17 mai 2023
Master 1 M.F., Orsay

Partiel de M.A.O. Calcul Formel Durée : 3 heures

Lorsqu'on évoque le coût d'un algorithme, on attend toujours une réponse de la forme $O(\dots)$: déterminer la constante implicite dans le symbole $O(\dots)$ n'est pas demandé. De plus, sauf mention explicite du contraire, on compte le nombre d'opérations arithmétiques (additions, multiplications, soustractions, divisions), dans $\mathbb{Z}$ ou dans un corps selon le contexte.

Il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes. Les parties 1, 2 et 3 sont indépendantes et il est conseillé de toutes les aborder (au moins en partie). Certains résultats des parties 1 et 2 sont utilisés dans la partie 4.

Partie 1 : Carrés dans $\mathbb{F}_p^*$

Dans cette partie on fixe un nombre premier $p \equiv 1 \bmod 4$. On rappelle que dans $\mathbb{F}_p^*$, la moitié des éléments exactement sont des carrés (c'est-à-dire de la forme x^2 avec $x \in \mathbb{F}_p^*$).

1. Soit $x \in \mathbb{F}_p^*$; on pose $y = x^{(p-1)/4}$. Démontrer qu'on a $y^2 = 1$ si x est un carré, et $y^2 = -1$ sinon.
2. Étant donné $x \in \mathbb{F}_p^*$, rappeler le nom de l'algorithme classique permettant de calculer efficacement $x^{(p-1)/4}$, et donner son coût en nombre d'opérations dans $\mathbb{F}_p$. *Dans cette question, aucune justification n'est demandée.*

Considérons l'algorithme suivant, qui détermine un élément $y \in \mathbb{F}_p^*$ tel que $y^2 = -1$:

- Choisir au hasard un élément $x \in \mathbb{F}_p^*$.
- Calculer $y = x^{(p-1)/4}$.
- Si $y^2 = -1$ renvoyer y, sinon recommencer au début.

On note X la variable aléatoire égale au nombre d'opérations arithmétiques dans $\mathbb{F}_p$ effectuées par cet algorithme. *On ne compte pas ici les opérations utilisées pour produire un élément aléatoire $x \in \mathbb{F}_p^*$.*

3. Déterminer l'espérance de X ; comparer ce coût moyen au coût de l'algorithme naïf consistant à tester un par un tous les éléments $y \in \mathbb{F}_p^*$ jusqu'à en trouver un tel que $y^2 = -1$.
4. ($\star$) Implémenter l'algorithme présenté ci-dessus sous la forme d'une fonction `racine` qui prend en entrée un entier p (qu'on suppose être un nombre premier congru à 1 modulo 4), et renvoie un élément $y \in \mathbb{F}_p^*$ tel que $y^2 = -1$.
5. ($\star$) Écrire sur la copie ce que renvoie la fonction précédente avec $p = 1009$.
6. En faisant tourner plusieurs fois la fonction `racine` de la question 4 avec la même valeur de p, deviner combien il existe d'éléments $y \in \mathbb{F}_p^*$ tels que $y^2 = -1$. Démontrer ensuite ce résultat.
7. Démontrer que tous les éléments $y \in \mathbb{F}_p^*$ tels que $y^2 = -1$ peuvent être renvoyés par la fonction `racine` de la question 4.
8. Si p est un nombre premier qui n'est pas congru à 1 modulo 4, existe-t-il $y \in \mathbb{F}_p^*$ tel que $y^2 = -1$?

Partie 2 : Autour de l'algorithme d'Euclide étendu

Dans cette partie on fixe deux entiers a et b tels que $a > b \geq 0$ et on s'intéresse à l'algorithme d'Euclide étendu qui permet de calculer le pgcd de a et b, ainsi qu'une relation de Bezout. A la j-ième étape, cet algorithme fournit une relation de la forme $r_j = au_j + bv_j$ (en convenant que $r_0 = a$ et $r_1 = b$). On se donne deux entiers R et V tels que $0 < R \leq a < RV$. On note j_0 le plus petit entier naturel tel que $r_{j_0} < R$.

9. Justifier que j_0 existe et qu'on a $j_0 \geq 1$.
10. Démontrer que pour tout j on a $u_j v_{j+1} - u_{j+1} v_j = (-1)^j$.
11. Démontrer qu'on a

$$r_{j_0} \equiv b\, v_{j_0} \bmod a, \quad 0 \leq r_{j_0} < R \quad \text{et} \quad 0 < |v_{j_0}| < V.$$

12. ($\star$) Implémenter une fonction `Euclide` qui prend en entrée quatre entiers a, b, R, V tels que $a > b \geq 0$ et $0 < R \leq a < RV$, et renvoie les entiers r_{j_0} et v_{j_0}.
13. ($\star$) Dans cette question on prend $a = 10^5$, $b = 20023$, $R = 10^4$ et $V = 20$. Calculer r_{j_0} et v_{j_0} en utilisant la fonction implémentée à la question précédente, et recopier les valeurs obtenues sur la copie.
14. Exprimer (en fonction de a ou b seulement) le coût, en nombre d'opérations arithmétiques dans $\mathbb{Z}$, de l'algorithme implémenté à la question 12.

Partie 3 : Sommes de deux carrés, approche naïve

Dans cette partie on fixe un nombre premier $p \equiv 1 \bmod 4$. On admet qu'il existe alors deux entiers s et t tels que $s^2 + t^2 = p$. Le but de cette partie est de déterminer de tels entiers ; on imagine que p peut être grand.

15. ($\star$) Sans utiliser les résultats des parties précédentes, proposer et implémenter un algorithme simple qui calcule s et t à partir de p en $O(\sqrt{p})$ opérations. Précisément on demande d'implémenter une fonction `somme` qui prend en entrée un entier p (qu'on suppose être un nombre premier congru à 1 modulo 4), et renvoie deux entiers s et t tels que $s^2 + t^2 = p$. Le coût de ce calcul doit impérativement être en $O(\sqrt{p})$ opérations arithmétiques dans $\mathbb{Z}$. *On rappelle que seules comptent ici les opérations arithmétiques : par exemple si* `L` *est une liste (même très longue), le test* `if x in L` *ne coûte aucune opération.* On pourra, si besoin, utiliser la fonction `index` qui donne l'indice d'un élément dans une liste.
16. ($\star$) En utilisant la fonction implémentée à la question précédente, déterminer deux entiers s et t tels que $s^2 + t^2 = 1009$. On recopiera ces deux entiers sur la copie.
17. Question facultative : expliquer comment on peut coder la fonction de la question 15 avec un nombre raisonnable de comparaisons entre entiers (et estimer ce nombre). *On ne demande pas d'implémenter cette méthode alternative.*

Partie 4 : Sommes de deux carrés, algorithme efficace

Dans cette partie on fixe encore un nombre premier $p \equiv 1 \bmod 4$.

18. Donner un algorithme qui combine ceux des questions 4 et 12 et permet de déterminer efficacement des entiers s et t tels que $s^2 + t^2 = p$; on démontrera qu'il est correct.
19. Calculer le coût moyen, en nombre d'opérations arithmétiques dans $\mathbb{Z}$, de l'algorithme de la question précédente ; le comparer à celui de la question 15.
20. ($\star$) Implémenter l'algorithme de la question 18 sous la forme d'une fonction `sommebis` qui prend en entrée un entier p (qu'on suppose être un nombre premier congru à 1 modulo 4), et renvoie deux entiers s et t tels que $s^2 + t^2 = p$.
21. ($\star$) Comme l'a démontré Clausen en 1855, le nombre

$$p = \frac{2^{64} + 1}{274177} = 67\,280\,421\,310\,721$$

est premier (et on l'admet). Déterminer deux entiers s et t tels que $s^2 + t^2 = p$, et inscrire sur la copie ces deux entiers.