Algorithmique et Programmation
TD n°11 : Factorisation de polynômes

École normale supérieure - Département d'informatique
algoL3@di.ens.fr

2013-2014

Exercice 1 APPLICATION DE L'ALGORITHME DE BERLEKAMP

Factoriser $X^9 + X^6 - X + 1$ sur $\mathbb{F}_3$.

Exercice 2 PGCD HEURISTIQUE

Soient $A, B \in \mathbb{Z}[x]$ des polynômes à coefficient entiers et n un entier. On cherche à montrer le bien-fondé de l'algorithme suivant qui calcule les coefficients $c_i \in \mathbb{Z}$ du PGCD $C = \sum c_i x^i$ de A et B :

$e = PGCD(A(n), B(n))$
$i = 0$
`tant que` $e \neq 0$
    $c_i = e$ `mod` n
    $e = (e - c_i)/n$
    $i = i + 1$
`fin tant que`
`retourner` $\sum c_i x^i$

où a mod b désigne l'unique entier de $]-b/2, b/2]$ congru à a modulo b.

1. On suppose que n est supérieur au double de la norme $|D|_\infty$ de tous les polynômes D qui sont diviseurs à la fois de A et de B (où la norme est définie par $|\sum_i \alpha_i x^i|_\infty = \max_i |\alpha_i|$).
   Montrer que le résultat G de l'algorithme est le PGCD de A et de B si et seulement si G divise A et B.
   Indication : On pourra utiliser (en le démontrant) que si t est un entier racine d'un polynôme $P \in \mathbb{Z}[X]$, alors $|t| \leq |P|_\infty$.
2. Montrer que si $n > 1 + min(|A|_\infty, |B|_\infty)$ et si le résultat G de l'algorithme divise A et B, alors c'est le PGCD de A et de B.
   Indication : On pourra utiliser (sans la démontrer) l'inégalité de Cauchy qui assure que si α est une racine d'un polynôme $P \in \mathbb{C}[X]$, alors
   $$|\alpha| < 1 + \frac{\max(|a_0|, |a_1|, \ldots, |a_{d-1}|)}{|a_d|} \text{ si } P(X) = a_d X^d + \cdots + a_1 X + a_0.$$
3. **[Bonus]** On choisit cette fois A et B primitifs (le PGCD de leurs coefficients est 1) et $n > 1 + 2\min(|A|_\infty, |B|_\infty)$.
   On note $p(G)$ la partie primitive du résultat G retourné par l'algorithme ($p(G)$ est G divisé par le PGCD de ses coefficients).
   Montrer que $p(G)$ est le PGCD de A et B si et seulement si $p(G)$ divise A et B. Peut-on déduire de ce résultat un algorithme effectif ?

Exercice 3 PGCD DE PLUSIEURS POLYNÔMES

Soient $\mathbb{F}$ un corps et $S \subset \mathbb{F}$ un sous-ensemble fini. Soient $f_1, \ldots, f_n \in \mathbb{F}[X]$ de degrés majorés par $d \in \mathbb{N}$. Montrer que l'algorithme probabiliste suivant retourne le PGCD de $f_1, \ldots, f_n$ avec une probabilité minorée par $1 - d/\#S$.

`tirer` $a_3, \ldots, a_n \in S$ `uniformément aléatoirement`
$g \leftarrow f_2 + \sum_{i=3}^{n} a_i f_i$

$h = \gcd(f_1, g)$

`retourner` h

Indication : On montrera d'abord qu'un polynôme $r \in F[X_1, X_2, \ldots, X_n]$ de degré total au plus d a au plus ds^{n-1} racines dans S^n.

Exercice 4 CRITÈRE D'IRRÉDUCTIBILITÉ

Donner un algorithme qui décide si le polynôme $f \in \mathbb{F}_p[X]$ de degré d est irréductible dans $\mathbb{F}_p$ avec au plus $d/2$ calculs de pgcd.

Exercice 5 RECHERCHE DE RACINES

Donner un algorithme qui calcule les racines d'un polynome $f \in \mathbb{F}_p[X]$ dans $\mathbb{F}_p$ en utilisant des calculs de PGCD bien choisis.

Exercice 6 FACTORISATION DANS $\mathbb{Q}[X]$

Soit $P(X) = X^{10} + X + 1$. En utilisant (par exemple) l'algorithme de Berlekamp, nous trouvons que la factorisation de P en facteur irréductibles unitaires sur $\mathbb{F}_p$ pour $p \in \{2, 3, 5\}$ est respectivement :

$$\begin{aligned} P &\equiv (X^3 + X + 1)(X^7 + X^5 + X^4 + X^3 + 1) \mod 2 \\ P &\equiv (X - 1)(X^3 - X^2 - X - 1)(X^6 - X^5 + X^4 - X^3 + X + 1) \mod 3 \\ P &\equiv (X^2 - X + 2)(X^8 + X^7 - X^6 + 2X^5 - X^4 + 2X^2 + 2X - 2) \mod 5. \end{aligned}$$

Que peut-on en déduire sur P dans $\mathbb{Q}[X]$?