Arithmétique | CM: 7

Par Lorenzo

18 octobre 2024

1 Arithmétique modulaire : $(\mathbb{Z}/n\mathbb{Z})$

Définition 1.1. *Soient $a, b \in \mathbb{Z}$. On dit que a et b sont **congrus modulo** n si $a-b \in n\mathbb{Z}$.*
On note alors $a \equiv b[n]$ ou encore $a \equiv b \mod n$.

Proposition 1.1.

1. *On a $a \equiv b[n] \iff \exists k \in \mathbb{Z}, a = b + kn$.*
   *On note $\overline{b} := \{b + nk \mid k \in \mathbb{Z}\} = \{a \in \mathbb{Z} \mid a \equiv b[n]\}$. On l'appelle la **classe de congruence**.*
2. *Supposons que $a = nq + r$ soit la division euclidienne de a par n. Alors $\overline{a} = \overline{r}$.*
3. *Il y a exactement n classes de congruence distinctes : les $\overline{r}$, pour $r \in \{0, 1, ..., n-1\}$. Elles sont disjointes 2 à 2.*

Définition 1.2. *On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruences.*
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ est un ensemble fini à n élements.

Démonstration 1.1.

À faire

□

Remarques 1.1. *La congruence est un relation d'équivalence ainsi les classes congruences sont les classes d'équivalences pour la relation de congruence.*
Ainsi $\mathbb{Z}/n\mathbb{Z}$ se réinterprète comme $\mathbb{Z}/R$ avec $xRy \iff x \equiv y[n]$

1.1 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Proposition 1.2.

Soient $a, a', b, b' \in \mathbb{Z}$ tels que $a \equiv a'[n]$ et $b \equiv b'[n]$ Alors $a + b \equiv a' + b'[n]$

Démonstration 1.2.

$(a - a') = kn$ *et* $(b - b') = k'n$ *avec* $k, k' \in \mathbb{Z}$
$(a + b) - (a' + b') = a - a' + b - b' = kn + k'n = (k + k')n$

Donc $a + b \equiv a' + b'[n]$

□

Définition 1.3. *Soient $a, b \in \mathbb{Z}$. On pose dans $\mathbb{Z}/n\mathbb{Z}$: $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \times \overline{b} = \overline{a \times b}$*

Proposition 1.3.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.
$\overline{0}$ est l'élement neutre pour l'addition et $\overline{1}$ est l'élement neutre pour la multiplication.

Démonstration 1.3.

À faire

□

Example 1.1. *On peut faire des tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$. Par exemple la table de multiplication de $\mathbb{Z}/3\mathbb{Z}$*

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Lemme 1.1. *Soient a et b dans $\mathbb{Z}$ tels que $a \equiv b[n]$.*
Pour tout $p \in \mathbb{N}^*$, $a^p \equiv b^p[n]$

Démonstration 1.4.

À faire

□

Remarques 1.2. *En revanche on n'a pas $p \equiv q[n] \implies a^p \equiv a^q[n]$*

Théorème 1.1. *$\{\mathbb{Z}/n\mathbb{Z}, +, \times\}$ est un corps si et seulement si n est premier.*

Démonstration 1.5.

À faire

□