Université Paris 13, Institut Galilée
Département de Mathématiques
Licence 2ème année Informatique
2013-2014

Cours de Mathématiques pour l'Informatique
Des nombres aux structures
Sylviane R. Schwer

Leçon du 4 mars 2014 : Introduction aux structures algébriques : les ensembles quotients de $\mathbb{Z}$ par les congruences modulo n

Nous savons qu'une relation d'équivalence $\mathcal{R}$ sur un ensemble E partitionne E en classes d'équivalence appelé ensemble quotient de E par $\mathcal{R}$ et noté $E/\mathcal{R}$. Réciproquement, on peut montrer, cf TD, que toute partition sur un ensemble E définie une classe d'équivalence et donc un ensemble quotient. Mais tout ensemble quotient ne peut hériter des opérations de E.

1 petit glossaire sur les structures algébriques classiques en informatique et en mathématiques

1.1 $(E, \perp)$

magma [commutatif] : $\perp$ loi de composition interne [commutative].

demi-groupe [commutatif]: magma [commutatif] associatif.

monoïde [commutatif] : semi-groupe [commutatif] possédant un élément neutre.

groupe [commutatif] : monoïde [commutatif] dont tout élément possède un inverse.

1.2 $(E, +, \times)$

$(E, +, \times, 0)$ **est un demi-anneau [commutatif] :** si

- $(E, +, 0)$ est un monoïde commutatif,
- $(E, \times)$ est un demi-groupe,
- $\times$ est distributif par rapport à $+$,
- 0 est absorbant pour le produit.

$(E, +, \times, 0, 1)$ **est un demi-anneau unitaire [commutatif] :** si

- $(E, +, 0)$ est un monoïde commutatif,
- $(E, \times)$ est un monoïde [commutatif],
- $\times$ est distributif par rapport à $+$,
- 0 est absorbant pour le produit.

$(E, +, \times, 0)$ **est un anneau [commutatif] :** si

- $(E, +, 0)$ est un groupe commutatif, Le symétrique de l'élément a est noté $-a$.
- $(E, \times)$ est un demi-groupe,
- $\times$ est distributif par rapport à $+$,

Contrairement aux semi-anneaux, le fait que 0 soit absorbant se déduit de l'existence d'un opposé et des autres axiomes :
$0 =$ [définition de l'opposé de $0 \times a$, $\forall a \in E$] $0 \times a - 0 \times a =$[0 est élément neutre] $(0+0)\times a+(-0\times a) =$[distributivité de $\times$ sur $+$ et associativité de $+$] $0\times a+0\times a-0\times a = 0 \times a$.

Même preuve pour l'absorption à droite.

$(E, +, \times, 0, 1)$ **est un anneau unitaire [commutatif] :** si

- $(E, +, 0)$ est un groupe commutatif,
- $(E, \times, 1)$ est un monoïde [commutatif],
- $\times$ est distributif par rapport à $+$.

Puisque l'anneau est unitaire, la preuve du 0 absorbant peut être simplifiée
Même preuve pour l'absorption à droite.

$(E, +, \times, 0, 1)$ **est un corps [commutatif] :** si

- $(E, +, 0)$ est un groupe commutatif,
- $(E_* = E - \{0\}, \times, 1)$ est un groupe [commutatif],
- $\times$ est distributif par rapport à $+$.

2 Congruence sur une structure algébrique

Définition 2.1 *Soit E un ensemble muni de plusieurs opérations $f_1, \cdots, f_n$. Une congruence $\mathcal{C}$ sur E est une relation d'équivalence compatible avec chacune des opérations f_i, c'est-à-dire que si f_i est d'arité k,*

$$\forall i, j \in \mathbb{N}, 1 \leq i, j \leq k, \quad [x_j \equiv y_j \quad (\mathcal{C})] \Longrightarrow [f_i(x_1, \cdots, x_k) \equiv f_i(y_1, \cdots, y_k) \quad (\mathcal{C})]$$

La compatibilité de la relation avec les opérations $f_1, \cdots, f_n$ de E permet de définir sur $E/\mathcal{R}$ les opérations $[f_1]_\mathcal{C}, \cdots, [f_n]_\mathcal{C}$ en posant $k_i =$ l'arité de f_i :

$$\forall i, 1 \leq i \leq k_i, \quad [f_i]_\mathcal{C}([x_1]_\mathcal{C}, \cdots, [x_{k_i}]_\mathcal{C}) = [f_i(x_1, \cdots, x_{k_i})]_\mathcal{C}$$

Certaines propriétés des f_i vont se transmettre à $[f_i]_\mathcal{C}$ et d'autres non. Nous allons examiner plus précisément cela sur la structure d'anneau commutatif $(\mathbb{Z}, +, \times, 0, 1)$ et les relations de congruence modulo n.

Rappelons que les relations définies dans $\mathbb{Z}$ par $a \equiv_n b \Longleftrightarrow a - b \in n\mathbb{Z}$, $\forall n \in \mathbb{N}$ sont des relations d'équivalence qui satisfont la

Proposition 2.1 *Soit $n \in \mathbb{N}, n > 1$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv_n b$ et $c \equiv_n d$, alors*

1. *compatibilité avec l'addition $a + c \equiv_n b + d$*
2. *compatibilité avec la soustraction $a - c \equiv_n b - d$*
3. *compatibilité avec la multiplication $a.c \equiv_n b.d$*
4. *stabilité additive des classes $k + a \equiv_n k + b$, $\forall k \in \mathbb{Z}$*
5. *stabilité multiplicative des classes $ka \equiv_n kb$, $\forall k \in \mathbb{Z}$*
6. *stabilité par élévation à une puissance $k \in \mathbb{N}*$ des classes : $a^k \equiv_n b^k$.*

Attention, l'exponentiation n'est pas stable : $a^c \not\equiv_n b^d$. Par exemple $2^1 \not\equiv_3 2^4$.

Dans $\mathbb{Z}$, relativement aux congruences modulo n, un vocabulaire spécifique est utilisé pour les représentants.

Définition 2.2 *Tout ensemble de n représentants de la congruence modulo n est appelé* ensemble complet de résidus modulo n.

Nous appellerons résidus euclidiens modulo n, l'ensemble $\{0, 1, \cdots, n-1\}$

Une autre famille intéressante, pour n impair est $\{-\frac{n-1}{2}, \cdots, -1, 0, 1, \cdots, \frac{n-1}{2}\}$.

Par exemple, modulo 7, les deux ensembles complets de résidus les plus utilisés sont $\{0, 1, 2, 3, 4, 5, 6\}$ et $\{-3, -2, -1, 0, 1, 2, 3\}$. Modulo 6, on peut trouver $\{0, 1, 2, 3, 4, 5\}$ et $\{-3, -2, -1, 0, 1, 2\}$ ou $\{-2, -1, 0, 1, 2, 3\}$.

3 Structure de $\mathbb{Z}/n\mathbb{Z}$ héritée de $(\mathbb{Z}, +, .)$, $n > 2$

Pour alléger l'écriture, n étant fixé, on note $\dot{x}$ la classe $[x]_{\equiv_n}$.

Soit $n \in \mathbb{N}, n > 1$. on note $\mathbb{Z}/n\mathbb{Z}$ et l'on choisit comme système complet de résidus les résidus euclidiens, soit $\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \cdots, \overbrace{n-1}^{\cdot}\}$.

Exemple : $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$ avec $\dot{0}$ l'ensemble des nombres pairs, $\dot{1}$ l'ensemble des nombres impairs.

3.1 Définitions des opérations sur $\mathbb{Z}/n\mathbb{Z}$ et propriétés héritées

3.1.1 Addition

L'application $\dot{+} \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (\dot{a}, \dot{b}) & \longmapsto & \dot{a}\dot{+}\dot{b} = \overbrace{a+b}^{\cdot} \end{array} \right.$
définit une opération interne sur $\mathbb{Z}/n\mathbb{Z}$ qui est

• commutative : $\dot{a}\dot{+}\dot{b} = (Def) = \overbrace{a+b}^{\cdot}$ =commutativité dans $\mathbb{Z} = \overbrace{b+a}^{\cdot} = (Def) = \dot{b}\dot{+}\dot{a}$

• associative : $(\dot{a}\dot{+}\dot{b})\dot{+}\dot{c} = (Def) = \overbrace{a+b}^{\cdot}\dot{+}\dot{c} = (Def) = \overbrace{(a+b)+c}^{\cdot}$=(associativité dans $\mathbb{Z}) = \overbrace{a+(b+c)}^{\cdot} = (Def) = \dot{a}\dot{+}\overbrace{b+c}^{\cdot} = (Def) = \dot{a}\dot{+}(\dot{b}\dot{+}\dot{c})$

• possède comme élément neutre $\dot{0}$: $\dot{a}\dot{+}\dot{0} = (Def) = \overbrace{a+0}^{\cdot} =$ (0 élément neutre de l'addition dans $\mathbb{Z}) = \dot{a}$.

• tout élément $\dot{a}$ possède un opposé $\overbrace{n-a}^{\cdot}$ pour l'addition : $\dot{a}\dot{+}\overbrace{n-a}^{\cdot} = (Def) = \dot{n} = \dot{0}$

Proposition 3.1 *$\forall n > 1$, $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{0})$ est un groupe commutatif additif (ou abélien).*

Table 1: table d'addition de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$

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

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$

$\dot{+}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{0}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{1}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$
$\dot{2}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$
$\dot{3}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{4}$	$\dot{4}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{5}$	$\dot{5}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$

3.1.2 Multiplication

L'application $\dot{\times} \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (\dot{a}, \dot{b}) & \longmapsto & \dot{a}\dot{\times}\dot{b} = \overbrace{a \times b}^{\cdot} \end{array} \right.$
définit une opération interne sur $\mathbb{Z}/n\mathbb{Z}$ qui est

• commutative : $\dot{a}\dot{\times}\dot{b} = (Def) = \dot{\overbrace{a \times b}}$ =commutativité dans $\mathbb{Z} = \dot{\overbrace{b \times a}} = (Def) = \dot{b}\dot{\times}\dot{a}$

• associative : $(\dot{a}\dot{\times}\dot{b})\dot{\times}\dot{c} = (Def) = \dot{\overbrace{a \times b}}\dot{\times}\dot{c} = (Def) = \dot{\overbrace{(a \times b) \times c}}$=associativité dans $\mathbb{Z} = \dot{\overbrace{a \times (b \times c)}} = Def = \dot{a}\dot{\times}\dot{\overbrace{b \times c}} = (Def) = \dot{a}\dot{\times}(\dot{b}\dot{\times}\dot{c})$

• possède comme élément neutre $\dot{1}$: $\dot{a}\dot{\times}\dot{1} = Def = \dot{\overbrace{a \times 1}} =$ (1 élément neutre de la multiplication dans $\mathbb{Z}$) $= \dot{a}$.

• possède comme élément absorbant $\dot{0}$: $\dot{a}\dot{\times}\dot{0} = Def = \dot{\overbrace{a \times 0}}$ =(0 élément absorbant de la multiplication dans $\mathbb{Z}$) $= \dot{0}$.

• distributive par rapport à l'addition : $(\dot{a}\dot{+}\dot{b})\dot{\times}\dot{c} = Def\dot{+} = \dot{\overbrace{a+b}}\dot{\times}\dot{c} = Def\dot{\times} = \dot{\overbrace{(a+b)\times c)}}$=(distributivité dans $\mathbb{Z}$) $= \dot{\overbrace{(a \times c) + (b \times c)}} = Def\dot{+} = \dot{\overbrace{a \times c}}\dot{+}\dot{\overbrace{b \times c}} = Def\dot{\times} = \dot{a}\dot{\times}\dot{b}\dot{+}\dot{b}\dot{\times}\dot{c}$

Proposition 3.2 $\forall n > 1$, $(\mathbb{Z}/n\mathbb{Z}, \dot{\times}, \dot{1})$ *est un monoïde commutatif multiplicatif.*

Proposition 3.3 $\forall n > 1$, $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}, \dot{0}, \dot{1})$ *est un anneau commutatif.*

Table 2: table de multiplication de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$

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

$\dot{\times}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{1}$	$\dot{3}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{1}$	$\dot{4}$	$\dot{2}$
$\dot{4}$	$\dot{0}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

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

Dans $\mathbb{Z}$, seuls $+1$ et -1 sont inversibles, se sont leurs propres inverses. Tous les nombres entiers non nuls sont réguliers pour la multiplication. L'observation des tables de multiplication données Table 2, montre que $\mathbb{Z}/n\mathbb{Z}$ possèdent des propriétés différentes selon n. Dans chaque cas, on retrouve bien le fait que $\dot{1}$ et $\dot{\overbrace{-1}} = \dot{\overbrace{n-1}}$ sont leurs propres inverses - héritage de $\mathbb{Z}$. en revanche, dans $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ on trouve des éléments non nuls diviseurs de $\dot{0}$. Dans $\mathbb{Z}/6\mathbb{Z}$, on trouve des éléments autres que $\dot{1}$ et $\dot{\overbrace{-1}}$ qui sont inversibles. Dans $\mathbb{Z}/5\mathbb{Z}$, tous les éléments non nuls sont inversibles.

3.2 Eléments inversibles et diviseurs de $\dot{0}$

Proposition 3.4 *Dans* $\mathbb{Z}/n\mathbb{Z}$*, soit* $a \in \mathbb{N}$*,*
$\dot{a}$ *est inversible si et seulement si* $a \wedge n = 1$*,*
$\dot{a}$ *est un diviseur de zéro si et seulement si* $a \wedge n \neq 1$*.*

Soit $a \in \mathbb{Z}$, $\dot{a}$ est inversible si et seulement si il existe $\dot{b}$ tel que $a\dot{\times}b = \dot{1}$, c'est-à-dire si et seulement si $a.b \equiv_n 1$, ce qui est équivalent à $\exists k \in \mathbb{Z}$ tel que $ab - 1 = kn$ ou $ab - kn = 1$. Daprès l'égalité de Bezout, on a $a \wedge n = 1$, la réciproque est évidente.
Si $a \wedge n \neq 1$, $\exists\ \delta, \alpha, \nu \in \mathbb{N}_*$ tels que $n = \delta\nu$ et $a = \delta\alpha$. $a\nu = \alpha\delta\nu = \alpha n$ donc $\dot{a}\dot{\nu} = \dot{0}$.
Si $0 < a, b < n$, tels que $\dot{a}\dot{\nu} = \dot{0}$, alors n divise $a.b$. Or n ne peut diviser b, donc il existe un diviseur $\delta > 1$ commun à n et a. □

Corollaire 3.1 $p \in \mathbb{P} \Longleftrightarrow (\mathbb{Z}/p\mathbb{Z}, \dot{+}, \dot{\times}, \dot{0}, \dot{1})$ *est un corps commutatif.*

Définition 3.1 $(\mathbb{Z}/n\mathbb{Z})^* = \{\dot{a} \in \mathbb{Z}/n\mathbb{Z}, a \wedge n = 1\}$.

- $(\mathbb{Z}/4\mathbb{Z})^* = \{\dot{1}, \dot{3}\}$
- $(\mathbb{Z}/5\mathbb{Z})^* = \{\dot{1}, \dot{2}, \dot{3}, \dot{4}\}$
- $(\mathbb{Z}/6\mathbb{Z})^* = \{\dot{1}, \dot{5}\}$
- $(\mathbb{Z}/12\mathbb{Z})^* = \{\dot{1}, \dot{5}, \dot{7}, \dot{11}\}$
- $(\mathbb{Z}/2\mathbb{Z})^* = \{\dot{1}\}$
- Si $n \geq 3$ et $\{\dot{1}, \dot{-1}\} \subseteq (\mathbb{Z}/2\mathbb{Z})^*$

Théorème 3.5 $(\mathbb{Z}/n\mathbb{Z})^*, \dot{*}, \dot{1})$ *est un groupe multiplicatif et l'on a*

$$(\dot{a}\dot{b})^{-1} = \dot{b}^{-1}\dot{a}^{-1}$$

Il suffit de montrer la stabilité par inversion qui repose sur $(\dot{a}^{-1})^{-1} = \dot{a}$. De plus, $(\dot{b}^{-1}\dot{a}^{-1})(\dot{a}\dot{b}) = [\dot{b}^{-1}(\dot{a}^{-1}\dot{a})\dot{b}] = \dot{1}$. □

D'après leur table de multiplication, $\varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2$. Plus généralement,

Définition 3.2 *On appelle indicateur d'Euler de n le cardinal de* $(\mathbb{Z}/n\mathbb{Z})^*$ *que l'on note* $\varphi(n)$.

$$Si \quad n \in \mathbb{P}, \quad \varphi(n) = n - 1.$$

Le cas où n est composé sera examiné plus tard. Cela ne nous empêche pas de prouver le

Théorème 3.6 (d'Euler)

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^* \quad a^{\varphi(n)} = \dot{1}$$

Preuve directe (sans passer par la théorie des groupes que l'on ne connait pas) : $a \in (\mathbb{Z}/n\mathbb{Z})^*$ est un élément inversible donc régulier de $\mathbb{Z}/n\mathbb{Z}$, donc
$\forall b, c \in (\mathbb{Z}/n\mathbb{Z})^*, a \times b = a \times c \Longleftrightarrow b = c$, ce qui signifie que l'application

$$f \left| \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ x & \longmapsto & a.x \end{array} \right.$$

est une injection dans un ensemble fini, donc une bijection. Comme $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe multiplicatif commutatif, soit $\{\alpha_1, \cdots, \alpha_{\varphi(n)}\} = (\mathbb{Z}/n\mathbb{Z})^*$,

$$\Pi_{i=1}^{\varphi(n)}\alpha_i = f(\Pi_{i=1}^{\varphi(n)}\alpha_i) = a^{\varphi(n)}\Pi_{i=1}^{\varphi(n)}\alpha_i.$$

En simplifiant par $\Pi_{i=1}^{\varphi(n)}\alpha_i$, on obtient le résultat. □

Interpréter dans $\mathbb{Z}$, le théorème d'Euler dit

Théorème 3.7 (de Fermat (le petit))

$$(p \in \mathbb{P}) \quad et \quad (a \wedge p = 1) \Longrightarrow (a^{p-1} \equiv_p 1)$$

Il a pour corollaire immédiat :

Corollaire 3.2

$$(p \in \mathbb{P}) \quad et \quad (a \in \mathbb{Z}) \Longrightarrow (a^p \equiv_p a)$$

Si $(a \wedge p = 1)$, l'égalité découle du petit théorème de Fermat. Sinon, $p|a$ donc $a \equiv_p 0$, et la stabilité par puissance p permet de conclure.

Nous allons donner une preuve du théorème de Wilson directe. Dans $(\mathbb{Z}/p\mathbb{Z})^*$ avec p premier, $\Pi_{i=1}^{p-1} \dot{i} = [(p-1)!]$.

Pour $p > 2$, chaque $\dot{i} \neq \dot{1}$ et $\overbrace{p-1}^{\cdot}$ possède un inverse différent de lui. En effet, $x^2 = \dot{1} \Longleftrightarrow (x - \dot{1})(x + \dot{1}) = \dot{0}$ dans un corps. Or $\overbrace{p-1}^{\cdot} = -\dot{1}$. Donc en simplifiant on obtient $-\dot{1} = [(p-1)!]$. D'où, en vérifiant directement pour $p = 2$

Théorème 3.8 (de Wilson)

$$p \in \mathbb{P} \Longrightarrow (p-1)! \equiv_p -1$$

3.3 Eléments symétriques dans $\mathbb{Z}/n\mathbb{Z}$, élévation à la puissance dans $\mathbb{Z}/n\mathbb{Z}$

3.3.1 éléments symétriques pour l'addition

L'inversion additive, qui associe à toute classe la classe opposée est compatible avec l'addition : $-\dot{a} = \overbrace{-a}^{\cdot}$, c'est donc une opération (unaire) de $\mathbb{Z}/n\mathbb{Z}$.

3.3.2 éléments symétriques pour la multiplication

L'inversion multiplicative n'est pas une opération de $\mathbb{Z}/n\mathbb{Z}$ car $(\dot{a})^{-1} \neq \overbrace{a-1}^{\cdot}$, c'est une simple fonction partielle de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, qui devient bijective dans $(\mathbb{Z}/n\mathbb{Z})^*$.

3.3.3 La fonction puissance n'est pas une opération définie dans $\mathbb{Z}/n\mathbb{Z}$.

Dans $\mathbb{Z}/n\mathbb{Z}$, que doit signifier $\dot{a}^{\dot{b}}$?

Positivité ou négativité n'a pas de signification pour les classes modulo n car elles sont stables par la fonction "opposé". Mais même en se restreignant aux éléments positifs de la classe, montrons que $\dot{a}^{\dot{b}} \neq \overbrace{a^b}^{\cdot}$. Prenons $n = 3$, $1 \equiv_3 4$, donc $\dot{1} = \dot{4}$. Or $2^1 \equiv_3 2$ et $2^4 \equiv_3 1$ donc le choix du représentant de l'exponentiel influe sur le résultat, ce qui n'est pas acceptable.

Il n'est donc pas possible de définir une opération d'exponentiation dans $\mathbb{Z}/n\mathbb{Z}$ comme x^y – dans laquelle x et y sont de même nature - dans $\mathbb{Z}/n\mathbb{Z}$. On a pu le faire dans $\mathbb{Z}$ en restreignant le second argument à $\mathbb{N}$ en considérant $\mathbb{N}$ comme inclus dans $\mathbb{Z}$.

En revanche, pour $n \in \mathbb{N}$ et $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$, l'expression $\dot{a}^n$ est parfaitement définie et vaut $\Pi_{k=1}^{n} \dot{a}$, mais $\mathbb{N}$ n'est pas ici un sous-ensemble de $\mathbb{Z}/n\mathbb{Z}$.

On parlera alors de puissance dans ce dernier cas, et d'exponentiation dans le premier cas. La puissance n d'un élément, c'est le produit de n occurrences de cet élément.

4 Etude des équations linéaires $ax = b$ in $\mathbb{Z}/n\mathbb{Z}$

Rappelons que l'on peut interpréter le théorème des restes chinois établit une bijection entre $\mathbb{Z}/n.m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si $n \wedge m = 1$, ce qui peut permettre de réduire la taille des ensembles dans lesquels on travaille.

4.1 cas $a \in (\mathbb{Z}/n\mathbb{Z})^*$

a possède un inverse $a^{-1} \in \mathbb{Z}/n\mathbb{Z}$. Il existe alors une unique solution : $\mathcal{S} = \{a^{-1}.b\}$.
Exemple $\dot{5}x = \dot{2}$ dans $\mathbb{Z}/6Z$, $\mathcal{S} = \{\dot{4}\}$ d'après le tableau 2.

4.2 cas a est un diviseur de zéro

Soit $\alpha, \beta \in \mathbb{N}$ les résidus euclidiens respectifs de a et b, c'est-à-dire $\dot{\alpha} = a$ et $\dot{\beta} = b$, soit $\delta = \alpha \wedge n$.

β n'est pas un multiple de δ alors il n'y a aucune solution : $\mathcal{S} = \emptyset$.

β est un multiple de δ alors il n'y a exactement $\delta = n \wedge \alpha$ solutions.

En effet, $ax = b \iff \alpha.x \equiv_n \beta \iff \frac{\alpha}{\delta}x \equiv_{\frac{n}{\delta}} \frac{\beta}{\delta}$ avec $\frac{\alpha}{\delta} \wedge \frac{n}{\delta} = 1$. Donc $\frac{\dot{\alpha}}{\delta}x = \frac{\dot{\beta}}{\delta}$ admet une solution unique dans $\mathbb{Z}/\frac{n}{\delta}\mathbb{Z}$, ce qui fait δ solution dans $\mathbb{Z}/n\mathbb{Z}$.
Exemple $\dot{2}x = \dot{4}$ dans $\mathbb{Z}/6Z$, $2 \wedge 6 = 2$, $\mathcal{S} = \{\dot{2}, \dot{5}\}$ d'après le tableau 2.

En particulierSi $a = \dot{0}$ et $b = \dot{0}$ alors il y a exactement n solutions : $\mathcal{S} = \mathbb{Z}/n\mathbb{Z}$.