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.

  ↳ $n \bmod m = 0$

  $n = m \cdot k$ PARA $k \in \mathbb{Z}$

  n É MÚLTIPLO DE m.

NOTAÇÃO: $m \mid n$

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

EX: $2 \mid 6$

$\pi \mid 2\pi$

- O MAIOR DIVISOR COMUM DE m E n É

$$mdc(m,n) = MAX\{k : k \mid m \in k \mid n\}$$

EX: $mdc(18,12) = 6$

$mdc(0,n) = n$ OBS $k \mid 0$ SE $\frac{0}{k} \in \mathbb{Z}$

- O MENOR MÚLTIPLO COMUM DE m E n É

$$mmc(m,n) = MIN\{k : m \mid k \in n \mid k\}$$

EX: $mmc(18,12) = 36$

- ALGORITMO DE EUCLIDES:

$n + m > n \bmod m + m$

$< m < n$

1) $MDC(0, n) = n$

2) $MDC(m, n) = mdc(n \bmod m, m)$

PROP: O CONJ. DE DIV. COMUNS DE n E m É IGUAL AO CONJ. DE DIV. COMUNS DE $n \bmod m$ E m

($\Rightarrow$) SUPONHA QUE $q \mid m$ E $q \mid n$. LOGO $n = n'q$, $m = m' \cdot q$.

E $n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor \cdot m = n'q - \left\lfloor \frac{n}{m} \right\rfloor \cdot m' \cdot q = q\left(n' - \left\lfloor \frac{n}{m} \right\rfloor \cdot m'\right)$

LOGO $q \mid n \bmod m$

($\Leftarrow$) SUPONHA QUE $q \mid m$ E $q \mid n \bmod m$. LOGO $m = m' \cdot q$ E $n \bmod m = r \cdot q$

TEMOS $n = \left\lfloor \frac{n}{m} \right\rfloor \cdot m + n \bmod m = \left\lfloor \frac{n}{m} \right\rfloor m'q + rq = q\left(\left\lfloor \frac{n}{m} \right\rfloor m' + r\right)$

EX: $mdc(12,18) = mdc(6,12) = mdc(0,6) = 6$

↦ TEMOS MAIS: PODEMOS ENCONTRAR m' E n' T.Q.

$$m' \cdot m + n' \cdot n = mdc(m,n)$$

PROP: DADOS INTEIROS m E n, $m < n$, EXISTEM $m', n' \in \mathbb{Z}$ T.Q.

$$m' \cdot m + n' \cdot n = mdc(m,n)$$

PROVA: SE $m = 0$, ENTÃO TOMAMOS $m' = 0$ E $n' = 1$, E TEMOS

$$m' \cdot m + n' \cdot n = 0 + n = mdc(0,n)$$

ENTÃO PODEMOS SUPOR QUE $m > 0$. SEJA $r = n \bmod m$

⟶ ▷

PROP: DADOS INTEIROS $m \in \mathbb{N}$, $m < n$, EXISTEM $m', n' \in \mathbb{Z}$ T.Q.

$$m' \cdot m + n' \cdot n = mdc(m, n)$$

PROVA: SE $m = 0$, ENTÃO TOMAMOS $m' = 0$ E $n' = 1$, E TEMOS

$$m' \cdot m + n' \cdot n = 0 + n = mdc(0, n)$$

ENTÃO PODEMOS SUPOR QUE $\underline{m > 0}$. SEJA $r = n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor \cdot m$

PELA HIPÓTESE DE INDUÇÃO, EXISTEM $r^*, m^* \in \mathbb{Z}$ T.Q.

$$r^* \cdot r + m^* \cdot m = mdc(r, m)$$

LOGO, $mdc(m, n) = mdc(r, m) = r^* \cdot r + m^* \cdot m$

$$= r^* \left(n - \left\lfloor \frac{n}{m} \right\rfloor m \right) + m^* \cdot m$$

$$= \underbrace{r^*}_{n'} n + \underbrace{\left(m^* - \left\lfloor \frac{n}{m} \right\rfloor r^* \right)}_{m'} \cdot m = n' \cdot n + m' \cdot m$$

EX: $mdc(12,18) = mdc(6,12) = mdc(0,6) = 6$

$\underbrace{r^* n}_{n'} + \underbrace{\left(m^* - \left\lfloor \frac{n}{m} \right\rfloor r^*\right)}_{m'} m$

$m = 0, \; n = 6 \; : \; m' = 0 \; , \; n' = 1$

$m = 6, \; n = 12 \; : \; mdc(6,12) \rightsquigarrow \; \underset{\| \; 0}{r^*} \; , \; \underset{\| \; 1}{m^*} = mdc(0,6)$

DEVOLVE $m' = (1 - 2 \cdot 0) = 1 \; , \; n' = 0$

$m = 12, \; n = 18 : \; mdc(12,18) \rightsquigarrow \; \underset{\| \; 1}{r^*} \; , \; \underset{\| \; 0}{m^*} = mdc(6,12)$

$m' = \left(0 + \left\lfloor \frac{18}{12} \right\rfloor \cdot 1\right) =$

$\underbrace{r^*}_{n'} n + \underbrace{\left(m^* - \left\lfloor \frac{n}{m} \right\rfloor r^*\right)}_{m'} m$

$mdc(6,12)$

$r = 0$

$r^*, m^* = mdc(0,6)$

$0 \quad 1$

$m' = 1 - 2 \cdot 0 = 1$

$m' = 0$

Devolve $1, 0$

$mdc(12,18)$

$r = 6$

$r^*, m^* = mdc(6,12)$

$1 \quad 0$

$m' = 0 - 1 \cdot 1 = -1$

$n' = 1$

Devolve $-1, 1$

$mdc(m,n)$: $m < n$

SE $m = 0$,

DEVOLVE $0, 1$

$r = n \mod m$

$r^*, m^* = mdc(r, m)$

$m' = m^* - \left\lfloor \frac{n}{m} \right\rfloor \cdot r^*$

$n' = r^*$

DEVOLVE m', n (T.q. $m'm + n'n = mdc(m,n)$)

$\rightsquigarrow$ DE FATO $-1 \cdot 12 + 1 \cdot 18 = 6$

PROP 1: SE $k \mid m$ E $k \mid n$, ENTÃO $k \mid am + bn$ $\forall a, b \in \mathbb{Z}$

PROVA: $m = m' \cdot k$ E $n = n' \cdot k$

ENTÃO $am + bn = a \cdot m' \cdot k + bn'k = (am' + bn') \cdot k \Rightarrow k \mid am + bn$

PROP 2: SE $k \mid m$ E $k \mid n$, ENTÃO $k \mid mdc(m, n)$

PROVA: SEJAM m' E n' T.Q. $m' \cdot m + n' \cdot n = mdc(m, n)$ (EXISTE PELO ALG. EUCLIDES)

PELA PROP 1 COM $a = m'$ E $b = n'$, $k \mid am + bn = mdc(m, n)$

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

n FIXADO

OBS: $\{ m : m \mid n \} = \{ \frac{n}{m} : m \mid n \}$

EX: $n = 18$

$\{ m : m \mid n \} = \{ 1, 2, 3, 6, 9, 18 \}$

$\{ \frac{n}{m} : m \mid n \} = \{ 18, 9, 6, 3, 2, 1 \}$

IVERSON: $\sum_{m \mid n} a_m = \sum_{k} \sum_{m > 0} a_m [n = k \cdot m]$

NÚMEROS PRIMOS

DEF: $p \in \mathbb{N}$ É PRIMO SE POSSUI APENAS DOIS DIVISORES

$\rightsquigarrow$ OS DIVISORES SÃO 1 E p.

CONVENÇÃO: 1 NÃO É PRIMO.

OBS: SE p E q SÃO PRIMOS, ENTÃO $mdc(p,q) = 1$

DEF: UM NÚMERO QUE NÃO É PRIMO É DITO COMPOSTO

JÁ VIMOS QUE TODO NÚMERO PODE SER ESCRITO COMO PRODUTO DE PRIMOS.

PERGUNTA: ESSA EXPANSÃO É ÚNICA?

FATORAÇÃO

EX: CONSIDERE OS NÚMEROS DO TIPO $a + b\sqrt{10}$

$$6 = 2 \cdot 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$$

TEOREMA FUNDAMENTAL DA ARITMETICA:

TODO NÚMERO NÚMERO NATURAL ADMITE UMA ÚNICA FATORAÇÃO EM PRIMOS

PROVA: INDUÇÃO EM n.

CERTAMENTE VALE P/ 2

SUPONHA QUE n TEM DUAS FATORAÇÕES

$$n = p_1 \cdot p_2 \cdots p_m = q_1 q_2 \cdots q_k \quad \text{COM} \quad 2 \leq p_1 \leq \cdots \leq p_m \quad \text{E} \quad 2 \leq q_1 \leq \cdots \leq q_k$$

SUPONHA, S.P.G., QUE $p_1 < q_1$

COMO p_1 E q_1 SÃO PRIMOS, TEMOS $mdc(p_1, q_1) = 1$

PELO ALG. DE EUCLIDES, EXISTEM a, b T.Q. $ap_1 + bq_1 = 1$

LOGO, TEMOS $ap_1 q_2 \cdots q_k + \underbrace{bq_1 \cdot q_2 \cdots q_k}_{n} = q_2 \cdots q_k$

COMO $p_1 \mid ap_1 q_2 \cdots q_k$ E $p_1 \mid bn = bq_1 \cdots q_k$, ENTÃO $p_1 \mid q_2 \cdots q_k < n$

CONSIDERE $n^* = \dfrac{q_2 \cdots q_k}{p_1} \in \mathbb{N}$

PELA H.I., n^* ADMITE UMA ÚNICA FATORAÇÃO DIGAMOS $n^* = r_1 \cdots r_s$

LOGO, $p_1 \cdot r_1 \cdots r_s$ É UMA FATORAÇÃO DE $n^* \cdot p_1 = q_2 \cdots q_k$

COMO $n^* \cdot p_1 = q_2 \cdots q_k < n$, PELA H.I. $p_1 r_1 \cdots r_s$ É A ÚNICA FATORAÇÃO DE $q_2 \cdots q_k$

LOGO, $p_1 \in \{q_2, \ldots, q_k\}$, UMA CONTRADIÇÃO $q_k \geq \cdots \geq q_2 \geq q_1 > p_1$ ∎

$$n = \prod_{p \text{ primos}} p^{n_p} \qquad \text{e} \qquad n_p \geq 0 \quad \forall p$$

Podemos pensar na seq. $\langle n_2, n_3, n_5, n_7, \ldots \rangle$

Ex: $12 = 2^2 \cdot 3$ é $\langle 2, 1, 0, 0, \ldots \rangle$

$18 = 2 \cdot 3^2$ é $\langle 1, 2, 0, 0, \ldots \rangle$

- Multiplicar n e m é somar suas repres.

$$12 \cdot 18 = 2^3 \cdot 3^3 \quad \langle 3, 3, 0, 0, \ldots \rangle$$

- Dividir é subtrair

$$18/6 = 3 \qquad \begin{matrix} \langle 1, 2, 0, 0 \ldots \rangle \\ \langle 1, 1, 0, 0, \ldots \rangle \end{matrix}$$

$K = mdc(m,n)$

$\Leftrightarrow$

$K_p = MIN(m_p, n_p) \quad \forall p$

$K = mmc(m,n)$

$\Leftrightarrow$

$K_p = MAX(m_p, n_p) \quad \forall p$

Ex: $6 = mdc(12,18) = \langle 1,1,0,0,\dots \rangle$

$mmc(12,18) = \langle 2,2,0,\dots \rangle = 2^2 \cdot 3^2 = 36$

$K = \langle k_2, k_3, k_5, \dots \rangle$

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

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

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

$12 = \langle 2,1,0,\dots \rangle$

$\underbrace{m \cdot n} = mdc(m,n)\ mmc(m,n)$

$(mn)_p = m_p + n_p$

$(mdc(m,n)\ mmc(m,n))$

$= MIN(m_p, n_p) \cdot MAX(m_p, n_p)$

$= m_p + n_p$

Quantos são os números primos?

Infinito

Prop: Fixe p. Se $p \mid m$, então $p \nmid m+1$

Prova: O menor múltiplo de p que é maior que m é $m+p > m+1$

Porque $p > 1$ ∎

Prop: Há infinitos números primos

Prova: Suponha que $p_1, \ldots, p_k$ são todos os primos.

Tome $M = \underbrace{p_1 \cdots p_k} + 1$

Como $p_i \mid p_1 \cdots p_k$, então $p_i \nmid M$. Logo M é primo. ∎

NÚMEROS DE EUCLIDES

- NÚMEROS PRIMOS DEFINIDOS PELA SEGUINTE REL. DE REC.

$$e_m = e_1 \cdot e_2 \cdots e_{m-1} + 1$$

$\mathrm{mdc}(e_i, e_j) = 1$

OS NÚMEROS DE EUCLIDES SÃO PRIMOS ENTRE SI

$e_1 = 2$

$e_2 = 3$

$e_3 = 7$

$e_4 = 43$

SÃO SEMPRE PRIMOS?

NÃO. $e_5 = 1807 = 13 \cdot 139$

OBS: e_6 É PRIMO, MAS $e_7 \cdots e_{17}$ NÃO SÃO PRIMOS

PROP: OS NÚMEROS DE EUCLIDES SÃO PRIMOS ENTRE SI

PROVA: e_i E e_j COM $e_i > e_j$

ENTÃO $e_i = e_1 \cdot e_2 \cdots e_j \cdots e_{i-1} + 1$

SEJA p PRIMO T.Q. $p \mid e_j$

PELA PROP., COMO p DIVIDE $e_1 \cdots e_{i-1}$, TEMOS QUE

p NÃO DIVIDE $e_1 \cdots e_{i-1} + 1 = e_i \Rightarrow \underline{p \nmid e_i}$

...

PROVA: COMO $e_i = e_1 \cdot e_2 \cdots e_j \cdots e_{i-1} + 1$, TEMOS

$$\underbrace{1}_{n'} \cdot e_i - \underbrace{\left(\prod_{k<i,\, k\neq j} e_k\right)}_{m'} \cdot \underbrace{e_j}_{m} = 1$$

LOGO, $mdc(e_i, e_j) = 1$

i.mdc $\in \{am + bm : a, b \in \mathbb{N}\}$

$= \{i \cdot mdc : i \in \mathbb{N}\}$

$\exists\, a, b$ T.Q.

$iam + ibm = mdc$

EXISTE FORMA FECHADA P/ OS NÚMEROS DE EUCLIDES

$$e_m = \underbrace{e_1 e_2 \cdots e_{m-2}}_{e_{m-1}-1} \cdot e_{m-1} + 1$$

$$e_{m-1} = e_1 \cdots e_{m-2} + 1$$

$$= (e_{m-1} - 1) e_{m-1} + 1$$

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

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.

TEMOS QUE $\pi(x) \sim \dfrac{x}{\ln x}$ $\left(\forall \varepsilon > 0 \text{ EXISTE } n_0 \text{ T.Q. } \varepsilon\ n \geq n_0, \text{ ENTÃO } \pi(n) \in \left(\dfrac{x}{\ln x} - \varepsilon, \dfrac{x}{\ln x} + \varepsilon\right)\right)$

PRIMOS GÉMEOS: ÍMPARES CONSECUTIVOS E PRIMOS

PARES DE PRIMOS DA FORMA $p, p+2$

$11, 13$, $17, 19$, $29, 31$, $41, 43$

FATORES FATORIAIS

$$n! = 1 \cdot 2 \cdot \cdots \cdot n = \prod_{K=1}^{n} K$$

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

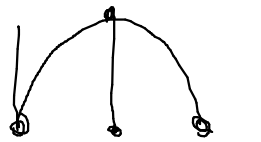
- $10! \approx \frac{3}{2} \cdot 10^6$

OBS: O NÚMERO DE DÍGITOS DE $n!$ É MAIOR QUE n, QUANDO $n \geq 25$

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

$$k(n+1-k) = -k^2 + k(n+1)$$

RAÍZES : 0 E $n+1$



LO $\frac{n+1}{2}$

NOTE $k(n+1-k)$ POSSUI MÁX QUANDO $k = \frac{n+1}{2}$ E MÍNIMO QUANDO $k = 1$

LOGO

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

$$n^n \leq \prod_{k=1}^{n} n \leq \underbrace{\prod_{k=1}^{n} k(n+1-k)}_{(n!)^2} \leq \prod_{k=1}^{n} \frac{1}{4}(n+1)^2 = \left(\frac{1}{4}(n+1)^2\right)^n$$

CONCLUÍMOS QUE

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

OU

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

- DADO PRIMO p, QUAL O EXPOENTE DE p EM $n!$

  ↳ DENOTAMOS POR $\epsilon_p(n!)$

EX: $4! = 24 = 2^3 \cdot 3 \Rightarrow \epsilon_2(4!) = 3,$

$\epsilon_3(4!) = 1$

EX: $\epsilon_2(10!)$

	1	2	3	4	5	6	7	8	9	10
2 \		X		X		X		X		2
4 \				X				X		
8 \								X		

$\epsilon_2(10!) = 8$

EM GERAL, TEMOS

$$\epsilon_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + \cdots = \sum_{k \geq 1} \left\lfloor \frac{n}{2^k} \right\rfloor$$

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

$$\Downarrow$$

$$\epsilon_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \cdots = \frac{n}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \frac{n}{p}\left(\frac{p}{p-1}\right) = \frac{n}{p-1}$$

$$S = 1 + \frac{1}{p} \cdots$$

$$pS = p + 1 + \cdots$$

$$(p-1)S = p$$

$$S = \frac{p}{p-1}$$

LOGO, $p^{\epsilon_p(n!)} < p^{\frac{n}{p-1}}$ (CONTRIBUIÇÃO DE p P/ $n!$)

Temos $p^{\epsilon_p(n!)} < p^{\frac{n}{p-1}}$

Como $p \leq 2^{p-1}$. Logo,

$$p^{\epsilon_p(n!)} \leq (2^{p-1})^{\frac{n}{p-1}} = 2^n$$

Portanto,

$$n! = \prod_{p \leq n} p^{\epsilon_p(n!)} \leq \prod_{p \leq n} 2^n = \underbrace{2^n \cdot 2^n \cdot \ldots \cdot 2^n}_{\#\text{Primos} \leq n} = 2^{n\pi(n)}$$

p Primos

$= \pi(n)$

Tirando $\log_2$ dos dois lados $n\pi(n) \geq \log n!$

Finalmente $\pi(n) \geq \frac{1}{n} \log n! \geq \frac{1}{n} \log n^{\frac{n}{2}} = \frac{1}{2} \log n$

$(1-\varepsilon)\frac{n}{\log n}$

PRIMOS ENTRE SI

- DIZEMOS QUE m E n SÃO PRIMOS ENTRE SI SE $mdc(m,n) = 1$

  OU "m É PRIMO COM RELAÇÃO n"

  NOTAÇÃO: $m \perp n$

- DIZEMOS QUE UMA FRAÇÃO $\frac{m}{n}$ ESTÁ EM SUA FORMA MAIS SIMPLES SE $m \perp n$

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

- QUANDO USAMOS A "PROJEÇÃO" $m = \langle m_2, m_3, \dots \rangle$ E $n = \langle n_2, n_3, \dots \rangle$

  ENTÃO $m \perp n$ SE E SÓ SE $MIN(m_p, n_p) = 0 \quad \forall p$ PRIMO.

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

PROVA: FIXE PRIMO p.

($\Rightarrow$) SUPONHA QUE $K \perp m$ E $K \perp n$,

ENTÃO $K_p = 0$ OU $m_p = n_p = 0$

LOGO $\min(K_p, m_p + n_p) = 0 \Rightarrow K \perp mn$

($\Leftarrow$) SUPONHA QUE $K \perp mn$

ENTÃO $K_p = 0$ OU $m_p + n_p = 0 \Rightarrow m_p = n_p = 0$

LOGO $\min(K_p, m_p) = \min(K_p, n_p) = 0 \Rightarrow K \perp m$ E $K \perp n$

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

PROVA: SUPONHA $\sqrt{p}$ É RACIONAL, i.e., $\exists a,b \in \mathbb{N}$ T.Q. $\sqrt{p} = \frac{a}{b}$

PODEMOS SUPOR QUE $a \perp b$.

TEMOS $p = a^2/b^2$, O QUE IMPLICA QUE $a^2 = p \cdot b^2$

COMO $p \mid pb^2$, ENTÃO $p \mid a^2$. LOGO $p \mid a$, OU SEJA $a = a'p$

SUBSTITUINDO, TEMOS $pb^2 = a'^2 p^2$ E, PORTANTO $b^2 = a'^2 p$

LOGO $p \mid b^2$, O QUE IMPLICA QUE $p \mid b$.

LOGO NÃO VALE $a \perp b$

PROP: SE p É PRIMO, ENTÃO $\sqrt{n}$ É IRRACIONAL (EX: $n=4$)

PROVA: SUPONHA x É RACIONAL, i.e., $\exists a,b \in \mathbb{N}$ T.Q. $x = \frac{a}{b}$

PODEMOS SUPOR QUE $a \perp b$.

TEMOS $x^2 = a^2/b^2$, O QUE IMPLICA QUE $a^2 = x^2 \cdot b^2$

COMO $x^2 \mid x^2 b^2$, ENTÃO $x^2 \mid a^2$. LOGO $x^2 \mid a$, OU SEJA $a = a'p$

SUBSTITUINDO, TEMOS $pb^2 = a'^2 p^2$ E, PORTANTO $b^2 = a'^2 p$

LOGO $p \mid b^2$, O QUE IMPLICA QUE $p \mid b$.

LOGO NÃO VALE $a \perp b$

∎

MOD: UMA RELAÇÃO DE CONGRUÊNCIA

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

- VAMOS USAR UMA NOVA NOTAÇÃO:

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

↳ LEMOS a E b SÃO CONGRUENTES MÓDULO m

EX: $9 \equiv -16 \pmod{5}$ POIS $9 \text{ MOD } 5 = 4 = -16 \text{ MOD } 5$

↳ $-20 + 4$

COMO x MOD m DIFERE x POR UM MÚLTIPLO DE m, $\left(\left\lfloor \frac{x}{m} \right\rfloor \cdot m\right)$

TEMOS QUE $a \equiv b \pmod m \iff a - b$ É MÚLTIPLO DE m

$$a = d_a \cdot m + r$$
$$b = d_b \cdot m + r$$

$$a - b = (d_a - d_b) \cdot m$$

- A RELAÇÃO DE CONGRUÊNCIA É UMA RELAÇÃO DE EQUIVALÊNCIA.

i) REFLEXIVA : $a \equiv a$

ii) SIMÉTRICA : $a \equiv b \implies b \equiv a$

iii) TRANSITIVA : $a \equiv b$ E $b \equiv c \implies a \equiv c$

OPERAÇÕES

PROP:

$$\left.\begin{array}{l} a \equiv b \\ c \equiv d \end{array}\right\} \pmod m \Rightarrow \begin{array}{l} a+c \equiv b+d \\ a-c \equiv b-d \end{array}$$

OBS: $a \equiv a + m \pmod m$

$m \equiv 0 \pmod m$

QUOCIENTE

PROVA:

DE FATO, $a-b$ ($k \cdot m$) e $c-d$ ($k' \cdot m$) SÃO MÚLTIPLOS DE m

LOGO $a-b+c-d \to (k+k')m$ SÃO MÚLTIPLOS DE m

$a-b-(c-d) \to (k-k')m$

LOGO,

$a+c \equiv b+d$

$a-c \equiv b-d$

EX: MOD 5

$15 + 18 \equiv 0 + 3 \equiv 3 \pmod 5$

$33 \pmod 5 \equiv 3$

$\overline{0} = \{0, 5, 10, 15, \ldots\}$

$\overline{1} = \{1, 6, 11, 16, \ldots\}$

$\overline{3} = \{3, 8, 13, 18, \ldots\}$

PROP: $X \equiv y \iff X - y$ É MÚLTIPLO DE m

SERÁ QUE SE

$a \equiv b$ E $c \equiv d$, ENTÃO $a \cdot c \equiv b \cdot d$? $(\text{MOD } m)$

DE FATO, $-bc + bc$

$ac - bd = (a-b)c + b(c-d) \equiv 0 \implies ac - bd$ MÚLTIPLO m

MÚLTIPLO DE m MÚLTIPLO DE m

LOGO, $ac \equiv bd$

POTÊNCIAS

$a \equiv b \implies a^n \equiv b^n$

$a = k_a m + r \qquad b = k_b \cdot m + r \implies (k_a m + r)^n = (k_a m)^n + ?(k_a m)^{n-1} \cdot r + ? \cdot m^2 + ? \cdot m^3 + \dots + r^n$

$(\text{MOD } m) = r^n$

EX: $2 \equiv -1 \ (\text{MOD } 3) \qquad 2^n \equiv (-1)^n \ (\text{MOD } 3)$

$\implies 2^n - 1$ É MÚLTIPLO DE 3 $\iff n$ É PAR

$2^n + 1$ É MÚLTIPLO DE 3 $\iff n$ É ÍMPAR

Divisão

$ad \equiv bd \pmod{m}$ **não implica que** $a \equiv b \pmod{m}$

Ex: $d = 0$

Ex: $\underbrace{3 \cdot 2}_{6} \equiv \underbrace{5 \cdot 2}_{10} \pmod{4}$ mas $3 \not\equiv 5 \pmod{4}$

$6 \equiv 2$

$10 \equiv 2$

Prop: Se $d \perp m$, então $ad \equiv bd \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$

PROP: SE $d \perp m$, ENTÃO $ad \equiv bd \pmod m \iff a \equiv b \pmod m$

PROVA: COMO $d \perp m$, TEMOS $mdc(d, m) = 1$.

LOGO, $\exists\, d', m'$ T.Q. $\underbrace{d' \cdot d + m' \cdot m}_{\text{MÚLTIPLO DE } m} = 1$

$\Rightarrow d' \cdot d \equiv 1 \pmod m$

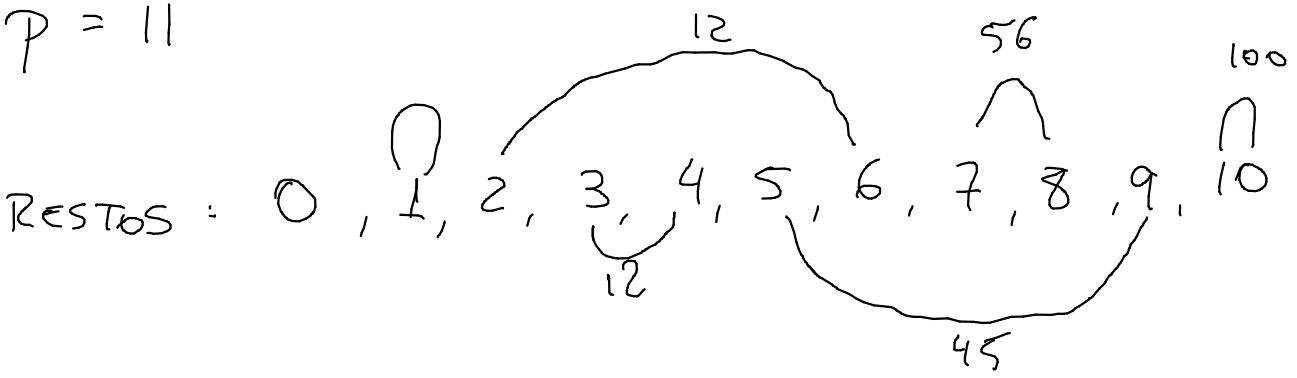
↳ "INVERSO MULTIPLICATIVO DE d"

SE $ad \equiv bd \pmod m$, ENTÃO $a\underset{\sim}{dd'} \equiv b\underset{\sim}{dd'} \pmod m$

LOGO, COMO $d'd \equiv 1$, TEMOS $a \equiv b \pmod m$. ∎

EM PARTICULAR, SE p É PRIMO, "TODO" NÚMERO POSSUI INV. MULT. DIFERENTE DE ZERO

EX: $p = 11$



$$1 \cdot 12 = 12 \equiv 1 \pmod{11}$$

$$12 \cdot 12 = 144 = 11 \cdot 13 + 1$$

PERGUNTA: O INVERSO MULTIPLICATIVO É ÚNICO?

SUPONHA QUE EXISTEM y, y' T.Q. $xy \equiv xy' \equiv 1 \pmod{p}$

$$xy \equiv 1$$

$$\Rightarrow (y'x)y \equiv y' \Rightarrow y \equiv y'$$

($y'x \equiv 1$)

EX: DIVISORES DE ZERO

DEF: $x \neq 0$ É DIVISOR DE ZERO SE $\exists y \neq 0$ T.Q. $xy \equiv 0 \pmod{m}$

EX: 2 É DIV. DE ZERO MOD 4, MOD 6

X PODE SER DIV. DE ZERO E TER INVERSO?

1) $\exists\ y$ T.Q. $xy \equiv 0$

2) $\exists\ z$ T.Q. $xz \equiv 1 \rightsquigarrow 0 \equiv xyz \equiv y$

Resíduos

Fixe uma base $\{m_1, m_2, \ldots, m_r\}$ t.q. $m_i \perp m_j \ \forall i,j$

Def: O resíduo de x, $Res(x)$, é o vetor

$$(x \bmod m_1, \ldots, x \bmod m_r)$$

EX: SISTEMA NÚMERICO RESIDUAL BASE: 3, 5

	X MOD 3	X MOD 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
15	0	0
16	1	1

- AS OPERAÇÕES DE SOMA, SUBTRAÇÃO, E MULTIPLICAÇÃO PODEM SER FEITAS INDEPEND. NO RESÍDUO

EX: $7 = (1,2)$ × $13 = (1,3)$

$7 \cdot 13 = 91$ $\quad (1,2) \times (1,3) = (1,1)$

$91 \pmod{15} = 1$

$91 \pmod{3} = 1$

$91 \pmod{5} = 1$

EX: $7 = (1,2)$

$7 \cdot 7 = (0,2) \cdot (1,2) = (1,4)$

11

49

- COMO OBTER $\mathbb{Z}$ A PARTIR DE $\mathrm{RES}(\mathbb{Z})$?

BASE $= (3,5) := (m,n)$

$$\mathbb{Z} = (x,y) = x\underbrace{(1,0)}_{10} + y\underbrace{(0,1)}_{6} \overset{?}{=} 10x + 6y$$

a b

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

PROBLEMA: QUANTAS SOLUÇÕES EXISTEM PARA A REL.

$$x^2 \equiv 1 \pmod{p^k}$$

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

A REL. $x^2 \equiv 1 \iff x^2 - 1 \equiv 0 \iff (x-1)(x+1) \equiv 0$

LOGO, $(x-1)(x+1)$ É MÚLTIPLO DE p^k

ISSO SÓ ACONTECE QUANDO $p^k \mid (x-1)$ OU $p^k \mid (x+1)$ (OU AMBOS)

SÓ QUANDO $p = 2$

SE $p > 2$, ENTÃO TEMOS DUAS SOLUÇÕES $p^k \mid (x-1) \iff (x-1) \equiv 0 \iff x \equiv 1$

$p^k \mid (x+1) \iff x+1 \equiv 0 \iff x \equiv -1$

SE $p=2$ E $2^k \mid (x-1)(x+1)$ ENTÃO UM DENTRE $(x-1)$ E $(x+1)$

NÃO É MÚLTIPLO DE 4 — 2^k — 2^{k-1} — 2 ✗

ENTÃO O OUTRO É MÚLTIPLO DE 2^{k-1}

ISSO NOS DÁ QUATRO SOLUÇÕES $x = \pm 1$ E $x \equiv 2^{k-1} \pm 1$

$x = 2^{k-1} - 1$

$(2^{k-1} - 1 \quad -1)(2^{k-1} + 1)$

$2^{k-1} - 1$ = PAR = $2r$; $x = 2^{k-1}$

$2^k \cdot r \equiv 0$

EX: $x^2 \equiv 1 \pmod 8$ → $k=3$

2^3

$x = 1, -1, 3, 5$

7

EX: $x^2 \equiv 1 \pmod{16}$ → $k=4$

$x = 1, 15, 7, 9$

$7^2 = 49 = 48 + 1$ (3·16)

$9^2 = 81 = 80 + 1$ (5·16)

TEOREMA DE WILSON: $(n-1)! \equiv -1 \pmod{n} \iff n$ É PRIMO

$n \neq 4$

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

SE n NÃO É PRIMO, ENTÃO $n = m \cdot k$, EM PARTICULAR $m, k \leq n-1$

MAS ENTÃO $(n-1)! = (n-1) \cdots m \cdots k \cdots 1 \equiv 0 \pmod{n}$

m k

$p^2 - 1 \quad \cdots \quad 3p \quad \cdots \quad 2p \quad \cdots \quad p$

p^2

SE $n=4$ $\quad (n-1)! = 3! = 6 = 2 \pmod{4}$

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

$p > 2$

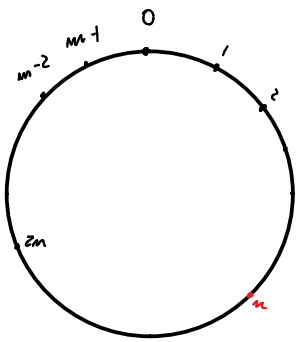
($\Leftarrow$) SE n É PRIMO, ENTÃO $(n-1)! \equiv -1 \pmod{n}$

$(n-1)! = 1 \cdot 2 \cdot 3 \cdots (n-1)$

EX: $n=13$

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

-1



Prop: Fixe m e n.

Os m números

$$\underbrace{0 \bmod m,\ n \bmod m,\ 2n \bmod m,\ \ldots,\ (m-1)n \bmod m}_{m \text{ valores}}$$

consistem precisamente de m/d cópias de

$$\underbrace{0,\ d,\ 2d,\ \ldots,\ m-d}$$

em alguma ordem, em que $d = \mathrm{mdc}(m,n)$.

Prova: Pelo Alg. de Euclides, há m', n' t.q.

$$m'm + n'n = \mathrm{mdc}(m,n) = d$$

Logo $n' \cdot n = d \pmod m$

e $i \cdot n' \cdot n = i \cdot d \pmod m$

Isso mostra que $0, d, 2d, \ldots, m-d$ aparecem

PROP: DADOS m E n, OS NÚMEROS

$0 \bmod m,\ n \bmod m,\ 2n \bmod m,\ \dots,\ (m-1)n \bmod m$

SÃO PRECISAMENTE d CÓPIAS DOS NÚMEROS $0, d, 2d, \dots, m-d$ EM ALGUMA ORDEM, EM QUE $d = mdc(m,n)$ $\quad \frac{m}{d}$

EX: $m = 12,\ n = 9$ $\quad m/d \quad d = 3$

0	9	18	27	36	45	54	63	72	81	90	99	m PRIMEIROS MÚLTIPLOS DE m
0	9	6	3	0	9	6	3	0	9	6	3	

PROVA: Pelo ALG. DE EUCLIDES, HÁ m', n' T.Q. $m'm + n'n = d$

LOGO, $n'n = d \pmod m$ E $in'n = id \pmod m$ $\forall i = 0, \dots, m-1$

↳ PODEMOS TOMAR $in' \in \{0, \dots, m-1\}$

ISSO IMPLICA QUE $0, d, \dots, m-d$ ESTÃO PRESENTES.

FIXE $j \in \{0, \dots, \frac{m}{d} - 1\}$. QUEREMOS CONTAR QUANTAS VEZES id APARECE

SEJA J MÍNIMO T.Q. $J \cdot n \equiv id \pmod d$, $J < m/d$

COMO m E n SÃO MÚLTIPLOS DE d, TEMOS $\frac{m \cdot n}{d}$ É INTEIRO, MÚLTIPLO DE m E DE n.

$= mmc(m,n)$

POIS QUANDO $J = \frac{m}{d} + J'$, $J' < J$

$J \cdot n = \frac{m}{d} \cdot n + J'n \equiv J'n$ ($\frac{m}{d} \cdot n \equiv 0$)

$d = mdc(m,n)$

$m = m^* d$

$n = n^* d$

$\frac{m \cdot n}{d} = \frac{m^* \cdot d \cdot n^* \cdot d}{d}$ ($m = m^* d$, $n = n^* d$)

LOGO $\quad Jn + k \cdot \frac{mn}{d} \equiv id \pmod d \quad \forall k.$

QUEREMOS $\quad Jn + \frac{kmn}{d} \leq (m-1)n$

$J + k\frac{m}{d} \leq (m-1)$

$k \leq \frac{md - d - Jd}{m} = d - \frac{d(J-1)}{m}$

$\frac{d(J-1)}{m} < \frac{d\left(\frac{m}{d} - 1\right)}{m} = \frac{-d}{m} < 1$

$k \leq d - 1$

↳ LOGO, HÁ "EXATAMENTE" d CÓPIAS DE id

PEQUENO TEOREMA DE FERMAT

SE p É PRIMO, ENTÃO $n^{p-1} \equiv 1 \pmod p$ $\quad \forall n \neq 0$

PROVA: COMO $n \perp p$, ENTÃO PELA PROPOSIÇÃO OS NÚMEROS

$$\left.\begin{matrix} n \bmod p,\ 2n \bmod p,\ \ldots,\ (p-1)n \bmod p \end{matrix}\right\} p-1 \text{ NÚMEROS}$$

SÃO OS NÚMEROS $1, 2, 3, \ldots, p-1$

MULTIPLICANDO ESTES NÚMEROS

$$n\,(2n)\cdot(3n)\cdots\big((p-1)n\big) = \underbrace{(1\cdot 2\cdots(p-1))}\ \underbrace{n^{p-1}}_{\equiv 1}$$

REORGANIZANDO

$$= \underbrace{1\cdot\ldots\cdot(p-1)}$$

WILSON − 1

PELO TEO. DE WILSON, $= -1$

TEMOS $\quad -n^{p-1} \equiv -1 \implies n^{p-1} \equiv 1$ $\quad \blacksquare$