Arithmétique — CM: 7

Par Lorenzo

18 octobre 2024

Définition 0.1. *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.

Proposition 0.1.

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

Démonstration 0.1.

$(a - a') = kn$ et $(b - b') = k'n$
$(a + b) - (a' + b') = a - a' + b - b' = kn + k'n = (k + k')n$
Donc $a + b \equiv a' + b'[n]$

□

Définition 0.2. *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 0.2.

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

Démonstration 0.2.

□

On peut faire des tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$

Example 0.1.

Lemme 0.1. *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 0.3.

Dans $\mathbb{Z}/n\mathbb{Z}$ on veut montrer que $\overline{a^p} = \overline{b^p}$
Or $\overline{a^p} = \overline{a \times ... \times a} = \overline{a} \times ... \times \overline{a} =$

□

Remarques 0.1. *En revanche on n'a pas $p \equiv q[n] \implies a^p \equiv a^q[n]$*

Théorème 0.1. *$\{\mathbb{Z}/n\mathbb{Z}, +, \times\}$ est un corps si et seulement si n est premier.*

Démonstration 0.4.

Dire que $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ c'est dire qu'il existe $\overline{u}$ tel que $\overline{au} = \overline{1} \iff \exists u \in \mathbb{Z}, \exists k \in \mathbb{Z}, au = 1 + kn \iff \exists u \in \mathbb{Z}, \exists k' \in \mathbb{Z}, au + k'n = 1$ Cette équation a des solutions si n et m sont premier entre eux (bezout)

□