers a et b. En sortie de l'algorithme, la variable a contient $\text{PGCD}(a, b)$.

```
tant que b > 0
    r ← reste de la division euclidienne de a par b
    a ← b
    b ← r
fin tant que
```

Autrement dit, $\text{PGCD}(a, b)$ est le dernier reste non nul quand on effectue des divisions euclidiennes successives.

Une implémentation possible en Python est la suivante :

```python
def euclide(a, b):
    while (b > 0):
        r = a % b
        a = b
        b = r
    return a
```

Exercice d'application 19. Calculer $\text{PGCD}(306, 758)$.

↪ On a, avec l'algorithme d'Euclide

$$\begin{array}{rrcl} & 758 & = & 306 \times 2 + \mathbf{146} \\ \text{puis} & 306 & = & \mathbf{146} \times 2 + 14 \\ \text{puis} & \mathbf{146} & = & 14 \times 10 + 6 \\ \text{puis} & 14 & = & 6 \times 2 + 2 \\ \text{puis} & 6 & = & 2 \times 3 + 0 \end{array}$$

Finalement, $\text{PGCD}(a, b)$ est le dernier reste non nul, à savoir 2.

◇◇

Définition 20.

Soit a et b deux entiers naturels non nuls. On dit que a et b sont **premiers entre eux** lorsque $\text{PGCD}(a, b) = 1$.

Exemple 21. $\text{PGCD}(3, 4) = 1$ donc 3 et 4 sont premiers entre eux.

Définition 22.

On dit qu'une fraction $\dfrac{a}{b}$ de deux entiers est **irréductible** lorsque a et b sont premiers entre eux.

Soit a et b deux entiers naturels non nuls. L'ensemble des entiers naturels non nuls qui sont à la fois multiples de a et de b est un sous-ensemble non vide (car il contient ab) de $\mathbf{N}$ donc il possède un plus petit élément.

Définition 23.

Soit a et b deux entiers naturels non nuls. On appelle **plus petit commun multiple** de a et b, et on note $\text{PPCM}(a,b)$ (ou $a \vee b$) le plus petit entier naturel non nul qui soit un multiple de a et de b.
On convient que, pour tout $a \in \mathbf{N}$, $\text{PPCM}(a,b) = 0$. En particulier, $\text{PPCM}(0,0) = 0$.

Remarque 24. $\max(a,b) \leqslant \text{PPCM}(a,b) \leqslant ab$

Exemple 25. Les multiples strictement positifs de 6 sont 6, 12, 18, 24, 30… et ceux de 8 sont 8, 16, 24, 32… donc $\text{PPCM}(6,8) = 24$.

Proposition 26.

Soit $(a,b) \in (\mathbf{N}^\star)^2$. Si $b \mid a$ alors $\text{PGCD}(a,b) = b$ et $\text{PPCM}(a,b) = a$.

Démonstration.
On suppose que $b|a$. Alors $b \leqslant a$ donc $\max(a,b) = a$ et $\min(a,b) = b$. On sait donc que $\text{PGCD}(a,b) \leqslant b$. Or b est un diviseur de a et de b donc $\text{PGCD}(a,b) = b$. De même, on sait que $a \leqslant \text{PPCM}(a,b)$ or a est multiple de a et de b donc $\text{PPCM}(a,b) = a$. □

Proposition 27.

Soit a et b deux entiers naturels non nuls et n un entier naturel. Si $a \mid n$ et $b \mid n$, alors $\text{PPCM}(a,b) \mid n$.

Démonstration.
On suppose que $a \mid n$ et $b \mid n$. On écrit la division euclidienne de n par $\text{PPCM}(a,b)$: on considère l'unique couple (q,r) d'entiers naturels tels que

$$n = \text{PPCM}(a,b) \times q + r \qquad \text{et} \qquad 0 \leqslant r < \text{PPCM}(a,b).$$

Comme $r = n - \text{PPCM}(a,b) \times q$, on peut affirmer que r est un multiple de a et de b. Or $r < \text{PPCM}(a,b)$ donc $r = 0$. Ceci démontre que $\text{PPCM}(a,b) \mid n$. □

Proposition 28.

Pour tout $(a,b) \in \mathbf{N}^2$, $\text{PGCD}(a,b) \times \text{PPCM}(a,b) = a \times b$.

Démonstration.
Supposons que $(a,b) \in \mathbf{N}^2$. Posons $\delta = \text{PGCD}(a,b)$ et $\mu = \text{PPCM}(a,b)$. Puisque δ divise a et b, il existe $(a',b') \in \mathbf{N}^2$, avec $\text{PGCD}(a',b') = 1$, tel que $\begin{cases} a &= \delta a' \\ b &= \delta b' \end{cases}$.
En particulier, $\delta a'b'$ est un multiple commun à a et b, donc à μ. Ainsi il existe $k \in \mathbf{N}$ tel que $\delta a'b' = k\mu$.
Comme μ est un multiple commun à a et b, il existe $(\alpha,\beta) \in \mathbf{N}^2$ tel que $\begin{cases} \mu &= \alpha a \\ \mu &= \beta b \end{cases}$. Ainsi $\begin{cases} b' &= k\alpha \\ a' &= k\beta \end{cases}$.
Or, $\text{PGCD}(a',b)' = 1$, donc $k = 1$. Ainsi $\delta a'b' = \mu$, et on conclut en multipliant par δ. □

◇◇

Remarque technique 29. Puisqu'on connaît un algorithme pour calculer le PGCD de deux nombres, la proposition donne immédiatement une méthode pour calculer le PPCM.

Exercice d'application 30. Déterminer $\text{PPCM}(132, 72)$.

$\hookrightarrow$ Commençons par déterminer $\text{PGCD}(132, 72)$. On a

$$\begin{array}{rrcl} & 132 & = & 72 \times 1 + 60 \\ \text{puis} & 72 & = & 60 \times 1 + 12 \\ \text{puis} & 60 & = & 12 \times 5 + 0 \end{array}$$

donc $\text{PGCD}(132, 72) = 12$. On en déduit

$$\text{PPCM}(132, 72) = \frac{132 \times 72}{12} = 132 \times 6 = 792.$$

◇◇

Corollaire 31.

Soit a et b deux nombres entiers naturels non nuls. Si a et b sont premiers entre eux, alors $\text{PPCM}(a, b) = ab$.

Démonstration.
Immédiat, puisque a et b premiers entre eux signifie que $\text{PGCD}(a, b) = 1$. □

Corollaire 32.

Soit a et b deux nombres entiers naturels non nuls premiers entre eux et n un entier naturel. Si $a \mid n$ et $b \mid n$, alors $ab \mid n$.

Démonstration.
Immédiat avec $\text{PGCD}(a, b) = 1$ et la Proposition 27. □

1.4. Nombres premiers

Définition 33.

On appelle **nombre premier** tout entier naturel non nul admettant exactement 2 diviseurs entiers naturels distincts : 1 et lui-même.

Exemple 34. Les premiers nombres premiers sont 2, 3, 5, 7, 11...

Remarque 35. Deux nombres premiers distincts sont premiers entre eux.

Proposition 36.

Tout nombre entier supérieur ou égal à 2 est divisible par un nombre premier

Démonstration.
Pour tout $n \in \mathbf{N} \setminus \{0, 1\}$, on note $\mathcal{P}_n$ la propriété

$$\mathcal{P}_n : \text{« pour tout } k \in [\![2; n]\!], k \text{ admet un diviseur premier »}.$$

La propriété $\mathcal{P}_2$ est vraie car 2 admet un diviseur premier : lui-même.

Soit $n \in \mathbf{N} \setminus \{0, 1\}$. On suppose que $\mathcal{P}_n$ est vraie. Si $n+1$ est premier, alors il a un diviseur premier : lui-même. Si $n+1$ n'est pas premier, alors il existe $k \in [\![2, n]\!]$ tel que $k \mid (n+1)$. Par hypothèse de récurrence, k possède un diviseur premier qui est *a fortiori* un diviseur premier de $n+1$ et donc $\mathcal{P}_{n+1}$ est vraie. □

Théorème 37.

Il existe une infinité de nombres premiers.

Démonstration.
Montrons ce résultat par l'absurde.
Supposons qu'il existe un nombre fini $n \geqslant 2$ de nombres premiers. Notons les $p_1, p_2, \dots, p_n$ et supposons que $p_1 < p_2 < \dots < p_n$. Considérons le nombre $N = p_1 p_2 \dots p_n + 1$. Alors $N \geqslant 2$.
D'après la proposition précédente, N admet un diviseur premier. Or aucun des nombres premiers p_1,... , p_n ne divise N puisque le reste de la division euclidienne de N par l'un des ces nombres vaut 1 (en effet N s'écrit $p_i.q + 1$ avec $q \in \mathbf{N}$ pour tout $i \in [\![1, n]\!]$). Contradiction ! □

◇◇

Remarque technique 38. Pour déterminer les nombres premiers inférieurs à une entier n fixé, on peut réaliser un **crible d'Ératosthène**. Le principe est le suivant :

- on écrit tous les nombres de 2 à n ;
- on conserve le nombre premier 2 et on rayon tous les multiples de 2 (qui ne sont donc pas premiers) ;
- pour chaque nombre suivant p non rayé, on conserve p et on raye les multiples de p ;
- lorsque l'algorithme s'arrête (on est arrivé à $\sqrt{n}$), tous les nombres non rayés sont les nombres premiers inférieurs à n.

Exercice d'application 39. Déterminer tous les nombres premiers inférieurs à 100.

↪ On détermine les 25 nombres premiers inférieurs à 100 :

- on colorie en rose les multiples de 2 strictement supérieurs à 2 ;
- on colorie en bleu les multiples de 3 strictement supérieurs à 3 (parmi les nombres qui restent) ;
- on colorie en jaune les multiples de 5 (on ne considère pas les multiples de 4, car 4 est déjà colorié, donc tous ses multiples sont aussi coloriés) ;
- on colorie en orange les multiples de 7 ;
- on s'arrête ici, car il ne reste plus de nombre non colorié inférieur à $\sqrt{100} = 10$.

Finalement, les 25 nombres premiers inférieurs à 100 apparaissent dans les cases blanches de la grille ci-après.

	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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Théorème 40 - Décomposition d'un nombre en produit de nombres premiers.

Tout entier naturel n supérieur ou égal à 2 admet une décomposition en facteurs premiers de la forme $n = q_1 q_2 \dots q_k$ où $q_1, \dots, q_k$ sont des nombres premiers. Cette décomposition est unique à l'ordre près des facteurs.
On peut également écrire cette décomposition sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où $p_1, \dots, p_r$ sont des nombres premiers distincts deux à deux et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls.

Démonstration.
Admis. □

Exemple 41. 1848 est divisible par 8 (car 848 est un multiple de 8), et $1848 = 8 \times 231$. De plus, 231 est divisible par 3 (car $2 + 3 + 1 = 6$ qui est divisible par 3), et $231 = 3 \times 77$. Finalement, $1848 = 2^3 \times 3 \times 7 \times 11$.

Exercice d'application 42. Déterminer la décomposition en facteurs premiers de $n = 277\ 200$.

↪ On a $n = 100 \times 2\ 772 = 2^2 \cdot 5^2 \cdot 396$. De plus, 2 772 est pair, d'où $n = 2^3 \cdot 5^2 \cdot 1\ 386$, puis comme 1 386 est pair, $n = 2^4 \cdot 5^2 \cdot 693$. Or 693 est divisible par 11, d'où $n = 2^4 \cdot 5^2 \cdot 11 \cdot 63$. Finalement,

$$n = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11.$$

Proposition 43.

Soit $(a,b) \in (\mathbf{N}\backslash\{0,1\})^2$, dont on écrit $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$ les décompositions en facteurs premiers (quitte à choisir $\alpha_i = 0$ ou $\beta_i = 0$ pour que les mêmes nombres premiers apparaissent dans les deux décompositions). On a :

$$\text{PGCD}(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \qquad \text{et} \qquad \text{PPCM}(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}.$$

Démonstration.
Admis. □

Remarque technique 44.

La Proposition 43 fournit une nouvelle méthode pour déterminer le PGCD ou le PPCM de deux entiers.

Exercice d'application 45. Déterminer PGCD(360, 336) et PPCM(360, 336).

↪ On a $360 = 2^3 \cdot 3^2 \cdot 5$ et $336 = 2^4 \cdot 3 \cdot 7$. Donc

$$\text{PGCD}(360,336) = 2^3 \times 3 = 24 \qquad \text{et} \qquad \text{PPCM}(360,336) = 2^4 \times 3^2 \times 5^1 \times 7^1 = 5\ 040.$$

Remarque technique 46.

Soit m, n, a, b quatre nombres entiers naturels non nuls. On veut mettre au même dénominateur les deux fractions $\frac{m}{a}$ et $\frac{n}{b}$. Le dénominateur commun « optimal » n'est pas nécessairement ab : c'est PPCM(a,b).

« Optimal » signifie ici que lorsqu'on additionne ou qu'on soustrait les deux fractions, la fraction obtenue avec pour dénominateur ab est simplifiable et que cette simplification peut être évitée en prenant pour dénominateur commun PPCM(a,b). (cela n'empêche pas que la fraction obtenue peut ne pas être irréductible.)

Exercice d'application 47. Calculer $A = \dfrac{11}{360} - \dfrac{5}{336}$.

↪ Puisque $\text{PPCM}(360,336) = 5\ 040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, on calcule :

$$A = \frac{11}{2^3 \cdot 3^2 \cdot 5} - \frac{5}{2^4 \cdot 3 \cdot 7} = \frac{11 \cdot 2 \cdot 7}{2^4 \cdot 3^2 \cdot 5 \cdot 7} - \frac{5^2 \cdot 3}{2^4 \cdot 3^2 \cdot 5 \cdot 7} = \frac{154 - 75}{2^4 \cdot 3^2 \cdot 5 \cdot 7} = \frac{79}{2^4 \cdot 3^2 \cdot 5 \cdot 7}.$$

2. Ensembles finis

Dans toute la suite, n désignera un entier naturel non nul.

2.1. Cardinal d'un ensemble fini

Intuitivement, un **ensemble fini de cardinal** n est un ensemble $\{x_1, ..., x_n\}$ comportant n éléments. Plus formellement, on a :

Définition 48.

On dit qu'un ensemble E est **fini** s'il vérifie l'une des deux conditions suivantes :

(a) E est l'ensemble vide, auquel cas on dit que son **cardinal** est nul ;

(b) E est en bijection avec $[\![1, n]\!]$, auquel cas on dit que son **cardinal** est n.

Le cardinal d'un ensemble fini E est noté $\mathrm{Card}(E)$, $|E|$ ou encore $\#E$.

Exemple 49. Card({🕯, 😎, 🍲, ☃, 🪑}) = 5.

Exemple 50. Soit $n \in \mathbf{N}^\star$. L'application $\begin{array}{ccc} [\![1, n]\!] & \longrightarrow & \mathbf{U}_n \\ k & \longmapsto & \mathrm{e}^{\frac{2ik\pi}{n}} \end{array}$ est bijective, donc $\mathbf{U}_n$ est fini et $\mathrm{Card}(\mathbf{U}_n) = n$.

Exercice d'application 51. Soit $(p, q) \in \mathbf{Z}^2$ avec $p \leqslant q$. Déterminer $\mathrm{Card}([\![p, q]\!])$.

↪ On a $\begin{array}{ccc} [\![1, q-p+1]\!] & \longrightarrow & [\![p, q]\!] \\ i & \longmapsto & p-1+i \end{array}$ bijective, donc le cardinal de $[\![p, q]\!]$ est $q - p + 1$.

Théorème 52.

Soit E un ensemble fini et F une partie de E.

1. F est un ensemble fini et $\mathrm{Card}(F) \leqslant \mathrm{Card}(E)$.
2. $F = E \iff \mathrm{Card}(F) = \mathrm{Card}(E)$.

Remarque technique 53. Pour montrer que deux ensembles finis A et B sont égaux, on peut se contenter de montrer que $A \subset B$ et $\mathrm{Card}(A) = \mathrm{Card}(B)$, au lieu de montrer $A \subset B$ et $B \subset A$.

Proposition 54.

Soit E et F deux ensembles finis et f une application de E dans F.

1. $f(E)$ est un ensemble fini, $\mathrm{Card}(f(E)) \leqslant \mathrm{Card}(F)$ et $\mathrm{Card}(f(E)) \leqslant \mathrm{Card}(E)$.
2. L'application f est injective, si et seulement si, $\mathrm{Card}(f(E)) = \mathrm{Card}(E)$ et dans ce cas $\mathrm{Card}(F) \geqslant \mathrm{Card}(E)$.
3. L'application f est surjective si, et seulement si, $\mathrm{Card}(f(E)) = \mathrm{Card}(F)$ et dans ce cas $\mathrm{Card}(F) \leqslant \mathrm{Card}(E)$.
4. L'application f est bijective si, et seulement si, $\mathrm{Card}(f(E)) = \mathrm{Card}(E) = \mathrm{Card}(F)$.

Démonstration.
Notons n le cardinal de E.

1. La finitude de $f(E)$ est évidente car $f(E)$ est une partie de F qui est un ensemble fini. Même chose pour la majoration par $\mathrm{Card}(F)$. On a $f(E) = \{f(x) \mid x \in E\}$ donc puisque E possède n éléments, $f(E)$ a au plus n éléments distincts donc $\mathrm{Card}(f(E)) \leqslant \mathrm{Card}(E)$.
2. $\mathrm{Card}(f(E))=\mathrm{Card}(E)$ si, et seulement si, tous les éléments de E ont des images distinctes par f, autrement dit si, et seulement si, f est injective. Comme $\mathrm{Card}(f(E))\leqslant\mathrm{Card}(F)$ et que $\mathrm{Card}(f(E))=\mathrm{Card}(E)$ on a le résultat.

3. Si f est surjective, alors $f(E) = F$ donc $\text{Card}(f(E)) = \text{Card}(F)$.
   Réciproquement, si $\text{Card}(f(E)) = \text{Card}(F)$, alors $f(E) = F$ car $f(E)$ est un sous-ensemble de F et donc f est surjective.
4. C'est une conséquence de 3 et 4.

□

Théorème 55 - Principe des tiroirs de Dirichlet.

Quand on doit ranger $n+1$ chaussettes dans n tiroirs, deux chaussettes au moins se retrouvent dans le même tiroir.

Démonstration.
Ranger $n+1$ chaussettes dans n tiroirs, c'est choisir une application d'un ensemble de cardinal $n+1$ dans un ensemble de cardinal n. Comme $n+1 > n$, une telle application n'est jamais injective, d'où le résultat. □

Exemple 56. Etant donnés trois entiers, il y a au moins deux de même parité (trois entiers à ranger dans deux tiroirs : celui des entiers pairs, et celui des entiers impairs).

Exercice d'application 57. Soit n un entier naturel non nul. On considère un ensemble de $n+1$ entiers choisis parmi 1, 2, 3,..., $2n$. Montrer qu'il existe deux entiers de cet ensemble dont la somme vaut $2n+1$ (exemple avec $n = 5$: choisissez 6 entiers distincts entre 1 et 10 ; il y en a deux dont la somme vaut 11).

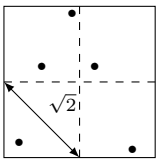
↪ Avec les entiers compris entre 1 et $2n$, on peut former n tiroirs : ce sont les paires d'entiers dont la somme vaut $2n+1$, *i.e.* les paires $\{1, 2n\}$, $\{2, 2n-1\}$,..., $\{n, n+1\}$. Si on range nos $n+1$ entiers dans ces tiroirs, il y a un tiroir qui en contient deux (et comme ils sont distincts...).

Exercice d'application 58. Montrer que, parmi les Lorrains chevelus, il en existe au moins deux avec exactement le même nombre de cheveux. On considérera qu'un individu possède au plus 300 000 cheveux, et qu'il y a environ 2 300 000 d'habitants en Lorraine.

↪ On considère 300 000 tiroirs, qui correspondent respectivement à 1 cheveux, 2 cheveux, etc. On place chaque Lorrain dans le tiroir correspondant à son nombre de cheveux sur la tête. Le principe des tiroirs assure lors qu'il y a au moins deux personnes ayant exactement le même nombre de cheveux sur la tête en Lorraine !

Exercice d'application 59. Etant donné cinq points dans un carré d'arête 2, montrer qu'on peut toujours en trouver deux distants d'au plus $\sqrt{2}$.

↪ Coupons simplement notre carré en quatre carrés comme indiqué ci-contre, et prenons les quatre sous-carrés ainsi formés pour « tiroirs ». On doit ranger cinq points quelconques dans quatre tiroirs, nous sommes donc forcés d'en ranger deux dans le même tiroirs. Au pire, ces points sont alors distant de $\sqrt{2}$, qui est la longueur de la diagonale de chaque sous-carré.



2.2. Réunion et différence

On rappelle que deux ensembles sont dits disjoints lorsque leur intersection est vide.

Proposition 60.

Soit A et B deux ensembles finis disjoints. L'ensemble $A \cup B$ est fini et

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B).$$

Démonstration.
Notons $n = \text{Card}(A)$ et $m = \text{Card}(B)$. Si $A = \{x_1, ..., x_n\}$ et $B = \{y_1, ..., y_m\}$, alors $A \cup B = \{x_1, ..., x_n, y_1, ..., y_m\}$ et puisque $A \cap B = \varnothing$, tous les éléments sont distincts. □

Corollaire 61.

Soit A une partie finie d'un ensemble fini E. Le complémentaire de A dans E est une partie finie et

$$\text{Card}(\complement_E A) = \text{Card}(E) - \text{Card}(A).$$

Démonstration.
Les ensembles A et $\complement_E A$ sont disjoints et $A \cup \complement_E A = E$ donc

$$\text{Card}(E) = \text{Card}(A) + \text{Card}(\complement_E A).$$

□

Par récurrence on peut généraliser la proposition précédente :

Proposition 62.

Soit $(A_k)_{1 \leqslant k \leqslant p}$ une famille de p ensembles finis deux à deux disjoints. L'ensemble $\bigcup_{k=1}^{p} A_k$ est un ensemble fini et

$$\text{Card}\left(\bigcup_{k=1}^{p} A_k\right) = \sum_{k=1}^{p} \text{Card}(A_k).$$

Démonstration.
Ce résultat s'obtient par récurrence en utilisant la Proposition 60. □

Exercice d'application 63. Déterminer le nombre d'entiers compris entre 1 et 1000 dont la somme des chiffres vaut 3.

↪ On va représenter un entier entre 1 et 999 par un triplet (a, b, c), où a est le chiffre des centaines, b celui des dizaines et c celui des unités. On cherche donc le nombre de triplets (a, b, c) d'entiers de $[\![0, 9]\!]$ tels que $a + b + c = 3$.
Notons $E = \left\{ (a, b, c) \in [\![0, 9]\!]^3 \;\middle|\; a + b + c = 3 \right\}$. Distinguons suivant la valeur prise par a : a peut valoir au maximum 3, ainsi $E = A_0 \cup A_1 \cup A_2 \cup A_3$, où

$$A_0 = \{(0, b, c) \mid b + c = 3\}, \quad A_1 = \{(1, b, c) \mid b + c = 2\},$$
$$A_2 = \{(2, b, c) \mid b + c = 1\}, \quad A_3 = \{(3, b, c) \mid b + c = 0\},$$

et les A_i sont clairement deux à deux disjoints. On a donc

$$\text{Card}(E) = \sum_{k=0}^{3} \text{Card}(A_i) = 4 + 3 + 2 + 1 = 10.$$

Il y a dix entiers compris entre 1 et 1000 dont la somme des chiffres vaut 3.

Lorsque les ensembles $A_1, ..., A_n$ de la proposition précédente sont disjoints et de même cardinal, la formule porte le joli nom de **principe du berger** (car un berger qui possède n moutons possède aussi $4n$ pattes de moutons !) :

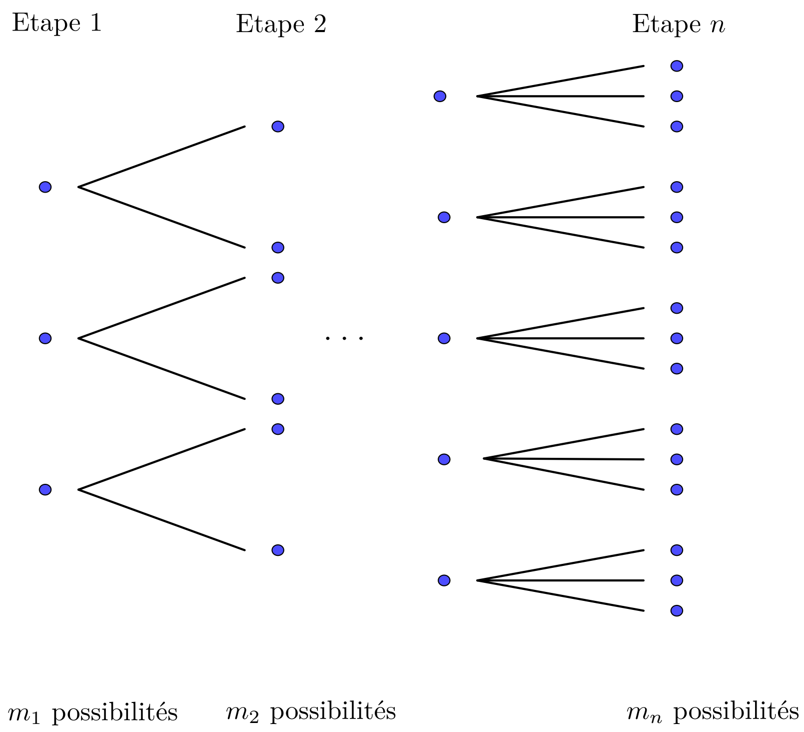
Corollaire 64 - Principe du berger ou principe multiplicatif.

Toute réunion disjointe de n ensembles de même cardinal p est un ensemble de cardinal np.

◇◇

Remarque technique 65. On utilisera ce principe quand un problème de dénombrement a été décomposé en deux sous-problèmes « étape 1 » et « étape 2 », avec n choix possibles pour l'étape 1 et p choix possibles *pour chacun de ces choix* dans l'étape 2. Le problème complet offre ainsi un total de np choix.

Bien entendu, on peut généraliser la méthode pour un nombre quelconque d'étapes.



S'il y a n étapes, et qu'à l'étape k, il y a m_k possibilités (m_k branches si on représente la situation avec un arbre), alors le nombre total d'objets est $m_1 \times m_2 \times \cdots \times m_n$.

Exercice d'application 66. Combien y a-t-il de couples (x, y) dans $[\![1, n]\!]^2$ tels que $x \neq y$?

$\hookrightarrow$ Pour construire un tel couple, on peut par exemple choisir x, puis choisir y. Il y a n valeurs possibles pour x et, pour chacune de ces n valeurs, il reste $n-1$ valeurs restantes pour y. Ainsi, il y a en tout $n(n-1)$ couples possibles.

Exercice d'application 67. En utilisant l'alphabet français (qui contient 26 lettres ☺), combien existe-t-il de mots de 3 lettres (successions de 3 lettres : le mot n'a pas forcément de sens) ne se terminant pas par la lettre e ?

$\hookrightarrow$

1. On choisit la première lettre : 26 possibilités ;
2. on choisit la deuxième lettre : 26 possibilités ;
3. on choisit la troisième lettre : 25 possibilités.

En tout, il y a $26 \times 26 \times 25 = 16\ 900$ possibilités.

Exercice d'application 68. En utilisant l'alphabet français, donner le nombre de mots de trois lettres que l'on peut former en obéissant aux règles suivantes :

- la première lettre du mot est l'une des voyelles A,E,I,O,U mais pas Y ;
- la deuxième lettre du mot est l'une des 3 lettres suivant, dans l'alphabet, la voyelle précédente ;
- la dernière lettre du mot est l'une des 6 voyelles A,E,I,O,U,Y, mais pas celle qui est la première lettre.

$\hookrightarrow$

1. On choisit la première lettre : 5 possibilités ;
2. on choisit la deuxième lettre : 3 possibilités (qui dépendent de la voyelle choisie à la première étape) ;
3. on choisit la dernière lettre : 5 possibilités (qui dépendent de la voyelle choisie à la première étape).

En tout, il y a $5 \times 3 \times 5 = 75$ possibilités.

Exercice d'application 69. A partir d'un alphabet de p lettres, combien de mots de n lettres peut-on former qui ne contiennent jamais deux lettres identiques consécutives ?

$\hookrightarrow$ Pour la première lettre, on peut choisir n'importe quelle lettre de l'alphabet : il y a p possibilités. Pour les lettres suivantes, on n'a plus que $p-1$ choix possibles si on veut éviter que deux lettres consécutives soient identiques. Au total, il y a donc $p(p-1)^{n-1}$ mots.

◇◇

◇◇

Remarque technique 70. On peut utiliser la Proposition 62 lorsqu'on est dans une situation ou l'on fait **soit** quelque chose, **soit** autre chose.

Exercice d'application 71. Une urne contient $2n$ boules numérotées de 1 à $2n$ qu'on tire successivement sans remise. Combien de tirages peut-on faire pour lesquels un numéro pair est toujours suivi d'un numéro impair et un numéro impair d'un numéro pair ?

$\hookrightarrow$ Il y a seulement deux types de tirages : ceux qui commencent par un numéro pair, et ceux qui commencent par un numéro impair. Nous allons dénombrer séparément ces deux ensembles de tirages et nous additionnerons à la fin les deux cardinaux obtenus.

Combien sont-ils à commencer par un numéro pair ? Faire un tel tirage, c'est tirer une boule paire (n possibilités), puis une boule impaire (n possibilités), puis de nouveau une boule paire ($n-1$ possibilités), puis une boule impaire ($n-1$ possibilités), etc. D'où un total de $n^2 \times (n-1)^2 \times \cdots \times 2^2 \times 1^2 = n!^2$ tirages.

Un raisonnement analogue montre que $n!^2$ tirages exactement commencent par un numéro impair.

Finalement, le nombre total de tirages est $n!^2 + n!^2 = 2 \times n!^2$.

◇◇

Exercice d'application 72. Soit $n \in \mathbf{N}^\star$. Dans une salle ayant n places, de combien de manières peut-on placer n élèves ?

$\hookrightarrow$ Imaginons (artificiellement) que les élèves arrivent l'un après l'autre (ce qui revient à les numéroter). Le placement peut être décrit par les étapes suivantes :

- choix de la place pour le premier élève : n possibilités ;
- choix de la place pour le deuxième élève : $n-1$ possibilités (il n'y a plus que $n-1$ places libres) ;
- choix de la place pour le troisième élève : $n-2$ possibilités ;

- ⋮
- choix de la place pour l'avant-dernier élève : 2 possibilités ;
- choix de la place pour le dernier élève : 1 possibilité.

Au total, il y a donc $n!$ placements possibles.
On a utilisé le principe multiplicatif en numérotant artificiellement les élèves ; on aurait pu également raisonner sur les tables et non sur les élèves :

- choix de l'élève pour la première table : n possibilités ;
- choix de l'élève pour la deuxième table : $n-1$ possibilités ;
- ⋮
- choix de l'élève pour l'avant-dernière table : 2 possibilités ;
- choix de l'élève pour la dernière table : 1 possibilité.

Exercice d'application 73. Dans une classe de 47 places, de combien de manières peut-on placer 41 élèves ?

↪ Raisonnons sur les élèves que l'on numérote artificiellement :

- choix de la table pour le premier élève : 47 possibilités ;
- choix de la table pour le deuxième élève : 46 possibilités ;
- ⋮
- choix de la table pour l'avant-dernier élève : 8 possibilités ;
- choix de la table pour le dernier élève : 7 possibilités.

Il y a donc $47 \times 46 \times \cdots \times 8 \times 7 = \dfrac{47!}{6!}$ façons de placer les élèves.

Aurait-on pu ici raisonner sur les tables ?
C'est possible, mais il faut commencer par choisir les 6 tables qui resteront inoccupées : appelons x le nombre de façons de choisir 6 tables parmi 47.
Le nombre de manières de placer les 41 élèves dans la salle est décrit par les étapes :

- choix des 6 places inoccupées : x possibilités ;
- choix de l'élève pour la première table non vide : 41 possibilités ;
- choix de l'élève pour la deuxième table non vide : 40 possibilités ;
- ⋮
- choix de l'élève pour l'avant-dernière table non vide : 2 possibilités ;
- choix de l'élève pour la dernière table non vide : 1 possibilité.

Au total, on obtient donc $x \times 41!$ façons de placer les élèves.

Puisqu'on a dénombré de deux manières le même ensemble, on en déduit que $x = \dfrac{47!}{6!41!}$. Il y a donc $\binom{47}{6}$ façons de choisir un ensemble de 6 tables dans une salle en contenant 47.

Pour l'instant nous avons vu le cardinal de la réunion d'ensembles disjoints. La proposition suivante traite le cas général :

Proposition 74.

Soit A et B deux ensembles finis. L'ensemble $A \cup B$ est fini et

$$\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B).$$

Démonstration.

• L'ensemble $A\backslash B$ est un sous-ensemble de A donc $A\backslash B$ est un ensemble fini. Comme $A \cup B = (A\backslash B) \cup B$, et que $A\backslash B$ et B sont disjoints, d'après la proposition 2, $A \cup B$ est fini.

• On a les égalités suivantes :

$$A \cup B = (A\backslash B) \cup B \qquad \text{et} \qquad A = (A\backslash B) \cup (A \cap B)$$

où chacune des réunions est une réunion d'ensembles disjoints. Ainsi

$$\text{Card}(A \cup B) = \text{Card}(A\backslash B) + \text{Card}(B) \qquad \text{et} \qquad \text{Card}(A) = \text{Card}(A\backslash B) + \text{Card}(A \cap B).$$

Le résultat en découle aisément. □

2.3. Produit cartésien et listes

Proposition 75.

Soit A et B deux ensembles finis non vides. L'ensemble $A \times B$ est fini et

$$\text{Card}(A \times B) = \text{Card}(A)\,\text{Card}(B).$$

Démonstration.
On note n et m les cardinaux respectifs de A et B.

On peut écrire $A = \{a_1, \ldots, a_n\}$ et

$$A \times B = \bigcup_{k=1}^{n} \{a_k\} \times B$$

qui est une réunion d'ensembles deux à deux disjoints. $\text{Card}(\{a_k\} \times B) = \text{Card}(B) = m$ donc $A \times B$ est la réunion disjointe de n ensembles de cardinal m d'où le résultat. □

Corollaire 76.

Soit $p \in \mathbf{N}^\star$ et A_1, A_2, ..., A_p p ensembles finis. Alors

$$\text{Card}(A_1 \times A_2 \times \cdots A_p) = \text{Card}(A_1) \times \text{Card}(A_2) \times \cdots \times \text{Card}(A_p).$$

Démonstration.
On peut le démontrer par récurrence, en utilisant la proposition précédente. □

Corollaire 77.

Soit $p \in \mathbf{N}^\star$ et A un ensemble fini. L'ensemble A^p est fini et

$$\text{Card}(A^p) = \big(\text{Card}(A)\big)^p.$$

Démonstration.
Immédiat en choisissant tous les ensembles égaux à A dans le corollaire précédent. □

Définition 78.

Soie E un ensemble et $p \geqslant 1$ un entier. On appelle $p-$**liste** d'éléments de E ou $p-$**uplet** d'éléments de E un élément de E^p.

Corollaire 79.

Soit E un ensemble à n éléments et $p \geqslant 1$ un entier. Le nombre de $p-$listes ou $p-$uplets d'éléments de E est égal à n^p.

Démonstration.
Conséquence directe du dernier corollaire. □

Remarque 80. Dans une liste, l'ordre des éléments compte. Un même élément peut figurer plusieurs fois dans une liste.

Exemple 81. Dans $E =$ {🕯, 😎, 🍲, ⛄, 🪑}, le triplet (🍲, 🍲, 😎) est une 3-liste.

◇◇

Remarque technique 82. Les listes sont utilisées pour modéliser des tirages **successifs** (car l'ordre compte) et **avec remise** (car les répétitions sont autorisées).

Exercice d'application 83. De combien de façons peut-on tirer cinq cartes successivement avec remise dans un jeu de 52 cartes ?

↪ D'après le Corollaire 79, la réponse est $52^5 = 380\ 204\ 032$.

Exercice d'application 84. Combien y a-t-il de mots de sept lettres contenant le mot « PCSI » (par exemple, « APCSIBC », « CDPCSIE ») ?

↪ Quand le mot « PCSI » apparaît dans un mot de sept lettres, il n'y apparaît qu'une seule fois. Pour construire un mot quelconque de sept lettres contenant le mot « PCSI », on peut donc procéder en deux étapes :

1. On choisit d'abord la position de la première lettre du mot « PCSI ». Il y a quatre possibilités (les positions 1, 2, 3 et 4).
2. On choisit ensuite les autres lettres, ce qui revient à choisir une 3-liste de l'alphabet : il y a 26^3 possibilités.

Finalement, il y a un total de $4 \times 26^3 = 70\ 304$ mots.

◇◇

2.4. Arrangements

On cherche à dénombrer le nombre de $p-$listes (ou $p-$uplets) d'éléments **distincts** dans un ensemble à n éléments.

Définition 85.

Soit E un ensemble et p un entier naturel non nul. On appelle $p-$**arrangement** de E une $p-$liste d'éléments distincts de E.

Exemple 86. Dans $E =$ {🕯, 😎, 🍲, ⛄, 🪑}, les triplets (🕯, 😎, 🍲) et (🍲, 🕯, 😎) sont deux 3-arrangements de E différents (l'ordre compte).

Proposition 87.

Soit E un ensemble fini à n éléments et p un entier naturel inférieur ou égal à n et strictement positif. Le nombre de $p-$arrangements de E vaut

$$n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}$$

Démonstration.
Pour créer un tel $p-$arrangement, on procède de la façon suivante :

- choix du premier élément de l'arrangement (n possibilités) ;
- choix du deuxième élément ($n-1$ possibilités) ;
- $\vdots$
- choix du $p-$ième élément ($n-p+1$ possibilités).

En utilisant le principe du berger, on obtient le résultat voulu. □

Exemple 88. Soit $n \in \mathbf{N}^\star$. Il existe $n!$ façons exactement d'ordonner les n éléments de $[\![1, n]\!]$.

Corollaire 89.

Soit E un ensemble fini de cardinal p et F un ensemble fini de cardinal $n \geqslant p$.
Il y a en tout $n(n-1)\dots(n-p+1) = \dfrac{n!}{(n-p)!}$ injections de E dans F.

Démonstration.
Appelons $x_1, x_2, \dots, x_p$ les éléments de E. Dénombrer les injections de E dans F revient à dénombrer le nombre de $p-$uplets $(f(x_1), f(x_2), \dots, f(x_p))$ d'éléments distincts (*i.e.* le nombre de $p-$arrangements) de F. □

◇◇

Remarque technique 90. Les arrangements sont utilisés pour modéliser des tirages **successifs et sans remise**.

Exercice d'application 91. De combien de façon peut-on tirer cinq cartes successivement sans remise dans un jeu de 52 cartes ?

↪ La Proposition 87 donne directement la réponse : $\dfrac{52!}{(52-5)!} = 52 \times 51 \times 50 \times 49 \times 48 = 311\ 875\ 200$.

Exercice d'application 92. Soit $n \in \mathbf{N}^\star$. De combien de façons peut-on asseoir n personnes

(a) sur un banc rectiligne ?

(b) autour d'une table ronde ?

↪

(a) On peut considérer que les personnes à asseoir sont numérotées de 1 à n. Les asseoir sur un banc rectiligne revient à la énumérer toutes dans un ordre quelconques, *i.e.* à se donner un arrangement quelconque de $[\![1, n]\!]$, d'où un total de $n!$ configurations possibles (cf. Exemple 88).

(b) La différence entre un banc rectiligne et une table ronde, c'est qu'il n'y a pas de premier place autour d'une table ronde : par exemple, on ne change pas la configuration des places assises quand on demande à chaque convive de se déplacer d'une place sur sa droite. pour asseoir n personnes autour d'une table rond, on peut procéder en deux étapes :

   1. on choisit arbitrairement la place de la personne numérotée 1 (on peut considérer qu'il n'y a qu'un seul choix, car la position de cette personne ne changera pas la configuration finale) ;

2. on lui donne des voisins de proche en proche par la droite, ce qui revient à se donner un $(n-1)$-arrangement quelconque de $[\![2, n]\!]$ (il y a donc $(n-1)!$ possibilités).

Au total, il y a $(n-1)!$ configurations possibles.

◇◇

2.5. Combinaisons

On rappelle que pour tout $(n, p) \in \mathbf{N}^2$, $\displaystyle\binom{n}{p}$ vaut 0 si $p > n$ et $\displaystyle\frac{n!}{p!(n-p)!}$ si $p \leqslant n$.

Définition 93.

Soit $p \in \mathbf{N}$. On pose $n = \text{Card}(E)$.
On appelle $p-$**combinaison** de E toute partie de E de cardinal p.

Exemple 94. Dans $E = \{$🕯, 😎, 🍲, ☃, 🪑$\}$, les ensembles $\{$🕯, 😎, 🍲$\}$, $\{$🍲, 🕯, 😎$\}$ et $\{$🍲, 🍲, 🕯, 😎$\}$ désignent les mêmes $3-$combinaisons (l'ordre ne compte pas).

Théorème 95.

Soit $p \in \mathbf{N}$. On pose $n = \text{Card}(E)$.
Il existe $\displaystyle\binom{n}{p}$ $p-$combinaisons de E.

Démonstration.
Pour $p \leqslant n$, notons C_n^p le nombre de $p-$combinaisons de E. Nous voulons montrer que $C_n^p = \frac{n!}{p!(n-p)!}$, *i.e.* que $\frac{n!}{(n-p)!} = C_n^p \times p!$. A gauche de cette égalité, nous reconnaissons le nombre de $p-$arrangements de E. Il nous suffit dès lors de compter d'une autre manière les $p-$arrangements de E :

1. on commence par choisir une $p-$combinaisons X quelconque de E, *i.e.* une partie de E de cardinal p. Il y a C_n^p possibilités ;
2. on choisit ensuite une façon d'ordonner les p éléments de X. Il y a $p!$ possibilités.

Au total, il y a donc $C_n^p \times p!$ $p-$arrangements de E. □

Dans une combinaison, qui est un ensemble et non une famille, les éléments sont donnés sans ordre. Ainsi :

◇◇

Remarque technique 96. Les combinaisons sont utilisées pour modéliser des tirages **simultanés**.

Exercice d'application 97. De combien de façons peut-on tirer cinq cartes simultanément dans un jeu de 52 cartes ?

$\hookrightarrow$ La réponse est $\binom{52}{5} = 2\ 598\ 960$.

Exercice d'application 98. On appelle **anagramme** d'un mot tout autre mot composé des mêmes lettres mais dans un ordre quelconque. Par exemple, une anagramme de « GALILEE » est « EGAILLE ». Une autre anagramme est aussi « AEEIGLL ».

Combien d'anagrammes du mot « BOROROS » (peuple amérindien du Brésil) existe-t-il ?

$\hookrightarrow$ Pour construire une anagramme de « BOROROS », on peut choisir d'abord la position des « O » (il y a $\binom{7}{3} = 35$ possibilités), puis celles des « R » (il y a $\binom{7-3}{2} = 6$ possibilités), puis celle du « B »

($\binom{2}{1} = 2$ possibilités) et enfin celle du « S » ($\binom{1}{1} = 1$ possibilité ; il ne reste plus qu'une place). D'où un total de $35 \times 6 \times 2 = 420$ anagrammes possibles.

Exercice d'application 99. Un jeu de tarot contient 78 cartes : 21 atouts, la carte que l'on appelle l'« excuse » et 14 cartes de chacune des 4 couleurs cœur, pique, trèfle et carreau. Combien de tirages simultanés de six cartes contiennent :

(a) 2 atouts et 4 trèfles ?

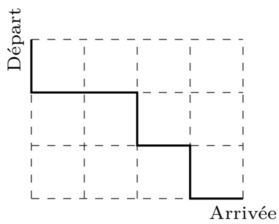
(b) exactement un atout et au moins 3 as ?

$\hookrightarrow$

(a) On choisit 2 atouts ($\binom{21}{2}$ possibilités) puis 4 trèfles ($\binom{14}{4}$ possibilités), d'où un total de $\binom{21}{2} \times \binom{14}{4} = 210\ 210$ tirages possibles.

(b) On peut construire $\binom{21}{1} \times \binom{4}{3} \times \binom{78-21-4}{2} = 115\ 752$ tirages contenant exactement un atout et exactement trois as. De plus, on peut construire $\binom{21}{1} \times \binom{4}{4} \times \binom{78-21-4}{1} = 1\ 113$ tirages contenant exactement un atout et les 4 as. Les deux alternatives étant disjointes, on obtient un total de $115\ 752 + 1\ 113 = 116\ 865$ tirages possibles.

Exercice d'application 100. Soit $(n, p) \in (\mathbf{N}^\star)^2$. Une fourmi se déplace sur une grille contenant n lignes et p colonnes (une représentation pour $n = 3$ et $p = 4$ est donnée ci-contre). Le départ est au coin supérieur gauche, et l'arrivée au coin inférieur droit. Combien de chemins de longueur minimale peut-elle emprunter pour gagner le point d'arrivée depuis son point de départ ?



$\hookrightarrow$ Un chemin de longueur minimale est ici entièrement déterminé par la donnée de n déplacements élémentaires vers le bas et p vers la droite. Tout chemin peut donc être identifié à un mot quelconque de $n + p$ lettres, donc n « B » (bas) et p « D » (droite). Le problème revient donc à déterminer le nombre de tels mots.

Il existe autant de tels mots que de façons de placer les « B », *i.e.* $\binom{n+p}{p}$.

Exercice d'application 101. Soit $(n, p) \in (\mathbf{N}^\star)^2$. On dispose de n urnes numérotées de 1 à n, dont chacune peut accueillir autant de boules qu'on le souhaite. De combien de manières peut-on y ranger p boules indiscernables ? Une représentation du problème pour $n = 4$ et $p = 10$ est donnée ci-après.

$\hookrightarrow$ Les rangements étudiés peuvent être vus sans ambiguïté comme des mots. On traduira par l'exemple la représentation ci-avant par le mot « $\circ\circ\circ|\circ\circ\circ\circ\circ\circ||\circ$ », dans lequel le symbole « $\circ$ » désigne une boule et le symbole « $|$ » la séparation de deux urnes successives. Les mots ainsi formés contiennent tous exactement p symboles « $\circ$ » et $n - 1$ symboles « $|$ » (attention : il y a n urnes, mais seulement $n - 1$ séparations entre elles). On s'est ainsi ramené à un simple problème de dénombrement d'anagrammes. Inversement, il est possible d'associer à tout anagramme de cette forme un unique rangement de boules.

En conclusion, le problème posé autorise exactement $\binom{n+p-1}{p}$ rangements ou anagrammes.

◇◇

2.6. Bilan pratique pour les exercices de dénombrement

En pratique, un problème de dénombrement peut être compliqué, mais il y a tout de même une trinité merveilleuse de modèles de base auxquels on peut presque toujours se ramener :

Propriétés de l'objet à dénombrer		Modélisé par	Exemple fondamental	Écriture
Ordre	Éléments tous distincts			
Non	Oui	Parties d'un ensemble E : on utilise des combinaisons	Tirages simultanés	$\{\ldots;\ldots;\ldots\}$
Oui	Non	$p-$uplets d'éléments d'un même ensemble E : on utilise des listes	Tirages successifs avec remise	$(\ldots;\ldots;\ldots)$
Oui	Oui	$p-$uplets d'éléments d'un même ensemble E, sans répétition : on utilise des arrangements	Tirages successifs sans remise	$(\ldots;\ldots;\ldots)$
Non	Non	On modifie la modélisation pour se ramener à l'un des trois cas précédents		

Exercice d'application 102. Combien y a-t-il de codes de 3 symboles commençant par 2 chiffres et se terminant par une lettre ?

↪ Un tel code est construit par étapes :

- choix d'un premier chiffre : 10 possibilités (c'est le nombre de chiffres entre 0 et 9) ;
- choix d'un deuxième chiffre : 10 possibilités ;
- choix d'une lettre : 26 possibilités.

Il y a donc $10 \times 10 \times 26$ codes possibles.

Exercice d'application 103. Combien y a-t-il de codes de trois chiffres deux à deux distincts ?

↪ Un tel code est construit par étapes :

- choix d'un premier chiffre : 10 possibilités ;
- choix d'un deuxième chiffre : 9 possibilités (car distinct du premier) ;
- choix d'un troisième chiffre : 8 possibilités (car distinct des deux premiers).

Il y a donc $10 \times 9 \times 8$ codes possibles.

Exercice d'application 104. Combien y a-t-il de codes de trois chiffres comportant au moins deux chiffres pairs ?

↪ Ces codes sont de deux types : ceux contenant exactement deux chiffres pairs (type 1), et ceux contenant exactement trois chiffres pairs (type 2).
Les codes du type 1 sont décrits par étapes :

- choix de la place du chiffre impair : 3 possibilités ;
- choix du chiffre impair : 5 possibilités ;
- choix du premier chiffre pair : 5 possibilités ;
- choix du deuxième chiffre pair : 5 possibilités.

Il y a donc 3×5^3 codes du type 1.

Les codes du type 2 sont eux aussi décrits par étape, chacune consistant à choisir un chiffre pair et comportant 5 possibilités ; il y a donc 5^3 codes du type 2.

Finalement, puisqu'il ne peut y avoir des codes de type 1 et 2 à la fois, il y a $3 \times 5^3 + 5^3$ codes de trois chiffres comportant au moins deux chiffres pairs.

Remarque technique 105.** Il est parfois plus simple de dénombrer le complémentaire d'un ensemble plutôt que l'ensemble lui-même : on utilise alors la formule $\text{Card}(E \setminus A) = \text{Card}(E) - \text{Card}(A)$ valable si $A \subset E$.

Exercice d'application 106. Dénombrer les codes de trois chiffres comportant au moins un chiffre pair.

↪ Le complémentaire est formé par les codes ne comportant aucun chiffre pair, c'est-à-dire les codes de trois chiffres impairs. Un tel code est construit par étapes :

- choix d'un premier chiffre impair : 5 possibilités ;
- choix d'un deuxième chiffre impair : 5 possibilités ;
- choix d'un troisième chiffre impair : 5 possibilités.

Il y a donc 5^3 codes ne comportant aucun chiffre pair. De même, on dénombre 10^3 codes de trois chiffres. Ainsi, il y a $10^3 - 5^3$ codes de trois chiffres comportant au moins un chiffre pair.

2.7. Démonstrations combinatoires de quelques formules déjà établies

Proposition 107 - Formule du capitaine.

Soit $n \in \mathbf{N}^\star$, soit $p \in [\![1, n]\!]$.

$$p\binom{n}{p} = n\binom{n-1}{p-1}.$$

Démonstration.
Pour établir cette formule, nous allons résoudre de deux manières le problème suivant : « de combien de manières peut-on former, à partir de n personnes, un équipe de p d'entre elles dont un capitaine ? ». On notera A la réponse.

- Méthode 1 : on commence par choisir les p membres de l'équipe ($\binom{n}{p}$ possibilités) puis on désigne le capitaine (p possibilités). On a donc $A = p \times \binom{n}{p}$.
- Méthode 2 : on choisit d'abord le capitaine (n possibilités) puis on complète son équipe en choisissant les $p-1$ autres membres de l'équipe ($\binom{n-1}{p-1}$ possibilités). Ainsi $A = n \times \binom{n}{p}$.

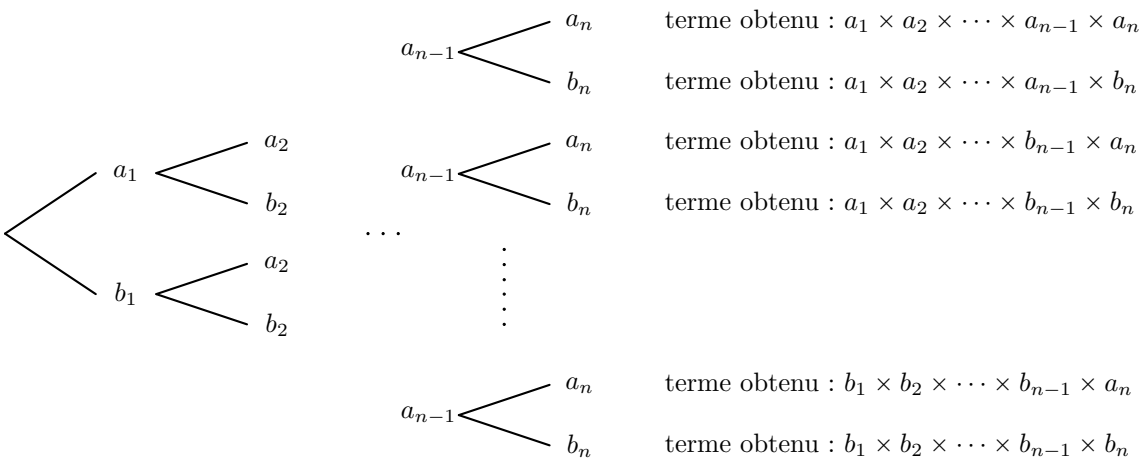
Finalement, $p\binom{n}{p} = n\binom{n-1}{p-1}$. □

Proposition 108 - Formule du binôme de Newton.

Soit $n \in \mathbf{N}^\star$ et $(a, b) \in \mathbf{C}^2$.

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration.
Soit $a, b \in \mathbf{C}$, soit $n \in \mathbf{N}^\star$ (la formule est clairement vraie pour $n = 0$). Posons pour $i \in [\![1, n]\!]$, $a_i = a$ et $b_i = b$.
Alors $(a+b)^n = (a_1 + b_1)(a_2 + b_2)\dots(a_n + b_n)$ et développer ce produit, c'est faire la somme de tous les termes obtenus en faisant les produits des éléments de chaque branche de l'arbre suivant :



Puisque tous les b_i sont égaux à b et tous les a_i sont égaux à a, les termes sont tous des produits de n facteurs égaux à a ou b, ils sont donc du type $a^k b^{n-k}$ avec $k \in [\![0, n]\!]$.
Soit $k \in [\![0, n]\!]$. Combien y a-t-il de termes du type $a^k b^{n-k}$? autant que de façons de choisir les k indices des facteurs a_i apparaissant dans ces produits (les indices des b_i sont alors les indices restants) : il y en a donc $\binom{n}{k}$ (il s'agit de choisir k indices parmi les n possibles).
Finalement, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$. □

Proposition 109 - Formule de Pascal.

Soit $n \in \mathbf{N}^\star$ et $p \in [\![1, n]\!]$.

$$\binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}.$$

Démonstration.
L'idée de la preuve consiste à remarquer qu'il y a deux types (distincts) de $p-$combinaisons de $[\![1, n+1]\!]$: celles qui contiennent $n+1$ et celles qui ne contiennent pas $n+1$.

Plus formellement, notons :

- A l'ensemble des parties de $[\![1, n+1]\!]$ de cardinal p (les $p-$combinaisons de $[\![1, n+1]\!]$) ;
- B l'ensemble des parties de $[\![1, n+1]\!]$ de cardinal p contenant $n+1$ (les $p-$combinaisons de $[\![1, n+1]\!]$ qui contiennent $n+1$) ;
- C l'ensemble des parties de $[\![1, n+1]\!]$ de cardinal p ne contenant pas $n+1$ (les $p-$combinaisons de $[\![1, n+1]\!]$ qui ne contiennent pas $n+1$).

On a immédiatement $\text{Card}(A) = \binom{n+1}{p}$ (nombre $p-$arrangements d'un ensemble contenant $n+1$ éléments). De plus, les éléments de C sont les parties de $[\![1, n]\!]$ de cardinal p, d'où $\text{Card}(C) = \binom{n}{p}$ (nombre de $p-$arrangements d'un ensemble contenant n éléments).

Les éléments de B sont les parties de $[\![1, n+1]\!]$ de cardinal p contenant $n+1$. Il y en a autant que de façons de choisir les $p-1$ autres éléments de la partie. Ainsi $\text{Card}(B) = \binom{n}{p-1}$ (nombre de $(p-1)-$arrangements d'un ensemble contenant n éléments).

Puisque $B \cap C = \varnothing$, on a $\text{Card}(A) = \text{Card}(B) + \text{Card}(C)$, et on reconnaît la formule de Pascal. □

2.8. Applications d'un ensemble fini dans un ensemble fini

Lemme 110.

Soit E un ensemble fini. L'application $\varphi : \begin{array}{ccc} \mathcal{P}(E) & \longrightarrow & \mathcal{F}(E,\{0,1\}) \\ A & \longmapsto & \mathbf{1}_A \end{array}$ est une bijection.

Démonstration.

- *Injectivité.* Soit A et B deux parties de E. Supposons que $\varphi(A) = \varphi(B)$ c'est-à-dire $\mathbf{1}_A = \mathbf{1}_B$. Alors pour tout $x \in E$, si $x \in A$ alors $\mathbf{1}_A(x) = 1$ donc $\mathbf{1}_B(x) = 1$ donc $x \in B$ et de même si $x \in B$, alors $x \in A$. Donc $A = B$.
- *Surjectivité.* Soit $f \in \mathcal{F}(E,\{0,1\})$. Posons $A = f^{-1}(\{1\})$ Alors pour tout $x \in E$, si $x \in A$ alors $\mathbf{1}_A(x) = 1 = f(x)$ et si $x \notin A$, $\mathbf{1}_A(x) = 0 = f(x)$ donc $f = \mathbf{1}_A$ donc $f = \varphi(A)$. □

Théorème 111 - Nombre de parties d'un ensemble.

Si E est un ensemble fini de cardinal n, alors $\mathcal{P}(E)$ est un ensemble fini et $\text{Card}(\mathcal{P}(E)) = 2^n$.

Démonstration.
Il suffit d'utiliser le lemme : puisque φ est une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E,\{0,1\})$ et puisque $\mathcal{F}(E,\{0,1\})$ est un ensemble fini de cardinal 2^n, on peut affirmer que $\mathcal{P}(E)$ est un ensemble fini de cardinal 2^n. □

Théorème 112.

Soit E et F deux ensembles finis de même cardinal et f une application de E dans F. Les propriétés suivantes sont équivalentes :

(i) l'application f est injective ;

(ii) l'application f est surjective ;

(iii) l'application f est bijective.

Démonstration.
Si f est injective, alors $\text{Card}(f(E)) = \text{Card}(E)$ donc $\text{Card}(f(E)) = \text{Card}(F)$ et donc f est aussi surjective donc bijective.

Si f est surjective, alors $\text{Card}(f(E)) = \text{Card}(F)$ donc $\text{Card}(f(E)) = \text{Card}(E)$ et donc f est aussi injective donc bijective.

□

Remarque 113. On peut montrer que si E et F sont deux ensembles tels que F soit un ensemble fini, et s'il existe une injection de E vers F, alors E est fini et $\text{Card}(E) \leqslant \text{Card}(F)$. En particulier, si un ensemble fini A est en bijection avec un autre ensemble B, alors B est fini et de même cardinal que A.

Proposition 114 - Nombre d'applications.

Si E et F sont deux ensembles finis non vides, alors le nombre d'applications de E dans F est un ensemble fini et $\text{Card}(F^E) = \text{Card}(F)^{\text{Card}(E)}$.

Démonstration.
Notons $p = \text{Card}\,(E)$ et $n = \text{Card}(F)$. On veut montrer que $\text{Card}(\mathcal{F}(E,F)) = n^p$.

On note $E = \{a_1, a_2, \ldots, a_p\}$. On dénombre les applications de E dans F :

- étape 1 : on choisit l'image de a_1 (il y a n possibilités) ;
- étape 2 : on choisit l'image de a_2 (il y a n possibilités) ;
- $\vdots$
- étape p : on choisit l'image de a_p (il y a n possibilités).

Finalement, pour définir une application de E dans F, on a fait p étapes avec pour chacune n possibilités, donc il y a en tout $\underbrace{n \times n \times \cdots \times n}_{p \text{ fois}} = n^p$ applications de E dans F. □

Proposition 115 - Nombre d'applications injectives.

Soit E et F deux ensembles finis, dont on note n et p les cardinaux respectifs. On suppose $p \leqslant n$. L'ensemble des applications injectives de E dans F est de cardinal $\frac{n!}{(n-p)!}$.

Démonstration.
Notons $E = \{a_1, ..., a_p\}$. On dénombre les applications injectives de E dans F :

- étape 1 : on choisit l'image de a_1 (il y a n possibilités) ;
- étape 2 : on choisit l'image de a_2 parmi les images non encore sélectionnées (il y a $n-1$ possibilités) ;
- étape 3 : on choisit l'image de a_3 parmi les images non encore sélectionnées (il y a $n-2$ possibilités) ;
- $\vdots$
- étape p : on choisit l'image de a_p parmi les images non encore sélectionnées (il y a $n-p+1$ possibilités).

Finalement, il y a $n \times (n-1) \times \cdots \times (n-p+1) = \frac{n!}{(n-p)!}$ façons de construire une application injective. □

Remarque 116. Dans la proposition précédente, si $n > p$, il n'y a pas d'application injective de E dans F.

Définition 117.

Soit E un ensemble fini non vide. On appelle **permutation** de E toute bijection de E dans E.

Exemple 118. Soit $E = \{$🕴, 😎, 🍩, 💐, 🚵$\}$. L'application $\sigma : E \longrightarrow E$ définie par $\sigma($🕴$) =$ 🍩, $\sigma($😎$) =$ 🕴, $\sigma($🍩$) =$ 😎, $\sigma($💐$) =$ 💐 et $\sigma($🚵$) =$ 🚵 est une permutation de E.

Proposition 119 - Nombre de bijections.

Si E est un ensemble fini non vide de cardinal $n > 0$, alors le nombre de permutations de E est égal à $n!$.

Démonstration.
Notons n le cardinal commun de E et F. On note $E = \{a_1, a_2, \ldots, a_n\}$. On dénombre les bijections de E dans E :

- étape 1 : on choisit l'image de a_1 (il y a n possibilités) ;
- étape 2 : on choisit l'image de a_2 (il y a $n-1$ possibilités, car l'application doit être injective) ;
- $\vdots$
- étape n : on choisit l'image de a_n (il y a $n-n+1=1$ possibilités).

Finalement, il y a $n\times(n-1)\times\cdots\times(n-n+1)=n!$ façons de construire une application bijective. □

Exercice d'application 120. On considère le digicode d'une porte d'entrée contenant les touches A, B, C et D. Sachant que le code de la porte est constitué des quatre lettres qui doivent être tapées exactement une fois, combien y-a-t-il de combinaisons possibles ?

↪ Le nombre de combinaisons correspond au nombre de permutation d'un ensemble à quatre éléments, à savoir $4!=24$ possibilités.

Exercice d'application 121. Soit $n\geqslant 3$. Combien y a-t-il de permutations de $[\![1,n]\!]$ qui envoient 1 sur 2 et 2 sur 3 ?

↪ Pour construire une telle permutation, on peut choisir l'image de 3 ($n-2$ possibilités), puis celle de 4 ($n-3$ possibilités), ... et enfin celle de n (1 possibilité). Ainsi, il y a $(n-2)\times(n-3)\times\cdots\times 1=(n-2)!$ permutations qui répondent à la question.

2.9. Cardinaux infinis (hors-programme)

Compter les éléments d'un ensemble fini non vide (de cardinal n) consiste à établir une bijection de $[\![1,n]\!]$ dans cet ensemble, ce qui revient à numéroter de 1 à n les éléments de cet ensemble. C'est avec cette idée qu'on peut prolonger la notion de cardinal aux ensembles infinis (bijection avec $\mathbf{N}$, $\mathbf{R}$) :

Définition 122.

Soit E un ensemble.
On dit que E est infini **dénombrable** si il existe une bijection entre $\mathbf{N}$ et E.
On dit que E est **indénombrable** si il n'est ni fini ni dénombrable.

Intuitivement, un ensemble dénombrable est donc un ensemble dont on peut numéroter les éléments.

Remarque 123. Pour montrer qu'un ensemble E est dénombrable, on peut montrer qu'il est en bijection avec un autre ensemble F dénombrable.

En effet, si F est dénombrable, il existe une bijection $f:F\to\mathbf{N}$. S'il existe une bijection $g:E\to F$, alors $f\circ g:E\to\mathbf{N}$ est une bijection.

Le résultat suivant est fondamental dans la théorie des cardinaux infinis, mais difficile à démontrer.

Théorème 124 - Théorème de Cantor-Bernstein.

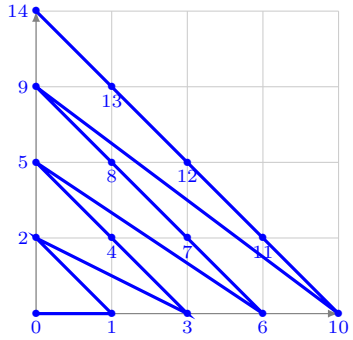
Soient E et F des ensembles. S'il existe une injection $E\to F$ et une injection $F\to E$, alors il existe une bijection entre E et F.

Proposition 125.

$\mathbf{Z}$ et $\mathbf{Q}$ sont dénombrables. Pour tout $k\geqslant 2$, $\mathbf{N}^k,\mathbf{Z}^k,\mathbf{Q}^k$ sont dénombrables.

Démonstration (idées de preuve). 1. Soit $\psi : \begin{array}{ccc} \mathbf{N}^2 & \longrightarrow & \mathbf{N} \\ (a,b) & \longmapsto & \begin{cases} 0 & \text{si} \quad (a,b)=(0,0) \\ \left(\sum_{k=0}^{a+b} k\right)+b & \text{sinon} \end{cases} \end{array}$.

On peut montrer que ψ est une bijection.



2. Pour tout $k \geqslant 3$, on pose $f_k : \begin{array}{ccc} \mathbf{N}^k & \longrightarrow & \mathbf{N}^{k-1} \\ (x_1,\dots,x_n) & \longmapsto & (\psi(x_1,x_2),x_3,\dots,x_n) \end{array}$. f_k est bijective car ψ l'est :
   (a) soient $(a,x_3,x_4,\dots,x_n) \in \mathbf{N}^{k-1}$. ψ est surjective donc il existe $(x_1,x_2) \in \mathbf{N}^2$ tel que $\psi(x_1,x_2)=a$. Donc $f_k(x_1,x_2,\dots,x_n)=(a,x_3,\dots,x_n)$.
   Tout élément de $\mathbf{N}^{k-1}$ a un antécédent par f_k donc f_k est surjective.
   (b) soient $(x_1,\dots,x_n)$, $(y_1,\dots,y_n)$ dans $\mathbf{N}^k$ tels que $\psi(x_1,\dots,x_n)=\psi(y_1,\dots,y_n)$. On a alors $\psi(x_1,x_2)=\psi(y_1,y_2)$ et pour tout $k \geqslant 3$, $x_k=y_k$.
   Comme ψ est injective, $(x_1,x_2)=(y_1,y_2)$.
   Donc f_k est injective.

   Donc, par récurrence, tous les $\mathbf{N}^k$ sont en bijection avec $\mathbf{N}^2$, donc sont dénombrables.
3. Soit $\varphi : \begin{array}{ccc} \mathbf{N} & \longrightarrow & \mathbf{Z} \\ 0 & \longmapsto & 0 \\ n & \longmapsto & (-1)^n \left\lfloor \dfrac{n+1}{2} \right\rfloor \end{array}$.

   $\forall y \in \mathbf{Z}$, si $y<0$, alors $\varphi(-2y-1)=(-1)^{-2y-1}\left\lfloor \dfrac{(-2y-1)+1}{2} \right\rfloor = -\lfloor -y \rfloor = y$.

   Si $y>0$, alors $\varphi(2y)=(-1)^{2y}\left\lfloor \dfrac{2y+1}{2} \right\rfloor = y$. Dans tous les cas, $y \in \mathrm{Im}(\varphi)$, donc φ est surjective.

   $\varphi(0)=0$. $n \mapsto \varphi(2n)$ est strictement croissante (et donc positive), donc injective. $n \mapsto \varphi(2n+1)$ est strictement décroissante (donc négative), donc injective.
   Donc φ est injective. $\mathbf{Z}$ est bien en bijection avec $\mathbf{N}$.
4. Pour tout $k \geqslant 2$, $\begin{array}{ccc} \mathbf{Z}^k & \longrightarrow & \mathbf{N}^k \\ (x_1,\dots,x_n) & \longmapsto & (\varphi(x_1),\dots,\varphi(x_n)) \end{array}$ est bijective. Donc $\mathbf{Z}^k$ est dénombrable.
5. Montrer que $\mathbf{Q}$ est dénombrable est un peu plus technique. On peut facilement construire une injection φ_1 de $\mathbf{Q}$ dans $\mathbf{N}^2$. A tout élément $x \in \mathbf{Q}$, on associe $\varphi_1(x)=(a,b)$ tel que a et b soient premiers entre eux et $x=a/b$.
   Il est encore plus simple de construire une injection de $\mathbf{N}$ dans $\mathbf{Q}$: il suffit de prendre φ_2 : $\begin{array}{ccc} \mathbf{N} & \longrightarrow & \mathbf{Q} \\ x & \longmapsto & x \end{array}$. On conclut par le théorème de Cantor-Bernstein.
6. Pour tout $k \geqslant 2$, $\begin{array}{ccc} \mathbf{Q}^k & \longrightarrow & \mathbf{N}^k \\ (x_1,\dots,x_n) & \longmapsto & (\varphi_2(x_1),\dots,\varphi_2(x_n)) \end{array}$ est bijective. Donc $\mathbf{Q}^k$ est dénombrable.

□

Proposition 126.

$\mathbf{R}$ est indénombrable.

Démonstration.
Cette preuve s'appelle l'**argument diagonal de Cantor**.

Supposons que $\mathbf{R}$ soit dénombrable. Cela signifie que l'on peut numéroter tous les réels : $x_0, x_1, x_2, \dots$. Autrement dit, $\mathbf{R} = \{x_k \mid k \in \mathbf{N}\}$.

On note a_i la partie entière de x_i et $b_1^i, b_2^i, b_3^i, \dots$ les chiffres successifs apparaissant après la virgule dans l'écriture décimale de a_i.

Soit alors le nombre réel y défini de la manière suivante : sa partie entière est $a_0 + 1$, puis le i-ème chiffre après la virgule de son écriture décimale est 1 si $b_i^i = 0$ et 0 si $b_i^i \geqslant 1$.

Ainsi, y est différent de x_0, car sa partie entière n'est pas celle de x_0. Il est aussi différent de x_i pour tout $i > 1$, car au moins une des décimales de leur écriture décimale est différente (et y ne se termine pas par une succession infinie de 9). Donc $y \notin \mathbf{R}$, ce qui est absurde. □

Illustration de l'argument diagonal sur un exemple :

$$\begin{array}{lccccccc}
a_0 = & \boxed{11}, & 7 & 6 & 4 & 0 & \cdots \\
a_1 = & 2, & \boxed{2} & 4 & 4 & 9 & \cdots \\
a_2 = & 1, & 6 & \boxed{0} & 3 & 1 & \cdots \\
a_3 = & 0, & 5 & 3 & \boxed{8} & 7 & \cdots \\
a_4 = & 12, & 8 & 1 & 0 & \boxed{6} & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
y = & 15, & 0 & 1 & 0 & 0 & \cdots
\end{array}$$

Théorème 127 - Théorème de Cantor.

Pour tout ensemble E, E et $\mathcal{P}(E)$ ne sont pas en bijection.

Démonstration.
Soit $f : E \to \mathcal{P}(E)$ une application. On pose

$$D = \{x \in E \mid x \notin f(x)\}.$$

Supposons qu'il existe $x \in E$ tel que $f(x) = D$.

Si $x \in D$, alors $x \notin f(x) = D$. Donc $x \notin D$. Absurde.

Si $x \notin D$, alors $x \in f(x) = D$. Donc $x \in D$. Absurde.

Donc D n'a pas d'antécédent par f. Il n'existe donc aucune surjection de E dans $\mathcal{P}(E)$. □

Conséquence : il n'existe pas de « plus grand cardinal », vu que tout ensemble est « plus petit » que l'ensemble de ses parties.

Terminons cette partie culturelle avec un énoncé dit indécidable : il a été prouvé qu'il est cohérent avec le reste des mathématiques, mais aussi que sa négation le serait tout autant. Il est donc impossible de prouver qu'il est vrai ou qu'il est faux.

Hypothèse 128 - Hypothèse du continu.

Tout sous-ensemble de $\mathbf{R}$ est fini, dénombrable, ou en bijection avec $\mathbf{R}$.