Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Examen terminal, le 16 juin 2023, 9h00-12h00

Documents autorisés, calculatrices interdites.

Exercice 1. Déterminer un générateur du groupe multiplicatif du corps $\mathbb{F}_{107}$.

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

$$K = \mathbb{F}_2[X]/(X^4 + X^3 + 1),$$

le générateur

$$g = \overline{X}$$

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

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

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

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

de $K^\times$.

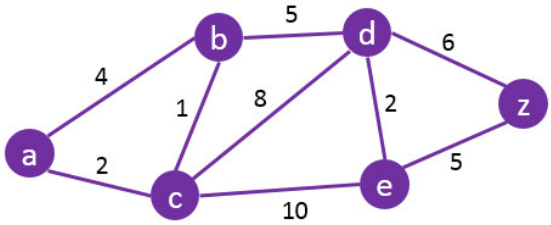
a. Vérifier que K est bien un corps.
b. Déterminer $|K|$.
c. Vérifier que g est bien un générateur de $K^\times$.
d. Déterminer la clé secrète qu'Alice et Bob partagent.

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 $\mathbb{Z}/600\mathbb{Z}$.

Exercice 4. Déterminer le symbole de Jacobi

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

Exercice 5. Considérons le graphe pondéré suivant



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