OS NÚMEROS PRIMOS *†‡

Milênios de estudo não foram suficientes para solucionar problemas aparentemente simples

Alberto Ricardo Prass[§,a]

[a]FisicaNet - www.fisica.net

A história dos números primos, de certa forma, é a própria história da Matemática, cujas origens se perdem no tempo. E, nos poucos milênios em que houve registro humano, muitos pensadores fizeram contribuições importantes para a teoria dos números, referindo-se, em particular, aos números primos. Citam-se, dentre eles, Euclides e Eratóstenes, na Grécia antiga; Pierre de Fermat, no século XVII; e Leonhard Euler, no século XVIII. Curiosamente, embora tenham constituído fonte de motivação para os estudos de matemáticos de todas as épocas, pouco ainda se sabe sobre esses números.

Por definição, um número é chamado de primo quando é divisível apenas por si mesmo e pela unidade. São primos 3, 5, 7, 11, 13, etc., enquanto não o são os números 4, 8, 27, 50 e assim por diante. Os números não primos são chamados **compostos**.

Uma das formas mais simples, porém trabalhosa, de encontrar os números primos inferiores a um número dado deve-se a Eratóstenes: seja, por exemplo, determinar os números primos contidos no intervalo de 1 a 100. O método de Eratóstenes consiste em escrever ordenadamente estes números e, sucessivamente, eliminar da tabela obtida os números distanciados entre si de 2 unidades, a partir do número 2; de 3 unidades, a partir do número 3; de 5 unidades a partir do número 5, e assim por diante, até 9. No intervalo considerado, sobram então apenas os números primos, ou seja:

| 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 | 71 | 73 | 79 | 83 | 89 |

O método é denominado, com muita propriedade, crivo de Erastótenes, porque ”opera” como uma peneira sobre um conjunto ordenado de números, separando os números primos dos demais.

Uma das poucas afirmações que se pode fazer com segurança a respeito dos números primos é que eles são em quantidade infinita. Essa demonstração cabe a Euclides, sendo feita por ”redução ao absurdo”. Presume-se que haja um número primo, p, maior que todos os outros. Ora, construindo-se o produto $1 \times 2 \times 3 \times 4 \times 5 \times 6 \ldots \times p$ (que é indicado, abreviadamente, por **p!** - leia-se ”p fatorial”) e somando uma unidade a este número, o resultado

$$p! + 1$$

não é divisível por qualquer número menor que p, excetuando-se a unidade. Tal número é, pois, primo, o que leva a uma contradição. Logo, a hipótese de partida, que tomava p como o maior dos números primos, é falsa.

---

*Adaptado da Enciclopédia Ciência Ilustrada, Vol 09, p.3540-3541

†Editado em LaTeX - Novembro, 2023

‡Este texto faz parte da série ENSAIOS - Minha busca particular pela sabedoria

§*Email address:* albertoprass@gmail.com

Conclui-se, em consequência, que o conjunto dos números primos é infinito.

Uma questão que apaixonou muitos matemáticos é se existiria alguma lei de formação para os números primos. Pierre de Fermat, um jurista francês que abraçou a Matemática por diversão, pensou ter respondido afirmativamente a esta pergunta, quando escreveu a fórmula:

$$F_n = 2^{2^n} + 1$$

Atribuindo valores inteiros a n (isto é, fazendo n=0, 1, 2, ...) encontra-se de fato, números primos. Mas isto somente é verdadeiro até n=4. Para n=5, conforme demonstrou Leonhard Euler, cerca de um século após Fermat, aquela expressão produz um número composto divisível por 641.

O Polinômio de Euler apresenta marcantes riquezas de propriedades aritméticas. A mais conhecida é a de ser um polinômio que, quando seus valores são tabelados, geram uma longa sequência de números primos.

$$f(n) = n^2 - n + 41$$

para n assumindo valores inteiros. Contudo, esta fórmula falha quando n=41, caso no qual fornece 41^2 , que é evidentemente um número composto, pois é produto de 41 por 41.

Há ainda mais um polinômio relacionado, que difere do primeiro por um sinal:

$$f(n) = n^2 + n + 41$$

Os valores são quase os mesmos, exceto que para 0 e 1 o valor não se repete e que a primalidade só vai até 39, pois ao valor 40 é atribuído o quadrado de 41.

Segue a tabela de valores para este f(n) entre 0 e 41

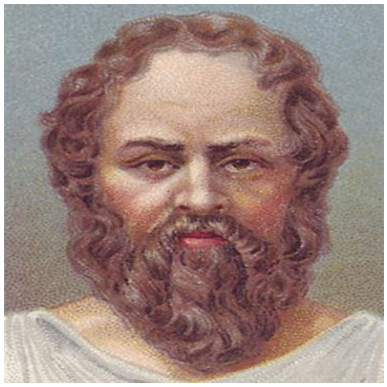
Tabela de valores de f(n)

n	f(n)	é primo
0	41	sim
1	41	sim
2	43	sim
3	47	sim
4	53	sim
5	61	sim
...	...	sim
40	1601	sim
41	1681	não

A existência de uma lei de formação para os números primos permanece, ainda, uma questão em aberto; de modo semelhante, não parece existir um critério para verificar se um dado número é ou não primo, sem que seja necessário proceder-se à divisão por todos os números menores que sua raiz quadrada.

OS MATEMÁTICOS

(a) EUCLIDES



(b) ERATÓSTENES

(c) FERMAT

(d) EULER

Matemáticos pioneiros no estudo dos números primos

Euclides (a), matemático alexandrino do século III AEC, conseguiu demonstrar de maneira extraordinariamente simples que existe uma quantidade infinita de números primos.

Eratóstenes (b), por sua vez, por volta do século II AEC, desenvolveu um método que permite encontrar todos os números primos inferiores a um certo número dado; tal método é conhecido, hoje, como ”crivo de Eratóstenes”.

Fermat (c), no século XVII, chegou à conclusão de que todos os números

$$F_n = 2^{2^n} + 1$$

são primos.

$$F_0 = 2^{2^0} + 1 = 3$$
$$F_1 = 2^{2^1} + 1 = 5$$
$$F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257$$
$$F_4 = 2^{2^4} + 1 = 65537$$

Euler (d), no entanto, um século depois, provou que Fermat estava errado. De fato, o número $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4.294.967.297 = 641 \times 6.700.417$ é um número composto, divisível por 641.

POLÍGONOS E NÚMEROS PRIMOS

Em fins do século XVIII, com apenas dezoito anos de idade, Karl Fridrich Gauss - que, com seu gênio, marcaria indelevelmente a Ciência de seu tempo - conseguiu relacionar a geometria com os números primos. Gauss demonstrou que, dos polígonos dotados de um número ímpar de lados, somente podem ser construídos com régua e compasso aqueles com número de lados coincidentes com um número de Fermat, isto é, número de forma $2^{2^n} + 1$. Os demais polígonos são construídos por métodos de aproximação ou pelo uso de transferidores.

Os primeiros números primos são 3, 5, 7, 11, 13, 17, 19 e 23. Destes, somente os números 3, 5 e 17 são números de Fermat (correspondentes, respectivamente, a n = 0, 1 e 2). Assim, apenas os polígonos com tais números de lados podem ser construídos usando-se exclusivamente régua e compasso.

GAUSS

PROGRAMAS PARA VERIFICAR SE UM NÚMERO É PRIMO

VISUAL BASIC

```
function primo(n as long) as boolean
 Dim aux as long,raiz as long
 if n<=3 then
  primo = n<>1
 else
  if n MOD 2 = 0 then
   primo = FALSE
  else
   aux = 3
   raiz = int(sqr(n))
   do while (n MOD aux <>0) AND (aux < raiz)
    aux =aux +2
   loop
   primo = n MOD aux <> 0
  end if
 end if
end function
```

PYTHON

```
num = int(input("Digite um número inteiro:"))
if num < 2:
    print('não primo')
elif num == 2:
    print('primo')
elif num % 2 == 0:
    print('não primo')
else:
    for i in range(3, num // 2, 2):
        if num % i == 0:
        print('não primo')
        break
    else:
        print('primo')
```

FORTRAN

```
Program prime_numbers
    implicit none
    integer i, j, n
    logical is_prime
    print *, "Digite um numero natural N:"
    read *, n
    do i = 2, n
        is_prime = .true.
        do j = 2, int(sqrt(dble(i)))
            if (mod(i,j) == 0) then
                is_prime = .false.
            end if
    end do
    if (is_prime) print *, i
    end do
end program
```

SITES SUGERIDOS

FisicaNET
https://www.fisica.net

Lista dos primeiros 10.000 números primos
https://pt.wikibooks.org/wiki/Teoria_de_n%C3%BAmeros/10000_primos