Matemática Discreta

1º Ano .... 2º Semestre

> **Nota**
> IN inclui o 0

- **Teoria de Números**
  - estudo das propriedades dos nºs inteiros $\mathbb{Z}$

- **Definição Múltiplo**

$a, b \in \mathbb{Z}$

a é múltiplo de b se existe um k pertencente a $\mathbb{Z}$ tal que $a = k \times b$
ou seja, b é divisor de a

- Notação:

$b|a$ → b é divisor de a

$a \,\dot{=}\, \dot{b}$ → a é múltiplo de b

- **Teorema**

$a, b \in \mathbb{Z}$

1. Se b é divisor de a $\Rightarrow$ $-b$ é divisor de a
2. Qualquer $b \neq 0$ é divisor de 0
3. 1 é divisor de a ; a é divisor de a $(a \neq 0)$
4. a e $-a$ têm exatamente os mesmos divisores

- **Definição - Máximo Divisor Comum**

$m, n \in \mathbb{Z}$ não simultaneamente nulos

- O máximo divisor comum de m e n é o maior número inteiro que é simultaneamente divisor de m e de n.
- $d \in \mathbb{Z}$ é mdc de m e n se $d|m$ e $d|n$ e para qualquer $d'|m$ e $d'|n$ se tem que $d'|d$

Notação: mdc(m,n) $m \frown n$

- **Teorema**

$m, n \in \mathbb{Z}$

1. $mdc(m,n) = mdc(n,m)$
2. $mdc(m,n) = mdc(-m,n) = mdc(m,-n) = mdc(-m,-n)$
3. $mdc(m,n) \geq 1$
4. $mdc(0,a) = |a|$
5. $mdc(m,m) = |m|$

- **Algoritmo de Euclides**

input $m, n \in \mathbb{N}$ não simultaneamente nulos
output $mdc(m,n)$ $mdc(120, 84)$

Quocientes		1	2	3
	120	84	36	12
Restos	36	12	0	

mdc = 12

$$\begin{array}{r|l} 120 & 84 \\ \hline 36 & 1 \end{array} \qquad \begin{array}{r|l} 84 & 36 \\ \hline 12 & 2 \end{array} \qquad \begin{array}{r|l} 36 & 12 \\ \hline 0 & 3 \end{array}$$

Correção do Algoritmo de Euclides

- O algoritmo termina sempre e calcula mdc (m, n)
  $\hookrightarrow n > R_1 > R_2 > \dots > R_J \dots$
  - Teorema:
    $mdc(a,b) = mdc(b, (a,b))$
  - Divisão Inteira:

$$\begin{array}{l|l} a & b \\ \hline R & q \end{array}$$

$mdc(a,b) = mdc(b,R)$

$a = b \times q + R$

$0 \leq R < b$

1 $d \in C_1$

$a = b \times q \in \mathbb{N} + mod(a,b)$

$(R - k' \times q) d = mod(a,b)$

- Teorema:
  $m, n \in \mathbb{Z}$ não simultaneamente nulos
  Existem sempre $x, y \in \mathbb{Z}$ (designados coeficientes de Bézout) tais que $mdc(m,n) = x \times m + y \times n$

	a's	q's	x's	y's
$a_0 \to$	m		1	0 *
$a_1 \to$	n	q_1	0	1
	a_2	q_2		
	a_3		x_{j-2}	y_{j-2}
	...		x_{j-1}	y_{j-1}
	a_j	q_j	x_j	y_j
	a_k		x_k	y_k
	0			

$\to$ Objetivo:
Preencher as colunas x e y de forma que, em cada linha
$a_j = x_j \times m + y_j \times n$

$\Rightarrow$ $\begin{array}{l|l} a_{j-2} & a_{j-1} \\ \hline a_j & q \end{array}$

* sempre

Equações Diofantinas

- Coeficientes das variáveis e o termo independente são números inteiros e têm soluções inteiras.
- Lineares com 2 variáveis (c constante).
  exemplo:
  calças $\to$ 28 €
  tops $\to$ 8 €
  total $\to$ 100 €

  $28x + 8y = 100$

  - Soluções possíveis:
    $x = 1, y = 9$
    $x = 3, y = 2$

  alternativa:
  $\underbrace{28x}_{par} + \underbrace{8y}_{par} = \underbrace{135}_{ímpar} \Rightarrow$ impossível

- Encontrar soluções:
  $252x + 87x = 270$
  - Coeficientes de Bézout: $-10, 29$
  - $mdc(252, 87) = 3$

$\Rightarrow$ $270 = 3 \times 90$

$252 \times (-10) + 57 \times 29 = 3$

$\hookrightarrow 90(252 \times (-10) + 57 \times 29) = 270 \Leftrightarrow$

$\Leftrightarrow 252 \times (\underbrace{-900}_{x}) + 57 \times (\underbrace{2610}_{y}) = 270$

Soluções: $x = -900$
$y = 2610$

- $ax + by = c$ tem solução, se e só se c é múltiplo de $mdc(a,b)$.

1 hipótese: x_0 e y_0 são solução
$ax_0 + by_0 = c$ $\qquad$ $mdc(a,b)$ é divisor de a e b
$\hookrightarrow k_1 \, mdc(a,b) x_0 + k_2 \, mdc(a,b) y_0 = c$
$\hookrightarrow (k_1 x_0 + k_2 y_0) \, mdc(a,b) = c$

② hipótese: c é múltiplo de $mdc(a,b)$

u e v são coeficientes de Bézout por a e b

$$\downarrow$$

$$a \times u + b \times v = mdc(a,b)$$

$$\downarrow$$

$$a \times u \times k + b \times v \times k = c \qquad c = k \times mdc(a,b)$$

○ Se x_0 e y_0 são solução, x e y são solução se e só se:

$$\begin{cases} x = x_0 + \dfrac{b}{mdc(a,b)} \times k \\[2ex] y = y_0 - \dfrac{a}{mdc(a,b)} \times k \end{cases}$$

exemplo:

$$252x + 87y = 270$$

$\hookrightarrow$ $\left.\begin{array}{l} x_0 = -900 \\ y_0 = 2610 \end{array}\right\}$ soluções

Conjunto de todas as soluções:

$$\begin{cases} x = -900 + \dfrac{87}{3} \times k \\[2ex] y = 2610 - \dfrac{252}{3} \times k \end{cases} \Leftrightarrow \begin{cases} x = -900 + 29k \\ y = 2610 - 84k \end{cases}, \quad k \in \mathbb{Z}$$

$k = 0$:

$x = -900$; $y = 2610$

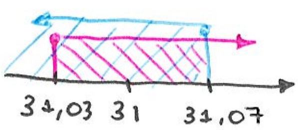
$k = 1$: $x = -871$

$y = 2526$ ...

Soluções não negativas:

$$\begin{cases} -900 + 29k \geq 0 \\ 2610 - 84k \geq 0 \end{cases} \Leftrightarrow \begin{cases} 29k \geq 900 \\ -84k \geq -2610 \end{cases} \Leftrightarrow \begin{cases} k \geq \dfrac{900}{29} \approx 31{,}03 \\[2ex] k \leq \dfrac{2610}{84} \approx 31{,}07 \end{cases}$$

$S = 31$



○ Primos Entre si

- m e n são primos entre si quando $mdc(m,n) = 1$

○ Mínimo Múltiplo Comum

- $a, b \in \mathbb{Z} \setminus \{0\}$
- O menor / mínimo múltiplo comum de a, b é o menor inteiro positivo que é múltiplo de a e b.

○ Congruência Módulo $n \in \mathbb{N}$:

- $a, b \in \mathbb{Z}$
- a é congruente módulo n com b se $a - b$ é múltiplo de n;
- Notação: $a \equiv_n b$
- Exemplos:

$23 \equiv_3 2$ porque $23 - 2 = 21$ é $\dot{3}$ $\qquad 23 \not\equiv_3 6$ " " $23 - 6 = 17$ ñ é $\dot{3}$

$23 \equiv_3 11$ " " $23 - 11 = 12$ é $\dot{3}$ $\qquad -5 \equiv_3 7$ " " $-5 - 7 = -12$ é $\dot{3}$

· Propriedades $(a, b \in \mathbb{Z},\ n \in \mathbb{N}_1)$

1. $a \equiv_n a$

   $a - a = 0$ é $\dot{n}$

2. se $a \equiv_n b$ então $b \equiv_n a$

3. se $a \equiv_n b$ e $b \equiv_n c$ então $a \equiv_n c$

   $a - c = (a-b) + (b-c) = (k_1 + k_2) \times n = \dot{n}$

4. $a \equiv_n \operatorname{mod}(a,n)$

   $$\begin{array}{r|l} a & n \\ \hline \operatorname{mod}(a,n) & q_1 \end{array} \rightarrow a = n \times q + \operatorname{mod}(a,n) \Leftrightarrow a - \operatorname{mod}(a,n) = n \times q = \dot{n}$$

5. Se $a \equiv_n a'$ e $b \equiv_n b'$, então:

   (i) $a + b \equiv_n a' + b'$

   (ii) $a \times b \equiv_n a' \times b'$

   (iii) $a^p \equiv_n (a')^p \quad p \in \mathbb{N}_1$

   (i) $(a+b) - (a' + b') = (a - a') + (b - b') = (k_1 + k_2) \times n = \dot{n}$

   (iii)

   $$a \equiv_n a' \xrightarrow{ii} a^2 \equiv_n (a')^2 \xrightarrow{ii} a^3 \equiv_n (a')^3 \ldots$$

6. $a, b, c \in \mathbb{Z} \setminus \{0\}$

   $a \times c \equiv_n b \times c$ se e só se $a \equiv_{\frac{n}{\operatorname{mdc}(c,n)}} b$

   $\hookrightarrow$ consequência:

   se c e n forem primos entre si:

   $a \times c \equiv_n b \times c$ se e só se $a \equiv_n b$

· m é múltiplo de 3 (divisível por 3) se e só se a soma dos seus dígitos é múltiplo de 3:

- $m = d_0 + d_1 \times 10 + d_2 \times 10^2 + d_n \times 10^n$
- $10 \equiv_3 1 \rightarrow 10^p \equiv_3 1^p$
- $d_i \equiv_3 d_i$, $10^i \equiv_3 1 \rightarrow d_i \times 10^i \equiv_3 d_i$
- $d_0 \equiv_3 d_0$
- $d_1 \times 10 \equiv_3 d_1$

  $\Big\rangle\ d_0 + d_1 \times 10 \equiv_3 d_0 + d_1 \rightarrow d_0 \times 1 + d_1 \times 10 + d_2 \times 10^2 \equiv_3 d_0 + d_1 + d_2$
- $m - d_0 + d_1 + \ldots + d_n = \underbrace{3k}_{\dot{3}} \Rightarrow m$ é $\dot{3} \Leftrightarrow d_0 + \ldots + d_n$ é $\dot{3}$

· Resolução de congruências

- $\alpha, \beta \in \mathbb{Z},\ n \in \mathbb{N}_2$
- $\alpha x \equiv_n \beta \rightarrow$ encontrar todos os valores de $x \in \mathbb{Z}$ que verifiquem a congruência
  - $5x \equiv_8 2$ $\quad \left.\begin{array}{l} x = 2 \\ x = 10 \end{array}\right\}$ caso simples (por inspeção)
  - caso geral:

    $\alpha x - \beta = nk \Leftrightarrow \alpha x - nk = \beta$

· Teorema

$\alpha x \equiv_n \beta$ tem solução se e só se β é múltiplo de $\operatorname{mdc}(\alpha, n)$

· exemplo: $132x \equiv_{15} 63 \rightarrow 132x - 15k = 63$

132		1	0
18	8	0	1
12	1	1	-8
3	4	-1	9
0			

$132(-1) + 15(9) = 3 \Leftrightarrow 132(-21) - 18(-189) = 63$

$x = -21 \rightarrow$ uma solução

$$x = x_0 + \frac{-n}{mdc(2,n)} - k$$

$$x = -21 - 5k = -16 - 5(k+1) = -16 - 5n$$

- Inverso Módulo ($n \in \mathbb{N}_1$)
  - Um inverso de α módulo n ($\alpha \in \mathbb{Z}$) é uma solução da congruência $\alpha x \equiv_n 1$
    - Notação: $\tilde{\alpha}$
    - exemplo: Inverso de 2 módulo 3

$$2x \equiv_3 1 \rightarrow 2x - 1 = 3n \Leftrightarrow 2x - 3n = 1$$

$x = 2$

$x = 8$

" " 4 " " 9

$$4x \equiv_9 1 \rightarrow 4x - 1 = 9n \Leftrightarrow 4x - 9n = 1$$

$x = -2$

- Teorema
  - α tem inverso módulo n se e só se 1 for múltiplo de $mdc(\alpha, n) = 1$ (α e n coprimos)
    - exemplo:

$$132x \equiv_{15} 63 \Leftrightarrow 12x \equiv_{15} 3 \qquad x = -1$$

$$\left.\begin{array}{l} 132 \equiv_{15} \bmod(132,15) = 12 \\ 63 \equiv_{15} \bmod(63,15) = 3 \end{array}\right\} 12 \equiv_{15} 3$$

- Teorema
  - $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}, n \in \mathbb{Z}$
  - Com $\alpha = n\alpha'$ e $\beta = n\beta'$ então por cada $x \in \mathbb{Z}$

    $\alpha x \equiv_n \beta$ se e só se $\alpha' x \equiv_n \beta'$ (têm exatamente as mesmas soluções)
  - Justificação:

$x \in \mathbb{Z}$

$\alpha x \equiv_n \beta \qquad \alpha x - nk = \beta \; k \in \mathbb{Z} \rightarrow (\alpha' + nk_1)x - nk = \beta' + nk_2$

$\hookrightarrow \alpha' x - \beta' = (-nk_1 x + nk + nk_2)$

$\hookrightarrow \alpha' x \equiv_n \beta'$

- Resolução de sistemas de congruências

$$x \in \mathbb{Z} \begin{cases} x \equiv_{m_1} k_1 \\ x \equiv_{m_2} k_2 \\ \vdots \\ x \equiv_{m_s} k_3 \end{cases}$$

- Teorema Chinês dos Restos
  - Sejam $m_1, m_2, \ldots, m_s \in \mathbb{N}_2$ com $mdc(m_1, m_2) = 1$, $i \neq j$ e $k_1, k_2, \ldots, k_s \in \mathbb{Z}$. Então o sistema:

$$\begin{cases} x \equiv_{m_1} k_1 \\ x \equiv_{m_2} k_2 \\ \vdots \\ x \equiv_{m_s} k_s \end{cases}$$

tem solução e o conjunto das soluções é dado por:

$$x_0 + Mt, \; t \in \mathbb{Z}$$

$M \rightarrow m_1 \times m_2 \times \cdots \times m_s$

$x_0 \rightarrow$ Solução Particular:

$$k_1 \underbrace{n_1}_{\frac{M}{m_1}} \underbrace{\tilde{n}_1}_{\text{inverso de } n_1 \text{ módulo } m_1} + k_2 n_2 \tilde{n}_2 + \ldots + k_s n_s \tilde{n}_s$$

- exemplo:

$$\begin{cases} x \equiv_3 1 \\ x \equiv_4 1 \\ x \equiv_7 4 \end{cases}$$

$\rightarrow$ Como $mdc(3,4) = mdc(4,7) = mdc(3,7) = 1$ podemos aplicar o TCR

$M = 3 \times 4 \times 7 = 84$

$$\left(1 \times \frac{84}{3} \times \tilde{n}_1 + 1 \times \frac{84}{4} \times \tilde{n}_2 + 4 \times \frac{84}{7} \times \tilde{n}_3\right) + 84t =$$

$\tilde{n}_1 \rightarrow 1 \qquad \tilde{n}_2 \rightarrow 1 \qquad \tilde{n}_3 \rightarrow 3$

$= (1 \times 28 \times 1 + 1 \times 21 \times 1 + 4 \times 12 \times 1) + 84t = 193 + 84t, t \in \mathbb{Z}$

- exemplo:

$$\begin{cases} x \equiv_5 1 \\ x \equiv_7 3 \\ x \equiv_9 5 \end{cases}$$

mdc(5,7) = mdc(7,9) = mdc(9,5) = 1, pelo que podemos usar o TCR

$x_0 + Mt = (1 \times 63 \times 7 + 3 \times 45 \times \underset{\text{ou } 5}{(-2)} + 5 \times 35 \times (-1)) + 315t =$

$M = 5 \times 7 \times 9 = 315$

$= (441 + (-270) - 175) + 315t = -4 + 315t, t \in \mathbb{Z}$

- exemplo:

$$\begin{cases} 2x \equiv_5 1 \\ 3x \equiv_9 6 \\ 8x \equiv_{14} 10 \end{cases} \Leftrightarrow \begin{cases} 2x \equiv_5 1 \\ x \equiv_{\underline{9}} 2 \\ \quad \text{mdc}(3,9) \\ 4x \equiv_{\underline{14}} 5 \\ \quad \text{mdc}(14,7) \end{cases} \Leftrightarrow \begin{cases} 2x \equiv_5 1 \\ x \equiv_3 2 \\ 4x \equiv_7 5 \end{cases}$$

$x = 3$

$x = 2$

$$\begin{cases} x \equiv_5 1 \times 3 = 3 \\ x \equiv_3 2 \\ x \equiv_7 5 \times 2 = 10 \end{cases} \Leftrightarrow \begin{cases} x \equiv_5 3 \\ x \equiv_3 2 \\ x \equiv_7 10 \end{cases}$$

- $\alpha x \equiv_n \beta \xrightarrow{\times \tilde{\alpha}} x \equiv_n \beta \tilde{\alpha}$

$\times \tilde{\alpha}$ (existe se mdc$(\alpha, n) = 1$)

- Dem:

$x \in \mathbb{Z}$

$\alpha x \equiv_n \beta$

$\downarrow \times \tilde{\alpha}$

$\tilde{\alpha} \alpha x \equiv_n \beta \tilde{\alpha} \rightarrow x \equiv_n \beta \tilde{\alpha}$

$1 \equiv_n \tilde{\alpha} \alpha$

$\downarrow$

$x \equiv_n \tilde{\alpha} \alpha x$

$\downarrow$

$x \equiv_n \beta \tilde{\alpha}$

> Nota:
> $\lfloor x \rfloor$ - maior inteiro menor ou igual a x

- Justificação do TCR
  1. x_0 é uma solução;
  2. Os inversos existem;
  3. $x_0 + Mt$, $t \in \mathbb{Z}$ é solução;
  4. Se y é solução, então y é da forma indicada;

Calendário Gregoriano / Perpétuo

- Juliano

1580º adiantado 10 dias

Anos Comuns - 365 dias

Anos Bissextos - 366

1 ano = 365,25 dias

- Gregoriano

1582 → 1600

anos séculos

Anos bissextos: $N \equiv_4 0 \wedge N \not\equiv_{100} 0$

ou

$N \equiv_{400} 0$, 4, 100

$\boxed{1}$ Calcular dia da semana de 1 de março do ano $N \geq 1600$

dias da semana: 0, 1, 2, 3, 4, 5, 6

Domingo (0) ... Sábado (6)

meses: 11 Janeiro, 12 Fevereiro | 1600 → 1 Março, 2 Abril, 3 Maio ... 10 Dezembro

exemplo: 11/03/2019 → 11/01/2019

17 fevereiro de 2015 → 17/12/2018

→ d_N - dia da semana de 1 de março de $N \geq 1600$:

$d_N \equiv_7 d_{1600} + \alpha$

α → nº de dias entre as 2 datas

d_{1600} → dia da semana de 1 de março de 1600

$$d_N \equiv_7 d_{1600} + \alpha \equiv_7 d_{1600} + (N-1600) + \left\lfloor \frac{N-1600}{4} \right\rfloor - \left\lfloor \frac{N-1600}{100} \right\rfloor + \left\lfloor \frac{N-1600}{400} \right\rfloor$$

- Se α for múltiplo de 7 (ou seja, $\alpha = \text{mod}(\alpha, 7) = 0$), então o dia N será no mesmo dia da semana.

α → 365 × nº de anos decorridos + 1 dia × nº de anos bissextos

(1 dia de 4 em 4 anos)(-1 ano de 100 em 100)

(+1 ano de 400 em 400)

$\rightarrow d_N \equiv_7 d_{1600} + (N-1600) + \left\lfloor \frac{N-1600}{4} \right\rfloor - \left\lfloor \frac{N-1600}{100} \right\rfloor + \left\lfloor \frac{N-1600}{400} \right\rfloor$

$N = 100 \times C + A$

(ex: $2015 = 20 \times 100 + 19$)

$\left\lfloor \frac{100C + A - 1600}{4} \right\rfloor = 25C + \left\lfloor \frac{A}{4} \right\rfloor - 400$

$\rightarrow d_N \equiv_7 d_{1600} + (100C + A - 1600) + 25 + \left\lfloor \frac{A}{4} \right\rfloor - 400 - C - \underbrace{\cancel{\left\lfloor \frac{A}{400} \right\rfloor}}_{=0} + 16 + \left\lfloor \frac{C}{4} \right\rfloor$

$-1600 - 400 - 16 - 4 = -1988 \equiv_7 \underbrace{\mathrm{mod}(1988,7)}_{=0}$

$100 + 25 - 1 = 124 \equiv \mathrm{mod}(124,7) = 8$

$d_N \equiv_7 d_{1600} + A + 5C + \left\lfloor \frac{A}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor$

$\rightarrow d_N \equiv_7 \underbrace{d_{1600}}_{?} + A + 5C + \left\lfloor \frac{A}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor$

N = 4 dígitos 1 de março de 2019 $\rightarrow 100 \times 20 + 19$
$\rightarrow$ foi uma 6ª feira (5)

$5 \equiv_7 d_{1600} + 19 + 5 \times 20 + \left\lfloor \frac{19}{4} \right\rfloor + \left\lfloor \frac{20}{4} \right\rfloor \equiv_7 d_{1600} + 2$

$19 + 100 + 4 + 5 = 128 \equiv_7 \mathrm{mod}(128,7) = 2$ $\hookrightarrow 5 - 2 = 3 \hookrightarrow$ foi numa 4ª feira

2 Generalização

Nº de dias de avanço da semana

$d_N \equiv_7 \cancel{3} + A + 5C + \left\lfloor \frac{A}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor + \boxed{\lfloor 2{,}6\,n - 0{,}2 \rfloor - \cancel{2}} + (k - \cancel{1})$

[$100 \times C + A$]

$\hookrightarrow$ ou $\left\lfloor \frac{13n - 1}{5} \right\rfloor - 2$ $n \rightarrow$ mês (março = 1, ...)

Nota:
$31 \equiv_7 3 \rightarrow$ 1 de março para 1 de abril há um adianto de 3 dias (de semana)

Exemplo: 1 de novembro de 1755 ($17 \times 100 + 55$)

1/9/1755

$d \equiv_7 \underbrace{55 + 5 \times 17 + \left\lfloor \frac{55}{4} \right\rfloor + \left\lfloor \frac{17}{4} \right\rfloor + \left\lfloor \frac{13 \times 9 - 1}{5} \right\rfloor + 1}_{181} \equiv_7 6$ $\hookrightarrow$ sábado

$181 \equiv_7 \mathrm{mod}(181,7) = 6$

$\boxed{d_N \equiv_7 A + 5C + \left\lfloor \frac{A}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor + \left\lfloor \frac{13n - 1}{5} \right\rfloor + \underset{\text{dia}}{k}}$

! meses começam em março !

∘ Generalização I do TCR

- Sejam $m_1, \ldots, m_s \in \mathbb{N}_2$, $k_1, \ldots, k_s \in \mathbb{Z}$ tais que $k_i - k_j$ é múltiplo de $\mathrm{mdc}(m_i, m_j)$, $i \neq j$, então o sistema:

$\begin{cases} x \equiv_{m_1} k_1 \\ x \equiv_{m_2} k_2 \\ x \equiv_{m_s} k_s \end{cases}$ tem soluções e o conjunto de todas as soluções é dado por:

$x = x_0 + Mt$

$M \hookrightarrow \mathrm{mmc}(m_1, \ldots, m_s)$

$x_0 \hookrightarrow k_{t_1} n_{t_1} \tilde{n}_{t_1} + k_{t_2} n_{t_2} \tilde{n}_{t_2} + \ldots + k_{t_s} n_{t_s} \tilde{n}_{t_s}$

$n_{t_1} \hookrightarrow \frac{M}{c_{t_1}}$

$1 < t_1 < t_2 < t_s < s$
- $\mathrm{mdc}(c_{t_1}, c_{t_2}, \ldots, c_{t_s}) = M$
- $\mathrm{mdc}(c_{t_i}, c_{t_j}) = 1$, $i \neq j$
- m_{t_i} múltiplo de c_{t_1}, $i = 1, \ldots, s$

exemplo:

$\begin{cases} x \equiv_3 2 \\ x \equiv_4 3 \\ x \equiv_{15} 14 \end{cases}$

$\mathrm{mdc}(3,4) = 1$ e $k_1 - k_2 = -1$ é $\dot{1}$
$\mathrm{mdc}(3,15) = 3$ e $k_1 - k_3 = 2 - 14 = 12$ é $\dot{3}$
$\mathrm{mdc}(4,15) = 1$ e $k_2 - k_3 = 11$ é $\dot{1}$

Nota:
$\mathrm{mmc}(a,b) = \frac{a \times b}{\mathrm{mdc}(a,b)}$

Logo, o conjunto de todas as soluções é:
$x = x_0 + Mt$, $t \in \mathbb{Z}$

3
$4 = 2^2$ $\Big\}\ \overset{c_1}{3} \times \overset{c_2}{2^2} \times \overset{c_3}{5} = 60$
$15 = 3 \times 5$

$\hookrightarrow \mathrm{mmc}(3,4,15) = 60$

$t_1 = 2$ $\quad c_2 = 4 \quad c_3 = 15$
$t_2 = 3$

mmc $(4,15) = 60$
mdc $(4,15) = 1$
m_2 é $\dot{c}_2$
m_3 é $\dot{c}_3$

$$x_0 = \underset{3}{k_2} \underset{\frac{60}{4}}{n_2} \tilde{n}_2 + \underset{14}{k_3} \underset{\frac{60}{15}}{n_3} \tilde{n}_3 = 3(15)(-1) + 14 \times 4 \times 4 = 179$$

Solução Geral: $x = 179 + 60t,\ t \in \mathbb{Z}$

- exemplo 2:

$$\begin{cases} x \equiv_4 1 \\ x \equiv_6 5 \\ x \equiv_7 4 \end{cases}$$

$\left.\begin{array}{lll} \text{mdc}(4,6) = 2 & \text{e} & 1-5 = -4 \text{ é } \dot{2} \\ \text{mdc}(4,7) = 1 & \text{e} & k_1 - k_2 \text{ é } \dot{1} \\ \text{mdc}(6,7) = 1 & \text{e} & k_2 - k_1 \text{ é } \dot{1} \end{array}\right\}$ logo, aplica-se o TCR

mmc $(4,6,7) = 84 \rightarrow \underset{c_1}{2^2} \times \underset{c_2}{3} \times \underset{c_3}{7}$

$t_1 = 1 \quad c_1 = 4$
$t_2 = 2 \quad c_2 = 3$
$t_3 = 3 \quad c_3 = 7$

mmc $(4,3,7) = 84$
mdc $(4,3) = 1$
mdc $(4,7) = 1$
mdc $(3,7) = 1$

$m_1 = 4$ é $\dot{c}_1 = 4$
$m_2 = 6$ é $\dot{c}_2 = 3$
$m_3 = 7$ é $\dot{c}_3 = 7$

$$x_0 = \underset{1}{k_1} \underset{\frac{84}{4}=21}{m_1} \tilde{m}_1 + \underset{5}{k_2} \underset{\frac{84}{3}=28}{m_2} \tilde{m}_2 + \underset{4}{k_3} \underset{\frac{84}{7}=12}{m_3} \tilde{m}_3 = 21 \times 1 + 5 \times 28 \times 1 + 4 \times 12 \times 3 = 305$$

$\tilde{m}_1 = 21x \equiv_4 1 \Leftrightarrow$	$\tilde{m}_2 = 28x \equiv_3 1 \Leftrightarrow$	$\tilde{m}_3 : 12x \equiv_7 1$
$\Leftrightarrow 21 \equiv_4 1 \Leftrightarrow$	$\Leftrightarrow 28 \equiv_3 1 \Leftrightarrow$	$\Leftrightarrow 12 \equiv_7 5$
$\Leftrightarrow x \equiv_4 1$	$\Leftrightarrow x \equiv_3$	$\frac{5x}{3} \equiv_7 1$

$x = 305 + 84t,\ t \in \mathbb{Z}$

○ Sistemas de Chave Pública

$\alpha \rightarrow \beta$
$\boxed{m}$

β 1 constrói:
- chave pública
- chave privada

β 2 Cria ou pública chave pública

α 3 Codifica c/ chave pública
$m \rightarrow m'$

α 4 Envia m' a β

β 5 $m' \rightarrow m$ descodifica com chave privada

○ Sistema RSA

Chave pública $\overset{\alpha \rightarrow \beta}{\boxed{m}}$
(n, a)
n: $p \times q$
p, q primos $\neq$
$a \in \mathbb{N} < (p-1)(q-1)$
mdc$(a, (p-1)(q-1)) = 1$

Chave Privada
(n, b)
$b \in \mathbb{N} < (p-1)(q-1)$
$a \times b \equiv_{(p-1)(q-1)} 1$

ESPAÇO DAS MENSAGENS	ENCRIPTAÇÃO	DESENCRIPTAÇÃO
$m \in \{0, 1, \dots, n-1\}$	$e(m) = \text{mod}(m^a, n)$	$d(m') = \text{mod}((m')^b, n)$

○ Correção do Sistema RSA

$\boxed{1}$ $d(e(m)) = m$

$\boxed{2}$ chave privada é de difícil cálculo conhecendo a chave pública

exemplos: $p = 11,\ q = 29$

1 - Explique a razão pela qual $(319, 13)$ pode ser uma chave pública no sistema RSA

$319 = 11 \times 29 \qquad (p-1)(q-1) = 10 \times 28 = 280$

$13 \in \mathbb{N} < 280 \qquad mdc(13, 280) = 1$

2. Calcule a chave privada correspondente

$(n, b) \qquad b < 280 \in \mathbb{N}$

$\downarrow \qquad a \times b \equiv_{280} 1 \rightarrow 13b \equiv_{280} 1 \qquad (319, 259)$

$(319, b)$

$13b - 280k = 1$

280		1	0
13	21	0	1
7	3	1	-21
0			

$n = -21 - 280k$

$k = -1$

$b = 259$

Matemática Discreta

Práticas

1. Calcular o número de divisores positivos

50	2
25	5
5	5
1	

$50 \rightarrow 2^1 \times 5^2 \rightarrow (1+1)\times(2+1) = 2\times 3 = 6$

2. Calcular os divisores positivos

$150 = 2^1 \times 5^2 \times 3^1$

5^0 5^1 5^2	1	5	25
2^1	2	10	50
3^1	3	15	75
	6	30	15

3. Calcular o número que tem x divisores positivos

nº div = 15 = 3×5 = 15×1 x, y, … tem de ser primo

15	15	3×5
(−1)	14	2, 4
	x^{14}	$x^4 \times y^2$

} substituir x, y

4. Calcular o máximo divisor comum

mdc (74, 44) = 2

Quocientes		1	1	1	7
	74	44	30	14	2
Restos	30	14	2	0	

$\rightarrow$ Máx Div Comum

↳ STOP

$\frac{74}{44}$ R = 30 Q = 1 $\frac{44}{30}$ R = 14 Q = 1 $\frac{30}{14}$ R = 2 Q = 2 $\frac{14}{2}$ R = 0 Q = 7

5. Coeficientes de Bézout mdc (2760, 17)

Restos	Quociente		
2760		1	0
17	−162	0	1
6	2		−162
5	1		324
1	5		−487
0			

colocar logo (sempre)

0 − 162×1

1 − 2 × (−162)

−162 − 1 × 324

6) Calcular mínimo múltiplo comum

mmc (20, 15, 45) = $(2^2\times 5,\ 3\times 5,\ 3^2\times 5)$

mmc (20, 15, 45) = $2^2\times 3^2\times 5$ → fatores de maior expoente

7) Equações Diofantinas → c múltiplo de mdc (a, b)

$\underset{ax}{252x} + \underset{by}{87x} = \underset{c}{270}$ mdc (252, 87) = 3

↳ Coeficientes de Bézout : −10, 29

$252\times(-10) + 57\times 29 = 3$

$90(252(-10) + 57\times 29) = 270$ (×90)

$252\times(-900) + 57\times(2610) = 270$

270 | 3

↳ = 90

Soluções Gerais:

$$x = x_0 + \frac{b}{mdc(a,b)} \times k \qquad \Rightarrow \qquad x = -900 + \frac{87}{3} \times k$$

$$y = y_0 - \frac{a}{mdc(a,b)} \times k \qquad \qquad y = 2610 - \frac{252}{3} \times k$$

8) Congruências - Resolver
(a-b é múltiplo de n $a \equiv_n b$)

$5x \equiv_8 2 \qquad \left.\begin{matrix} x=2 \\ x=10 \end{matrix}\right\}$ por inspeção

caso geral: $\alpha x \equiv_n \beta$ → tem sol se β é múltiplo de $mdc(\alpha, n)$

$\alpha x - \beta = nk \Leftrightarrow \alpha x - nk = \beta$

9) Inverso de módulo n

$2x \equiv_3 1 \rightarrow 2x - 1 = 3n \Leftrightarrow 2x - 3n = 1$

10) Teorema Chinês dos Restos

$mdc(m_1, m_2) = 1$

$$\begin{cases} x \equiv_{m_1} k_1 \\ x \equiv_{m_2} k_2 \\ \vdots \\ x \equiv_{m_s} k_s \end{cases} \longrightarrow \text{solução } x_0 + Mt$$

M → $m_1 \times m_2 \times \dots \times m_s$

x_0: $k_1 \underbrace{n_1}_{\frac{M}{m_1}} \tilde{n}_1 + k_2 n_2 \tilde{n}_2 + \dots$

Simplificar congruências:
1. Inverso módulo
2. $mod(u, \alpha)$

1) $10x \equiv_9 4$

$\tilde{\alpha}: 10x \equiv_9 1$

$x = 4$

$x \equiv_9 16 \; (4 \times 4)$

2) $mod(16, 9) = 7$

$x \equiv_9 7$

$$\frac{a}{c} \equiv_{\frac{n}{mdc(c,n)}} \frac{b}{c}$$

11) TCR - Generalização

$k_1 - k_2$ é $mdc(m_1, m_2)$

$$\begin{cases} x \equiv_{m_1} k_1 \\ x \equiv_{m_2} k_2 \\ x \equiv_{m_s} k_3 \end{cases} \qquad x = x_0 + Mt$$

M → $mmc(m_1, \dots, m_s)$

x_0: $k_1 \underbrace{n_1}_{\frac{M}{c_1}} \tilde{n}_1 + \dots +$

ex:
$$\begin{cases} x \equiv_5 2 \\ x \equiv_8 2 \\ x \equiv_{12} 10 \end{cases} \qquad mmc(5, 8, 12) = (5, 2^3, 2^2 \times 3) = \overset{c_1}{5} \times \overset{c_2}{2^3} \times \overset{c_3}{3}$$

$$\begin{cases} x \equiv_5 2 \\ x \equiv_8 2 \\ x \equiv_3 10 \end{cases} \quad \dots$$

12) Chave pública e privada com p e q

(n, a)
- n → $p \times q$
- a → $< (p-1)(q-1)$ $(mdc(a, (p-1)(q-1)) = 1)$ → escolher um qualquer

(n, b)
- → $IN < (p-1)(q-1)$

$a \times b \equiv_{(p-1)(q-1)} 1$
→ Resolver → algoritmo euclides e diofantinas

13

Encriptar: m = mensagem

$e(m) = mod(m^a, n)$

Desencriptar:

$d(m') = mod((m')^b, n)$

ex: $m = 453$

$mod(453^a, n)$

$mod(453^{17}, 2867) \rightarrow mod(453^{17}, 2867) \equiv_{2867} 453^{17}$

chave pública
↳ (2867, 17)

$\equiv_{2867} 453 \times 453^{16}$

$\equiv_{2867} 453 \times (453^2)^8$

$453^2 = 205209 \div 2867 = 71$

$205209 - (2867 \times 71) = 1652$

$\equiv_{2867} 453 \times (1652^2)^4$

$88597 \div 2867 = 30$

$88597 - (30 \times 2867) = 2587$

$\equiv_{2867} 453 \times (88597)^4$

$\equiv_{2867} 453 \times (2587)^4$

...

$\equiv_{2867} 1702$

Pequeno Teorema de Fermat

$x^p \equiv_p x$