Lista dos Resultados Vistos

(27 de junho 2022)

Definição: $a, b \in \mathbb{Z}$. Diremos que a/b se existe $c \in \mathbb{Z}$ tal que $b = a.c$.

Lema (1): Se a/b, b/c então a/c.

Lema (2): Se a/b, a/c então $a/rb+sc$, $\forall r, s \in \mathbb{Z}$.

Princípio da Boa Ordenação: Todo subconjunto de $\mathbb{N}$ ≠ ∅ tem um menor elemento.

Teorema (Algoritmo de Euclides): Sejam $a, b \in \mathbb{N}$. Então existem únicos $q, r \in \mathbb{Z}$ tais que $a = bq + r$, com $0 \leq r < b$.

Definição: Diremos que $d = mdc(a,b)$ se: ① d/a, d/b; ② Se d^*/a e d^*/b então $d^* \leq d$.

Lema (3): Se $d = mdc(a,b)$ então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Lema (4): Se $d = mdc(a,b)$ então existem $r, s \in \mathbb{Z}$ tq $d = ra + sb$.

Corolário: Seja $d = mdc(a,b)$. Se d^*/a, d^*/b então d^*/d.

Lema (5): Se a/bc e $mdc(a,b) = 1$ então a/c.

Lema (6): Escreva $a = bq + r$. Então $mdc(a,b) = mdc(b,r)$.

Algoritmo de Euclides para o cálculo do mdc:

$$
\begin{aligned}
a &= bq + r \\
b &= rq_1 + r_1 \\
&\vdots \\
r_{n-3} &= r_{n-2}q_n + r_{n-1} \\
r_{n-2} &= r_{n-1}q_{n+1}
\end{aligned}
\qquad \Rightarrow \qquad r_{n-1} = mdc(a,b)
$$

Equação Diofantina Linear em duas variáveis: $ax + by = c \quad (1)$

Lema (1): A equação (1) tem soluções inteiras $\Leftrightarrow$ $\text{mdc}(a,b)$ divide c.

Lema (2): Se $x_0, y_0 \in \mathbb{Z}$ é uma solução da equação (1) então todas as demais soluções são do tipo: $x_t = x_0 + \frac{b}{d}t$, $y_t = y_0 - \frac{a}{d}t$, com $t \in \mathbb{Z}$ e $d = \text{mdc}(a,b)$.

Corolário: Se $\text{mdc}(a,b) = 1$ então a equação (1) sempre tem solução, independente do valor de $c \in \mathbb{Z}$.

Indução Matemática (1ª forma)

Seja $\mathcal{N} \subseteq \mathbb{N} \cup \{0\}$ e escreva $\mathcal{N} = \{n_0, n_1, n_2, \dots\}$ com $n_0 < n_1 < n_2 < \dots$

Seja $p(n)$ uma proposição lógica que depende de n.

Se:

(1) $p(n_0)$ é verdadeiro;

(2) Se $p(n_k)$ ser verdadeiro implica que $p(n_{k+1})$ é também verdadeiro $\forall\, n_k \in \mathcal{N}$

então

$p(n)$ é verdadeiro para todo $n \in \mathcal{N}$.

Indução (2ª forma)

* somente modifica a hipótese (2) anterior, mantendo a conclusão.

(1) $p(n_0)$ é verdadeiro;

(2) $p(n_j)$ é verdadeiro, $\forall\, j < k$ então $p(n_k)$ é verdadeiro

Definição: $p \in \mathbb{N}$, $p \neq 1$ é chamado de primo se os únicos divisores positivos de p são 1 e p.

Lema (9): Seja p um primo. Se $p \nmid a$ então $\text{mdc}(p, a) = 1$.

Lema (10): Sejam p um primo e $a, b \in \mathbb{Z}$. Se $p \mid ab$ então $p \mid a$ ou $p \mid b$.

Lema (11): Sejam p, q_1, q_2 primos. Se $p \mid q_1 \cdot q_2$ então $p = q_1$ ou $p = q_2$.

Lema (12): Sejam $p, q_1, \dots, q_n$ primos. Se $p \mid q_1 \cdot q_2 \cdots q_n$ então $\exists\, j \in \{1, 2, \dots, n\}$ tal que $p = q_j$.

Definição: $m \in \mathbb{N}$, $m \neq 1$ é chamado de composto se m não é primo.

Lema (13): Sejam p, q primos distintos. Se $p \mid a$ e $q \mid a$ então $pq \mid a$.

Teorema Fundamental da Aritmética:

Todo número natural maior que 1 pode ser escrito de maneira única (a menos da ordem dos fatores) como um produto de primos.

Lema (14): Sejam $q, p_1, \dots, p_r$ primos. Se $q^m \mid p_1^{t_1} \cdots p_r^{t_n}$ então $\exists\, j \in \{1, 2, \dots, r\}$ tal que $q = p_j$ e $m \leq t_j$.

Lema (15): Seja $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_s^{r_s}$, com $p_1, \dots, p_s$ primos distintos. Então

$$d \mid n \iff d = p_1^{\ell_1} \cdot p_2^{\ell_2} \cdots p_s^{\ell_s}, \text{ com } 0 \leq \ell_i \leq r_i, \quad i = 1, 2, \dots, s.$$

Definição: $m = mmc(a,b)$ se: (1) a/m, b/m; (2) se a/m^*, b/m^* então $m \leq m^*$

Lema (17): Sejam $a, b \in \mathbb{N}$ e escreva $a = p_1^{r_1} \cdots p_s^{r_s}$ e $b = p_1^{\ell_1} \cdots p_s^{\ell_s}$ com $r_j \geq 0$ e $\ell_j \geq 0$, para $j = 1, 2, \ldots, s$ e $p_1 < p_2 < \cdots < p_s$ primos.

Defina $v_j = \min\{r_j, \ell_j\}$ e $u_j = \max\{r_j, \ell_j\}$ com $j = 1, 2, \ldots, s$

então

$$mdc(a,b) = p_1^{v_1} \cdots p_s^{v_s} \quad \text{e} \quad mmc(a,b) = p_1^{u_1} \cdots p_s^{u_s}$$

Corolário: Se a/m^* e b/m^* então $mmc(a,b)$ divide m^*.

Lema (18): $mdc(a,b) \cdot mmc(a,b) = a \cdot b$