

TEORIA DOS NÚMEROS

- DADOS $m, n \in \mathbb{R}$, DIZEMOS QUE m DIVIDE n OU n É DIVISÍVEL POR m SE $\frac{n}{m}$ É INTEIRO.

$$\hookrightarrow n \bmod m = 0$$

$$n = m \cdot k \text{ PARA ALGUM } k$$

n É MÚLTIPLO DE m

NOTAÇÃO: $m \mid n$

SE m NÃO DIVIDE n , DIZEMOS $m \nmid n$

$$\text{EX: } 2 \mid 6$$

$$\pi \mid 2\pi \rightarrow \text{TAMBÉM SE APLICA A NÚMEROS REAIS}$$

MAS EM GERAL VAMOS PENSAR EM INTEIROS

- O MAIOR DIVISOR COMUM DE DOIS INTEIROS m E n É

$$\text{MDC}(m, n) = \max \{ k : k \mid m \text{ E } k \mid n \}$$

$$\text{EX: } \text{MDC}(18, 12) = 6$$

$$\text{MDC}(0, n) = n$$

- O MENOR MÚLTIPLO COMUM DE DOIS NÚMEROS INTEIROS m E n É

$$\text{MMC}(m, n) = \min \{ k : m \mid k \text{ E } n \mid k \}$$

$$\text{EX: } \text{MMC}(18, 12) = 36$$

• ALGORITMO DE EUCLIDES: USA A SEGUINTE REL. DE RECORRÊNCIA

$$\text{MDC}(0, n) = n$$

PENSAMOS $n > m$

$$\text{MDC}(m, n) = \text{MDC}(n \bmod m, m) \quad m > 0$$

→ A RECORRÊNCIA VALE PORQUE TODO DIVISOR COMUM DE m E n É TAMBÉM UM DIVISOR COMUM DE m E $n \bmod m$.

$$\text{LEMOS QUE } n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor m$$

$$\text{EX: } \text{MDC}(12, 18) = \text{MDC}(6, 12) = \text{MDC}(0, 6) = 6$$

→ O ALGORITMO DE EUCLIDES NOS DÁ MAIS: É POSSÍVEL ENCONTRAR INTEIROS m' E n' TAIS QUE

$$m \cdot m' + n \cdot n' = \text{MDC}(m, n)$$

* SE $m = 0$, TOMAMOS $m' = 0$ E $n' = 1$ E TEMOS

$$m \cdot m' + n \cdot n' = n = \text{MDC}(m, n)$$

* SE $m > 0$, SEJA $r = n \bmod m$. TEMOS $r = n - \left\lfloor \frac{n}{m} \right\rfloor m$
POR "INDUÇÃO" EM $m + n$, EXISTEM r' E m'' TAIS QUE

$$r' \cdot r + m'' \cdot m = \text{MDC}(m, r)$$

COMO $r = n - \left\lfloor \frac{n}{m} \right\rfloor m$, TEMOS

$$\begin{aligned} \text{MDC}(n, m) &= \text{MDC}(m, r) = r' \cdot r + m'' \cdot m \\ &= r' \left(n - \left\lfloor \frac{n}{m} \right\rfloor m \right) + m'' \cdot m \\ &= r' \cdot n + \left(m'' - \left\lfloor \frac{n}{m} \right\rfloor r' \right) \cdot m \end{aligned}$$

ASSIM, TEMOS $n' = r'$ E $m' = m'' - \left\lfloor \frac{n}{m} \right\rfloor r'$

EX: $m = 12$ $n = 18$

TEMOS $\text{mdc}(12, 18) = \text{mdc}(6, 12) = \text{mdc}(0, 6) = 6$

• PELO CASO BASE, TEMOS $0 \cdot 0 + 1 \cdot 6 = 6$

• ASSIM, TEMOS $m_2 = m_1 = 0$ E $m_2 = m_1 - \left\lfloor \frac{12}{6} \right\rfloor \cdot 0 = 1$

• NOTE QUE $1 \cdot 6 + 0 \cdot 12 = 6$

• FINALMENTE, $m_3 = m_2 = 1$ E $m_3 = m_2 - \left\lfloor \frac{18}{12} \right\rfloor \cdot 1 = -1$

• PORTANTO $-1 \cdot 12 + 1 \cdot 18 = 6$

• MAS d É DE FATO O MAIOR DIVISOR COMUM DE m E n ?

• NOTE QUE SE d' É UM DIVISOR COMUM DE m E n , ENTÃO d' DEVE DIVIDIR $am + bn$ PARA TODO $a, b \in \mathbb{Z}$.

• LOGO d' DIVIDE $m' \cdot m + n' \cdot n = d$.

• ISSO IMPLICA QUE $d' \leq d$!

PROP: SE $K \mid m$ E $K \mid n$, ENTÃO $K \mid \text{mdc}(m, n)$

• ISSO IMPLICA QUE TODO DIVISOR COMUM DE m E n É DIVISOR DE d .

REGRA IMPORTANTE: $\sum_{m \mid n} a_m = \sum_{m \mid n} a_{m/n}$

• SEJA $K = \{m : m \mid n\}$. A FUNÇÃO $f: K \rightarrow K$ É BIJETIVA!

REGRA UM POUCO MAIS GERAL: $\sum_{m \mid n} a_m = \sum_k \sum_{m \geq 0} a_m [n = mk]$

SOMA DUPLA

PROP:
$$\sum_{m \mid n} \sum_{k \mid m} a_{k,m} = \sum_{k \mid n} \sum_{\ell \mid (n/k)} a_{k,k\ell}$$

PROVA: NO LADO ESQUERDO PODEMOS ESCRIVER

$$\sum_{j, \ell} \sum_{k, m > 0} a_{k,m} [m = jm] [m = k\ell] = \sum_j \sum_{\ell, k > 0} a_{k,k\ell} [m = jk\ell]$$

BASTA
TROCAR
 m E j

NO LADO DIREITO PODEMOS ESCRIVER

$$\sum_{j, m} \sum_{k, \ell > 0} a_{k,k\ell} [m = k\ell] \left[\frac{m}{k} = m\ell \right] = \sum_m \sum_{\ell, k > 0} a_{k,k\ell} [m = m\ell k]$$

NÚMEROS PRIMOS

- Um inteiro p é dito **PRIMO** se possui apenas dois divisores
 - ↳ OS DIVISORES SÃO 1 E p .
 - ↳ CONVENÇÃO: 1 NÃO É PRIMO

Primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

- Um número que não é primo é dito **COMPOSTO**
 - ↳ SÃO OS NÚMEROS QUE POSSUEM 3 OU MAIS DIVISORES
- TODO INTEIRO POSITIVO PODE SER ESCRITO COMO UM PRODUTO DE NÚMEROS PRIMOS.

EX: $12 = 2 \cdot 2 \cdot 3$

NOTAÇÃO: $m = p_1 \cdots p_m = \prod_{k=1}^m p_k \quad p_1 \leq \cdots \leq p_m$

↳ NOTAÇÃO ANALOGA A $\sum$ PARA PRODUTOS.

O PRODUTO DE ZERO TERMOS É CONVENÇIONADO SER 1

- ↳ SE m POSSUI UM DIVISOR m_1 , ENTÃO PODEMOS ESCRIVER $m = m_1 \cdot m_2$ E "POR INDUÇÃO" m_1 E m_2 PODEM SER ESCRITOS COMO PRODUTO DE PRIMOS. LOGO, m PODE SER ESCRITO COMO PRODUTO DE PRIMOS.

- PERGUNTA: ESSA EXPANSÃO É ÚNICA?
↳ OU FATORAÇÃO

EX: CONSIDERE O CONJUNTO DE NÚMEROS DO TIPO $a + b\sqrt{10}$ ONDE $a, b \in \mathbb{Z}$. NOTE QUE $6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$

TEOREMA FUNDAMENTAL DA ARITMÉTICA: TODO NÚMERO NATURAL ADMITE UMA ÚNICA FATORAÇÃO

PROVA: INDUÇÃO EM n . CERTAMENTE VALE PARA $n=1$.

SEJA $n > 1$ E QUE TODO $m' < n$ FATORA DE FORMA ÚNICA
SUPONHA QUE n TENHA DUAS FATORAÇÕES $\hookrightarrow$ H.I.

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_k \text{ com } p_1 \leq \dots \leq p_m, q_1 \leq \dots \leq q_k$$

PRIMOS

SUPONHA QUE $p_1 < q_1$. COMO p_1 E q_1 SÃO PRIMOS,
TEMOS $\text{mdc}(p_1, q_1) = 1$.

PELO ALGORITMO DE EUCLIDES, EXISTEM $a, b \in \mathbb{Z}$ T.q

$$ap_1 + bq_1 = 1$$

LOGO, TEMOS $ap_1 \cdot q_2 \cdot \dots \cdot q_k + bq_1 \cdot q_2 \cdot \dots \cdot q_k = q_2 \cdot \dots \cdot q_k$

NOTE QUE p_1 DIVIDE TANTO $ap_1 \cdot q_2 \cdot \dots \cdot q_k$ QUANTO $bq_1 \cdot q_2 \cdot \dots \cdot q_k$
LOGO, p_1 DIVIDE $q_2 \cdot \dots \cdot q_k$

ISSO IMPLICA QUE $q_2 \cdot \dots \cdot q_k / p_1$ É INTEIRO

$\hookrightarrow$ PELA H.I.

NOTE QUE $q_2 \cdot \dots \cdot q_k / p_1 < n$. LOGO, HÁ UMA ÚNICA FATORAÇÃO

$$q_2 \cdot \dots \cdot q_k / p_1 = q'_1 \cdot \dots \cdot q'_r$$

ISSO IMPLICA QUE HÁ UMA FATORAÇÃO DE $q_2 \cdot \dots \cdot q_k$ CONTENDO p_1
MAS, COMO $q_2 \cdot \dots \cdot q_k < n$, SUA FATORAÇÃO É ÚNICA.

ISSO CONTRADIZ O FATO QUE $p_1 < q_1 \leq q_2 \leq \dots \leq q_k$.

$\hookrightarrow$ H.I.

LOGO, TEMOS $p_1 = q_1$.

NOVAMENTE, $p_2 \cdot \dots \cdot p_m = q_2 \cdot \dots \cdot q_k < n$ POSSUI UMA ÚNICA FATORAÇÃO, O QUE IMPLICA $p_i = q_i \quad \forall i$ E $m = k$.

- TAMBÉM É INTERESSANTE ESCREVER

$$n = \prod_{p \text{ PRIMO}} p^{m_p}, \text{ ONDE } m_p \geq 0$$

→ PRODUTO DE TODOS OS PRIMOS (A MAIORIA DOS m_p 'S É NULA)

- PODEMOS PENSAR NA SEQUÊNCIA $\langle m_2, m_3, m_5, \dots \rangle$ COMO UM SISTEMA NUMÉRICO PARA INTEIROS POSITIVOS

EX: A REPRESENTAÇÃO DE 12 É $\langle 2, 1, 0, 0, \dots \rangle$

18 É $\langle 1, 2, 0, 0, \dots \rangle$

- MULTIPLICAR DOIS NÚMEROS É EQUIVALENTE A SOMAR SUAS REPRES.

$$K = m \cdot n \iff K_p = m_p + n_p \text{ PARA TODO } p$$

É

$$m \mid n \iff m_p \leq n_p \text{ PARA TODO } p$$

- OBTENEMOS IMEDIATAMENTE QUE

$$K = \text{mdc}(m, n) \iff K_p = \text{MIN}(m_p, n_p)$$

$$K = \text{mmc}(m, n) \iff K_p = \text{MAX}(m_p, n_p)$$

$$\text{EX: } \text{mdc}(12, 18) = 2^{\text{MIN}(2,1)} \cdot 3^{\text{MIN}(1,2)} = 2 \cdot 3 = 6$$

$$\text{mmc}(12, 18) = 2^{\text{MAX}(2,1)} \cdot 3^{\text{MAX}(1,2)} = 2^2 \cdot 3^2 = 36$$

EXEMPLOS DE PRIMOS

PERGUNTA: QUANTOS PRIMOS EXISTEM?

→ INFINITOS

PROVA: SUPONHA QUE EXISTE UM NÚMERO FINITO DE PRIMOS,
DIGAMOS $2, 3, \dots, p_k$.

CONSIDERE O NÚMERO $M = 2 \cdot 3 \cdot \dots \cdot p_k + 1$

COMO TODOS OS PRIMOS DIVIDEM $M-1$,
ELES NÃO PODEM DIVIDIR M . LOGO M É PRIMO. CONTRADIÇÃO $\square$

NÚMEROS DE EUCLIDES

• NÚMEROS DEFINIDOS PELA RELAÇÃO DE RECORRÊNCIA

$$e_n = e_1 \cdot \dots \cdot e_{n-1} + 1, \text{ quando } n \geq 1$$

$$\rightarrow e_1 = 1 + 1 = 2$$

$$e_2 = 2 + 1 = 3$$

$$e_3 = 2 \cdot 3 + 1 = 7$$

$$e_4 = 2 \cdot 3 \cdot 7 + 1 = 43$$

→ SÃO SEMPRE PRIMOS?

$$\rightarrow e_5 = 1807 = 13 \cdot 139$$

ORS: e_6 É PRIMO, MAS $e_7, \dots, e_{17}$ NÃO SÃO

→ OS NÚMEROS DE EUCLIDES SÃO PRIMOS ENTRE SI!

→ ISTO É $\text{mdc}(e_m, e_n) = 1$

→ NÃO POSSUEM
FATOR PRIMO COMUM

PROP: OS NÚMEROS DE EUCLIDES SÃO PRIMOS ENTRE SI.

PROVA: USAMOS O ALGORITMO DE EUCLIDES:

SEJAM e_m E e_n DOIS NÚMEROS DE EUCLIDES, COM $n > m$.

LOGO $e_n = e_1 \cdot \dots \cdot e_m \cdot \dots \cdot e_{n-1} + 1$ E, PORTANTO, $e_n \bmod e_m = 1$.

ASSIM, $\text{mdc}(e_m, e_n) = \text{mdc}(1, e_m) = \text{mdc}(0, 1) = 1$. $\square$

PERGUNTA: HÁ UMA FÓRMULA FECHADA P/ OS NÚMEROS DE EUCLIDES?

$$e_n = e_1 \cdot \dots \cdot e_{n-2} \cdot e_{n-1} + 1$$

$$= (e_{n-1} - 1) \cdot e_{n-1} + 1$$

$$= e_{n-1}^2 - e_{n-1} + 1$$

NÚMEROS DE MERSENNE: $2^p - 1$, COM p PRIMO

↳ NEM SEMPRE É PRIMO:

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

MAIOR PRIMO CONHECIDO: $2^{216091} - 1$

DEF: DADO $x \in \mathbb{N}$, DENOTAMOS POR $\pi(x)$ O NÚMERO DE PRIMOS MENORES OU IGUAIS A x .

$$\leadsto \text{TEMOS } \pi(x) \sim \frac{x}{\ln x}$$

PRIMOS GÊMEOS: ÍMPARES CONSECUTIVOS E PRIMOS

PARES DE NÚMEROS PRIMOS DO TIPO p E $p+2$.

FATORES FATORIAIS

$$n! = 1 \cdot 2 \cdot \dots \cdot n = \prod_{k=1}^n k$$

→ ISSO IMPLICA QUE $0! = 1$

• $n!$ É O NÚMERO DE PERMUTAÇÕES DE n OBJETOS DISTINTOS

• $10! \approx \frac{3}{2}$ MILHÕES

• O NÚMERO DE DÍGITOS EM $n!$ É MAIOR QUE n QUANDO $n \geq 25$

• $n!$ É BASTANTE GRANDE:

$$n!^2 = (1 \cdot \dots \cdot n)(1 \cdot \dots \cdot n) = \prod_{k=1}^n k(n+1-k)$$

→ COMO O POLINÔMIO $k(n+1-k) = \frac{1}{4}(n+1)^2 - (k - \frac{1}{2}(n+1))^2$ ATINGE O MÍNIMO EM $k=1$ E MÁXIMO EM $k = \frac{1}{2}(n+1)$, TEMOS

$$n \leq k(n+1-k) \leq \frac{1}{4}(n+1)^2$$

O QUE IMPLICA EM

$$\prod_{k=1}^n n \leq n!^2 \leq \prod_{k=1}^n \frac{(n+1)^2}{4}$$

OU SEJA

$$n^{\frac{n}{2}} \leq n! \leq \frac{(n+1)^n}{2^n}$$

OU TAMBÉM

$$2^{\frac{n}{2} \log n} \leq n! \leq 2^{n(\log(n+1) - 1)}$$

$n!$ CRESCE EXPONENCIALMENTE

FÓRMULA DE STIRLING: $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$

• DADO PRIMO p , QUAL A MAIOR POTÊNCIA DE p QUE DIVIDE $n!$?

→ QUEREMOS O EXPOENTE DE p NA FATORAÇÃO DE $n!$

→ DENOTAMOS ESTE NÚMERO POR $e_p(n!)$

EX: $e_2(10!)$

	1	2	3	4	5	6	7	8	9	10	
DIVISÍVEL POR 2		X		X		X		X		X	$5 = \lfloor 10/2 \rfloor$
DIVISÍVEL POR 4				X				X			$2 = \lfloor 10/4 \rfloor$
DIVISÍVEL POR 8								X			$1 = \lfloor 10/8 \rfloor$
											8

→ PARA n GERAL ISSO DÁ

$$e_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + \dots = \sum_{k \geq 1} \left\lfloor \frac{n}{2^k} \right\rfloor$$

EX: $e_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$

EM BINÁRIO

$$\begin{aligned} (1100100)_2 &= 100 \\ (110010)_2 &= 50 \\ (11001)_2 &= 25 \\ (1100)_2 &= 12 \\ (110)_2 &= 6 \\ (11)_2 &= 3 \\ (1)_2 &= 1 \end{aligned}$$

OBS: $e_2(n!) = n - \nu_2(n)$, ONDE $\nu_2(n)$ É O NÚMERO DE 1'S NA REPRESENTAÇÃO BINÁRIA DE n .

ISSO ACONTECE PORQUE CADA 1 CONTRIBUI COM 2^m EM $n!$, PARA ALGUM m , E ENTÃO CONTRIBUI COM

$$2^{m-1} + 2^{m-2} + \dots + 2^0 = 2^m - 1 \text{ EM } e_2(n!)$$

• GENERALIZANDO :

$$e_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

⇒ NOTE QUE $e_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \dots$

$$= \frac{n}{p} \left(1 + \frac{1}{p} + \dots \right) = \frac{n}{p} \left(\frac{p}{p-1} \right) = \frac{n}{p-1}$$

⇒ DE FATO, NOTE QUE $v_2(n) \leq \lceil \log n \rceil$

↳ ASSINTOTICAMENTE MUITO MENOR QUE n .

• LOGO, TEMOS $p^{e_p(n!)} < p^{\frac{n}{p-1}}$

↳ CONTRIBUIÇÃO DE p EM $n!$

⇒ COMO $p \leq 2^{p-1}$, TEMOS $p^{e_p(n!)} < p^{\frac{n}{p-1}} \leq 2^n$

↳ A CONTRIBUIÇÃO DE QUALQUER PRIMO EM $n!$ É MENOR QUE 2^n

• PODEMOS OBTER UMA COTA PARA $\pi(n)$.

COMO CADA PRIMO CONTRIBUI COM MENOS DO QUE 2^n , TEMOS

$$n! = \prod_{\substack{p \text{ PRIMO} \\ p \leq n}} p^{e_p(n!)} < \prod_{\substack{p \text{ PRIMO} \\ p \leq n}} 2^n = 2^{n\pi(n)}$$

PRIMOS ENTRE SI

- DOIS NÚMEROS m E n SÃO DITOS **PRIMOS ENTRE SI** SE $\text{mdc}(m,n)$

DIZEMOS TAMBÉM QUE m É PRIMO EM RELAÇÃO A n

NOTAÇÃO: $m \perp n$

- UMA FRAÇÃO m/n ESTÁ EM SUA FORMA MAIS SIMPLES SE $m \perp n$

⇒ EM PARTICULAR, TEMOS $\frac{m}{\text{mdc}(m,n)} \perp \frac{n}{\text{mdc}(m,n)}$

⇒ QUANDO USAMOS A REPRESENTAÇÃO EM EXPONENTES PRIMOS

$$m = \langle m_2, m_3, m_5, \dots \rangle$$

$$n = \langle n_2, n_3, n_5, \dots \rangle$$

É FÁCIL VER QUE $m \perp n$ SE $\min(m_p, n_p) = 0 \quad \forall p$
↳ EQUIV. A $m_p \cdot n_p = 0$

PROP: $K \perp m$ E $K \perp n \iff K \perp m \cdot n$

PROVA: TEMOS $K_p \cdot m_p = K_p \cdot n_p$ PARA TODO p .

ENTÃO, DADO p PRIMO TEMOS $K_p = 0$ OU $m_p = n_p = 0$

NOS DOIS CASOS TEMOS $K_p(m_p + n_p) = 0$.

COMO $m \cdot n = \langle m_2 + n_2, m_3 + n_3, \dots \rangle$, TEMOS $K \perp m \cdot n$.

PROP: SE p É PRIMO, ENTÃO $\sqrt{p}$ É IRRACIONAL.

PROVA: SUPONHA QUE $\sqrt{p} = \frac{a}{b}$ COM $a, b \in \mathbb{N}$ E $a \perp b$.

TEMOS $p = a^2/b^2$, O QUE IMPLICA $a^2 = pb^2$.

COMO $p \nmid pb^2$, TEMOS $p \nmid a^2$, O QUE IMPLICA $p \nmid a$. LOGO $a = p \cdot a'$

SUBSTITUINDO, TEMOS $pb^2 = a^2 = a'^2 p^2$. LOGO $b^2 = pa'^2$.

COMO $p \nmid pa'^2$, TEMOS $p \nmid b^2$, O QUE IMPLICA $p \nmid b$, E $\text{mdc}(a,b) \geq p$.

CONTRADIÇÃO COM $a \perp b$.

MOD: A RELAÇÃO DE CONGRUÊNCIA

- DEFINIMOS MOD COMO O RESTO DE UMA DIVISÃO.

$$m \text{ MOD } n = m - \left\lfloor \frac{m}{n} \right\rfloor n$$

- VAMOS USAR UMA NOTAÇÃO DIFERENTE:

$$a \equiv b \pmod{m} \iff a \text{ MOD } m = b \text{ MOD } m$$

↓
TEMOS a É CONGRUENTE A b MÓDULO m

Ex: $9 \equiv -16 \pmod{5}$ pois $9 \text{ MOD } 5 = 4 = -16 \text{ MOD } 5$
↳ $-20 + 4$

- COMO $x \text{ MOD } m$ DIFERE DE x POR UM MÚLTIPLO DE m $\left(\left\lfloor \frac{x}{m} \right\rfloor m\right)$
TEMOS $a \equiv b \pmod{m} \iff a - b$ É UM MÚLTIPLO DE m

NADE FATO, TEMOS $a = k_a \cdot m + a'$ E $b = k_b \cdot m + b'$
ONDE $k_a = \left\lfloor \frac{a}{m} \right\rfloor$ E $a' = a \text{ MOD } m$ E $k_b = \left\lfloor \frac{b}{m} \right\rfloor$ E $b' = b \text{ MOD } m$

ASSIM, $a - b = k_a m + a' - k_b m - b' = (k_a - k_b)m + (a' - b')$

SE $a' = a \text{ MOD } m = b \text{ MOD } m = b'$, TEMOS $a - b = (k_a - k_b)m$.

- A RELAÇÃO DE CONGRUÊNCIA É UMA RELAÇÃO DE EQUIVALÊNCIA.

- REFLEXIVA: $a \equiv a$
- SIMÉTRICA: $a \equiv b \implies b \equiv a$
- TRANSITIVA: $a \equiv b$ E $b \equiv c \implies a \equiv c$

OPERAÇÕES

• SOMA

$$a \equiv b \text{ e } c \equiv d \Rightarrow \begin{matrix} a+c \equiv b+d \\ a-c \equiv b-d \end{matrix} \pmod{m}$$

DE FATO, SE $a-b$ E $c-d$ SÃO MÚLTIPLOS DE m , ENTÃO

$$(a-b) + (c-d) \text{ e } (a-b) - (c-d) \text{ SÃO MÚLTIPLOS DE } m.$$

• MULTIPLICAÇÃO POR ELEMENTOS CONGRUENTES

$$a \equiv b \text{ e } c \equiv d \Rightarrow ac \equiv bd \pmod{m} \quad b, c \text{ INTEIROS}$$

$$ac - bd = \underbrace{(a-b)c}_{\text{MÚLTIPLO DE } m} + b \underbrace{(c-d)}_{\text{MÚLTIPLO DE } m}$$

• POTÊNCIAS

$$a \equiv b \Rightarrow a^n \equiv b^n \pmod{m} \quad n \geq 0 \text{ INTEIRO}$$

EX: COMO $2 \equiv -1 \pmod{3}$, TEMOS $2^m \equiv (-1)^m \pmod{3}$ E, PORTANTO

$$2^m - 1 \text{ É MÚLTIPLO DE } 3 \iff m \text{ É PAR}$$

• DIVISÃO : $ad \equiv bd \pmod{m}$ NÃO IMPLICA QUE $a \equiv b$

$$\text{EX: } 3 \cdot 2 \equiv 5 \cdot 2 \pmod{4} \quad \text{MAS } 3 \not\equiv 5$$

$\leadsto$ MAS ISSO VALE QUANDO $d \perp m$:

$$ad \equiv bd \iff a \equiv b \pmod{m} \quad a, b, d, m \text{ INTEIROS } d \perp m$$

EX: SE $15 \equiv 35 \pmod{m}$, ENTÃO $3 \equiv 7$, EXCETO SE m É MÚLTIPLO DE 5

Prop: Sejam d e m inteiros primos entre si. Então

$$ad \equiv bd \pmod{md} \iff a \equiv b \pmod{m}$$

Prova: Como $d \perp m$, temos $\text{mdc}(d, m) = 1$ e, portanto, existem d' e m' t.q.

$$d' \cdot d + m' \cdot m = 1 \implies d'd \equiv 1$$

Se $ad \equiv bd$, podemos multiplicar ambos os lados por d' , obtendo

$$add' \equiv bdd'$$

Multip. por a e b
nos dois lados

Como $d'd \equiv 1$, temos $add' \equiv a$ e $bdd' \equiv b$ □

↗ O número d' funciona como $1/d$:

↳ Dizemos que d' é o **inverso de d** .

• **DIVISÃO TAMBÉM DA BASE**

$$ad \equiv bd \pmod{md} \iff a \equiv b \pmod{m}, \quad d \neq 0$$

↗ Também vale para a, b, d, m reais

↗ Vale porque $(a \bmod m)d = ad \bmod md$

MUDANÇA DE BASE

SE TEMOS $a \equiv b \pmod{100}$ $\Rightarrow a-b$ É MÚLTIPLO DE 100
ENTÃO TEMOS $a \equiv b \pmod{10}$ $\Rightarrow a-b$ É MÚLTIPLO DE 10
 $\hookrightarrow$ ou QUALQUER DIVISOR DE 100.

$\Rightarrow$ EM GERAL, $a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod{m}$ d INTEIRO

$\Rightarrow$ PODEMOS MUDAR PARA UMA BASE MAIOR? SIM.

$$a \equiv b \pmod{m} \quad \text{e} \quad a \equiv b \pmod{n}$$

$\Leftrightarrow$

$$a \equiv b \pmod{\text{MMC}(m,n)}$$

$m, n > 0$ INTEIROS

EX: $a \equiv b \pmod{12}$ e $18 \Rightarrow a \equiv b \pmod{36}$

PROVA: $a-b$ É MÚLTIPLO TANTO DE m QUANTO DE n ,
ENTÃO É MÚLTIPLO DE $\text{MMC}(m,n)$.

$\Rightarrow$ QUANDO $m \perp n$, TEMOS $\text{MMC}(m,n) = m \cdot n$.

$$\text{EX: } a \equiv b \pmod{100} \Leftrightarrow a \equiv b \pmod{25} \text{ e } a \equiv b \pmod{4}$$

$\Rightarrow$ AS BASES m E n PODEM CONTINUAR SENDO DIVIDIDAS ATÉ QUE TODOS OS PRIMOS SEJAM ISOLADOS:

$$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{p^{m_p}} \quad \forall p$$

$$\text{SE } m = \prod_{p \text{ PRIMO}} p^{m_p}$$

RESÍDUOS

→ SISTEMA NÚMÉRICO RESIDUAL

• $\text{Res}(x) = (x \bmod m_1, \dots, x \bmod m_r)$ ONDE $m_j \perp m_k, 1 \leq j < k \leq r$.

→ CONHECER $\text{Res}(x)$ NÃO SIGNIFICA CONHECER TUDO SOBRE x ,
MAS SIGNIFICA CONHECER $x \bmod m$, ONDE $m = m_1 \cdots m_r$.

EX: SISTEMA NÚMÉRICO RESIDUAL COM DUAS BASES : 3 E 5

$x \bmod 15$	$x \bmod 3$	$x \bmod 5$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2
8	2	3
9	0	4
10	1	0
11	2	1
12	0	2
13	1	3
14	2	4

→ CADA PAR ORDENADO $(x \bmod 3, x \bmod 5)$ APARECE EXATAMENTE
UMA VEZ, JÁ QUE $x \bmod 3 = y \bmod 3$ E $x \bmod 5 = y \bmod 5$
IMPLICA QUE $x \bmod 15 = y \bmod 15$.

- AS OPERAÇÕES DE SOMA, SUBTRAÇÃO, E MULTIPLICAÇÃO PODEM SER FEITAS INDEPENDENTEMENTE NO RESÍDUO:

EX: SE QUISERMOS MULTIPLICAR $7 = (1, 2)$ POR $13 = (1, 3)$ MÓDULO 15
 BASTA CALCULAR $1 \cdot 1 \text{ MOD } 3 = 1$ E $2 \cdot 3 \text{ MOD } 5 = 1$.
 OBTÉMOS $(1, 1) = 1$ MÓDULO 15. ISTO É $7 \cdot 13 = 1 \pmod{15}$

- COMO OBTER $z \text{ MOD } m$ A PARTIR DE $\text{RES}(x)$?

→ SABEMOS QUE $z = (x, y)$ PARA ALGUM x E y
 ENTÃO PODEMOS ESCREVER $z = x \underbrace{(1, 0)}_a + y \underbrace{(0, 1)}_b$

NO CASO MÓDULO 15, SABEMOS QUE $a = 10$ E $b = 6$
 $\Rightarrow z \equiv 10x + 6y \pmod{15}$

PERGUNTA: COMO ENCONTRAR a E b QUANDO m E n SÃO GRANDES?

PROBLEMA: QUANTAS SOLUÇÕES EXISTEM PARA A RELAÇÃO DE CONGRUÊNCIA

$$x^2 \equiv 1 \pmod{m}$$

OBS: DUAS SOLUÇÕES x, x' SÃO IGUAIS SE $x \equiv x'$.

- CONSIDERE INICIALMENTE O CASO NO QUAL $m = p^k$.
 A RELAÇÃO PODE SER ESCRITA COMO

$$x^2 - 1 \equiv 0 \iff (x+1)(x-1) \equiv 0 \pmod{p^k}$$

ISSO SÓ ACONTECE SE $p^k \mid (x+1)$ OU $p^k \mid (x-1)$. (OU DIVIDE AMBOS)
 SE $p \geq 2$, ISSO NOS DÁ EXATAMENTE DUAS SOLUÇÕES: $x \equiv 1$ E $x \equiv -1$

APENAS
QUANDO $p=2$

SE $p=2$ E $p^k \mid (x-1)(x+1)$, ENTÃO UM ENTRE $(x-1)$ E $(x+1)$ É PAR,
 MAS NÃO É MÚLTIPLO DE 4. LOGO, O OUTRO É MÚLTIPLO DE 2^{k-1} .
 ISSO NOS DÁ QUATRO SOLUÇÕES: $x \equiv \pm 1$ E $x \equiv 2^{k-1} \pm 1$

→ No caso $p^k=8$, as quatro soluções são $1, 3, 5, 7 \pmod{8}$

→ Isso nos diz que o quadrado de qualquer número ímpar é da forma $8m+1$

No caso geral sabemos que $x^2 \equiv 1 \pmod{m}$ se e somente se $x^2 \equiv 1 \pmod{p^{m_p}}$ para todos primos com $m_p > 0$.

Cada primo é independente dos outros e possuem exatamente duas soluções (exceto para $p=2$).

Logo, se m tem exatamente r divisores primos, o número total de soluções de $x^2 \equiv 1 \pmod{m}$ é 2^r , exceto se m for par

→ O número certo é $2^{r + [8|m] + [4|m] - [2|m]}$

PROPOSIÇÃO: Os m números

$$0 \pmod{m}, m \pmod{m}, 2m \pmod{m}, \dots, (m-1)m \pmod{m}$$

consistem em precisamente d cópias dos m/d números

$$0, d, 2d, \dots, m-d$$

em alguma ordem, onde $d = \text{mdc}(m, m)$

PROVA: Pelo alg. de Euclides temos $n' \in m'$ t.q. $m' \cdot n + m' \cdot m = d$
seja $j \in \{0, \dots, m-1\}$ t.q. $j \equiv m' \pmod{m}$

Note que $m' \cdot n \equiv d \pmod{m}$, logo $j \cdot n \equiv d \pmod{m}$

Além disso para cada $i \in \{0, \dots, \frac{m}{d}-1\}$, temos $i \cdot j \cdot n \equiv i \cdot d \pmod{m}$

Isso mostra que todos os $i \cdot d$'s aparecem. $i' \in \{0, \dots, m-1\}$

→ Fixe i . Para cada $k \in \{1, \dots, d\}$ tome

$$(i + k \frac{m}{d}) \cdot n \equiv i \cdot j \cdot n + k \frac{m \cdot n}{d} \equiv i \cdot j \cdot n \pmod{m}$$

TEOREMA DE WILSON

$$(n-1)! \equiv -1 \pmod{n} \Leftrightarrow n \text{ é PRIMO}$$

PROVA: $(\Rightarrow)$ SE $(n-1)! \equiv -1 \pmod{n}$, ENTÃO n É PRIMO:

SE n NÃO É PRIMO, ENTÃO $n = m \cdot k$ PARA $m, k \leq n$.
EM PARTICULAR $m, k \leq n-1$, O QUE IMPLICA QUE m E k
SÃO FATORES DE $(n-1)!$.

ENTÃO $(n-1)!$ É MÚLTIPLO DE n . LOGO $(n-1)! \equiv 0 \pmod{n}$

$(\Leftarrow)$ SE n É PRIMO, ENTÃO $(n-1)! \equiv -1 \pmod{n}$

SEJA m T.q. $m \perp n$, PELO ALG. DE EUCLIDES, EXISTEM m' E n'
T.q.

$$m' \cdot m + n' \cdot n = 1$$

LOGO, $m' \cdot m \equiv 1 \pmod{n}$. ISSO É, m' É INVERSO DE m .

ALÉM DISSO, CADA NÚMERO POSSUI APENAS UM INVERSO.

PODEMOS EMPARELHAR CADA NÚMERO COM SEU INVERSO

EX: $n = 13$

$$(13-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv 12 \equiv -1 \pmod{13}$$

$$\begin{aligned} m \cdot m' &\equiv m \cdot m'' \\ m' \cdot m \cdot m' &\equiv m' \cdot m \cdot m'' \\ m' &\equiv m'' \end{aligned}$$

COMO 1 E $(n-1)$ SÃO SEUS PRÓPRIOS INVERSO, TEMOS

$$(n-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{n}.$$

□

OPS: SE x É SEU PRÓPRIO INVERSO, ENTÃO $x^2 \equiv 1 \pmod{p}$
VIMOS QUE ISSO SÓ OCEE QUANDO $x \equiv 1$ OU $x \equiv -1$.

PEQUENO TEOREMA DE FERMAT

SE p É PRIMO, ENTÃO $m^{p-1} \equiv 1 \pmod{p}$

PROVA: COMO $m \not\equiv 0 \pmod{p}$, PELA PROPOSIÇÃO OS NÚMEROS

$m \pmod{p}, 2m \pmod{p}, \dots, (p-1)m \pmod{p}$

SÃO OS NÚMEROS $1, 2, \dots, p-1$ EM ALGUMA ORDEM.

MULTIPLICANDO TODOS ESSES NÚMEROS OBTÉMOS

$$\begin{aligned} m \cdot (2m) \cdot \dots \cdot (p-1)m &= (p-1)! \cdot m^{p-1} \\ &\equiv (p-1)! \pmod{p} \end{aligned}$$

COMO $(p-1)!$ NÃO É DIVISÍVEL POR p , HÁ a, b T.q.

$$a(p-1)! + bp = 1$$

Q SEJA, HÁ a T.q. $a(p-1)! \equiv 1 \pmod{p}$.

Logo,

$$a \cdot (p-1)! m^{p-1} \equiv a(p-1)! \pmod{p}$$

$$\Rightarrow m^{p-1} \equiv 1 \pmod{p}.$$

$$F_1 \in Mw$$

DEF: $\varphi(m)$ É A QUANTIDADE DE INTEIROS EM $\{0, \dots, m-1\}$ QUE SÃO PRIMOS EM RELAÇÃO A m .

$$\phi(m) = \left| \left\{ n : 0 \leq n \leq m-1, n \perp m \right\} \right|$$

CHAMOS $\varphi(m)$ DO TOTIENTE (FUNÇÃO TOTIENTE DE EULER)

Ex: $\varphi(L) = L$, $\varphi(p) = p-1 \quad \forall p \in \text{Primo}$

EX: $\varphi(m) < m-1$ se p NAO É PRIMO.

EX: SE $m = p^k$, ENTÃO OS MÚLTIPLOS DE p EM $\{0, \dots, p^k - 1\}$ SÃO

$$\{0, p, 2p, \dots, p^k - p\} \quad \leadsto \text{3AO } p^{k-1} \text{ DELES.}$$

Logo $\varphi(p^k) = p^k - p^{k-1}$

- Se m é composto, digamos $m = m_1 \cdot m_2$, então temos um sistema numérico residual. Isto é se $0 \leq m < m$ então

$$n \perp m \iff (n \bmod m_1) \perp m_1 \wedge (n \bmod m_2) \perp m_2$$

Logo, $\varphi(m) = \varphi(m_1) \cdot \varphi(m_2)$

Ex: $\varphi(12) = \varphi(4) \cdot \varphi(3) = 2 \cdot 2 = 4$ PORQUE SE $n \perp 12$, ENTÃO

$$\underbrace{n \bmod 4}_{=1 \text{ or } 3} \perp 4 \in \underbrace{n \bmod 3}_{=1 \text{ or } 2} \perp 3$$

$$\text{On } S \in \mathcal{S}_A \quad m \perp 12 \quad S \in \quad m = \begin{matrix} (1,1) & (1,2) & (3,1) & (3,2) \\ \perp & \in & \neq & \parallel \end{matrix}$$

FUNÇÕES MULTIPLICATIVAS

DEF: UMA FUNÇÃO f É MULTIPLICATIVA SE $f(1) = 1$ E

$$f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2) \quad \text{QUANDO } m_1 \perp m_2$$

EX: φ

$$\text{EX: } f(m) = m^\alpha \quad \text{PARA } \alpha \text{ FIXADO}$$

UMA FUNÇÃO MULTIPLICATIVA É COMPLETAMENTE DEFINIDA PELOS SEUS VALORES EM POTÊNCIAS DE PRIMOS.

$$\text{SE } m = \prod_p p^{m_p}, \text{ ENTÃO } f(m) = \prod_p f(p^{m_p})$$

NO CASO DE φ , TEMOS

$$\varphi(m) = \prod_{p|m} (p^{m_p} - p^{m_p-1}) = m \prod_{p|m} (1 - 1/p)$$

$$\text{EX: } \varphi(12) = (4-2)(3-1) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right)$$

PERGUNTA: SE f É MULTIPLICATIVA, O QUE PODEMOS AFIRMAR SOBRE

$$g(m) = \sum_{d|m} f(d)$$

PROP: g É MULTIPLICATIVA.

PROVA: SEJA $m = m_1 m_2$ COM $m_1 \perp m_2$, ENTÃO

$$\begin{aligned} g(m) &= \sum_{d|m} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 \cdot d_2) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1) \cdot f(d_2) \\ &= \sum_{d_1|m_1} f(d_1) \cdot \sum_{d_2|m_2} f(d_2) = g(m_1) \cdot g(m_2) \end{aligned}$$



PROP: SE f É UMA FUNÇÃO TAL QUE $g(m) = \sum_{d|m} f(d)$ É MÚLTIPlicATIVA,
ENTÃO f É MÚLTIPlicATIVA.

PROVA: INDUÇÃO EM m

CASO BASE: SE $m=1$, TEMOS $1 = g(1) = \sum_{d|1} f(d) = f(1)$

HIPÓTESE DE INDUÇÃO: SUPONHA QUE $f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$ SE $m_1 \perp m_2$
E $m > m_1, m_2$

PASSO INDUTIVO: SE $m = m_1 \cdot m_2$ COM $m_1 \perp m_2$, ENTÃO

$$g(m_1, m_2) = \sum_{d|m_1 m_2} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2)$$

NOTE QUE $d_1 \perp d_2$ POIS $m_1 \perp m_2$.

PELA HIPÓTESE DE INDUÇÃO, TEMOS $f(d_1) \cdot f(d_2)$
EXCETO SE $(d_1, d_2) = (m_1, m_2)$.

LOGO

$$\sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2) = \left(\sum_{d_1|m_1} f(d_1) \cdot \sum_{d_2|m_2} f(d_2) \right) - f(m_1) \cdot f(m_2) + f(m_1 m_2)$$

$$= g(m_1) \cdot g(m_2) = \sum_{d_1|m_1} f(d_1) \cdot \sum_{d_2|m_2} f(d_2)$$

$$\text{Logo, } -f(m_1) \cdot f(m_2) + f(m_1 m_2) = 0$$

□

A FUNÇÃO DE MÖBIUS μ É DADA POR $\sum_{d|m} \mu(d) = [m=1]$

$$\text{EX: } \mu(1) = \sum_{d|1} \mu(d) = [m=1] = 1$$

$$\text{SE } p \text{ É PRIMO, TEMOS } 0 = [p=1] = \sum_{d|p} \mu(d) = \mu(1) + \mu(p) \\ \text{LOGO } \mu(p) = -1$$

$$\text{SE } m = p^k \text{ COM } p \text{ PRIMO E } k > 1, \text{ ENTÃO (POR INDUÇÃO) } \mu(m) = 0.$$

$$\text{SEJA } g(m) = \sum_{d|m} f(d)$$

$$\text{NOTE QUE } \sum_{d|m} \mu(d) g\left(\frac{m}{d}\right) = \sum_{d|m} \mu\left(\frac{m}{d}\right) g(d)$$

$$\begin{aligned} &= \sum_{d|m} \mu\left(\frac{m}{d}\right) \sum_{k|d} f(k) \\ &= \sum_{k|m} \sum_{d|(m/k)} \mu\left(\frac{m}{kd}\right) f(k) \\ &= \sum_{k|m} \sum_{d|(m/k)} \mu(d) f(k) \\ &= \sum_{k|m} [m/k=1] f(k) = f(m) \end{aligned}$$

NOTE QUE $g(m) = [m=1]$ É MULTIPLICATIVO.
LOGO, PELA PROP. μ É MULTIPLICATIVA.

ASSIM, TEMOS

$$\mu(m) = \prod_{p|m} \mu(p^{m_p}) = \begin{cases} (-1)^r & \text{SE } m = p_1 \cdots p_r \\ 0 & \text{SE } m_p \geq 2 \text{ PARA ALGUM } p. \end{cases}$$