Cours : Arithmétique

Antoine Boivin

3 février 2025

Table des matières

1 Les nombres entiers

1.1 Les entiers naturels et le principe de récurrence

Axiome 1.1 (de Peano)**.** Il existe un ensemble $\mathbb{N}$ et une fonction $s : \mathbb{N} \to \mathbb{N}$ (appelée fonction successeur) tels que :

- $\mathbb{N}$ est non-vide et contient un élément noté 0.
- $0 \notin s(\mathbb{N})$ (il n'existe pas d'entier naturel avec comme successeur 0).
- La fonction s est injective (si deux entiers ont le même successeur alors ils sont égaux).
- Si A est un sous-ensemble de $\mathbb{N}$ tel que $0 \in A$ et $s(A) \subset A$ alors $A = \mathbb{N}$ (un sous-ensemble de $\mathbb{N}$ contenant 0 et tel que si $a \in A$ alors $s(a) \in A$ est $\mathbb{N}$ tout entier.

On se fixe un tel couple $(\mathbb{N}, s)$ pour le reste du cours. Les éléments de $\mathbb{N}$ sont appelés « entiers naturels ».

Définition 1.2. Soit E un ensemble non-vide. On appelle suite dans E toute fonction $u\colon \mathbb{N} \to E$. On écrit u_n au lieu de $u(n)$ et donc $u = (u_n)_{n\in\mathbb{N}}$.

Théorème 1.3 (Récurrence)**.** *Soit $(\mathscr{P}_n)_{n\in\mathbb{N}}$ une suite d'assertions. Supposons que $\mathscr{P}_0$ soit vraie et que pour tout $n \in \mathbb{N}$, si $\mathscr{P}_n$ est vraie alors $\mathscr{P}_{s(n)}$ est vraie. Alors $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. On considère l'ensemble

$$A \coloneqq \{n \in \mathbb{N} \mid \mathscr{P}_n \text{ est vraie}\}.$$

C'est un sous-ensemble de $\mathbb{N}$ qui contient 0 ($\mathscr{P}_0$ est vraie) et pour tout $n \in A$, $s(n) \in A$. On en déduit donc que $A = \mathbb{N}$ et donc pour tout $n \in \mathbb{N}$, l'assertion $\mathscr{P}_n$ est vraie. □

Exemple 1.4. Soit (u_n) une suite dans $\mathbb{N}$ telle que $u_0 = 0$ et telle que pour tout $n \in \mathbb{N}$, $u_{s(n)} = s(u_n)$.

Montrons par récurrence que $\forall n \in \mathbb{N}, u_n = n$.

Notons, pour $n \in \mathbb{N}$, $\mathscr{P}_n$ l'assertion « $u_n = n$ ».

Initialisation : pour $n = 0$, on a $u_0 = 0$ par définition. L'assertion $\mathscr{P}_0$ est vraie.

Hérédité : Soit $n \in \mathbb{N}$ et supposons l'assertion $\mathscr{P}_n$ vraie i.e. $u_n = n$. Alors

$$u_{s(n)} = s(u_n) \overset{HR}{=} s(n)$$

On a donc montré que pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ implique $\mathscr{P}_{s(n)}$.

Conclusion : Par le principe de récurrence, on a :

$$\forall n \in \mathbb{N}, u_n = n.$$

On a ainsi montré que tout élément de $\mathbb{N}$ s'écrit comme une composée de la fonction successeur appliquée à 0.

Avertissement 1.5.

- Ne pas oublier l'initialisation.
- Ne pas écrire « Supposons que $\mathscr{P}_n$ est vraie pour tout n » ou « Supposons qu'il existe n tel que $\mathscr{P}_n$ est vraie ».
  Dans les deux cas, le raisonnement par récurrence est faux quoi qu'il arrive.
- Il faut utiliser l'hypothèse de récurrence (i.e. le fait que $\mathscr{P}_n$ soit vraie) quelque part dans l'hérédité. Sinon, le raisonnement par récurrence est superflu et un raisonnement direct fonctionne.

— Une récurrence se fait sur $\mathbb{N}$ (ou un de ses sous-ensembles) pas sur $\mathbb{R}$ ou sur un autre ensemble.

Remarque 1.6. On peut commencer une récurrence à un rang n_0 (i.e. vérifier l'initialisation pour $n = n_0$). Si on note $(\mathscr{P}_n)_{n \geq n_0}$ la suite d'assertions que l'on veut montrer, on peut considérer la suite auxiliaire $(\mathscr{R}_n)$ définie par

$$\mathscr{R}_n = \begin{cases} \text{« } 0 = 0 \text{ »} & \text{si } n < n_0 \\ \mathscr{P}_n & \text{si } n \geq n_0 \end{cases}$$

et montrer par récurrence que $\mathscr{R}_n$ est vraie pour tout $n \in \mathbb{N}$ (si P et Q sont deux assertions vraies alors $P \Rightarrow Q$ est vraie aussi).

Remarque 1.7. Pour définir une suite (u_n) de E, il y a deux possibilités :
— pour tout $n \in \mathbb{N}$, se donner un élément de E ;
— se donner u_0 et pour tout $n \in \mathbb{N}$, une façon de calculer u_{n+1} en fonction de u_n

Définition 1.8. On appelle addition la fonction $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie [1] par récurrence par :
— $\forall a \in \mathbb{N}, a + 0 = a$;
— $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, a + s(b) = s(a + b)$.
On appelle multiplication la fonction $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie [2] par récurrence par :
— $\forall a \in \mathbb{N}, a \times 0 = 0$;
— $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, a \times s(b) = (a \times b) + a$.

Remarque 1.9. Si on note 1 le successeur de 0 alors $a + 1 = s(a)$. Dans la suite, on notera $a + 1$ le successeur de a ($a + 2$ le successeur de $a + 1$,...).

Notation 1.10. La multiplication s'écrit aussi $a \cdot b$ ou ab (si le contexte est clair).

Proposition 1.11. *Soient* $p, q, r \in \mathbb{N}$. *Alors*
— $p + q = q + p$ *(commutativité de +)* ;
— $p + (q + r) = (p + q) + r$ *(associativité de +)* ;
— $p + 0 = p$ *(0 est l'élément neutre de +)* ;
— $p(q + r) = pq + pr$ *(distributivité de $\times$ par rapport à +)* ;
— $p(qr) = (pq)r$ *(associativité de $\times$)* ;
— $p \times 1 = 1 \times p = p$ *(1 est l'élément neutre de $\times$)*
— $pq = qp$ *(commutativité de $\times$)* ;

Remarque 1.12. On dit que le couple $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des monoïdes.

Définition 1.13. Soient $a, b \in \mathbb{N}$. On dit que a est supérieur [3] à b, on note $a \geq b$, s'il existe $n \in \mathbb{N}$ tel que $a = b + n$. L'entier a est strictement supérieur à b si $a \geq b$ et $a \neq b$.
On dit que a est inférieur (resp. strictement inférieur) à b si $b \geq a$ (resp. $b > a$).

Proposition 1.14. *Soient* $a, b, c, d \in \mathbb{N}$ *tels que* $a \geq c$ *et* $b \geq d$. *Alors*

1. $a + b \geq c + d$;

1. Plus précisément, on fixe un $a \in \mathbb{N}$ et on construit la suite $(u_b = a + b)_{b \in \mathbb{N}}$ par
— $u_0 = a$
— $u_{s(n)} = s(u_n)$.

2. Plus précisément, on fixe un $a \in \mathbb{N}$ et on construit la suite $(u_b = a \times b)_{b \in \mathbb{N}}$ par
— $u_0 = 0$
— $u_{s(n)} = u_n + b$.

3. sous-entendu « ou égal »

2. $ab \geq cd$.

Démonstration. Soient $n, m \in \mathbb{N}$ tels que $a = c + n$ et $b = d + m$. Alors

$$a + b = (c + d) + \underbrace{n + m}_{\in \mathbb{N}}$$

et

$$ab = (c + n)(d + m) = cd + \underbrace{cm + nd + nm}_{\in \mathbb{N}}$$

□

Corollaire 1.15 (Récurrence double)**.** *Soit $(\mathscr{P}_n)_{n\in\mathbb{N}}$ une suite d'assertions. Supposons que $\mathscr{P}_0$ et $\mathscr{P}_1$ soient vraie et que pour tout $n \in \mathbb{N}$, si $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ sont vraies alors $\mathscr{P}_{n+2}$ est vraie. Alors $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. Pour $n \in \mathbb{N}$, on note $\mathscr{R}_n$ l'assertion « $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ sont vraies ». On peut remarquer que si pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie alors en particulier, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ est vraie.

On va montrer par récurrence (simple) que $\mathscr{R}_n$ est vraie pour tout $n \in \mathbb{N}$.

Initialisation : Comme $\mathscr{P}_0$ et $\mathscr{P}_1$ sont vraies par hypothèse alors $\mathscr{R}_0$ est vraie

Hérédité : Soit $n \in \mathbb{N}$ et supposons l'assertion $\mathscr{R}_n$ vraie i.e. $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ est vraie.

Par hypothèse, le fait que $\mathscr{P}_n$ et $\mathscr{P}_{n+1}$ est vraie implique que $\mathscr{P}_{n+2}$, et donc que $\mathscr{R}_{n+1}$ est vraie puisqu'on a déjà supposé que $\mathscr{P}_{n+1}$ était vraie.

Conclusion : Par le principe de récurrence, on a montré que pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie et donc $\mathscr{P}_n$ est vraie aussi. □

Corollaire 1.16 (Récurrence forte)**.** *Soit $(\mathscr{P}_n)_{n\in\mathbb{N}}$ une suite d'assertions. Supposons que $\mathscr{P}_0$ soit vraie et que pour tout $n \in \mathbb{N}$, si $\mathscr{P}_k$ est vraie pour tout $k < n + 1$ alors $\mathscr{P}_{n+1}$ est vraie. Alors $\mathscr{P}_n$ est vraie pour tout $n \in \mathbb{N}$.*

Démonstration. Pour $n \in \mathbb{N}$, on note $\mathscr{R}_n$ l'assertion « $\mathscr{P}_k$ est vraie pour $k < n + 1$ ». On peut remarquer que si pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie alors en particulier, pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ est vraie.

On va montrer par récurrence (simple) que $\mathscr{R}_n$ est vraie pour tout $n \in \mathbb{N}$.

Initialisation : Comme $\mathscr{P}_0$ est vraie par hypothèse alors $\mathscr{R}_0$ est vraie

Hérédité : Soit $n \in \mathbb{N}$ et supposons l'assertion $\mathscr{R}_n$ vraie i.e. $\mathscr{P}_k$ est vraie pour $k < n + 1$.

Par hypothèse, cela implique que $\mathscr{P}_{n+1}$, cela implique ainsi que $\mathscr{R}_{n+1}$ est vraie puisqu'on a déjà supposé que $\mathscr{P}_k$ était vraie pour $k < n + 1$.

Conclusion : Par le principe de récurrence, on a montré que pour tout $n \in \mathbb{N}$, $\mathscr{R}_n$ est vraie et donc $\mathscr{P}_n$ est vraie aussi. □

Théorème 1.17. *Toute partie non vide A de $\mathbb{N}$ admet un et un seul plus petit élément, noté* $\min A$. *On a ainsi* $\forall a \in A, a \geq \min A$.

Démonstration. Soit A un sous-ensemble non vide de $\mathbb{N}$. Supposons par l'absurde que A n'ait pas de minimum.

On va maintenant en déduire que cela entraîne que A est vide. Pour cela, montrons par récurrence forte que l'assertion $\mathscr{P}_n : n \notin A$ est vraie pour tout $n \in \mathbb{N}$:

Initialisation : Si $0 \in A$ alors comme $A \subset \mathbb{N}$, on a en particulier, $\forall n \in A, a \geq 0$ i.e. $0 = \min(A)$. On en déduit donc que $0 \notin A$.

Hérédité : Soit $n \in \mathbb{N}$ et supposons que pour $k < n + 1$, $\mathscr{P}_k$ est vraie i.e. $\forall k < n + 1, k \notin A$. En particulier, cela veut dire que pour tout $a \in A$, $a \geq n + 1$. Ainsi, si $n + 1 \in A$ alors on aurait $\min(A) = n + 1$. Ce qui est impossible donc $n + 1 \notin A$ et donc $\mathscr{P}_{n+1}$ est vraie.

Conclusion : On en déduit que pour tout $n \in \mathbb{N}$, $\mathscr{P}_n$ est vraie et donc A est vide. □

1.2 Description de $\mathbb{Z}$

Construction 1.18. *On décrit l'ensemble $\mathbb{Z}$ de la façon suivante : c'est l'ensemble des couples d'entiers naturels $(a, b) \in \mathbb{N}^2$ où on identifie*[4] *deux couples (a, b) et (c, d) si $a + c = b + d$.*
On notera par $\overline{(a, b)}$ n'importe quel couple identifié[5] *à (a, b).*
On notera[6] *ensuite, pour $n \in \mathbb{N}$, le couple $\overline{(n, 0)}$ par n et ce faisant $\mathbb{N} \subset \mathbb{Z}$.*
On peut étendre[7] *la somme sur $\mathbb{N}$ en une opération sur $\mathbb{Z}$:*

$$\overline{(a, b)} + \overline{(c, d)} \coloneqq \overline{(a + c, b + d)}.$$

On remarque que pour tout élément $N = \overline{(a, b)}$ de $\mathbb{Z}$, $0 + N = N$ et qu'il existe un unique $N' \in \mathbb{Z}$ (qui vaut $\overline{(b, a)}$) tel que $N + N' = 0$. On notera N' par $-N$ et on dira que c'est opposé de N. Comme au moins un des deux éléments N et $-N$ est dans $\mathbb{N}$ (car si $b \geq a$, c'est $N = a - b$ et sinon, c'est $-N = b - a$) on en déduit que

$$\mathbb{Z} = \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\}.$$

Dans cette écriture, on a $\overline{(a, b)} = a + (-b)$ (que l'on écrira $a - b$).
On peut ensuite définir une multiplication sur $\mathbb{Z}$ de la façon suivante :

$$\overline{(a, b)} \cdot \overline{(c, d)} \coloneqq \overline{(bd + ac, bc + ad)}.$$

Cette définition peut se réécrire de la façon suivante :

$$(a - b) \cdot (c - d) = (ac + bd) - (bc + ad)$$

Les opérations $+$ et $\times$ héritent des propriétés de leur restriction sur $\mathbb{N}$ et on retrouve la règle des signes usuelles ($+ \cdot + = +, + \cdot - = -, - \cdot + = -, - \cdot - = +$).
On peut définir une fonction $|\cdot| : \mathbb{Z} \to \mathbb{N}$, appelée valeur absolue, par

$$\forall n \in \mathbb{Z}, |n| \coloneqq \begin{cases} n & \text{si } n \in \mathbb{N} \\ -n & \text{sinon} \end{cases}$$

Définition 1.19. Soient $a, b \in \mathbb{Z}$ deux entiers. On dit que a divise b ou que b est un multiple de a s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.
On note alors $a \mid b$.

Proposition 1.20.
- — *pour tout $a \in \mathbb{Z}$, $a|a$ (la divisibilité est réflexive) ;*
- — *pour tout $a, b, c \in \mathbb{Z}$, $(a|b$ et $b|c) \Rightarrow a|c$ (la divisibilité est transitive) ;*
- — *pour tout $a, b, c \in \mathbb{Z}$, $a|b \Rightarrow a|bc$;*
- — *pour tout $a, b, c \in \mathbb{Z}$, $(a|b$ et $a|c) \Rightarrow a|(b + c)$;*
- — *pour tout $a, b, p, q \in \mathbb{Z}$, $(a|b$ et $p|q) \Rightarrow ap|bq$;*

Remarque 1.21. Un entier est uniquement déterminé par l'ensemble de ses diviseurs puisque le plus grand d'entre eux est le nombre lui-même.

Remarque 1.22. Tout entier naturel $p \geq 2$ a au moins deux diviseurs positifs : 1 et p

Lemme 1.23. *1 n'a qu'un diviseur positif, lui-même.*

4. la relation ainsi définie est appelé relation d'équivalence et un élément de $\mathbb{Z}$ est une classe d'équivalence de cette relation.
5. ce qui est (presque) équivalent à utiliser l'ensemble des couples identifiés à (a, b)
6. De la même façon que, malgré le fait que $\mathbb{Q}$ soit l'ensemble des fractions, on écrit n pour la fraction $\frac{n}{1}$.
7. il faut vérifier que cela ne dépend pas des représentants que l'on choisit i.e. si (a, b) s'identifie à (a', b') et (c, d) avec (c', d'), on veut que les deux résultats obtenus coïncident.

Démonstration. Soit d un diviseur positif de 1 (en particulier $d \neq 0$). Il existe $c \in \mathbb{N} \setminus \{0\}$ tel que $1 = dc$. On a donc

$$1 = dc \geq d$$

On en déduit donc $d = 1$. □

Proposition 1.24. *Soient* $a, b \in \mathbb{Z} \setminus \{0\}$ *tels que* $a \mid b$ *et* $b \mid a$. *Alors* $a = \pm b$.

Démonstration. Soient $c, d \in \mathbb{N}$ tel que $c|a| = |b|$ et $d|b| = |a|$. Alors $cd|a| = |a|$ et donc $cd = 1$. On déduit du lemme précédent que $c = d = 1$ et donc $|a| = |b|$. □

Remarque 1.25. Si $a, b \in \mathbb{N}$ alors on a l'égalité $a = b$. On dit alors que $|$ est anti-symétrique.

Définition 1.26. On dit que $p \geq 2$ est un nombre premier s'il a exactement deux diviseurs positifs : 1 et lui-même. On notera $\mathbb{P}$ l'ensemble des nombres premiers.

Remarque 1.27. En particulier, 1 n'est pas premier.

Exemple 1.28. Les 26 premiers nombres premiers sont :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101.$$

Théorème 1.29. *Tout entier naturel non nul* n *est le produit de nombres premiers (1 est le produit vide) i.e. pour tout* $n \in \mathbb{N} \setminus \{0\}$, *il existe des nombres premiers (non nécessairement distincts)* $p_1, \ldots, p_r$ *tels que* $n = p_1 \ldots p_r$.

Démonstration. On va démontrer le théorème par une récurrence forte.

Initialisation : Pour $n = 1$ il n'y a rien à montrer.

Hérédité : Soit $n \in \mathbb{N} \setminus \{0\}$. On suppose que le résultat est vrai pour tout $k = 1, \ldots, n$, et on le montre pour $n + 1$. Si $n + 1$ est déjà premier, la démonstration se termine là. Sinon, on peut écrire $n + 1 = qm$, avec $2 \leq q, m \leq n$. Par l'hypothèse de récurrence, on peut écrire $q = p_1 \ldots p_s$ et $m = p_{s+1} \ldots p_r$, où pour tout i, p_i est premier. On obtient donc $n = p_1 \ldots p_r$.

On conclut par le principe de récurrence. □

Corollaire 1.30. *Tout entier non nul* n *est produit de* ± 1 *avec des nombres premiers i.e. pour tout* $n \in \mathbb{Z} \setminus \{0\}$, *il existe un signe* ± 1 *et des premiers* $p_1, \ldots, p_r$ *tels que* $n = \pm p_1 \ldots p_r$

Démonstration. Soit $n \in \mathbb{Z} \setminus \{0\}$. On applique le résultat précédent à $|n|$ et on utilise le fait que $n = \pm |n|$. □

Théorème 1.31. *Il y a une infinité de nombres premiers.*

Démonstration. Supposons par l'absurde qu'il y a un nombre fini de nombres premiers que l'on notera $p_1, \ldots, p_n$. Soit q un diviseur premier de $A = p_1 \ldots p_n + 1$ et $k \in \mathbb{N}$ tel que $A = qp$. Si $q = p_i$ pour un $i \in \{1, \ldots, n\}$, alors[8] $q(p - p_1 \ldots \widehat{p_i} \ldots p_n) = 1$ et donc q divise 1, ce qui n'est pas possible. On en déduit qu'un facteur premier de A ne serait pas dans l'ensemble $\{p_1, \ldots, p_n\}$, ce qui est absurde. Par conséquent, il existe une infinité de nombres premiers. □

Notation 1.32. Soit $a, b \in \mathbb{Z}$. On note $a \geq b$ (resp. $a > b$) si $a - b \in \mathbb{N}$ (resp. $a - b \in \mathbb{N} \setminus \{0\}$) et $a \leq b$ (resp. $a < b$) si $b - a \in \mathbb{N}$ (resp. $b - a \in \mathbb{N} \setminus \{0\}$).

Lemme 1.33. *Pour tout* $n \in \mathbb{Z}$, $|n| = \max(n, -n)$.

8. $\widehat{\ }$ désigne un élément omis

Proposition 1.34. *Soient* $a, b, c, d \in \mathbb{Z}$ *tels que* $a \leq b$ *et* $c \leq d$. *Alors* $a + c \leq b + d$ *et si* $a, c \in \mathbb{N}$ *alors* $ac \leq bd$ *et si* $b, d \leq 0$ *alors* $ac \geq bd$.

Démonstration. Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \leq b$ et $c \leq d$. Alors $b - a \in \mathbb{N}$ et $d - c \in \mathbb{N}$ et donc $b - a + d - c \in \mathbb{N}$. Autrement dit, $b + d \geq a + c$.
Pour la multiplication, on va commencer par supposer $c = d$. Alors si $c \geq 0$, on a $c(b - a) \in \mathbb{N}$ et donc $ca \geq bc$ et si $c \leq 0$ alors $c(a - b) \in \mathbb{N}$ et donc $cb \leq ca$.
Pour $d \geq c \geq 0$ alors $c(b - a) + b(d - c) \in \mathbb{N}$ et donc $ac \geq bd$ et si $0 \geq d \geq c$ alors $c(a - b) + b(c - d) \in \mathbb{N}$ et donc $ca \geq bd$. □

Définition 1.35. Un ensemble $A \subset \mathbb{Z}$ est dit minoré (resp. majoré) s'il existe $m \in \mathbb{Z}$ tel que $m \leq a$ (resp. $a \leq m$) pour tout $a \in A$.

Proposition 1.36. *Toute partie minorée de* $\mathbb{Z}$ *admet un et un seul plus petit élément. Toute partie majorée* A *de* $\mathbb{Z}$ *admet un et un seul plus grand élément.*

Démonstration. Supposons $A \subset \mathbb{Z}$ minorée par m. Alors $A - m := \{a - m \mid a \in A\}$ est une partie de $\mathbb{N}$ qui est minorée, donc $A - m$ admet un plus petit élément $\min(A - m)$. Alors $m + \min(A - m)$ est le plus petit élément de A. En effet, il existe un $a \in A$ tel que $a - m = \min(A - m)$, donc pour tout $b \in A$, on a $a = m + \min(A - m) \leq m + b - m = b$, donc $a = \min A$. Si b est aussi le plus petit élément de A alors $a \leq b$ et $b \leq a$, donc $a = b$. La deuxième affirmation se fait de la même façon. □

1.3 Division euclidienne

Théorème 1.37. *Soient* $a, b \in \mathbb{Z}$ *deux entiers avec* $b \neq 0$. *Alors*[9] *il existe un unique couple* (q, r) *d'entiers tel que*

$$a = bq + r$$

où $0 \leq r < |b|$.
On dit que q *est le quotient de la division euclidienne de* a *(le dividende) par* b *(le diviseur) et* r *est le reste.*

Démonstration. On suppose que $b > 0$ (le cas $b < 0$ se fait à partir du cas $b > 0$: si $-a = (-b)q + r$ avec $0 \leq r < -b$ alors si $r = 0$, on a $a = bq$ et si $r > 0$ alors $a = b(q + 1) + (-r - b)$, ici, $0 < -r - b < -b$). On considère l'ensemble

$$A := \{n \in \mathbb{Z} \mid a - nb < b\}.$$

Comme $|a| \geq a$ alors $|a|b \geq |a| \geq a$ (car $b \geq 1$) et donc $|a|b + b \geq a + b > a$. Il suit que $|a| \in A$, donc l'ensemble A n'est pas vide.

Montrons que l'ensemble A est minoré.

Pour $n \in A$, on a :

$$(n + 1)b > a \geq -|a| \geq -|a|b.$$

(car $|a|b \geq |a| \geq -a$, donc $a \geq -|a| \geq -|a|b$). Comme $b > 0$ alors $n + 1 \geq -|a|$, donc $n \geq -|a| - 1$ et A est minoré par $-|a| - 1$. Comme A est un sous-ensemble non-vide et minoré de $\mathbb{Z}$ alors il a un minimum que l'on notera q. On a ainsi $a - qb < b$ et $a - (q - 1)b \geq b$ (car $q - 1 \notin A$). Notons par r l'entier $a - bq$. Alors

$$r = a - bq = a - (q - 1)b - b \geq b - b = 0.$$

Le couple (q, r) vérifie bien les hypothèses de l'énoncé.

9. ce résultat et le fait que $\forall a, b \in \mathbb{Z} \setminus \{0\}, |ab| \geq |a|$ fait de la fonction $|\cdot|$ un stathme euclidien. On dit aussi $(\mathbb{Z}, |\cdot|)$ est un anneau euclidien.

On suppose que p et q vérifient

$$0 \leq a - qb < b, \quad 0 \leq a - pb < b.$$

Alors $a-(p-1)b \geq b > a-qb$, donc $qb > (p-1)b$, donc $q > p-1$, d'où $q \geq p$. En échangeant le rôle de p et q on obtient également $p \geq q$, donc $p = q$. □

Exemple 1.38. $1842 = 17 \times 108 + 6$

Proposition 1.39. *Soient* a, b *deux entiers.* b *divise* a *si, et seulement si, le reste de la division euclidienne de* a *par* b *est nul.*

Démonstration. Soient q, r le quotient et du reste de la division euclidienne de a par b. Si b divise a alors il existe $c \in \mathbb{Z}$ tel que $a = bc$. Par unicité du reste de la division euclidienne, on en déduit que $r = 0$. Réciproquement, si $r = 0$ alors $a = bq$ et donc b divise a. □

2 PGCD et PPCM

2.1 Définitions et propriétés

Lemme 2.1. *Soient* $a, b \in \mathbb{Z}$ *avec* $b \neq 0$. *Soient* q *et* r *le quotient et le reste de la division euclidienne de* a *par* b. *Les diviseurs communs de* a *et* b *sont les mêmes que les diviseurs communs de* b *et* r. *Plus généralement, pour tout* $k \in \{0, \ldots, q\}$, *les diviseurs communs de* a *et* b *sont les mêmes que les diviseurs communs de* b *et* $a - kb$.

Démonstration. Soit d un diviseur commun de a et b. Alors d divise bq (compatibilité avec la multiplication) et donc $r = a - bq$ (compatibilité avec la somme). Réciproquement, si d divise b et r alors il divise aussi $a = bq + r$. Le cas général se fait de la même façon. □

Théorème 2.2. *Soient* $a, b \in \mathbb{Z}$. *Il existe un unique entier naturel* d *dont les diviseurs sont les diviseurs communs de* a *et* b, *c'est-à-dire tel que pour tout* $n \in \mathbb{Z}$,

$$n \mid d \Leftrightarrow n \mid a \text{ et } n \mid b$$

De plus, il existe deux entiers u, v *tels que* $au + bv = d$.

Démonstration. Quitte à remplacer a par $-a$ ou b par $-b$, on peut supposer $a, b \in \mathbb{N}$.
Existence :
Démontrons par récurrence forte sur b que pour tout entier a, il existe un entier d dont les diviseurs sont les diviseurs communs à a et b et tel qu'il existe u et v tels que $au + bv = d$.
Initialisation : Si $b = 0$ alors $d = a$, $u = 1$ et $v = 0$ conviennent.
Hérédité : Soit $n \in \mathbb{N}$ et supposons le résultat vrai pour $b < n + 1$. Soit $a \in \mathbb{N}$. Comme $b = n + 1$ est non-nul, on peut faire la division euclidienne de a par b (on notera q le quotient et r le reste). Alors $r < n + 1$. On peut donc appliquer l'hypothèse de récurrence avec r (et b) : il existe un entier d dont les diviseurs sont les diviseurs communs de b et r et des entiers u_0, v_0 tels que

$$bu_0 + rv_0 = d$$

Par le lemme précédent, les diviseurs de d sont également les diviseurs de a et b. On a aussi l'égalité suivante :

$$d = bu_0 + rv_0 = bu_0 + (a - bq)v_0 = b(u_0 - qv_0) + av_0$$

Le triplet $(d, v_0, u_0 - qv_0)$ convient.
Conclusion : Si $d < 0$, il ne reste qu'à prendre sa valeur absolue pour conclure.
Unicité
Supposons qu'il existe d_1 et d_2 qui vérifient le problème. Alors d_1 divise a et b et donc divise d_2. De la même façon, d_2 divise d_1. d_1 et d_2 sont associés. Si les deux sont positifs alors ils sont égaux. □

Définition 2.3. L'entier d ainsi obtenu est appelé PGCD (plus grand diviseur commun) et est noté $\mathrm{PGCD}(a, b)$ ou $a \wedge b$. Le couple (u, v) est appelé couple de coefficients de Bézout de a et b.

Proposition 2.4. *Soient $a, b, c \in \mathbb{Z}$. Alors*

$$a \wedge b = b \wedge a$$

et

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

Démonstration. 1) Soit $d \in \mathbb{Z}$. Alors on a les équivalences suivantes :

$$d \mid a \wedge b \Leftrightarrow d \mid a \text{ et } d \mid b \Leftrightarrow d \mid b \text{ et } d \mid a \Leftrightarrow d \mid b \wedge a.$$

2) Soit $d \in \mathbb{Z}$. Alors on a les équivalences suivantes :

$$\begin{aligned} d \mid a \wedge (b \wedge c) &\Leftrightarrow (d \mid a \text{ et } d \mid (b \wedge c)) \Leftrightarrow (d \mid a \text{ et } d \mid b \text{ et } d \mid c) \\ &\Leftrightarrow (d \mid (a \wedge b) \text{ et } d \mid c) \Leftrightarrow d \mid (a \wedge b) \wedge c \end{aligned}$$

On conclut avec la remarque 1.21. □

Proposition 2.5. *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Notons q et r le quotient et le reste de la division euclidienne de a par b. Alors $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(r, b)$. Plus généralement, pour tout $k \in \{0, \ldots, q\}$, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a - kb, b)$.*

Démonstration. Soit $k \in \{0, \ldots, q\}$. Par le lemme 2.1, les diviseurs communs de a et b et ceux de b et $a - kb$ sont identiques. En particulier, ils ont le même PGCD. □

Lemme 2.6. *Une suite strictement décroissante d'entiers (i.e. une suite (u_n) telle que pour tout $n \in \mathbb{N}$, $u_n > u_{n+1}$) finit par être négative.*

Démonstration. Supposons par l'absurde que u_n est strictement positif pour tout $n \in \mathbb{N}$. Alors l'ensemble $A \coloneqq \{u_n \mid n \in \mathbb{N}\}$ est un sous-ensemble non-vide de $\mathbb{N}$. Il existe donc $n_0 \in \mathbb{N}$ tel que $u_{n_0} = \min(A)$. On obtient alors une contradiction car $A \ni u_{n_0+1} < u_{n_0} = \min(A)$. □

Proposition 2.7 (Algorithme d'Euclide)**.** *Soient $a, b \in \mathbb{Z} \setminus \{0\}$. Notons (a_n) la suite d'entiers définie (par récurrence double) comme suit (tant que cela est bien défini) :*

- *$a_0 = a$ et $a_1 = b$;*
- *pour tout $n \in \mathbb{N}$, a_{n+2} est le reste de la division euclidienne de a_n par a_{n+1}.*

La suite (a_n) finit par devenir nulle et le PGCD de A et B est le dernier a_n non nul.

Démonstration. Par le lemme précédent, la suite strictement décroissante d'entiers naturels $(|a_n|)$ ne peut pas rester strictement positive, elle finit par devenir nulle. On en déduit que la suite (a_n) devient nulle à partir d'un certain rang (que l'on notera N). Par itération de la proposition 2.1, on a :

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a_N, a_{N+1}) = \mathrm{PGCD}(a_N, 0) = |a_N|$$

(car 0 est divisible par tous les entiers). □

Remarque 2.8. On trouve les coefficients de Bézout en « remontant » cette algorithme : les égalités $\begin{cases} a_{N-3} = q_{N-1}a_{N-2} + a_{N-1} \\ a_{N-2} = q_{N-2}a_{N-1} + a_N \end{cases}$ deviennent

$$\begin{aligned} a_N &= a_{N-2} - q_{N-2}a_{N-1} = a_{N-2} - q_{N-2}(a_{N-3} - q_{N-1}a_{N-2}) \\ &= (1 + q_{N-2}q_{N-1})a_{N-2} - q_{N-2}a_{N-3} \end{aligned}$$

Et ainsi jusqu'à $a = a_0$ et $b = a_1$.

Exemple 2.9. Calculons PGCD$(42, 27)$:

$$\begin{aligned} 42 &= 27 \times 1 + 15 \\ 27 &= 15 \times 1 + 12 \\ 15 &= 12 \times 1 + 3 \\ 12 &= 3 \times 4 + 0 \end{aligned}$$

On en déduit que PGCD$(42, 27) = 3$. Quand aux coefficients de Bézout, on obtient :

$$\begin{aligned} 3 &= 15 - 12 \times 1 \\ &= 15 - (27 - 15 \times 1) = 15 \times 2 - 27 \\ &= (42 - 27) \times 2 - 27 = 42 \times 2 - 27 \times 3 \end{aligned}$$

$(2, -3)$ est donc une paire de coefficients de Bézout pour 42 et 27.

Proposition 2.10. *Soient $a, b \in \mathbb{Z}$. Il existe un unique entier naturel m dont les multiples sont les multiples communs de a et b, c'est-à-dire tel que pour tout entier $n \in \mathbb{Z}$,*

$$m \mid n \Leftrightarrow a \mid n \text{ et } b \mid n$$

Définition 2.11. L'entier m ainsi obtenu est appelé PPCM (plus petit multiple commun) et est noté PPCM(a, b) ou $a \vee b$.

Proposition 2.12. *Soient $a, b, c \in \mathbb{Z}$. Alors*

$$a \vee b = b \vee a$$

et

$$a \vee (b \vee c) = (a \vee b) \vee c$$

Démonstration. Même démonstration que le PGCD. □

Proposition 2.13. *Soient $a, b \in \mathbb{Z}$. Si $p = pa_1$ et $b = pb_1$ avec $p, a_1, b_1 \in \mathbb{Z}$ et p positif. alors*

$$a \wedge b = p(a_1 \wedge b_1) \text{ et } a \vee b = p(a_1 \vee b_1)$$

Démonstration. Si a et b sont nuls alors les résultats sont immédiats. Supposons que $a \neq 0 \neq b$. Soit $q \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :

1. $q \mid a_1 \wedge b_1$
2. $q \mid a_1$ et $q \mid b_1$
3. $pq \mid a$ et $pq \mid b$
4. $pq \mid a \wedge b$

En particulier, en prenant $q = a_1 \wedge b_1$, on obtient que $p(a_1 \wedge b_1)$ divise $a \wedge b$. De plus, comme p est un diviseur commun de a et b alors p divise $a \wedge b$ i.e. il existe r tel que $a \wedge b = pr$. On déduit des équivalences précédentes avec $q = r$ que $r \mid a_1 \wedge b_1$ et donc $a \wedge b = pr \mid p(a_1 \wedge b_1)$ et donc $a \wedge b$ et $p(a_1 \wedge b_1)$ sont associés. Comme p, $a \wedge b$ et $a_1 \wedge b_1$ sont unitaires alors on en déduit que

$$a \wedge b = p(a_1 \wedge b_1).$$

Le cas du PPCM se fait de la même façon. □

Définition 2.14. Deux entiers a, b sont dits premiers entre eux si leur PGCD vaut 1.

Corollaire 2.15. *Soient $a, b \in \mathbb{Z}$. Il existe deux entiers $a_1, b_1 \in \mathbb{Z}$ tels que $a_1 \wedge b_1 = 1$ et tels que $a = (a \wedge b)a_1$ et $b = (a \wedge b)b_1$.*

Démonstration. On utilise la proposition précédente avec $p = a \wedge b$. □

Remarque 2.16. Ce résultat nous donne l'existence d'une représentation irréductible d'une fraction : si on a une fraction $\frac{a}{b}$ alors $\frac{a_0}{b_0}$ est une représentation irréductible de cette fraction i.e. $\frac{a}{b} = \frac{(a \wedge b)a_1}{(a \wedge b)b_1} = \frac{a_1}{b_1}$ et $a_1 \wedge b_1 = 1$.

2.2 Théorèmes de Bézout et de Gauß

Proposition 2.17 (Identité de Bézout)**.** *Deux entiers $a, b \in \mathbb{Z}$ sont premiers entre eux si, et seulement si, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration. L'implication vient de la définition du PGCD. Réciproquement, supposons qu'il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$. Si d divise a et b alors d divise $au + bv = 1$ et donc $d = 1$. On en déduit donc que $\mathrm{PGCD}(a, b) = 1$. □

Théorème 2.18 (Gauß)**.** *Soient $a, b, c \in \mathbb{Z}$. Si a et b sont premiers entre eux et a divise bc alors a divise c.*

Démonstration. Comme a et b sont premiers entre eux alors il existe deux entiers u, v tels que $au + bv = 1$. On en déduit donc $auc + bvc = c$. Comme a divise bc alors a divise c. □

Corollaire 2.19. *Si a et b sont deux entiers premiers entre eux, alors*

$$a \vee b = |ab|$$

Démonstration. Les multiples de ab sont des multiples de a et de b. Réciproquement, soit n un multiple commun de a et b. Il existe un entier q tel que $n = bq$. Comme a divise $n = bq$ et $a \wedge b = 1$ alors a divise q. On en déduit que ab divise n.
On en déduit que les multiples de ab sont les multiples communs de a et de b. On en déduit donc que $a \vee b$ et ab sont associés. □

Corollaire 2.20. *Soient $a, b \in \mathbb{Z}$. Alors $|ab| = (a \wedge b)(a \vee b)$*

Démonstration. Soient $a, b \in \mathbb{Z}$. Si $a = 0$ ou $b = 0$ alors le résultat est immédiat. Supposons donc que $a \neq 0 \neq b$. Par définition du PGCD, il existe a_1 et b_1 deux entiers tels que

$$\begin{cases} a = a_1 a \wedge b \\ b = b_1 a \wedge b \end{cases}$$

Les entiers a_1 et b_1 sont premiers entre eux. On en déduit donc que

$$a_1 \vee b_1 = |a_1 b_1|$$

On en déduit donc que

$$|ab| = (a \wedge b)^2 |a_1 b_1| = (a \wedge b)^2 a_1 \vee b_1 = (a \wedge b)(a_1 a \wedge b) \vee (b_1 a \wedge b) = (a \wedge b)(a \vee b).$$

□

Interlude : Équations diophantiennes On cherche à résoudre les équations

$$ax + by = c \tag{*}$$

d'inconnues $x, y \in \mathbb{Z}$ et avec $a, b, c \in \mathbb{Z}$ fixés.
Soit $d \coloneqq a \wedge b$. Si d ne divise pas c alors l'équation n'a pas de solution (car d divise tout combinaison $ax + by$ avec $x, y \in \mathbb{Z}$). Sinon, on note a_0, b_0, c_0 les entiers tels que $a = da_0$, $b = db_0$ et $c = dc_0$. L'équation (*) est alors équivalente à l'équation

$$a_0 x + b_0 y = c_0 \tag{**}$$

Comme a_0 et b_0 sont premiers entre eux alors il existe un couple de Bézout (u, v) tel que $au + bv = 1$ et donc $auc_0 + bvc_0 = c_0$ i.e. $(x_0 \coloneqq uc_0, y_0 \coloneqq vc_0)$ est une solution particulière de (**). On peut donc écrire (**) sous la forme suivante :

$$a_0(x - x_0) + b_0(y - y_0) = 0 \tag{***}$$

Comme a_0 et b_0 sont premiers et que a_0 divise $b_0(y - y_0)$ alors par le théorème de Gauß, a_0 divise $y - y_0$ i.e. il existe $k \in \mathbb{Z}$ tel que $y = y_0 + ka_0$. En injectant cette expression dans (***), on obtient

$$a_0(x - x_0) + b_0 k a_0 = 0$$

et donc $x = x_0 - b_0 k$.
Réciproquement, les couples $(x_0 - b_0 k, y_0 + ka_0)$ (avec $k \in \mathbb{Z}$) sont solutions de (***) et donc de (*).

3 Théorème fondamental de l'arithmétique

Proposition 3.1. *Un nombre premier p est premier avec tous les entiers qu'il ne divise pas.*

Démonstration. Soit q un entier. Comme $p \wedge q$ divise p et p est premier alors $p \wedge q = 1$ ou $p \wedge q = p$. Alors soit p et q sont premiers entre eux soit p divise q. □

Corollaire 3.2 (Euclide)**.** *Un nombre premier divise un produit d'entiers si, et seulement si, il divise l'un des facteurs.*

Démonstration. Soient $p_1, \ldots, p_n \in \mathbb{Z} \setminus \{0, \pm 1\}$ des entiers. Soit $p \in \mathbb{N}$ un nombre premier qui divise $\prod_{i=1}^{n} p_i$. Supposons, par l'absurde que p ne divise aucun des p_i. Alors par la proposition précédente, pour tout i, $p \wedge p_i = 1$. Comme p divise $\prod_{i=1}^{n} p_i$ alors par itération du théorème de Gauß, p divise $\prod_{i>k} p_i$ pour tout $k \geq 0$. En particulier, p divise 1 i.e. $p = \pm 1$ qui ne sont donc pas premier , contradiction ! □

Théorème 3.3 (fondamental de l'arithmétique)**.** *Tout entier non nul n est le produit de ± 1 et de nombres premiers (1 est le produit vide). Cette décomposition est unique à permutation des facteurs près* [10].

10. On dit que l'anneau $\mathbb{Z}$ est factoriel

Démonstration. **Existence** Déjà fait.
Unicité : Soit $a = \pm a_1 \dots a_n$ une telle décomposition de l'entier a. Le signe $\pm$ est le signe de a. Les nombres premiers a_i divise a et réciproquement, les nombres premiers qui divisent a divisent l'un des a_i qui sont égaux car premiers. Les nombres apparaissant dans la décomposition sont donc tous les nombres premiers divisant a.
Soient deux décompositions de a :

$$a = \pm p_1^{\alpha_1} \dots p_r^{\alpha_r} = \pm p_1^{\beta_1} \dots p_r^{\beta_r}$$

où les p_i sont des nombres premiers distincts deux à deux. Supposons, par l'absurde qu'il existe un i tel que $\alpha_i \neq \beta_i$ Fixons-en un (sans perte de généralité, on peut supposer $\alpha_i < \beta_i$ et donc $\beta_i - \alpha_i \geq 1$). Alors

$$\prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i - \alpha_i} \prod_{j \neq i} p_j^{\beta_j}$$

Alors p_i divise $\prod_{j \neq i} p_j^{\alpha_j}$, ce qui absurde puisque p_i est premier avec les p_j, $j \neq i$. On en déduit que, pour tout i, $\alpha_i = \beta_i$ et donc la décomposition est unique à permutation près. □

Corollaire 3.4. *Soient* a, b *deux entiers non-nuls. Si*

$$a = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n} \text{ et } b = \pm p_1^{\beta_1} \dots p_n^{\beta_n}$$

où $p_1, \dots, p_n$ *sont des nombres premiers distincts deux-à-deux, alors on a :*

$$a \mid b \Leftrightarrow (\forall 1 \leq i \leq n, \alpha_i \leq \beta_i).$$

De plus,

$$a \wedge b = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)} \text{ et } a \vee b = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

Démonstration. Si $a \mid b$ alors pour tout i, $p_i^{\alpha_i}$ divise a et donc divise b. On en déduit que $\alpha_i \leq \beta_i$ (par unicité de la décomposition en facteurs premiers). Réciproquement, si pour tout i, $\alpha_i \leq \beta_i$ alors $p_i^{\alpha_i}$ divise $p_i^{\beta_i}$ et donc $\prod_i p_i^{\alpha_i}$ divise $\prod_i p_i^{\beta_i}$ i.e. a divise b.
Les diviseurs premiers communs de a et de b sont de la forme

$$d = p_1^{\delta_1} \dots p_n^{\delta_n}$$

avec $\delta_i \leq \alpha_i$ et $\delta_i \leq \alpha_i$ (i.e. $\delta_i \leq \min(\alpha_i, \beta_i)$) pour $1 \leq i \leq n$. On en déduit que le PGCD de a et b est

$$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} \dots p_n^{\min(\alpha_n, \beta_n)}.$$

De la même façon, les multiples positifs communs de a et de b sont de la forme

$$d = p_1^{\mu_1} \dots p_n^{\mu_n}$$

avec $\mu_i \geq \alpha_i$ et $\mu_i \geq \alpha_i$ (i.e. $\mu_i \geq \max(\alpha_i, \beta_i)$) pour $1 \leq i \leq n$. On en déduit que le PPCM de a et b est

$$a \vee b = p_1^{\max(\alpha_1, \beta_1)} \dots p_n^{\max(\alpha_n, \beta_n)}.$$

□

Corollaire 3.5. *Soit* $n \in \mathbb{N}$ *non nul et* p *un nombre premier. Il existe un unique exposant* $\nu_p(n)$ *tel que* $p^{\nu_p(n)} \mid n$ *et* $p^{\nu_p(n)+1}$ *ne divise pas* n*).*

Définition 3.6. L'entier $\nu_p(n)$ est appelé valuation[11] p-adique[12] de n

Corollaire 3.7. *1. Pour $n \in \mathbb{N}\setminus\{0\}$, $\nu_p(n) = 0$ sauf pour un nombre fini de p, cela justifie l'écriture :* $n = \prod_{p\in\mathbb{P}} p^{\nu_p(n)}$.

2. $\forall a, b \in \mathbb{N}\setminus\{0\}, \forall p \in \mathbb{P}, \nu_p(ab) = \nu_p(a) + \nu_p(b)$

3. $\forall a, b \in \mathbb{N}\setminus\{0\}, \forall p \in \mathbb{P}, \nu_p(a \pm b) \geq \min(\nu_p(a), \nu_p(b))$, *avec égalité si* $\nu_p(a) \neq \nu_p(b)$

4. $\forall a, b \in \mathbb{N}\setminus\{0\}, \forall p \in \mathbb{P}, \nu_p(a\wedge b) = \min(\nu_p(a), \nu_p(b)), \nu_p(a\vee b) = \max(\nu_p(a), \nu_p(b))$

Démonstration. 1) Il n'y a qu'un nombre fini de nombres premiers dans la décomposition en facteurs premiers d'un entier.

2) Soit $a, b \in \mathbb{N}\setminus\{0\}$. Alors[13]

$$ab = \prod_{p\in\mathbb{P}} p^{\nu_p(a)} \prod_{p\in\mathbb{P}} p^{\nu_p(b)} = \prod_{p\in\mathbb{P}} p^{\nu_p(a)+\nu_p(b)}$$

Par unicité de la décomposition en facteurs premiers, on en déduit que $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ pour tout premier p.

3) Soient $a, b \in \mathbb{N}\setminus\{0\}$ et p un nombre premier. Il existe $d, e \in \mathbb{N}$ tel que $a = dp^{\nu_p(a)}$ et $b = dp^{\nu_p(b)}$. Alors

$$a \pm b = p^{\min(\nu_p(a),\nu_p(b))} \underbrace{(dp^{\overbrace{\nu_p(a) - \min(\nu_p(a),\nu_p(b))}^{\in\mathbb{N}}} \pm ep^{\overbrace{\nu_p(b) - \min(\nu_p(a),\nu_p(b))}^{\in\mathbb{N}}})}_{\in\mathbb{N}}$$

On en déduit donc que $\nu_p(a \pm b) \geq \min(\nu_p(a), \nu_p(b))$ et si $\nu_p(a) \neq \nu_p(b)$, un des termes de la somme est divisible par p et pas l'autre donc, la somme n'est pas divisible par p, ce qui donc est un cas d'égalité.

4) Soient $a, b \in \mathbb{N}\setminus\{0\}$ et p un nombre premier. Alors, par le lemme 3.4, on a :

$$a \wedge b = \left(\prod_{p\in\mathbb{P}} p^{\nu_p(a)}\right) \wedge \left(\prod_{p\in\mathbb{P}} p^{\nu_p(b)}\right) = \prod_{p\in\mathbb{P}} p^{\min(\nu_p(a),\nu_p(b))}$$

Par unicité de la décomposition en facteurs premiers, on en déduit que $\nu_p(a\wedge b) = \min(\nu_p(a), \nu_p(b))$. Idem pour le PPCM. □

Proposition 3.8. *Pour tous nombres entiers non nuls a, b, c, on a*

$$a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c) \quad \textit{et} \quad a\vee(b\wedge c) = (a\vee b)\wedge(a\vee c).$$

Démonstration. Cela vient du résultat précédent et du fait que pour tout α, β, γ,

$$\min(\alpha, \max(\beta, \gamma)) = \max(\min(\alpha, \beta), \min(\alpha, \gamma))$$

11. Une valuation (discrète) est une fonction $v\colon A \to \mathbb{Z}\cup\{+\infty\}$ (avec l'ordre prolongeant celui sur $\mathbb{Z}$ et tel que $n < +\infty$ pour tout $n \in \mathbb{Z}$), où A est un anneau commutatif, telle que
— $\forall x \in A, v(x) = +\infty \Leftrightarrow x = 0$
— $\forall x, y \in A, v(xy) = v(x) + v(y)$ (où $n + (+\infty) = +\infty$)
— $\forall x, y \in A, v(x + y) = \min(v(x), v(y))$

12. On peut étendre cette valuation à $\mathbb{Q}$ de la façon suivante : si m, n sont premiers entre eux alors

$$\nu_p\left(\frac{m}{n}\right) \coloneqq \nu_p(m) - \nu_p(n)$$

Un théorème d'Ostrowski énonce que les valuations p-adiques sont les seules valuations (discrètes) sur $\mathbb{Q}$ (à coefficient multiplicatif près) qui ne soient pas triviales (i.e. $v(0) = +\infty$ et 0 sinon).

13. Cette écriture est légitime car il n'y a qu'un nombre fini de facteurs différents de 1 qui apparaissent

et

$$\max(\alpha, \min(\beta, \gamma)) = \min(\max(\alpha, \beta), \min(\alpha, \gamma))$$

Si $\alpha \geq \max(\beta, \gamma)$ alors $\alpha \geq \beta$ et $\alpha \geq \gamma$ et donc on a à gauche et à droite $\max(\beta, \gamma)$.

Si $\alpha \leq \beta$ alors à gauche, on a α et à droite $\max(\alpha, \min(\alpha, \gamma) = \alpha$ (car $\min(\alpha, \gamma) \leq \alpha$) et si $\alpha \leq \gamma$ alors à gauche, on a α et à droite $\max(\min(\alpha, \beta), \alpha) = \alpha$ (car $\min(\alpha, \beta) \leq \alpha$) □

4 Systèmes de numération

Dans la première section, nous avons décrit les entiers naturels comme une itération de la fonction successeur de 0. Le but de cette section est de donner une façon efficace de les décrire.
De façon analogue à l'écriture des mots, nous allons utiliser un alphabet (i.e. un ensemble de symboles que l'on appelera ici « chiffres ») et écrire les entiers naturels comme une concaténation d'éléments de cet alphabet.

Exemple 4.1. Dans la suite, on notera Σ l'alphabet en question.

- L'écriture décimale usuelle où $\Sigma = \{0, 1, 2, \ldots, 9\}$ et où une suite finie $\overline{c_n \ldots c_1 c_0}^{10}$ (qu'on écrira la plupart du temps $c_n \ldots c_1 c_0$) représente le nombre $c_n 10^n + c_{n-1} 10^{n-1} + \ldots + c_1 10 + c_0$. L'écriture 83874 représente ainsi le nombre $8 \times 10^4 + 3 \times 10^3 + 8 \times 10^2 + 7 \times 10 + 4$.
- L'écriture binaire où $\Sigma = \{0, 1\}$ et où une suite finie $\overline{c_n \ldots c_1 c_0}^2$ représente le nombre $c_n 2^n + c_{n-1} 2^{n-1} + \ldots + c_1 2 + c_0$. L'écriture $\overline{10001}^2$ représente le nombre $1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$ qui s'écrit 17 en écriture décimale.
- Plus généralement, si b est un entier supérieur à 2, on peut utiliser l'alphabet $\Sigma = \{0, \ldots, b-1\}$ et considérer que la suite finie $\overline{c_n \ldots c_0}^b$ (le b et le surlignement peut ne pas être écrit s'il n'y a pas d'ambiguïté) représente[14] le nombre $c_n b^n + c_{n-1} b^{n-1} + \ldots + c_1 b + c_0$.
- Il existe d'autres systèmes de numération : on peut prendre $\Sigma = \{0, 1\}$ et considérer que la suite finie $\overline{c_n \ldots c_0}$ représente[15] le nombre $c_n F_n + \ldots + c_1 F_1 + c_0$ (où (F_n) est la suite de Fibonacci définie par récurrence double par $F_0 = F_1 = 1$ et pour tout $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$)

Théorème 4.2. *Soit b un entier supérieur à 2. Pour tout entier naturel N, il existe un unique e et d'uniques chiffres (en base b) $c_0, \ldots, c_e$, avec $c_e \neq 0$, tels que $N = \overline{c_e \ldots c_1 c_0}$.*

Démonstration. Montrons tout d'abord l'existence de l'écriture : Considérons les suites (q_n) définie par $q_0 = N$ et $r_0 = 0$ et q_{n+1} est le quotient de la division euclidienne de q_n par b et r_{n+1} son reste. Comme (q_n) est une suite strictement décroissante d'entiers naturels, elle finit par s'annuler. Notons n_0 le plus petit entier pour lequel $q_{n_0} = 0$. On en déduit alors que

$$N = q_1 b + r_1 = (q_2 b + r_2) b + r_1 = \ldots = \sum_{i=1}^{n_0} r_i b^{i-1}$$

On obtient donc une écriture de N ($e = n_0 - 1$ et $c_i = r_{i-1}$).

14. si $36 \geq b > 10$, on continue la suite $0, \ldots, 9$ par $A, B, \ldots, Z$ puis si $b \geq 37$, on finit par écrire les différents chiffres entre « ; » : en base 97, $\overline{12;7;85}$ représente le nombre $12 \times 97^2 + 7 \times 97 + 85$ qui s'écrit 113672 en écriture décimale

15. Un théorème de Zeckendorf nous dit que tout entier peut s'écrire sous cette forme en imposant que deux c_i consécutifs ne peuvent pas être simultanément égaux à 1

Montrons l'unicité de e : Soit $\overline{c_e \dots c_0}$ et $\overline{d_f \dots d_0}$ deux écritures de N. On a alors $c_e \neq 0 \neq d_f$. Par conséquent, $N \geq b^e$ et $N \geq b^f$. De plus, comme les $c_i \in \{0, \dots, b-1\}$, on a alors

$$b_e < N = \sum_{k=0}^{f} d_k b^k \leq (b-1) \sum_{k=0}^{f} b^k = b^{f+1} - 1 < b^{f+1}$$

On en déduit donc $e < f+1$ et $e \leq f$. Par symétrie de rôles, on a $f \leq e$ et donc $e = f$.

Montrons l'unicité de l'écriture :
Supposons par l'absurde qu'il y a deux écritures distinctes $\overline{d_e \dots d_0}$ et $\overline{c_e \dots c_0}$ de N i.e. qu'il existe un i tel que $c_i \neq d_i$. Notons i le plus grand entier tel que $c_i \neq d_i$. Par définition, on a alors, pour tout $j \geq i$, $c_j = d_j$. On a donc

$$0 = \left(\sum_{k=0}^{e} c_k b^k \right) - \left(\sum_{k=0}^{e} d_k b^k \right) = \sum_{k=0}^{e} (c_k - d_k) b^k = \sum_{k=0}^{i} (c_k - d_k) b^k$$

On a $|c_i - d_i| \geq 1$ (car $c_i \neq d_i$) et pour $1 \leq k \leq i-1$, $|c_k - d_k| \leq |b - 1 - 0| = b - 1$. D'où

$$\begin{aligned} b^i &\leq |(c_i - d_i) b^i| \\ &\leq \left| \sum_{k=0}^{i-1} (c_k - d_k) b^k \right| \overset{\text{IT}}{\leq} \sum_{k=0}^{i-1} |c_k - d_k| b^k \\ &\leq \sum_{k=0}^{i-1} (b-1) b^k = b^i - 1 \end{aligned}$$

On obtient ainsi une contradiction. □

Exemple 4.3. 17 en base $2, 3, 4$:

$$\begin{aligned} 17 &= 8 \times 2 + 1 = (4 \times 2 + 0) \times 2 + 1 \\ &= ((2 \times 2 + 0) \times 2 + 0) \times 2 + 1 = (((1 \times 2 + 0) \times 2 + 0) \times 2 + 0) \times 2 + 1 \\ &= ((((0 \times 2 + 1) \times 2 + 0) \times 2 + 0) \times 2 + 0) \times 2 + 1 \\ &= 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \\ 17 &= 5 \times 3 + 2 = (1 \times 3 + 2) \times 3 + 2 = ((0 \times 3 + 1) \times 3 + 2) \times 3 + 2 \\ &= 3^2 + 2 \times 3^1 + 2 \times 2^0 \\ 17 &= 4 \times 4 + 1 = (1 \times 4 + 0) \times 4 + 1 = ((0 \times 4 + 1) \times 4 + 0) \times 4 + 1 = 1 \times 4^2 + 0 \times 4 + 1 \times 4^0. \end{aligned}$$

5 Arithmétique modulaire

5.1 $\mathbb{Z}/n\mathbb{Z}$

Définition 5.1. Soit $n \geq 2$ un entier et soient $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n, et on note $a \equiv b \mod n$ si a et b ont le même reste de la division euclidienne par n ou, de façon équivalente, si $a - b$ est un multiple de n.

On note $x + n\mathbb{Z}$ l'ensemble de tous les entiers y congrus à x modulo n. Lorsque n est fixé, on note souvent $\overline{x}$ au lieu de $x + n\mathbb{Z}$:

$$\overline{x} = \{y \in \mathbb{Z} \mid x - y \in n\mathbb{Z}\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes $\overline{x}$ avec $x \in \mathbb{Z}$.

Lemme 5.2. *Soient* $n \geq 2$ *et* $x, y \in \mathbb{Z}$. *Alors* $x + n\mathbb{Z} = y + n\mathbb{Z}$ *si, et seulement si,* $x \equiv y \mod n$.

Démonstration. Si $x + n\mathbb{Z} = y + n\mathbb{Z}$ alors $y \in x + n\mathbb{Z}$ et donc n divise $y - x$. Réciproquement, si $x \equiv y \mod n$ alors il existe $k \in \mathbb{Z}$ tel que $x = y + nk$. Si $x + n\ell \in x + n\mathbb{Z}$ alors $x + n\ell = y - nk + n\ell = y + y + (\ell - k) \in y + n\mathbb{Z}$ et si $y + n\ell \in y + n\mathbb{Z}$ alors $y + n\ell = x + nk + n\ell = x + n(k + \ell) \in x + n\mathbb{Z}$. On en déduit donc que $x + n\mathbb{Z} = y + n\mathbb{Z}$. □

Proposition 5.3. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ *et est donc de cardinal* n.

Démonstration. Pour chaque $x \in \mathbb{Z}$, on effectue la division euclidienne $x = qn + r$ avec $0 \leq r \leq n - 1$. Alors $x \equiv r \mod n$ et on obtient le résultat. □

Lemme 5.4. *Soit* $n \in \mathbb{N}, n \geq 2$. *Pour tout* x, y, a, b *tel que* $x \equiv a \mod n$ *et* $y \equiv b \mod n$, *on a*

— $x + y \equiv a + b \mod n$
— $xy \equiv ab \mod n$

Démonstration. Par hypothèse, il existe $p, q \in \mathbb{Z}$ tels que $x = a + pn$ et $y = b + qn$. Alors

$$x + y = (a + b) + \underbrace{(p + q)}_{\in \mathbb{Z}} n$$

et

$$xy = ab + \underbrace{(pb + aq + pqn)}_{\in \mathbb{Z}} n$$

□

Proposition 5.5. *Les opérations* $(\overline{x}, \overline{y}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mapsto \overline{x + y} \in \mathbb{Z}/n\mathbb{Z}$ *et* $(\overline{x}, \overline{y}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mapsto \overline{xy} \in \mathbb{Z}/n\mathbb{Z}$ *sont bien définies*

Démonstration. Le lemme précédent nous dit que si $\overline{x} = \overline{a}$ et $\overline{y} = \overline{b}$ alors $\overline{x + y} = \overline{a + b}$ et $\overline{xy} = \overline{ab}$, ce qui revient à dire que les deux opérations sont bien définies. □

Notation 5.6. On note $\overline{+}$ et $\overline{\times}$ ces deux opérations.

Proposition 5.7. *Pour* $n \geq 2$, *les opérations* $\overline{+}$ *et* $\overline{\times}$ *de* $\mathbb{Z}/n\mathbb{Z}$ *héritent des propriétés de* $+$ *et* $\times$ *de* $\mathbb{Z}$.

Théorème 5.8 (des restes chinois)**.** *Soient* $a, b \in \mathbb{N} \setminus \{0, 1\}$ *tels que* $a \wedge b = 1$. *La fonction* $\varphi : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ *définie par* $\varphi(x + ab\mathbb{Z}) = (x + a\mathbb{Z}, x + b\mathbb{Z})$ *est une bijection dont la réciproque est donnée par*

$$\psi(x + a\mathbb{Z}, y + b\mathbb{Z}) = bvx + auy + ab\mathbb{Z}$$

où $au + bv = 1$ *est une relation de Bézout (qui existe car* a *et* b *sont premiers entre eux).*

Autrement dit, si a et b sont premiers entre eux alors pour $m, n \in \mathbb{Z}$, il existe un unique $p \in \{0, \ldots, ab - 1\}$ tel que $\begin{cases} x \equiv m \mod a \\ y \equiv n \mod b \end{cases} \Leftrightarrow x \equiv p \mod ab$ et alors, $p \equiv m \mod a$ et $q \equiv n \mod b$.

Démonstration. La fonction φ est bien définie car si $y \equiv x \mod ab$ alors $x \equiv y \mod a$ et $x \equiv y \mod b$ et la fonction ψ est bien définie car si $x \equiv x_0 \mod a$ (i.e. $x = x_0 + ak$ pour $k \in \mathbb{Z}$) et $y \equiv y_0 \mod b$ (i.e. $y = y_0 + b\ell$ pour $\ell \in \mathbb{Z}$) alors

$$bvx + auy = bv(x_0 + ak) + au(y_0 + b\ell) = bvx_0 + auy_0 + ab(kv + \ell u) \equiv auy_0 + bvx_0 \mod ab$$

Pour $x + ab\mathbb{Z} \in \mathbb{Z}/ab\mathbb{Z}$, on a :

$$\psi(\phi(x + ab\mathbb{Z})) = \psi(x + a\mathbb{Z}, x + b\mathbb{Z}) = bvx + aux + ab\mathbb{Z} = x + ab\mathbb{Z}$$

et pour $(x + a\mathbb{Z}, y + b\mathbb{Z}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, on a :

$$\begin{aligned}\varphi(\psi(x + a\mathbb{Z}, y + b\mathbb{Z})) &= \varphi(bvx + auy + ab\mathbb{Z}) = (bvx + auy + a\mathbb{Z}, bvx + auy + b\mathbb{Z}) \\ &= (bvx + a\mathbb{Z}, auy + b\mathbb{Z}) \\ &= ((1 - au)x + a\mathbb{Z}, (1 - bv)y + b\mathbb{Z}) \\ &= (x + a\mathbb{Z}, y + b\mathbb{Z})\end{aligned}$$

On en déduit ainsi que φ et ψ sont réciproques l'une de l'autre et sont donc des bijections. □

Remarque 5.9.

1. Par unicité de la bijection réciproque, la fonction ψ ne dépend pas du couple (u, v) choisi.
2. On peut remarquer que les fonctions φ et ψ sont compatibles avec les opérations $\overline{+}$ et $\overline{\times}$:
$$\forall \overline{m}, \overline{n} \in \mathbb{Z}/ab\mathbb{Z}, \varphi(\overline{m}\overline{+}\overline{n}) = \varphi(\overline{m})\overline{+}\varphi(\overline{n})$$
et
$$\forall \overline{m}, \overline{n} \in \mathbb{Z}/ab\mathbb{Z}, \varphi(\overline{m}\overline{\times}\overline{n}) = \varphi(\overline{m})\overline{\times}\varphi(\overline{n})$$
(idem pour ψ)

Soient $a_1, \ldots, a_n$ des nombres naturels premiers entre eux deux à deux. Le système

$$\begin{cases} z \equiv x_1 \mod a_1 \\ z \equiv x_2 \mod a_2 \\ \vdots \\ z \equiv x_n \mod a_n \end{cases}$$

admet une infinité de solutions $z \in z_0 + a_1 \cdots a_n\mathbb{Z}$. Pour trouver le z_0 on procède comme suit :
On note $a = a_1 \cdots a_n$ et $b_i = \prod_{j \neq i} a_j$, $i = 1, \ldots, n$. Alors $\text{PGCD}(b_i, a_i) = 1$ (car les a_i sont premiers entre eux deux à deux). On prend un couple de Bézout (u_i, v_i) tel que $u_i b_i + v_i a_i = 1$. Il suit que $b_i u_i \equiv \delta_{i,j} \mod a_j$, où $\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$.
Il suffit de prendre $z_0 = x_1 b_1 u_1 + \ldots + x_n b_n u_n$.

Définition 5.10. Un élément $\overline{x}$ est dit inversible (pour la multiplication) s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x}\overline{\times}\overline{y} = \overline{1}$. On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble [16] des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 5.11. *Pour $n \geq 2$, on a :*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{x + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \mid 1 \leq x \leq n \text{ et } \text{PGCD}(x, n) = 1\}$$

Démonstration. On procède par double inclusion :
Soit $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^*$. Alors, par définition, il existe $\overline{y} \in (\mathbb{Z}/n\mathbb{Z})$ tel que $\overline{xy} = \overline{1}$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que

$$xy = 1 + nk$$

On obtient une identité de Bézout entre x et n. On en déduit que $\text{PGCD}(n, k) = 1$.
Réciproquement, si on prend $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ avec $\text{PGCD}(x, n) = 1$. Alors, on a une identité de Bézout (u, v) tel que $xu + nv = 1$ et donc $\overline{xu} = \overline{1}$. □

16. On dira souvent « groupe des inversibles » car la multiplication de $\mathbb{Z}/n\mathbb{Z}$ se restreint en une loi sur $(\mathbb{Z}/n\mathbb{Z})^*$ qui en fait un groupe.

Exemple 5.12. — Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.
— $(\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1}, \overline{3}\}$ et $(\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$.

Corollaire 5.13. *Soient a, b deux entiers premiers entre eux. Alors la bijection φ précédente induit une bijection entre les inversibles*

$$\varphi_{|(\mathbb{Z}/ab\mathbb{Z})^*} : (\mathbb{Z}/ab\mathbb{Z})^* \to (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*.$$

Démonstration. Soit $x \in \mathbb{Z}$. Alors x est premier avec ab si, et seulement si, x est premier avec a et b (car $\min(\alpha + \beta, \gamma) \geq 1$ si, et seulement si, $\gamma \geq 1$ et ($\alpha \geq 1$ ou $\beta \geq 1$) où α, β, γ sont les différentes valuations de respectivement a, b et x). On conclut avec la proposition précédente. □

Remarque 5.14. C'est aussi un corollaire immédiat du deuxième point de la remarque 5.9

5.2 Fonction indicatrice d'Euler

Lemme 5.15. *Soit p un nombre premier. Alors, pour tout $k \in \{1, \dots, p-1\}$, p divise $\binom{p}{k}$.*

Démonstration. Soit $k \in \{1, \dots, p-1\}$. Alors

$$k\binom{p}{k} = k\frac{p!}{(p-k)!k!} = \frac{p!}{(p-k)!(k-1)!} = p\binom{p-1}{k-1}.$$

Comme p et k sont premiers entre eux alors par le théorème de Gauß, p divise $\binom{p}{k}$ □

Théorème 5.16 (Petit théorème de Fermat)**.** *Soit p un nombre premier et soit $a \in \mathbb{Z}$. On a $a^p \equiv a \mod p$. De plus, si $\mathrm{PGCD}(a, p) = 1$ alors $a^{p-1} \equiv 1 \mod p$.*

Démonstration. Soit $a \in \mathbb{Z}$. Si $a \equiv 0 \mod p$ alors $a^p \equiv 0 \mod p$ et donc $a^p \equiv a \mod p$. Grâce au lemme précédent, on sait que, pour tout $k \in \mathbb{Z}$,

$$(k+1)^p = \sum_{i=0}^{p} \binom{p}{i} k^i \equiv k^p + 1 \mod p$$

En itérant ces congruences à partir du cas $k = 0$, on en déduit le résultat.
Si $\mathrm{PGCD}(a, p) = 1$ alors il existe $u \in \mathbb{Z}$ tel que $au \equiv 1 \mod p$ et donc on a $ua^p \equiv ua \mod p$ i.e. $a^{p-1} \equiv 1 \mod p$. □

Exemple 5.17. Calculons le reste de la division euclidienne de 679^{999} par 13. On a

$$679 \equiv 52 \times 13 + 3 \equiv 3 \mod 13$$

donc $679^{999} \equiv 3^{999} \mod 13$. Or le petit théorème de Fermat nous dit que $3^{12} \equiv 1 \mod 13$ car 13 est premier. On effectue donc la division euclidienne de 999 par 12 : $999 \equiv 83 \times 12 + 3$ pour en déduire que $679^{999} \equiv 3^{999} \equiv 3^3 \equiv 1 \mod 13$.

Définition 5.18. On appelle fonction indicatrice d'Euler la fonction $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ donnée par

$$\varphi(n) \coloneqq \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^*).$$

Théorème 5.19. *Si $\mathrm{PGCD}(x, n) = 1$ alors $x^{\varphi(n)} \equiv 1 \mod n$.*

Démonstration. Voir TD3 □

Pour calculer la valeur de $\varphi(n)$, nous allons tout d'abord montrer que φ est multiplicative.

Proposition 5.20. *Soient $n \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \ldots, a_n$ des nombres premiers entre eux deux-à-deux. Alors*

$$\varphi\left(\prod_{i=1}^{n} a_i\right) = \prod_{i=1}^{n} \varphi(a_i).$$

Démonstration. Montrons ce résultat par récurrence sur n.

Initialisation : Le cas $n = 2$ est une conséquence immédiate du lemme des restes chinois.

Hérédité : Soit $n \geq 2$ et supposons la propriété vraie au rang n.

Soient $a_1, \ldots, a_{n+1}$ des nombres entiers premiers entre eux deux-à-deux. Alors a_{n+1} et $\prod_{i=1}^{n} a_i$ sont premiers entre eux. Grâce à l'initialisation, on a :

$$\varphi\left(\prod_{i=1}^{n+1} a_i\right) = \varphi\left(\prod_{i=1}^{n} a_i\right) \varphi(a_{n+1}).$$

Puis grâce à l'hypothèse de récurrence,

$$\varphi\left(\prod_{i=1}^{n+1} a_i\right) = \prod_{i=1}^{n} \varphi\left(a_i\right) \varphi(a_{n+1}) = \prod_{i=1}^{n+1} \varphi\left(a_i\right).$$

Par le principe de récurrence, on obtient le résultat désiré. □

Proposition 5.21. *Si $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ alors*

$$\varphi(n) = \prod_{p \in \mathbb{P}} p^{\nu_p(n)-1}(p-1).$$

Démonstration. Ceci se démontre en deux étapes grâce au résultat précédent.

1. Si $n = p^d$ alors

$$\begin{aligned}\varphi(n) &= \mathrm{Card}\{x \in \{1, \ldots, p^d\} \mid \mathrm{PGCD}(x, p^d) = 1\} \\ &= \mathrm{Card}\{x \in \{1, \ldots, p^d\} \mid p \mid x\} \\ &= p^d - \mathrm{Card}\{p, 2p, \ldots, p^{d-1}p\} = p^d - p^{d-1} \\ &= p^{d-1}(p-1).\end{aligned}$$

2. Si $n = \prod_{i=1}^{d} p_i^{a_i}$ alors comme les $p_i^{a_i}$ sont premiers entre eux, on obtient grâce à la proposition précédente et au cas précédent, les égalités suivantes :

$$\varphi(n) = \varphi\left(\prod_{i=1}^{d} p_i^{a_i}\right) = \prod_{i=1}^{d} \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^{d} p_i^{a_i-1}\left(p_i - 1\right)$$

□