Math pour l'info - Séance d'exercices bilan

Consignes pour les exercices

- **Complétez tous les exercices** : chacun doit être terminé, même si vous finissez certains après la séance.
- **Posez des questions** : je reste disponible pour clarifier ou expliquer, mais je ne corrigerai pas chaque exercice individuellement pendant/après la séance.
- Vous devez choisir **un exercice par chapitre** et le rendre à la fin de la séance.
- Vous devez également rendre tous les exercices de la partie bonus.

Partie 1 — Complexité calculatoire

Exercice 1.1 — Analyse d’un algorithme composite

On considère l’algorithme suivant :

```
Entrée : un tableau A de n entiers

1. Trier A par tri à bulles
2. Effectuer une recherche dichotomique de la valeur 42 dans A
```

1. Calcule la complexité globale de cet algorithme (en pire cas), en utilisant les notations asymptotiques.
2. Justifie pourquoi le tri est nécessaire avant la recherche.

Exercice 1.2 — Analyse d’un pseudo-code avec branchements

Considère le pseudo-code suivant :

```
Entrée : entier n

si n est pair :
    pour i de 1 à n faire :
        pour j de 1 à log₂(n) faire :
            opération élémentaire
sinon :
    pour i de 1 à n² faire :
        opération élémentaire
```

1. Donne la complexité dans le pire cas.
2. Donne la complexité dans le meilleur cas.
3. Donne la complexité dans le cas moyen (si on suppose que n a autant de chances d'être pair que impair)

Exercice 1.3 — Traitement de paires dans un tableau

On considère l’algorithme suivant :

```
Entrée : tableau A de n entiers
Sortie : la liste des paires (i, j) telles que A[i] + A[j] = 0

pour i de 0 à n−1 faire :
    pour j de i+1 à n−1 faire :
        si A[i] + A[j] = 0 :
            ajouter (i, j) à la liste
```

1. Donne la complexité asymptotique.
2. Quelle hypothèse sur A permettrait d’éviter complètement la deuxième boucle ?

Exercice 1.4 — Récurrence

On considère l’algorithme récursif suivant :

```
fonction mystère(n) :
    si n ≤ 1 :
        retourner 1
    sinon :
        a ← mystère(n/2)
        b ← mystère(n/2)
        pour i de 1 à n faire :
            opération élémentaire
        retourner a + b + n
```

1. Écris la relation de récurrence associée.
2. Compare brièvement cette complexité avec celle du tri fusion.

Partie 2 — Preuves

Exercice 2.1 — Preuve par induction simple

Prouve par **induction** la formule suivante :

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

Exercice 2.2 — Induction sur une propriété algébrique

Montre par **induction** que pour tout entier $n \geq 1$:

$$2^n > n^2 \quad \text{pour } n \geq 5$$

Exercice 2.3 — Preuve par l'absurde : Il n'existe pas de plus grand nombre réel

Prouve par **absurde** qu'il **n'existe pas de plus grand réel**, c'est-à-dire :

> Il n'existe **aucun** nombre réel $M \in \mathbb{R}$ tel que $\forall x \in \mathbb{R}, x \leq M$.

Exercice 2.4 — Algorithme inexact et contre-exemple

Un algorithme prétend déterminer si un entier n est premier en le testant uniquement contre les diviseurs 2, 3, 5, 7.
Démontre l'exactitude ou l'inexactitude de cet algorithme.

Partie 3 — Structures discrètes : Ensembles et relations

Exercice 3.1 — Opérations ensemblistes

Soient $A = 1, 2, 3, 4,$ $B = \{3, 4, 5, 6\}$, et $C = \{2, 4, 6, 8\}$. Calcule :

1. $A \cup B$, $A \cap C$,$(A \cup B) - C$
2. Le complément de A dans l'univers $U = \{1, \ldots, 8\}$
3. Le produit cartésien $A \times \{x, y\}$

Exercice 3.2 — Relations et propriétés

On définit la relation R sur $\mathbb{Z}$ par :

$$x \; R \; y \iff x - y \text{ est pair}$$

1. Quel type de relation est R
2. Démontre-le.

Exercice 3.3 — Ordre partiel sur un ensemble de chaînes

Soit l'ensemble $S = \{'''','' a'','' aa'','' aaa''\}$ et la relation R définie par :

$$x \; R \; y \iff x \text{ est un préfixe de } y$$

1. Vérifie que cette relation est réflexive, transitive et antisymétrique.
2. Quel type de relation est donc R ?

Exercice 3.4 — Analyse des propriétés d'une relation

Soit l'ensemble $E = \{1, 2, 3\}$ et la relation $R = \{(1, 2), (2, 3), (1, 3), (2, 2)\}$

1. Cette relation est-elle réflexive sur E ?
2. Est-elle symétrique ? Justifie.
3. Est-elle transitive ? Justifie avec au moins un exemple ou contre-exemple.

Partie Bonus

Génération de clés RSA

Soit $p = 5$, $q = 11$, et $e = 3$

1. Calcule n
2. Calcule $\phi(n)$
3. Trouve $d \in \mathbb{N}$ tel que $e \cdot d \equiv 1 \mod \phi(n)$

Trouver des collisions dans une fonction simple

On définit une fonction de hachage simplifiée $h : \text{chaînes de caractères} \to \mathbb{Z}_{10}$ qui fonctionne comme suit :

1. Chaque lettre est convertie en sa position dans l'alphabet (a = 1, b = 2, ..., z = 26)
2. On fait la **somme des positions**, puis on prend le **résultat modulo 10**.

Par exemple :

- $h(abc) = (1 + 2 + 3) \mod 10 = 6$
- $h(aaa) = (1 + 1 + 1) \mod 10 = 3$

Questions :

1. Calcule la valeur de h pour au moins 5 chaînes différentes de ton choix.
2. Trouve au moins deux paires différentes de chaînes qui donnent la même valeur de hachage.
3. Explique pourquoi les collisions sont inévitables dans cette fonction.
4. Propose une amélioration possible (même simple) pour limiter les collisions.