Université Claude Bernard (Lyon-I)
École Normale Supérieure de Lyon

Magistère Informatique et Modélisation
Module Calcul formel et cryptographie

Vendredi 16 novembre 2001
Durée : 2 heures 30.
Les notes de cours et les calculettes sont autorisées.

Dans tout ce qui suit la notation $\mathbb{F}_p$ représente le corps fini à p éléments

Exercice 1

Soit p un nombre premier impair. On note $\left(\frac{x}{p}\right)$ le symbole de Legendre, qui vaut 0 si x est un multiple de p et, quand x n'est pas multiple de p, 1 ou -1, selon que x est, ou n'est pas, un carré modulo p. Soit a un élément *non nul* de $\mathbb{F}_p$. On se propose de démontrer que, pour $x \in \mathbb{F}_p$, les évènements x *est un carré non nul* et $x + a$ *est un carré non nul* sont à peu près indépendants, c'est à dire que le nombre des $x \in \mathbb{F}_p$ tels que $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$ est environ $\frac{p}{4}$. On note donc A_p le nombre des entiers $x \in \{0, 1, \ldots, p-1\}$ tels que $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$.

1. Dans le cas où $a = 1$ calculer A_7.
2. On pose $S_p = \sum_{x=0}^{p-1} \left[1 + \left(\frac{x}{p}\right)\right] \left[1 + \left(\frac{x+a}{p}\right)\right]$. Montrer que
$$S_p = 4\,A_p + 2 + \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right).$$
3. On est ainsi ramené au calcul de S_p. Montrer que
$$S_p = p + \sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right).$$
4. Pour $1 \leq x \leq p-1$, soit y l'inverse de x modulo p. Montrer que
$$\left(\frac{x(x+a)}{p}\right) = \left(\frac{1+ay}{p}\right).$$
5. En déduire que $S_p = p - 1$, puis la valeur de A_p, et enfin l'encadrement
$$\frac{p-5}{4} \leq A_p \leq \frac{p-1}{4}.$$

Exercice 2

p est un nombre premier fixé. On note E_n l'ensemble des polynômes unitaires de degré n à coefficients dans $\mathbb{F}_p$. Soit ρ_n le nombre moyen des racines dans $\mathbb{F}_p$ d'un polynôme de E_n, chaque racine étant comptée une fois, même quand c'est une racine multiple. On se propose d'expliciter la valeur de ρ_n.

1. Combien y a-t-il de polynômes dans E_n admettant 0 pour racine ?

2. Plus généralement, soit $a \in \mathbb{F}_p$. Combien y a-t-il de polynômes dans E_n admettant a pour racine ? Soit X_a la variable aléatoire définie sur l'ensemble fini E_n, muni de la probabilité uniforme, par

$$X_a(f) = \begin{cases} 1 & \text{si } a \text{ est racine de } f \\ 0 & \text{sinon.} \end{cases}$$

   Quelle est l'espérance de X_a ?

3. Soit X la variable aléatoire définie sur E_n par $X = X_0 + X_1 + \ldots + X_{p-1}$. Calculer l'espérance de X. En déduire la valeur de ρ_n.

Problème

Dans ce problème b est un élément de $\mathbb{F}_5$, et u le polynôme $u = X^5 + X + b$.

1. Montrer que l'application $X \to X^5 + X$ est une bijection de $\mathbb{F}_5$ sur $\mathbb{F}_5$. En déduire que, pour tout $b \in \mathbb{F}_5$ le polynôme u admet une racine et une seule x_b dans $\mathbb{F}_5$. Exprimer simplement x_b en fonction de b.

2. Soit v le polynôme $v = X^2 + bX$. Montrer que v est solution de la congruence

$$v^5 - v \equiv 0 \pmod{u}.$$

   En déduire que u divise le polynôme $v(v-1)(v-2)(v-3)(v-4)$, puis que les facteurs irréductibles de u sont de degré au plus 2.

3. Montrer que u est le produit de $X - x_b$ par deux polynômes irréductibles de degré 2, qui sont de la forme

$$v + s,\ v + t, \qquad \text{avec } s, t \in \mathbb{F}_5,\ s \neq t.$$

4. Ecrire la factorisation de u en polynômes irréductibles sur $\mathbb{F}_5$ lorsque $b = 1$.

5. Montrer que les racines complexes de $z^5 + z + 6$ vérifient $|z| < 1.5$.

6. Montrer que X^5+X+6 admet une unique décomposition en facteurs irréductibles dans $(\mathbb{Z}/25\mathbb{Z})[X]$ que vous expliciterez.

7. En déduire que $X^5 + X + 6$ est irréductible dans l'anneau $\mathbb{Z}[X]$.