1. Arithmétique élémentaire, $\mathbb{Z}/n\mathbb{Z}$

Exercice 1.1 Trouver les sous-groupes de $\mathbb{Z}$ contenant $24\mathbb{Z}$ et donner leurs relations d'inclusion.

Rappel : Identité de Bézout

Si $d = \text{PGCD}(a, b)$, il existe u et v dans $\mathbb{Z}$ tels que $au + bv = d$.

Exercice 1.2 Résoudre dans $\mathbb{Z}$:

a) $3x + 5y = 4$ b) $261x - 406y = 87$
c) $15x - 9y = 21$ d) $15x + 54y = 38$
e) $17x + 19y = 23$

Exercice 1.3
- Donner un exemple de trois nombres entiers p, q, a tels que $p|a$, $q|a \not\Longrightarrow pq|a$. A quelle condition l'implication est-elle vraie ?
- Donner un exemple de trois nombres entiers p, a, b tels que $p|ab \not\Longrightarrow p|a$ ou $p|b$. A quelle condition l'implication est-elle vraie ?

Exercice 1.4 Soient a et b deux nombres entiers positifs et premiers entre-eux. Montrer que si le produit ab est une puissance k-ième ($k \geq 2$) alors les nombres a et b le sont également.

Exercice 1.5 Déterminer les solutions $n \in \mathbb{Z}$ des systèmes :

$$a) \begin{cases} n \equiv 3 \pmod{17} \\ n \equiv 4 \pmod{11} \\ n \equiv 5 \pmod{6} \end{cases} \qquad b) \begin{cases} n \equiv 3 \pmod{6} \\ n \equiv 2 \pmod{5} \\ n \equiv 6 \pmod{7} \end{cases} \qquad c) \begin{cases} 2x \equiv 3 \pmod{5} \\ 3x \equiv 2 \pmod{4} \end{cases}$$

Exercice 1.6 Résoudre dans $\mathbb{Z}$:

$$a) \begin{cases} 3x \equiv 3 \pmod{6} \\ 2x \equiv 10 \pmod{3} \\ 2x \equiv 4 \pmod{4} \end{cases} \qquad b) \begin{cases} 2x \equiv 2 \pmod{8} \\ x \equiv 2 \pmod{11} \\ 5x \equiv 5 \pmod{6} \end{cases} \qquad c) \begin{cases} 3y \equiv 11 \pmod{2} \\ 2y \equiv 10 \pmod{6} \\ y \equiv 12 \pmod{40} \end{cases}$$

Exercice 1.7 Un phare émet un signal jaune toutes les 15 minutes et un signal rouge toutes les 28 minutes. On aperçoit le signal jaune a 0h02 mn et le rouge a 0h08 mn. A quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

Exercice 1.8 Barry Botter vient d'apprendre un nouveau tour : si vous pensez à un nombre entre 0 et 1000, et que vous lui donnez les restes de ce nombre modulo 5,11 et 19, il vous retrouve en moins de 5 secondes (avec sa calculette magique quand même, qui possède une touche "modulo") le nombre de départ. Quel est le truc de Botter ? Est-ce que ce tour pourrait marcher en demandant des restes différents ? (par exemple modulo 10,22 et 38 ? ou modulo 5,7 et 11 ?)

Exercice 1.9 Vous connaissez sans doute le critère de divisibilité par 9 : on fait la somme des chiffres, puis la somme des chiffres du résultat, et ainsi de suite... Si le résultat final est 9, le nombre de départ était divisible par 9.

1. Montrer que ce critère repose sur le fait que $10 \equiv 1 \pmod{9}$.
2. De façon analogue, inventer un critère de divisibilité par 7 (disons pour un nombre à 3 chiffres, ou plus si vous êtes ambitieux) et par 11 (sans doute plus facile).

Exercice 1.10 Quel est le dernier chiffre de 2009^{2009} dans l'écriture décimale ? Dans l'écriture diadique ? Dans l'écriture triadique ?

Exercice 1.11 Calculer le dernier chiffre de 7^{25}. Même question avec $7^{100!}$.

Rappel : Indicatrice d'Euler

L'indicatrice d'Euler $\varphi(n)$ est définie comme le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.12

1. Calculer les tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 5$ et $n = 6$.
2. Lister les éléments inversibles dans chaque cas. Quelles sont les indicatrices d'Euler $\varphi(n)$?

Exercice 1.13 Calculer la valeur $\varphi(m)$ de l'indicatrice d'Euler pour :

a) $m = 13$ b) $m = 12$ c) $m = 8$ d) $m = 27$

Quelle est la formule générale pour $\varphi(m)$?

Exercice 1.14 Soit n un entier strictement positif.

a) Montrer que les trois assertions suivantes sont équivalentes

1. $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$;
2. k et n sont premiers entre eux ;
3. $\bar{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

b) Montrer que si $\text{pgcd}(n, m) = 1$ alors $\varphi(nm) = \varphi(n)\varphi(m)$.

c) Calculer $\varphi(p^n)$ lorsque p est premier, puis $\varphi(n)$ pour tout entier n.

d) Montrer par récurrence que $n = \sum_{d|n} \varphi(d)$.

Rappel : Pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^{\varphi(n)} = 1$

Exercice 1.15 (Preuve élémentaire du petit théorème de Fermat)

1. Montrer que pour tout couple d'entiers a et b et tout p premier, on a :

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

2. En déduire le petit théorème de Fermat :

$$n^p \equiv n \pmod{p}.$$

3. A quelle condition a-t-on $n^{p-1} \equiv 1 \pmod{p}$?

Exercice 1.16 Calculer l'indicatrice d'Euler $\varphi(100)$, montrer que $7^{40} \equiv 1 \pmod{100}$ et en déduire les deux derniers chiffres des nombres $7^{100!}$ et $7^{(9^8)}$.

Calculer les deux derniers chiffres de $7^{(3^{(7^{1000})})}$.