

# teoria de números computacional

---

cláudia mendes araújo

2024/2025

lcc+Imat | uminho

## números primos

---

**teorema. (teorema fundamental da aritmética)** Todo o inteiro positivo maior que 1 escreve-se, de modo único, como um produto de primos, com os fatores primos no produto escritos por ordem não decrescente.

Uma aplicação deste resultado é a prova de que  $\sqrt{2}$  é um número irracional:

Suponhamos que  $\sqrt{2}$  é um número racional. Então, podemos escrever

$$\sqrt{2} = \frac{a}{b},$$

onde  $a$  e  $b$  são inteiros primos entre si, com  $b \neq 0$ . Elevando ambos os membros ao quadrado, obtemos

$$2 = \frac{a^2}{b^2},$$

o que implica que

$$2b^2 = a^2.$$

Como 2 divide  $a^2$ , segue-se que 2 também divide  $a$ .

Assim, podemos escrever  $a = 2c$  para algum inteiro  $c$ .

Substituindo na equação anterior, obtemos

$$b^2 = 2c^2.$$

Dado que 2 divide  $b^2$ , conclui-se que 2 também divide  $b$ .

Contudo, isto contradiz a hipótese inicial de que  $a$  e  $b$  são primos entre si, pois 2 não pode dividir simultaneamente ambos.

Esta contradição demonstra que  $\sqrt{2}$  é um número irracional.

Os testes que distinguem entre números primos e compostos são fundamentais. Tais testes são chamados **testes de primalidade**.

Sabemos que, se  $n$  for um número composto, então  $n$  tem um fator primo que não excede  $\sqrt{n}$ .

De facto, sendo  $n$  composto, podemos escrever  $n = ab$ , onde  $a$  e  $b$  são inteiros tais que  $1 < a \leq b < n$ .

Suponhamos que  $a > \sqrt{n}$ . Temos  $b \geq a > \sqrt{n}$ , e, portanto,  $ab > n$ , o que é uma contradição. Sabemos que  $a$  tem um divisor primo, o qual também é divisor de  $n$  e, claramente, não excede  $\sqrt{n}$ .

O teste de primalidade mais básico é a **divisão por tentativa**, que nos diz que um número inteiro  $n$  é primo se e somente se não for divisível por nenhum número primo que não exceda  $\sqrt{n}$ .

### divisão por tentativa ( $n$ é primo?):

testar a divisibilidade de  $n$  pelos primos  $p$  tais que  $p \leq \lfloor \sqrt{n} \rfloor$ .

**exemplo:** Testemos se 531 é primo pela divisão por tentativa.

Tendo em conta que

$$529 = 23^2 < 531 < 24^2 = 576,$$

sabemos que  $23 < \sqrt{531} < 24$ .

Assim,  $\lfloor \sqrt{531} \rfloor = 23$ , pelo que basta percorrer a divisibilidade de 531 pelos primos  $p$  tais que  $p \leq 23$  para averiguar se 531 é ou não primo. 2 não divide 531, mas 3 divide 531, donde 531 não é primo.

**exemplo:** Testemos, agora, se 37 é primo pela divisão por tentativa.

Tendo em conta que

$$36 = 6^2 < 37 < 7^2 = 49,$$

sabemos que  $6 < \sqrt{37} < 7$ .

Assim,  $\lfloor \sqrt{37} \rfloor = 6$ , pelo que basta averiguar a divisibilidade de 37 por 2, 3 e 5. Como  $2 \nmid 37$ ,  $3 \nmid 37$  e  $5 \nmid 37$ , podemos concluir que 37 é primo.

Podemos utilizar o facto de que todo o número composto  $n$  admite um divisor primo que não excede  $\sqrt{n}$  para encontrar todos os números primos menores ou iguais a um dado número positivo  $n$ . Este procedimento é conhecido como **Crivo de Eratóstenes** (300 a.C), pois foi inventado pelo matemático grego Eratóstenes.

crivo de Eratóstenes:

- (1) Listam-se todos os inteiros de 2 a  $n$  de acordo com a ordem usual;
- (2) Eliminam-se, sistematicamente, todos os números compostos, cancelando todos os múltiplos de primos  $p$  (distintos de  $p$ ), com  $p$  tais que  $p \leq \sqrt{n}$ ;
- (3) Os elementos restantes (i.e., os números que não passaram no crivo) são os **primos inferiores a  $n$** .

## crivo de Eratóstenes – exemplo

**exemplo.** Para determinar todos os primos inferiores a 100, começamos por listar todos os naturais de 2 a 100:

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



































































## crivo de Eratóstenes – exemplo

Eliminando os múltiplos de 2 superiores a 2, obtemos:







































































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

## crivo de Eratóstenes – exemplo

Eliminando os múltiplos de 3 distintos deste primo, obtemos:

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			100

Eliminando os múltiplos de 5 distintos de 5, obtemos:

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			100

## crivo de Eratóstenes – exemplo

Por fim, eliminando os múltiplos de 7 distintos deste primo, obtemos os primos inferiores a 100:

	2	3	■	5	■	7	■	■	■
11	■	13	■	■	■	17	■	19	■
■	■	23	■	■	■	■	■	29	■
31	■	■	■	■	■	37	■	■	■
41	■	43	■	■	■	47	■	■	■
■	■	53	■	■	■	■	■	59	■
61	■	■	■	■	■	67	■	■	■
71	■	73	■	■	■	■	■	79	■
■	■	83	■	■	■	■	■	89	■
■	■	■	■	■	■	97	■	■	100

Descrevemos, de seguida, uma técnica de fatorização interessante, embora nem sempre eficiente. Esta técnica, descoberta por **Fermat** (séc. XVII), é conhecida como **fatorização de Fermat** e baseia-se no seguinte lema:

**lema.** Se  $n$  for um número inteiro positivo ímpar, então existe uma correspondência biunívoca entre as fatorizações de  $n$  em dois inteiros positivos e as diferenças de dois quadrados iguais a  $n$ .

**demonstração.** Seja  $n$  um número inteiro positivo ímpar e considere-se uma fatorização  $n = ab$ , com  $a$  e  $b$  inteiros positivos.

Então,  $n$  pode ser escrito como a diferença de dois quadrados:

$$n = ab = s^2 - t^2,$$

onde

$$s = \frac{a+b}{2}, \quad t = \frac{a-b}{2}$$

são ambos inteiros, pois  $a$  e  $b$  são ímpares.

Reciprocamente, se  $n$  for a diferença de dois quadrados, ou seja,  $n = s^2 - t^2$ , então podemos fatorizar  $n$  como:

$$n = (s - t)(s + t).$$

### fatorização de Fermat:

Para aplicar este método, procuramos soluções da equação:

$$n = s^2 - t^2,$$

isto é, procuramos quadrados perfeitos da forma

$$s^2 - n.$$

Note-se que se  $s$  é tal que  $s^2 - n = t^2$ , então,  $s^2 = n + t^2 \geq n$ . Assim,  $s$  tem de ser grande o suficiente para que  $s^2$  seja maior ou igual a  $n$ . O menor valor possível para  $s$  que satisfaça  $s^2 \geq n$  é  $s = \lceil \sqrt{n} \rceil$ .

Assim, para encontrar fatorizações de  $n$ , investigamos a sequência de inteiros:

$$s^2 - n, \quad (s + 1)^2 - n, \quad (s + 2)^2 - n, \quad \dots$$

onde  $s$  é o menor inteiro maior que  $\sqrt{n}$ .

Começamos com  $s = \lceil \sqrt{n} \rceil$  e vamos aumentando  $s$ , verificando se  $s^2 - n$  é um quadrado perfeito.

O pior caso acontece quando  $s$  cresce até atingir  $s = \frac{n+1}{2}$ : neste ponto, a diferença de quadrados torna-se:

$$s^2 - t^2 = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = n,$$

o que equivale à fatorização trivial  $n = n \times 1$ .

Este procedimento garante que a fatorização será eventualmente encontrada.

**exemplo:** Fatorizemos  $n = 5959$  pelo método de Fermat.

Começamos por notar que  $\lceil \sqrt{5959} \rceil = 78$ .

Tomamos  $s = 78$  e calculamos  $s^2 - n$ . Como

$$s^2 - n = 78^2 - 5959 = 85$$

e 85 não é um quadrado perfeito, incrementamos  $s$ .

Consideramos  $s = 79$  e calculamos  $s^2 - n$ . Dado que

$$s^2 - n = 79^2 - 5959 = 244$$

e 244 não é um quadrado perfeito, aumentamos  $s$ .

Tomamos  $s = 80$  e calculamos  $s^2 - n$ . Como

$$s^2 - n = 80^2 - 5959 = 441 = 21^2,$$

encontramos a fatorização

$$\begin{aligned} 5959 &= (80 - 21)(80 + 21) \\ &= 59 \times 101. \end{aligned}$$



A fatorização de Fermat pode ser muito ineficiente. Para fatorizar  $n$  usando esta técnica, pode ser necessário verificar até  $\frac{n+1}{2} - \lfloor \sqrt{n} \rfloor$  números para determinar se são quadrados perfeitos.

Este algoritmo é eficiente quanto temos poucos passos no incremento de  $s$  (até obter  $s^2 - n$  quadrado perfeito).

O método é mais eficaz quando  $n$  tem dois fatores próximos. Se um número tiver um fator pequeno e outro muito grande, o algoritmo pode demorar muito tempo a encontrar a fatorização. Embora raramente seja utilizado para fatorizar números grandes, a sua ideia fundamental serve de base para algoritmos de fatorização mais avançados, amplamente usados em cálculos computacionais.