# Teoria dos Números: Teorema Fundamental da Aritmética (1.5)

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

# Conteúdo programático

- 1.5) Teorema Fundamental da Aritmética

# Inteiros Relativamente Primos

- Dois inteiros $a$ e $b$ são *relativamente primos* ou *coprimos* se $mdc(a, b) = 1$.
- Assim, se $a$ e $b$ são relativamente primo, então existem inteiros $x$ e $y$ tais que $ax + by = 1$
- Por outro lado, se $ax + by = 1$, então $a$ e $b$ são relativamente primos.
- Exemplos:
  - (a) Observe que: mdc(12, 35) $=$ 1, mdc(49, 18) $=$ 1, mdc(21, 64) $=$ 1, mdc(-28, 45) $=$ 1
  - (b) Se $p$ e $q$ são primos distintos, então $mdc(p, q) = 1$.
  - (c) Para qualquer inteiro $a$, temos $mdc(a, a + 1) = 1$, pois qualquer fator comum de $a$ e $a + 1$ deve dividir seus diferença $(a + 1) - a = 1$.

- **Teorema**: Suponha que $mdc(a, b) = 1$, e $a$ e $b$ dividem $c$. Então $ab$ divide $c$.
- **Teorema**: Suponha $a|bc$ e $mdc(a, b) = 1$. Então $a|c$
  - **Prova**: Como mdc($a$, $b$) $= 1$, existem $x$ e $y$ tais que $ax + by = 1$.
  - Multiplicando por $c$ resulta: $acx + bcy = c$
  - Temos $a|acx$.
  - Além disso, $a|bcy$ pois, por hipótese, $a|bc$.
  - Assim, a divide a soma $acx + bcy = c$.
- **Corolário**: Suponha que $a$ primo $p$ divida o produto $ab$. Então $p|a$ ou $p|b$.

# Teorema Fundamental da Aritmética

- Teorema: Todo inteiro $n > 1$ pode ser escrito como um produto de primos.
- Podem diferentes produtos de primos produzir o mesmo número? Claramente, podemos reorganizar a ordem dos fatores primos, por exemplo, $30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$
- Teorema (Teorema Fundamental da Aritmética): Todo inteiro $n > 1$ pode ser expresso de forma única (exceto para ordem) como um produto de números primos.

# Teorema Fundamental da Aritmética

- Os primos na fatoração de $n$ não precisam ser distintos.
- Freqüentemente, é útil reunir todos os primos
- Então $n$ pode ser expresso exclusivamente na forma $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ onde os $m_i$ são positivos e $p_1 < p_2 < \cdots < p_r$ .
- Isso é chamado de fatoração canônica de $n$.

# Exemplo 1 - MDC

- Dados $a = 2^4 \times 3^3 \times 7 \times 11 \times 13$ e $b = 2^3 \times 3^2 \times 5^2 \times 11 \times 17$. Encontre $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$
  - Primeiro encontramos $d = \text{mdc}(a, b)$.
    - ★ Esses primos $p$, que aparecem em $a$ e $b$, 2, 3 e 11, também aparecerão em $d$, e o expoente de $p$, em $d$ será o menor de seus expoentes em $a$ e $b$. item Assim
    - ★ $d = \text{mdc}(a, b) = 2^3 \times 3^2 \times 11 = 792$

# Exemplo 1 - MMC

- Dados $a = 2^4 \times 3^3 \times 7 \times 11 \times 13$ e $b = 2^3 \times 3^2 \times 5^2 \times 11 \times 17$. Encontre $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$
  - A seguir encontramos $m = \text{mmc}(a, b)$.
    - ★ Esses primos $p$, que aparecem em $a$ ou $b$, 2, 3, 5, 7, 11, 13 e 17, serão também aparecem em $m$, e o expoente de $p$ em $m$ será o maior de seus expoentes em $a$ e $b$. Por isso
    - ★ $m = \text{mmc}(a, b) = 2^4 \times 3^3 \times 5^2 \times 7 \times 11 \times 13 \times 17$

# Observação sobre o Teorema Fundamental da Aritmética

- Estamos tão acostumados a usar números como se o Teorema Fundamental da Aritmética fosse verdadeiro que pode parecer que não precisa de prova
- É uma homenagem a Euclides, que primeiro provou o teorema, que ele reconheceu que requer prova.
- Enfatizamos a não trivialidade do teorema dando um exemplo de um sistema de números que não não satisfaz este teorema.

# Exemplo 2

Seja $F$ o conjunto dos inteiros positivos da forma $3x + 1$.

- Assim $F$ consiste nos números: 1, 4, 7, 10, 13, 16, 19, 22, $\cdots$
- Observe que o produto de dois números em $F$ está novamente em $F$ pois: $(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$
- Nossa definição de primos faz todo o sentido em $F$
- Embora $4 = 2 \cdot 2$ , o número 2 não está em $F$.
- Assim 4 é primo em $F$ já que 4 não tem fatores exceto 1 e 4.
- Da mesma forma 10, 22, 25, $\cdots$ são primos em $F$
- Listamos os primeiros primos em $F$ : 4, 7, 10, 13, 19, 22, 25, $\cdots$ item Nota $100 = 3(33) + 1$ pertence a F .
  - No entanto, 100 tem duas fatorações essencialmente diferentes em primos de $F$; nomeadamente, $100 = 4 \cdot 25$ e $100 = 10 \cdot 10$
  - Portanto, não há fatoração única em primos em $F$

.

# Próximo tópico do conteúdo programático

- 1.6) Relação de congruência

# Relação de congruência

- Seja $m$ um inteiro positivo. Dizemos que $a$ é congruente a $b$ módulo $m$, escrito
  $a \equiv b$ (módulo $m$) ou simplesmente $a \equiv b \pmod{m}$
  se $m$ divide a diferença $a - b$ .
- O inteiro $m$ é chamado de módulo. A negação de $a \equiv b \pmod{m}$ é escrita $a \not\equiv b \pmod{m}$.
- Por exemplo
  1. $87 \equiv 23 \pmod{4}$ já que 4 divide 87 - 23 $=$ 64.
  2. $67 \equiv 1 \pmod{6}$ já que 6 divide 67 - 1 $=$ 66.
  3. $72 \equiv -5 \pmod{7}$ já que 7 divide 72 - (-5) $=$ 77.
  4. $27 \not\equiv 8 \pmod{9}$ já que 9 não divide 27 - 8 $=$ 19.