Primos e Maiores Divisores Comuns
Matemática Discreta

Prof. MSc. Samy Sá

Universidade Federal do Ceará
Campus de Quixadá

17 de março de 2014

Outline

Números Primos

Encontrando Números Primos

Resultados Importantes

Conjecturas e Problemas em Aberto

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Outline

Números Primos

Encontrando Números Primos

Resultados Importantes

Conjecturas e Problemas em Aberto

Números Primos

- São considerados os blocos básicos de construção da aritmética.
- Essenciais para criptografia moderna.
- O conceito de número primo é baseado no de divisibilidade.

Números Primos

Todo inteiro maior que 1 tem dois ou mais divisores.

Definição

Um inteiro p maior que 1 *é dito primo se os únicos divisores positivos de p são* 1 *e p. Dizemos que um inteiro positivo maior que* 1 *que não é primo é um número composto.*

Exemplo

O número 11 *é primo, pois seus únicos divisores positivos são* 1 *e* 11*. O número* 15 *é composto, pois seus divisores são* $1, 3, 5, 15$*.*

Números Primos

Todo inteiro maior que 1 tem dois ou mais divisores.

Definição

Um inteiro p maior que 1 é dito primo se os únicos divisores positivos de p são 1 e p. Dizemos que um inteiro positivo maior que 1 que não é primo é um número composto.

Exemplo

O número 11 é primo, pois seus únicos divisores positivos são 1 e 11. O número 15 é composto, pois seus divisores são $1, 3, 5, 15$.

Constatação:

Um inteiro n é composto se e somente se existir um inteiro a tal que $a|n$ e $1 < a < n$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Teorema Fundamental da Aritmética

Os primos são os blocos básicos de construção da aritmética.

Teorema

Todo inteiro maior que 1 *pode ser escrito de maneira única como um primo ou o produto de dois ou mais números primos escritos em ordem cescente.*

Teorema Fundamental da Aritmética

Os primos são os blocos básicos de construção da aritmética.

Teorema

Todo inteiro maior que 1 *pode ser escrito de maneira única como um primo ou o produto de dois ou mais números primos escritos em ordem cescente.*

Exemplo

- $100 = 2.2.5.5$
- $641 = 641$
- $999 = 3.3.3.37$
- $1024 = 2.2.2.2.2.2.2.2.2.2$

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Encontrando Fatorações

O método principal envolve tentativa e erro:

1. Tente dividir o número por 2... (repita até falhar)
2. Tente dividir o número por 3... (repita até falhar)
3. Tente dividir o número por 5... (repita até falhar)

...

Essa dificuldade é base para a criptografia moderna, pois dificulta encontrar os números capazes de decodificar uma mensagem.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Prova

Se n é composto, existe $a|n$ *tal que* $1 < a < n$.

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Prova

Se n é composto, existe $a|n$ *tal que* $1 < a < n$. *Logo,* $n = ab$, *onde* $a, b \in \mathbb{Z}_+$ *e* $a, b > 1$.

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Prova

Se n é composto, existe $a|n$ *tal que* $1 < a < n$.*Logo,* $n = ab$*, onde* $a, b \in \mathbb{Z}_+$ *e* $a, b > 1$.*Mostraremos que* $a \leq \sqrt{n}$ *ou* $b \leq \sqrt{n}$.

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Prova

Se n é composto, existe $a|n$ *tal que* $1 < a < n$. *Logo,* $n = ab$, *onde* $a, b \in \mathbb{Z}_+$ *e* $a, b > 1$. *Mostraremos que* $a \leq \sqrt{n}$ *ou* $b \leq \sqrt{n}$. *Por contradição, suponha que* $a > \sqrt{n}$ *e* $b > \sqrt{n}$.

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Prova

Se n é composto, existe $a|n$ *tal que* $1 < a < n$. *Logo,* $n = ab$, *onde* $a, b \in \mathbb{Z}_+$ *e* $a, b > 1$. *Mostraremos que* $a \leq \sqrt{n}$ *ou* $b \leq \sqrt{n}$. *Por contradição, suponha que* $a > \sqrt{n}$ *e* $b > \sqrt{n}$. *Nesse caso,* $ab > \sqrt{n}\sqrt{n} = n$, *um absurdo.*

Encontrando Fatorações

Alguns resultados que veremos facilitam implementações.

Teorema

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

Prova

Se n é composto, existe $a|n$ *tal que* $1 < a < n$. *Logo,* $n = ab$, *onde* $a, b \in \mathbb{Z}_+$ *e* $a, b > 1$. *Mostraremos que* $a \leq \sqrt{n}$ *ou* $b \leq \sqrt{n}$. *Por contradição, suponha que* $a > \sqrt{n}$ *e* $b > \sqrt{n}$. *Nesse caso,* $ab > \sqrt{n}\sqrt{n} = n$, *um absurdo. Logo,* $a \leq \sqrt{n}$ *ou* $b \leq \sqrt{n}$ *e n tem ao menos um divisor primo menor ou igual a* $\sqrt{n}$. ■

Outline

Números Primos

Encontrando Números Primos

Resultados Importantes

Conjecturas e Problemas em Aberto

Encontrando Números Primos

Alguns resultados que veremos facilitam implementações.

Teorema

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

Encontrando Números Primos

Alguns resultados que veremos facilitam implementações.

Teorema

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

Constatação:

Basta procurarmos fatores primos até $\sqrt{n}$.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Encontrando Números Primos

Alguns resultados que veremos facilitam implementações.

Teorema

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

Constatação:

Basta procurarmos fatores primos até $\sqrt{n}$.

Exemplo

Considere fatorar o número 101. *Os únicos primso que não excedem* $\sqrt{101}$ *são* $2, 3, 5, 7$. *Como* 101 *não é divisível por nenhum destes,* 101 *é primo.*

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Encontrando Números Primos

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

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

Integers divisible by 3 other than 3 receive an underline.

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

Integers divisible by 5 other than 5 receive an underline.

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

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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

Figura: Método: A Colheita de Eratosthenes

Outline

Números Primos

Encontrando Números Primos

Resultados Importantes

Conjecturas e Problemas em Aberto

Números Primos

PERGUNTA:

Quantos números primos existem?

Números Primos

PERGUNTA:

Quantos números primos existem?

Teorema

Existem infinitos números primos.

Números Primos

PERGUNTA:

Quantos números primos existem?

Teorema

Existem infinitos números primos.

Prova

Suponha que existem apenas uma quantidade finita de primos n, a dizer, os números $p_1, p_2, \ldots, p_n$.

Números Primos

PERGUNTA:

Quantos números primos existem?

Teorema

Existem infinitos números primos.

Prova

Suponha que existem apenas uma quantidade finita de primos n, a dizer, os números $p_1, p_2, ..., p_n$. Considere

$$Q = p_1.p_2.....p_n + 1.$$

Números Primos

PERGUNTA:
Quantos números primos existem?

Teorema
Existem infinitos números primos.

Prova
Suponha que existem apenas uma quantidade finita de primos n, a dizer, os números $p_1, p_2, ..., p_n$. *Considere*

$$Q = p_1.p_2.....p_n + 1.$$

Pelo teorema fundamental da aritmética, Q deve ter um divisor primo diferente de 1 *e de Q ou será primo*

Números Primos

PERGUNTA:
Quantos números primos existem?

Teorema
Existem infinitos números primos.

Prova
Suponha que existem apenas uma quantidade finita de primos n, a dizer, os números $p_1, p_2, ..., p_n$. *Considere*

$$Q = p_1.p_2.....p_n + 1.$$

Pelo teorema fundamental da aritmética, Q deve ter um divisor primo diferente de 1 *e de Q ou será primo , mas nenhum número primo conhecido* $p_1, p_2, ..., p_n$ *divide Q.*

Números Primos

PERGUNTA:
Quantos números primos existem?

Teorema
Existem infinitos números primos.

Prova
Suponha que existem apenas uma quantidade finita de primos n, a dizer, os números $p_1, p_2, ..., p_n$. *Considere*

$$Q = p_1.p_2.....p_n + 1.$$

Pelo teorema fundamental da aritmética, Q deve ter um divisor primo diferente de 1 *e de Q ou será primo , mas nenhum número primo conhecido* $p_1, p_2, ..., p_n$ *divide Q.Portanto, Q é primo ou tem divisores primos não listados.* ■

Busca por Números Primos

- Programas de computador para encontrar novos primos são objeto de pesquisa.
- Conhecemos primos grandes como $2^{43.112.609} - 1$, um primo de Mersenne.

Universidade Federal do Ceará
Computer Science Department
Samy Sá (samy@ufc.br)

Busca por Números Primos

- Programas de computador para encontrar novos primos são objeto de pesquisa.
- Conhecemos primos grandes como $2^{43.112.609} - 1$, um primo de Mersenne.

PERGUNTA:

Com que frequência os primos aparecem?

Busca por Números Primos

PERGUNTA:

Com que frequência os primos aparecem?

Teorema

A razão entre números de primos que não excedem x e $x/\ln x$ se aproxima de 1 à medida que x cresce em direção ao infinito.

Progressões Aritméticas e Primos

- Todo número inteiro ímpar está em uma das duas progressões $4k + 1$ ou $4k + 3$.
- Cada progressão $ak + b$ em que a, b não têm divisores comuns contém infinitos primos.

Outline

Números Primos

Encontrando Números Primos

Resultados Importantes

Conjecturas e Problemas em Aberto

Funções para Primos

Seria útil encontrarmos uma função $f(n)$ para definir primos.

Conjectura:

Considere a função $f(n) = n^2 - n + 41$. É certo que $f(n)$ é primo para todo n.

Funções para Primos

Seria útil encontrarmos uma função $f(n)$ para definir primos.

Conjectura:

Considere a função $f(n) = n^2 - n + 41$. *É certo que* $f(n)$ *é primo para todo* n.

Constatação:

Podemos verificar que a função gera números primos para todo $n \leq 40$, *mas a afirmação é falsa. Se* $n = 41$, *teremos* $f(n) = 41^2 - 41 - 41 = 41.41 - 2.41 = 41.39$, *divisível por* 3.

Conjectura de Goldbach

Conjectura:

Todo número ímpar maior que 5 *é a soma de três primos.*

Conjectura de Goldbach

Conjectura:

Todo número ímpar maior que 5 *é a soma de três primos.*

- Antes da criação de computadores, a conjectura já havia sido verificada para milhões de inteiros.
- Até o meio de 2011, todos os inteiros até $1,6.10^{18}$ haviam sido verificados.

Conjectura de Goldbach

Conjectura:

Todo número ímpar maior que 5 *é a soma de três primos.*

- Antes da criação de computadores, a conjectura já havia sido verificada para milhões de inteiros.
- Até o meio de 2011, todos os inteiros até $1,6.10^{18}$ haviam sido verificados.
- Resultados mais fracos foram provados:
  1. Todo inteiro mairo que 2 é a soma de no máximo 6 números primos. [Ramaré, 1995]

Conjectura de Goldbach

Conjectura:

Todo número ímpar maior que 5 *é a soma de três primos.*

- Antes da criação de computadores, a conjectura já havia sido verificada para milhões de inteiros.
- Até o meio de 2011, todos os inteiros até $1,6.10^{18}$ haviam sido verificados.
- Resultados mais fracos foram provados:
  1. Todo inteiro mairo que 2 é a soma de no máximo 6 números primos. [Ramaré, 1995]
  2. Todo inteiro suficientemente grande é a soma de um primo e um segundo número que ou é primo ou é o produto de dois primos. [Chen, 1966]

Conjecturas sobre Primos

- Várias conjecturas sugerem sequências em que existiriam infinitos primos.
- Um exemplo sugere que existem infinitos da forma $n^2 + 1$.

Conjecturas sobre Primos

- Várias conjecturas sugerem sequências em que existiriam infinitos primos.
- Um exemplo sugere que existem infinitos da forma $n^2 + 1$.
- Um resultado mais fraco foi provado:
  - Há infinitos inteiros positivos n tais que $n^2 + 1$ é a soma de um primo e um segundo número que ou é primo ou é o produto de dois primos. [Iwaniec, 1973]

Primos Gêmeos

Pares de primos com diferença 2 são ditos *gêmeos*. Ex: 5 e 7, 11 e 13, ...

Conjectura:

Existem infinitos pares de primos gêmeos.

Primos Gêmeos

Pares de primos com diferença 2 são ditos *gêmeos*. Ex: 5 e 7, 11 e 13, ...

Conjectura:

Existem infinitos pares de primos gêmeos.

- Até o meio de 2011, o recorde de números gêmeos tem os primos $65.516.468.355.2^{333.333} \pm 1$, que tem 100.355 dígitos.