T.D. 2 : Arithmétique

1 Équations $ax + by = c$

Exercice 1. Considérons l'équation

$$(E) \quad ax + by = c$$

où $a, b, c \in \mathbb{Z}^*$. Posons $d = \operatorname{pgcd}(a, b)$.

(1) Montrer que l'équation (E) admet des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $d|c$.

(2) Soient $u, v \in \mathbb{Z}$ tels que $au + bv = d$ et supposons que $d|c$. Montrer que l'ensemble des solutions de l'équation (E) s'écrit sous la forme :

$$S = \left\{ \left(\frac{cu - bk}{d}, \frac{cv + ak}{d} \right) \in \mathbb{Z}^2 : k \in \mathbb{Z} \right\}.$$

Exercice 2.

(1) En utilisant l'algorithme d'Euclide, déterminer le PGCD de 1761 et 1567.

(2) En déduire la valeur du PPCM de 1761 et 1567.

(3) Posons $d = \operatorname{pgcd}(1761, 1567)$. Trouver des entiers relatifs u_0 et v_0 tels que $d = 1761u_0 + 1567v_0$.

(4) En déduire tous les couples (u, v) d'entiers relatifs tels que $d = 1761u + 1567v$.

Exercice 3. Déterminer tous les entiers x, y vérifiant :

(1) $56x + 35y = 7$.

(2) $56x + 35y = 10$.

Exercice 4. Résoudre dans $\mathbb{Z}$ l'équation

$$1665x + 1035y = 45.$$

2 Petit théorème de Fermat

Exercice 5.

(1) Enoncer le petit théorème de Fermat.

(2) Calculer $55555^{55555} \pmod 7$.

Exercice 6.

(1) Trouver le reste de la division par 13 du nombre 100^{1000}.

(2) Trouver le reste de la division par 17 du nombre 14^{3141}.

Exercice 7. Soient a et n des entiers avec $n \geqslant 2$. On appelle **ordre de a modulo n**, le plus petit $k > 0$ tel que

$$a^k \equiv 1 \pmod n.$$

(1) Montrer que si un tel entier k existe, alors a et n sont premiers entre eux.

(2) Supposons que a et n sont premiers entre eux et que $k > 0$ est l'ordre de a modulo n. Montrer que s'il existe $m \in \mathbb{N}$ tel que $a^m \equiv 1 \pmod n$, alors m est un multiple de k.

(3) *Application :* montrer que si $n > 1$ divise $2^n + 1$, alors n est divisible par 3.

3 Théorème des restes chinois

Exercice 8. Soient n_1 et n_2 deux entiers naturels premiers entre eux. Considérons le système de congruences

$$(S): \quad \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases} .$$

(1) Montrer qu'il existe $u_0, v_0 \in \mathbb{Z}$ tels que $a_1 + n_1 u_0 = a_2 + n_2 v_0$.

(2) Montrer qu'on peut remplacer le système (S) par l'équation équivalente

$$x \equiv b \pmod{n_1 n_2}, \quad \text{où} \quad b = a_1 + n_1 u_0.$$

(3) Montrer que le système (S) admet une unique solution modulo $n = n_1 n_2$.

Exercice 9. Résoudre dans $\mathbb{Z}$ le système :

$$\begin{cases} x \equiv 12 \pmod{65} \\ x \equiv 13 \pmod{99} \end{cases}$$

Exercice 10. Résoudre dans $\mathbb{Z}$ les systèmes d'équations en x :

$$\begin{cases} x \equiv 3[23] \\ x \equiv 6[22] \end{cases}, \quad \begin{cases} x \equiv 1234[7896] \\ x \equiv 4325[68324] \end{cases}, \quad \begin{cases} x \equiv 2[14] \\ x \equiv 4[28] \end{cases} .$$

Exercice 11. Mon panier peut contenir au plus cent œufs.

- Si je le vide par trois œufs à la fois, il en reste un.
- Si je le vide par huit œufs à la fois, il en reste deux.
- Si je le vide par sept œufs à la fois, il en reste cinq.

Combien ai-je d'œufs ?

4 Fonction indicatrice d'Euler

Exercice 12.

1. Rappeler la définition de la fonction indicatrice d'Euler φ.
2. Montrer que pour tout nombre premier p et tout entier $n \geq 1$, on a $\varphi(p^n) = p^n - p^{n-1}$.
3. Soient p et q sont deux nombres premiers distincts. Rappeler la valeur de $\varphi(pq)$ en fonction de p et q.

Exercice 13. Montrer que pour tout entier $n \geq 3$, l'entier $\varphi(n)$ est pair.

Exercice 14. Soient m et n des entiers naturels non nuls. Montrer que si m divise n alors $\varphi(m)$ divise $\varphi(n)$.

Exercice 15. Calculer $\varphi(80)$, $\varphi(100)$, $\varphi(168)$, $\varphi(1000)$, $\varphi(1950)$.

5 L'anneau $\mathbb{Z}/nZ$

Exercice 16. Dresser les tables d'addition et de multiplication de l'ensemble $\mathbb{Z}/6\mathbb{Z}$. Quels sont les éléments inversibles par la multiplication ?

Exercice 17. Dans $\mathbb{Z}/12\mathbb{Z}$, quel est le symétrique de $\overline{4}$, $\overline{7}$ et $\overline{9}$? Calculer $\overline{7} - \overline{11}$.

Exercice 18. Montrer que chaque élément de $(\mathbb{Z}/8\mathbb{Z}, +)$ s'écrit sous la forme $k \times \overline{3}$ où $k \in \mathbb{Z}$.