Arithmétique - L3 - MI
Contrôle n°3 - 2010
CORRIGE

Question

Soit $f \in \mathbb{F}_2[x]$ le polynôme défini par

$$f = x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + 1.$$

1. Dérouler l'algorithme de Berlekamp afin de déterminer un facteur non trivial g de f dans $\mathbb{F}_2[x]$.
   Effectuer dans sage :

```
A=GF(2)['x']
x=A.gen()
f=x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + 1
d=f.degree()
r=[]
for i in range(d):
  r.append(list(x^(2*i)%f+x^d)[:d])
Q=matrix(r)
I=identity_matrix(GF(2),d)
V=(Q-I).left_kernel()
```

   et on obtient que le noyau à gauche de la matrice

$$Q - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

   est

$$V = \mathrm{RowSpan}_{\mathbb{F}_2} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   La dernière ligne est une solution non triviale de $b(I-Q) = 0$ et correspond au polynôme k suivant

```
k=A(list(V[2]))
```

i.e., $k = x^8 + x^7 + x^6 + x^5 + x^3 + x^2$. Le polynôme f divise bien $k^2 - k$. En effet, $k^2 - k = f\ell$, où $\ell = x^7 + x^6 + x^5 + x^4 + x^3 + x^2$. D'après Berlekamp, les polynômes

```
g=gcd(k,f)
h=gcd(k+1,f)
```

fournissent une factorisation $f = gh$ non triviale de f. En effet,

$$g = x^5 + x^3 + 1, \; h = x^4 + x^3 + 1, \text{ et } gh = x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + 1 = f.$$

2. Montrer que g et le quotient $h = f/g$ sont irréductibles

   Notons tout d'abord que ni g ni h n'ont des racines dans $\mathbb{F}_2$. Si h était réductible, h serait le produit de deux polynômes de degré 2 sans racine dans $\mathbb{F}_2$. Or, le seul polynôme dans $\mathbb{F}_2[x]$ de degré 2 qui n'a pas de racine est $x^2 + x + 1$. Comme

   $$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq h,$$

   h est bien irréductible.

   De même, si g était réductible, g serait le produit d'un polynôme de degré 2 et un de degré 3, tous deux sans racine dans $\mathbb{F}_2$. En particulier, g serait divisible par $x^2 + x + 1$. Or,

   $$g \pmod{x^2 + x + 1} = x + 1 \neq 0.$$

   Par conséquent, g est également irréductible.

3. Quelle est la décomposition en facteurs irréductibles de f ?

   D'après ce que nous venons de voir, $f = gh$ où g et h sont irréductibles. C'est donc la décomposition de f en facteurs irréductibles.