Solutionnaire

POLYTECHNIQUE MONTRÉAL

Contrôle périodique 2

LOG2810

Sigle du cours

Sigle et titre du cours	*Groupe*	*Trimestre*
LOG2810 Structures discrètes	**Tous**	**Automne 2022**
Professeur	***Local***	***Téléphone***
Aurel Randolph, Chargé de cours Lévis Thériault, Coordonnateur		

Jour	*Date*	*Durée*	*Heures*
Samedi	**5 novembre 2022**	**1h**	**10h30-11h30**

Documentation	*Calculatrice*	
☐ Aucune ☒ Toute ☒ Voir directives particulières	☐ Aucune ☐ Toutes ☒ Non programmable (AEP)	**Les appareils électroniques personnels sont interdits.**

Question 1 (**5 points**)

On définit sur $\mathbf{E} = \mathbb{Z} \times \mathbb{N}^*$ la relation ***R*** par :

(a, b) ***R*** (s, t) si et seulement si **at = bs**

R est-elle une relation d'équivalence ? Justifiez votre réponse.

Réponse :

R est-elle une relation d'équivalence si elle est réflexive, symétrique et transitive.

- **Réflexivité**

  Soit (a, b) ∈ **E**. On a ab = ab, alors (a, b) ***R*** (a, b).
  R est donc réflexive.

- **Symétrie**

  Soit (a, b) ∈ **E** et (s t) ∈ **E** tel que (a, b) ***R*** (s, t).
  (a, b) ***R*** (s, t), alors at = bs
  at = bs alors ta = sb, soit sb = ta.
  On a donc (s, t) ***R*** (a, b).
  R est symétrique.

- **Transitivité**

  Soit (a, b) ∈ **E**, (c, d) ∈ **E** et (s, t) ∈ **E** tel que (a, b) ***R*** (c, d) et (c, d) ***R*** (s, t).
  (a, b) ***R*** (c, d) alors, ad = bc
  (c, d) ***R*** (s, t) alors, ct = ds

  (ad = bc) et (ct = ds), alors (adt = bct) et (bct = bds)
  (adt = bct) et (bct = bds), alors (adt = bds)
  (adt = bds) et d ∈ $\mathbb{N}^*$, alors (at = bs)
  Ainsi (ad = bc) et (ct = ds), alors (at = bs)
  On a donc (a, b) ***R*** (s, t).
  R est transitive.

CQFD

Question 2 (**2.5 points**)

Donnez une définition récursive de l'ensemble des entiers qui ne sont pas divisibles par 7.

Réponse :

- Solution 1

Sot **S** l'ensemble des entiers qui ne sont pas divisibles par 7. La définition récursive de **S** est :

1 ∈ **S**, 2 ∈ **S**, 3 ∈ **S**, 4 ∈ **S**, 5 ∈ **S**, 6 ∈ **S**
∀ x ∈ **S, (x + 7)** ∈ **S**

- Solution 2 (moins élégante, mais admise)

Sot **S** l'ensemble des entiers qui ne sont pas divisibles par 7. La définition récursive de **S** est :

1 ∈ **S**, 2 ∈ **S**, 3 ∈ **S**, 4 ∈ **S**, 5 ∈ **S**, 6 ∈ **S**
∀ x ∈ **S, 7x+1** ∈ **S, 7x+2** ∈ **S, 7x+3** ∈ **S, 7x+4** ∈ **S, 7x+5** ∈ **S, 7x+6** ∈ **S**

Question 3 (**4.5 points)**
On considère la clé publique RSA (***e*** = 11, ***n*** = 319).
Note : Les calculs suivants vous sont fournis.

- 319 = 11 x 29
- $10^{11} \equiv 263 \pmod{319}$
- $2^9 \equiv 193 \pmod{319}$
- $263^2 = 216 \times 319 + 265$
- 772 = 2 x 319 + 134
- 134 x 265 = 111 x 319 + 101

a. (**1.5 point**) Quel est le message ***C*** chiffré à partir du message ***M*** = 200 ?

Réponse :

$C = M^e = 200^{11} = (2.100)^{11} = 2^{11} \times 100^{11} = 2^{11} \times (10^{11})^2$

D'après l'énoncé $10^{11} \equiv 263 \pmod{319}$, alors $(10^{11})^2 \equiv 263^2 \pmod{319}$

$263^2 = 216 \times 319 + 265$ alors $263^2 \equiv 265 \pmod{319}$. Donc $(10^{11})^2 \equiv 265 \pmod{319}$

$2^{11} = 2^9 \times 2^2 = 4 \times 2^9$, alors $2^{11} \equiv 4 \times 193 \pmod{319}$

$2^{11} \equiv 772 \pmod{319}$

$2^{11} \equiv 134 \pmod{319}$

$2^{11} \times (10^{11})^2 \equiv 134 \times 265 \pmod{319}$

$2^{11} \times (10^{11})^2 \equiv 101 \pmod{319}$

D'où $C = 101$.

b. (**3 points**) En utilisant l'algorithme d'Euclide étendu, déterminez la clé privée ***d*** correspondant à la clé publique. Vous devez présenter toutes les étapes de votre calcul.

Réponse :

On a $e \times d \equiv 1 \pmod{i}$ avec i = ppcm(10, 28) = 140.

Il faut donc résoudre $11d \equiv 1 \pmod{140}$ soit 11d +140z = 1

Pour l'algorithme d'Euclide étendu on considère les vecteurs [11, 1, 0][140, 0, 1]. Ce qui donne

[11, 1, 0][140, 0, 1]
[11, 1, 0][8, -12, 1]
[3, 13, -1][8, -12, 1]
[3, 13, -1][2, -38, 3]
[1, 51, -4][2, -38, 3]
[1, 51, -4][1, -89, 7]

On peut prendre **d = 51**.

Question 4 (**5 points)**

En utilisant l'induction mathématique, montrez que pour tout entier naturel n,

11 divise $2^{6n+3} + 3^{2n+1}$

Réponse :

Soit P(n) : $2^{6n+3} + 3^{2n+1}$est divisible par 11.

Étape de base

Pour n=0, on a :

$2^{6n+3} + 3^{2n+1} = 2^3 + 3^1 = 8 + 3 = 11$

11 est divisible par 11.

P(0) est donc vrai.

Étape inductive

Supposons pour un certain $n \geq 0$ que P(n) est vrai et montrons que P(n+1) est vrai, c'est-à-dire que $2^{6(n+1)+3} + 3^{2(n+1)+1}$ est divisible par 11.

$2^{6(n+1)+3} + 3^{2(n+1)+1} = 2^6.2^{6n+3} + 3^2.3^{2n+1}$

Par hypothèse d'induction, $2^{6n+3} + 3^{2n+1}$est divisible par 11. Posons $2^{6n+3} + 3^{2n+1} = 11k$, avec k entier.

On a : $2^{6n+3} = 11k - 3^{2n+1}$. Remplaçons cette expression dans $2^6.2^{6n+3} + 3^2.3^{2n+1}$.

$2^{6(n+1)+3} + 3^{2(n+1)+1} = 2^6.2^{6n+3} + 3^2.3^{2n+1}$ devient successivement :

$2^{6(n+1)+3} + 3^{2(n+1)+1} = 2^6.(11k - 3^{2n+1}) + 3^2.3^{2n+1}$

$2^{6(n+1)+3} + 3^{2(n+1)+1} = 2^6.11k - 3^{2n+1}(2^6 - 3^2)$

$2^{6(n+1)+3} + 3^{2(n+1)+1} = 2^6.11k - 55.3^{2n+1}$

$2^{6(n+1)+3} + 3^{2(n+1)+1} = 11(2^6.k - 5.3^{2n+1})$

$2^{6(n+1)+3} + 3^{2(n+1)+1}$ est donc divisible par 11.

Il s'en suit que P(n+1) est vrai et que P(n) → P(n+1) est vrai.

Conclusion

P(0) est vrai et $\forall n \geq 0$ P(n) → P(n+1) est vrai

On peut alors conclure que pour tout entier naturel n, $n^5 - n2^{6n+3} + 3^{2n+1}$ est divisible par 11.

Question 5 (**3 points)**

Donnez une évaluation de la complexité en Grand-**O** de $(\mathbf{n^3 + 3^n})(\mathbf{2^n + n^2})$. Justifiez votre réponse.

Réponse :

Plusieurs évaluations sont possibles.

- Exemple d'évaluation :

$\mathbf{n^3 + 3^n}$ est O($\mathbf{3^n}$) et $\mathbf{2^n + n^2}$ est O($\mathbf{2^n}$), alors $(\mathbf{n^3 + 3^n})(\mathbf{2^n + n^2})$ est O($\mathbf{3^n.2^n}$), soit $\mathbf{O(6^n)}$.