Algorithmique et Programmation
TD n°7 : Entiers

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

2013-2014

Exercice 1 MULTI-EXPONENTIATION

Soit $\mathbb{G}$ un groupe abéelien (noté multiplicativement). Proposer un algorithme qui étant donnés t éléments $g_1, \ldots, g_t$ du groupe $\mathbb{G}$ et des entiers positifs $n_1, \ldots, n_t$ calcule le produit $g_1^{n_1} \ldots g_t^{n_t} \in \mathbb{G}$ en $O(\ell + 2^t)$ multiplications dans $\mathbb{G}$ (où ℓ est la taille en bits de $\max(n_1, \ldots, n_t)$).

Exercice 2 NOMBRES PSEUDO-PREMIERS DE FERMAT EN BASE a

Soit $a \geq 2$ un entier.

1. Montrer $n = (a^{2p} - 1)/(a^2 - 1)$ est un nombre entier composé si p est un nombre impair.
2. Montrer que si p est un nombre premier ne divisant pas $a^2 - 1$, alors $2p$ divise $n - 1$.
3. En déduire qu'il existe une infinité de nombres pseudo-premiers de Fermat en base a.

Exercice 3 NOMBRES DE FERMAT ET TEST DE PRIMALITÉ DE PÉPIN

1. Soit k un entier positif. Montrer que si l'entier 2^k+1 est un nombre premier alors k est une puissance de 2.

On appelle n-ème nombre de Fermat le nombre $F_n = 2^{2^n} + 1$ pour $n > 0$.

2. Montrer que si F_n est premier, alors un entier g est un générateur de $\mathbb{Z}_{F_n}^*$ si et seulement si

$$\left(\frac{g}{F_n}\right) = -1.$$

   En déduire que si F_n est premier alors 3 est un générateur de $\mathbb{Z}_{F_n}^*$.

3. Montrer que si $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ alors F_n est premier.

Exercice 4 ALGORITHME DE SHANKS

Considérons un groupe multiplicatif cyclique $\mathbb{G}$ engendré par $g \in \mathbb{G}$ d'ordre connu q. Proposer un algorithme de résolution de logarithme discret par compromis temps-mémoire de complexité $O(\sqrt{q})$ opérations de groupe en temps et $O(\sqrt{q})$ éléments de groupe en mémoire.

Indication. On pourra remarquer que pour tout élément $h = g^x \in \mathbb{G}$, l'entier x s'écrit sous la forme $x = x_1 T + x_0$ avec $0 \leq x_1 < T$ et $0 \leq x_2 < T$ pour $T = \lceil \sqrt{q} \rceil + 1$.

Exercice 5 ALGORITHME DE POHLIG-HELLMAN

Soit $\mathbb{G}$ un groupe cyclique d'ordre fini n dont la décomposition en facteurs premiers est connue.

1. Montrer que si $n = pq$ est le produit de nombres premiers distincts p et q alors il existe un algorithme qui résout le problème du logarithme discret dans $\mathbb{G}$ en $O(\sqrt{p} + \sqrt{q} + \log(n))$ multiplications dans $\mathbb{G}$.
2. Montrer que si $n = p^e$ où p est un nombre premier et $e \geq 2$ est un entier alors il existe un algorithme qui résout le problème du logarithme discret dans $\mathbb{G}$ en $O(e(\sqrt{p} + \log(n)))$ multiplications dans $\mathbb{G}$.
3. En déduire que si $n = q_1^{e_1} \cdots q_k^{e_k}$ où les q_i sont des nombres premiers deux à deux distincts), alors il existe un algorithme qui résout le problème du logarithme discret en $O\left(\sum_{i=1}^k e_i(\sqrt{q_i} + \log(n))\right)$ opérations dans le groupe $\mathbb{G}$.

Exercice 6 EXTRACTION DE RACINE CARRÉE MODULO p

Soit p un nombre premier impair.

1. Nous supposons que $p \equiv 3 \bmod 4$. Donner un algorithme de complexité $O(\log^3 p)$ opérations binaires qui, étant donné $\alpha \in \{1, \ldots, p-1\}$ tel que $\left(\frac{\alpha}{p}\right) = 1$, retourne $\beta \in \{1, \ldots, p-1\}$ tel que $\beta^2 \equiv \alpha \bmod p$.

Nous supposons désormais que $p \equiv 1 \bmod 4$. Posons $p = 2^h m + 1$ avec m impair.

2. Donner un algorithme probabiliste qui étant donné p retourne un élément γ de $\{1, \ldots, p-1\}$ tel que $\left(\frac{\gamma}{p}\right) = -1$ en temps espéré $O(\log^2 p)$ opérations binaires. Montrer que pour un tel γ, l'élément $\delta = \gamma^m$ engendre l'unique sous-groupe d'ordre 2^h de $\mathbb{Z}_p^*$.
3. Soit $\alpha \in \{1, \ldots, p-1\}$ tel que $(\alpha|p) = 1$. Montrer que α^m appartient au sous-groupe engendré par δ et en utilisant un algorithme de logarithme discret, en déduire un algorithme pour calculer une racine carré de α^m modulo p.
4. Conclure en donnant un algorithme permettant de calculer les racines carrés de α en temps $O((\log p)^3)$.