POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

LOG2810

STRUCTURES DISCRÈTES

Contrôle périodique 2

Automne 2021

SOLUTIONNAIRE:

Directives:

- La durée du contrôle périodique est de 60 minutes.
- Vous devez compléter cet examen seul, sans l'aide de personne et en utilisant aucun outil de communication.
- L'examen est sur un total de 20 points.
- Répondez directement sur ce document Word (docx).
- Vous avez 15 minutes additionnelles pour produire le PDF et le soumettre dans la boîte de remise de votre section de cours.
- Générez le PDF avec le nom sous le format **SectionDeCours-Matricule.pdf** (exemple 01-1234567.pdf).
- Dans l'intérêt de l'équité pour tous les étudiants, vous devez modifier le fichier Word (docx) fourni. Modifier le fichier EXCLUT le fait d'intégrer des scans de rédaction manuscrite ou d'y écrire avec un stylet.
- Aucun retard ne sera toléré.
- Aucun courriel ne sera accepté.

LOG2810-01-02-03 Contrôle périodique 2

Prénom:

Nom:

Matricule:

LOG2810-01-02-03 Contrôle périodique 2

Exercice 1 Relation (5 points)

Montrez que la relation R définie dans $\mathbb{N}^* = \{1,2,\ldots\}$ comme ci-dessous est une relation d'ordre.

$$pRq \leftrightarrow \exists k \in \mathbb{N}^*, q = p^k$$

Réponse:

Montrons que la relation est une relation d'ordre en montrant qu'elle est réflexive, antisymétrique et transitive.

Réflexivité

Soit p un entier non nul.

On a $p=p^1$. Donc il existe k un entier non nul tel que $p=p^k$.

On en déduit que R est réflexive.

Antisymétrie

Soit p et q deux entiers non nuls tel que ***p R q*** et ***q R p***.

Par définition :

$pRq \leftrightarrow \exists k_1 \in N^*, q = p^{k_1}$

$pRq \leftrightarrow \exists k_2 \in N^*, p = q^{k_2}$

En remplaçant q dans la 2ème égalité par son expression de la 1ère égalité, on obtient :

$p = p^{k_1 \times k_2}$

Ainsi on a $k_1 \times k_2 = 1$, soit $k_1 = k_2 = 1$

D'où $p = q$

R est donc antisymétrique

Transitivité

Soit p, q et s trois entiers non nuls tel que ***p R q*** et ***q R s***.

Par définition :

$pRq \leftrightarrow \exists k_1 \in N^*, q = p^{k_1}$

$qRs \leftrightarrow \exists k_2 \in N^*, s = q^{k_2}$

En remplaçant q dans la 2ème égalité par son ***p R q*** expression de la 1ère égalité, on obtient :

$s = p^{k_1 \times k_2}$

En posant $k = k_1 \times k_2$ on a $s = p^k$**. Ainsi *p R s*.**

R est donc transitive.

LOG2810-01-02-03 Contrôle périodique 2

<u>Exercice 2</u> Algorithmes (4 points)

Trouvez une paire de témoins C et k afin de vérifier que $\sum_{i=0}^{n} i$ est $O(n^2)$?

Réponse:

Nous savons que $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Il faut maintenant trouver C et k tel que $\frac{n(n+1)}{2} \leq Cn^2$ pour tout $n > k$

Si nous supposons n positif, nous pouvons diviser par $n^2/2$ à gauche et à droite de l'inégalité. Nous obtenons:

$1 + \frac{1}{n} \leq 2C$.

Choisissons $k = 1$. Alors pour $n > k$, le terme de gauche sera plus petit ou égal à 2. Nous avons donc $2 \leq 2C$ et en divisant par 2 de chaque côté nous avons $1 \leq C$

Et nous obtenons ainsi les deux témoins k = 1 et C = 1.

<u>Exercice 3</u> Théorie des nombres (6 points)

a) **(3 points)** Calculez $3^{100}\ (mod\ 23)$ en utilisant le petit théorème de Fermat. Montrez chaque étape de votre calcul. (Une réponse sans l'utilisation du petit théorème de Fermat ne donnera aucun point)

Réponse:

Le nombre 23 est un nombre premier. Nous pouvons donc utiliser le petit théorème de Fermat. Selon ce théorème:

$3^{22} \equiv 1\ (mod\ 23)$

$(3^{22})^4 \equiv 1\ (mod\ 23)$

$3^{100} = 3^{12}(3^{22})^4 \equiv 3^{12}\ (mod\ 23)$

Il faut encore calculer 3^{12}. Il est possible de faire le calcul par étapes.

$3^3 = 27 \equiv 4\ (mod\ 23)$

$3^{12} = (3^3)^4 \equiv 4^4\ (mod\ 23)$

$4^4 = 64 \times 4 \equiv 18 \times 4 \equiv 72 \equiv 3\ (mod\ 23)$

b) **(3 points)** Résolvez dans l'ensemble des entiers, l'équation:

$$3x \equiv 4\ (mod\ 7)$$

Donnez l'expression générant toutes les solutions possibles.

Réponse:

Nous pouvons utiliser l'algorithme d'Euclide étendu epgcd([3, 1, 0], [7, 0, 1]) nous trouvons s = 5 et t = -2. L'inverse multiplicatif de 3 (mod 7) est donc 5. Si on multiplie des deux côtés de l'expression par 5 nous obtenons $x \equiv 20 \equiv 6\ (mod\ 7)$.

Les solutions sont donc $x = 6 + 7k$ pour tout entier k.

Exercice 4 Induction (5 points)

En utilisant une preuve par induction, démontrez que 7 divise $2^{n+2} + 3^{2n+1}$ pour tout entier $n \geq 1$. Montrez chaque étape de votre preuve.

Indice: Durant le déroulement de la preuve vous devriez obtenir l'expression suivante: $2 \times (2^{k+2} + 3^{2k+1}) + 7 \times 3^{2k+1}$.

Réponse:

P(n) : 7 divise $2^{n+2} + 3^{2n+1}$

1. Condition de base

Pour n = 1, $2^{1+2} + 3^{2+1}$ = 8 + 27 = 35 = 5 x 7. La condition de base pour P(1) est donc vraie.

2. Étape inductive

Supposons que P(k) soit vraie. Alors on peut écrire $2^{k+2} + 3^{2k+1} = 7c$ où c est un certain nombre entier. Notons que l'hypothèse d'induction peut se réécrire.

Pour $k + 1$ nous avons :

$$
\begin{aligned}
2^{(k+1)+2} + 3^{2(k+1)+1} &= 2^{k+1+2} + 3^{2k+2+1} \\
&= 2 \times 2^{k+2} + 3^{2k+1+2} \\
&= 2 \times 2^{k+2} + 3^2 \times 3^{2k+1} \\
&= 2 \times 2^{k+2} + 9 \times 3^{2k+1} \\
&= 2 \times 2^{k+2} + (2 + 7) \times 3^{2k+1} \\
&= 2 \times 2^{k+2} + 2 \times 3^{2k+1} + 7 \times 3^{2k+1}
\end{aligned}
$$

$$= 2(2^{k+2} + 3^{2k+1}) + 7 \times 3^{2k+1}$$

$$= 2(7c) + 7 \times 3^{2k+1}$$

$$= 7(2c + 3^{2k+1})$$

Cette expression est divisible par 7.

Ce qui complète la preuve de l'implication $P(k) \to P(k+1)$ et par conséquent avec la preuve de la condition de base on complète la preuve par induction.