Université Lyon 1 et ENS Lyon
Magistère MIM
2001/2002

10 janvier 2002
durée 3 heures

Calcul formel et Cryptographie

Les deux parties A et B sont indépendantes; à l'intérieur de chaque partie toute question peut être traitée en admettant le résultat des précédentes.
Les calculettes et les notes de cours sont autorisées.

A

On notera $(v_n)_{n\geq 0}$ la suite de Fibonacci privée de ses deux premiers termes, c'est-à-dire la suite définie par

$$v_0 = 1; \quad v_1 = 2; \quad v_{n+2} = v_{n+1} + v_n$$

dont les premiers termes sont $1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$

On dit que l'entier m admet une représentation de Fibonacci (ou F-représentation) lorsqu'il peut s'écrire sous la forme $m = \sum_{k=0}^{n} a_k v_k$ où les coefficients a_k valent 0 ou 1. On notera cette écriture $\overline{a_n a_{n-1} \ldots a_1 a_0}$, avec, par convention, $a_n = 1$. Ainsi, la représentation $1 + 3 + 5 + 21$ du nombre 30 se notera $\overline{1001101}$.

On appelle représentation de Zeckendorff (ou Z-représentation) toute représentation de Fibonacci de m où n'apparaissent pas deux nombres consécutifs de la suite v_n; autrement dit, dont l'écriture ne comporte pas deux chiffres 1 consécutifs. Ainsi, $\overline{1001101}$ n'est pas une Z-représentation du nombre 30. En revanche, $\overline{1010001}$ en est une.

1. Donner toutes les F-représentations du nombre 37, en précisant pour chacune si elle est ou non une Z-représentation.

2. Soit n un entier naturel et $s = \lfloor \frac{n}{2} \rfloor$ la partie entière de $n/2$. On pose

$$\sigma_n = \sum_{k=0}^{s} v_{n-2k}; \qquad S_n = \sum_{k=0}^{n} v_k.$$

   Montrer que, pour $n \geq 0$, on a $\sigma_n = v_{n+1} - 1$ et $S_n = v_{n+2} - 2$.

3. Soit $m = \sum_{k=0}^{n} a_k v_k$ une Z-représentation de m avec $a_n = 1$.

   (a) Prouver l'inégalité $m \leq \sigma_n$.

(b) En déduire que v_n est le plus grand des nombres de Fibonacci qui sont inférieurs ou égaux à m.

4. (a) Prouver que tout entier m admet une unique Z-représentation et donner un algorithme permettant de calculer la Z-représentation d'un entier m donné (on supposera que la suite v_n est connue).

   (b) Application numérique : donner la Z-représentation du nombre 272.

   (c) Donner pour tout n la Z-représentation des nombres v_n, σ_n et S_n.

5. Montrer que, pour tout $n \geq 0$, on a

$$v_n = \left(\frac{5+3\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{5-3\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

6. On note $z(m)$ le nombre de chiffres de la Z-représentation du nombre m, et $b(m)$ celui de son écriture binaire.

   (a) En utilisant la valeur de v_n donnée à la question précédente, donner un équivalent simple de $z(m)$ lorsque $m \to \infty$

   (b) Etudier le comportement du rapport $z(m)/b(m)$ lorsque $m \to \infty$.

B

1. (a) Soit K un corps, a et b deux entiers positifs. On écrit $a = bq + r$ la division euclidienne de a par b. Montrer que, dans la division euclidienne (dans $K[X]$) de $X^a - 1$ par $X^b - 1$, le reste est $X^r - 1$; quel est le quotient? En déduire que $\text{pgcd}(X^a - 1, X^b - 1) = X^{\text{pgcd}(a,b)} - 1$.

   (b) Soit m un entier positif. Soit $S(X) \in \mathbb{F}_2[X]$, de degré strictement inférieur à m. Montrer que les coefficients dans le développement en série entière sur $\mathbb{F}_2$ de la fraction

$$\frac{S(X)}{1+X^m} = c_0 + c_1 X + c_2 X^2 + \ldots$$

   sont périodiques et vérifient $c_{n+m} = c_n$ pour tout $n \geq 0$.

   (c) Soit $k \geq 1$ et $m_1, m_2, \ldots, m_k$ des entiers positifs. Soit $h = h(k)$ défini par $2^{h-1} < k \leq 2^h$. On pose $\omega = \text{ppcm}(m_1, m_2, \ldots, m_k)$ et $\Omega = 2^h\omega$. Montrer que le polynôme $(1+X^{m_1})(1+X^{m_2})\ldots(1+X^{m_k})$ divise $1 + X^\Omega = (1+X^\omega)^{2^h}$ dans $\mathbb{F}_2[X]$. Soit $S(X) \in \mathbb{F}_2[X]$, de degré inférieur à $m_1 + m_2 + \ldots + m_k$; montrer que les coefficients dans le développement en série entière sur $\mathbb{F}_2$ de la fraction

$$\frac{S(X)}{(1+X^{m_1})(1+X^{m_2})\ldots(1+X^{m_k})} = c_0 + c_1 X + c_2 X^2 + \ldots$$

   vérifient $c_{n+\Omega} = c_n$ pour tout $n \geq 0$.

(d) Soit une suite d'éléments de $\mathbb{F}_2$: $a_0, a_1, a_2, \dots$ qu'on suppose périodique de période M (c'est-à-dire que $a_{n+M} = a_n$ pour tout $n \geq 0$). On désigne par W_a le nombre de 1 parmi $a_0, a_1, a_2, \dots a_{M-1}$, et par $\delta_a = W_a/M$ la densité des 1 dans la suite (a_n). Soit une autre suite d'éléments de $\mathbb{F}_2$: $b_0, b_1, \dots$ de période N et de densité δ_b. Dans $\mathbb{F}_2$, on pose $c_n = a_n + b_n$. Montrer que, si M et N sont premiers entre eux, la suite c_n est périodique de période MN et que l'on a

$$\delta_c = \delta_a + \delta_b - 2\delta_a\delta_b = \frac{1}{2} - 2\left(\delta_a - \frac{1}{2}\right)\left(\delta_b - \frac{1}{2}\right).$$

Montrer que $\left|\delta_c - \frac{1}{2}\right| \leq \min\left(\left|\delta_a - \frac{1}{2}\right|, \left|\delta_b - \frac{1}{2}\right|\right)$.

2. (a) Soit $p \geq 3$ un nombre premier. Montrer que, si p ne divise pas n, les polynômes de $\mathbb{F}_2[X]$:

$$\Phi_p(X) = 1 + X + X^2 + \dots + X^{p-1} = \frac{1 - X^p}{1 - X} = \frac{1 + X^p}{1 + X}$$

et $1 + X^n$ sont premiers entre eux dans $\mathbb{F}_2[X]$.

(b) Pour s entier positif, on pose

$$E_s(X) = (1 + X)(1 + X^2) \dots (1 + X^s) \in F_2[X]$$

et

$$G(X) = \frac{E_{p+1}(X)}{\Phi_p(X)} = E_{p-1}(X)(1 + X)(1 + X^{p+1}).$$

Montrer que les polynômes Φ_p et G sont premiers entre eux dans $\mathbb{F}_2[X]$ et que l'on a la décomposition en éléments simples

$$\frac{1}{E_{p+1}(X)} = \frac{U(X)}{G(X)} + \frac{V(X)}{\Phi_p(X)}$$

où $U(X), V(X) \in \mathbb{F}_2[X]$ vérifient $\deg(U) < \deg(G)$ et $\deg(V) \leq p - 2$.

(c) On considère le développement en série entière de la fraction rationnelle $\dfrac{V(X)}{\Phi_p(X)} = v_0 + v_1X + v_2X^2 + \dots$ avec $v_n \in \mathbb{F}_2$. Montrer que les coefficients v_n sont de période p; autrement dit que $v_{n+p} = v_n$ pour tout $n \geq 0$.

(d) On considère le développement en série entière de la fraction rationnelle $\dfrac{U(X)}{G(X)} = u_0 + u_1X + u_2X^2 + \dots$ avec $u_n \in \mathbb{F}_2$. Montrer que les coefficients u_n sont périodiques de période non multiple de p; autrement dit qu'il existe Ω non multiple de p tel que $u_{n+\Omega} = u_n$ pour tout $n \geq 0$.

3. On considère l'anneau $\mathcal{A}_p = \mathbb{F}_2[X]/(1+X^p)$. Un élément de $\mathcal{A}_p$ est un polynôme $A(X)$ de degré $d \leq p-1$ à coefficients 0 ou 1. L'addition (resp. la multiplication) de deux éléments de $\mathcal{A}_p$ est l'addition (resp. la multiplication) dans $\mathbb{F}_2[X]$, modulo $1+X^p$.

   (a) Pour s entier vérifiant $1 \leq s \leq p-1$, on pose $F_s(X) = E_s(X) \bmod 1+X^p \in \mathcal{A}_p$ où E_s a été défini en 2(b). Montrer que $(F_{p-1}(X))^2 = F_{p-1}(X^2) = F_{p-1}(X)$.

   (b) On désignera par J_p le sous ensemble de $\mathcal{A}_p$ formé des polynômes de $\mathcal{A}_p$ qui admettent 1 comme racine; autrement dit, les polynômes $A(X) \in \mathcal{A}_p$ qui s'écrivent $A(X) = (1+X)B(X)$ avec $B(X) \in \mathcal{A}_p$. Montrer que J_p est stable pour l'addition et la multiplication de $\mathcal{A}_p$.

   (c) On pose dans $\mathbb{F}_2[X]$: $\psi_p(X) = 1 + \Phi_p(X) = X + X^2 + \ldots + X^{p-1}$. Montrer que $\psi_p \in J_p$, et que, dans $\mathcal{A}_p$, $(1+X)\psi_p(X) = 1+X$.

   (d) Montrer que pour tout $A \in J_p$, on a $\psi_p A = A$; autrement dit, ψ_p est l'élément unité de J_p.

   (e) On suppose $p \equiv 3 \pmod 4$. Montrer que $1+X$ est inversible dans J_p et que $(1+X)^{-1} = 1 + X^2 + X^4 + \ldots + X^{p-1}$.

   (f) On suppose $p \equiv 1 \pmod 4$. Montrer que $1+X$ est inversible dans J_p et préciser son inverse.

   (g) Montrer que pour n entier, $1 \leq n \leq p-1$, $1+X^n$ est inversible dans J_p. Montrer que F_{p-1} (défini en 3(a)) appartient à J_p, est inversible dans J_p et que $F_{p-1} = \psi_p$.

4. (a) On pose $H(X) = G(X) \bmod 1+X^p$ où $G(X)$ a été défini en 2(b). Montrer que $H(X) \in J_p$ et que $H(X) = (1+X)^2$. Montrer que le polynôme $V(X)$ défini en 2(b) vérifie $(1+X)V(X) \in J_p$ et que, dans J_p, on a $(1+X)V(X) = (1+X)^{-1}$.

   (b) Montrer que le nombre de 1 parmi $v_0, v_1, \ldots, v_{p-1}$ (où les v_i ont été définis en 2(c)) vaut $(p \pm 1)/2$.

   (c) Soit E_{p+1} comme dans 2(b), et le développement en série entière de $1/E_{p+1}$ sur $\mathbb{F}_2$:

$$\frac{1}{E_{p+1}(X)} = \frac{1}{(1+X)(1+X^2)\ldots(1+X^{p+1})} = e_0 + e_1 X + e_2 X^2 + \ldots$$

   Montrer que la suite e_n est périodique et que sa densité δ_e vérifie $|\delta_e - 1/2| \leq 1/2p$.