POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG1810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES ET CRYPTOGRAPHIE

H2025

Solutionnaire

Exercice 1 :

Prouvez que, pour tout entier $n \geq 1$, le nombre $4n^3 + 6n^2 + 4n + 1$ n'est pas premier.

Réponse :

Observons la factorisation suivante :

$$4n^3 + 6n^2 + 4n + 1 \ = \ (2n + 1)(2n^2 + 2n + 1).$$

En effet, en développant le produit $(2n + 1)(2n^2 + 2n + 1)$, on obtient :

$$\begin{aligned}(2n + 1)(2n^2 + 2n + 1) &= 2n \cdot 2n^2 + 2n \cdot 2n + 2n \cdot 1 + 1 \cdot 2n^2 + 1 \cdot 2n + 1 \\ &= 4n^3 + 6n^2 + 4n + 1.\end{aligned}$$

Pour tout $n \geq 1$,

$$2n + 1 \ \geq \ 3 \quad \text{et} \quad 2n^2 + 2n + 1 \ \geq \ 5.$$

Chacun de ces deux facteurs est donc strictement supérieur à 1. Le produit

$$(2n + 1)(2n^2 + 2n + 1)$$

est nécessairement un produit de deux nombres ≥ 2. Ainsi, il ne peut pas être premier.

Donc, pour tout entier $n \geq 1$, le nombre $4n^3 + 6n^2 + 4n + 1$ n'est pas premier.

Exercice 2 :

Dans le cadre d'un chiffrement RSA, on considère les valeurs $\mathrm{p} = 17$ et $\mathrm{q} = 23$.

a) Calculez la base modulaire $\mathbf{n}$

Réponse :
La base modulaire est le produit des deux nombres premiers p et q, c'est-à-dire :

$$\mathrm{n} = \mathrm{p} \cdot \mathrm{q} = 17 \cdot 23 = 391$$

Ainsi, la base modulaire n est 391.

b) Calculez l'indicatrice de Carmichael $\mathbf{i}$

Réponse :
L'indicatrice de Carmichael est le plus petit commun multiple de $\mathrm{p} - 1$ et $\mathrm{q} - 1$.

$$(\mathrm{p} - 1) = (17 - 1) = 16 = 2^4$$

$$(\mathrm{q} - 1) = (23 - 1) = 22 = 2 \cdot 11$$

Donc,

$$\mathrm{i} = \mathrm{PPCM}(\mathrm{p} - 1, \mathrm{q} - 1) = \mathrm{PPCM}(16{,}22) = 2^4 \cdot 11 = 176$$

Ainsi, l'indicatrice de Carmichael i est 176.

c) En considérant que la clé de chiffrement est $\mathbf{e} = \mathbf{5}$, calculez la valeur de la clé privée $\mathbf{d}$

Réponse :
On doit trouver l'inverse multiplicatif d tel que $\mathrm{e} \cdot \mathrm{d} \equiv 1 \bmod \mathrm{i}$.

$$\mathrm{e} \cdot \mathrm{d} \equiv 1 \bmod \mathrm{i} \Longrightarrow 5 \cdot \mathrm{d} \equiv 1 \bmod 176$$

On a donc l'équation $5\mathrm{d} + 176\mathrm{a} = 1$.
5 et 176 sont relativement premiers.
Résolvons l'équation via l'algorithme d'Euclide étendu.

$$[5, 1, 0]\ [176, 0, 1]$$

$$[5, 1, 0]\ [1, -35, 1]$$

$$[1, 141, -4]\ [1, -35, 1]$$

On peut donc prendre $\mathrm{d} = 141$ comme clé privée.
On vérifiera aisément que $5 \cdot 141 \equiv 1 \bmod 176$.

d) Quel est le message $\mathbf{C}$ chiffré à partir du message $\mathbf{M} = \mathbf{0726}$?

<u>**Note**</u> : Les calculs suivants vous sont fournis :

$$22^5 = 13180 \cdot 391 + 252$$

$$33^5 = 100090 \cdot 391 + 203$$

Réponse :

$$\mathrm{C} = \mathrm{M}^{\mathrm{e}} \bmod \mathrm{n}, \quad \text{soit} \quad 0726^5 \bmod 391$$

Ainsi,

$$0726^5 \equiv (22 \cdot 33)^5 \bmod 391 \equiv 22^5 \cdot 33^5 \bmod 391 \equiv 252 \cdot 203 \bmod 391$$

Or,

$$252 \cdot 203 = 51156 \quad \text{et} \quad 51156 = 130 \cdot 391 + 326$$

Alors,

$$252 \cdot 203 \equiv 326 \bmod 391$$

D'où,

$$\mathrm{C} = 0326$$

Exercice 3 :

Calculez la valeur de

$$\sum_{k=1}^{69420} \big((2k+1) \bmod 7\big)$$

Montrez toutes les étapes de votre réponse, y compris les calculs nécessaires pour la division de 69420 par 7.

<u>**Note :**</u>

$$69420 = 7 \times 9917 \ + \ 1,$$
$$69422 = 7 \times 9917 \ + \ 3$$

Réponse :

Notons

$$S \ = \ \sum_{k=1}^{69420} (2k+1).$$

Sans tenir compte du $\bmod 7$ pour l'instant, développons cette somme :

$$S = \sum_{k=1}^{69420} 2\,k \ + \ \sum_{k=1}^{69420} 1 = 2 \sum_{k=1}^{69420} k \ + \ 69420.$$

La somme des premiers 69420 entiers est

$$\sum_{k=1}^{69420} k = \frac{69420 \times (69420+1)}{2} = \frac{69420 \times 69421}{2}.$$

On obtient donc

$$S = 2 \times \frac{69420 \times 69421}{2} + 69420 = 69420 \times 69421 + 69420.$$

Factorisons 69420 :

$$S = 69420\,(69421+1) = 69420 \times 69422.$$

C'est cette valeur qu'on veut ensuite réduire modulo 7.

Nous allons calculer séparément

$$69420 \bmod 7 \quad \text{et} \quad 69422 \bmod 7,$$

puis multiplier les deux résultats (en tenant compte du $\bmod 7$).

D'après les calculs fournis

$$69420 = 7 \times 9917 \; + \; 1,$$

et
$$69422 = 7 \times 9917 \; + \; 3,$$

par consequent :

$$69422 \equiv 3 \pmod 7 \text{ et } 69422 \equiv 1 \pmod 7$$

Ainsi,

$$S = 69420 \times 69422 \;\equiv\; (69420 \bmod 7) \times (69422 \bmod 7) \;\equiv\; 1 \times 3 \;=\; 3 \pmod 7.$$

Donc la somme

$$\sum_{k=1}^{69420} (2k+1)$$

vaut donc $3 \pmod 7$. En d'autres termes,

$$\sum_{k=1}^{69420} \big((2k+1) \bmod 7\big) \;=\; 3 \quad (\bmod\; 7).$$

Exercice 4 :

Théo, passionné d'énigmes, découvre une lettre mystérieuse annonçant qu'il peut accéder à un trésor ancestral s'il parvient à décrypter un code secret N. La lettre contient ces indices :

- **Premier Indice :** Le nombre N est congru à 3 modulo 5, c'est-à-dire
$$N \equiv 3 \pmod 5.$$
- **Deuxième Indice :** Le nombre N est congru à 1 modulo 4, c'est-à-dire
$$N \equiv 1 \pmod 4.$$
- **Troisième Indice :** Le nombre N est congru à 6 modulo 7, c'est-à-dire
$$N \equiv 6 \pmod 7.$$
- **Quatrième Indice :** Pour confirmer la justesse du code, il faut que
$$N^{\varphi(11)} \equiv 1 \pmod{11},$$
sachant que $\varphi(11) = 10$ puisque 11 est un nombre premier.

Déterminez le plus petit entier N qui satisfait ces conditions et démontrez la validité de N en utilisant le théorème de Fermat.

Réponse :

Les deux premiers indices impliquent :

$$\begin{cases} N \equiv 3 \pmod 5 & \Rightarrow & N = 5a + 3, & a \in \mathbb{Z}, \\ N \equiv 1 \pmod 4 & \Rightarrow & N = 4b + 1, & b \in \mathbb{Z}. \end{cases}$$

Pour trouver un N commun, on peut chercher par essais :

- Les nombres de la forme $4b + 1$ sont : 1,5,9,13,17, …
- Ceux de la forme $5a + 3$ sont : 3,8,13,18,23, …

On remarque que 13 apparaît dans les deux listes. Ainsi, la solution commune est :

$$N \equiv 13 \pmod{20}.$$

On peut donc écrire :

$$N = 13 + 20k, \quad k \in \mathbb{Z}.$$

Étape 2 : Intégration de la troisième congruence

Le troisième indice indique :

$$N \equiv 6 \pmod 7.$$

En substituant $N = 13 + 20k$, on obtient :

$$13 + 20k \equiv 6 \pmod 7.$$

Comme $13 \equiv 6 \pmod{7}$, cette équation se simplifie en :

$$6 + 20k \equiv 6 \pmod{7} \quad \Rightarrow \quad 20k \equiv 0 \pmod{7}.$$

Or, $20 \equiv 6 \pmod{7}$, donc :

$$6k \equiv 0 \pmod{7}.$$

Comme 6 et 7 sont premiers entre eux, il en découle que :

$$k \equiv 0 \pmod{7} \quad \Rightarrow \quad k = 7m, \quad m \in \mathbb{Z}.$$

La solution s'écrit alors :

$$N = 13 + 20 \times 7m = 13 + 140m.$$

Pour obtenir le plus petit entier positif, on prend $m = 0$:

$$N = 13.$$

Le quatrième indice exige que :

$$N^{10} \equiv 1 \pmod{11}.$$

Calculons :

$$13 \bmod 11 = 2.$$

Il faut donc vérifier que :

$$2^{10} \equiv 1 \pmod{11}.$$

On sait que $2^{10} = 1024$. Pour obtenir $1024 \bmod 11$, on peut remarquer que :

$$1024 = 11 \times 93 + 1,$$

donc :

$$1024 \equiv 1 \pmod{11}.$$

Ainsi, on a bien :

$$13^{10} \equiv 2^{10} \equiv 1 \pmod{11}.$$

Conclusion : Le plus petit entier N vérifiant toutes les conditions est $\boxed{13}$. Le code secret qui ouvre le trésor de Théo est donc 13, et sa validité est confirmée par le théorème de Fermat.

Exercices suggérés pour la semaine :

Rosen **8e Edition**, chapitre 4 :

Section 4.1 : 4.1.1, 4.1.2, 4.1.4, 4.1.7, 4.1.10, 4.1.14, 4.1.19, 4.1.23, 4.1.26, 4.1.31, 4.1.34, 4.1.39

Section 4.2 : 4.2.1, 4.2.2, 4.2.4, 4.2.7, 4.2.11, 4.2.15, 4.2.21, 4.2.25, 4.2.29, 4.2.34, 4.2.37, 4.2.41

Section 4.3 : 4.3.1, 4.3.2, 4.3.6, 4.3.10, 4.3.14, 4.3.17, 4.3.20, 4.3.24, 4.3.28, 4.3.32, 4.3.36, 4.3.40

Section 4.4 : 4.4.58, 4.4.59, 4.4.60, 4.4.63, 4.4.66, 4.4.70, 4.4.73, 4.4.76, 4.4.79, 4.4.82

Section 4.5 : 4.5.1, 4.5.3, 4.5.6, 4.5.9, 4.5.12, 4.5.14, 4.5.18, 4.5.20, 4.5.23, 4.5.27, 4.5.29, 4.5.31

Section 4.6 : 4.6.2, 4.6.4, 4.6.6, 4.6.10, 4.6.13, 4.6.15, 4.6.19, 4.6.22, 4.6.25, 4.6.28, 4.6.31, 4.6.34