# Exercices

**Exercice 1.** Soit $A$ un anneau commutatif et $M$ une partie de $A$. On apelle annulateur de $M$ l'ensemble des éléments $a \in A$ tels que $am = 0_A$ pour tout $m \in M$.
Montrer que l'annulateur de $M$ est un idéal de $A$.

**Exercice 2.** Soit $A$ un anneau commutatif et $D$ l'ensemble des diviseurs de zéro dans $A$. Montrer que pour tout $(a, b) \in A^2$ :

1. $ab \in D \Rightarrow \big(a \in D \text{ ou } b \in D\big)$ ;
2. $\big(a \in D \text{ ou } b \in D\big) \Rightarrow ab \in D \cup \{0\}$.

**Exercice 3.** Soit $A$ un anneau, un élément $x$ de $A$ est dit nilpotent lorsqu'il existe un entier naturel $n$ tel que $x^n = 0_A$.

1. Soit $x, y \in A$, montrer que si $xy$ est nilpotent, alors $yx$ est nilpotent.
2. Soit $x \in A$, montrer que si $x$ est nilpotent, alors $1_A - x$ est inversible.
3. On suppose que $A$ est commutatif, montrer que l'ensemble des éléments nilpotents de $A$ est un idéal de $A$.

**Exercice 4.** Soit $G$ le groupe des inversibles de $\mathbb{Z}/32\mathbb{Z}$.

1. Quel est le cardinal de $G$ ?
2. Quels sont les ordres de $\bar{5}$ et $\overline{15}$ dans $G$ ?
3. Montrer que :
$$\begin{array}{rccc} f & : & (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +) & \longrightarrow & (G, \times) \\ & & \bar{a}, \bar{b} & \longmapsto & \bar{5}^a \overline{15}^b \end{array}$$
est un isomorphisme de groupes.

**Exercice 5.** Montrer que si un nombre qui s'écrit $abcdef$ en base 10 est divisible par 13, alors le nombre qui s'écrit $bcdefa$ en base 10 l'est aussi.
Pourquoi peut-on affirmer immédiatement que 691 691 est divisible par 13 ?

**Exercice 6.**

1. Soit $p$ un nombre premier supérieur à 5. Montrer que $24 \mid p^2 - 1$.
2. Soit $n \in \mathbb{N}^*$, montrer que $42 \mid n^{13} - n$.

**Exercice 7.** Montrer que $\overline{47}$ est inversible dans $\mathbb{Z}/2011\mathbb{Z}$ et déterminer son inverse.

**Exercice 8.** Soit $\varphi$ la fonction indicatrice d'Euler. Montrer que : $\forall n \in \mathbb{N}^*, \sum_{d|n} \varphi(d) = n$.

Indication : considérer pour chacune des $n$ fractions $\frac{k}{n}$ avec $k \in [\![1\,;n]\!]$ leur écriture irréductible $\frac{a}{d}$.

**Exercice 9.** Soit $p$ un nombre premier impair.

1. Montrer que : $\binom{2p}{p} = \sum_{k=0}^{2p} \binom{p}{k}^2$.
2. En déduire que : $\binom{2p}{p} \equiv 2\ [p^2]$.

**Exercice 10.** Anneau $\mathbb{Z}[\sqrt{2}]$.

1. Montrer que
$$A = \left\{a + b\sqrt{2};\ \text{avec } a, b \in \mathbb{Z}\right\}$$
est le plus petit sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z} \cup \left\{\sqrt{2}\right\}$.
On note $U$ le groupe des inversibles de $A$.
2. Montrer que : $\forall x \in \mathbb{Z}[\sqrt{2}], \exists!(a, b) \in \mathbb{Z}^2 \mid x = a + b\sqrt{2}$ et en déduire $N : a + b\sqrt{2}) = \left|a^2 - 2b^2\right|$ est bien définie de $A$ dans $\mathbb{N}$.
3. Montrer que $N$ est multiplicative, c'est à dire
$$\forall (x, y) \in A^2, N(xy) = N(x)N(y);$$
en déduire qu'un élément $z \in A$ est inversible si et seulement si $N(z) = 1$.
4. Montrer que $1 + \sqrt{2} \in U$, puis : $\forall n \in \mathbb{Z}, (1 + \sqrt{2})^n \in U$.
5. Soit $z = a + b\sqrt{2} \in U$ avec $a, b \in \mathbb{N}$.
   (a) Montrer que $a \neq 0$.
   (b) Montrer qu'il existe un unique $n \in \mathbb{N}$ tel que : $(1 + \sqrt{2})^n \leqslant z < (1 + \sqrt{2})^{n+1}$
   (c) Montrer qu'il existe $a', b' \in \mathbb{N}$ tels que $z(1 + \sqrt{2})^{-n} = a' + b'\sqrt{2}$.
   (d) Montrer que $z = (1 + \sqrt{2})^n$.
6. Montrer que $U = \left\{\pm(1 + \sqrt{2})^n;\ \text{avec } n \in \mathbb{Z}\right\}$.

**Exercice 11.** Soit $A$ un anneau commutatif et $I$ un idéal de $A$. On appelle radical de $I$ :
$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}, x^n \in I\}\,.$$
1. Soit $x \in \sqrt{I}$ et $n \in \mathbb{N}$ tels que $x^n \in I$, montrer que : $\forall m \geqslant n, x^m \in I$.
2. Montrer que $\sqrt{I}$ est un idéal de $A$.
3. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.
4. Soit $J$ un idéal de $A$, montrer :
$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} \text{ et } \sqrt{I} + \sqrt{J} \subset \sqrt{I + J}.$$
5. Dans $\mathbb{Z}$, déterminer $\sqrt{3648\mathbb{Z}}$.

**Exercice 12.** Théorème de Wilson.
Soit $p \in \mathbb{N}^*$.

1. On suppose dans cette question que $p$ est premier.
   (a) Résoudre l'équation $a = a^{-1}$ dans $F_p$.
   (b) En déduire la valeur du produit $\prod_{a \in \mathbb{F}_p^*} a$.
2. Montrer que $p$ est premier si et seulement si $(p-1)! \equiv -1\ [p]$.
3. Application : Montrer que si $p$ est un nombre premier de la forme $4n+1$ avec $n \in \mathbb{N}$, alors $\bar{-1}$ admet une racine carrée dans $F_p$.

**Exercice 13. Chiffrement RSA (Rivest, Shamir, Adleman)**
Soit $p$ et $q$ deux nombres premiers distincts. On pose $n = pq$.

1. Déterminer $\varphi(n)$, l'indicatrice d'Euler de $n$.
2. Montrer que pour tout $x \in \mathbb{Z}$ et tout $q \in \mathbb{N}$, $x^{q\varphi(n)+1} \equiv x\ [n]$.
3. Soit $k$ un entier naturel premier avec $\varphi(n)$. Montrer qu'il existe $m \in \mathbb{N}$ tel que $km \equiv 1\ [\varphi(n)]$. En déduire que $x^{km} \equiv x\ [n]$.
4. Le chiffrement RSA utilise deux clés : une clé publique $k$ pour chiffrer et une clé privée $m$ pour déchiffrer des données. Les deux clés sont crées par Alice qui souhaite recevoir des données confidentielles. Alice rend la clé publique accessible et conserve la clé privée. Si $x$ est un entier strictement inférieur à $n$, le message chiffré est la classe de $x^k$ modulo $n$.
   (a) Comment Alice peut-elle déchiffrer le message ?
   (b) Exemple : pour $p = 3, q = 11, k = 3$, quelle est la clé $m$ ? La clé publique est $(n, k) = (33, 3)$ et la clé privée est $(33, m)$. Bob veut envoyer le message $M = 4$ à Alice, quelle est le code ? Décoder.
   (c) Sur quoi repose la sécurité du système ?

**Exercice 14.**

1. Résoudre pour $x \in \mathbb{Z}/5\mathbb{Z}$ :
$$\bar{3}x + \bar{2} = -\bar{1}.$$
2. Résoudre pour $x \in \mathbb{Z}$ :
$$\begin{cases} 3x + 2 \equiv -1\ [5] \\ 3x - 1 \equiv 3\ [7] \end{cases}$$
3. Résoudre pour $x \in \mathbb{Z}$ :
$$\begin{cases} 5x \equiv 8\ [12] \\ 2x \equiv 17\ [21] \end{cases}$$
4. Résoudre pour $x, y \in \mathbb{Z}$ :
$$\begin{cases} 5x + 2y \equiv 3\ [6] \\ 2x + 4y \equiv 1\ [5] \end{cases}$$

**Exercice 15.** Soit $K$ un sous-corps de $\mathbb{C}$ et $\mathbb{K} \in \mathbb{K}[X]$.

1. Soit $A, B \in \mathbb{K}[X]$, montrer que les PGCD de $A$ et de $B$ calculés dans $\mathbb{C}[X]$ ou dans $\mathbb{K}[X]$ sont égaux.
2. Montrer que $P$ et $P'$ sont premiers entre eux si et seulement si $P$ n'a que des racines simples dans $\mathbb{C}$.
3. Calculer le PGCD de $P$ et de $P'$ dans $\mathbb{K}[X]$.

# Banque CCINP

**Exercice 16 (CCINP 86).**

1. Soit $(a, b, p) \in \mathbb{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
2. Soit $p$ un nombre premier.
   (a) Prouver que $\forall k \in [\![1, p-1]\!]$, $p$ divise $\binom{p}{k} k!$ puis en déduire que $p$ divise $\binom{p}{k}$.
   (b) Prouver que : $\forall n \in \mathbb{N},\ n^p \equiv n\ [p]$.
   **Indication** : procéder par récurrence.
   (c) En déduire, pour tout entier naturel $n$, que : $p$ne divise pas $n \Longrightarrow n^{p-1} \equiv 1\ [p]$.

**Exercice 17 (CCINP 94).**

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit $a$ et $b$ deux entiers naturels premiers entre eux.
   Soit $c \in \mathbb{N}$.
   Prouver que : $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.
3. On considère le système $(S)$ : $\begin{cases} x \equiv 6\ [17] \\ x \equiv 4\ [15] \end{cases}$ dans lequel l'inconnue $x$ appartient à $\mathbb{Z}$.
   (a) Déterminer une solution particulière $x_0$ de $(S)$ dans $\mathbb{Z}$.
   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système $(S)$.