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

Exercice 1.1 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 1.2 Déterminer les solutions $n \in \mathbb{Z}$ des systèmes :

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

Exercice 1.3 Résoudre dans $\mathbb{Z}$:

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

Exercice 1.4 Calculer les pgcd des couples de polynômes de $\mathbb{Z}[X]$ suivants :

$$a)\ X^3 + 3X^2 + 3X + 2,\ X^3 - 7X - 6. \qquad b)\ X^3 + 7X^2 + 8X - 16,\ X^3 + 6X^2 + 5X - 12$$

Exercice 1.5 Résoudre dans $\mathbb{R}[X]$ le système de congruences :

$$\begin{cases} P(X) \equiv X - 2 \pmod{X^2} \\ P(X) \equiv 1 \pmod{X - 1} \end{cases}$$

Exercice 1.6 1) Soient $x, y, z \in \mathbb{Z}$ tels que $x^2 + y^2 = z^2$. On suppose tout d'abord x, y, z premiers entre eux dans leur ensemble, autrement dit, que leur pgcd est 1. Montrer : qu'ils sont premiers entre eux deux à deux ; que x ou y est impair, mais pas les deux ; que z est impair.

2) On suppose que c'est x qui est impair. Montrer que $z - x$ et $z + x$ ont pour pgcd 2, puis que $(z - x)/2$ et $(z + x)/2$ sont des carrés. En déduire qu'il existe $u, v \in \mathbb{Z}$ tels que $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$.

3) Décrire toutes les solutions entières de l?équation $x^2 + y^2 = z^2$ sans hypothèse sur x, y, z.

4) Montrer que l'équation $x^4 + y^4 = z^4$ n'admet pas de solutions entières non évidentes, i.e. telles que $xy = 0$.

Exercice 1.7 1) Montrer que le reste de la division euclidienne de $X^a - 1$ par $X^b - 1$ est $X^r - 1$, où r est le reste de la division euclidienne de a par b.

2) Montrer que le pgcd de $X^n - 1$ et $X^m - 1$ est $X^q - 1$, où q est le pgcd de m et n.

Exercice 1.8 Rain Man 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 le nombre de départ. Quel est le truc de Rain Man (qui calcule "modulo" à une vitesse de calculette) ? 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

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

Exercice 1.12 Quel est le dernier chiffre de 2013^{2013} dans l'écriture décimale ? Dans l'écriture diadique ? Dans l'écriture triadique ?

Exercice 1.13 Soit n un entier strictement positif. On note $\varphi(n)$ l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$.
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 $n = \sum_{d|n} \varphi(d)$.

Exercice 1.14 (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 1.15 Calculer l'indicatrice d'Euler $\varphi(100)$, montrer que $7^{40} \equiv 1 \pmod{100}$ et en déduire les deux derniers chiffres du nombre $7^{(9^8)}$.