COMPLEX - TD 08
décembre 2023

Énoncé

Exercice 1 : Quelques rappels d'arithmétiques

1.a] Montrer que si a diviser bc, et si $\text{pgcd}(a, b) = 1$ alors a divise c.

1.b] En déduire que si $c \equiv d\ [a]$, $c \equiv d\ [b]$ et $\text{pgcd}(a, b) = 1$ alors $c \equiv d\ [ab]$. Qu'en est-il si a et b ne sont pas premiers entre eux ?

1.c] Montrer que l'ensemble des nombres premiers est infini. On pourra raisonner par l'absurde en supposant que l'ensemble des nombres premiers est un ensemble fini $P = \{p_1, p_2, \ldots, p_k\}$.

Indication : construire un nouveau nombre premier à partir du produit de ces nombres.

1.d] Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, peut-on affirmer que :

1. $a + c \equiv b + d\ [n]$?
2. $ac \equiv bd\ [n]$?
3. $a^k \equiv b^k\ [n]$? (où k est un entier positif quelconque)

1.e] Si $ac \equiv bc\ [n]$, peut-on affirmer que $a \equiv b\ [n]$? Si oui le prouver, si non donner un contre-exemple puis une condition sur c et n pour que cela soit vrai.

Exercice 2 : Identité de Bézout

2.a] Déterminer deux entiers u et v pour chaque identité de Bézout suivante :

1. $714u + 340v = \text{pgcd}(714, 340)$;
2. $255u + 141v = \text{pgcd}(255, 141)$.

Exercice 3 : Certificats de primalité de Pratt (*cf* première partie du cours)

3.a] En admettant qu'un entier n est premier si et seulement si le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique d'ordre premier $n - 1$, montrer le *théorème de Lucas* qui affirme qu'un entier n est premier si et seulement s'il existe un entier $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1 \bmod n$ mais $a^{(n-1)/q} \not\equiv 1 \bmod n$ pour tout diviseur premier q de $n - 1$.

3.b] En déduire que tout nombre premier admet un certificat de primalité polynomial (en sa longueur binaire) et que la primalité est dans $\mathcal{NP}$.

Indication : On pourra montrer par récurrence qu'un certificat (récursif) démontrant la propriété de la question précédente nécessite moins de $(6 \log n - 4)$ entiers inférieurs à n.

Exercice 4 : Nombres de Carmichael

Un *nombre de Carmichael* est un entier composé tel que $a^n \equiv a \bmod n$ pour tout entier $a \geq 1$.

4.a] Montrer qu'un nombre de Carmichael est nécessairement impair.

4.b] Soient n un nombre de Carmichael et p un facteur premier (impair) de n. Montrer que p^2 ne divise pas n et que $p-1$ divise $n-1$.

4.c] Réciproquement, montrer que si n est un entier composé impair sans facteur carré, et tel que pour tout entier p divisant n, $p-1$ divise $n-1$ alors n est un nombre de Carmichael.

Exercice 5 : Vérification de produits matriciels

Nous considérons le problème suivant :

— **Entrée :** trois matrices A, B et C de taille $n \times n$ à coefficients dans $\mathbb{R}$.
— **Question :** vérifier si $A \cdot B = C$.

Pour mémoire, nous avons :

$$(AB)_{i,j} = \sum_{k=1}^{n} A_{i,k} B_{k,j}, \forall i, j, 1 \leq i, j \leq n.$$

5.a] Proposer un algorithme déterministe simple permettant de résoudre ce problème et donner sa complexité.

On considère maintenant sur l'algorithme probabiliste suivant :

Entrée : un entier $D > 1$, 3 matrices A, B et C dans de taille $n \times n$ à coefficients dans $\mathbb{R}$.

Sortie : `Oui` si $A \times B = C$ et **Non** autrement.

1. Choisir aléatoirement un vecteur colonne $\mathbf{x} \in \{0, \ldots, D-1\}^n$.
2. **res** $\leftarrow A\,(B \cdot \mathbf{x}) - C \cdot \mathbf{x}$.
3. **Si res** est nul alors **retourner** `Oui`, sinon **retourner** `Non`.

5.b] Donner la complexité de calculer un produit matrice-vecteur.

5.c] En déduire la complexité de l'algorithme ci-dessus.

5.d] Montrer que si $A \times B = C$, alors l'algorithme retourne toujours `Oui`.

On note $\mathbf{X} = (X_1, \ldots, X_n)^{\mathrm{T}}$ un vecteur (colonne) de variables, et $\mathbf{RES}(\mathbf{X}) = (A \times B - C)\mathbf{X} = (\mathrm{RES}_1(\mathbf{X}), \ldots, \mathrm{RES}_n(\mathbf{X})$.

5.e] Soit $i, 1 \leq i \leq n$. Montrer que si $\mathrm{RES}_i(\mathbf{X})$ est non nul, alors :

$$\Pr_{\mathbf{x}\in\{0,\ldots,D-1\}^n}\big(\mathrm{RES}_i(\mathbf{x}) = 0\big) \leq \frac{1}{D}.$$

5.f] En déduire :

$$\Pr\big(\text{Algo retourne } \texttt{Oui} \mid AB \neq C\big) \leq \frac{1}{D}.$$

Compléments

Exercice 6 : Test de primalité de Miller-Rabin

Soit $n \geq 3$ un entier composé impair. Notons $n = m2^h + 1$ avec m impair et soit $a \in \mathbb{Z}$ un entier premier à n. Considèrons la suite $(b_0, b_1, \ldots, b_h)$ d'entiers définie par :

$$b_0 \equiv a^m \bmod n, \quad b_1 \equiv b_0^2 \bmod n, \quad \ldots, \quad b_h \equiv b_{h-1}^2 \bmod n.$$

6.a] Considérons l'ensemble $\Upsilon_n = \{a \in \mathbb{Z}_n^*, \alpha^n \equiv 1 \bmod n\}$. Montrer que Υ_n est un sous-groupe de $\mathbb{Z}_n^*$ qui contient tous les entiers $a \in \mathbb{Z}_n^*$ pour lesquels la suite $(b_0, b_1, \ldots, b_h)$ vérifie les deux conditions du test de Miller-Rabin (*i.e.* $b_h = 1$. et si $b_0 \neq 1$, il existe un indice $i \in \{0, \ldots, h-1\}$ tel que $b_i \equiv -1 \bmod n$).

6.b] Montrer que si $\Upsilon_n \neq \mathbb{Z}_n^*$ alors le nombre d'entiers $a \in \mathbb{Z}_n^*$, pour lesquels la suite $(b_0, b_1, \ldots, b_h)$ vérifie les deux conditions précédentes, est inférieur à $(n-1)/2$.

Nous supposons désormais que $\Upsilon_n = \mathbb{Z}_n^*$.

6.c] Montrer que n peut s'écrire $n = n_1 n_2$ où $n_1, n_2 \geq 2$ sont deux entiers premiers entre eux.

6.d] Considérons j l'entier maximal pour lequel il existe un élément v de $\mathbb{Z}_n^*$ tel que $v^{2^j m} = -1 \bmod n$ et l'ensemble $\Psi_n = \{a \in \mathbb{Z}_n^*, \alpha^{2^j m} \equiv \pm 1 \bmod n\}$.
Montrer que Ψ_n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ et notons $v \in \Psi_n$ tel que $v^{2^j m} \equiv -1 \bmod n$.

6.e] Montrer qu'il existe un élément $w \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que $w \equiv v \bmod n_1$ et $w \equiv 1 \bmod n_2$.

6.f] Montrer que $w^{2^j m} \not\equiv \pm 1 \bmod n$ et que $w^{2^{j+1} m} \equiv 1 \bmod n$.

6.g] Conclure

Exercice 7 : Extraction de racine carrée modulo p

Sit p un nombre premier impair.

7.a] Montrer que si a est un entier non divisible par p, alors $a^{(p-1)/2} \equiv 1 \bmod p$ si a est un carré modulo p et $a^{(p-1)/2} \equiv -1 \bmod p$ sinon.

7.b] Nous supposons que $p \equiv 3 \bmod 4$. Donner un algorithme déterministe de complexité $O(\log^3 p)$ opérations binaires qui, étant donné $a \in \{1, \ldots, p-1\}$ tel que $a^{(p-1)/2} \equiv 1 \bmod p$ retourne $b \in \{1, \ldots, p-1\}$ tel que $b^2 \equiv \alpha \bmod p$.

Indication : On pourra calculer $a^{(p+1)/4} \bmod p$.

Nous supposons désormais que $p \equiv 1 \bmod 4$. Posons $p = 2^h m + 1$ avec m impair.

7.c] Donner un algorithme probabiliste qui, étant donné p, retourne un entier $\gamma \in \{1, \ldots, p-1\}$ tel que $\gamma^{(p-1)/2} \equiv -1 \bmod p$ en temps espéré $O(\log^3 p)$ opérations binaires.

7.d] Montrer que pour un tel γ, $\delta = \gamma^m$ engendre l'unique sous-groupe d'ordre 2^h de $(\mathbb{Z}/p\mathbb{Z})^*$.

7.e] Soit $a \in \{1, \ldots, p-1\}$ tel que $a^{(p-1)/2} \equiv 1 \bmod p$. Montrer que α^m appartient au sous-groupe engendré par δ

7.f] ($\star$) Proposer un algorithme qui retourne l'entier $i \in \{0, \ldots, 2^h - 1\}$ tel que $\alpha^m = \delta^x$.

7.g] En déduire un algorithme pour calculer une racine carré de α^m modulo p.

7.h] Conclure en donnant un algorithme permettant de calculer les racines carrés de α en temps $O((\log p)^3)$.

Exercice 8 : Test de primalité de Agrawal-Biswas

8.a] Montrer que n est un nombre premier si et seulement si n divise tous les coefficients binomiaux $\binom{n}{i}$ pour $i \in \{2, \ldots, n-1\}$.

8.b] En déduire que n est un nombre premier si et seulement si

$$(X+1)^n \equiv X^n + 1 \bmod n. \tag{1}$$

8.c] Expliquer pourquoi il n'est pas possible d'appliquer le lemme de Schwartz-Zippel à l'équation (1) pour obtenir un test de composition/primalité probabiliste avec des propriétés similaires au test de Miller-Rabin. Dire quel test on obtiendrait si on le faisait cependant.

8.d] Nous supposons dans toute la suite que n est un nombre composé qui n'est pas une puissance d'un nombre premier. Soient p un diviseur premier de n et $a \geq 1$ un entier tel que p^a divise n mais p^{a+1} ne divise pas n. Montrer que $\binom{n}{p^a}$ n'est pas divisible par p et en déduire que

$$(X+1)^n \not\equiv X^n + 1 \bmod p. \tag{2}$$

8.e] Soit $\ell \geq 1$ un entier. Montrer que le polynôme $P_p(X) = ((X+1)^n - X^n - 1) \bmod p$ a au plus $\lfloor n/\ell \rfloor$ diviseurs irréductibles de degré ℓ dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

8.f] Soit $\ell \geq 1$ un entier. Nous admettons que pour $n > p > 16$, le nombre I_ℓ de polynômes irréductibles unitaires (*i.e.* de coefficient dominant égal à 1) de degré ℓ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ vérifie $I_\ell \geq p^\ell/(2\ell)$.
Montrer que pour $n > p > 16$ et $\ell = \lceil \log_2 n \rceil$, la probabilité qu'un polynôme unitaire $Q_p(X)$ de degré ℓ tiré uniformément aléatoirement dans $(\mathbb{Z}/p\mathbb{Z})[X]$ soit irréductible et ne divise pas $P_p(X)$ est supérieure ou égale à $1/4\ell$.

8.g] Montrer que pour $n > p > 16$ et $\ell = \lceil \log_2 n \rceil$, la probabilité qu'un polynôme unitaire $Q_n(X)$ de degré ℓ tiré uniformément aléatoirement dans $(\mathbb{Z}/n\mathbb{Z})[X]$ ne divise pas $P_n(X) = ((X+1)^n - X^n - 1) \bmod n$ est supérieure ou égale à $1/4\ell$.

8.h] En déduire un nouveau test de primalité/composition et une nouvelle démonstration que le langage des nombres premiers appartient à $\mathcal{BPP}$.

Exercice 9 : Isomorphisme Simultané de Matrices

Soit $n > 1$ un entier et p un nombre premier. On considère le problème d'*Isomorphisme Simultané de Matrices* (`IsoMat`) :

> **Entrée :** $m \geq 1$, des matrices $M_1, \ldots, M_m \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ et $M'_1, \ldots, M'_m \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$.
> **Question :** Trouver une matrice inversible $S \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ telle que
>
> $$S \cdot M_i \cdot S^{-1} = M'_i, \forall i \in \{1, \ldots, m\}$$

9.a] Expliquer comment vérifier qu'une matrice $S \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ est solution de `IsoMat` en temps polynomial et de manière déterministe.

9.b] Soient $M_1, \ldots, M_m \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ et $M'_1, \ldots, M'_m \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ des matrices. Montrer que si $S \in \mathbb{Z}_N^{n\times n}$ est inversible alors :

$$S \cdot M_i = M'_i \cdot S, \forall i \in \{1, \ldots, m\} \iff S \cdot M_i \cdot S^{-1} = M'_i, \forall i \in \{1, \ldots, m\}.$$

9.c] En utilisant la question précédente, montrer que trouver une matrice $S \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ telle que $S \cdot M_i \cdot S^{-1} = M'_i, \forall i \in \{1, \ldots, m\}$ se réduit à résoudre un système linéaire de $m \cdot n^2$ équations et n^2 variables.

La question précédente permet de trouver un entier d et des matrices $B_1, \ldots, B_d \in (\mathbb{Z}/p\mathbb{Z})^{n\times n}$ telles que pour tout $\lambda_1, \ldots, \lambda_m \in (\mathbb{Z}/p\mathbb{Z})$, la matrice $S = \sum_{i=1}^{d} \lambda_i \cdot B_d$ vérifie

$$S \cdot M_i \cdot S^{-1} = M'_i, \forall i \in \{1, \ldots, m\}.$$

Dans la suite, on suppose que l'ensemble $\mathcal{S} = \left\{ \sum_{i=1}^{d} \lambda_i \cdot B_d \mid \lambda_1, \ldots, \lambda_d \in (\mathbb{Z}/p\mathbb{Z}) \right\}$ contient au moins une matrice inversible.

9.d] Donner la probabilité que $\sum_{i=1}^{d} \lambda_i \cdot B_d$ soit inversible pour des $\lambda_1, \ldots, \lambda_m \in (\mathbb{Z}/p\mathbb{Z})$ tirés aléatoirement.

9.e] Proposer un algorithme polynomial probabiliste permettant de résoudre `IsoMat`. Vous donnerez la probabilité de succès de votre algorithme.

Exercice 10 : Couplages parfaits

Soit $G = (V, E)$ un graphe avec n sommets ($|V| = n$).

- Un ensemble d'arêtes $M \subseteq E$ est un **couplage** si on ne peut trouver deux arêtes e' et e dans M incidentes à un même sommet.
- Un **couplage parfait** est un couplage $M \subseteq E$ tel que pour chaque sommet $v \in V$ il existe une unique arête dans M incidente à v.

Pour un graphe $G = (V, E)$, on construit une matrice sommet-sommet A de taille $|V| \times |V|$ tel que :

- $A[i, j] = x_{i,j}$, si $\{i, j\} \in E$ et $i < j$.
- $A[i, j] = -x_{j,i}$, si $\{i, j\} \in E$ et $i > j$.
- 0, sinon.

On admet le résultat suivant :

$$\text{Det}(A) \text{ est nul } \iff \text{ il n'existe pas de couplage parfait de } G.$$

10.a] On considère $G = (\{1, 2, 3\}, \{\{1, 2\}\}$. Monter que G n'admet pas de couplage parfait.

10.b] Proposer un algorithme (probabiliste) pour décider de l'existence d'un couplage parfait.

10.c] Donner les caractéristiques de l'algorithme : type (Las-Vegas ou Monte-Carlo), complexité et probabilité d'erreur.