$\mathbb{Z}/n\mathbb{Z}$

1 Congruences

1.1 Définition

Définition. Soit $n \in \mathbb{N}^*$. Pour $a, b \in \mathbb{Z}$, on dit que a **est congru à** b **modulo** n si et seulement si $n \mid b - a$.
On note $a \equiv b\ [n]$ ou parfois $a \equiv b \bmod n$.

Proposition. La relation de congruence modulo n est un relation d'équivalence sur $\mathbb{Z}$.

divise

$a, b \in \mathbb{Z}$ $\quad a \equiv b\ [n]$

signifie $\quad b - a$ divisible par n

rel. éq. : RST

- Réflexive : $a \equiv a\ [n]$ car $a - a = 0 = 0 \cdot n$
- Symétrique : Si $a \equiv b\ [n]$ alors $b \equiv a\ [n]$

  en effet si $n \mid b - a$, $n \mid a - b$
- Transitive Si $a \equiv b\ [n]$, $b \equiv c\ [n]$ alors $a \equiv c\ [n]$

car $c - a = (c - b) + (b - a) \in n\mathbb{Z}$

1.2 Compatibilité avec les lois

Proposition. Soit $n \in \mathbb{N}^*$, $a, b, c, d \in \mathbb{Z}$. On a alors :

$$\left.\begin{array}{l} a \equiv b\ [n] \\ c \equiv d\ [n] \end{array}\right\} \Longrightarrow a + c \equiv b + d\ [n]$$

$$\left.\begin{array}{l} a \equiv b\ [n] \\ c \equiv d\ [n] \end{array}\right\} \Longrightarrow ac \equiv bd\ [n]$$

Corollaire. Si $a \equiv b\ [n]$, alors pour tout $k \in \mathbb{N}$, $a^k \equiv b^k\ [n]$.

Exemple. Justifier le critère de divisibilité par 3 : la somme des chiffres dans l'écriture en base 10 est divisible par 3.

$3 \mid 2025$?

L'écriture en base de 10 de $a \in \mathbb{N}$:

$$a = \sum_{k=0}^{d} a_k 10^k \qquad a_k \in \{0, \dots, 9\}$$

$10 \equiv 1\ [3]$ donc $10^k \equiv 1^k\ [3]$

$\equiv 1\ [3]$

donc $a \equiv \sum_{k=0}^{d} a_k\ [3]$

donc a et $\sum_{k=0}^{d} a_k$ ont même reste dans la div. eucl. par 3

$3 \mid a \Leftrightarrow 3 \mid \sum_{k=0}^{d} a_k$

1.3 Le petit théorème de Fermat

Petit théorème de Fermat.

Soit p un nombre premier, a un entier non multiple de p. Alors :

$$a^{p-1} \equiv 1 \ [p]$$

Preuve : par récurrence sur $a \in \mathbb{N}^*$: $a^p \equiv a \ [p]$

- pour $a = 1$:

$$1^p = 1 \equiv 1 \ [p]$$

- On suppose $a^p \equiv a \ [p]$

Alors $(a+1)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1$

$$\equiv a + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k \ [p]$$

par HR

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = p \cdot \frac{(p-1)!}{k!\,(p-k)!} \in \mathbb{Z}$$

divisible par p

$$\equiv 0 \ [p]$$

classique

$$k \binom{p}{k} = p \cdot \frac{(p-1)!}{(k-1)!\,(p-1-k+1)!}$$

$$= p \underbrace{\binom{p-1}{k-1}}_{\in \mathbb{Z}}$$

donc $p \mid k \binom{p}{k}$

or p premier, $k \in \{1, \dots, p-1\}$

donc $p \wedge k = 1$

donc par le lemme de Gauss $p \mid \binom{p}{k}$

Donc $(a+1)^p \equiv a + 1 + \sum 0 \quad [p]$

$\equiv a + 1 \quad [p]$

Ainsi, par récurrence $\forall a \in \mathbb{N}^*, \ a^p \equiv a \ [p]$

on suppose a premier avec p

$a^p - a \equiv 0 \ (p)$

ie $p \mid a^p - a = (a^{p-1} - 1)a$

or $p \wedge a = 1$ donc par le lemme de Gauss

$p \mid a^{p-1} - 1$

ie $a^{p-1} \equiv 1 \quad [p]$

2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

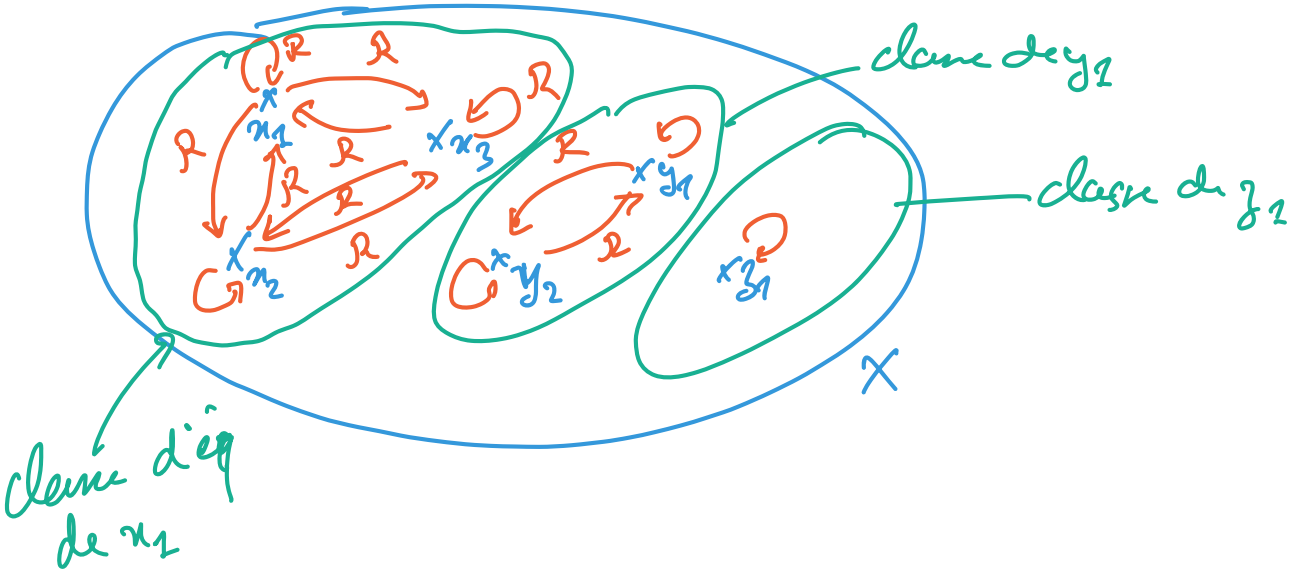
2.1 Complément : ensemble quotient

Définition. Soit X un ensemble et $\mathcal{R}$ une relation d'équivalence sur X. Pour $x \in X$, on appelle **classe d'équivalence de x pour la relation $\mathcal{R}$**, et on note $\overline{x}$, l'ensemble des éléments $y \in X$ tels que $y\mathcal{R}x$:

$$y \in \overline{x} \iff y\mathcal{R}x$$

Proposition. Si $y \in \overline{x}$, alors $\overline{y} = \overline{x}$. On dit que y **est un représentant de la classe d'équivalence** $\overline{x}$.

Proposition. Les classes d'équivalences pour $\mathcal{R}$ forment une partition de X : elles sont non vides, deux à deux disjointes et leur réunion est X.



$x_2 \in \overline{x_1}$ $\quad x_1 \in \overline{x_2}$ $\quad \overline{x_1} = \overline{x_2}$

pour Soit $y \in \overline{x}$

Mque $\overline{y} = \overline{x}$

- Soit $z \in \overline{y}$

ie $z \mathcal{R} y$ $\quad$ or $y \in \overline{x}$

donc $y \mathcal{R} x$

par transitivité, $z \mathcal{R} x$

ie $z \in \overline{x}$

- $\supset$ de même

Preuve :

- $\forall x \in X, \quad x \in \overline{x}$

  donc $E \subset \bigcup$ classes d'éq

- Toute classe d'éq a un représentant,

  donc est non vide

- Reste 2 à 2 disjointes :

  Rq : $\exists z \in \overline{x} \cap \overline{y} \Rightarrow \overline{x} = \overline{y}$

  Si $\exists z \in \overline{x} \cap \overline{y}$

  alors $z \mathcal{R} x$ et $z \mathcal{R} y$

  donc par transitivité $x \mathcal{R} y$

  donc $\overline{x} = \overline{y}$

2.2 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition. Soit $n \geqslant 2$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.

Exemple. Pour $n = 2$, on a :

$$\mathbb{Z}/2\mathbb{Z} = \{I, P\} = \{\overline{0}, \overline{1}\}$$

$\mathbb{Z} = \{\underbrace{0, 2, -2, 4, -4, 6, -6 \dots}_{P \quad \overline{0} \quad \overline{10}}, \underbrace{1, -1, 3, -3, 5, -5, \dots}_{\overline{1}}\}$

$\mathbb{Z}/2\mathbb{Z}$

Proposition. Soit $n \geqslant 2$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un ensemble à n éléments, que l'on peut décrire ainsi :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

• Soit $a, b \in \{0, \dots, n-1\}$

On suppose $\overline{a} = \overline{b}$ ie $a \equiv b \ [n]$

ie $n \mid b - a \in \{-(n-1) \dots, n-1\}$

donc $b - a = 0$ ie $b = a$

donc les n classes d'éq $\overline{0}, \dots, \overline{(n-1)}$ sont distinctes,

• $\forall a \in \mathbb{Z}$, r reste dans la div eucl de

a par n,

$a = nq + r$

$\equiv r \ [n]$ donc $a \in \overline{r}$

Remarque. *La description donnée ci-dessus n'est pas la seule possible. Ainsi :*

$$\begin{aligned}\mathbb{Z}/7\mathbb{Z} &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\} \\ &= \{\overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\}\end{aligned}$$

2.3 Structure d'anneau

Rappel. Pour $n \geqslant 2$, il existe une unique loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, encore notée $+$, pour laquelle l'application $k \mapsto \overline{k}$ soit un morphisme de groupes, i.e. :

$$\forall a, b \in \mathbb{Z},\ \overline{a+b} = \overline{a} + \overline{b}$$

Remarque. *Si l'on considère $x, y \in \mathbb{Z}/n\mathbb{Z}$ et que l'on veut parler de $x+y$, on envisage donc $a, b \in \mathbb{Z}$ qui sont des représentants des classes d'équivalence x et y : $\overline{a} = x$ et $\overline{b} = y$. Alors :*

$$x + y = \overline{a+b}$$

la déf de $x+y$ est indép du choix de a et b.

On note a_2, b_2 tq $x = \overline{a_2}$ $y = \overline{b_2}$

Rq $\overline{a_2 + b_2} = \overline{a+b}$

car $\overline{a} = \overline{a_2} = x$ donc $a \equiv a_2 \ [n]$

de même $b \equiv b_2 \ [n]$

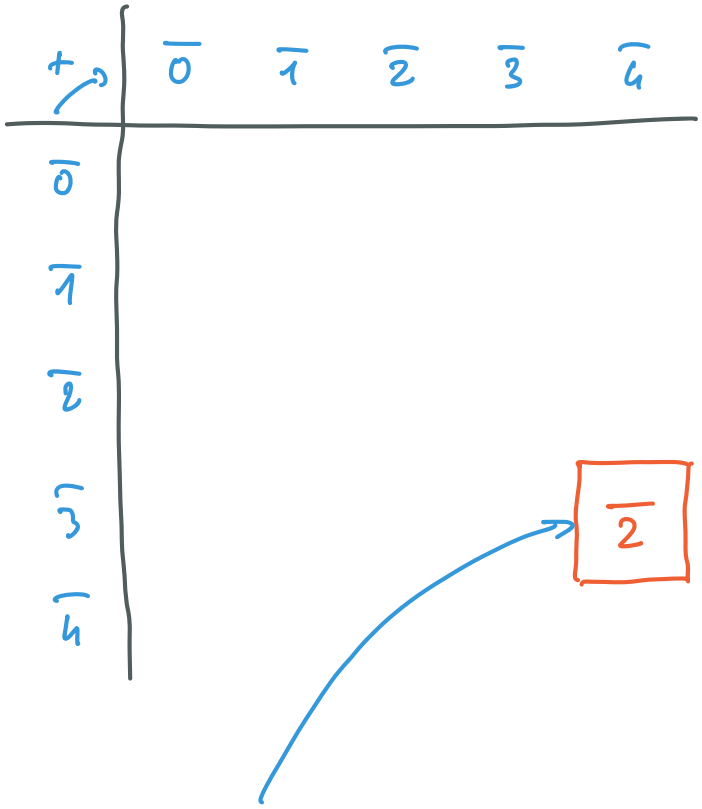
donc $a+b \equiv a_2 + b_2 \ [n]$

ie $\overline{a+b} = \overline{a_2+b_2}$

Rmq : le neutre de $+$ dans $\mathbb{Z}/n\mathbb{Z}$

est $\overline{0} = \overline{n}$

Exemple. Dresser la table d'addition de $\mathbb{Z}/5\mathbb{Z}$.



Proposition. Pour $n \geqslant 2$, il existe une unique loi interne sur $\mathbb{Z}/n\mathbb{Z}$, notée $\times$, pour laquelle l'application :

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array}$$ vérifie :

$$\forall a, b \in \mathbb{Z},\ \overline{a \times b} = \overline{a} \times \overline{b}$$

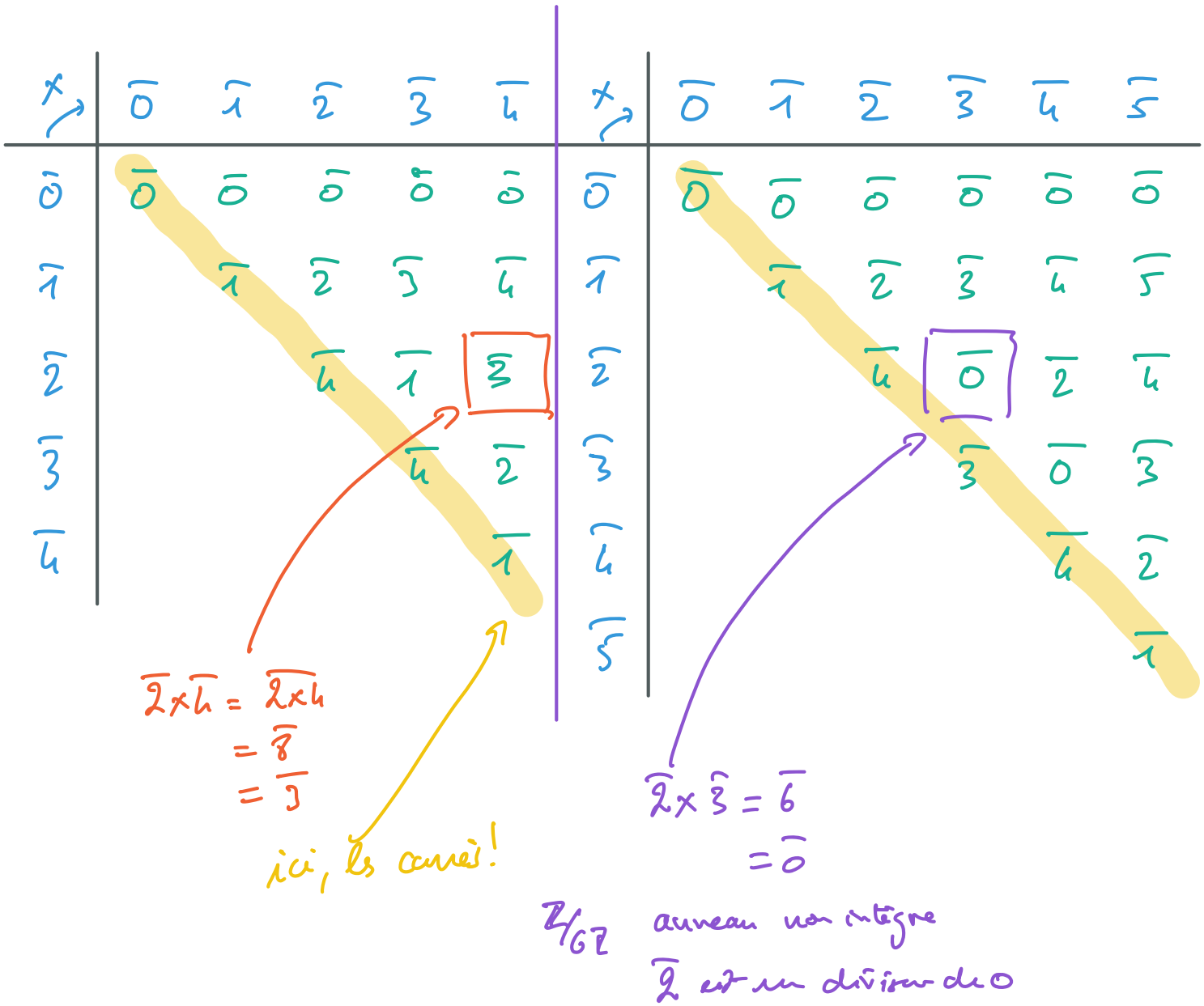
Alors $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, dont l'unité est $\overline{1}$.

Remarque. *Notons bien que :*

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array}$$

est un morphisme surjectif de l'anneau $(\mathbb{Z}, +, \times)$ sur l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Dresser la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$, de $\mathbb{Z}/6\mathbb{Z}$.



$\mathbb{Z}/6\mathbb{Z}$ anneau non intègre

$\overline{2}$ est un diviseur de 0

Résolvons : $x^2 = \overline{4}$ dans $\mathbb{Z}/5\mathbb{Z}$ $\Leftrightarrow x = \overline{2}$ ou $x = \overline{3}$ | $x^2 = \overline{2}$ dans $\mathbb{Z}/5\mathbb{Z}$ $\Leftrightarrow \phi$

2.4 Calcul dans $\mathbb{Z}/n\mathbb{Z}$

Remarque. *On travaille dans $\mathbb{Z}/n\mathbb{Z}$, où $n \geqslant 2$.*
Pour $k, a \in \mathbb{Z}$, que représentent :

$k\,\overline{a}$, $\overline{ka}$ *et* $\overline{k}\,\overline{a}$

$k\overline{a} = \underbrace{\overline{a}+\overline{a}+\cdots+\overline{a}}_{k \text{ fois}} = \overline{(a+\cdots+a)} = \overline{(ka)} = \overline{(k \times a)}$

$= \overline{k} \times \overline{a}$

Remarque. *On évite de dire : « soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ », mais plutôt : « soit $x \in \mathbb{Z}/n\mathbb{Z}$ et a un représentant de x, c'est-à-dire tel que $x = \overline{a}$.*
En particulier, si on définit :

$$f : \mathbb{Z}/n\mathbb{Z} \to \ldots$$

on peut vouloir écrire $\overline{a} \mapsto f(a)$, c'est-à-dire définir $f(x)$ en utilisant un représentant de x. Mais il faut bien justifier qu'alors, la définition est indépendante du choix du représentant :

$$x = \overline{a} = \overline{b} \implies f(a) = f(b)$$

Exemple. Est-ce que l'écriture suivante, dans $\mathbb{Z}/17\mathbb{Z}$, a du sens ?

$$\overline{15} \times (\overline{3})^{-1} = \overline{5}$$

$\overline{3}$ est inversible ?

oui, car on remarque que $\overline{3 \times 6} = \overline{18}$

$\overline{3} \times \overline{6} = \overline{1}$

donc $\overline{3}$ est inversible et $(\overline{3})^{-1} = \overline{6}$

et $\overline{15} \times (\overline{3})^{-1} = \overline{15} \times \overline{6}$

$= \overline{15 \times 6}$ ...

$\overline{15} \times (\overline{3})^{-1} = \overline{(15 \times 3^{-1})} = \overline{5}$

$15 \times 3^{-1} \in \mathbb{Z}$

$\overline{15}$ dans $\mathbb{Z}/17\mathbb{Z}$

on valide

$\overline{5} \times \overline{3} = \overline{15}$

donc $\overline{5} = \overline{15} \times (\overline{3})^{-1}$

Exemple. Résoudre, dans $\mathbb{Z}/11\mathbb{Z}$, l'équation :

$$x^2 - \bar{6}x + \bar{5} = \bar{0} \quad (E)$$

$x^2 - \bar{6}x + \bar{5}$

$= x^2 - 2 \times \bar{3}\, x + \bar{9} - \bar{4}$

$= (x - \bar{3})^2 - \bar{4}$

$(E) \iff (x - \bar{3})^2 = \bar{4}$

or, dans $\mathbb{Z}/11\mathbb{Z}$: $\bar{0}^2 = \bar{0}$

$\mathbb{Z}/11\mathbb{Z} = \{\bar{k}\}$ où $k \in [\![-5, 5]\!]$

$(\bar{-1})^2 = \bar{1}^2 = \bar{1}$

$(\bar{-2})^2 = \bar{2}^2 = \bar{4}$

$(\bar{-3})^2 = \bar{3}^2 = \bar{9}$

$(\bar{-4})^2 = \bar{4}^2 = \bar{16} = \bar{5}$

$(\bar{-5})^2 = \bar{5}^2 = \bar{25} = \bar{3}$

donc $(E) \iff x - \bar{3} = \bar{2}$ ou $x - \bar{3} = -\bar{2}$

$\iff x = \bar{5}$ ou $x = \bar{1}$

Π2 : $(E) \quad (x - \bar{3})^2 = \bar{4} = \bar{2}^2$

$\iff (x - \bar{3})^2 - \bar{2}^2 = \bar{0}$

$\iff (x - \bar{5})(x - \bar{1}) = \bar{0}$ intègre !

Exemple. Résoudre, dans $\mathbb{Z}/31\mathbb{Z}$, l'équation :

$$x^2 - \overline{11}x - \overline{1} = \overline{0}$$

$$x^2 - \overline{11}\,x - \overline{1} = x^2 + \overline{20}\,x - \overline{1}$$

$$= (x + \overline{10})^2 - \overline{101}$$

$$= (x + \overline{10})^2 - \overline{8}$$

$$(E) \iff (x + \overline{10})^2 = \overline{8}$$

On cherche les carrés dans $\mathbb{Z}/31\mathbb{Z}$:

$$\overline{0}^2 = \overline{0}$$

$$(-1)^2 = \overline{-1}^2 = \overline{1}$$

$$(-2)^2 = \overline{-2}^2 = \overline{4}$$

$$\overline{3}^2 = \overline{9}$$

$$\overline{4}^2 = \overline{16}$$

$$\overline{-5}^2 = \overline{25}$$

$$\overline{6}^2 = \overline{5}$$

$$\overline{-7}^2 = \overline{49} = \overline{18}$$

$$\overline{-8}^2 = \overline{64} = \overline{2}$$

$$\overline{9}^2 = \overline{81} = \overline{19}$$

$$\overline{10}^2 = \overline{100} = \overline{7}$$

$$\overline{11}^2 = \overline{121} = -\overline{3} = \overline{28}$$

$\overline{12}^2 = \overline{144} = \overline{20}$

$\overline{13}^2 = \overline{169} = \overline{14}$

$\overline{14}^2 = \overline{196} = \overline{15}$

$\overline{155} = \overline{186} = \overline{217} = \overline{0}$

$(-\overline{17})^2 = \overline{15}^2 = \overline{225} = \overline{8}$

$(E) \iff (x+\overline{10})^2 = \overline{8}$

$\iff x+\overline{10} = \overline{15}$ ou $x+\overline{10} = -\overline{15}$

$\iff x = \overline{5}$ ou $x = -\overline{25} = \overline{6}$

$$\mathcal{S} = \{\overline{5}, \overline{6}\}$$

Exemple. Discuter, suivant les valeurs de $a \in \mathbb{Z}/13\mathbb{Z}$, le nombre de solutions de l'équation :

$$x^2 + x + a = \overline{0}$$

$x^2 + x + a = x^2 - \overline{12}x + a$

$= (x-\overline{6})^2 - \overline{36} + a$

$= (x-\overline{6})^2 - \overline{10} + a$

donc $(E) \iff (x-\overline{6})^2 = \overline{10} - a$

Dans $\mathbb{Z}/13\mathbb{Z}$ $\quad \overline{0}^2 = \overline{0}$

$(-\overline{1})^2 = (\overline{1})^2 = \overline{1}$

$(-\overline{2})^2 = \overline{2}^2 = \overline{4}$

$$(\overline{-3})^2 = \overline{3}^2 = \overline{9}$$

$$(\overline{-4})^2 = \overline{4}^2 = \overline{3}$$

$$(\overline{-5})^2 = \overline{5}^2 = \overline{-1} = \overline{12}$$

$$(\overline{-6})^2 = \overline{6}^2 = \overline{-3} = \overline{10}$$

(E) a 1 solution $\Leftrightarrow \overline{10} - a = \overline{0}$

$\Leftrightarrow a = \overline{10}$

(E) a 2 solutions $\Leftrightarrow \overline{10} - a \in \{\overline{1}, \overline{4}, \overline{9}, \overline{3}, \overline{12}, \overline{5}\}$

$\Leftrightarrow a \in \{\overline{9}, \overline{6}, \overline{1}, \overline{7}, \overline{-2}, \overline{0}\}$
$\overline{-2} = \overline{12}$

(E) a 0 solution $\Leftrightarrow$ a n'est pas l'une des val. précédentes.

Proposition. Pour p premier, calculer $\mathrm{Card}(A)$ où :

$$A = \left\{ x^2,\ x \in \left(\mathbb{Z}/p\mathbb{Z}\right)^* \right\}$$

3 Inversibles de $\mathbb{Z}/n\mathbb{Z}$

Théorème.

Soit n entier, $n \geqslant 2$. Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les classes $\overline{k}$ où $k \in \{0, \dots, n-1\}$ est premier avec n.

Remarque. *Ce sont les générateurs du groupe cyclique* $(\mathbb{Z}/n\mathbb{Z}, +)$.

Notation : On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$

(on trouve aussi les notations : $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

$(\mathbb{Z}/n\mathbb{Z})^\times$

ce n'est pas $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$)

Pour l'anneau $\mathbb{Z}$

$$\mathbb{Z}^* = \{-1, 1\} \neq \mathbb{Z} \setminus \{0\}$$

Preuve :

$\Leftarrow$ Soit $k \in \{0, .., n-1\}$ premier avec n

$k \wedge n = 1$

donc par le th de Bézout, $\exists u, v \in \mathbb{Z}$

tq $ku + nv = 1$

donc $ku \equiv 1 \quad [n]$

donc $k\overline{u} = \overline{1}$

donc $\overline{k}$ inversible, d'inverse $\overline{u}$

$\Rightarrow$ Soit $k \in \{0, \dots, n-1\}$ tq $\overline{k}$ inversible

donc $\exists x \in \mathbb{Z}/n\mathbb{Z}$ tq $\overline{k}x = \overline{1}$

On note u un représentant de x : $x = \overline{u}$

$\overline{k}\,\overline{u} = \overline{1}$

ie $ku \equiv 1 \quad [n]$

donc $\exists v \in \mathbb{Z}$ tq $ku = 1 + nv$

donc $ku - nv = 1$

donc (Bézout) $k \wedge n = 1$

Définition. On note $\varphi(n)$ le nombre d'inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$:

$$\varphi(n) = \text{Card}\left(\{k \in \{0, \dots, n-1\},\ k \wedge n = 1\}\right)$$

φ s'appelle **l'indicatrice d'Euler**.

Remarque. *On convient que* $\varphi(1) = 1$.

$\varphi(n) = \text{Card}\left((\mathbb{Z}/n\mathbb{Z})^*\right)$

Théorème d'Euler.

Soit $n \geqslant 2$. Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\ [n]$.

Remarque. *Lorsque n est premier, on reconnaît le petit théorème de Fermat.*

(cf Rude Lagrange des groupes cycliques)

Preuve

On suppose $a \wedge n = 1$

donc $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

Notons $y = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$

$= \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} \overline{a}x$ (chg° d'indice $x = ax'$)

car $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$, $x \mapsto \overline{a}x$ bijective

de réciproque $x \mapsto \overline{a}^{-1}x$

$= \overline{a}^{\operatorname{Card}(\mathbb{Z}/n\mathbb{Z})^*} \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$

$= \overline{a}^{\varphi(n)}\, y$

donc (y inversible) $\overline{1} = \overline{a}^{\varphi(n)}$ dans $\mathbb{Z}/n\mathbb{Z}$

ie $a^{\varphi(n)} \equiv 1 \quad [n]$

Corollaire Petit Th de Fermat.

On suppose p premier.

$\forall k \in \{1, \dots, p-1\}$, $k \wedge p = 1$

donc $(\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$= \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$

donc $\varphi(p) = p - 1$

pour $a \wedge p$, $a^{p-1} \equiv 1 \quad [p]$