ENS Lyon 2014 - 2015

Préparation à l'agrégation externe Option C

Devoir à la maison - A rendre le Mercredi 22 Octobre 2014

Première partie : Etude analytique de l'algorithme d'Euclide

Pour tous entiers $n, m \in \mathbb{N}^*$, on note $\tau(m, n)$ le nombre de divisions nécessaires dans l'algorithme d'Euclide classique pour calculer le pgcd de m et n en commençant par diviser m par n. On a par exemple $\tau(1, 2) = 2$ et $\tau(2, 1) = 1$.

Exercice 1.1

1. Ecrire un algorithme permettant de calculer $\tau(m, n)$.
2. Désignons par $(F_n)_{n\geq 0}$ la suite de Fibonacci, avec $F_0 = 0$ et $F_1 = 1$.
   (a) A l'aide de l'algorithme précédent, calculer les 50 premières valeurs de $\tau(F_{n+2}, F_{n+1})$.
   (b) Démontrer que pour tout $n \geq 0$, on a $\tau(F_{n+2}, F_{n+1}) = n$.
3. Ecrire un algorithme permettant de vérifier que $\max\{\tau(m, n),\ 0 < m, n < N\}$ est atteint par le couple (F_r, F_{r+1}), où r désigne le plus grand entier tel que l'on ait $F_{r+1} < N$.
4. Tester cet algorithme sur quelques exemples, puis prouver que la propriété énoncée dans la question précédente est effectivement vraie.

Exercice 1.2

Posons $\alpha := \frac{1+\sqrt{5}}{2}$ et $\beta := \frac{1-\sqrt{5}}{2}$.

1. Exprimer F_n en fonction de α et de β.
2. Vérifier que l'on a $|\beta^n| \leq \frac{\sqrt{5}}{2}$.
3. En déduire que F_n est l'entier le plus proche de $\frac{\alpha^n}{\sqrt{5}}$.
4. Démontrer que pour tous entiers m, n vérifiant $0 < m, n < N$, on a
$$\tau(m, n) \leq \frac{\ln(\sqrt{5}N)}{\ln \alpha} .$$
5. Déterminer deux réels a, b (que l'on exprimera avec trois chiffres significatifs) tels que l'on ait numériquement :
$$\forall 1 \leq m, n \leq N - 1,\ \tau(m, n) \leq a + b \ln N .$$

Exercice 1.3

On rappelle que l'on désigne par φ la fonction indicatrice d'Euler. Pour tout entier $n \geq 1$, notons I_n l'ensemble des entiers $k \in \{1, \ldots, n-1\}$ premiers avec n et posons alors
$$T_n := \frac{1}{n}\sum_{k=1}^{n-1} \tau(k, n) \quad \text{et} \quad \tau_n := \frac{1}{\varphi(n)} \sum_{k\in I_n} \tau(k, n) .$$

Si x est un réel quelconque, on pose $T_x := T_{[x]}$ et $\tau_x := \tau_{[x]}$.

1. Représenter les graphes des fonctions T et τ sur le même repère. Que constatez-vous ?
2. Vérifier graphiquement qu'il existe un entier n_0 pour lequel $0,843 \ln x + 1,47 + n_0$ est une bonne approximation de τ_x. Quel est l'ordre de grandeur de n_0 ?

Seconde partie : L'algorithme de Cantor-Zassenhaus

Dans cet exercice, tous les polynômes seront à coefficients dans $\mathbb{F}_p$. On pourra utiliser les polynômes suivants pour tester les procédures proposées :

$P_1(X) = (X-3)^7(X-5)^{16}$; $P_2(X) = (X-2)^2(X-3)^7(X-5)^{49}$; $P_3(X) = (X-2)^{25}(X-3)^7(X-5)^{49}$.

Exercice 2.1 : Réduction au cas des polynômes sans facteur carré

1. Donner une caractérisation des éléments de $\mathbb{F}_p[X]$ dont le polynôme dérivé est nul.
2. Ecrire une procédure prenant en entrée un polynôme $P(X) \in \mathbb{F}_p[X]$ et renvoyant, lorsque le polynôme dérivé de P est nul, un polynôme $R(X) \in \mathbb{F}_p[X]$ tel que l'on ait $P(X) = R(X^p)$.
3. Montrer que tout élément de $\mathbb{F}_p[X]$ peut être écrit de manière unique sous la forme $R(X^{p^k})$ avec $k \geq 0$ entier et $R(X) \in \mathbb{F}_p[X]$ de polynôme dérivé non nul.
4. Ecrire une procédure prenant en entrée un polynôme $P(X) \in \mathbb{F}_p[X]$ et renvoyant le triplet $\left(k, \text{pgcd}(R, R'), \dfrac{R}{\text{pgcd(R, R')}}\right)$ où R et k sont comme dans la question précédente.
5. Déduire de ce qui précède une procédure permettant de décomposer un polynôme de $\mathbb{F}_p[X]$ en produit de puissances p^*-ièmes de polynômes sans facteur carré.
6. Décomposer $X^7 + X^6 - X^5 - X^2 - X + 1$ en produit de polynômes sans facteur carré dans $\mathbb{F}_2[X]$.

Exercice 2.2 : Classement par degré des facteurs irréductibles

Ecrire une procédure qui décompose un polynôme sans facteur carré $P(X) \in \mathbb{F}_p[X]$ sous la forme $\prod_{i \in I} P_i$ où P_i n'admet que des facteurs irréductibles de degré i et qui renvoie aussi les degrés i.

Exercice 2.3 : Aspects probabilistes de l'algorithme

On suppose ici que p est impair et que P est un polynôme de degré $n \geq 1$ sans facteur carré et dont tous les facteurs irréductibles sont de même degré $d < n$. Pour tout polynôme de U degré inférieur ou égal à $n-1$, on introduit les trois polynômes suivants :

$$\tilde{P}_1(X) := \text{pgcd}(P(X), U(X)^{\frac{p^d-1}{2}}+1)\ ,\ \tilde{P}_{-1}(X) := \text{pgcd}(U(X)^{\frac{p^d-1}{2}}-1)\ \text{ et } \tilde{P}_0(X) := \text{pgcd}(P(X), U(X))\ .$$

1. Montrer que pour tout polynôme $R(X) \in \mathbb{F}_p[X]$ et tout entier $k \geq 0$, $X^{p^k} - X$ divise $R(X)^{p^k} - R(X)$.
2. Justifier l'introduction des polynômes $\tilde{P}_1(X)$, $\tilde{P}_{-1}(X)$ et $\tilde{P}_0(X)$.
3. Ecrire une procédure qui tire un tel polynôme U au hasard et renvoie le triplet $(\tilde{P}_1(X), \tilde{P}_{-1}(X), \tilde{P}_0(X))$ qui lui est associé.
4. Supposons que P et U soient premiers entre eux et notons Q un facteur irréductible de P sur $\mathbb{F}_p$. Montrer que Q divise U si et seulement si $U(x)$ est un carré dans $\mathbb{F}_{p^d}$ pour toute racine x de Q.
5. En déduire que si $U \in \mathbb{F}_p[X]$ est un polynôme de degré inférieur ou égal à $n-1$ premier avec P et tiré au hasard, la probabilité qu'aucun des deux polynômes $\tilde{P}_1(X)$ et $\tilde{P}_{-1}(X)$ ne soit un facteur non trivial de P est égale à 2^{1-r} avec $r := \frac{n}{d}$.
6. Exprimer la proportion de polynômes $U \in \mathbb{F}_p[X]$ de degré inférieur ou égal à $n-1$ tels que l'un des polynômes $\tilde{P}_1(X)$, $\tilde{P}_{-1}(X)$ ou $\tilde{P}_0(X)$ soit un facteur non trivial de P.
7. Ecrire une procédure prenant en entrée le polynôme P, les degrés de ses facteurs irréductibles, et un entier $N \geq 0$, et qui tente, dans la limite de N essais, de trouver un facteur non trivial de P par tirage au hasard successif de polynômes $U \in \mathbb{F}_p[X]$ de degré inférieur ou égal à $n-1$.

Exercice 2.4 : Algorithme de Cantor-Zassenhaus

Déduire de ce qui a été fait dans les trois exercices précédents une programmation de l'algorithme de Cantor-Zassenhaus.