Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Examen terminal, le 18 juin 2014, 9h00–12h00

Documents et calculatrices sont interdits.

Question de cours. Qu'est-ce que l'échange de clé Diffie-Hellman ? Expliquer comment et pourquoi ce procédé fonctionne. Dire sur quoi est basée la sécurité de ce protocole.

Exercice 1. Soit P_n un n-gon convexe dans le plan, quel que soit l'entier $n \geq 3$. Une diagonale dans P_n est une droite reliant deux sommets non consécutifs de P_n. Soit a_n le nombre de diagonales de P_n, pour $n \geq 3$. Soit $F = \sum_{n\geq 0} a_{n+3} X^n$ la série génératrice associée.

a. Montrer par récurrence que $a_{n+1} = a_n + n - 1$ pour tout entier $n \geq 3$.

b. Montrer que
$$F = \frac{1}{(1-X)^3} - \frac{1}{(1-X)}.$$

c. En déduire que $a_n = \frac{1}{2}n(n-3)$, quel que soit $n \geq 3$.

Exercice 2. Soit G le graphe de Figure 1 ci-dessous. Est-ce que G est biparti ? Si oui, le démontrer. Sinon, expliquer pourquoi il ne l'est pas.

Exercice 3. Soit G un graphe connexe fini pondéré. Notons V l'ensemble de ses sommets, E l'ensemble de ses arêtes, et $w\colon E \to \mathbb{R}^{+,\star}$ la fonction poids de G. Soit $v_0 \in V$. On étudie l'algorithme suivant qui construit par récurrence une application «prédécesseur» $q\colon V \setminus \{v_0\} \to V$.

A l'initialisation, on pose $S_0 = \{v_0\}$ et $q_0\colon S_0 \setminus \{v_0\} \to S_0$ l'unique application de l'ensemble vide $S_0 \setminus \{v_0\}$ dans S_0. Supposons qu'au rang n on a construit $S_n \subseteq V$ et $q_n\colon S_n \setminus \{v_0\} \to S_n$. Si $S_n = V$ on pose $q = q_n$ et l'algorithme a terminé. Si $S_n \subsetneq V$, soient $v \in V \setminus S_n$ et $u \in S_n$, avec $\{u, v\} \in E$, tels que le poids $w(\{u, v\})$ de l'arête $\{u, v\}$ est minimal. On pose $S_{n+1} = S_n \cup \{v\}$ et on définit $q_{n+1}\colon S_{n+1} \setminus \{v_0\} \to S_{n+1}$ par

$$q_{n+1}(t) = \begin{cases} q_n(t) & \text{si } t \in S_n \setminus \{v_0\}, \text{ et} \\ u & \text{si } t = v. \end{cases}$$

a. Dérouler l'algorithme ci-dessus où G est le graphe pondéré de Figure 2, et $v_0 = 0$.

b. Soit G un graphe connexe fini pondéré quelconque, et soit v_0 l'un de ses sommets. Soit q l'application «prédécesseur» construit en effectuant l'algorithme ci-dessus sur le graphe G. Le chemin

$$v, q(v), q^2(v), \ldots, q^d(v),$$

où d est le plus petit entier naturel tel que $q^d(v) = v_0$, est-il le chemin le plus court de v à v_0 pour tout sommet v de G ? Si oui, le démontrer. Sinon, donner un contre-exemple explicite.

Exercice 4. L'énoncé (E) ci-dessous est-il vrai ou faux ? S'il est vrai, le démontrer. S'il est faux donner un contre-exemple.

(E) Pour tout corps fini K et pour tout sous-groupe G de $K^\star$, il existe un sous-corps L de K tel que $L^\star = G$.

Exercice 5. Déterminer le 21-ième polynôme cyclotomique Φ_{21} sur $\mathbb{Q}$.

Barème indicatif sur 20 points :

Q de cours	2 pts
Exercice 1	4 pts
Exercice 2	2 pts
Exercice 3	4 pts
Exercice 4	4 pts
Exercice 5	4 pts

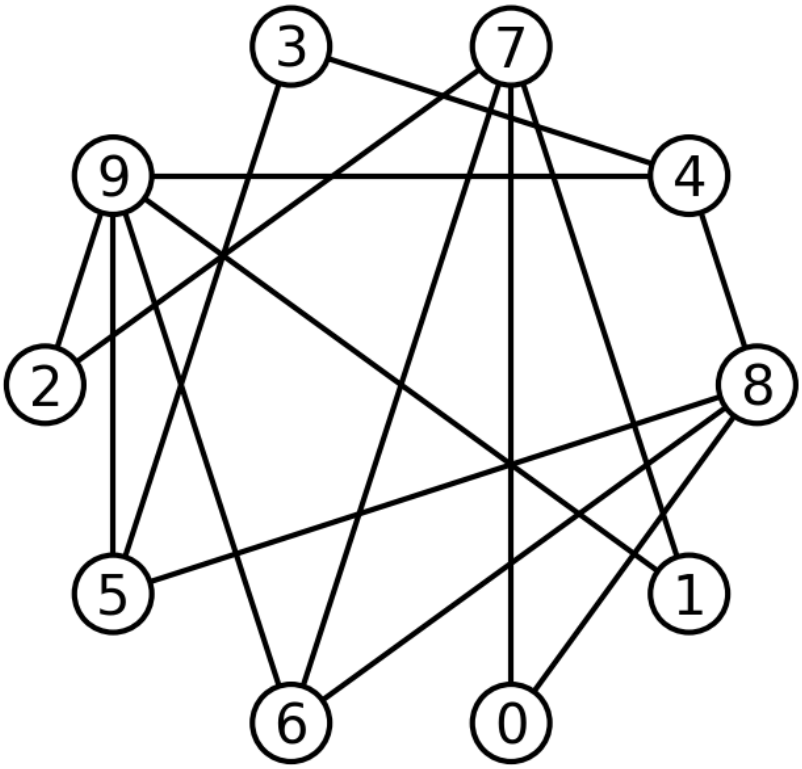

FIGURE 1 – Le graphe de l'exercice 2

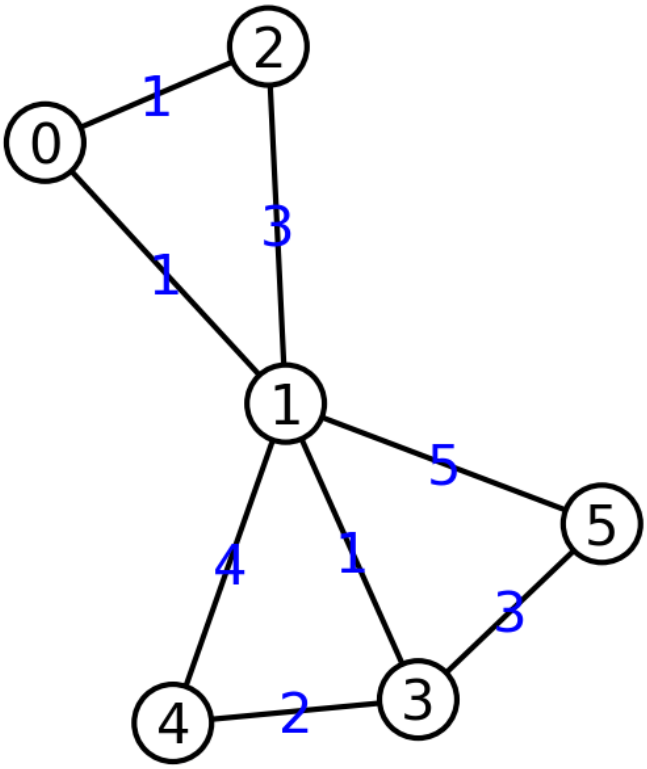

FIGURE 2 – Le graphe pondéré de l'exercice 3a