Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Exercice 1 : Soit $n \in \mathbb{N}^*$. On note $A = \mathbb{Z}/n\mathbb{Z}$.

1. Montrer que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les idéaux dA où d est un diviseur de n.
2. Si d est un diviseur de n, déterminer l'anneau A/dA.
3. Déterminer les idéaux maximaux et les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2 : Soit $n \in \mathbb{N}^*$.

1. Montrer que l'ensemble I des éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ est un idéal principal, puis donner un générateur de cet idéal.
2. Combien d'éléments nilpotents admet l'anneau $\mathbb{Z}/n\mathbb{Z}$?

Exercice 3 : Déterminer les éléments nilpotents de l'anneau $\mathbb{Z}/360\mathbb{Z}$.

Exercice 4 : Quel est le nombre d'idempotents de l'anneau $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$?

Exercice 5 : Déterminer les éléments idempotents de l'anneau $\mathbb{Z}/187\mathbb{Z}$.

Exercice 6 : Soit $n \in \mathbb{N}^*$. On note $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ le groupe des automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$

1. Montrer que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.
2. Déterminer le groupe des automorphismes d'anneaux de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 7 : Soit $(m, n) \in (\mathbb{N}^*)^2$.

1. Combien existe-t-il de morphismes de groupes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?
2. Combien existe-t-il de morphismes d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice 8 : Soit $n \in \mathbb{N}$ avec $n \geqslant 2$. Montrer que les conditions suivantes sont équivalentes.

(i) L'entier n est un nombre premier.
(ii) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.
(iii) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Exercice 9 :

1. Combien d'éléments inversibles y a-t-il dans $\mathbb{Z}/180\mathbb{Z}$?
2. Déterminer l'inverse de 89 dans $\mathbb{Z}/180\mathbb{Z}$.

Exercice 10 : Déterminer les entiers $n \in \mathbb{N}^*$ tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Exercice 11 : Montrer que le groupe $(\mathbb{Z}/54\mathbb{Z})^\times$ est cyclique et déterminer le nombre de générateurs qu'il admet.

Exercice 12 : Déterminer le reste dans la division euclidienne de 44^{1999} par 25.

Exercice 13 : Déterminer les deux derniers chiffres de 3^{2004}.

Exercice 14 : Soit $(m, n) \in (\mathbb{N}^*)^2$ avec $m \wedge n = 1$. On peut écrire $n = 2^{k_1} \cdot 5^{k_2} \cdot p$ avec $(k_1, k_2, p) \in \mathbb{N}^3$ tel que les entiers 10 et p soient premier entre eux.

1. Montrer que la période de m/n est l'ordre de 10 dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$.
2. En déduire que la période de m/n divise $\varphi(n)$.

Exercice 15 (Cryptage RSA) **:** Soit $(n, e) \in (\mathbb{N}^*)^2$ où n est un entier sans facteur carré. Montrer que l'application

$$\alpha_e : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto x^e.$$

est bijective si et seulement si $e \wedge \varphi(n) = 1$.

Exercice 16 : Montrer que $\varphi(n)$ est pair pour tout $n \in \mathbb{N}$ avec $n \geqslant 3$.

Exercice 17 : Montrer que pour tout $n \in \mathbb{N}$ avec $n \geqslant 2$, on a

$$\varphi(n) \geqslant \frac{n \ln 2}{\ln n + \ln 2}.$$

Exercice 18 : Montrer que l'on a

$$\liminf_{n\in\mathbb{N}} \frac{\varphi(n)}{n} = 0 \quad \text{et} \quad \limsup_{n\in\mathbb{N}} \frac{\varphi(n)}{n} = 1.$$

Exercice 19 : Soit $(S, B) \in \mathscr{M}_n(\mathbb{R})^2$ définie par

$$\forall (i,j) \in [\![1,n]\!]^2, \quad s_{ij} = i \wedge j \quad \text{et} \quad b_{ij} = \begin{cases} 1 & \text{si} \quad i \mid j \\ 0 & \text{sinon.} \end{cases}$$

1. Calculer la matrice $B^{\mathrm{T}}DB$ où $D = \mathrm{Diag}(\varphi(1), \ldots, \varphi(n)) \in \mathscr{M}_n(\mathbb{R})$.
2. En déduire le déterminant de la matrice S.

Exercice 20 : Soit $n \in \mathbb{N}$ que l'on écrit $n = 10q + r$ avec $q \in \mathbb{N}$ et $r \in [\![0, 9]\!]$.

1. Montrer que $7 \mid n$ si et seulement si $7 \mid q - 2r$.
2. Est ce que $7 \mid 11228$? Est ce que $7 \mid 15637$?

Exercice 21 : Montrer que 11 divise $2^{123} + 3^{121}$.

Exercice 22 : Montrer pour tout $n \in \mathbb{N}$ que

(i) $6 \mid 5n^3 + n$, (ii) $7 \mid 3^{2n+1} + 2^{n+2}$, (iii) $11 \mid 3^{8n} \times 5^4 + 5^{6n} \times 7^3$,
(iv) $5 \mid 2^{2n+1} + 3^{2n+1}$, (v) $9 \mid 4^n - 1 - 3n$, (vi) $15^2 \mid 16^n - 1 - 15n$.

Exercice 23 : Montrer que pour tout entier $n \geqslant 2$, on a $10 \mid 2^{2^n} - 6$.

Exercice 24 : Montrer pour tout $n \in \mathbb{N}$ que la plus grande puissance de 2 divisant $5^{2^n} - 1$ est 2^{n+2}.

Exercice 25 : Soient $(a, b) \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$. Montrer que

$$a \equiv b \ [n] \quad \Rightarrow \quad a^n \equiv b^n \ [n^2].$$

Exercice 26 : Soit $(x, y) \in \mathbb{N}^2$. Montrer l'équivalence

$$7 \mid x \quad \text{et} \quad 7 \mid y \quad \Leftrightarrow \quad 7 \mid x^2 + y^2.$$

Exercice 27 : On souhaite résoudre $x^2 + y^2 + z^2 = x^2y^2$ pour $(x, y, z) \in \mathbb{Z}^3$.

1. Montrer que si (x, y, z) est solution, alors x, y et z sont pairs.
2. En déduire les solutions de l'équation.

Exercice 28 : On souhaite résoudre $5x^3 + 11y^3 = 13z^3$ pour $(x, y, z) \in \mathbb{Z}^3$.

1. Montrer que si (x, y, z) est solution, alors 13 divise x, y et z.
2. En déduire les solutions de l'équation.

Exercice 29 : Résoudre les systèmes d'inconnue $(x, y) \in \mathbb{Z}^2$ ci-dessous.

$$(i) \begin{cases} 4x + 9y \equiv 4 \ [48] \\ 3x + 8y \equiv 7 \ [48] \end{cases} \qquad (ii) \begin{cases} 4x - 11y \equiv 3 \ [48] \\ 3x + 8y \equiv 4 \ [48] \end{cases}$$

Exercice 30 : Soit $(m, n) \in (\mathbb{N}^*)^2$. Montrer que $m \wedge n = 1$ si et seulement si on a un isomorphisme de groupes

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Exercice 31 : Résoudre les systèmes d'inconnue $x \in \mathbb{Z}$ ci-dessous.

$$(i)\ \begin{cases} x \equiv 5 \ [12] \\ x \equiv 7 \ [11] \end{cases} \qquad (ii)\ \begin{cases} x \equiv 2 \ [56] \\ x \equiv 1 \ [45] \end{cases}$$

Exercice 32 : Soit $(m,n) \in (\mathbb{N}^*)^2$. On définit l'application

$$\alpha : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto (\bar{x}, \bar{x}).$$

1. Montrer que α est un morphisme d'anneaux de noyau $(m \vee n)\mathbb{Z}$ et que
$$\mathrm{Im}(\alpha) = \{(\bar{x}, \bar{y}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mid x \equiv y \ [m \wedge n]\}.$$
2. Résoudre les systèmes d'inconnue $x \in \mathbb{Z}$ ci-dessous.

$$(i)\ \begin{cases} x \equiv 25 \ [40] \\ x \equiv 35 \ [60] \end{cases} \qquad (ii)\ \begin{cases} x \equiv 25 \ [40] \\ x \equiv 5 \ [60] \end{cases}$$

Exercice 33 :

(i) L'entier 99 est-il un carré modulo 197 ?

(ii) L'entier 219 est-il un carré modulo 383 ?

Exercice 34 : Résoudre l'équation $x^2 - 23y = 54$ avec $(x,y) \in \mathbb{Z}^2$.

Exercice 35 : Résoudre l'équation $x^2 + 3x + 1 \equiv 0[55]$ pour $x \in \mathbb{Z}$.

Exercice 36 : Soient $p \in \mathbb{N}$ un nombre premier impair et $(a,b,c) \in \mathbb{Z}$ un triplet tel que $a \wedge p = b \wedge p = 1$. Montrer que l'équation $ax^2 + by^2 \equiv c[p]$ admet une infinité de solutions $(x,y) \in \mathbb{Z}^2$.

Exercice 37 : Soit p un nombre premier vérifiant $p > 3$. Montrer que 3 est un carré modulo p si et seulement si $p \equiv \pm 1[12]$.

Exercice 38 : Soit $p = 2^{2^n} + 1$ un nombre premier de Fermat avec $n \in \mathbb{N}^*$. Montrer que la classe de 3 engendre le groupe $(\mathbb{Z}/p\mathbb{Z})^*$.

Exercice 39 : Montrer qu'il existe une infinité de nombres premiers congrus à 2 modulo 3.

Exercice 40 : Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Exercice 41 : Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Exercice 42 (Théorème de Wilson) **:** Soit $p \in \mathbb{N}$ avec $p > 1$. Montrer que p est un nombre premier si et seulement si $(p-1)! + 1 \equiv 0[p]$.

Exercice 43 : Soit $p \in \mathbb{N}$ un nombre premier avec $p \equiv 1[4]$. Montrer que

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1[p].$$

Exercice 44 : Soient $n \in \mathbb{N}^*$ et p est un nombre premier. Combien de groupes abéliens d'ordre p^n existe-t-il à isomorphisme près ?

Exercice 45 : Déterminer les facteurs invariants des groupes abéliens suivants.

$$(i)\ \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}, \quad (ii)\ \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/135\mathbb{Z} \times \mathbb{Z}/75\mathbb{Z}.$$

Exercice 46 : Déterminer les facteurs invariants de $(\mathbb{Z}/187\mathbb{Z})^\times$.

Exercice 47 : Un anneau commutatif de cardinal 4 est-il nécessairement isomorphe à l'anneau $\mathbb{Z}/4\mathbb{Z}$ ou à l'anneau $(\mathbb{Z}/2\mathbb{Z})^2$?

Indications

Exercice 1 : On a $A/dA \simeq \mathbb{Z}/d\mathbb{Z}$. Les idéaux maximaux et les idéaux premiers sont les mêmes. Il s'agit des pA où p est un diviseur premier de n.

Exercice 2 : Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de l'entier n, alors on a $I = (p_1 \cdots p_k)$. On trouve $p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}$ éléments nilpotents dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 3 : Les éléments nilpotents sont les classes des multiples de 30.

Exercice 4 : Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de l'entier n, alors en utilisant le théorème Chinois et le lemme de Gauss, on trouve qu'il y a 2^k idempotents.

Exercice 5 : En utilisant le lemme Chinois, on trouve que les éléments idempotents sont les classes de 0, 1, 34 et 154.

Exercice 7 : Pour la question 1, si $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupe, on remarque que l'ordre de $\varphi(1)$ divise $m \wedge n$. Réciproquement, chacun des éléments de $\mathbb{Z}/n\mathbb{Z}$ dont l'ordre divise $m \wedge n$ permet de construire un morphisme $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, donc il y a $m \wedge n$ morphismes de groupes. Pour la question 2, on a nécessairement $\varphi(1) = 1$. On doit donc avoir que $n \mid m \wedge n$, ce qui n'est que possible si n divise m. Ainsi, si n ne divise pas m, il n'y a pas de morphismes d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ et dans le cas contraire, il n'y en a que 1.

Exercice 9 : Il y a $\varphi(180) = 48$ éléments inversibles dans $\mathbb{Z}/180\mathbb{Z}$. L'inverse de 89 dans $\mathbb{Z}/180\mathbb{Z}$ est 89.

Exercice 10 : Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n \mid 4$, $n = p^k$ ou $n = 2p^k$ avec $k \in \mathbb{N}^*$ et p est un nombre premier impair.

Exercice 11 : Le groupe admet $\varphi(\varphi(54)) = 6$ générateurs.

Exercice 12 : On trouve 4.

Exercice 13 : On trouve 81.

Exercice 14 : On commence par remarquer que l'on peut écrire $\frac{m}{n} = \frac{m'}{p} \cdot 10^{-k}$ avec $m' \wedge n = 1$. Comme m/n et m'/p ont les mêmes périodes, on peut donc supposer que $k_1 = k_2 = 0$ et $n = p$. En notant r la longueur de la partie non périodique, on obtient que ℓ est un période de m/n si et seulement si

$$10^{r+\ell} m - 10^r m \equiv 0[n] \quad \Leftrightarrow \quad 10^\ell \equiv 1[n],$$

d'où le résultat.

Exercice 15 : Si l'application α_e est bijective, alors on obtient par restriction un automorphisme de $(\mathbb{Z}/n\mathbb{Z})^\times$. Le noyau de ce dernier est constitué des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ dont l'ordre divise e. Il ne peut que être trivial si $e \wedge \varphi(n) = 1$. Réciproquement, il existe $f \in \mathbb{N}$ tel que $ef \equiv 1[\varphi(n)]$. On vérifie avec le lemme Chinois que $\alpha_e \circ \alpha_f = \mathrm{Id}$ en utilisant que n est sans facteur carré.

Exercice 16 : L'élément -1 est d'ordre 2 dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 18 : Si $(p_n)_{n\in\mathbb{N}}$ est la suite des nombres premiers, considérer $x_n = p_1 \cdots p_n$ et $y_n = p_n$.

Exercice 19 : On a $S = B^{\mathrm{T}} D B$, donc $\det(S) = \prod_{k=1}^n \varphi(k)$.

Exercice 22 : Les solutions sont

(i) Modulo 6, on a $5n^3 + n = -(n-1)n(n+1)$ qui est divisible par 6.

(ii) Modulo 7, on a $3^{2n+1} + 2^{n+2} = 9^n \cdot 3 + 2^n \cdot 4 = 2^n \cdot 7 = 0$.

(iii) Modulo 11, on a $3^{8n} \cdot 5^4 + 5^{6n} \cdot 7^3 = 5^n \cdot 9 + 5^n \cdot 2 = 0$.

(iv) Modulo 5, on a $2^{2n+1} + 3^{n+1} = 4^n \cdot 2 + 9^n \cdot 3 = 4^n \cdot 5 = 0$.

(v) Modulo 9 par récurrence, on a $4^{n+1} - 1 - 3n = 3(4^n - 1) = 0$ car $3 \mid 4^n - 1$.

(vi) Modulo 15^2 par récurrence, on a $16^{n+1} - 1 - 15n = 15(16^n - 1) = 0$.

Exercice 26 : Regarder les valeurs possibles de $x^2 + y^2$ modulo 7.

Exercice 27 : On regarde modulo 4 pour montrer que x, y et z sont pairs. En décomposant $x, y \in \mathbb{Z}^*$ en produit d'une puissance de 2 et d'un nombre impair, puis en raisonnant modulo 4, on en déduit que $(x, y, z) = (0, 0, 0)$.

Exercice 28 : On a $x^3 \equiv 3y^3[13]$. En étudiant les cubes modulo 13, on en déduit que $x \equiv y \equiv 0[13]$. On conclut que $(x, y, z) = (0, 0, 0)$ est l'unique solution de l'équation.

Exercice 29 : Les solutions du système (i) sont les $(x, y) \in \mathbb{Z}^2$ tels que $x \equiv 1[48]$ et $y \equiv 8[48]$. Les solutions du système (ii) sont les $(x, y) \in \mathbb{Z}^2$ tels que $x \equiv 4[48]$ et $y \equiv 23[48]$.

Exercice 30 : L'implication directe est le théorème Chinois. Réciproquement s'il existe un nombre premier p divisant m et n, compter le nombre d'éléments d'ordre p dans chacun des groupes.

Exercice 31 : En utilisant le théorème Chinois, on trouve que les solutions du système (i) sont les entiers $x \in \mathbb{Z}$ tels que $x \equiv 29[132]$ et celles du système (ii) sont les entiers $x \in \mathbb{Z}$ tels que $x \equiv 226[2520]$.

Exercice 32 : D'après la question 1, le système (i) n'a pas de solution. Les solutions du système (ii) sont les entiers $x \in \mathbb{Z}$ tels que $x \equiv 65[120]$.

Exercice 33 : En utilisant la loi de réciprocité quadratique, on trouve que 99 n'est pas un carré modulo 197 et que 219 est un carré modulo 383.

Exercice 34 : Si $(x, y) \in \mathbb{Z}^2$ est solution, alors $x^2 \equiv 7[23]$ ce qui n'est pas possible.

Exercice 35 : Avec le lemme Chinois, on se ramène à résoudre l'équation dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/11\mathbb{Z}$. On trouve finalement que les solutions sont les $x \in \mathbb{Z}$ avec $x \equiv 6[55]$ ou $x \equiv 46[55]$.

Exercice 36 : Dénombrer les possibilités pour ax^2 et pour $c - by^2$.

Exercice 38 : Remarquer que la classe de 3 engendre le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ si et seulement si 3 n'est pas un carré modulo p.

Exercice 39 : Supposer qu'il n'y en ait qu'un nombre fini $p_1, \dots, p_k$ et introduire $m = 3p_1 \dots p_k - 1$.

Exercice 40 : Supposer qu'il n'y en ait qu'un nombre fini $p_1, \dots, p_k$ et introduire $m = (p_1 \dots p_k)^2 + 1$.

Exercice 41 : Supposer qu'il n'y en ait qu'un nombre fini $p_1, \dots, p_k$ et introduire $m = 4p_1 \dots p_k - 1$.

Exercice 44 : Par le théorème de structure, il y en a le nombre de partitions de l'entier n.

Exercice 45 : On trouve $(2520, 4, 2)$ et $(5400, 15, 3)$.

Exercice 46 : On trouve $(80, 2)$.

Exercice 47 : Non, on peut montrer qu'il y a 4 anneaux commutatifs de cardinal 4 à isomorphisme près qui sont $\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{F}_4$ et $\mathbb{F}_2[X]/(X^2)$.