POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

LOG1810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES

E2023

SOLUTIONNAIRE

Exercice 1

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 2

Calculez $\left[\left(PPCM(32,8)\right)^{PGCD(51,39)} mod\ 13\right]^{PGCD(66,34)} (mod\ 11)$ où $\boldsymbol{PPCM(a,b)}$ correspond au plus petit commun multiple de $\boldsymbol{a}$ et $\boldsymbol{b}$ et $\boldsymbol{PGCD(a,b)}$ correspond au plus grand commun diviseur de $\boldsymbol{a}$ et $\boldsymbol{b}$. Montrez toutes les étapes de votre réponse.

Solution :

Évaluons d'abord $PPCM(32,8)$.
On sait que $32 = 2^5$ et $8 = 2^3$.
Alors, $PPCM(32,8) = 2^{\max(5,3)} = 2^5 = 32$.
Évaluons ensuite $PGCD(51,39)$.
$PGCD(51,39) = PGCD(12,39) = PGCD(12,3) = PGCD(3,3) = 3$.
On en déduit que, $\left(PPCM(32,8)\right)^{PGCD(51,39)} = (32)^3$.
Or, $32 \equiv 6(mod\ 13)$, donc $(32)^3 \equiv (6)^3 (mod\ 13)$.
Ou encore, $(6)^3 = 216$ et $216 = 16 \cdot 13 + 8$.
Ainsi, $(32)^3 \equiv 8(mod\ 13)$.

Évaluons maintenant $PGCD(66,34)$.
$PGCD(66,34) = PGCD(32,34) = PGCD(32,2) = PGCD(2,2) = 2$.
Et donc, calculer $\left[\left(PPCM(32,8)\right)^{PGCD(51,39)} mod\ 13\right]^{PGCD(66,34)} (mod\ 11)$ revient à calculer $8^2 (mod\ 11)$.
Or, $8^2 = 64$ et $64 = 5 \cdot 11 + 9$.
Et enfin, $8^2 \equiv 9(mod\ 11)$.

D'où, $\left[\left(PPCM(32,8)\right)^{PGCD(51,39)} mod\ 13\right]^{PGCD(66,34)} \equiv 9(mod\ 11)$.

Exercice 3

Calculez $\left[\sum_{k=1}^{2023}\left((2k+1)\ mod\ 31\right)\right](mod\ 31)$. Montrez toutes les étapes de votre réponse.

Solution :

Soit m un entier positif et a_1, a_2, a_3, …, 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,
$a_1 + a_2 + a_3 + \cdots + a_n \equiv [(a_1\ mod\ m) + (a_2\ mod\ m) + (a_3\ mod\ m) + \cdots (a_n\ mod\ m)](mod\ m)$.
Et donc, calculer $\left[\sum_{k=1}^{2023}\left((2k+1)\ mod\ 31\right)\right](mod\ 31)$ revient à calculer $\left[\sum_{k=1}^{2023}(2k+1)\right](mod\ 31)$.
De plus, $\sum_{k=1}^{2023}(2k+1) = \sum_{k=1}^{2023} 2k + \sum_{k=1}^{2023} 1 = \frac{2\cdot 2023\cdot 2024}{2} + (2023 - 1 + 1) = 2023 \cdot 2025$.
D'une part, $2023 = 65 \cdot 31 + 8$.
D'autre part, $2025 = 65 \cdot 31 + 10$.
Ainsi, $\left[\sum_{k=1}^{2023}(2k+1)\right] \equiv 2023 \cdot 2025(mod\ 31) \equiv 8 \cdot 10(mod\ 31) \equiv 18(mod\ 31)$.

D'où, $\left[\sum_{k=1}^{2023}\left((2k+1)\ mod\ 31\right)\right] \equiv 18(mod\ 31)$.

Exercice 4

Dans le cadre d'un chiffrement RSA, on considère les valeurs $\boldsymbol{p} = 17$ (qui est le 7ème nombre premier) et $\boldsymbol{q} = 23$ (qui est le 9ème nombre premier).

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 :

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

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 $\boldsymbol{e}\cdot\boldsymbol{d}\equiv 1(mod\ \boldsymbol{i})$.
$\boldsymbol{e}\cdot\boldsymbol{d}\equiv 1(mod\ \boldsymbol{i})\Rightarrow 5\cdot\boldsymbol{d}\equiv 1(mod\ 176)$.
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 $\boldsymbol{M}=726$?
Indices : Les calculs suivants vous sont fournis.
(I.) $22^5=13\,180\cdot 391+252$
(II.) $33^5=100\,090\cdot 391+203$

Solution :

$\boldsymbol{C}=\boldsymbol{M}^{\boldsymbol{e}}\ mod\ \boldsymbol{n}$, soit $726^5\ mod\ 391$.
Ainsi, $726^5\equiv(22\cdot 33)^5\ mod\ 391\equiv 22^5\cdot 33^5\ mod\ 391\equiv 252\cdot 203\ mod\ 391$.
Or, $252\cdot 203=51\,156$ et $51\,156=130\cdot 391+326$.
Alors, $252\cdot 203\equiv 326\ mod\ 391$.
D'où $\boldsymbol{C}$ = 326.

Exercice 5

Montrez que 7 divise $2222^{5555} + 5555^{2222}$.

Indices : Les calculs suivants vous sont fournis.

(I.) 5555 = 6 · 925 + 5
(II.) 2222 = 7 · 317 + 3
(III.) 2222 = 6 · 370 + 2
(IV.) 5555 = 7 · 793 + 4

Solution :

7 est un nombre premier et 7 ne divise pas 2222.
En appliquant le petit théorème de Fermat, $2222^6 \equiv 1\ (mod\ 7)$.
Or, 5555 = 6 · 925 + 5, donc $2222^{5555} \equiv 1^{925} \cdot 2222^5\ (mod\ 7)$.
Ainsi, $2222^{5555} \equiv 2222^5\ (mod\ 7)$.
Or, 2222 = 7 · 317 + 3, donc $2222 \equiv 3\ (mod\ 7)$.
Donc, $2222^5 \equiv 3^5\ (mod\ 7)$, soit $2222^5 \equiv 5\ (mod\ 7)$.
D'où $2222^{5555} \equiv 5\ (mod\ 7)$.

Similairement, 7 est un nombre premier et 7 ne divise pas 5555.
En appliquant le petit théorème de Fermat, $5555^6 \equiv 1\ (mod\ 7)$.
Or, 2222 = 6 · 370 + 2, donc $5555^{2222} \equiv 1^{370} \cdot 5555^2\ (mod\ 7)$.
Ainsi, $5555^{2222} \equiv 5555^2\ (mod\ 7)$.
Or, 5555 = 7 · 793 + 4, donc $5555 \equiv 4\ (mod\ 7)$.
Donc, $5555^2 \equiv 4^2\ (mod\ 7)$, soit $5555^2 \equiv 2\ (mod\ 7)$.
D'où $5555^{2222} \equiv 2\ (mod\ 7)$.

Enfin, nous obtenons
$2222^{5555} \equiv 5\ (mod\ 7)$ et $5555^{2222} \equiv 2\ (mod\ 7)$,
Alors $(2222^{5555} + 5555^{2222}) \equiv (5+2)\ (mod\ 7)$.
Soit $(2222^{5555} + 5555^{2222}) \equiv 0$ (mod 7).
D'où 7 divise $2222^{5555} + 5555^{2222}$.
CQFD

Exercice 6

Soit a un entier et n un entier naturel. En utilisant vos connaissances en théorie des nombres, montrez que $(a^{4n+1} - a)$ est divisible par 5.

Solution :

$(a^{4n+1} - a) = a(a^{4n} - 1) = a((a^4)^n - 1)$

Les deux cas sont :

- **Cas 1)** a est divisible par 5

- **Cas 2)** a n'est pas divisible par 5

Cas 1) a est divisible par 5
Si a est divisible par 5, alors trivialement $a((a^4)^n - 1)$ est divisible par 5.

Cas 2) a n'est pas divisible par 5
a n'est pas divisible par 5 et 5 est premier.
D'après le petit théorème de Fermat, on a : $a^4 \equiv 1(mod\ 5)$.
Et donc, $(a^4)^n \equiv (1)^n(mod\ 5)$, soit $(a^4)^n \equiv 1(mod\ 5)$.
On obtient successivement :

$(a^4)^n \equiv 1(mod\ 3) \quad \Leftrightarrow (a^4)^n - 1 \equiv 0(mod\ 5)$
$\Leftrightarrow a((a^4)^n - 1) \equiv 0(mod\ 5)$

Ainsi lorsque a n'est pas divisible par 5, $(a^{4n+1} - a)$ est également divisible par 5.

Dans les deux cas, $(a^{4n+1} - a)$ est divisible par 5.
CQFD

Exercice 7
Calculez [($101^{493}\ mod\ 13$) · ($101^{508}\ mod\ 13$)] (mod 13). Montrez toutes les étapes de votre réponse.

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, $101^{493} \cdot 101^{508} = 101^{1001} \equiv [(101^{493}\ mod\ 13) \cdot (101^{508}\ mod\ 13)]\ (mod\ 13)$.
Donc, calculer [($101^{493}\ mod\ 13$) · ($101^{508}\ mod\ 13$)] (mod 13) revient à calculer 101^{1001} (mod 13).
$101 \equiv 10$ (mod 13), alors $101^{1001} \equiv 10^{1001}$ (mod 13).
13 est un nombre premier et 13 ne divise pas 10.
Par le petit théorème de Fermat, on sait que $10^{12} \equiv 1$ (mod 13).
Or, 1001 = 12 · 83 + 5.
Et donc, $10^{1001} = (10^{12})^{83} \cdot 10^5 \equiv 1^{83} \cdot 10^5$ (mod 13) $\equiv 1 \cdot 10^5$ (mod 13) $\equiv 10^5$ (mod 13).
Puisque $10^5 = 10\ (10^2)^2$.
Et $10^2 = 100 \equiv 9$ (mod 13).
Donc $10^5 = 10\ (10^2)^2 \equiv 10 \cdot 9^2$ (mod 13) $\equiv 10 \cdot 81$ (mod 13) $\equiv 10 \cdot 3$ (mod 13) $\equiv 30$ (mod 13)
$\equiv 4$ (mod 13).
D'où [($101^{493}\ mod\ 13$) · ($101^{508}\ mod\ 13$)] (mod 13) $= 101^{1001}$ (mod 13) $\equiv 4$ (mod 13).