20 mai 2026
Master 1 M.F., Orsay

Corrigé du partiel de M.A.O. Calcul Formel Durée : 3 heures

Ce problème est consacré à l'algorithme de Cornacchia, qui fait l'objet de la partie 3. Cet algorithme intervient dans les tests de primalité liés aux courbes elliptiques, qui sont les plus efficaces connus à ce jour (hormis ceux consacrés à des nombres premiers d'une type particulier, comme les nombres de Mersenne). La preuve de la partie 4 est fondée sur un article de Basilla paru en 2004.

Partie 1 : Carrés dans certains corps finis

1. Pour commencer, on représente une classe mod p par l'unique élément compris entre 0 et $p-1$ qu'elle contient. Pour additionner, soustraire ou multiplier, on effectue l'opération correspondante dans $\mathbb{Z}$ sur les représentants, puis on réduit modulo p : le coût est de $O(1)$ opérations arithmétiques dans $\mathbb{Z}$ puisque la division euclidienne est l'une des 4 opérations dans $\mathbb{Z}$. Pour calculer l'inverse de la classe de x, avec $1 \leq x \leq p-1$, on calcule une relation de Bezout $ux + vp = 1$ et alors l'inverse est la classe de u. En utilisant l'algorithme d'Euclide étendu cela coûte $O(\log p)$ opérations arithmétiques dans $\mathbb{Z}$.
2. Si $x = y^2$ alors $x^{(p-1)/2} = y^{p-1} = 1$. Donc le polynôme $X^{(p-1)/2} - 1$ a pour racines tous les carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$. Or il y en a $(p-1)/2$ (car l'application $y \mapsto y^2$ est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans lui-même de noyau $\{-1, 1\}$) donc ce sont les seules.
3. ($\star$) Voir le Jupyter Notebook !
4. ($\star$) Voir le Jupyter Notebook ! a_1 et a_2 sont des carrés mod p, mais pas a_3.
5. Par exponentiation rapide, le coût est $O(\log p)$ multiplications dans $\mathbb{Z}/p\mathbb{Z}$, donc $O(\log p)$ opérations arithmétiques dans $\mathbb{Z}$ en utilisant la question 1.
6. (a) L'application $\mathbb{K} \to \mathbb{K}$, $y \mapsto y^2$ est un morphisme de corps (c'est le morphisme de Frobenius), car $\mathbb{K}$ est de caractéristique 2. Elle est donc injective ; comme $\mathbb{K}$ est fini elle est bijective.
   (b) En posant $y = x^{2^{n-1}}$ on a $y^2 = x^{2^n} = x$ donc y est la racine carrée cherchée.
   (c) Par exponentiation rapide, on calcule y en $O(n)$ multiplications dans $\mathbb{K}$.

Partie 2 : Une équation diophantienne

7. ($\star$) On remarque déjà que si (x, y) est une solution de (1) alors x et y sont compris entre 1 et $\sqrt{p}$. L'algorithme le plus naïf consiste donc à faire parcourir cet intervalle à x, et aussi à y ; pour chaque couple (x, y) on calcule $x^2 + dy^2$ et on teste si c'est égal à p. Le coût est alors de $O(p)$ opérations arithmétiques dans $\mathbb{Z}$.
   On peut faire mieux en calculant la liste L des x^2, pour x compris entre 1 et $\sqrt{p}$. En posant $c = x^2$ et $c' = y^2$, résoudre (1) se ramène à trouver $c, c' \in L$ tels que $c + dc' = p$. On peut alors faire parcourir à c' la liste L, et pour chaque valeur de c' tester si $p - dc' \in L$.
   L'implémentation la plus simple est probablement de voir L comme un dictionnaire, la valeur x correspondant à la clef x^2. Cela permet de tester facilement si $p - dc' \in L$, et si oui de trouver x tel que $p - dc' = x^2$. Accéder à un dictionnaire ne coûte aucune

opération arithmétique (en fait si, mais elles sont cachées dans l'implémentation des dictionnaires). Le coût de l'algorithme est alors en $O(\sqrt{p})$ opérations arithmétiques dans $\mathbb{Z}$. En outre le coût (amorti) en temps de la recherche dans un dictionnaire est en $O(1)$ donc le temps de calcul est aussi en $O(\sqrt{p})$.

Une autre façon de faire est de calculer la racine carrée (si elle est entière) de $p - dy^2$, pour chaque y possible. On peut le faire par dichotomie : initialement on sait qu'elle est entre 0 et $\lfloor\sqrt{p}\rfloor$. A chaque étape, on élève au carré le milieu de l'intervalle où elle se situe, et on compare ce carré à $p - dy^2$ pour couper l'intervalle en deux. On a ainsi des intervalles dont les bornes sont entières, et dont la longueur est (essentiellement) divisée par deux à chaque étape. Au bout de $O(\log p)$ étapes cet intervalle est de longueur 1. Finalement le coût de ce calcul de racine carrée entière est de $O(\log p)$ multiplications dans $\mathbb{Z}$; il permet soit de trouver la racine carrée, soit de montrer que $p - dy^2$ n'est pas un carré parfait. Au total, cela permet de résoudre l'équation (1) en $O(\sqrt{p}\log p)$ opérations arithmétiques dans $\mathbb{Z}$.

Une dernière méthode (implémentée dans le corrigée) consiste à faire tester directement par `Sage` si un entier k est un carré : on regarde si $k = \lfloor\sqrt{k}\rfloor^2$. La méthode `k.is_square()` fait cela encore plus efficacement (mais ici, lorsque k est un carré on a aussi besoin de sa racine carrée).

8. ($\star$) Voir le Jupyter Notebook ! On trouve $(2, 17)$ pour d_1, $(30, 7)$ pour d_2, et pas de solution pour d_3.
9. Voir question 7.
10. (a) Si $\delta \geq 2$ divise à la fois x et y, alors δ^2 divise $p = x^2 + dy^2$ ce qui est contradictoire.
    (b) On a $1 \leq y \leq p - 1$ et p premier donc $\mathrm{pgcd}(y, p) = 1$. Par l'algorithme d'Euclide étendu on trouve $u \in \mathbb{Z}$ tel que $uy \equiv 1 \bmod p$. On a alors $(ux)^2 \equiv -du^2y^2 \equiv -d \bmod p$; en particulier, $-d$ est un carré modulo p.
    (c) Pour tout $x \in \mathbb{Z}$ on a $x^2 \equiv 0 \bmod 4$ ou $x^2 \equiv 1 \bmod 4$. Si $d \equiv 1 \bmod 4$ alors pour tous $x, y \in \mathbb{Z}$ l'entier $x^2 + dy^2$ est congru à $x^2 + y^2$ donc à 0, 1 ou 2 modulo 4 : si $p \equiv 3 \bmod 4$ l'équation (1) n'a aucune solution.
11. ($\star$) Voir le Jupyter Notebook ! Une méthode est d'utiliser la question 10 (c) en exhibant un couple (d, p) (par exemple $(5, 7)$) tel que $d \equiv 1 \bmod 4$, $p \equiv 3 \bmod 4$ et que $-d$ soit un carré modulo p.

Partie 3 : Un algorithme efficace

12. Par l'algorithme d'Euclide, l'entier N existe et $r_N = \mathrm{pgcd}(p, t) = 1$ puisque p est premier et $1 \leq t < p$. La suite (r_k) étant strictement décroissante avec $r_N = 1 \ < \sqrt{p} < r_0 = p$, il existe k compris entre 1 et N tel que $r_k < \sqrt{p} \leq r_{k-1}$. L'inégalité est stricte car $\sqrt{p}$ n'est pas un entier.
13. ($\star$) Voir le Jupyter Notebook !
14. ($\star$) Voir le Jupyter Notebook ! On obtient $t = 45209247$.
15. ($\star$) Grâce au théorème 1 il suffit de calculer $x = r_k$ et $y = |v_k|$, puis de tester si $x_k + dy_k^2 = p$.
16. ($\star$) Voir le Jupyter Notebook ! On n'obtient pas de solution pour d_1, mais on trouve $(21664, 1633)$ pour d_2 et $(29506, 109)$ pour d_3.

17. On sait que l'algorithme d'Euclide étendu coûte $O(\log p)$ opérations arithmétiques dans $\mathbb{Z}$. Ici c'est le même algorithme sauf qu'on l'interrompt avant la fin : le coût est encore $O(\log p)$ opérations arithmétiques dans $\mathbb{Z}$. Par hypothèse le coût supplémentaire lié à l'utilisation de la méthode `x.sqrt()` à la question 13 ne change pas cette estimation.

Partie 4 : Preuve du théorème 1

18. On procède par récurrence ; les propriétés cherchées sont vraies pour $i = 1$. Si elles sont vraies pour un certain i, alors v_{i-1} et $-q_i v_i$ ont même signe, à savoir celui de $(-1)^i$. Donc $v_{i+1} = v_{i-1} + (-q_i v_i)$ est aussi du signe de $(-1)^i$, et on a $|v_{i+1}| \geq |-q_i v_i| \geq |v_i|$.
19. Soit i tel que $0 \leq i \leq N+1$. On a
$$r_i^2 = (u_i p + v_i t)^2 \equiv v_i^2 t^2 \equiv -d v_i^2 \bmod p.$$
20. Par la question précédente, $r_k^2 + d v_k^2$ est un multiple de p, et un entier strictement positif. Par définition de k, on a $r_k^2 < p$. Donc en supposant que $d v_k^2 < p$, on en déduit $r_k^2 + d v_k^2 < 2p$ d'où $r_k^2 + d v_k^2 = p$.
21. Montrons par récurrence que L est engendré par w_i et w_{i+1}. C'est vrai pour $i = 0$ par définition. Si c'est vrai pour un certain $i \geq 0$ alors c'est vrai pour $i+1$ car $w_{i+2} = w_i - q_{i+1} w_{i+1}$.
22. Soit (x, y) une solution de l'équation (1). On a $x^2 = p - dy^2 \equiv (yt)^2 \bmod p$ donc (quitte à changer x en $-x$) on peut supposer que $x \equiv yt \bmod p$. Il existe donc $j \in \mathbb{Z}$ tel que $x = yt + pj$, ce qui donne $(x, y) = j(p, 0) + y(t, 1) \in L$.
23. Si $k = 1$ alors $|v_k| = 1 \leq y$ et $d v_k^2 = d < p$. On peut donc supposer $k \geq 2$. Notons
$$(x_1, y_1) = (-1)^{k-1} w_{k-2} = ((-1)^{k-1} r_{k-2}, (-1)^{k-1} v_{k-2})$$
et
$$(x_2, y_2) = (-1)^k w_{k-1} = ((-1)^k r_{k-1}, (-1)^k v_{k-1}).$$
On a alors $x_1 x_2 < 0$, $|x_2| < |x_1|$, $y_1 \geq 0$ et $y_2 > 0$ d'après la question 18. De plus les couples (x_1, y_1) et (x_2, y_2) engendrent L d'après la question 21.
Soit (x, y) une solution de l'équation (1). D'après la question 22, quitte à changer x en $-x$ on peut supposer $(x, y) \in L$. On a aussi $y > 0$ et
$$x^2 < x^2 + dy^2 = p < r_{k-1}^2 = x_2^2$$
par définition de k, d'où $|x| < |x_2|$. On peut donc appliquer le Lemme 2 admis par l'énoncé avec $L_0 = L$, ce qui donne
$$y \geq y_1 + \left\lfloor \frac{-x_1}{x_2} \right\rfloor y_2 = (-1)^{k-1} \left(v_{k-2} - \left\lfloor \frac{r_{k-2}}{r_{k-1}} \right\rfloor v_{k-1} \right) = (-1)^{k-1} v_k = |v_k|$$
en utilisant la définition de la suite (v_j) et la question 18. On a donc $d v_k^2 \leq dy^2 = p - x^2 < p$.
Pour conclure la preuve du théorème 1, supposons que l'équation (1) possède une solution (x, y). On vient d'en déduire que $d v_k^2 < p$, et alors d'après la question 20 le couple $(r_k, |v_k|)$ est une solution.

24. Quitte à remplacer chaque x_i par $-x_i$ (ce qui modifie L_0 en conséquence), on peut supposer $x_2 > 0$, et on a alors $x_1 < -x_2 < 0$.

Posons $u_1 = (x_1, y_1)$, $u_2 = (x_2, y_2)$, et $u_0 = u_1 + \left\lfloor \frac{-x_1}{x_2} \right\rfloor u_2$. Notons (x_0, y_0) les coordonnées de u_0. Alors on a $u_0 \in L_0$, $y_0 \geq y_2 > 0$, et $-x_2 < x_1 + \left\lfloor \frac{-x_1}{x_2} \right\rfloor x_2 = x_0 \leq 0$ d'où $|x_0| < |x_2|$. Donc le point u_0 fait partie des couples sur lesquels on prend le minimum de y.

Considérons maintenant un couple $(x, y) \in L_0$ tel que $y > 0$ et $|x| < |x_2|$. Il ne reste qu'à démontrer l'inégalité $y \geq y_0$. Il existe $a, b \in \mathbb{Z}$ tels que $(x, y) = au_1 + bu_2$. Si $a \leq 0$ alors $0 < y = ay_1 + by_2 \leq by_2$ donc $b > 0$, ce qui donne $b \geq 1$ et $x = ax_1 + bx_2 \geq bx_2 \geq x_2 > 0$: c'est impossible. Donc $a \geq 1$.

Comme $|x| = |ax_1 + bx_2| < x_2$, on a $-x_2 - ax_1 < bx_2$ d'où $-1 + a\frac{-x_1}{x_2} < b$ avec b entier, ce qui donne $b \geq \lfloor -ax_1/x_2 \rfloor$. On en déduit que

$$\begin{aligned} y - y_0 &= (a-1)y_1 + (b - \lfloor -x_1/x_2 \rfloor)y_2 \\ &\geq (a-1)y_1 + (\lfloor -ax_1/x_2 \rfloor - \lfloor -x_1/x_2 \rfloor)y_2 \\ &\geq 0 \end{aligned}$$

car $a \geq 1$, ce qui termine la preuve.