12 juin 2023
Master 1 M.F., Orsay

Examen 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. La partie 1 est indépendante des parties 2 et 3.

Partie 1 : le problème du logarithme discret

La motivation de ce sujet est le problème du logarithme discret. Soit G un groupe fini (noté multiplicativement), et g et h deux éléments de G. On suppose qu'il existe un entier $a \geq 0$ tel que $h = g^a$. Dans ce contexte, résoudre le problème du logarithme discret signifie trouver un entier $a \geq 0$ vérifiant $h = g^a$.

1. Donner un algorithme naïf de résolution de ce problème, et estimer son coût (en nombre d'opérations dans le groupe G) en fonction du cardinal de G.
2. ($\star$) Implémenter l'algorithme de la question précédente dans le groupe multiplicatif $G = \mathbb{K}^*$ des éléments inversibles d'un corps fini $\mathbb{K}$. Précisément, on demande d'implémenter une fonction `LogDiscret` qui prend en entrée un corps fini $\mathbb{K}$ et deux éléments $g, h \in \mathbb{K}$, et renvoie un entier $a \geq 0$ tel que $h = g^a$ si un tel entier existe. S'il n'existe pas de tel entier, la fonction doit renvoyer -1.
3. ($\star$) En utilisant la fonction `LogDiscret` de la question précédente, déterminer une valeur de a dans la situation suivante : $\mathbb{K} = \mathbb{F}_{3221}$, $h = 458$ et $g = 177$.

Considérons, dans la fin de cette partie, la situation suivante. Deux personnes, nommées habituellement Alice et Bob, veulent créer un secret qu'elles seront seules à détenir. Le problème est que toutes les communications entre Alice et Bob sont susceptibles d'être interceptées par un espion. Alice et Bob procèdent alors comme suit.

Alice choisit un grand nombre premier p, et calcule un entier g dont la classe modulo p est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. Elle choisit aussi un entier a au hasard, et calcule l'entier $A \in \{1, \dots, p-1\}$ tel que $g^a \equiv A \mod p$. Elle garde l'entier a secret, et envoie le triplet (p, g, A) à Bob.

De son côté, Bob choisit alors un entier b au hasard, et calcule l'entier $B \in \{1, \dots, p-1\}$ tel que $g^b \equiv B \mod p$. Il envoie cet entier B à Alice, et garde b secret. On note enfin S l'unique entier compris entre 1 et $p-1$ tel que $g^{ab} \equiv S \mod p$.

4. Expliquer comment Alice et Bob peuvent, chacun séparément, calculer cet entier S : il s'agit de leur secret commun.
5. ($\star$) Dans cette question seulement, on prend la place d'Alice. On suppose qu'elle a choisi $p = 1009$, $g = 17$ et $a = 130$. On admet que la classe de g modulo p est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. Enfin on suppose qu'elle a reçu $B = 403$ de la part de Bob. Calculer alors le secret S.

6. Un espion a intercepté toutes les communications entre Alice et Bob, et sait aussi résoudre efficacement le problème du logarithme discret dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Démontrer que l'espion peut alors déterminer S.
7. ($\star$) Dans cette dernière question on prend la place de l'espion, qui a intercepté les communications et connaît les valeurs suivantes : $p = 1009$, $g = 17$, $A = 20$, $B = 283$. En utilisant éventuellement la fonction `LogDiscret` implémentée à la question 2, calculer le secret S.

Partie 2 : divisibilités entre polynômes

Dans cette partie on fixe un nombre premier p, un entier $\ell \geq 1$, et on pose $q = p^\ell$. On se donne aussi un élément x_0 de $\mathbb{F}_q^*$.

8. En raisonnant par récurrence sur k, démontrer que pour tous $j, k \geq 0$ tels que p ne divise pas j, il existe un polynôme $S_{j,k} \in \mathbb{F}_q[X]$, vérifiant $S_{j,k}(0) = 0$, tel qu'on ait l'égalité suivante dans $\mathbb{F}_q[X]$:

$$(X + x_0)^{jp^k} = x_0^{jp^k} + jx_0^{(j-1)p^k} X^{p^k}(1 + S_{j,k}(X)).$$

9. Dans cette question seulement, on s'intéresse au coût du calcul de $(X - x_0)^n \in \mathbb{F}_q[X]$ pour un entier n supposé grand. Calculer ce coût, en distinguant selon qu'on utilise l'exponentiation rapide ou pas, dans chacune des trois situations suivantes :
   (i) On compte les multiplications dans $\mathbb{F}_q[X]$.
   (ii) On compte les opérations arithmétiques dans $\mathbb{F}_q$, et la multiplication des polynômes à coefficients dans $\mathbb{F}_q$ est implémentée de façon naïve.
   (iii) On compte les opérations arithmétiques dans $\mathbb{F}_q$, et on dispose d'une implémentation de l'algorithme de Karatsuba.
10. ($\star$) Implémenter une fonction `PolySjk` qui prend en entrée un corps fini $\mathbb{K}$, un élément $x_0 \in \mathbb{K}$, un nombre premier p et deux entiers j, k, et renvoie (en supposant que p est la caractéristique de $\mathbb{K}$ et que p ne divise pas j) le polynôme $S_{j,k} \in \mathbb{K}[X]$ défini à la question 8. *On pourra utiliser sans restriction les fonctions de Sage, par exemple pour calculer les puissances d'un polynôme.*
11. ($\star$) En utilisant la fonction `PolySjk` de la question précédente, calculer $S_{3,2}$ avec $q = 1009^2$ (où l'on réalisera $\mathbb{F}_q$ comme corps de rupture sur $\mathbb{F}_{1009}$ du polynôme $P = X^2 + 1008X + 11$) et x_0 la racine privilégiée de P dans $\mathbb{F}_q$.
12. Soient $j, k \geq 0$. Démontrer que $x_0^{jp^k} = 1$ si, et seulement si, j est un multiple de l'ordre de x_0 dans le groupe multiplicatif $\mathbb{F}_q^*$.
13. Soit $t, n \geq 1$. En remplaçant X par $X - x_0$ dans la question 8, déduire des questions 8 et 12 que les deux assertions suivantes sont équivalentes :
   (i) $(X - x_0)^t$ divise $X^n - 1$ dans $\mathbb{F}_q[X]$.
   (ii) n est multiple de $p^\delta \omega$, où ω est l'ordre de x_0 dans $\mathbb{F}_q^*$ et $\delta \geq 0$ est le plus petit entier tel que $p^\delta \geq t$.

Partie 3 : ordre multiplicatif d'une matrice

Dans cette troisième partie on se donne un nombre premier p, un entier $d \geq 1$, et une matrice $M \in \mathrm{GL}_d(\mathbb{F}_p)$. On cherche à déterminer l'ordre de M dans le groupe multiplicatif $\mathrm{GL}_d(\mathbb{F}_p)$.

On note $\mu_M \in \mathbb{F}_p[X]$ le polynôme minimal de la matrice M, qui est unitaire par définition. On écrit $\mu_M = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ la décomposition de μ_M en produit d'irréductibles dans $\mathbb{F}_p[X]$. Autrement dit, les polynômes $P_1, \ldots, P_r$ sont unitaires et irréductibles dans $\mathbb{F}_p[X]$, et deux à deux distincts ; les entiers $e_1, \ldots, e_r$ sont strictement positifs.

Pour tout entier i compris entre 1 et r, on pose $d_i = \deg P_i$ et $q_i = p^{d_i}$.

14. Démontrer que pour tout entier i compris entre 1 et r, il existe un corps fini $\mathbb{K}_i$ de cardinal q_i et un élément $x_i \in \mathbb{K}_i$ tels que $P_i(x_i) = 0$.
15. Soit $k \geq 0$. Démontrer qu'on a $M^k = I_d$ si, et seulement si, pour tout i le polynôme $P_i^{e_i}$ divise $X^k - 1$ dans $\mathbb{F}_p[X]$.
16. Démontrer que pour tout entier i compris entre 1 et r, les deux assertions suivantes sont équivalentes :
    (i) $P_i^{e_i}$ divise $X^k - 1$ dans $\mathbb{F}_p[X]$.
    (ii) $(X - x_i)^{e_i}$ divise $X^k - 1$ dans $\mathbb{K}_i[X]$, où x_i et $\mathbb{K}_i$ ont été définis à la question 14.
17. En utilisant les questions 13, 15 et 16, démontrer que l'ordre de M dans $\mathrm{GL}_d(\mathbb{F}_p)$ est

$$p^\delta \,\mathrm{ppcm}(\mathrm{ord}(x_1), \ldots, \mathrm{ord}(x_r))$$

    où $\delta \geq 0$ est le plus petit entier vérifiant $p^\delta \geq e_i$ pour tout i, et $\mathrm{ord}(x_i)$ est l'ordre de x_i dans le groupe multiplicatif $\mathbb{K}_i^*$.

Partie 4 : le problème du logarithme discret dans $\mathrm{GL}_d(\mathbb{F}_p)$

Dans cette dernière partie on se donne un nombre premier p, un entier $d \geq 1$, et deux matrices $A, M \in \mathrm{GL}_d(\mathbb{F}_p)$. On suppose qu'il existe un entier $a \geq 0$ tel que $A = M^a$.

Pour résoudre le problème du logarithme discret, on suppose A et M connues, et on cherche à déterminer a.

On reprend les notations de la partie précédente ; d'après la question 17, l'ordre de M dans $\mathrm{GL}_d(\mathbb{F}_p)$ est

$$p^\delta \,\mathrm{ppcm}(\mathrm{ord}(x_1), \ldots, \mathrm{ord}(x_r)).$$

18. Justifier que l'entier a est unique modulo l'ordre de M, et que pour le déterminer il suffit de connaître ses classes de congruence modulo p^δ, $\mathrm{ord}(x_1)$, …, $\mathrm{ord}(x_r)$.
19. Soit i un entier compris entre 1 et r ; on reprend les notations x_i et $\mathbb{K}_i$ de la question 14. On note $Q_i \in \mathrm{GL}_d(\mathbb{K}_i)$ une matrice inversible dont la première colonne est un vecteur propre de M pour la valeur propre x_i. Déterminer la première colonne de $Q_i^{-1} M Q_i$, puis (en fonction de a) celle de $Q_i^{-1} A Q_i$.
20. Dans cette question on suppose qu'on sait calculer une matrice Q_i comme dans la question précédente, et qu'on sait résoudre efficacement le problème du logarithme discret dans le groupe $\mathbb{K}_i^*$. Montrer comment on peut alors calculer efficacement la classe de congruence de a modulo $\mathrm{ord}(x_i)$.

Pour tout $e \geq 2$ on note $J_e(x)$ la matrice suivante, qui est carrée de taille e avec des x sur la diagonale, des 1 juste au-dessus et des 0 partout ailleurs :

$$J_e(x) = \begin{bmatrix} x & 1 & 0 & \dots & 0 & 0 \\ 0 & x & 1 & \dots & 0 & 0 \\ 0 & 0 & x & \ddots & 0 & 0 \\ \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & x & 1 \\ 0 & 0 & 0 & \dots & 0 & x \end{bmatrix}.$$

21. Soit i un entier tel que $e_i \geq 2$. Construire une matrice inversible $Q'_i \in \mathrm{GL}_d(\mathbb{K}_i)$ telle qu'on ait

$$Q_i'^{-1} M Q'_i = \begin{bmatrix} J_{e_i}(x_i) & \star \\ 0 & \star \end{bmatrix}$$

où la matrice de droite est donnée par blocs, les étoiles désignant des blocs quelconques. En déduire comment adapter la question 20 pour calculer efficacement la classe de congruence de a modulo p.

22. En notant $u \in \{0, \dots, p-1\}$ un entier tel que $a \equiv u \bmod p$ et en considérant les matrices $A' = AM^{-u}$ et $M' = M^p$, conclure ce problème en montrant que si on sait résoudre efficacement le problème du logarithme discret dans le groupe multiplicatif de toute extension finie de $\mathbb{F}_p$ de degré au plus d, alors on peut aussi le résoudre efficacement dans $\mathrm{GL}_d(\mathbb{F}_p)$.