20 mai 2026
Master 1 M.F., Orsay

Partiel de M.A.O. Calcul Formel Durée : 3 heures

L'accès à internet et l'utilisation des téléphones portables et montres connectées sont interdits.

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. Sauf mention explicite du contraire, toutes les fonctions de `Sage` peuvent être utilisées dans les codes.

Il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes. La partie 1 porte sur les carrés dans un corps fini ; c'est une sorte de préambule qui n'est pas directement utilisé dans la suite (sauf éventuellement pour la question 11). Les parties 2 à 4 étudient des algorithmes de résolution d'une équation diophantienne.

Partie 1 : Carrés dans certains corps finis

Dans cette partie on note p un nombre premier impair.

1. Rappeler en quelques mots comment on peut implémenter les quatre opérations dans $\mathbb{Z}/p\mathbb{Z}$ (addition, soustraction, multiplication, division), à partir de ces opérations dans $\mathbb{Z}$. Donner le coût de chacune d'entre elles, en nombre d'opérations dans $\mathbb{Z}$.
2. Soit $x \in \mathbb{Z}/p\mathbb{Z}$ non nul. Démontrer qu'on a $x^{(p-1)/2} = 1$ si, et seulement si, x est un carré.
3. ($\star$) En utilisant la question précédente, implémenter en `Sage` une fonction `est_carre` qui prend en entrée deux entiers a et p (avec p premier) et renvoie :
$$\begin{cases} \texttt{nul} \text{ si } a \equiv 0 \bmod p, \\ \texttt{carre} \text{ s'il existe } b \in \mathbb{Z} \text{ tel que } \ a \equiv b^2 \not\equiv 0 \bmod p, \\ \texttt{non\_carre} \text{ sinon.} \end{cases}$$
4. ($\star$) Dans cette question seulement, on pose $p = 10^9 + 7$. En utilisant la fonction `est_carre`, déterminer si chacun des entiers suivants est un carré modulo p :
$$a_1 = 12345678, \quad a_2 = 123456789, \quad a_3 = 1234567890.$$
5. Déterminer le coût, en nombre d'opérations arithmétiques dans $\mathbb{Z}$, de la fonction `est_carre` implémentée à la question 3.
6. Dans cette question 6 on note $\mathbb{K}$ un corps fini de cardinal 2^n, avec $n \geq 1$, et on fixe un élément $x \in \mathbb{K}$.
   (*a*) Démontrer qu'il existe un élément $y \in \mathbb{K}$, et un seul, tel que $y^2 = x$.
   (*b*) Expliquer comment on peut calculer efficacement y à partir de x.
   (*c*) En suivant la méthode de la question (*b*), quel est le coût du calcul de y (en nombre d'opérations arithmétiques dans $\mathbb{K}$) ?

Partie 2 : Une équation diophantienne

Dans toute la suite du problème on se donne un nombre premier impair p et un entier d tel que $1 \leq d \leq p-1$. On cherche à résoudre l'équation

$$x^2 + dy^2 = p \text{ d'inconnues } x, y \in \mathbb{N}^*. \tag{1}$$

7. ($\star$) Implémenter en `Sage` une fonction `recherche_naive` qui prend en entrée deux entiers p et d (avec p premier et $1 \leq d \leq p-1$) et renvoie une solution (x, y) de l'équation (1) si une telle solution existe, et la chaîne de caractères `pas_de_solution` sinon. *Le calcul du coût de cette fonction fera l'objet de la question 9 ci-dessous. La moitié des points de cette question 7 sera attribuée quelle que soit la complexité de la fonction* `recherche_naive`. *Pour obtenir la totalité des points, il faut que le coût soit en* $O(\sqrt{p})$ *ou en* $O(\sqrt{p}\log p)$ *opérations arithmétiques dans* $\mathbb{Z}$.
8. ($\star$) Dans cette question on prend $p = 2027$. Pour chacun des entiers d suivants, que renvoie la fonction `recherche_naive` ?

$$d_1 = 7, \quad d_2 = 23, \quad d_3 = 31.$$

9. Déterminer le coût, en nombre d'opérations arithmétiques dans $\mathbb{Z}$, de la fonction `recherche_naive` implémentée à la question 7. *On rappelle que seules les opérations arithmétiques dans* $\mathbb{Z}$ *doivent être prises en compte dans le calcul. D'éventuelles remarques sur la façon d'implémenter efficacement cette fonction, ou sur l'influence d'autres facteurs sur le temps d'exécution, seront appréciées si elles sont pertinentes.*
10. Dans cette question 10 on suppose que l'équation (1) possède une solution (x, y). Les questions (a), (b), (c) sont indépendantes.
    (a) Démontrer que x et y sont premiers entre eux.
    (b) Démontrer que $-d$ est un carré modulo p, et expliquer comment construire à partir de x et y un entier a tel que $a^2 \equiv -d \bmod p$.
    (c) Que dire si $d \equiv 1 \bmod 4$ et $p \equiv 3 \bmod 4$?
11. ($\star$) En utilisant (ou pas) la question précédente et/ou la partie 1, exhiber un couple (d, p) tel que $-d$ soit un carré modulo p mais que l'équation (1) ne possède aucune solution.

Partie 3 : Un algorithme efficace

Dans cette partie, on étudie un algorithme qui permet de résoudre efficacement l'équation (1). On se donne p et d tels que

$$p \geq 3 \text{ est premier, } 1 \leq d \leq p-1, \text{ et } -d \text{ est un carré modulo } p. \tag{2}$$

On suppose donné un entier t tel que

$$1 \leq t \leq p/2 \qquad \text{et} \qquad t^2 \equiv -d \bmod p. \tag{3}$$

On pose $r_0 = p$, $r_1 = t$, et pour tout entier $i \geq 1$ on note $r_{i-1} = q_i r_i + r_{i+1}$ la division euclidienne de r_{i-1} par r_i. On note N l'entier tel que $r_N \neq 0$ et $r_{N+1} = 0$.

On pose aussi

$$u_0 = 1, \quad u_1 = 0, \quad u_{i+1} = u_{i-1} - q_i u_i \text{ pour } 1 \leq i \leq N,$$

et

$$v_0 = 0, \quad v_1 = 1, \quad v_{i+1} = v_{i-1} - q_i v_i \text{ pour } 1 \leq i \leq N.$$

Enfin on note k l'entier tel que $r_k < \sqrt{p} < r_{k-1}$. Dans cette partie on admet le théorème suivant :

Théorème 1 *Si l'équation* (1) *possède une solution, alors* $(x, y) = (r_k, |v_k|)$ *en est une.*

12. Justifier que l'entier k existe.
13. ($\star$) On rappelle que si x désigne un élément de $\mathbb{Z}/p\mathbb{Z}$, alors en `Sage` la méthode `x.sqrt()` renvoie une racine carrée de x modulo p. En utilisant cette méthode, implémenter en `Sage` une fonction `calcul_t` qui prend en entrée deux entiers p et d vérifiant (2) et renvoie un entier t vérifiant $1 \leq t \leq p/2$ et $t^2 \equiv -d \bmod p$.
14. ($\star$) Que renvoie la fonction `calcul_t` lorsque $p = 10^9 + 7$ et $d = 123$?
15. ($\star$) En utilisant le théorème 1, implémenter en `Sage` une fonction `recherche_efficace` qui prend en entrée deux entiers p et d vérifiant (2) et renvoie une solution (x, y) de l'équation (1) s'il en existe, et la chaîne de caractères `pas_de_solution` sinon.
16. ($\star$) Dans cette question on prend $p = 10^9 + 7$. Pour chacun des entiers d suivants, que renvoie la fonction `recherche_efficace` ?

$$d_1 = 123, \quad d_2 = 199, \quad d_3 = 10891.$$

17. Déterminer le coût, en nombre d'opérations arithmétiques dans $\mathbb{Z}$, de la fonction `recherche_efficace` implémentée à la question 15. *On considèrera qu'un appel à la méthode* `x.sqrt()` *évoquée à la question 13 coûte* $O(\log p)$ *opérations arithmétiques dans* $\mathbb{Z}$.

Partie 4 : Preuve du théorème 1

Dans cette partie on va démontrer le théorème 1. Pour cela on rappelle que

$$r_i = pu_i + tv_i \text{ pour tout } i \in \{0, \ldots, N+1\}.$$

18. Démontrer que

$$(-1)^{i-1} v_i \geq 0 \quad \text{et} \quad |v_{i-1}| \leq |v_i| \quad \text{pour tout } i \in \{1, \ldots, N+1\}.$$

19. Démontrer que $r_i^2 \equiv -dv_i^2 \bmod p$ pour tout i tel que $0 \leq i \leq N+1$.
20. Démontrer que si $dv_k^2 < p$ alors le couple (x, y) formé par $x = r_k$ et $y = |v_k|$ est une solution de l'équation (1).

Notons L le sous-groupe de $\mathbb{Z}^2$ engendré par les couples $(p, 0)$ et $(t, 1)$, c'est-à-dire l'ensemble des $a(p, 0) + b(t, 1)$ avec $a, b \in \mathbb{Z}$. Posons aussi $w_i = (r_i, v_i)$ pour tout i tel que $0 \leq i \leq N+1$.

21. Démontrer que pour tout $i \in \{0, \ldots, N\}$, le sous-groupe L est engendré par w_i et w_{i+1}.
22. Démontrer que si (x, y) est une solution de l'équation (1) alors (x, y) ou $(-x, y)$ appartient à L.

Pour terminer la preuve du théorème 1 on admet provisoirement le lemme suivant :

Lemme 2 *Soient* $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ *tels que* $x_1 x_2 < 0$, $|x_2| < |x_1|$, $y_1 \geq 0$ *et* $y_2 > 0$. *Notons* L_0 *le sous-groupe de* $\mathbb{Z}^2$ *engendré par les couples* (x_1, y_1) *et* (x_2, y_2). *Alors la valeur minimale de* y, *prise sur l'ensemble des couples* $(x, y) \in L_0$ *tels que* $y > 0$ *et* $|x| < |x_2|$, *est obtenue pour le couple suivant (où* $\lfloor \alpha \rfloor$ *est la partie entière d'un réel* α*) :*

$$(x, y) = (x_1, y_1) + \left\lfloor \frac{-x_1}{x_2} \right\rfloor (x_2, y_2).$$

23. Démontrer que si (x, y) est une solution de l'équation (1) alors $y \geq |v_k|$ et $dv_k^2 < p$. Conclure alors la preuve du théorème 1.
24. (Bonus) Démontrer le lemme 2.