POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG2810
STRUCTURES DISCRÈTES

CONTRÔLE PÉRIODIQUE 2

H2023

SOLUTIONNAIRE

Exercice 1 (**3.5 points)**

On considère dans l'ensemble des entiers plus grands que 1, la relation R définie par :

$$\mathbf{a}\ \mathrm{R}\ \mathbf{b} \text{ si et seulement si } \mathbf{a^b \leq b^a}$$

La relation est-elle transitive ? Justifiez votre réponse.

Réponse :

Soit a, b et c trois entiers plus grands que 1 tel que $\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$.

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $a^b \leq b^a$ et $b^c \leq c^b$.

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $b \log a \leq a \log b$ et $c \log b \leq b \log c$.

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $bc \log a \leq ac \log b$ et $ac \log b \leq ab \log c$

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $bc \log a \leq ac \log b \leq ab \log c$

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $bc \log a \leq ab \log c$

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $c \log a \leq a \log c$, car b est non nul.

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $a^c \leq c^a$.

$\mathbf{a}\ \mathrm{R}\ \mathbf{b}$ et $\mathbf{b}\ \mathrm{R}\ \mathbf{c}$, alors $\mathbf{a}\ \mathrm{R}\ \mathbf{c}$.

R est donc transitive.

Exercice 2 (**3.5 points)**

Est-ce que ***log(n/2)*** est θ***(log n)*** ? Justifiez votre réponse.

Réponse :

n/2 est O*(n)* et n est O (*n/2*) donc ***n/2*** est θ***(n)***

Par conséquent, ***log(n/2)*** est θ***(log n)***

Exercice 3 (**4 points)**

Bob utilise le protocole RSA et publie sa clé publique **n = 187** et **e = 3**.

a. **(2 points)** Chiffrez le message **m = 25** avec la clé publique de Bob.

Réponse :

Soit C le message chiffré.

$C = m^e \bmod n$, soit $C = 25^3 \bmod 187$. D'où **C = 104**

b. **(2 points)** En considérant que l'indicatrice de Carmichael est **160**, quelle est la clé privée de Bob ?

Réponse :

Soit d la clé privée de Bob.

d.e est ≡ 1 (mod 160)
Nous obtenons l'équation 3d + 160t = 1.
En utilisant l'algorithme d'Euclide étendu et en considérant les vecteurs [3, 1, 0][160, 0, 1] on obtient les vecteurs [1, 107, -2][1, -53, 1]. On peut donc retenir **d=107**.

Exercice 4 (**5 points)**
En utilisant vos connaissances en congruences, montrez que pour tout entier positif ou nul **n**,

11 divise $3^{5n} + 5^{5n+1} + 4^{5n+2}$

Réponse :

- $3^{5n} = (3^5)^n$. Or $3^5 \equiv 1 \pmod{11}$ donc $(3^5)^n \equiv 1 \pmod{11}$ et par suite $3^{5n} \equiv 1 \pmod{11}$
- $5^{5n+1} = 5.(5^5)^n$. Or $5^5 \equiv 1 \pmod{11}$ donc $(5^5)^n \equiv 1 \pmod{11}$ et par suite $5^{5n+1} \equiv 5 \pmod{11}$
- $4^{5n+2} = 16.(4^5)^n$. Or $4^5 \equiv 1 \pmod{11}$ et $16 \equiv 5 \pmod{11}$ donc $16.(4^5)^n \equiv 5 \pmod{11}$ et par suite $4^{5n+2} \equiv 5 \pmod{11}$

Des calculs précédents, on déduit que : $3^{5n} + 5^{5n+1} + 4^{5n+2} \equiv (1+5+5) \bmod (11)$
Ainsi, $3^{5n} + 5^{5n+1} + 4^{5n+2} \equiv 11 \bmod (11)$, c'est à dire que $3^{5n} + 5^{5n+1} + 4^{5n+2} \equiv 0 \bmod (11)$
D'où 11 divise $3^{5n} + 5^{5n+1} + 4^{5n+2}$

Exercice 5 (**4 points)**
Montrez par récurrence que pour tout entier positif non nul **n**,

$$\mathbf{2^n > n}$$

Réponse :
Soit la P(n) : $2^n > n$ avec n un entier positif non nul.
Cas de base :
Prenons n = 1. On a $2^1 = 2$. Or $2 > 1$ donc $2^1 > 1$.
P(1) est vraie.
Supposons que P(n) est vrai pour un entier positif non nul n quelconque et montrons que P(n+1) est vrai c'est-à-dire que $2^{n+1} > n+1$.
Par hypothèse d'induction, $2^n > n$. De plus, $2^n > 1$ pour tout $n \geq 1$.
En sommant les 2 inégalités, $2^n + 2^n > n + 1$ donc $2^{n+1} > n+1$.
P(n+1) est alors vrai.
Par conséquent, $\forall n \geq 1$, P(n) → P(n+1) est vrai
On peut donc conclure d'après le principe d'induction que $\forall n \geq 1$, $2^n > n$.