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

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

Exercice 1.1 1. Soient $a, b \in \mathbb{Z} \setminus \{0\}$ et $c \in \mathbb{Z}$. Rappeler une condition nécessaire et suffisante pour que l'équation $ax+by = c$ ait une solution entière $(x, y) \in \mathbb{Z}^2$. Lorsque cette équation a une solution $(x_0, y_0) \in \mathbb{Z}^2$ déterminer l'ensemble de ses solutions dans $\mathbb{Z}^2$ en fonction de x_0, y_0, a, b.

2. Résoudre dans $\mathbb{Z}^2$:

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

Exercice 1.2 – 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 1.3 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 1.4 (Triplets pythagoriciens) Déterminer tous les triplets d'entiers (x, y, z) tels que $x^2 + y^2 = z^2$;

Indications :

1. vérifier que l'on peut se rammener à la recherche de solutions où x, y, z sont positifs et premiers entre eux deux à deux ;
2. étudier ensuite la parité de x, y et z ;
3. en supposant que y est pair, montrer que $z + y$ et $z - y$ sont premiers entre eux et en déduire que ces deux nombres sont des carrés.

Exercice 1.5 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 1.6 Quel est le dernier chiffre de 1989^{2011} dans l'écriture décimale ? Dans l'écriture diadique ? Dans l'écriture triadique ?

Exercice 1.7 Calculer le dernier chiffre dans l'écriture décimale de 7^{25}. Même question avec $7^{100!}$.

Exercice 1.8

1. Calculer les tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 5$ et $n = 6$.
2. Dans chaque cas faire la liste des éléments inversibles pour la multiplication.
3. Soit $n \geq 1$ et k un entier. Montrer que la classe $\bar{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication si et seulement si k et n sont premiers entre-eux.
4. Déterminer l'inverse multiplicatif de $\overline{6}$ dans $\mathbb{Z}/37\mathbb{Z}$. Même question pour $\overline{11}$ dans $\mathbb{Z}/24\mathbb{Z}$.

Exercice 1.9 Déterminer les solutions $n \in \mathbb{Z}$ des systèmes :

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

Exercice 1.10 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 1.11 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 ?

Indicatrice d'Euler. Pour $n \geq 1$, l'indicatrice d'Euler $\varphi(n)$ est définie comme le nombre d'éléments inversibles pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.12

1. Calculer $\varphi(13)$, $\varphi(12)$, $\varphi(8)$, $\varphi(27)$.
2. Que vaut $\varphi(p^r)$ pour p un nombre premier et r un entier strcitement positif ?
3. Si n et m sont deux entiers strictement positifs premiers entre-eux, comment s'exprime $\varphi(mn)$ en fonction de $\varphi(m)$ et de $\varphi(n)$?
4. Donner une formule générale de $\varphi(n)$ en fonction de n.
5. Montrer par récurrence que pour tout $n \geq 1$,
$$n = \sum_{d|n} \varphi(d).$$

Rappel. Soit $n > 1$. Pour tout entier a premier avec n, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Exercice 1.13 (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 1.14 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 $7^{(3^{(7^{1000})})}$.

Exercice 1.15 Soient n et m deux entiers strictements positifs premiers entre eux. Montrer que
$$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{nm}.$$