École Normale Supérieure **2012-2013**
Département d'Informatique

Algorithmique et Programmation
TD n° 11 : Polynômes

Exercice 1. 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 calcule l'unique entier de $]-b/2, b/2]$ égal 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.
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.
3. On choisit cette fois A et B primitifs (le PGCD de leurs coefficients est 1) et $n > 1+2\min(|A|_\infty, |B|_\infty)$. Peut-on déduire de ce résultat un algorithme effectif ?

Exercice 2. 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} solutions dans S^n.

Exercice 3. 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 4. 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 5. 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 :

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

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

Exercice 6. Considérons le polynôme

$$P(X) = X^6 - 6X^4 - 2X^3 - 7X^2 + 6X + 1.$$

1. Montrer que si $Q \in \mathbb{Z}[X]$ est un polynôme de degré au plus 3 divisant P, alors la valeur absolue des coefficients de Q est au plus 23.
2. En remarquant que la factorisation de P en facteurs irréductibles dans $\mathbb{F}_{47}[X]$ est

   $$P \equiv (X - 22)(X - 13)(X - 12)(X + 12)(X^2 - 12X - 4) \bmod 47$$

   donner la factorisation de P en facteurs irréductibles dans $\mathbb{Z}[X]$.