3 - Números Primos

Números primos - definição

Definição

Um inteiro $p > 1$ diz-se um número primo se 1 e p são os seus únicos divisores positivos.

Exemplo:

7 é um número primo porque os seus divisores positivos são 1 e 7 .

12 não é um número primo uma vez que os seus divisores positivos são: $1, 2, 3, 4, 6, 12$.

Note-se que como 12 não é primo, podemos escrevê-lo como o produto de dois factores inteiros maiores do que 1:

$$12 = 3 \times 4 \qquad \text{ou} \qquad 12 = 2 \times 6$$

razão pela qual dizemos que 12 é um número composto .

Números primos - propriedades

Teorema

Sejam $a, b \in \mathbb{N}$ *e* p *um número primo. Então:*

$$p|ab \quad \Longrightarrow \quad p|a \quad \vee \quad p|b$$

Exemplo : $3|4 \times 9$ e como 3 é primo, temos que ter $3|4$ (falso) ou $3|9$ (verdadeiro).

Exemplo : $6|4 \times 9$ mas no entanto $6 \nmid 4$ e $6 \nmid 9$. Isto acontece porque 6 não é primo.

Corolário

Sejam $a_1, a_2, \cdots, a_n \in \mathbb{N}$ *e* p *um número primo. Então:*

$$p|a_1\ a_2\ \cdots\ a_n \quad \Longrightarrow \quad p|a_i \quad \text{para algum } i$$

Decomposição em números primos

Se um número inteiro n não for primo, ou seja, se for composto, então ele pode escrever-se como o produto de dois factores inteiros: $a > 1$ e $b > 1$, isto é:

$$n = a\,b$$

Se a e/ou b não forem primos, então eles próprios podem ser decompostos como o produto de dois factores inteiros > 1.

Repetindo este processo para todos os factores que não são primos, a certa altura iremos obter n como um produto de um número finito de factores primos.

Ordenando os factores primos por ordem crescente e agrupando os primos repetidos numa única potência, obtemos uma decomposição única para n como um produto de factores primos.

Decomposição em números primos - exemplo

O número 792 é composto, uma vez que é divisível por 2.

Vamos decompor 792 num produto de factores primos:

792	2	$792 = 2 \times 396$
396	2	$396 = 2 \times 198$
198	2	$198 = 2 \times 99$
99	3	$99 = 3 \times 33$
33	3	$33 = 3 \times 11$
11	11	
1		

Logo, $792 = 2 \times 2 \times 2 \times 3 \times 3 \times 11 = 2^3 \times 3^2 \times 11$

Esta decomposição de 792 em factores primos é única .

Teorema fundamental da Aritmética

Teorema

Todo o inteiro $n > 1$ *pode ser decomposto como um produto de números primos, de forma <u>única</u>:*

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

onde,

$p_1 < p_2 < \cdots < p_k$ *são números primos e* $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_k \in \mathbb{N}$.

Divisores positivos

Proposição

Se um inteiro $n > 1$ *tem decomposição em primos:*

$$n = p_1^{\alpha_1} \, p_2^{\alpha_2} \, \cdots \, p_k^{\alpha_k}$$

então os divisores positivos de n *são da forma:*

$$p_1^{\beta_1} \, p_2^{\beta_2} \, \cdots \, p_k^{\beta_k} \qquad \text{com} \qquad 0 \leq \beta_i \leq \alpha_i$$

e o número de divisores positivos de n *é dado por:*

$$(\alpha_1 + 1) \, (\alpha_2 + 1) \, \cdots (\alpha_k + 1)$$

Divisores positivos - exemplo

Já vimos que

$$792 = 2^3 \times 3^2 \times 11$$

Logo o número de divisores positivos de 792 é dado por:

$$(3+1) \times (2+1) \times (1+1) = 4 \times 3 \times 2 = 24$$

Para determinarmos todos os divisores positivos de 792, temos que considerar todas as combinações possíveis para os expoentes dos primos $2, 3$ e 11 .

Para o expoente do primo 2 temos as possibilidades: $0, 1, 2, 3$

Para o expoente do primo 3 temos as possibilidades: $0, 1, 2$

Para o expoente do primo 11 temos as possibilidades: $0, 1$

Divisores positivos - exemplo

Abaixo temos a lista de todos os divisores positivos do inteiro:

$$792 = 2^3 \times 3^2 \times 11$$

1	2	2^2	2^3
3	2×3	$2^2 \times 3$	$2^3 \times 3$
3^2	2×3^2	$2^2 \times 3^2$	$2^3 \times 3^2$
11	2×11	$2^2 \times 11$	$2^3 \times 11$
3×11	$2 \times 3 \times 11$	$2^2 \times 3 \times 11$	$2^3 \times 3 \times 11$
$3^2 \times 11$	$2 \times 3^2 \times 11$	$2^2 \times 3^2 \times 11$	$2^3 \times 3^2 \times 11$

M.D.C. e M.M.C.

Teorema

Sejam n *e* m *inteiros maiores do que* 1*, com a seguinte decomposição em primos:*

$$n = p_1^{\alpha_1} \, p_2^{\alpha_2} \, \cdots \, p_k^{\alpha_k} \qquad\qquad m = q_1^{\beta_1} \, q_2^{\beta_2} \, \cdots \, q_r^{\beta_r}$$

Então

1. *O m.d.c.*(n, m) *é o produto dos primos comuns às duas decomposições, elevados ao menor dos expoentes.*

2. *O m.m.c.*(n, m) *é o produto dos primos comuns e não comuns às duas decomposições, elevados ao maior dos expoentes.*

M.D.C. e M.M.C. - exemplo

Vamos usar a decomposição em primos para calcular m.d.c. e o m.m.c. entre os inteiros 792 e 738.

738	2
369	3
123	3
41	41
1	

Temos então que:

$$792 = 2^3 \times 3^2 \times 11 \qquad 738 = 2 \times 3^2 \times 41$$

e portanto

$$\text{m.d.c.}(792, 738) = 2 \times 3^2 \qquad \text{m.m.c.}(792, 738) = 2^3 \times 3^2 \times 11 \times 41$$

Decomposição em números primos - exemplo

Para decompor um inteiro $n > 1$ em factores primos, ou para testar se esse inteiro é primo, basta procurar divisores de n que sejam primos , até ao valor $\sqrt{n}$, uma vez que

$$n = \sqrt{n} \times \sqrt{n}$$

Exemplo: Queremos decompor 1379 em factores primos.

Como $40 \times 40 = 1600$ temos que $\sqrt{1379} < 40$ e portanto basta testar como divisores os primos até 40.

Por exemplo, 41 é primo, mas se 1379 fosse divisível por 41 teríamos

$$1379 = 41 \times a$$

e portanto a seria um divisor inteiro de 1379 menor do que 40.

Decomposição em números primos - exemplo

O inteiro 1379 não é divisível pelos primos $2, 3, 5$ mas é divisível por 7 . De facto

$$1379 = 7 \times 197$$

Basta-nos agora decompor 197 e para isso basta-nos procurar divisores primos até $\sqrt{197} < 15$.

Como já testamos os primos $2, 3, 5$ basta então testar como divisores os primos $7, 11, 13$.

Como 197 não é divisível pelos primos $7, 11, 13$ então 197 é um número primo. Logo a decomposição de 1379 em factores primos é:

$$1379 = 7 \times 197$$

Existência de uma infinidade de primos

Teorema

Existe uma infinidade de números primos.

Demonstração - Vamos supor que existe um número finito de números primos

$$p_1 < p_2 < \cdots < p_k$$

e seja

$$n = (p_1\ p_2\ \cdots\ p_k) + 1$$

Como $n > p_k$ então n não é primo e portanto existe um primo p_i tal que $p_i | n$. Então,

$$p_i | n = (p_1\ p_2\ \cdots\ p_k) + 1 \quad \wedge \quad p_i | p_1\ p_2\ \cdots\ p_k \quad \Longrightarrow \quad p_i | 1$$

o que é uma contradição pois como p_i é primo, temos que $p_i > 1$.

O Crivo de Eratóstenes

O O Crivo de Eratóstenes é um processo para encontrar todos os inteiros primos até um valor previamente fixado.

Vamos usar esse processo para encontrar todos os primos até 100:

- Começamos por listar todos os inteiros até 100 e riscamos o número 1
- O número seguinte da lista é o 2 (que é *primo*) e riscamos da lista todos os múltiplos de 2
- O número seguinte da lista é o 3 (que é *primo*) e riscamos da lista todos os múltiplos de 3
- O número seguinte da lista é o 5 (que é *primo*) e riscamos da lista todos os múltiplos de 5
- O número seguinte da lista é o 7 (que é *primo*) e riscamos da lista todos os múltiplos de 7

A lista dos números não riscados é a lista de todos os *primos* até 100.

O Crivo de Eratóstenes

1	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

O Crivo de Eratóstenes

1	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

Os números a vermelho constituem a lista dos primos até 100.