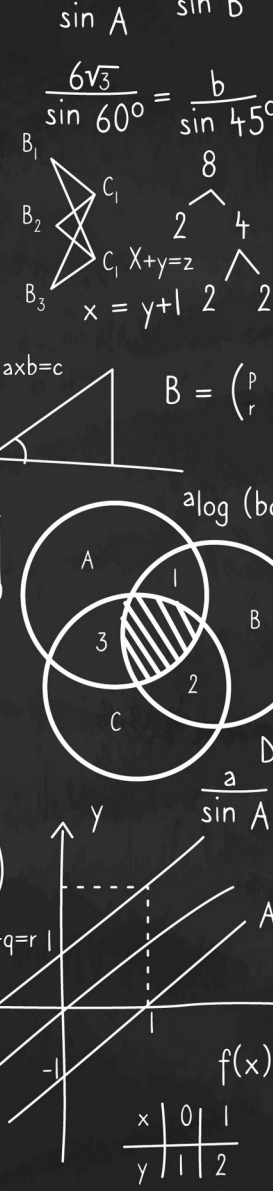


Matemática Discreta 2

Aula 05

Cristiane Loesch

cristiane.costa@unb.br

Brasília
2025

NÚMEROS PRIMOS

Seja $p \in \mathbb{N}^*$, $p > 1$, p é dito PRIMO se os únicos fatores positivos de p são 1 e p .

NÚMEROS PRIMOS

Seja $p \in \mathbb{N}^*$, $p > 1$, p é dito PRIMO se os únicos fatores positivos de p são 1 e p .

Um número $c \in \mathbb{N}^*$, $c > 1$, que não é primo é dito COMPOSTO, ou seja, $c \in \mathbb{N}^*$ é composto se, e somente se, $\exists a \in \mathbb{N}^* / a | c \wedge 1 < a < c$.

NÚMEROS PRIMOS – CRIVO DE ERASTÓTENES

EXEMPLO

1	11	21	31	41	51	61	71	81	91
2	12	22	32	42	52	62	72	82	92
3	13	23	33	43	53	63	73	83	93
4	14	24	34	44	54	64	74	84	94
5	15	25	35	45	55	65	75	85	95
6	16	26	36	46	56	66	76	86	96
7	17	27	37	47	57	67	77	87	97
8	18	28	38	48	58	68	78	88	98
9	19	29	39	49	59	69	79	89	99
10	20	30	40	50	60	70	80	90	100

NÚMEROS PRIMOS – CRIVO DE ERASTÓTENES

EXEMPLO

Excluir números pares exceto o 2

1	11	21	31	41	51	61	71	81	91
2									
3	13	23	33	43	53	63	73	83	93
5	15	25	35	45	55	65	75	85	95
7	17	27	37	47	57	67	77	87	97
9	19	29	39	49	59	69	79	89	99

NÚMEROS PRIMOS – CRIVO DE ERASTÓTENES

EXEMPLO

Excluir números pares exceto o 2

Excluir números múltiplo de 3,

1	11		31	41		61	71		91
2									
3	13	23		43	53		73	83	
5		25	35		55	65		85	95
7	17		37	47		67	77		97
	19	29		49	59		79	89	

NÚMEROS PRIMOS – CRIVO DE ERASTÓTENES

EXEMPLO

Excluir números pares exceto o 2

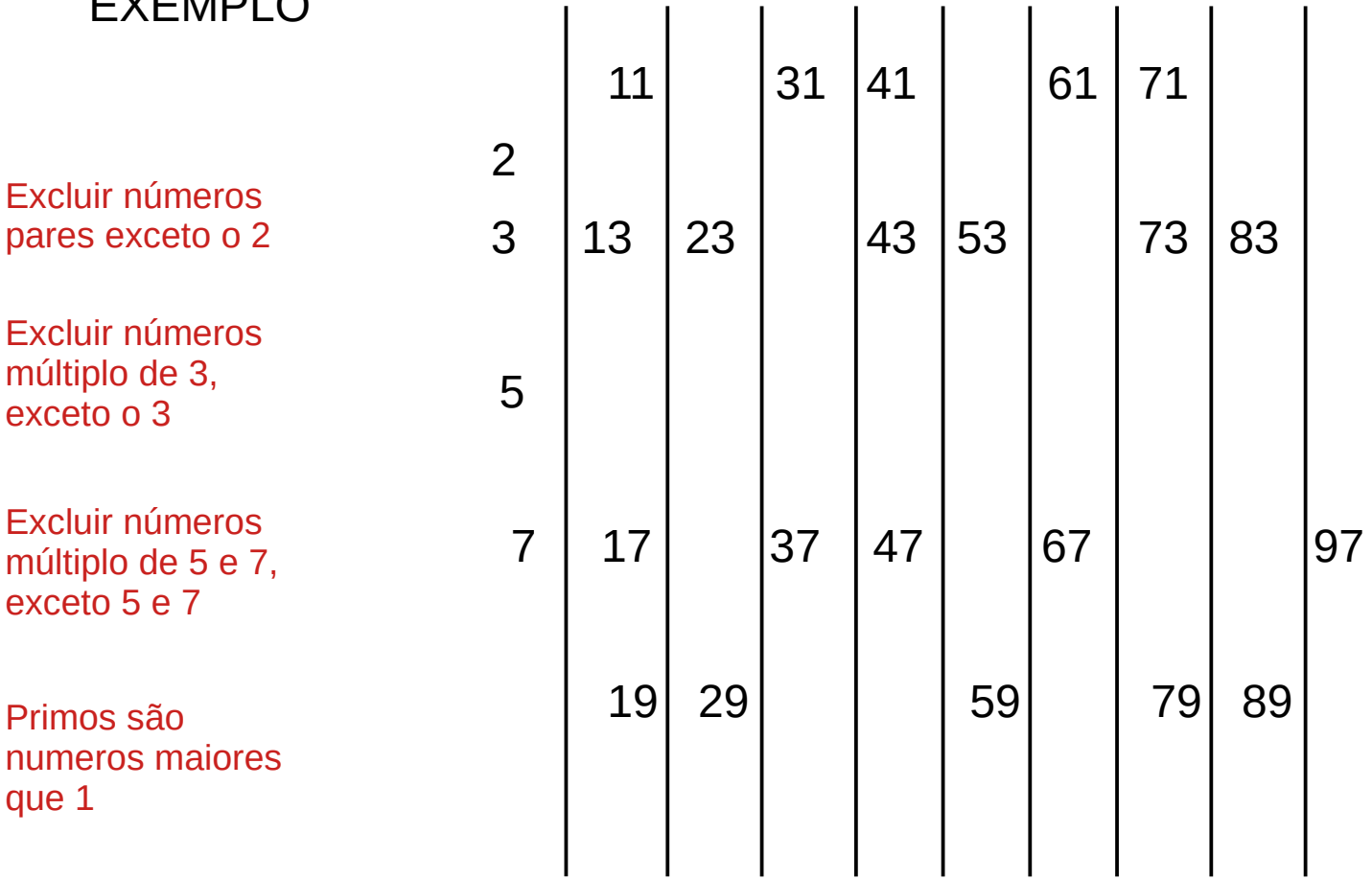
Excluir números múltiplo de 3, exceto o 3

Excluir números múltiplo de 5 e 7, exceto 5 e 7

1	11		31	41		61	71		91
2									
3	13	23		43	53		73	83	
5									
7	17		37	47		67			97
	19	29			59		79	89	

NÚMEROS PRIMOS – CRIVO DE ERASTÓTENES

EXEMPLO



NÚMEROS PRIMOS

Proposições

→ Se p e q são primos e p|q => p=q

→ Se p é primo e p$\nmid$a => mdc(p, a) =1 (demonstrar)

NÚMEROS PRIMOS

Proposições

→ Se p e q são primos e p|q => p=q

→ Se p é primo e p$\not|$a => mdc(p, a) =1 (demonstrar)

PROPRIEDADES:
(Lema de Euclides)

Sejam a, b, p números inteiros

i) se p é primo e p|ab então ou p|a ou p|b (demonstrar – pesquise)

ii) se $p|a^2$ => p|a (demonstrar – pesquise)

NÚMEROS PRIMOS

Exemplo:

Se n é composto, então tem um divisor primo menor ou igual a $\sqrt{n}$

Seja $a \in \mathbb{Z} / 1 < a < n \wedge n = ab$ ou $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$

por contradição:

$$a > \sqrt{n} \wedge b > \sqrt{n}$$

$$a \cdot b > \sqrt{n} \cdot \sqrt{n}$$

$$a \cdot b > n \quad \text{absurdo!}$$

Logo, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$

NÚMEROS PRIMOS

Como saber se N é primo?

* deve-se dividi-lo por todos os primos d para os quais

$$d^2 < N \quad \text{ou} \quad d < \sqrt{N}$$

Exemplo: são primos?

a) 97

b) 143

c)391

NÚMEROS PRIMOS

TEOREMA FUNDAMENTAL DA ARITMÉTICA

Todo inteiro n> 1 ou é primo ou pode ser escrito de forma única como um produto de fatores primos, onde os fatores primos são escritos em ordem não decrescente.

PESQUISAR DEMONSTRAÇÃO – POR INDUÇÃO

NÚMEROS PRIMOS : Primos Gêmeos

→ existem infinitos números primos gêmeos

→ são primos cuja diferença entre eles é a - b = 2

Exemplos:

3 e 5
5 e 7
11 e 13
17 e 19
4967 e 4969
etc

NÚMEROS PRIMOS : Primos de Mersenne

Número de Mersenne: $Mn = 2^n - 1$

* família de números

* quando n é primo, Mn são chamados primos de Mersenne

* nem todo Mn é primo

* muito utilizados em Criptografia

→ Criptogafia:

* números cada vez maiores para a criação de chaves
* tecnologia + rápida → números primos maiores
* utilizam primos de Mersenne

NÚMEROS PRIMOS : Primos de Mersenne

PROPOSIÇÃO:

- Se 2^n-1 é primo, então n é primo.

* o fato de n ser primo não implica Mn primo

Exemplo: $2^2 - 1 = 3$
$2^3 - 1 = 5$
$2^5 - 1 = 31$

O **maior número primo conhecido** é $2^{136\,279\,841} - 1$, que possui 41 024 320 algarismos quando escrito na base 10.

PROPOSIÇÃO:

- Sejam a e n números naturais maiores do que 1. Se a^n-1 é primo, então $a=2$ e n é primo. Equivalentemente, se $a>2$ ou n é composto, então a^n-1 é composto

NÚMEROS PRIMOS : Primos de Mersenne

VEJA:

https://impa.br/notices/por-que-a-descoberta-do-maior-numero-primo-importa/#:~:text=O%20novo%20maior%20n%C3%BAmero%20primo%20da%20hist%C3%B3ria%20%C3%A9%20o,de%20Mersenne%20descoberto%20at%C3%A9%20agora.

NÚMEROS PRIMOS : Conjecturas de GoldBach's

Todo inteiro par n, n>2, é a soma de dois primos.

EXEMPLO:

4 = 2+2
6 = 3+3
8 = 3+5
10 = 5+5
12 = 5+7
14 = 7+7
...

* tal conjectura foi testada para todos os inteiros positivos até $4x10^8$
Mas não existe prova

NÚMEROS PRIMOS

DECOMPOSIÇÃO EM FATORES PRIMOS

Dado um inteiro n , $n \neq -1, 0, 1$. Existem primos $p_1 < \ldots < p_k$ e $\alpha_1, \ldots, \alpha_k$, univocamente determinados, tais que :

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

EXEMPLO:

$480 = 2^5 \cdot 3 \cdot 5 \rightarrow 480 = 2^5 \cdot 3^1 \cdot 5^1 \cdot 7^0$

$560 = 2^4 \cdot 5 \cdot 7 \rightarrow 560 = 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^1$

* vantagem: escrever os dois números utilizando o mesmo conjunto de primos

* desvantagem: expoentes nulos estarão presentes.

Obs: decomposição em fatores primos: potencias positivas em ordem crescente

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \leq \beta_i \leq \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

PESQUISAR

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \le \beta_i \le \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

EXEMPLO: Divisores de 480 e 560

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \le \beta_i \le \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

EXEMPLO: Divisores de 480 e 560

480 = 2^5 . 3 . 5

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \le \beta_i \le \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

EXEMPLO: Divisores de 480 e 560

$480 = 2^5 \cdot 3 \cdot 5$

D(480)

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \le \beta_i \le \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

EXEMPLO: Divisores de 480 e 560

480 = 2^5 . 3 . 5 2 . 3

D(480)

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \le \beta_i \le \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

EXEMPLO: Divisores de 480 e 560

480 = 2^5 . 3 . 5

D(480)

2 . 3
2^2 .3
2^3 . 3
2^4 . 3
2^5 . 3

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

Seja $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ e $\alpha_i \in \mathbb{N}$. Todo divisor positivo de n é da forma

$$n = \pm p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

$$0 \le \beta_i \le \alpha_i \quad , \quad \forall\, i = 1, \dots, k$$

EXEMPLO: Divisores de 480 e 560

480 = 2^5 . 3 . 5

D(480)

2 . 3
2^2 .3
2^3 . 3
2^4 . 3
2^5 . 3

2 . 5
2^2 . 5
2^3 . 5
2^4 . 5
2^5 . 5

3 . 5
2 . 3 . 5
2^2 . 3. 5
2^3 . 3 . 5
2^4 . 3 . 5
2^5 . 3 . 5

NÚMEROS PRIMOS

Suponha que a decomposição de n em fatores primos seja

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Sejam

$$m = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

um divisor de n com $0 \le \beta_i \le \alpha_i$, $\forall i = 1, \dots, k$.

Quantos são os valores possíveis que β_i pode assumir => $\alpha_i + 1$

O número de divisores de n é igual a:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \dots (\alpha_k + 1)$$

NÚMEROS PRIMOS

QUANTIDADE DE DIVISORES DE UM INTEIRO

$$d(n)=(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)...(\alpha_k+1)$$

EXEMPLO: Divisores de 480 e 560

480 = 2^5 . 3 . 5

D(480) = (5+1)(1+1)(1+1) = 6 . 2. 2 = 24

NÚMEROS PRIMOS

EXERCÍCIO:

4) Pesquisar quais são as regras de divisibilidade entre 2 e 11

NÚMEROS PRIMOS

EXERCÍCIO:

4) Pesquisar quais são as regras de divisibilidade entre 2 e 11