POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

LOG1810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES

A2023

SOLUTIONNAIRE

Exercice 1

Utilisez l'algorithme d'Euclide étendu pour trouver le PGCD de $\mathbf{1\,110}$ et $\mathbf{99\,999}$.

Solution :

On utilise les vecteurs de l'algorithme d'Euclide étendu, soit :

$[1\,110,\ 1,\ 0][99\,999,\ 0,\ 1]$
$[1\,110,\ 1,\ 0][99, -90,\ 1]$
$[21,\ 991, -11][99, -90,\ 1]$
$[21,\ 991, -11][15, -4\,054,\ 45]$
$[6,\ 5\,045, -56][15, -4\,054,\ 45]$
$[6,\ 5\,045, -56][3, -14\,144,\ 157]$
$[3,\ 19\,189, -213][3, -14\,144,\ 157]$

D'où le PGCD de 1 110 et 99 999 est **3**.

Exercice 2

Calculez $\left[\sum_{k=1}^{2025}\left(\left(2^{k-1}+1\right) mod\ 7\right)\right](mod\ 7)$. Détaillez votre réponse.

Note : Les calculs suivants vous sont fournis.

- $2025 = 6 \cdot 337 + 3$
- $2024 = 7 \cdot 289 + 1$

Solution :

Soit m un entier positif et $a_1, a_2, a_3, \ldots, a_n$ des entiers.
Par la définition de la congruence, on sait que :

$$\begin{aligned} a_1 &\equiv (a_1\ mod\ m)(mod\ m) \\ a_2 &\equiv (a_2\ mod\ m)(mod\ m) \\ a_3 &\equiv (a_3\ mod\ m)(mod\ m) \\ &\vdots \\ a_n &\equiv (a_n\ mod\ m)(mod\ m) \end{aligned}$$

Par conséquent,

$$a_1 + a_2 + a_3 + \cdots + a_n \equiv [(a_1\ mod\ m) + (a_2\ mod\ m) + (a_3\ mod\ m) + \cdots (a_n\ mod\ m)](mod\ m)$$

Alors, calculer $\left[\sum_{k=1}^{2025}\left(\left(2^{k-1}+1\right) mod\ 7\right)\right](mod\ 7)$ revient donc à calculer :

$$\left[\sum_{k=1}^{2025}\left(2^{k-1}+1\right)\right](mod\ 7)$$

De plus, $\sum_{k=1}^{2025}\left(2^{k-1}+1\right) = \sum_{k=1-1}^{2025-1}\left(2^{k-1+1}+1\right)$
$= \sum_{k=0}^{2024}\left(2^{k}+1\right)$
$= \left(\sum_{k=0}^{2024} 2^{k}\right) + \left(\sum_{k=0}^{2024} 1\right)$

$$= \left(\frac{2^{2024+1}-1}{2-1}\right) + (2024 - 0 + 1)$$
$$= 2^{2025} + 2024.$$

D'une part, on sait que $2025 = 6 \cdot 337 + 3$.

Et donc, $2^{2025} \equiv 2^{6\cdot 337+3} \ (mod\ 7)$
$\equiv (2^6)^{337} \cdot 2^3 \ (mod\ 7)$

D'après le petit théorème de Fermat,

- 7 étant premier
- 2 et 7 sont premiers entre eux

On a ainsi : $2^6 \equiv 1(mod\ 7)$.

On obtient alors

$$(2^6)^{337} \cdot 2^3 \equiv 1 \cdot 2^3 (mod\ 7)$$

Soit

$$(2^6)^{337} \cdot 2^3 \equiv 8\ (mod\ 7)$$

Ou encore

$$(2^6)^{337} \cdot 2^3 \equiv 1\ (mod\ 7)$$

D'où $2^{2025} \equiv 1\ (mod\ 7)$.

D'autre part, on sait que $2024 = 7 \cdot 289 + 1$.
Ce qui implique que $2024 \equiv 1\ (mod\ 7)$.

Ainsi, $\left[\sum_{k=1}^{2025}\left(2^{k-1}+1\right)\right] \equiv 2^{2025} + 2024\ (mod\ 7) \equiv 1 + 1\ (mod\ 7) \equiv 2\ (mod\ 7)$.

D'où $\left[\sum_{k=1}^{2025}\left(\left(2^{k-1}+1\right)\ mod\ 7\right)\right] \equiv 2\ (mod\ 7)$.

Exercice 3

Soit $\boldsymbol{p} = 2025$ et $\boldsymbol{q} = 2025^{2025}$. Quel est le reste de la division de $\boldsymbol{p^q + q^p}$ par 7 ? Détaillez votre réponse.

Note : $\forall k \in \mathbb{N}^*, 3^k \equiv 3\ (mod\ 6)$.

Solution :

Évaluons d'abord, $p\ (mod\ 7)$.
$2025 \equiv 2\ (mod\ 7)$ alors $2025^k \equiv 2^k\ (mod\ 7)$ avec k entier.
Donc, $p^q + q^p \equiv 2025^{(2025^{2025})} + (2025^{2025})^{2025}\ (mod\ 7)$
$\equiv 2^{(2025^{2025})} + 2^{(2025^2)}\ (mod\ 7)$

D'après le petit théorème de Fermat,

- 7 étant premier
- 2 et 7 sont premiers entre eux

On a donc : $2^6 \equiv 1(mod\ 7)$.

D'une part, il suffit donc de rechercher le reste de la division de 2025^{2025} par 6 pour évaluer $2^{(2025^{2025})}\ (mod\ 7)$.
$2025 \equiv 3\ (mod\ 6)$ alors $2025^{2025} \equiv 3^{2025}\ (mod\ 6)$.
Or, $\forall k \in \mathbb{N}^*, 3^k \equiv 3\ (mod\ 6)$ alors $3^{2025} \equiv 3\ (mod\ 6)$.
Par suite, $2025^{2025} \equiv 3\ (mod\ 6)$, ce qui signifie que $2025^{2025} = 6n + 3$ avec n entier.

Et d'autre part, il suffit de rechercher le reste de la division de 2025^2 par 6 pour évaluer $2^{(2025^2)}\ (mod\ 7)$.
$2025 \equiv 3\ (mod\ 6)$ alors $2025^2 \equiv 3^2(mod\ 6)$.
Et par suite, $2025^2 \equiv 3\ (mod\ 6)$, ce qui signifie que $2025^2 = 6n + 3$ avec n entier.

Ainsi,

$$2^{(2025^{2025})} + 2^{(2025^2)} \equiv 2^3 + 2^3\ (mod\ 7)$$

Soit

$$2^{(2025^{2025})} + 2^{(2025^2)} \equiv 16\ (mod\ 7)$$

Ou encore

$$2^{(2025^{2025})} + 2^{(2025^2)} \equiv 2\ (mod\ 7)$$

D'où $p^q + q^p \equiv 2\ (mod\ 7)$.

Exercice 4

Le millésime est une notion essentielle dans le monde de la viticulture et du vin. Il fait référence à l'année de récolte des raisins utilisés pour produire un vin donné. Chaque millésime est unique, car il est influencé par les conditions climatiques, les pratiques viticoles et les caractéristiques propres à chaque région viticole. Lors d'une dégustation de vins millésimés, un sommelier observe une congruence linéaire particulière entre les millésimes des bouteilles et les caractéristiques des raisins utilisés. Il constate que tous les millésimes qui sont divisibles par 5 ont également la particularité de laisser un reste de 1 lorsqu'ils sont divisés par 3. Quels sont tous les millésimes après J.-C. (après l'année zéro) qui satisfont ces conditions. Montrez toutes les étapes de votre réponse.

L'abus d'alcool est dangereux pour la santé, à consommer avec modération.

Solution :

Pour ce faire, nous devons résoudre le système d'équation suivant :

$$\begin{cases} m \equiv 0\ (mod\ 5) \\ m \equiv 1\ (mod\ 3) \end{cases}$$

Où $m \in \mathbb{N}^*$.

Elles peuvent être réécrites comme suit :

$$\begin{cases} m = 5a \\ m = 3b + 1 \end{cases}$$

On obtient donc :

$$5a = 3b + 1$$

En réécrivant, on a :

$$5a - 3b = 1$$

Il suffit donc de résoudre l'équation :

$$5a' + 3b' = 1$$

5 et 3 sont relativement premiers.

Résolvons l'équation via l'algorithme d'Euclide étendu :

$[5,\ 1,\ 0][3,\ 0,\ 1]$
$[2,\ 1, -1][3,\ 0,\ 1]$
$[2,\ 1, -1][1, -1,\ 2]$
$[1,\ 2, -3][1, -1,\ 2]$

On peut prendre $a' = -1$ et $b' = 2$ comme une des solutions de $\mathbf{5a' + 3b' = 1}$.
On en déduit que $a = -1$ et $b = -2$ constituent une solution particulière de l'équation $\mathbf{5a - 3b = 1}$.
Les solutions recherchées pour l'équation $\mathbf{5a - 3b = 1}$ sont donc de la forme :

$$\begin{cases} a = 3k - 1 \\ b = 5k - 2 \end{cases}$$

Avec $k \in \mathbb{N}^*$.
Ainsi, on obtient :

$$\begin{cases} m = 5a \\ m = 3b + 1 \end{cases} \Leftrightarrow \begin{cases} m = 5(3k - 1) \\ m = 3(5k - 2) + 1 \end{cases} \Leftrightarrow \begin{cases} m = 15k - 5 \\ m = 15k - 5 \end{cases}$$

De ce fait, tous les millésimes apr. J.-C. m divisibles par 5 qui laissent un reste de 1 lorsqu'ils sont divisés par 3 sont $\{m \in \mathbb{N}^* \mid m = 15k - 5\}$ avec $k \in \mathbb{N}^*$.

Exercice 5

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

a) Calculez la base modulaire $\boldsymbol{n}$.

Solution :

La base modulaire est le produit des deux nombres premiers $\boldsymbol{p}$ et $\boldsymbol{q}$, c'est-à-dire :

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

Ainsi, la base modulaire $\boldsymbol{n}$ est 391.

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

Solution :

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

$(\boldsymbol{p}-1)=(17-1)=16=2^4$
$(\boldsymbol{q}-1)=(23-1)=22=2\cdot 11$

Donc, $\boldsymbol{i}=PPCM(\boldsymbol{p}-1,\boldsymbol{q}-1)=PPCM(16,22)=2^{\max(4,1)}\cdot 11^{\max(0,1)}=2^4\cdot 11=176$.
Ainsi, l'indicatrice de Carmichael $\boldsymbol{i}$ est 176.

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

Solution :

On doit trouver l'inverse multiplicatif $\boldsymbol{d}$ tel que $\boldsymbol{e}\cdot\boldsymbol{d}\equiv 1\ (mod\ \boldsymbol{i})$.
$\boldsymbol{e}\cdot\boldsymbol{d}\equiv 1(mod\ \boldsymbol{i})$ alors $5\cdot\boldsymbol{d}\equiv 1\ (mod\ 176)$.
On a donc l'équation $5\,\boldsymbol{d}+176\,\boldsymbol{a}=1$.
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 $\boldsymbol{d}=141$ comme clé privée.
On vérifiera aisément que $5\cdot 141\equiv 1\ (mod\ 176)$.

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

Note : Les calculs suivants vous sont fournis.

- $22^5=13\,180\cdot 391+252$
- $33^5=100\,090\cdot 391+203$

Solution :

$\boldsymbol{C}=\boldsymbol{M}^{\boldsymbol{e}}\ mod\ \boldsymbol{n}$, soit $0726^5\ mod\ 391$.
Ainsi, $0726^5\equiv(22\cdot 33)^5\ (mod\ 391)\equiv 22^5\cdot 33^5\ (mod\ 391)\equiv 252\cdot 203\ (mod\ 391)$.
Or, $252\cdot 203=51\,156$ et $51\,156=130\cdot 391+326$.
Alors, $252\cdot 203\equiv 326\ (mod\ 391)$.
D'où $\boldsymbol{C}=0326$.

Exercice 6

Calculez $[(3^{493}\ mod\ 1039) \cdot (3^{531}\ mod\ 1039)]\ (mod\ 1039)$. Détaillez votre réponse.

Note : Les calculs suivants vous sont fournis.

- $27^4 = 1039 \cdot 511 + 512$
- $9 \cdot 512 = 1039 \cdot 4 + 452$

Solution :

Soit m un entier positif et a et b des entiers,
Par la définition de la congruence, on sait que

$$a \equiv (a\ mod\ m)(mod\ m)$$
$$b \equiv (b\ mod\ m)(mod\ m)$$

Par conséquent,

$$a \cdot b \equiv [(a\ mod\ m) \cdot (b\ mod\ m)](mod\ m)$$

Ainsi, calculer $[(3^{493}\ mod\ 1039) \cdot (3^{531}\ mod\ 1039)]\ (mod\ 1039)$ revient à calculer :

$$3^{1024}\ (mod\ 1039)$$

D'après le petit théorème de Fermat, 1039 étant premier et 3 ne divise pas 1039, on a :

$$3^{1038} \equiv 1\ (mod\ 1039) \qquad \textbf{(I.)}$$

Or, $1038 = 1024 + 14$.
Alors $3^{1038} \equiv 3^{1024} \cdot 3^{14}\ (mod\ 1039)$.

D'une part, $3^{14} \equiv (3^2)^7\ (mod\ 1039)$
$\equiv (3^2) \cdot (3^2)^6\ (mod\ 1039)$
$\equiv (3^2) \cdot (3^2)^{2\cdot 3}\ (mod\ 1039)$
$\equiv (3^2) \cdot (3^3)^{2\cdot 2}\ (mod\ 1039)$
$\equiv 9 \cdot (27)^4\ (mod\ 1039)$

On sait que $27^4 = 1039 \cdot 511 + 512$.
Alors, $9 \cdot (27)^4 \equiv 9 \cdot 512\ (mod\ 1039)$.
Aussi, on sait que $9 \cdot 512 = 1039 \cdot 4 + 452$.
Et donc, $9 \cdot 512 \equiv 452\ (mod\ 1039)$.
D'où $3^{14} \equiv 452\ (mod\ 1039)$.

D'autre part, supposons que $3^{1024} \equiv a\ (mod\ 1039)$.

Par suite,

$$3^{1024} \cdot 3^{14} \equiv a \cdot 452\ (mod\ 1039) \qquad \textbf{(II.)}$$

Avec **(I.)** et **(II.)**, on déduit que

$$452a \equiv 1\ (mod\ 1039)$$

Il nous faut alors résoudre l'équation suivante :

$$452\ a + 1039\ b = 1$$

452 et 1039 sont relativement premiers.
Résolvons l'équation via l'algorithme d'Euclide étendu.

$[452,\ 1,\ 0]\ [1039,\ 0,\ 1]$
$[452,\ 1,\ 0]\ [135, -2,\ 1]$
$[47,\ 7, -3]\ [135, -2,\ 1]$
$[47,\ 7, -3]\ [41, -16,\ 7]$
$[6,\ 23, -10]\ [41, -16,\ 7]$
$[6,\ 23, -10][5, -154,\ 67]$
$[1,\ 177, -77]\ [5, -154,\ 67]$
$[1,\ 177, -77]\ [1, -862,\ 375]$

Ainsi, on peut donc prendre $a = 177$ et conclure que

$$[(3^{493}\ mod\ 1039) \cdot (3^{531}\ mod\ 1039)] \equiv 177\ (mod\ 1039)$$

Exercice 7 (Facultatif)
En utilisant vos connaissances en congruences, montrez que

$$\forall n \in \mathbb{N},\ \ 11 \text{ divise } 4^{5n+2} + 3^{5n} + 5^{5n+1}$$

Solution :

- $4^{5n+2} = 4^2 \cdot (4^2 \cdot 4^2 \cdot 4)^n = 16 \cdot (16 \cdot 16 \cdot 4)^n$.
  Or, $16 \equiv 5\ (mod\ 11)$ donc $16 \cdot 16 \cdot 4 \equiv 5 \cdot 5 \cdot 4\ (mod\ 11) \equiv 100\ (mod\ 11) \equiv 1\ (mod\ 11)$.
  Alors $(16 \cdot 16 \cdot 4)^n \equiv 1\ (mod\ 11)$ et par suite, $4^{5n+2} \equiv 5\ (mod\ 11)$.

- $3^{5n} = (3^5)^n = (3^2 \cdot 3^2 \cdot 3)^n = (9 \cdot 9 \cdot 3)^n = (81 \cdot 3)^n$.
  Or, $81 \equiv 4\ (mod\ 11)$ donc $81 \cdot 3 \equiv 4 \cdot 3\ (mod\ 11) \equiv 12\ (mod\ 11) \equiv 1\ (mod\ 11)$.
  Alors $(81 \cdot 3)^n \equiv 1\ (mod\ 11)$ et par suite, $3^{5n} \equiv 1\ (mod\ 11)$.

- $5^{5n+1} = 5 \cdot (5^2 \cdot 5^2 \cdot 5)^n = 5 \cdot (25 \cdot 25 \cdot 5)^n$.
  Or, $25 \equiv 3\ (mod\ 11)$ donc $25 \cdot 25 \cdot 5 \equiv 3 \cdot 3 \cdot 5\ (mod\ 11) \equiv 45\ (mod\ 11) \equiv 1\ (mod\ 11)$.
  Alors $(5^2 \cdot 5^2 \cdot 5)^n \equiv 1\ (mod\ 11)$ et par suite, $5^{5n+1} \equiv 5\ (mod\ 11)$.

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