Fundamentos de Teoria da Computação Aula 10

Priscila Marques Kai

TEORIA DOS NÚMEROS

"A Teoria dos Números preocupa-se, pelo menos em seus aspectos elementares, com as propriedades dos inteiros e, mais particularmente, dos inteiros positivos 1, 2, 3,... (também conhecidos como números naturais). Esta ênfase remonta aos gregos antigos para quem a palavra número significava inteiro positivo, e nada mais."

- BURTON, David M. Teoria Elementar dos Números, 7ª edição. Rio de Janeiro: Grupo GEN, 2016. 9788521631026. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788521631026

AGENDA DA AULA

- Teoria dos números
  - Divisibilidade
  - mdc, mmc
  - Algoritmo de Euclides
  - Teorema Fundamental da Aritmética

TEORIA DOS NÚMEROS

INTRODUÇÃO A TEORIA DOS NÚMEROS

Divisibilidade

Dados dois inteiros d e a, dizemos que d *divide* a, ou d é um *divisor* de a, ou ainda que a é um *múltiplo* de d, denotado na forma

$$d \mid a$$

se existir $q \in \mathbb{Z}$ com a = qd. Caso contrário, escrevemos $d \nmid a$.

Ex:

$$-5 \mid 10 \text{ mas } 10 \nmid -5.$$

TEORIA DOS NÚMEROS

DIVISIBILIDADE

Algumas propriedades importantes da divisibilidade:

Sejam $a, b, c, d \in \mathbb{Z}$

(i) ("d divide") Se $d \mid a$ e $d \mid b$, então $d \mid ax + bx$ para qualquer combinação linear $ax + bx$ de a e b com coeficientes $x, y \in \mathbb{Z}$.

(ii) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

(iii) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

TEORIA DOS NÚMEROS

DIVISIBILIDADE

Sejam $a, b, c, d \in \mathbb{Z}$

(i) ("d divide") Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.

Demonstração:

Se $d \mid a$ e $d \mid b$, então podemos escrever

$a = q_1 d$

$b = q_2 d$

com $q_1, q_2 \in \mathbb{Z}$,

logo, $ax + by = q_1 dx + q_2 dy$

$= \mathrm{d}(q_1 x + q_2 y)$

$= dm$, com $\mathrm{m} = q_1 x + q_2 y$

Como $q_1 x + q_2 y \in \mathbb{Z}$, temos $d \mid ax + by$

TEORIA DOS NÚMEROS

DIVISIBILIDADE

Sejam $a, b, c, d \in \mathbb{Z}$

(ii) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

Demonstração:

Suponha que $d \mid a$ e $a \neq 0$

$a = qd$

com $q \neq 0$, podemos analisar o módulo dos lados da equação

assim,

$|q| \geq 1$ e $|a| = |d||q| \geq |d|$

Portanto,

$|d| \leq |a|$

Se $q = 0$

$a = qd$

$= 0 \cdot d$

$= 0$

TEORIA DOS NÚMEROS

DIVISIBILIDADE

Sejam $a, b, c, d \in \mathbb{Z}$

(iii) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração:

Se que $a \mid b$ e $b \mid c$, então existe $q_1, q_2 \in \mathbb{Z}$ tais que

$b = aq_1$ e $c = bq_2$, logo $c = a.q_1q_2$ e portanto $a \mid c$.

TEORIA DOS NÚMEROS

MDC, MMC

Dados dois números inteiros a e b com $a \neq 0$ ou b $\neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos D_a e D_b respectivamente, e a intersecção de tais conjuntos $D_a \cap D_b$ é finita (pela "limitação") e não vazia (já que 1 pertence à intersecção).

Por ser finito, $D_a \cap D_b$ possui elemento máximo, que é chamado de *máximo divisor comum* (mdc) dos números a e b.

- *máximo divisor comum* (mdc) entre dois inteiros positivos a e b: denotado por mdc(a, b), tal que $n \mid a$ e $n \mid b$.
- quando mdc(a,b) = 1 dizemos que a e b são primos entre si.

TEORIA DOS NÚMEROS

MDC, MMC

Por outro lado, se denotarmos por M_n o conjunto dos múltiplos positivos de n, dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a intersecção $M_a \cap M_b$ é não vazia (pois $|ab|$ está na intersecção).

Como os naturais são bem ordenados, $M_a \cap M_b$ possui elemento mínimo, assim, a intersecção $M_a \cap M_b$ é um conjunto não vazio de números naturais, possuindo um menor elemento. Tal número é chamado *mínimo múltiplo comum* (mmc) de a e b, denotado por mmc(a,b)

TEORIA DOS NÚMEROS

MDC, MMC

Exemplo: Considerando a = 24 e b = 16, calcule o mmc(a,b) e mdc(a,b).

TEORIA DOS NÚMEROS

MDC, MMC

Exemplo: Considerando a = 24 e b = 16, calcule o mmc(a,b) e mdc(a,b).

24 | 2	16 | 2	24,16 | 2
12 | 2	8 | 2	12, 8 | 2
6 | 2	4 | 2	6, 4 | 2
3 | 3	2 | 2	3, 2 | 2
1 | $2^3 \cdot 3$	1 | $2^3 \cdot 2$	3, 1 | 3
		1, 1 | $2^4 \cdot 3$

mmc(24,16) = 48

mdc(24,16) = 8

TEORIA DOS NÚMEROS

MDC, MMC

Agora, considere a = 191 e b = 359. Calcule o mmc(a,b) e mdc(a,b).

TEORIA DOS NÚMEROS

MDC, MMC

Agora, considere a = 191 e b = 359. Calcule o mmc(a,b) e mdc(a,b).

191 | 191 359 | 359 191, 359 | 191

1 | 1 | 1, 359 | 359

1, 1 | 191·359

mmc(191,359) = 68569

mdc(24,16) = 1

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

Para calcularmos a mdc e o mmc de maneira eficiente, será abordado o *algoritmo de Euclides* ou *algoritmo das divisões sucessivas*.

Primeiramente, vamos relembrar o conceito de *divisão euclidiana*, ou *divisão com resto*

dados $a,b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ com

$$a = bq + \mathrm{r} \qquad \text{e} \qquad 0 \leq r < |b|.$$

sendo q o *quociente* e r o *resto da divisão* de a por b. O resto r é também denotado por a mod b.

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

O algoritmo de Euclides foi descrito pelo matemático grego Euclides há mais de 2300 anos, sendo um dos algoritmos mais antigos conhecidos.

- máximo divisor comum (mdc): o mdc entre dois inteiros positivos a e b é denotado por mdc(a, b), tal que $n \mid a$ e $n \mid b$.

- Algoritmo Euclidiano: Se $a = bq + r$, então mdc(a,b) = mdc(b,r).

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

Casos triviais do mdc(a, b) que não necessitam do algoritmo de Euclides:

mdc(a, a) = a.

a | a e não existe um inteiro maior que divida a.

mdc(a, 0) = a.

pela propriedade "*limitação*"

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

O algoritmo de Euclides funciona por meio de uma sucessão de divisões.

Para encontrar mdc(a, b), supondo que $a > b$,

1) Divida primeiro a por b, obtendo um *quociente* e um *resto*.
2) Formalmente, nesse instante temos $a = q_1 b + r_1$, em que $0 \leq r1 < b$. A seguir, divida o divisor b, pelo resto r_1, obtendo $b = q_2 r_1 + r_2$, em que $0 \leq r_2 < r_1$.
3) Novamente, divida o divisor, r_1, pelo resto r_2, obtendo $r_1 = q_3 r_2 + r_3$, em que $0 \leq r_3 < r_2$.

Temos aqui um processo em laço, com os restos ficando sucessivamente menores.

Esse processo termina quando encontramos um resto 0; o máximo divisor comum é o último divisor utilizado.

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

Exemplo: Calcule o mdc(420, 66)

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

Exemplo: Calcule o mdc(420, 66)

$$420 = 6 \cdot 66 + 24$$
$$66 = 2 \cdot 24 + 18$$
$$24 = 1 \cdot 18 + 6$$
$$18 = 3 \cdot 6 + 0$$

Assim, temos $mdc(420, 66) = mdc(66, 24) = mdc(24, 18) = mdc(18, 6) = mdc(6, 0) = 6$

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

Exemplo: Calcule o mdc(45235218, 612374)

TEORIA DOS NÚMEROS

ALGORITMO DE EUCLIDES

MDC (inteiro positivo *a*; inteiro positivo *b*)
//a > b
Variáveis locais:
inteiros *i*, *j*
    $i = a$
    $j = b$
    enquanto $j \neq 0$ **faça**
        calcule $i = qj + r, 0 \leq r < j$
        $i = j$
        $j = r$
    fim do enquanto
    // i agora tem o valor mdc(*a*, *b*)
    retorne *i*;
fim da função *MDC*

```python
def algoritmo_euclides(a, b):
    while b != 0:
        a = b
    b = a % b
    return a
```

TEORIA DOS NÚMEROS

MDC, MMC e Algoritmo de Euclides

Assim, o algoritmo de Euclides pode ser usado como uma ferramenta para o cálculo do mdc. Agora veremos o algoritmo de Euclides estendido conhecido como *Lema de Bézout* (ou identidade de Bézout).

O teorema mostra que é sempre possível escrever o mdc de dois números como a combinação linear destes (com coeficientes inteiros.)

Sejam $a,b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com

$$ax + by = \text{mdc}(a,b).$$

Portanto se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \text{mdc}(a,b)$.

TEORIA DOS NÚMEROS

Lema de Bézout (ou identidade de Bézout)

Usando o algoritmo de Euclides, o mdc(420, 66) = 6. E 6 pode ser escrito como uma combinação linear de 420 e 66:

$$6 = 3(420) - 19(66)$$

Embora seja fácil verificar neste exemplo que 3(420) - 19(66) tem o valor 6, os valores dos coeficientes 3 e -19 parecem misteriosos. Como eles foram obtidos?

TEORIA DOS NÚMEROS

Lema de Bézout (ou identidade de Bézout)

Usando o algoritmo de Euclides, o mdc(420, 66) = 6. E 6 pode ser escrito como uma combinação linear de 420 e 66:

$$6 = 3(420) - 19(66)$$

o mdc (420, 66) pode ser calculado pelos seguintes passos?

1) $420 = 6 \cdot 66 + 24$
2) $66 = 2 \cdot 24 + 18$
3) $24 = 1 \cdot 18 + 6$
4) $18 = 3 \cdot 6 + 0$

reescrevendo 1,2,3 → $6 = 24 - 1 \cdot 18$
$18 = 66 - 2 \cdot 24$
$24 = 420 - 6 \cdot 66$

Agora usamos essas equações fazendo diversas substituições:

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 \\ &= 24 - 1 \cdot (66 - 2 \cdot 24) \\ &= 24 - 1 \cdot (66 - 48) \\ &= 72 - 66 \end{aligned}$$

$$\begin{aligned} &= 3 \cdot 24 - 66 \\ &= 3 \cdot (420 - 6 \cdot 66) - 66 \\ &= 3 \cdot (420 - 396) - 66 \\ &= 3 \cdot 420 - 3 \cdot 396 - 66 \\ &= 3 \cdot 420 - 1188 - 66 \\ &= 3 \cdot 420 - 19 \cdot 66 \end{aligned}$$

que revela a combinação linear de 420 e 66 que fornece o valor 6

Exercícios

1) Calcule o MDC de 149 e 59.
2) Calcule o MDC de 211 e 47.
3) Calcule o MDC de 33101 e 32041.
4) Calcule o MDC de 14965 e 2370.
5) Calcule o MDC de 10000321 e 242609.
6) Calcule o MDC de 26584236 e 735767.
7) Valéria tem 48 bolas de futebol e 32 bolas de vôlei. Ela quer dividi-las em caixas, com o mesmo número de bolas em cada caixa. Qual é o maior número de bolas que ela pode colocar em cada caixa de modo que todas as bolas de futebol e basquete sejam usadas?
8) Um decorador tem 151 flores vermelhas e 348 flores brancas. Ele deseja fazer buquês com o mesmo número de flores de cada cor em cada buquê. Qual é o maior número de flores que ele pode colocar em cada buquê?