Sabemos que todo o número inteiro n é divisível por n, por $-n$, por 1 e por -1 (*i.e.* $n \mid n$, $-n \mid n$, $1 \mid n$, $-1 \mid n$).

Definição

Um número inteiro $p > 1$ diz-se um número primo se os únicos divisores inteiros positivos são 1 e p. Se p não é primo, então p diz-se um número composto.

Denota-se por $\mathbb{P}$ o conjunto de todos os número primos.

NOTAS:

- Os cinco primeiros primos são: 2,3,5,7 e 11.
- 2 é o único primo par.
- o maior primo conhecido é

$$2^{82589933} - 1$$

que é um número com 24 862 048 dígitos (provado que é primo em 7 de dezembro de 2018).

Teorema

Sejam $a, b \in \mathbb{Z}$ e $p \in \mathbb{P}$. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

PROVA

Se p é primo e $p \nmid a$, então $\text{m.d.c.}(a, p) = 1$. Assim, como $p \mid a$, pelo Lema de Euclides, $p \mid b$.

Corolário

Sejam $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z}$ e $p \in \mathbb{P}$. Se $p \mid a_1 \cdots a_n$, então $p \mid a_k$ para algum $k \in \{1, 2, \ldots, n\}$.

Corolário

Sejam $n \in \mathbb{N}$, $p_1, \ldots, p_n, p \in \mathbb{P}$. Se $p \mid p_1 \cdots p_n$, então $p = p_k$ para algum $k \in \{1, 2, \ldots, n\}$.

Teorema Fundamental da Aritmética

Todo o número natural maior do que 1 escreve-se como um produto de números primos. Essa escrita é única a menos da ordem dos fatores.

PROVA (Existência)

Comecemos por provar, por indução completa, que, para todo o $n \in \mathbb{N} \setminus \{1\}$, existem primos, $p_1, \ldots, p_k \in \mathbb{P}$, com $k \geq 1$, tais que $n = p_1 \cdots p_k$.

Notemos que o enunciado é verdadeiro para $n = 2$, pois $2 = p_1$ e $k = 1$.

Por hipótese de indução, suponhamos que o enunciado é verdadeiro para todo o número natural menor do que um certo n. Pretendemos provar que também é válido para n.

Se n é primo, então $k = 1$ e $n = p_1$.
Se n não é primo, então, como $n > 1$, existem $a, b \in \mathbb{N}$, tais que $n = ab$ e $1 < a, b < n$.
Por hipótese de indução, existem $q_1, \ldots, q_{k_1}$ e $q'_1, \ldots q'_{k_2}$ primos tais que

$$a = q_1 \cdots q_{k_1} \quad \text{e} \quad b = q'_1 \cdots q'_{k_2}.$$

Assim, $k = k_1 + k_2$ e n é um produto de primos:

$$n = a\,b = q_1 \cdots q_{k_1}\, q'_1 \cdots q'_{k_2}$$

.

PROVA (Unicidade)

Suponhamos que existem duas fatorizações de n como produto de números primos :

$$n = p_1 \cdots p_{k_1} = q_1 \cdots q_{k_2}.$$

Sem perda de generalidade, suponhamos também que $k_1 < k_2$, $p_1 < p_2 < \cdots < p_{k_1}$ e $q_1 < q_2 < \cdots < q_{k_2}$.

Então, $p_1 \mid n$, pelo que $p_1 = q_t$ para algum $t \in \{1, \ldots, k_2\}$. Logo $q_1 \leq p_1$.
Reciprocamente, como $q_1 \mid n$, viria que $p_1 \leq q_1$. Assim, $p_1 = q_1$ e, consequentemente,

$$p_2 \cdots p_{k_1} = q_2 \cdots q_{k_2}.$$

Repetindo, sucessivamente, a argumentação anterior ao fim de k_1 etapas obter-se-ia que

$$p_1 = q_1, \quad \ldots \quad , p_{k_1} = q_{k_1} \quad \text{e} \quad 1 = q_{k_1+1} \cdots q_{k_2}$$

o que implica que $k_2 = k_1$ e que as duas fatorizações são iguais.

Usando a operação de potênciação diríamos que todo o natural $n > 1$ admite uma única fatorização da forma

$$n = p_1^{r_1} \cdots p_k^{r_k}$$

com $k \geq 1$ e $p_1, \ldots, p_k$ números primos tais que $p_1 < \cdots < p_k$. Tal fatorização será designada a fatorização de n em primos.

Proposição

Seja n um o número natural e $n = p_1^{r_1} \cdots p_k^{r_k}$ a fatorização de n em primos. O conjunto dos divisores de n é o conjunto

$$D_n = \{p_1^{c_1} \cdots p_k^{c_k} \mid 0 \leq c_i \leq r_i \text{ para } i = 1, \ldots, k\}.$$

PROVA

Notar que

$$n = p_1^{r_1} \cdots p_k^{r_k} = p_1^{c_1} \cdots p_k^{c_k} \cdot p_1^{r_1 - c_1} \cdots p_k^{r_k - c_k},$$

com $0 \leq c_i \leq r_i$ para $i = 1, \ldots, k$, pelo que todos os elementos de D_n são divisores de n.

Reciprocamente, se $d \in \mathbb{N}$ é tal que $d \mid n$, então existe $x \in \mathbb{N}$ tal que $n = d\,x$. Qualquer primo que divide d ou que divide x também divide n. Assim, os primos que ocorrem na fatorização de d e na fatorização de x são elementos do conjunto $\{p_1, \ldots, p_k\}$, pelo que

$$d = p_1^{c_1} \cdots p_k^{c_k} \quad \text{e} \quad x = p_1^{c'_1} \cdots p_k^{c'_k}$$

com $0 \leq c_i$, $0 \leq c'_i$ para $i = 1, \ldots, k$, e

$$n = p_1^{r_1} \cdots p_k^{r_k} = p_1^{c_1} \cdots p_k^{c_k} \cdot p_1^{c'_1} \cdots p_k^{c'_k} = p_1^{c_1 + c'_1} \cdots p_k^{c_k + c'_k}.$$

Pelo Teorema Fundmental da Aritmética, a fatorização de n em primos é única e, então,

$$r_i = c_i + c'_i, \quad \text{para} \quad i = 1, \ldots, k.$$

Consequentemente, $c_i \leq r_i$ para $i = 1, \ldots, k$.

Existem $(r_1 + 1)(r_2 + 1) \cdots (r_k + 1)$ divisores positivos de n.

Proposição

Sejam a e b número naturais cujas fatorizações em primos são:

$$a = p_1^{m_1} \cdots p_k^{m_k} \quad \text{e} \quad b = p_1^{n_1} \cdots p_k^{n_k}$$

Então,

1. $\text{m.d.c.}(a, b) = p_1^{d_1} \cdots p_k^{d_k}$ em que $d_i = \min(a_i, b_i)$ para $i = 1, \ldots, k$;
2. $\text{m.m.c.}(a, b) = p_1^{c_1} \cdots p_k^{c_k}$ em que $c_i = \max(a_i, b_i)$ para $i = 1, \ldots, k$;

EXEMPLO 5

$$\text{m.d.c.}(101400, 15444) = ? \qquad \text{m.m.c.}(101400, 15444) = ?$$

$$\left.\begin{array}{l} 101400 = 2^3 \times 3 \times 5^2 \times 13^2 \\ 15444 = 2^2 \times 3^3 \times 11 \times 13 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{m.d.c.}(101400, 15444) = 2^2 \times 3^1 \times 5^0 \times 11^0 \times 13^1 \\ \text{m.m.c.}(101400, 15444) = 2^3 \times 3^3 \times 5^2 \times 11^1 \times 13^2 \end{array}\right.$$

EXEMPLO 6

Fatorizar o número $n = 6858432000$ em primos.

É fácil verificar que o número é múltiplo de 10, pelo que é múlptiplo de 2 e de 5, pelo fazendo divisões sucessivas por 2 e por 5, viria que

$$n = 2^9 \times 5^3 \times 107163.$$

Fazendo tentativas de divisão por 3 viria que

$$n = 2^9 \times 3^7 \times 5^3 \times 49$$

e de seguida obtém-se facilmente a fatorização de n em primos

$$n = 2^9 \times 3^7 \times 5^3 \times 7^2$$

pois é fácil verificar que $2, 3, 5$ e 7 são primos.

A dificuldade reside em reconhecer um número primo e na determinação dos números primos que dividem um número natural.

Proposição

Todo o número composto n admite um divisor primo menor ou igual a $\sqrt{n}$.

PROVA

Sejam $a, b > 1$ tais que $n = a \times b$. Se $a, b > \sqrt{n}$, então

$$n = a \times b > \sqrt{n} \times \sqrt{n} = n,$$

o que é absurdo. Então a ou b é menor do que $\sqrt{n}$ e há pelo menos um fator primo de a ou de b, respetivamente, que também é fator primo de n e menor do que $\sqrt{n}$.

Problema

Como calcular, no caso geral a fatorização em números primos de um número inteiro maior do que 1 ?

Algoritmo de fatorização por ensaios de divisão sucessivos

Entrada: $n > 2$ e $P = (p_i)_{i \leq m}$ uma lista de primos.

1. $f = (), e = 0, i = 1, d = p_1$.
2. Se $d > \sqrt{n}$, então $f \leftarrow f \cdot (\{n, 1\})$ e terminar.
3. Se $d|n$, então
   $e \leftarrow e + 1$, $n \leftarrow$ quociente da divisão de n por d, repetir 3..
4. Se $e \neq 0$, então $f \leftarrow f \cdot (\{d, e\})$.
5. Se $n = 1$, então terminar.
6. $i \leftarrow i + 1$.
7. Se $i \leq |P|$, então $d \leftarrow p_i$, $e = 0$, voltar a 2..
8. Terminar com mensagem de que f pode não ser a lista completa de fatores primos de n.

Saída: f lista ordenada dos menores divisores primos e respetivos expoentes que ocorrem na fatorização de n.

Problema

Como calcular uma lista ordenada de números primos para entrada do algoritmo acima?

O crivo de Eratóstenes é uma lista que contém todos os números primos menores do que um dado número inteiro $n > 2$.

Algoritmo de construção do crivo

Entrada: $n > 2$.

1. $P = (p_i)_i = (2, 3, 4, 5, 6, 7, \ldots, n)$, $i = 1$.
2. Se $p_i > \sqrt{n}$, então terminar.
3. $P \leftarrow$ sequência que resulta de P por se retirar os elementos da forma kp_i para $2 \leq K \leq \frac{n}{p_i}$.
4. $i \leftarrow i + 1$, voltar a 2..

Saída: lista ordenada P dos números primos menores ou iguais a n.

EXEMPLO 7

Usar o algoritmo Algoritmo de construção do crivo de Eratóstenes para determinar todos os primos inferiores a 28.

- $P = (2, 3, 4, 5, 6, \ldots, 28)$;
- 1ª iteração $i = 1$, $p_1 = 2$, $2 \leq k \leq \frac{28}{2}$.
  Então os elementos de P da forma kp_i, ou seja, da forma $2k$ são:
  $4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28$.
  Resultado da 1ª iteração:

$$P = (2, 3, 5, \ldots, 2n + 1, \ldots, 25, 27);$$

- 2ª iteração $i = 2$, $p_2 = 3$, $2 \leq k \leq \frac{28}{3}$.
  Então os elementosde P da forma kp_2, ou seja, da forma $3k$ são: $9, 15, 21, 27$.
  Resultado da 2ª iteração:

$$P = (2, 3, 5, 7, 11, 13, 17, 19, 23, 25);$$

- 3ª iteração $i = 3$, $p_5 = 5$, $2 \leq k \leq \frac{28}{5}$.
  Então os elementos de P da forma kp_3, ou seja, da forma $5k$ é : 25.
  Resultado da 3ª iteração:

$$P = (2, 3, 5, 7, 11, 13, 17, 19, 23).$$

O processo termina na 3ª iteração, dado que $\sqrt{28} \simeq 5, 29$.

EXEMPLO 8

- Fatorizar o número $n = 434847593$ em primos.

Se tentarmos divisões sucessivas pelos menores primos, dificilmente encontramos um divisor. Deveríamos fazer tentativas até $\sqrt{n}$, sendo que $20853 < \sqrt{n} < 20854$.

De facto, o menor número que divide n é 20849, o que conduziria a obter

$$n = 20849 \times 20857.$$

Para este caso existem métodos que apontam rapidamente para esta fatorização, sem garantir que os fatores 20849 e 20857 são primos. Em tal caso, como poderíamos saber se 20849 e/ou 20857 são primos?

- Como fatorizar $n_1 = 20849$?

Notar que

$$144 < \sqrt{20849} < 145.$$

Então deveríamos tentar dividir n_1, sucessivamente, por todos os primos inferiores a 144, até encontrar um que dividisse n_1.

Como não se encontra um número nessas condições, então conclui-se que 20849 é primo.

- Como fatorizar $n_2 = 20857$?

Teorema de Euclides

O conjunto $\mathbb{P}$ dos números primos é infinito.

PROVA

Suponhamos que o conjunto $\mathbb{P}$ é finito, ou seja, que

$$\mathbb{P} = \{p_1, p_2, \ldots, p_k\}$$

com $k \in \mathbb{N}$. Seja N o produto de todos os primos mais um, *i.e.*,

$$N = p_1 \cdots p_k + 1.$$

Então, $N \in \mathbb{N}$, $N > 1$ e, consequentemente, N é um produto de números primos pelo Teorema Fundamental da Aritmética. Seja p um primo que divide N. Assim,

$$p \mid p_1 \cdots p_k + 1 \qquad \text{e } p \mid p_1 \cdots p_k.$$

Isto implicava que $p \mid 1$, o que contradiz o facto p ser primo. A contradição resultou de se supor que $\mathbb{P}$ é finito.

Proposição

Seja $k \in \mathbb{N}$. Existem k inteiros consecutivos que não são primos.

PROVA

Para qualquer $j \in \{2, \ldots, k+1\}$, $(k+1)! + j$ não é primo, porque é divisível por j.

EXEMPLO 9

No intervalo $[1001! + 2, 1001! + 1001]$ não há números inteiros primos.

Definição

O número de primos menores ou iguais a um dado x é representado por $\pi(x)$ sendo π designada a função de distribuição de números primos.

Pelo Teorema de Euclides sobre números primos, conclui-se que

$$\lim_{x \to +\infty} \pi(x) = +\infty.$$

O valor de $\pi(10^{27})$ foi publicado em 2015, por David Baugh e Kim Walisch e é

$$\pi(10^{27}) = 16\,352\,460\,426\,841\,680\,446\,427\,399$$

Distribuição de frequência de números primos

n	$\pi(n)$	$\frac{\pi(n)}{n}$
10	4	0, 4
10^2	25	0.25
10^3	168	0.168
10^4	1229	0, 1229
10^5	9592	0.09592
10^6	78498	0.078498
10^7	664579	0.0664579
⋮	⋮	⋮
10^{14}	3204941750802	0.03204941750802
⋮	⋮	⋮
10^{20}	2220819602560918840	0.02220819602560918840

Decréscimo de ocorrências de números primos

Intervalo	Número de primos
$1 - 100$	25
$100 - 200$	21
$200 - 300$	16
$300 - 400$	16
$400 - 500$	17
$500 - 600$	14
$600 - 700$	16
$700 - 800$	14
$800 - 900$	15
$900 - 1000$	14

Intervalo	Número de primos
$10^6 - 10^6 + 100$	6
$10^6 + 100 - 10^6 + 200$	10
$10^6 + 200 - 10^6 + 300$	8
$10^6 + 300 - 10^6 + 400$	8
$10^6 + 400 - 10^6 + 500$	7
$10^6 + 500 - 10^6 + 600$	7
$10^6 + 600 - 10^6 + 700$	10
$10^6 + 700 - 10^6 + 800$	5
$10^6 + 800 - 10^6 + 900$	6
$10^6 + 900 - 10^6 + 1000$	8

À medida que se percorre o conjunto ordenado dos números naturais, os números primos tendem a ocorrer com menor frequência.

O menor intervalo entre primos verifica-se entre os números 2 e 3, após o que um intervalo entre primos tem no mínimo comprimento 2, como por exemplo entre 5 e 7.

Definição

Se p e $p+2$ são dois números inteiros primos, então tais números designam-se primos gémeos.

Conjetura

Existe uma infinidade de primos gémeos.

Maiores primos gémeos

Primos gémeos	Nº dígitos	Ano
$2996863034895 \times 2^{1290000} \pm 1$	388342	2016
$3756801695685 \times 2^{666669} \pm 1$	200700	2011
$65516468355 \times 2^{333333} \pm 1$	100355	2009
$12770275971 \times 2^{222225} \pm 1$	66907	2017
$70965694293 \times 2^{2200006} \pm 1$	60219	2016
$66444866235 \times 2^{200003} \pm 1$	60218	2016

Definição

Uma progressão aritmética de n primos é uma sequência de números primos do tipo

$$p,\ p+d,\ p+2d,\ \ldots\ ,p+(n-1)d$$

em que p é o primeiro termo, d é a amplitude constante dos intervalos entre termos e $p+(n-1)d$ é o último termo.

EXEMPLO 10

Progressão aritmética de 5 primos com $p=5$ e $d=6$:

$$5, 11, 17, 23, 29.$$

A maior progressão aritmética conhecida tem comprimento 27. (23 de setembro de 2019, Rob Gahan).

Teorema (Green & Tao, 2004)

Existem progressões aritméticas finitas arbitrariamente longas.