Exercice 1.
Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}_{>0}$.

1) Rappeler la définition du plus grand diviseur commun de a et b et énoncer l'identité de Bézout.

2) Décrire l'algorithme d'Euclide (sans remontée) et démontrer qu'il permet de calculer le PGCD voulu.

3) Rappeler la définition de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

4) Démontrer que la classe de a modulo n est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

5) Résoudre les équations

$$(a)\ \ 8x \equiv 16 \pmod{57}, \qquad (b)\ \ 8x \equiv 16 \pmod{58},$$
$$(c)\ \ 8x \equiv 15 \pmod{58}.$$

Exercice 2.
On considère les deux propriétés suivantes pour $P \in \mathbb{R}[X]$:

$$(i)\ \ \forall x \in \mathbb{R},\ P(x) \geqslant 0, \qquad (ii)\ \ \exists A, B \in \mathbb{R}[X],\ P = A^2 + B^2.$$

1) En s'inspirant de l'égalité
$$|z|^2|w|^2 = |zw|^2,$$
montrer que si $P, Q \in \mathbb{R}[X]$ vérifient (ii) alors PQ aussi.

2) Montrer que les polynômes irréductibles, unitaires et de degré 2 de $\mathbb{R}[X]$ vérifient (ii).

3) Soit $P \in \mathbb{R}[X]\backslash\{0\}$ de décomposition en facteurs irréductibles
$$P = \lambda \prod_{i=1}^{n} (X - a_i)^{\alpha_i} \prod_{j=1}^{m} (X^2 + p_j X + q_j)^{\beta_j}.$$
On suppose que P vérifie la condition (i). Démontrer successivement que :
   (a) les entiers α_i sont tous pairs,
   (b) $\lambda > 0$,
   (c) P vérifie la condition (ii).

4) Établir finalement l'équivalence des conditions (i) et (ii).

Exercice 3.
Le déplacement d'un pendule simple est régit par l'équation différentielle
$$\theta'' + \frac{g}{\ell} \sin\theta = 0$$
où $\theta : \mathbb{R} \to \mathbb{R}$ est l'angle du pendule au cours du temps, g est la constante de pesanteur et ℓ est la longueur du pendule.

1) Faire un dessin représentant la situation de l'énoncé.

2) Pourquoi l'approximation $\sin\theta \approx \theta$ est-elle envisageable lorsque la position initiale du pendule est proche de l'équilibre ?

3) En déduire une formule approchée pour l'angle du pendule au cours du temps en supposant que le pendule est lâché au temps $t = 0$ à l'angle θ_0.

4) En déduire une approximation de la période du mouvement du pendule.

Exercice 4.
Soit $n \in \mathbb{N}_{>0}$ et soit $A \in M_n(\mathbb{R})$. On considère le système d'équations différentielles

$$X' = AX \tag{1}$$

où $X : \mathbb{R} \to \mathbb{R}^n$.
On suppose A diagonalisable.

1) Montrer que le système différentiel (1) est équivalent au système

$$Y' = DY \tag{2}$$

où $A = PDP^{-1}$ avec $P \in GL(n, \mathbb{R})$, $D \in M_n(\mathbb{R})$ diagonale et $Y = P^{-1}X$.

2) En déduire les solutions de (1).

3) Résoudre le système différentiel

$$\begin{cases} x' = 10x + 2y - 8z, \\ y' = -5x + 2y + 7z, \\ z' = 4x + 2y - 2z. \end{cases}$$

On considère maintenant l'équation différentielle linéaire homogène du second ordre à coefficients constants

$$y'' + by' + cy = 0. \tag{3}$$

4) En introduisant une deuxième équation $y' = z$, réécrire l'équation (3) sous la forme d'un système différentiel

$$X' = AX$$

avec $A \in M_2(\mathbb{R})$.

5) Calculer le polynôme caractéristique χ_A de A. Que reconnait-on ?

6) En déduire les solutions de l'équation différentielle (3) lorsque χ_A est scindé à racines simples sur $\mathbb{R}$.

7) Proposer une généralisation de ce résultat pour une équation différentielle linéaire homogène d'ordre $n \in \mathbb{N}_{>0}$ à coefficients constants.

Exercice 5.

1) Énoncer et démontrer le lemme de Gauss.

2) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$. Démontrer que si $\frac{\alpha}{\beta} \in \mathbb{Q}$ est sous-forme irréductible alors

$$\frac{\alpha}{\beta} \text{ est racine de } P \implies \alpha \mid a_0 \text{ et } \beta \mid a_n.$$

3) En déduire que si $p \in \mathbb{N}_{\geqslant 2}$ et si $n \in \mathbb{N}_{\geqslant 0}$ n'est pas la puissance p-ième d'un entier, $\sqrt[p]{n}$ est irrationnel.

4) Déterminer les racines rationnelles des polynômes

$$P = X^6 + X^3 + 1, \qquad Q = 4X^3 + 12X^2 + 8X + 28.$$

Exercice 6.
On considère $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

1) Donner la définition d'une racine de multiplicité $k \in \mathbb{N}_{\geqslant 0}$ pour un polynôme $P \in \mathbb{F}[X]$.

2) Soient $P \in \mathbb{F}[X]$, $x \in \mathbb{F}$ et $k \in \mathbb{N}_{>0}$. Rappeler le critère faisant intervenir les dérivées de P pour que x soit une racine de multiplicité au moins k de P puis le démontrer.

3) (a) Déterminer les triplets $(a, b, c) \in \mathbb{R}^3$ tels que $X^5 + aX^2 + bX + c$ soit divisible par $(X-1)^3$ puis le factoriser en irréductibles sur $\mathbb{R}$ pour chacun des triplets trouvés.

(b) Si $a, b, c \in \mathbb{R}$, on considère le polynôme

$$P(X) = X^6 - 5X^4 + aX^2 + bX + c \in \mathbb{R}[X].$$

Déterminer les triplets (a, b, c) tels que P admette une racine d'ordre au moins 4 dans $\mathbb{R}$.

4) Démontrer que pour tout $n \in \mathbb{N}_{\geqslant 0}$, le polynôme

$$P = \sum_{k=0}^{n} \frac{1}{k!} X^k \in \mathbb{C}[X]$$

est à racines simples.

5) (a) Montrer à l'aide du lemme de Rolle que si $P \in \mathbb{R}[X]$ est de degré $n \geqslant 2$ et scindé à racines simples alors P' est aussi scindé à racines simples.

(b) En déduire que si $P = \sum_k a_k X^k \in \mathbb{R}[X]$ est de degré au moins 2 et scindé à racines simples, il n'existe pas d'entier $k \in \{0, \ldots, \deg P - 2\}$ tel que

$$a_k = a_{k+1} = 0.$$

Exercice 7.
On considère la fonction indicatrice d'Euler

$$\varphi : \begin{array}{ccc} \mathbb{N}_{>0} & \to & \mathbb{N}_{>0} \\ n & \mapsto & \mathrm{card}\{k \in \mathbb{N}_{>0} \mid k \leqslant n \text{ et } k \wedge n = 1\} \end{array}.$$

1) (a) Énoncer le théorème des restes chinois.

(b) Justifier l'égalité

$$\forall n \in \mathbb{N}_{>0}, \quad \varphi(n) = \mathrm{card}\, \mathbb{Z}/n\mathbb{Z}^{\times}.$$

(c) En déduire que si $n, m \in \mathbb{N}_{>0}$ sont premiers entre eux alors

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(d) Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}_{>0}$. Calculer $\varphi(p^{\alpha})$.

(e) En déduire une formule pour $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n.

2) On fixe $n \in \mathbb{N}_{>0}$.

(a) Démontrer que si $k \in \mathbb{N}_{\geqslant 0}$, l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$\mathrm{ord}(\overline{k}) = \frac{n}{n \wedge k}.$$

(b) En déduire que pour tout diviseur d de n, il y a $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.

(c) En partitionnant $\mathbb{Z}/n\mathbb{Z}$ suivant l'ordre de ses éléments, en déduire la formule

$$n = \sum_{d|n} \varphi(d).$$

Exercice 8.
Soit $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. On dit qu'une famille $(P_1, \ldots, P_s) \in \mathbb{F}[X]^s$ est échelonnée en degré si

$$n < m \implies \deg P_n \leqslant \deg P_m.$$

1) Démontrer qu'une famille échelonnée en degré de $\mathbb{F}[X]$ est libre dans le $\mathbb{F}$-espace vectoriel $\mathbb{F}[X]$.

2) (a) En déduire que pour tout $a \in \mathbb{F}$, et tout polynôme $P \in \mathbb{F}[X]$, il existe d'uniques scalaires $\lambda_0, \ldots, \lambda_{\deg P} \in \mathbb{F}$ vérifiant

$$P = \sum_{k=0}^{\deg P} \lambda_k (X - a)^k.$$

(b) Démontrer que pour tout $k \in \{0, \ldots, \deg P\}$, on a

$$\lambda_k = \frac{1}{k!} P^{(k)}(a).$$

3) Soit $n \in \mathbb{N}_{>0}$. On considère la dérivation discrète

$$\Delta : \begin{array}{ccc} \mathbb{F}[X] & \to & \mathbb{F}[X] \\ P & \mapsto & P(X+1) - P(X) \end{array}.$$

(a) Justifier que Δ induit un endomorphisme de $\mathbb{F}_n[X]$.

(b) Montrer que la famille $(H_0, \dots, H_n)$ définie par

$$\begin{cases} H_0 = 1 \\ H_k = \frac{X(X-1)\cdots(X-k+1)}{k!} \text{ si } k \geqslant 1 \end{cases}$$

est une base de $\mathbb{F}_n[X]$ puis calculer la matrice de $\Delta_{|\mathbb{F}_n[X]}$ dans cette base.

(c) Sans faire plus de calculs, diriez-vous que $\Delta_{|\mathbb{F}_n[X]}$ est diagonalisable ?

(d) Montrer que pour tout $P \in \mathbb{F}[X]$, il existe $k \in \mathbb{N}_{\geqslant 0}$ vérifiant $\Delta^k(P) = 0$ mais que pourtant, Δ n'est pourtant pas nilpotent.

Exercice 9.
On considère $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

1) Énoncer puis démontrer le théorème de la division euclidienne dans $\mathbb{F}[X]$. La preuve de l'existence devra fournie par un algorithme.

2) Soit E un $\mathbb{F}$-espace vectoriel de dimension finie $n \in \mathbb{N}_{\geqslant 0}$ et soit $u \in L(E)$.

(a) Justifier que la famille $(\mathrm{id}_E, u, u^2, \dots)$ de $L(E)$ est liée.

(b) En déduire que u admet un polynôme annulateur non nul et donner une borne supérieure sur son degré.

(c) On considère μ_u un polynôme unitaire annulateur de degré minimal de u. Montrer que si P est un polynôme annulateur de u alors $\mu_u \mid P$.

(d) En déduire que μ_u est l'unique polynôme unitaire annulateur de degré minimal de u.

(e) Déterminer le polynôme minimal de l'endomorphisme de $\mathbb{R}^4$ donné par

$$u(e_1) = e_1,\ u(e_2) = e_2,\ u(e_3) = 2e_3,\ u(e_4) = 4e_4.$$

Exercice 10.

1) Donner trois définitions équivalentes de la relation de congruence $a \equiv b \pmod{n}$.

2) Démontrer ou réfuter les implications suivantes

(a) $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$,

(b) $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n} \implies a^c \equiv b^d \pmod{n}$,

(c) $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$,

(d) $ab \equiv ac \pmod{n} \implies b \equiv c \pmod{n}$,

(e) $ab \equiv ac \pmod{an} \implies b \equiv c \pmod{n}$.

3) Soient $a, b, c \in \mathbb{Z}$. On considère l'équation

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

d'inconnues $x, y \in \mathbb{Z}$ où $a, b, c \in \mathbb{Z}$ sont donnés.

(a) Démontrer que si l'équation (E) admet une solution alors $a \wedge b \mid c$.

(b) On suppose à partie de maintenant que $a \wedge b \mid c$. En déduire que l'équation (E) est équivalente à l'équation

$$a'x + b'y = c' \tag{E'}$$

où

$$a' = \frac{a}{a \wedge b}, \qquad b' = \frac{b}{a \wedge b}n \qquad c' = \frac{c}{a \wedge b}.$$

(c) Démontrer à l'aide de l'identité de Bézout que l'équation (E') admet une solution (x_0, y_0).

(d) Soit (x, y) une autre solution de (E'), montrer que $a' \mid y - y_0$ et $b' \mid x - x_0$.

(e) En déduire que l'ensemble des solutions de (E') est

$$\{(x_0 + b'k, y_0 - a'k \mid k \in \mathbb{Z}\}.$$

(f) Résoudre les équations diophantiennes

$$4x + 6y = 11, \tag{E_1}$$

$$5x + 2y = 1. \tag{E_2}$$

Exercice 11.
On considère $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ et E un $\mathbb{F}$-espace vectoriel.

1) (a) Énoncer le lemme des noyaux.

(b) Expliquer comment en déduire que si un endomorphisme de E admet un polynôme annulateur scindé à racines simples sur $\mathbb{F}$ alors il est diagonalisable.

(c) Montrer que si $p \in L(E)$ vérifie $p^2 = p$ alors p est la projection sur $\ker(p - \mathrm{id}_E)$ parallèlement à $\ker p$ et que si $s \in L(E)$ vérifie $s^2 = \mathrm{id}_E$ alors s est la symétrie d'axe $\ker(s - \mathrm{id}_E)$ le long de $\ker(s + \mathrm{id}_E)$.

2) On considère le $\mathbb{R}$-espace vectoriel $C^\infty(\mathbb{R})$ des fonctions lisses de $\mathbb{R}$ dans $\mathbb{R}$ et définit l'endomorphisme

$$D : \begin{array}{ccc} C^\infty(\mathbb{R}) & \to & C^\infty(\mathbb{R}) \\ f & \mapsto & f' \end{array}.$$

On souhaite déterminer l'ensemble $\mathcal{S}$ des solutions de l'équation différentielle

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0 \tag{1}$$

d'inconnue $y \in C^n(\mathbb{R})$ où $a_0, \ldots, a_{n-1} \in \mathbb{R}$, $a_n \in \mathbb{R}\backslash\{0\}$.

(a) Montrer que $\mathcal{S} \subset C^\infty(\mathbb{R})$ puis constater que $\mathcal{S} = \ker P(D)$ où

$$P \coloneqq \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X].$$

(b) On suppose à partir de maintenant que P est scindé sur $\mathbb{R}$ et on pose

$$P = \prod_{k=1}^{s} (X - \lambda_k)^{n_k}$$

sa décomposition en facteurs irréductibles. Montrer que

$$\mathcal{S} = \bigoplus_{k=1}^{s} \ker\Big((D - \lambda_k \mathrm{id}_E)^{n_k}\Big).$$

(c) Soient $\lambda \in \mathbb{R}$ et $k \in \mathbb{N}_{>0}$. En remarquant que

$$D(ye^{-\lambda t}) = e^{-\lambda t}(D - \lambda)(y),$$

montrer via une récurrence que

$$(D - \lambda)^k y = 0 \iff D^k(ye^{-\lambda t}) = 0$$

puis en déduire $\mathcal{S}$.

(d) Résoudre l'équation différentielle

$$y^{(5)} - 4y^{(4)} - 6y^{(3)} + 32y^{(2)} - 35y' + 12y = 0.$$

Exercice 12.

1) Rappeler la définition d'un nombre premier.

2) Écrire un algorithme (sous la forme d'une suite d'instructions) permettant de déterminer tous les nombres premiers inférieurs à une borne choisie par l'utilisateur. Justifier qu'il accomplit bien cette tâche.

3) On se propose de démontrer de plusieurs manières différentes l'existence d'une infinité de nombres premiers.

(a) Montrer que si $p_1, \ldots, p_n$ sont des nombres premiers distincts alors $p_1 \cdots p_n + 1$ admet un diviseur premier différent de $p_1, \ldots, p_n$. En déduire que $\mathbb{P}$ est infini.

(b) On admet que la série

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

est divergente. En déduire que $\mathbb{P}$ est infini.

(c) Si $n \in \mathbb{N}_{\geqslant 0}$, on pose $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Montrer que pour tout $n \in \mathbb{N}_{>0}$, on a

$$F_0 \cdots F_{n-1} = F_n - 2.$$

En déduire que $F_n \wedge F_0 \cdots F_{n-1} = 1$ et puis que $\mathbb{P}$ est infini.

(d) Montrer que si $p_1, \ldots, p_n$ sont des nombres premiers distincts tous congrus à 3 modulo 4 alors

$$4p_1 \cdots p_n - 1$$

admet un diviseur premier congru à 3 modulo 4 différent de $p_1, \ldots, p_n$. En déduire que $\mathbb{P} \cap (3 + 4\mathbb{Z})$ est infini.

(e) On admet que si -1 est un carré modulo $p \in \mathbb{P}$ alors $p \equiv 1 \pmod 4$. Montrer que si $p_1, \ldots, p_n$ sont des nombres premiers distincts tous congrus à 1 modulo 4 alors

$$4(p_1 \cdots p_n)^2 + 1$$

admet un diviseur premier congru à 1 modulo 4 différent de $p_1, \ldots, p_n$. En déduire que $\mathbb{P} \cap (1 + 4\mathbb{Z})$ est infini.

Exercice 13.

1) Donner la définition des suites adjacentes puis le théorème fondamental les concernant.

2) Le but de cette question est de démontrer le théorème des valeurs intermédiaires avec la méthode dite de la dichotomie.

On considère une fonction $f : [a, b] \to \mathbb{R}$ continue et vérifiant $f(a) < 0$, $f(b) \geqslant 0$. On considère les suites $(a_n)_n$ et $(b_n)_n$ construites de la manière suivante :

- $a_0 = a$ et $b_0 = b$,
- si a_n et b_n sont construits, on pose

$$\begin{cases} a_{n+1} = \frac{a_n + b_n}{2}, b_{n+1} = b_n \text{ si } f\left(\frac{a_n+b_n}{2}\right) < 0, \\ a_{n+1} = a_n, b_{n+1} = \frac{a_n+b_n}{2} \text{ si } f\left(\frac{a_n+b_n}{2}\right) \geqslant 0. \end{cases}$$

(a) Démontrer que les suites $(a_n)_n$ et $(b_n)_n$ sont adjacentes et convergent vers un réel $c \in [a, b]$.

(b) Montrer que $f(c) = 0$.

(c) Écrire un algorithme de dichotomie en se basant sur la preuve précédente. Il permettra d'obtenir une valeur approchée à ϵ près d'un zéro de f.

3) Le but de cette question est de démontrer que e est un nombre irrationnel. On considère pour cela les suites $(u_n)_n$ et $(v_n)_n$ définies par

$$u_n = \sum_{k=0}^{n} \frac{1}{k!}, \qquad v_n = u_n + \frac{1}{nn!}.$$

(a) Montrer que les suites $(u_n)_n$ et $(v_n)_n$ sont adjacentes et convergent vers e.

(b) En déduire que pour tout $n \in \mathbb{N}_{>0}$, on a

$$n!\, u_n < n!\, e \leqslant n!\, u_n + \frac{1}{n}.$$

(c) En déduire via un raisonnement par l'absurde que e est irrationnel.

Exercice 14.

1) Montrer que l'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre 1 sur $\mathbb{R}$ est un espace vectoriel.

2) Énoncer le théorème de Cauchy-Lipschitz.

3) Rappeler et démontrer sa conséquence sur la structure de l'espace des solutions d'une équation différentielle linéaire homogène d'ordre 1 sur $\mathbb{R}$ lorsque le coefficient devant y' ne s'annule jamais.

4) Démontrer via la méthode dite de la variation de la constante que si $p, f : \mathbb{R} \to \mathbb{R}$ sont continues alors les solutions de l'équation différentielle

$$y' + py = f$$

sont exactement les fonctions de la forme

$$t \mapsto \alpha e^{-\int_0^t p(x)\mathrm{d}x} + \int_0^t f(u) e^{\int_t^u p(x)\mathrm{d}x} \mathrm{d}u$$

avec $\alpha \in \mathbb{R}$.

5) Déterminer les fonctions développables en série entière autour de 0 qui sont solutions du problème de Cauchy

$$\begin{cases} y''(t) + ty'(t) + y(t) = 1, \\ y(0) = 0, \\ y'(0) = 0. \end{cases}$$

On pensera à préciser le rayon de convergence du développement en série entière de la solution.

6) (a) Résoudre l'équation différentielle

$$ty'(t) = 2y(t) \qquad (E)$$

sur $\mathbb{R}_+^*$ puis sur $\mathbb{R}_-^*$.

(b) Montrer que si y_+ est une solution de (E) sur $\mathbb{R}_+^*$ et y_- est une solution de (E) sur $\mathbb{R}_-^*$ alors

$$y : t \mapsto \begin{cases} y_+(t) \text{ si } t > 0 \\ 0 \text{ si } t = 0 \\ y_-(t) \text{ si } t < 0 \end{cases}$$

est une solution de (E) sur $\mathbb{R}$.

(c) En déduire que l'espace des solutions de (E) sur $\mathbb{R}$ est de dimension 2.

(d) Pourquoi le résultat de la question 6) (c) est-il étonnant ? Comment l'expliquez vous ?

Exercice 15. Soit $f : [a, b] \to \mathbb{R}$ une fonction de classe C^2 sur $[a, b]$ vérifiant $f(a) < 0$, $f(b) > 0$, $f' > 0$ et $f'' > 0$.

1) Démontrer qu'il existe un unique $\gamma \in]a, b[$ tel que $f(\gamma) = 0$.

2) On pose $x_0 = b$. Déterminer l'abscisse x_1 du point d'intersection de la tangente à la courbe représentative de f au point d'abscisse x_0 avec l'axe des abscisses. Justifier que $x_1 \in [\gamma, b]$.

3) On réitère le procédé et on construit ainsi une suite (x_n) vérifiant la relation de récurrence $x_{n+1} = \varphi(x_n)$ avec $\varphi(x) = x - \frac{f(x)}{f'(x)}$. Démontrer que la suite (x_n) converge vers γ.

4) On souhaite estimer la vitesse de convergence de (x_n) vers γ.

(a) Justifier que, pour tout $x \in [a, b]$, on a

$$|f(\gamma) - f(x) - f'(x)(\gamma - x)| \leqslant \frac{|x - \gamma|^2}{2} \max_{y \in [a,b]} |f''(y)|.$$

(b) En déduire que pour tout $n \in \mathbb{N}_{\geqslant 0}$, on a

$$|x_{n+1} - \gamma| \leqslant k|x_n - \gamma|^2$$

avec $k = \dfrac{1}{2} \dfrac{\max_{y \in [a,b]} |f''(y)|}{\max_{y \in [a,b]} |f'(y)|}$.

5) Démontrer que, pour tout $n \geqslant 0$, on a $k|x_n - \gamma| \leqslant (k|x_0 - \gamma|)^{2^n}$.

6) Montrer que la fonction f définie par $f(x) = x^2 - 3$ vérifie les conditions d'application des résultats précédents avec $a = 1,7$, $b = 1,8$. En déduire une méthode pour calculer une valeur approchée de $\sqrt{3}$ à 10^{-20} près et donner une borne supérieure pour le nombre d'étapes nécessaires. Qu'en pensez-vous ?

Exercice 16. 1) On fixe trois entiers $a, b, c \in \mathbb{Z}$ premiers entre eux deux-à-deux.

(a) Justifier l'existence de $u_1, v_1, u_2, v_2, u_3, v_3 \in \mathbb{Z}$ tels que

$$au_1 + bcv_1 = 1, \quad bu_2 + acv_2 = 1, \quad cu_3 + abv_3 = 1.$$

(b) On pose

$$\Phi : \begin{array}{ccc} \mathbb{Z}/abc\mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z} \\ \overline{x} & \mapsto & (\overline{x}, \overline{x}, \overline{x}) \end{array},$$

$$\Psi : \begin{array}{ccc} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z} & \to & \mathbb{Z}/abc\mathbb{Z} \\ (\overline{x}, \overline{y}, \overline{z}) & \mapsto & \overline{xbcv_1 + yavc_2 + zabv_3} \end{array}.$$

Montrer que Φ et Ψ sont bien définies et sont les réciproques l'une de l'autre. En déduire l'isomorphisme de groupes

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z} \simeq \mathbb{Z}/abc\mathbb{Z}.$$

2) (a) Soit $n \in \mathbb{Z}$. Rappeler, étant donné un diviseur d de n, le nombre de sous-groupes d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ et les donner explicitement.

(b) Soient $a, b, c \in \mathbb{Z}$ tels que

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z} \simeq \mathbb{Z}/abc\mathbb{Z}.$$

Montrer que a, b, c sont premiers entre eux deux-à-deux.
Indication : Si p est un diviseur premier commun de deux des entiers a, b, c, on pourra montrer que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$ admet deux sous-groupes d'ordre p.

3) Un texte de Sun Zi datant du quatrième siècle propose le problème suivant :

Soient des objets en nombre inconnu. Si on les compte par 3, il en reste 2 ; par 5, il en reste 3 ; par 7, il en reste 2. Combien y a-t-il d'objets ?
Réponse : 23.
Règle
En comptant par 3, il en reste 2 : pose 140.
En comptant par 5, il en reste 3 : pose 63.
En comptant par 7, il en reste 2 : pose 30.
Faire la somme de ces trois nombres : 233, soustraire 210, d'où la réponse.
En général, pour chaque unité restante d'un décompte par 3*, poser* 70*; pour chaque unité restante d'un décompte par* 5*, poser* 21*; pour chaque unité restante d'un décompte par* 7*, poser* 15*. Si la somme vaut* 106 *ou plus, soustraire* 105 *pour trouver la réponse.*

Justifier que la méthode proposée par Sun Zi fonctionne bien.