Plaquette 3 – Coefficients de Bézout et inverses modulaires

PGCD, théorème de Bézout, Gauss — Terminale maths expertes

Exercices

Méthode

On apprend à **remonter l'algorithme d'Euclide** pour écrire une identité de Bézout $au + bv = d$, à s'en servir pour démontrer que deux entiers sont premiers entre eux, à calculer un **inverse modulaire**, et à résoudre des congruences $ax \equiv b \pmod{n}$ que la simple table ne suffit plus à traiter.

Exercice 1 – Remonter l'algorithme d'Euclide

a) Montrer que 45 et 32 sont premiers entre eux.

b) Déterminer un couple d'entiers $(u\,;v)$ tel que $45u + 32v = 1$.

Exercice 2 – Bézout avec un PGCD non trivial

a) Calculer $\text{pgcd}(1\,071\,;462)$.

b) Déterminer un couple $(u\,;v)$ tel que $1\,071u + 462v = \text{pgcd}(1\,071\,;462)$.

Exercice 3 – Démontrer avec le théorème de Bézout

Soit n un entier naturel. Montrer que $2n + 3$ et $3n + 4$ sont premiers entre eux.

Exercice 4 – Tous les couples de Bézout

a) Trouver un couple d'entiers $(u\,;v)$ tel que $5u + 3v = 1$.

b) Déterminer **tous** les couples solutions.

Exercice 5 – Calculer un inverse modulaire

Déterminer l'inverse de 17 modulo 43, c'est-à-dire l'entier a de $\{0\,;\ldots\,;42\}$ tel que $17a \equiv 1 \pmod{43}$.

Exercice 6 – Résoudre grâce à l'inverse

Résoudre dans $\mathbb{Z}$ l'équation $17x \equiv 5 \pmod{43}$.

Exercice 7 – Déchiffrer un message affine

Les lettres sont codées par $A = 0$, …, $Z = 25$, et le chiffrement est $y \equiv 7x + 4 \pmod{26}$.

a) Justifier que ce chiffrement est déchiffrable et déterminer l'inverse de 7 modulo 26.

b) Déchiffrer le message LGXYOH.

Exercice 8 – Un inverse par simple lecture

a) Vérifier que $2\,026 = 45 \times 45 + 1$ et en déduire l'inverse de 45 modulo 2 026.

b) Résoudre $45x \equiv 7 \pmod{2\,026}$.

Exercice 9 – Un module non premier

a) Déterminer l'inverse de 11 modulo 30.

b) Résoudre $11x \equiv 7 \pmod{30}$.

Exercice 10 – Quand l'inverse n'existe pas

a) Montrer que 6 n'a pas d'inverse modulo 22.

b) Résoudre malgré tout $6x \equiv 4 \pmod{22}$.

Exercice 11 – Un système par Bézout

Résoudre le système

$$x \equiv 2 \pmod{7} \quad \text{et} \quad x \equiv 5 \pmod{9}$$

en utilisant une identité de Bézout entre 7 et 9.

Exercice 12 – Un PGCD à discuter

Soit n un entier naturel et $d = \operatorname{pgcd}\left(n^2 + n + 1\,;\, n + 2\right)$.

a) Montrer que d divise 3.

b) Préciser les valeurs de n pour lesquelles $d = 3$.

Exercice 13 – Mesurer un litre

On dispose de deux récipients non gradués de 5 L et 3 L, d'un robinet et d'un évier.

Expliquer, à l'aide d'une identité de Bézout, comment obtenir exactement 1 L dans le récipient de 5 L.

Exercice 14 – Premier avec a et avec b, donc avec ab

Soit a et b deux entiers premiers entre eux.

a) Montrer que $\operatorname{pgcd}(a + b\,;\, ab) = 1$.

b) Illustrer avec $a = 4$ et $b = 9$.

Exercice 15 – Bilan : Bézout de bout en bout

a) Déterminer un couple $(u\,;\, v)$ tel que $31u + 17v = 1$.

b) En déduire l'inverse de 17 modulo 31, puis résoudre $17x \equiv 9 \pmod{31}$.

c) On dispose de récipients de 7 L et 4 L. Peut-on mesurer exactement 1 L ? Et avec des récipients de 6 L et 9 L ?