EXERCICES AVEC COURS INTÉGRÉ SUR UNE INITIATION À L'ALGÈBRE POUR CONSTRUIRE LE CRYPTOSYSTÈME RSA

S. Labopin

Table des matières

1 Prérequis sur les structures algébriques

1.1 Lois de composition internes binaires sur un ensemble

Définition (loi de composition interne sur un ensemble)
Soit E un ensemble.
On appelle **loi de composition interne** une application $\star$ définie sur $E \times E$ et à valeur dans E, autrement dit :

$$\begin{array}{rccc} \star : & E \times E & \to & E \\ & (x,y) & \mapsto & \star(x,y) \end{array}$$

Exemple (loi de composition interne sur un ensemble)
On note E l'ensemble des chaînes de caractères.
Alors l'opération de concaténation $\star$ est une loi de composition interne sur E :

$$\begin{array}{rccc} \star : & E \times E & \to & E \\ & (\text{"}c_1...c_p\text{"},\text{"}d_1...d_q\text{"}) & \mapsto & \star(\text{"}c_1...c_p\text{"},\text{"}d_1...d_q\text{"}) = \text{"}c_1...c_pd_1...d_q\text{"} \end{array}$$

En particulier :

$$\star(\texttt{"Bien","\ joué\ !"}) = \texttt{"Bien\ joué\ !"}$$

Une telle application $\star$ associe donc un élément de E à chaque couple d'éléments de E.

Notation (loi de composition interne sur un ensemble)
Soit E un ensemble et $\star$ une loi de composition interne sur E.
On note :

$$\forall\ (x,y) \in E \times E,\ x \star y = \star(x,y)$$

Notation-Exemple (loi de composition interne sur un ensemble)
L'addition + est une loi de composition interne sur $\mathbb{Z}$ puisque c'est une foncton qui, à chaque couple d'entiers relatifs, associe un entier relatif, leur somme.
Au lieu de noter

$$\begin{array}{rccc} + : & \mathbb{Z}^2 & \to & \mathbb{Z} \\ & (m,n) & \mapsto & +(m,n) \end{array}$$

On note souvent

$$\begin{array}{rccc} + : & \mathbb{Z}^2 & \to & \mathbb{Z} \\ & (m,n) & \mapsto & m+n \end{array}$$

1.2 Groupes

Définition (groupe)
On appelle **groupe** la donnée notée $(G,\star)$ d'un ensemble G et d'une loi de composition interne $\star$ sur G vérifiant les trois assertions suivantes :

- $\star$ est associative :

$$\forall\ (x,y,z) \in G^3,\ (x \star y) \star z = x \star (y \star z)$$

- Il existe un élément neutre $e \in G$ pour la loi $\star$:

$$\exists\ e \in G \mid \forall\ x \in G,\ x \star e = e \star x = x$$

- Tous les éléments de G admette un symétrique par rapport à la loi $\star$:

$$\forall\ x \in G,\ \exists\ y \in G \mid\ x \star y = y \star x = e$$

Exercice (groupe)
L'ensemble des chaînes de caractères muni de la concaténation forme-t-il un groupe ?

Exemple-Exercice (le groupe diédral D_2)
Dans un plan $\mathscr{P}$ muni d'un repère $\left(O, \vec{i}, \vec{j}\right)$, on note les points $A = (-1;0)$ et $B = (1;0)$.
On note D_2 l'ensemble à 4 éléments où ces 4 éléments sont les 4 applications suivantes :

- L'identité de $\mathscr{P}$ id : $\begin{array}{ccc} \mathscr{P} & \to & \mathscr{P} \\ M & \to & M \end{array}$
- La symétrie axiale s_x par rapport à l'axe des abscisses s_x : $\begin{array}{ccc} \mathscr{P} & \to & \mathscr{P} \\ \begin{pmatrix} a \\ b \end{pmatrix} & \to & \begin{pmatrix} a \\ -b \end{pmatrix} \end{array}$
- La symétrie axiale s_y par rapport à l'axe des ordonnées s_y : $\begin{array}{ccc} \mathscr{P} & \to & \mathscr{P} \\ \begin{pmatrix} a \\ b \end{pmatrix} & \to & \begin{pmatrix} -a \\ b \end{pmatrix} \end{array}$
- La symétrie centrale s_O par rapport à l'origine s_O : $\begin{array}{ccc} \mathscr{P} & \to & \mathscr{P} \\ \begin{pmatrix} a \\ b \end{pmatrix} & \to & \begin{pmatrix} -a \\ -b \end{pmatrix} \end{array}$

On note $G = \{id,\ s_x, s_y, s_O\}$. L'ensemble G est en fait l'ensemble de toutes les isométries du plan qui conservent le segment $[A,B]$.
Démontrer que $(G,\circ)$ où $\circ$ est la loi de composition des applications $\mathscr{P} \to \mathscr{P}$ est un groupe.

Définition (groupe abélien)
On appelle **groupe abélien** un groupe $(G,\star)$ tel que la loi $\star$ est commutative, c'est-à-dire vérifiant :

$$\forall\ (x,y) \in G^2,\ x \star y = y \star x$$

Exemple-Exercice (« les deux premiers groupes de l'arithmétique »)
Démontrer que $(\mathbb{Z},+)$ et $(\mathbb{Z}^*,\times)$ sont des groupes abéliens.

Théorème (« les deux premiers groupes de l'arithmétique »)
$(\mathbb{Z},+)$ et $(\mathbb{Z}^*,\times)$ sont des groupes abéliens.

Exemple-Exercice (le groupe diédral $(D_2,\circ)$ est abélien)
Démontrer que le groupe diédral $(D_2,\circ)$ est un groupe abélien.

Exemple-Exercice (le groupe diédral $(D_3,\circ)$ n'est pas abélien)
On note :

- $j = e^{\frac{2i\pi}{3}}$
- A, B et C les points du plan $\mathscr{P}$ d'affixes respectifs 1, j et j^2
- D_3 l'ensemble des isométries de $\mathscr{P}$ qui conservent le triangle ABC

1) Déterminer les 6 éléments de D_3.
2) Démontrer que $(D_3,\circ)$ est un groupe.
3) Démontrer que $(D_3,\circ)$ n'est pas un groupe abélien.

1.3 Anneaux

Définition (anneau)
On appelle **anneau** la donnée notée $(A, \star, \sharp)$ d'un ensemble A et de deux lois de compositions internes $\star$ et $\sharp$ sur A vérifiant les quatre assertions suivantes :

- $(A, \star)$ est un groupe abélien.
- La loi $\sharp$ est associative, c'est-à-dire :

$$\forall\ (x,y,z) \in A^3,\ (x\sharp y)\sharp z = x\sharp(y\sharp z)$$

- Il existe un élément neutre $1_A \in A$ pour la loi $\sharp$, c'est-à-dire :

$$\exists\, 1_A \in A \mid \forall\ x \in A,\ x\sharp 1_A = 1_A \sharp x = x$$

- La loi $\sharp$ est distributive par rapport à la loi $\star$, c'est-à-dire :

$$\forall\ (x,y,z) \in A^3,\ \begin{cases} x\sharp(y\star z) = (x\sharp y)\star(x\sharp z) \\ (y\star z)\sharp x = (y\sharp x)\star(z\sharp x) \end{cases}$$

Exemple-Exercice (l'**anneau des nombres entiers relatifs** $(\mathbb{Z}, +, \times)$)
Démontrer que $(\mathbb{Z}, +, \times)$ est un anneau.

Théorème
Soit $n \in \mathbb{N}^*$.
Alors $(\mathbb{Z}, +, \times)$ est un anneau.

1.4 Sous-structures

1.4.1 Sous-groupes d'un groupe

Définition (sous-groupe)
Soient $(G, \star)$ un groupe.
On appelle **sous-groupe** de $(G, \star)$ un groupe $(H, \tilde{\star})$ vérifiant :

- H est un sous-ensemble de G.
- $\star$ est un prolongement de $\tilde{\star}$, c'est-à-dire :

$$\forall\ (x,y) \in H^2,\ x \star y = x \tilde{\star} y$$

Exemple-exercice (**sous-groupe constitué des multiples d'un entier**)
Soit $n \in \mathbb{N}^*$.
On note H l'ensemble des multiples de n, c'est-à-dire l'ensemble des entiers relatifs qui sont divisibles par n :

$$n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, 4n, \ldots\}$$

On note aussi :

$$\begin{array}{rccc} \tilde{+} : & n\mathbb{Z} \times n\mathbb{Z} & \to & n\mathbb{Z} \\ & (x,y) & \mapsto & x+y \end{array}$$

Démontrer que $(n\mathbb{Z}, \tilde{+})$ est un sous-groupe de $(\mathbb{Z}, +)$.

Abus de langage :
On notera abusivement de la même façon une loi de composition interne et le prolongement de cette loi que l'on considère.
Par exemple, dans l'exercice précédent, on peut simplifier les notations en écrivant « $\tilde{+} = +$ » alors que ces deux applications sont pourtant différentes puisqu'elles n'ont ni le même ensemble de départ ni le même ensemble d'arrivée (L'ensemble de départ de $+$ est $\mathbb{Z} \times \mathbb{Z}$ et son ensemble d'arrivée est $\mathbb{Z}$.).
C'est ainsi qu'on écrira par exemple $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

Théorème (**sous-groupe constitué des multiples d'un entier**)
Soit $n \in \mathbb{N}^*$.
Alors $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.

Définition-exemple-exercice (groupe des éléments inversibles d'un anneau)
Soit $(A, \star, \sharp)$ un anneau.
On note 1_A l'élément neutre de A pour la loi $\sharp$.
On note aussi $U(A, \star, \sharp)$ ou plus simplement $U(A)$ l'ensemble des éléments de A qui admettent un symétrique par rapport à la loi $\sharp$, c'est-à-dire :

$$U(A) = \{x \in A \mid \exists\, y \in A \mid x \sharp y = y \sharp x = 1_A\}$$

Démontrer que $(U, \sharp)$ est un groupe.

⚠
- $(U(A), \sharp)$ n'est pas un sous-groupe de $(A, +)$.
- En revanche, si $(A, \sharp)$ est un groupe, $(U(A), \sharp)$ est un sous-groupe de $(A, \sharp)$.
- Si $(A, \sharp)$ n'est pas un groupe, alors on ne peut pas dire que $(U(A), \sharp)$ est un sous-groupe de $(A, \sharp)$.

Définition (groupe des éléments inversibles d'un anneau)
Soit $(A, \star, \sharp)$ un anneau.
On appelle **groupe des éléments inversibles de l'anneau** A le groupe $(U(A), \sharp)$.

Exercice-exemple (groupe des éléments inversibles d'un anneau)
Quel est le groupe des éléments inversibles de l'anneau $(\mathbb{Z}, +, \times)$?

1.4.2 Idéaux d'un anneau

Définition (idéal d'un anneau)
On appelle **idéal d'un anneau** $(A, \star, \sharp)$ un sous-ensemble I de A vérifiant les deux assertions suivantes :

- $(I, \star)$ est un sous-groupe de $(A, \star)$.
- I absorbe la loi $\sharp$, c'est-à-dire :

$$\forall\, a \in A,\ \forall\, i \in I,\ \begin{cases} a \sharp i \in I \\ i \sharp a \in I \end{cases}$$

Exemple-Exercice (l'**idéal $n\mathbb{Z}$ de l'anneau $(\mathbb{Z}, +, \times)$**)
Soit $n \in \mathbb{N}^*$.
Démontrer que $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

1.5 Quotient d'un anneau par un idéal

Notation (des sous-ensembles importants d'un anneau)
Soient $(A, \star, \sharp)$ un anneau et I un idéal de A.
On note :

$$\forall\, a \in A,\ a \star I = \{a \star i,\ i \in I\}$$

Autrement dit, pour $a \in I$ fixé, $a \star I$ est un sous-ensemble de A, c'est l'ensemble de tous les éléments de A de la forme $a \star i$ où i est un élément de I.

Exemples (l'**ensemble des entiers relatifs congrus à r modulo n**)
Soit $n \in \mathbb{N}^*$.
On considère l'anneau $(\mathbb{Z}, +, \times)$ et son idéal $n\mathbb{Z}$.

- Pour $r \in [\![0, n-1]\!]$ fixé, l'ensemble

$$\boldsymbol{r + n\mathbb{Z} = \{..., r-3n, r-2n, r-n, r, r+n, r+2n, r+3n, ...\}}$$

est

l'ensemble des entiers relatifs congrus à r modulo n

c'est-à-dire

l'ensemble des entiers dont le reste de leur division euclidienne par n est r

- $1 + 2\mathbb{Z} = \{..., -5, -3, -1, 1, 3, 5, 7, ...\}$ est l'ensemble des entiers impairs, c'est-à-dire ceux dont le reste de la division euclidienne par 2 est 1.
- $17 = 3 + 2 \times 7 \in 3 + 7\mathbb{Z}$
  Autrement dit, le reste de la division euclidienne de 17 par 7 est 3.
  Autrement dit, 17 est congru à 3 modulo 7.

Notation (un ensemble important de sous-ensembles d'un anneau)
Soient $(A, \star, \sharp)$ un anneau et I un idéal de A.
On note :

$$\frac{A}{I} = \{a \star I,\ a \in A\}$$

Autrement dit, $\frac{A}{I}$ est l'ensemble de tous les sous-ensemble de A de la forme $a \star I$ où a est un élément de A.

Exemple-Exercice (« l'**anneau des entiers modulo n** »)
Soit $n \in \mathbb{N}^*$.
On considère l'anneau $(\mathbb{Z}, +, \times)$ et son idéal $n\mathbb{Z}$.

1) Les éléments de l'ensemble $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont-ils des ensembles finis ou des ensembles infinis ?
2) Démontrer que :

$$\boldsymbol{\frac{\mathbb{Z}}{n\mathbb{Z}} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, 3 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}}$$

3) Combien l'ensemble $\frac{\mathbb{Z}}{n\mathbb{Z}}$ a-t-il d'éléments ?

Théorème (des lois de compositions internes sur le quotient d'un anneau par l'un de ses idéaux)
Soient $(A, \star, \sharp)$ un anneau et I un idéal de A.
Soient encore $(a, a', b, b') \in A^4$ tel que : $\begin{cases} a \star I = a' \star I \\ b \star I = b' \star I \end{cases}$
Alors on a les égalités d'ensemble suivants :

$$(a \star b) \star I = (a' \star b') \star I \qquad\qquad (a \sharp b) \star I = (a' \sharp b') \star I$$

Début de la démonstration du théorème précédent

Soient $(A,\star,\sharp)$ un anneau, I un idéal de A et $(a,a',b,b') \in A^4$ tel que : $\begin{cases} a\star I = a'\star I \\ b\star I = b'\star I \end{cases}$

Démontrons que $(a\star b)\star I = (a'\star b')\star I$ par double inclusion.
Par symétrie des rôles, il suffit de montrer l'inclusion $(a'\star b')\star I \subset (a\star b)\star I$.
Soit $x \in (a'\star b')\star I$.
Par définition de $(a'\star b')\star I$, il existe $i_1 \in I$ tel que :

$$x = a'\star b'\star i_1$$

Par ailleurs, en notant 0_A le neutre pour la loi $\star$, comme $a' = a'\star 0_A \in a'\star I = a\star I$ et $b' = b'\star 0_A \in b'\star I = b\star I$, on a aussi par définition :

- Il existe $i_2 \in I$ tel que $a' = a\star i_2$
- Il existe $i_3 \in I$ tel que $b' = b\star i_3$

En définitive :

$$x = a'\star b'\star i_1 = a\star i_2\star b\star i_3\star i_1 = a\star b\star \underbrace{(i_1\star i_2\star i_3)}_{\in I} \in (a\star b)\star I \qquad \square$$

Exercice-fin de la démonstration
Finir la démonstration du théorème précédent.

Théorème (des lois de compositions internes sur le quotient d'un anneau par l'un de ses idéaux)
Soient $(A,\star,\sharp)$ un anneau et I un idéal de A.
Alors :

- Les deux application suivantes sont bien définies :

$$\begin{array}{rccc} \overline{\star}: & \frac{A}{I}\times\frac{A}{I} & \to & \frac{A}{I} \\ & (a\star I, b\star I) & \mapsto & (a\star b)\star I \end{array} \qquad \begin{array}{rccc} \overline{\sharp}: & \frac{A}{I}\times\frac{A}{I} & \to & \frac{A}{I} \\ & (a\star I, b\star I) & \mapsto & (a\sharp b)\star I \end{array}$$

- $\left(\frac{A}{I},\overline{\star},\overline{\sharp}\right)$ est un anneau.

Exemple (**anneau des entiers modulo n**)
Soit $n \in \mathbb{N}^*$.
Via le théorème précédent, on obtient :

- **Les deux application suivantes sont bien définies :**

$$\begin{array}{rccc} \overline{+}: & \frac{\mathbb{Z}}{n\mathbb{Z}}\times\frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & (a+n\mathbb{Z}, b+n\mathbb{Z}) & \mapsto & (a+b)+n\mathbb{Z} \end{array} \qquad \begin{array}{rccc} \overline{\times}: & \frac{\mathbb{Z}}{n\mathbb{Z}}\times\frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & (a+n\mathbb{Z}, b+n\mathbb{Z}) & \mapsto & (a\times b)+n\mathbb{Z} \end{array}$$

- **$\left(\frac{\mathbb{Z}}{n\mathbb{Z}},\overline{+},\overline{\times}\right)$ est un anneau**.

Notation-abus de notation-exemple (**anneau des entiers modulo n**)
Soit $n \in \mathbb{N}^*$.

- On fait encore des abus de notation « $+ = \overline{+}$ » et og $\times = \overline{\times}$ » en écrivant par exemple « **$\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$ est un anneau**. ».
- Pour $k \in \mathbb{Z}$, on note :

$$\boxed{\overline{k} = k+n\mathbb{Z}}$$

- Par exemple :
  - Dans l'anneau $\left(\frac{\mathbb{Z}}{2\mathbb{Z}},+,\times\right)$:
    - $\overline{0}$ est l'ensemble des entiers relatifs pairs.
    - $\overline{1}$ est l'ensemble des entiers relatifs impairs.
  - Dans l'anneau $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$, $\overline{0}$ est l'ensemble des multiples de n.
- On continue d'utiliser cette notation **en notant de la même façon $\overline{k}$ les ensembles $k+n\mathbb{Z}$ et $k+m\mathbb{Z}$ même si $m \neq n$, le contexte indiquant si $\overline{k}$ désigne $k+n\mathbb{Z}$ ou bien $k+m\mathbb{Z}$**.

Commentaire
On démontrera bientôt un résultat fondamental pour le cryptosystème RSA, à savoir que le groupe des éléments inversibles de l'anneau $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ est l'ensemble des $\overline{a}$ tel que a et n n'admettent aucun diviseur commun dans $\mathbb{N} \setminus \{0;1\}$.

2 Arithmétique de $\mathbb{Z}$

2.1 Division euclidienne et divisibilité

Exemples (division euclidienne dans $\mathbb{Z}$)

- Quand on veut ranger 16 œufs dans des boîtes de 6, on remplit 2 boîtes complètement puis il reste encore 4 œufs qui ne peuvent pas remplir complètement une troisième boîte de 6 :

$$16 = \underbrace{2 \times 6}_{\text{2 boîtes de 6}} + \underbrace{4}_{\text{Il reste 4 œufs.}}$$

  - On a fait la division euclidienne de 16 par 6.
  - Dans cette **division euclidienne** :
    - 16 est le **dividende**.
    - 6 est le **diviseur**.
    - 2 est le **quotient**.
    - 4 est le **reste**.
  - ⚠ Les égalités « $16 = 3 \times 6 + (-2)$ » et « $16 = 1 \times 6 + 10$ » ne sont pas **la** division euclidienne de 16 par 6 car on n'a ni $0 \leq -2 < 6$ ni $0 \leq 10 < 6$.
  - Comme le reste de la division euclidienne de 16 par 6 est non nul, 6 n'est pas un diviseur de 16. On ne peut pas ranger tous les 16 œufs dans un nombre entier de fois un boîte de 6.
- $99 = 9 \times 11 + 0$ est la division euclidienne de 99 par 11 car $0 \leq 0 < 11$.
  On peut ranger 99 œufs dans 9 boîtes de 11 « sans qu'il en reste ».
- Quand les nombres sont plus grands, on peut poser la division euclidienne comme on le faisait à l'école :

	3	7	2	7	1	4	3
−(	2	8	6	↓)		2	6
	0	8	6	7			
−(	0	8	5	8)			
	0	0	0	9			

Combien il y va de fois 143 dans 372 ? Il y va 2 fois et il reste 86.
On abaisse 7.
Combien il y va de fois 143 dans 867 ? Il y va 6 fois et il reste 9.
Autrement dit, la division euclidienne de 3 727 par 143 est l'égalité suivante :

$$\underbrace{3\,727}_{\text{« 3 727 œufs »}} \underbrace{=}_{\text{« c'est »}} \underbrace{26 \times 143}_{\text{« 26 boîtes de 143 œufs »}} \underbrace{+}_{\text{« et »}} \underbrace{9}_{\text{« il en reste 9 »}}$$

Exercice-exemple (division euclidienne dans $\mathbb{Z}$)

1) Expliquer pourquoi l'égalité « $17 = 2 \times 6 + 5$ » est la division euclidienne de 17 par 6.
2) Expliquer pourquoi l'égalité « $17 = 6 \times 2 + 5$ » n'est pas la division euclidienne de 17 par 2.
3) Écrire la division euclidienne de 17 par 2.

Théorème-définition (division euclidienne dans $\mathbb{Z}$)
Soient n un entier relatif et d un entier relatif non nul.
Alors il existe un unique entier relatif d et un unique entier relatif r tels que :

$$\begin{cases} n = qd + r \\ 0 \leq r < |d| \end{cases}$$

- L'égalité « $n = qd + r$ » telle que $0 \leq r < |d|$ est appelée la **division euclidienne** de n par d.
- Dans cette égalité :
  - n est appelé le **dividende**.
  - d est appelé le **diviseur**.
  - q est appelé le **quotient**.
  - r est appelé le **reste**.

Exercice-exemple (division euclidienne dans $\mathbb{Z}$)

1) Expliquer pourquoi l'égalité « $17 = 3 \times 6 + (-1)$ » n'est pas la division euclidienne de 17 par 6.
2) Écrire la division euclidienne de -17 par 6.

Exercice (les sous-groupes de $(\mathbb{Z},+)$ sont monogènes)
En utilisant le théorème de division euclidienne, démontrer que les seuls sous-groupes de $(\mathbb{Z},+)$ sont les groupes de la forme $(n\mathbb{Z},+)$ avec $n \in \mathbb{N}$.
Indication : Si on considère un sous-groupe $(H,+)$ non trivial de $(\mathbb{Z},+)$, on peut montrer que $H = n\mathbb{Z}$ avec $n = min(H \cap \mathbb{N}^*)$.

Définition (divisibilité)
Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$.
On dit que n **divise** a lorsque le reste de la division euclidienne de a par n est nulle.
Autrement dit :

$$\boldsymbol{n \text{ divise } a \iff \exists\, d \in \mathbb{Z} \mid a = d \times n}$$

Dans ce cas, on dit aussi que a est un **multiple** de n ou que n est un **diviseur** de a.

2.2 Congruence

Exercice (congruence)
Soient $n \in \mathbb{N}^*$ et $(a,b) \in \mathbb{Z}^2$.
Démontrer que les assertions suivantes sont équivalentes :

i) $n \mid b-a$
ii) a et b ont le même reste dans la division euclidienne par n
iii) $a + n\mathbb{Z} = b + n\mathbb{Z}$

Définition (congruence)
Soient $n \in \mathbb{N}^*$ et $(a,b) \in \mathbb{Z}^2$.
On dit que a et b sont **congrus modulo n** et on note

$$\boldsymbol{a \equiv b\ [n]}$$

lorsque l'une des assertions suivantes est vérifiée :

i) $n \mid b-a$
ii) a et b ont le même reste dans la division euclidienne par n
iii) $a + n\mathbb{Z} = b + n\mathbb{Z}$

Remarque (congruence)
Cette dernière assertion peut encore s'écrire :

$$\boldsymbol{\overline{a} = \overline{b}}$$

Exercice (compatibilité de l'addition et de la multiplication avec la congruence)
Soient $n \in \mathbb{N}$ et $(a,a',b,b') \in \mathbb{Z}^4$ tel que $\begin{cases} a \equiv a'\ [n] \\ b \equiv b'\ [n] \end{cases}$
En utilisant la structure d'anneau $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$, démontrer que :

$$a+b \equiv a'+b'\ [n] \qquad\qquad ab \equiv a'b'\ [n]$$

Théorème (compatibilité de l'addition et de la multiplication avec la congruence)
Soient $n \in \mathbb{N}$ et $(a,a',b,b') \in \mathbb{Z}^4$.
Alors :

$$\left.\begin{array}{l} \boldsymbol{a \equiv a'\ [n]} \\ \boldsymbol{b \equiv b'\ [n]} \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} \boldsymbol{a+b \equiv a'+b'\ [n]} \\ \boldsymbol{ab \equiv a'b'\ [n]} \end{array}\right.$$

Exemple (compatibilité de l'addition et de la multiplication avec la congruence)
Dans l'anneau $\left(\frac{\mathbb{Z}}{7\mathbb{Z}},+,\times\right)$:

$$\begin{aligned}
\overline{1\,000\,000\,019} &= \overline{1\,000\,000\,000} + \overline{19} \\
&= \overline{10^9} + \overline{19} \\
&= \overline{10\times10\times10\times10\times10\times10\times10\times10\times10} + \overline{19} \\
&= \overline{10}\times\overline{10}\times\overline{10}\times\overline{10}\times\overline{10}\times\overline{10}\times\overline{10}\times\overline{10}\times\overline{10} + \overline{19} \\
&= \left(\overline{10}\right)^9 + \overline{19} \\
&= \left(\overline{1\times7+3}\right)^9 + \overline{2\times7+5} \\
&= \left(\overline{3}\right)^9 + \overline{5} \\
&= \left(\overline{3}\right)^{3\times3} + \overline{5} \\
&= \left(\left(\overline{3}\right)^3\right)^3 + \overline{5} \\
&= \left(\overline{3^3}\right)^3 + \overline{5} \\
&= \left(\overline{27}\right)^3 + \overline{5} \\
&= \left(\overline{3\times7+6}\right)^3 + \overline{5} \\
&= \left(\overline{6}\right)^3 + \overline{5} \\
&= \overline{36}\times\overline{6} + \overline{5} \\
&= \overline{5\times7+1}\times\overline{6} + \overline{5} \\
&= \overline{1}\times\overline{6} + \overline{5} \\
&= \overline{6} + \overline{5} \\
&= \overline{6+5} \\
&= \overline{11} \\
&= \overline{1\times7+4} \\
&= \overline{4}
\end{aligned}$$

Donc le reste de la division euclidienne de 1 000 000 019 par 7 est 4 :

$$1\,000\,000\,019 \equiv 4\ [7]$$

Exercice (application de la compatibilité de l'addition et de la multiplication avec la congruence)
Démontrer qu'un entier relatif est divisible par 9 si et seulement si la somme des chiffres de son écriture décimale est divisible par 9.

Exercice (application de la compatibilité de l'addition et de la multiplication avec la congruence)

1) Démontrer que :

$$10^6 \equiv 1\ [7]$$

2) En déduire :

$$\sum_{k=1}^{10} 10^{10^k} \equiv 5\ [7]$$

Exercice (application de la compatibilité de l'addition et de la multiplication avec la congruence)
Démontrer que pour tout $n \in \mathbb{N}$, 7 divise $1 + 2^{2^n} + 4^{2^n}$.

2.3 Algorithme d'Euclide, PGCD (Plus Grand Commun Diviseur) et coefficients de Bézout

Exercice (PGCD et démonstration du lemme de Bézout)
Soient $n \in \mathbb{N}^*$ et $(a_1, a_2, ..., a_n) \in \mathbb{Z}^n$ non tous nuls.
On note :

$$\sum_{i=1}^{n} a_i\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + ... + a_n\mathbb{Z} = \underbrace{\{a_1b_1 + a_2b_2 + ... + a_nb_n \in \mathbb{Z},\ (b_1, b_2, ..., b_n) \in \mathbb{Z}^n\}}_{\text{ensemble des entiers de la forme } a_1b_1 + a_2b_2 + ... + a_nb_n \text{ avec } (b_1, b_2, ..., b_n) \in \mathbb{Z}^n}$$

1) Démontrer que $a_1\mathbb{Z} + a_2\mathbb{Z} + ... + a_n\mathbb{Z}$ forme un groupe avec la loi $+$.
2) En déduire qu'il existe $d \in \mathbb{N}$ tel que :

$$d\mathbb{Z} = \sum_{i=1}^{n} a_i\mathbb{Z}$$

3) Démontrer que :

$$\forall\ i \in [\![1; n]\!],\ d \mid a_i$$

4) Soit d' un diviseur commun à tous les a_i.
Démontrer que : $d' \mid d$
5) En déduire que d est le plus grand entier qui divise tous les a_i.

Définition (**P**lus **G**rand **C**ommun **D**iviseur (**PGCD**))
Soient $n \in \mathbb{N}^*$ et $(a_1, a_2, ..., a_n) \in \mathbb{Z}^n$ non tous nuls.
On appelle **plus grand commun diviseur de la familles d'entiers a_1,...,a_n** l'unique entiers naturel noté $PGCD(a_1, ..., a_n)$ tel que :

$$\sum_{i=1}^{n} a_i\mathbb{Z} = PGCD(a_1, ..., a_n)\mathbb{Z}$$

Remarque (« le PGCD est comme son nom l'indique... »)
D'après l'exercice précédent, il s'agit effectivement du plus grand entier naturel qui divise simultanément tous les entiers relatifs de la famille concernée.

Théorème (**Lemme de Bézout**)
Soient $n \in \mathbb{N}^*$ et $(a_1, a_2, ..., a_n) \in \mathbb{Z}^n$ non tous nuls.
Alors :

$$\exists\ (u_1, u_2, ..., u_n) \in \mathbb{Z}^n \mid PGCD(a_1, ..., a_n) = \sum_{i=1}^{n} u_i a_i$$

Commentaire
Le PGCD d'une famille de deux entiers relatifs et leurs coefficients u_1 et u_2 vérifiant l'égalité précédente appelés bientôt « coefficients de Bézout » vont jouer un rôle fondamental dans le cryptosystème RSA.
⚠De tels coefficients ne sont pas uniques.
Les algorithmes qui suivent sont très importants car ils permettent de calculer ce PGCD et des coefficients de Bézout.

Définition-notation-exercice (**algorithme d'Euclide**)
Soit $(a,b)\in\mathbb{Z}^2$ tel que $|a|>|b|$.
Pour $x\in\mathbb{Z}$, on note $\mathscr{D}(x)=\{u\in\mathbb{Z},\ u\mid x\}$ l'ensemble des diviseurs de x.

1) Soit q_0 et r_0 le quotient et le reste de la division euclidienne de a par b.
Démontrer que :
$$\mathscr{D}(a)\cap\mathscr{D}(b)=\mathscr{D}(b)\cap\mathscr{D}(r_0)$$

2) On suppose que $r_0\neq 0$.
Soit q_1 et r_1 le quotient et le reste de la division euclidienne de b par r_0.
Démontrer que :
$$\mathscr{D}(b)\cap\mathscr{D}(r_0)=\mathscr{D}(r_0)\cap\mathscr{D}(r_1)$$

3) On suppose que $r_1\neq 0$.
Soit q_2 et r_2 le quotient et le reste de la division euclidienne de r_0 par r_1.
Démontrer que :
$$\mathscr{D}(r_0)\cap\mathscr{D}(r_1)=\mathscr{D}(r_1)\cap\mathscr{D}(r_2)$$

4) On continue de définir les termes de la suite $(r_n)_n$ avec cet algorithme qu'on appelle l'**algorithme d'Euclide** tant que le reste de la division euclidienne n'est pas nul.
   a) Démontrer que la suite $(r_n)_n$ est strictement décroissante.
   b) En déduire que l'algorithme d'Euclide est fini.
   c) Le dernier terme de la suite $(r_n)_n$ est donc nul.
   Démontrer que l'avant-dernier terme de la suite $(r_n)_n$ est $PGCD(a,b)$.

Exercice (algorithme d'Euclide)
Via l'algorithme d'Euclide, implémenter en *Python* une fonction qui retourne le PGCD de ses deux arguments.

Définition-exercice (**algorithme d'Euclide étendu**)
Soit $(a,b)\in\mathbb{Z}^2$ tel que $|a|>|b|$.

1) À chaque étape de l'algorithme d'Euclide, on aurait pu aussi déterminer une expression du reste sous la forme $ua+vb$ comme ci-dessous :

$a=q_0b+r_0$	$r_0=a-q_0b$	$u_0=1$	$v_0=-q_0$
$b=q_1r_0+r_1$	$r_1=b-q_1r_0=b-q_1\left(u_0a+v_0b\right)=-q_1u_0a+\left(1-q_1v_0\right)b$	$u_1=-q_1u_0$	$v_1=1-q_1v_0$
$r_0=q_2r_1+r_2$	$r_2=r_0-q_2r_1=\left(u_0a+v_0b\right)-q_2\left(u_1a+v_1b\right)=\left(u_0-q_2u_1\right)a+\left(v_0-q_2v_1\right)b$	$u_2=u_0-q_2u_1$	$v_2=v_0-q_2v_1$
$r_1=q_3r_2+r_3$	$r_3=r_1-q_3r_2=\left(u_1a+v_1b\right)-q_3\left(u_2a+v_2b\right)=\left(u_1-q_3u_2\right)a+\left(v_1-q_3v_2\right)b$	$u_3=u_1-q_3u_2$	$v_3=v_1-q_3v_2$
...	...	...	...
$r_{k-1}=q_{k+1}r_k+r_{k+1}$	$r_{k+1}=r_{k-1}-q_{k+1}r_k=...=\left(u_{k-1}-q_{k+1}u_k\right)a+\left(v_{k-1}-q_{k+1}v_k\right)b$	$u_{k+1}=u_{k-1}-q_{k+1}u_k$	$v_{k+1}=v_{k-1}-q_{k+1}v_k$
$r_k=q_{k+2}r_{k+1}+0$			

On appelle cet algorithme l'**algorithme d'Euclide étendu**.
En utilisant l'**algorithme d'Euclide étendu**, démontrer que :
$$\exists\ (u,v)\in\mathbb{Z}^2\ \mid\ PGCD(a,b)=ua+vb$$

2) Deux entiers relatifs u et v tels que $PGCD(a,b)=ua+vb$ sont appelés des coefficients de Bézout de a et de b.
Via l'**algorithme d'Euclide étendu**, implémenter en *Python* une fonction qui retourne des coefficients de Bézout de ses deux arguments.

Exercice (expression de deux coefficients de Bézout en fonction des quotients successifs de l'algorithme d'Euclide)
Soit $(a,b) \in \mathbb{Z}^2$ tel que $|a| > |b|$.
On reprend les notations q_k et r_k précédentes de l'algorithme d'Euclide.

1) Déterminer une matrice $A_0 \in \mathcal{M}_2(\mathbb{Z})$ telle que :

$$\begin{pmatrix} a \\ b \end{pmatrix} = A_0 \begin{pmatrix} b \\ r_0 \end{pmatrix}$$

2) Déterminer une matrice $A_1 \in \mathcal{M}_2(\mathbb{Z})$ telle que :

$$\begin{pmatrix} b \\ r_0 \end{pmatrix} = A_1 \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

3) En déduire une famille finie A_0, A_1, ..., A_u de matrices de $\mathcal{M}_2(\mathbb{Z})$ telle que :

$$\begin{pmatrix} a \\ b \end{pmatrix} = A_0 A_1 ... A_u \begin{pmatrix} PGCD(a,b) \\ 0 \end{pmatrix}$$

4) En déduire que :

$$\begin{pmatrix} PGCD(a,b) \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_u \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{u-1} \end{pmatrix} ... \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

5) En déduire une une fonction *Python* qui retourne des coefficients de Bézout de ses deux arguments via l'algorithme d'Euclide et du calcul matriciel.

2.4 Nombres premiers et conséquences de l'algorithme d'Euclide

Définition-notation (nombres premiers)
Les entiers naturels différents de 1 qui ne sont divisibles que par 1 et eux-même sont appelés les **nombres premiers**.
On note :

$$\mathscr{P} = \text{l'ensemble des nombres premiers}$$

Définition (nombres premiers entre eux)
Soient $n \in \mathbb{N}^*$ et $(a_1, a_2, ..., a_n) \in \mathbb{Z}^n$.
On dit que les nombres a_1, a_2,...,a_n sont **premiers entre eux** lorsque que $PGCD(a_1, ..., a_n) = 1$.

Exercice (démonstration du théorème de Bézout)
Soit $(a,b) \in \mathbb{Z}^2$.

1) Supposons que a et b sont premiers entre eux.
Démontrer que : $\exists\ (u,v) \in \mathbb{Z}^2 \mid ua + vb = 1$
2) Supposons maintenant que : $\exists\ (u,v) \in \mathbb{Z}^2 \mid ua + vb = 1$
Démontrer que a et b sont premiers entre eux.
Indication : Utiliser le lemme de Bézout pour montrer qu'un diviseur commun à a et b divise 1.

Théorème (**théorème de Bézout**)
Soit $(a,b) \in \mathbb{Z}^2$.
Alors :

$$\boldsymbol{PGCD(a,b) = 1 \iff \exists\ (u,v) \in \mathbb{Z}^2 \mid ua + vb = 1}$$

Exercice (démonstrations du lemme de Gauss et du lemme d'Euclide)

1) Soient $(a,b,c) \in \mathbb{Z}^3$ tel que $a \mid bc$ et $PGCD(a,b) = 1$.
   a) Appliquer le théorème de Bézout à a et b.
   b) En déduire que $a \mid c$.
   Indications : Multiplier la relation de Bézout par c et expliciter l'assertion « $a \mid bc$ » en vu de factoriser par a.
2) Soient $p \in \mathscr{P}$ et $(a,b) \in \mathbb{Z}^2$ tel que $p \mid ab$ et $p \nmid a$.
Utiliser la question précédente pour démontrer que : $p \mid b$

Théorème (**lemme de Gauss**)
Soient $(a,b,c) \in \mathbb{Z}^3$.
Alors :

$$\left.\begin{array}{l} a \mid bc \\ PGCD(a,b) = 1 \end{array}\right\} \Longrightarrow a \mid c$$

Théorème (**lemme d'Euclide**)
Soit $(p,a,b) \in \mathbb{Z}^3$.
Alors :

$$\left.\begin{array}{l} p \mid ab \\ p \in \mathscr{P} \end{array}\right\} \Longrightarrow (p \mid a \text{ ou } p \mid b)$$

Exercice (démonstration de l'existence d'un diviseur premier)
Soit $n \in \mathbb{N} \setminus \{0;1\}$.

1) Démontrer que : $\mathscr{D}(n) \cap \mathbb{N}^* \neq \emptyset$
2) On note : $p = \min(\mathscr{D}(n) \cap \mathbb{N}^*)$
   Soit $(a,b) \in \mathbb{N}^2$ tel que $p = ab$ et $a \neq 1$.
   a) Démontrer que : $a \in \mathscr{D}(n) \cap \mathbb{N}^*$
   b) En déduire que : $a = p$
   c) En déduire que : $p \in \mathscr{P}$

Théorème (**existence d'un diviseur premier**)
Soit $n \in \mathbb{N} \setminus \{0;1\}$.
Alors :

$$\exists\, p \in \mathscr{P} \mid p \text{ divise } n$$

Théorème-notation-définition (**Théorème fondamental de l'arithmétique** et **valuation p-adique d'un entier**)
Soit $n \in \mathbb{N} \setminus \{0;1\}$.
Pout tout $p \in \mathscr{P}$, on appelle valuation p-adique et on note $v_p(n)$ le plus grand entier k tel que p^k divise n (on a donc $p^{v_p(n)}$ divise n).
On a l'existence et l'unicité de la décomposition de n en produit de nombres premiers suivante :

- *(Existence)*

$$n = \prod_{p \in \mathscr{P}} p^{v_p(n)}$$

  Remarque : On a noté abusivement le produit fini $\prod_{p \in \mathscr{P} \mid p \text{ divise } n} p^{v_p(n)}$ avec « le produit infini $\prod_{p \in \mathscr{P}} p^{v_p(n)}$ ».
  Comme $v_p(n) = 0$ et $p^0 = 1$ pour tout p premier sauf pour un nombre fini de nombres premiers, on a noté « 1 » avec « un produit comportant un nombre infini de facteurs 1 ».
- *(Unicité)*
  De plus, cette décomposition est unique, c'est-à-dire :

$$\forall\, \left(w_p(n)\right)_{p \in \mathscr{P}} \in \mathbb{N}^{\mathscr{P}},\ \left(n = \prod_{p \in \mathscr{P}} p^{w_p(n)} \Longrightarrow \forall\, p \in \mathscr{P},\ w_p(n) = v_p(n)\right)$$

Exemple (une décomposition primaire)

- $540 = 2^2 \times 3^3 \times 5$ (Une factorisation de 540 existe.)
- Si $540 = 2^\alpha \times 3^\beta \times 5^\gamma \times 7^\delta$, alors $\left\{\begin{array}{l} \alpha = v_2(540) = 2 \\ \beta = v_3(540) = 3 \\ \gamma = v_5(540) = 1 \\ \delta = v_7(540) = 0 \end{array}\right.$ (Cette factorisation de 540 est unique.)

Exercice (une application du théorème fondamental de l'arithmétique)
Démontrer qu'un entier naturel qui est à la fois le carré d'un entier et le cube d'un entier est aussi le carré d'un cube d'un entier.

Exercice-démonstration (Théorème fondamental de l'arithmétique)
Démontrer le théorème fondamental de l'arithmétique par récurrence sur n en utilisant le théorème « existence d'un diviseur premier ».

Théorème (Conséquences du théorème fondamental de l'arithmétique)

- Soit $(a,b) \in \mathbb{N}^2$.
  Alors :

$$a \mid b \iff \forall\ p \in \mathscr{P},\ v_p(a) \leq v_p(b)$$
$$PGCD(a,b) = 1 \iff \forall\ p \in \mathscr{P},\ \left(v_p(a) = 0 \text{ ou } v_p(b) = 0\right)$$

- Soient $n \in \mathbb{N}^*$, $b \in \mathbb{Z}$ et $(a_1, a_2, ..., a_n) \in \mathbb{Z}^n$.
  Alors :

$$\left.\begin{array}{l} \boldsymbol{a_1, a_2, ..., a_n} \textbf{ deux à deux premiers entre eux} \\ \boldsymbol{\forall\ i \in [\![1;n]\!],\ a_i \mid b} \end{array}\right\} \Longrightarrow \prod_{i=1}^{n} a_i \mid b$$

Commentaire
Cette dernière conséquence est très importante.
En effet, on va voir dans la section suivante qu'elle permet factoriser non pas le nombre entier n avec sa décomposition en facteurs premiers

$$p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$$

mais l'anneau $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ avec le produit d'anneaux

$$\left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}}, +, \times\right) \times \left(\frac{\mathbb{Z}}{p_2^{\alpha_2}\mathbb{Z}}, +, \times\right) \times ... \times \left(\frac{\mathbb{Z}}{p_r^{\alpha_r}\mathbb{Z}}, +, \times\right)$$

On va voir aussi dans la section suivante que cette dernière décomposition induit une décomposition du groupe des éléments inversibles $\left(U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right), \times\right)$ de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ en le produit de groupes :

$$\left(U\left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}}\right), \times\right) \times \left(U\left(\frac{\mathbb{Z}}{p_2^{\alpha_2}\mathbb{Z}}\right), \times\right) \times ... \times \left(U\left(\frac{\mathbb{Z}}{p_r^{\alpha_r}\mathbb{Z}}\right), \times\right)$$

Cette dernière décomposition va alors fournir une expression du nombre d'entiers naturels appartenant à $[\![1;n]\!]$ qui sont premiers avec n (ie l'indicatrice d'Euler notée $\phi(n)$) en fonction de la décomposition en facteurs premiers de n.
Et cette dernière expression de l'indicatrice d'Euler est fondamentale pour construire le cryptosystème RSA.

3 Application à l'étude des anneaux $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$

3.1 Applications aux cardinaux des groupes finis et définition du sous-groupe engendré par un élément

Exercice (Les classes latérales forment une partition)
Soient $(G, \star)$ un groupe, $(H, \star)$ un sous-groupe de $(G, \star)$ et $(g_1, g_2) \in G^2$.
On suppose que $(g_1 \star H) \cap (g_2 \star H) \neq \emptyset$. Autrement dit, on suppose qu'il existe $x \in G$ tel que $x \in (g_1 \star H) \cap (g_2 \star H)$.

1) Démontrer qu'il existe $(h,k) \in H^2$ tel que : $g_1 \star h = g_2 \star k$
2) En déduire que : $g_1 \in g_2 \star H$
   Indication : Multiplier à droite par le symétrique de h pour la loi $\star$.
3) En déduire que : $g_1 \star H \subset g_2 \star H$
4) Démontrer que : $g_1 \star H = g_2 \star H$

Théorème (Les classes latérales forment une partition)
Soient $(G, \star)$, $(H, \star)$ un sous-groupe de $(G, \star)$ et $(g_1, g_2) \in G^2$.
Alors :

$$(g_1 \star H) \cap (g_2 \star H) = \emptyset \text{ ou } g_1 \star H = g_2 \star H$$

Exercice (Les classes latérales ont le même nombre d'éléments)
Soient $(G,\star)$ un groupe, $(H,\star)$ un sous-groupe de $(G,\star)$ et $(g_1,g_2)\in G^2$.
On note u le symétrique de g_1 pour la loi $\star$.
On note aussi :

$$\begin{array}{rccc}\Psi: & g_1\star H & \to & g_2\star H\\ & x & \mapsto & g_2\star u\star x\end{array}$$

1) Démontrer que l'application Ψ est bien définie.
Indication : Il s'agit de montrer que : $\forall\ h\in H,\ g_2\star u\star g_1\star h\in g_2\star H$
2) Démontrer que l'application Ψ est surjective.
Autrement dit, démontrer que chaque élément de l'ensemble d'arrivée admet au moins un antécédent :

$$\forall\ y\in g_2\star H,\ \exists\ x\in g_1\star H\ \mid\ \Psi(x)=y$$

3) Démontrer que l'application Ψ est injective.
Autrement dit, démontrer que deux éléments différents de l'ensemble de départ ne peuvent pas avoir la même image :

$$\forall\ (x_1,x_2)\in\left(g_1\star H\right)^2,\ (\Psi(x_1)=\Psi(x_2)\implies x_1=x_2)$$

Commentaire : On a ainsi démontré que l'on peut « ranger » tous les éléments de $(g_1\star H)\cup(g_2\star H)$ deux par deux où chaque couple « marrie » un élément x de $g_1\star H$ avec son image $\Psi(x)\in g_2\star H$.
Une telle application qui peut faire ces « marriages » est appelée une bijection.
L'existence d'une bijection entre deux ensembles est intéressante car elle implique que les deux ensembles ont le même nombre d'éléments.

Exemple (partitionnement du groupe $(\mathbb{Z},+)$ par les classes modulo n)
Soient $n\in\mathbb{N}^*$ et $(i,j)\in[\![0;n-1]\!]^2$.
On considère le groupe $(\mathbb{Z},+)$ et son sous-groupe $(n\mathbb{Z},+)$.

- Les classes latérales considérées dans les deux théorèmes précédents sont :

$$0+n\mathbb{Z},\ 1+n\mathbb{Z},\ 2+n\mathbb{Z},...,(n-1)+n\mathbb{Z}$$

- Elles forment bien une partition de $\mathbb{Z}$.
Autrement dit, elles recouvrent bien $\mathbb{Z}$ sans se chevaucher :

$$\underbrace{(i+n\mathbb{Z})\cap(j+n\mathbb{Z})=\emptyset \text{ ou } i+n\mathbb{Z}=j+n\mathbb{Z}}_{\text{Elles ne se chevauchent pas.}}\qquad\underbrace{\mathbb{Z}=\bigcup_{i=0}^{n-1}(i+n\mathbb{Z})}_{\text{Elles recouvrent }\mathbb{Z}.}$$

- L'application suivante est bien une bijection :

$$\begin{array}{rccc}\Psi: & i+n\mathbb{Z} & \to & j+n\mathbb{Z}\\ & i+nk & \mapsto & j+(-i)+i+nk=j+nk\end{array}$$

Tous les éléments de $i+n\mathbb{Z}$ et de $j+n\mathbb{Z}$ « sont mariés » par Ψ.
Les couples sont de la forme $\left(\underbrace{i+nk}_{\in i+n\mathbb{Z}},\underbrace{j+nk}_{\in j+n\mathbb{Z}}\right)$.

Remarque
Dans l'exemple précédent, les classes latérales ont bien le même nombre d'éléments mais elles sont infinies (ie elles sont un nombre infini d'éléments). Il y a autant de mariage que d'entiers relatifs : On pourrait numéroter ces marriages avec les entiers relatifs ; par exemple, le marriage numéro (-7) est $\left(\underbrace{i+n\times(-7)}_{\in i+n\mathbb{Z}},\underbrace{j+n\times(-7)}_{\in j+n\mathbb{Z}}\right)$.
On introduit alors maintenant « une machine à fabriquer des sous-groupes » afin de pouvoir appliquer « ces marriages » avec un groupe fini et l'un de ses sous-groupe en vu d'obtenir une relation de divisibilité.

Exercice-notation (groupe engendré par un élément)
Soient $(G,\star)$ un groupe et $g\in G$.
On note e l'élément neutre de G et u le symétrique de g pour la loi $\star$.
On note aussi :

$$\langle g\rangle = \{...,u\star u\star u,u\star u,u,e,g,g\star g,g\star g\star g,g\star g\star g\star g,...\} = \{...,g^{-3},g^{-2},g^{-1},g^0,g^1,g^2,g^3,g^4,...\} = \left\{g^k,k\in\mathbb{Z}\right\}$$

1) Démontrer que $\left(\langle g\rangle,\star\right)$ est un sous-groupe de $(G,\star)$.
2) Dans cette question, on suppose que : $(G,\star)=\left(\frac{\mathbb{Z}}{8\mathbb{Z}},+\right)$
   a) Déterminer $\langle 2+8\mathbb{Z}\rangle$
   b) Déterminer $\langle 3+8\mathbb{Z}\rangle$

Définition-théorème (**groupe engendré par un élément**)
Soient $(G,\star)$ un groupe et $g\in G$.

- **$\left(\langle g\rangle,\star\right)$ est un sous-groupe de $(G,\star)$**.
- On appelle **$\left(\langle g\rangle,\star\right)$ le sous-groupe de $(G,\star)$ engendré par l'élément g**.

Exemple (partionnement du groupe fini $\left(\frac{\mathbb{Z}}{8\mathbb{Z}},+\right)$ par les classes latérales relatives au sous-groupe $(\langle 2+8\mathbb{Z}\rangle,+)$)
En notant $\forall\ k\in[\![0;7]\!]$, $\overline{k}=k+8\mathbb{Z}$, on a :

$$\frac{\mathbb{Z}}{8\mathbb{Z}} = \left(\overline{0}+\langle\overline{2}\rangle\right) \underset{\text{disjointe}}{\cup} \left(\overline{1}+\langle\overline{2}\rangle\right)$$

En effet :

$$\begin{aligned}\left(\overline{0}+\langle\overline{2}\rangle\right)\cup\left(\overline{1}+\langle\overline{2}\rangle\right) &= \{\overline{0},\overline{2},\overline{4},\overline{6}\}\cup\{\overline{1},\overline{3},\overline{5},\overline{7}\}\\ &= \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7}\}\\ &= \frac{\mathbb{Z}}{8\mathbb{Z}}\end{aligned}$$

Remarque
Soient $(G,\star)$ un groupe fini et $(H,\star)$ un sous-groupe fini de $(G,\star)$.
Ce qui précède montre que l'on peut décomposer l'ensemble G en une réunion disjointe finie de sous-ensembles ayant chacun le même nombre d'éléments que H :

$$G = H \underset{\text{disjointe}}{\cup} \left(g_1\star H\right) \underset{\text{disjointe}}{\cup} \left(g_2\star H\right) \underset{\text{disjointe}}{\cup} ... \underset{\text{disjointe}}{\cup} \left(g_r\star H\right)$$

On peut ainsi exprimer le nombre d'éléments $|G|$ de G en fonction du nombre d'élément $|H|$ de H comme suit :

$$\begin{aligned}|G| &= \underbrace{|H|+\left|g_1\star H\right|+\left|g_2\star H\right|+...+\left|g_r\star H\right|}_{r+1\text{ termes}}\\ &= \underbrace{|H|+|H|+|H|+...+|H|}_{r+1\text{ termes}} \qquad \text{(car les classes latérales ont toutes } |H| \text{ éléments)}\\ &= (r+1)\,|H|\end{aligned}$$

On vient donc de démontrer le très important théorème de Lagrange :

Théorème (**théorème de Lagrange**)
Soient **$(G,\star)$ un groupe fini et $(H,\star)$ un sous-groupe de $(G,\star)$**.
Alors le nombre d'éléments $|H|$ de H divise le nombre d'éléments $|G|$ de G :

$$|H| \text{ divise } |G|$$

3.2 Application à la détermination du groupe des éléments inversibles de l'anneau $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$ et définition de l'indicatrice d'Euler

Définition-notation (groupe des éléments inversibles d'un anneau)
Soit $(A,\star,\sharp)$ un anneau.

- On dit qu'un élément a de A est inversible lorsqu'il admet un inverse pour la loi $\sharp$.
- Dans la section « Sous-groupes d'un groupe », on a déjà montré que l'ensemble de tous les éléments inversibles de A forme un groupe pour la loi $\sharp$.
  On appelle ce groupe le **groupe des éléments inversibles de l'anneau** $(A,\star,\sharp)$.
- On note $\boldsymbol{U(A,\star,\sharp)}$ ou $\boldsymbol{U(A)}$ l'ensemble des éléments inversibles de l'anneau $(A,\star,\sharp)$.

Exemple (groupe des éléments inversibles d'un anneau)
Le groupe des éléments inversibles de l'anneau $(\mathbb{Z},+,\times)$ est $U((\mathbb{Z},+,\times)) = (\{-1;+1\},\times)$.

Exercice-exemple (groupe des éléments inversibles des anneaux $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$)
Soient $(n,a)\in(\mathbb{N}^*)^2$.
En utilisant le théorème de Bézout, démontrer que :

$$a+n\mathbb{Z} \text{ est un élément inversible de l'anneau } \left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right) \iff PGCD(n,a)=1$$

Théorème (groupe des éléments inversibles des anneaux $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$)
Soient $n\in\mathbb{N}^*$.
Alors :

$$\boldsymbol{U\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right) = \{a+n\mathbb{Z},\ a \text{ et } n \text{ sont premiers entre eux.}\}}$$

Définition-notation (indicatrice d'Euler)
On appelle fonction **indicatrice d'Euler** la fonction notée comme suit :

$$\begin{array}{rccl} \boldsymbol{\phi}: & \mathbb{N}^* & \to & \mathbb{N}^* \\ & \boldsymbol{n} & \mapsto & \textbf{le nombre d'éléments de } [\![1;n]\!] \textbf{ qui sont premiers avec } \boldsymbol{n} \end{array}$$

Exemple (indicatrice d'Euler)
Les éléments de $[\![1;20]\!]$ qui sont premiers avec 20 sont 1, 3, 7, 9, 11, 13, 17 et 19.
Donc : $\phi(20)=8$

Théorème (l'indicatrice d'Euler est le cardinal du groupe des éléments inversibles de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)$)

$$\boldsymbol{\forall\, n\in\mathbb{N}^*,\ \phi(n) = \left|U\left(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times\right)\right|}$$

Exercice-exemple (indicatrice d'Euler des puissances des nombres premiers)
Soient $p\in\mathscr{P}$ et $\alpha\in\mathbb{N}^*$.

1) Démontrer que : $\phi(p) = p-1$
2) Démontrer que : $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Exercice (démonstration du théorème d'Euler)
Soient $(n,a) \in (\mathbb{N}^*)^2$ tel que $PGCD(n,a) = 1$.
On note : $\forall\ k \in \mathbb{Z},\ \overline{k} = k + n\mathbb{Z}$
On a donc :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1},\}$$

On note $(\langle a \rangle, \times)$ le sous-groupe de $U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ engendré par a.
⚠ Dans cet exercice, la notation $\langle a \rangle$ ne fait pas référence au sous-groupe de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ engendré par a.

1) En appliquant l'un des théorèmes précédents, démontrer que : $a \in U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$
2) a) Démontrer qu'il existe $k \in \mathbb{N}^*$ tel que $\overline{a}^k = \overline{1}$.
   Indication : L'ensemble $\{\overline{1}, \overline{a}, \overline{a}^2, \overline{a}^3, ...\}$ est fini puisque c'est un sous-ensemble de l'ensemble fini $U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$.
   b) On note $\sigma(a)$ le plus petit entier naturel k tel que $\overline{a}^k = \overline{1}$.
   Démontrer que : $\sigma(a) = |\langle a \rangle|$
   c) Démontrer que : $\sigma(a)$ divise $\left|U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\right|$
   d) Démontrer que : $\sigma(a)$ divise $\phi(n)$
3) En déduire que : $\overline{a}^{\phi(n)} = \overline{1}$
4) En déduire que : $a^{\phi(n)} \equiv 1\,[n]$

Théorème (**théorème d'Euler**)
Soient $(n,a) \in (\mathbb{N}^*)^2$ tel que $\boldsymbol{PGCD(n,a) = 1}$.
Alors on a :

$$\boldsymbol{a^{\phi(n)} \equiv 1\,[n]}$$

Exercice (Démonstration du **petit théorème de Fermat**)
Soient $a \in \mathbb{N}^*$ et $\boldsymbol{p \in \mathscr{P}}$.
En utilisant le théorème d'Euler, démontrer que :

$$\boldsymbol{a^p \equiv 1\,[n]}$$

3.3 Application à la factorisation des anneaux $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$

Théorème-définition (produit de groupes et d'anneaux)
Soient $r \in \mathbb{N}^*$ et $(A_1, \star_1, \sharp_1)$, $(A_2, \star_2, \sharp_2)$,...,$(A_r, \star_r, \sharp_r)$ r anneaux.
On rappelle que le produit cartésien $\prod_{i=1}^{r} A_i = A_1 \times A_2 \times ... \times A_r$ des ensembles A_1,...,A_r est l'ensemble suivant :

$$\prod_{i=1}^{r} A_i = A_1 \times A_2 \times ... \times A_r = \{(a_1, ..., a_r) \mid \forall\ i \in [\![1;r]\!],\ a_i \in a_i\}$$

On note les applications suivantes :

$$\begin{array}{rccc} \star : & \left(\prod_{i=1}^{r} A_i\right) \times \left(\prod_{i=1}^{r} A_i\right) & \to & \prod_{i=1}^{r} A_i \\ & ((a_1,...,a_r),(b_1,...,b_r)) & \mapsto & (a_1 \star_1 b_1, ..., a_r \star_r b_r) \end{array} \qquad \begin{array}{rccc} \sharp : & \left(\prod_{i=1}^{r} A_i\right) \times \left(\prod_{i=1}^{r} A_i\right) & \to & \prod_{i=1}^{r} A_i \\ & ((a_1,...,a_r),(b_1,...,b_r)) & \mapsto & (a_1 \sharp_1 b_1, ..., a_r \sharp_r b_r) \end{array}$$

Alors :

- $\left(\prod_{i=1}^{r} A_i, \star\right)$ est un groupe abélien.
- $\left(\prod_{i=1}^{r} A_i, \star, \sharp\right)$ est un anneau.
- Le groupe des éléments inversibles du produit d'anneaux est le produit des groupes des éléments inversibles :

$$U\left(\prod_{i=1}^{r} A_i\right) = \prod_{i=1}^{r} U(A_i)$$

Exemple (produit de anneaux)
Les application suivantes sont des lois de composition internes sur l'ensemble $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$ et forme même un anneau avec cet ensemble :

$$\begin{array}{rccc} + : & \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) & \to & \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \\ & ((i+2\mathbb{Z}, j+3\mathbb{Z}), (k+2\mathbb{Z}, l+3\mathbb{Z})) & \mapsto & (i+k+2\mathbb{Z}, j+l+3\mathbb{Z}) \end{array} \qquad \begin{array}{rccc} \times : & \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}\right) & \to & \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \\ & ((i+2\mathbb{Z}, j+3\mathbb{Z}), (k+2\mathbb{Z}, l+3\mathbb{Z})) & \mapsto & (ik+2\mathbb{Z}, jl+3\mathbb{Z}) \end{array}$$

Par exemple, avec des abus de notation tels que $m+2\mathbb{Z} = \overline{k}$ et $n+3\mathbb{Z} = \overline{k}$, on a :

$$(\overline{0},\overline{0}) + (\overline{1},\overline{2}) = (\overline{1},\overline{2}) \qquad (\overline{1},\overline{1}) + (\overline{1},\overline{2}) = (\overline{0},\overline{0}) \qquad (\overline{1},\overline{2}) + (\overline{1},\overline{2}) = (\overline{0},\overline{1})$$

$$(\overline{1},\overline{1}) \times (\overline{1},\overline{2}) = (\overline{1},\overline{2}) \qquad (\overline{0},\overline{2}) \times (\overline{1},\overline{2}) = (\overline{0},\overline{1})$$

Exercice (Démonstration de la décomposition primaire des anneaux modulaires)
Soient $r \in \mathbb{N}^*$ et $(n_1, ..., n_r) \in (\mathbb{N}^*)^r$ un r-uplet d'entiers deux à deux premiers entre eux.

L'objectif de cet exercice est de montrer que l'application suivante est une bijection entre l'anneau $\frac{\mathbb{Z}}{\left(\prod_{i=1}^{k} n_i\right)\mathbb{Z}}$ et l'anneau $\prod_{i=1}^{k} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$ qui préserve leur sous-groupes d'éléments inversibles :

$$\begin{array}{rccc} \Psi : & \frac{\mathbb{Z}}{\left(\prod_{i=1}^{r} n_i\right)\mathbb{Z}} & \to & \prod_{i=1}^{r} \frac{\mathbb{Z}}{n_i\mathbb{Z}} \\ & x + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z} & \mapsto & (x + n_1\mathbb{Z}, ..., x + n_r\mathbb{Z}) \end{array}$$

1) Démontrer que Ψ est bien définie, c'est-à-dire démontrer que si $x_1 + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z} = x_2 + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z}$, alors on a bien $(x_1 + n_1\mathbb{Z}, ..., x_1 + n_r\mathbb{Z}) = (x_2 + n_1\mathbb{Z}, ..., x_2 + n_r\mathbb{Z})$.
2) Démontrer que les anneaux $\frac{\mathbb{Z}}{\left(\prod_{i=1}^{k} n_i\right)\mathbb{Z}}$ et $\prod_{i=1}^{k} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$ ont le même nombre d'éléments.
3) Pour montrer que Ψ est bijective, il suffit donc comme dans l'exercice « Les classes latérales ont le même nombre d'éléments » de démontrer que deux éléments différents de l'ensemble de départ ne peuvent pas avoir la même image :

$$\forall\ (\overline{x_1}, \overline{x_2}) \in \left(\frac{\mathbb{Z}}{\left(\prod_{i=1}^{r} n_i\right)\mathbb{Z}}\right)^2,\ \left(\Psi(\overline{x_1}) = \Psi(\overline{x_2}) \implies \overline{x_1} = \overline{x_2}\right)$$

Soit $(x_1, x_2) \in \mathbb{Z}^2$ tel que $\Psi\left(x_1 + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z}\right) = \Psi\left(x_2 + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z}\right)$.

a) Démontrer que :

$$\forall\ i \in [\![1; r]\!],\ n_i \text{ divise } x_2 - x_1$$

b) En utilisant le théorème « conséquences du théorème fondamental de l'arithmétique », démontrer que :

$$x_1 + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z} = x_2 + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z}$$

c) On montre pour finir dans cette question que Ψ envoie les éléments inversibles de l'anneau $\frac{\mathbb{Z}}{\left(\prod_{i=1}^{k} n_i\right)\mathbb{Z}}$ sur les éléments inversibles de l'anneau $\prod_{i=1}^{r} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$:

$$\Psi\left(U\left(\frac{\mathbb{Z}}{\left(\prod_{i=1}^{k} n_i\right)\mathbb{Z}}\right)\right) = U\left(\prod_{i=1}^{r} \frac{\mathbb{Z}}{n_i\mathbb{Z}}\right) = \prod_{i=1}^{r} U\left(\frac{\mathbb{Z}}{n_i\mathbb{Z}}\right)$$

Indication : En vertu du théorème « groupe des éléments inversibles des anneaux $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$ », il s'agit donc de montrer que si x est premier avec $\prod_{i=1}^{r} n_i$, alors x est premier avec n_i pour tout $i \in [\![1; r]\!]$.

Théorème (**décomposition primaire des anneaux modulaires**)
Soient $n \in \mathbb{N} \setminus \{0;1\}$.
On note la décomposition primaire de n comme suit :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

Alors l'application suivante est une bijection entre l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et l'anneau $\prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}$ qui préserve leur sous-groupes d'éléments inversibles :

$$\begin{array}{rccc} \Psi : & \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \prod_{i=1}^{r} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}} \\ & x + \left(\prod_{i=1}^{r} n_i\right)\mathbb{Z} & \mapsto & (x + n_1\mathbb{Z}, ..., x + n_r\mathbb{Z}) \end{array}$$

3.4 Conséquences de la factorisation des anneaux $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times\right)$

3.4.1 Le théorème chinois

Théorème (**le théorème chinois**)
Soient $r \in \mathbb{N}^*$, $(a_1, ..., a_r) \in \mathbb{Z}^r$ et $(n_1, ..., n_r) \in (\mathbb{N}^*)^r$ un r-uplet d'entiers deux à deux premiers entre eux.
Alors le système d'équations modulaires suivant d'inconnue x admet une infinité de solutions :

$$\begin{cases} x \equiv a_1 \, [n_1] \\ x \equiv a_2 \, [n_2] \\ ... \\ x \equiv a_r \, [n_r] \end{cases}$$

De plus, si x_0 est une solution, alors l'ensemble de toutes les solutions est l'ensemble suivant :

$$\mathscr{S} = x_0 + \prod_{i=1}^{r} n_i$$

Exercice (démonstration du théorème chinois)
En utilisant, le théorème de décomposition primaire des anneaux modulaires, démontrer le théorème chinois.

3.4.2 Une expression de l'indicatrice d'Euler d'un entier en fonction de sa décomposition primaire

Exercice (expression de l'indicatrice d'Euler d'un entier en fonction de sa décomposition primaire)
Soient $n \in \mathbb{N} \setminus \{0;1\}$.
On note la décomposition primaire de n comme suit :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

a) En utilisant, le théorème de décomposition primaire des anneaux modulaires, démontrer que :

$$\phi(n) = \prod_{i=1}^{r} \phi\left(p_i^{\alpha_i}\right)$$

b) En déduire que :

$$\phi(n) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

c) En déduire que :

$$\phi(n) = n \prod_{\substack{p \in \mathscr{P} \\ v_p(n) \neq 0}} \left(1 - \frac{1}{p}\right)$$

Théorème (**expression de l'indicatrice d'Euler d'un entier en fonction de ses diviseurs premiers**)

$$\forall\, n \in \mathbb{N}^*,\ \phi(n) = n \times \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \neq 0}} \left(1 - \frac{1}{p}\right)$$

4 Application à la construction du cryptosystème RSA

Exercice (cryptosystème RSA)
Soit $(p,q) \in \mathscr{P}^2$ tel que $p \neq q$.
On note le module du cryptosystème :

$$n = pq$$

Soit $e \in \mathbb{N}$ tel que :

$$\begin{cases} PGCD\left(e, \phi(n)\right) = 1 \\ 1 \leq e \leq \phi(n) - 1 \end{cases}$$

On appelle e l'exposant de la clé publique.
Soit $M \in [\![0; n-1]\!]$ tel que $PGCD(M,n) = 1$.
M correspond à la valeur numérique encodant un bloc du message que l'on souhaite crypter puis décrypter.
Et on suppose qu'une telle valeur M est toujours première avec n (Ce qui permettra d'appliquer le théorème d'Euler.).
Le module n du cryptosystème et l'exposant e de la clé publique sont des informations publiques qui permette de crypter le bloc M de message via l'application suivante :

$$\begin{array}{rccc} f: & \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & \overline{X} & \mapsto & \overline{X^e} \end{array}$$

On a noté ici $\overline{x} = x + n\mathbb{Z}$ et on continuera d'utiliser cette notation dans la suite.
Le bloc de message crypté est donc $\overline{M^e}$.
La sécurité du cryptosystème est assurée par le fait qu'il est impossible à ce jour de déterminer la réciproque de f, la fonction pour décrypter, à partir des informations publiques n et e si les nombres p, q et e sont bien choisis.

1) Démontrer que e appartient au groupe des éléments inversibles de l'anneau $\left(\frac{\mathbb{Z}}{\phi(n)\mathbb{Z}}, \overline{+}, \overline{\times}\right)$.
On note d l'unique élément de $[\![1; \phi(n)-1]\!]$ tel que $d + \phi(n)\mathbb{Z}$ est le symétrique de $e + \phi(n)\mathbb{Z}$ pour la loi $\overline{\times}$ du groupe des éléments inversibles de l'anneau $\left(\frac{\mathbb{Z}}{\phi(n)\mathbb{Z}}, \overline{+}, \overline{\times}\right)$.
On appelle d l'exposant de la clé privée.

2) Contrairement à l'exposant de clé publique, d est une information privée car elle permet de décryter un bloc de message suivant l'application g suivante :

$$\begin{array}{rccc} g: & \frac{\mathbb{Z}}{n\mathbb{Z}} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & \overline{X} & \mapsto & \overline{X^d} \end{array}$$

En utilisant que $d + \phi(n)\mathbb{Z}$ est le symétrique de $e + \phi(n)\mathbb{Z}$ pour la loi $\overline{\times}$ et le théorème d'Euler, démontrer que g décrypte bien le bloc M de message :

$$g\left(\overline{M^e}\right) = \overline{M}$$

3) *Application numérique*
⚠Si les nombres p, q et e ne sont pas bien choisis, par exemple si on choisit p et q trop petit, le cryptosystème n'est plus sécurisé.
Pour illustrer une telle faille, on considère par exemple le cas particulier suivant :

$$\begin{cases} n = 143 \\ e = 7 \\ M^e \equiv 46\,[143] \end{cases}$$

Le bloc M de message est donc cryté avec la valeur 46.
Décryter le valeur 46. Autrement dit, déterminer M.