

ARITHMÉTIQUE ET APPLICATIONS, COMBINATOIRE ET
GRAPHES

Examen terminal, le 7 mai 2015, 14h00–17h00

Documents et calculatrices sont interdits.

Question de cours. Soit φ la fonction totient, ou l'indicatrice, d'Euler. Montrer que

$$n = \sum_{d|n} \varphi(d)$$

pour tout entier naturel non nul n , où la somme est prise sur tous les diviseurs positifs d de n .

Exercice 1. Soit $(a_n)_{n \in \mathbb{N}}$ la suite dans \mathbb{Q} définie par la relation de récurrence

$$(n+2)a_{n+2} = (n+1)a_{n+1} + na_n$$

pour tout $n \in \mathbb{N}$, et par les valeurs initiales $a_0 = a_1 = 1$. Soit F la série génératrice $\sum_{n=0}^{\infty} a_n X^n$ dans $\mathbb{Q}[[X]]$.

a. Montrer que

$$DF = \frac{1}{1 - X - X^2}$$

dans $\mathbb{Q}[[X]]$, où DF est la série formelle dérivée de F .

b. En déduire une formule close pour a_n .

Exercice 2. Soit G le graphe pondéré ci-dessous. Déterminer, à l'aide de l'algorithme de Dijkstra, le chemin le plus court dans G du sommet 0 à n'importe quel autre sommet de G .

Exercice 3. a. Dire parmi les polynômes unitaires suivants de $\mathbb{F}_3[X]$: $P_1 := X^3 + X + 1$, $P_2 := X^3 - X - 1$, lequel est irréductible ?

b. Notons-le Q . L'anneau quotient $K := \mathbb{F}_3[X]/(Q)$ est-il un corps ?

c. Donner une \mathbb{F}_3 -base de K .

d. En déduire le cardinal de K .

e. Considérons la classe $\alpha = \overline{X}$ dans K . Pour $a, b, c \in \mathbb{F}_3$, Ecrire $\left(\overline{aX^2 + bX + c}\right)^2$ dans K comme polynôme de degré 2 en α .

f. Donner l'ordre de la classe $\alpha = \overline{X}$ dans le groupe multiplicatif K^* .

g. Résoudre (en b) l'équation $\left(\overline{2X^2 + bX + 1}\right)^2 = \alpha$ dans K .

h. En déduire un élément β générateur du groupe multiplicatif K^* .

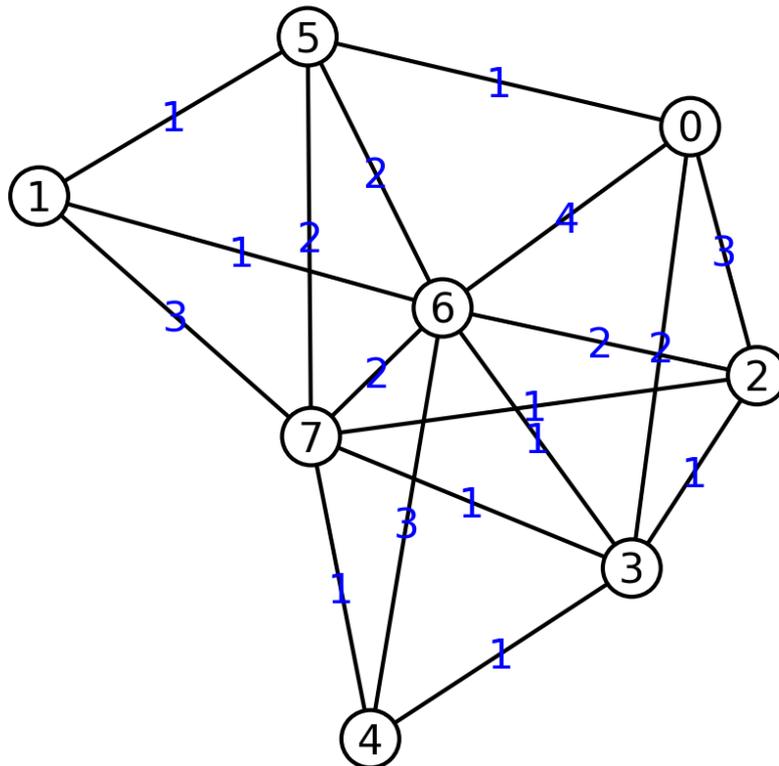
i. Déterminer les sous-corps de K .

Exercice 4. Alice et Bob communiquent par le code correcteur d'erreurs BCH[15, 7]. Alice envoie le mot de code $c \in F_2^{15}$. Bob reçoit le mot

$$r = (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$$

On suppose qu'il y a au plus 2 erreurs dans la transmission.

- Déterminer le nombre d'erreurs.
- Déterminer le mot de code c .



Barème indicatif sur 20 points :

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