

Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHÉMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Examen terminal, le 10 mai 2023, 8h30-11h30

Documents autorisés, calculatrices interdites.

Exercice 1. Déterminer un générateur du groupe multiplicatif du corps \mathbb{F}_{101} .

Exercice 2. Alice et Bob veulent établir une clé secrète commune par le procédé de Diffie-Hellman. Alice communique à Bob le corps fini

$$K = \mathbb{F}_2[X]/(X^4 + X + 1),$$

le générateur

$$g = \overline{X + 1}$$

du groupe multiplicatif K^\times de K , et l'élément

$$h = \overline{X^3 + X^2 + 1}$$

de K^\times . Bob répond en communiquant à Alice l'élément

$$k = \overline{X^3 + 1}$$

de K^\times .

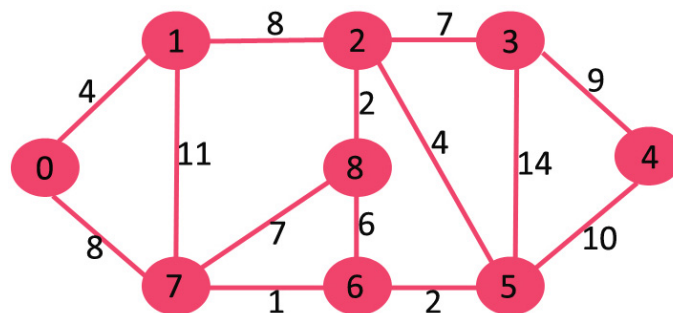
- Vérifier que K est bien un corps.
- Déterminer $|K|$.
- Vérifier que g est bien un générateur de K^\times .
- Déterminer la clé secrète qu'Alice et Bob partagent.

Exercice 3. Déterminer 4 entiers relatifs k, ℓ, m, n tels que la famille $\bar{k}, \bar{\ell}, \bar{m}, \bar{n}$ engendre le groupe multiplicatif de l'anneau $\mathbb{Z}/360\mathbb{Z}$.

Exercice 4. Déterminer le symbole de Jacobi

$$\left(\frac{1789}{2023}\right).$$

Exercice 5. Considérons le graphe pondéré suivant



Dérouler l'algorithme de Dijkstra afin de déterminer le chemin le plus court du sommet 0 aux autres sommets du graphe.