10 juin 2025
Master 1 M.F., Orsay

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

*Cet examen est consacré à une étude (partielle) des codes de résidus quadratiques, et de leurs automorphismes.*

**Partie 1 : Autour des carrés modulo $p$**

1. ($\star$) Voir le Notebook !
2. ($\star$) La réponse est oui dans le premier cas et non dans le deuxième. Noter qu'une complexité en $O(p)$ ne fait pas terminer en temps raisonnable le cas $10^9 + 7$ pour la deuxième version du Notebook.
3. Par exponention rapide, le coût du calcul de $a^{(p-1)/2}$ est de $O(\log((p-1)/2)) = O(\log p)$ multiplications. L'important est de faire ces multiplications dans $\mathbb{F}_p$ : cela revient donc à $O(\log p)$ multiplications dans $\mathbb{Z}$ (entre entiers compris entre 0 et $p-1$), et $O(\log p)$ divisions euclidiennes dans $\mathbb{Z}$ (à chaque fois on divise par $p$ un entier compris entre 0 et $p^2$). L'erreur à ne pas commettre aurait été de calculer $a^{(p-1)/2}$ avant de le réduire modulo $p$. En effet avec les valeurs de $a$ et $p$ de la question 2 cet entier aurait été monstrueux !
4. ($\star$) Voir le Notebook !
5. ($\star$) Voir le Notebook !
6. ($\star$) On obtient $50, 52, 53, 54$ et $55$.
7. ($\star$) La version via le calcul du symbole de Legendre, à savoir vérifier si $a^{\frac{p-1}{2}}$ vaut 1 ou $-1$ dans les deux premières versions a un coût qui consiste à calculer $O(p)$ fois une puissance $\frac{p-1}{2}$, ce qui par exponentiation rapide nécessite $O(\log(p))$ multiplications et divisions euclidiennes. On obtient finalement un coût total de $O(p\log(p))$ opérations arithmétiques dans $\mathbb{Z}$.
   On pouvait aussi raisonner plus naïvement avec les trois denières versions. On peut aussi calculer le carré de chaque élément non nul de $\mathbb{F}_p$, ce qui coûte $O(p)$ multiplications dans $\mathbb{F}_p$. Chaque multiplication dans $\mathbb{F}_p$ est une multiplication dans $\mathbb{Z}$ suivie d'une division euclidienne (dont on prend le reste) ; le coût est donc de $O(p)$ opérations arithmétiques dans $\mathbb{Z}$. On a donc une version plus efficace en termes du nombre d'opérations dans $\mathbb{Z}$ mais on peut se demander ce qu'il en est en termes de comparaisons (à savoir d'opérations du type `a==b` ou `a<b`).
   Les premières versions effectuent $O(p)$ comparaisons. Si on s'intéresse aux comparaisons des versions 3 et 4, la difficulté provient du fait que chaque élément de $\Sigma_0$ doit apparaître une et une seule fois dans la liste : il faut donc éliminer les répétitions. Une façon naïve de le faire est de parcourir la liste, en testant à chaque fois si l'élément qu'on rencontre fait partie de ceux qu'on a déjà vus. Le coût est alors de $O(p^2)$ comparaisons. Il s'agit de la quatrième version du Notebook. Noter que la troisième version du Notebook a le même coût dans le pire cas. Pour être plus efficace, on peut créer la liste des $p-1$ carrés (avec répétitions), la trier (ce qui coûte $O(p\log p)$ comparaisons) puis la parcourir pour éliminer les doublons. L'élimination des doublons est alors plus facile, car il s'agit juste de comparer chaque élément avec le suivant. Il s'agit de la cinquième version du Notebook.

8. Soit $u, v \in \mathbb{Z}$ tels que $u \equiv v \bmod p$ : il existe $k \in \mathbb{Z}$ tel que $u = v + kp$. Quitte à permuter $u$ et $v$, on peut supposer $k \geq 0$. Comme $X^p \equiv 1 \bmod (X^p - 1)$, on a $X^{kp} = (X^p)^k \equiv 1 \bmod (X^p - 1)$ donc $X^u = X^v X^{kp} \equiv X^v \bmod (X^p - 1)$. Ainsi, pour $j \in \mathbb{Z}/p\mathbb{Z}$ l'image de $X^j$ dans $\mathbb{F}_2[X]/(X^p - 1)$ ne dépend pas de l'entier (ici $u$ ou $v$) qu'on choisit comme représentant de la classe $j$.

9. Notons $\overline{e}(X)$ l'image de $e(X)$ dans $\mathbb{F}_2[X]/(X^p - 1)$. Comme $(P + Q)^2 = P^2 + Q^2$ pour tous $P, Q \in \mathbb{F}_2[X]$, on a

$$\overline{e}(X)^2 = \sum_{k \in \Sigma} X^{2k} = \sum_{j \in \Sigma} X^j = \overline{e}(X)$$

en effectuant le changement d'indice $j = 2k$, justifié par le fait que l'application $k \mapsto 2k$ est une bijection de $\Sigma$ dans $\Sigma$ puisque 2 est un carré non nul modulo $p$. Par ailleurs on a

$$\overline{e}(X) + \overline{e}(X^{p-1}) = \sum_{k \in \Sigma} X^k + \sum_{k \in \Sigma} X^{-k} = \sum_{k \in \mathbb{F}_p^\times} X^k$$

car $(\Sigma, -\Sigma)$ est une partition de $\mathbb{F}_p^\times$ puisque $-1$ n'est pas un carré.

10. Le polynôme $X^p - 1 \in \mathbb{F}_2[X]$ est séparable, puisque sa dérivée $pX^{p-1}$ est scindée avec 0 pour unique racine (puisque $p$ est impair) et que 0 n'est pas racine de $X^p - 1$. Notons $\mathbb{K}$ un corps de décomposition de ce polynôme sur $\mathbb{F}_2$. Alors $\mathbb{K}$ est une extension finie de $\mathbb{F}_2$, et $X^p - 1$ possède $p$ racines distinctes dans $\mathbb{K}$. L'une d'elles est 1 ; en notant $\alpha$ une autre racine on a $\alpha^p = 1$ et $\alpha \neq 1$.

11. Comme $\alpha^p = 1$ on peut évaluer en $\alpha$ les congruences obtenues à la question 9. On obtient $e(\alpha)^2 = e(\alpha)$, donc $e(\alpha)$ (qui a priori appartient à $\mathbb{K}$) est dans $\mathbb{F}_2$. On obtient aussi, puisque $\alpha \neq 1$ :

$$e(\alpha) + e(\alpha^{-1}) = \sum_{i=1}^{p-1} \alpha^i = \alpha \cdot \frac{1 - \alpha^{p-1}}{1 - \alpha} = \frac{\alpha - 1}{1 - \alpha} = -1 = 1.$$

12. L'ordre de $\alpha$ dans le groupe multiplicatif $\mathbb{F}_p^\times$ divise $p$, et ce n'est pas 1. Comme $p$ est premier, c'est donc $p$ : les éléments $\alpha^j$ sont deux à deux distincts pour $0 \leq j \leq p - 1$. En particulier, $g(X)$ est scindé à racines simples sur $\mathbb{K}$. Pour tout $j \in \Sigma_0$ on a

$$e(\alpha^j) = \sum_{k \in \Sigma} \alpha^{jk} = \sum_{i \in \Sigma} \alpha^i = e(\alpha) = 0$$

en utilisant la notation $\alpha^i$ pour $i \in \mathbb{F}_p$, justifiée par le fait que $\alpha^p = 1$, et la bijection $k \mapsto jk$, de $\Sigma$ dans lui-même. Donc toutes les racines de $g(X)$ sont des racines de $e(X)$. Finalement, $g(X)$ divise $e(X)$. On a aussi $(\alpha^j)^p - 1 = 0$ pour tout $j \in \Sigma_0$, donc de même $g(X)$ divise $X^p - 1$, et ainsi $g(X)$ divise $\operatorname{pgcd}(e(X), X^p - 1)$. Réciproquement, comme $X^p - 1$ est scindé à racines simples sur $\mathbb{K}$ (avec les $\alpha^i$ pour racines, $i \in \mathbb{F}_p$), le polynôme $\operatorname{pgcd}(e(X), X^p - 1)$ l'est aussi. Si il ne divise pas $g(X)$ alors il existe $i \in \mathbb{F}_p$ tel que $\alpha^i$ soit racine de $e(X)$ mais pas de $g(X)$, d'où $i \notin \Sigma$. Si $i = 0$ alors $e(1) = 0$, ce qui n'est pas le cas puisque $\operatorname{Card} \Sigma_0 = \frac{p-1}{2}$ est impair. Donc $i \in \mathbb{F}_p^\times \setminus \Sigma$. Comme $-1$ n'est pas un carré modulo $p$, on en déduit que $-i \in \Sigma$, donc $k \mapsto -ik$ est une bijection de $\Sigma$ dans lui-même et on a

$$0 = e(\alpha^i) = \sum_{k \in \Sigma} \alpha^{ik} = \sum_{k \in \Sigma} \alpha^{-k} = e(\alpha^{-1}) = 1 - e(\alpha) = 1$$

en utilisant la question 11. Cette contradiction termine la preuve.

13. L'algorithme d'Euclide permet de calculer le pgcd de la question 12 en $O(p^2)$ opérations arithmétiques dans $\mathbb{F}_2$.
14. ($\star$) On peut utiliser l'algorithme de Berlekamp apràs avoir effectué une division euclidienne ! Voir le Notebook !

**Partie 2 : Un exemple de code**

15. ($\star$) Il s'agit simplement de trouver les carrés modulo 7, d'en déduire le polynôme $e(X)$ et enfin de calculer $g(X)$ à partir du résultat de la question 12. Voir le Notebook !
16. On a $\mathcal{C} \subset \mathbb{F}_2^7$ puisque $g(X)$ est vu comme un diviseur de $X^7 - 1$, donc la longueur de $\mathcal{C}$ est $n = 7$. Sa dimension est $k = n - \deg(g) = 4$.
17. ($\star$) Voir le Notebook !
18. On trouve que $\mathcal{C}$ est de distance $d = 3$. Il suffit de constater que le poids minimal d'un mot non nul du code est 3. Comme il n'y a que $2^4 - 1 = 15$ mots non nuls dans le code, on peut juste les observer un par un pour le vérifier.
19. Le code $\mathcal{C}$ peut détecter $d - 1 = 2$ erreurs, et en corriger $\lfloor \frac{d-1}{2} \rfloor = 1$.
20. Une boule fermée de rayon 1 est composée de son centre, et des 7 mots qu'on obtient à partir du centre en modifiant un bit exactement. On a donc $N = 8$ ce qui donne bien $N \cdot 2^k = 2^7$ puisque $k = 4$.
21. De façon générale, pour un code $\mathcal{C}$ de dimension $k$ et de distance $d$, si on reçoit un mot $r$ qui n'est pas dans le code on cherche le mot $c \in \mathcal{C}$ le plus proche de $r$ (au sens où le poids de $r - c$ est minimal). On y parvient si $r$ est dans la boule de centre $c$ et de rayon $t = \lfloor \frac{d-1}{2} \rfloor$, où $t$ est le nombre d'erreurs que le code peut corriger. Par construction ces $2^k$ boules sont deux à deux distinctes. Un code parfait est un code pour lequel elles forment une partition de $\mathbb{F}_2^n$. Lorsque ce n'est pas le cas (ce qui malheureusement est très fréquent !), il existe des mots $r$ qui n'appartiennent à aucune de ces boules. Si on admet qu'au maximum $t$ erreurs de transmission ont lieu, on ne doit jamais recevoir un tel mot. La "place" occupée par ces mots est donc perdue.
22. On ajoute un bit de parité à tout mot de $\mathcal{C}$. Précisément, pour $m \in \mathcal{C}$ on pose $f(m) = (m, 0)$ si $m$ est de poids pair, et $f(m) = (m, 1)$ si $m$ est de poids impair. Alors le code *étendu* $\mathcal{C}' \subset \mathbb{F}_2^8$ formé par les mots $f(m)$ pour $m \in \mathcal{C}$ est de longueur 8, de dimension 4 et de distance 4.

**Partie 3 : Générateurs idempotents**

23. Comme $n$ est impair, le polynôme $X^n - 1$ est séparable (comme à la question 10) donc sans facteur carré. Donc $g_\mathcal{C}$ et $h_\mathcal{C}$ sont premiers entre eux, et il existe une relation de Bezout $U g_\mathcal{C} + V h_\mathcal{C} = 1$. On a vu en cours qu'il existe toujours une telle relation vérifiant en outre $\deg U < \deg h_\mathcal{C}$ et $\deg V < \deg g_\mathcal{C}$ ; on peut le retrouver en remplaçant $U$ par le reste de sa division euclidienne par $h_\mathcal{C}$.

24. A partir de $g_{\mathcal{C}}$ on commence par calculer $h_{\mathcal{C}}$ en faisant la division euclidienne de $X^n-1$ par $g_{\mathcal{C}}$, ce qui coûte $O(n^2)$ opérations arithmétiques dans $\mathbb{F}_2$. Puis l'algorithme d'Euclide étendu permet de calculer $U$ et $V$, avec le même coût. Enfin le produit $E = Ug_{\mathcal{C}}$ a encore le même coût (on pourrait économiser en utilisant l'algorithme de Karatsuba, mais cela ne gagnerait rien au final). Le bilan est donc un coût en $O(n^2)$ opérations arithmétiques dans $\mathbb{F}_2$.

25. ($\star$) Voir le Notebook !

26. Le polynôme $E(X)h_{\mathcal{C}}(X) = U(X)g_{\mathcal{C}}(X)h_{\mathcal{C}}(X) = U(X)\cdot(X^n-1)$ est multiple de $X^n-1$. On a donc

$$E(X)^2 = E(X)U(X)g_{\mathcal{C}}(X) = E(X) - E(X)V(X)h_{\mathcal{C}}(X) \equiv E(X) \bmod (X^n-1)$$

et

$$g_{\mathcal{C}}(X)E(X) = g_{\mathcal{C}}(X) - g_{\mathcal{C}}(X)V(X)h_{\mathcal{C}}(X) \equiv g_{\mathcal{C}}(X) \bmod (X^n-1).$$

27. Tout d'abord on a bien $\deg E \leq n-1$. Notons $\mathcal{C}'$ l'idéal de $\mathbb{F}_2[X]/(X^n-1)$ engendré par $E$. Comme $E = Ug_{\mathcal{C}}$ on a $\mathcal{C}' \subset \mathcal{C}$. Mais on a aussi $g_{\mathcal{C}}(X) \equiv g_{\mathcal{C}}(X)E(X) \bmod (X^n-1)$ donc $\mathcal{C} \subset \mathcal{C}'$. Finalement $\mathcal{C}' = \mathcal{C} : E(X)$ est un générateur de $\mathcal{C}$.

28. Si la classe de $Q$ modulo $X^n-1$ appartient à $\mathcal{C}$, il existe $S$ tel que $Q(X) \equiv S(X)g_{\mathcal{C}}(X) \bmod (X^n-1)$. On a alors d'après la question 26

$$Q(X)E(X) \equiv S(X)g_{\mathcal{C}}(X)E(X) \equiv S(X)g_{\mathcal{C}}(X) \equiv Q(X) \bmod (X^n-1).$$

Réciproquement, si cette congruence est vérifiée alors la classe de $Q(X)$ modulo $X^n-1$ appartient à l'idéal de $\mathbb{F}_2[X]/(X^n-1)$ engendré par $E(X)$, qui est $\mathcal{C}$ d'après la question précédente.

29. Soit $\widetilde{E}(X)$ un générateur de $\mathcal{C}$ pour lequel la question 28 est vraie. Comme $E(X)$ et $\widetilde{E}(X)$ appartiennent à $\mathcal{C}$ on a

$$\widetilde{E}(X) \equiv \widetilde{E}(X)\cdot E(X) \equiv E(X) \bmod (X^n-1)$$

en utilisant deux fois la propriété de la question 28. Etant donné que $\deg \widetilde{E}(X) \leq n-1$ par définition d'un générateur, on obtient $\widetilde{E}(X) = E(X)$.

30. Le polynôme $g_{\mathcal{C}}$ divise $X^n-1$ par hypothèse, et $E(X)$ par définition, donc il divise $\operatorname{pgcd}(E(X), X^n-1)$. Réciproquement, la question 28 montre que $g_{\mathcal{C}}(X)E(X) \equiv g_{\mathcal{C}}(X) \bmod (X^n-1)$ donc il existe $T \in \mathbb{F}_2[X]$ tel que

$$g_{\mathcal{C}}(X) = g_{\mathcal{C}}(X)E(X) + T(X)(X^n-1).$$

Cela montre que $\operatorname{pgcd}(E(X), X^n-1)$ divise $g_{\mathcal{C}}(X)$, donc finalement que ces deux polynômes sont égaux (puisqu'ils sont unitaires, comme tout polynôme non nul à coefficients dans $\mathbb{F}_2$).

**Partie 4 : Des homographies particulières**

31. Supposons que $g_0 = h_M \in \mathcal{H}$, avec $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{K})$. On a $h_M(\infty) = 0$ donc $c \neq 0$ et $a = 0$, et aussi $h_M(0) = \infty$ donc $d = 0$. Ainsi, $h(x) = \frac{b}{cx} = \frac{1}{x}$ pour tout $x \in \mathbb{K}^\times$, donc $b = c$ et $1 = ad - bc = -b^2$. Finalement, $-1$ est un carré dans $\mathbb{K}$. Réciproquement, si $-1 = b^2$ avec $b \in \mathbb{K}$ alors $g_0 = h_M \in \mathcal{H}$ avec $M = \left[\begin{smallmatrix} 0 & b \\ b & 0 \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{K})$.

32. Soit $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{K})$. Pour tout $x \in \mathbb{K}$ pour lequel ça a un sens, on a si $c \neq 0$ :

$$\frac{ax+b}{cx+d} = \frac{a}{c} + c^{-2} \cdot \frac{-1}{x + d/c} = t_{a/c} \circ \mu_{(c^{-1})^2} \circ g \circ t_{d/c}(x),$$

et en écrivant le produit matriciel correspondant on voit que cela fournit une décomposition de $M$ qui se traduit par $h_M = t_{a/c} \circ \mu_{(c^{-1})^2} \circ g \circ t_{d/c}$. Si $c = 0$ alors $a \neq 0$ et $d = a^{-1}$ donc $h_M = t_{ab} \circ \mu_{a^2}$.

**Partie 5 : Automorphismes d'un code**

33. Tout d'abord, le polynôme $e(X)$ défini au début de la partie 1 est un générateur de $\mathcal{C}$. En effet, le polynôme $g(X)$ défini à la fin de la partie 1 vérifie $g(X) = \mathrm{pgcd}(e(X), X^p - 1)$ d'après la question 12. Cela montre que dans $\mathbb{F}_2[X]$ les idéaux $(g(X), X^p - 1)$ et $(e(X), X^p - 1)$ sont les mêmes ; donc $e(X)$ est un générateur du code cyclique $\mathcal{C}$ engendré par $g(X)$ (au sens de la définition d'un générateur donnée au début de la partie 3).

Par ailleurs, on a des bijections entre $\mathbb{F}_2^p$, $\mathbb{F}_2[X]/(X^p - 1)$ et $\mathcal{P}(\mathbb{F}_p)$. Via ces identifications, la somme (dans $\mathbb{F}_2^p$ ou $\mathbb{F}_2[X]/(X^p - 1)$) correspond à la différence symétrique dans $\mathcal{P}(\mathbb{F}_p)$. La permutation cyclique dans $\mathbb{F}_2^p$ correspond à la multiplication par $X$ dans $\mathbb{F}_2[X]/(X^p - 1)$ et à l'application $\mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x+1$. Enfin le polynôme $e(X)$ correspond à la partie $\Sigma_0 \subset \mathbb{F}_p$. Or $\mathcal{C}$ est l'idéal de $\mathbb{F}_2[X]/(X^p - 1)$ engendré par la classe de $e(X)$, c'est-à-dire l'ensemble des sommes d'éléments de la forme $X^j e(X) \bmod (X^p - 1)$ avec $j \in \mathbb{N}$. Donc $\mathcal{C}$ correspond à la plus petite partie de $\mathcal{P}(\mathbb{F}_p)$ (pour l'inclusion) qui soit stable par différence symétrique et par permutation circulaire, et qui contienne l'ensemble $\Sigma$.

34. On a $\mathrm{Card}\Sigma = \frac{p-1}{2}$ impair, donc $\Sigma \cup \{\infty\}$ appartient à $\mathcal{C}_1$. Pour tout $r \in \mathbb{F}_p$, on pose $m_r = (r + \Sigma) \cup \{\infty\} \in \mathcal{C}_1$, où $r + \Sigma$ est l'ensemble des $r + \sigma$ avec $\sigma \in \Sigma$. D'après la question précédente, $\mathcal{C}_1$ est la plus petite partie de $\mathcal{P}(\mathbb{P}^1(\mathbb{F}_p))$ qui soit stable par différence symétrique et qui contienne les $m_r$, $m \in \mathbb{F}_p$.

D'après la question 32, il suffit de montrer que $g$, $t_a$ et $\mu_{b^2}$ sont des automorphismes de $\mathcal{C}_1$. Comme $t_a(m_r) = m_{r+a}$ et $\mu_{b^2}(m_r) = m_{b^2 r}$ pour $a \in \mathbb{F}_p$ et $b \in \mathbb{F}_p^\times$, il est clair que $t_a$ et $\mu_{b^2}$ sont des automorphismes de $\mathcal{C}_1$. Il ne reste qu'à le démontrer pour $g$.

Pour cela on note $-\Sigma$ l'ensemble des opposés des éléments de $\Sigma$ ; il s'agit exactement des non-carrés de $\mathbb{F}_p^\times$. On a alors $g(m_0) = (-\Sigma) \cup \{0\} = m_0 \oplus \mathbf{1} \in \mathcal{C}_1$ en notant $\mathbf{1} = \mathbb{P}^1(\mathbb{F}_p) \in \mathcal{C}_1$. Il reste à démontrer que $g(m_r) \in \mathcal{C}_1$ pour tout $r \in \mathbb{F}_p^\times$. Supposons que $r$ est un carré. Alors $g(m_r)$ est l'ensemble formé par 0 et les $s = -1/(r+i)$ pour $i \in \Sigma$, puisqu'on a $r + i \neq 0$. Un élément $s \in \mathbb{F}_p^\times$ appartient à $g(m_r)$ si, et seulement si, on a $(rs+1)/s \in -\Sigma$. Pour $s \in \Sigma$, cela équivaut à $rs + 1 \in -\Sigma$ ; pour $s \in -\Sigma$, cela équivaut à $rs + 1 \in \Sigma$. On a donc $g(m_r) = \{0\} \sqcup A \sqcup B$ en posant $A = \{s \in \Sigma,\, rs + 1 \in -\Sigma\}$

et $B = \{s \in -\Sigma,\, rs + 1 \in \Sigma\}$. On montre de même que $m_{g(r)} = \{0, \infty\} \sqcup B \sqcup C$ avec $C = \{s \in \Sigma,\, rs + 1 \in \Sigma\}$. Comme $A \oplus C = \Sigma$ on en déduit que $g(m_r) \oplus m_{g(r)} = m_0$ ce qui donne $g(m_r) = m_0 \oplus m_{g(r)} \in \mathcal{C}_1$. Le cas où $r$ n'est pas un carré se traite de façon analogue.