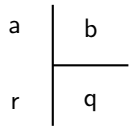
Annexe A Structures algébriques et division euclidienne

A.1 Division euclidienne

Théorème 1 (division euclidienne dans $\mathbb{N}$)
Soient deux entiers $a \in \mathbb{N}$ et $b \in \mathbb{N}$. Si b n'est pas nul, alors

$$\exists!(q,r) \in \mathbb{N}^2, \quad a = bq + r \quad \text{et} \quad r < b.$$



Exercice 2 — *Montrer que :*

(i) $\frac{49}{333} = 0,\overline{147}$ *;*

(ii) un réel est rationnel si, et seulement si, il possède un développement décimal périodique.

Théorème 3 (division euclidienne dans $\mathbb{K}[X]$)
Soient deux polynômes $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$. Si B n'est pas nul, alors

$$\exists!(Q,R) \in \mathbb{K}[X]^2, \quad A = BQ + R \quad \text{et} \quad \deg R < \deg B.$$

Exercice 4 — *Pour tout $n \in \mathbb{N}$, déterminer le reste R_n de la division euclidienne du polynôme X^n par le polynôme $X^2 - (n-2)X - (n-1)$.*

A.2 Structures algébriques

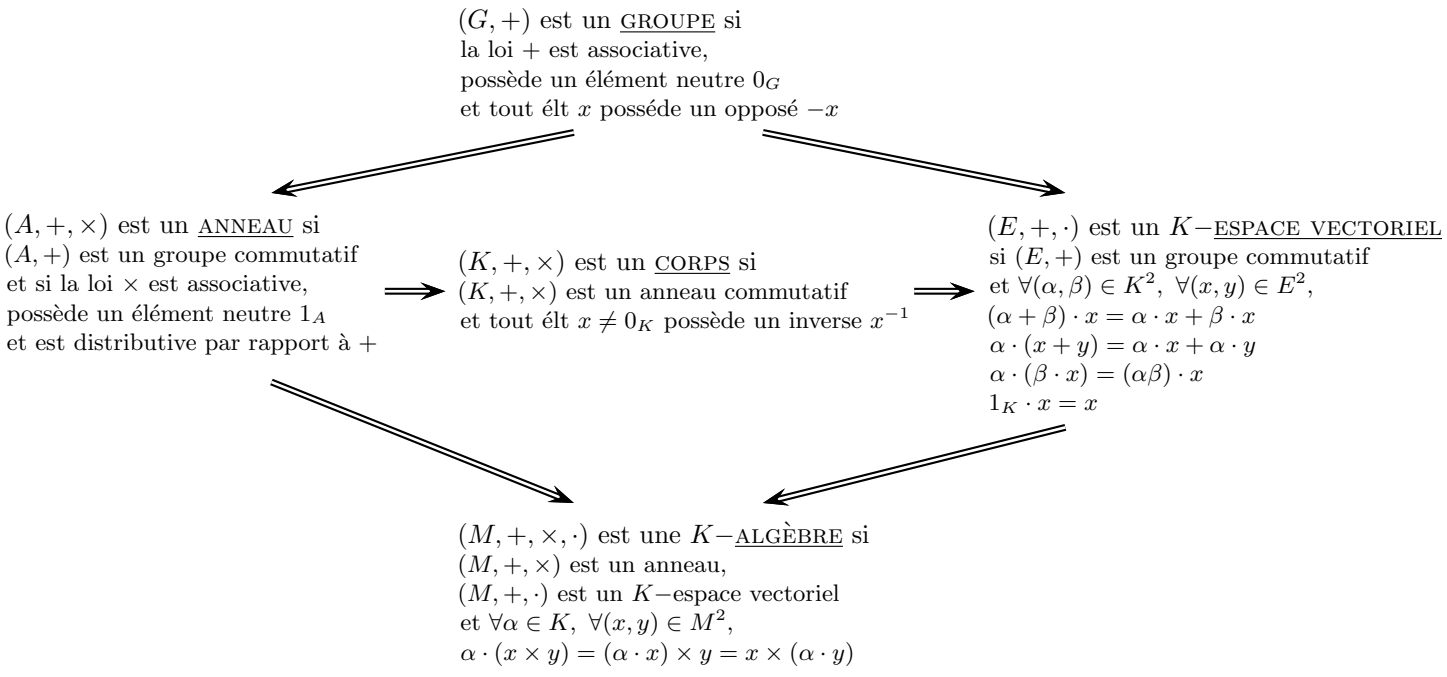


Figure A.1 – Structures algébriques

On dit qu'une partie H d'un groupe $(G,+)$ est un sous-groupe de G si H est stable par $+$ et si, muni de la loi induite, $(H,+)$ est encore un groupe. On définit de même un sous-anneau, un sous-corps, un sous-espace vectoriel et une sous-algèbre.

EXERCICE 5 (**les sous-groupes additifs de $\mathbb{Z}$**) —

1. *Soit $n \in \mathbb{Z}$. Montrer que l'ensemble $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\} = \{y \in \mathbb{Z} \mid \exists x \in \mathbb{Z},\ y = nx\}$ des multiples de n est un sous-groupe de $(\mathbb{Z},+)$.*
2. *Réciproquement, montrer que : si H est un sous-groupe de $(\mathbb{Z},+)$, alors il existe $n \in \mathbb{Z}$ tel que $H = n\mathbb{Z}$.*

A.3 Idéaux

DÉFINITION 6
Soit $(A,+,\times)$ une anneau commutatif :

on appelle **idéal** de A tout sous-groupe I de $(A,+)$ tel que $\forall (i,a) \in I \times A,\ i \times a \in I$.

EXEMPLE 7 —

1. *Pour tout $a \in \mathbb{K}$, l'ensemble des polynômes s'annulant en a est un idéal de l'anneau $\mathbb{K}[X]$.*

   Preuve — *La somme de deux polynômes s'annulant en a s'annule en a, l'opposé d'un polynôme s'annulant en a s'annule en a et le polynôme nul aussi. L'ensemble I des polynômes s'annulant en a est donc un sous-groupe additif de $\mathbb{K}[X]$. De plus, le produit d'un polynôme s'annulant en a et d'un polynôme quelconque est un polynôme s'annulant en a. Donc I est un idéal de l'anneau $\mathbb{K}[X]$.* □

2. *L'ensemble des suites tendant vers 0 n'est pas un idéal de l'anneau des suites mais est un idéal de l'anneau des suites bornées.*

   Preuve — *L'ensemble des suites tendant vers 0 est un sous-groupe additif de l'ensemble des suites. Mais le produit de $(n+1)_{n\in\mathbb{N}}$ et de $\left(\frac{1}{n+1}\right)_{n\in\mathbb{N}}$ ne tend pas vers 0. Par contre, toute suite tendant vers 0 est bornée et le produit d'une suite tendant vers 0 et d'une suite bornée est une suite tendant vers 0.* □

PROPOSITION 8 (**les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$**)

1. Dans tout anneau commutatif $(A,+,\times)$, pour tout $k \in A$, l'ensemble
$$k \times A = \{k \times x,\ x \in A\} = \{y \in A \mid \exists x \in A, y = k \times x\}$$
des multiples de k est un idéal de A (appelé l'idéal de A engendré par k).
2. I est un idéal de $\mathbb{Z}$ si, et seulement si, il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.
3. I est un idéal de $\mathbb{K}[X]$ si, et seulement si, il existe $P \in \mathbb{K}[X]$ tel que $I = P\,\mathbb{K}[X]$.

Preuve —

1. Soit $k \in A$. L'ensemble $k \times A$ est un sous-groupe additif de a car, pour tout $(x_1,x_2) \in A^2$:
   — $0 \times x_1 = 0$, d'où 0 appartient à $k \times A$;
   — par distributivité, $k \times x_1 + k \times x_2$ est égal à $k \times (x_1 + x_2)$ et appartient donc à $k \times A$;
   — l'opposé $-(k \times x_1)$ est égal à $k \times (-x_1)$ et appartient donc à $k \times A$.
   De plus, $(k \times x_1) \times x_2 = k \times (x_1 \times x_2)$ par associativité. Donc $k \times A$ est un idéal.
   En particulier, $n\mathbb{Z}$ et $P\,\mathbb{K}[X]$ sont des idéaux. Réciproquement :
2. Si I est un idéal de $\mathbb{Z}$, alors $(I,+)$ est un sous-groupe de $(\mathbb{Z},+)$, donc I est de la forme $n\mathbb{Z}$ d'après l'exercice 5.
3. Si I contient seulement le polynôme nul, alors $I = 0\,\mathbb{K}[X]$. Sinon, l'ensemble des degrés des polynômes non nuls de I est une partie non vide de $\mathbb{N}$ et possède donc un minimum d. Soit alors $P \in I$ tel que $\deg P = d$. D'une part, $P\,\mathbb{K}[X] \subset I$ car I est un idéal. D'autre part, $I \subset P\,\mathbb{K}[X]$ car, après division euclidienne par P, tout polynôme de I s'écrit $PQ + R$, or $PQ \in I$, donc $R \in I$. Or $\deg R < d$, d'où R est nul.

□

EXERCICE 9 — *Montrer que le noyau d'un morphisme d'anneaux commutatifs est un idéal.*

PROPOSITION 10
Dans un anneau commutatif $(A, +, \times)$, la somme de deux idéaux et l'intersection de deux idéaux sont encore des idéaux. En particulier, dans l'anneau $(\mathbb{Z}, +, \times)$ des entiers relatifs,

$$\forall (p,q) \in \mathbb{Z}^2, \quad p\mathbb{Z} + q\mathbb{Z} = \text{pgcd}(p,q)\mathbb{Z} \qquad \text{et} \qquad p\mathbb{Z} \cap q\mathbb{Z} = \text{ppcm}(p,q)\mathbb{Z}$$

car $\forall (d,p) \in \mathbb{Z}^2,\ d \mid p \iff p\mathbb{Z} \subset d\mathbb{Z}$ (*i.e.* tout multiple de p est un multiple de d.)

Preuve — On sait que l'intersection $I \cap J$ ou la somme $I + J$ de deux sous-groupes $(I, +)$ et $(J, +)$ d'un groupe $(A, +)$ est encore un sous-groupe. Si, de plus, I et J sont des idéaux, alors $\forall (a, i, j) \in A \times I \times J,\ i \times a \in I$ et $j \times a \in J$. Par suite : si $x \in I \cap J$, alors $ax \in I \cap J$; si $x \in I + J$, alors $\exists (i,j) \in I \times J,\ x = i + j$, d'où $a \times x = a \times i + a \times j \in I + J$.

En particulier, si $(p,q) \in \mathbb{Z}^2$, alors il existe $d \in \mathbb{Z}$ tel que $p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z}$ d'après la proposition 8. Or $d \mid p$ car $p\mathbb{Z} \subset d\mathbb{Z}$ et, de même, $d \mid q$, d'où d est un diviseur commun à p et q. Et c'est le plus grand car : si δ est un diviseur commun à p et q, alors δ divise tous les éléments de $p\mathbb{Z} + q\mathbb{Z}$, donc tous les éléments de $d\mathbb{Z}$, et en particulier d, qui est donc le *pgcd*. De même pour le *ppcm*. □

COROLLAIRE 11
(Lemme de Bézout) Deux entiers relatifs a et b sont premiers entre eux *ssi* $\exists (u,v) \in \mathbb{Z}^2,\ a \times u + b \times v = 1$.
(Lemme de Gauss) Si a divise bc et a est premier avec b, alors a divise c.

Preuve — (Bézout) $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$ si, et seulement si, $\exists (u,v) \in \mathbb{Z}^2,\ a \times u + b \times v = 1$.

(Gauss) Si a est premier avec b, alors $\exists (u,v) \in \mathbb{Z}^2,\ a \times u + b \times v = 1$. D'où $ac \times u + bc \times v = c$. Si, de plus, a divise bc, alors (comme a divise ac) il divise aussi $ac \times u + bc \times v$, c'est-à-dire c. □

EXERCICE 12 — *Montrer que : si b et c sont premiers entre eux et divisent a, alors bc divise a.*

A.4 L'ALGORITHME D'EUCLIDE

LEMME 13
Pour tout couple d'entiers naturels $(a,b) \in \mathbb{N}^2$ tel que $b \neq 0$, $\text{pgcd}(a,b) = \text{pgcd}(b, a \mod b)$.

Preuve — Soient q et $r = a \mod b$ les quotient et reste de la division euclidienne de a par b. Si d divise a et b, alors d divise b et $r = a - q \cdot b$. Réciproquement : si d divise b et r, alors d divise $a = q \cdot b + r$ et b. Les entiers a et b d'une part, b et r d'autre part ayant les mêmes diviseurs, ils ont le même *pgcd*. □

Algorithme 1: Algorithme d'Euclide

Entrée: Deux entiers naturels a et b et $a \geqslant b$
Sortie: Le pgcd de a et b

```
1 A ← a ; B ← b ;
2 tant que B ≠ 0 faire
3 |   R ← A mod B;                    //Le reste de la division euclidienne
4 |   A ← B ;
5 |   B ← R ;
6 retourner A
```

PROPOSITION 14
L'algorithme d'Euclide s'arrête sur toutes ses entrées et calcule le pgcd de ses deux entrées.

Preuve — On établit que la grandeur $\mathcal{V}(A,B) = B$ est un variant de la boucle **tant que** et que cette boucle admet la propriété invariante suivante, $\mathcal{I}$: $\text{pgcd}(a,b) = \text{pgcd}(A,B)$ et $A \in \mathbb{N}$ et $B \in \mathbb{N}$.

- Montrons que la propriété $\mathcal{I}$ est bien une propriété invariante.
  - Initialement $A = a$ et $B = b$ avec $a \in \mathbb{N}$ et $b \in \mathbb{N}$, $\mathcal{I}$ découle de telles hypothèses.

- Nommons $\underline{A}, \underline{B}$ les valeurs de A et B au début d'une itération de boucle et $\overline{A}, \overline{B}$ les valeurs de A et B à la fin de cette même itération de boucle. Supposons que $\underline{A}, \underline{B}$ satisfont $\mathcal{I}$ et la *condition de boucle* et montrons que $\overline{A}, \overline{B}$ satisfont $\mathcal{I}$. Par lecture de l'algorithme : $\overline{A} = \underline{B}$ et $\overline{B} = \underline{A} \mod \underline{B} \neq 0$. Du lemme 13 : $\mathsf{pgcd}(\overline{A}, \overline{B}) = \mathsf{pgcd}(\underline{A}, \underline{B})$. De plus $\overline{A} = \underline{B} \in \mathbb{N}$ et $\overline{B} = \underline{A} \mod \underline{B}$ d'où par propriété de la division euclidienne $\overline{B} \in \mathbb{N}$.

- Montrons que la grandeur $\mathcal{V}$ est bien un variant de boucle.

  - $\mathcal{V}$ est à valeurs dans l'espace bien fondé $(\mathbb{N}, \leqslant)$, par propriété $\mathcal{I}$.
  - Nommons $\underline{A}, \underline{B}$ les valeurs de A et B au début d'une itération de boucle et $\overline{A}, \overline{B}$ les valeurs de A et B à la fin de cette même itération de boucle. Par lecture de l'algorithme : $\mathcal{V}(\overline{A}, \overline{B}) = \overline{B} = \underline{A} \mod \underline{B} < \underline{B} = \mathcal{V}(\underline{A}, \underline{B})$.

  $\mathcal{V}$ est donc bien un variant de l'algorithme d'Euclide.

On conclut donc que la boucle **tant que** de l'algorithme d'Euclide termine, et ce sur toutes entrées, et produit un état des variables vérifiant $\mathcal{I}$ ainsi que la négation de la condition de boucle. En particulier $\mathsf{pgcd}(A, B) = \mathsf{pgcd}(a, b)$ et $B = 0$. Or $\mathsf{pgcd}(A, 0) = A = \mathsf{pgcd}(a, b)$. On en déduit la correction de l'algorithme. □

PROPOSITION 15
En notant $(C_n)_{n\in\mathbb{N}}$ la suite donnant la complexité pire cas, en nombre de tours de boucle, de l'algorithme d'Euclide, sur des entrées inférieures à n, $C_n = \Theta(\log n)$.

Preuve —

- On montre dans un premier temps que si l'algorithme d'Euclide effectue $p \in \mathbb{N}$ itérations de boucle sur des entrées a et b alors $a \geq F_{p+1}$ où $(F_p)_{p\in\mathbb{N}}$ est la suite de Fibonacci. En effet, considérons la suite finie des valeurs des variables $(A_i)_{i\in[\![0,p]\!]}$ et $(B_i)_{i\in[\![0,p]\!]}$ en tête des p tours de boucle, numérotées dans l'ordre inverse de leur exécution : $a = A_p$. Notons $(Q_i)_{i\in[\![1,p]\!]}$ la suite des quotients des divisions euclidiennes de A par B.

$$\begin{aligned}
A_p &= Q_p B_p (= A_{p-1}) + R_p (= A_{p-2}) \\
A_{p-1} &= Q_{p-1} B_{p-1} (= A_{p-2}) + R_{p-1} (= A_{p-3}) \\
&\dots = \dots \\
A_i &= Q_i B_i (= A_{i-1}) + R_{i-1} (= A_{i-2}) \\
&\dots = \dots \\
A_1 &= Q_1 A_0 + 0
\end{aligned}
\qquad\qquad
\begin{aligned}
A_p &= Q_p A_{p-1} + A_{p-2} \\
A_{p-1} &= Q_{p-1} A_{p-2} + A_{p-3} \\
&\dots = \dots \\
A_i &= Q_i A_{i-1} + A_{i-2} \\
&\dots = \dots \\
A_1 &= Q_1 A_0 + 0
\end{aligned}$$

  Remarquons que par divisions euclidiennes : $\forall i \in [\![1, p-1]\!], A_{i-1} < A_i$, de plus par hypothèse sur l'algorithme d'Euclide $a(= A_p) \geqslant b(= A_{p-1})$. Ainsi les $(A_i)_{i\in[\![0,p]\!]}$ forment une suite croissante. On en déduit que $\forall i \in [\![1, p]\!], Q_i \geq 1$, et donc $\forall i \in [\![1, p]\!], A_i \geq A_{i-1} + A_{i-2}$ (en prolongeant $A_{-1} = 0$). De plus $A_0 > 0$. Finalement, une récurrence nous donne : $\forall i \in [\![-1, p]\!], A_i \geq F_{i+1}$.

- Dans un second temps, on se rappelle que la suite de Fibonacci a une croissance exponentielle, à savoir :

$$\forall p \geqslant 2,\ \phi^{p-2} \leqslant F_p \leqslant \phi^{p-1}$$

  en notant $\phi = \frac{1+\sqrt{5}}{2}$ le nombre d'or, qui est une solution de l'équation $x^2 - x - 1 = 0$.

- Finalement, on encadre C_n. Soit $n \in \mathbb{N}$ avec $n \geqslant 2$, on rappelle que la suite de Fibonacci est strictement croissante, soit donc $p \in \mathbb{N}$ tel que $F_p \leqslant n < F_{p+1}$. On remarque que $n \geqslant 2$ donc $p \geqslant 2$ car $F_2 = 1$ et donc on peut utiliser l'encadrement obtenu ci-avant : $\phi^{p-2} \leqslant n < \phi^p$, soit donc $\log_\phi(n) < p \leqslant \log_\phi(n) + 2$ par croissance de $\log_\phi$. L'exécution de l'algorithme d'Euclide sur les entrées (F_p, F_{p-1}) conduit à la séquence de p tours de boucles $(F_p, F_{p-1}, F_{p-2}, \dots, F_0)$ pour les valeurs de A. Finalement C_n étant une complexité pire cas : $C_n \geqslant p > \log_\phi(n)$.

  Il nous reste donc à majorer C_n. Supposons qu'il existe deux entrées $(a, b) \in \mathbb{N}^2$ telles que $a \leqslant n$ et $b \leqslant n$ conduisant à un nombre de tours de boucle $q > \lceil \log_\phi(n) + 1 \rceil$. On déduit des remarques précédentes que $A_q = a \geq F_{q+1}$. En utilisant la croissance de la suite de Fibonacci : $a > F_{\lceil \log_\phi(n) \rceil + 2} = \phi^{\lceil \log_\phi(n) \rceil} \geq \phi^{\log_\phi(n)} = n$ ce qui est absurde car $a \leqslant n$. On en conclut donc que toutes entrées $(a, b) \in \mathbb{N}^2$ telles que $a \leqslant n$ et $b \leqslant n$ conduisent à un nombre de tours de boucle $\leq \lceil \log_\phi(n) + 1 \rceil$. Soit $C_n \leqslant \lceil \log_\phi(n) + 1 \rceil \leqslant \log_\phi(n) + 2$.

□

REMARQUE 16 — *L'algorithme 1 d'Euclide modifie les entiers A et B en préservant l'invariant suivant : A et B sont une combinaison entière affine des valeurs de a et b initiales. En effet à chaque tour de boucle on effectue l'opération : $(A, B) \leftarrow (B, A - QB)$ où $Q = A/B$. Ce résultat nous intéresse particulièrement puisque le lemme de Bézout nous donne l'existence d'une combinaison linéaire entière de a et b valant $\mathsf{pgcd}(a, b)$. En reprenant les notations $(A_i)_{i\in[\![0,n]\!]}$ introduites ci-dessus, et en notant u_i et v_i de sorte que $A_i = u_i a + v_i b$, en remarquant que $A_i = Q_i A_{i-1} + A_{i-2}$ on déduit $A_{i-2} = (u_i - Q_i u_{i-1})a + (v_i - Q_i v_{i-1})b$.*

Algorithme 2: Algorithme d'Euclide étendu

Entrée: Deux entiers naturels a et b et $a \geqslant b$
Sortie: Le pgcd de a et b, les coefficients de Bézout

$A \leftarrow a$; $B \leftarrow b$; $U \leftarrow 1$; $V \leftarrow 0$; $U' \leftarrow 0$; $V' \leftarrow 1$;
tant que $B \neq 0$ **faire**
  $Q \leftarrow A/B$; `//Le quotient de la division euclidienne`
  $(A, B) \leftarrow (B, A - QB)$;
  $(U, V, U', V') \leftarrow (U', V', U - QU', V - QV')$
retourner A, U, V

PROPOSITION 17
L'algorithme d'Euclide étendu s'arrête sur toutes ses entrées (a, b) et calcule un triplet (d, u, v) tel que $d = \mathsf{pgcd}(a, b)$ et $d = au + bv$

A.5 L'ANNEAU $\mathbb{Z}/n\mathbb{Z}$

DÉFINITION 18
Soit $n \in \mathbb{N}^*$. La relation $x \equiv a[n]$ (« x est congru à a modulo n ») définie par $n \mid (x - a)$ est une relation d'équivalence sur $\mathbb{Z}$. L'ensemble $\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a[n]\}$ est la classe d'équivalence de a. L'ensemble $\left\{\overline{1}; \overline{2}; \cdots; \overline{n}\right\}$ des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.

Ainsi, pour tout $(x, a) \in \mathbb{Z}^2$, $\overline{x} = \overline{a} \iff x \equiv a[n]$. Et, parce que $\big(x \equiv a[n] \text{ et } y \equiv b[n]\big) \implies \big(x + y \equiv (a + b)[n] \text{ et } x \times y \equiv (a \times b)[n]\big)$, on peut définir $\overline{x} + \overline{y} = \overline{x + y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$, ce qui fait de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ un anneau commutatif.

PROPOSITION 19
$x \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^*$ si, et seulement si, $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est inversible. Par suite $\mathbb{Z}/n\mathbb{Z}$ est un corps (noté aussi $\mathbb{F}_n$) si, et seulement si, $n \in \mathbb{N}^*$ est un nombre premier.

Preuve — Soit x un entier relatif : $\overline{x}$ est inversible *ssi* il existe $u \in \mathbb{Z}$ tel que $\overline{x} \times \overline{u} = \overline{1}$, *ssi* il existe $u \in \mathbb{Z}$ tel que $xu \equiv 1[n]$, *ssi* il existe $(u, v) \in \mathbb{Z}^2$ tel que $xu + nv = 1$. D'après le lemme de Bézout, c'est le cas *ssi* x est premier avec n. Par suite l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps *ssi* tous les élements autres que l'élément nul $\overline{n}$ sont inversibles, *ssi* n est premier avec tous les éléments de $[\![1, n - 1]\!]$, *ssi* n est premier. □

MÉTHODE 20 (calculer un inverse ou le retour de Bézout) — *Insistons sur la caractère calculable de l'inverse d'un élément x dans $\mathbb{Z}/n\mathbb{Z}$ lorsque n est premier. En effet, étant donné un entier $x \in \mathbb{Z}/n\mathbb{Z}$ et $n \in \mathbb{Z}$ premier, l'exécution de l'algorithme d'Euclide étendu sur les entrées (n, x) conduit au calcul d'un triplet (d, u, v) de sorte que $d = \mathsf{pgcd}(n, x) = 1$, et $1 = nu + vx$. Soit finalement $vx \equiv 1[n]$ et donc $\overline{vx} = 1$ soit $\overline{v}$ est l'inverse de $\overline{x}$.*

PROPOSITION 21 (théorème chinois)
Si a et b sont premiers entre eux, alors deux congruences modulo a et modulo b équivalent à une congruence modulo ab car les anneaux $\mathbb{Z}/(ab)\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes.

Preuve — Notons $\pi_a : \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$, $x \mapsto \overline{x}$ et de même π_b et π_{ab}. L'application $f : \mathbb{Z}/(ab)\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $\pi_{ab}(x) \mapsto \big(\pi_a(x), \pi_b(x)\big)$ est un isomorphisme d'anneaux. D'une part elle est bien définie et c'est un morphisme d'anneaux.

D'autre part ses ensembles de départ et d'arrivée ont le même cardinal ab, elle est donc bijective *ssi* elle est injective. Ce qu'elle est car : si $\pi_a(x)$ et $\pi_b(x)$ sont nuls, alors a et b divisent x, d'où (exercice 12) ab divise x car a et b sont premiers entre eux, donc $\pi_{ab}(x)$ est nul. □

MÉTHODE 22 (Résoudre un système de congruences avec l'algorithme d'Euclide étendu) — *Soit donc une famille $(p_1, p_2, \ldots, p_n)$ d'entiers deux à deux premiers entre eux. On souhaite construire un isomorphisme*

de $(\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n\mathbb{Z}) \to \mathbb{Z}/p_1p_2\dots p_n\mathbb{Z}$. *Ainsi étant donné un élément* x *dont on connaît uniquement les valeurs* $x_1 = x \mod p_1$, $x_2 = x \mod p_2$, …, $x_n = x \mod p_n$ *on cherche à calculer la valeur de* $x \mod p_1p_2\dots p_n$. *Pour ce faire on construit une famille d'entiers* $(l_i)_{i\in[\![1,n]\!]}$ *tels que* $l_i \mod p_j = \delta_{i,j}$. *Armé d'une telle famille on pourra alors construire l'entier* $x = x_1l_1 + x_2l_2 + \cdots + x_nl_n$ *qui sera bien tel que* $\forall j \in [\![1,n]\!]$, $x \mod p_i = x_i$. *Pour tout* $i \in [\![1,n]\!]$ *et tout* $j \neq i$, l_i *doit donc être multiple de* p_j, *soit donc* $K_i = p_1p_2\dots p_{i-1}p_{i+1}\dots p_n$ *qui convient. Mais il faut de plus que* $l_i \mod p_i = 1$, *or* $K_i \mod p_i$ *n'est pas nécessairement* 1. *On peut toutefois calculer l'inverse de* K_i *dans* $\mathbb{Z}/p_i\mathbb{Z}$ *grâce à l'algorithme d'Euclide étendu, notons* J_i *cette inverse. Finalement* K_iJ_i *est tel que pour tout* $j \neq i$ $K_iJ_i \mod p_j = 0$ *car* K_i *est multiple de* p_j *et* $K_iJ_i \mod p_i = 1$. *On conclut donc que le choix* $l_i = K_iJ_i$ *convient.*

Exemple 23 — *On cherche les entiers relatifs* x *tels que* $x \equiv 2[3]$, $x \equiv 4[5], y \equiv 2[8]$. *On note que* $p_1 = 3$, $p_2 = 5$ *et* $p_3 = 8$ *sont premiers entre eux deux à deux. On calcule* $K_1 = 5 \times 8 = 40$, $K_2 = 3 \times 8 = 24$ *et* $K_3 = 3 \times 5 = 15$. *On calcule les inverses des* K_i *module* p_i *au moyen de l'algorithme d'Euclide étendu :*

- $3 \times (-13) + 40 \times 1 = 1$ *donc* $J_1 = \overline{40}^{-1} = \overline{1}$ *dans* $\mathbb{Z}/3\mathbb{Z}$;
- $5 \times 5 + 24 \times (-1) = 1$ *donc* $J_2 = \overline{21}^{-1} = \overline{-1}$ *dans* $\mathbb{Z}/5\mathbb{Z}$;
- $8 \times 2 + 15 \times (-1) = 1$ *donc* $J_3 = \overline{15}^{-1} = \overline{-1}$ *dans* $\mathbb{Z}/8\mathbb{Z}$.

On fabrique alors les entiers $l_1 = K_1J_1 = 40$, $l_2 = -24$ *et* $l_3 = -15$. *Donc*

$$\begin{cases} x \equiv 2[3] \\ x \equiv 4[5] \\ y \equiv 2[8] \end{cases} \quad \Leftrightarrow \quad x \equiv 2l_1 + 4l_2 + 2l_3[120] \quad \Leftrightarrow x \equiv -46[120]$$

Définition 24
Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ (*i.e.* le nombre d'entiers de $[\![1,n]\!]$ premiers avec n) est noté $\varphi(n)$. L'application $\varphi : \mathbb{N}^* \to \mathbb{N}$, $n \mapsto \varphi(n)$ est appelée l'**indicatrice d'Euler**.

Méthode 25 (Comment calculer l'indicatrice d'Euler) —

(i) Si p *est premier, alors* $\varphi(p) = p - 1$ *et* $\forall k \in \mathbb{N}^*$, $\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.

(ii) Si a *et* b *sont premiers entre eux, alors* $\varphi(ab) = \varphi(a)\varphi(b)$.

(iii) Si $p_1, \cdots, p_k$ *sont les diviseurs premiers de* n, *alors* $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$.

Preuve — (*i*) Si p est premier, alors : les éléments de $[\![1,p]\!]$ premiers avec p sont $1, \cdots, p-1$, donc $\varphi(p) = p - 1$. Et un élément de $[\![1,p^k]\!]$ est premier avec p^k *ssi* il est premier avec p *ssi* il n'est pas un multiple de p. Or $[\![1,p^k]\!]$ contient p^{k-1} multiples de p. Donc $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

(*ii*) Il y a $\varphi(a)$ inversibles dans $\mathbb{Z}/a\mathbb{Z}$ et il y en a $\varphi(b)$ dans $\mathbb{Z}/b\mathbb{Z}$. Il y en a donc $\varphi(a)\varphi(b)$ dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et autant dans $\mathbb{Z}/(ab)\mathbb{Z}$ par l'isomorphisme du théorème chinois si a et b sont premiers entre eux.

(*iii*) n est de la forme $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, d'où $\varphi(n) = \varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k}) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$. □

A.6 L'ordre d'un élément

Si a est un élément d'un groupe $(G, \cdot)$ d'élément neutre 1, alors l'ensemble $\{\cdots; a^{-2}; a^{-1}; 1; a^1; a^2; \cdots\} = \{a^k, k \in \mathbb{Z}\}$ est un sous-groupe de G, appelé le sous-groupe engendré par a ; c'est le plus petit sous-groupe de G contenant a.

Si ce sous-groupe est un ensemble fini, alors son cardinal est appelé l'**ordre** de a. L'ordre de a est alors le plus petit entier k strictement positif tel que $a^k = 1$. Et les entiers k tels que $a^k = 1$ sont les multiples de l'ordre de a. On dit que le groupe G est monogène s'il est lui-même engendré par un élément et qu'il est **cyclique** s'il est monogène et fini.

EXERCICE 26 — *Décomposer en cycles disjoints la permutation* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 2 & 6 & 1 & 3 \end{pmatrix}$ *du groupe symétrique* S_7 *et en déduire l'ordre de* σ.

PROPOSITION 27 (Théorème de Lagrange)
Si a est un élément d'un groupe G fini, alors l'ordre de a divise le cardinal de G.

Preuve — *(La preuve qui suit est valable seulement si G est commutatif.)* L'application $G \to G, x \mapsto ax$ est bijective. D'où le produit $\prod_{x \in G} x$ de tous les éléments du groupe est aussi égal à $\prod_{x \in G} (ax) = a^n \prod_{x \in G} x$, en notant n le cardinal de G. Donc $a^n = 1$. □

COROLLAIRE 28
(Théorème d'Euler) Si $a \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^*$, alors $a^{\varphi(n)} \equiv 1[n]$.
(Petit théorème de Fermat) Si p est un nombre premier, alors $\forall a \in \mathbb{Z},\ a^p \equiv a[p]$.

Preuve — (Euler) Si a est premier avec n, alors $\overline{a}$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ a pour cardinal $\varphi(n)$. L'ordre de $\overline{a}$ divise donc $\varphi(n)$. Par suite $\overline{a}^{\varphi(n)} = \overline{1}$. Autrement dit $a^{\varphi(n)} \equiv 1[n]$.

(Fermat) Parce que p est premier : ou bien a est divisible par p, d'où a^p l'est aussi, donc $a^p \equiv a \equiv 0[p]$. Ou bien a est premier avec p et alors, d'après le théorème d'Euler, $a^{p-1} \equiv 1[p]$, d'où $a^p \equiv a[p]$. □

EXERCICE 29 — *Calculer* $\varphi(10)$ *et en déduire que le dernier chiffre de l'écriture décimale de* 3^{345} *est 3. Calculer* $\varphi(100)$ *et en déduire les deux derniers chiffres de l'écriture décimale de* 3^{345} *sont 4 et 3.*