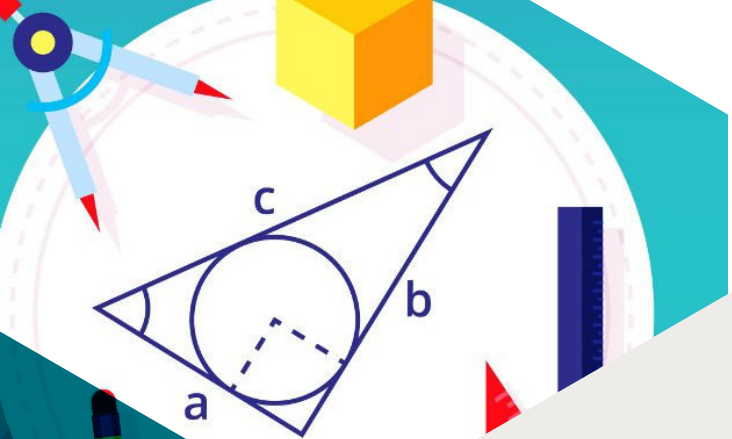


ELEMENTOS DE ARITMÉTICA

Aula 05

Números Primos. O Teorema Fundamental da Aritmética.

Karla Lima

Sumário

Números Primos

Introdução

Os números primos são essenciais em muitos campos da matemática e têm diversas aplicações:

- **Criptografia:** os números primos são a base de muitos algoritmos de criptografia, como o algoritmo RSA. A segurança desses algoritmos depende da dificuldade de fatorar grandes números em seus fatores primos. Isso é fundamental para garantir a segurança de transações financeiras online, comunicações seguras e muitas outras formas de troca de informações sensíveis.

Introdução

- **Matemática Computacional:** Os números primos desempenham um papel importante em várias áreas da computação, como na geração de números aleatórios, na fatoração de números inteiros e na otimização de algoritmos.

Introdução

- **Codificação de Dados:** Em muitos sistemas de comunicação e armazenamento de dados, os números primos são usados em esquemas de codificação para garantir a integridade dos dados e facilitar a detecção de erros.

Introdução

- **Modelagem em Física e Ciência:** Em áreas como a física, os números primos também podem emergir em modelos matemáticos que descrevem fenômenos naturais, como na teoria dos números quânticos.

Introdução

- **Teoria dos Números:** Os números primos são fundamentais para o estudo da teoria dos números, que investiga as propriedades dos números e suas relações. Problemas clássicos como o Último Teorema de Fermat, a Conjectura de Goldbach e a Hipótese de Riemann estão intrinsecamente ligados aos números primos.

Introdução

- Último Teorema de Fermat (veja esse vídeo com a história desse problema):
  - Foi proposto pelo matemático Pierre de Fermat no século XVII.
  - Ele diz o seguinte: para a equação

$$x^n + y^n = z^n$$

    não há solução para x, y, z inteiros positivos para $n > 2$.
  - Foi um dos problemas mais famosos e difíceis da matemática. Só foi provado em 1994 por Andrew Wiles.
  - É uma generalização do Teorema de Pitágoras, fazendo $n = 2$. Nesse caso, há soluções inteiras positivas x, y, z.

Problemas do Milênio

- A Conjectura de Goldbach e a Hipótese de Riemann são dois dos sete Problemas do Milênio, que são problemas matemáticos importantes e desafiadores estabelecidos pelo Clay Mathematics Institute em 2000.
- Resolver qualquer um desses problemas resulta em uma recompensa de um milhão de dólares.

Problemas do Milênio

- A Conjectura de Goldbach: veja esse vídeo com a história desse problema.
- É uma ideia matemática que diz que todo número par maior que 2 pode ser escrito como a soma de dois números primos.
- Por exemplo, 4 é $2 + 2$, 6 é $3 + 3$, 8 é $3 + 5$, e assim por diante.
- Embora tenha sido testada para números muito grandes, ainda não foi provada de forma geral, então continua sendo uma conjectura, uma ideia que os matemáticos ainda estão tentando provar ou desaprovar.

Problemas do Milênio

- A Hipótese de Riemann: veja esse vídeo com a história desse problema.
- Em 1859, Bernhard Riemann escreveu uma certa fórmula $\zeta(x)$, chamada função zeta. Ela já aparecera em trabalhos de Euler de 1740, mas Riemann estendeu a definição para os números complexos, e mostrou que essa função nos diz muita coisa sobre os números primos.
- Uma questão crucial era quais são os zeros, ou seja, os valores de x tais que $\zeta(x) = 0$.

Problemas do Milênio

- À parte os pares negativos -2, -4, -6 etc., Riemann sabia que existem muitos outros zeros, e acreditava que todos têm parte real igual a $1/2$.
- Não sendo capaz de provar, aceitou esse fato como hipótese, deduzindo vários resultados a partir dele.
- Muitos matemáticos fizeram o mesmo desde então, resultando em dúzias de teoremas “provisórios”, cuja validade depende de que alguém prove a hipótese.

Definição

Definição 1

Um número natural diferente de 1 *e que é apenas múltiplo de 1 e de si próprio é chamado de* ***número primo****. Um número diferente de 1 que* ***não é primo*** *é chamado de* ***número composto****.*

Definição

Definição 1

Um número natural diferente de 1 *e que é apenas múltiplo de 1 e de si próprio é chamado de* ***número primo****. Um número diferente de 1 que* ***não é primo*** *é chamado de* ***número composto****.*

- Por exemplo, os números 2, 3, 5 e 7 são números primos.
- Já os números 4, 6 e 8 são números compostos, por serem múltiplos de 2.
- O número 1 não é nem primo nem composto.

Exemplos

1. Diga quais dos seguintes números são primos e quais são compostos:

$$9, 10, 11, 12, 13, 15, 17, 21, 23, 47, 49.$$

Exemplos

1. Diga quais dos seguintes números são primos e quais são compostos:

$$9, 10, 11, 12, 13, 15, 17, 21, 23, 47, 49.$$

2. Os números compostos são em número infinito, pois os números pares diferentes de 2 são em número infinito. Justifique tal afirmação.

Quantos primos existem?

- Quantos são os números primos?
- Euclides de Alexandria (300 a.C.), mostrou que existem **INFINITOS**.
- Como ele fez isso? Veremos um pouco mais adiante.

Encontrar Números Primos

- Determinar se um dado número é primo ou composto pode ser uma tarefa muito árdua.
- Para se ter uma ideia da dificuldade, você saberia dizer se o número 241 é primo?

Encontrar Números Primos

Muito mais difícil é decidir se o número 4294967297 é primo ou composto. Dois dos maiores matemáticos da história divergiram na resposta:

- O matemático francês Pierre de Fermat (1601-1655) afirmou que esse número é primo.
- O matemático suíço Leonhard Euler (1707-1783) afirmou que é composto.
- Quem tinha razão? Também veremos um pouco mais adiante.

O Crivo de Eratóstenes

O **Crivo de Eratóstenes** é um método simples e eficiente para encontrar todos os números primos até um certo limite. Funciona assim:

- Começando com uma lista de números de 2 até o limite desejado, marque o número 2 como primo.
- Em seguida, remova todos os múltiplos de 2 da lista, pois eles não podem ser primos.
- Depois disso, marque o próximo número não marcado na lista como primo (que será 3). Repita o processo, removendo os múltiplos do número marcado mais recentemente e marcando o próximo número não marcado como primo. Continue até que todos os números na lista tenham sido marcados ou removidos. Os números restantes na lista são todos primos.

O Crivo de Eratóstenes

- Repita o processo, removendo os múltiplos do número marcado mais recentemente e marcando o próximo número não marcado como primo.
- Continue até que todos os números na lista tenham sido marcados ou removidos.
- Os números restantes na lista são todos primos.

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

- Múltiplos de 2
- Múltiplos de 3
- Múltiplos de 5
- Múltiplos de 7

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

- Os elementos da primeira linha que são primos: 2, 3, 5 e 7.
- Os números restantes, abaixo da primeira linha, em preto são os números primos que estão entre 1 e 50.

Encontrar Números Primos

- Encontrar números primos é difícil principalmente por causa da sua natureza aleatória e dispersa.
- Os números primos não seguem um padrão previsível.
- Eles podem aparecer aparentemente aleatoriamente em qualquer lugar na sequência numérica, tornando difícil prever onde encontrá-los.

Encontrar Números Primos

- À medida que você avança na sequência numérica, a densidade de números primos diminui.
- Isso significa que, à medida que você busca por números primos maiores, precisa verificar uma quantidade cada vez maior de números não primos entre eles.

O Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética

- O Teorema Fundamental da Aritmética é como uma "receita"que diz que você pode sempre "quebrar"qualquer número natural maior que 1 em seus ingredientes básicos (números primos), e que essa "receita"é única, exceto pela ordem em que você escreve os ingredientes.

O Teorema Fundamental da Aritmética

- Por exemplo, se você pegar o número 12, pode **ser fatorado** em 2 x 2 x 3. Esses são números primos (2 e 3), e quando você os multiplica juntos, obtém 12.
- Não importa como você faça a fatoração, sempre terá 2, 2 e 3 como fatores primos.

O Teorema Fundamental da Aritmética

- O teorema diz também que a **ordem** em que você escreve esses números primos **não importa**.
- Por exemplo, você poderia ter escrito 3 x 2 x 2 em vez de 2 x 2 x 3. Ainda assim, o resultado seria o mesmo: 12.

Teorema

Teorema 1

(O Teorema Fundamental da Aritmética) *Dado um número $a \geq 2$, existem um número $r > 0$, os números primos $p_1 < p_2 < \cdots < p_r$ e números não nulos $n_1, n_2, \ldots, n_r$ tais que*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r};$$

além disso, esta escrita é única.

Exemplo

Exemplo 1

Decomponha em produtos de primos os seguintes números: 4, 6, 8, 28, 84 e 320.

Quantos Primos Existem?

Nosso objetivo é explicar a demonstração de Euclides, para a seguinte proposição:

Proposição 1

*Existem **INFINITOS** números primos.*

- O método utilizado na prova é chamado de **redução ao absurdo**.
- Suponha que existem **finitos** números primos, todos listados no conjunto

$$P = \{p_1, p_2, \ldots, p_n\}.$$

Quantos Primos Existem?

- Considere o número $x = 1 + p_1 p_2 \cdots p_n$.
- Temos que $x > p_1, x > p_2, \ldots, x > p_n$.
- Logo, x é um número composto, pois é maior (e, portanto, diferente) do que qualquer número primo.
- Sendo x composto, ele seria múltiplo de algum número primo p_i, listado em P.

Quantos Primos Existem?

Vimos na aula anterior a seguinte proposição:

Sejam dados números naturais a, b e c tais que a é múltiplo de c. Então

$a + b$ é múltiplo de c se, e somente se, b é múltiplo de c.

Quantos Primos Existem?

- Como $p_1 p_2 \cdots p_n$ é múltiplo de qualquer um dos primos listados, pela proposição, temos que

$$1 + p_1 p_2 \cdots p_n \text{ é múltiplo de } p_i \text{ se, e somente se, 1 é múltiplo de } p_i.$$

- Mas 1 não é múltiplo de nenhum primo, apenas de si próprio.
- Chegamos num **absurdo**!

Quantos Primos Existem?

- O absurdo foi gerado pela suposição de que x é um número composto.
- Logo, x é um número primo.
- Mas é um número primo diferente de qualquer número primo listado em P.
- Portanto, outro absurdo. Agora vindo da suposição de que existem **finitos** números primos.

Quantos Primos Existem?

- Com essa demonstração, concluímos que dado qualquer conjunto finito de números primos, sempre conseguimos um número primo diferente dos listados.

Resumindo a Demonstração de Euclides

1. **Suposição Contrária:** A prova começa com a negação da tese que queremos provar. No caso da infinitude de números primos, Euclides começa supondo que há apenas um número finito de números primos.
2. **Construção de um Novo Primo:** Com essa suposição em mente, Euclides considera o produto de todos esses supostos primos finitos e adiciona 1 a esse produto.
   Esse novo número resultante não pode ser múltiplo de nenhum dos números primos em nossa lista finita, pois, se fosse, o número 1 também seria múltiplo do mesmo número primo.

Resumindo a Demonstração de Euclides

3. **Contradição:** Portanto, esse novo número primo é ou ele mesmo um número primo não contido em nossa lista original ou então possui fatores primos que não estão na lista. Em ambos os casos, isso contradiz nossa suposição inicial de que há apenas um número finito de números primos.
4. **Conclusão:** Como a suposição inicial leva a uma contradição lógica, devemos concluir que nossa suposição estava errada.
   Portanto, deve haver, de fato, uma quantidade infinita de números primos.

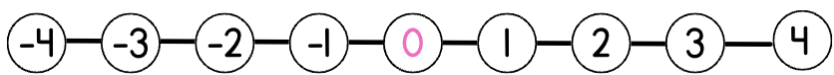
Os Números Inteiros

Introdução

- Até o momento, dados dois números naturais a e b, o número $b - a$ só foi definido quando $b > a$.
- **Caso b $<$ a:** Quando só se tinha os números naturais, haviam situações em que surgiam questões de "falta"ou "dívida", que não podiam ser adequadamente expressas usando apenas números naturais.
- **Caso a $=$ b:** O mesmo ocorria para representação da ausência de quantidade ou valor.

Introdução

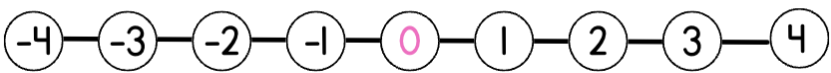
- Os números inteiros foram criados para preencher lacunas nos números naturais e para fornecer uma estrutura matemática mais robusta que pudesse lidar com uma variedade maior de problemas e situações da vida real.



- O zero atua como um ponto de referência fundamental na linha numérica.

Introdução

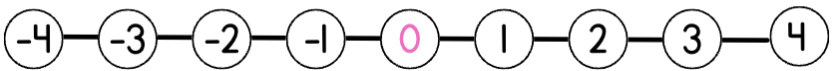
- O zero divide os números em positivos e negativos, fornecendo uma base para a contagem e representação de valores.



- **Inteiros Positivos:** estão à direita do zero.
- **Inteiros Negativos:** estão à esquerda do zero.

Introdução

- Os números 1 e -1, 2 e -2, 3 e -3 etc. são chamados de **números simétricos**.



- Cada par possui a mesma distância para o número zero.
- O elemento 0 não é nem positivo, nem negativo, é o seu próprio simétrico.

O Simétrico

Representando por $-a$ o simétrico de a, seja ele positivo, negativo ou nulo, temos sempre que

$$-(-a) = a.$$

Ou seja,

- $-(-1) = 1$ (O simétrico do número -1 é o 1);
- $-[-(-3)] = -3$ (O simétrico do simétrico de -3 é o próprio -3).

Notação

- Usamos o símbolo $\mathbb{Z}$ para representar o conjunto dos números inteiros.

Operações e Propriedades

- A operação de adição é estendida aos números inteiros.
- A adição continua tendo as propriedades comutativa e associativa e é compatível com a relação de ordem.

Operações e Propriedades

- A diferença $b - a$, é o número obtido deslocando b para a esquerda a posições, se $a > 0$.
- A diferença $b - a$, é o número obtido deslocando b para a direita a posições, se $a < 0$.
- No caso em que $a = b$, temos $a - a = 0$.
- Temos $a + 0 = 0 + a = a$, pois o zero indica que não movemos o número de lugar.

Operações e Propriedades

- Escrevemos

$$a - b = a + (-b).$$

- Ou seja, a subtração $a - b$ nada mais é do que somar a ao simétrico de b.

Operações e Propriedades

- A multiplicação nos números inteiros é definida como segue:
  - Se $a, b > 0$, então a multiplicação se dá como nos números naturais.
  - Se $a = 0$, então $0 \cdot b = 0$.
  - Se Se $a, b > 0$, então:

$$(-a) \cdot b = a \cdot (-b) = -(a\cdot)$$

e

$$(-a) \cdot (-b) = a \cdot b.$$

Problemas

Problema 1

Problema 1

Mostre que em $\mathbb{Z}$, continua valendo a propriedade:

$$\text{Se } a, b, c \in \mathbb{Z}, \text{ com } a + c = b + c, \text{ então } a = b.$$

Problema 2

Problema 2

Mostre que em $\mathbb{Z}$, continua valendo a propriedade:

$$\text{Se } a, b \in \mathbb{Z}\text{, então } (b - a) + a = b \text{ e } (a + b) - b = a.$$

Problema 3

Problema 3

Mostre com exemplos que a subtração não é uma operação nem comutativa, nem associativa. Com isso, discorra sobre a vantagem em pensar nela como $a - b = a + (-b)$.

Problema 4

Problema 4

Mostre que se $a \cdot c = b \cdot c$, com $c \neq 0$, então $a = b$.

Problema 5

Problema 5

Sobre a compatibilidade com a ordem:

- *Se* $a < b$ *e* $c > 0$*, então* $c \cdot a < b \cdot c$*.*
- *Porém, se* $c < 0$*, mostre que* $c \cdot a < b \cdot c$ *não é verdade.*