Teoria dos números II
Números Primos

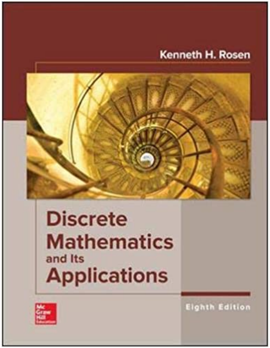
André Gustavo dos Santos[1]

[1] Departamento de Informática
Universidade Federal de Viçosa

INF230 - 2021/1

Conteúdo

Os slides seguintes são baseados nas seções 4.3.1 a 4.3.5 do livro texto da disciplina:



ROSEN, Kenneth H.
Discrete mathematics and its applications.
McGraw-Hill Education, 8th edition, 2018

Introdução

- Na aula passada vimos divisibilidade de inteiros
- Um conceito importante relacionado à divisibilidade é o denúmeros primos
- O estudo de primos vem desde os tempos antigos
- Há milhares de anos já se sabe que existem infinitos números primos
- Vários resultados foram encontrados por matemáticos nos últimos 400 anos
- O teorema fundamental da aritmética é um deles
- Várias conjecturas sobre primos ainda estão em aberto
- E os primos têm um papel importante na criptografia moderna

Primos - definição

- Todo inteiro maior que 1 é divisível por pelo menos dois inteiros, pois todo número inteiro é divisível por 1 e por ele mesmo
- Inteiros positivos que têm exatamente esses dois divisores são chamados primos

Definição

Um inteiro p maior que 1 é chamado **primo** se seus únicos fatores positivos são 1 e p. Um inteiro positivo maior que 1 que não é primo é chamado **composto**.

Obs.: um inteiro n é composto se e somente se houver um inteiro a tal que $a|n$ e $1 < a < n$.

Primos - exemplos

Os números abaixo são primos ou compostos?

- 7: primo, pois tem exatamente dois divisores, 1 e 7.
- 9: composto, pois tem divisor entre 1 e 9, o 3.
- 1: nem primo nem composto (veja as definições no slide anterior).

Teorema Fundamental da Aritmética

- Os primos são os blocos que constroem os números inteiros positivos

Teorema Fundamental da Aritmética

Todo inteiro maior que 1 pode ser escrito de forma única como um primo ou como produto de dois ou mais primos, em que os fatores primos são escritos em ordem não decrescente.

Exemplos

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Obs.: esta decomposição é chamada fatoração em números primos

UFV

Divisão por tentativa

- É importante mostrar que um dado número é primo
- Em criptografia, números primos grandes são usados para tornar uma mensagem secreta
- Um dos métodos para mostrar que um número é primo é baseado na seguinte observação

Teorema 2

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

Prova

- Se n é composto, então existe um inteiro a tal que $a|n$ e $1 < a < n$
- Como n é positivo e $a|n$, então $n = ab$ para algum inteiro positivo b
- Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então $ab > \sqrt{n}\sqrt{n} = n$, uma contradição. Logo, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$
- Como a e b são divisores de n, então n tem divisor $\leq \sqrt{n}$
- Este divisor ou é primo ou, pelo teorema fundamental da aritmética, tem fatores primos menores que ele mesmo
- Em qualquer dos casos, n tem um fator primo menor ou igual a $\sqrt{n}$. $\square$

Divisão por tentativa

- O teorema anterior diz que um número é primo se não for divisível por nenhum primo menor ou igual à sua raiz quadrada
- Isto leva a um algoritmo força-bruta chamado divisão por tentativa

Mostre que 101 é primo

- 101 não é divisível por 2, 3, 5 nem 7, os únicos primos $\leq \sqrt{101}$. Logo, é primo.

Fatoração em números primos

- Vimos que todo inteiro tem uma fatoração em primos
- É útil ter um método para encontrar tal fatoração
- Como encontrar a fatoração em primos de um número n?
  - Comece dividindo n por sucessivos primos, começando do menor, 2
  - Se n tiver um fator primo, ele terá algum menor que $\sqrt{n}$
  - Se não encontrar nenhum até $\sqrt{n}$, então n é primo
  - Do contrário, se encontrar um fator primo p, continue fatorando n/p (note que n/p não tem fator primo $< p$, pois começamos dos menores)
  - Novamente, se n/p não tiver fator primo nenhum até sua raiz, então n/p é primo
  - Do contrário, se encontrar um fator primo q, continue fatorando $n/p/q$
  - Continue até que a fatoração seja reduzida a um primo

Fatoração em números primos

Exemplo: fatoração de 7007

- Começamos dividindo 7007 por sucessivos primos, começando de 2
- Os primos 2, 3 e 5 não dividem 7007, mas $7|7007$, com $7007/7 = 1001$
- Continuamos, dividindo 1001 por sucessivos primos, começando de 7
- $7|1001$, com $1001/7 = 143$
- Continuamos, dividindo 143 por sucessivos primos, começando de 7
- 7 não divide 143, mas $11|143$, com $143/11 = 13$
- 13 é primo, fim. A fatoração em primos de 7007 é $7.7.11.13 = 7^2.11.13$.

Crivo de Eratóstenes

- Pelo teorema 2, os números compostos até 100 devem ter algum fator primo ≤ 10
- Os primos até 10 são 2, 3, 5 e 7
- Então os primos até 100 são estes quatro e os números não divisíveis por eles
- Uma forma de encontrar todos eles é usar o Crivo de Eratóstenes
- Esse é um método antigo para encontrar todos os primos até um dado valor
- O seguinte exemplo ilustra o funcionamento do método

Crivo de Eratóstenes

Encontrar todos os primos até 100

- Escreva todos os números
- Marque todos os múltiplos de 2
- Marque todos os múltiplos de 3
- Marque todos os múltiplos de 5
- Marque todos os múltiplos de 7
- Os que sobraram são 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

Fonte: ROSEN, K H. Discrete mathematics and its applications. McGraw-Hill Education, 8th edition, 2018.

UFV

Eficiência dos algoritmos

- O método mostrado para testar primalidade faz $\mathcal{O}(\sqrt{n})$ operações de resto
- O crivo de Eratóstenes para gerar a lista de primos faz $n \sum_{p \leq n} \frac{1}{p}$ marcações, sendo possível mostrar que isso corresponde a $\mathcal{O}(n \log \log n)$
- Tais algoritmos não são polinomiais, pois n é o valor da entrada, não o tamanho[1]
- Na verdade, o tamanho da entrada é $\log n$, que é o número de bits do valor n; tais algoritmos são, então, exponenciais em relação ao tamanho da entrada
- Um teste de primalidade realmente polinomial foi proposto pelos indianos M. Agrawal, N. Kayal e N. Saxena em 2002. Inicialmente $\tilde{\mathcal{O}}((\log n)^{12})$, que já colocou o teste de primalidade na classe $\mathcal{P}$, foi refinado posteriormente para $\tilde{\mathcal{O}}((\log n)^{6})$
- Já para o problema de fatoração em primos não é conhecido um algoritmo polinomial; e nisto reside a segurança dos métodos de criptografia modernos.

[1] são classificados como pseudo-polinomiais

Infinidade dos primos

- Há muito se sabe que existem infinitos primos
- Uma das provas foi dado por Euclides, e é considerada uma das provas mais bonitas da matemática

Teorema 3

Há um número infinito de primos.

Prova (por contradição)

- Suponha que não, que existam finitos primos. Sejam $p_1, p_2, \ldots, p_n$ todos esses primos.
- Considere o inteiro $Q = p_1 p_2 \ldots p_n + 1$
- Pelo teorema fund. da aritmética, Q é primo ou pode ser descrito por produto de primos
- Mas nenhum dos primos listados divide Q, pois se $p_j | Q$, então $p_j | Q - p_1 p_2 \ldots p_n = 1$
- Então há algum fator primo que não está na lista $p_1, p_2, \cdots, p_n$ (ou Q ou algum fator de Q)
- Uma contradição porque assumimos que a lista $p_1, p_2, \ldots, p_n$ inclui todos primos
- Consequentemente, há um número infinitos de primos. $\square$

UFV

Distribuição de primos

- Teorema 3 nos diz que há infinitos primos, mas quantos há até um inteiro x?
- Esta questão tem interessado matemáticos há muitos anos
- No século XVIII eles produziram muitas tabelas de primos para tentar encontrar alguma evidência da distribuição de primos
- Alguns dos grandes matemáticos da época, incluindo Gauss and Legendre, conjecturaram (mas não provaram) o seguinte:

Teorema dos números primos

Seja $\pi(x)$ o número de primos de 1 a x. Então, a razão entre $\pi(x)$ e $x/\ln x$ tende a 1, quando x cresce sem limite.

- O teorema foi provado pela primeira vez em 1896, de forma independente, pelo matemático francês Jacques Hadamard e pelo matemático belga Charles-Jean Gustave Nicholas de la Vallée-Poussin, usando teoria de variáveis complexas
- Provas por outras técnicas foram feitas depois, todas também bem complicadas
- E também refinamentos na estimativa do erro destaa aproximação bem como aproximações usando outras funções

UFV

Distribuição de primos

- Resultados da aproximação de $\pi(x)$ por $x/\ln x$

TABLE 2 Approximating $\pi(x)$ by $x/\ln x$.

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78,498	72,382.4	1.084
10^7	664,579	620,420.7	1.071
10^8	5,761,455	5,428,681.0	1.061
10^9	50,847,534	48,254,942.4	1.054
10^{10}	455,052,512	434,294,481.9	1.048

- Até 2017, o número de primos até 10^n foi calculado para todo $n \leq 26$
  - $\pi(10^{26}) = 1.699.246.750.872.437.141.327.603$ *(valor exato)*
  - $\pi(10^{26})/(10^{26}/\ln 26) = 1,01729$ *(diferença relativa)*
  - $\pi(10^{26}) - (10^{26}/\ln 26) = 28.883.358.936.853.188.823.261$ *(diferença absoluta)*

Probabilidade

- Qual a probabilidade de um número escolhido aleatoriamente ser primo?
- O teorema dos números primos diz há aproximadamente $x/\ln x$ primos de 1 a x
- Então a chance de um número escolhido aleatoriamente entre 1 e n ser primo é aproximadamente $(n/\ln n)/n = 1/\ln n$
- Usando este teorema e cálculo, pode-se mostrar que a probabilidade de n ser primo é também aproximadamente $\frac{1}{\ln n}$
- Exemplo: um número de 1000 dígitos tem $\frac{1}{\ln 10^{1000}}$ chance de ser primo ($\approx \frac{1}{2300}$)

Primos de Mersenne

- Como há infinitos primos, para qualquer primo há outros maiores que ele
- É natural então que haja uma busca por primos cada vez maiores
- Nos últimos 300 anos, o maior primo conhecido era quase sempre da forma $2^p - 1$, em que p é primo
- Primos nesse formato são chamados primos de Mersenne, homenagem ao monge francês Marin Mersenne que os estudou no século XVII

Exemplos

- $2^2 - 1 = 3$, primo
- $2^3 - 1 = 7$, primo
- $2^5 - 1 = 31$, primo
- $2^7 - 1 = 127$, primo
- $2^1 1 - 1 = 2047$, que não é primo

- A razão para os maiores primos conhecidos serem geralmente primos de Mersenne é que há um teste extremamente eficiente, chamado teste de Lucas–Lehmer, para determinar se $2^p - 1$ é primo. E não há para outros formatos.

Primos de Mersenne

- Em 1644, Mersenne afirmou que $2^p - 1$ é primo para

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

mas é composto para todos os outros primos p até 257.

- Demorou mais de 300 anos para se determinar que Mersenne em 5 deles:
  - $2^p - 1$ não é primo para $p = 67$ e $p = 257$
  - e é primo para $p = 61$, $p = 87$ e $p = 107$

Obs.: para se ter uma ideia da dificuldade, saiba que

$2^{61} - 1 = 2305843009213693951,$
$2^{67} - 1 = 147573952589676412927,$
$2^{257} - 1 =$
$231584178474632390847141970017375815706539969331281128078915168015826259279871$

Primos de Mersenne

- A busca por primos de Mersenne tem sido constante desde a invenção dos computadores
- Até 2006 eram conhecidos 43; até 2017 já eram 50
- Em dezembro de 2017 foi encontrado o primo $2^{277.232.917} - 1$, o maior até então, um número com mais de 23 milhões de dígitos

- Existe um grande esforço, o *Great Internet Mersenne Prime Search* (GIMPS)
- A busca tem aplicação prática: o teste de Lucas–Lehmer é comumente usado no controle de qualidade de supercomputadores
- Inclusive, em 2016, um bug no processador Intel Skylake foi descoberto ao se executar um software do GIMPS

Conjecturas e problemas em aberto

- A teoria dos números é conhecida como um tópico fácil de se formular conjecturas, algumas das quais muito difíceis de serem demonstradas
- Umas permaneceram abertas por muitos anos, e há outras ainda em aberto!
- Mais que isso, a teoria dos números é conhecida pela facilidade de constrruir conjecturas de fácil entendimento, mas que resistem a todas as técnicas de prova, exceto as mais sofistificadas (em algumas casos, a todas mesmo!)
- Muitos problemas famosos sobre números primos ainda esperam soluções de pessoas brilhantes
- A seguir um exemplo inicial e depois três problemas famosos em aberto
- Esses problemas mostram que questões que parecem simples permanecem sem resposta mesmo no século XXI

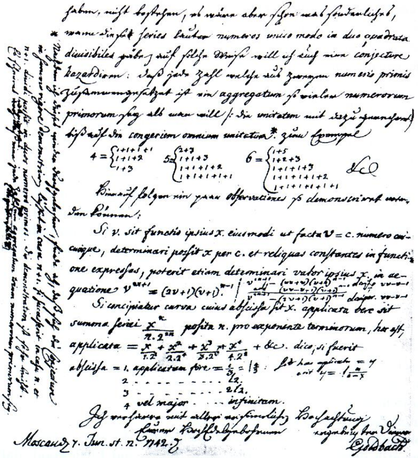
Exemplo inicial

Função $f(n)$ tal que $f(n)$ é primo para todo n

- Seria útil conhecer uma função $f(n)$ cujo valor é primo para todo n
- Centenas de anos atrás os matemáticos verificaram muitas funções polinomiais
- Um bom exemplo é $f(n) = n^2 - n + 41$
- Verifique que $f(n)$ de fato é primo para $n = 1, 2, 3, 4..., 40$
- Isto leva a uma conjectura de que $f(n)$ é primo para todo n
- ...
- Mas note que $f(41) = 41^2 - 41 + 41 = 41^2$, que não é primo...
- Será que podemos construir uma função polinômial $f(n)$ que é primo para todo n?
- É possível mostrar que para coeficientes inteiros, não. Para qualquer função polinomial $f(n)$ de coeficientes inteiros, existe algum y tal que $f(y)$ não é primo.

Conjectura de Goldbach

- Em 1742, o matemático Christian Goldbach conjecturou, em uma carta ao matemático Leonhard Euler, que todo inteiro ímpar > 5 é a soma de três primos.



Fonte: wikipedia

Conjectura de Goldbach

- Em 1742, o matemático Christian Goldbach conjecturou, em uma carta ao matemático Leonhard Euler, que todo inteiro ímpar > 5 é a soma de três primos.
- Euler respondeu dizendo que isto é equivalente a dizer que todo inteiro par > 2 é a soma de dois primos.

Conjectura de Goldbach

Todo inteiro par > 2 é a soma de dois primos.

- Por exemplo: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 7 + 5$.
- Ela havia sido verificada, à mao, para números até quase 1 milhão
- Com uso de computadores, já foi verificada para todo inteiro par até $4 \cdot 10^{18}$
- Alguns resultados mais fracos foram provados
  - Todo inteiro par > 2 é a soma de no máximo seis primos (provado por O. Ramaré, 1995)
  - Todo inteiro suficiente grande é a soma de um primo e de um número que ou é primo ou é o produto de dois primos (provado por J. R. Chen, 1966)
- A conjectura, entretanto, ainda permanece em aberto.

Primos no formato $n^2 + 1$

- Há muitas conjecturas que afirmam que há infinitos primos em um certo formato

Conjectura

Existem infinitos números primos da forma $n^2 + 1$, sendo n um inteiro positivo

- Por exemplo: $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$
- O melhor resultado conhecido é o seguinte
  - Existem infinitos números positivos n em que $n^2 + 1$ é primo ou produto de dois primos (provado por Henryk Iwaniecin, 1973)
- A conjectura, entretanto, ainda permanece em aberto.

Primos gêmeos

- Primos gêmeos são pares de primos que se diferenciam por 2 unidades
- Por exemplo, 3 e 5, 5 e 7, 11 e 13, 17 e 19, e 4967 e 4969

Conjectura dos primos gêmeos

Existem infinitos pares de primos gêmeos

- O melhor resultado conhecido é o seguinte
  - Existem infinitos pares p e $p + 2$, em que p é primo e $p + 2$ é primo ou produto de dois primos (provado por J. R. Chen, 1966)
- O recorde mundial de primos gêmeos, no início de 2018, consistia nos números $2.996.863.034.895 \cdot 2^{1.290.000} \pm 1$, que são números de 388.342 dígitos.
- A conjectura, entretanto, ainda permanece em aberto.

UFV

Bounded gap conjecture

- Seja $P(n)$ a proposição de que existem infinitos pares de primos de diferença exatamente n.
- A conjectura dos primos gêmeos é a proposição de que $P(2)$ é verdadeira.
- Matemáticos que trabalham na conjectura dos primos gêmeos formularam uma mais fraca, conhecida como *Bounded gap conjecture*

Bounded gap conjecture

Existe um inteiro n para o qual $P(N)$ é verdadeira

- A comunidade científica ficou surpresa quando Yitang Zhang, um chinês professor da Univ. de New Hampshire[2], que não publicava papers desde 2001, provou a conjectura em 2013. Em particular, ele provou que:
  - Existe um número $N < 70.000.000$ para o qual $P(N)$ é verdadeira (Yitang Zhang, 2013)
- Usando tal resultado, um grupo de matemáticos conseguiu baixar o gap para 246

[2] Fez doutorado na Univ. de Purdue; entre a conclusão do doutorado e o emprego como professor, trabalhou em serviços de contabilidade, foi entregador de comidas em New York e trabalhou no Subway em Kentucky.