$m \in \mathbb{Z} \setminus \{0\}$ Em $m\mathbb{Z}$ temos:

$$\bar{a} + \bar{b} = \overline{a+b} \quad , \quad \bar{a} \cdot \bar{b} = \overline{ab} \quad , \quad -\bar{a} = \overline{-a}$$

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}_m \, , \quad \bar{a} + \bar{b} = \bar{b} + \bar{a}$$

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

$$a/_{m\mathbb{Z}} + b/_{m\mathbb{Z}} = \frac{a+b}{m\mathbb{Z}} = \frac{b+a}{m\mathbb{Z}} = b/_{m\mathbb{Z}} + a/_{m\mathbb{Z}}$$

$$(\bar{a} + \bar{b}) \cdot \bar{c} = \overline{a+b} \cdot \bar{c} = \overline{(a+b)c} = \overline{ac+bc} = \bar{a}\bar{c} + \bar{b}\bar{c} =$$

$$= \bar{a}\bar{c} + \bar{b}\bar{c} \, .$$

Se m é primo, então $\mathbb{Z}_m$ é um corpo, ou seja,
$\forall \bar{a} \in \mathbb{Z}_m \setminus \{\bar{0}\} \; \exists \, \bar{b} \in \mathbb{Z}_m$ t.q. $\bar{a}\bar{b} = \bar{1}$.
Reciprocamente, se $\mathbb{Z}_m$ é um corpo, então m é primo.

Def. Uma equação congruencial (linear) é uma equação do tipo $ax \equiv b \pmod m$, com $a, b, m \in \mathbb{Z}$.

$\Updownarrow$

$(ax)m\mathbb{Z}\,b \Leftrightarrow ax - b$ é múltiplo de m

Teorema A equação congruencial $ax \equiv b \pmod m$ é solucionável (em $\mathbb{Z}$) sse os mdc de a e m dividem b.

Dem.

Sejam d e $-d$ os mdc de a e m, com $d > 0$.

$\Rightarrow$ Seja c uma solução da equação. Então $ac \equiv b \pmod m$, ou seja, $\exists k \in \mathbb{Z}$ t.q. $ac - b = km$. Segue $ac - km = b$ e, então, como $d \mid ac$ e $d \mid km$, isso implica que $d \mid b$.

$\Leftarrow$ Suponha-se, agora, que $d \mid b$ e seja $h \in \mathbb{Z}$ t.q. $b = dh$. Pelo algoritmo das divisões subsequentes de Euclides, $\exists u, v \in \mathbb{Z}$ t.q. $au + mv = d$. Multiplicando tudo por h, temos $auh + mvh = dh = b$. De $auh + mvh = b$, segue $auh - b = mvh$ e, portanto $auh \equiv b \pmod m$. Logo, uh é uma solução de $ax \equiv b \pmod m$.

$3x \equiv 2 \pmod 9$ Se a e m são primos entre si, $ax \equiv b \pmod m$ é solucionável $\forall b \in \mathbb{Z}$.

Se c for uma solução de $ax \equiv b \pmod m$, o conjunto de todas as soluções é exatamente $\overline{c}_{m\mathbb{Z}} = \{c + km : k \in \mathbb{Z}\}$

equivalentes $\begin{cases} 24x \equiv 16 \pmod 8 \\ 0 \cdot x \equiv 0 \pmod 8 \end{cases}$ vale $\forall x \in \mathbb{Z}$.

$\left.\begin{array}{l} 27x \equiv 17 \pmod 8 \\ 3x \equiv 1 \pmod 8 \end{array}\right\}$ são equivalentes

> Uma solução c é $u \cdot b$, onde $au + mv = d$ e $dh = b$

27	8	3	2	1
	3	2	1	

$d = 1 \Rightarrow h = b = 17$

$1 = 3 - 2 = 27 - 3 \cdot 8 - (8 - 2 \cdot 3) = 27 - 4 \cdot 8 + 2 \cdot 3 =$

$= 27 - 4 \cdot 8 + 2(27 - 3 \cdot 8) = 3 \cdot 27 - 10 \cdot 8 \qquad u = 3$

$c = uh = 3 \cdot 17 = 51 \qquad S = \overline{51} = \{51 + 8k : k \in \mathbb{Z}\}$

8	3	2	1
	2	1	

$d = 1 \qquad 1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8$

$u = 3 \quad h = 1 \quad , \quad c = uh = 3$

$S = \overline{3} = \{3 + 8k : k \in \mathbb{Z}\}$

51	8
3	6

$\overline{51} = \overline{3}$

$25x \equiv 31 \pmod{64}$

d, u, h

$d \in \mathrm{mdc}(a,m)$, $au + mv = d$

$dh = b$

64	25	14	11	3	2	1
	2	1	1	3	1	

$d = 1, \quad h = b = 31$

$1 = 3 - 2 = 14 - 11 - (11 - 3 \cdot 3) = 14 - 2 \cdot 11 + 3 \cdot (14 - 11) = 4 \cdot 14 - 5 \cdot 11 =$

$= 4 \cdot (64 - 2 \cdot 25) - 5 (25 - 14) = 4 \cdot 64 - 13 \cdot 25 + 5 (64 - 2 \cdot 25) =$

$= 9 \cdot 64 - 23 \cdot 25 \qquad u = -23 \qquad c = uh = -23 \cdot 31 = -713$

$S = \{-713 + k \cdot 64 \mid k \in \mathbb{Z}\} = \overline{-713} = \overline{55}$

$-713 \mid 64$
$-(-768) \; -12$
55

$a = bq + r \qquad 0 \le r < b$

$3 \mid 2$
$-2 \quad 1$
1

$-3 \mid 2$
$2 \quad -1$
-1

$-3 \mid 2$
$4 \quad -2$
1

Def. Uma **equação diofantina** é uma equação do tipo $ax+by=c$, nas incógnitas x e y e com coeficientes $a, b, c \in \mathbb{Z}$.
Uma solução dela é um par $(x_0, y_0) \in \mathbb{Z}^2$ t.q. $ax_0 + by_0 = c$.

Teorema A equação diofantina $ax+by=c$ tem soluções sse os mdc de a e b dividem c.

Demonstração 1
Um par $(x_0, y_0) \in \mathbb{Z}^2$ é solução da eq. sse
$ax_0 + by_0 = c \iff ax_0 - c = b\cdot(-y_0) \iff ax_0 \equiv c \pmod b$
Então esse x_0 existe sse os mdc de a e b dividem c.

Demonstração 2
$\Rightarrow$| Seja (x_0, y_0) uma solução da equação; então $ax_0+by_0=c$.
Se $d \in mdc(a,b)$, $d|a$ e $d|b$. Logo $d|ax_0+by_0=c$.
$\Leftarrow$| Seja $d \in mdc(a,b)$ e vamos supor que $d|c$, ou seja, $\exists h \in \mathbb{Z}(dh=c)$. Pelo T. de Bézout, $\exists u, v \in \mathbb{Z}$ t.q.
$au+bv=d$ e, então $a(uh)+b(vh)=dh=c$.
Logo, o par (uh, vh) é solução de $ax+by=c$.

Se $ax+by=c$ tem solução (x_0, y_0), o conjunto de todas as soluções da equação é:
$$S = \left\{\left(x_0 - k\frac{b}{d}, y_0 + k\frac{a}{d}\right) : k \in \mathbb{Z}\right\}.$$

$$\overset{a}{137}x + \overset{b}{24}y = \overset{c}{7} \qquad d, u, v, h \qquad dh = c$$

137	24	17	7	3	1	0
	5	1	2	2	3	

$d = 1 \quad h = c = 7$

$$1 = 7 - 2\cdot 3 = 24 - 17 - 2\cdot(17 - 2\cdot 7) = 24 - 3\cdot 17 + 4\cdot 7 =$$

$$= 24 - 3(137 - 5\cdot 24) + 4(24 - 17) = -3\cdot 137 + 20\cdot 24 - 4\cdot(137 - 5\cdot 24) =$$

$$= \underbrace{-7}_{u}\cdot 137 + \underbrace{40}_{v}\cdot 24 \qquad (hu, hv)$$

pois $(137\cdot u + 24\cdot v = d)\cdot h \Rightarrow 137\cdot hu + 24\cdot hv = c$

$$(x_0, y_0) = (-7\cdot 7, 40\cdot 7) = (-49, 280)$$

$$S = \{(-49 - k\cdot 24, 280 + k\cdot 137) : k \in \mathbb{Z}\}.$$

Se $k = -2$, $(-1, 6) \in S$

$60x - 32y = 12$ $\quad d, u, v, h$

$dh = 12$ e $60u - 32v = d$

60	32	28	4	0
	1	1	7	

$d = 4, \quad h = 3$

$4 = 32 - 28 = 32 - (60 - 32) = -60 + 2 \cdot 32 = 60 \cdot \underset{u}{(-1)} - 32 \cdot \underset{v}{(-2)}$

$(x_0, y_0) = (-3, -6)$ $\qquad b/d = 15$ $\qquad a/d = -8$

$$S = \{(-3 - 15k, -6 - 8k) : k \in \mathbb{Z}\} =$$

$$= \{(-3 + 15k, -6 + 8k) : k \in \mathbb{Z}\}$$

$au + bv = d$ $\qquad c = dh$

$auh + bvh = dh = c$ $\qquad (x_0, y_0) = (uh, vh)$