Teoria dos Números: tópicos 1.2 e 1.3)

Prof. Rafael Alves Bonfim de Queiroz
rafael.queiroz@ufop.edu.br

Conteúdo programático

- 1.2) Algoritmo da divisão
- 1.3) Divisibilidade e primo

Algoritmo de divisão usando uma calculadora

Suponha que a e b sejam ambos positivos. Então pode-se encontrar o quociente q e o resto r usando uma calculadora como segue:

- **Passo 1**. Divida a por b usando a calculadora, ou seja, encontre a/b.
- **Passo 2**. Seja q a parte inteira de a/b, ou seja, seja $q = \text{int}(a/b)$.
- **Passo 3**. Seja r a diferença entre a e bq, ou seja, seja $r = a - bq$.

- **Exemplo 1**: Seja $a = 4461$ e $b = 16$.
  $a/b = 278,8125\cdots$, então $q = 278$, $r = 4461 - 16(278) = 13$.
- **Exemplo 2**: Seja $a = -262$ e $b = 3$.
  - Primeiro dividimos $|a| = 262$ por $b = 3$. Então $q = 87$ e $r = 1$
    $262 = 3(87) + 1$
  - $a = -262$, então multiplicamos por -1 obtendo
    -262 = 3(-87) - 1
  - -1 é negativo e, portanto, não pode ser r. Corrigimos isso adicionando e subtraindo o valor de b (que é 3) da seguinte forma: -262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2
- Exemplo 3: Seja $b = 2$. Então qualquer inteiro a pode ser escrito na forma $a = 2q + r$, onde $0 \leq r < 2$. Assim, r só pode ser 0 ou 1. Assim, todo inteiro é da forma $2k$ ou $2k + 1$.

Divisibilidade

- Sejam a e b inteiros com $a \neq 0$. Suponha $ac = b$ para algum inteiro c. Dizemos então que a divide b ou b é divisível por a, e denotamos isso escrevendo

$$a|b$$

- Dizemos também que b é um múltiplo de a ou que a é um fator ou divisor de b.
- **Teorema**: Suponha que a, b, c sejam inteiros.
  - (i) Se $a|b$ e $b|c$, então $a|c$.
  - (ii) Se $a|b$ então, para qualquer inteiro x, $a|bx$.
  - (iii) Se $a|b$ e $a|c$, então $a|(b+c)$ e $a|(b-c)$.
  - (iv) Se $a|b$ e $b \neq 0$, então $a = \pm b$ ou $|a| < |b|$.
  - (v) Se $a|b$ e $b|a$, então $|a| = |b|$, ou seja, $a = \pm b$.
  - (vi) Se $a|1$, então $a = \pm 1$
- **Corolário**: Suponha $a|b$ e $a|c$. Então, para quaisquer inteiros x e y, $a|(bx+cy)$. A expressão $bx+cy$ será chamada de combinação linear de b e c.

Primo

- Um inteiro positivo $p > 1$ é chamado de número primo ou primo se seus únicos divisores forem ± 1 e $\pm p$, isto é, se p tem apenas divisores triviais.
- Se $n > 1$ não é primo, então n é dito composto.
  - se $n > 1$ é composto então $n = ab$ onde $1 < a, b < n$.
- **Teorema**: Todo inteiro $n > 1$ pode ser escrito como um produto de primos.
- **Teorema**: Não existe primo maior, ou seja, existe um número infinito de primos.