Corrigé de l'examenr partiel du vendredi 16 novembre 2001

Exercice 1

1. Dans le cas où $a = 1$ calculer A_7. Les carrés non nuls modulo 7 sont $\{1, 2, 4\}$. Le seul carré non nul x tel que $x + 1$ soit aussi un carré non nul est $x = 1$, et donc $A_7 = 1$.

2. Si l'un des symboles $\left(\frac{x}{p}\right), \left(\frac{x+a}{p}\right)$ est égal à -1 le terme d'indice x dans la somme S_p est nul. Si $x = 0$ le terme d'indice x est égal à $1 + \left(\frac{a}{p}\right)$. Si $x = -a$ le terme d'indice x est égal à $1 + \left(\frac{-a}{p}\right)$. Les termes restants sont ceux pour lesquels $\left(\frac{x}{p}\right) = \left(\frac{x+a}{p}\right) = 1$. Ils sont au nombre de A_p, et chacun prend la valeur $2 \times 2 = 4$. D'où $S_p = 4\,A_p + 2 + \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right)$.

3. En développant le terme d'indice x dans la somme S_p on obtient
$$S_p = \sum_{x=0}^{p-1} 1 + \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) + \sum_{x=0}^{p-1} \left(\frac{a+x}{p}\right) + \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{a+x}{p}\right)$$
La première somme vaut p, la deuxième et la troisième sont nulles, et la dernière, en utilisant la multiplicativité du symbole de Legendre, s'écrit encore
$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{a+x}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x(x+a)}{p}\right),$$
d'où $S_p = p + \sum_{x=0}^{p-1} \left(\frac{x(x+a)}{p}\right) = p + \sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right)$.

4. Pour $1 \le x \le p-1$, soit y l'inverse de x modulo p. Alors
$$\begin{aligned}\left(\frac{x(x+a)}{p}\right) &= \left(\frac{xxy(x+a)}{p}\right) = \left(\frac{x^2}{p}\right)\left(\frac{y(x+a)}{p}\right)\\ &= \left(\frac{yx+ay}{p}\right) = \left(\frac{1+ay}{p}\right)\end{aligned}$$

5. Quand x décrit l'ensemble $\mathbb{F}_p^*$, il en est de même de son inverse y, et, par la question précédente on a
$$\sum_{x=1}^{p-1} \left(\frac{x(x+a)}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{1+ay}{p}\right).$$
Comme a est inversible modulo p, l'application $y \to 1 + ay$ est une bijection de $\mathbb{F}_p$ sur $\mathbb{F}_p$. L'image de 0 par cette bijection est 1. Il en résulte que, lorsque y prend les valeurs $1, 2, \ldots, p-1$, $1 + ay$ prend toutes les valeurs de $\mathbb{F}_p$, sauf la valeur 1, et on a
$$\sum_{y=1}^{p-1} \left(\frac{1+ay}{p}\right) = \sum_{u=0}^{p} \left(\frac{u}{p}\right) - \left(\frac{1}{p}\right) = 0 - 1 = -1.$$

La question (3) donne alors $S_p = p - 1$, et enfin, par la question (2)

$$A_p = \frac{1}{4}\left[p - 3 - \left(\frac{a}{p}\right) - \left(\frac{-a}{p}\right)\right].$$

Comme la somme $\left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right)$ est comprise entre -2 et 2, on en déduit

$$\frac{p-5}{4} \leq A_p \leq \frac{p-1}{4}.$$

Remarquons que, lorsque p est de la forme $p = 4k+3$, la seule valeur entière de l'intervalle ci dessus est $\frac{p-3}{4}$, et donc $A_p = \frac{p-3}{4}$.

Exercice 2

1. Les polynômes admettant 0 pour racines sont les polynômes dont le terme constant est nul. Les coefficients de $x, x^2, \ldots, x^{n-1}$ sont arbitraires, ce qui donne p^{n-1} choix.

2. Un polynôme unitaire P de $\mathbb{F}_p[x]$ admet a pour racine si, et seulement si, il est de la forme $P(x) = (X - a)Q(x)$, avec Q, unitaire de degré $n-1$. Il y a autant de tels polynômes que de polynômes unitaires de degré $n-1$, soit p^{n-1}. La variable X_a est une variable de Bernouilli qui prend p^{n-1} fois la valeur 1. Son espérance est donc $\frac{p^{n-1}}{p^n} = \frac{1}{p}$.

3. Soit f un polynôme unitaire de degré n. Le nombre de ses racines dans $\mathbb{F}_p$ est égal à la somme

$$X_0(f) + X_1(f) + \ldots + X_{p-1}(f),$$

autrement dit, la variable aléatoire X définie sur E_n, qui associe à un polynôme f le nombre de ses racines dans $\mathbb{F}_p$, est la somme des X_i, pour $0 \leq i \leq p-1$. Son espérance est la somme des espérances des X_i (il n'est pas nécessaire que les variables X_i soient indépendantes) c'est à dire $\sum_{i=0}^{p-1} \frac{1}{p} = 1$.

Problème

1. Sur $\mathbb{F}_5$ l'application $x \to x^5$ coïncide avec l'application identique $x \to x$. Il en résulte que $x \to x^5 + x$ coïncide avec l'application $x \to 2x$. La fonction polynôme associée au polynôme u est donc l'application $x \to 2x + b$. L'équation $u(x) = 0$ s'écrit donc $2x + b = 0$ soit encore $6x + 3b = 0$, ou encore $x = 2b$.

2. En utilisant l'identité de Fobenius $(\alpha + \beta)^5 = \alpha^5 + \beta^5$, et l'égalité de Fermat $b^5 = b$, on obtient, modulo u,

$$\begin{aligned} v^5 &\equiv X^5(X+b)^5 \equiv X^5(X^5+b^5) \equiv X^5(X^5+b) \pmod{u} \\ &\equiv X^5(-X) = (-X-b)(-X) \equiv X^2 + bX \equiv v \pmod{u} \end{aligned}$$

Ceci signifie que u divise $v^5 - v = v(v+1)(v+2)(v+3)(v+4)$. Chaque facteur irréductible w de u divise donc l'un des polynômes $v, v+1, v+2, v+3, v+4$. Comme chacun de ces polynômes est de degré 2, w est de degré au plus 2.

3. On a vu qu'il y a exactement un facteur irréductible w de degré 1. Les autres w sont donc de degré exactement 2, il y en a deux, et comme chacun divise l'un des $v+s$, il coïncide avec celui ci. En outre s n'est pas nul, car $v+0=v=X(X+b)$ admet deux racines dans $\mathbb{F}_5$. La factorisation de u est donc de la forme

$$u=(X-x_b)(v+s)(v+t), \quad (s,t\in\{1,2,3,4\},\ s\neq t)$$

4. Lorsque $b=1$ on a $x_b=2$, et la factorisation de u est de la forme

$$\begin{aligned} X^5+X+1 &= (X+3)(X^2+X+s)(X^2+X+t) \\ &= X^5+X^3(s+t+2)+\ldots+3st. \end{aligned}$$

En identifiant les coefficient X^3 et les termes constants on obtient les équations $s+t+2=0$ et $3st=1$ qui donnent $s=1$ et $t=2$, et enfin

$$u=(X+3)(X^2+X+1)(X^2+X+2).$$

5. Soit z une racine de $f(X)=X^5+X+6$. Alors z n'est pas nul et vérifie $\dfrac{1}{z^4}+\dfrac{6}{z^5}=-1$. La minoration $|z|\geq\dfrac{3}{2}$ entraine alors

$$1=\left|\frac{1}{z^4}+\frac{6}{z^5}\right|\leq\left|\frac{1}{z^4}\right|+\left|\frac{6}{z^5}\right|\leq\frac{2^4}{3^4}+\frac{6\times 2^5}{3^5}=\frac{240}{243}<1,$$

ce qui est faux. Donc $|z|<1.5$.

6. Rappelons que, pour p premier, et $n\geq 2$, l'anneau des polynnômes à coefficients dans $(\mathbb{Z}/p^n\mathbb{Z})$ n'est pas un anneau factoriel, c'est à dire qu'il existe des polynômes admettant deux décompositions en produit d'irréductibles. Il suffit de considérer par exemple, les deux décompositions suivantes dans $(\mathbb{Z}/4\mathbb{Z})[X]$

$$X^2=(X-2)(X+2).$$

Cependant, le théorème de Hensel dit que si F est un polynôme unitaire de $(\mathbb{Z}/p^n\mathbb{Z})[X]$, qui, lorsque on le considère comme un polynôme de $\mathbb{F}_p[X]$ est sans facteur carré, alors f admet une unique décomposition en produit d'irréductibles dans $(\mathbb{Z}/p^n\mathbb{Z})[X]$. Le polynôme $f(X)=X^5+X+6$ a pour image dans $\mathbb{F}_5[X]$ le polynôme u étudiie dans le questions précédentes, qui est sans facteur carré dans $\mathbb{F}_5[X]$. Par le lemme de Hensel f admet une unique factorisation en produit d'irréductibles modulo 25, et, de plus cette décomposition est un relèvement de la décomposition dans $\mathbb{F}_5[X]$, $u=(X-2)(X^2+X+1)(X^2+X+2)$ c'est à dire de la forme

$$X^5+X+6=(X-2-5\lambda)(v+1+5A)(v+2+5B)$$

avec $\lambda\in\mathbb{Z}/25\mathbb{Z}$, $\deg(A),\deg(B)\leq 1$. On vérifie que le seul élément $2+5\lambda$ dans $\mathbb{Z}/25\mathbb{Z}$ qui annule f est 12. Le facteur de degré 1 est donc $X-12$. On effectue alors le quotient de f par $X-12$ modulo 25. On trouve

$$X^4+12X^3-6X^2+3X+12.$$

D'où l'équation modulo 25

$$\begin{aligned} X^4+12X^3-6X^2+3X+12 &\equiv (X^2+X+1+5A)(X^2+X+2+5B) \\ &\equiv X^4+2X^3+4X^2+3X+2+5A(v+2)+5B(v+1) \pmod{25}. \end{aligned}$$

Après simplification, et division par 5 des deux membres, cette équation équivaut à

$$2X^3 - 2X^2 + 2 \equiv A(v+2) + B(v+1) \pmod 5,$$

qui, vu $(v+2) - (v+1) = 1$, admet la solution

$$A = 2X^3 - 2X^2 + 2, \quad B = -2X^3 + 2X^2 - 2.$$

Ce couple (A, B) ne vérifie pas la condition des degrés $\deg(A) \leq 1$, $\deg(B) \leq 1$. Pour y remédier on effectue la division euclidienne (dans $\mathbb{F}_5[X]$),

$$2X^3 - 2X^2 + 2 = (X^2 + X + 1)(2X + 1) + 2X + 1,$$

on remplace A par $2X + 1$, et B par $B + (X^2 + X + 2)(2X + 1)$. Cela donne

$$A = 2X + 1, \quad B = -2X^3 + 2X^2 - 2 + 2X^3 + 3X^2 + 5X + 2 = 0 \pmod 5,$$

et enfin la factorisation modulo 25 de f

$$X^2 + X + 6 = (X - 12)(X^2 + 11X + 6)(X^2 + X + 2).$$

7. Supposons f réductible dans $\mathbb{Z}[X]$. Comme f n'a pas de racine entière (par la question (5) une telle racine serait dans $\{-1, 0, 1\}$), il n'admet pas de facteur de degré 1 et sa décomposition est nécessairement de la forme $f = gh$, avec g et h unitaires, $\deg(g) = 2$, et $\deg(h) = 3$,

$$g = x^2 + \tau_1 x + \tau_2, \qquad h = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3.$$

En tenant compte de ce ques les racines de g et h sont plus petites que 1.5 en valeur absolue, et que les τ_i et σ_i sont des entiers, les expressions des τ_i et des σ_i au moyen des fonctions symétriques élémentaires des racines donnent

$$|\tau_1| \leq 2,\ |\tau_2| \leq 2, \qquad |\sigma_1| \leq 4,\ |\sigma_2| \leq 6,\ |\sigma_3| \leq 3.$$

Les coefficients de g et h sont donc tous majorés en valeur absolue par 6, et à fortiori par 12. Cette décomposition $f = gh$ dans $\mathbb{Z}[X]$ fournit ainsi une décomposition en deux facteurs de f dans $(\mathbb{Z}/25\mathbb{Z})[X]$ (en représentant chaque classe de $\mathbb{Z}/(25\mathbb{Z})$ par son unique représentant appartenant à l'intervalle $[-12, +12]$). Or, par le lemme de Hensel, une telle décomposition s'obtient en regroupant en deux classes les 3 facteurs irréductibles $X - 12, X^2 + 11X + 6, X^2 + X + 2$ de la décomposition obtenue à la question précédente. Il n'y a que deux possibilités qui sont

$$g = X^2 + X + 2, \qquad h = (X - 12)(X^2 + 11X + 6) = X^3 - X^2 - X + 3$$

ou bien

$$g = X^2 + 11X + 6, \qquad h = (X - 12)(X^2 + X + 2) = X^3 - 11X^2 - 10X + 1.$$

Aucun de ces deux choix ne fournit une décomposition de f en un produit de deux facteurs dans $(\mathbb{Z}/25\mathbb{Z})[X]$. La contradiction obtenue prouve l'irréductibilité de f dans $\mathbb{Z}[X]$.