Def. $(A, f_1, \dots, f_m)$ estrutura algébrica, com $\nu_1, \dots, \nu_m$ as aridade de $f_1, \dots, f_m$ respectivamente, uma congruência em A é uma equivalencia ϑ em A tal que, $\forall i = 1, \dots, m$ $\forall a_1, \dots, a_{\nu_i}, b_1, \dots, b_{\nu_i} \in A$, vale:

$$a_1 \vartheta b_1, \dots, a_{\nu_i} \vartheta b_{\nu_i} \Rightarrow f_i(a_1, \dots, a_{\nu_i}) \vartheta f_i(b_1, \dots, b_{\nu_i})$$

Exemplo $(A, \cdot)$ $\cdot$ oper. binária

Uma equivalência ϑ em A é congruência sse $\forall a_1, a_2, b_1, b_2 \in A$,

$$a_1 \vartheta b_1 \text{ e } a_2 \vartheta b_2 \Rightarrow a_1 \cdot a_2 \vartheta b_1 \cdot b_2 .$$

Se ϑ é uma congruência em $(A, f_1, \dots, f_n)$, então $A/_\vartheta$ é uma estrutura do mesmo tipo de A, com as operações definidas como segue, $\forall i = 1, \dots, n$:

$\forall a_1/_\vartheta, \dots, a_{v_i}/_\vartheta$, $f_i\left(a_1/_\vartheta, \dots, a_{v_i}/_\vartheta\right) = \dfrac{f_i(a_1, \dots, a_{v_i})}{\vartheta}$.

$(\mathbb{Z}, +, \cdot, -, 0, 1)$ anel comutativo com identidade

Uma congruência nesta estrutura é uma equivalência ϑ t.q. $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$, se $a_1 \vartheta b_1$ e $a_2 \vartheta b_2$, então:

- $a_1 + a_2 \,\vartheta\, b_1 + b_2$
- $a_1 a_2 \,\vartheta\, b_1 b_2$
- $-a_1 \,\vartheta\, -b_1$

$\forall m \in \mathbb{Z}$, seja $m\mathbb{Z}$ a relação binária em $\mathbb{Z}$ definida por: $a \, m\mathbb{Z} \, b$ sse $\exists k \in \mathbb{Z} \, (a-b = km)$, ou seja, sse $a-b$ é múltiplo de m.

Obs.: $0\mathbb{Z} = \Delta$, a relação de igualdade.

$a \, 0\mathbb{Z} \, b$ sse $\exists k \in \mathbb{Z} \, (a-b = k \cdot 0 = 0)$ sse $a = b$.

A partir de agora, as relações $m\mathbb{Z}$ consideradas serão apenas aquelas com $m \neq 0$.

$\forall a \in \mathbb{Z}$, $a - a = 0 = 0 \cdot m$. Logo $a \, m\mathbb{Z} \, a$ e $m\mathbb{Z}$ é reflexiva.

$\forall a, b \in \mathbb{Z}$, se $a \, m\mathbb{Z} \, b$, então $\exists k \in \mathbb{Z} \, (a - b = km) \Rightarrow$
$\Rightarrow b - a = -(a - b) = (-k)m \Rightarrow b \, m\mathbb{Z} \, a$. $m\mathbb{Z}$ é simétrica.

$\forall a, b, c \in \mathbb{Z}$ t.q. $a \, m\mathbb{Z} \, b$ e $b \, m\mathbb{Z} \, c$, $\exists h, k \in \mathbb{Z}$ t.q.
$a - b = hm$ e $b - c = km \Rightarrow a - c = a - b + b - c = hm + km =$
$= (h + k)m \Rightarrow a \, m\mathbb{Z} \, c$. $m\mathbb{Z}$ é transitiva.

$m\mathbb{Z}$ é uma equivalência em $\mathbb{Z}$ $\forall m \in \mathbb{Z}$.

Obs.: $\forall m$, $m\mathbb{Z} = (-m)\mathbb{Z}$.

Seja $m \in \mathbb{Z} \setminus \{0\}$, sejam $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ t.q. $a_1 \, m\mathbb{Z} \, b_1$ e $a_2 \, m\mathbb{Z} \, b_2$, e sejam h e k os inteiros t.q. $a_1 - b_1 = hm$ e $a_2 - b_2 = km$.

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = hm + km = (h+k)m$$

$$\Rightarrow a_1 + a_2 \; m\mathbb{Z} \; b_1 + b_2$$

$$\left.\begin{array}{l} a_1 - b_1 = hm \Rightarrow a_1 = b_1 + hm \\ a_2 - b_2 = km \Rightarrow a_2 = b_2 + km \end{array}\right] \Rightarrow$$

$$a_1 \cdot a_2 = (b_1 + hm)(b_2 + km) = b_1 b_2 + b_1 km + b_2 hm + hkm^2 =$$

$$= b_1 b_2 + m(b_1 k + b_2 h + hkm) \Rightarrow$$

$$\Rightarrow a_1 a_2 - b_1 b_2 = (b_1 k + b_2 h + hkm) \cdot m \Rightarrow a_1 a_2 \; m\mathbb{Z} \; b_1 b_2$$

$$-a_1 - (-b_1) = b_1 - a_1 = -(a_1 - b_1) = -hm \Rightarrow -a_1 \; m\mathbb{Z} \; -b_1.$$

Logo, $m\mathbb{Z}$ é uma congruência em $\mathbb{Z}$, chamada <u>congruência módulo m</u>.

Escreve-se $a \, m\mathbb{Z} \, b$ ou $a \equiv b \pmod{m}$

Equivalentemente:

$a \, m\mathbb{Z} \, b$ sse a e b têm o mesmo resto na divisão por m

$a-b=km \Rightarrow a=b+km$. Se $b=qm+r$, $0\leq r<m$,

então $a=qm+r+km=(q+k)m+r$, $0\leq r<m$.

Logo, a e b têm o mesmo resto na divisão por m.

Reciprocamente, se $a=q_1m+r$ e $b=q_2m+r$, com

$0\leq r<m$, então $a-b=q_1m+r-(q_2m+r)=$

$=(q_1-q_2)m+\cancel{r-r}=(q_1-q_2)m \Rightarrow a \, m\mathbb{Z} \, b$.

Seja $\mathbb{Z}_m$ o quociente $\mathbb{Z}/_{m\mathbb{Z}}$.

$\mathbb{Z}_m$ tem exatamente m elementos.

$$\mathbb{Z}_m = \left\{ {}^{0}/_{m\mathbb{Z}}, {}^{1}/_{m\mathbb{Z}}, \dots, \frac{m-1}{m\mathbb{Z}} \right\} = \left\{ \bar{0}, \bar{1}, \dots, \overline{m-1} \right\}$$

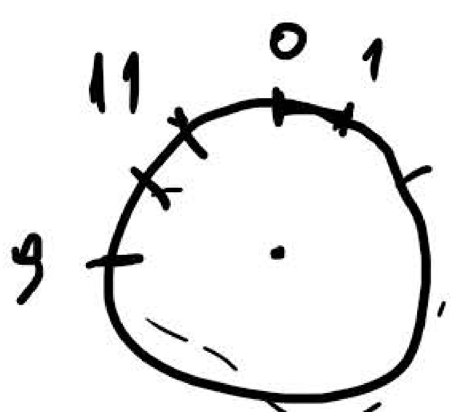
$$\bar{0} = \{ a \in \mathbb{Z} : \exists k \in \mathbb{Z} \, (a = km) \}$$

$$\bar{1} = \{ a \in \mathbb{Z} : \exists k \in \mathbb{Z} \, (a = km + 1) \}$$

$$\vdots$$

$$\overline{m-1} = \{ a \in \mathbb{Z} : \exists k \in \mathbb{Z} \, (a = km + (m-1)) \}.$$

$\bar{a} + \bar{b} = \overline{a+b} = \bar{r}$ $\quad r$ é o resto da divisão $a+b \,\lfloor m$



$$\bar{9} + \bar{5} = \overline{14} = \bar{2}$$

Proposição Se ϑ é uma congruência em $(\mathbb{Z},+,\cdot,-,0,1)$, então $\exists m\in\mathbb{Z}$ t.q. $\vartheta = m\mathbb{Z}$.

Dem.

Consideremos $0/\vartheta$. $\forall a,b\in\mathbb{Z}$, se $a\,\vartheta\, b$, então $a-b\;\vartheta\; b-b=0$, ou seja, $a-b\in 0/\vartheta$.

Se $0/\vartheta=\{0\}$, então $a\,\vartheta\, b \Rightarrow a-b=0 \Rightarrow a=b$.

Logo $\vartheta=\Delta=0\mathbb{Z}$.

Se $0/\vartheta\neq\{0\}$, então $\exists \min\{n\in\mathbb{N}\setminus\{0\} : n\in 0/\vartheta\}=m$.

Como $m\,\vartheta\,0$, então $\forall k\in\mathbb{Z}$, $km\;\vartheta\; k.0=0 \Rightarrow$

$\Rightarrow \forall k\in\mathbb{Z}$, $km\in 0/\vartheta \Rightarrow 0/m\mathbb{Z}\subseteq 0/\vartheta$.

Seja $a\in 0/\vartheta$, isto é, $a\,\vartheta\,0$ e sejam $q,r\in\mathbb{Z}$ t.q. $a=qm+r$, $0\leq r<m$. $qm+r\;\vartheta\;0$ e, por outro lado, $-qm\;\vartheta\;0 \Rightarrow (qm+r)-qm\;\vartheta\;0+0 \Rightarrow r\,\vartheta\,0$.

Como m é o menor natural t.q. $m\,\vartheta\,0$, segue que $r=0$ e, então, $a=qm$. Logo $a\in 0/m\mathbb{Z}$ e portanto $0/m\mathbb{Z}=0/\vartheta$.

$\forall a,b\in\vartheta$, $a\,\vartheta\,b \Leftrightarrow a-b\;\vartheta\;0 \Leftrightarrow a-b\in 0/\vartheta$

$\Leftrightarrow a-b\in 0/m\mathbb{Z} \Leftrightarrow a-b\;m\mathbb{Z}\;0 \Leftrightarrow a\;m\mathbb{Z}\;b$.

Logo $\vartheta=m\mathbb{Z}$.

Em $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $(x+y)^2 = (x+y)(x+y) =$

$= x^2 + xy + yx + y^2 = x^2 + \bar{2}xy + y^2 = x^2 + \bar{0}xy + y^2 = x^2 + y^2$

Em $\mathbb{Z}_p$, com p primo, $(x+y)^p = x^p + y^p$.

$0/2\mathbb{Z}$ = {pares} $1/2\mathbb{Z}$ = {impares}

$(2+3)^2 = 2^2 + 2\cdot 2\cdot 3 + 3^2 = 25$

$(\bar{2}+\bar{3})^2 = \bar{2}^2 + \cancel{\underbrace{\bar{2}}_{=\bar{0}} \cdot \bar{2} \cdot \bar{3}} + \bar{3}^2 = \bar{2}^2 + \bar{3}^2 = \bar{4} + \bar{9} = \overline{13} = \bar{1}$

$\parallel$

$(\bar{0}+\bar{1})^2 = \bar{1}^2 = \bar{1}$