



FACULTE DES SCIENCES ET DE TECHNOLOGIE

Département de Maths-Info.

Année Univ : 2025/2026

Master-1 informatique CySIA

Module : Mathématiques pour Cryptographie

Responsable du module : Mr. H. KHIAR

T.D n°01 du 1^{er} semestre

EXERCICE 01 : Donner la division euclidienne de $a=2025$ par $b=89$.

- Déterminer le reste de 2025^{17} modulo 89.
- Montrer que si $a \equiv b[n]$ alors $a^k \equiv b^k [n]$ pour tout entier k .

EXERCICE 02 : Calculer le $\text{pgcd}(891, 399)$ avec l'algorithme d'Euclide.

- En déduire des entiers x, y tels que $891x + 399y = \text{pgcd}(891, 399)$.
- Montrer que l'équation $891x \equiv 15[399]$ admet une solution et la donner.

EXERCICE 03 : Résoudre $77x \equiv 33[143]$ $77x \equiv 35[143]$.

- Vérifier combien de solutions modulo 143 existent dans les deux congruences.
- Généraliser : Sous quelles conditions $ax \equiv b[n]$ admet une solution ?

EXERCICE 04 : En écrit en base 4 : $(2x1)_4 = 45$. Trouver x .

- De même, en base 5 : $(x34)_5 = 94$.
- De même, en base 7 : $(5x2)_7 = 285$.

EXERCICE 05 : On cherche un chiffre x tel que $(1x1)_3 = N_{10}$ avec N divisible par 5. Trouver les valeurs possibles de x .

- En base 6 : $(2x4)_6 \equiv 1[7]$. Déterminer x .

EXERCICE 06 :

- En base 8 : $(x73)_8 = (4y5)_{10}$. Trouver le couple (x, y) .
- En base 9 : $(3x7)_9 = (2y4)_{10}$. Trouver le couple (x, y) .
- En base 16 : $(Bx)_{16} = (191)_{10}$. Trouver x .
- En base 16 : $(1xA)_{16} = (410)_{10}$. Trouver x .

EXERCICE 07 : Etudier suivant l'entier naturel non nul n le reste de la division euclidienne de 7^n sur 9.

- Déterminer n pour que $16^{3n} + 16^n - 2$ soit divisible par 9.

EXERCICE 08 : Résoudre dans $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$ les équations :

$$3x=5, 2x=4 \text{ et } (x+2)(x+3)=0.$$

EXERCICE 09 : Montrer que pour tout entier naturel n le nombre $3n^3 + 6n$ est divisible par 9.