POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG2810
STRUCTURES DISCRÈTES

TD 7 : **THÉORIE DES NOMBRES**
H2022

SOLUTIONNAIRE

Directives pour la remise :

- La remise est individuelle, mais le travail en équipe est encouragé.
- La remise est individuelle se fait à la fin de la séance de TD.
- Répondez directement sur ce document Word (docx). Dans l'intérêt de l'équité pour tous les étudiants, vous devez modifier le fichier Word. Modifiez le fichier **EXCLUT** le fait d'intégrer des scans de rédaction manuscrite ou d'y écrire avec un stylet.
- Lorsque vous avez terminé, générez un PDF avec le nom sous le format :
  Matricule-TDNuméro.pdf (exemple : 1234567-TD1.pdf).
- Téléversez votre fichier PDF dans la boîte de remise située dans la Zone TDs de la page Moodle du cours.
- Choisissez la boîte de remise qui correspond à votre section de TD.
- **Aucun retard et aucune remise par courriel ne seront acceptés.**
- **Le non-respect des consignes entraînera automatiquement la note 0 pour ce TD.**

Exercice 1. On dispose de :

- deux bidons vides, l'un de 6 litres et l'autre de 11 litres
- d'un contenant de 50 litres de capacité, muni de robinet pour des prélèvements de son contenu. Le contenant est vide.
- d'une source d'eau muni d'un robinet pour prélever de l'eau.

a) Proposez une solution pour mettre 13 litres d'eau dans le contenant, en utilisant uniquement les deux bidons. Expliquez votre démarche.

Réponse :

1ère Solution

- On charge le bidon de 6L qu'on déverse dans le contenant, qui contient alors 6 L.
- On charge le bidon de 6L qu'on déverse dans le contenant, qui contient alors 12 L.
- On extrait du contenant 11L d'eau avec le bidon de 11L. Il reste 1 litre dans le contenant.
- On charge le bidon de 6L qu'on déverse dans le contenant, qui contient alors 7 L.
- On charge le bidon de 6L qu'on déverse dans le contenant, qui contient alors 13 L.

2ème Solution

- On charge le bidon de 11L qu'on déverse dans le contenant, qui contient alors 11 L
- On extrait du contenant 6L d'eau avec le bidon de 6L. Il reste 5 litres dans le contenant
- On charge le bidon de 11L qu'on déverse dans le contenant, qui contient alors 16 L
- On extrait du contenant 6L d'eau avec le bidon de 6L. Il reste 10 litres dans le contenant
- On extrait du contenant 6L d'eau avec le bidon de 6L. Il reste 4 litres dans le contenant
- On charge le bidon de 11L qu'on déverse dans le contenant, qui contient alors 15 L
- On extrait du contenant 6L litres d'eau avec le bidon de 6L. Il reste 9 litres dans le contenant
- On extrait du contenant 6L litres d'eau avec le bidon de 6L. Il reste 3 litres dans le contenant
- On charge le bidon de 11L qu'on déverse dans le contenant, qui contient alors 14 L
- On extrait du contenant 6L litres d'eau avec le bidon de 6L. Il reste 8 litres dans le contenant
- On extrait du contenant 6L litres d'eau avec le bidon de 6L. Il reste 2 litres dans le contenant
- On charge le bidon de 11L qu'on déverse dans le contenant, qui contient alors 13 L

b) Comment pouvez-vous exploiter vos connaissances en théorie des nombres pour répondre à la question précédente ?

Réponse :

On peut résoudre l'équation 6n + 11m =13 ou précisément 6n + 11m =1. De plus i faudra considérer un prélèvement dans le contenant comme une opération avec un signe négatif (-) et un remplissage comme une opération avec un signe positif.

La résolution de l'équation pourrait avoir comme solution (2, -1) ou encore (-4, 9). Elles peuvent servir de base de raisonnement. Il vous revient de combiner librement les remplissages (+) et les extractions (-). C'est justement le (2, -1) qui est utilisée au début de la première solution.

Attention à ne pas multiplier le résultat directement par 13 à cause de la limitation de la capacité du contenant à 50L. Exemple (2, -1) donnerait (26, -13) comme une des solutions à l'équation 6n + 11m =13. Appliqué ce résultat directement ne tiendrait pas compte de la limitation de la capacité. Par contre, en y allant diligemment, on peut y arriver.

Exercice 2. Dans le cadre d'un chiffrement RSA, on considère les valeurs p=53, q=11

a) Calculez la base modulaire n.

Réponse :

La base modulaire est n = p.q = 53.11= 583

b) Calculez l'indicatrice de Carmichael i = ppcm(p - 1, q - 1)

Réponse :

i= ppcm(52, 10)

i=260

c) En considérant que la clé de chiffrement est e=113, Calculez la valeur de la clé privée d

Réponse :

e.d ≡ 1 (mod i)

e.d ≡ 1 (mod 260)

113d ≡ 1 (mod 260)

Nous avons donc l'équation 113d +260x = 1

113 et 260 sont relativement premiers.

Résolvons l'équation avec l'algorithme d'Euclide étendu.

[113, 1, 0][260, 0, 1]

[113, 1, 0][147, -1, 1]

[113, 1, 0][34, -2, 1]

[79, 3, -1][34, -2, 1]

[45, 5, -2][34, -2, 1]

[11, 7, -3][34, -2, 1]

[11, 7, -3][23, -9, 4]

[11, 7, -3][12, -16, 7]

[11, 7, -3][1, -23, 10]

…

[2, 214, -93][1, -23, 10]

[1, 237, -103][1, -23, 10]

On peut prendre d=237 comme clé privée.

On vérifiera aisément que 113.237 ≡ 1 (mod 260)

d) **(Facultatif)** Le message à crypter est découpé en 3 blocs comme ci-dessous. Quel est le résultat du chiffrement.

090 086 067

Réponse :

Chiffrement bloc 1 : 090^{113} mod 583 = 052

Chiffrement bloc 2 : 086^{113} mod 583 = 080

Chiffrement bloc 3 : 067^{113} mod 583 = 551

Le résultat du chiffrement est : 052 080 551

e) **(Facultatif)** Vérifiez le résultat précédent en appliquant la clé privée pour le déchiffrer.

Réponse :

Il faut déchiffrer 052 080 551 en calculant les 3 blocs

$052^{237} \bmod 583$

$080^{237} \bmod 583$

$551^{237} \bmod 583$

Exercice 3. Soit n un nombre premier et a un entier naturel. Montrez que :

$(a+1)^n - a^n - 1$ est divisible par n.

Réponse :

n étant premier, d'après le petit théorème de Fermat, on a :

$a^n \equiv a \pmod n$ et $(a+1)^n \equiv (a+1) \pmod n$

En soustrayant la première expression de la 2ème expression, on obtient successivement :

$(a+1)^n - a^n \equiv ((a+1)- a) \pmod n$

$(a+1)^n - a^n \equiv 1 \pmod n$

$(a+1)^n - a^n - 1 \equiv 0 \pmod n$

D'où $(a+1)^n - a^n - 1$ est divisible par n.

Exercice 4. Résolvez modulo 18 l'équation suivante :

$$\mathbf{5x + 13 = 16}$$

Réponse :

On a : $5x + 13 \equiv 16 \pmod{18}$

Après simplification, on obtient : $5x \equiv 3 \pmod{18}$

Il s'agit alors de résoudre l'équation $5x+ 18m = 3$.

5 et 18 étant relativement premiers, nous résolvons dans un 1er temps l'équation $5x+ 18m = 1$.

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

[5, 1, 0][18, 0, 1]

[5, 1, 0][3, -3, 1]

[2, 4, -1][3, -3, 1]

…

[1, 11, -3][1, -7, 2]

On obtient les couples (11, -3) et (-7, 2).

Retenons le couple (11, -3). L'équation initiale étant $5x+ 18m = 3$, il suffit de considérer (3x11, -3 x 3) soit (33, -9).

La valeur x recherchée est donc **x = 33 + 18k**, avec k entier.

Exercice 5. Calculez $3^{1024} \bmod 1039$

Réponse :

1039 est un nombre premier. D'après le petit théorème de Fermat $3^{1038} \equiv 1 \pmod{1039}$.
0n sait que 1038 = 1024 + 14 donc $3^{1038} = 3^{1024.}\ 3^{14}$.
$3^{1024.}\ 3^{14} \equiv 1 \pmod{1039}$
$3^{14} = (3^2)^7 = (3^2)\,(3^3)^4 = (3^2)\,(27)^4 = 9 \times 27^4$
$27^3 \equiv 981 \pmod{1039}$
$27^4 \equiv (981 \times 27) \pmod{1039}$
$27^4 \equiv 512 \pmod{1039}$
$9.\ 27^4 \equiv (9 \times 512) \pmod{1039}$
$9.\ 27^4 \equiv 452 \pmod{1039}$ d'où $3^{14} \equiv 452 \pmod{1039}$
Supposons que $3^{1024.} \equiv y \pmod{1039}$. Puisque $3^{14} \equiv 452 \pmod{1039}$, on a :
$3^{1024.}\ 3^{14} \equiv 452y \pmod{1039}$. Or $3^{1038} \equiv 1 \pmod{1039}$. Donc, $452y \equiv 1 \pmod{1039}$
Il nous faut alors résoudre l'équation 452y + 1037m = 1.
On peut utiliser les vecteurs avec l'algorithme d'Euclide étendu.
On considère donc les vecteurs [452, 1, 0][1039, 0, 1]
Après résolution on obtient [1, 177, -77][1, -862, 375]
On peut donc prendre y = 177 et conclure que **$3^{1024.} \equiv 177 \pmod{1039}$**.

Exercice 6. Soit x un entier. Trouvez x tel que (x mod 88 = 2) et (x mod 27 = 1).

Réponse :

(x mod 88 = 2) et (x mod 27 = 1) peuvent être réécrits comme suit : (x = 88 y + 2) et (x = 27 z +1)
On obtient : 88 y + 2 = 27 z +1. 88 et 27 étant relativement premiers.
En réécrivant, on a -88y+27z = 1
Il suffit donc de résoudre l'équation 88 p + 27 z = 1. Ce qui donne avec l'algorithme d'Euclide étendu les vecteurs [1, 4, -13][1, -23, 75]
On peut prendre p=4 et z = -13, soit y = -4 et z = -13. On en déduit que **x = -350**.