Université Paris 8 Année 2020–2021

Master Mathématiques et applications

Algorithmes arithmétiques – Devoir à la maison

à rendre pour le dimanche 10 janvier 2021, **dernier délai**

Documents à fournir. Vous devez rendre par email

1. un fichier contenant vos réponses aux questions, qui sera obligatoirement au format `.pdf`,
2. une archive (format `.zip`) contenant vos programmes.

L'email sera adressé à `julien.lavauzelle@univ-paris8.fr` avant le dimanche 10 janvier 2021, 23h59. Au-delà de cette date, le devoir ne sera ni lu ni évalué.

Exercice : algorithme de Tonelli-Shanks

Dans tout l'exercice, on fixe un nombre premier $p \geq 3$. On écrit p sous la forme $p = 2^e n + 1$ où $e \geq 1$ et n est impair.

On considère l'algorithme suivant, dû à Tonelli et Shanks, qui a pour but de calculer une racine dcarrée modulo p.

Algorithme 1 : Algorithme de Tonelli-Shanks

Entrée : $p \geq 3$ premier $a \in \{0, \dots, p-1\}$ qui est un carré modulo p
Sortie : un entier $x \in \{0, \dots, p-1\}$ tel que $x^2 \equiv a \mod p$

Calculer $e \geq 1$ et n impair tel que $p = 2^e n + 1$.
Poser $\ell = 1$.
Tant que $\ell = 1$ **faire**
    Tirer uniformément $u \in \{1, \dots, p-1\}$.
    Calculer le symbole de Legendre $\ell = \left(\frac{u}{p}\right)$.
Poser $k = e$.
Calculer $z = u^n \mod p$.
Calculer $x = a^{(n+1)/2} \mod p$
Calculer $b = a^n \mod p$.
Tant que $b \neq 1$ **faire**
    Calculer le plus petit entier $m \geq 1$ tel que $b^{2^m} \equiv 1 \mod p$.
    Calculer $t = z^{2^{k-m-1}} \mod p$.
    Calculer $z = t^2 \mod p$.
    Calculer $b = bz \mod p$.
    Calculer $x = xt \mod p$.
    Poser $k = m$
Retourner x.

Preuve de l'algorithme

On se propose de démontrer que la valeur de retour de l'algorithme de Tonelli-Shanks, lorsqu'il prend en entrée un nombre premier $p \geq 3$ et un résidu quadratique non-nul $a \leq p-1$, est une racine carrée de a modulo p.

L'algorithme étudié est l'Algorithme 1.

Question 1.– En sortie de la première boucle **Tant que** (c'est-à-dire, à l'étape 5), le nombre u est-il un carré ou un non-carré modulo p ?

Question 2.– Démontrer que $ab \equiv x^2 \mod p$ en entrée de la seconde boucle (étape 10).

Question 3.– Démontrer qu'à chaque tour de boucle, on a $ab \equiv x^2 \mod p$ en fin de boucle, c'est-à-dire après exécution de l'étape 16.

Question 4.– En déduire que **si l'algorithme se termine**, alors il retourne une racine carrée de a modulo p.

Il reste donc à démontrer que l'algorithme retourne une valeur, c'est-à-dire que les deux boucles se terminent.

Question 5.– Expliquer pourquoi la première boucle se termine.

Question 6.– Démontrer que la deuxième boucle se termine après au plus e itérations. Pour cela, on étudiera les ordres de b et z modulo p en entrée et sortie de boucle.

Complexité de l'algorithme

Question 7.– Combien y a-t-il de carrés dans $\mathbb{F}_p$? En déduire le nombre moyen de tirages de u à effectuer pour dépasser la première boucle.

Question 8.– Calculer la complexité de l'algorithme de Tonelli-Shanks en fonction de p. On donnera cette complexité en fonction de

- la quantité L_p qui représente une majoration de la complexité du calcul d'un symbole de Legendre,
- les quantités M_p, S_p et R_p qui représentent respectivement le coût d'une multiplication, d'un carré et d'une réduction modulo p d'un entier $y \leq p^2$.

Attention : lorsqu'on effectue l'opération $u^n \mod p$, l'entier u^n est probablement de taille $> p^2$. On devra donc décomposer ce calcul pour calculer précisément sa complexité.

Implantation de l'algorithme

Pour l'implantation, veuillez choisir parmi les langages de programmation suivants : `C`, `C++`, `python`, `java`, `OCaml`, `julia`.

Question 9.– Implanter l'algorithme qui calcule le symbole de Legendre (voir en annexe). En effectuant des expérimentations sur des valeurs de p assez grandes, proposer une complexité pour la valeur de L_p.

Question 10.– Implanter l'algorithme de Tonelli-Shanks. Le tester, par exemple avec les valeurs proposées dans la Table 1. Avec votre implantation, jusqu'à quelle valeur de $\lceil \log_2 p \rceil$ le calcul prend-il moins d'une seconde ?

Si l'algorithme est correctement implanté, le résultat à obtenir pour les valeurs donnés dans la Table 1 doit être immédiat. Si ce n'est pas le cas, c'est peut-être dû aux affectations du type $z = u^n \mod p$, dont une implantation naïve peut être très coûteuse. Si besoin, construisez à la main une fonction `pow_mod_p(u,n,p)`.

Question 11.– Donner une complexité expérimentale de l'algorithme de Tonelli-Shanks en fonction de p.

Bonus : comparaison avec l'algorithme de Cipolla

Question 12.– BONUS. Implanter l'algorithme de Cipolla vu en cours. Comparer expérimentalement sa complexité avec celle de l'algorihtme de Tonelli-Shanks.

Annexe

On donne d'abord une table de racines carrées modulo p.

p	$\lceil \log_2 p \rceil$	a	x
907	10	141	105
1032959	20	124729	778978
1071788713	30	881541419	508518185
1099267487173	40	788111815361	23638826712
1125869389264507	50	319707244227995	469868020198319
1152917689909581353	60	853197802109168738	1050211281810539034
1180591143880253100313	70	87067585006025147696	684550728486713860840
1208925760009984399315567	80	725485820599100152666180	111256904488739353156573 3

TABLE 1 – Exemples de racines carrées modulo p.

Voici un algorithme permettant de calculer le symbole de Legendre $\left(\frac{a}{p}\right)$. Cet algorithme n'est clairement pas optimisé, et vous pouvez un implanter un plus rapide si vous le souhaitez.

Algorithme 2 : Calcul du symbole de Legendre

Entrée : $a \in \mathbb{Z}$ et $p \geq 2$ premier
Sortie : le symbole de Legendre $\left(\frac{a}{p}\right)$

```
Si a = 0
    Retourner 0
Si a = 1 ou p = 2
    Retourner 1
Si a = p − 1
    Si a ≡ 0 mod 4
        Retourner 1
    Sinon
        Retourner −1
Si a ≡ 0 mod 2
    Si p ≡ 1 mod 8 ou p ≡ 3 mod 8
        Retourner Legendre(a/2, p)
    Sinon
        Retourner (−1)× Legendre(a/2, p)
Si a ≥ p
    Retourner Legendre(a mod p, p)
Si a mod 4 == 1 ou p mod 4 == 1
    Retourner Legendre(p, a)
Sinon
    Retourner (−1)× Legendre(p, a)
```