Université Paris 8 Année 2022–2023

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Solutions feuille de TD 3

06/10/2022

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/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 $\mathbb{F}_p$.

Solutions de l'Exercice 1.

Solution Q1. On a

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

donc $N(x) \in \mathbb{F}_p$. Par ailleurs, on observe que $N : \mathbb{F}_q^\times \to \mathbb{F}_p^\times$ est un morphisme de groupes. En effet,

$$N(xy) = (xy) \cdot (xy)^p \cdot \cdots \cdot (xy)^{p^k-1} = x \cdot x^p \cdot \cdots \cdot x^{p^k-1} \times y \cdot y^p \cdot \cdots \cdot y^{p^k-1} = N(x)N(y)$$

et $N(1) = 1$. Par ailleurs, le nombre d'éléments dans le noyau de N est $|\ker N| \leq \frac{q-1}{p-1}$ car $N(X) - 1$ est un polynôme de degré $\frac{q-1}{p-1}$ sur $\mathbb{F}_q$. Par conséquent,

$$|\mathrm{im} N| = \frac{|\mathbb{F}_q^\times|}{|\ker N|} \geq \frac{q-1}{(q-1)/(p-1)} = p - 1,$$

donc $\mathrm{im} N = \mathbb{F}_q^\times$ en tant que morphisme $\mathbb{F}_q^\times \to \mathbb{F}_p^\times$. Comme $N(0) = 0$, il resulte que N est surjective.

Solution Q2. Le calcul de la norme correspond à $k-1$ multiplications et $k-1$ élévations à la puissance p dans $\mathbb{F}_q$. Notons que $z \mapsto z^p$ est l'automorphisme de Frobenius, donc facilement implantable et très efficace à calculer dans une base *normale* de $\mathbb{F}_q/\mathbb{F}_p$.

On a donc besoin de $O(\log_p q)$ opérations élémentaires dans $\mathbb{F}_q$. Si l'on souhaite une complexité en nombre d'opérations binaires, il faut multiplier par le coût de la multiplication dans $\mathbb{F}_q$, naïvement $O(\log^2 q)$ (mais on peut faire mieux).

Solution Q3. On a

$$x^{(q-1)/2} = (x^{(q-1)/(p-1)})^{(p-1)/2} = N(x)^{(p-1)/2}.$$

On a donc $x^{(q-1)/2} = 1 \iff N(x)^{(p-1)/2} = 1$, autrement dit,

$$x \text{ carré dans } \mathbb{F}_q \quad \iff \quad N(x) \text{ carré dans } \mathbb{F}_p.$$

Solution Q4.

L'algorithme est le suivant :

1. Calculer $n = N(x) \in \mathbb{F}_p$
2. Calculer $b = \left(\frac{n}{p}\right)$
3. Retourner « carré » si $b = 1$ et « non-carré » sinon.

Le calcul du symbole de Jacobi peut se faire à l'aide de l'algorithme d'Euclide, et a une complexité en $O(\log(n)\log(p))$ opérations binaires.

Exercice 2. ($\star\star$) Calcul d'une racine carrée modulo p, pour $p \equiv 5 \bmod 8$.

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.

Solutions de l'Exercice 2.

Solution Q1. On a $2^{(p-1)/2} = -1$ dans $\mathbb{F}_p$ si et seulement si 2 n'est pas un carré dans $\mathbb{F}_p$. On va utiliser le symbole de Legendre $\left(\frac{2}{p}\right)$. Que vaut $(p^2-1)/8$ si $p \equiv 5 \bmod 8$?

$$\frac{(8k+5)^2-1}{8} = \frac{64k^2+80k+25-1}{8} = 8k^2+10k+3\,.$$

Donc $\left(\frac{2}{p}\right) = -1$ et 2 n'est pas un carré dans $\mathbb{F}_p$.

Solution Q2. Si a est un carré, on a $a^{(p+1)/2} = a$ et donc

$$-4a^3(2a)^{(p-5)/2} = -2^{2+(p-5)/2}a^{3+(p-5)/2} = -2^{(p-1)/2}a^{(p+1)/2} = (-1)\times 2^{(p-1)/2}\times a = a$$

où la dernière égalité est déduite de la question 1.

Solution Q3. On a

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$$

donc -1 est un carré.

Par ailleurs, comme a est un carré on a $a^{(p-1)/2} = 1$ donc

$$i^2 = 4a^2v^4 = 2^{2+(p-5)/4}a^{2+(p-5)/4} = -1\times a^{(p-1)/2} = -1$$

Solution Q4. On a $(1-i)^2 = -2i$ et $i = 2av^2$ donc donc

$$a^2v^2(1-i)^2 = a^2v^2 \times (-2) \times 2av^2 = -4a^3v^4 = -4a^3(2a)^{(p-5)/2} = a$$

La dernière égalité provient de la question 3. On a donc exprimé a comme le carré d'un élément de $\mathbb{F}_p$: $av(1-i)$.

Exercice 3. ($\star$) 💻 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.

Solutions de l'Exercice 3.

Voir scripts sur la page web.

Exercice 4. ($\star\star$) 💻 Implantation du calcul du symbole de Jacobi.

Question 1.– Implanter un algorithme qui prend en entrée deux entiers relatifs a et n, et qui calcule le symbole de Jacobi $\left(\frac{a}{n}\right)$.

Question 2.– Estimer la complexité de l'algorithme implanté.

Solutions de l'Exercice 4.

Voir dans un fichier `sagemath` annexe.

Exercice 5. ($\star\star\star$) 💻 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 expérimentale de la complexité de vos algorithmes. Commenter.

Solutions de l'Exercice 5.

Voir dans un fichier `sagemath` annexe.