COMPLEX - TD 08
2025-2026

Énoncé

Exercice 1 : Quelques rappels d'arithmétiques

1.a] Montrer que si a divise 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 : Certificats de primalité de Pratt (*cf* première partie du cours)

2.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 $n - 1$.

2.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 démontrant la propriété de la question précédente nécessite moins de $(6 \log n - 4)$ entiers inférieurs à n.

Exercice 3 : Vérification de produits matriciels – Algorithme de Freivalds

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 :

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

3.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 $\mathcal{M}_n(\mathbb{R})$.

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`.

3.b] Donner la complexité de l'algorithme ci-dessus.

3.c] Montrer que si $A \cdot B = C$, alors l'algorithme retourne toujours `Oui`.

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

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

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

3.e] En déduire $\Pr\big(\text{Algorithme retourne } \texttt{Oui} \mid AB \neq C\big) \leq 1/D$.

Exercice 4 : Test d'identités entières

Il a été récemment démontré que l'entier 42 s'écrit sous la forme d'une somme de trois cubes de la façon suivante :

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 \quad (1)$$

Trouver cette décomposition a demandé une grande puissance de calcul et même si sa vérification est plus simple, elle demande d'écrire des nombres entiers de plus de 50 chiffres décimaux. Dans cet exercice, nous allons reprendre le principe de la « preuve par 9 » sous une forme probabiliste pour tester des identités sur des entiers (de façon similaire au test d'identités polynomiales vu en cours).

4.a] Montrer que la relation (1) est vraie modulo 10.

4.b] Étant donné deux entiers a_1 et a_2 strictement inférieurs en valeur absolue à une borne $B \geq 2$ (c'est-à-dire tels que $|a_1| < B$ et $|a_2| < B$). Montrer que $a_1 = a_2$ si et seulement si il existe des nombres premiers distincts $p_1, \ldots, p_\ell$ tels que

$$a_1 \equiv a_2 \bmod p_i, \forall i \in \{1, \ldots, \ell\} \text{ et } p_1 \cdots p_\ell > 2B$$

4.c] Soient deux entiers a_1 et a_2 représentés sous une forme polynomiale comme dans l'équation (1). Soit $B \geq 2$ une borne supérieure stricte sur a_1 et a_2 en valeur absolue (c'est-à-dire telle que $|a_1| < B$ et $|a_2| < B$). Supposons que $a_1 \neq a_2$.

Montrer qu'il existe une constante $c > 0$ telle que, pour tout entier $n \geq 1$, la probabilité qu'un nombre premier inférieur à 2^n tiré uniformément aléatoirement divise $(a_1 - a_2)$ est inférieure ou égale à $cn \log(B)/2^n$.

Indication. Rappelons une forme faible du théorème des nombres premiers qui affirme qu'il existe une constante $c' > 0$ telle que, pour tout entier $n \geq 1$, le nombre de nombres premiers inférieurs à 2^n, est supérieur ou égal à $c' \cdot 2^n/n$.

4.d] Soit $B \geq 2$. Un entier a avec $|a| < B$ est dit *représentable sous une forme polynomiale utilisant d opérations arithmétiques*, si il existe un polynôme P en n variables et n entiers $\alpha_1, \ldots, \alpha_n$ avec $|\alpha_i| < B$ tels que $a = P(\alpha_1, \ldots, \alpha_n)$ et l'évaluation du polynôme P nécessite au plus d additions d'entiers et d multiplications d'entiers.

Donner un algorithme probabiliste pour tester si deux entiers a_1 et a_2, représentés sous une forme polynomiale utilisant d opérations arithmétiques et avec $|a_1| < B$ et $|a_2| < B$, sont égaux. Estimer sa probabilité d'erreur et sa complexité.

Exercice 5 : 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 $|V| \times |V|$ telle que (1) $A[i, j] = x_{i,j}$, si $\{i, j\} \in E$ et $i < j$, (2) $A[i, j] = -x_{j,i}$, si $\{i, j\} \in E$ et $i > j$ et (3) $A[i, j] = 0$, sinon. Nous admettons le résultat suivant :

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

5.a] Considérons $G = (\{1, 2, 3\}, \{\{1, 2\}\})$. Montrer que G n'admet pas de couplage parfait.

5.b] Proposer un algorithme (probabiliste) pour décider de l'existence d'un couplage parfait. Donner les caractéristiques de l'algorithme : type (Las-Vegas ou Monte-Carlo), complexité et probabilité d'erreur.

Compléments

Exercice 6 : Nombres de Carmichael

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

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

6.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 $n-1$.

6.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 7 : 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 :

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

7.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 $b_i \equiv -1 \bmod n$).

7.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 $\Upsilon_n = \mathbb{Z}_n^*$.

7.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.

7.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 $v^{2^j m} \equiv -1 \bmod n$.

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

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

7.g] Conclure

Exercice 8 : Extraction de racine carrée modulo p

Sit p un nombre premier impair.

8.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.

8.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.

8.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.

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

8.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

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

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

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

Exercice 9 : Test de primalité de Agrawal-Biswas

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

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

$$(X+1)^n \equiv X^n + 1 \bmod n. \tag{2}$$

9.c] Expliquer pourquoi il n'est pas possible d'appliquer le lemme de Schwartz-Zippel à l'équation (2) 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.

9.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

$$(X+1)^n \not\equiv X^n + 1 \bmod p. \tag{3}$$

9.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 $(\mathbb{Z}/p\mathbb{Z})[X]$.

9.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 $1/4\ell$.

9.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 $1/4\ell$.

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

Exercice 10 : 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
>
> $$S \cdot M_i \cdot S^{-1} = M'_i, \forall i \in \{1, \ldots, m\}$$

10.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.

10.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 :

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

10.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.

10.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.

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

Exercice 11 : 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 :

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

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

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

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