Material Teórico - Módulo Divisibilidade

Números primos

Sexto Ano do Ensino Fundamental

Autor: Prof. Fabrício Siqueira Benevides
Revisor: Prof. Antonio Caminha M. Neto

29 de março de 2023

PORTAL DA MATEMÁTICA
OBMEP

1 Números Primos

Lembre-se de que um número **primo** é um número natural diferente de que 1 que possui como divisores apenas o número 1 e ele mesmo. Por exemplo, $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ são números primos. Um números natural que não é primo e é diferente de 0 e de 1 é chamado de **composto**.

Lembre-se de que um número inteiro é **par** se, e somente se, ele é divisível por 2; por exemplo, $0, 2, 4, 6, 8, 10, 12, 14, \ldots$ são números pares. Também, um número inteiro que não é par é chamado de **ímpar**; por exemplo, $1, 3, 5, 7, 9, 11, 13, \ldots$ são números ímpares.

Todo número par diferente de 2, possui pelo menos três divisores positivos: 1, 2 e ele mesmo; portanto, não é primo. Dessa forma, 2 é o único primo par. Por outro lado, nem todo número ímpar é primo.

Usando o mesmo raciocínio, podemos garantir que 3 é o único múltiplo de 3 que é um número primo.

Outra observação é que se tentarmos dividir qualquer número por um número que seja maior do que sua metade e menor do que ele próprio, o resultado não será inteiro (pois será um número real entre 1 e 2). Assim, todo divisor de um número natural n, diferente do próprio n, precisa ser menor ou igual a $n/2$.

Em geral, decidir se um dado número é primo é um processo bastante trabalho (veja a seção 4).

Exemplo 1. *Verifique quais dos números abaixo são primos:*

(a) 13.

(b) 675.

(c) 2000.

(d) 211.

Solução.
(a) 13 é primo. Para ver isso, note primeiro que 13 é ímpar e que $13/2 = 6{,}5$. Assim, basta tentar dividir 13 por cada

inteiro de 2 até 6 e ver que o resultado nunca será inteiro: 13/2, 13/3, 13/4, 13/5, 13/6 não são inteiros.

(b) 1675 não é primo. Apesar de 1675 ser um número ímpar, logo, não divisível por 2, quando buscamos por outros divisores de 1675 tentando dividi-lo por 3, depois por 4, depois por 5, ..., rapidamente percebemos que ele é múltiplo de 5:

$$675 = 5 \times 135.$$

(c) 2000 claramente não é primo, pois é par e maior que 2. De fato, $2000 = 2 \times 1000$, logo, 2000 tem pelo menos quatro divisores: $1, 2, 1000$ e 2000.
(d) 211 é primo. Primeiramente, veja que 211 é ímpar e que $211/2 = 105{,}5$. Seguindo o raciocínio do item (a), teríamos que tentar dividir 211 por cada um dos números de 2 até 105, o que seria extenuante. Contudo, há duas coisas que podemos fazer para simplificar essa tarefa.

Inicialmente, como 211 é ímpar, todos os seus divisores precisam ser ímpares. Isso reduz o trabalho pela metade: bastaria tentar dividir 211 por cada número ímpar de 3 até 105. Ainda assim, teríamos que fazer 52 divisões...

A segunda observação nos ajuda muito mais. Veja que a raiz quadrada de 211 está entre 14 e 15, já que

$$14^2 = 196 < 211 < 225 = 15^2.$$

Se tentarmos escrever 211 como um produto de dois números naturais, digamos $211 = ab$, veja que pelo menos um desses números precisa ser menor ou igual a 14. Do contrário, teríamos $a \geq 15$ e $b \geq 15$, o que resultaria em $ab \geq 15 \times 15 = 225 > 211$, o que é impossível.

Usando as duas observações acima, concluímos que, para garantir que 211 é primo, basta tentar dividi-lo por cada número ímpar de 2 até 14. Ou seja, temos de observar que o resultado de cada uma das divisões a seguir não é inteiro: $211/3, 211/5, 211/7, 211/9, 211/11, 211/13$. Mas isso é imediato □

A seguir destacamos a segunda observação usada para resolver o último item do exemplo anterior.

Observação 2. *Se n é um número natural composto, então n possui um divisor maior que* 1 *e menor ou igual $\sqrt{n}$.*

Demonstração. Se $n = ab$ onde $1 < a \leq b < n$, então

$$n = ab \geq a^2.$$

Logo, $a^2 \leq n$, o que garante que $a \leq \sqrt{n}$. □

Na sessão seguinte usaremos esse tipo de ideia para construir uma lista de todos os números primos menores ou iguais a um dado valor.

2 Eratóstenes

Eratóstenes foi um estudioso que viveu no século III a.C. Nasceu em Cirene, na África, e morreu em Alexandria, na Grécia.

Naquela época, não havia uma distinção clara entre Matemática, Física, Filosofia e outras ciências. Assim, era muito comum que um estudioso tivesse trabalhos em diferentes áreas. Porém, Eratóstenes se destacou bastante em conseguir trabalhar numa quantidade de áreas maior do que o usual, ficando

conhecido por seus trabalhos como matemático, astrônomo, geógrafo, filósofo, poeta, gramático e bibliotecário. Na área da Matemática, uma de suas mais famosas contribuições foi a de estimar com precisão a circunferência da Terra (um dos primeiros a conseguir esse feito).

Outra grande contribuição foi seu famoso *crivo*, usado para calcular todos os números primos menores ou iguais a um dado valor. Esse crivo é bastante eficiente e usado até os dias de hoje.

A palavra "crivo" refere-se a um utensílio que é usado para separar impurezas (areia, palha) de grãos (cereais). Ou seja, é essencialmente uma peneira. Assim, o *crivo de Eratóstenes* recebeu esse nome por se tratar de um método que separa números primeiros dos demais.

3 O crivo de Eratóstenes

Começamos escolhendo um número natural n. Por exemplo, $n = 56$. Agora, listamos todos os números de 1 a 56 em um quadro. Nosso objetivo é determinar quais são todos os números primos de 1 até 56.

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

Uma possibilidade seria testar cada um desses números, como fizemos com os números no exemplo da primeira seção.

Mas isso geraria bastante trabalho duplicado, além de muitas contas de divisão.

Ao invés de fazer isso, o crivo de Eratóstenes faz um processo de eliminação, onde em cada passo descartamos da tabela alguns números que temos certeza que são compostos. Fazemos isso várias vezes de um modo bem específico para que, ao final do processo, tenhamos certeza de que os números que sobrarem sejam todos primos. Uma vantagem do método é que trabalhamos apenas com multiplicações (não sendo necessário efetuar divisões ou extrações de raízes quadradas).

Inicialmente, descartamos o número 1, que não é primo, e marcamos o número 2, que sabemos que é primo.

~~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

Em seguida, observados que todos os múltiplos de 2 (exceto o próprio 2) são compostos e descartamos todos eles.

~~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~~

O primeiro número da tabela que ainda não foi riscado é número 3, que claramente é primo. Agora, marcaremos o número 3 como primo e descartaremos da tabela todos os demais múltiplos de 3 (que são compostos).

~~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~~

Vemos acima que o próximo número da tabela que ainda não foi marcado como primo e nem foi descartado é o 5. Dessa forma, concluímos que 5 é primo e descartamos todos os seus múltiplos.

~~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~~

O próximo número não marcado é o 7. Vamos analisar com mais calma o que está acontecendo. Como nos casos anteriores concluímos que 7 é primo. O motivo disso é que, a essa altura, todos os múltiplos de todos os números primos menores do que 7 já foram eliminados da tabela. Como o 7 sobreviveu até aqui, ele não possui nenhum divisor primo menor do que ele; portanto, ele é primo.

Como de costume, procedemos eliminando da tabela todos os múltiplos de 7, que são maiores do que o próprio 7, ou seja, 7×2, 7×3, 7×4, 7×5, 7×6, 7×7 e 7×8. (Veja que $7 \times 9 > 56$, logo, não precisa ser considerado). Veja que poderíamos começar a fazer isso a partir do número 7×7, ignorando os múltiplos menores. Isso porque todos os números da forma $7k$, com k no conjunto $\{2, 3, 4, 5, 6\}$, já foram eliminados anteriormente (pois nos passos anteriores já eliminamos da tabela todos os múltiplos de 2, de 3, de 4 — uma vez que estes também são múltiplos de 2 —, de 5 e de 6 — já que são múltiplos de 2 e de 3).

Assim, nesse passo, basta eliminar os números $7 \times 7 = 49$ e $7 \times 8 = 56$, sendo que o segundo também já havia sido eliminado (por ser múltiplo de 2).

~~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~~

Finalmente, o próximo número da tabela que ainda não foi eliminado é o número 11 (veja que 9 é ímpar, mas já foi eliminado, por ser múltiplo de 3). Assim, 11 é declarado como primo. O próximo passo seria eliminar os múltiplos de 11, mas, conforme discutido no passo anterior, podemos começar a partir do número 11×11, pois já sabemos que todos múltiplos da forma $11k$ onde $k \in \{2, 3, 4, \ldots, 10\}$ já foram eliminados (ou sequer estão na tabela). Contudo, $11 \times 11 = 121 > 56$. Logo, nenhum número novo será eliminado ao continuar o processo.

Com isso, todos os números da tabela que ainda não foram eliminados podem ser declarados como primos!

~~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~~

Concluímos que todos os números primos de 1 até 56 são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.$$

Resumo: Se quisermos aplicar o crivo de Eratóstenes para uma tabela maior basta seguir o procedimento:

Começamos da mesma forma que fizemos no exemplo acima, eliminando o número 1, marcando 2 como primo e eliminando todos os números pares maiores do que 2. Em seguida, em cada passo, definimos p como o menor número da tabela que ainda não foi eliminado e declaramos p como primo. Se p^2 é maior do que o maior número da tabela, encerramos o processo e declaramos todos os números que ainda não foram eliminados como primos. Caso contrário, eliminamos da tabela todos os múltiplos de p maiores ou iguais a p^2. Feito isso, olhamos para o próximo número depois de p que ainda não foi eliminado e continuamos o processo.

4 Leitura complementar

Do ponto de vista da teoria da computação, o problema de decidir se um número dado é primo (ou não) pode ser resolvido em um tempo razoável. Com isso, queremos dizer que existem métodos (algoritmos) avançados para isso. O primeiro método determinístico comprovadamente eficiente (que demora um "tempo polinomial na quantidade de dígitos do número') foi descoberto em 2002 pelos indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena, sendo conhecido como o *algoritmo AKS de primalidade* (note que A, K e S são as iniciais de seus sobrenomes).

De toda forma, quando o número é composto, surpreendentemente, apesar do método acima conseguir afirmar com toda certeza que o número é composto, ele não é capaz de calcular os fatores do número de forma rápida. Essa ineficiência em encontrar divisores grandes de números grandes, mesmo com o uso de computadores super poderosos, faz com que seja possível criar certos métodos de criptografia, onde uma

mensagem é codificada e só pode ser lida por usuários que possuem uma chave (senha).

Para computadores, números como 17.572.687, que possuem 8 algarismos ainda são considerados muito pequenos. Quando falamos aqui em "número grandes" pensamos em números com pelo menos 100 algarismos. Nessa faixa, o problema de fatoração já é impraticável computacionalmente, ao ponto de que mesmo os computadores mais rápidos existentes levariam mais do que a idade do Universo para resolvê-lo.

O maior número primo conhecido (até hoje, março de 2023) é

$$2^{82.589.933} - 1.$$

Ele possui 24.862.048 algarismos (na notação decimal) e é chamado um *primo de Mersenne*, pois é da forma $2^p - 1$ onde p também é um número primo. (Cuidado: nem todo número dessa forma é primo; por exemplo, $2^{11} - 1 = 2047$ é composto, uma vez que $2047 = 23 \cdot 89$.)

Dicas para o Professor

Este material complementa o da aula anterior e pode ser feito dentro da série de encontros sobre divisibilidade. Sozinho, ele pode ser feito de maneira relativamente rápida, não tomando todo o tempo de uma aula de 50 minutos. Entretanto, é importante que o professor faça exemplos com bastante cuidado, no quadro-negro, ilustrando o crivo de Eratóstenes passo a passo.

As sugestões [1], [2] e [3] de leitura complementar a seguir contém muito mais sobre primos. A sugestão [4] é uma ficção interessante sobre um matemático aficcionado por números primos.

Sugestões de Leitura Complementar

1. A. Caminha. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*, terceira edição. Rio de Janeiro, Editora S.B.M., 2022.

2. E. de Alencar Filho. *Teoria Elementar dos Números*. São Paulo, Nobel, 1989.

3. J.H. Conway, R.K. Guy. *O Livro dos Números*. Lisboa, Gradiva, 1999.

4. A. Doxiadis. *Tio Petrus e a Conjectura de Goldbach*. São Paulo, Editora34, 2001.