ARITMÉTICA

PROF. LUCIANO MONTEIRO DE CASTRO

Conteúdo

1. Introdução / Pré-requisitos 1
2. Divisão Euclidiana e Divisibilidade 1
3. Máximo Divisor Comum (M.D.C.) 2
3.1. Algoritmo de Euclides 2
4. Números Primos 3

1. Introdução / Pré-requisitos

Este texto apresenta alguns fatos da Aritmética dos números inteiros, de forma resumida. Supõe-se que o leitor está familiarizado com as propriedades básicas da adição, subtração e multiplicação de números inteiros, com as relações de ordem nesse conjunto e com a noção intuitiva de que um conjunto não vazio de inteiros positivos (ou não negativos) possui um elemento mínimo. Uma construção formal (axiomática) dos fatos apresentados está além do escopo deste trabalho, e pode ser encontrada pelo leitor interessado em diversos bons livros sobre o assunto.

2. Divisão Euclidiana e Divisibilidade

Dados os inteiros n e d, com $d > 0$, existem inteiros q e r, únicos, tais que

$$n = qd + r \quad \text{e} \quad 0 \leq r < d.$$

Para provar este fato, basta ver que r é o menor elemento não negativo do conjunto de inteiros da forma $n - xd$, com $x \in \mathbb{Z}$.

Os números q e r são chamados, respectivamente, *quociente* e *resto* da divisão de n por d. Quando $r = 0$, dizemos que d é *divisor* de n, ou ainda que n é *múltiplo* de d. Neste caso, temos $n = qd$ e, em particular, $|d| \leq |n|$.

3. Máximo Divisor Comum (M.D.C.)

Dados dois inteiros a e b chamamos de *máximo divisor comum* (abreviadamente *mdc*) de a e b ao maior inteiro m que é simultaneamente divisor de a e de b.

Teorema 3.1. (Fundamentação do Algoritmo de Euclides) *Seja* c *o resto da divisão do inteiro* a *pelo inteiro (positivo)* b*. Então* $\text{mdc}(a, b) = \text{mdc}(b, c)$.

Demonstração. Pela divisão euclidiana, existe um inteiro q tal que $a = qb + c$. Sejam $m = \text{mdc}(a, b)$ e $n = \text{mdc}(b, c)$. Como m é divisor tanto de a como de b, existem inteiros a_1 e b_1 tais que $a = ma_1$ e $b = mb_1$. Assim, $c = a - qb = ma_1 - qmb_1 = m(a_1 - qb_1)$, logo m é divisor comum entre b e c, o que implica que $m \leq n$. Analogamente, como n é divisor tanto de b como de c, também é divisor de $a = qb + c$, logo é divisor comum entre a e b e, portanto, $n \leq m$. Isso prova que $m = n$, como queríamos. □

3.1. **Algoritmo de Euclides.** Podemos calcular o mdc entre dois inteiros aplicando recursivamente o teorema anterior, obtendo o chamado *método das divisões sucessivas* ou *Algoritmo de Euclides*.

Exercício 3.2 (Exemplo)**.** Para calcular o mdc entre 330 e 126, dividimos 330 por 126 e encontramos o resto 78. A seguir dividimos 126 por 78 e o resto é 48. Continuamos dividindo 78 por 48 (resto 30), 48 por 30 (resto 18) e 30 por 18 (resto 6). Como 18 é múltiplo de 6, concluímos que o mdc procurado é 6, pois o teorema 3.1 garante que

$$\text{mdc}(330, 126) = \text{mdc}(126, 78) = \text{mdc}(78, 48) = \text{mdc}(48, 30) = \text{mdc}(30, 18) = \text{mdc}(18, 6) = 6.$$

Teorema 3.3. (Teorema de Bézout) *Dados os inteiros* a *e* b*, existem inteiros* x *e* y *tais que* $\text{mdc}(a, b) = ax + by$.

Demonstração. Seja m o menor elemento positivo do conjunto I de todos os inteiros da forma $ax+by$, com x e y inteiros. Dividindo a por m encontramos $a = qm+r$, com q e r inteiros e $0 \leq r < m$. Por ser um elemento de I, m é a soma de um múltiplo de a com um múltiplo de b, logo $r = a - qm$ também será uma soma deste tipo e, portanto, elemento de I. Como $r < m$ e m é o menor elemento

positivo de I, concluímos que $r = 0$, isto é, m é divisor de a. Analogamente, provamos que m é divisor de b. Agora, se d é um divisor comum qualquer de a e b, d é divisor de qualquer elemento de I, logo d é divisor de m, o que implica que $d \leq m$. Assim, $m = \text{mdc}(a, b)$. □

Corolário 3.4. *Todo divisor comum de dois inteiros é divisor de seu mdc.*

Teorema 3.5. *Se o produto* bc *é múltiplo de* a *e* $\text{mdc}(a, b) = 1$*, então* c *é múltiplo de* a*.*

Demonstração. Pelo Teorema de Bézout, existem inteiros x e y tais que $1 = ax + by$. Multiplicando por c obtemos $c = cax + bcy$. Como cax e bcy são múltiplos de a, c é múltiplo de a. □

4. Números Primos

Chamamos de *primo* um número inteiro positivo que possua exatamente dois divisores positivos. Por exemplo, os primeiros dez números primos são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Lema 4.1. *Se o produto* ab *é múltiplo de um número primo* p*, então* a *é múltiplo de* p *ou* b *é múltiplo de* p*.*

Demonstração. Segue imediatamente de 3.5. □

Teorema 4.2. (Teorema Fundamental da Aritmética) *Todo número inteiro positivo maior que* 1 *pode ser representado de forma única como um produto de números primos (salvo ordem dos fatores).*

Demonstração. Se $n > 1$ é primo, não há o que demonstrar. Se n não é primo, então possui um divisor a diferente de 1 e de n, logo $n = a \cdot b$, com $a > 1$ e $b > 1$. Se ambos os fatores a e b são primos, o teorema está demonstrado. Caso contrário repetimos o processo para a ou b (ou ambos). Como a cada passo obtemos fatores menores, este procedimento deve terminar em um número finito de passos. Neste ponto, todos os fatores obtidos devem ser primos (caso contrário seria possível continuar o processo). Agora, suponha que n tenha duas representações distintas como produto de números primos. Então, existirá um primo p de uma

representação que não está presente na outra. Utilizando recursivamente o lema anterior concluímos que p é divisor de um primo q, com $p \neq q$, uma contradição pois $1, p, q$ seriam 3 divisores positivos distintos de q. $\square$