Université Paris 8 Année 2021–2022

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Feuille de TD 3

06/10/2021

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/algorithmes-arithmetiques.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

---

Exercice 1. $(\star)$ Test de résiduosité quadratique sur $\mathbb{F}_q$.

Dans cet exercice, on se place dans $\mathbb{F}_q$ avec $q = p^k$ et p impair, et on cherche à tester si un élément $a \in \mathbb{F}_q$ est un carré. Pour cela, on définit la norme d'un élément $x \in \mathbb{F}_q$ comme :

$$N(x) = x \cdot x^p \cdot x^{p^2} \cdot \cdots \cdot x^{p^{k-1}}.$$

Question 1.– Démontrer que $N(x) \in \mathbb{F}_p$ et que N est surjective.

Question 2.– Quelle est la complexité algorithmique du calcul de $N(x)$?

Question 3.– Démontrer que x est un carré dans $\mathbb{F}_q$ si et seulement si $N(x)$ est un carré dans $\mathbb{F}_p$.

Question 4.– En déduire un algorithme simple pour déterminer si x est un carré dans $\mathbb{F}_q$, et en donner la complexité en nombre d'opérations élémentaires sur $\mathbb{F}_p$.

Exercice 2. $(\star\star)$ Calcul d'un carré dans le cas $p \equiv 5 \bmod 8$.

Soit $a \in \mathbb{F}_p$ un carré où p est un nombre premier tel que $p \equiv 5 \bmod 8$. On cherche à calculer efficacement une racine carrée de a dans ce cas spécifique.

On rappelle que le symbole de Legendre $\left(\frac{2}{p}\right)$ est égal à $(-1)^{(p^2-1)/8}$.

Question 1.– Démontrer que $2^{(p-1)/2} = -1$ dans $\mathbb{F}_p$.

Question 2.– En déduire que si a est un carré, alors $a = -4a^3(2a)^{(p-5)/2}$.

On pose maintenant $v = (2a)^{(p-5)/8}$.

Question 3.– Démontrer que -1 est un carré dans $\mathbb{F}_p$ et que $i = 2av^2$ en est une racine carrée.

Question 4.– Démontrer que $a = a^2v^2(1-i)^2$ et en déduire un algorithme pour calculer une racine carrée de a. Donner sa complexité.

Exercice 3. $(\star\star\star)$ 💻 Implantation d'un algorithme d'extraction de racine carrée dans $\mathbb{Z}/N\mathbb{Z}$.

Dans cet exercice, on se propose d'implanter un algorithme générique d'extraction de racine carrée modulo N, où $N = \prod_{i=1}^{k} p_i^{e_i}$ est un entier quelconque ≥ 2.

Question 1.– Implanter un algorithme qui teste si un élément est un carré modulo p (calcul du symbole de Legendre par exemple).

Question 2.– Implanter l'algorithme de Cipolla, qui calcule l'ensemble des racines carrées d'un entier a modulo p, où p est un nombre premier impair.

Question 3.– Implanter un algorithme qui calcule l'ensemble des racines carrées d'un entier modulo p^k, où p est premier et $k \geq 1$. Si on le souhaite, on pourra écrire deux fonctions : l'une pour le cas $p = 2$ et l'autre pour le cas p impair.

Question 4.– Implanter un algorithme qui calcule toutes les racines carrées d'un entier modulo N. On supposera que la factorisation de N est connue et donnée en paramètre de l'algorithme, par exemple sous la forme d'une liste $[(p_i, e_1), (p_2, e_2), \ldots, (p_k, e_k)]$.

Question 5.– Donner une estimation epérimentale de la complexité de vos algorithmes. Commenter.