

Fiche TD 02 :

Exercice 01 : Algorithme d'Euclide

Calculer :

1. $\text{Pgcd}(136, 33)$
2. $\text{Pgcd}(1928, 364)$
3. $\text{Pgcd}(546738492, 6754024)$

Exercice 02 : Algorithme d'Euclide Etendu

Trouver les coefficients de Bezout pour les nombres entiers suivants :

1. $(a ; b) = (50; 17)$
2. $(a ; b) = (280 ; 11)$
3. $(a ; b) = (50 , 35)$
4. $(a ; b) = (4864, 3458)$

Exercice 03 : Inverse multiplicatif

1. Calculer l'inverse multiplicatif de **317 mod 521**
2. Résoudre dans \mathbb{Z} les équations suivant :

- $17x \equiv 10 \pmod{50}$

$\text{Pgcd}(17, 50) = 1 \implies 17$ admet un inverse 17^{-1} On le calcule à l'aide de l'algorithme d'Euclide étendu : $17^{-1} = 3$

On multiplie l'équation par 17^{-1} , on obtient $17^{-1} \cdot 17x = 17^{-1} \cdot 10 \pmod{50} \implies x = 3 \cdot 10 \pmod{50} \implies x \equiv 30 \pmod{50}$

- $35x \equiv 10 \pmod{50}$
- $35y \equiv 11 \pmod{50}$

Exercice 04 : RSA

Considérez le système de chiffrement RSA avec $p=19$ et $q=23$:

1. Calculer n et son indicatrice d'Euclide $\Phi(n)$.
2. Calculer l'exposant d associé à $e=9$, puis $e=14$.
3. Calculer l'exposant d associé à $e=17$.