

Números Primos e Máximo Divisor Comum

QXD0008 – Matemática Discreta



UNIVERSIDADE
FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Prof. Lucas Ismaily
ismailybf@ufc.br

Universidade Federal do Ceará

2º semestre/2025



Tópicos desta aula

Nesta apresentação:

- Definição formal de números primos
- Verificação de primalidade
- Aplicações de números primos: fatoração
- Conceitos de máximo divisor comum, de mínimo múltiplo comum, e algumas formas de calculá-los



Referências para esta aula

- **Seção 3.5** do livro: [Matemática Discreta e suas Aplicações](#).
Autor: Kenneth H. Rosen. Sexta Edição.
- **Seção 4.3** do livro: [Discrete Mathematics and Its Applications](#).
Author: Kenneth H. Rosen. Seventh Edition. **(English version)**

Introdução



Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Então, dado n inteiro, cada m que divide n satisfaz:

- $m \neq 0$
- se $n \neq 0$, então $|m| \leq |n|$
- se $n > 0$, então $m \leq n$
- m também divide $-n$
- se $n < 0$, então $m \geq n$
- $-m$ também divide n .

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Exemplo:

Quem são os divisores de 3? Cada m que divide 3 satisfaz:

- $m \neq 0$
- se $3 > 0$, então $m \leq 3$
- como $3 \neq 0$, então $|m| \leq 3$
- m também divide -3
- -3 também divide m .

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Exemplo:

Quem são os divisores de 3? Cada m que divide 3 satisfaz:

- $m \neq 0$
- se $3 > 0$, então $m \leq 3$
- como $3 \neq 0$, então $|m| \leq 3$
- m também divide -3
- -3 também divide m .

Ou seja, $-3 \leq m \leq 3$ para todo inteiro m que divide 3.

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Exemplo:

Quem são os divisores de 3? Cada m que divide 3 satisfaz:

- $m \neq 0$
- se $3 > 0$, então $m \leq 3$
- como $3 \neq 0$, então $|m| \leq 3$
- m também divide -3
- -3 também divide m .

ENTÃO, vamos testar cada $-3 \leq m \leq 3$.

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Exemplo:

Quem são os divisores de 3?

- | | | |
|----------------|---------------|---------------|
| • $-3 \mid 3?$ | | • $1 \mid 3?$ |
| • $-2 \mid 3?$ | • $0 \mid 3?$ | • $2 \mid 3?$ |
| • $-1 \mid 3?$ | | • $3 \mid 3?$ |

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Exemplo:

Quem são os divisores de 3?

- | | | |
|------------------|-----------------|-----------------|
| • $-3 \mid 3?$ ✓ | | • $1 \mid 3?$ ✓ |
| • $-2 \mid 3?$ ✗ | • $0 \mid 3?$ ✗ | • $2 \mid 3?$ ✗ |
| • $-1 \mid 3?$ ✓ | | • $3 \mid 3?$ ✓ |

Contando divisores

- **Definição (Divisibilidade):** Sejam a e b números inteiros com $a \neq 0$, dizemos que a **divide** b se e somente se existe um inteiro c tal que $b = ac$.

Lembre-se: Dizemos que a é um **divisor** de b se e somente se a divide b .

Exemplo:

Quem são os divisores de 3?

- | | |
|------------------|-----------------|
| • $-3 \mid 3?$ ✓ | • $1 \mid 3?$ ✓ |
| • $-2 \mid 3?$ ✗ | • $2 \mid 3?$ ✗ |
| • $-1 \mid 3?$ ✓ | • $3 \mid 3?$ ✓ |
| • $0 \mid 3?$ ✗ | |

Assim, 3 tem quatro divisores: -3 , -1 , 1 e 3 .

Contando divisores

- Os tópicos desta aula giram em torno destas perguntas:
 1. **Quem** são os divisores de um inteiro?
 2. **Quantos** são os divisores de um inteiro?
- Por simplicidade, lidaremos apenas com números positivos.

Números Primos



Números Primos

- **Definição (número primo):** Um inteiro $n > 1$ é chamado **primo** se e somente se n tem exatamente dois divisores positivos.
- **Definição (número composto):** Um inteiro $n > 1$ que não é primo é chamado **composto**.

Números Primos

- **Definição (número primo):** Um inteiro $n > 1$ é chamado **primo** se e somente se n tem exatamente dois divisores positivos.
- **Definição (número composto):** Um inteiro $n > 1$ que não é primo é chamado **composto**.

Exemplo:

- 11 é primo, pois seus divisores positivos são 1 e 11 (exatamente 2).

Números Primos

- **Definição (número primo):** Um inteiro $n > 1$ é chamado **primo** se e somente se n tem exatamente dois divisores positivos.
- **Definição (número composto):** Um inteiro $n > 1$ que não é primo é chamado **composto**.

Exemplo:

- 11 é primo, pois seus divisores positivos são 1 e 11 (exatamente 2).
- 15 é composto, pois seus divisores positivos são 1, 3, 5 e 15 (mais que 2).

Números Primos

- **Definição (número primo):** Um inteiro $n > 1$ é chamado **primo** se e somente se n tem exatamente dois divisores positivos.
- **Definição (número composto):** Um inteiro $n > 1$ que não é primo é chamado **composto**.

Números Primos

- **Definição (número primo):** Um inteiro $n > 1$ é chamado **primo** se e somente se n tem exatamente dois divisores positivos.
- **Definição (número composto):** Um inteiro $n > 1$ que não é primo é chamado **composto**.

Note que:

- Para todo $n \neq 0$, temos $1|n$.
- Para todo $n \neq 0$, temos $n|n$.

Números Primos

- **Definição (número primo):** Um inteiro $n > 1$ é chamado **primo** se e somente se n tem exatamente dois divisores positivos.
- **Definição (número composto):** Um inteiro $n > 1$ que não é primo é chamado **composto**.

Note que:

- Para todo $n \neq 0$, temos $1|n$.
- Para todo $n \neq 0$, temos $n|n$.

Portanto...

- ☞ Todo inteiro $n > 1$ tem no mínimo dois divisores positivos.
- ☞ Um inteiro $n > 1$ é primo se e somente se os únicos divisores de n são 1 e n .
- ☞ Um inteiro $n > 1$ é composto se e somente se n tem três ou mais divisores positivos.

Primos: Blocos de construção dos inteiros positivos

Primos: Blocos de construção dos inteiros positivos

- ① Se um inteiro $n > 1$ não é primo, então existe um inteiro positivo k tal que $k|n$ e $1 < k < n$.

Primos: Blocos de construção dos inteiros positivos

- ① Se um inteiro $n > 1$ não é primo, então existe um inteiro positivo k tal que $k|n$ e $1 < k < n$.
- ② Como $k|n$, pela definição de divisibilidade, existe um inteiro positivo c tal que $n = k \cdot c$. Como $1 < k < n$, concluímos também que $1 < c < n$.

Primos: Blocos de construção dos inteiros positivos

- ① Se um inteiro $n > 1$ não é primo, então existe um inteiro positivo k tal que $k|n$ e $1 < k < n$.
- ② Como $k|n$, pela definição de divisibilidade, existe um inteiro positivo c tal que $n = k \cdot c$. Como $1 < k < n$, concluímos também que $1 < c < n$.
- ③ Logo, podemos escrever n como um produto de dois inteiros positivos k e c menores que ele.
 - se um desses divisores não é primo, escrevemo-lo como o produto de dois inteiros menores que ele.

Primos: Blocos de construção dos inteiros positivos

- ① Se um inteiro $n > 1$ não é primo, então existe um inteiro positivo k tal que $k|n$ e $1 < k < n$.
- ② Como $k|n$, pela definição de divisibilidade, existe um inteiro positivo c tal que $n = k \cdot c$. Como $1 < k < n$, concluímos também que $1 < c < n$.
- ③ Logo, podemos escrever n como um produto de dois inteiros positivos k e c menores que ele.
 - se um desses divisores não é primo, escrevemo-lo como o produto de dois inteiros menores que ele.
- ④ Esse processo termina somente com números primos. Fato provado há mais de 2000 anos pelos gregos e é conhecido pelo seguinte teorema:

Primos: Blocos de construção dos inteiros positivos

- ① Se um inteiro $n > 1$ não é primo, então existe um inteiro positivo k tal que $k|n$ e $1 < k < n$.
- ② Como $k|n$, pela definição de divisibilidade, existe um inteiro positivo c tal que $n = k \cdot c$. Como $1 < k < n$, concluímos também que $1 < c < n$.
- ③ Logo, podemos escrever n como um produto de dois inteiros positivos k e c menores que ele.
 - se um desses divisores não é primo, escrevemo-lo como o produto de dois inteiros menores que ele.
- ④ Esse processo termina somente com números primos. Fato provado há mais de 2000 anos pelos gregos e é conhecido pelo seguinte teorema:

Teorema Fundamental da Aritmética: Todo inteiro $n > 1$ pode ser escrito de maneira única como um primo ou como o produto de dois ou mais números primos escritos em ordem crescente.

Teorema Fundamental da Aritmética

Teorema Fundamental da Aritmética: Todo inteiro $n > 1$ pode ser escrito de maneira única como um primo ou como o produto de dois ou mais números primos escritos em ordem crescente.

Exemplos:

- $2 = 2$
- $15 = 3 \cdot 5$
- $20 = 2 \cdot 2 \cdot 5$
- $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37$

Teorema Fundamental da Aritmética

Teorema Fundamental da Aritmética: Todo inteiro $n > 1$ pode ser escrito de maneira única como um primo ou como o produto de dois ou mais números primos escritos em ordem crescente.

Exemplos:

- $2 = 2$
- $15 = 3 \cdot 5$
- $20 = 2 \cdot 2 \cdot 5$
- $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37$

Note que:

- cada primo nestas listas é um **divisor** ou **fator** do número reescrito.
- um produto de primos em ordem crescente é a **fatoração** de um inteiro.

Teste de Primalidade



Teste de Primalidade

- A propriedade de ser um primo é chamada **primalidade**.

Como determinar se um inteiro $n > 1$ é primo?

Teste de Primalidade

- A propriedade de ser um primo é chamada **primalidade**.

Como determinar se um inteiro $n > 1$ é primo?

- **Primeira ideia:** averiguar se n é divisível por todos os números primos k com $1 < k < n$.

Teste de Primalidade

- A propriedade de ser um primo é chamada **primalidade**.

Como determinar se um inteiro $n > 1$ é primo?

- **Primeira ideia:** averiguar se n é divisível por todos os números primos k com $1 < k < n$.
- **Será mesmo preciso testar todos os primos maiores que 1 e menores que n ? Ou podemos nos livrar de testar alguns?**

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.
- Logo, pela definição de um fator de um inteiro positivo, temos que $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.
- Logo, pela definição de um fator de um inteiro positivo, temos que $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
- **Alegação:** Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.
- Logo, pela definição de um fator de um inteiro positivo, temos que $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
- **Alegação:** Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
Suponha, por absurdo, que $a > \sqrt{n}$ e $b > \sqrt{n}$.

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.
- Logo, pela definição de um fator de um inteiro positivo, temos que $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
- **Alegação:** Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
Suponha, por absurdo, que $a > \sqrt{n}$ e $b > \sqrt{n}$. Então $ab > \sqrt{n}\sqrt{n} = n$, o que é uma contradição. Consequentemente, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.
- Logo, pela definição de um fator de um inteiro positivo, temos que $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
- **Alegação:** Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
Suponha, por absurdo, que $a > \sqrt{n}$ e $b > \sqrt{n}$. Então $ab > \sqrt{n}\sqrt{n} = n$, o que é uma contradição. Consequentemente, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
- Logo, n possui um divisor positivo que não é maior que \sqrt{n} .

Teste de Primalidade

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

Demonstração:

- Seja n inteiro composto. Então n possui um fator a , tal que $1 < a < n$.
- Logo, pela definição de um fator de um inteiro positivo, temos que $n = ab$, onde ambos a e b são inteiros positivos maiores que 1.
- **Alegação:** Temos que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
Suponha, por absurdo, que $a > \sqrt{n}$ e $b > \sqrt{n}$. Então $ab > \sqrt{n}\sqrt{n} = n$, o que é uma contradição. Consequentemente, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
- Logo, n possui um divisor positivo que não é maior que \sqrt{n} .
- Esse divisor ou é um primo ou, pelo Teorema Fundamental da Aritmética, possui um divisor primo. Em qualquer dos casos, n possui um divisor primo menor ou igual a \sqrt{n} . □

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.
- Há apenas quatro primos neste intervalo: 2, 3, 5, 7.

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.
- Há apenas quatro primos neste intervalo: 2, 3, 5, 7.
 - $2 \nmid 101$, pois $101 \bmod 2 = 1$.

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.
- Há apenas quatro primos neste intervalo: 2, 3, 5, 7.
 - $2 \nmid 101$, pois $101 \bmod 2 = 1$.
 - $3 \nmid 101$, pois $101 \bmod 3 = 2$.

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.
- Há apenas quatro primos neste intervalo: 2, 3, 5, 7.
 - $2 \nmid 101$, pois $101 \bmod 2 = 1$.
 - $5 \nmid 101$, pois $101 \bmod 5 = 1$.
 - $3 \nmid 101$, pois $101 \bmod 3 = 2$.

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.
- Há apenas quatro primos neste intervalo: 2, 3, 5, 7.
 - $2 \nmid 101$, pois $101 \bmod 2 = 1$.
 - $5 \nmid 101$, pois $101 \bmod 5 = 1$.
 - $3 \nmid 101$, pois $101 \bmod 3 = 2$.
 - $7 \nmid 101$, pois $101 \bmod 7 = 3$.

Teste de Primalidade

Segue do teorema anterior, que:

Corolário. Um inteiro n é primo se ele não é divisível por nenhum primo menor ou igual a \sqrt{n} .

Exemplo: O 101 é primo?

- Precisamos verificar se $p|101$ para cada inteiro $p \leq \sqrt{101}$ que seja primo, ou seja, para cada $p \leq 10$ (arredondando para baixo) que seja primo.
- Há apenas quatro primos neste intervalo: 2, 3, 5, 7.
 - $2 \nmid 101$, pois $101 \bmod 2 = 1$. ◦ $5 \nmid 101$, pois $101 \bmod 5 = 1$.
 - $3 \nmid 101$, pois $101 \bmod 3 = 2$. ◦ $7 \nmid 101$, pois $101 \bmod 7 = 3$.
- Como nenhum primo $p \leq \sqrt{101}$ divide 101, temos que 101 é primo.

Algoritmo de Fatoração



Teorema Fundamental da Aritmética

Voltando ao Teorema Fundamental da Aritmética...

Teorema Fundamental da Aritmética: Todo inteiro $n > 1$ pode ser escrito de maneira única como um primo ou como o produto de dois ou mais números primos escritos em ordem crescente.

Exemplos:

- $2 = 2$
- $15 = 3 \cdot 5$
- $20 = 2 \cdot 2 \cdot 5$
- $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37$
- **Como determinar a fatoração em números primos de um inteiro $n > 1$ qualquer?**

O algoritmo de fatoração

Ideia: Tentar dividir n por um primo de cada vez, em ordem crescente.
Para cada primo visitado, divida o resultado obtido até falhar.

O algoritmo de fatoração

Ideia: Tentar dividir n por um primo de cada vez, em ordem crescente.
Para cada primo visitado, divida o resultado obtido até falhar.

Considere que:

- **Primos** é uma lista inicializada com todos os primos conhecidos em ordem crescente.

O algoritmo de fatoração

Ideia: Tentar dividir n por um primo de cada vez, em ordem crescente.
Para cada primo visitado, divida o resultado obtido até falhar.

Considere que:

- **Primos** é uma lista inicializada com todos os primos conhecidos em ordem crescente.

Algoritmo: Fatoração de n

Entrada: inteiro n .

Saída: Fatoração de n em números primos.

1. **para** k **em** Primos **faça** {
2. **enquanto** $n > 1$ e $k|n$ **faça** {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }

O algoritmo de fatoração

É possível sermos mais eficientes.

- Pelo “Teorema \sqrt{n} ”, podemos parar assim que $k > \sqrt{n}$ mesmo considerando atualizações de n .
- Isso nos permitiria inicializar **Primos** somente com os primos até \sqrt{n} .
- Nesse caso, quando $k > \sqrt{n}$, teremos $n = 1$ ou que n é primo.

O algoritmo de fatoração

É possível termos mais eficientes.

- Pelo “Teorema \sqrt{n} ”, podemos parar assim que $k > \sqrt{n}$ mesmo considerando atualizações de n .
- Isso nos permitiria inicializar **Primos** somente com os primos até \sqrt{n} .
- Nesse caso, quando $k > \sqrt{n}$, teremos $n = 1$ ou que n é primo.

Algoritmo: Fatoração de n (Revisado)

1. **para** k em Primos, **sendo** $k \leq \sqrt{n}$, **faça** {
2. **enquanto** $n > 1$ e $k|n$ **faça** {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. **para** k em Primos, **sendo** $k \leq \sqrt{n}$, **faça** {
2. **enquanto** $n > 1$ e $k|n$ **faça** {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 1 ("Para"):

Variáveis: $k = 2$, $n = 99$ ($k \leq \sqrt{n}$)

Linha 2. Como $2 \nmid 99$, não entramos no **enquanto**

99

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 1 (“Para”):

Variáveis: $k = 2$, $n = 99$ ($k \leq \sqrt{n}$)

Linha 2. Como $2 \nmid 99$, não entramos no **enquanto**

Linha 6. Como $99 \neq 1$, continuamos.

99

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 99$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 \mid 99$, entramos no **enquanto**

99

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ **faça** {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 99$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 \mid 99$, entramos no **enquanto**

Linha 3. imprimimos 3 na saída

99 | 3

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 33$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 \mid 99$, entramos no **enquanto**

Linha 3. imprimimos 3 na saída

Linha 4. e atualizamos n para $99 \text{ div } 3 = 33$

99		3
33		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 33$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 \mid 33$, continuamos no **enquanto**

99		3
33		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 33$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 | 33$, continuamos no **enquanto**

Linha 3. imprimimos 3 na saída

99		3
33		3

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 11$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 | 33$, continuamos no **enquanto**

Linha 3. imprimimos 3 na saída

Linha 4. e atualizamos n para $33 \text{ div } 3 = 11$

99		3
33		3
11		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 11$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 \nmid 11$, saímos do **enquanto**

99		3
33		3
11		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. **para** k em Primos, **sendo** $k \leq \sqrt{n}$, **faça** {
2. **enquanto** $n > 1$ e $k|n$ **faça** {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 2 ("Para"):

Variáveis: $k = 3$, $n = 11$ ($k \leq \sqrt{n}$)

Linha 2. Como $3 \nmid 11$, saímos do **enquanto**

Linha 6. Como $11 \neq 1$, continuamos

99		3
33		3
11		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, sendo $k \leq \sqrt{n}$, faça {
2. enquanto $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. se $n = 1$, encerre.
7. }
8. se $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 3 ("Para"):

Variáveis: $k = 5$, $n = 11$ ($k > \sqrt{n}$)

Linha 1. Como $5 > \sqrt{11}$, saímos do para

99		3
33		3
11		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 3 ("Para"):

Variáveis: $k = 5$, $n = 11$ ($k > \sqrt{n}$)

Linha 1. Como $5 > \sqrt{11}$, saímos do **para**

Linha 8. Como $11 \neq 1$, imprimimos 11 na saída

99		3
33		3
11		11

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 3 ("Para"):

Variáveis: $k = 5$, $n = 11$ ($k > \sqrt{n}$)

Linha 1. Como $5 > \sqrt{11}$, saímos do **para**

Linha 8. Como $11 \neq 1$, imprimimos 11 na saída
atualizamos n para 1

99		3
33		3
11		11
1		

O algoritmo de fatoração

Algoritmo: Fatoração de n (Revisado)

1. para k em Primos, **sendo** $k \leq \sqrt{n}$, faça {
2. **enquanto** $n > 1$ e $k|n$ faça {
3. imprima k na saída
4. $n := n \text{ div } k$
5. }
6. **se** $n = 1$, encerre.
7. }
8. **se** $n \neq 1$, imprima n na saída e encerre.

Executaremos o algoritmo para $n = 99$.

Iteração 3 ("Para"):

Variáveis: $k = 5$, $n = 11$ ($k > \sqrt{n}$)

Linha 1. Como $5 > \sqrt{11}$, saímos do **para**

Linha 8. Como $11 \neq 1$, imprimimos 11 na saída atualizamos n para 1, e encerramos.

$$\begin{array}{r|l}
 99 & 3 \\
 33 & 3 \\
 11 & 11 \\
 1 & \hline
 & 3^2 \cdot 11
 \end{array}$$

Infinitude dos primos



Infinitude dos primos

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Prova da alegação:

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Prova da alegação:

Suponha, por absurdo, que $p_j \mid Q$.

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Prova da alegação:

Suponha, por absurdo, que $p_j \mid Q$. Então, p_j divide o número $Q - p_1 p_2 \cdots p_n = 1$, o que é uma contradição.

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Prova da alegação:

Suponha, por absurdo, que $p_j \mid Q$. Então, p_j divide o número $Q - p_1 p_2 \cdots p_n = 1$, o que é uma contradição.

Então, existe um primo que não está na lista $p_1 p_2 \cdots p_n$.

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Prova da alegação:

Suponha, por absurdo, que $p_j \mid Q$. Então, p_j divide o número $Q - p_1 p_2 \cdots p_n = 1$, o que é uma contradição.

Então, existe um primo que não está na lista $p_1 p_2 \cdots p_n$.

Ou este primo é o Q (se ele for primo) ou ele é um fator primo de Q .

Infinitude dos primos

Teorema. Existe uma quantidade infinita de números primos.

Demonstração:

Por contradição. Suponha que existem finitos números primos p_1, p_2, \dots, p_n .

Seja $Q = p_1 p_2 \cdots p_n + 1$.

Pelo Teorema Fundamental da Aritmética, Q é primo ou pode ser escrito como o produto de dois ou mais primos.

Alegação: Nenhum primo p_j da lista p_1, p_2, \dots, p_n divide Q .

Prova da alegação:

Suponha, por absurdo, que $p_j \mid Q$. Então, p_j divide o número $Q - p_1 p_2 \cdots p_n = 1$, o que é uma contradição.

Então, existe um primo que não está na lista $p_1 p_2 \cdots p_n$.

Ou este primo é o Q (se ele for primo) ou ele é um fator primo de Q .

Isso é uma contradição porque supomos que a lista $p_1 p_2 \cdots p_n$ contém todos os primos. Consequentemente, existem infinitos primos. \square

Infinitude dos primos

Observações:

- Na prova do teorema anterior não sabemos se Q é primo!
- Esse é um exemplo de prova não construtiva para um enunciado existencial.
- Para que essa prova fosse construtiva, nós deveríamos ter dado explicitamente um primo ausente na lista original de n primos.

Encontrando primos: Crivo de Eratóstenes



O Crivo de Eratóstenes

Ideia: Encontrar todos os primos no intervalo $1 < k \leq n$.

O Crivo de Eratóstenes

Ideia: Encontrar todos os primos no intervalo $1 < k \leq n$.

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

O Crivo de Eratóstenes

Ideia: Encontrar todos os primos no intervalo $1 < k \leq n$.

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Executaremos o algoritmo para $n = 100$.

O Crivo de Eratóstenes

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 1:

$k = 2$ não marcado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 1:

$k = 2$ marcado
com “**primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 1:

$k = 2$ marcado com

“**primo**”

e cada múltiplo de 2

identificado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 1:

$k = 2$ marcado com

“**primo**”

e cada múltiplo de 2

marcado com “**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 2:

$k = 3$ não marcado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 2:

$k = 3$ marcado
com “**primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 2:

$k = 3$ marcado
com “**primo**”
e cada múltiplo de 3
identificado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 2:

$k = 3$ marcado

com “**primo**”

e cada múltiplo de 3

marcado com “**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 3:

$k = 4$ marcado
com “**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 4:

$k = 5$ não marcado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 4:

$k = 5$ marcado
com “**primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 4:

$k = 5$ marcado
com “**primo**”
e cada múltiplo de 5
identificado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Iteração 4:

$k = 5$ marcado

com “**primo**”

e cada múltiplo de 5

marcado com “**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Avançando um pouco...

Iteração 6:

$k = 7$ marcado
com “**primo**”
e cada múltiplo de 7
identificado

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Avançando um pouco...

Iteração 6:

$k = 7$ marcado

com “**primo**”

e cada múltiplo de 7

marcado com “**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 1)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até n **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”

Avançando até o fim.

Iteração 99:

$k = 100$ marcado
como “**não-primo**”

	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

A execução do algoritmo já estaria completa após a iteração 10, pois:

(Teorema \sqrt{n}): Se n é um inteiro composto, então n possui um divisor primo menor ou igual a \sqrt{n} .

- Para verificarmos se números de 2 a n são primos ou compostos, basta executar o Crivo de Eratóstenes com testes por primos até \sqrt{n} .

O Crivo de Eratóstenes

Algoritmo: Crivo de Eratóstenes (Versão 2)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até \sqrt{n} **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”
6. **para** j de k até n **faça**
7. **se** j não marcado, marque com “**primo**”

Avançando um pouco...

Iteração 6:

$k = 7$ marcado

com “**primo**”

e cada múltiplo de 7

marcado com “**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 2)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até \sqrt{n} **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”
6. **para** j de k até n **faça**
7. **se** j não marcado, marque com “**primo**”

Avançando mais um pouco...

Iteração 9:

$k = 10$ marcado com
“**não-primo**”

	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

Algoritmo: Crivo de Eratóstenes (Versão 2)

1. Adicione todos os inteiros de 2 a n a uma lista.
2. **para** k de 2 até \sqrt{n} **faça**
3. **se** k não estiver marcado **faça**
4. marque k com “**primo**”
5. marque cada múltiplo de k com “**não-primo**”
6. **para** j de k até n **faça**
7. **se** j não marcado, marque com “**primo**”

**E então executamos
o segundo laço**

Logo após Iteração 9:

cada número
não marcado deverá ser
marcado com “**primo**”

	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

Distribuição dos números primos



Distribuição dos números primos

- Vimos que existe uma quantidade infinita de números primos.

Distribuição dos números primos

- Vimos que existe uma quantidade infinita de números primos.
- A sequência de primos apresenta uma certa irregularidade. Vemos grandes “lacunas” e também primos que são muito próximos.
 - Quão grande são essas lacunas?

Distribuição dos números primos

- Vimos que existe uma quantidade infinita de números primos.
- A sequência de primos apresenta uma certa irregularidade. Vemos grandes “lacunas” e também primos que são muito próximos.
 - Quão grande são essas lacunas?
- Vamos provar que essas lacunas ficam cada vez maiores quando consideramos números cada vez maiores.

Distribuição dos números primos

- Vimos que existe uma quantidade infinita de números primos.
- A sequência de primos apresenta uma certa irregularidade. Vemos grandes “lacunas” e também primos que são muito próximos.
 - Quão grande são essas lacunas?
- Vamos provar que essas lacunas ficam cada vez maiores quando consideramos números cada vez maiores.

Para isso, precisaremos da seguinte definição:

- **Definição (Fatorial):** Para todo inteiro positivo n , o produto de todos os inteiros de 1 até n é chamado de **fatorial de n** e é denotado por $n!$.
 - Equivalentemente, $n! = 1 \cdot 2 \cdot 3 \cdots n$.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Demonstração:

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Demonstração:

- Seja n um inteiro positivo. Seja $x = (n + 1)! + 2$.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Demonstração:

- Seja n um inteiro positivo. Seja $x = (n + 1)! + 2$.
- Vamos mostrar que nenhum dos números $x, x + 1, x + 2, \dots, x + (n - 1)$ é primo. Como essa é uma sequência de n inteiros positivos consecutivos, isso é suficiente para provar o teorema.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Demonstração:

- Seja n um inteiro positivo. Seja $x = (n + 1)! + 2$.
- Vamos mostrar que nenhum dos números $x, x + 1, x + 2, \dots, x + (n - 1)$ é primo. Como essa é uma sequência de n inteiros positivos consecutivos, isso é suficiente para provar o teorema.
- Para ver que x não é primo, note que:

$$x = (n + 1)! + 2$$

$$x = (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1)) + 2$$

$$= 2 \cdot [(1 \cdot 3 \cdot 4 \cdots (n + 1)) + 1].$$

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Demonstração:

- Seja n um inteiro positivo. Seja $x = (n + 1)! + 2$.
- Vamos mostrar que nenhum dos números $x, x + 1, x + 2, \dots, x + (n - 1)$ é primo. Como essa é uma sequência de n inteiros positivos consecutivos, isso é suficiente para provar o teorema.
- Para ver que x não é primo, note que:

$$\begin{aligned}x &= (n + 1)! + 2 \\x &= (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1)) + 2 \\&= 2 \cdot [(1 \cdot 3 \cdot 4 \cdots (n + 1)) + 1].\end{aligned}$$

Assim, x pode ser escrito como o produto de dois inteiros positivos menores. Então, x não é primo.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

- Para ver que $x + 1$ não é primo, note que:

$$\begin{aligned}x + 1 &= (n + 1)! + 3 \\&= (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1)) + 3 \\&= 3 \cdot [(1 \cdot 3 \cdot 4 \cdots (n + 1)) + 1].\end{aligned}$$

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

- Para ver que $x + 1$ não é primo, note que:

$$\begin{aligned}x + 1 &= (n + 1)! + 3 \\&= (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1)) + 3 \\&= 3 \cdot [(1 \cdot 3 \cdot 4 \cdots (n + 1)) + 1].\end{aligned}$$

Assim, $x + 1$ pode ser escrito como o produto de dois inteiros positivos menores. Então, $x + 1$ não é primo.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

- Para ver que $x + 1$ não é primo, note que:

$$\begin{aligned}x + 1 &= (n + 1)! + 3 \\&= (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1)) + 3 \\&= 3 \cdot [(1 \cdot 3 \cdot 4 \cdots (n + 1)) + 1].\end{aligned}$$

Assim, $x + 1$ pode ser escrito como o produto de dois inteiros positivos menores. Então, $x + 1$ não é primo.

- Assim como fizemos para x e $x + 1$, fazemos para os demais números da sequência. De fato, esse mesmo raciocínio é naturalmente generalizado para os demais casos.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

- Generalizando, considere um número $x + i$ com $0 \leq i \leq n - 1$.

Distribuição dos números primos

Teorema. Para todo inteiro positivo n , existem n inteiros compostos consecutivos.

Continuação da Demonstração:

- Generalizando, considere um número $x + i$ com $0 \leq i \leq n - 1$.
- Então,

$$\begin{aligned}x + i &= (n + 1)! + (i + 2) \\&= (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1)) + (i + 2) \\&= (i + 2) \cdot [(1 \cdot 2 \cdot 3 \cdots (i + 1) \cdot (i + 3) \cdots (n + 1)) + 1].\end{aligned}$$

Então, $x + i$ não é primo, para $0 \leq i \leq n - 1$.

Portanto, existem n inteiros compostos consecutivos. □

Aplicações da Fatoração de Inteiros



Aplicações da Fatoração de Inteiros

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.

Aplicações da Fatoração de Inteiros

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.

Exemplos

- $2^{10} = 1024$
- $2^{20} = 1048576$
- $2^{30} = 1073741824$
- $2^{10} \cdot 3^{10} = 60466176$
- $2^{10} \cdot 5^{10} = 10000000000$
- $3^{10} \cdot 5^{10} = 576650390625$

Aplicações da Fatoração de Inteiros

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.
- **Todos os divisores de n podem ser obtidos pela fatoração de n .**

Aplicações da Fatoração de Inteiros

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.
- **Todos os divisores de n podem ser obtidos pela fatoração de n .**

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

Note que:

1. Primos cujo expoente não foram anotados têm expoente igual a 1.
2. Primos que não foram anotados têm expoente igual a 0.

Ou seja, calculamos $99 = 3^2 \cdot 11 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 17^0 \dots$

Aplicações da Fatoração de Inteiros

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.
- **Todos os divisores primos de n estão na fatoração de n .**

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

Do ponto de vista de que $99 = 3^2 \cdot 11 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 17^0 \dots$

- | | |
|---|--|
| • Não existe nenhum k múltiplo de 2 tal que $k \mid 99$ | • $11 \mid 99$ |
| • $3 \mid 99$ | • Não existe nenhum k múltiplo de 13 tal que $k \mid 99$ |
| • Não existe nenhum k múltiplo de 5 tal que $k \mid 99$ | • Não existe nenhum k múltiplo de 17 tal que $k \mid 99$ |
| • Não existe nenhum k múltiplo de 7 tal que $k \mid 99$ | • \dots |

Aplicação: Encontrar Divisores

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.
- Todos os divisores primos de n estão na fatoração de n .

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

Todos os divisores de 99 codificados na sua forma fatorada:

- | | | |
|-------------------------|-------------------------|-------------------------|
| • $3^0 \cdot 11^0 = 1$ | • $3^1 \cdot 11^0 = 3$ | • $3^2 \cdot 11^0 = 9$ |
| • $3^0 \cdot 11^1 = 11$ | • $3^1 \cdot 11^1 = 33$ | • $3^2 \cdot 11^1 = 99$ |

Independente de como escrevemos 99, seus divisores serão os mesmos, mas a forma fatorada revela também os primos que aparecem na fatoração desses divisores.

Aplicação: Encontrar Divisores

- A fatoração de um número determina de que número estamos falando.
 - Números diferentes têm fatorações diferentes.
- Podemos representar números muito grandes usando números relativamente pequenos.
- Todos os divisores primos de n estão na fatoração de n .

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

Todos os divisores de 99 codificados na sua forma fatorada:

- | | | |
|-------------------------|-------------------------|-------------------------|
| • $3^0 \cdot 11^0 = 1$ | • $3^1 \cdot 11^0 = 3$ | • $3^2 \cdot 11^0 = 9$ |
| • $3^0 \cdot 11^1 = 11$ | • $3^1 \cdot 11^1 = 33$ | • $3^2 \cdot 11^1 = 99$ |

Então basta variarmos os expoentes de cada primo de 0 até o valor de expoente que esse primo apresenta na fatoração de n para encontrarmos todos os divisores de n .

Aplicação: Calcular Quantidade de Divisores

E se quisermos saber apenas **quantos** divisores um número tem?

A fatoração do número também diz isso.

Aplicação: Calcular Quantidade de Divisores

E se quisermos saber apenas **quantos** divisores um número tem?

A fatoração do número também diz isso.

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

E vimos que basta variarmos os expoentes de cada primo de 0 até o valor de expoente que esse primo apresenta na fatoração de n para encontrarmos todos os divisores de n .

Aplicação: Calcular Quantidade de Divisores

E se quisermos saber apenas **quantos** divisores um número tem?

A fatoração do número também diz isso.

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

E vimos que basta variarmos os expoentes de cada primo de 0 até o valor de expoente que esse primo apresenta na fatoração de n para encontrarmos todos os divisores de n .

Então...

- se variarmos o expoente de 3 de 0 até 2, teremos 3 possíveis valores.
- se variarmos o expoente de 11 de 0 até 1, teremos 2 possíveis valores.

Aplicação: Calcular Quantidade de Divisores

E se quisermos saber apenas **quantos** divisores um número tem?

A fatoração do número também diz isso.

Exemplo

Calculamos anteriormente que $99 = 3^2 \cdot 11$

E vimos que basta variarmos os expoentes de cada primo de 0 até o valor de expoente que esse primo apresenta na fatoração de n para encontrarmos todos os divisores de n .

Então...

- se variarmos o expoente de 3 de 0 até 2, teremos 3 possíveis valores.
- se variarmos o expoente de 11 de 0 até 1, teremos 2 possíveis valores.

Como os expoentes são independentes,
devemos multiplicar os números de possíveis valores.

Concluimos, portanto, que 99 tem $3 \cdot 2 = 6$ divisores.

Aplicação: Calcular Quantidade de Divisores

Exemplo

Pelo Algoritmo de Fatoração, encontraremos que $120 = 2^3 \cdot 3^1 \cdot 5^1$

Então...

- se variarmos o expoente de 2 de 0 até 3, teremos 4 possíveis valores.
- se variarmos o expoente de 3 de 0 até 1, teremos 2 possíveis valores.
- se variarmos o expoente de 5 de 0 até 1, teremos 2 possíveis valores.

**Como os expoentes são independentes,
devemos multiplicar os números de possíveis valores.**

Concluimos, portanto, que 120 tem $4 \cdot 2 \cdot 2 = 16$ divisores.

Aplicação: Calcular Quantidade de Divisores

Exemplo

Pelo Algoritmo de Fatoração, encontraremos que $120 = 2^3 \cdot 3^1 \cdot 5^1$

De fato, 120 tem 16 divisores...

- | | | | |
|----------------------------------|----------------------------------|----------------------------------|-----------------------------------|
| ● $2^0 \cdot 3^0 \cdot 5^0 = 1$ | ● $2^1 \cdot 3^0 \cdot 5^0 = 2$ | ● $2^2 \cdot 3^0 \cdot 5^0 = 4$ | ● $2^3 \cdot 3^0 \cdot 5^0 = 8$ |
| ● $2^0 \cdot 3^0 \cdot 5^1 = 5$ | ● $2^1 \cdot 3^0 \cdot 5^1 = 10$ | ● $2^2 \cdot 3^0 \cdot 5^1 = 20$ | ● $2^3 \cdot 3^0 \cdot 5^1 = 40$ |
| ● $2^0 \cdot 3^1 \cdot 5^0 = 3$ | ● $2^1 \cdot 3^1 \cdot 5^0 = 6$ | ● $2^2 \cdot 3^1 \cdot 5^0 = 12$ | ● $2^3 \cdot 3^1 \cdot 5^0 = 24$ |
| ● $2^0 \cdot 3^1 \cdot 5^1 = 15$ | ● $2^1 \cdot 3^1 \cdot 5^1 = 30$ | ● $2^2 \cdot 3^1 \cdot 5^1 = 60$ | ● $2^3 \cdot 3^1 \cdot 5^1 = 120$ |

Máximo Divisor Comum



Máximo Divisor Comum

- **Definição (Máximo divisor comum):** Sejam a e b dois inteiros, pelo menos um deles diferente de zero. O **máximo divisor comum** de a e b é o maior inteiro d tal que $d \mid a$ e $d \mid b$.
- O máximo divisor comum de a e b é denotado por $\text{MDC}(a, b)$
- Denotamos por $D(a)$ o conjunto dos divisores de a .

Máximo Divisor Comum

- **Definição (Máximo divisor comum):** Sejam a e b dois inteiros, pelo menos um deles diferente de zero. O **máximo divisor comum** de a e b é o maior inteiro d tal que $d \mid a$ e $d \mid b$.
- O máximo divisor comum de a e b é denotado por $\text{MDC}(a, b)$
- Denotamos por $D(a)$ o conjunto dos divisores de a .

Exemplo:

Dados os inteiros 3 e 5, temos que:

- $D(3) = \{1, 3\}$, $D(5) = \{1, 5\}$ e $\text{MDC}(5, 3) = 1$

Máximo Divisor Comum

- **Definição (Máximo divisor comum):** Sejam a e b dois inteiros, pelo menos um deles diferente de zero. O **máximo divisor comum** de a e b é o maior inteiro d tal que $d \mid a$ e $d \mid b$.
- O máximo divisor comum de a e b é denotado por $\text{MDC}(a, b)$
- Denotamos por $D(a)$ o conjunto dos divisores de a .

Exemplo:

Dados os inteiros 3 e 5, temos que:

- $D(3) = \{1, 3\}$, $D(5) = \{1, 5\}$ e $\text{MDC}(5, 3) = 1$

Obs.1: para quaisquer dois inteiros não negativos a e b , temos que $D(a) \cap D(b) \neq \emptyset$, pois $1 \mid a$ e $1 \mid b$.

Obs.2: Como já sabemos calcular divisores de um número por fatoração, temos como calcular os divisores comuns a dois ou mais números.

Obs.3: E se sabemos encontrar divisores comuns a dois ou mais números, podemos indentificar o maior deles!

Máximo Divisor Comum

Estratégia 1: Calcular os divisores dos dois números e compará-los.

Cálculo do MDC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

- $99 = 3^2 \cdot 11^1$
- $120 = 2^3 \cdot 3^1 \cdot 5^1$

Cálculo do MDC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

- $99 = 3^2 \cdot 11^1$
- $120 = 2^3 \cdot 3^1 \cdot 5^1$

Então calculamos que:

1. $D(99) = \{1, 3, 9, 11, 33, 99\}$
2. $D(120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$

Cálculo do MDC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

- $99 = 3^2 \cdot 11^1$
- $120 = 2^3 \cdot 3^1 \cdot 5^1$

Então calculamos que:

1. $D(99) = \{1, 3, 9, 11, 33, 99\}$
2. $D(120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$

Comparando as listas, os únicos divisores comuns de 99 e 120 são 1 e 3.

Portanto, $MDC(99, 120) = 3$.

Máximo Divisor Comum

Obs.2: Como já sabemos calcular divisores de um número por fatoração, temos como calcular os divisores comuns a dois ou mais números.

Obs.3: E se sabemos encontrar divisores comuns a dois ou mais números, **podemos indentificar o maior deles!**

Estratégia 2: Calcular o MDC a partir dos **fatores comuns**.

Cálculo do MDC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

- $99 = 3^2 \cdot 11^1$
- $120 = 2^3 \cdot 3^1 \cdot 5^1$

Cálculo do MDC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

- $99 = 3^2 \cdot 11^1$
- $120 = 2^3 \cdot 3^1 \cdot 5^1$

Note que:

1. Todo divisor de 99 é combinação de $(3^0, 3^1, 3^2)$ com $(11^0, 11^1)$.
2. Todo divisor de 120 é combinação de $(2^0, 2^1, 2^2, 2^3)$ com $(3^0, 3^1)$ e com $(5^0, 5^1)$.

Cálculo do MDC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

- $99 = 3^2 \cdot 11^1$
- $120 = 2^3 \cdot 3^1 \cdot 5^1$

Note que:

1. Todo divisor de 99 é combinação de $(3^0, 3^1, 3^2)$ com $(11^0, 11^1)$.
2. Todo divisor de 120 é combinação de $(2^0, 2^1, 2^2, 2^3)$ com $(3^0, 3^1)$ e com $(5^0, 5^1)$.

Então os divisores comuns de 99 e 120 **só podem ser** combinações de 3^0 ou 3^1 , o que nos permite construir apenas os números 1 e 3.

Portanto, $\text{MDC}(99, 120) = 3$.

Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

Então, $\text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$.

Demonstração:

Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

Demonstração:

A fim de provar que esta fórmula para $\text{MDC}(a, b)$ é válida, devemos mostrar que o inteiro do lado direito da igualdade divide ambos a e b e que não existe nenhum inteiro maior que também o faça.

Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

Demonstração:

A fim de provar que esta fórmula para $\text{MDC}(a, b)$ é válida, devemos mostrar que o inteiro do lado direito da igualdade divide ambos a e b e que não existe nenhum inteiro maior que também o faça.

De fato, este inteiro divide a e b porque o expoente de cada primo p_j na fórmula não excede o expoente que p_j tem tanto na fatoração de a quanto na fatoração de b .

Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

Demonstração:

A fim de provar que esta fórmula para $\text{MDC}(a, b)$ é válida, devemos mostrar que o inteiro do lado direito da igualdade divide ambos a e b e que não existe nenhum inteiro maior que também o faça.

De fato, este inteiro divide a e b porque o expoente de cada primo p_j na fórmula não excede o expoente que p_j tem tanto na fatoração de a quanto na fatoração de b .

Além disso, nenhum inteiro maior pode dividir a e b porque os expoentes dos primos nesta fórmula não pode ser incrementado, e nenhum outro primo pode ser incluído.



Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

Então, $\text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$.

Exemplo

Pelo Algoritmo da Fatoração, encontramos que $99 = 3^2 \cdot 11^1$ e
 $120 = 2^3 \cdot 3^1 \cdot 5^1$

Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

Exemplo

Pelo Algoritmo da Fatoração, encontramos que $99 = 3^2 \cdot 11^1$ e

$$120 = 2^3 \cdot 3^1 \cdot 5^1$$

Os primos que ocorrem com expoentes positivos nestas fatorações são 2, 3, 5 e 11.

Então, percebamos estas fatorações como $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e

$$120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$$

Cálculo do MDC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

Então, $\text{MDC}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$.

Exemplo

Pelo Algoritmo da Fatoração, encontramos que $99 = 3^2 \cdot 11^1$ e
 $120 = 2^3 \cdot 3^1 \cdot 5^1$

Os primos que ocorrem com expoentes positivos nestas fatorações são 2, 3, 5 e 11.

Então, percebamos estas fatorações como $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e
 $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$

Logo, $\text{MDC}(120, 99) = 2^{\min(0,3)} \cdot 3^{\min(2,1)} \cdot 5^{\min(0,1)} \cdot 11^{\min(1,0)}$
 $= 2^0 \cdot 3^1 \cdot 5^1 \cdot 11^0 = 3$

Mínimo Múltiplo Comum



Cálculo do MMC

Definição

Dados dois inteiros a e b diferentes de zero, o mínimo múltiplo comum de a e b é o menor inteiro positivo d tal que $a \mid d$ e $b \mid d$.

Cálculo do MMC

Definição

Dados dois inteiros a e b diferentes de zero, o mínimo múltiplo comum de a e b é o menor inteiro positivo d tal que $a \mid d$ e $b \mid d$.

Notação

A função $\text{MMC}(a, b)$ retorna o mínimo múltiplo comum de a, b .

Cálculo do MMC

Definição

Dados dois inteiros a e b diferentes de zero, o mínimo múltiplo comum de a e b é o menor inteiro positivo d tal que $a \mid d$ e $b \mid d$.

Notação

A função $\text{MMC}(a, b)$ retorna o mínimo múltiplo comum de a, b .

Onde o MMC aparece?

Mínimo múltiplo comum aparece quando queremos adicionar duas frações:

- para adicionar duas frações com denominadores a e b , iniciamos reescrevendo-os com o denominador comum $\text{MMC}(a, b)$.
- **Exemplo:** Somar $\frac{1}{6} + \frac{1}{4}$.

Como $\text{MMC}(6, 4) = 12$, temos que $\frac{2}{12} + \frac{3}{12} = \frac{5}{12}$.

Cálculo do MMC

Podemos calcular o MMC de a e b a partir de seus múltiplos.

- Para encontrar múltiplos de um número, basta multiplicá-lo pelos inteiros positivos.
- **Mas cada inteiro terá infinitos múltiplos positivos, dificultando encontrarmos os números que se repetem nas duas listas.**

Cálculo do MMC

Podemos calcular o MMC de a e b a partir de seus múltiplos.

- Para encontrar múltiplos de um número, basta multiplicá-lo pelos inteiros positivos.
- **Mas cada inteiro terá infinitos múltiplos positivos, dificultando encontrarmos os números que se repetem nas duas listas.**

Estratégia 1: Calcular o MMC a partir dos **fatores comuns**.

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Note que:

- Todo múltiplo de 99 precisa reter os fatores 3^2 e 11^1 .
- Todo múltiplo de 120 precisa reter os fatores 2^3 , 3^1 e 5^1 .

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Note que:

- Todo múltiplo de 99 precisa reter os fatores 3^2 e 11^1 .
- Todo múltiplo de 120 precisa reter os fatores 2^3 , 3^1 e 5^1 .

Então, o menor múltiplo comum de 99 e 120 terá estes fatores e nada mais. Além disso, como $3^1 \mid 3^2$, basta usarmos 3^2 para incluir os dois fatores de base 3.

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Note que:

- Todo múltiplo de 99 precisa reter os fatores 3^2 e 11^1 .
- Todo múltiplo de 120 precisa reter os fatores 2^3 , 3^1 e 5^1 .

Então, o menor múltiplo comum de 99 e 120 terá estes fatores e nada mais. Além disso, como $3^1 \mid 3^2$, basta usarmos 3^2 para incluir os dois fatores de base 3.

Portanto, $\text{MMC}(99, 120) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1 = 3960$.

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

$$\text{MDC}(99, 120) = 3960$$

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

$$\text{MDC}(99, 120) = 3960$$

Observe que:

- $3960 \text{ div } 99 = 40.$
- $3960 \text{ div } 120 = 33.$

Cálculo do MMC

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

$$\text{MDC}(99, 120) = 3960$$

Observe que:

- $3960 \text{ div } 99 = 40.$
- $3960 \text{ div } 120 = 33.$

Ou seja, a estratégia de calcular múltiplos de cada número para comparar as duas listas exigiria ao menos 40 múltiplos de 99 e 33 múltiplos de 120, o que não é nada eficiente.

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

Então, $\text{MMC}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$.

Demonstração:

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MMC}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}.$$

Demonstração:

A fórmula dada para $\text{MMC}(a, b)$ é válida porque um mínimo múltiplo comum de a e b tem pelo menos $\max(a_i, b_i)$ fatores p_i na sua fatoração prima.

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MMC}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}.$$

Demonstração:

A fórmula dada para $\text{MMC}(a, b)$ é válida porque um mínimo múltiplo comum de a e b tem pelo menos $\max(a_i, b_i)$ fatores p_i na sua fatoração prima.

Além disso, o mínimo múltiplo comum não tem nenhum outro fator primo além daqueles que estão em a e b . □

Cálculo do MMC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

Então, $\text{MMC}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$.

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Cálculo do MMC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

Então, $\text{MMC}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$.

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Os primos que ocorrem com expoentes positivos nestas fatorações são 2, 3, 5 e 11.

Então convém entendermos estas fatorações como $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

Cálculo do MMC

Teorema. Dados a e b inteiros positivos, considere que p_1, p_2, \dots, p_n são todos os primos que ocorrem com expoentes positivos nas fatorações de a ou de b . Isto nos permite escrever que

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$\text{Então, } \text{MMC}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}.$$

Exemplo

Pelo Algoritmo de Fatoração, encontramos que

$$99 = 3^2 \cdot 11^1 \quad \text{e} \quad 120 = 2^3 \cdot 3^1 \cdot 5^1$$

Os primos que ocorrem com expoentes positivos nestas fatorações são 2, 3, 5 e 11.

Então convém entendermos estas fatorações como $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

$$\begin{aligned} \text{Então, } \text{MMC}(99, 120) &= 2^{\max(0,3)} \cdot 3^{\max(2,1)} \cdot 5^{\max(0,1)} \cdot 11^{\max(1,0)} \\ &= 2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1 = 3960 \end{aligned}$$

Cálculo do MMC a partir do MDC

Teorema. Sejam a, b inteiros positivos.
Então, $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Exemplo

Anteriormente, calculamos $\text{MMC}(99, 120) = 3960$ e $\text{MDC}(99, 120) = 3$.

Note que:

- $3960 \cdot 3 = 11880$
- $99 \cdot 120 = 11880$

Ou seja, $\text{MMC}(99, 120) \cdot \text{MDC}(99, 120) = 99 \cdot 120$, como diz o teorema.

Cálculo do MMC a partir do MDC

Teorema. Sejam a, b inteiros positivos.
Então, $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Exemplo

Anteriormente, calculamos $\text{MMC}(99, 120) = 3960$ e $\text{MDC}(99, 120) = 3$.

Note que:

- $3960 \cdot 3 = 11880$
- $99 \cdot 120 = 11880$

Mas por que isso acontece?

Lembre que $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

Cálculo do MMC a partir do MDC

Teorema. Sejam a, b inteiros positivos. Então
 $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Exemplo

Anteriormente, calculamos $\text{MMC}(99, 120) = 3960$ e $\text{MDC}(99, 120) = 3$.

Note que:

- $3960 \cdot 3 = 11880$
- $99 \cdot 120 = 11880$

Mas por que isso acontece?

Lembre que $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

Daí, calculamos

$$\text{MDC}(99, 120) = 2^{\min(0,3)} \cdot 3^{\min(2,1)} \cdot 5^{\min(0,1)} \cdot 11^{\min(1,0)}$$

Cálculo do MMC a partir do MDC

Teorema. Sejam a, b inteiros positivos. Então
 $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Exemplo

Anteriormente, calculamos $\text{MMC}(99, 120) = 3960$ e $\text{MDC}(99, 120) = 3$.

Note que:

- $3960 \cdot 3 = 11880$
- $99 \cdot 120 = 11880$

Mas por que isso acontece?

Lembre que $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

Daí, calculamos

$$\text{MDC}(99, 120) = 2^{\min(0,3)} \cdot 3^{\min(2,1)} \cdot 5^{\min(0,1)} \cdot 11^{\min(1,0)} = 2^0 \cdot 3^1 \cdot 5^0 \cdot 11^0$$

Cálculo do MMC a partir do MDC

Teorema. Sejam a, b inteiros positivos. Então
 $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Exemplo

Anteriormente, calculamos $\text{MMC}(99, 120) = 3960$ e $\text{MDC}(99, 120) = 3$.

Note que:

- $3960 \cdot 3 = 11880$
- $99 \cdot 120 = 11880$

Mas por que isso acontece?

Lembre que $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

Daí, calculamos

$$\text{MDC}(99, 120) = 2^{\min(0,3)} \cdot 3^{\min(2,1)} \cdot 5^{\min(0,1)} \cdot 11^{\min(1,0)} = 2^0 \cdot 3^1 \cdot 5^0 \cdot 11^0$$

$$\text{e } \text{MMC}(99, 120) = 2^{\max(0,3)} \cdot 3^{\max(2,1)} \cdot 5^{\max(0,1)} \cdot 11^{\max(1,0)}$$

Cálculo do MMC a partir do MDC

Teorema. Sejam a, b inteiros positivos. Então
 $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Exemplo

Anteriormente, calculamos $\text{MMC}(99, 120) = 3960$ e $\text{MDC}(99, 120) = 3$.

Note que:

- $3960 \cdot 3 = 11880$
- $99 \cdot 120 = 11880$

Mas por que isso acontece?

Lembre que $99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$ e $120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$.

Daí, calculamos

$$\text{MDC}(99, 120) = 2^{\min(0,3)} \cdot 3^{\min(2,1)} \cdot 5^{\min(0,1)} \cdot 11^{\min(1,0)} = 2^0 \cdot 3^1 \cdot 5^0 \cdot 11^0$$

$$\text{e } \text{MMC}(99, 120) = 2^{\max(0,3)} \cdot 3^{\max(2,1)} \cdot 5^{\max(0,1)} \cdot 11^{\max(1,0)} = 2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1$$

Cálculo do MMC a partir do MDC

Nossos números são:

$$99 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1$$

$$120 = 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0$$

$$\text{MDC}(99, 120) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 11^0$$

$$\text{MMC}(99, 120) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1$$

Logo,

$$\begin{aligned} 99 \cdot 120 &= (2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1) \cdot (2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0) \\ &= 2^0 \cdot 3^2 \cdot 5^0 \cdot 11^1 \cdot 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^0 \\ &= 2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1 \cdot 2^0 \cdot 3^1 \cdot 5^0 \cdot 11^0 \\ &= (2^3 \cdot 3^2 \cdot 5^1 \cdot 11^1) \cdot (2^0 \cdot 3^1 \cdot 5^0 \cdot 11^0) \\ &= \text{MMC}(99, 120) \cdot \text{MDC}(99, 120) \end{aligned}$$

Exercício

- (1) Prove que: para quaisquer dois números c e d , tem-se que $\min(c, d) + \max(c, d) = c + d$.

Usando o enunciado do exercício acima, prove o seguinte teorema:

Teorema. Sejam a, b inteiros positivos.
Então, $\text{MMC}(a, b) \cdot \text{MDC}(a, b) = a \cdot b$.

Dica: Use também as fatorações em números primos de a e b e as fórmulas para $\text{MDC}(a, b)$ e $\text{MMC}(a, b)$ (vistas nesta aula) em termos destas fatorações.

FIM

