

## Algorithmes Arithmétiques II – Feuille de TD 3

17/10/2023

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

<https://lvz1.fr/teaching/2023-24/aa.html>

(★) exercice fondamental    (★★) pour s'entraîner    (★★★) pour aller plus loin    ☞ sur machine

**Exercice 1. (★) Test de résiduosit  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   tester si un  l ment  $a \in \mathbb{F}_q$  est un carr . Pour cela, on d finit la norme d'un  l ment  $x \in \mathbb{F}_q$  comme :

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

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

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

**Question 3.**– D montrer que  $x$  est un carr  dans  $\mathbb{F}_q$  si et seulement si  $N(x)$  est un carr  dans  $\mathbb{F}_p$ .

**Question 4.**– En d duire un algorithme simple pour d terminer si  $x$  est un carr  dans  $\mathbb{F}_q$ , et en donner la complexit  en nombre d'op rations  l mentaires sur  $\mathbb{F}_p$ .

**Exercice 2. (★★) Calcul d'une racine carr e modulo  $p$ , pour  $p \equiv 5 \pmod{8}$ .**

Soit  $a \in \mathbb{F}_p$  un carr  o   $p$  est un nombre premier tel que  $p \equiv 5 \pmod{8}$ . On cherche   calculer efficacement une racine carr e de  $a$  dans ce cas sp cifique.

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

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

**Question 2.**– En d duire que si  $a$  est un carr , alors  $a = -4a^3(2a)^{(p-5)/2}$ .

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

**Question 3.**– D montrer que  $-1$  est un carr  dans  $\mathbb{F}_p$  et que  $i = 2av^2$  en est une racine carr e.

**Question 4.**– D montrer que  $a = a^2v^2(1-i)^2$  et en d duire un algorithme pour calculer une racine carr e de  $a$ . Donner sa complexit .

### Exercice 3. (★) □ Implantation de la méthode de Héron.

**Question 1.**– Implantez la méthode de Héron pour le calcul de racines carrées entières.

**Question 2.**– Testez votre implantation, avec en entrée des entiers de taille croissante, en allant jusqu'à plusieurs centaines de bits. Observez-vous des problèmes (boucle infinie, résultat faux)? Commentez si c'est le cas.

### Exercice 4. (★★★) □ Implantation d'un algorithme d'extraction de racine carrée dans

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  $\geq 2$ .

**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  $[(p_1, e_1), (p_2, e_2), \dots, (p_k, e_k)]$ .

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