4.2 Congruences et division euclidienne dans $\mathbb{Z}$

Voici une très belle théorie, due en très grande partie à K.F. GAUSS.
Cette théorie propose une méthode d'étude des nombres, à partir des restes de la division euclidienne. Elle est apparue dans un livre publié en latin, au XIX ˚ siècle, sous le titre :≪ ***Disquitionnae arithmeticae*** *≫* ***(Recherches arithmétiques)****.En fait, la méthode est apparue pour résoudre un autre problème, appelé* ***Théorème de FERMAT****. Ce problème a été résolu en 1989.*

4.2.1 Notion de multiple

1. Soit $n \in \mathbb{Z}$; on appelle multiple de n, un nombre $m \in \mathbb{Z}$ tel qu'il existe $k \in \mathbb{Z}$ tel que $m = kn$
2. L'ensemble des multiples de n est l'ensemble $n\mathbb{Z}$ où :

$$n\mathbb{Z} = \{m \in \mathbb{Z} \text{ tels qu'il existe } k \in \mathbb{Z} \text{ tel que } m = n \times k\}$$

Remarque 10 :

1. Nous reviendrons sur cette notion en 5.1.1 en étudiant la divisibilité dans $\mathbb{Z}$
2. Exemples d'ensembles de multiples :
   - $0\mathbb{Z} = \{0\}$ et $1 \times \mathbb{Z} = \mathbb{Z}$
   - $2\mathbb{Z}$ est l'ensemble des nombres pairs (l'ensemble des multiples de 2)
   - Les nombres impairs sont donc $\mathbb{Z} \setminus 2\mathbb{Z}$; l'ensemble des nombres impairs, est aussi $2\mathbb{Z}+1$, c'est à dire
   $$2\mathbb{Z}+1 = \{m \in \mathbb{Z} \text{ tels qu'il existe } k \in \mathbb{Z} \text{ tel que } m = 2 \times k + 1\}$$
3. Soit $n \in \mathbb{N}$; alors, nous avons $(-n)\,\mathbb{Z} = n\mathbb{Z}$. Il est donc inutile d'étudier les ensembles de multiples, dans $\mathbb{Z}$ d'entiers strictement négatifs.
4. Pour $n \in \mathbb{N}$ et $p \in \mathbb{Z}$, on peut généraliser les ensembles $n\mathbb{Z}+p$ par :
$$n\mathbb{Z}+p = \{m \in \mathbb{Z} \text{ tels qu'il existe } k \in \mathbb{Z} \text{ tel que } m = n \times k + p\}$$

4.2.2 Théorème

Soit $n \in \mathbb{N}$. L'ensemble $n\mathbb{Z}$ des multiples de n est un anneau commutatif

Démonstration

1. Il est facile de démontrer que $(n\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Z}, +)$
   → D'une part, $n\mathbb{Z} \neq \emptyset$ puisque $0 \in n\mathbb{Z}$
   → D'autre part, pour tout $x \in n\mathbb{Z}$ et tout $y \in n\mathbb{Z}$, nous avons $x - y = kn - k'n = n\,(k - k') \in n\mathbb{Z}$
   Donc $(n\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Z}, +)$
2. De plus, pour tout $x \in n\mathbb{Z}$ et tout $y \in n\mathbb{Z}$, nous avons $x \times y = kn \times k'n = n\,(kk'n) \in n\mathbb{Z}$

Remarque 11 :

1. On remarquera de plus que, si $x \in \mathbb{Z}$ et $y \in n\mathbb{Z}$, alors $xy \in n\mathbb{Z}$, puisque $xy = x\,(nk) = n\,(xk)$. $n\mathbb{Z}$ est donc aussi un idéal de $\mathbb{Z}$
2. $n\mathbb{Z}$ n'est pas un anneau unitaire puisque $1 \notin n\mathbb{Z}$

4.2.3 Définition de la relation de congruence

1. Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$
   Dans $\mathbb{Z}$, on dit que ≪ x **est congru à** y **modulo** n ≫ et on écrit $x \equiv y\,[n]$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $x - y = kn \iff x - y \in n\mathbb{Z}$
2. La relation de congruence est une relation d'équivalence

Démonstration

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$

1. **La relation de congruence est évidemment réflexive**
   Soit $x \in \mathbb{Z}$
   Alors $x - x = 0 = 0 \times n$ et donc $x \equiv x\,[n]$
2. **La relation de congruence est symétrique**
   Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$
   Supposons $x \equiv y\,[n]$.
   Alors il existe $k \in \mathbb{Z}$ tel que $x - y = k \times n$ et donc $y - x = (-k) \times n$, c'est à dire $y \equiv x\,[n]$
   Donc, si $x \equiv y\,[n]$, alors $y \equiv x\,[n]$
3. **La relation de congruence est transitive**
   Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ et $z \in \mathbb{Z}$
   Supposons $x \equiv y\,[n]$ et $y \equiv z\,[n]$.
   Alors, il existe $k \in \mathbb{Z}$ tel que $x - y = kn$ et $k_1 \in \mathbb{Z}$ tel que $y - z = k_1 n$. En additionnant, nous obtenons :
   $$(x - y) + (y - z) = kn + k_1 n \iff x - z = (k + k_1)\, n \iff x \equiv z\,[n]$$
   Ainsi, si $x \equiv y\,[n]$ et $y \equiv z\,[n]$, alors $x \equiv z\,[n]$

Exemple 1 :

1. $13 \equiv 8\ [5]$ car, $13 - 8 = 1 \times 5$
2. $115 \equiv 11\ [13]$ car, $115 - 11 = 104 = 8 \times 13$
3. $967 \equiv 16420\ [17]$ car $967 - 16420 = -(909) \times 17$

Exercice 1 :

Montrer que $3 \times 2^{11} \equiv 2^{12}\ [2^8]$

4.2.4 Propriétés

La relation de congruence est compatible avec l'addition et la multiplication, c'est à dire que si $x \equiv y\,[n]$ et $z \equiv t\,[n]$, alors :
$$x + z \equiv y + t\,[n] \text{ et } xz \equiv yt\,[n]$$
D'autre part, si $x \equiv y\,[n]$, alors, pour tout $p \in \mathbb{N}$, $x^p \equiv y^p\,[n]$

Démonstration

Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $z \in \mathbb{Z}$ et $t \in \mathbb{Z}$ tels que $x \equiv y\,[n]$ et $z \equiv t\,[n]$.
Nous avons alors $x - y = kn$ et $z - t = k_1 n$ avec $k \in \mathbb{Z}$ et $k_1 \in \mathbb{Z}$.

⇒ **Montrons que nous avons** $x + z \equiv y + t\,[n]$
En additionnant, nous obtenons :
$$(x - y) + (z - t) = (k + k_1)\, n \iff (x + z) - (y + t) = (k + k_1)\, n$$
C'est à dire que nous avons $x + z \equiv y + t\,[n]$

⇒ **Montrons que nous avons** $xz \equiv yt\,[n]$

▷ Supposons $x \equiv y\,[n]$ et montrons que, pour tout $z \in \mathbb{Z}$, alors $xz \equiv yz\,[n]$
Si $x \equiv y\,[n]$, alors $x - y = kn$ avec $k \in \mathbb{Z}$ et, en multipliant par $z \in \mathbb{Z}$, nous obtenons :
$$z\,(x - y) = zkn \iff zx - zy = (zk)\, n \iff xz \equiv yz\,[n]$$

▷ Supposons, maintenant $x \equiv y\,[n]$ et $z \equiv t\,[n]$. Alors $xz \equiv yz\,[n]$ et $zy \equiv ty\,[n]$, et donc, par transitivité, $xz \equiv yt\,[n]$

⇒ Si $x \equiv y\,[n]$, en itérant les résultats ci-dessus, nous avons $x \times x \equiv y \times y\,[n] \iff x^2 \equiv y^2\,[n]$, et, en itérant, pour $p \in \mathbb{N}$, nous obtenons $x^p \equiv y^p\,[n]$

Remarque 12 :

1. **Classes d'équivalence dans la relation de congruence**
   ▷ La classe d'équivalence de $x \in \mathbb{Z}$, dans la relation de congruence modulo n, est l'ensemble des éléments de $\mathbb{Z}$ qui sont en relation avec x, ou congrus à x modulo n
   Soit donc $x \in \mathbb{Z}$, on cherche

$$\dot{x} = \{y \in \mathbb{Z} \text{ tels que } x \equiv y\,[n]\} = \{y \in \mathbb{Z} \text{ tels que } y = x + kn \text{ où } k \in \mathbb{Z}\} = x + n\mathbb{Z}$$

   ▷ **Par exemple**, dans la relation de congruence modulo 4,

$$\dot{3} = \{\ldots, -5, -1, +3, +7, +11, \ldots\} = 3 + 4\mathbb{Z}$$

2. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence modulo n
3. Soient $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$.
   Nous nous posons la question de savoir s'il est possible de faire des opérations sur les classes d'équivalence, un peu comme dans $\mathbb{Z}$
   Il faudrait pouvoir définir :$\dot{x} + \dot{y}$ et $\dot{x} \times \dot{y}$; c'est ce qui est fait dans la proposition suivante. Il y a cependant de nombreux problèmes que l'on peut se poser, en particulier celui de savoir si le résultat des opérations dépend des représentants choisis.

4.2.5 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

1. Définition de l'addition et de la multiplication dans $\mathbb{Z}/n\mathbb{Z}$
   Pour $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{y} \in \mathbb{Z}/n\mathbb{Z}$
   ▷ **On définit l'addition par :** $\dot{x} + \dot{y} = \overbrace{x + y}^{\cdot}$
   ▷ **On définit la multiplication par :** $\dot{x} \times \dot{y} = \overbrace{xy}^{\cdot}$
   Ces opérations sont indépendantes des représentants choisis
2. Muni de ces 2 opérations, $\mathbb{Z}/n\mathbb{Z}$, est un anneau commutatif.

Démonstration

1. **Le résultat de ces opérations est indépendant des représentants choisis ;**
   ▷ Addition
   En effet, si $x \equiv y\,[n]$ et si $a \equiv b\,[n]$, alors, $\dot{x} = \dot{y}$ et $\dot{a} = \dot{b}$
   Etudions $\overbrace{a + x}^{\cdot}$ et $\overbrace{y + b}^{\cdot}$.
   Par définition, $\overbrace{x + a}^{\cdot} = \dot{x} + \dot{a}$ et $\overbrace{y + b}^{\cdot} = \dot{y} + \dot{b}$.
   Comme, la relation de congruence est compatible avec l'addition, nous avons $x + a \equiv y + b\,[n]$, c'est à dire $\overbrace{x + a}^{\cdot} = \overbrace{y + b}^{\cdot}$
   Pour conclure, nous avons donc : $\dot{x} + \dot{a} = \overbrace{x + a}^{\cdot} = \overbrace{y + b}^{\cdot}) = \dot{y} + \dot{b}$
   Le résultat de l'opération est donc indépendant des représentants choisis.
   ▷ La démonstration est la même pour la multiplication *(à faire !)*
2. **Muni de ces 2 opérations, $\mathbb{Z}/n\mathbb{Z}$, est un anneau commutatif.**
   La démonstration est très simple
   ⇒ Tout d'abord, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif
   ▷ L'addition est commutative, puisque, pour tout $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{y} \in \mathbb{Z}/n\mathbb{Z}$:

$$\dot{x} + \dot{y} = \overbrace{x + y}^{\cdot} = \overbrace{y + x}^{\cdot} = \dot{y} + \dot{x}$$

▷ Sans coup férir, l'addition est associative, puisque, pour tout $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$, $\dot{y} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{z} \in \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned}\dot{x} + (\dot{y} + \dot{z}) = &\quad \dot{x} + \left(\dot{\overbrace{y + z}}\right) = \dot{\overbrace{x + y + z}} \\ = &\quad \dot{\overbrace{(x + y) + z}} = \dot{\overbrace{x + y}} + \dot{z} \\ = &\quad (\dot{x} + \dot{y}) + \dot{z} = \dot{x} + \dot{y} + \dot{z}\end{aligned}$$

▷ Le neutre pour l'addition est évidemment $\dot{0}$

▷ Et le symétrique de $\dot{x}$ est donc $\dot{\overbrace{(-x)}}$

⇒ La multiplication est commutative, distributive par rapport à l'addition et possède un neutre

▷ La multiplication est commutative, puisque, pour tout $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{y} \in \mathbb{Z}/n\mathbb{Z}$:

$$\dot{x} \times \dot{y} = \dot{\overbrace{x \times y}} = \dot{\overbrace{y \times x}} = \dot{y} \times \dot{x}$$

▷ Sans difficulté, la multiplication est associative.

▷ Le neutre pour la multiplication est évidemment $\dot{1}$

▷ Et la multiplication est distributive par rapport à l'addition.
En effet, pour tout $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$, $\dot{y} \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{z} \in \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned}\dot{x} \times (\dot{y} + \dot{z}) = &\quad \dot{x} \times \left(\dot{\overbrace{y + z}}\right) = \dot{\overbrace{x\,(y + z)}} \\ = &\quad \dot{\overbrace{xy + xz}} = \dot{\overbrace{xy}} + \dot{\overbrace{xz}} = \dot{x}\dot{y} + \dot{x}\dot{z}\end{aligned}$$

Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est bien un anneau commutatif

Remarque 13 :

On peut construire une application « projection »

$$\left\{\begin{array}{ccc} p : \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longrightarrow & p\,(x) = \dot{x} \end{array}\right.$$

D'après 4.2.5, cette projection est telle que : $p\,(x + y) = p\,(x) + p\,(y)$ et $p\,(xy) = p\,(x)\,p\,(y)$
p est un morphisme d'anneau

4.2.6 Division euclidienne dans $\mathbb{Z}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, c'est à dire $b \neq 0$
Alors, il existe un unique couple d'entiers relatifs (q, r) tels que

$$a = bq + r \text{ et } 0 \leqslant r < |b|$$

q est le quotient et r le reste

Démonstration

1. Rappelons la propriété d'Archimède vue en 2.5.1 :
Pour tout $a \in \mathbb{N}$, pour tout $b \in \mathbb{N}^*$, il existe $k \in \mathbb{N}$ tel que $a < kb$
Si $x > 0$, alors, pour tout $y \in \mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que $nx > y$.
On peut remarquer que l'énoncé de 2.5.1 est différent, mais, en fait, il n'y a rien de changé, puisque si $y \in \mathbb{Z}$, y pouvant être négatif, nous avons alors toujours $nx > y$ puisque $n \in \mathbb{N}$ et $y \in \mathbb{N}$
2. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, c'est à dire $b \neq 0$.
Considérons l'ensemble $\mathcal{M}\,(a, b)$ défini par :

$$\mathcal{M}\,(a, b) = \{t \in \mathbb{N} \text{ où } t = a - sb \text{ avec } s \in \mathbb{Z}\}$$

→ $\mathcal{M}(a,b)$ **est non vide**
C'est ici que nous allons utiliser la propriété d'Archimède 2.5.1
De $b \in \mathbb{Z}^*$, nous avons $|b| \in \mathbb{N}$ et $|b| > 0$.
D'après la propriété d'Archimède, il existe $m \in \mathbb{N}$ tel que $m|b| > -a$, c'est à dire tel que $a + m|b| > 0$
⋆ Si $b > 0$, alors, nous avons $a + m|b| > 0 \Longleftrightarrow a + mb > 0$ et en posant $s = -m$, nous avons $t = a - sb > 0$ et donc $t \in \mathcal{M}(a,b)$
⋆ Par contre, si $b < 0$, alors, nous avons $a + m|b| > 0 \Longleftrightarrow a - mb > 0$ et en posant $s = m$, nous avons $t = a - sb > 0$ et donc $t \in \mathcal{M}(a,b)$
Nous venons de démontrer que $\mathcal{M}(a,b) \neq \emptyset$

→ $\mathcal{M}(a,b)$ **possède un plus petit élément**
Par construction, $\mathcal{M}(a,b) \subset \mathbb{N}$.
D'après les axiômes 2.1.2 de construction de $\mathbb{N}$, toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
Donc, $\mathcal{M}(a,b)$ possède un plus petit élément.

→ **Si r est le plus petit élément de $\mathcal{M}(a,b)$, alors** $0 \leqslant r < |b|$
Nous appelons donc r le plus petit élément de $\mathcal{M}(a,b)$
⋆ Tout d'abord, par la définition de $\mathcal{M}(a,b)$, nous avons $r \geqslant 0$
⋆ Montrons maintenant que nous avons $r < |b|$
r, le plus petit élément de $\mathcal{M}(a,b)$ et donc $r \in \mathcal{M}(a,b)$, c'est à dire qu'il existe $q \in \mathbb{Z}$ tel que $r = a - bq$.
Supposons $r \geqslant |b| \Longleftrightarrow r - |b| \geqslant 0$. Posons, maintenant, $t_0 = r - |b| = a - bq - |b|$
▷ Si $b > 0$, alors $|b| = b$ et $t_0 = a - b(q+1)$, et d'après la définition de $\mathcal{M}(a,b)$, nous avons $t_0 \in \mathcal{M}(a,b)$ et

$$t_0 - r = a - b(q+1) - a + bq = -b \leqslant 0$$

C'est à dire $t_0 \leqslant r$, et r n'est plus le plus petit élément de $\mathcal{M}(a,b)$; il y a donc contradiction.
▷ Maintenant, si $b < 0$, alors $|b| = -b$ et $t_0 = a - b(q-1)$, et d'après la définition de $\mathcal{M}(a,b)$, nous avons à nouveau $t_0 \in \mathcal{M}(a,b)$ et

$$t_0 - r = a - b(q-1) - a + bq = b \leqslant 0$$

C'est à dire $t_0 \leqslant r$, et r n'est plus le plus petit élément de $\mathcal{M}(a,b)$; il y a donc contradiction.
Donc, les contradictions mènent à la conclusion $r < |b|$
⋆ En synthèse, nous avons bien $0 \leqslant r < |b|$

Il existe donc bien un couple d'entiers relatifs (q,r) tels que

$$a = bq + r \text{ et } 0 \leqslant r < |b|$$

3. Montrons l'unicité du couple (q,r)
Supposons donc qu'il existe 2 couples d'entiers relatifs (q_1,r_1) et (q_2,r_2) tels que :

$$a = bq_1 + r_1 \text{ avec } 0 \leqslant r_1 < |b| \text{ et } a = bq_2 + r_2 \text{ avec } 0 \leqslant r_2 < |b|$$

Alors $bq_1 + r_1 = bq_2 + r_2 \Longleftrightarrow b(q_1 - q_2) = r_2 - r_1$
→ De l'égalité $b(q_1 - q_2) = r_2 - r_1$, nous tirons $|b|\,|q_1 - q_2| = |r_2 - r_1|$
Si $q_1 \neq q_2$, alors, comme $q_1 - q_2 \in \mathbb{Z}$, nous avons $|q_1 - q_2| \geqslant 1$ et donc $|b|\,|q_1 - q_2| \geqslant |b|$, c'est à dire $|r_2 - r_1| \geqslant |b|$
→ Or, de $0 \leqslant r_1 < |b|$ et de $0 \leqslant r_1 < |b|$, nous déduisons $-|b| < r_2 - r_1 < |b|$, c'est à dire $|r_2 - r_1| < |b|$
Il y a donc contradiction et nous avons $q_1 = q_2$ et $r_1 = r_2$

Et le théorème est démontré

Remarque 14 :

1. Le théorème 4.2.6 est le pilier de l'arithmétique
2. Nous pouvons trouver plusieurs couples d'entiers relatifs (q, r) tels que $a = bq + r$. L'unicité provient de la condition supplémentaire $0 \leqslant r < |b|$

   Exemple

   Etudions la division de 12 par 7
   - ◇ Nous avons $12 = 1 \times 7 + 5$ et nous avons $0 \leqslant 5 < 7$
   - ◇ Mais, nous avons aussi $12 = 2 \times 7 + -2$ ou encore $12 = -1 \times 7 + 19$
   - ◇ Il n'y a qu'un seul couple (q, r) tel que $12 = 1 \times 7 + 5$ avec $0 \leqslant 5 < 7$

Exercice 2 :

Soient $b \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Comparer les quotients q_1, q_2 et q_3 des divisions de a par b, de $2a$ par b et de $(2a + b)$ par $2b$

4.2.7 Proposition

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$
x et y sont congrus modulo n si et seulement si ils ont même reste dans la division par n

Démonstration

1. **Supposons x et y congrus modulo n**
   On va montrer que x et y admettent même reste dans la division par n
   Si x et y sont congrus modulo n, alors $x - y = kn$ où $k \in \mathbb{Z}$
   La division par n donne : $x = an + r$ et $y = bn + r'$ où r et r' sont tels que $0 \leqslant r \leqslant n - 1$ et $0 \leqslant r' \leqslant n - 1$.
   Donc, $x - y = (a - b)\, n + (r - r')$, où on aura $-(n - 1) \leqslant r - r' \leqslant (n - 1)$; $x - y$ étant un multiple de n, la seule possibilité pour $r - r'$ est d'être nul ; donc : $r = r'$
2. **Supposons que x et y ont même reste dans la division par n**
   Alors, $x = an + b$ où $0 \leqslant b < n$, et $y = a'n + b$.
   Donc,
   $$x - y = (an + b) - (a'n + b) = n\,(a - a')$$
   Ce qui montre que $x \equiv y\,[n]$

Remarque 15 :

Donc, si r est le reste de la division de x par n, on a $x \equiv r\,[n]$

4.2.8 Proposition

$\mathbb{Z}/n\mathbb{Z}$ est un ensemble de n classes qui sont, en fait, tous les restes dans la division par n, c'est à dire :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \ldots, \overbrace{(n-2)}^{\cdot}, \overbrace{(n-1)}^{\cdot}\right\}$$

Démonstration

Tout $x \in \mathbb{Z}$ est congru, modulo n à un reste dans la division par n. Comme il y a n restes, il y a donc n classes

Exemple 2 :

1. Dans $\mathbb{Z}/5\mathbb{Z}$, nous avons :

$$\mathbb{Z}/5\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\} = \left\{\overset{\cdot}{(-4)}, \overset{\cdot}{(-3)}, \overset{\cdot}{(-2)}, \overset{\cdot}{(-1)}, \dot{0}\right\} = \left\{\overset{\cdot}{11}, \overset{\cdot}{12}, \overset{\cdot}{13}, \overset{\cdot}{14}, \overset{\cdot}{15}\right\}$$

   etc...

2. Dans $\mathbb{Z}/2^n\mathbb{Z}$, l'ensemble des classes d'équivalence est donné par :$\mathbb{Z}/2^n\mathbb{Z} = \left\{\overset{\cdot}{-2^{n-1}}, \ldots, \overset{\cdot}{-2^{n-1}-1}\right\}$

3. **Tables d'addition et de multiplication**
   (a) On a ici, la table d'addition de $\mathbb{Z}/5\mathbb{Z}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

   (b) Et voici la table de multiplication de $\mathbb{Z}/6\mathbb{Z}$

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

   On remarquera que $\mathbb{Z}/6\mathbb{Z}$ admet de véritables diviseurs de zéro :3 et 4, car on a $3 \times 4 = 0$,

4.2.9 Définition

On dit qu'un élement u de $\mathbb{Z}/n\mathbb{Z}$ est inversible ,s'il existe $v \in \mathbb{Z}/n\mathbb{Z}$ tel que $uv = 1$

Exercice 3 :

1. Faites la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$ *(Cette fois -ci, nous remarquerons que que $\mathbb{Z}/5\mathbb{Z}$ ne possède pas de diviseurs de 0)*
2. Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $\dot{2} + x = \dot{1}$ d'inconnue x
3. Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $\dot{3}x = \dot{2}$ d'inconnue x
4. Trouver, dans $\mathbb{Z}/5\mathbb{Z}$, les inconnues $x \in \mathbb{Z}/5\mathbb{Z}$ et $y \in \mathbb{Z}/5\mathbb{Z}$ vérifiant le système

$$\begin{cases} \dot{2}x + \dot{3}y = \dot{2} \\ \dot{1}x + \dot{2}y = \dot{4} \end{cases}$$

5. Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $x^2 + \dot{2}x - \dot{3} = \dot{0}$ d'inconnue x
6. Résoudre dans $\mathbb{Z}/5\mathbb{Z}$, l'équation $x^2 - x - \dot{2} = \dot{0}$

4.2.10 Exercices complémentaires

Exercice 4 :

Montrer que l'implication suivante est vraie : $x \equiv 4\,[8] \Longrightarrow x^2 \equiv 16\,[64]$.

Exercice 5 :

1. Trouver les entiers relatifs $x \in \mathbb{Z}$ tels que $x^2 + x + 1 \equiv 0\,[4]$
2. Démontrer que, pour tout $x \in \mathbb{Z}$, nous avons $x^3 - x \equiv 0\,[3]$

Exercice 6 :

Rechercher les éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$

Exercice 7 :

Trouver r tel que $x \equiv r\,[n]$, avec r entier et $0 \leqslant r < n$, dans les cas suivants :

1. $x = 1789$ et $n = 7$
2. $x = 1815$ et $n = 2^3$
3. $x = 4^{56}$ et $n = 2^{56}$

Exercice 8 :

Résoudre les congruences suivantes :

1. $3x \equiv 7\,[16]$
2. $5x + 7 \equiv 6\,[23]$
3. $4x \equiv 9\,[13]$
4. $2x + 8 \equiv 5\,[33]$
5. $3x + 9 \equiv 8x + 61\,[64]$
6. $4x + 3 \equiv 7x + 2\,[11]$

Exercice 9 :

Montrer que, pour tout entier naturel $n \in \mathbb{N}$, n^3 est de la forme $7k + 1$, $7k - 1$, $7k$

Exercice 10 :

Calculer les restes, modulo 7, des nombres 2^n et 3^n ; trouver alors $n$tel que $2^n + 3^n \equiv 0\,[7]$

Exercice 11 :

Erwann est représentant de commerce.
Partant de Vannes, il parcourt la Bretagne en respectant toujours les mêmes étapes :
il va à Nantes, puis à Rennes, puis à saint Brieuc ; de là il va à Brest, ensuite à Quimper et revient à Vannes.
En une année, il fait 147 étapes ; où se trouve-t-il à la fin de sa huitième année de travail ?

Exercice 12 :

1. Calculer le reste, modulo 7, de $(32)^{48}$, de $(237)^{349}$
2. Calculer le reste modulo 13 de $(100)^{100}$
3. Montrer que $2^{70} + 3^{70}$ est divisible par 13

Exercice 13 :

Critère de divisibilité par 9

1. Etudier les congruences de 10^n modulo 9
2. En déduire qu'un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9

Exercice 14 :

Trouver les trois derniers chiffres de $1! + 2! + 3! + \cdots + (2022)! + (2023)! + (2024)!$

Exercice 15 :

1. Démontrer que $(\forall k \in \mathbb{N})\,(\forall r \in \mathbb{N})\,\left(7^{4k+r} \equiv 7^r\,[10]\right)$
2. Etudier les classes de 7^n modulo 4
3. Quel est le chiffre des unités de $7^{(7^7)}$?

Exercice 16 :

Démontrer que Pour tout $n \in \mathbb{N}$ et $n \geqslant 2$:

1. $7^n - 7^{n-2} \equiv 12\,[36]$
2. $9^n - 9^{n-2} \equiv 16\,[64]$
3. $11^n - 11^{n-2} \equiv 20\,[100]$
4. Pour tout $m \in \mathbb{N}$,$(2m+1)^n - (2m+1)^{n-2} \equiv 4m\,\left[4m^2\right]$

Exercice 17 :

Preuve par 9
Le but de l'exercice est de démontrer la proposition suivante appelée preuve par 9 dont l'énoncé est ci-après :

> On cherche à vérifier le résultat de la multiplication $a \times b = c$.
>
> 1. On fait la somme des chiffres composant l'entier a et on itère jusqu'à n'avoir plus qu'un seul chiffre A appartenant à l'ensemble $\{0, 1, 2, \ldots, 9\}$.
> 2. On fait de même pour b et c ; on obtient respectivement les chiffres B et C. On calcule $A \times B$ et on fait à nouveau la somme des chiffres ; on obtient le chiffre C'
> 3. Si la multiplication $a \times b = c$ était correcte, on doit avoir : $C = C'$

1. Montrez que tout nombre entier est congru à la somme de ses chiffres modulo 9
2. Vérifier le calcul suivant en utilisant la preuve par 9 :$43 \times 164 = 7042$
3. Démontrer la proposition de la preuve par 9

Exercice 18 :

Considérons l'anneau $\mathbb{Z}/33\mathbb{Z}$

1. Soit $f : \mathbb{Z}/33\mathbb{Z} \longrightarrow \mathbb{Z}/33\mathbb{Z}$ définie par :

$$\left\{\begin{array}{rcl} f : \mathbb{Z}/33\mathbb{Z} & \longrightarrow & \mathbb{Z}/33\mathbb{Z} \\ x & \longmapsto & f(x) = 17x + 9 \end{array}\right.$$

   - ▷ Trouver l'inverse de 17 dans l'anneau $\mathbb{Z}/33\mathbb{Z}$
   - ▷ Résoudre, dans $\mathbb{Z}/33\mathbb{Z}$ l'équation $f(x) = 0$
   - ▷ Montrer que f est une bijection dont on donnera la bijection réciproque

2. Soit $g : \mathbb{Z}/33\mathbb{Z} \longrightarrow \mathbb{Z}/33\mathbb{Z}$ définie par :

$$\left\{\begin{array}{rcl} g : \mathbb{Z}/33\mathbb{Z} & \longrightarrow & \mathbb{Z}/33\mathbb{Z} \\ x & \longmapsto & g(x) = 22x + 7 \end{array}\right.$$

   Quel est l'ensemble des images des éléments de $\mathbb{Z}/33\mathbb{Z}$ par g ?

Exercice 19 :

Un entier naturel $n \in \mathbb{N}$ s'écrit $n = \overline{(x20y1)}_5$ en base 5. Déterminer tous les couples (x, y) pour lesquels n est divisible par 6