Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Examen terminal, le 19 juin 2013, 9h00–12h00

Documents et calculatrices sont interdits.

Question de cours. Soit G un graphe. Montrer que G est biparti si et seulement si tout cycle fini de G est de longueur paire.

Exercice 1. Soit μ la fonction de Möbius définie par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts}, \\ 0 & \text{sinon.} \end{cases}$$

a. Pour $n \in \mathbb{N}^\star$, montrer que $\sum_{d|n} \mu(d) = 0$ si $n \neq 1$, et que $\sum_{d|n} \mu(d) = 1$ si $n = 1$.

b. Déterminer la série formelle $(1 - X^n)^{-\mu(n)/n}$ pour $n \in \mathbb{N}^\star$.

Soit F la série formelle définie par

$$F = \prod_{n \geq 1} (1 - X^n)^{-\mu(n)/n}.$$

c. Le produit infini ci-dessus, pourquoi est-il bien défini ?

d. Montrer que $\log(F) = X$.

e. En déduire que $F = \exp$.

Exercice 2. Soit p un nombre premier et soient m, n des entiers naturels non nuls.

a. Montrer que $p^m - 1$ divise $p^n - 1$ lorsque m divise n.

La suite de l'exercice consiste à démontrer la réciproque. Supposons donc que $p^m - 1$ divise $p^n - 1$ désormais.

b. Montrer que le polynôme $X^{p^m-1} - 1$ divise $X^{p^n-1} - 1$ dans $\mathbb{F}_p[X]$.

c. En déduire que le polynôme $X^{p^m-1} - 1$ possède $p^m - 1$ racines distinctes dans le corps $\mathbb{F}_{p^n}$.

d. En déduire que $\mathbb{F}_{p^n}$ contient $\mathbb{F}_{p^m}$ comme sous-corps.

e. En considérant $\mathbb{F}_{p^n}$ comme espace vectoriel sur $\mathbb{F}_{p^m}$, montrer que m divise n.

T. S. V. P.

Exercice 3. Soit un alphabet comprenant les 26 lettres, de A à Z, qui seront numérotées de 0 à 25, puis le blanc ␣, numéroté 26, et enfin le point ".", numéroté 27. On identifie naturellement cet alphabet élargi à $\frac{\mathbb{Z}}{28\mathbb{Z}}$ et on définit dessus une fonction de cryptage $\mathcal{C}$ qui a chaque lettre x associe la lettre correspondant à $\mathcal{C}(x)$ où $\mathcal{C}(x) = ax + b \bmod 28$.

a. Par exemple, si $a = 5$ et $b = 12$ quelle sera l'image de la lettre G ? Quelle sera l'antécédant de la lettre B ?

b. Pour que le message puisse être retrouvé sans ambiguïté, il faut évidemment que la fonction $\mathcal{C}$ soit injective. Donner une condition nécessaire et suffisante, portant sur a et b, qui garantit l'injectivité de $\mathcal{C}$.

c. Une espionne intercepte un message codé à l'aide d'une telle fonction. Elle analyse la fréquence des lettres et s'aperçoit que les deux signes les plus fréquents du code sont le B et ". ". Or les deux signes les plus utilisés en français sont l'espace ␣ et le E. Elle en déduit que B est l'image de l'espace et que "." est l'image du E.

   (i) Ecrire un système de deux équations modulo 28 vérifié par a et b.

   (ii) Résoudre ce système en a et b et vérifier que l'espionne ne peut retrouver la fonction $\mathcal{C}$ de cryptage à l'aide de ces seules informations.

   (iii) Elle continue donc son analyse des fréquences des lettres du message codé qu'elle a intercepté et cherche le troisième signe le plus fréquent. Il correspond en français au S. Est-ce que cette donnée supplémentaire lui permettra de trouver $\mathcal{C}$? Pourquoi ?