Números Primos e MDC

Wladimir Araújo Tavares [1]

[1]Universidade Federal do Ceará - Campus de Quixadá

31 de outubro de 2016

Números Primos e MDC

Definição

Um inteiro p maior que 1 é chamado de primo se os únicos fatores de p são 1 e p. Um inteiro positivo maior que 1 que não é primo é chamado composto. Um número n é composto se somente se existe um inteiro a tal que $a|n$ *e* $1 < a < n$.

Teorema

(Teorema Fundamental de Aritmética) Todo inteiro maior que 1 pode ser escrito unicamente como primo ou como o produto de dois ou mais primos.

Determine a decomposição em primos do número 100.

100	2
50	2
25	5
5	5
1	$(2^2) \cdot (5^2)$

Determine a decomposição em primos do número 120.

120	2
60	2
30	2
15	3
5	5
1	$(2^3) \cdot (3^1) \cdot (5^1)$

Algoritmo de Fatoração

```
def factor(n):
    i = 2
    factor = []
    while( n > 1):
        cont = 0
        while( n%i == 0):
            n = n/i
            cont = cont + 1
        if cont > 0:
            factor.append( (i, cont) )
        i = i + 1
    return factor
```

Exemplos

```
Entre com um numero: 123421
[(83, 1), (1487, 1)]
Entre com um numero: 1234
[(2, 1), (617, 1)]
Entre com um numero: 1020
[(2, 2), (3, 1), (5, 1), (17, 1)]
```

Algoritmo de Fatoração

```
primeFactor n = factorAux n 2
factorAux 1 _ = []
factorAux n f
    | mod n f == 0 = f : factorAux (div n f) f
    | otherwise = factorAux n (f+1)
```

Algoritmo de Fatoração

```
*Main> primeFactor 100
[2,2,5,5]
*Main> primeFactor 123421
[83,1487]
*Main> primeFactor 1234
[2,617]
*Main> primeFactor 1020
[2,2,3,5,17]
```

Teorema

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

Demonstração.

Se n é composto, pela definição, existe um $a \in \mathbb{Z}$ tal que $a|n$ e $1 < a < n$. Portanto, $n = ab$, onde $b \in \mathbb{Z}$ e $b > 1$. Suponha por absurdo que todos os divisores de n são maiores que n, ou seja, $a > \sqrt{n}$ e $b > \sqrt{n}$. Logo, $ab > \sqrt{n} \cdot \sqrt{n} > n$, o que é uma contradição. Pelo teorema fundamental de aritmética, a é um divisor primo ou existe um divisor primo menores que a. □

Exemplo

Mostre que 101 é primo.
Basta testar se existe algum primo menores que $\sqrt{101} \approx 10,04$ *é um divisor de 101. Os primos menores que* $\sqrt{101}$ *são 2,3,5 e 7. Como,* $2 \nmid 101$, $3 \nmid 101$, $5 \nmid 101$ *e* $7 \nmid 101$. *Logo, 101 é primo.*

Exemplo

Encontre um fatorização de 7007.

7007	*7*	$\sqrt{7007} \approx 83,7$
1001	*7*	$\sqrt{1001} \approx 31,63$
143	*11*	$\sqrt{143} \approx 11,95$
13	*13*	$\sqrt{13} \approx 3,6$
1	$(7^2) \cdot 11 \cdot 13$	

Algoritmo de fatorização otimizado

```
def factor(n):
    i = 2
    factor = []
    while( n > 1 ):
        cont = 0
        while( n%i == 0):
            n = n/i
            cont = cont + 1
        if cont > 0:
            factor.append( (i, cont) )
        #if n > 1 and i*i > n then  n is prime
        if n > 1 and i*i > n:
            factor.append( (n,1) )
            n = n / n
        i = i + 1
    return factor
```

Algoritmo de Fatoração

```
primeFactor2 n = factorAux2 n 2
factorAux2 1 _ = []
factorAux2 n f
    | mod n f == 0 = f : factorAux (div n f) f
    | f*f > n = [n]
    | otherwise = factorAux n (f+1)
```

Crivo de Eratóstenes

```
def sieve(list):
    result = []
    result.append(list[0])
    if len(list) == 1:
        return result
    else:
        newlist = []
        for i in range(1,len(list)):
            if list[i] % list[0] != 0:
                newlist.append(list[i])
        result.extend( sieve(newlist) )
        return result
```

Exemplo

Entre com um numero: 1000
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137,
139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,
211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277,
281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359,
367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439,
443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521,
523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607,
613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683,
691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773,
787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863,
877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967,
971, 977, 983, 991, 997]

Crivo de Eratóstenes

```
crivo [] = []
crivo (x:xs) = x :
    crivo [ y | y <- xs, mod y x /= 0]
```

Infinitude dos primos

Teorema

Existem infinitos números primos.

Demonstração.

Suponha por absurdo que existe uma quantidade finita de números primos. Seja $\{p_1, p_2, \ldots, p_n\}$ uma lista de todos os números primos. Seja $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Pelo teorema fundamental da aritmética, Q é primo ou Q pode ser escrito como o produto de primo. Por outro lado, $p \nmid Q$ para todo $p \in \{p_1, p_2, \ldots, p_n\}$. Logo, existe um primo p que não aparece na lista. Esse primo pode ser o próprio Q ou algum fator primo de Q. Uma contradição porque assumimos inicialmente que listamos todos os primos. $\square$

Observações

- Na prova, não afirmamos que Q é primo.
- Essa é uma prova de existência não construtiva que para todo lista de primos, existe um primo que não está na lista.

Prova Existencial: Não construtiva

Mostre que existe um irracional x e y tal que x^y é racional.

Demonstração.

Sabemos que $\sqrt{2}$ é irracional. Considerando $\sqrt{2}^{\sqrt{2}}$, temos dois casos:

1. $\sqrt{2}^{\sqrt{2}}$ é racional. Neste caso, tome $x = y = \sqrt{2}$.
2. $\sqrt{2}^{\sqrt{2}}$ é irracional. Neste caso, tome $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2$

Infinite de primos

Teorema

Existem infinitos primos da forma $4n + 3$

Demonstração.

Assuma por absurdo que existe um número finito de primos da forma 4n + 3, digamos $3, p_1, p_2, \ldots, p_n$. Seja $Q = 4p_1p_2 \ldots p_n + 3$ .Podemos mostrar que existe um primo na fatoração de Q da forma 4n + 3. Se todos os fatores primos fossem da forma 4n + 1 isso implicaria que Q também seria dessa forma, o que é uma contradição. Porém, nenhum desse primos $p_0, p_1, \ldots, p_n$ divide Q. Se $3|Q$ e $3|3$ então $3|Q - 3 = 4p_1p_2 \ldots p_n$, contradizendo o fato que $3 \neq p_i$. Se $p_i|Q$ e $p_i|4p_1p_2 \ldots p_k$ então $p_i|Q - 4p_1p_2 \ldots p_k$, contradizendo o fato que $p_i \neq 3$.
Logo, existe um primo p da forma $4k + 3$ que não foi listado. □

Teorema de distribuição dos números primos

Teorema

A razão entre o números de primos menores que n, denotado por $\pi(x)$, *e* $\frac{x}{lnx}$ *aproxima-se de 1 quando x tende ao infinito , ou seja,*

$$\lim_{x \to \infty} \frac{x}{x/lnx} = 1 \tag{1}$$

Teorema de distribuição dos números primos

```
crivo [] = []
crivo (x:xs) = x : crivo [ y | y <- xs, mod y x /=
prime_theorem n = (  a , b , ratio )
    where
        a = length (crivo [2..n])
        b = (fromIntegral n)/(log (fromIntegral n)
        ratio = (fromIntegral a)/b
```

Máximo Divisor Comum

Definição

Seja a e b inteiros, ambos diferente de zero. O maior inteiro d tal que $d|a$ e $d|b$ é chamado de máximo divisor comum de a e b, é denotado por $mdc(a, b)$.

Exemplo

Exemplo

O maior divisor comum de 24 e 36?

24	36	(2)
12	18	(2)
6	9	2
3	9	(3)
1	3	3
1	1	$2^3 \cdot 3^2 = 72$

O máximo divisor comum de 24 e 36 é $2 \cdot 2 \cdot 3 = 12$

Exemplo

Exemplo

O máximo divisor comum de 17 e 22?

17	*22*	*2*
17	*11*	*11*
17	*1*	*17*
1	*1*	$2 \cdot 11 \cdot 17 = 374$

Primos entre si

Definição

Os inteiros a e b são primos entre si se $mdc(a, b) = 1$.

Definição

Os inteiros $a_1, a_2, \ldots, a_n$ são dois a dois primos entre si se $mdc(a_i, a_j) = 1$ para todo $1 \leq i < j \leq n$.

Definição

Seja dois inteiros a e b, ambos diferentes de zero. Suponha a fatoração em primos de a e b

$$a = p_1^{a_1} \cdot p_2^{a_2} \ldots p_n^{a_n} \text{ e } b = p_1^{b_1} \cdot p_2^{b_2} \ldots p_n^{b_n} \tag{2}$$

O máximo divisor comum de a e b é dado por

$$mdc(a,b) = p_1^{min(a_1,b_1)} \cdot p_2^{min(a_2,b_2)} \ldots p_n^{min(a_n,b_n)} \tag{3}$$

Definição

O menor múltiplo comum de inteiros positivos a e b é o menor inteiro positivo que é divisível por a e b, é denotado por $mmc(a, b)$.

Definição

Seja dois inteiros a e b, ambos diferentes de zero. Suponha a fatoração em primos de a e b

$$a = p_1^{a_1} \cdot p_2^{a_2} \dots p_n^{a_n} \text{ e } b = p_1^{b_1} \cdot p_2^{b_2} \dots p_n^{b_n} \tag{4}$$

O menor múltiplo comum de a e b é dado por

$$mmc(a, b) = p_1^{max(a_1,b_1)} \cdot p_2^{max(a_2,b_2)} \dots p_n^{max(a_n,b_n)} \tag{5}$$

Exemplo

Qual é o máximo divisor comum e menor múltiplo comum de $2^3 3^5 7^2$ *e* $2^4 3^3$*?*

$$mdc(2^3 3^5 7^2, 2^4 3^3) = 2^3 3^3 \tag{6}$$

$$mmc(2^3 3^5 7^2, 2^4 3^3) = 2^4 3^5 7^2 \tag{7}$$

Algoritmo de Euclides

Exemplo

Vamos calcular o mdc(287,91). Primeiramente, divida 287 por 91:

$$287 = 91 \cdot 3 + 14 \tag{8}$$

Todo divisor de 91 e 287 é divisor de $14 = 287 - 91 \cdot 3$.
Todo divisor de 91 e 14 é divisor de $287 = 91 \cdot 3 + 14$.
Logo, o mdc(287,91) é igual ao mdc(91,14).
$mdc(91,14) = mdc(14,7) = mdc(7,0) = 7$.

Lema de Euclides

Lema

Dado a e b inteiros tal que $r = a - b\lfloor \frac{a}{b} \rfloor$. Se $d|a$ e $d|b$ sse $d|r$ e $d|b$.

Demonstração.

Como $d|a$ e $d|b$, existem inteiros k e k' tais que $a = dk$ e $b = dk'$.
Logo, r pode ser escrito como

$$r = a - b\lfloor \frac{a}{b} \rfloor = dk - dk'\lfloor \frac{a}{b} \rfloor = d(k - k'\lfloor \frac{a}{b} \rfloor) \tag{9}$$

Concluímos que $d|r$ e $d|b$.
Como $d|r$ e $d|b$, existem inteiros k e k' tais que $r = dk$ e $b = dk'$.
Logo, a pode ser escrito como

$$a = r + b\lfloor \frac{a}{b} \rfloor = dk + dk'\lfloor \frac{a}{b} \rfloor = d(k + k'\lfloor \frac{a}{b} \rfloor) \tag{10}$$

Concluímos que $d|a$ e $d|b$.

Identidade de Bézout

Definição

Se a e b são inteiros positivos, então existe inteiros m e n tal que $mdc(a, b) = ma + nb$ que são chamados de coeficientes de Bézout. A equação $mdc(a, b) = ma + mb$ é chamada de identidade de Bézout.

Identidade de Bézout

Exemplo

Encontre os coeficientes de Bézout para 252 e 198?

O algoritmo de Euclides realiza as seguintes operações:

$$
\begin{array}{lcll}
252 & = & 1 \cdot 198 + 54 & 54 = 252 - 1 \cdot 198 \\
198 & = & 3 \cdot 54 + 36 & 36 = 198 - 3 \cdot 54 \\
54 & = & 1 \cdot 36 + 18 & 18 = 54 - 1 \cdot 36 \\
36 & = & 2 \cdot 18 &
\end{array}
$$

Substituindo as expressões, temos:

$$
\begin{array}{lcl}
18 & = & 54 - 1 \cdot 36 \\
 & = & 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198 \\
 & = & 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198
\end{array}
$$

Os coeficientes de Bézout são 4 e -5.

Identidade de Bézout

R	Q	m	n	
a	$*$	1	0	$a = ma + nb$
b	$*$	0	1	$b = ma + nb$
r_1	q_1	m_1	n_1	$r_1 = m_1 a + n_1 b$
r_2	q_2	m_2	n_2	$r_2 = m_2 a + n_2 b$
$\vdots$				
r_{j-1}	q_{j-1}	m_{j-1}	n_{j-1}	$r_{j-1} = m_{j-1} a + n_{j-1} b$
r_j	q_j	m_j	n_j	$r_j = m_j a + n_j b$
r_{j+1}	q_{j+1}	m_{j+1}	n_{j+1}	$r_{j+1} = m_{j+1} a + n_{j+1} b$

$$
\begin{aligned}
r_{j+1} &= r_{j-1} - q_{j+1} r_j \\
&= m_{j-1} a + n_{j-1} b - q_{j+1}(m_j a + n_j b) \\
&= (m_{j-1} - q_{j+1} m_j) a + (n_{j-1} - q_{j+1} n_j) b
\end{aligned}
$$

Identidade de Bézout

R	Q	m	n
252	*	1	0
198	*	0	1
54	1	1	-1
36	3	-3	4
18	1	4	-5

Identidade de Bézout

Exemplo

Encontre os coeficientes de Bézout para 78 e 35?

O algoritmo de Euclides realiza as seguintes operações:

$$
\begin{array}{lcll}
78 & = & 2 \cdot 35 + 8 & 8 = 78 - 2 \cdot 35 \\
35 & = & 4 \cdot 8 + 3 & 3 = 35 - 4 \cdot 8 \\
8 & = & 2 \cdot 3 + 2 & 2 = 8 - 2 \cdot 3 \\
3 & = & 1 \cdot 2 + 1 & 1 = 3 - 1 \cdot 2 \\
2 & = & 2 \cdot 1 &
\end{array}
$$

Substituindo as expressões, temos:

$$
\begin{array}{lcl}
1 & = & 3 - 1 \cdot 2 \\
 & = & 3 - 1 \cdot (8 - 2 \cdot 3) = -1 \cdot 8 + 3 \cdot 3 \\
 & = & -1 \cdot 8 + 3 \cdot (35 - 4 \cdot 8) = 3 \cdot 35 - 13 \cdot 8 \\
 & = & 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) = 29 \cdot 35 - 13 \cdot 78
\end{array}
$$

Os coeficientes de Bézout são 29 e -13.

Identidade de Bézout

R	Q	m	n
78	*	1	0
35	*	0	1
8	2	1	-2
3	4	-4	9
2	2	9	-20
1	1	-13	29

Encontre os coeficientes de Bézout:

1. 102 e 38
2. 4021 e 2014

Teorema

Se a,b e c são inteiros positivos tal que $gcd(a, b) = 1$ *e* $a|bc$ *então* $a|c$.

Demonstração.

Usando o teorema de Bézout, existem inteiros s e t tal que

$$sa + tb = 1 \tag{11}$$

Multiplicando a equação por c, temos

$$csa + ctb = c \tag{12}$$

Se $a|bc$ então $a|ctb$. Se $a|csa$ e $a|ctb$ então $a|csa + ctb$. Logo, $a|c$. □

Teorema

Seja m um inteiro positivo e a, b e c inteiros. Se $ac \equiv bc(\ mod\ m)$ e $gcd(c, m) = 1$ então $a \equiv b(mod\ m)$

Demonstração.

Como $ac \equiv bc(\ mod\ m)$, então $m|ac - bc = c(a - b)$. Como gcd(c,m) = 1, então $m|(a - b)$. Então $a \equiv b(mod\ m)$ □

Resolvendo congruência linear

Considere

$$ax \equiv b \ (mod \ m) \tag{13}$$

Para resolver esta equação basta encontrar $\bar{a}$ tal que $\bar{a}a \equiv 1 \ (mod \ m)$, ou seja, seu inverso multiplicativo. Logo,

$$\begin{aligned} ax &\equiv b \ (mod \ m) \\ \bar{a}ax &\equiv \bar{a}b \ (mod \ m) \\ x &\equiv \bar{a}b \ (mod \ m) \end{aligned}$$

Resolvendo congruência linear

Considere

$$3x \equiv 2 \ (mod\ 5) \tag{14}$$

Método 1: Inspeção

$\times$	0	1	2	3	4
3	0	3	1	4	2

Logo,

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ &= 5k + 4,\ k \in \mathbb{Z} \end{aligned}$$

Resolvendo congruência linear

Considere

$$3x \equiv 2 \ (mod \ 5) \tag{15}$$

Método 1: Inverso Multiplicativo

R	Q	m	n
5	*	1	0
3	*	0	1
2	1	1	-1
1	1	-1	2

Como $-1 \cdot 5 + 2 \cdot 3 = 1$, temos que $2 \cdot 3 \equiv 1 \ (mod \ 5)$.

$$3x \equiv 2 \ (mod \ 5) \Leftrightarrow 2 \cdot 3 \cdot x \equiv 2 \cdot 2 \ (mod \ 5) \Leftrightarrow x \equiv 4 \ (mod \ 5)$$

Exercicio

Resolva a seguinte congruência linear:

1. $3x \equiv 4 \ (mod \ 7)$
2. $19x \equiv 4 \ (mod \ 141)$
3. $55x \equiv 34 \ (mod \ 89)$
4. $89x \equiv 2 \ (mod \ 232)$