Chapitre 11

Entiers naturels et dénombrement

Mathieu Mansuy - Professeur de Mathématiques en supérieures PCSI au Lycée Saint Louis (Paris)
mansuy.mathieu@hotmail.fr

1 Rudiments d'arithmétique

1.1 Multiples et diviseurs d'un entier

Définition.

Étant donnés deux entiers a, b, on dit que a **divise** b, ou a **est un diviseur de** b, ou que b **est multiple de** a, s'il existe un entier c tel que $b = ac$. On note alors $a|b$.

Notations. On notera $\mathcal{D}(b)$ l'ensemble des diviseurs de b, et $a\mathbb{Z}$ l'ensemble des multiples de a.

Exemple.

- $\mathcal{D}(12) = \{1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12\}$, $\mathcal{D}(11) = \{1, -1, 11, -11\}$.
- $0\mathbb{Z} = \{0\}$ et $D(0) = \mathbb{Z}$.
- $\pm 1\mathbb{Z} = \mathbb{Z}$ et $D(\pm 1) = \{-1, 1\}$.

Remarque. Soient $a, b \in \mathbb{Z}$. On a $a|b$ si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$. En effet :

$\Leftarrow$ Si $b\mathbb{Z} \subset a\mathbb{Z}$, alors $b \in a\mathbb{Z}$, et donc il existe $c \in \mathbb{Z}$ tel que $b = ac$, soit encore $a|b$.

$\Rightarrow$ Supposons que $a|b$, alors il existe $c \in \mathbb{Z}$ tel que $b = ac$. Alors pour tout $k \in \mathbb{Z}$, $bk = a(ck) \in a\mathbb{Z}$. Ainsi $b\mathbb{Z} \subset a\mathbb{Z}$.

Propriété 1

Soient a, b, c des entiers.

(1) $(a|b$ et $a|c) \Rightarrow a|b + c$.

(2) $a|b \Rightarrow a|bc$.

(3) $(a|b$ et $b|a) \Rightarrow |a| = |b|$.

(4) $(a|b$ et $c|d) \Rightarrow ac|bd$.

(5) $ab|c \Rightarrow a|c$ et $b|c$.

Remarque. La réciproque du dernier point est fausse : 6 et 4 divisent 12, mais $24 = 6 \times 4$ ne divise pas 12.

Preuve.

(1) Supposons que $a|b$ et $a|c$. Alors il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $c = k_2 a$. D'où par somme $b + c = (k_1 + k_2)a$, i.e. $a|(b + c)$.

(2) Si $a|b$, alors il existe $k \in \mathbb{Z}$ tel que $b = ak$. D'où $bc = akc = a(kc)$ et donc $a|bc$.

(3) Supposons que $a|b$ et $b|a$. Alors il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $a = k_2 b$. Alors $b = k_1 k_2 b$. Si $b = 0$, alors $a = 0$ et on a le résultat. Si $b \neq 0$, alors $k_1 k_2 = 1$ et $k_1 = k_2 = \pm 1$. Ainsi $a = \pm b$, et donc $|a| = |b|$.

(4) Supposons que $a|b$ et $c|d$. Alors il existe $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $d = k_2 c$. D'où par produit : $bd = (k_1 a)(k_2 c) = (k_1 k_2)ac$ et donc $ac|bd$.

(5) Si $ab|c$, alors il existe $k \in \mathbb{Z}$ tel que $c = abk$, ce qui ce réécrit $c = a(bk) = b(ak)$. Ainsi $a|c$ et $b|c$.

□

Exemple. ♦ Montrer que pour tout entier impair n, $n^2 - 1$ est multiple de 8.

Il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. D'où $n^2 - 1 = 4q(q + 1)$ qui est un multiple de 8 car comme les entiers q et $q + 1$ sont consécutifs, l'un d'eux est pair, et on a $n^2 - 1 = 8\frac{q(q+1)}{2}$ avec $\frac{q(q+1)}{2} \in \mathbb{Z}$.

♦ Montrer que pour tout entier naturel n, $2^{3n} - 1$ est multiple de 7.

On le montre par récurrence sur $n \in \mathbb{N}$.
La propriété est vraie pour $n = 0$.
Supposons la propriété vraie au rang $n \in \mathbb{N}$: $\exists k \in \mathbb{Z} : 2^{3n} - 1 = 7k$. Au rang $n + 1$ on a :

$$2^{3(n+1)} - 1 = 8 \times 2^{3n} - 1 \overset{HR}{=} 8 \times (7k + 1) - 1 = (7 + 1)(7k + 1) - 1 = 7(7k + k + 1) + 1 - 1$$

La propriété est donc vraie au rang $n+1$. On conclut par principe de récurrence.

Exemple. Pour tout $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, $(a-b)$ divise $(a^n - b^n)$.

Exercice. Critères de divisibilité par $3, 9, 11$.
On considère un entier naturel n dont l'écriture décimale est $n = a_p \dots a_1 a_0$, de sorte que :

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

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

On utilise que $10 = 9 + 1$, d'où par le binôme de Newton pour tout $k \in \mathbb{N}$:

$$10^k = (9+1)^k = \sum_{i=0}^{k} \binom{k}{i} 9^k \text{ de la forme } 3q_k + 1.$$

Ainsi :

$$n = \sum_{k=0}^{p} a_k 10^k = 3(\sum_{k=0}^{p} q_k a_k) + \sum_{k=0}^{p} a_k.$$

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

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

On procède comme précédement.

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

On utilise que $10 = 11 - 1$, d'où par le binôme de Newton pour tout $k \in \mathbb{N}$:

$$10^k = (11-1)^k = \sum_{i=0}^{k} \binom{k}{i} 11^k (-1)^{k-i} \text{ de la forme } 11q_k + (-1)^k.$$

Ainsi :

$$n = \sum_{k=0}^{p} a_k 10^k = 11(\sum_{k=0}^{p} q_k a_k) + \sum_{k=0}^{p} (-1)^k a_k.$$

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

1.2 Division euclidienne dans $\mathbb{N}$

Théorème 2

On considère un nombre entier naturel n et un nombre entier naturel $b > 0$.
Alors il existe un unique couple (q, r) appartenant à $\mathbb{N} \times \mathbb{N}$ tel que :

$$n = qb + r \text{ et } 0 \leq r < b.$$

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

Preuve. • *Unicité du couple* (q, r).
Supposons qu'il existe deux couples d'entiers naturels (q_1, r_1) et (q_2, r_2) tels que :

$$n = q_1 b + r_1, \quad n = q_2 b + r_2 \text{ et } 0 \leq r_1, r_2 < b.$$

On en déduit par différence : $(q_1 - q_2)b = r_2 - r_1$. Ainsi $r_2 - r_1$ est un multiple de b et $-b < r_2 - r_1 < b$. D'où $r_2 - r_1 = 0$, et donc $r_1 = r_2$. En reportant, on obtient alors $q_1 = q_2$.

• *Existence du couple* (q, r).
Par récurrence sur n, montrons $\mathcal{P}(n) : \exists (q, r) \in \mathbb{N}^2 : n = qb + r$ et $0 \leq r < b$.
La propriété est vraie pour $n = 0$ en prenant $(q, r) = (0, 0)$.
Supposons la propriété $\mathcal{P}(k)$ vraie pour tout $k \leq n - 1$ et montrons que $\mathcal{P}(n)$ est vraie :
Si $n < b$, le couple $(q, r) = (0, n)$ convient.
Si $n \geq n$, on a $0 \leq n - b < n$. Par hypothèse de récurrence, il existe un couple $(q, r) \in \mathbb{N}^2$ tel que

$$n - b = qb + r \text{ et } 0 \leq r < b$$

ce qu'on peut réécrire comme suit :

$$\exists (q, r) \in \mathbb{N}^2 : n = q(b + 1) + r \text{ et } 0 \leq r < b.$$

Ainsi le couple $(q + 1, r)$ convient ici. On a donc montré la propriété $\mathcal{P}(n)$.
On conclut par principe de récurrence que la propriété $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$. □

Propriété 3

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

Preuve.

⇒ 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.

⇐ 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.

□

Exercice. Écrire un algorithme de division euclidienne.

Entrer $n \geq 0$ et $b > 0$. $q \leftarrow 0$; $r \leftarrow n$; Tant que $r \geq b$, faire :

| $r \leftarrow r - b$;
| $q \leftarrow q + 1$;

Sortir q et r ;

1.3 PGCD et PPCM

1.3.1 PGCD

Définition.

Soient $(a, b) \in \mathbb{N}^2$, $(a, b) \neq (0, 0)$. L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathbb{N}$ des diviseurs communs positifs de a et de b est une partie non vide et finie de $\mathbb{N}$. Elle admet donc un plus grand élément appelé Plus Grand Commun Diviseur, noté $PGCD(a, b)$ ou $a \wedge b$.

Remarques.

- $a \wedge b = b \wedge a$.
- Si $a > 0$, on a $a \wedge 0 = a$.
- Par convention, on posera $0 \wedge 0 = 0$.
- On peut étendre la définition du $PGCD$ dans le cas où $a, b \in \mathbb{Z}$ en posant $a \wedge b = |a| \wedge |b|$.

Exemple. $\mathcal{D}(6) \cap \mathbb{N} = \{1, 2, 3, 6\}$, $\mathcal{D}(8) \cap \mathbb{N} = \{1, 2, 4, 8\}$, donc $6 \wedge 8 = 2$.

1.3.2 Algorithme d'Euclide et PGCD

Propriété 4

Soient a et b deux entiers naturels avec $b > 0$. Si r désigne le reste de la division de a par b, alors :

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

Preuve. 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 $d|b$.

□

Description de l'algorithme d'Euclide.
On définit une suite d'entiers naturels (r_k) telle que :

- $r_0 = a$, $r_1 = b$,
- Pour $k \geq 1$, on suppose r_k et r_{k-1}.
  Si $r_k > 0$, on note r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k. En particulier $r_{k+1} < r_k$.

La suite (r_k) est une suite d'entiers naturels strictement décroissante. Il existe donc $N \in \mathbb{N}$ telle que $r_N \neq 0$ et $r_{N+1} \neq 0$.

Propriété 5 (Deuxième caractérisation du $PGCD$)

Soient $(a, b) \in \mathbb{N}^2 \setminus \{(0, 0)\}$. Le PGCD de a et b est le dernier reste non nul quand on effectue les divisions euclidiennes successives.

Preuve. Grâce au résultat précédent, on obtient que :

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

Par définition, $a \wedge b$ est le plus grand diviseur positif de a et de b. C'est donc r_N, le dernier reste non nul quand on effectue les divisions euclidiennes successives. □

Exemple. Calculer $162 \wedge 207$.

On effectue les divisions euclidiennes successives :

$$\begin{aligned} 207 &= 162 \times 1 + 45 \\ 162 &= 45 \times 3 + 27 \\ 45 &= 27 \times 1 + 18 \\ 27 &= 18 \times 1 + 9 \\ 18 &= 9 \times 2 + 0 \end{aligned}$$

Ainsi $162 \wedge 207 = 9$.

Exercice. Écrire un algorithme déterminant le PGCD de deux entiers naturels a et b.

Entrer a et b. $q \leftarrow 0$; $r \leftarrow n$; Tant que $b > 0$, faire :

| $r \leftarrow$ reste de la division euclidienne de a par b ;
| $a \leftarrow b$;
| $b \leftarrow r$;

Sortir a ;

Propriété 6 (Troisième caractérisation du PGCD)

Soient $(a,b) \in \mathbb{N}$, $d \in \mathbb{N}$. Alors :
d est le PGCD de a et b si et seulement si : $\begin{cases} d \text{ divise } a \text{ et } b \\ \forall n \in \mathbb{N}, \Big(n|a \text{ et } n|b\Big) \implies n|d \end{cases}$.

Preuve.

- Par définition du $PGCD$, $a \wedge b$ divise a et b.
  Soit d un diviseur de a et b alors $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$. Par la proposition précédente, $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$, donc $d \in \mathcal{D}(a \wedge b)$ et d divise $a \wedge b$.
- Soit d un entier naturel satisfaisant les conditions. Alors :
  - d divise a et b donc $d \in \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$ donc d divise $a \wedge b$.
    De plus, $a \wedge b$ est un diviseur commun de a et b donc on a $a \wedge b|d$ (deuxième hypothèse).

  Ainsi $a \wedge b|d$ et $d|a \wedge b$, donc $d = \pm a \wedge b$. Comme ces éléments sont supposés positifs, on obtient finalement $d = a \wedge b$. donc $d = a \wedge b$.

□

1.3.3 PPCM

Rappel. Tout sous-ensemble non vide A de $\mathbb{N}$ admet un plus petit élément, c'est à dire :

$$\exists m \in A, \quad \forall a \in A, \quad m \leq a.$$

Définition.

Soient $a, b \in \mathbb{N}^*$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$ des multiples communs strictement positifs de a et de b est une partie non vide de $\mathbb{N}$ (car par exemple $ab \in a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$). Elle admet donc un plus petit élément appelé Plus Petit Commun Multiple, noté $PPCM(a,b)$ ou $a \vee b$.

Remarques.

- $a \vee b = b \vee a$.
- On pose par convention $a \vee 0 = a$ pour tout $a \in \mathbb{N}$. En particulier, $0 \vee 0 = 0$.

Exemple. $6\mathbb{Z} \cap \mathbb{N}^* = \{6, 12, 18, 24, 30, \dots\}$, $8\mathbb{Z} \cap \mathbb{N}^* = \{8, 16, 24, 32, \dots\}$, donc $6 \vee 8 = 24$.

Propriété 7 (Caractérisation du PPCM)

Soient a et b deux entiers naturels non nuls. Soit $m \in \mathbb{N}$.
m est le PPCM de a et b si et seulement si : $\begin{cases} a \text{ et } b \text{ divise } m \\ \forall m' \in \mathbb{N}, \Big(a|m' \text{ et } b|m'\Big) \implies m|m' \end{cases}$.

Preuve.

$\Rightarrow$ Supposons que $m = a \vee b$. Alors par définition, a et b divisent m.

Montrons le deuxième point. Soit m' un multiple commun de a et b. Posons $\delta = (a \vee b) \wedge m'$. On veut montrer que $\delta = a \vee b$ (car alors $a \vee b|m'$).

On a d'une part $a|m'$ et $a|a \vee b$, donc $a|(a \vee b) \wedge m' = \delta$. De même $b|\delta$. Donc par définition du PPCM, on obtient $a \vee b \leq \delta$.

D'autre part on a par définition de δ : $\delta|a \vee b$. Ainsi $\delta = a \vee b$. D'où le résultat.

$\Leftarrow$ Soit m un entier satisfaisant ces deux propriétés. On a :

- m est un multiple de a et de b. Alors en se servant de ce qu'on vient de montrer, on a donc $a \vee b | m$.
- $a \vee b$ est un multiple de a et de b. D'où par hypothèse sur m, $m | a \vee b$.

Ainsi $a \vee b = m$ (les deux nombres étant positifs).

□

Propriété 8

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

Preuve. Si $a = 0$ ou $b = 0$, la relation est clairement vérifiée.

Supposons à présent $a, b \neq 0$ et posons $\delta = a \wedge b$ et $\mu = a \vee b$.

Montrons que $\delta\mu | ab$. On a $\delta | a$ et $\delta | b$, donc il existe $a', b' \in \mathbb{Z}$ tels que $a = a'\delta$ et $b = b'\delta$. Posons $m = \delta a' b' = ab' = a'b$. Alors $a | m$ et $b | m$, donc $\mu | m$ par propriété du PPCM. Ainsi $\delta\mu | \delta m = ab$.

Montrons que $ab | \delta\mu$. Puisque ab est un multiple du PPCM μ, il existe $n \in \mathbb{N}$ tel que $ab = \mu n$. Or μ est un multiple de a, donc il existe $c \in \mathbb{N}$ tel que $\mu = ac$. Alors $ab = \mu n = acn$ implique $b = cn$ (car $a \neq 0$). Donc $n | b$. De même, on montre que $n | a$. Ainsi par propriété du PGCD, $n | \delta$. On en déduit que $ab = \mu n$ divise $\mu\delta$.

Finalement on a montré que $\delta\mu | ab$ et que $ab | \mu\delta$, donc $ab = \delta\mu$ (ces nombres étant tous positifs). □

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

1.4 Nombres premiers

Définition.

On dit qu'un entier naturel $p \geq 2$ est **premier** si ses seuls diviseurs sont ± 1 et $\pm p$.

Remarques.

- On notera $\mathbb{P}$ l'ensemble des nombres premiers. Ainsi :

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}.$$

- 2 est le seul nombre premier pair.
- $n \in \mathbb{N}$ n'est pas premier si $n = 0, 1$ ou si $\exists a, b \geq 2$ tels que $n = ab$.
- Pour déterminer si un entier $n \geq 2$ est premier, il suffit de tester sa divisibilité par tout entier $2 \leq d \leq \sqrt{n}$.

Propriété 9

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

Preuve. On le montre par récurrence sur $n \geq 2$.
Si $n = 2$, la propriété est vraie puisque 2 est premier.
Supposons la propriété vraie pour tout $2 \leq k < n$. Au rang n :

- Si n est premier, le résultat est établi.
- Sinon $\exists a, b$ tels que $n = ab$ avec $2 \leq a, b < n$. On applique l'hypothèse de récurrence à a ou b : il existe donc p premier divisant a ou b, et donc n.

Ceci prouve la propriété au rang n. □

Propriété 10

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

Preuve. Par l'absurde, supposons que l'ensemble des nombres premiers soit fini $\mathbb{P} = \{p_1, p_2, \ldots, p_N\}$. Considérons alors l'entier $N = p_1 \times p_2 \times \cdots \times p_N + 1$. Par la proposition précédente, N est divisible par un nombre premier, c'est à dire par un entier p_k avec $1 \leq k \leq N$. Mais alors p_k divise N et p_k divise le produit $p_1 \times p_2 \times \cdots \times p_N$, donc il divise $N - p_1 \times p_2 \times \cdots \times p_N = 1$. Ce qui est impossible puisque $p_k \geq 2$. □

Crible d'Eratosthène (-276, -194).

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.

	2	3	■	5	■	7	■	■	■
11	■	13	■	■	■	17	■	19	■
■	■	23	■	■	■	■	■	29	■
31	■	■	■	■	■	37	■	■	■
41	■	43	■	■	■	47	■	■	■

Exemple de nombres premiers : les nombres de Fermat (1601-1665)
Les nombres de Fermat sont ceux de la forme $F_n = 2^{2^n} + 1$ avec $n \geq 0$. Fermat a montré que F_n est premier pour $n = 0, \ldots, 4$, et a conjecturé que $F_n \in \mathbb{P}$ pour tout n. Cette conjecture s'est avérée fausse : Euler (1707-1783) montra que $F_5 = 4294967297$ est divisible par 641. Jusqu'à aujourd'hui, on a trouvé aucun autre nombre de Fermat premier. On ne sait même pas s'il y en a.

Théorème 11 (Théorème fondamental de l'arithmétique)

Tout nombre entier $n \in \mathbb{N} - \{0, 1\}$ peut s'écrire comme un produit de facteurs premiers positifs:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \text{ avec } p_i \in \mathbb{P} \text{ deux à deux distincts et } \alpha_i \in \mathbb{N}^*$$

De plus, cette décomposition est unique à l'ordre près, et elle sera appelée la **décomposition primaire** de n, dans laquelle les exposants α_i désigneront les **valuations** associées aux **facteurs premiers** p_i.

Propriété 12 (calcul explicite du PGCD et du PPCM)

Soit un entier $a, b \in \mathbb{N} - \{0,1\}$ dont on donne les décompositions primaires génériques : $a = \prod_{p\in\mathbb{P}} p^{\alpha_p}$ et $b = \prod_{p\in\mathbb{P}} p^{\beta_p}$ avec $\alpha_p, \beta_p \in \mathbb{N}$.

(1) $a|b \Leftrightarrow \forall p \in \mathbb{P}$, $\alpha_p \leq \beta_p$.

(2) $a \wedge b = \prod_{p\in\mathbb{P}} p^{min(\alpha_p,\beta_p)}$.

(3) $a \vee b = \prod_{p\in\mathbb{P}} p^{max(\alpha_p,\beta_p)}$

Preuve.

(1) Supposons que $a|b$, alors il existe $c \in N^*$ tel que $b = ac$. On décompose c en produits de facteurs premiers : $c = \prod_{p\in\mathbb{P}} p^{\gamma_p}$. D'où en reportant dans l'égalité $b = ac$, on obtient :

$$\prod_{p\in\mathbb{P}} p^{\beta_p} = \prod_{p\in\mathbb{P}} p^{\alpha_p+\gamma_p}.$$

Par unicité de la décomposition en produit de facteurs premiers, on obtient $\beta_p = \alpha_p + \gamma_p$ pour tout p, et donc $\alpha_p \leq \beta_p$.

Réciproquement, supposons que pour tout $p \in \mathbb{P}$ on ait $\alpha_p \leq \beta_p$. Posons $c = \prod_{p\in\mathbb{P}} p^{\beta_p-\alpha_p}$. On a $c \in \mathbb{N}$ et $b = ac$. Donc $a|b$.

(2) $d = \prod_{p\in\mathbb{P}} p^{min(\alpha_p,\beta_p)}$ est bien un diviseur de a et de b (car $min(\alpha_p, \beta_p) \leq \alpha_p, \beta_p$ pour tout $p \in \mathbb{P}$). Et si d' divise a et b, $d' = \prod_{p\in\mathbb{P}} p^{\delta_p}$, alors par le premier point $\delta_p \leq \alpha_p$ et $\delta_p \leq \beta_p$, soit $\delta_p \leq \min(\alpha_p, \beta_p)$ pour tout $p \in \mathbb{P}$. Donc d' divise d. En utilisant la caractérisation du PGCD, on obtient $d = a \wedge b$.

(3) On procède de façon similaire.

□

Exemple. On peut montrer que $9100 = (2)^2(5)^2(7)(13)$ et $1848 = (2)^3(3)(7)(11)$. On en déduit donc :

$$9100 \wedge 1848 = 2^2 \times 7 = 28 \text{ , et } 9100 \vee 1848 = 2^3 \times 3 \times 5^2 \times 7 \times 11 \times 13 = 600600$$

2 Dénombrement

2.1 Généralités sur les ensembles finis

- Intuitivement, un ensemble fini de cardinal n est un ensemble $\{x_1, \ldots, x_n\}$, où les x_i décrivent E et sont deux à deux distincts.
- En interprétant ceci avec l'application $h : \begin{array}{ccc} [|1,n|] & \to & E \\ i & \mapsto & x_i \end{array}$, le fait que les x_i décrivent E signifie que h est surjective. Le fait que les x_i soient deux à deux distincts, que h est injective. Ceci motive la définition suivante.

Définition.

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

- E est l'ensemble vide, auquel cas on dit que son **cardinal** est nul.
- E est en bijection avec $\{1, 2, \ldots, n\}$, auquel cas on dit que son **cardinal** est n.

Remarque. Si les ensembles $\{1, 2, \dots, n\}$ et $\{1, 2, \dots, m\}$ sont en bijection, alors $n = m$. Le cardinal d'un ensemble fini E est donc bien défini. On le note $Card(E)$. Il indique le nombre d'éléments de E.

Exemple.

- $[|p, q|]$ est fini de cardinal $q - p + 1$ (prendre $h = i \in [|1, q - p + 1|] \mapsto p - 1 + i$).
- 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 $Card(\mathbb{U}_n) = n$.

Propriété 13 (cas particulier d'un sous-ensemble)

Soit E un ensemble fini. Alors:

(1) toute partie F de E est finie, et $Card(F) \leq Card(E)$.

(2) De plus si $Card(F) = Card(E)$, alors $F = E$.

Remarque.

- 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 $\mathbf{1}_F$ est sa fonction caractéristique, on a :

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

Propriété 14

Soient E et F deux ensembles.

(1) 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 : $Card(E) = Card(F)$.

(2) Soit $h : E \to F$ une application injective. Si F est fini, alors E est fini et $Card(E) \leq Card(F)$.

(3) Soit $h : E \to F$ une application surjective. Si E est fini, alors F est fini et $Card(F) \leq Card(E)$.

Preuve.

(1) Supposons 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.

On montre de même que si F est fini de cardinal n alors E est fini de cardinal n (en utilisant $h^{-1} : F \to E$).

(2) Supposons F fini. Posons $g : E \to h(E)$, $x \mapsto h(x)$. 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, $Card(E) = Card(h(E)) \leq Card(F)$.

(3) On suppose qu'il existe $h : E \to F$ surjective. Montrons alors qu'il existe $g : F \to E$ injective (on sera alors ramené au deuxième point).

Pour tout $a \in F$, notons $x_a \in E$ un antécédent de a par h (existe bien car h surjective). Posons $g : F \to E$, $a \mapsto x_a$. Montrons que g est injective :

Soient $(a, b) \in F^2$ tel que $g(a) = g(b)$. On a donc $x_a = x_b$. Or $h(x_a) = a$ et $h(x_b) = b$ par définition de x_a et x_b. Ainsi $a = b$ et g est injective. On conclut alors avec le premier point puisque E est fini.

□

Conséquence. Une application d'un ensemble fini dans un autre dont le cardinal est strictement inférieur au premier, ne peut pas être injective : il existe donc nécessairement deux éléments qui ont la même image. C'est ce que l'on appelle familièrement **principe des tiroirs** :

> Si on range p chaussettes dans n tiroirs et que $n < p$, il existe au moins deux chaussettes qui sont dans le même tiroir.

Exemple. En notant que :

- une personne a au plus 200000 cheveux,
- Bordeaux compte 239 000 habitants,

montrer que deux bordelais au moins ont exactement le même nombre de cheveux.

On réparti les bordelais selon leur nombre de cheveux, dans 200001 tiroirs. Puisque Bordeaux compte 239 000 habitants, le principe des tiroirs nous garantie que deux personnes au moins ont le même nombre de cheveux.

Propriété 15

Soient E, F deux ensembles de même cardinal n. On considère une application $f : E \to F$. Alors:

$$f \text{ est bijective} \Leftrightarrow f \text{ est injective} \Leftrightarrow f \text{ est surjective}$$

Preuve.

- Si f est bijective, alors f est injective et surjective.
- Supposons f injective. L'application f réalise une bijection de E sur $f(E)$. On en déduit que $Card(E) = Card(f(E))$. Comme $f(E)$ est une partie à n éléments de F un ensemble à n éléments, on a donc $f(E) = E$. Ainsi f est surjective et donc bijective.
- Supposons $f : E \to F$ surjective. On construit alors comme précédemment une application $g : F \to E$ injective telle que $f \circ g = Id_F$ (en choisissant pour chaque élément $y \in F$ un antécédent $g(y) \in E$ par f). En appliquant le point précédent, on en déduit que g est bijective. D'où f bijective puisque $f \circ g = Id_F$.

□

2.2 Opérations sur les ensembles et cardinaux

Propriété 16

Soient E, F deux ensembles finis. Alors $E \cup F$ est un ensemble fini et :

$$Card(E \cup F) = Card(E) + Card(F) - Card(E \cap F).$$

En particulier, si E et F disjoints, on a : $Card(E \cup F) = Card(E) + Card(F)$.

Preuve. Montrons cette égalité. Pour cela, on rappelle que :

$$\mathbf{1}_{E\cup F} = \mathbf{1}_E + \mathbf{1}_F - \mathbf{1}_{E\cap F}.$$

On évalue l'égalité précédente en x et on somme pour tous les $x \in E \cup F$. D'où avec la remarque précédente.

$$Card(E \cup F) = Card(E) + Card(F) - Card(E \cap F).$$

Le cas où E et F sont disjoints est immédiat. □

Propriété 17

Soient E, F deux ensembles finis.
Alors $E \times F = \{(x, y),\ x \in E \text{ et } y \in F\}$ est fini et:

$$Card(E \times F) = Card(E) \times Card(F)$$

Preuve. Notons $n = Card(E)$, $p = Card(F)$ et $E = \{e_1, e_2, \ldots, e_n\}$, $F = \{f_1, f_2, \ldots, f_p\}$. On a la partition suivante de $E \times F$:

$$E \times F = (\{e_1\} \times F) \cup (\{e_2\} \times F) \cup \cdots \cup (\{e_n\} \times F).$$

D'autre part, pour tout $1 \leq i \leq n$, on a :

$$\{e_i\} \times F = \{(e_i, f_1), (e_i, f_2), \ldots, (e_i, f_p)\}.$$

Donc $Card(F) = Card(\{e_i\} \times F)$. En utilisant la propriété précédente, on obtient finalement :

$$Card(E \times F) = \sum_{1 \leq i \leq n} Card(\{e_i\} \times F) == \sum_{1 \leq i \leq n} Card(F) = nCard(F) = Card(E) \times Card(F).$$

□

Remarque. Cette propriété se généralise immédiatement par récurrence : si E_1, ... E_p des ensembles finis, alors $E_1 \times E_2 \times \cdots \times E_p$ est fini et

$$Card(E_1 \times \cdots \times E_p) = \prod_{i=1}^{n} Card(E_i).$$

En particulier si E est un ensemble fini, E^p est fini de cardinal $(Card(E))^p$ $(p \geq 1)$.

2.3 Dénombrement des ensembles d'applications

Définition.

Soit E un ensemble fini. Une **p-liste** de E est un p-uplet d'éléments de E, c'est à dire un élément de $E^p = E \times \cdots \times E$.

Remarque. L'ordre des éléments compte et il peut y avoir des répétitions.

Propriété 18

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

Preuve. Cela découle de $\text{Card}(E^p) = \text{Card}(E)^p$. □

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 lettre sont exactement les p-listes de lettres. Il y en a n^p.

Propriété 19

Soit E un ensemble fini de cardinal n, et $p \in \mathbb{N}^*$. Le nombre de p-listes (ou p-uplets) d'éléments distincts de E est égal à $n(n-1)\ldots(n-p+1)$.

Preuve. En effet, pour composer un tel p-uplet $(e_1, e_2, \ldots, e_p)$, on a n choix possibles pour la première composante $e_1 \in E$, $n-1$ choix possibles pour la deuxième composante $e_2 \in E \setminus \{e_1\}$, ..., $n-p+1$ choix possibles pour la dernière composante $e_p \in E \setminus \{e_1, e_2, \ldots, e_{p-1}\}$. D'où finalement $n(n-1)\ldots(n-p+1)$ p-uplets d'éléments distincts de E. □

Exemple.

- Il y a $\dfrac{45!}{40!}$ 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 $20 \times 19 \times 18 = 6840$.

Propriété 20

Si l'ensemble de départ E est de cardinal p et l'ensemble d'arrivée F est de cardinal n, alors l'ensemble des applications de E dans F, noté $\mathcal{A}(E,F)$, est fini et:

$$Card(\mathcal{A}(E,F)) = n^p.$$

Preuve. Notons $e_1, e_2, \dots, e_p$ les p éléments de l'ensemble E. On considère l'application φ de $\mathcal{A}(E,F)$ dans $F^p = F \times F \times \cdots \times F$ (p fois) définie par :

$$\varphi : f \in \mathcal{A}(E,F) \mapsto (f(e_1), f(e_2), \dots f(e_p)) \in F^p.$$

Tout p-uplet $(f_1, f_2, \dots, f_p)$ admet pour unique antécédent par φ l'application $f \in \mathcal{A}(E,F)$ définie par $f(e_i) = f_i$ pour tout $1 \leq i \leq p$. Ainsi φ est bijective, et les ensembles $\mathcal{A}(E,F)$ et F^p sont équipotents. Ils ont donc même cardinal, soit :

$$Card(\mathcal{A}(E,F)) = Card(F^p) = Card(F)^p = n^p.$$

□

Propriété 21

Soit E un ensemble fini de cardinal n, et $\mathcal{P}(E)$ l'ensemble des parties de E. Alors on a $Card(\mathcal{P}(E)) = 2^n$.

Preuve. On introduit l'application qui à une partie A de E associe sa fonction indicatrice $\mathbf{1}_A$ est une bijection de $\mathcal{P}(E)$ dans $\mathcal{A}(E, \{0,1\})$. □

Propriété 22

Si l'ensemble de départ E est de cardinal p et l'ensemble d'arrivée F est de cardinal n, alors il y a $\dfrac{n!}{(n-p)!} = n(n-1)\dots(n-p+1)$ injections de E dans F si $p \leq n$, 0 sinon.

Preuve. On a vu que l'application $\varphi : f \in \mathcal{A}(E,F) \mapsto (f(1), f(2), \dots f(p)) \in F^p$ est bijective. On montre de plus aisément que $f \in \mathcal{A}(E,F)$ est injective si et seulement si $\varphi(f)$ est une p-liste d'éléments distincts de F. Ainsi l'application φ se restreint en une bijection de l'ensemble des applications injectives de E dans F sur l'ensemble des p-listes d'éléments distincts de F, dont on connait le cardinal grâce à une proposition précédente. □

Propriété 23

Soit E un ensemble fini de cardinal n. On note $S(E)$ désigne l'ensemble des bijections de E sur E (appelées également permutations dans le cas particulier où E est fini). Alors $S(E)$ est fini et:

$$Card(S(E)) = n!$$

Preuve. D'après les propositions précédentes, les permutations de E sont en fait les injections de E dans E et il y en a $\dfrac{n!}{(n-n)!} = n!$. □

2.4 Dénombrement des parties d'un ensemble fini

Définition.

Soit E un ensemble fini de cardinal n, et $p \in \mathbb{N}$. On appelle **p-combinaison de** E toute partie de E à p éléments.

Propriété 24

Soient E un ensemble fini de cardinal n et $p \in \mathbb{N}$. Le nombre de partie de E de cardinal p (ou p-combinaison de E) est $\binom{n}{p}$.

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

- $Card\left(\mathcal{C}(n,p)\right)$ choix pour l'ensemble des éléments du p-uplet (qui est une partie de E à p éléments) ;
- $p!$ choix pour ordonner cet ensemble.

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

Différence entre les p-arrangements et les parties à p éléments :

- Pour les p-listes d'éléments distincts, on tient compte de l'ordre.
- Pour les parties à p éléments, aucun ordre pris en compte.

On utilise donc les combinaisons dans tous les problèmes de choix simultanés de p éléments distincts parmi n, sans considération d'ordre et sans répétition.

Exemple. Dans une classe, on souhaite constituer des groupes de colles de 3 personnes (l'ordre des groupes n'étant pas pris en compte. Combien de répartitions possibles peut-on avoir?

Pour constituer des groupes de colles :

- on choisit 3 élèves pour constituer le 1er groupe : $\binom{48}{3}$ possibilité.
- Une fois le premier groupe de colles réalisé, je choisis 3 élèves parmi les 45 restants pour former le 2ème groupe : il y a $\binom{45}{3}$ choix.
- Ainsi de suite, ...
- Je compose le 16ème groupe : $\binom{3}{3}$ choix.

On a ainsi :

$$\binom{48}{3} \times \binom{45}{3} \times \cdots \times \binom{3}{3} = \prod_{i=1}^{16} \binom{3i}{3} = \prod_{i=1}^{16} \frac{(3i)!}{(3(i-1))!3!} = \frac{48!}{1!}\frac{1}{(3!)^{16}} = \frac{48!}{6^{16}} \text{ choix.}$$

Mais on a construit des 16-arrangements de groupes de colles : $(G_1, G_2, ..., G_{16})$ alors que ce que l'on cherche à compter ce sont les ensembles $\{G_1, G_2, ..., G_{16}\}$ de 16 groupes, sans ordre. Il faut donc diviser par 16!, nombre de façons de permuter $G_1, ..., G_{16}$. On obtient : $\frac{48!}{6^{16}\times 16!}$.

Propriété 25 (formule du triangle de Pascal)

Pour tout couple $(n,k) \in \mathbb{N}^2$, on a la relation :

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Preuve. Notons E_{n+1} un ensemble fini de cardinal $n+1$, qu'on écrit $E_{n+1} = \{e_{n+1}\} \cup E_n$, avec E_n le complémentaire de $\{e_{n+1}\}$ dans E_{n+1}. En particulier $Card(E_n) = n$.
Soit A une partie de E_{n+1} à $k+1$ éléments. On a alors deux cas possible :

- A contient l'élément e_{n+1}. Dans ce cas A est de la forme $A = F_n \cup \{e_{n+1}\}$ avec F_n une partie de E_n à k éléments.

  On a autant de telles parties que de parties F_n de E_n à k éléments, c'est à dire $\binom{n}{k}$.

- A ne contient pas l'élément e_{n+1}. Dans ce cas, une telle partie est de la forme $A = F_n$ avec F_n une partie de E_n à $k+1$ éléments.

  On a autant de telles parties que de parties F_n de E_n à $k+1$ éléments, c'est à dire $\binom{n}{k+1}$.

On en déduit l'éqalité souhaité : $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$. □

Exercice. Retrouver à l'aide d'un argument combinatoire $\binom{n}{k} = \binom{n}{n-k}$.

Pour tout entier naturel k, on note $\mathcal{P}_k(E)$ l'ensemble des parties de E à k éléments. On a h : $\begin{array}{ccc} \mathcal{P}_k(E) & \to & \mathcal{P}_{n-k}(E) \\ A & \mapsto & E\backslash A \end{array}$ bijective, donc $\mathcal{P}_k(E)$ est équipotent à $\mathcal{P}_{n-k}(E)$ et $\binom{n}{k} = \binom{n}{n-k}$.

Propriété 26 (Formule du binôme de Newton)

Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$, on a :

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

Preuve. Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$, on a :

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

Développer tout ce produit revient à choisir dans chaque facteur l'élément a ou l'élément b. Si on choisit k fois l'élément a $(0 \leq k \leq n)$, on a donc pris $n-k$ fois l'élément b pour obtenir l'élément $a^k b^{n-k}$. Reste à déterminer son coefficient : il s'agit du nombre d'occurrences de $a^k b^{n-k}$ après avoir tout développer. Or ce nombre est précisément $\binom{n}{k}$, puisqu'il correspond à choisir k fois l'élément a parmi les n facteurs du produit. D'où finalement :

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

□

Propriété 27

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

Preuve. En effet, $\mathcal{P}(E)$ est l'union disjointe des sous-ensembles $\mathcal{P}_k(E)$ des parties de E à k éléments, avec $0 \leq k \leq n$. Chacun de ces sous-ensembles est bien fini de cardinal $\binom{n}{k}$. On en déduit que $\mathcal{P}(E)$ est fini, de cardinal :

$$\mathcal{P}(E) = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

par la formule du binôme de Newton. □

Exercice. Application aux problèmes de rangement avec ou sans répétition.
Déterminer le nombre de façons de ranger p objets dans n boîtes numérotées de 1 à n :

- sans répétition ;

- avec répétition.

• Rangement sans répétition (chaque boite contient au plus un objet).
Ce problème peut se modéliser par une suite de n symboles 0 ou 1 telle que le i^e symbole vaut 1 si il y a un objet dans la i^e boite, et 0 sinon. Par exemple la suite $(1101000\dots)$ indique que les boîtes 1 et 2 contiennent un objet, la boite 3 est vide, ... Une telle suite est complètement déterminée par la partie à p éléments qui contient les 1. Il y a donc $\binom{n}{p}$ **rangements sans répétition de p objets dans n boites**.

• Rangement avec répétition (chaque boite contient plusieurs objets).
Ce problème peut se modéliser par une suite de $n+p-1$ symboles 1 ou $\bullet$ dont p sont des 1 (ils représentent les objets) et $n-1$ sont des $\bullet$ (ils représentent les $n-1$ séparations entre les n boites). Par exemple la suite $(11\bullet 1\bullet\bullet 111\bullet\dots)$ indique que la boîte 1 contient deux objets, la 2 contient un objet, la boite 3 est vide, ... Une telle suite est complètement déterminée par la partie à p éléments qui contient les 1. Il y a donc $\binom{n+p-1}{p}$ **rangements avec répétition de p objets dans n boites**.