Chapitre 14 : Arithmétique et dénombrement

Axiomes de Péano :

- $\mathbb{N}$ est un ensemble non vide, il existe $0 \in \mathbb{N}$, et il existe une application $f : \mathbb{N} \to \mathbb{N}$ tel que
- $f(\mathbb{N}) \subset$
- $\mathbb{N}$ n'est pas majoré ;
- toute partie non vide de $\mathbb{N}$ admet un plut petit élément ;
- toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément .

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

1.1 Divisibilité dans $\mathbb{N}$

Définition

Soit $(a,b) \in \mathbb{N}^2$. On dit que a divise b si et seulement si il existe $c \in \mathbb{N}$ tel que $b = ac$. On note $a|b$.
On dit aussi dans ce cas que a est un diviseur de b ou que b est un multiple de a.

Notation : On notera $\mathscr{D}(b)$ l'ensemble des diviseurs de b dans $\mathbb{N}$.
Remarque :

- $\mathscr{D}(0) = \mathbb{N}$
- $\forall b \in \mathbb{N}, \left(0|b \iff b = 0\right)$

Proposition

Soit $(a,b,c,d) \in \mathbb{N}^4$, soit $n \in \mathbb{N}^*$,

1. Si $a|b$ et $b|c$, alors $a|c$
2. Si $a|b$ et $a|c$, alors : $\forall (p,q) \in \mathbb{N}^2,\ a|(pb+qc)$
3. Si $a|b$ et $b|a$, alors $a = b$ (la réciproque est vraie)
4. Si $a \neq 0$ et si $b|a$, alors $b \leq a$
5. Si $a|b$ et $c|d$, alors : $ac|bd$
6. $an|bn \iff a|b$.

Démonstration.

1. Supposons que $a|b$ et $b|c$. Alors, il existe $k_1, k_2 \in \mathbb{N}$ tels que $b = k_1 a$ et $c = k_2 b$. Ainsi, $c = (k_2 k_1)a$ avec $k_1 k_2 \in \mathbb{N}$.
   Ainsi, a divise c.
2. Supposons que $a|b$ et $a|c$. Alors il existe $k_1, k_2 \in \mathbb{N}$ tels que $b = k_1 a$ et $c = k_2 a$.
   Soient $p, q \in \mathbb{R}$, par somme $pb + qc = (pk_1 + qk_2)a$ avec $pk_1 + qk_2 \in \mathbb{N}$. Donc $a|(pb+qc)$.
3. Supposons que $a|b$ et $b|a$. Alors, il existe $(p,q) \in \mathbb{N}^2$ tel que $a = bp$ et $b = aq$. On en déduit donc que $a = bp = apq$.
   D'où $a(1-pq) = 0$. Ainsi, $a = 0$ ou $1 - pq = 0$.
   - Si $a = 0$ alors $b = 0$ car $a|b$ et on a bien le résultat annoncé.
   - $1 = pq$ alors $p = q = 1$ car (car p et q sont des entiers naturels) d'où $b = a$.
4. Supposons que $a \neq 0$ et que $b|a$, alors il existe $n \in \mathbb{N}$ tel que $a = bn$. Puisque $a \neq 0$, on a $n > 0$ donc $n \geq 1$. Ainsi, $bn \geq b$, donc $a \geq b$.
5. Supposons que $a|b$ et $c|d$. Alors il existe $k_1, k_2 \in \mathbb{N}$ tels que $b = k_1 a$ et $d = k_2 c$.
   D'où par produit : $bd = (k_1 a)(k_2 c) = (k_1 k_2)ac$ avec $k_1 k_2 \in \mathbb{N}$ et donc $ac|bd$.
6. $$\begin{aligned} an|bn &\iff \exists k \in \mathbb{N},\ bn = kan \\ &\iff \exists k \in \mathbb{N},\ b = ka \quad (\text{car } n \neq 0) \\ &\iff a|b \end{aligned}$$

□

Exemple : Montrer que pour tout entier naturel impair n, $n^2 - 1$ est multiple de 8.
Soit $n \in \mathbb{N}$ impair. Il existe $k \in \mathbb{N}$ tel que $n = 2k+1$. D'où $n^2 - 1 = 4k(k+1)$. Or, $2|k(k+1)$ car les entiers k et $k+1$ sont deux entiers consécutifs donc l'un d'eux est pair. Ainsi, $2|4k(k+1)$. Ainsi, $8|n^2 - 1$.

Théorème de division euclidienne dans $\mathbb{N}$

Soient $n \in \mathbb{N}$ et $p \in \mathbb{N}^*$. Alors il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que

$$n = pq + r \quad \text{et} \quad 0 \leq r < p.$$

On dit que q est le **quotient** et r le **reste** dans la **division euclidienne** de n par p.

Démonstration. Raisonnons par analyse synthèse :
Analyse :
Supposons qu'il existe $(q,r) \in \mathbb{N}^2$ tel que $n = pq + r$ et $0 \leq r < p$.
On a alors : $\dfrac{n}{p} = q + \dfrac{r}{p}$.
Or, $0 \leq r < p$ donc $0 \leq \dfrac{r}{p} < 1$.
Ainsi, $q \leq \dfrac{n}{p} < q+1$ donc $q = \left\lfloor \dfrac{n}{p} \right\rfloor$.
On a alors : $r = a - p\left\lfloor \dfrac{n}{p} \right\rfloor$.
Synthèse :
Posons $q = \left\lfloor \dfrac{n}{p} \right\rfloor$ et $r = n - pq$.
On a $q \in \mathbb{N}$ et $r \in \mathbb{Z}$.
De plus, $\left\lfloor \dfrac{n}{p} \right\rfloor \leq \dfrac{n}{p} < \left\lfloor \dfrac{n}{p} \right\rfloor + 1$.
Ainsi : $q \leq \dfrac{n}{p} < q+1$.
D'où : $pq \leq n < pq + p$.
Donc $0 \leq r < p$.
Ainsi, q et r conviennent.
Finalement, on a prouvé qu'il existe un unique $(q,r) \in \mathbb{N}^2$ tel que $n = pq + r$ et $0 \leq r < n$. □

Remarque : Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^*$. b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

- $\Rightarrow$ Si b divise a, alors il existe $q \in \mathbb{N}$ tel que $a = bq$. Par unicité dans la division euclidienne, on en déduit que le reste de la division euclidienne de a par b est égal à 0.
- $\Leftarrow$ Supposons que le reste de la division euclidienne de a par b soit nul. Alors il existe q tel que $a = bq + 0 = bq$, et donc b divise a.

1.2 PGCD,PPCM

1.2.1 PGCD

Définition

Soient $a, b \in \mathbb{N}^*$. Il existe un unique $d \in \mathbb{N}^*$ tel que $\begin{cases} d \text{ divise } a \text{ et } b \\ \forall n \in \mathbb{N}, \left(n|a \text{ et } n|b\right) \implies n|d \end{cases}$.
d est appelé Plus Grand Commun Diviseur de a et b et est noté $\text{pgcd}(a,b)$ ou $a \wedge b$.

Remarque : $\text{pgcd}(a,b)$ est le plus grand entier naturel qui divise de a et b pour la relation $\leq$.

- On sait déjà que $\text{pgcd}(a,b)$ est un diviseur de a et b.
- De plus, soit d un diviseur de a et b. Alors $d|a$ et $d|b$. On a alors $d|\text{pgcd}(a,b)$. Or, $\text{pgcd}(a,b) \neq 0$. Donc $d \leq \text{pgcd}(a,b)$.

Exemple : $\mathscr{D}(6) = \{1,2,3,6\}$ et $\mathscr{D}(8) = \{1,2,4,8\}$ donc $\text{pgcd}(6,8) = 2$.

Remarque :

- $a \wedge b = b \wedge a$
- On a : $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$, c'est à dire :

$$\forall n \in \mathbb{N},\ (n|a \text{ et } n|b) \iff n|\text{pgcd}(a,b)$$

- Soient $a, b \in \mathbb{N}^*$.
  On dit que a et b sont premiers entre eux si et seulement si leur seul diviseur commun est 1. Ainsi, a et b sont premiers entre eux si et seulement si $\text{pgcd}(a,b) = 1$.

Lemme

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Si r désigne le reste de la division de a par b, alors :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$$

Démonstration. On effectue la division euclidienne de a par b : $a = bq + r$ avec $0 \leq r < b$. Alors :

- $\subseteq$ si d est un diviseur de a et b, alors $d|a - bq = r$, donc $d|b$ et $d|r$.
- $\supseteq$ si d est un diviseur de b et r, alors $d|bq + r = a$, donc $d|a$ et $d|b$.

□

Algorithme d'Euclide

Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.

- On pose $r_0 = a$ et $r_1 = b$.
- Soit $k \geq 1$, on suppose r_k et r_{k-1} construits.
  Si $r_k > 0$, on effectue alors la division euclidienne de r_{k-1} par r_k :
  $$r_{k-1} = r_k \times q_k + r_{k+1} \text{ avec } 0 \leq r_{k+1} < r_k.$$
  Sous l'hypothèse $r_k > 0$, on a donc défini r_{k+1}, avec $0 \leq r_k < r_{k+1}$.
- La suite $(r_k)_{k \geq 1}$ est une suite strictement décroissante d'entiers naturels et est donc finie.
  Ainsi, il existe donc $N \in \mathbb{N}$ tel que $r_N > 0$ et $r_{N+1} = 0$.

Avec ces notations, on a : $a \wedge b = r_N$.

Proposition

Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.
Le PGCD de a et b est le dernier reste non nul quand on effectue les divisions euclidiennes successives.

Démonstration. En utilisant les notations précédentes, on a :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r_2) = \mathscr{D}(r_N) \cap \mathscr{D}(r_{N+1}) = \mathscr{D}(r_N) \cap \mathscr{D}(0) = \mathscr{D}(r_N) \cap \mathbb{N} = \mathscr{D}(r_N).$$

Ainsi, $r_N \in \mathscr{D}(r_N) = \mathscr{D}(a) \cap \mathscr{D}(b)$ donc $r_N|a$ et $r_N|b$.
De plus, soit $n \in \mathbb{N}$ tel que $n|a$ et $n|b$ alors $n \in \mathscr{D}(a)$ et $n \in \mathscr{D}(b)$ donc $n \in \mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r_N)$. Donc $n|r_N$.
Ainsi, $r_N = a \wedge b$. □

Algorithme

En Python, cela donne :

```
def pgcd(a,b):
    c=b
    while (c>0):
        r=a%c
        a,c=c,r
    return a
```

Exemple : Calculons le pgcd de 164 et 36.
$164 = 4 \times 36 + 20$
$36 = 20 + 16$
$20 = 16 + 4$
$16 = 4 \times 4 + 0$.
Ainsi, $\text{pgcd}(16, 36) = 4$.

Proposition : Homogénéité du PGCD

$$\forall (a, b, c) \in \mathbb{N}^*, \ \text{pgcd}(ca, cb) = c \times \text{pgcd}(a, b)$$

Démonstration. Soient $a,b,c \in \mathbb{N}^*$.

- $c|ac$ et $c|bc$ donc $c|\text{pgcd}(ac,bc)$.
  Ainsi, il existe $k \in \mathbb{N}$ tel que $\text{pgcd}(ac,bc) = kc$.
- Montrons que $k = \text{pgcd}(a,b)$.
  - $kc|\text{pgcd}(ac,bc)$ donc $kc|ac$ et $kc|bc$.
    D'où $k|a$ et $k|b$ car $c \neq 0$.
  - Soit $d \in \mathbb{N}$ tel que $d|a$ et $d|b$.
    Alors, $dc|ac$ et $dc|bc$ donc $dc|\text{pgcd}(ac,bc)$.
    Donc $dc|kc$ d'où $d|k$ car $c \neq 0$.

  Ainsi, $k = \text{pgcd}(a,b)$.

□

1.2.2 PPCM

Définition

Soient $a,b \in \mathbb{N}^*$. Il existe un unique entier $m \in \mathbb{N}^*$ tel que : $\begin{cases} a \text{ et } b \text{ divise } m \text{ (i.e } m \text{ est un multiple de } a \text{ et } b) \\ \forall n \in \mathbb{N}, \left(a|n \text{ et } b|n\right) \implies m|n \end{cases}$.
m est appelé Plus Petit Commun Multiple de a et b et noté $\text{ppcm}(a,b)$ ou $a \vee b$.

Remarque : $\text{ppcm}(a,b)$ est le plus petit entier naturel qui est un multiple de a et b pour la relation $\leq$.

- On sait déjà que $\text{ppcm}(a,b)$ est un multiple de a et b.
- De plus, soit m un multiple non nul de a et b. Alors $a|m$ et $b|m$. On a alors $\text{ppcm}(a,b)|m$. Or, $m \neq 0$. Donc $\text{ppcm}(a,b) \leq m$.

Exemple : Les multiples de 6 dans $\mathbb{N}$ sont : 0,6,12,24,30 ...
Les multiples de 8 dans $\mathbb{N}$ sont : 0,8,16,24,32 ...
Ainsi, $\text{ppcm}(6,8) = 24$.
Remarque :

- $a \vee b = b \vee a$.
- Ainsi : $\forall n \in \mathbb{N}$, $(a|n \text{ et } b|n) \iff \text{ppcm}(a,b)|n$.

Proposition

Pour tout $(a,b) \in (\mathbb{N}^*)^2$, $(a \wedge b) \times (a \vee b) = a \times b$.

Remarque : On sait calculer en pratique le PGCD de deux nombres. Grâce à cette formule, on obtient également un moyen de calculer leur PPCM.

Proposition : Homogénéité du PPCM

$$\forall (a,b,c) \in \mathbb{N}^*, \ \text{ppcm}(ac,bc) = c \times \text{ppcm}(a,b)$$

Démonstration. Soient $a,b,c \in \mathbb{N}^*$.
On a : $\text{ppcm}(ac,bc) \times \text{pgcd}(ac,bc) = acbc$.
Or, par homogénéité du pgcd, on a $\text{pgcd}(ac,bc) = c \times \text{pgcd}(a,b)$.
Donc $\text{ppcm}(ac,bc) \times \text{pgcd}(a,b) \times c = abc^2$.
Comme $c \neq 0$, on en déduit que $\text{ppcm}(ac,bc)\text{pgcd}(a,b) = abc$.
Or, $ab = \text{ppcm}(a,b)\text{pgcd}(a,b)$.
Donc $\text{ppcm}(ac,bc)\text{pgcd}(a,b) = \text{pgcd}(a,b)\text{ppcm}(a,b)c$.
Or, $\text{pgcd}(a,b) \neq 0$ donc $\text{ppcm}(ac,bc) = c \times \text{ppcm}(a,b)$. □

1.3 Nombres premiers

Définition

Un élément $p \in \mathbb{N}$ est dit premier si $p \geq 2$ et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui même.

⚠ 1 n'est pas premier.

Crible D'Eratosthène

L'objectif est de faire la liste des nombres premiers inférieurs à un entier n donné.
Le principe est le suivant :

- On écrit tous les nombres de 2 à n
- On conserve le nombre premier 2 et on raye tous les multiples de 2 (qui ne sont donc pas premiers)
- Pour chaque nombre suivant p non rayé, on conserve p et on raye tous les multiples de p.
- Lorsque l'algorithme s'arrête (on est arrivé à n), tous les nombres non rayés sont les nombres premiers inférieurs ou égaux à n.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~16~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

Proposition

Tout nombre entier $n \geq 2$ possède au moins un diviseur premier.

Démonstration. On le montre par récurrence sur $n \geq 2$.

- Pour $n = 2$, la propriété est vraie puisque 2 est premier.
- Soit $n \geq 2$, supposons que tout nombre premier $k \in [\![2, n]\!]$ admet au moins un diviseur premier.
  - Si $n+1$ est premier, le résultat est établi.
  - Sinon il existe $a, b \in \mathbb{N}$ tels que $n+1 = ab$ avec $2 \leq a, b < n+1$. On applique l'hypothèse de récurrence à a ou b : il existe donc p premier divisant a ou b, et donc $n+1$.

  Ceci prouve la propriété au rang $n+1$.
- Ainsi, tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

□

Proposition (Théorème d'Euclide)

L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Démonstration. Par l'absurde, supposons que l'ensemble des nombres premiers est fini : $\mathbb{P} = \{p_1, p_2, \ldots, p_k\}$.
Considérons alors l'entier $N = \left(\prod_{i=1}^{k} p_i\right) + 1$. Par la proposition précédente, N est divisible par un nombre premier.
Ainsi, il existe $l \in [\![1, k]\!]$ tel que p_l divise N. De plus, p_l divise le produit $\prod_{i=1}^{k} p_i$, donc p_l divise $N - \prod_{i=1}^{k} p_i$. Ainsi, $p_l | 1$.
Ce qui est impossible puisque $p_l \geq 2$. □

Théorème : Décomposition en facteurs premiers

Tout entier supérieur ou égal à 2 admet une décomposition en produit de nombres premiers, unique à l'ordre des facteurs près. Autrement dit , si $n \in \mathbb{N}$ et $n \geq 2$, alors il existe $r \in \mathbb{N}^*$, des nombres premiers deux à deux distincts $p_1, \ldots, p_r$, et des entiers naturels non nuls $\alpha_1, \ldots, \alpha_r$ tels que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.

Exemple :

- Décomposition de 2016 :

2016	2
1008	2
504	2
252	2
126	2
63	3
21	3
7	7
1	

  Ainsi : $2016 = 2^5 \times 3^2 \times 7$.

- Décomposition de 4020 :

4020	2
2010	2
1005	3
335	5
67	67
1	

  De plus, 67 est premier car 67 n'admet aucun diviseur premier inférieur ou égal à sa racine carrée ($\sqrt{67} \simeq 8$).
  On a donc $4020 = 2^2 \times 3 \times 5 \times 67$.

Proposition

Soient $a, b \in \mathbb{N} \setminus \{0,1\}$ tels que $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ où $p_1,\ p_2, ...,\ p_r$ est sont des nombres premiers distincts deux à deux, et $\alpha_1, ..., \alpha_r \in \mathbb{N}$, $\beta_1, ..., \beta_r \in \mathbb{N}$ (éventuellement nuls pour tenir compte d'un nombre premier qui pourrait ne diviser qu'un seul des deux entiers a ou b). Soit $d \in \mathbb{N}$. Alors :

$$d|a \text{ si et seulement si } d = \prod_{i=1}^{r} p_i^{\gamma_i} \text{ où, pour tout } i \in [\![1,r]\!],\ \gamma_i \in [\![0,\alpha_i]\!].$$

$$\text{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \times p_2^{\min(\alpha_2,\beta_2)} \times ... \times p_r^{\min(\alpha_r,\beta_r)}$$

$$\text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \times p_2^{\max(\alpha_2,\beta_2)} \times ... \times p_k^{\max(\alpha_r,\beta_r)}$$

Démonstration.

- Supposons que $d = \prod_{i=1}^{r} p_i^{\gamma_i}$ avec $\gamma_i \leq \alpha_i$ pour tout $i \in [\![1,r]\!]$. En posant $c = \prod_{i=1}^{r} p_i^{\alpha_i - \gamma_i}$, on obtient $dc = a$, donc d divise a.
  Réciproquement, si d divise a alors, il existe $c \in N^*$ tel que $a = dc$. Les diviseurs premiers de d et c divisent a donc sont inclus dans $\{p_1, ..., p_r\}$. Ainsi, pour tout $i \in [\![0,r]\!]$, il existe des entiers naturels γ_i, δ_i tels que $c = \prod_{i=1}^{r} p_i^{\delta_i}$ et $d = \prod_{i=1}^{r} p_i^{\gamma_i}$. On a alors :
  $$\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r} p_i^{\gamma_i + \delta_i}.$$
  Par unicité de la décomposition en produit de facteurs premiers de a, on obtient $\alpha_i = \gamma_i + \delta_i$ pour tout $i \in [\![1,r]\!]$, et donc pour tout $i \in [\![1,r]\!]$, $\gamma_i \leq \alpha_i$.

- Posons $d = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$.
  - Pour tout $i \in [\![1,r]\!]$, $\min(\alpha_i,\beta_i) \leq \alpha_i$ et $\min(\alpha_i,\beta_i) \leq \beta_i$.
    Ainsi, avec le premier point, d divise a et b.
  - Soit $n \in \mathbb{N}$ tel que n divise a et n divise b.
    Avec le premier point, il existe $\delta_1, ...\delta_r \in \mathbb{N}$ tel que $n = \prod_{i=1}^{r} p_i^{\delta_i}$ et pour tout $i \in [\![1,r]\!]$, $\delta_i \in [\![0,\alpha_i]\!]$ et $\delta_i \in [\![0,\beta_i]\!]$.
    Ainsi, pour tout $i \in [\![1,r]\!]$, $\delta_i \in [\![0,\min(\alpha_i,\beta_i)]\!]$. Ainsi, Donc n divise d.

  On obtient $d = \text{pgcd}(a,b)$.

- On a : $\text{pgcd}(a,b)\text{ppcm}(a,b) = ab = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i}$
  D'où $\text{ppcm}(a,b) \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)} = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i}$.
  Ainsi, $\text{ppcm}(a,b) = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i-\min(\alpha_i,\beta_i)}$.
  Soit $i \in [\![1,r]\!]$, on a : $\alpha_i + \beta_i - \min(\alpha_i,\beta_i) = \max(\alpha_i,\beta_i)$. En effet :

- Si $\alpha_i \geq \beta_i$. Alors, $\min(\alpha_i, \beta_i) = \beta_i$ et $\max(\alpha_i, \beta_i) = \alpha_i$.
  Ainsi, $\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \alpha_i + \beta_i - \beta_i = \alpha_i = \max(\alpha_i, \beta_i)$.
- Si $\alpha_i < \beta_i$. Alors, $\min(\alpha_i, \beta_i) = \alpha_i$ et $\max(\alpha_i, \beta_i) = \beta_i$.
  Ainsi, $\alpha_i + \beta_i - \min(\alpha_i, \beta_i) = \alpha_i + \beta_i - \alpha_i = \beta_i = \max(\alpha_i, \beta_i)$.

□

Exemple : Posons $a = 756$ et $b = 350$.
On a : $756 = 2^2 \times 3^3 \times 7^1$ et $350 = 2^1 \times 5^2 \times 7^1$.
D'où : $\text{pgcd}(756, 350) = 2^1 \times 7^1 = 14$ et $\text{ppcm}(756, 350) = 2^2 \times 3^3 \times 5^2 \times 7^1 = 18900$.

2 Ensembles finis

2.1 Définition et premières propriétés

Définition

Un ensemble E non vide est dit fini, s'il existe un entier naturel non nul n et une bijection de $[\![1, n]\!]$ dans E.
L'entier n, s'il existe, est unique et est appelé cardinal de E. On le note $\text{Card}(E)$ (ou $|E|$ ou $\#E$).
Un ensemble qui n'est pas fini est dit infini.

Remarque : Le cardinal de E représente le nombre d'éléments de E.
Exemple :

- Par convention $\emptyset$ est fini de cardinal 0.
- $[\![1, n]\!]$ est fini de cardinal n (prendre $h = id_{[\![1,n]\!]}$).
- $[\![p, q]\!]$ est fini de cardinal $q - p + 1$ (prendre $\begin{array}{rccc} h : & [\![1, q-p+1]\!] & \to & [\![p, q]\!] \\ & i & \mapsto & p-1+i \end{array}$).
- Soit $n \in \mathbb{N}^*$ et $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. L'application : $\begin{array}{ccc} [\![1, n]\!] & \to & \mathbb{U}_n \\ k & \mapsto & e^{\frac{2ik\pi}{n}} \end{array}$ est bijective, donc $\mathbb{U}_n$ est fini et $|\mathbb{U}_n| = n$.

Remarque : Soit E un ensemble fini de cardinal $n \geq 1$.
Une bijection $\begin{array}{ccc} [\![1, n]\!] & \to & E \\ i & \mapsto & a_i \end{array}$ permet de numéroter les éléments de E et d'écrire $E = \{a_1, ..., a_n\}$.

Lemme

Si E est fini non vide et $a \in E$, alors $E \backslash \{a\}$ est fini et $\text{Card}(E \backslash \{a\}) = \text{Card}(E) - 1$.

Démonstration. Comme E est fini, il existe $n \in \mathbb{N}^*$ et $h : [\![1, n]\!] \to E$ bijection.

- Supposons que $h(n) = a$. On pose alors $\begin{array}{rccc} g : & [\![1, n-1]\!] & \to & E \backslash \{a\} \\ & i & \mapsto & h(i) \end{array}$.
  - g est bien définie. soit $i \in [\![1, n-1]\!]$. Par l'absurde, si $h(i) = a$ alors $h(i) = h(n)$ donc $i = n$ car h est injective. Absurde.
    Ainsi, $h(i) \in [\![1, n-1]\!]$.
  - g est injective :
    Soit $i, j \in [\![1, n-1]\!]$. Supposons que $g(i) = g(j)$. Alors $h(i) = h(j)$ donc $i = j$ par injectivité de h.
    Ainsi g est injective.
  - g est surjective :
    Soit $x \in E \backslash \{a\}$. Comme h est surjective, il existe $i \in [\![1, n]\!]$ tel que $h(i) = x$.
    Montrons par l'absurde que $i \neq n$. Supposons que $i = n$.
    Alors $x = h(i) = h(n) = a$. Absurde.
    Ainsi, $i \in [\![1, n-1]\!]$ et $g(i) = x$ donc g est surjective.

  Ainsi, g est bijective donc $E \backslash \{a\}$ est fini de cardinal $n - 1$.
- Supposons désormais que $h(n) \neq a$.
  Posons $t : \left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & \left\{ \begin{array}{l} a \text{ si } x = h(n) \\ h(n) \text{ si } x = a \\ x \text{ sinon} \end{array} \right. \end{array} \right.$.
  l'application t échange a et $h(n)$.
  On a $t \circ t = id_E$ donc t est bijective.

Posons $h_1 = t \circ h$. h_1 est bijective comme composée de fonctions qui le sont.
De plus, $h_1(n) = t(h(n)) = a$.
On peut donc appliquer le premier point avec h_1.
Ainsi $E\backslash\{a\}$ est fini de cardinal $n-1$.

□

Théorème : Partie d'un ensemble fini

Soit E un ensemble fini et F est un sous-ensemble de E, alors :

- F est fini et $\text{Card}(F) \leq \text{Card}(E)$.
- $\text{Card}(F) = \text{Card}(E)$ si et seulement si $F = E$.

Démonstration. On raisonne par récurrence.
Pour tout $n \in \mathbb{N}$, on pose :

$\mathscr{P}(n)$: « Si E est un ensemble fini de cardinal n, tout sous-ensemble F de E est fini de cardinal inférieur ou égal à n, avec égalité si et seulement si $F = E$ »

- Pour $n = 0$, soit E un ensemble de cardinal 0.
  Alors $E = \emptyset$ et le seul sous-ensemble de E est $F = \emptyset$. Il est fini de cardinal 0, donc $\mathscr{P}(0)$ est vraie.
- Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie.
  Soient E un ensemble de cardinal $n+1$ et F un sous-ensemble de E.
  Si $F = E$, alors F est fini de cardinal $n+1$.
  Supposons $F \neq E$. On a alors $a \in E\backslash F$. D'après le lemme précédent, $E_1 = E\backslash\{a\}$ est fini de cardinal n, et $F \subset E_1$ (puisque $a \notin F$). Par hypothèse de récurrence, on a donc F fini de cardinal $\leq \text{Card}(E_1) = n < n+1$. Ainsi, on a $\text{Card}(F) \leq \text{Card}(E)$ avec égalité si et seulement si $F = E$.
  On a donc montré que $\mathscr{P}(n+1)$ est vraie.
  En conclusion : $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

□

Remarque :

- Ainsi si E et F sont deux ensembles de même cardinaux, il suffit de montrer une inclusion pour avoir l'égalité.
- Si F est un sous-ensemble d'un ensemble fini E, si $\mathbf{1}_F : E \to \{0,1\}$ est sa fonction indicatrice, on a :

$$\text{Card}(F) = \sum_{x \in E} \mathbf{1}_F(x).$$

Proposition

Soient E et F deux ensembles.

- Soit $h : E \to F$ une application bijective. E est fini de cardinal n si et seulement si F est fini de cardinal n.
  On a alors : $\text{Card}(E) = \text{Card}(F)$.
- Soit $h : E \to F$ une application injective. Si F est fini, alors E est fini et $\text{Card}(E) \leq \text{Card}(F)$.
- Soit $h : E \to F$ une application surjective. Si E est fini, alors F est fini et $\text{Card}(F) \leq \text{Card}(E)$.

Démonstration.

- Comme E est fini de cardinal n, il existe $g : [\![1,n]\!] \to E$ bijective. Alors $h \circ g$ est bijective (comme composée de fonctions bijectives) de $[\![1,n]\!]$ dans F, donc F est fini de cardinal n.
  $h^{-1} : F \to E$ est une bijection. Si F est fini de cardinal n alors d'après le sens précédent (en échangeant E et F), E est fini de cardinal n.
- Supposons F fini. Posons $\begin{array}{rccc} g : & E & \to & h(E) \\ & x & \mapsto & h(x) \end{array}$.
  g est toujours injective (car h l'est) et surjective, donc bijective. Comme $h(E) \subset F$, $h(E)$ est fini de cardinal plus petit que celui de F. Ainsi, $\text{Card}(E) = \text{Card}(h(E)) \leq \text{Card}(F)$.
- Supposons E fini.
  On pose $\begin{array}{rccc} g : & F & \to & E \\ & x & \mapsto & \text{un antécédent de } x \text{ par } h \end{array}$.
  - g est bien définie car h est surjective.
  - Montrons que g est injective.
    Soient $x, y \in F$, supposons que $g(x) = g(y)$.
    $g(x)$ et $g(y)$ sont respectivement des antécédents de x et de y par h, donc $h(g(x)) = x$ et $h(g(y)) = y$.
    D'où $x = h(g(x)) = h(g(y)) = y$ et g est injective.

On conclut alors avec le premier point.

□

Théorème

Soient E et F ensembles finis de même cardinal n. On considère Soit $f : E \to F$. Alors :

f est injective si et seulement si f est surjective si et seulement si f est bijective.

Démonstration.

- Si f est bijective, elle est injective et surjective.
- Supposons f injective.
  On pose alors $g : \begin{array}{ccc} E & \to & f(E) \\ x & \mapsto & f(x) \end{array}$.
  g est injective car f l'est, et g est surjective.
  Ainsi g est bijective donc $\text{Card}(f(E)) = \text{Card}(E) = \text{Card}(F)$.
  De plus, $f(E) \subset F$ donc $f(E) = F$.
  Ainsi f est surjective, donc bijective.
- Supposons f surjective et montrons par l'absurde que f est injective.
  Supposons f non injective.
  Alors il existe $x, y \in E$ tel que $f(x) = f(y)$ et $x \neq y$.
  Soient $E_1 = E \backslash \{y\}$ et $g : \left\{ \begin{array}{ccc} E_1 & \to & F \\ u & \mapsto & h(u) \end{array} \right.$.
  Montrons que g est encore surjective :
  Soit $v \in F$. Il existe $u \in E$ tel que $f(u) = v$.
  - si $u \neq y$ alors $u \in E_1$
  - si $u = y$ alors $f(x) = f(y) = v$ et $x \in E_1$.

  Ainsi, g est encore surjective, donc $\text{Card}(E_1) \geq \text{Card}(F)$ par la proposition précédente. Or, $\text{Card}(E_1) = \text{Card}(E) - 1$.
  Ainsi $\text{Card}(E) - 1 \geq \text{Card}(E)$ absurde.
  Donc h est injective, donc bijective.

□

Remarque : Ceci devient faux pour des ensembles infinis : $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \mapsto & x+1 \end{array} \right.$ est injective non surjective par exemple.

2.2 Opérations sur les cardinaux

Proposition

Si A et B sont deux ensembles finis disjoints (c'est à dire que $A \cap B = \emptyset$), alors $A \cup B$ est fini et

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

Démonstration. Notons n le cardinal de A et p celui de B.
Il existe $f : A \to [\![1, n]\!]$ et $g : B \to [\![1, p]\!]$.
Posons $h : \left\{ \begin{array}{ccc} A \cup B & \to & [\![1, n+p]\!] \\ x & \mapsto & \left\{ \begin{array}{ll} f(x) & \text{si } x \in A \\ g(x) + n & \text{si } x \in B \end{array} \right. \end{array} \right.$.

- h est bien défini car $A \cap B = \emptyset$ donc tout élément de $A \cup B$ admet bien une unique image et $h(A \cup B) \subset [\![1, n+p]\!]$.
- h est surjective : Soit $u[\![1, n+p]\!]$.
  - si $u \in [\![1, n]\!]$, posons $x = f^{-1}(u) \in A$.
    On a $h(x) = f(f^{-1}(u)) = u$.
  - si $u \in [\![n+1, n+p]\!]$, $u - n \in [\![1, p]\!]$.
    Posons $x = g^{-1}(u - n) \in B$.
    On a $h(x) = g(g^{-1}(u - n)) + n = u - n + n = u$.

  Ainsi, h est surjective.
- h est injective :
  Soient $x, x' \in A \cup B$ tel que $h(x) = h(x')$.
  - Si $x \in A$ et $x' \in B$ alors $h(x) \in [\![1, n]\!]$ et $h(x') \in [\![n+1, n+p]\!]$. Impossible.

- De même, il est impossible d'avoir $x \in B$, $x' \in A$ et $h(x) = h(x')$.
- Si $x, x' \in A$, on a $h(x) = h(x')$. Donc $f(x) = f(x')$.
  Or, f est injective donc $x = x'$.
- Si $x, x' \in B$, on a $h(x) = h(x')$. Donc $g(x) + n = g(x') + n$.
  D'où $g(x) = g(x')$. Or, g est injective donc $x = x'$.

Ainsi, h est injective.
Donc h est bijective et $A \cup B$ est fini de cardinal $n + p$.

□

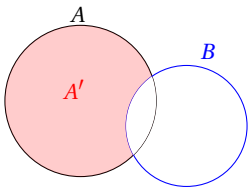
Corollaire

Si E est fini et $A \in \mathscr{P}(E)$, alors $\text{Card}(E \setminus A) = \text{Card}(E) - \text{Card}(A)$.

Proposition

Soient A et B deux ensembles finis. Alors $A \cup B$ est fini et on a : $\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$.

Démonstration.



On pose $A' = A \setminus B$.

- On a :
$$A' \cap (A \cap B) = A \cap C_E^B \cap A \cap B = \emptyset.$$
Et :
$$A' \cup (A \cap B) = (A \cap C_E^B) \cup (A \cap B) = A \cap (C_E^B \cup B) = A \cap E = A.$$
D'après la proposition précédente, on a $\text{Card}(A') = \text{Card}(A) - \text{Card}(A \cap B)$.
- De plus, on a :
$$A' \cap B = A \cap C_E^B \cap B = A \cap \emptyset = \emptyset.$$
Et :
$$A' \cup B = (A \cap C_E^B) \cup B = (A \cup B) \cap (C_E^B \cup B) = (A \cup B) \cap E = A \cup B.$$
Ainsi, d'après la proposition précédente, on a $\text{Card}(A \cup B) = \text{Card}(A') + \text{Card}(B)$
- Finalement, on obtient : $\text{Card}(A \cup B) = \text{Card}(A') + \text{Card}(B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$.

□

Corollaire

Soient A_1, ..., A_n des ensembles finis deux à deux disjoints. Alors $\bigcup_{k=1}^{n} A_k$ est fini et on a :

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

Démonstration. Ce résultat se prouve par récurrence. □

Proposition : Produit cartésien

Soient E et F deux ensembles finis, alors $E \times F$ est fini et $\text{Card}(E \times F) = \text{Card}(E)\text{Card}(F)$.

Démonstration. Notons $n = \text{Card}(E)$, $p = \text{Card}(F)$ et $E = \{e_1, \dots, e_n\}$ où les e_i sont deux à deux distincts.
$E \times F = \Big(\{e_1\} \times F\Big) \cup \Big(\{e_2\} \times F\Big) \cup \dots \cup \Big(\{e_n\} \times F\Big)$.
Pour tout $i \in [\![1, n]\!]$, on pose $F_i = \Big(\{e_i\} \times F\Big)$.
Les F_i avec $i \in [\![1, n]\!]$ sont deux à deux disjoints et $E \times F = \bigcup_{i=1}^{n} F_i$.
Ainsi, $\text{Card}(E \times F) = \sum_{i=1}^{p} \text{Card}(F_i)$.
Soit $i \in [\![1, p]\!]$, l'application $f_i : \begin{array}{ccc} F & \to & F_i \\ f & \mapsto & (e_i, f) \end{array}$ est bijective, donc $\text{Card}(F_i) = \text{Card}(F) = p$.
Ainsi $\text{Card}(E \times F) = \sum_{i=1}^{n} \text{Card}(F_i) = \sum_{i=1}^{n} p = np$. □

Corollaire

- Soient E_1, ... E_p des ensembles finis. Alors $E_1 \times E_2 \times \dots \times E_p$ est fini et $\text{Card}(E_1 \times \dots \times E_p) = \prod_{i=1}^{n} \text{Card}(E_i)$.
- En particulier, si E est un ensemble fini, pour tout $p \in \mathbb{N}^*$, E^p est fini de cardinal $(\text{Card}(E))^p$.

Démonstration.
- Le premier point se montre par récurrence avec la proposition précédente.
- Le deuxième découle du premier.

□

3 Dénombrement

3.1 Listes

Soit E un ensemble et $p \in \mathbb{N}^*$.
On rappelle qu'une p-liste d'éléments de E est un élément de E^p. L'ordre des éléments compte et il peut y avoir des répétitions.

Proposition Nombre de p-listes

Soit E un ensemble fini et $p \in \mathbb{N}^*$. Le nombre de p-liste (ou p-uplets) de E est égal à $\text{Card}(E)^p$.

Démonstration. En effet, $\text{Card}(E^p) = \text{Card}(E)^p$. □

Exemple : Combien de mots de p lettres (ayant un sens ou non) peut-on former avec un alphabet de n lettres ?
Les mots de p lettres sont exactement les p-listes de lettres. Il y en a n^p.

Proposition : Nombre d'applications d'un ensemble fini dans un autre

Soient E et F sont deux ensembles finis. Alors l'ensemble $\mathscr{F}(E, F)$ des applications de E dans F est un ensemble fini et $\text{Card}(\mathscr{F}(E, F)) = \text{Card}(F)^{\text{Card}(E)}$.

Démonstration. Notons p le cardinal de E et $E = \{e_1, ..., e_p\}$ (les e_i étant deux à deux distincts).
Construire une application $f : E \to F$ revient à se donner les images par f de tous les éléments de E.
Or, on a :
$\text{Card}(F)$ choix pour $f(e_1)$
$\text{Card}(F)$ choix pour $f(e_2)$
⋮
$\text{Card}(F)$ choix pour $f(e_p)$
Au total, cela fait $\text{Card}'F)^p = \text{Card}(F)^{\text{Card}(E)}$ choix. □

Proposition : Nombre de parties d'un ensemble fini

Soit E un ensemble fini. Alors l'ensemble $\mathscr{P}(E)$ des parties de E est fini et $\text{Card}(\mathscr{P}(E)) = 2^{\text{Card}(E)}$.

Démonstration. Notons p le cardinal de E et $E = \{e_1, ..., e_p\}$ (les e_i étant deux à deux distincts).
Définir une partie A de E revient à déterminer pour tout $i \in [\![1, p]\!]$ si $e_i \in A$ ou non.
Ainsi, on a :
pour e_1, on a 2 choix : $x_1 \in A$ ou $x_1 \notin A$
pour e_2, on a 2 choix : $x_2 \in A$ ou $x_2 \notin A$
$\vdots$
pour e_p, on a 2 choix : $x_p \in A$ ou $x_p \notin A$
Au total, cela fait 2^p choix. □

Proposition : Nombre de p-listes d'éléments distincts

Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}^*$. Le nombre de p-listes ou p-uplets d'éléments deux à deux distincts de E est égal à :

$$\begin{cases} \dfrac{n!}{(n-p)!} & \text{si } p \leq n \\ 0 & \text{si } p > n \end{cases}$$

Démonstration.

- Supposons d'abord $p \leq n$.
  Pour construire un p-uplet $(e_1, ..., e_p)$ d'éléments deux à deux distincts de E, on a :
  * n choix pour le premier élément ($e_1 \in E$).
  * $n-1$ choix pour le deuxième élément ($e_2 \in E \setminus \{e_1\}$).
    $\vdots$
  * $n-p+1$ choix pour le dernier ($e_p \in E \setminus \{e_1, ..., e_{p-1}\}$).

  Au total cela fait $n(n-1)\dots(n-p+1) = \frac{n!}{(n-p)!}$ choix.
- Si $p > n$, on ne peut pas trouver p éléments distincts dans E.

□

Exemple :

- Une urne contient 40 boules numérotées de 1 à 40. On pioche successivement 5 boules. Combien y-a-t-il de tirages possibles ?
  Il y a $\dfrac{40!}{35!}$ possibilités de tirer 5 boules numérotées entre 1 et 40 (en tenant compte de l'ordre).
- Une course de chevaux comporte 20 partants. Le nombre de résultats possibles de tiercés dans l'ordre est : $20 \times 19 \times 18 = 6840$.

Proposition : Nombre d'injections

Le nombre d'injections d'un ensemble E de cardinal $p \in \mathbb{N}^*$ dans un ensemble F de cardinal $n \in \mathbb{N}^*$ est :

$$\begin{cases} \dfrac{n!}{(n-p)!} & \text{si } p \leq n \\ 0 & \text{si } p > n \end{cases}$$

Démonstration. Notons p le cardinal de E et $E = \{e_1, ..., e_p\}$ (les e_i étant 2 à 2 distincts).
Construire une application $f : E \to F$ revient à se donner les images par f de tous les éléments de E.
De plus, f est injective si et seulement si les $f(e_i)$ avec $i \in [\![1, p]\!]$ sont deux à deux distincts.

- Si $n < p$, comme pour tout $i \in [\![1, p]\!]$, $f(e_i) \in F$, il ne peut pas y avoir p éléments distincts dans F.
- Supposons désormais $n \geq p$.
  On a :
  n choix pour $f(e_1) : f(e_1) \in F$.
  $n-1$ choix pour $f(e_2) : f(e_2) \in F \setminus \{f(e_1)\}$.
  $\vdots$
  $n-(p-1)$ choix pour $f(e_p) : f(e_p) \in F \setminus \{f(e_1), ..., f(e_{p-1})\}$.
  Au total, cela fait : $n(n-1)...(n-p+1) = \dfrac{n!}{(n-p)!}$.

□

Corollaire

Si E est un ensemble fini de cardinal n. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E sur E (appelées également permutations de E). Alors $\mathfrak{S}(E)$ est fini et :

$$Card(\mathfrak{S}(E)) = n!$$

Démonstration. Puisque E est fini, on peut dire, d'après le cours, qu'il revient au même de chercher les applications de E dans E qui sont bijectives ou celles qui sont qui sont injectives. Ainsi, d'après la proposition précédente, le nombre de bijections de E dans E est donc $n!$. □

3.2 Dénombrement des parties d'une ensemble fini

Proposition

Soient E un ensemble fini de cardinal n et $p \in [\![0, n]\!]$. Le nombre de partie à p éléments de E est $\binom{n}{p}$.

Démonstration. Notons $\mathscr{A}(n,p)$ l'ensemble des p-listes d'éléments distincts de E, et $\mathscr{C}(n,p)$ l'ensemble des parties de p éléments de E.
Pour construire un p-uplet d'éléments de E deux à deux distincts, on a :

- $\text{Card}\left(\mathscr{C}(n,p)\right)$ choix pour l'ensemble des éléments du p-uplet (qui est une partie de E à p éléments).
- $p!$ choix pour ordonner ces éléments (nombre de bijections d'un ensemble de cardinal p dans lui même).

Ainsi, on a $p!\text{Card}\left(\mathscr{C}(n,p)\right) = \text{Card}\left(\mathscr{A}(n,p)\right) = \dfrac{n!}{(n-p)!}$ donc $\text{Card}\left(\mathscr{C}(n,p)\right) = \dfrac{n!}{(n-p)!p!} = \binom{n}{p}$. □

Remarque : Un sous-ensemble à p éléments de E de cardinal p est aussi appelée p-combinaison de E.
Exemple : Soit E un ensemble fini de cardinal $n \in \mathbb{N}$.
Pour tout entier naturel $k \in [\![0, n]\!]$, on pose $\mathscr{P}_k(E) = \{X \in \mathscr{P}(E),\ \text{Card}(X) = k\}$
L'application $\begin{array}{rccc} h: & \mathscr{P}_k(E) & \to & \mathscr{P}_{n-k}(E) \\ & A & \mapsto & C_E^A \end{array}$ est bijective.
En effet, soient $(A,B) \in \mathscr{P}_k(E) \times \mathscr{P}_{n-k}(E)$.
On a :

$$\begin{aligned} h(A) = B &\iff C_E^A = B \\ &\iff C_E^{C_E^A} = C_E^B \\ &\iff A = C_E^B \end{aligned}$$

Ainsi, h est bijective.
De plus, $\mathscr{P}_k(E), \mathscr{P}n-k(E) \subset \mathscr{P}(E)$ qui est fini. Ainsi, $\mathscr{P}_k(E)$ et $\mathscr{P}n-k(E)$ sont finis.
On a de plus : $\text{Card}(\mathscr{P}_k(E)) = \text{Card}(\mathscr{P}_k(E))$. Donc :

$$\binom{n}{k} = \text{Card}\left(\mathscr{P}_k(E)\right) = \text{Card}\left(\mathscr{P}_{n-k}(E)\right) = \binom{n}{n-k}.$$

Proposition

Si E est un ensemble fini à n éléments, alors l'ensemble $\mathscr{P}(E)$ des parties de E est fini de cardinal 2^n.

Démonstration. Pour tout entier naturel $k \in [\![0, n]\!]$, on pose $\mathscr{P}_k(E) = \{X \in \mathscr{P}(E),\ \text{Card}(X) = k\}$.
$\mathscr{P}(E)$ est l'union disjointe des $\mathscr{P}_k(E)$ pour $k \in [\![0, n]\!]$ et les $\mathscr{P}_k(E)$ avec $k \in [\![0, n]\!]$ sont des ensembles finis. Ainsi :

$$\text{Card}\left(\mathscr{P}(E)\right) = \sum_{k=0}^{n} \text{Card}\left(\mathscr{P}_k(E)\right).$$

Or : $\forall k \in [\![0, n]\!],\ \text{Card}\left(\mathscr{P}_k(E)\right) = \binom{n}{k}$.
Ainsi, par la formule du binôme de Newton, on a :

$$\text{Card}\left(\mathscr{P}(E)\right) = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

par la formule du binôme de Newton. □

Démonstration combinatoire des formules de Pascal et du binôme de Newton.

Rappel : Formule de Pascal : Soient $n \in \mathbb{N}^*$ et $p \in [\![1, n-1]\!]$ alors on a : $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$

Binôme de Newton : Soient $(a,b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$ alors $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Démonstration. Donnons ici des preuves combinatoires :

- Soient $n \in \mathbb{N}^*$ et $p \in [\![1, n-1]\!]$.

  Considérons un ensemble E de cardinal n. Il y a $\binom{n}{p}$ parties à p éléments.

  Soit $a \in E$, pour avoir une partie de E à p éléments, on distingue :

  - Celles qui contiennent a. Il y en a $\binom{n-1}{p-1}$: choix de $p-1$ éléments parmi les $n-1$ éléments de $E\backslash\{a\}$.
  - Celles qui ne contiennent pas a. Il y en a $\binom{n-1}{p}$: choix de p éléments parmi les $n-1$ de $E\backslash\{a\}$.

  Comme ces ensembles sont disjoints, on a : $\binom{n-1}{p-1} + \binom{n-1}{p} = \binom{n}{p}$ et on retrouve la formule de Pascal.

- Soit $n \in \mathbb{N}$. Commençons par écrire l'égalité :

$$(a+b)^n = \underbrace{(a+b) \times (a+b) \times \ldots \times (a+b)}_{n \text{ fois}}$$

  Pour développer ce produit, il faut additionner tous les produits possibles du type :

$$\underbrace{a \times a \times b \times a \times \ldots \times b \times a}_{n \text{ termes}}$$

  Tous ces produits seront de la forme $a^k b^{n-k}$ avec $k \in [\![0, n]\!]$. On prend un facteur dans chaque parenthèse. Pour k fixé dans $[\![0, n]\!]$, il a $\binom{n}{k}$ façons d'obtenir $a^k b^{n-k}$. On choisit pour cela k parenthèses où l'on prend le complexe a, et on prendra nécessairement b dans les $n-k$ restantes. On obtient donc la formule annoncée.

□