Anneau $\mathbf{Z}/n\mathbf{Z}$. Théorèmes d'Euler et de Fermat. Théorème chinois.

Exercice 1. **1.** Montrer que l'anneau $\mathbf{Z}/2\mathbf{Z}$ ne possède que deux éléments, $\overline{0}$ et $\overline{1}$; en dresser les tables de multiplication et d'addition.
2. Ecrire les tables de multiplication de $\mathbf{Z}/6\mathbf{Z}$ et $\mathbf{Z}/7\mathbf{Z}$.

Exercice 2. **1.** Soit x un nombre premier à 10. Par quel(s) chiffre(s) peut se terminer x^{168} ?
2. Quels sont les entiers naturels a tels que 3^a se termine par le chiffre 1 en base 10 ?
3. Quels sont les couples d'entiers naturels (a, b) tels que $3^a 7^b$ se termine par le chiffre 1 en base 10 ?

Exercice 3. **1.** Montrer qu'un nombre est congru modulo 9 à la somme de ses chiffres.
2. Quel est le reste de la division par 9 de $7777777^{4444444}$?

Exercice 4. **1.** Déterminer le reste de la division de 247^{349} par 7.
2. Montrer que $2^{36} + 5^{18}$ est divisible par 41.
3. Montrer que $5^4 \times 2^{28} \equiv 1 \pmod{641}$, $5^4 \equiv -2^4 \pmod{641}$, puis que 641 divise $2^{32} + 1$.

Exercice 5. Le but de cet exercice est de montrer qu'il n'existe pas d'entier n supérieur ou égal à 2 tel que n divise $2^n - 1$. On va raisonner par l'absurde. Supposons qu'un tel n existe, et notons p le plus petit diviseur premier de n.
1) Montrer que $p > 2$.
2) On note δ l'ordre de la classe de 2 dans $(\mathbf{Z}/p\mathbf{Z})^*$.
a) Montrer que δ divise $p - 1$.
b) Montrer que δ divise n.
c) Conclure.

Exercice 6. Le but de cet exercice est de montrer le théorème de Wilson : *un entier n strictement positif est premier si et seulement si* $(n-1)! \equiv -1 \pmod{\text{n}}$.
1. Question préliminaire : Soit p un nombre premier. Combien de solutions l'équation $x^2 = 1$ admet-elle dans l'anneau $\mathbf{Z}/p\mathbf{Z}$?
2. Soit p un nombre premier impair. Montrer que $(p-1)! \equiv -1 (\text{mod p})$.
3. Soit $n \geq 2$ un entier tel que n divise $(n-1)!+1$. Montrer que $\mathbf{Z}/n\mathbf{Z}$ est un corps. (Indication : si $1 \leq a \leq n-1$, quelle est l'inverse de a dans $(\mathbf{Z}/n\mathbf{Z})^*$?)
4. Conclure.

Exercice 7. Quel est le plus petit entier naturel multiple de 7 qui soit congru à 1 modulo 2, 3, 4, 5 et 6 ?

Exercice 8. 1. Calculer le reste de la division euclidienne de 3^{683} par 245.
2. a) Calculer le reste de la division euclidienne de 3^{164} par 88.
b) Calculer l'ordre de 3 dans $(\mathbf{Z}/88\mathbf{Z})^*$.
c) Quel est l'ordre de 7 dans $(\mathbf{Z}/88\mathbf{Z})^*$?

Exercice 9. 1. Ecrire le tableau des puissances de 2 dans $\mathbf{Z}/41\mathbf{Z}$.
2. En déduire les ordres respectifs de 2, 3, 4, 5 et 6 dans $(\mathbf{Z}/41\mathbf{Z})^*$. Lequel de ces éléments est-il un générateur de $(\mathbf{Z}/41\mathbf{Z})^*$?
3. Le nombre 7 est-il un générateur de $(\mathbf{Z}/41\mathbf{Z})^*$? Pourquoi ?
4. Combien y a-t-il de générateurs de $(\mathbf{Z}/41\mathbf{Z})^*$? Justifier le calcul.
5. Déterminer un entier $1 \leq i \leq 40$ tel que $2 \equiv 6^i \pmod{41}$; justifier l'unicité de i.
6. Déduire de la question précédente un entier $1 \leq j \leq 40$ tel que $3 \equiv 6^j \pmod{41}$.

Exercice 10. Montrer que les anneaux $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ et $\mathbf{Z}/6\mathbf{Z}$ sont isomorphes. Donner un isomorphisme ainsi que l'isomorphisme réciproque.

Exercice 11. Un bateau de pirates s'empare d'un butin en pièces d'or. Les 17 pirates décident de se répartir également les pièces et de donner le reste au cuisinier : celui-ci reçoit 6 pièces. Une bagarre éclate à l'issue de laquelle 6 pirates sont tués, les survivants refont la répartition et le cuisinier se retrouve avec 10 pièces. Une tempête tue ensuite 7 autre pirates, le cuisinier voit sa part réduite à 3 pièces. Il décide alors d'empoisonner les survivants et de s'emparer du trésor. Combien de pièces d'or possèdera-t-il au minimum ?

Exercice 12. 1. Expliquer pourquoi 5 est inversible dans $\mathbf{Z}/27\mathbf{Z}$ et donner son inverse.
2. Résoudre dans $\mathbf{Z}$ l'équation $5x \equiv 4 \pmod{27}$.
3. Résoudre dans $\mathbf{Z}$ le système d'équations

$$\begin{cases} 5x & \equiv & 4 & \pmod{27} \\ 12x & \equiv & 9 & \pmod{51}. \end{cases}$$

Exercice 13. 1. Donner la liste des éléments de $(\mathbf{Z}/22\mathbf{Z})^*$.
2. Montrer que $(\mathbf{Z}/22\mathbf{Z})^*$ est cyclique.
3. Donner la liste (*explicite*) des générateurs de $(\mathbf{Z}/22\mathbf{Z})^*$.
4. Montrer que $\mathbf{Z}/100\mathbf{Z}$ n'est pas cyclique, et que tous ses éléments sont d'ordre divisant 20.