10 juin 2025
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 $O(\cdots)$: déterminer la constante implicite dans le symbole $O(\cdots)$ 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.

Les questions précédées du symbole ($\star$) sont prévues pour être résolues, au moins en partie, à l'aide de `Sage`. Toutes les fonctions implémentées en `Sage` peuvent être utilisées, sauf mention explicite du contraire. Si une réponse est demandée dans la question, merci de la recopier sur la copie.

Il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes. Hormis la partie 5, toutes les parties sont indépendantes les unes des autres (sauf la première question de la partie 2, mais on peut l'admettre pour continuer la partie 2).

Partie 1 : Autour des carrés modulo p

Dans cette partie on fixe un nombre premier p tel que $p \equiv -1 \bmod 8$. On note $\Sigma \subset \mathbb{F}_p^\times$ l'ensemble des carrés non nuls modulo p, c'est-à-dire

$$\Sigma = \{x^2,\ x \in \mathbb{F}_p^\times\}.$$

On rappelle les propriétés suivantes, qu'on pourra utiliser sans démonstration :

- Σ est un sous-groupe du groupe multiplicatif $\mathbb{F}_p^\times$, et son cardinal est $\frac{p-1}{2}$.
- Si $x, y \in \mathbb{F}_p^\times \setminus \Sigma$ alors $xy \in \Sigma$.
- On a $2 \in \Sigma$ et $-1 \notin \Sigma$ (puisque $p \equiv -1 \bmod 8$).
- Étant donné $x \in \mathbb{F}_p$, on a : $x \in \Sigma$ si, et seulement si, $x^{(p-1)/2} = 1$.

On note Σ_0 l'ensemble des entiers $k \in [\![1, p-1]\!]$ dont la classe modulo p appartient à Σ, et on considère le polynôme

$$e(X) = \sum_{k \in \Sigma_0} X^k \in \mathbb{F}_2[X].$$

1. ($\star$) Implémenter en `Sage` une fonction `test_sigma` qui prend en entrée un nombre premier impair p et un entier a, et renvoie `True` si la classe de a modulo p appartient à Σ, et `False` sinon. *On prendra garde à implémenter cette fonction de façon efficace, pour qu'elle fonctionne même avec de grandes valeurs de p. Toute fonction de* `Sage` *peut être utilisée, à l'exception de celle permettant directement de dire si a est un carré modulo p.*
2. ($\star$) La classe de $a = 12345678$ modulo $p = 2^{17} - 1$ appartient-elle à Σ ? Et pour $p = 10^9 + 7$?
3. Calculer le coût, en nombre d'opérations arithmétiques dans $\mathbb{Z}$, de la fonction `test_sigma` implémentée à la question 1.
4. ($\star$) Implémenter en `Sage` une fonction `sigma_zero` qui prend en entrée un nombre premier p (dont on pourra supposer qu'il vérifie $p \equiv -1 \bmod 8$) et renvoie la liste des éléments de Σ_0 (les éléments de Σ_0 peuvent apparaître dans un ordre quelconque dans cette liste, mais chacun doit être présent une et une seule fois).

5. ($\star$) Afficher ce que renvoie la fonction `sigma_zero` pour $p = 23$. *Il n'est pas nécessaire de recopier sur la copie la réponse donnée par Sage.*
6. ($\star$) Déterminer lorsque $p = 1031$ la liste des éléments de Σ_0 compris (au sens large) entre 50 et 55.
7. Calculer le coût de la fonction `sigma_zero` en nombre d'opérations arithmétiques dans $\mathbb{Z}$. *Il s'agit de la fonction* `sigma_zero` *telle qu'elle a été implémentée à la question 4, mais si vous pensez qu'une autre implémentation aurait été plus efficace, vous devez la détailler précisément sur votre copie et c'est alors cette implémentation efficace que vous devez considérer.*
8. Justifier que l'élément $X^j \in \mathbb{F}_2[X]/(X^p-1)$ a un sens pour $j \in \mathbb{Z}/p\mathbb{Z}$. *Dans les questions suivantes, il est conseillé de raisonner dans* $\mathbb{F}_2[X]/(X^p-1)$ *et d'utiliser cette propriété.*
9. Démontrer que

$$e(X)^2 \equiv e(X) \bmod (X^p-1) \quad \text{et} \quad e(X) + e(X^{p-1}) \equiv \sum_{i=1}^{p-1} X^i \bmod (X^p-1).$$

10. Justifier qu'il existe une extension finie $\mathbb{K}$ de $\mathbb{F}_2$, et un élément $\alpha \in \mathbb{K}$, tels que $\alpha^p = 1$ et $\alpha \neq 1$. *Un tel élément* α *est fixé dans la suite.*
11. En utilisant les deux résultats de la question 9, démontrer que

$$e(\alpha) \in \mathbb{F}_2 \quad \text{et} \quad e(\alpha) + e(\alpha^{-1}) = 1.$$

Quitte à remplacer α par α^{-1}, on suppose désormais que $e(\alpha) = 0$. On considère le polynôme

$$g(X) = \prod_{j \in \Sigma_0} (X - \alpha^j).$$

12. Démontrer que $g(X)$ divise $e(X)$, et ensuite que $g(X) = \mathrm{pgcd}(e(X), X^p - 1)$.
13. Rappeler le nom de l'algorithme qui permet de calculer $g(X)$ à partir de $e(X)$ en utilisant la question 12 ; quel est son coût en nombre d'opérations arithmétiques dans $\mathbb{F}_2$?
14. ($\star$) Rappeler le nom de l'algorithme, vu en cours, qui permet de déterminer un facteur irréductible de $X^p - 1 \in \mathbb{F}_2[X]$ distinct de $X - 1$. Déterminer le polynôme g via sa définition dans le cas $p = 23$. Vérifier votre résultat grâce à la question 12. *On ne demande pas de recopier le résultat sur votre copie.*

Partie 2 : Un exemple de code

Dans cette partie on étudie le code cyclique $\mathcal{C} \subset \mathbb{F}_2^7$ engendré par le polynôme g construit dans la partie 1 avec $p = 7$. *Ce polynôme sera explicité dans la question 15 ; les questions suivantes de cette partie peuvent être traitées indépendamment de la partie 1.* Dans les questions 15 à 22 il est *interdit* d'utiliser les fonctions de `Sage` consacrées spécifiquement aux codes correcteurs d'erreurs telles que `Codes.CyclicCode`.

15. ($\star$) En appliquant les résultats de la partie 1 avec $p = 7$, montrer que $g(X) = 1+X+X^3$.
16. Quelle est la longueur de $\mathcal{C}$, et sa dimension ?
17. ($\star$) Donner la liste des éléments de $\mathcal{C}$. *Il n'est pas demandé de la recopier sur la copie.*

18. Quelle est la distance de $\mathcal{C}$? *On pourra, au choix, utiliser* `Sage` *ou faire des constatations à la main à partir du résultat de la question précédente. Dans ce deuxième cas, il est impératif d'expliquer clairement sur la copie ce qu'on constate.*
19. Combien d'erreur(s) le code $\mathcal{C}$ peut-il détecter, respectivement corriger ?
20. Notons d la distance de $\mathcal{C}$, k sa dimension, et N le cardinal d'une boule fermée de rayon $\lfloor \frac{d-1}{2} \rfloor$ dans $\mathbb{F}_2^7$. Calculer N et en déduire qu'on a $N \cdot 2^k = 2^7$.
21. Pour traduire l'égalité $N \cdot 2^k = 2^7$ obtenue à la question précédente, on dit que le code $\mathcal{C}$ est *parfait*. Justifier cette terminologie.
22. Rappeler le procédé vu en cours permettant de construire à partir de $\mathcal{C}$ un code $\mathcal{C}'$ de longueur 8, et donner les paramètres de $\mathcal{C}'$.

Partie 3 : Générateurs idempotents

Dans cette partie (qui est indépendante des précédentes) on considère un entier impair $n \geq 3$ et un idéal $\mathcal{C}$ de $\mathbb{F}_2[X]/(X^n - 1)$. On appelle *générateur* de $\mathcal{C}$ tout polynôme $F \in \mathbb{F}_2[X]$ de degré au plus $n-1$ tel que

$$\mathcal{C} = \{FQ \bmod (X^n - 1),\ Q \in \mathbb{F}_2[X]\}.$$

On a vu en cours qu'il existe un unique générateur de $\mathcal{C}$ qui divise $X^n - 1$. On le note $g_\mathcal{C}$. On note aussi $h_\mathcal{C}$ l'unique polynôme de $\mathbb{F}_2[X]$ tel que $g_\mathcal{C}(X)h_\mathcal{C}(X) = X^n - 1$.

23. Démontrer qu'il existe $U, V \in \mathbb{F}_2[X]$ tels que

$$\deg U < \deg h_\mathcal{C}, \quad \deg V < \deg g_\mathcal{C} \quad \text{et} \quad U g_\mathcal{C} + V h_\mathcal{C} = 1.$$

On considère maintenant le polynôme

$$E(X) = U(X)g_\mathcal{C}(X) = 1 - V(X)h_\mathcal{C}(X) \in \mathbb{F}_2[X],$$

dont la classe modulo $(X^n - 1)$ appartient à $\mathcal{C}$.

24. Quel est le coût, en nombre d'opérations arithmétiques dans $\mathbb{F}_2$, du calcul de $E(X)$ à partir de $g_\mathcal{C}$?
25. ($\star$) Soient $n = 31$ et $g_\mathcal{C} = X^5 + X^4 + X^2 + X + 1$. Déterminer le polynôme $E(X)$ correspondant.
26. Démontrer que $X^n - 1$ divise $E(X)h_\mathcal{C}(X)$, et en déduire que

$$E(X)^2 \equiv E(X) \bmod (X^n - 1) \quad \text{et} \quad g_\mathcal{C}(X)E(X) \equiv g_\mathcal{C}(X) \bmod (X^n - 1).$$

27. Démontrer que $E(X)$ est un générateur de $\mathcal{C}$.
28. Soit $Q \in \mathbb{F}_2[X]$. Démontrer que la classe de Q modulo $X^n - 1$ appartient à $\mathcal{C}$ si, et seulement si, $Q(X)E(X) \equiv Q(X) \bmod (X^n - 1)$.
29. Montrer que $E(X)$ est le seul générateur de $\mathcal{C}$ pour lequel la question précédente est vraie.
30. Démontrer que $g_\mathcal{C}(X) = \mathrm{pgcd}(E(X), X^n - 1)$.

Partie 4 : Des homographies particulières

Dans cette partie (qui est indépendante des précédentes) on note p un nombre premier impair, q une puissance de p, et $\mathbb{K}$ un corps fini de cardinal q. On appelle *droite projective* l'ensemble $\mathbb{P}^1(\mathbb{K}) = \mathbb{K} \cup \{\infty\}$, où ∞ est un symbole qui n'appartient pas à $\mathbb{K}$. On note $\mathrm{SL}_2(\mathbb{K})$ le groupe des matrices carrées 2×2 à coefficients dans $\mathbb{K}$ de déterminant 1. Pour $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{K})$ on note h_M la fonction de $\mathbb{P}^1(\mathbb{K})$ dans $\mathbb{P}^1(\mathbb{K})$ définie, pour tout $x \in \mathbb{P}^1(\mathbb{K})$, par :

$$h_M(x) = \begin{cases} \infty \text{ si } x = \infty \text{ et } c = 0 \\ a/c \text{ si } x = \infty \text{ et } c \neq 0 \\ \infty \text{ si } x = -d/c \text{ et } c \neq 0 \\ \frac{ax+b}{cx+d} \text{ sinon.} \end{cases}$$

On admet que pour tous $M, N \in \mathrm{SL}_2(\mathbb{K})$ on a $h_M \circ h_N = h_{MN}$. Comme $h_{I_2} = \mathrm{Id}_{\mathbb{P}^1(\mathbb{K})}$ on en déduit que pour tout $M \in \mathrm{SL}_2(\mathbb{K})$, la fonction h_M est bijective de réciproque $h_{M^{-1}}$. On note $\mathcal{H}$ l'ensemble des fonctions de la forme h_M avec $M \in \mathrm{SL}_2(\mathbb{K})$: c'est un groupe pour la composition.

31. Notons g_0 la fonction qui échange 0 et ∞, et envoie tout $x \in \mathbb{K}^\times$ sur $1/x$. Donner une condition nécessaire et suffisante portant sur le corps $\mathbb{K}$ pour que g_0 appartienne à $\mathcal{H}$.

On pose maintenant pour $a \in \mathbb{K}$ et $b \in \mathbb{K}^\times$:

$$g = h_{\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]}, \quad t_a = h_{\left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right]}, \quad \mu_{b^2} = h_{\left[\begin{smallmatrix} b & 0 \\ 0 & b^{-1} \end{smallmatrix}\right]}$$

de telle sorte que pour tout $x \in \mathbb{K}^\times$ on a

$$g(x) = -1/x, \quad t_a(x) = x + a, \quad \mu_{b^2}(x) = b^2 x.$$

32. Montrer que le groupe $\mathcal{H}$ est engendré par les fonctions g, t_a, μ_{b^2} pour $a \in \mathbb{K}$ et $b \in \mathbb{K}^\times$.

Partie 5 : Automorphismes d'un code

Dans cette partie qui utilise tout ce qui précède, on fixe un nombre premier p tel que $p \equiv -1 \bmod 8$. On reprend le polynôme $g(X)$ défini à la fin de la partie 1, et on note $\mathcal{C}$ le code cyclique engendré par g. On identifie maintenant un polynôme $\sum_{i \in \mathbb{F}_p} a_i X^i$ de $\mathbb{F}_2[X]/(X^p - 1)$ avec la partie

$$A = \{i \in \mathbb{F}_p,\, a_i = 1\}.$$

Via cette identification, tout mot du code correspond à une partie de $\mathbb{F}_p$, et le code $\mathcal{C}$ correspond donc à une partie notée $\mathcal{C}_0$ de l'ensemble $\mathcal{P}(\mathbb{F}_p)$ des parties de $\mathbb{F}_p$.

On note $A_1 \oplus A_2$ la différence symétrique de deux parties A_1 et A_2 de $\mathbb{F}_p$. On rappelle que par définition,

$$A_1 \oplus A_2 = \Big(A_1 \cup A_2\Big) \setminus \Big(A_1 \cap A_2\Big).$$

33. Démontrer que $\mathcal{C}_0$ est la plus petite partie de $\mathcal{P}(\mathbb{F}_p)$ (pour l'inclusion) qui soit stable par différence symétrique, par l'application $\mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x + 1$, et qui contienne l'ensemble Σ des carrés non nuls de $\mathbb{F}_p$.

Étant donnée une partie A de $\mathbb{F}_p$, on pose $f(A) = A$ si $\mathrm{Card}\, A$ est pair, et $f(A) = A \cup \{\infty\}$ si $\mathrm{Card}\, A$ est impair. Dans tous les cas, $f(A)$ est donc une partie de $\mathbb{P}^1(\mathbb{F}_p)$ de cardinal pair. On note alors $\mathcal{C}_1 = f(\mathcal{C}_0)$ l'ensemble des $f(A)$ pour $A \in \mathcal{C}_0$. On appelle *automorphisme* du code $\mathcal{C}_1$ toute application $h : \mathbb{P}^1(\mathbb{F}_p) \to \mathbb{P}^1(\mathbb{F}_p)$ vérifiant $h(B) \in \mathcal{C}_1$ pour tout $B \in \mathcal{C}_1$.

34. Démontrer que pour tout $M \in \mathrm{SL}_2(\mathbb{F}_p)$, l'homographie h_M est un automorphisme du code $\mathcal{C}_1$.