

TD 6 : Arithmétique modulaire

Christina Boura

Exercice 1 *Calculs modulaires*

Calculer :

1. $24000 \bmod 24$
2. $38 \bmod 13$
3. $14 \cdot 17 \bmod 15$
4. $3 \cdot (1 + 22) \bmod 11$

Exercice 2 *Algorithme d'Euclide étendu*

Soient $a = 1234$ et $b = 357$.

1. Calculer le $\text{pgcd}(a, b)$ en utilisant l'algorithme d'Euclide.
2. Calculer $u, v \in \mathbb{Z}$ tels que $u \cdot a + v \cdot b = \text{pgcd}(a, b)$.
3. Calculer l'inverse de b modulo a .

Exercice 3 *Fonction ϕ d'Euler*

1. Calculer $\phi(156)$.
2. Calculer $\phi(8800)$.
3. Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}_{20} = \{0, 1, 2, \dots, 19\}$?

Exercice 4 *Calculs modulaires à l'aide des théorèmes de Fermat et de Euler*

1. Calculer $2^{751} \bmod 31$.
2. Calculer $2^{2683} \bmod 55$.

Exercice 5 *Calcul de l'inverse avec les théorèmes de Fermat et de Euler*

Calculer l'inverse $a^{-1} \bmod n$ en utilisant le petit théorème de Fermat (si applicable) ou le théorème d'Euler sinon :

1. $a = 4, n = 7$
2. $a = 5, n = 12$
3. $a = 6, n = 13$