Université de Bordeaux
Mathématiques

N1MA8W02 – Master
Année 2017–2018

Devoir Surveillé, 7 mars 2018
Durée 1h30.

À la fin de l'épreuve, votre fichier “`votre_nomDS.sage`” ou “`votre_nomDS.sws`” est à envoyer à l'adresse : `arnaud.jehanne@u-bordeaux.fr`

Exercice 1 – [UNE STRATÉGIE ALTERNATIVE POUR LA DIVISION EUCLIDIENNE]
Soit K un corps. pour tout polynôme $F \in K[x]$, et tout entier k, on note

$$\mathrm{rev}_k(F)(x) = x^k F\left(\frac{1}{x}\right).$$

1) Montrer que si $k \geqslant \deg F$, alors $\mathrm{rev}_k(F) \in K[x]$ et que si $k = \deg F$, alors $\mathrm{rev}_k(\mathrm{rev}_k(F)) = F$.

2) On note `Kx` l'anneau $K[x]$. Écrire sur votre fichier sage une fonction `rev(Kx,k,F)` qui rend le polynôme $\mathrm{rev}_k(F)$ si $k \geqslant \deg F$ et "Erreur" sinon. Attention de bien rendre un polynôme. On rappelle que si `A` est un polynôme vu par sage comme un élément de $K(x)$, alors `Kx(A)` sera bien considéré comme un élément de $K[x]$.

3) Soient F et G deux polynômes non nuls de $K[x]$ de degrés respectifs m et n tels que $m \geqslant n$. Soient Q et R le quotient et le reste de la division euclidienne de F par G. Montrer que

$$\mathrm{rev}_m(F) = \mathrm{rev}_{m-n}(Q)\mathrm{rev}_n(G) + x^{m-n+1}\mathrm{rev}_{n-1}(R).$$

4) Montrer que la classe de $\mathrm{rev}_n(G)$ dans $K[x]/(x^{m-n+1})$ est inversible.

5) On rappelle que si A et B sont deux polynômes, la commande `xgcd(A,B)` rend (d, u, v) où $d = \mathrm{pgcd}(A, B)$ et $Au + Bv = d$. Écrire sur votre fichier sage une fonction `Inverse1(A,B)` qui utilise `xgcd` pour rendre un polynôme A^* tel que $AA^* \equiv 1 \mod B$ si A est inversible modulo B et qui rend “Erreur” sinon.

6) On considère l'algorithme suivant.
`Division euclidienne(F,G)`
Entrées : $F, G \in K[x]$ tels que $G \neq 0$, $n \in \mathbb{N} \setminus \{0\}$.
Sorties : le quotient et le reste de la division euclidienne de F par G.
  Si $\deg F < \deg G$, sortir $(0, F)$.
  $(m, n) = (\deg F, \deg G)$
  $G_1 = \mathrm{rev}_n(G)^{-1} \mod x^{m-n+1}$
  $Q_1 = \mathrm{rev}_m(F)G_1 \mod x^{m-n+1}$
  $Q = \mathrm{rev}_{m-n}(Q_1)$
  Sortir $(Q, F - GQ)$

Exécuter cet algorithme “à la main” sur les polynômes de $\mathbb{F}_{17}[x]$ suivants. $F = 5x^5+4x^4+3x^3+2x^2+x$ et $G = x^2+2x+3$. Il n'est pas demandé ici d'implémenter l'algorithme sur machine, mais plutôt de l'exécuter pas à pas, en s'aidant de sage. On indiquera les commandes utilisées et les résultats intermédiaires obtenus.

7) Démontrer que cet algorithme donne bien le resultat annoncé.

8) Répondre à l'une des deux questions suivantes.

a) Quelle est la complexité algébrique du calcul de l'inverse modulaire G_1 en appliquant l'algorithme d'Euclide étendu ?

b) Quelle est la complexité algébrique de la division euclidienne classique de F par G ?

La réponse est la même pour les deux questions. La stratégie proposée ne semble donc pas apporter d'amélioration. Heureusement, l'exercice 2 propose un algorithme plus rapide pour calculer G_1.

Exercice 2 – [INVERSION RAPIDE MODULO x^n]

Soit K un corps. Soient $F \in K[x]$ et n un entier naturel non nul. On suppose que $F(0) = 1$. On sait que dans ce cas, la classe de F dans $K[x]/(x^n)$ est inversible. Cet exercice porte sur un algorithme rapide pour calculer son inverse.

Soit (A_i) la suite définie de la manière suivante.

$$A_0 = 1 \quad , \quad A_{i+1} = 2A_i - FA_i^2 \quad \forall i \geqslant 0.$$

1) Montrer que $FA_i \equiv 1 \mod x^{2^i}$. pour tout $i \geqslant 0$.

2) En déduire un algorithme pour calculer l'inverse de F modulo x^n et écrire la fonction correspondante `Inverse2(n,F)` sur votre fichier sage. On s'efforcera d'optimiser la complexité de cette fonction.

3) On suppose que la complexité algébrique de la multiplication de deux polynômes de $K[x]$ de degrés inférieurs à un entier N est en $O(N \log N)$. On rappelle que prendre le reste de la division d'un polynôme par x^N revient à tronquer le polynôme : on ne prend pas cette opération en compte dans le calcul de la complexité algébrique.

Soient $C(n)$ la complexité algébrique de `Inverse2(n,F)` et $r = \lceil \log n \rceil$ le plus petit entier supérieur ou égal à $\log n$. Montrer que $C(n)$ est en $O(r2^r)$. En déduire que $C(n)$ est en $O(n \log n)$.

Exercice 3 – [DIVISION EUCLIDIENNE RAPIDE]

Écrire sur votre fichier sage une fonction `Division(F,G)` qui en utilisant certaines fonctions des questions précédentes effectue la division euclidienne F par G avec une complexité algébrique en $O(N \log N)$, où F et G sont des polynômes de $K[x]$ de degrés inférieurs à N et tels que $G \neq 0$ (on suppose encore que la multiplication de tels polynômes est en $O(N \log N)$).

Quelques commandes.

Pour définir le corps $K = \mathbb{F}_{17}$: `K=GF(17)`.

Si K est un corps codé par `K`, on définit $K[x]$ par `Kx.<x>=PolynomialRing(K)`

Si A est un polynôme de $K[x]$ considéré par sage comme une fraction rationnelle, alors après la commande `A=Kx(A)`, `A` sera vu par sage comme un polynôme.

Soient A et B sont deux polynômes de $K[x]$.

`xgcd(A,B)` donne $(d, u, v) \in K[x]^3$ où $d = \text{pgcd}(A, B)$ et où $Au + Bv = d$.

`A % B` donne le reste de la division de A par B.