Ens-Lyon. Licence Informatique

Calcul formel et cryptographie
Corrigé du contrôle du vendredi 2 juin 2006

Exercice 1

1. Puisque $n-1-(p-1) = p(q-1)$ est un multiple de d, la congruence $b^d \equiv 1 \bmod n$ implique $b^{n-1} \equiv 1 \bmod n$.
2. Réciproquement si $b^{n-1} \equiv 1 \bmod n$, on a a fortiori

$$b^{n-1} \equiv 1 \bmod p \tag{1}$$

. Cela implique que b est premier avec p, et, par le théorème de Fermat, on a aussi

$$b^{p-1} \equiv 1 \bmod p. \tag{2}$$

Les équations (1) et (2) expriment que l'ordre de b modulo p, $O_p(b)$ est un diviseur de $n-1$ et aussi un diviseur de $p-1$. C'est donc un diviseur de

$$\mathrm{pgcd}(n-1, q-1) = \mathrm{pgcd}(p-1+p(q-1), q-1) = \mathrm{pgcd}(p-1, q-1) = d.$$

Ainsi $b^d = 1 \bmod p$. On démontre de la même façon que $b^d = 1 \bmod q$. Ainsi $b^d - 1$ est donc un multiple de p et q, donc un multiple de n.

3. Écrivons $p-1 = dp_1$. Soit g un générateur du groupe multiplicatif $\mathbb{F}_p^\star$. Tout élément x de $\mathbb{F}_p^\star$ s'écrit de manière unique $x = g^a$, avec $0 \leq a < p-1$. Un tel élément satisfait $x^d = 1$ si et seulement si $g^{ad} = 1$, c'est à dire si ad est un multiple de $p-1 = dp_1$, donc si et seulement si a est un multiple de p_1. Le nombre des multiples de p_1 qui sont plus petits que $p-1$ est $(p-1)/p_1 = d$.
4. Par définition b est un faux témoin de primalité de n si $b^{n-1} \equiv 1 \bmod n$. Par le (a) ceci équivaut à $b^d \equiv 1 \bmod n$. Par le théorème des restes chinois tout $b \in \mathbb{F}_p^\star$ est uniquement déterminé par les deux entiers u et v, $0 \leq u < p$ et $0 \leq v < q$ tels que $b \equiv u \bmod p$, et $b \equiv v \bmod q$. Pour que $b^d \equiv 1 \bmod n$, il faut et il suffit que

$$u^d \equiv 1 \bmod p, \qquad v^d \equiv 1 \bmod q.$$

Par la question précédente il y a d choix convenables de u et d choix pour v d'où $d \times d = b^2$ choix pour b.

5. Si $q = 2p + 1$, on a

$$d = (p-1, q-1) = (p-1, 2p) = (p-1, 2p-2(p-1)) = (p-1, 2) = \begin{cases} 2 \text{ si } p \text{ est imapir} \\ 1 \text{ si } p = 2. \end{cases}$$

Le nombre de faux témoins de primalité est donc $d^2 = 4$ si p est impair et $d^2 = 1$ si $p = 2$ (et, dans ce cas $n = 10$).

6. Si $q = 2p - 1$, on a

$$d = (p - 1, q - 1) = (p - 1, 2p - 2) = p - 1.$$

Le nombre de faux témoins de primalité est donc $d^2 = (p - 1)^2$. Le nombre des b premiers avec n jusqu'à n est $\varphi(n) = (p - 1)(q - 1) = 2(p - 1)^2$. La proportion de faux témoins de primalité de n est donc $(p - 1)^2/2(p - 1)^2 = 1/2$.

Exercice 2

1. Le développement en série entière de $x^{k-1}/(1 - x^8/16)$ est

$$x^{k-1} \frac{1}{1 - \frac{x^8}{16}} = x^{k-1} \sum_{n=0}^{\infty} \frac{x^{8n}}{16^n} = \sum_{n=0}^{\infty} \frac{x^{8n+k-1}}{16^n}$$

Cette série entière est intégrable terme à terme sur $[0, 1]$. On en déduit

$$I_k = \int_0^1 \sum_{n=0}^{\infty} \frac{x^{8n+k-1}}{16^n} = \sum_{n=0}^{+\infty} \frac{1}{16^n} \int_0^1 x^{8n+k-1} dx = \sum_{n=0}^{\infty} \frac{1}{16^n} \frac{1}{8n + k}. \tag{3}$$

2. (a) Par le théorème de Minkowski, $\lambda_1(L) \leq \gamma_n \det(L) \leq \sqrt{(n)} \det(L)$. Ici la dimension de L est $n = 9$, et $\det(L) = J_9 = \text{round}(10^{13}\pi)$. On obtient donc

$$\lambda_1(L) \leq 3(10^{13}\pi)^{1/9} \leq 94.8$$

   (b) Par le théorème 10.18, point (3) du cours, avec un réseau de dimension $n = 9$ on peut affirmer que $\|Y_1\|_\infty \leq 2^{(9-1)/2} \lambda_1(L) = 16\lambda_1(L) \leq 1517$

3. Puisque la longueur de $Y_1 = Y_1^\star$ est la plus courte des longueurs des $Y_j^\star$ par le théorème 10.9, $\lambda_1(L) = \|Y_1\|_\infty$.

4. En utilisant (3) l'équation $\pi = 4I_1 - 2I_4 - I_5 - I_6$ se réecrit

$$\pi = \sum_{n=0}^{+\infty} \left(\frac{4}{8n + 1} - \frac{2}{8n + 4} - \frac{1}{8n + 5} - \frac{1}{8n + 6} \right) \frac{1}{16^n}.$$

5. Il faut prouver que

$$4I_1 - 2I84 - I_5 - I6 = \int_0^1 \frac{4 - 2t^3 - t^4 - t^5}{1 - \frac{1}{16}t^8} = \pi.$$

En utilisant la décomposition de l'énoncé

$$\begin{aligned}\int_0^1 \frac{4 - 2t^3 - t^4 - t^5}{1 - \frac{1}{16}t^8} &= -\int_0^1 \frac{4t}{2 - t^2}dt + \int_0^1 \frac{8 - 4t}{t^2 - 2t + 2}dt \\ &= -2\log 2 + \int_0^1 \frac{4(1-t)+4}{(1-t)^2+1}dt = -2\log 2 + 2\log 2 + \pi = \pi.\end{aligned}$$

Exercice 3

1. Pour $b = 0$, $u = X^5 - 1 = (X-1)^5$ (car, en caractéristique 5, l'élevation à la puissance 5^{iem} est additive).
2. Puisque tout $x \in \mathbb{F}_5$ satisfait $x^5 = x$, la fonction polynôme associée à u est $x \mapsto (b+1)x + 1$. Si $b = -1$ c'est la focntion constante 1, sinon elle s'annule une fois en $1/(b+1)$.
3. La colonne j de la matrice de Berlekamp Q est formée des cordonnées de $\overline{X}^j$ dans la base canonique $(\overline{1}, \overline{X}, \overline{X}^2, \overline{X}^3, \overline{X}^4)$ de $F_5[X]/(u)$. En calculant

$$\begin{aligned}1 &\equiv 1 \bmod u \\ X^5 &\equiv -bX + 1 \bmod u \qquad (4) \\ X^{10} &\equiv (bX-1)^2 \equiv b^2X^2 - 2bX + 1 \bmod u \qquad (5) \\ X^{15} &\equiv (-bX+1)^3 \equiv -b^3X^3 + 3b^2X^2 - 3bX + 1 \bmod u \\ X^{20} &\equiv (-bX+1)^4 \equiv b^4X^4 - 4b^3X^3 + 6b^2X^2 - 4bX + 1\end{aligned}$$

on obtient

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & -b & -2b & -3b & -4b \\ 0 & 0 & b^2 & 3b^2 & b^2 \\ 0 & 0 & 0 & -b^3 & -4b^3 \\ 0 & 0 & 0 & 0 & b^4 \end{pmatrix} \qquad Q - \mathrm{Id} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & -b-1 & -2b & -3b & -4b \\ 0 & 0 & b^2-1 & 3b^2 & b^2 \\ 0 & 0 & 0 & -b^3-1 & -4b^3 \\ 0 & 0 & 0 & 0 & b^4-1 \end{pmatrix}$$

4. Si $b = -1$, la matrice $Q - \mathrm{Id}$ est

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & -2 & 2 & 3 & 4 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

En ajoutant la première ligne à la seconde on voit immédiatement que cette matrice est de rang 4. Son noyau est de dimension 1, et par le théorème de Berlekamp u est irréductible.

5. Lorsque $b = 1$,e n utilisant (5) et (4), (avec $b-1$) pour réduire X^{10} et X^5 modulo u, on obtient

$$\begin{aligned} v(X)^5 &= (X^2 - X)^5 = X^{10} - X^5 \\ &\equiv X^2 - 2X + 1 - (-X + 1) \pmod{u} \\ &\equiv X^2 - X \pmod{u}, \end{aligned}$$

soit $v^5 \equiv v \pmod{u}$. Le polynôme u divise donc

$$v^5 - v = v(v-1)(v-2)(v-3)(v-4).$$

Chaque facteur irréductible w de u divise l'un des $v - s$. Si w est de degré 2 il coïncide avec $v - s$, puisque $v - s$ est aussi de degré 2.

6. Par la première question u admet une unique racine dans $\mathbb{F}_5$ qui est $1/(b+1) = 1/2 = 6/2 = 3$. Le polynôme u est donc le produit d'un unique facteur de degré 1, $X - 3$, et de deux facteurs de degré 2, qui, par la question précédentes sont de la forme $v - c$, et $v - d$, avec $c, d \in \mathbb{F}_5$. Donc

$$\begin{aligned} u = (X-3)(X^2 - X + c)(X^2 - X + d) & \\ = X^5 + (c + d + 2)X^3 + \cdots + 2cd. & \quad (6) \end{aligned}$$

En écrivant que le coefficient de X^3 est nul, et que le terme constant est -1 on obtient

$$c + d = -2 = 3, \quad 2cd = -1 = 4.$$

Les nombres c et d sont donc les racines de l'équation du second degré

$$z^2 - 2z + 2 = 0,$$

c'est à dire la paire $(1, 2)$. D'où la factorisation

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

7. Si $|z| > 3/2$, on a $|z^4| > 81/16 > 5$, et donc

$$z^5 + z = \left|z^5\right| \left|1 + \frac{1}{z^4}\right| > \frac{243}{32}(1 - 1/5) = \frac{243}{32}\frac{4}{5} = \frac{243}{40} > 6.$$

Si donc $|z| > 1.5$ on a $|z^5 + z| > 6$, ce qui implique $z^5 + z + 6 \neq 0$.

8. Soit $w = X^2 - sx + p \in \mathbb{Z}[X]$ un diviseur unitaire de degré 2 de $X^5 + X + 6$. Alors $s = z_1 + z_2$ et $p = z_1 z_2$, où z_1 et z_2 sont les racines (dans $\mathbb{C}$) de w. Par la question précédente

$$|s| = |z_1 + z_2| \leq |z_1| + |z_2| < 1.5 + 1.5 = 3, \qquad |p| = |z_1|\, z_2 < (1.5)^2 < 2.25.$$

Puisque s et p sont entiers, ils sont majorés par 2.

9. Puisque $6 \equiv 1 \bmod 5$, on a, modulo 5,

$$(X^5 + X - 6) \equiv (X + 2)(X^2 - X + 1)(X^2 - X + 2).$$

Soit $u = AB$ une factorisation de $X^5 + X - 6$ en deux polynômes de $\mathbb{Z}[X]$, non constants, et, necessairement unitaires, avec $\deg A \leq \deg B$. Alors, modulo 5,

$$AB \equiv (X - 2)(X^2 - X + 1)(X^2 - X + 2).$$

Soit, dans $\mathbb{F}_5[X]$,

$$\overline{A}\,\overline{B} = \overline{X - 2}\,\overline{X^2 - X + 1}\,\overline{X^2 - X + 2}.$$

Par unicité de la décomposition en facteurs premiers dans $\mathbb{F}_5[X]$, l'une des trois congruences modulo 5

$$A \equiv X - 1, \quad A \equiv X^2 - X + 1, \quad A \equiv X^2 - X + 2,$$

est vraie. Puisque les coefficients de A sont majorés par 2, si l'une de ces congruences est vraie, c'est une égalité. Autrement dit, si $X^2 + X + 6$ admet une décomposition non triviale dans $\mathbb{Z}[X]$ l'un des facteurs est $X - 2$ ou $X^2 - X + 1$ ou $X^2 - X + 2$. Il suffit de tester la divisibilité par chacun de ces trois polynômes. Seul le dernier divise $X^5 + X - 6$, et cela donne la factorisation

$$X^5 - X + 6 = (X^2 - X + 2)(X^3 - X^2 - X + 3).$$