12 juin 2023
Master 1 M.F., Orsay

Corrigé de l'examen de M.A.O. Calcul Formel

Partie 1 : le problème du logarithme discret

1. Pour commencer, comme $h = g^a$ on a immédiatement pour tout entier b l'équivalence suivante : $h = g^b$ si et seulement si b est congru à a modulo l'ordre de g dans G. En particulier il existe un tel entier a compris entre 1 et le cardinal de G (puisque l'ordre de g est majoré par ce cardinal). L'algorithme naïf consiste, pour chaque entier a compris entre 1 et le cardinal de G, à calculer g^a : si on trouve un entier a pour lequel $g^a = h$, on renvoie cet entier. Dans le cas contraire, aucun tel entier a n'existe. Le coût de cet algorithme est $O(n)$ opérations dans G, où n est le cardinal de G, si on calcule g^a de proche en proche : $g^a = g \cdot g^{a-1}$, sachant que g^{a-1} a été calculé à l'étape précédente.
2. ($\star$) Voir le Jupyter Notebook !
3. ($\star$) On obtient $a = 2023$.
4. Alice connaît p, B et a, donc elle peut calculer la classe de B^a modulo p, qui est celle de S. De même, Bob connaît p, A et b donc peut calculer le reste dans la division euclidienne de A^b par p, qui est S.
5. ($\star$) On obtient $S = 591$.
6. L'espion connaît p, g, A et B. Il sait qu'il existe a tel que $A = g^a$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. En résolvant le problème du logarithme discret il trouve un entier a' tel que $A = g^{a'}$. Cela montre que a' est congru à a modulo l'ordre de g. Comme l'ordre de $B = g^b$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ divise celui de g, on a $B^{a'} = B^a$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Donc en calculant le reste dans la division euclidienne de B^a par p, l'espion arrive à déterminer S.
7. ($\star$) On obtient $S = 280$.

Partie 2 : divisibilités entre polynômes

8. Pour $k = 0$, l'existence de $S_{j,k}$ vient simplement du développement de $(X + x_0)^j$ par la formule du binôme de Newton, puisque jx_0^{j-1} est inversible dans $\mathbb{K}$ (grâce à l'hypothèse selon laquelle la caractéristique de $\mathbb{K}$, qui est p, est première avec j). Supposons la formule vérifiée pour un certain entier $k \geq 0$. On a alors :

$$\begin{aligned}(X + x_0)^{jp^{k+1}} &= \left((X + x_0)^{jp^k}\right)^p = \left(x_0^{jp^k}\right)^p + \left(jx_0^{(j-1)p^k} X^{jp^k}(1 + S_{j,k}(X))\right)^p \\ &= x_0^{jp^{k+1}} + jx_0^{(j-1)p^{k+1}} X^{jp^{k+1}}(1 + S_{j,k}(X)^p)\end{aligned}$$

   puisque $j^p = j$ dans le sous-corps premier de $\mathbb{K}$ (qui est isomorphe à $\mathbb{Z}/p\mathbb{Z}$). En posant $S_{j,k+1}(X) = S_{j,k}(X)^p$ on a bien $S_{j,k+1}(0) = 0$ et la récurrence est terminée.
9. (i) Par l'exponentiation rapide, on utilise seulement $O(\log n)$ multiplications entre polynômes de $\mathbb{F}_q[X]$. L'algorithme naïf en utilise $O(n)$ (en fait, $n - 1$ si on veut être précis) : on calcule de proche en proche les puissances successives de $X - x_0$.

(*ii*) Comme la multiplication des polynômes à coefficients dans $\mathbb{F}_q$ est implémentée de façon naïve, le produit de deux polynômes de degrés majorés par d et d' se calcule en $O(dd')$ opérations arithmétiques dans $\mathbb{F}_q$ (à condition que $d, d' \geq 1$). Par l'exponentiation rapide, les polynômes qui interviennent dans les calculs ont toujours des degrés majorés par n. Donc chaque multiplication de polynômes coûte $O(n^2)$ opérations arithmétiques dans $\mathbb{F}_q$. Comme il y a $O(\log n)$ telles multiplications, le coût est en $O(n^2 \log n)$. Ce n'est cependant qu'une majoration ; on peut raffiner légèrement cette borne, en supposant (pour simplifier) que $n = 2^k$ est une puissance de 2. Sous cette hypothèse, on calcule successivement les $(X - x_0)^{2^j}$ pour j allant de 1 à k. Le calcul de $(X - x_0)^{2^j}$ se fait en mettant au carré le polynôme précédent $(X - x_0)^{2^{j-1}}$, ce qui coûte $O(2^{2(j-1)})$ opérations. Le coût global du calcul est donc $\sum_{j=1}^{k} O(4^{j-1}) = O(4^k) = O(n^2)$. Cette majoration est optimale (à la valeur près de la constante implicite dans le symbole O, évidemment) puisque le dernier produit coûte à lui seul $O(4^{k-1}) = O(n^2)$ opérations et pas moins.
Si on utilise l'algorithme naïf de calcul de $(X - x_0)^n$, on calcule de proche en proche les $(X - x_0)^\ell$ pour ℓ allant de 2 à n. Le calcul de $(X - x_0)^\ell$ se fait en multipliant $(X - x_0)^{\ell-1}$ par $X - x_0$, ce qui coûte $O(\ell)$ opérations. En sommant sur ℓ on obtient un coût en $O(n^2)$ opérations arithmétiques dans $\mathbb{F}_q$. Cela montre que dans cette situation, l'exponentiation rapide n'apporte rien de mieux par rapport à l'algorithme naïf d'exponentiation.

(*iii*) L'algorithme de Karatsuba permet de multiplier deux polynômes de degré au plus d en $O(d^\alpha)$ opérations arithmétiques dans $\mathbb{F}_q$, avec $\alpha = \log_2(3) = 1.58\ldots$. Si on utilise l'exponentiation rapide, le calcul est similaire à celui du (*ii*). On obtient directement une majoration du coût en $O(n^\alpha \log n)$, et en supposant (pour simplifier) que $n = 2^k$ est une puissance de 2 on a un coût en $\sum_{j=1}^{k} O(3^{j-1}) = O(3^k) = O(n^\alpha)$. On peut démontrer que cette majoration est valable même si n n'est pas une puissance de 2.
Si on utilise l'algorithme naïf de calcul de $(X - x_0)^n$, on ne va pas bénéficier de l'algorithme de Karatsuba. En effet, pour multiplier $(X - x_0)^{\ell-1}$ par $X - x_0$ en utilisant cet algorithme, on majore (grossièrement) le degré de $X - x_0$ par $\ell - 1$ et on utilise $O(\ell^\alpha)$ opérations dans $\mathbb{F}_q$. C'est nettement moins efficace que de multiplier naïvement ces deux polynômes. Donc avec l'algorithme naïf d'exponentiation on utilise $O(n^2)$ opérations comme au (*ii*). Si on tenait à utiliser l'algorithme de Karatsuba le coût serait de $\sum_{\ell=2}^{n} O(\ell^\alpha) = O(n^{\alpha+1})$ opérations.

10. ($\star$) Voir le Jupyter Notebook !
11. ($\star$) On obtient
$$S_{3,2}(X) = (845x_0 + 378)X^{2036162} + (642x_0 + 367)X^{1018081}.$$
12. Notons ω l'ordre de x_0 dans le groupe multiplicatif $\mathbb{F}_q^*$. Alors ω divise $\mathrm{Card}(\mathbb{F}_q^*) = q - 1$, donc ω est premier avec p. Soient maintenant $j, k \geq 0$. On a $x_0^{jp^k} = 1$ si, et seulement si, ω divise jp^k. Comme ω est premier avec p, c'est le cas si, et seulement si, ω divise j.
13. En remplaçant X par $X - x_0$ dans la formule de la question 8, il vient
$$X^{jp^k} = x_0^{jp^k} + jx_0^{(j-1)p^k}(X - x_0)^{p^k}(1 + S_{j,k}(X - x_0)). \tag{1}$$
Soit $t, n \geq 1$. Supposons d'abord que n est multiple de $p^\delta\omega$. Comme ω est premier avec p, on peut appliquer la formule précédente avec $n = jp^k$, $k \geq \delta$ (donc $p^k \geq t$) et j

multiple de ω mais pas de p. D'après la question 12 on a $x_0^{jp^k} = 1$. Donc l'équation (1) donne $X^n \equiv 1 \bmod (X - x_0)^t$, ce qui démontre (i).
Réciproquement, supposons que $X^n \equiv 1 \bmod (X - x_0)^t$. Comme $t \geq 1$, cela implique $x_0^n = 1$: n est multiple de ω. On peut donc appliquer l'équation (1) en notant $n = jp^k$ avec j divisible par ω mais pas par p (puisque ω est premier avec p). D'après la question 12 on a $x_0^{jp^k} = 1$. Comme $X^n \equiv 1 \bmod (X - x_0)^t$, on en déduit

$$jx_0^{(j-1)p^k}(X - x_0)^{p^k}(1 + S_{j,k}(X - x_0)) \equiv 0 \bmod (X - x_0)^t.$$

Comme j est premier avec p et que x_0 est non nul, cela implique $p^k \geq t$ et termine la preuve.

Partie 3 : ordre multiplicatif d'une matrice

14. Comme P_i est irréductible dans $\mathbb{F}_p[X]$, on peut considérer un corps de rupture $\mathbb{K}_i$ de P_i sur $\mathbb{F}_p$; il est muni d'une racine $x_i \in \mathbb{K}_i$ de P_i. Il s'agit d'une extension de $\mathbb{F}_p$ de degré d_i : c'est un corps fini de cardinal q_i.
15. Soit $k \geq 0$. On a $M^k = I_d$ si, et seulement si, le polynôme $X^k - 1$ est annulateur de M. Cela signifie que μ_M divise $X^k - 1$ dans $\mathbb{F}_p[X]$, et équivaut à ce que pour tout i le polynôme $P_i^{e_i}$ divise $X^k - 1$ (puisque les $P_i^{e_i}$ sont premiers entre eux deux à deux).
16. Comme x_i est une racine de P_i dans $\mathbb{K}_i$, il existe $L_i(X) \in \mathbb{K}_i[X]$ tel que $P_i = (X - x_i)L_i$. Donc $(X - x_i)^{e_i}$ divise $P_i^{e_i}$ dans $\mathbb{K}_i[X]$, ce qui montre que (i) implique (ii).
Réciproquement, comme P_i est unitaire et irréductible dans $\mathbb{F}_p[X]$ on a $P_i = \prod_{\ell=0}^{d_i-1}(X - x_i^{p^\ell})$. De plus en appliquant ℓ fois le morphisme de Frobenius $y \mapsto y^p$ aux coefficients de la relation $X^k - 1 = (X - x_i)^{e_i}T_i(X)$ où $T_i \in \mathbb{K}_i[X]$, on voit que $(X - x_i^{p^\ell})^{e_i}$ divise $X^k - 1$ dans $\mathbb{K}_i[X]$, puisque $(-1)^{p^\ell} = -1$ dans $\mathbb{K}_i$ (y compris si $p = 2$, puisqu'alors $-1 = 1$). Comme les $x_i^{p^\ell}$ sont deux à deux distincts, on obtient finalement que $P_i^{e_i}$ divise $X^k - 1$ dans $\mathbb{K}_i[X]$. Comme les deux polynômes en jeu sont à coefficients dans $\mathbb{F}_p[X]$, cette divisibilité a lieu aussi dans $\mathbb{F}_p[X]$.
17. Soit $k \geq 0$. D'après la question 15 on a $M^k = I_d$ si, et seulement si, pour tout i le polynôme $P_i^{e_i}$ divise $X^k - 1$ dans $\mathbb{F}_p[X]$. D'après la question 16, c'est le cas si, et seulement si, pour tout i le polynôme $(X - x_i)^{e_i}$ divise $X^k - 1$ dans $\mathbb{K}_i[X]$. D'après la question 13, cela signifie que k est multiple de $p^\delta\omega$, avec $\omega = \mathrm{ppcm}(\mathrm{ord}(x_1), \ldots, \mathrm{ord}(x_r))$, puisque ω est premier avec p.

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

18. On a vu à la question 1 que l'entier a est unique modulo l'ordre de M. Par le théorème chinois, pour connaître a modulo l'ordre de M, il suffit de connaître ses classes de congruence modulo p^δ et modulo $\mathrm{ppcm}(\mathrm{ord}(x_1), \ldots, \mathrm{ord}(x_r))$ puisque p^δ et ce ppcm sont premiers entre eux. Les ordres des x_i ne sont pas forcément premiers entre eux, mais si on connaît les classes de congruence de a modulo les $\mathrm{ord}(x_i)$ alors cela détermine celle de a modulo leur ppcm.

19. Notons E_1 le premier vecteur de la base canonique de $M_{d,1}(\mathbb{K}_i)$. Alors la première colonne de $Q_i^{-1}MQ_i$ est $Q_i^{-1}MQ_iE_1 = Q_i^{-1}x_iQ_iE_1 = x_iE_1$ puisque la première colonne de Q_i, qui est Q_iE_1, est un vecteur propre de M pour la valeur propre x_i. Comme $A = M^a$, on a $Q_i^{-1}AQ_i = (Q_i^{-1}MQ_i)^a$. En calculant par blocs on voit que la première colonne de $Q_i^{-1}AQ_i$ est donc formée par un coefficient x_i^a suivi de $d-1$ zéros.

20. En calculant le coefficient en position $(1,1)$ de $Q_i^{-1}AQ_i$ on obtient x_i^a. Comme on connaît x_i et que par hypothèse on sait résoudre efficacement le problème du logarithme discret dans le groupe $\mathbb{K}_i^*$, cela permet de calculer efficacement la classe de congruence de a modulo $\mathrm{ord}(x_i)$.

21. Soit i un entier tel que $e_i \geq 2$. Par définition de e_i il existe un vecteur colonne V_i, à coefficients dans $\mathbb{K}_i$, qui appartient au noyau de $(M - x_iI_d)^{e_i}$ mais pas à celui de $(M - x_iI_d)^{e_i-1}$. La famille formée par les $(M - x_iI_d)^\ell V_i$ avec $0 \leq \ell \leq e_i - 1$ est libre donc il existe une matrice inversible $Q_i' \in \mathrm{GL}_d(\mathbb{K}_i)$ dont ce sont les e_i premières colonnes. On a alors
$$Q_i'^{-1}MQ_i' = \begin{bmatrix} J_{e_i}(x_i) & \star \\ 0 & \star \end{bmatrix}$$
par un calcul analogue à celui de la question 19, ce qui donne grâce à un produit par blocs :
$$Q_i'^{-1}MQ_i' = \begin{bmatrix} (J_{e_i}(x_i))^a & \star \\ 0 & \star \end{bmatrix}.$$
Par une récurrence immédiate sur a, on montre que le coefficient en position $(1,2)$ de cette matrice est ax_i^{a-1}. On peut calculer x_i^{a-1} puisqu'on connaît la classe de congruence de a modulo $\mathrm{ord}(x_i)$ d'après la question 20. On en déduit alors la valeur de a vu comme un élément de $\mathbb{K}_i$. Comme il s'agit d'un corps de caractéristique p, cela signifie qu'on obtient a modulo p.

22. La question précédente permet de trouver $u \in \{0, \ldots, p-1\}$ tel que $a \equiv u \bmod p$. Notons $A' = AM^{-u}$ et $M' = M^p$. Alors on a $A' = M'^{a'}$ en posant $a' = (a-u)/p$. La valuation p-adique de a' est strictement inférieure à celle de a : en itérant cette procédure on se ramène au cas où a n'est pas divisible par p, et la question 20 permet de conclure. Finalement, 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 $\mathrm{GL}_d(\mathbb{F}_p)$ (car déterminer le polynôme minimal de M, sa factorisation, et les matrices Q_i et Q_i' peut se faire en temps raisonnable).