17 mai 2023
Master 1 M.F., Orsay

Corrigé du partiel de M.A.O. Calcul Formel

Partie 1 : Carrés dans $\mathbb{F}_p^*$

1. Si $x = a^2$ avec $a \in \mathbb{F}_p^*$ alors $y^2 = x^{(p-1)/2} = a^{p-1} = 1$. Donc le polynôme $X^{(p-1)/2} - 1$ possède pour racines tous les carrés de $\mathbb{F}_p^*$. Or il y a exactement $(p-1)/2$ carrés, c'est-à-dire autant que le degré de ce polynôme : ce sont donc les seules racines. Si $x \in \mathbb{F}_p^*$ n'est pas un carré, on a donc $y^2 = x^{(p-1)/2} \neq 1$. Par ailleurs $(y^2)^2 = x^{p-1} = 1$ donc y^2 est une racine du polynôme $X^2 - 1 = (X-1)(X+1)$. Finalement on a bien $y^2 = -1$ (on a évidemment $1 \neq -1$ dans $\mathbb{F}_p$ puisque p est impair).
2. On peut calculer $x^{(p-1)/4}$ par exponentiation rapide, en utilisant $O(\log((p-1)/4)) = O(\log(p))$ multiplications dans $\mathbb{F}_p$.
3. Notons Y la variable aléatoire égale au nombre de passages dans la boucle. Le fait de choisir au hasard un élément $x \in \mathbb{F}_p^*$, de calculer $y = x^{(p-1)/4}$ et de tester si $y^2 = -1$ est une expérience de Bernoulli, dont le succès est le fait que $y^2 = -1$. La probabilité de succès est $1/2$, car d'après la question 1 le succès est équivalent au fait que x ne soit pas un carré, ce qui a une chance sur deux de se produire (il est clairement sous-entendu dans l'énoncé que le choix aléatoire de x est effectué suivant la loi uniforme sur $\mathbb{F}_p^*$, et il est rappelé qu'il y a autant de carrés que de non-carrés). Comme Y est le temps d'attente du premier succès, Y suit la loi géométrique de paramètre $1/2$. L'espérance de Y vaut donc $1/(1/2) = 2$. Comme chaque passage dans la boucle coûte $O(\log(p))$ multiplications dans $\mathbb{F}_p$ d'après la question 2, on a $X = O(Y \log(p))$ donc $E(X) = O(E(Y)\log(p)) = O(\log(p))$. C'est bien mieux que le coût de l'algorithme naïf consistant à tester un par un tous les éléments $y \in \mathbb{F}_p^*$ jusqu'à en trouver un tel que $y^2 = -1$, qui est $O(p)$ (et pas mieux que cela, car si on n'a pas de chance les deux éléments y qui conviennent seront parmi les derniers qu'on va tester).
4. ($\star$) Voir le Jupyter Notebook !
5. ($\star$) On obtient 540 ou 469.
6. Fixons un nombre premier $p \equiv 1 \bmod 4$. Quand on applique plusieurs fois la fonction `racine` de la question 4 avec cette même valeur de p, on obtient deux valeurs différentes. Montrons qu'il y a exactement deux éléments $y \in \mathbb{F}_p^*$ tels que $y^2 = -1$. Tout d'abord il y en a au plus deux, car ce sont des racines du polynôme $X^2 + 1$ dans $\mathbb{F}_p$. Ensuite il y en a au moins une, notée y_0, d'après la question 1 : il suffit de poser $y_0 = x_0^{(p-1)/4}$ où $x_0 \in \mathbb{F}_p^*$ n'est pas un carré, et un tel x_0 existe bien. Enfin, on a $(-y_0)^2 = y_0^2 = -1$ et $y_0 \neq -y_0$ (puisque $2y_0 \neq 0$, car 2 est inversible dans $\mathbb{F}_p$), donc il y a exactement deux solutions : y_0 et $-y_0$.
7. On reprend les notations de la question précédente. Par construction, y_0 peut être renvoyé par la fonction `racine`, si le générateur aléatoire donne $x = x_0$. Or on sait que $\mathbb{F}_p^*$ est cyclique : notons ω un générateur, et supposons que le générateur aléatoire donne $x = \omega^2 x_0$ (qui est également un non-carré). Alors on a $y = x^{(p-1)/4} = \omega^{(p-1)/2} y_0 = -y_0$ (puisque $\omega^{(p-1)/2}$ est l'unique élément d'ordre 2 dans $\mathbb{F}_p^*$, à savoir -1). Donc chacun des deux éléments $y \in \mathbb{F}_p^*$ tels que $y^2 = -1$ peut être renvoyé par la fonction `racine`.

8. Si $p = 2$, l'élement $y = 1$ vérifie $y^2 = 1 = -1$. Si p est un nombre premier congru à 3 modulo 4, il n'existe aucun $y \in \mathbb{F}_p^*$ tel que $y^2 = -1$. En effet si un tel y existait, on aurait $1 = y^{p-1} = (-1)^{(p-1)/2} = -1$ dans $\mathbb{F}_p$, ce qui est impossible.

Partie 2 : Autour de l'algorithme d'Euclide étendu

9. Notons j_1 le premier indice tel que $r_{j_1} = 0$. On a alors $0 = r_{j_1} < \ldots < r_1 < r_0 = a$. Notons E l'ensemble formé par les entiers $j \in \{0, \ldots, j_1\}$ tels que $r_j < R$. Comme $0 < R \leq a$, on a $j_1 \in E$ et $0 \notin E$. Donc l'ensemble fini E est non vide : il possède un plus petit élément j_0, et on a $j_0 \neq 0$ donc $j_0 \geq 1$.
10. La relation $u_j v_{j+1} - u_{j+1} v_j = (-1)^j$ est vraie pour $j = 0$ puisque $u_0 = v_1 = 1$ et $u_1 = v_0 = 0$. Si elle est vraie pour $j-1$, avec $1 \leq j \leq j_1 - 1$, alors on utilise les relations $u_{j+1} = u_{j-1} - u_j q_j$ et $v_{j+1} = v_{j-1} - v_j q_j$ où q_j est le quotient dans la division euclidienne de r_{j-1} par r_j, de telle sorte que $r_{j+1} = r_{j-1} - r_j q_j$. On en déduit

$$u_j v_{j+1} - u_{j+1} v_j = u_j(v_{j-1} - v_j q_j) - (u_{j-1} - u_j q_j) v_j = u_j v_{j-1} - u_{j-1} v_j = (-1)^j$$

ce qui termine la récurrence.
11. On a $0 = r_{j_1} \leq r_{j_0} < R$ par construction de j_0, puisque $j_0 \leq j_1$. On a aussi $r_{j_0} = a\,u_{j_0} + b\,v_{j_0} \equiv b\,v_{j_0} \bmod a$. Il reste à démontrer que $v_{j_0} \neq 0$ et $|v_{j_0}| < V$. Pour cela, on commence par constater que

$$u_j \text{ est du signe de } (-1)^j, \quad v_j \text{ du signe de } (-1)^{j+1}, \quad |u_j| \leq |u_{j+1}| \quad \text{et} \quad |v_j| \leq |v_{j+1}|$$

pour tout j tel que $0 \leq j \leq j_1 - 1$; cela découle, par une récurrence immédiate, des relations $u_{j+1} = u_{j-1} - u_j q_j$ et $v_{j+1} = v_{j-1} - v_j q_j$ où $q_j \geq 1$ est le quotient dans la division euclidienne de r_{j-1} par r_j, de telle sorte que $r_{j+1} = r_{j-1} - r_j q_j$.
Considérons maintenant un entier j tel que $0 \leq j \leq j_1 - 1$. On a d'après la question 10 :

$$\begin{aligned} a &= |v_{j+1} a u_j - v_j a u_{j+1}| = |v_{j+1}(r_j - b v_j) - v_j(r_{j+1} - b v_{j+1})| \\ &= |v_{j+1} r_j - v_j r_{j+1}| = |v_{j+1}| r_j + |v_j| r_{j+1} \geq |v_{j+1}| r_j \end{aligned}$$

car v_j et v_{j+1} sont de signes opposés. Pour $j = j_0 - 1$ on a donc $R|v_{j_0}| \leq |v_{j_0}| r_{j_0 - 1} \leq a < RV$ par minimalité de j_0, d'où $|v_{j_0}| < V$. Enfin, si on v_{j_0} était nul, alors on aurait soit $r_{j_0} = 0$ (et alors u_{j_0} serait nul lui aussi, ce qui contredirait la question 10), soit $|r_{j_0}| = a|u_{j_0}| \geq a = r_0$ (d'où $j_0 = 0$ ce qui contredit la question 9).
12. ($\star$) Voir le Jupyter Notebook !
13. ($\star$) On obtient $r_{j_0} = 115$ et $v_{j_0} = 5$.
14. On effectue partiellement l'algorithme d'Euclide étendu, donc le coût est majoré par celui de l'algorithme d'Euclide étendu qui est en $O(\log a)$ opérations arithmétiques dans $\mathbb{Z}$ (en fait même en $O(\log b)$ opérations, ce qui est plus précis si b est beaucoup plus petit que a, mais ce raffinement est inutile ici).

Partie 3 : Sommes de deux carrés, approche naïve

15. ($\star$) On peut construire la liste `L` des s^2 pour s entier compris entre 1 et la partie entière de $\sqrt{p}$, ce qui coûte $O(\sqrt{p})$ multiplications. Ensuite pour $x = s^2$ dans `L`, on teste si $p - x = p - s^2$ figure dans la liste `L`. On s'arrête quand c'est le cas. Voir le Notebook !

16. ($\star$) On trouve $s = 15$ et $t = 28$.

17. ($\star$) L'algorithme précédent coûte $O(\sqrt{p})$ opérations et $O(\sqrt{p})$ recherches dans une liste de $O(\sqrt{p})$ éléments. A priori, chaque telle recherche nécessite de parcourir la liste en entier (dans le pire des cas), ce qui conduit à $O(p)$ comparaisons (et pas moins). Cependant il s'agit d'une liste triée, donc on peut tester si `x in L` par dichotomie, en $O(\log(\sqrt{p})) = O(\log(p))$ comparaisons par élément `x`, donc $O(\sqrt{p}\log(p))$ au total.
    En fait on peut même faire encore mieux : une fois la liste `L` construite, on utilise deux indices $x = s^2$ et $y = t^2$ pour la parcourir, x à partir du début et y à partir de la fin. Lorsque $x + y < p$, on remplace x par l'élément suivant de `L`. Au contraire, lorsque $x + y > p$, on remplace y par l'élément précédent. A un moment, on aura $x + y = p$ et on renverra x et y (ou plutôt leurs racines carrées, qui sont leurs positions dans la liste `L`). De cette façon, on a au maximum $2\sqrt{p}$ passages dans la boucle donc on utilise seulement $O(\sqrt{p})$ comparaisons. Voir le Notebook !

Partie 4 : Sommes de deux carrés, algorithme efficace

18. Comme p est premier et congru à 1 modulo 4, la question 4 montre comment trouver un élément $y \in \mathbb{F}_p^*$ tel que $y^2 = -1$. Notons b le représentant dans $\mathbb{Z}$ de la classe $y \in \mathbb{Z}/p\mathbb{Z}$ tel que $0 < b < p$. On reprend les notations de la partie 2 avec $a = p$, cet entier b, et des entiers R et V qu'on précisera plus loin. D'après la question 11, p divise $r_{j_0} - b\, v_{j_0}$, donc dans $\mathbb{Z}/p\mathbb{Z}$ on a $r_{j_0}^2 + v_{j_0}^2 = (r_{j_0} - y\, v_{j_0})(r_{j_0} + y\, v_{j_0}) = 0$ puisque $y^2 = -1$. Autrement dit, l'entier $r_{j_0}^2 + v_{j_0}^2$ est multiple de p. Or cet entier est strictement positif puisque $v_{j_0} \neq 0$ (d'après la question 11), et cette question donne aussi

$$r_{j_0}^2 + v_{j_0}^2 \leq (R-1)^2 + (V-1)^2 < 2p$$

    en prenant $R = V = \lceil \sqrt{p} \rceil$ (qui est le plus petit entier supérieur ou égal à $\sqrt{p}$; comme p n'est pas un carré, on a $R = V = \lfloor \sqrt{p} \rfloor + 1$) ; on a bien $0 < R \leq p < RV$. On a donc $r_{j_0}^2 + v_{j_0}^2 = p$: les entiers $s = r_{j_0}$ et $t = v_{j_0}$ déterminés à la question 12 conviennent.

19. D'après la question 3, l'algorithme de la question 4 coûte en moyenne $O(\log p)$ multiplications dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; chacune d'entre elles est une multiplication dans $\mathbb{Z}$ suivie d'une division euclidienne par p. Cela représente donc $O(\log p)$ opérations dans $\mathbb{Z}$. Par ailleurs la question 14 montre qu'on peut aussi déterminer r_{j_0} et v_{j_0} en $O(\log p)$ opérations dans $\mathbb{Z}$. Finalement, l'algorithme de la question précédente coûte donc $O(\log p)$ opérations arithmétiques dans $\mathbb{Z}$. C'est beaucoup plus efficace que l'algorithme de la question 15.

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

21. ($\star$) On trouve

$$s = 8083111 \text{ et } t = 1394180.$$