Divisão

$32 \,\underline{|\,45}$
$32 \quad 0$ $\rightarrow 32 = 45 \times 0 + 32$

$234 \,\underline{|\,9}$
$54 \quad 26$
0 $\rightarrow -234 = -9 \times 26 + 0$

$a|b$ = "a divide b"

$a|b$ e $a|c \Rightarrow a|xb+yc \quad (x,y \in \mathbb{Z})$

$a|b$ e $b|c \Rightarrow ac|bd$

Algoritmo de divisao:

$a = bq + r$ e $a \leq r < b$

m.d.c. → máximo divisor comum

$d = \text{m.d.c.}(a,b)$

↳ 1) $d|a$ e $d|b$

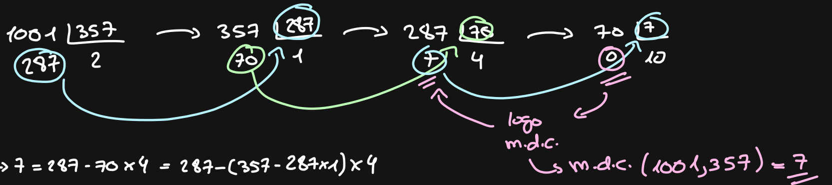
↳ 2) $\forall c \in \mathbb{N}, c|a$ e $c|b \Rightarrow c \leq d$

Primos entre si:

→ se $\text{m.d.c.}(a,b) = 1$ $\dashrightarrow$ $ax+by=1$, para alguns $x,y \in \mathbb{Z}$

$d = \text{m.d.c.}(a,b) \Rightarrow \exists\, x,y \in \mathbb{Z}$ t.q. $d = ax+by$

Algoritmo de Euclides (para fazer o m.d.c)



↳ $\text{m.d.c.}(1001,357) = \underline{\underline{7}}$

$\rightarrow 7 = 287 - 70 \times 4 = 287 - (357 - 287 \times 1) \times 4$

$= 287 \times 5 - 357 \times 4 = (1001 - 357 \times 2) \times 5 - 357 \times 4$

$= 1001 \times 5 - 357 \times 14$

$\Leftrightarrow \underset{d}{7} = \underset{a}{1001} \times \underset{x}{5} + \underset{b}{357} \times \underset{y}{(-14)}$

nº Primo:

$P > 1$ é um nº primo se $\underline{1}$ e $\underline{P}$ são os únicos divisores positivos de P

Lema de Euclides

$a|bc$ e $\text{m.d.c.}(a,b) = 1 \Rightarrow a|c$

$12 = 4 \times 3 \quad 12 = 6 \times 2$

- $2|4 \times 3$ e $\text{m.d.c.}(2,3) = 1$
  ↳ $2|4$
- $3|6 \times 2$ e $\text{m.d.c}(3,2) = 1$
  ↳ $3|6$
- $72 = 9 \times 8$

  $12|9 \times 8$ e $12 \nmid 9$ e $12 \nmid 8$

  $\text{m.d.c.}(12,9) = 3 \neq 1$

  $\text{m.d.c.}(12,8) = 4 \neq 1$

  $\Rightarrow$ O lema não se aplica

Fatorização, m.d.c, m.m.c.

$$\begin{array}{r|l} 507 & 3 \\ 169 & 13 \\ 13 & 13 \\ 1 & \end{array} \qquad \begin{array}{r|l} 1287 & 3 \\ 429 & 3 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array}$$

$507 = \underline{3}\times\underline{13}\times 13 = 3\times 13^2$

$1287 = \underline{3\times3}\times 11\times \underline{13} = 3^2\times11\times13$

→ máximo múltiplo comum ⇒ m.d.c.$(507,1287) = 3\times13$ → o nº tem de aparecer nas 2 e usar o que tem o menor expoente

→ mínimo múltiplo comum → m.m.c.$(507,1287) = 3^2\times11\times13^2$ ⇒ todos os nºs que aparecem e com o maior expoente

ou

m.d.c.(a,b) ⇒ Alg. Euclides

m.m.c.$(a,b) \Rightarrow \dfrac{a.b}{\text{m.d.c.}(a,b)}$

$(a,b\in\mathbb{N})$

m.m.c.:

- $a\,|\,m$ e $b\,|\,m$
- $a\,|\,c$ e $b\,|\,c \Rightarrow m\leq c$
- m.m.c.$(a,b) = ab \Leftrightarrow$ m.d.c.$(a,b)=1$

Equação diofantina (linear):

$ax+by=c \qquad a,b,c\in\mathbb{Z}$

Existe solução sse m.d.c.$(a,b)=c$ ou m.d.c.$(a,b)=k$ e $k\,|\,c$

Solução particular: $(x,y)=(x_0,y_0)$

Solução geral: $\begin{cases} x = x_0 + \dfrac{b}{d}t \\ y = y_0 - \dfrac{a}{d}t \end{cases}, t\in\mathbb{Z}$

$d = \text{m.d.c.}(a,b)$

exemplo 1)

$56x+72y=40$

m.d.c.$(56,72)=8$ e $8\,|\,40$ → logo, Eq. é solúvel (tem solução)

$72 = 56\times1+16$ $\qquad 56 = 16\times3+8$

$$\begin{array}{r|l} 72 & 56 \\ \hline 16 & 1 \end{array} \qquad \begin{array}{r|l} 56 & 16 \\ \hline 8 & 2 \end{array} \qquad \begin{array}{r|l} 16 & 8 \\ \hline 0 & 2 \end{array}$$

Solução particular:

$56x+72y=40$

$8 = 56 - 16\times3 = 56-(72-56\times1)\times3 = 56\times4-72\times3 = \underbrace{56\times4+72\times(-3)}_{\times5} = \underbrace{8}_{\times5}$

$\Rightarrow 56\times\underbrace{20}_{x}+72\times\underbrace{(-15)}_{y}=40$

→ solução particular: $(x_0,y_0)=(20,-15)$

→ Solução geral: $\begin{cases} x = 20+\dfrac{72}{8}t \\ y = -15-\dfrac{56}{8}t \end{cases}, t\in\mathbb{Z}$

$\Leftrightarrow \begin{cases} x = 20+9t \\ y = -15-7t \end{cases}, t\in\mathbb{Z}$

exemplo 2)

→ $8x-15y=4$

$$\begin{array}{r|l} 15 & 8 \\ \hline 7 & 1 \end{array} \qquad \begin{array}{r|l} 8 & 7 \\ \hline \boxed{1} & 1 \end{array} \qquad \begin{array}{r|l} 7 & 1 \\ \hline 0 & 7 \end{array}$$

- m.d.c. $(8,15)=1\,|\,4$, logo a equação é solúvel

- Solução particular: $1 = 8-7\cdot1 = 8-(15\cdot1)\cdot1 = \underset{\text{"8x"}}{\underline{8}}\cdot2-\underset{\text{"15y"}}{\underline{15}}\cdot1 = \underset{\times4}{1} \Leftrightarrow 4(8\times2-15\times1)=4 \Leftrightarrow 8\times\underset{x}{8}-15\times\underset{y}{4}=4$

  ↳ $(x_0,y_0)=(8,4)$

  ↳ $\begin{cases} a = 8\times8=64 \\ b = 15\times4=60 \end{cases}$

- Solução geral:

$\begin{cases} x = 8+\left(\frac{-15}{1}\right)\cdot t \\ y = 4-\left(\frac{8}{1}\right)\cdot t \end{cases} \Leftrightarrow \begin{cases} x = 8-15t \\ y = 4-2t \end{cases}, t\in\mathbb{Z}$ → Determinar x e y t.q. $x>0$ e $y>0$ → $\begin{cases} 8-15t>0 \\ 4-8t>0 \end{cases} \Leftrightarrow \begin{cases} -15t>-8 \\ -8t>-4 \end{cases} \Leftrightarrow \begin{cases} t<\frac{8}{15}=0{,}53 \\ t<\frac{4}{8}=0{,}5 \end{cases}$

↳ $t=0$
$x=8$
$y=4$
$a=64$
$b=60$

↳ $t=-1$
$x=23$
$y=12$
$a=184$
$b=180$

↳ $t=-2$
$x=38$
$y=20$
$a=304$
$b=300$

Módulo / Congruências módulo n

$a \equiv b (\mathrm{mod}\, n)$ ⇒ a e b têm o mesmo resto na divisão por n

$91 \equiv \underline{\underline{0}} (\mathrm{mod}\, 7)$

$91 \,\underline{|7}$
$21 \quad 13$
$\underline{\underline{0}}$

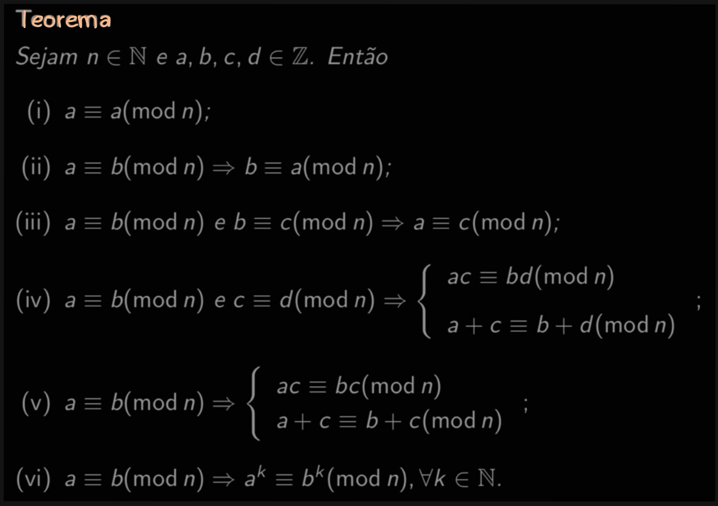
$17 \not\equiv \underline{\underline{13}} (\mathrm{mod}\, 2)$

$17 \,\underline{|2}$
$\underline{\underline{1}} \quad 8$

↳ $17 \equiv 1 (\mathrm{mod}\, 2)$

Sistema complelo de residuos módulo (scrm)

Seja $n \in \mathbb{N}$. Um conjunto de n inteiros $\{a_1, a_2, \dots, a_n\}$ diz-se um scrm n se todo o inteiro é congruente módulo n com um e um só a_k $(k \in \{1, 2, \dots, n\})$.



Teorema

Sejam $n \in \mathbb{N}$ e $a, b, c, d \in \mathbb{Z}$. Então

(i) $a \equiv a (\mathrm{mod}\, n)$;

(ii) $a \equiv b (\mathrm{mod}\, n) \Rightarrow b \equiv a (\mathrm{mod}\, n)$;

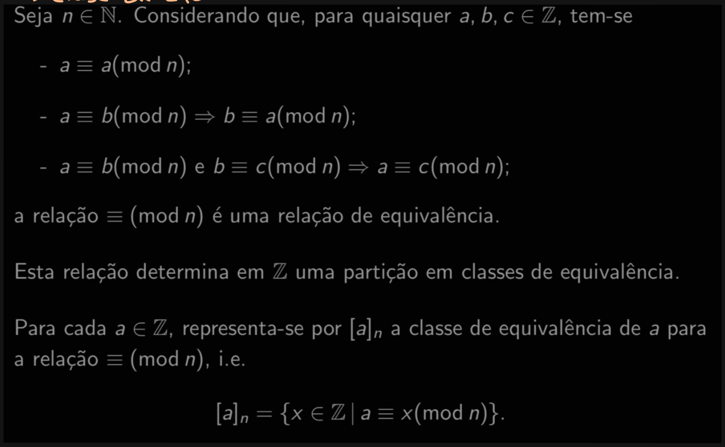
(iii) $a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n) \Rightarrow a \equiv c (\mathrm{mod}\, n)$;

(iv) $a \equiv b (\mathrm{mod}\, n)$ e $c \equiv d (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bd (\mathrm{mod}\, n) \\ a + c \equiv b + d (\mathrm{mod}\, n) \end{cases}$;

(v) $a \equiv b (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bc (\mathrm{mod}\, n) \\ a + c \equiv b + c (\mathrm{mod}\, n) \end{cases}$;

(vi) $a \equiv b (\mathrm{mod}\, n) \Rightarrow a^k \equiv b^k (\mathrm{mod}\, n), \forall k \in \mathbb{N}$.

→ Classe de equivalência



Seja $n \in \mathbb{N}$. Considerando que, para quaisquer $a, b, c \in \mathbb{Z}$, tem-se

- $a \equiv a (\mathrm{mod}\, n)$;
- $a \equiv b (\mathrm{mod}\, n) \Rightarrow b \equiv a (\mathrm{mod}\, n)$;
- $a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n) \Rightarrow a \equiv c (\mathrm{mod}\, n)$;

a relação $\equiv (\mathrm{mod}\, n)$ é uma relação de equivalência.

Esta relação determina em $\mathbb{Z}$ uma partição em classes de equivalência.

Para cada $a \in \mathbb{Z}$, representa-se por $[a]_n$ a classe de equivalência de a para a relação $\equiv (\mathrm{mod}\, n)$, i.e.

$$[a]_n = \{x \in \mathbb{Z} \,|\, a \equiv x (\mathrm{mod}\, n)\}.$$

41^{63} ⇒ $41 \,\underline{|7}$
$6 \quad 5$
→ $41 \equiv 6 (\mathrm{mod}\, \underline{\underline{7}})$ → $41^{63} \equiv 6^{63} (\mathrm{mod}\, 7)$

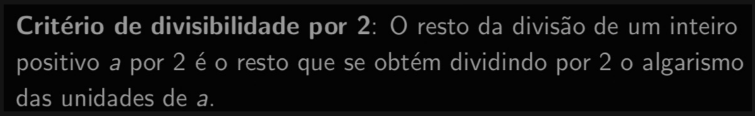
$6 - \underline{\underline{7}} = -1$

$41 \equiv -1 (\mathrm{mod}\, 7) \Rightarrow 41^{63} \equiv (-1)^{63} (\mathrm{mod}\, 7) \Rightarrow 41^{63} \equiv -1 (\mathrm{mod}\, 7) \Rightarrow 41^{63} \equiv 6 (\mathrm{mod}\, 7)$

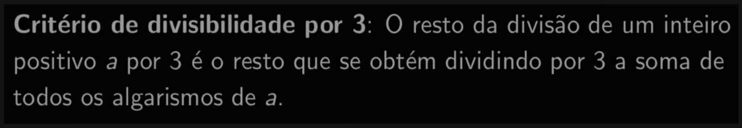
$-1 + 7 = 6$

Critérios de divisibilidade:

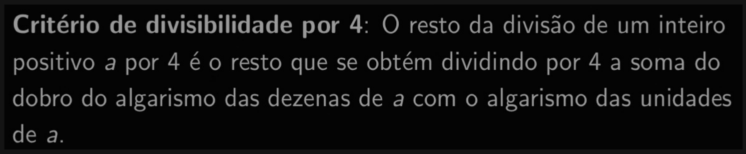
$\overline{abcde}$ → são digitos e não uma multiplicação



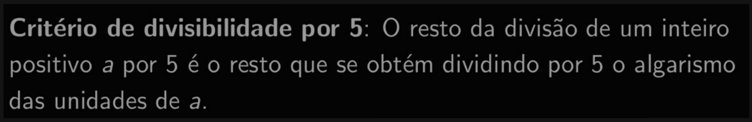
Critério de divisibilidade por 2: O resto da divisão de um inteiro positivo a por 2 é o resto que se obtém dividindo por 2 o algarismo das unidades de a.



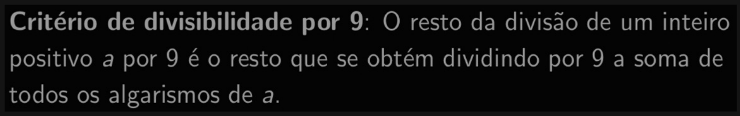
Critério de divisibilidade por 3: O resto da divisão de um inteiro positivo a por 3 é o resto que se obtém dividindo por 3 a soma de todos os algarismos de a.



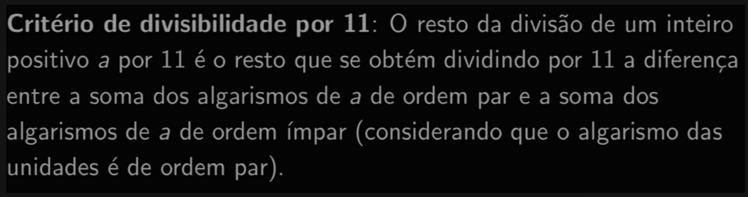
Critério de divisibilidade por 4: O resto da divisão de um inteiro positivo a por 4 é o resto que se obtém dividindo por 4 a soma do dobro do algarismo das dezenas de a com o algarismo das unidades de a.



Critério de divisibilidade por 5: O resto da divisão de um inteiro positivo a por 5 é o resto que se obtém dividindo por 5 o algarismo das unidades de a.



Critério de divisibilidade por 9: O resto da divisão de um inteiro positivo a por 9 é o resto que se obtém dividindo por 9 a soma de todos os algarismos de a.



Critério de divisibilidade por 11: O resto da divisão de um inteiro positivo a por 11 é o resto que se obtém dividindo por 11 a diferença entre a soma dos algarismos de a de ordem par e a soma dos algarismos de a de ordem ímpar (considerando que o algarismo das unidades é de ordem par).

49. Determine os dígitos x e y tais que o número $\overline{34xx58y}$ é simultaneamente divisível por 9 e por 11.

$n = \overline{34xx58y}$ → quer dizer que são digitos e não uma conta → logo x e y são digitos

Critérios de divisibilidade

- por 9 • $n \equiv 0 \pmod 9$ → soma dos digitos $\equiv 0 \pmod 9$ → $3+4+x+x+5+8+y \equiv 0 \pmod 9 \Leftrightarrow 2x+y+20 \equiv 0 \pmod 9 \Leftrightarrow 2x+y \equiv -20 \pmod 9$
- por 11 • $n \equiv 0 \pmod{11}$ → $y - \cancel{8} + \cancel{5} - \cancel{x} + \cancel{x} - 4 + \cancel{3} \equiv 0 \pmod{11} \Leftrightarrow y \equiv 4 \pmod{11}$

↳ Logo, $y = 4$ pois $y \in \{0, \dots, 9\}$

$x = ?$

$2x + y \equiv -20 \pmod 9$

$\Leftrightarrow 2x + 4 \equiv -20 \pmod 9$

$\Leftrightarrow 2x \equiv -24 \pmod 9$ $\quad -24 + 27 = 3$

$\Leftrightarrow 2x \equiv 3 \pmod 9$

↳ congruência linear

- Classes possíveis:

↳ $x \in \{0, \dots, 8\}$ → por tentativas → $\underline{\underline{x = 6}}$ → $2 \times 6 \equiv 3 \pmod 9$

Res.:

$2x \equiv 3 \pmod 9 \Leftrightarrow 2x - 3 = 9y$

$\Leftrightarrow 2x - 9y = 3$ → equação diofantina

Sistemas de congruências lineares

$ax \equiv b \pmod n$

$\Leftrightarrow ax - b = ny$, para algum $y \in \mathbb{Z}$

$\Leftrightarrow ax - ny = b$

↳ equação diofantina

exemplo 1)

$12x \equiv 6 \pmod{16}$

$12x - 16y = 6$

↳ existem exatamente $\underline{\underline{d}}$ soluções módulo n, mas congruentes entre si.

↳ dividir 12, 16 pelo m.d.c. se m.d.c. | 6

↳ m.d.c. $(12, 16) = 4 \nmid 6$ → logo não solúvel

$12 = 4 \times 3$

$16 = 4^2$

↳ se fosse solúvel → dividir 12, 16 por 4

↓

exemplo

→ $12x \equiv 8 \pmod{16}$

↳ m.d.c. $(12, 16) \mid 8$ → logo existe solução

$\underline{\underline{4}}$

↳ $\Leftrightarrow \frac{12x}{4} = \frac{8}{4} \left(\bmod \frac{16}{4}\right)$

$\Leftrightarrow 3x \equiv 2 \pmod 4$

↳ m.d.c. $(3, 4) = 1$ → tentar escrever $3x$ como $4x$ _ + _

↓

$3x \equiv 2 \pmod 4 \Leftrightarrow 4x \underbrace{-x}_{\text{resto}} = 2 \pmod 4$ → $4x \equiv 0 \pmod 4$

$a \equiv b \pmod n \Rightarrow ca \equiv cb \pmod n$

MAS

$ca \equiv cb \pmod n \Rightarrow a \equiv b \pmod n$ se m.d.c.$(n, c) = 1$

n e c são primos

$ax \equiv b \pmod n \Rightarrow ax + c \equiv b + c \pmod n$

$4x - x \equiv 2 \pmod 4$ > $-4x \equiv 0 \pmod 4$

$\Leftrightarrow -x \equiv 2 \pmod 4$

$\Leftrightarrow x = -2 \pmod 4$

↓ $+4$ ↓

$\Leftrightarrow x = 2 \pmod 4$

$\Leftrightarrow x = 2 + 4t, \ t \in \mathbb{Z}$ → $t \in \{0, 1, \dots, d-1\}$ → $t \in \{0, 1, 2, 3\}$ $+3$

$\Leftrightarrow x \in [2]_4$ → $x = 2 + \frac{n}{d} \cdot t = 2 + \frac{16}{4} \cdot t = 2 + 4t$

→ $16 \,\lfloor 3$ ① 5 → -3 → $16 \,\lfloor 3$ (−2) 6 → $16 \,\lfloor 3$ ① 5 → $+3.2$ → $16 \,\lfloor 3$ 7 3 ↳ $5-2$

$ax \equiv b \pmod n \Leftrightarrow px \equiv b \pmod n$ ←

$ax = kn + px$

↓

$a \equiv 2 \pmod 4$

↳ $a + 4x \equiv 2 \pmod 4$ →

$14 \,\lfloor 3$ 2 4

$17 \,\lfloor 3$ 2 5

$20 \,\lfloor 3$ 2 6

⋮

exemplo 2)

$12x \equiv 24 \pmod{35}$

m.d.C. (12, 35) = 1 | 24 -> Logo, existe uma única solução módulo 35

$12 = 4 \times 3$
$35 = 7 \times 5$

$\Leftrightarrow \frac{12x}{12} \equiv \frac{24}{12} \pmod{35}$ -> m.d.c.(12, 35) = 1

$\Leftrightarrow x \equiv 2 \pmod{35}$

$\Leftrightarrow x \in [2]_{35}$

↳ menor solução não negativa $(x \geq 0)$

$x = 2 + 35t, t \in \mathbb{Z}$ -> logo $t = 0$ -> $x = 2$

↳ maior solução não positiva $(x \leq 0)$

$t = -1$ -> $x = -33$

Em alternativa: -> 24 não fosse divisível por 12

$12x \equiv 24 \pmod{35}$

$\Leftrightarrow 3x . 12x \equiv 3 \times 24 \pmod{35}$

$\Leftrightarrow 36x \equiv 72 \pmod{35}$

$\Leftrightarrow 36x \equiv 2 \pmod{35}$

$\Leftrightarrow 35x + x = 2 \pmod{35}$

↳ $35 \equiv 0 \pmod{35}$

$\Leftrightarrow x = 2 \pmod{35}$

$\Leftrightarrow x \in [2]_{35}$

$\Leftrightarrow x = 2 + 35t, t \in \mathbb{Z}$

$72 \,\underline{|\, 35}$
$\underline{\underline{2}} \quad 2$

$72 - 35 - 35 = 2$

exemplo 3)

$10x \equiv 14 \pmod{16}$

m.d.c. (10, 16) = 2 | 14 -> logo existem $\underline{2}$ soluções ($\underline{2}$ classes de equivalência)

$10 = 2 \times 5$
$16 = 2 \times 2 \times 2 \times 2$

$\Leftrightarrow \frac{10x}{2} \equiv \frac{14}{2} \left(\mathrm{mod} \frac{16}{2}\right)$

$\Leftrightarrow 5x \equiv 7 \pmod{8}$

$\Leftrightarrow 5x . 3 \equiv 3 . 7 \pmod{8}$

$\Leftrightarrow 15x \equiv 21 \pmod{8}$

$\Leftrightarrow 15x \equiv 5 \pmod{8}$

$\Leftrightarrow 16x - 1x \equiv 5 \pmod{8}$

↳ $16 \equiv 0 \pmod{8}$

$\Leftrightarrow -x \equiv 5 \pmod{8}$

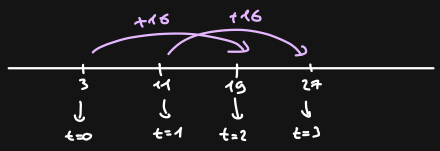
$\Leftrightarrow x \equiv -5 \pmod{8}$

$\Leftrightarrow x \equiv 3 \pmod{8}$

$\Leftrightarrow x \in [3]_8$

$\Leftrightarrow x = 3 + 8t, t \in \mathbb{Z}$

$21 \,\underline{|\, 8}$
$\underline{-16} \quad 2$
5



$[3]_8 = [3]_{16} \cup [11]_{16}$ ⇒ 2 soluções módulo 16 "distintas"

Teorema Chinês dos Restos

exemplo 1)

$$\begin{cases} x \equiv \overset{a_1}{1} \pmod 3 \\ x \equiv \overset{a_2}{2} \pmod 5 \\ x \equiv \overset{a_3}{3} \pmod 7 \end{cases}$$

$m.d.c.(3,5) = \boxed{1}$

$m.d.c.(3,7) = \boxed{1}$ → logo existe apenas uma solução pelo T.C.R.

$m.d.c.(5,7) = \boxed{1}$

$\Downarrow$

$n = 3 \times 5 \times 7 = 105$

somar os módulos

$\hookrightarrow N_1 = \frac{n}{3} = 35$

$\hookrightarrow N_2 = \frac{n}{5} = 21$

$\hookrightarrow N_3 = \frac{n}{7} = 15$

sempre 1, independente do sistema

$$\Rightarrow \begin{matrix} N_1 x = 1 \pmod 3 \\ N_2 x \equiv 1 \pmod 5 \\ N_3 x \equiv 1 \pmod 7 \end{matrix} \Leftrightarrow \begin{matrix} 35x \equiv 1 \pmod 3 \\ 21x \equiv 1 \pmod 5 \\ 15x \equiv 1 \pmod 7 \end{matrix} \Leftrightarrow \begin{matrix} 36x - x \equiv 1 \pmod 3 \\ 20x + x \equiv 1 \pmod 5 \\ 14x + x \equiv 1 \pmod 7 \end{matrix} \Leftrightarrow \begin{matrix} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 7 \end{matrix}$$

$\boxed{x_1 = 2}$

$\boxed{x_2 = 1}$

$\boxed{x_3 = 1}$

Solução particular do sistema:

$$\begin{aligned} \bar{x} &= x_1 \cdot N_1 \cdot a_1 + x_2 \cdot N_2 \cdot a_2 + x_3 \cdot N_3 \cdot a_3 \\ &= 2 \cdot 35 \cdot 1 + 1 \cdot 21 \cdot 2 + 1 \cdot 15 \cdot 3 \\ &= \underline{\underline{157}} \end{aligned}$$

Solução geral do sistema:

$$x \equiv \underset{\bar{x}}{157} \pmod{\underset{n}{105}} \Leftrightarrow x \equiv 52 \pmod{105} \Leftrightarrow x \in [52]_{105} \Leftrightarrow x = 52 + 105t,\ t \in \mathbb{Z}$$

exemplo 2)

$$\begin{cases} x \equiv 16 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 6 \\ x \equiv 5 \pmod{12} \end{cases}$$

$mod(3,6) \neq 1 \Rightarrow$ Não se pode aplicar o T.C.R

$\hookrightarrow$ generalização deste Teorema (pg. 167)

$m.d.c.(2,3) = 1 \mid 2-1=1$ ✓

$m.d.c.(2,6) = 2 \mid 5-1=4$ ✓

$m.d.c.(2,12) = 2 \mid 5-1=4$ ✓

$mdc(3,6) = 3 \mid 5-2=3$ ✓

$mdc.(3,12) = 3 \mid 5-2=3$ ✓

$m.d.c.(6,12) = 6 \mid 5-5=0$ ✓

⇒ logo, temos uma única solução

$\hookrightarrow n = m.m.c.(2,3,6,12) = \underline{\underline{12}}$

mínimo múltiplo comum dos módulos

$\hookrightarrow 2=2$

$3=3$

$\boxed{6=2\times3}$

$\boxed{12=2^2\times3}$

Sistema equivalente:

$$\begin{cases} x \equiv 1 \pmod{\underline{\underline{2}}}^{\times} \\ x \equiv 2 \pmod{\underline{\underline{3}}} \\ \boxed{\begin{matrix} x \equiv 5 \pmod{\underline{\underline{2}}}^{\times} \\ x \equiv 5 \pmod{\underline{\underline{3}}} \end{matrix}} \\ \boxed{\begin{matrix} x \equiv 5 \pmod{\boxed{2^2}} \\ x \equiv 5 \pmod{\underline{\underline{3}}} \end{matrix}} \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \pmod{2^2} \\ x \equiv 2 \pmod 3 \end{cases}$$

→ maior pot. 2

⇒ Agora, usar o T.C.R.

$m.d.c.(4,3) = 1$ ⇒

solução: $x \equiv 5 \pmod{12}$