Lista de exercícios 01 - FMC

Andriel Vinicius de M. Fernandes

7 de abril de 2024

Teorema 1 *Teorema Fundamental da Aritmética: Todo inteiro positivo n pode ser escrito de maneira única como o produto de números primos, onde os fatores primos são escritos em ordem crescente de grandeza.*

1 Primos

1. Mostre que se n é um inteiro composto qualquer ele possui um divisor primo menor ou igual a $\sqrt{n}$.
   Demonstração.
   Seja n um inteiro composto arbitrário.
   Logo, **(1)** pelo Teorema Fundamental da Aritmética, $\exists a, b \in \mathbb{Z}, n = a \cdot b$, com $a, b > 1$.
   (2) Note que, aplicando a definição de divisibilidade em **(1)**, temos que $a|n$.
   (3) Suponha que $a \leq b$.
   Note que:

$$\begin{aligned}
a \leq b &\implies a \leq \frac{n}{a} && (\text{Para } b = \frac{n}{a}) \\
&\implies a^2 \leq n && (\text{Por aritmética}) \\
&\implies \sqrt{a^2} \leq \sqrt{n} && (\text{Por aritmética}) \\
&\implies a \leq \sqrt{n} && (\text{Por aritmética})
\end{aligned}$$

   (4) Logo, $a \leq \sqrt{n}$.
   Assim, temos dois casos para a:

- a é primo. Nesse caso, a não é decomposto em outros fatores e é imediato que a é divisor primo de n tal que $a \leq \sqrt{n}$ por **(4)** e **(2)**.
- a é composto. Nesse caso, pelo Teorema Fundamental da Aritmética, temos que a é resultado de um produto de números primos, onde um desses é um inteiro primo p. Aplicando a def. de divisibilidade, temos que $\exists p_0 \in \mathbb{Z}, p \cdot p_0 = a \iff p|a$. Assim, se $p|a$ e $a|n$ por **(2)**, então $p|n$ pela transitividade da divisão. Note ainda que $p \leq a \leq \sqrt{n} \implies p \leq \sqrt{n}$ por **(4)**.

(5) Portanto, está mostrado que existe sempre um divisor primo de um natural qualquer menor ou igual à raiz quadrada deste natural.

2. Demonstre o Lema de Euclides: sejam $a, b, p \in \mathbb{Z}$ com p primo; se $p|ab$, então $p|a$ ou $p|b$ (note que é possível que p divida tanto a quanto b).
Demonstração.
Sejam $a, b, p \in \mathbb{Z}$, onde p é primo.
(1) Assuma $p|ab$.
Suponha $p \nmid a$. Logo, **(2)** $mdc(a, p) = 1$.
(3) Note que $\exists s, t \in \mathbb{Z}; mdc(a, p) = sa + tp$, pelo Teorema de Bezout.
(4) Note que $sa + tp = 1$, por **(3)** e **(2)**.
(5) Note também que $p|p$, logo $p|p \cdot (bt)$ por propriedade de divisibilidade.
(6) Note também que $p|ab$, logo $p|ab \cdot (s)$ por propriedade de divisibilidade.
(7) Dessa forma, temos que

$$\begin{aligned} p|((p \cdot bt) + (ab \cdot s)) &= p|b \cdot (sa + tp) && \text{(Por aritmética)} \\ &= p|b && \text{(Por } \mathbf{(4)}\text{)} \end{aligned}$$

(8) Portanto, $p|b$ e o lema é válido.

3. Demonstre que para qualquer inteiro n, se $n \mod 7 = 2$, então $n^2 \mod 7 = 2$.
Resolução.
Tome $n = 9$. Note que

$$\begin{aligned} 9 \mod 7 &= 9 - ((\frac{9}{7}) \cdot 7) && \text{(Por def. de mod)} \\ &= 9 - 7 && \text{(Por aritmética)} \\ &= 2 \end{aligned}$$

Mas, tomando $n^2 = 9^2 = 81$, temos:

$$\begin{aligned}
81 \mod 7 &= 81 - ((\frac{81}{7} \cdot 7) && \text{(Por def. de mod)} \\
&= 81 - 77 && \text{(Por aritmética)} \\
&= 4
\end{aligned}$$

Portanto, a proposição é falsa.