École Normale Supérieure **2008-2009**
Département d'Informatique

Algorithmique et Programmation
Examen

Notes de cours autorisées à l'exception de tout autre document.

Le résultat d'une question peut être utilisé dans la suite du problème même si elle n'a pas été résolue.

Durée : 3 heures

Exercice 1. Factorisation dans $\mathbb{Z}$

Soit m un entier ; on note $2 = p_1 < p_2 < \cdots < p_m$ la suite des m plus petits nombres premiers. On rappelle que $p_m \simeq m \ln m$. On dit qu'un entier Y est *m-friable* si sa décomposition en facteurs premiers n'inclut que des p_i pour $i \in \{1, \ldots, m\}$. Un tel nombre s'écrit $Y = p_1^{e_1} \ldots p_m^{e_m}$ pour une suite finie d'exposants $(e_1, \ldots, e_m)$ avec $e_i \geq 0$ pour $i \in \{1, \ldots, m\}$. La recherche des entiers friables est à la base des méthodes les plus efficaces pour factoriser les entiers et le but de l'exercice est, étant donné un entier N, d'étudier un algorithme de génération de nombres m-friables qui soient des carrés modulo N et d'optimiser sa complexité par un choix judicieux de m.

1. Soient m et r deux entiers. Montrer que le nombre de suites finies d'entiers $e = (e_1, \ldots, e_m)$ telles que $e_1 + \cdots e_m \leq r$ est égal au coefficient binomial $\binom{m+r}{r}$.

   Indication : On pourra représenter une telle suite en coloriant les entiers de 1 à $r+m$ en deux couleurs : les e_1 premiers en blanc, suivi d'un noir, suivi de e_2 blancs et ainsi de suite.

2. On suppose r pair. Soit $e = (e_1, \ldots, e_m)$ une suite finie d'entiers telle que $e_1 + \cdots + e_m \leq r$. Montrer que le nombre de façons d'écrire cette suite comme somme terme à terme de deux suites finies $e' = (e'_1, \ldots, e'_m)$ et $e'' = (e''_1, \ldots, e''_m)$ avec $e'_1 + \cdots + e'_m \leq r/2$ et $e''_1 + \cdots + e''_m \leq r/2$ est majoré par $\binom{r}{r/2}$.

3. Soit $N > 2p_m$ un entier impair ; on pose $r = \lfloor \ln N / \ln p_m \rfloor$. Déduire de la question *1* que la probabilité qu'un entier X choisi uniformément aléatoirement dans $[1, N]$ soit m-friable est au moins $(m^r / Nr!)$.

4. On suppose désormais que la décomposition en facteurs premiers de N s'écrit $q_1^{f_1} \ldots q_d^{f_d}$ (avec $f_i > 0$ pour $i \in \{1, \ldots, d\}$) et on définit s comme le plus grand entier pair inférieur ou égal à $\ln N / \ln p_m$ (soit $s = 2\lfloor \ln N / 2 \ln p_m \rfloor$).

   (a) Montrer qu'un entier $Y \in [0, N]$ est un carré modulo N dès que tous les symboles de Legendre $(Y|q_j)$ sont égaux à 1 pour $j \in \{1, \ldots, d\}$.

   (b) Montrer qu'un tel carré modulo N a exactement 2^d racines carrées.

   Indication : On pourra commencer par traiter le cas où tous les exposants f_i sont égaux à 1 et traiter le cas le plus général par une récurrence.

5. À toute suite d'exposants $e = (e_1, \ldots, e_m)$ telles que $e_1 + \cdots + e_m \leq s/2$, on associe l'entier $U(e) = p_1^{e_1} \ldots p_m^{e_m} \bmod N$ et la suite des symboles de Legendre $\lambda(e) = ((U(e)|q_1), \ldots, (U(e)|q_d))$. Montrer que si e' et e'' sont deux suites d'exposants telles que $\lambda(e') = \lambda(e'')$ alors $U(e') \cdot U(e'')$ est un carré modulo N.

6. Pour toute suite $a \in \{-1,+1\}^d$, on note n_a le nombre de suite d'exposants $e = (e_1, \ldots, e_m)$ telles que $e_1 + \cdots + e_m \leq s/2$ et $\lambda(e) = a$. Montrer que le nombre d'entiers $X \in [0, N]$ tel que $X^2 \bmod N$ soit m-friable est minoré par

$$\frac{2^d}{\binom{s}{s/2}} \sum_{a \in \{-1,+1\}^d} (n_a)^2.$$

7. Déduire de ce qui précède que la probabilité qu'un entier $X \in [0, N]$ choisi au hasard produise un carré $X^2 \bmod N$ m-friable est au moins $m^s/Ns!$.
8. Expliquer pourquoi la complexité d'un algorithme qui teste si $X^2 \bmod N$ est m-friable est en $O(m(\ln N)^2)$.
9. On choisit m de sorte que $\ln m = \sqrt{\ln N \ln\ln N}$. Montrer que les quantités $Ns!/m^s$ et $m(\ln N)^2$ sont bornées par une fonction de la forme

$$\exp(O(\sqrt{\ln N \ln\ln N})).$$

En déduire un majorant de la complexité en moyenne qui d'un algorithme qui choisit les valeurs successives de X uniformément aléatoirement dans $[0, N]$ et teste si $X^2 \bmod N$ est m-friable jusqu'à obtenir un succès.

Exercice 2. FACTORISATION DANS $\mathbb{Q}[X]$

Dans cet exercice, nous allons exposer une méthode de factorisation dans $\mathbb{Q}[X]$. Cet algorithme va utiliser l'algorithme de Berlekamp ou tout autre algorithme pour factoriser dans un $\mathbb{Z}/p\mathbb{Z}[X]$ et ensuite on utilisera l'algorithme LLL pour pouvoir à partir d'un facteur irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ obtenir un facteur irréductible dans $\mathbb{Z}[X]$.

Pour tout entier $m \in \mathbb{N}$, on définit la norme $\left\| \sum_{i=0}^{m} a_i X^i \right\|$ d'un polynôme de $\mathbb{Q}[X]$ comme la norme euclidienne du vecteur $(a_0, \ldots, a_m) \in \mathbb{Q}^{m+1}$.

On rappelle l'*inégalité d'Hadamard* qui sera utile pour résoudre de nombreuses questions de l'exercice : la valeur absolue du déterminant d'une matrice carrée réelle $(A_{i,j})_{1 \leq i,j \leq n}$ est inférieur au produit des normes euclidiennes de ses n vecteurs lignes (ou colonnes)

$$|\det((A_{i,j})_{1 \leq i,j \leq n})| \leq \|(A_{1,j})_{1 \leq j \leq n}\| \cdot \|(A_{2,j})_{1 \leq j \leq n}\| \cdots \|(A_{n,j})_{1 \leq j \leq n}\|.$$

1. Montrer comment ramener le problème général de la factorisation dans $\mathbb{Q}[X]$ à la factorisation d'un polynôme de $\mathbb{Z}[X]$ unitaire et sans facteurs carrés.
2. Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ un polynôme unitaire sans facteurs carrés de degré n. Montrer qu'il existe un nombre premier p_0 inférieur ou égal à $4n \ln \max_{i \in \{0,\ldots,n\}} |a_i| + 4n \ln n$ tel que $f \bmod p_0$ soit sans facteurs carrés dans $(\mathbb{Z}/p_0\mathbb{Z})[X]$.

   Indication : On pourra utiliser l'inégalité d'Hadamard et le théorème des nombres premiers sous la forme $\sum_{p \leq x} \ln p \sim x$ (où la somme est prise sur tous les nombres premiers $p \leq x$).
3. Soient $f, h \in \mathbb{Z}[X]$ de degrés respectifs n et ℓ. Supposons qu'il existe $g \in \mathbb{Z}[X]$ unitaire et non constant qui divise f et h modulo un entier $m \in \mathbb{N}^*$ vérifiant $m > \|f\|^\ell \|h\|^n$. Montrer que le pgcd de f et h n'est pas constant.

4. On désigne par p un nombre premier et k un entier positif et on suppose que f et h vérifient les propriétés suivantes :
   – h est unitaire ;
   – (h mod p^k) divise (f mod p^k) dans $\mathbb{Z}/p^k\mathbb{Z}[X]$;
   – (h mod p) est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$;
   – (h mod p)^2 ne divise pas (f mod p) dans $\mathbb{Z}/p\mathbb{Z}[X]$.

   (a) Montrer que le polynôme f a un facteur irréductible unique au signe près h_0 dans $\mathbb{Z}[X]$ tel que (h mod p^k) divise (h_0 mod p^k) dans $\mathbb{Z}/p^k\mathbb{Z}[X]$.

   (b) Montrer que si $g \in \mathbb{Z}[X]$ divise f dans $\mathbb{Z}[X]$, alors les trois assertions suivantes sont équivalentes :

      i. (h mod p) divise (g mod p) dans $\mathbb{Z}/p\mathbb{Z}[X]$;

      ii. (h mod p^k) divise (g mod p^k) dans $\mathbb{Z}/p^k\mathbb{Z}[X]$;

      iii. h_0 divise g dans $\mathbb{Z}[X]$.

5. Pour la suite, on fixe un entier $m \geq \ell$ et soit Λ l'ensemble des polynômes de $\mathbb{Z}[X]$ de degré inférieur ou égal à m dont l'image canonique dans $\mathbb{Z}/p^k\mathbb{Z}[X]$ est divisible par (h mod p^k).
   Montrer que Λ est un réseau de $\mathbb{R}^{m+1}$ (en identifiant $\sum_{i=0}^{m} a_i X^i$ et $(a_0, \ldots, a_m)$) dont une base est donnée par
   $$\{p^k X^i | 0 \leq i < \ell\} \cup \{hX^j | 0 \leq j \leq m - \ell\}.$$
   En déduire le volume de Λ.

6. Soit $b \in \Lambda$ vérifiant $p^k > \|f\|^{n-1}\|b\|^n$. Montrer que b est divisible par h_0 et que $\operatorname{pgcd}(f, b) \neq 1$.

7. Le but de cette question est de montrer que ce résultat reste vrai si $p^{k\ell} > \|f\|^{n-1}\|b\|^n$.

   (a) Posons $e = \deg g$ et $m' = \deg b$. Posons
   $$M = \{\lambda f + \mu b, \lambda, \mu \in \mathbb{Z}[X], \deg(\lambda) < m' - e, \deg(\mu) < n - e\}$$
   avec $M \subset \mathbb{Z} + \mathbb{Z}X^e + \mathbb{Z}X^{e+1} + \cdots + \mathbb{Z}X^{n+m'-e-1}$ et posons M' la projection de M sur $\mathbb{Z}X^e + \mathbb{Z}X^{e+1} + \cdots + \mathbb{Z}X^{n+m'-e-1}$. Montrer que M' est un réseau de rang $n + m' - 2e$, dont le volume est strictement inférieur à $p^{k\ell}$.

   (b) Soit $g = \operatorname{pgcd}(f, b)$. Montrer que si h ne divise pas g dans $\mathbb{Z}/p\mathbb{Z}[X]$ alors il existe des polynômes $\lambda_0, \mu_0 \in \mathbb{Z}/p^k\mathbb{Z}[X]$ tels que
   $$\lambda_0 h + \mu_0 g \equiv 1 \bmod p^k.$$

   (c) En déduire que si h ne divise pas g dans $\mathbb{Z}/p\mathbb{Z}[X]$ alors $\{v \in M | \deg(v) < e + \ell\} \subset p^k\mathbb{Z}[X]$.

   (d) En remarquant que M' comme tout sous-réseau de $\mathbb{Z}^{n+m'-e-1}$ admet une base échelonnée, montrer que si h ne divise pas g dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors le volume de M' est supérieur ou égal à $p^{k\ell}$.

   (e) Conclure.

8. Montrer que si $(b_1, \ldots, b_{m+1})$ est une base LLL-réduite de Λ et si
   $$p^{k\ell} > 2^{n(n-1)/2} \binom{n-1}{\lfloor (n-1)/2 \rfloor}^n n^{n/2} \|f\|^{2n-1},$$
   alors :
   – soit $\operatorname{pgcd}(f, b_1)$ est un facteur non trivial de f ;
   – soit f est irréductible dans $\mathbb{Z}[X]$.

9. En déduire un algorithme de factorisation polynomial dans $\mathbb{Q}[X]$.