26 mai 2025
Master 1 M.F., Orsay

Partiel 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. La partie 1 de ce problème introduit la notion fondamentale étudiée dans toute la suite (sauf la partie 4), celle de témoin d'un entier. Les parties 2 et 3, qui sont indépendantes entre elles, utilisent cette notion. La partie 4, consacrée aux puissances dans un groupe cyclique, n'utilise rien de ce qui précède. Enfin la partie 5 utilise les parties 1 et 4 pour démontrer un théorème énoncé au début de la partie 2 et admis dans les parties 2 et 3.

Partie 1 : Notion de témoin

Dans tout le problème on considère un entier impair $n \geq 3$, qu'on écrit sous la forme

$$n = 1 + 2^s t \text{ avec } s \geq 1 \text{ et } t \text{ impair.} \tag{1}$$

1. ($\star$) Implémenter en Sage une fonction `calcul_s` qui prend en entrée un entier $n \geq 3$ (supposé impair) et renvoie s. Que renvoie cette fonction pour $n = 4225$?

On dit qu'un entier a est *un témoin* de n si on a

$$2 \leq a \leq n-1, \quad a^t \not\equiv 1 \bmod n, \quad \text{et} \quad a^{2^i t} \not\equiv -1 \bmod n \text{ pour tout } i \in [\![0, s-1]\!].$$

2. Montrer que si n est composé (c'est-à-dire non premier) alors tout entier $a \in [\![2, n-1]\!]$ tel que $\mathrm{pgcd}(a, n) \neq 1$ est un témoin de n.
3. Montrer que si $n = p$ est premier alors il ne possède aucun témoin. *Indication : en supposant que a est un témoin, on pourra considérer le plus petit entier $i \in [\![0, s]\!]$ tel que $a^{2^i t} \equiv 1 \bmod p$ et s'intéresser à $a^{2^{i-1} t}$.*
4. ($\star$) Implémenter en Sage une fonction `est_temoin` qui prend en entrée deux entiers n et a (avec $n \geq 3$ impair) et renvoie `True` si a est un témoin de n, et `False` sinon. Est-ce que 2 est un témoin de 561 ? Et 3 ? Et 50 ? *Toutes les fonctions implémentées en `Sage` peuvent être utilisées, ici comme dans tout l'énoncé, par exemple pour calculer une puissance.*
5. ($\star$) Donner la liste des entiers $2 \leq a \leq 51$ qui sont des témoins de $n = 561$. *Indication : il y a 49 tels entiers a.*
6. Donner le nom de l'algorithme vu en cours qui permet de tester si a^t est congru à 1 modulo n. Quel est le coût de ce test en nombre d'opérations arithmétiques dans $\mathbb{Z}$?

7. Calculer le coût de la fonction `est_temoin` implémentée à la question 4, d'abord en fonction de s et de t, puis uniquement en fonction de n.
8. Les deux programmes ci-dessous, qui prennent chacun en entrée deux entiers $a \in [\![0, n-1]\!]$ et $t \in \mathbb{N}^*$, permettent de tester si a^t est congru à 1 modulo n. Lequel des deux est le plus efficace et pourquoi ?

Version 1

```
def test1(a,t):
    r=1;
    N=n;
    A=a;
    while(N>0):
        if N%2 == 1:
           r=r*A
        A=A*A;
        N=N//2;
    return((r%n)==1)
```

Version 2

```
def test2(a,t):
    r=1;
    N=n;
    A=a;
    while(N>0):
        if N%2 == 1:
           r=(r*A)%n
        A=(A*A)%n;
        N=N//2;
    return(r==1)
```

Partie 2 : Proportion de témoins

À la fin de ce problème on aura démontré le théorème suivant :

Théorème 1 *Soit $n \geq 11$ un entier impair composé (c'est-à-dire non premier). Alors au moins 3/4 des entiers $a \in [\![2, n-1]\!]$ tels que* $\mathrm{pgcd}(a, n) = 1$ *sont des témoins de n.*

Le but de cette partie est d'illustrer ce théorème sur des exemples.

9. ($\star$) Implémenter en Sage une fonction `proportion` qui prend en entrée un entier $n \geq 3$ supposé impair, et renvoie la proportion de témoins parmi les entiers $a \in [\![2, n-1]\!]$.
10. ($\star$) Combien vaut cette proportion pour $n = 12403$? Commenter en lien avec le théorème 1.
11. ($\star$) En moyenne sur les entiers impairs n composés compris entre 11 et 10^3, quelle est la proportion de témoins parmi les entiers $a \in [\![2, n-1]\!]$? *On rappelle que la commande* `is_prime` *permet de tester si un entier est premier.*

Partie 3 : Un test probabiliste

Dans cette partie on admet le théorème 1 énoncé dans la partie 2. On fixe un entier $K \geq 1$ et on répète K fois (au maximum) ce qui suit :

- Choisir aléatoirement un entier $a \in [\![2, n-1]\!]$.
- Tester si a est un témoin de n.
- Si a est un témoin, renvoyer "n est composé" et arrêter le programme.
- Sinon, continuer le programme.

Si on arrive à la fin des K passages dans cette boucle, on renvoie "n est probablement premier".

12. En supposant K suffisamment grand (ce qui sera précisé par la suite), que peut-on dire en fonction de ce que renvoie le programme ?

13. ($\star$) Implémenter en Sage une fonction `test` qui prend en entrée deux entiers n et K (avec $n \geq 3$ impair) et renvoie `True` si l'algorithme renvoie "n est probablement premier", et `False` sinon.
14. ($\star$) En utilisant la fonction `test` implémentée à la question précédente, que peut-on dire de l'entier $n = 12403$?

Pour formaliser les choses, on fixe un entier $k \geq 2$ et on introduit une variable aléatoire X à valeurs dans l'ensemble des entiers impairs compris entre 2^k et 2^{k+1}, de loi uniforme (c'est-à-dire que $P(X = n)$ ne dépend pas de l'entier impair $n \in [\![2^k, 2^{k+1}]\!]$). On note p_k la probabilité de l'évènement "X est un nombre premier", noté $[X \in \mathcal{P}_k]$ où $\mathcal{P}_k$ désigne l'ensemble des nombres premiers compris entre 2^k et 2^{k+1}.
On fixe un entier $K \geq 1$ et on considère le test probabiliste ci-dessus, appliqué à X. On note T l'évènement : « ce test renvoie "n est probablement premier" ».

15. Combien vaut la probabilité conditionnelle $P(T|X \in \mathcal{P}_k)$? *On note $P(A|B)$, ou $P_B(A)$, la probabilité d'un évènement A sachant que B est réalisé.*
16. En utilisant le théorème 1 énoncé ci-dessus, majorer $P(T|X \notin \mathcal{P}_k)$ en fonction de K.
17. Déduire des questions précédentes une minoration de $P(X \in \mathcal{P}_k|T)$ en fonction de K et de $p_k = P(X \in \mathcal{P}_k)$.
18. Pourquoi est-il intéressant de minorer $P(X \in \mathcal{P}_k|T)$?
19. Donner une relation entre K et p_k qui assure que $P(X \in \mathcal{P}_k|T) \geq 1-10^{-6}$. En admettant que $\frac{2}{k\ln(2)}$ est une bonne valeur approchée de p_k, donner explicitement (en fonction de k) une valeur de K pour laquelle cette relation est vérifiée et commenter l'efficacité de cet algorithme ; on admettra que choisir aléatoirement un entier $a \in [\![2, n-1]\!]$ a le même coût que $O(1)$ opérations arithmétiques.
20. Dans cette question on veut tester si X est premier, pour s'en servir (s'il l'est) comme l'un des deux nombres premiers d'une clef RSA. Quel ordre de grandeur doit-on choisir pour k ? Dans le contexte de la question précédente, quel est l'ordre de grandeur du nombre d'opérations arithmétiques nécessaires pour tester si X est premier ?
21. Expliquer brièvement comment utiliser cette partie pour générer une clef RSA, et en estimer le coût en moyenne (en ordre de grandeur).

Partie 4 : Puissances dans un groupe cyclique

Dans cette partie (qui est indépendante des précédentes) on considère un groupe cyclique G de cardinal φ, noté multiplicativement. On note 1 son élément neutre.

22. Soit $g_0 \in G$ et $m \geq 1$; posons $k = \mathrm{pgcd}(m, \varphi)$. Montrer que l'équation $g^m = g_0$ possède au moins une solution $g \in G$ si, et seulement si, on a $g_0^{\varphi/k} = 1$, et que dans ce cas elle possède exactement k solutions.

Dans la suite de cette partie on fixe un élément $\alpha \in G$ d'ordre 2 ; on suppose donc que φ est pair. On note $\varphi = 2^u v$ avec v impair et $u \geq 1$. On se donne aussi un entier impair $t \geq 1$ et on pose $w = \mathrm{pgcd}(t, v)$.

23. Montrer que l'équation $g^t = 1$ possède exactement w solutions $g \in G$.

24. Soit $j \geq 0$. Montrer que l'équation $g^{2^j t} = \alpha$ possède exactement $2^j w$ solutions $g \in G$ si $j \leq u-1$, et aucune si $j \geq u$.

Partie 5 : Preuve du théorème 1

Soit $n \geq 11$ un entier impair composé ; on écrit $n-1 = 2^s t$ avec t impair et $s \geq 1$. On note $n = p_1^{a_1} \cdots p_N^{a_N}$ la décomposition de n en produit de facteurs premiers, avec $p_1 < \cdots < p_N$ premiers impairs et $a_1, \ldots, a_N \geq 1$. On rappelle que les groupes multiplicatifs $(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ sont cycliques de cardinal $p_i^{a_i-1}(p_i-1)$, ce qui permet d'utiliser les résultats de la partie 4.

Pour tout $i \in [\![1, N]\!]$ on pose $\varphi_i = p_i^{a_i-1}(p_i-1)$ que l'on écrit sous la forme $\varphi_i = 2^{u_i} v_i$ avec v_i impair et $u_i \geq 1$. On note $w_i = \mathrm{pgcd}(t, v_i)$, $v_i' = v_i/w_i$, $U = u_1 + \cdots + u_N$, $V = v_1 \cdots v_N$ et $V' = v_1' \cdots v_N'$, de telle sorte que $\varphi(n) = 2^U V$, où φ est l'indicatrice d'Euler.

25. Démontrer que l'équation $x^t = 1$ possède exactement V/V' solutions $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
26. Soit $j \geq 0$. Démontrer que l'équation $x^{2^j t} = -1$ ne possède aucune solution $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ si $j \geq \min(u_1, \ldots, u_N)$, et en possède exactement $2^{jN} V/V'$ sinon.
27. Déduire des questions précédentes que parmi les entiers $a \in [\![2, n-1]\!]$ premiers avec n, exactement A ne sont pas des témoins de n avec

$$A = \Big(1 + \frac{2^{Nr}-1}{2^N-1}\Big)\frac{V}{V'} \quad \text{où} \quad r = \min(s, u_1, \ldots, u_N).$$

28. Conclure la preuve du théorème 1 en distinguant selon que $N = 1$ ou $N \geq 2$.
29. ($\star$) Expliquer ce qu'a de particulier l'entier 12403 de la question 10, et déterminer les 6 plus petits entiers pour lesquels le même phénomène se produit.