Devoir à la maison n° 2
Algèbres de Boole
Congruences modulo n - Entiers modulo n

Exercice 1 :

1. Soit n un entier naturel non nul, et a un entier quelconque.
   Donner la définition du résidu de a modulo n.
2. Calculer le plus judicieusement possible les résidus modulo 7 des entiers $53, 53^2$ et 53^3.
3. En déduire le résidu modulo 7 de 53^5.

Exercice 2 :

1. Soit n un entier quelconque. Ecrire la division euclidienne de n par 5. Quels sont alors les restes possibles dans cette division ?
2. Pour chaque valeur possible de ce reste, calculer le résidu modulo 5 de n^2, n^3 et n^4.
   On pourra présenter les résultats dans un tableau pour plus de clarté.
3. En déduire que pour tout entier n il existe un entier k tel que $n^4 = 5k$ ou $n^4 = 1 + 5k$.

Exercice 3 :

1. Construire la table de multiplication dans $\mathbb{Z}/8\mathbb{Z}$.
2. Déterminer les éléments inversibles dans $\mathbb{Z}/8\mathbb{Z}$ et déterminer leurs inverses.
3. Quels sont les diviseurs de zéro dans $\mathbb{Z}/8\mathbb{Z}$? Justifiez votre réponse.
4. Résoudre dans $\mathbb{Z}/8\mathbb{Z}$ les équations $\dot{5}\dot{x} = \dot{7}$ et $\dot{4}\dot{x} = \dot{4}$.

Exercice 4 : On considère l'ensemble $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$.

1. Dresser la table de multiplication dans $\mathbb{Z}/4\mathbb{Z}$.
2. Résoudre dans $\mathbb{Z}/4\mathbb{Z}$ l'équation $\dot{2}x = \dot{2}$.
3. Résoudre dans $\mathbb{Z}/4\mathbb{Z}$ le système $\left\{ \begin{array}{lcl} \dot{2}x + \dot{3}y & = & \dot{2} \\ \dot{2}x + \dot{1}y & = & \dot{2} \end{array} \right.$
4. Résoudre dans $\mathbb{Z}/4\mathbb{Z}$ l'équation $\dot{2}x^2 + \dot{2}x = \dot{0}$.

Exercice 5 : Résoudre dans $\mathbb{Z}$ la congruence $3x \equiv 8 \; mod 14$.

Exercice 6 : Soit $(E, +, \times, ')$ une algèbre de Boole **quelconque**.

1. Déterminer les compléments dans E de
   (a) $b'c + cd$
   (b) $bc' + b'a + ac$
2. Montrer les égalités suivantes :
   (a) $a + a'b = a + b$
   (b) $a + a'b + a'b'c = a + b + c$
   (c) $(a + b + c')(a + b' + c)(a' + b + c) = a'b'c' + ab + ac + bc$

Solution :

Exercice 1 :

1. Le résidu de a modulo n est le reste dans la division euclidienne de a par n. C'est donc le plus petit entier positif qui soit congru à a modulo n.
2. Ecrivons la division euclidienne de 53 par 7 : $53 = 7 \times 7 + 4$.
   Le résidu de 53 modulo 7 est donc 4. On peut alors écrire que $53 \equiv 4\ (mod\ 7)$.

   D'après l'une des propriétés du cours on a donc $53^2 \equiv 4^2\ (mod\ 7)$.
   Or $4^2 = 16$ et $16 \equiv 2\ (mod\ 7)$. Ainsi $53^2 \equiv 2\ (mod\ 7)$ et le résidu de 53^2 modulo 7 est 2.

   $53^3 = 53^2 \times 53$ donc $53^3 \equiv 2 \times 4\ (mod\ 7)$. Or $2 \times 4 = 8$ et $8 \equiv 1\ (mod\ 7)$.
   Donc le résidu de 53^3 modulo 7 est égal à 1.
3. $53^5 = 53^2 \times 53^3$ donc $53^5 \equiv 2 \times 1\ (mod\ 7)$. Ainsi le résidu de 53^5 modulo 7 est égal à 2.

Exercice 2 :

1. Il existe des entiers q et r uniques tels que $n = 5q + r$, avec $0 \leqslant r < 5$. Le reste r peut donc prendre toutes valeurs entières de 0 à 4.
2.

r	n^2	n^3	n^4
0	0	0	0
1	1	1	1
2	4	3	1
3	4	2	1
4	1	4	1

Dans la colonne de n^2 on note le résidu de n^2 modulo 5. On procède de façon analogue pour les colonnes de n^3 et n^4.
Rappel : $n \equiv r\ (mod\ 5)$ donc $n^2 \equiv r^2\ (mod\ 5)$.
Enfin on utilise le fait que $n^3 = n^2 \times n$ et que $n^4 = (n^2)^2$, ou que $n^4 = n^3 \times n$.

3. On constate que le résidu de n^4 modulo 5 ne peut prendre que les valeurs 0 et 1.
   $n^4 \equiv 0\ (mod\ 5) \iff$ il existe un entier k tel que $n^4 = 5k$.
   Et $n^4 \equiv 1\ (mod\ 5) \iff$ il existe un entier k tel que $n^4 = 1 + 5k$.

Exercice 3 :

1. Dressons la table de multiplication dans $\mathbb{Z}/8\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \dot{7}\}$:

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{1}$	$\dot{4}$	$\dot{7}$	$\dot{2}$	$\dot{5}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{0}$	$\dot{4}$
$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{2}$	$\dot{7}$	$\dot{4}$	$\dot{1}$	$\dot{6}$	$\dot{3}$
$\dot{6}$	$\dot{0}$	$\dot{6}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{7}$	$\dot{0}$	$\dot{7}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

2. Les éléments inversibles sont $\dot{1}, \dot{3}, \dot{5}$ et $\dot{7}$.
   De plus $\dot{1}^{-1} = \dot{1}$, $\dot{3}^{-1} = \dot{3}$, $\dot{5}^{-1} = \dot{5}$ et $\dot{7}^{-1} = \dot{7}$ d'après la table ci-contre.
3. Les classes $\dot{0}, \dot{2}, \dot{4}$ et $\dot{6}$ sont les diviseurs de zéro car $\dot{0} \times \dot{1} = \dot{0}$, $\dot{2} \times \dot{4} = \dot{0}$, $\dot{4} \times \dot{2} = \dot{0}$ et $\dot{6} \times \dot{4} = \dot{0}$.
4. Dans la ligne de la table de multiplication correspondant à $\dot{5}$, on lit que l'équation $\dot{5}\dot{x} = \dot{7}$ possède comme unique solution $\dot{x} = \dot{3}$. Alors $\mathcal{S} = \{\dot{3}\}$.
   Dans la ligne de la table de multiplication correspondant à $\dot{4}$, on lit que l'équation $\dot{4}\dot{x} = \dot{4}$ possède comme solutions $\dot{1}, \dot{3}, \dot{5}$ et $\dot{7}$.
   Alors $\mathcal{S} = \{\dot{1}, \dot{3}, \dot{5}, \dot{7}\}$.

Exercice 4 :

1. Dressons la table de multiplication dans $\mathbb{Z}/_{4\mathbb{Z}} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$:

$\times$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

2. Dans la ligne de la table de multiplication correspondant à $\dot{2}$, on lit que l'équation $\dot{2}\dot{x} = \dot{2}$ possède comme solutions $\dot{1}$ et $\dot{3}$. Alors $\mathcal{S} = \{\dot{1}, \dot{3}\}$.

3. $\left\{\begin{array}{rcll} \dot{2}x + \dot{3}y & = & \dot{2} & L_1 \\ \dot{2}x + \dot{1}y & = & \dot{2} & L_2 \end{array}\right. \iff \left\{\begin{array}{rcll} \dot{2}x + \dot{3}y & = & \dot{2} & L_1 \\ \dot{2}y & = & \dot{0} & L_2 \leftarrow L_1 - L_2 \end{array}\right.$

   D'après la table de multiplication, l'équation $\dot{2}y = \dot{0}$ admet comme solutions $\dot{0}$ et $\dot{2}$.

   D'après L_1, $y = \dot{0} \iff \dot{2}x = \dot{2} \iff (x = \dot{1}$ ou $x = \dot{3})$ d'après la question 2.
   Et $y = \dot{2} \iff \dot{2}x + \dot{6} = \dot{2} \iff \dot{2}x + \dot{2} = \dot{2} \iff \dot{2}x = \dot{0} \iff (x = \dot{0}$ ou $x = \dot{2})$.

   Le système admet donc 4 couples solutions : $\mathcal{S} = \{(\dot{1}, \dot{0}), (\dot{3}, \dot{0}), (\dot{0}, \dot{2}), (\dot{2}, \dot{2})\}$.

4.

$\dot{x}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}x^2 + \dot{2}x$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$

   Alors $\mathcal{S} = \mathbb{Z}/_{4\mathbb{Z}} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$.

Exercice 5 : *Résoudre dans $\mathbb{Z}$ la congruence $3x \equiv 8\ mod 14$.*

$3x \equiv 8\ mod\ 14 \iff \dot{3}\dot{x} = \dot{8}$ dans $\mathbb{Z}/_{14\mathbb{Z}}$.
$\dot{3}$ est inversible car PGCD(3, 14)=1 ($14 = 1 \times 7$ et 3 est premier). Les éléments inversibles dans $\mathbb{Z}/_{14\mathbb{Z}}$ sont les classes $\dot{a}$ telles que a ne soit ni multiple de 2 ni de 7, puisqu'on doit avoir PGCD(a,14)=1. Le tableau suivant permet de chercher l'inverse de $\dot{3}$ parmi les éléments inversibles de $\mathbb{Z}/_{14\mathbb{Z}}$.

$\dot{x} \in (\mathbb{Z}/_{14\mathbb{Z}})^*$	$\dot{1}$	$\dot{3}$	$\dot{5}$
$\dot{3}\dot{x}$	$\dot{3}$	$\dot{9}$	$\dot{1}$

Alors $\dot{3}^{-1} = \dot{5}$.
Ainsi $\dot{3}\dot{x} = \dot{8} \iff \dot{x} = \dot{3}^{-1} \times \dot{8} \iff \dot{x} = \dot{5} \times \dot{8} = \dot{40} = \dot{12}$
$\iff \exists k \in \mathbb{Z}$ tel que $x = 12 + 14k$
Alors l'ensemble des solutions de la congruence $3x \equiv 8\ mod\ 14$ est
$\mathcal{S} = \{12 + 14k / k \in \mathbb{Z}\}$.

Exercice 6 :

1. Calculs des compléments en utilisant les lois de Morgan
   (a) $(b'c + cd)' = (b'c)'(cd)' = (b + c')(c' + d')$
   (b) $(bc' + b'a + ac)' = (bc')'(b'a)'(ac)' = (b' + c)(b + a')(a' + c')$
2. Egalités
   (a) $a + a'b = (a + a')(a + b) = 1 \times (a + b) = a + b$
   (b) $a + a'b + a'b'c = a + a'(b + b'c)$
   .. $= a + a'(b + c)$ d'après l'égalité (a)
   .. $= a + (b + c)$ en remplaçant b par $b + c$ dans l'égalité (a)
   .. $= a + b + c$

(c) $(a+b+c')(a+b'+c)(a'+b+c) = (a+(b+c')(b'+c))(a'+b+c)$ d'après la distributivité de + par rapport à $\times$
.. $= (a+bb'+bc+c'b'+c'c)(a'+b+c)$
.. $= (a+bc+c'b')(a'+b+c)$
.. $= aa'+bca'+a'c'b'+ab+bcb+c'b'b+ac+bcc+c'b'c$
.. $= a'b'c'+bca'+bc+ac+ab$
.. $= a'b'c'+ab+ac+bc$ car bca' est "absorbé" par bc

Deuxième méthode :
$(a+b+c')(a+b'+c)(a'+b+c) = (a+ab'+ac+bb'+bc+c'a+c'b'+c'c)(a'+b+c)$
.. $= (a+bc+c'b')(a'+b+c)$ car $a+ax = a\ \forall x$
.. $= aa'+ab+ac+bca'+bcb+bcc+c'b'a'+c'b'b+c'b'c$
.. $= a'b'c'+ab+ac+bc$