Universidade de São Paulo

Álgebra

Versão de 29 de agosto de 2018

Níckolas de Aguiar Alves

Álgebra

Níckolas de Aguiar Alves

São Paulo
29 de agosto de 2018

Lista de tarefas pendentes

Foi Littlewood quem disse que todo inteiro positivo era um dos amigos pessoais de Ramanujan.

The Indian Mathematician Ramanujan
Godfrey H. Hardy

Sumário

Prefácio

As presentes notas foram escritas como um método de estudo de conteúdos introdutórios de Álgebra. Tendo como autor um graduando, estão sujeitas a erros e ainda necessitam passar por um processo minucioso de revisão de provas. Além disso, é importantíssimo ressaltar que ainda estão em uma versão preliminar, e possivelmente passarão por um processo de cortes, inserções e reordenamentos para que possam assumir uma estrutura mais adequada.

O texto foi escrito com base principal em [4]. Conteúdo, a ordem de alguns conteúdos foi trocada (o Capítulo 1, por exemplo, deriva de um apêndice de [4]) e outros foram muito mais aprofundados (os resultados da Seção §2 acerca de ordens foram provados pelo autor com base nas definições obtidas em [10]).

É perceptível a pequena quantidade de exemplos ao longo do texto. Isso se deve às notas tentarem, tanto quanto possível, construir-se sobre as proposições e definições de forma que elas sejam o próprio exemplo. Ao invés de dar diversos exemplos de relações de ordem parcial ampla, prefere-se fornecer a definição, deduzir alguns resultados, definir a relação de menor ou igual em $\mathbb{N}$ e mostrar que satisfaz as hipóteses de uma ordem ampla. Desta forma, mantém-se em certos pontos um tratamento um pouco mais abstrato, mas em geral o texto se apega fortemente ao objeto de estudo, que crê-se ser consideravelmente concreto em comparação com outros tópicos de Álgebra.

Ao final das notas, pode-se ainda encontrar um Glossário de Definições, que sumariza todas as definições feitas ao longo dos capítulos e apêndices. Seu objetivo é fornecer uma referência rápida ao leitor.

Desde já o autor agradece pelo interesse em seu trabalho e se dispõe a receber críticas, elogios e/ou sugestões via e-mail por alves.nickolas@usp.br. Caso seja de interesse, outros de seus trabalhos podem ser encontrados em seu website pessoal, `http://soc.if.usp.br/~nickolas`.

Níckolas de Aguiar Alves
29 de agosto de 2018

Capítulo 1

Construção de Sistemas Numéricos Básicos

> O método de "postular" o que queremos tem muitas vantagens; elas são as mesmas vantagens do roubo sobre o trabalho honesto.
>
> *Introduction to Mathematical Philosophy*
> Bertrand Russel

§1: Axiomas de Peano e Operações em $\mathbb{N}$

Postulado 1:
Admitimos a existência dos três conceitos primitivos:

i. número natural;

ii. zero;

iii. sucessor. ♠

Notação:
Denotaremos o zero por 0, o sucessor de um número natural n por $\sigma(n)$ e o conjunto dos números naturais por $\mathbb{N}$. ♣

Axioma 2 [Axiomas de Peano]**:**
Admitimos a validade dos seguintes axiomas:

i. 0 é um número natural;

ii. a todo número natural n está associado um sucessor $\sigma(n)$, que também é um número natural;

iii. 0 não é o sucessor de número algum;

iv. $\sigma(n) = \sigma(m) \Rightarrow n = m$;

v. Princípio da Indução Matemática: se $S \subseteq \mathbb{N}$ satisfaz:

   (a) $0 \in S$;

   (b) $n \in S \Rightarrow \sigma(n) \in S$.

Então $S = \mathbb{N}$ ♠

Observação:
Utilizando as nomenclaturas modernas de conjuntos e funções, pode-se enunciar os Postulados e Axiomas de Peano de maneira alternativa. ♣

Postulado [Axiomas de Peano]**:**
Admitimos a existência de um conjunto $\mathbb{N}$, denominado conjunto dos números naturais, e de uma função $\sigma\colon \mathbb{N} \to \mathbb{N}$, denominada sucessor, tais que:

i. $\exists\, 0 \in \mathbb{N}; 0 \notin \operatorname{Ran}\sigma$;

ii. σ é injetora;

iii. seja $S \subseteq \mathbb{N}$ tal que

   (a) $0 \in S$;

   (b) $n \in S \Rightarrow \sigma(n) \in S$.

   Então $S = \mathbb{N}$. ♠

Notação:
$\mathbb{N}^* \equiv \mathbb{N} \setminus \{0\}$. ♣

Lema 1:
$\mathbb{N}^* \neq \varnothing$. □

Demonstração:
Pelo Axioma 2.i e pelo Axioma 2.ii, existe $\sigma(0) \in \mathbb{N}$. Pelo Axioma 2.iii, $0 \neq \sigma(0)$. Logo, $\sigma(0) \in \mathbb{N}^*$. Conclui-se que $\mathbb{N}^* \neq \varnothing$. ■

Proposição 2:
$\operatorname{Ran}\sigma = \mathbb{N}^*$. □

Demonstração:
Considere o conjunto $S := \{0\} \cup \operatorname{Ran}\sigma$. Claramente $0 \in S$ e, se $n \in S$, $\sigma(n) \in S$. Sabemos que $\exists\, \sigma(n) \in S$ pois, $\forall n \in S, n = 0 \vee n \in \operatorname{Ran}\sigma$. Se $n = 0$, então o Axioma 2.i e o Axioma 2.ii garantem que existe $\sigma(n) \in \mathbb{N}$. Se $n \in \operatorname{Ran}\sigma$, então o Axioma 2.ii nos diz que $n \in \mathbb{N}$ e o mesmo axioma garante que existe $\sigma(n) \in \mathbb{N}$. Logo - como $0 \in \mathbb{N}$ pelo Axioma 2.i e $\operatorname{Ran}\sigma \subseteq \mathbb{N}$ pelo Axioma 2.ii e, portanto, $S \subseteq \mathbb{N}$ - o Axioma 2.v nos leva à conclusão de que $S = \mathbb{N}$.
Segue então que

$$\begin{aligned}
\mathbb{N} &= S,\\
\mathbb{N} \setminus \{0\} &= (\{0\} \cup \operatorname{Ran}\sigma) \setminus \{0\},\\
\mathbb{N}^* &= (\{0\} \cup \operatorname{Ran}\sigma) \cap \mathbb{N}^*,\\
\mathbb{N}^* &= (\{0\} \cap \mathbb{N}^*) \cup (\operatorname{Ran}\sigma \cap \mathbb{N}^*),\\
\mathbb{N}^* &= \varnothing \cup (\operatorname{Ran}\sigma \cap \mathbb{N}^*),\\
\mathbb{N}^* &= \operatorname{Ran}\sigma \setminus \{0\},\\
\mathbb{N}^* &= \operatorname{Ran}\sigma. && \text{(Axioma 2.iii)}
\end{aligned}$$

Assim concluímos a demontração. ■

Corolário 3:
$\forall\, n \in \mathbb{N}^*, \exists\, m \in \mathbb{N}; n = \sigma(m)$. □

Demonstração:
O enunciado decorre trivialmente do Axioma 2.ii e da Proposição 2. ■

Definição 1 [Antecessor]**:**
Seja $n \in \mathbb{N}^*$. Dizemos que o número natural m que satisfaz $\sigma(m) = n$ é o *antecessor* de n e que n é o *sucessor* de m. Também dizemos que m *antecede* n e que n *sucede* m. ♠

Notação:
Seja $n \in \mathbb{N}^*$. Denotaremos o antecessor de n por $\alpha(n)$. ♣

Definição 2 [Adição]**:**
Seja $m \in \mathbb{N}$ um número natural dado. Então definimos a *soma*, também chamada de *adição* e denotada por $+$, de m com outro número natural por

i. $m + 0 = m$;

ii. $m + \sigma(n) = \sigma(m + n); \forall\, n \in \mathbb{N}$. ♠

Proposição 4:
Seja $m \in \mathbb{N}$ *um número natural dado. Então a soma* $m + n$ *está bem-definida para todo número natural* n. □

Demonstração:
Seja $S := \{n \in \mathbb{N};\ m + n \text{ está bem definido}\}$. Da Definição 2.i sabemos que $0 \in S$. Do Corolário 3 sabemos que $\mathbb{N} \subseteq S$. Pela Proposição 2 sabemos então que $n \in S \Rightarrow \sigma(n) \in S$, visto que $\operatorname{Ran} \sigma \subseteq S \subseteq \mathbb{N}$. Teremos então, pelo Axioma 2.v, que $S = \mathbb{N}$. ■

Observação:
Como, para cada $m \in \mathbb{N}$, $m + n$ está bem-definida para todo $n \in N$, vê-se que $m + n$ está bem definida $\forall\, m, n \in \mathbb{N}$. ♣

Proposição 5:
A adição de números naturais é associativa, i.e.,

$$m + (n + p) = (m + n) + p, \forall\, m, n, p \in \mathbb{N}.$$ □

Demonstração:
Seja $S := \{p \in \mathbb{N}; m + (n + p) = (m + n) + p, \forall\, m, n \in \mathbb{N}\}$. Queremos provar que $S = \mathbb{N}$.
Claramente vale que $0 \in S$, pois, pela Definição 2.i temos que

$$m + (n + 0) = m + n = (m + n) + 0.$$

Suponhamos que $p \in S$ e provemos que, neste caso, $\sigma(p) \in S$. Veja que

$$\begin{aligned} m + (n + \sigma(p)) &= m + \sigma(n + p), && \text{(Definição 2.ii)} \\ &= \sigma(m + (n + p)), && \text{(Definição 2.ii)} \\ &= \sigma((m + n) + p), && \text{(por hipótese)} \\ &= (m + n) + \sigma(p). && \text{(Definição 2.ii)} \end{aligned}$$

Assim, vemos que $p \in S \Rightarrow \sigma(p) \in S$. Como $S \subseteq \mathbb{N}$ e $0 \in S$, o Axioma 2.v implica que $S = \mathbb{N}$, encerrando a demonstração. ■

Lema 6:
$m + 0 = m = 0 + m, \forall\, m \in \mathbb{N}$. □

Demonstração:

Pela Definição 2.i, $m + 0 = m, \forall\, m \in \mathbb{N}$. Resta provar que $0 + m = m, \forall\, m \in \mathbb{N}$.

Seja $S := \{m \in \mathbb{N}; 0 + m = m\}$. É claro que $S \subseteq \mathbb{N}$ e que $0 \in S$, este último pois $0 + 0 = 0$, pela Definição 2.i.

Suponha que $m \in S$. Então $\sigma(m) \in S$, pois

$$\begin{aligned} 0 + \sigma(m) &= \sigma(0 + m), && \text{(Definição 2.ii)} \\ &= \sigma(m). && \text{(por hipótese)} \end{aligned}$$

Logo, o Axioma 2.v nos diz que $S = \mathbb{N}$, concluindo a demonstração. ■

Proposição 7:

$\exists!\, m \in \mathbb{N}; m + n = n = n + m, \forall\, n \in \mathbb{N}$. *Além disso, este único* m *é o elemento zero.* □

Demonstração:

Suponha que $m, p \in \mathbb{N}$ satisfazem esta condição. Então segue que

$$\begin{aligned} m + p &= p = p + m, \\ p + m &= m = m + p, \\ \therefore\ m &= p. \end{aligned}$$

Pelo Lema 6 sabemos que 0 satisfaz a condição desejada e, pelo argumento acima, sabemos que é o único número natural que o faz. ■

Definição 3 [Elemento Nulo]**:**

Devido à Proposição 7 diremos que 0 é o *elemento neutro aditivo*, ou *elemento nulo*, de $\mathbb{N}$. ♠

Definição 4 [Um]**:**

Chamaremos de *um*, e indicaremos por 1, o sucessor de 0, *i.e.*, $1 \equiv \sigma(0)$. ♠

Lema 8:

$\sigma(m) = 1 + m, \forall\, m \in \mathbb{N}$. □

Demonstração:

Seja $S := \{m \in \mathbb{N}; \sigma(m) = 1 + m\}$. Sabemos que $S \subseteq \mathbb{N}$ e que $0 \in S$, este último porque, pela Definição 2.i e pela Definição 4, $1 + 0 = 1 = \sigma(0)$. Além disso, se $n \in S$, então $\sigma(n) \in S$, pois

$$\begin{aligned} 1 + \sigma(n) &= \sigma(1 + n), && \text{(Definição 2.ii)} \\ &= \sigma(\sigma(n)). && \text{(por hipótese)} \end{aligned}$$

Assim, o Axioma 2.v implica que $S = \mathbb{N}$. ■

Proposição 9:

A adição de números naturais é comutativa, i.e.,

$$m + n = n + m, \forall\, m, n \in \mathbb{N}.$$ □

Demonstração:

Seja $S := \{n \in \mathbb{N}; m + n = n + m, \forall\, m \in \mathbb{N}\}$. É claro que $S \subseteq \mathbb{N}$ e sabemos que $0 \in S$, pois a Proposição 7 nos diz que $m + 0 = m = 0 + m, \forall\, m \in \mathbb{N}$.

Suponhamos que $n \in S$. Então $\sigma(n) \in S$, pois

$$\begin{aligned} m + \sigma(n) &= \sigma(m + n), && \text{(Definição 2.ii)} \\ &= \sigma(n + m), && \text{(por hipótese)} \\ &= 1 + (n + m), && \text{(Lema 8)} \\ &= (1 + n) + m, && \text{(Proposição 5)} \\ &= \sigma(n) + m. && \text{(Lema 8)} \end{aligned}$$

Teremos então, pelo Axioma 2.v, que $S = \mathbb{N}$. ■

Proposição 10:
A soma de números naturais admite a Lei do Cancelamento, i.e.,

$$m + p = n + p \Rightarrow m = n, \forall\, m, n, p \in \mathbb{N}.$$ □

Demonstração:
Seja o conjunto S definido por

$$S := \{p \in \mathbb{N}; m + p = n + p \Rightarrow m = n, \forall\, m, n \in \mathbb{N}\}.$$

Evidentemente $S \subseteq \mathbb{N}$. Note que $0 \in S$, pois, pela Definição 2.i, $a + 0 = b + 0 \Rightarrow a = b$.
Se $p \in S$, então $\sigma(p) \in S$, pois, se $m + \sigma(p) = n + \sigma(p)$,

$$\begin{aligned} m + \sigma(p) &= n + \sigma(p), \\ \sigma(m + p) &= \sigma(n + p), && \text{(Definição 2.ii)} \\ m + p &= n + p, && \text{(Axioma 2.iv)} \\ m &= n. && \text{(por hipótese)} \end{aligned}$$

Logo, pelo Axioma 2.v, $S = \mathbb{N}$. ■

Lema 11:
Sejam $m, n \in \mathbb{N}$. *Então* $m + n = 0 \Leftrightarrow m = n = 0$. □

Demonstração:
Da Definição 2.i decorre trivialmente que $0 + 0 = 0$, de forma que a volta está demonstrada.
Concentremo-nos, pois, na ida. Suponhamos, sem perda de generalidade, que $m \in \mathbb{N}^*$. Então, da Proposição 2, sabemos que $\exists\, p \in \mathbb{N}; \sigma(p) = m$. Note então que

$$\begin{aligned} 0 &= m + n, && \text{(por hipótese)} \\ &= \sigma(p) + n, && \text{(Proposição 2)} \\ &= n + \sigma(p), && \text{(Proposição 9)} \\ &= \sigma(n + p). && \text{(Definição 2.ii)} \end{aligned}$$

Logo, concluímos que existe um número natural do qual 0 é sucessor. Contudo, isso contradiz o Axioma 2.iii. Por absurdo, concluímos sem perda de generalidade que é impossível que $m \in \mathbb{N}^*$. Portanto, $m = n = 0$. ■

Lema 12:
Sejam $m, n \in \mathbb{N}$ *tais que* $m + n = 1$. *Então ou* $m = 1$ *e* $n = 0$ *ou* $m = 0$ *e* $n = 1$. □

Demonstração:
Sabemos que m e n não são ambos nulos pois, se o fossem, ter-se-ia que $m + n = 0 + 0 = 0$. Como $m + n = 1$, isso claramente é falso. Logo, pela Proposição 2, ao menos um deles é sucessor de um número natural, que chamaremos de p. Sem perda de generalidade, suponhamos m não-nulo e $\sigma(p) = m$.
Teremos então que $n + \sigma(p) = \sigma(0)$. Pela Definição 2 2.ii, vale que $\sigma(n + p) = \sigma(0)$. Pelo Axioma 2 2.iv, $n + p = 0$. Pelo Lema 11, $n = p = 0$. Logo, $m = \sigma(p) = 1$. Caso m seja nulo, tem-se a demostração análoga fazendo $n = \sigma(p)$. ■

Definição 5 [Multiplicação]**:**
Seja $m \in \mathbb{N}$ um número natural dado. Então definimos o *produto*, também chamado de *multiplicação* e denotado por $\cdot$, de m com outro número natural por

i. $m \cdot 0 = 0$;

ii. $m \cdot \sigma(n) = (m \cdot n) + m, \forall\, n \in \mathbb{N}$. ♠

Proposição 13:
Seja $m \in \mathbb{N}$ *um número natural dado. Então o produto* $m \cdot n$ *está bem-definido para todo número natural* n. □

Demonstração:
Seja $S := \{n \in \mathbb{N};\ m \cdot n \text{ está bem definido}\}$. É claro que $S \subseteq \mathbb{N}$. Da Definição 5.i sabemos que $0 \in S$.

Como a soma de números naturais é bem-definida (Proposição 4), a Definição 5.ii garante que, se $n \in S$, então $\sigma(n) \in S$. Teremos então, pelo Axioma 2.v, que $S = \mathbb{N}$. ■

Observação:
Como, para cada $m \in \mathbb{N}$, $m \cdot n$ está bem-definida para todo $n \in \mathrm{N}$, vê-se que $m \cdot n$ está bem definida $\forall\, m, n \in \mathbb{N}$. ♣

Lema 14:
$1 \cdot m = m, \forall\, m \in \mathbb{N}$. □

Demonstração:
Seja $S := \{m \in \mathbb{N}; 1 \cdot m = m\}$. É evidente que $S \subseteq \mathbb{N}$ e, pela Definição 5.i, $1 \cdot 0 = 0 \Rightarrow 0 \in S$. Suponha que $n \in S$. Então $\sigma(n) \in S$, pois

$$\begin{aligned} 1 \cdot \sigma(n) &= (1 \cdot n) + 1, && \text{(Definição 5.ii)} \\ &= n + 1, && \text{(por hipótese)} \\ &= 1 + n, && \text{(Proposição 9)} \\ &= \sigma(n). && \text{(Lema 8)} \end{aligned}$$

Logo, do Axioma 2.v resulta que $S = \mathbb{N}$. ■

Proposição 15:
$\exists!\, m \in \mathbb{N}; m \cdot n = n = n \cdot m, \forall\, n \in \mathbb{N}$. *Além disso, este único* m *é o elemento* 1. □

Demonstração:
Suponha que $m, p \in \mathbb{N}$ satisfazem esta condição. Então segue que

$$\begin{aligned} & m \cdot p = p = p \cdot m, \\ & p \cdot m = m = m \cdot p, \\ \therefore\ & p = m. \end{aligned}$$

Sabemos, do Lema 14, que $1 \cdot m = m, \forall\, m \in \mathbb{N}$. Além disso, vale que $m \cdot 1 = m$, pois

$$\begin{aligned} m \cdot 1 &= m \cdot \sigma(0), && \text{(Definição 4)} \\ &= (m \cdot 0) + m, && \text{(Definição 5.ii)} \\ &= 0 + m, && \text{(Definição 5.i)} \\ &= m. && \text{(Proposição 7)} \end{aligned}$$

Logo, 1 é o único número natural que satisfaz a condição desejada, concluindo a demonstração. ■

Definição 6 [Identidade]:
Devido à Proposição 15 diremos que 1 é o *elemento neutro multiplicativo*, ou *identidade*, de $\mathbb{N}$. ♠

Proposição 16:
O produto de números naturais se distribui sobre a soma de números naturais, i.e.,

$$m \cdot (n + p) = (m \cdot n) + (m \cdot p), \forall\, m, n, p \in \mathbb{N} \qquad \square$$

Demonstração:
Seja $S := \{p \in \mathbb{N}; m \cdot (n + p) = (m \cdot n) + (m \cdot p), \forall\, m, n \in \mathbb{N}\}$. É evidente que $S \subseteq \mathbb{N}$. Queremos provar que $S = \mathbb{N}$.
Podemos constatar facilmente que $0 \in S$, pois

$$\begin{aligned} m \cdot (n + 0) &= m \cdot n, && \text{(Proposição 7)} \\ &= (m \cdot n) + 0, && \text{(Proposição 7)} \\ &= (m \cdot n) + (m \cdot 0). && \text{(Definição 5.i)} \end{aligned}$$

Suponhamos agora que $p \in S$. Então $\sigma(p) \in S$. Afinal,

$$\begin{aligned} m \cdot (n + \sigma(p)) &= m \cdot \sigma(n + p), && \text{(Definição 2.ii)} \\ &= (m \cdot (n + p)) + m, && \text{(Definição 5.ii)} \\ &= ((m \cdot n) + (m \cdot p)) + m, && \text{(por hipótese)} \\ &= (m \cdot n) + (m \cdot p) + m, && \text{(Proposição 5)} \\ &= (m \cdot n) + (m \cdot \sigma(p)). && \text{(Definição 5.ii)} \end{aligned}$$

Logo, pelo Axioma 2.v, vale que $S = \mathbb{N}$. ■

Proposição 17:
A multiplicação de números naturais é associativa, i.e.,

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p, \forall\, m, n, p \in \mathbb{N}. \qquad \square$$

Demonstração:
Seja $S := \{p \in \mathbb{N}; m \cdot (n \cdot p) = (m \cdot n) \cdot p, \forall\, m, n \in \mathbb{N}\}$. Sabemos que $S \subseteq \mathbb{N}$ e queremos provar que $S = \mathbb{N}$.
Vale que $0 \in S$, pois

$$\begin{aligned} m \cdot (n \cdot 0) &= m \cdot 0, && \text{(Definição 5.i)} \\ &= 0, && \text{(Definição 5.i)} \\ &= (m \cdot n) \cdot 0. && \text{(Definição 5.i)} \end{aligned}$$

Suponhamos que $p \in S$. Então $\sigma(p) \in S$, pois

$$\begin{aligned} m \cdot (n \cdot \sigma(p)) &= m \cdot ((n \cdot p) + n)\,, && \text{(Definição 5.ii)} \\ &= (m \cdot (n \cdot p)) + (m \cdot n), && \text{(Proposição 16)} \\ &= ((m \cdot n) \cdot p) + (m \cdot n), && \text{(por hipótese)} \\ &= (m \cdot n) \cdot \sigma(p). && \text{(Definição 5.ii)} \end{aligned}$$

Usando o Axioma 2.v, concluímos que $S = \mathbb{N}$. ■

Lema 18:
$m \cdot 0 = 0 \cdot m = 0, \forall\, m \in \mathbb{N}$. □

Demonstração:
Pela Definição 5.i sabemos que $m \cdot 0 = 0, \forall\, m \in \mathbb{N}$. Resta apenas provarmos que $0 \cdot m = o, \forall\, m \in \mathbb{N}$.

Tome $S := \{m \in \mathbb{N}; 0 \cdot m = 0\}$. É claro que $S \subseteq \mathbb{N}$. Queremos provar que $S = \mathbb{N}$.

Sabemos que $0 \in S$, pois, pela Definição 5.i vale que $0 \cdot 0 = 0$. Vale que $m \in S \Rightarrow \sigma(m) \in S$, pois

$$\begin{aligned} 0 \cdot \sigma(m) &= 0 \cdot m + 0, && \text{(Definição 5.i)} \\ 0 \cdot \sigma(m) &= 0 \cdot m, && \text{(Definição 2.i)} \\ 0 \cdot \sigma(m) &= 0. && \text{(por hipótese)} \end{aligned}$$

Logo, pelo Axioma 2.v vale que $S = \mathbb{N}$, nos levando à conclusão de que $0 \cdot m = 0, \forall\, m \in \mathbb{N}$.

Assim, concluímos que, de fato, $m \cdot 0 = 0 \cdot m = 0, \forall\, m \in \mathbb{N}$. ■

Lema 19:

$(m + n) \cdot p = (m \cdot p) + (n \cdot p), \forall\, m, n, p \in \mathbb{N}$. □

Demonstração:

Seja $S := \{p \in \mathbb{N}; (m + n) \cdot p = (m \cdot p) + (n \cdot p), \forall\, m, n \in \mathbb{N}\}$. É claro que $S \subseteq \mathbb{N}$. Queremos provar que $S = \mathbb{N}$.

$0 \in S$, pois

$$\begin{aligned} (m + n) \cdot 0 &= 0, && \text{(Definição 5.i)} \\ &= m \cdot 0, && \text{(Definição 5.i)} \\ &= (m \cdot 0) + 0, && \text{(Definição 2.i)} \\ &= (m \cdot 0) + (n \cdot 0). && \text{(Definição 5.i)} \end{aligned}$$

$p \in S \Rightarrow \sigma(p) \in S$, pois

$$\begin{aligned} (m + n) \cdot \sigma(p) &= ((m + n) \cdot p) + (m + n), && \text{(Definição 5.ii)} \\ &= (m \cdot p) + (n \cdot p) + (m + n), && \text{(por hipótese)} \\ &= (m \cdot p) + (n \cdot p) + m + n, && \text{(Proposição 5)} \\ &= (m \cdot p) + m + (n \cdot p) + n, && \text{(Proposição 9)} \\ &= (m \cdot \sigma(p)) + (n \cdot \sigma(p)). && \text{(Definição 5.ii)} \end{aligned}$$

Pelo Axioma 2.v, $S = \mathbb{N}$. ■

Proposição 20:

A multiplicação de números naturais é comutativa, i.e.,

$$m \cdot n = n \cdot m, \forall\, m, n \in \mathbb{N}.$$ □

Demonstração:

Seja $S := \{n \in \mathbb{N}; m \cdot n = n \cdot m, \forall\, m \in \mathbb{N}\}$. Sabemos que $S \subseteq \mathbb{N}$ e queremos provar que $S = \mathbb{N}$. Pelo Lema 18 sabemos que $0 \in S$.

Se supormos que $n \in S$, então $\sigma(n) \in S$, pois

$$\begin{aligned} m \cdot \sigma(n) &= (m \cdot n) + m, && \text{(Definição 5.ii)} \\ &= m + (m \cdot n), && \text{(Proposição 9)} \\ &= m + (n \cdot m), && \text{(por hipótese)} \\ &= (1 \cdot m) + (n \cdot m), && \text{(Proposição 15)} \\ &= (1 + n) \cdot m, && \text{(Lema 19)} \\ &= \sigma(n) \cdot m. && \text{(Lema 8)} \end{aligned}$$

Concluímos então, por meio do Axioma 2.v, que $S = \mathbb{N}$, encerrando assim a demonstração. ■

Teorema 21:

Sejam $m, n \in \mathbb{N}$. *Então uma, e somente uma, das alternativas seguintes é verdadeira:*

i. $m = n$;

ii. $\exists\, p \in \mathbb{N}^*; m + p = n$;

iii. $\exists\, q \in \mathbb{N}^*; m = n + q$. □

Demonstração:

Primeiramente, notemos que as condições são mutuamente exclusivas, *i.e.*, não é possível que duas sejam satisfeitas simultaneamente.

i $\Rightarrow \neg$ ii: Fixe $m, n \in \mathbb{N}$ tais que $m = n$, *i.e.*, vale i. Seja $p \in \mathbb{N}; m + p = n$. Então $p = 0$, pois, como $m = n = m + p$,

$$\begin{aligned} m &= p + m, \\ 0 + m &= p + m, \\ 0 &= p. && \text{(Proposição 10)} \end{aligned}$$

Logo, p não pode estar em $\mathbb{N}^*$, o que implica que ii é falsa.

ii $\Rightarrow \neg$ iii: Sejam $m, n, p \in \mathbb{N}, p \neq 0$, tais que $m + p = n$, *i.e.*, vale ii. Suponhamos, por absurdo, que exista $q \in \mathbb{N}$ tal que $m = n + q$. Então é claro que $m = m + p + q$ e seguirá que

$$\begin{aligned} m &= p + q + m, \\ 0 + m &= p + q + m, \\ 0 &= p + q. && \text{(Proposição 10)} \end{aligned}$$

Pelo Lema 11, sabemos que isso implica que $p = q = 0$, contradizendo a hipótese inicial de que $p \neq 0$. Logo, chegamos a um absurdo, forçando-nos a concluir que não existe tal q.

Por argumentação análoga à feita para demonstrar que i $\Rightarrow \neg$ ii pode-se concluir que i $\Rightarrow \neg$ iii. Tomando as contrapositivas das afirmações demonstradas previamente vemos que ii $\Rightarrow \neg$ i, iii $\Rightarrow \neg$ i e iii $\Rightarrow \neg$ ii. Logo, as afirmações são mutuamente exclusivas.

Tome $m \in \mathbb{N}$. Definimos o conjunto S_m por

$$S_m := \{n \in \mathbb{N}; (m = n) \vee (m + p = n) \vee (m = n + q), p, q \in \mathbb{N}^*\}.$$

É evidente que, para cada $m \in \mathbb{N}$, $S_m \subseteq \mathbb{N}$. Também é válido que $0 \in S_m$, pois, se $m = 0$, a primeira condição é satisfeita. Se $m \neq 0$, então $m = 0 + m$, satisfazendo a terceira condição com $q = m$.

Suponha agora que, para um dado $m \in \mathbb{N}$, $n \in S_m$. Então $\sigma(n) \in S_m$, pois:

i. Se $m = n$, então $m + 1 = n + 1$ e, pelo Lema 8, $m + 1 = \sigma(n)$. Logo, $\sigma(n)$ satisfaz a segunda condição, de forma que, de fato, $\sigma(n) \in S_m$.

ii. Se $m + p = n$, para algum $p \in \mathbb{N}^*$, então $m + p + 1 = n + 1$ e, pelo Lema 8, $m + p + 1 = \sigma(n)$. Novamente concluímos que $\sigma(n)$ satisfaz a segunda condição e, portanto, $\sigma(n) \in S_m$.

iii. Se $m = n + q$, para algum $q \in \mathbb{N}^*$, a Proposição 2 nos informa que $\exists\, p \in \mathbb{N}; \sigma(p) = q$. Logo, teremos que

$$\begin{aligned} m &= n + \sigma(p), \\ &= \sigma(n + p), \\ &= \sigma(p + n), \\ &= p + \sigma(n), \\ &= \sigma(n) + p. \end{aligned}$$

Se $q = 1$, então $p = 0$ e, portanto, $m = \sigma(n)$, satisfazendo a primeira condição. Se $q \neq 1$, então $p \in \mathbb{N}^*$ e tem-se satisfeita a terceira condição. Logo, $\sigma(n) \in S_m$.

Logo, pelo Axioma 2.v, vale que $S_m = \mathbb{N}, \forall\, m \in \mathbb{N}$, garantindo que, dados dois números naturais quaisquer, uma das três condições listadas é satisfeita. Juntando isto ao provado no início da demonstração, teremos que somente uma delas pode ser satisfeita, *quod erat demonstrandum*. ■

Observação:

Na demonstração do Teorema 21 utilizamos, de forma implícita, a Definição 2, a Definição 4, a Proposição 5, a Proposição 7 e a Proposição 9. De agora em diante faremos isso com mais frequência, pressupondo os passos que as envolvem como evidentes. O mesmo será feito com relação ao uso da Definição 5, da Proposição 15, da Proposição 16, da Proposição 17 e da Proposição 20. ♣

Notação:

Doravante deixaremos, a depender da conveniência, o sinal $\cdot$, que denota o produto de naturais, subentendido. Por exemplo, dados dois números naturais m e n, denotaremos seu produto por $mn \equiv m \cdot n$. Além disso, sempre entenderemos a presença dos parênteses ao utilizar qualquer uma das notações, *e.g.*

$$mn + pq \equiv m \cdot n + p \cdot q \equiv (m \cdot n) + (p \cdot q).$$ ♣

Corolário 22:

Sejam $m, n \in \mathbb{N}$. *Então ao menos uma das alternativas seguintes é verdadeira:*

i. $\exists\, p \in \mathbb{N}; m + p = n$;

ii. $\exists\, q \in \mathbb{N}; m = n + q$.

Além disso, as duas alternativas serão satisfeitas se, e somente se, $p = q = 0$. □

Demonstração:

Do Teorema 21 sabemos que, $\forall\, m, n \in \mathbb{N}$, é satisfeita uma, e somente uma, das seguintes:

T.i $m = n$;

T.ii $\exists\, p \in \mathbb{N}^*; m + p = n$;

T.iii $\exists\, q \in \mathbb{N}^*; m = n + q$.

É trivial constatar que, se T.ii valer, i será satisfeita. Se T.iii valer, ii será satisfeita. Se T.i valer, i e ii serão satisfeitas.

Suponha que i e ii são satisfeitas. Então vale que

$$\begin{aligned} m &= m + p + q, \\ 0 + m &= p + q + m, \\ 0 &= p + q. && \text{(Proposição 10)} \end{aligned}$$

Pelo Lema 11, vale que $p = q = 0$, concluindo a demonstração. ■

§2: Ordenando os Naturais

Definição 7 [Relação Binária]**:**

Sejam A e B conjuntos e seja o seu produto cartesiano $A \times B$. Diremos que um subconjuntos $R \subseteq A \times B$ é uma *relação binária*, ou simplesmente uma *relação*, entre A e B. ♠

Definição 8 [Relação Inversa]**:**

Sejam A e B conjuntos e R uma relação entre A e B. Definimos a *relação inversa* de R, R^{-1}, por

$$R^{-1} := \{(b,a) \in B \times A; (a,b) \in R\}. \quad \spadesuit$$

Definição 9 [Ordem Parcial Ampla]**:**

Seja A um conjunto e $R \subseteq A \times A$ uma relação binária em A. Diremos que R é uma *relação de ordem parcial ampla* em A se satisfizer as seguintes condições:

i. $\forall x \in A, (x,x) \in R$, *i.e.*, todo elemento de A está relacionado consigo mesmo (reflexividade);

ii. $\forall x,y \in A, ((x,y) \in R \wedge (y,x) \in R) \Rightarrow x = y$ (antissimetria);

iii. $\forall x,y,z \in A, ((x,y) \in R \wedge (y,z) \in R) \Rightarrow (x,z) \in R$ (transitividade). $\spadesuit$

Proposição 23:

Seja A um conjunto e R uma relação de ordem parcial ampla em A. Então R^{-1} também o é. $\square$

Demonstração:

$\forall x \in A, (x,x) \in R \Rightarrow (x,x) \in R^{-1}$. Logo, vale a propriedade reflexiva. Também vale a propriedade antissimétrica. De fato,

$$\begin{aligned}\left((y,x) \in R^{-1} \wedge (x,y) \in R^{-1}\right) &\Rightarrow ((x,y) \in R \wedge (y,x) \in R), \\ &\Rightarrow x = y.\end{aligned}$$

Finalmente, verifica-se a validade da propriedade transitiva, pois

$$\begin{aligned}\left((z,y) \in R^{-1} \wedge (y,x) \in R^{-1}\right) &\Rightarrow ((y,z) \in R \wedge (x,y) \in R), \\ &\Rightarrow ((x,y) \in R \wedge (y,z) \in R), \\ &\Rightarrow (x,z) \in R, \\ &\Rightarrow (z,x) \in R^{-1}.\end{aligned} \quad \blacksquare$$

Notação:

Seja A um conjunto e R uma relação de ordem parcial ampla em A.

$$x, y \in A; (x,y) \in R \Rrightarrow x \preccurlyeq y \vee y \succcurlyeq x.$$

Diremos que $\preccurlyeq$ é uma relação de ordem parcial ampla em A e que $\succcurlyeq$ é a sua relação inversa. $\clubsuit$

Observação:

Com o uso da notação $\preccurlyeq$, pode-se escrever a definição de ordem parcial ampla de outra maneira. $\clubsuit$

Definição:

Seja A um conjunto e $\preccurlyeq$ uma relação binária em A. Diremos que $\preccurlyeq$ é uma relação de ordem parcial ampla em A se satisfizer as seguintes condições:

i. $\forall x \in A, x \preccurlyeq x$, *i.e.*, todo elemento de A está relacionado consigo mesmo (reflexividade);

ii. $\forall x,y \in A, (x \preccurlyeq y \wedge y \preccurlyeq x) \Rightarrow x = y$ (antissimetria);

iii. $\forall x,y,z \in A, (x \preccurlyeq y \wedge y \preccurlyeq z) \Rightarrow x \preccurlyeq z$ (transitividade). $\spadesuit$

Definição 10 [Menor ou Igual]**:**

Sejam $m, n \in \mathbb{N}$. Diremos que m é *menor ou igual* a n, e escreveremos $m \leqslant n$, se existir $p \in \mathbb{N}$ tal que $m + p = n$. Se $m \leqslant n$, também dizemos que n é *maior ou igual* a m e escrevemos $n \geqslant m$, onde $\geqslant$ denota a relação inversa de $\leqslant$. ♠

Proposição 24:

A relação menor ou igual é uma relação de ordem parcial ampla. □

Demonstração:

Seja $n \in \mathbb{N}$. Como $n + 0 = n$ e, pelo Axioma 2.i, $0 \in \mathbb{N}$, vemos que $n \leqslant n, \forall\, n \in \mathbb{N}$. Logo, $\leqslant$ é reflexiva.

Sejam, agora, $m, n, \in \mathbb{N}$ tais que $m \leqslant n$ e $n \leqslant m$. Então, pela Definição 10, $\exists\, p, q \in \mathbb{N}$;

$$\begin{aligned} p + m &= n, \\ m &= n + q. \end{aligned}$$

Pelo Corolário 22, as duas condições são satisfeitas se, e somente se, $p = q = 0$. Logo, $m = n$ e vê-se que $\leqslant$ é antissimétrica.

Por fim, sejam $m, n, p \in \mathbb{N}$ tais que $m \leqslant n$ e $n \leqslant p$. Então sabemos, pela Definição 10, que $\exists\, q, r \in \mathbb{N}$;

$$\begin{aligned} m + r &= n, \\ n + q &= p. \end{aligned}$$

Logo, constata-se que $m + r + q = p$. Pela Definição 2, sabemos que $r + q \in \mathbb{N}$. Como $m + (r + q) = p$, a Definição 10 implica imediatamente que $m \leqslant p$, confirmando que $\leqslant$ é transitiva. ■

Definição 11 [Ordem Parcial Estrita]**:**

Seja A um conjunto e $R \subseteq A \times A$ uma relação binária em A. Diremos que R é uma *relação de ordem parcial estrita* em A se satisfizer as seguintes condições:

i. $\forall\, x \in A, (x, x) \notin R$, *i.e.*, nenhum elemento de A está relacionado consigo mesmo (irreflexividade);

ii. $\forall\, x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$ (transitividade). ♠

Proposição 25:

Seja A um conjunto e R uma relação de ordem parcial estrita em A. Então R^{-1} também o é. □

Demonstração:

$\forall\, x \in A, (x, x) \notin R \Rightarrow (x, x) \notin R^{-1}$. Logo, vale a propriedade irreflexiva.

Verifica-se também a validade da propriedade transitiva, pois, tal como feito na demonstração da Proposição 23,

$$\begin{aligned} \left((z, y) \in R^{-1} \wedge (y, x) \in R^{-1}\right) &\Rightarrow ((y, z) \in R \wedge (x, y) \in R)\,, \\ &\Rightarrow ((x, y) \in R \wedge (y, z) \in R)\,, \\ &\Rightarrow (x, z) \in R, \\ &\Rightarrow (z, x) \in R^{-1}. \end{aligned}$$ ■

Notação:

Seja A um conjunto e R uma relação de ordem parcial estrita em A.

$$x, y \in A; (x, y) \in R \Rrightarrow x \prec y \vee y \succ x.$$

Diremos que $\prec$ é uma relação de ordem parcial estrita em A e que $\succ$ é a sua relação inversa. ♣

Observação:

Com o uso da notação $\prec$, pode-se escrever a definição de ordem parcial estrita de outra maneira, tal como feito para a ordem parcial ampla. ♣

Definição:

Seja A um conjunto e $\prec$ uma relação binária em A. Diremos que $\prec$ é uma relação de ordem parcial ampla em A se satisfizer as seguintes condições:

i. $\forall\, x \in A, x \not\prec x$, *i.e.*, nenhum elemento de A está relacionado consigo mesmo (irreflexividade);

ii. $\forall\, x, y, z \in A, (x \prec y \wedge y \prec z) \Rightarrow x \prec z$ (transitividade). ♠

Proposição 26:

Seja A *um conjunto e* $\prec$ *uma relação de ordem parcial estrita em* A. *Então* $\prec$ *é assimétrica,* i.e., *satisfaz a seguinte propriedade:*

$$\forall\, x, y \in A, x \prec y \Rightarrow y \not\prec x.$$ □

Demonstração:

Suponha, por absurdo, que existam $x, y \in A; x \prec y$ e $y \prec x$. Então, pela transitividade da ordem parcial estrita (Definição 11.ii), sabemos que

$$x \prec y \wedge y \prec x \Rightarrow x \prec x.$$

Contudo, isso contradiz a propriedade irreflexiva da ordem parcial estrita (Definição 11.i). Atingimos um absurdo. Percebemos então que não é possível que $x \prec y$ e $y \prec x$ ao mesmo tempo, *i.e.*, $x \prec y \Rightarrow y \not\prec x$. ■

Proposição 27:

Seja A *um conjunto. Se* $\preccurlyeq$ *é uma relação de ordem parcial ampla em* A, *então a relação* $\prec$, *definida por*

$$(x \prec y) \Leftrightarrow (x \preccurlyeq y \wedge x \neq y), \forall\, x, y \in A,$$

é uma relação de ordem parcial estrita em A.

Analogamente, se $\prec$ *é uma relação de ordem parcial estrita em* A, *a relação* $\preccurlyeq$ *definida por*

$$(x \preccurlyeq y) \Leftrightarrow (x \prec y \vee x \neq y), \forall\, x, y \in A,$$

é uma relação de ordem parcial ampla em A. □

Demonstração:

Para ambos os casos a propriedade transitiva decorre trivialmente da Definição 9.iii ou da Definição 11.ii.

Seja $\preccurlyeq$ uma relação de ordem parcial ampla. Então a relação $\prec$ definida acima é uma relação de ordem parcial estrita, pois, além de ser transitiva pelo argumento recém fornecido, é irreflexiva:

$$\begin{aligned} x = y &\Rightarrow \neg\left(x \preccurlyeq y \wedge x \neq y\right), \\ &\Rightarrow \neg(x \prec y), \forall\, x, y \in A. \end{aligned}$$

Seja $\prec$ uma relação de ordem parcial estrita. Então a relação $\preccurlyeq$ definida acima é uma relação de ordem parcial ampla, pois, além de ser transitiva pelo argumento fornecido no início desta demonstração, é reflexiva, pois

$$\begin{aligned} x = y &\Rightarrow (x \prec y \vee x = y), \\ &\Rightarrow x \preccurlyeq y, \forall\, x, y \in A. \end{aligned}$$

A antissimetria vem de que

$$(x \preccurlyeq y \wedge y \preccurlyeq x) \Rightarrow [(x \prec y \vee x = y) \wedge (y \prec x \vee x = y)]\,.$$

Supondo, por absurdo, que $x \neq y$, teremos que

$$(x \preccurlyeq y \wedge y \preccurlyeq x) \Leftrightarrow (x \prec y \wedge y \prec x)\,.$$

Como o termo à direita é sempre falso (pela Definição 11.i), atingimos um absurdo. Logo, é preciso que $x = y$, implicando que $\preccurlyeq$ é, de fato, antissimétrica. ■

Definição 12 [Ordem Correspondente]**:**
Seja A um conjunto com uma relação de ordem parcial ampla ou estrita. Definimos a *ordem correspondente* à primeira segundo

i. se $\preccurlyeq$ é uma relação de ordem parcial ampla sobre A, sua ordem correspondente $\prec$ é definida por $x \prec y \Leftrightarrow (x \preccurlyeq y \wedge x \neq y), \forall x, y \in A$;

ii. se $\prec$ é uma relação de ordem parcial estrita sobre A, sua ordem correspondente $\preccurlyeq$ é definida por $x \preccurlyeq y \Leftrightarrow (x \prec y \vee x = y), \forall x, y \in A$. ♠

Definição 13 [Estritamente Menor]**:**
Sejam $m, n \in \mathbb{N}$. Diremos que m é *menor* (ou *estritamente menor*) que n, e escreveremos $m < n$, se valerem simultaneamente as seguintes condições:

i. $m \leqslant n$;

ii. $m \neq n$.

Se $m < n$, também dizemos que n é *maior* (ou *estritamente maior*) que m e escrevemos $n > m$, onde $>$ denota a relação inversa de $<$. ♠

Observação:
Pela Proposição 27, a relação $<$ é uma relação de ordem parcial estrita em $\mathbb{N}$, pois é a ordem correspondente de $\leqslant$. ♣

Proposição 28:
Sejam $m, n \in \mathbb{N}$. *Então vale que*

$$m < n \Leftrightarrow \exists\, p \in \mathbb{N}^*; m + p = n.$$ □

Demonstração:
Pela Definição 13 e pela Definição 10, $m < n$ se, e somente se, $\exists\, p \in \mathbb{N}; m + p = n$ e $m \neq n$. No entanto, pelo Teorema 21, uma, e apenas uma, das seguintes alternativas é verdadeira:

T.i $m = n$;

T.ii $\exists\, p \in \mathbb{N}^*; m + p = n$;

T.iii $\exists\, q \in \mathbb{N}^*; m = n + q$.

É evidente que as condições T.i e T.iii não são satisfeitas. Logo, T.ii é verdadeira.
A volta é simples: se existir $p \in \mathbb{N}^*; m + p = n$, é claro que $\exists\, p \in \mathbb{N}; m + p = n$ e $m \neq n$ (devido à Proposição 7). Logo, ter-se-á que $m < n$. ■

Lema 29:
Seja $m \in \mathbb{N}$. *Vale que* $m < \sigma(m)$. □

Demonstração:
Vale, pelo Lema 8, que $m + 1 = \sigma(m)$. Logo, pela Proposição 28, $n < \sigma(n)$. ■

Definição 14 [Incomparabilidade]**:**
Seja A um conjunto e R uma relação sobre A. Dizemos que dois elementos $x, y \in A, x \neq y$, são *incomparáveis* por R, e escrevemos $x \parallel y$, se, e somente se, $(x, y), (y, x) \notin R$. Se dois elementos não são incomparáveis por R, dizemos que são *comparáveis* por R e escrevemos $x \nparallel y$. ♠

Definição 15 [Relação de Ordem Total]**:**
Seja A um conjunto e R uma relação de ordem parcial, estrita ou ampla, sobre A. Diremos que R é uma *relação de ordem total* (ampla ou estrita) sobre A se todos os elementos de A foram comparáveis por R. De forma mais específica,

i. se A é um conjunto e $\preccurlyeq$ é uma relação de ordem parcial ampla sobre A, diremos que $\preccurlyeq$ é uma *relação de ordem total ampla* sobre A se, e somente se, valer a dicotomia:

$$\forall x, y \in A, (x \preccurlyeq y \vee y \preccurlyeq x);$$

ii. se A é um conjunto e $\prec$ é uma relação de ordem parcial estrita sobre A, diremos que $\prec$ é uma *relação de ordem total estrita* sobre A se, e somente se, valer a tricotomia:

$$\forall x, y \in A, (x = y \vee x \prec y \vee y \prec x).$$ ♠

Proposição 30:
Sejam $\prec$ e $\preccurlyeq$ relações de ordem parcial estrita e ampla, respectivamente, sobre um mesmo conjunto A. $\prec$ é a ordem correspondente a $\preccurlyeq$ se, e somente se, $\preccurlyeq$ for a ordem correspondente a $\prec$, i.e., $\forall x, y \in A$,

$$[x \prec y \Leftrightarrow (x \preccurlyeq y \wedge x \neq y)] \Leftrightarrow [x \preccurlyeq y \Leftrightarrow (x \prec y \vee x = y)].$$ □

Demonstração:
$\Rightarrow$: supomos $x \prec y \Leftrightarrow (x \preccurlyeq y \wedge x \neq y)$. Então segue que

$$\begin{aligned}
[x \prec y \vee x = y] &\Leftrightarrow [(x \preccurlyeq y \wedge x \neq y) \vee x = y], && \text{(por hipótese)}\\
&\Leftrightarrow [(x \preccurlyeq y \vee x = y) \wedge (x \neq y \vee x = y)],\\
&\Leftrightarrow [x \preccurlyeq y \vee x = y],\\
&\Leftrightarrow x \preccurlyeq y. && \text{(Definição 9.i)}
\end{aligned}$$

$\Leftarrow$: supomos $x \preccurlyeq y \Leftrightarrow (x \prec y \vee x = y)$. Então segue que

$$\begin{aligned}
[x \preccurlyeq y \wedge x \neq y] &\Leftrightarrow [(x \prec y \vee x = y) \wedge x \neq y], && \text{(por hipótese)}\\
&\Leftrightarrow [(x \prec y \wedge x \neq y) \vee (x = y \wedge x \neq y)],\\
&\Leftrightarrow [x \prec y \wedge x \neq y].
\end{aligned}$$

Contudo, pela Definição 11.i, sabemos que $x = y \Rightarrow x \nprec y$. Logo, tomando a contrapositiva desta afirmação, teremos que $x \prec y \Rightarrow x \neq y$. Assim concluímos que, de fato,

$$[x \preccurlyeq y \wedge x \neq y] \Leftrightarrow x \prec y.$$ ■

Proposição 31:
Seja A um conjunto. Seja $\preccurlyeq$ uma relação de ordem parcial ampla em A e seja $\prec$ sua ordem correspondente. Então $\preccurlyeq$ será uma ordem total se, e somente se, $\prec$ também o for. □

Demonstração:

$$\begin{aligned}\forall x, y \in A, [x \preccurlyeq y \vee y \preccurlyeq x] &\Leftrightarrow \forall x, y \in A, [(x \prec y \vee x = y) \vee (y \prec x \vee x = y)]\,, \\ &\Leftrightarrow \forall x, y \in A, [x = y \vee x \prec y \vee y \prec x]\,.\end{aligned}$$ ■

Proposição 32:
As relações de ordem definidas em $\mathbb{N}$, $\leqslant$ *e* $<$, *são totais.* □

Demonstração:
O Corolário 22 implica diretamente que, $\forall\, m, n \in \mathbb{N}, m \leqslant n$ ou $n \leqslant m$. Logo, $\leqslant$ é uma relação de ordem total. Pela Proposição 31, $<$ também é total. ■

Proposição 33:
Sejam $m, n, p \in \mathbb{N}$. *Então valem:*

i. $m \leqslant n \Leftrightarrow m + p \leqslant n + p$;

ii. $m \leqslant n \Rightarrow mp \leqslant np$. □

Demonstração:
Se $m \leqslant n$, então $\exists\, q \in \mathbb{N}; m + q = n$. Segue que

$$\begin{aligned} m + q &= n, \\ m + q + p &= n + p, \\ (m + p) + q &= n + p. \end{aligned}$$

Logo, $m + p \leqslant n + p$. A volta vem da inversão dos passos, permitida pela Proposição 10.
Além disso, vemos também que

$$\begin{aligned} m + q &= n, \\ (m + q)p &= np, \\ mp + qp &= np. \qquad \text{(Lema 19)} \end{aligned}$$

Portanto, $mp \leqslant np$. Isso conclui a demonstração. ■

Corolário 34:
Sejam $m, n, p, q \in \mathbb{N}, q \neq 0$. *Então valem:*

i. $m < n \Leftrightarrow m + p < n + p$;

ii. $m < n \Rightarrow mq < nq$. □

Demonstração:
Análoga à da Proposição 33. ■

Observação:
Note que, na demonstração da Proposição 33.ii, se $p = 0$ ter-se-á um problema para o caso de uma ordem estrita: $(m + q) \cdot 0 = n \cdot 0 \Rightarrow m \cdot 0 + 0 = n \cdot 0$. Pela Proposição 28, isso implica que $m \cdot 0 \not< n \cdot 0$. Logo, ao estender a Proposição 33.ii para a relação $<$ foi preciso exigir que $p \in \mathbb{N}^*$. ♣

Corolário 35:
Sejam $m, n, p \in \mathbb{N}$. *Então* $m < n \Rightarrow m < n + p$. □

Demonstração:
Análoga à da Proposição 33. ■

Proposição 36:
O produto de números naturais admite a Lei do Cancelamento, i.e.,

$$m \cdot p = n \cdot p \Rightarrow m = n, \forall\, m, n \in \mathbb{N}, p \in \mathbb{N}^*. \qquad \square$$

Demonstração:
Pela Proposição 32, $m = n$ ou $m < n$ ou $m > n$. Se $m > n$, sabemos, pelo Corolário 34.ii, que $mp > np$, o que contradiz a hipótese. Se $m < n$, então o mesmo Corolário fornece que $mp < np$. Logo, resulta da Proposição 32 que $m = n$. ■

Corolário 37:
Sejam $m, n, p \in \mathbb{N}, p \neq 0$. *Então vale que* $m \leqslant n \Leftrightarrow mp \leqslant np$. □

Demonstração:

$$\begin{aligned} mp + qp &= np, && \\ (m+q)p &= np, && \text{(Lema 19)} \\ m + q &= n. && \text{(Proposição 36)} \end{aligned}$$

A ida foi provada na Proposição 33. ■

Corolário 38:
Sejam $m, n, p \in \mathbb{N}, p \neq 0$. *Então vale que* $m < n \Leftrightarrow mp < np$. □

Demonstração:
Análoga à do Corolário 37. ■

Lema 39:
Sejam $m \in \mathbb{N}$ *e* $n \in \mathbb{N}; m \leqslant n \leqslant \sigma(m)$. *Então* $n = m$ *ou* $n = \sigma(m)$. □

Demonstração:
Primeiramente notemos que, devido ao Lema 29, faz sentido escrever $m \leqslant n \leqslant \sigma(m)$ pois, $\forall\, m \in \mathbb{N}$, $m \leqslant \sigma(m)$.

Dito isso, suponha, por absurdo, que exista n nessas condições. Então, pela Definição 10 existem $p, q \in \mathbb{N}$ tais que

$$\begin{aligned} m + p &= n, \\ n + q &= \sigma(m). \end{aligned}$$

Segue que $m+p+q = \sigma(m)$. Pelo Lema 8 e pela Proposição 10 vale que $p+q = 1$. Pelo Lema 12, $p = 1$ e $q = 0$ ou $p = 0$ e $q = 1$.

Se $p = 1$ e $q = 0$, $n = \sigma(m)$. Se $p = 0$ e $q = 1$, $n = m$. ■

Definição 16 [Mínimo e Máximo]**:**
Seja A um conjunto e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que um elemento $x \in A$ é um *mínimo* ou *primeiro elemento* de A se, e somente se, $x \preccurlyeq y, \forall\, y \in A$. Analogamente, diremos que um elemento $z \in A$ é um *máximo* ou *último elemento* de A se, e somente se, $y \preccurlyeq z, \forall\, y \in A$. ♠

Proposição 40:
Seja A *um conjunto,* $\preccurlyeq$ *uma relação de ordem parcial ampla sobre* A *e* x *um mínimo (máximo) de* A. *Então* x *é o único mínimo (máximo) de* A. □

Demonstração:
Suponha que $x, y \in A$ sejam mínimos (máximos) de A. Então vale que $x \preccurlyeq y$ e $y \preccurlyeq x$. Como $\preccurlyeq$ é uma relação de ordem parcial ampla, a Definição 9.i implica que $x = y$. ■

Notação:

Seja A um conjunto e $\preccurlyeq$ uma relação de ordem parcial ampla em A. Se existir elemento mínimo em A, denotá-lo-emos por $\min A$. Se existir elemento máximo em A, denotá-lo-emos por $\max A$. ♣

Lema 41:

Considere $\mathbb{N}$ *com a relação* $\leqslant$. *Vale que* $0 = \min \mathbb{N}$. □

Demonstração:

Sabemos da Proposição 7 que $0+m = m, \forall\, m \in \mathbb{N}$. Logo, claramente decorre da Definição 10 que $0 \leqslant m, \forall\, m \in \mathbb{N}$. Pela Definição 16, $0 = \min \mathbb{N}$. ■

Proposição 42:

Seja $n \in \mathbb{N}; n \geqslant 1$. *Então* n *admite antecessor.* □

Demonstração:

Da Proposição 2 sabemos que n só não admitirá antecessor se $n = 0$. Do Lema 29, sabemos que $0 < 1$. Logo, $0 \ngeqslant 1$, implicando que todo número natural maior ou igual a 1 é diferente de 0 e, portanto, admite antecessor. ■

Notação:

Seja $n \in \mathbb{N}$. Introduzimos as seguintes notações:

i. $L_n := \{m \in \mathbb{N}; m < n\}$;

ii. $G_n := \{m \in \mathbb{N}; m > n\}$.

♣

Proposição 43:

Seja $n \in \mathbb{N}^*$. *Vale que* $\alpha(n) = \max L_n$. □

Demonstração:

Pelo Lema 29, sabemos que $\alpha(n) \in L_n$. Suponha, por absurdo, que existe $m \in L_n; m \geqslant \alpha(n)$. Então existe $p \in \mathbb{N}; \alpha(n) + p = m$ e teremos, pela Proposição 32, que ou $p < 1$, ou $p = 1$ ou $p > 1$.

Se $p < 1$, o Lema 39 implica que, como $1 = \sigma(0)$, $p = 0$. Logo, $\alpha(n) + 0 = \alpha(n) = m$.

Se $p \geqslant 1$, a Proposição 42 informa que p admite antecessor. Logo, ter-se-á que:

$$\begin{aligned} \alpha(n) + p &= m, \\ \alpha(n) + 1 + \alpha(p) &= m, \\ n + \alpha(p) &= m. \end{aligned}$$

Portanto, $n \leqslant m$. Como $\leqslant$ é uma relação de ordem parcial ampla, segue que $m \nleqslant n$, a menos que $m = n$. Se $m = n$, é claro que $m \notin L_n$. Se não, $m > n$ e $m \notin L_n$. De uma forma ou de outra, atingimos um absurdo.

Logo, concluímos que não existe m em L_n que seja maior que $\alpha(n)$. Como $\leqslant$ é total, segue que todo elemento de L_n ou é menor ou é igual a $\alpha(n)$. Conclui-se que $\alpha(n) = \max L_n$. ■

Lema 44:

Seja A *um conjunto não-vazio,* $B \subseteq A$ *e* $\preccurlyeq$ *uma relação de ordem parcial ampla em* A. *Suponhamos que* A *admite mínimo. Se* $\min A \in B$, *então* $\min B = \min A$. □

Demonstração:

Como $\min A$ é o mínimo de A, $\min A \preccurlyeq x, \forall\, x \in A$. Como $B \subseteq A$, isso implica em particular que $\min A \preccurlyeq y, \forall\, y \in B$. Logo, $\min A$ é mínimo de B e, como o mínimo de um conjunto é único pela Proposição 40, $\min A = \min B$. ■

Corolário 45:

Seja A um conjunto não-vazio, $B \subseteq A$ e $\preccurlyeq$ uma relação de ordem parcial ampla em A. Suponhamos que A admite máximo. Se $\max A \in B$, então $\max B = \max A$. □

Demonstração:

Como $\max A$ é o máximo de A, $\max A \succcurlyeq x, \forall\, x \in A$. Como $B \subseteq A$, isso implica em particular que $\max A \succcurlyeq y, \forall\, y \in B$. Logo, $\max A$ é máximo de B e, como o máximo de um conjunto é único pela Proposição 40, $\max A = \max B$. ■

Definição 17 [Boa Ordem]**:**

Seja A um conjunto e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que $\preccurlyeq$ é uma *boa ordem* se, e somente se, todo subconjunto não-vazio de A admitir mínimo. Ou seja,

$$\forall\, B \subseteq A, B \neq \varnothing, \exists\, x \in B; \forall\, y \in B, x \preccurlyeq y.$$

Se $\preccurlyeq$ for uma boa ordem sobre A, diremos que A é *bem ordenado*. ♠

Proposição 46:

Seja A um conjunto não-vazio e $\preccurlyeq$ uma relação de ordem parcial ampla. Se $\preccurlyeq$ for uma boa ordem, $\preccurlyeq$ será uma ordem total. □

Tomar essa preocupação em todo o resto?

Demonstração:

Se A for um conjunto unitário, a demonstração é trivial, pois $x \preccurlyeq x$, onde $x \in A$. Se não, tome $x \in A$. Como A é bem ordenado e $\{x, y\} \subseteq A, \forall\, y \in A$, existe mínimo em $\{x, y\}$. Suponhamos, sem perda de generalidade, que este mínimo seja x. Então $x \preccurlyeq y$ e, portanto, $x \nparallel y$. Como x e y são arbitrários, isso nos leva a concluir que $x \nparallel y, \forall\, x, y \in A$ e, portanto, $\preccurlyeq$ é total. ■

Teorema 47 [Teorema da Boa Ordem]**:**

$\mathbb{N}$ é bem ordenado pela relação $\leqslant$. □

Demonstração:

Seja $S \subseteq \mathbb{N}, S \neq \varnothing$. Se $0 \in S$, claramente S possui mínimo, pelo Lema 41 e pelo Lema 44. Consideremos então, de agora em diante, apenas os casos em que $0 \notin S$.

Considere o conjunto $S' := \{n \in \mathbb{N}; n \leqslant m, \forall\, m \in S\}$. Como $S \neq \varnothing$, ter-se á que $S' \subseteq \mathbb{N} \backslash S \subset \mathbb{N}$. Logo, $S' \neq \mathbb{N}$. Como $0 \in S'$, pelo primeiro parágrafo dessa demonstração, é preciso que exista $n \in S'; \sigma(n) \notin S'$. Caso contrário, o Axioma 2.v seria satisfeito e ter-se-ia que $S' = \mathbb{N}$.

Seja n um elemento de S' que satisfaça essa condição. Como $\sigma(n) \notin S'$, teremos pela Proposição 32 que $\sigma(n) \geqslant m$, para algum $m \in S$. Além disso, teremos pelo Corolário 22 que $\sigma(n) > m$, para este $m \in S$. Caso contrário, valeria que $\sigma(n) \leqslant m \Rightarrow \sigma(n) \in S'$.

Clamamos então que $k \in S$. Afinal, se $k \notin S$, teríamos que existe $m \in \mathbb{N}$ tal que $k \leqslant m < \sigma(k)$, o que é impossível pelo Lema 39. Logo, $k \in S$ e, como $k \in S'$, $k \leqslant n, \forall\, n \in S$. Concluímos que $k = \min S$ e, portanto, todo subconjunto não-vazio de $\mathbb{N}$ possui mínimo. Pela Definição 17, isso nos diz que $\mathbb{N}$ é bem ordenado por $\leqslant$. ■

Definição 18 [Minorante e Majorante]**:**

Seja A um conjunto, $B \subseteq A$ e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que um elemento $x \in A$ é um *minorante*, ou uma *cota inferior*, de B se, e somente se, $x \preccurlyeq y, \forall\, y \in B$. Analogamente, diremos que um elemento $z \in A$ é um *majorante*, ou uma *cota superior*, de B se, e somente se, $y \preccurlyeq z, \forall\, y \in B$. ♠

Definição 19 [Conjunto Limitado]**:**

Seja A um conjunto, $B \subseteq A$ e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que B é *limitado superiormente (inferiormente)* se admitir majorante (minorante). ♠

Proposição 48:
Seja $S \subseteq \mathbb{N}$ um subconjunto não-vazio de $\mathbb{N}$ limitado superiormente. Então S admite máximo e este é o menor majorante de S. □

Demonstração:
Seja $M(S) := \{m \in \mathbb{N}; m \geqslant n, \forall\, n \in S\}$. Visto que S é limitado superiormente, sabemos que $M(S)$ é não-vazio. Como $M(S) \subseteq \mathbb{N}$, pelo Teorema 47 sabemos que $M(S)$ admite mínimo. Perceba que, como $\min M(S)$ é majorante de S, $\min M(S) \geqslant n, \forall\, n \in S$ e, portanto, se $\min M(S) \in S$, então $\min M(S) = \max S$.

Suponhamos, por absurdo, que $\min M(S) \notin S$. Então $\min M(S) > n, \forall\, n \in S$. Logo, $S \subseteq L_{\min M(S)}$. Pela Proposição 43, $\alpha(\min M(S)) = \max L_{\min M(S)}$ e, portanto, $\alpha(\min M(S)) \geqslant n, \forall\, n \in S$. Contudo, isso implicaria que $\alpha(\min M(S))$ é majorante de S, o que é absurdo visto que $\min M(S)$ é o mínimo do conjunto dos majorantes de S e, pelo Lema 29, $\alpha(\min M(S)) < \min M(S)$. Logo, conclui-se que é preciso que $\min M(S) \in S$ e, portanto, $\min M(S) = \max S$. ■

Corolário 49:
Seja S um conjunto não-vazio e $\preccurlyeq$ uma relação de ordem parcial total ampla em S. Se existir $\min S$, então este é minorante de S. Se existir $\max S$, então este é majorante de S. □

Demonstração:
Sabemos que $\min S \preccurlyeq x, \forall\, x \in S$. Logo, $\min S$ é minorante de S. A demonstração é análoga para $\max S$. ■

Proposição 50:
$\mathbb{N}$ não é limitado superiormente. □

Demonstração:
Suponha, por absurdo, que $\mathbb{N}$ seja limitado superiormente. Então, pela Proposição 48, $\mathbb{N}$ admite máximo. Seja $m = \max \mathbb{N}$. Pelo Axioma 2 2.ii, $\sigma(m) \in \mathbb{N}$. Contudo, como $m = \max \mathbb{N}$, temos que $\sigma(m) \leqslant m$, contradizendo o Lema 29, que clama que $n < \sigma(n), \forall\, n \in \mathbb{N}$. Chegamos a um absurdo. Logo, $\mathbb{N}$ não é limitado superiormente. ■

Teorema 51 [Propriedade Arquimediana]**:**
Sejam $m, n \in \mathbb{N}, m \neq 0$. Então $\exists\, p \in \mathbb{N}; mp > n$. □

Demonstração:
Seja $S := \{n \in \mathbb{N} | \exists\, p \in \mathbb{N}; mp > n, \forall\, m \in \mathbb{N}^*\}$. É evidente que $S \subseteq \mathbb{N}$ e, pelo Lema 41, percebe-se que $0 \in \mathbb{N}$.

Antes de prosseguirmos, note que, como $m \in \mathbb{N}^*$, m admite antecessor pela Proposição 2.

Suponhamos agora que $n \in S$. Então $\sigma(n) \in S$, pois, dado $m \in \mathbb{N}^*$ e $p \in \mathbb{N}$ tais que $mp > n$, segue que

$$\begin{aligned} mp &> n \\ mp + 1 &> n + 1 && \text{(Corolário 34.i)} \\ mp + 1 + \alpha(m) &> \sigma(n) && \text{(Corolário 35)} \\ mp + m &> \sigma(n) && \text{(Lema 8)} \\ m \cdot \sigma(p) &> \sigma(n) && \text{(Definição 5.ii)} \end{aligned}$$

Logo, $\sigma(n) \in S$. Pelo Axioma 2.v, concluímos que $S = \mathbb{N}$. ■

§3: Construindo $\mathbb{Z}$

Definição 20 [Relação de Equivalência]**:**

Seja A um conjunto e $R \subseteq A \times A$ uma relação. Diremos que R é uma *relação de equivalência* em A se satisfizer as seguintes condições:

i. $\forall\, x \in A, (x, x) \in R$ (reflexividade);

ii. $\forall\, x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$ (simetria);

iii. $\forall\, x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$ (transitividade). ♠

Notação:

Seja A um conjunto e R uma relação de equivalência em A.

$$x, y \in A; (x, y) \in R \Rrightarrow x \sim y.$$

Diremos que $\sim$ é uma relação de equivalência em A. ♣

Observação:

Com o uso da notação $\sim$ pode-se escrever a definição de relação de equivalência de outra maneira. ♣

Definição:

Seja A um conjunto e $\sim$ uma relação binária em A. Diremos que $\sim$ é uma relação de equivalência em A se satisfizer as seguintes condições:

i. $\forall\, x \in A, x \sim x$ (reflexividade);

ii. $\forall\, x, y \in A, x \sim y \Rightarrow y \sim x$ (antissimetria);

iii. $\forall\, x, y, z \in A, (x \sim y \wedge y \sim z) \Rightarrow x \sim z$ (transitividade). ♠

Definição 21 [Classe de Equivalência]**:**

Sejam A um conjunto, $\sim$ uma relação de equivalência em A e $x \in A$. Denominaremos *classe de equivalência de x*, denotada por $[x]$, o conjunto definido por

$$[x] := \{y \in A; y \sim x\}.$$ ♠

Lema 52:

Sejam A um conjunto, $\sim$ uma relação de equivalência em A e $x \in A$. Vale que $[x] \neq \varnothing$. □

Demonstração:

Como $\sim$ é uma relação de equivalência, vale pela Definição 20.i que $x \sim x$. Logo, $x \in [x]$. Conclui-se que $[x] \neq \varnothing$. ■

Lema 53:

Sejam A um conjunto, $\sim$ uma relação de equivalência em A e $x, y \in A$. Se $x \not\sim y$, então $[x] \cap [y] = \varnothing$. □

Demonstração:

Assuma, por absurdo, que $\exists\, z \in [x] \cap [y]$. Então vale que $z \sim x$ e $z \sim y$. Logo, pela Definição 20.ii e pela Definição 20.iii vale que $x \sim y$, contradizendo a hipótese inicial de que $x \not\sim y$. Absurdo. Logo, $[x] \cap [y] = \varnothing$. ■

Lema 54:

Sejam A um conjunto, $\sim$ uma relação de equivalência em A e $x, y \in A$. Vale que $x \sim y \Leftrightarrow [x] = [y]$. □

Demonstração:

$\Rightarrow$: sem perda de generalidade, seja $z \in [x]$. Então $z \sim x$. Se $x \sim y$, então, pela Definição 20.iii, $z \sim y$. Logo, $z \in [y] \Rightarrow [x] \subseteq [y]$. Com um argumento análogo para $[y]$, obtém-se que $[y] \subseteq [x]$ e, portanto, $[x] = [y]$.

$\Leftarrow$: sabemos que $y \in [y]$ pela Definição 20.i. Como $[y] = [x]$, isso implica que $y \in [x]$. Logo, pela Definição 21, sabemos que $y \sim x$. Pela Definição 20.i, concluímos que $x \sim y$. ■

Definição 22 [Decomposição]**:**

Seja A um conjunto. Uma *decomposição*, ou *partição*, de A é uma família $\mathscr{A}$ de subconjuntos não-vazios de A, dois a dois disjuntos, cuja união é o próprio A. Isto é, uma família de subconjuntos de A satisfazendo:

i. $\forall\, S, T \in \mathscr{A}, S \neq T \Rightarrow S \cap T = \varnothing$;

ii. $\bigcup \mathscr{A} = A$;

iii. $\forall\, S \in \mathscr{A}, S \neq \varnothing$. ♠

Proposição 55:

As diferentes classes de equivalência de uma relação de equivalência num conjunto A fornecem uma decomposição de A.

Reciprocamente, dada uma decomposição de A, podemos definir uma relação de equivalência em A cujas classes sejam, precisamente, os subconjuntos dados. □

Demonstração:

A primeira afirmação decorre diretamente do Lema 52, do Lema 53 e do fato de que, pela Definição 20.i, $x \in [x], \forall\, x \in A$. Logo, é claro que a união disjunta das classes de equivalência irá se igualar ao conjunto.

Demonstremos agora a segunda afirmação: dada uma decomposição $\mathscr{A}$ de A, diremos que dois elementos de A são equivalentes se pertencerem ao mesmo elemento de $\mathscr{A}$ (que é um subconjunto de A). Como $\bigcup \mathscr{A} = A$, é claro que todo elemento de A precisa pertencer a um elemento da decomposição. Logo, vale a propriedade reflexiva.

Sejam $x, y \in A$. Se x e y pertencem ao mesmo elemento da decomposição, é claro que y e x pertencem ao mesmo elemento da decomposição. Finalmente, se $x, y \in S$ e $y, z \in T$, sabemos que $x, y, z \in S = T$, visto que $S \neq T \Rightarrow S \cap T = \varnothing$ e evidentemente $y \in S \cap T$. Logo, vale a propriedade transitiva.

Desta forma, demonstramos que é possível construir uma relação de equivalência em um conjunto A a partir de uma decomposição $\mathscr{A}$ de A. Resta demonstrar que as classes dessa relação são, precisamente, os elementos de $\mathscr{A}$. É simples constatar que $[x]$ é, de fato, o elemento de $\mathscr{A}$ que inclui x, mas o que garante que todo elemento de $\mathscr{A}$ possui uma classe associada? Simples: como nenhum elemento da decomposição pode ser vazio, todos eles possuem ao menos um elemento de A. Logo, a classe deste elemento é igual ao elemento da decomposição. ■

Definição 23 [Conjunto Quociente]**:**

Seja A um conjunto e $\sim$ uma relação de equivalência em A. Definimos o *conjunto quociente* de A por $\sim$, denotado por $A/\!\sim$, como o conjunto formado por todas as classes de equivalência determinadas por $\sim$ em A, *i.e.*,

$$A/\!\sim \;:= \{[x]; x \in A\}.$$ ♠

Definição 24 [Relação de Equivalência em $\mathbb{N} \times \mathbb{N}$]**:**

Considere o conjunto

$$\mathbb{N} \times \mathbb{N} = \{(m, n); m, n \in \mathbb{N}\}.$$

Definimos a relação $\sim$ em $\mathbb{N} \times \mathbb{N}$ de forma que, dados dois elementos $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. ♠

Proposição 56:
A relação $\sim$ definida em $\mathbb{N} \times \mathbb{N}$ é uma relação de equivalência. □

Demonstração:
Seja $(a, b) \in \mathbb{N} \times \mathbb{N}$. Claramente $(a, b) \sim (a, b)$, pois $a + b = a + b$. Logo, $\sim$ é reflexiva.

Seja $(c, d \in \mathbb{N} \times \mathbb{N})$ e suponha que $(a, b) \sim (c, d)$. Então vale que $a + d = b + c$. Logo, $c + b = d + a$ e, portanto, $(c, d) \sim (a, b)$. Portanto, $\sim$ é simétrica.

Seja $(e, f) \in \mathbb{N} \times \mathbb{N}$ e suponha que $(c, d) \sim (e, f)$. Sabe-se então que $c + f = d + e$ e, como $a + d = b + c$, segue que:

$$\begin{aligned}
c + f &= d + e, \\
a + c + f &= a + d + e, \\
a + c + f &= b + c + e, \\
a + f &= b + e. && \text{(Proposição 10)}
\end{aligned}$$

Conclui-se que $(a, b) \sim (e, f)$ e, portanto, $\sim$ é transitiva. Logo, $\sim$ é relação de equivalência. ■

Definição 25 [Números Inteiros]**:**
Doravante utilizaremos a notação $\mathbb{Z} \equiv \mathbb{N} \times \mathbb{N}/\sim$ e iremos nos referenciar aos elementos de $\mathbb{Z}$ como *números inteiros*, ou simplesmente *inteiros*. ♠

Lema 57:
Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$. *Vale que* $[(a, b)] = [(c, d)]$ *se, e somente se,* $c = a + m$ *e* $d = b + m$ *ou* $a = c + m$ *e* $b = d + m$, *para algum* $m \in \mathbb{N}$. □

Demonstração:
$\Leftarrow$: suponhamos, sem perda de generalidade, que $c = a + m$ e $d = b + m$. Pelo Lema 54, sabemos que o enunciado é equivalente a dizer que $(a, b) \sim (a + m, b + m)$. Pela Definição 24, basta provar que $a + b + m = b + a + m$. Como $a + b + m = a + b + m$, é suficiente invocar a Proposição 9 uma única vez para obter então que, de fato, $[(a, b)] = [(a + m, b + m)], \forall\, m \in \mathbb{N}$.

$\Rightarrow$: consideremos primeiramente o caso em que $c \leqslant a$ (como $\leqslant$ é total, pela Proposição 32, este caso é possível). Então $c + p = a$, para algum $p \in \mathbb{N}$. Visto que $[(a, b)] = [(c, d)]$, o Lema 54 informa que $a + d = c + b$ e, portanto, $c + p + d = c + b$. Pela Proposição 10, $b = d + p$. Defina $m = p$ e está concluída a demonstração.

Consideremos então o caso em que $a \leqslant c$ (novamente, como $\leqslant$ é total pela Proposição 32, este caso é possível). Então $a + p = c$, para algum $p \in \mathbb{N}$. Visto que $[(a, b)] = [(c, d)]$, o Lema 54 informa que $a + d = c + b$ e, portanto, $a + d = a + p + b$. Pela Proposição 10, $d = b + p$. Defina $m = p$ e está concluída a demonstração. ■

Definição 26 [Adição de Inteiros]**:**
Sejam $\alpha = [(a, b)], \beta = [(c, d)] \in \mathbb{Z}$. Definimos a *adição*, ou *soma*, de α e β, por

$$\alpha + \beta := [(a + c, b + d)].$$ ♠

Proposição 58:
Sejam $[(a, b)], [(c, d)] \in \mathbb{Z}$. *Sejam* $(a', b') \sim (a, b)$ *e* $(c', d') \sim (c, d)$. *Então* $[(a + c, b + d)] = [(a' + c', b' + d')]$. □

Demonstração:
$(a', b') \sim (a, b) \Rightarrow a' + b = b' + a$. Analogamente, $(c', d') \sim (c, d) \Rightarrow c' + d = d' + c$. Logo,

segue que

$$\begin{aligned} a' + b + c' + d &= a + b' + c + d', \\ (a' + c') + (b + d) &= (a + c) + (b' + d'), \\ (a' + c', b' + d') &\sim (a + c, b + d), && \text{(Definição 24)} \\ [(a' + c', b' + d')] &= [(a + c, b + d)]. && \text{(Lema 54)} \end{aligned}$$

Assim concluímos a demonstração. ∎

Proposição 59:
A adição de números inteiros admite as seguintes propriedades:

i. $\forall \alpha, \beta, \gamma \in \mathbb{Z}, (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ *(associatividade);*

ii. $\exists\, 0 \in \mathbb{Z}; \alpha + 0 = 0 + \alpha = \alpha, \forall \alpha \in \mathbb{Z}$ *(existência de neutro);*

iii. $\forall \alpha \in \mathbb{Z}, \exists (-\alpha) \in \mathbb{Z}; (\alpha + (-\alpha)) = -\alpha + \alpha = 0$ *(existência de oposto);*

iv. $\forall \alpha, \beta \in \mathbb{Z}, \alpha + \beta = \beta + \alpha$ *(comutatividade).* □

Demonstração:
Sejam $\alpha = [(a, a')]$, $\beta = [(b, b')]$ e $\gamma = [(c, c')]$. Teremos que

$$\begin{aligned} ([(a, a')] + [(b, b')]) + [(c, c')] &= ([(a + b, a' + b')]) + [(c, c')], && \text{(Definição 26)} \\ &= [((a + b) + c, (a' + b') + c')], && \text{(Definição 26)} \\ &= [(a + (b + c), a' + (b' + c'))], && \text{(Proposição 5)} \\ &= [(a, a')] + [(b + c, b' + c')], && \text{(Definição 26)} \\ &= [(a, a')] + ([(b, b')] + [(c, c')]). && \text{(Definição 26)} \end{aligned}$$

Logo, a adição de inteiros é associativa.
Note também que

$$\begin{aligned} [(a, a')] + [(0, 0)] &= [(a + 0, a' + 0)], && \text{(Definição 26)} \\ &= [(0 + a, 0 + a')] = [(0, 0)] + [(a, a')], && \text{(Proposição 9)} \\ &= [(a, a')]. && \text{(Definição 2.i)} \end{aligned}$$

Logo, a adição de inteiros admite elemento neutro, que é dado por $[(0, 0)]$. Usando o Lema 57, vemos que o elemento neutro aditivo de $\mathbb{Z}$ é, de forma geral, dado por $[(m, m)]$, $m \in \mathbb{N}$.
Além disso, perceba que

$$\begin{aligned} [(a, a')] + [(a', a)] &= [(a + a', a' + a)], && \text{(Definição 26)} \\ &= [(a' + a, a + a')] = [(a', a)] + [(a, a')], && \text{(Proposição 9)} \\ &= [(0, 0)]. && \text{(Lema 57)} \end{aligned}$$

Assim confirmamos que todo número inteiro possui inverso aditivo.
Finalmente, ressaltamos que

$$\begin{aligned} [(a, a')] + [(b, b')] &= [(a + b, a' + b')], && \text{(Definição 26)} \\ &= [(b + a, b' + a')], && \text{(Proposição 9)} \\ &= [(b, b')] + [(a, a')]. && \text{(Definição 26)} \end{aligned}$$

Desta forma percebemos que a adição de inteiros também é comutativa, encerrando a demonstração. ∎

Definição 27 [Zero]**:**
Como o elemento $[(a, a)] \in \mathbb{Z}$ herda a propriedade aditiva do zero natural, denotamos esse número inteiro por 0 e também o denominamos *zero*. ♠

Definição 28 [Oposto]**:**
Dado $\alpha = [(a, a')] \in \mathbb{Z}$, definimos o oposto de α, denotado por $-\alpha$, segundo $-\alpha := [(a', a)]$. A motivação para esta definição flui da demonstração da Proposição 59.iii. ♠

Definição 29 [Multiplicação de Inteiros]**:**
Sejam $\alpha = [(a, b)]\,, \beta = [(c, d)] \in \mathbb{Z}$. Definimos a *multiplicação*, ou *produto*, de α e β, por

$$\alpha \cdot \beta := [(ac + bd, ad + bc)]\,.$$ ♠

Proposição 60:
Sejam $[(a, b)]\,, [(c, d)] \in \mathbb{Z}$. *Sejam* $(a', b') \sim (a, b)$ *e* $(c', d') \sim (c, d)$. *Então* $[(ac+bd, ad+bc)] = [(a'c' + b'd', a'd' + b'c')]$. □

Demonstração:
$(a', b') \sim (a, b) \Rightarrow a' + b = b' + a$. Analogamente, $(c', d') \sim (c, d) \Rightarrow c' + d = d' + c$. Logo, segue que

$$\begin{aligned}
a + b' = a' + b &\Rightarrow ac + b'c = a'c + bc,\\
a' + b = a + b' &\Rightarrow a'd + bd = ad + b'd,\\
&\Rightarrow ac + bd + a'd + b'c = ad + bc + a'c + b'd,\\
&\Rightarrow [(ac + bd, ad + bc)] = [(a'c + b'd, a'd + b'c)]\,.
\end{aligned}$$

Além disso, vê-se que

$$\begin{aligned}
c + d' = c' + d &\Rightarrow a'c + a'd' = a'c' + a'd,\\
c' + d = c + d' &\Rightarrow b'c' + b'd = b'c + b'd',\\
&\Rightarrow a'c + b'd + a'd' + b'c' = a'd + b'c + a'c' + b'd',\\
&\Rightarrow [(a'c + b'd, a'd + b'c)] = [(a'c' + b'd', a'd' + b'c')].
\end{aligned}$$

Como $[(ac + bd, ad + bc)] = [(a'c + b'd, a'd + b'c)] = [(a'c' + b'd', a'd' + b'c')]$, concluímos a demonstração. ■

Proposição 61:
A multiplicação de números inteiros admite as seguintes propriedades:

i. $\forall\, \alpha, \beta, \gamma \in \mathbb{Z}, (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ *(associatividade);*

ii. $\exists\, 1 \in \mathbb{Z}; \alpha \cdot 1 = 1 \cdot \alpha = \alpha, \forall\, \alpha \in \mathbb{Z}$ *(existência de neutro);*

iii. $\forall\, \alpha, \beta, \gamma \in \mathbb{Z}, \alpha \neq 0, \alpha \cdot \beta = \alpha \cdot \gamma \Rightarrow \beta = \gamma$ *(Lei do Cancelamento);*

iv. $\forall\, \alpha, \beta \in \mathbb{Z}, \alpha \cdot \beta = \beta \cdot \alpha$ *(comutatividade);*

v. $\forall\, \alpha, \beta, \gamma \in \mathbb{Z}, \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ *(distributividade).* □

Demonstração:

Sejam $\alpha = [(a, a')]$, $\beta = [(b, b')]$, $\gamma = [(c, c')]$. Tem-se que

$$\begin{aligned}
([(a, a')] \cdot [(b, b')]) \cdot [(c, c')] &= ([(ab + a'b', ab' + a'b)]) \cdot [(c, c')]\,, \\
&= [((ab + a'b') \cdot c + (ab' + a'b) \cdot c', \\
&\quad (ab' + a'b) \cdot c + (ab + a'b') \cdot c')]\,, \\
&= [(abc + a'b'c + ab'c' + a'bc', \\
&\quad ab'c + a'bc + abc' + a'b'c')]\,, \\
&= [(a \cdot (bc + b'c') + a' \cdot (b'c + bc'), \\
&\quad a \cdot (b'c + bc') + a' \cdot (bc + b'c'))]\,, \\
&= [(a \cdot (bc + b'c') + a' \cdot (b'c + bc'), \\
&\quad a \cdot (b'c + bc') + a' \cdot (bc + b'c'))]\,, \\
&= [(a, a')] \cdot [(bc + b'c', b'c + bc')]\,, \\
&= [(a, a')] \cdot ([(b, b')] \cdot [(c, c')])\,.
\end{aligned}$$

Logo, a multiplicação de inteiros é associativa. Note que utilizamos as propriedades associativa e comutativa das operações com números naturais, bem como a definição de multiplicação de inteiros, acima.

Além disso, notamos que

$$\begin{aligned}
[(a, a')] \cdot [(1, 0)] &= [(a \cdot 1 + a' \cdot 0, a' \cdot 1 + a \cdot 0)]\,, && \text{(Definição 29)} \\
&= [(a, a')]\,, \\
&= [(1 \cdot a + 0 \cdot a', 0 \cdot a + 1 \cdot a')]\,, \\
&= [(1, 0)] \cdot [(a, a')]\,. && \text{(Definição 29)}
\end{aligned}$$

Assim vemos que existe, de fato, um elemento neutro multiplicativo (ou identidade) nos inteiros, o elemento $[(1, 0)]$. Note que o Lema 57 implica que $[(\sigma(m), m)]$ é a identidade de $\mathbb{Z}$, $\forall\, m \in \mathbb{N}$.

Percebe-se ainda que

$$[(a, a')] \cdot [(b, b')] = [(a, a')] \cdot [(c, c')]\,, [(ab + a'b', ab' + a'b)] \quad = [(ac + a'c', ac' + a'c)]\,.$$

Do Lema 54, sabemos que isso implica que

$$\begin{aligned}
ab + a'b' + ac' + a'c &= ac + a'c' + ab' + a'b, \\
a(b + c') + a'(b' + c) &= a(c + b') + a'(c' + b).
\end{aligned}$$

Como $\alpha \neq 0$ e $0 = [(m, m)], \forall\, m \in \mathbb{N}$, vemos que $a \neq a'$. Logo, pelo Teorema 21, ou $a = a' + q$ ou $a' = a + q$, para algum $q \in \mathbb{N}^*$. Sem perda de generalidade, suponhamos que $a' < a$ e, portanto, $a = a' + q$. Teremos então que:

$$\begin{aligned}
a(b + c') + a'(b' + c) &= a(c + b') + a'(c' + b), \\
a(b + c') + (a + q)(b' + c) &= a(c + b') + (a + q)(c' + b), \\
a(b + c') + a(b' + c) + q(b' + c) &= a(c + b') + a(c' + b) + q(c' + b), && \text{(Proposição 16)} \\
q(b' + c) &= q(c' + b), && \text{(Proposição 10)} \\
c + b' &= b + c', && \text{(Proposição 36)} \\
(c, c') &\sim (b, b')\,, && \text{(Definição 24)} \\
[(b, b')] &= [(c, c')]\,,
\end{aligned}$$

demonstrando que vale a Lei do Cancelamento para o produto de números inteiros.

A seguir, vê-se que

$$\begin{aligned}
[(a,a')]\cdot[(b,b')] &= [(ab+a'b', ab'+a'b)]\,, && \text{(Definição 29)}\\
&= [(ba+b'a', ba'+b'a)]\,,\\
&= [(b,b')]\cdot[(a,a')]\,. && \text{(Definição 29)}
\end{aligned}$$

Isto prova a comutatividade do produto de inteiros.

Finalmente, mostramos que

$$\begin{aligned}
[(a,a')]\cdot([(b,b')]+[(c,c')]) &= [(a,a')]\cdot[(b+c, b'+c')]\,, && \text{(Definição 26)}\\
&= [(a(b+c)+a'(b'+c'), a(b'+c')+a'(b+c))]\,,\\
& && \text{(Definição 29)}\\
&= [(ab+a'b'+ac+a'c', ab'+a'b+ac'+a'c)]\,,\\
&= [(ab+a'b', ab'+a'b)]+[(ac+a'c', ac'+a'c)]\,,\\
& && \text{(Definição 26)}\\
&= ([(a,a')]\cdot[(b,b')])+([(a,a')]\cdot[(c,c')])\,, && \text{(Definição 29)}
\end{aligned}$$

o que demonstra a validade da distributividade do produto sobre a soma de inteiros. ■

Definição 30 [Um]**:**

Como o elemento $[(\sigma(m), m)] \in \mathbb{Z}$ herda a propriedade multiplicativa do um natural, denotamos esse número inteiro por 1 e também o denominamos *um*. ♠

§4: Ordenando os Inteiros

Definição 31 [Menor ou Igual em $\mathbb{Z}$]**:**

Sejam $\alpha = [(a,a')]$ e $\beta = [(b,b')]$ números inteiros. Diremos que α é *menor ou igual* a β, e escreveremos $\alpha \leqslant \beta$, se $a+d \leqslant b+c$. Neste caso, também diremos que β é *maior ou igual* a α e escreveremos $\beta \geqslant \alpha$, onde $\geqslant$ denota a relação inversa de $\leqslant$. ♠

Proposição 62:

A relação $\leqslant$ *está bem definida em* $\mathbb{Z}$, i.e., *se* $[(a,a')] \sim [(c,c')]$ *e* $[(b,b')] \sim [(d,d')]$ *forem inteiros,* $a+b' \leqslant b+a' \Leftrightarrow c+d' \leqslant d+c'$. □

Demonstração:

$$\begin{cases}[(a,a')] \sim [(c,c')] \Rightarrow a+c' = a'+c\\ [(b,b')] \sim [(d,d')] \Rightarrow b+d' = b'+d\end{cases}.$$

$$\begin{aligned}
a+b' &\leqslant b+a',\\
a+b'+c+c'+d+d' &\leqslant b+a'+c+c'+d+d', && \text{(Proposição 33)}\\
b'+d+a+c'+c+d' &\leqslant b+d'+a'+c+c'+d,\\
b+d'+a'+c+c+d' &\leqslant b+d'+a'+c+c'+d, && \text{(por hipótese)}\\
c+d' &\leqslant c'+d. && \text{(Proposição 33)}
\end{aligned}$$

É claro que a volta pode ser demonstrada simplesmente revertendo os passos. ■

Proposição 63:
A relação menor ou igual definida em $\mathbb{Z}$ é uma relação de ordem total ampla. □

Demonstração:
Da Proposição 56 segue que $\leqslant$ é reflexiva.
Sejam $\alpha = [(a, a')]$ e $\beta = [(b, b')]$ inteiros com $\alpha \leqslant \beta$ e $\beta \leqslant \alpha$. Então vale que

$$\begin{cases} a + b' \leqslant a' + b \\ a' + b \leqslant a + b' \end{cases} .$$

Pela Proposição 24 vale que $a + b' = a' + b$. Logo, o Lema 54 garante que $[(a, a')] = [(b, b')]$ e, portanto, que $\leqslant$ é antissimétrica.
Seja $\gamma = [(c, c')]$ e suponhamos que $\alpha \leqslant \beta$ e $\beta \leqslant \gamma$. Então vale que

$$\begin{cases} a + b' \leqslant a' + b \\ b + c' \leqslant b' + c \end{cases} .$$

Logo,

$$\begin{aligned} a + b' + c + c' &\leqslant a' + b + c + c', && \text{(Proposição 33)} \\ a + c' + b' + c &\leqslant a' + c + b + c', && \\ a + c' + b' + c &\leqslant a' + c + b' + c, && \text{(por hipótese)} \\ a + c' &\leqslant a' + c, && \text{(Proposição 10)} \\ [(a, a')] &\leqslant [(c, c')], && \text{(Definição 31)} \end{aligned}$$

Assim percebe-se que $\leqslant$ é transitiva em $\mathbb{Z}$.
Finalmente, resta provar a totalidade da relação menor ou igual. Sejam α e β inteiros quaisquer, mas representados pelas classes de equivalência como acima definidos. Queremos saber se sempre é verdade ou que $a + b' \leqslant b + a'$ ou que $a' + b \leqslant b' + a$, $\forall\, a, a', b, b' \in \mathbb{N}$. Como a adição de naturais é fechada[1], o Corolário 22 implica na totalidade de $\leqslant$. ■

Definição 32 [Estritamente Menor em $\mathbb{Z}$]**:**
Definimos a relação $<$ em $\mathbb{Z}$ como a ordem correspondente de $\leqslant$. Pela Proposição 31 e pela Proposição 27, $<$ é uma relação de ordem total estrita em $\mathbb{Z}$. ♠

Proposição 64:
Sejam $\alpha = [(a, a')]\,, \beta = [(b, b')] \in \mathbb{Z}$. *Então vale que*

$$\alpha < \beta \Leftrightarrow a + b' < a' + b.$$ □

Demonstração:
Pelo Lema 54,

$$\alpha = \beta \Leftrightarrow a + b' = a' + b.$$

Como sabemos que $\alpha \leqslant \beta$, sabemos que $a + b' \leqslant a' + b$. Mas como $\alpha \neq \beta$, sabemos que $a + b' \neq a' + b$. Logo, $a + b' < a' + b$. Se $a + b' < a' + b$, é claro que $\alpha \neq \beta$, pelo Lema 57, e $\alpha \leqslant \beta$. Logo, $\alpha < \beta$. ■

Proposição 65:
Sejam $\alpha, \beta, \gamma, \delta \in \mathbb{Z}, 0 \leqslant \delta$. *Então valem:*

i. $\alpha \leqslant \beta \Leftrightarrow \alpha + \gamma \leqslant \beta + \gamma$;

[1] Definição 2

ii. $\alpha \leqslant \beta \Leftrightarrow \alpha\delta \leqslant \beta\delta$. □

Demonstração:

Sejam $\alpha = [(a, a')]\,, \beta = [(b, b')]\,, \gamma = [(c, c')]\,, \delta = [(d, d')]$. Suponhamos $\alpha \leqslant \beta$. Então segue que

$$\begin{aligned} a + b' &\leqslant b + a', \\ a + b' + c + c' &\leqslant b + a' + c + c', && \text{(Proposição 33.i)} \\ (a + c) + (b' + c') &\leqslant (b + c) + (a' + c'), \\ [(a + c, a' + c')] &\leqslant [(b + c, b' + c')]\,, \\ [(a, a')] + [(c, c')] &\leqslant [(b, b')] + [(c, c')]\,. \end{aligned}$$

A volta é demonstrada revertendo o argumento.

Como $0 \leqslant \delta$, sabemos que $d' + 0 \leqslant 0 + d$, *i.e.*, $d' \leqslant d$. Logo, $\exists\, m \in \mathbb{N}; d' + m = d$. Vem então do Lema 57 que $\delta = [(m, 0)]$. Segue então que

$$\begin{aligned} a + b' &\leqslant b + a', \\ (a + b') \cdot m &\leqslant (a' + b) \cdot m, && \text{(Proposição 33.ii)} \\ am + b'm &\leqslant a'm + bm, \\ [(am, a'm)] &\leqslant [(bm, b'm)]\,, \\ [(a, a')] \cdot [(m, 0)] &\leqslant [(b, b')] \cdot [(m, 0)]\,, \\ [(a, a')] \cdot [(d, d')] &\leqslant [(b, b')] \cdot [(d, d')]\,. \end{aligned}$$

A volta é demonstrada revertendo o argumento com o auxílio do Corolário 37. ■

Definição 33 [Inteiros Positivos e Negativos]**:**

Seja $\alpha \in \mathbb{Z}$. Diremos que α é *positivo* se, e somente se, $0 < \alpha$. Diremos que α é *negativo* se, e somente se, $\alpha < 0$. ♠

Lema 66:

Todo inteiro positivo pode ser escrito na forma $[(m, 0)]$, *com* $m \in \mathbb{N}^*$. *Analogamente, todo inteiro negativo pode ser escrito na forma* $[(0, m)]$, *com* $m \in \mathbb{N}^*$. □

Demonstração:

Seja $\alpha = [(a, a')]$. Suponhamos, sem perda de generalidade, que α seja positivo. Então vale que $a' < a$. Logo, $a' + m = a$, para algum $m \in \mathbb{N}^*$. Pelo Lema 57, vale então que $[(a, a')] = [(m, 0)]$. Logo, todo inteiro positivo pode ser escrito na forma $[(m, 0)]$, com $m \in \mathbb{N}^*$. A demonstração para α negativo é análoga. ■

Notação:

Denotaremos o conjunto dos inteiros não-negativos por $\mathbb{Z}_+$ e o dos inteiros não-positivos por $\mathbb{Z}_-$. A ausência do zero nestes conjuntos ou no próprio $\mathbb{Z}$ será indicada por um asterisco: $\mathbb{Z}_+^*$, $\mathbb{Z}_-^*$ e $\mathbb{Z}^*$. Em suma,

$$\begin{aligned} \mathbb{Z}_+ &:= \{[(m, 0)]\,, m \in \mathbb{N}\}, \\ \mathbb{Z}_- &:= \{[(0, m)]\,, m \in \mathbb{N}\}, \\ \mathbb{Z}_+^* &:= \{[(m, 0)]\,, m \in \mathbb{N}^*\}, \\ \mathbb{Z}_-^* &:= \{[(0, m)]\,, m \in \mathbb{N}^*\}, \\ \mathbb{Z}^* &:= \mathbb{Z} \setminus \{0\}\,. \end{aligned}$$

♣

Teorema 67 [Princípio da Boa Ordem em $\mathbb{Z}$]**:**

$\mathbb{Z}_+$ é bem ordenado pela relação $\leqslant$, i.e., *todo conjunto não-vazio de inteiros não-negativos admite mínimo.* □

Demonstração:

Seja $\varnothing \subset A \subseteq \mathbb{Z}_+$. Pelo Lema 66, todo elemento de A pode ser escrito na forma $[(m, 0)]$, para algum $m \in \mathbb{N}$. Note que, dados $[(m, 0)], [(n, 0)] \in \mathbb{Z}$, $[(m, 0)] \leqslant [(n, 0)] \Leftrightarrow m \leqslant n$, visto que $m + 0 = m, \forall\, m \in \mathbb{N}$[2].

Definimos então o conjunto $A_{\mathbb{N}} := \{m \in \mathbb{N}; [(m, 0)] \in A\}$. Pelo Teorema 47, $\exists \min A_{\mathbb{N}}$. Pela observação acima, $[(\min A_{\mathbb{N}}, 0)] \leqslant [(m, 0)], \forall\, m \in A_{\mathbb{N}}$. Portanto, $[(\min A_{\mathbb{N}}, 0)] \leqslant \alpha, \forall\, \alpha \in A$. Logo, $\min A = [(\min A_{\mathbb{N}}, 0)]$, provando que A possui elemento mínimo e, por consequência, $\mathbb{Z}_+$ é bem ordenado por $\leqslant$. ■

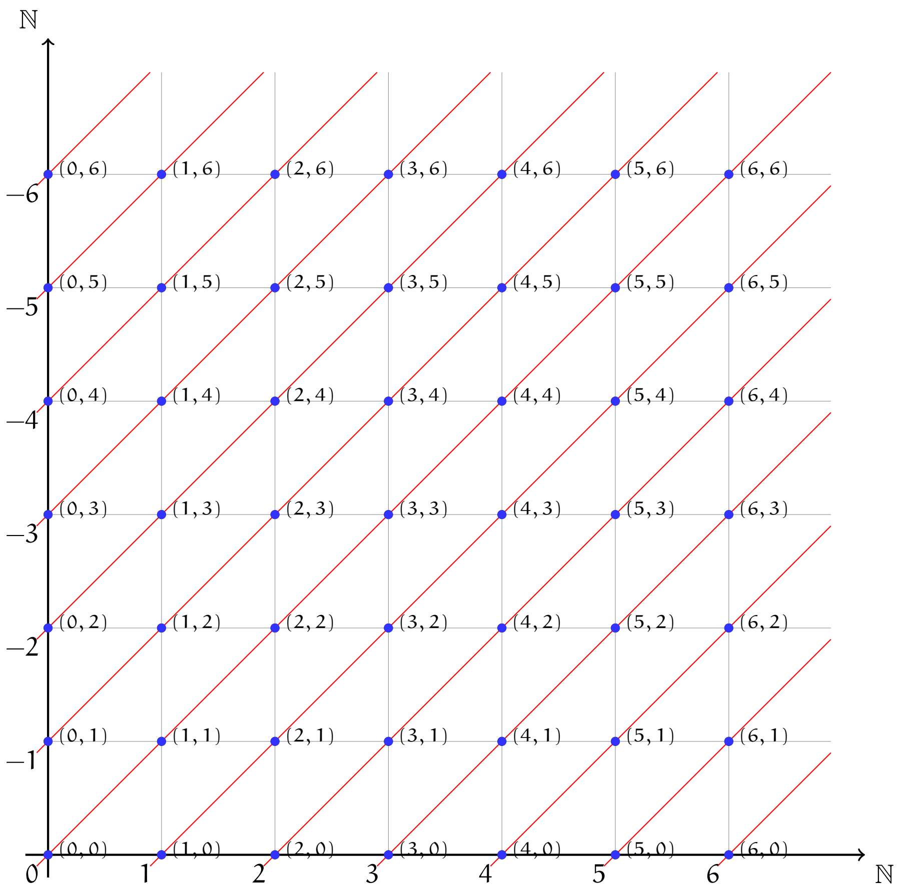

Figura 1.1: *Esquematização da construção de $\mathbb{Z}$ a partir de $\mathbb{N} \times \mathbb{N}$. Os pontos em azul representam os elementos de $\mathbb{N} \times \mathbb{N}$ e as retas em vermelho as classes de equivalência que definem os elementos de $\mathbb{Z}$. Note que cada classe de equivalência representa o inteiro em que a reta se inicia. Os sinais negativos no eixo vertical tem propósito ilustrativo.*

[2]Proposição 7

Capítulo 2

Propriedades dos Números Inteiros

A proposição acima é ocasionalmente útil.

Comentário após a demonstração de que
$1 + 1 = 2$, *Principia Mathematica, Volume II*
Bertrand Russel

§5: Operações com Inteiros

Propriedade:
Conforme demonstrado nas Seções §3 e §4, o conjunto dos números inteiros, $\mathbb{Z}$, dotado das operações $+$ e $\cdot$ e da relação $\leqslant$ (e $<$) satisfaz as seguintes propriedades:

P.1 $\forall\, a, b, c \in \mathbb{Z}, a + (b + c) = (a + b) + c$ (Proposição 59.i);

P.2 $\exists\, 0 \in \mathbb{Z}; \forall\, a \in \mathbb{Z}, a + 0 = 0 + a = a$ (Proposição 59.ii);

P.3 $\forall\, a \in \mathbb{Z}, \exists -a \in \mathbb{Z}; a + (-a) = (-a) + a = 0$ (Proposição 59.iii);

P.4 $\forall\, a, b \in \mathbb{Z}, a + b = b + a$ (Proposição 59.iv);

P.5 $\forall\, a, b, c \in \mathbb{Z}, a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Proposição 61.i);

P.6 $\exists\, 1 \in \mathbb{Z}^*; \forall\, a \in \mathbb{Z}, a \cdot 1 = 1 \cdot a = a$ (Proposição 61.ii);

P.7 $\forall\, a, b, c \in \mathbb{Z}, c \neq 0, a \cdot c = b \cdot c \Rightarrow a = b$ (Proposição 61.iii);

P.8 $\forall\, a, b \in \mathbb{Z}, a \cdot b = b \cdot a$ (Proposição 61.iv);

P.9 $\forall\, a, b, c \in \mathbb{Z}, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (Proposição 61.v);

P.10 $\forall\, a \in \mathbb{Z}, a \leqslant a$ (Proposição 63);

P.11 $\forall\, a, b \in \mathbb{Z}, (a \leqslant b \wedge b \leqslant a) \Rightarrow a = b$ (Proposição 63);

P.12 $\forall\, a, b, c \in \mathbb{Z}, (a \leqslant b \wedge b \leqslant c) \Rightarrow a \leqslant c$ (Proposição 63);

P.13 $\forall\, a, b \in \mathbb{Z}, (a = b \vee a < b \vee a > b)$ (Proposição 63);

P.14 $\forall\, a, b, c \in \mathbb{Z}, a \leqslant b \Rightarrow a + c \leqslant b + c$ (Proposição 65.i);

P.15 $\forall\, a, b, c \in \mathbb{Z}, 0 \leqslant c, a \leqslant b \Rightarrow a \cdot c \leqslant b \cdot c$ (Proposição 65.ii);

P.16 $\forall\, A \subseteq \mathbb{Z}_+, A \neq \varnothing, \exists \min A$ (Teorema 67). ♠

Proposição 68:
$\forall\, a, b, c \in \mathbb{Z}, a + c = b + c \Rightarrow a = b, c + a = c + b \Rightarrow a = b.$ □

Demonstração:

$$
\begin{aligned}
c + a &= c + b, \\
a + c &= b + c, && \text{(P.4)} \\
(a + c) + (-c) &= (b + c) + (-c), && \text{(P.3)} \\
a + (c + (-c)) &= b + (c + (-c))\,, && \text{(P.1)} \\
a + 0 &= b + 0, && \text{(P.3)} \\
a &= b, . && \text{(P.2)}
\end{aligned}
$$

Isto conclui a demonstração. ■

Lema 69:
$\exists!\, 0 \in \mathbb{Z}$ *que satisfaz P.2.* □

Demonstração:
Suponha que e_a e e_b sejam inteiros e satisfaçam as propriedades do 0 (P.2). Então vale que

$$
\begin{cases}
e_a + e_b = e_b + e_a = e_a \\
e_a + e_b = e_b + e_a = e_b
\end{cases}
\Rightarrow e_a = e_b.
$$

Logo, como 0 sabidamente satisfaz estas propriedades, vemos que ele é o único inteiro que o faz. ■

Lema 70:
$\exists!\, 1 \in \mathbb{Z}$ *que satisfaz P.6.* □

Demonstração:
Suponha que e_a e e_b sejam inteiros e satisfaçam as propriedades do 1 (P.6). Então vale que

$$
\begin{cases}
e_a \cdot e_b = e_b \cdot e_a = e_a \\
e_a \cdot e_b = e_b \cdot e_a = e_b
\end{cases}
\Rightarrow e_a = e_b.
$$

Logo, como 1 sabidamente satisfaz estas propriedades, vemos que ele é o único inteiro que o faz. ■

Proposição 71:
$\forall\, a \in \mathbb{Z}, a \cdot 0 = 0 \cdot a = 0.$ □

Demonstração:

$$
\begin{aligned}
(0 \cdot a) + (0 \cdot a) &= (0 + 0) \cdot a, && \text{(P.9)} \\
&= 0 \cdot a. && \text{(P.2)}
\end{aligned}
$$

Logo, $0 \cdot a$ satisfaz P.2. Pelo Lema 69, $0 \cdot a = 0$. ■

Proposição 72:
$\forall\, a, b \in \mathbb{Z}, a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$. □

Demonstração:
Pela Proposição 71, $a \cdot 0 = 0$. Logo, se $a \cdot b = 0$, $a \cdot b = a \cdot 0$. Se $a = 0$, a demonstração está encerrada. Se não, $b = 0$ por P.7. ■

Lema 73:
$\forall\, a \in \mathbb{Z}, \exists! -a \in \mathbb{Z}; a + (-a) = (-a) + a = 0$. □

Demonstração:
Suponha que a^* e a' satisfaçam P.3. Então vale que $a^* + a = 0 = a' + a$. Pela Proposição 68, $a^* = a'$. ■

Proposição 74:
Seja $a \in \mathbb{Z}$. *Vale que* $-(-a) = a$. □

Demonstração:
Perceba que

$$\begin{cases} a + (-a) = -a + a = 0 \\ -(-a) + (-a) = -a + (-(-a)) = 0 \end{cases}.$$

Logo, tanto a quanto $-(-a)$ satisfazem P.3 para $-a$. Pelo Lema 73, $-(-a) = a$. ■

Lema 75:
Seja $a \in \mathbb{Z}$. *Vale que* $-a = -1 \cdot a$. □

Demonstração:

$$\begin{aligned} a + (-1 \cdot a) &= (1 \cdot a) + (-1 \cdot a), && \text{(P.6)} \\ &= (1 + (-1)) \cdot a, && \text{(P.9)} \\ &= 0 \cdot a, && \text{(P.3)} \\ &= 0. && \text{(Proposição 71)} \end{aligned}$$

Isto conclui a demonstração. ■

Lema 76:
$(-1) \cdot (-1) = 1$. □

Demonstração:

$$\begin{aligned} (-1) \cdot (-1) &= -(-1), && \text{(Lema 75)} \\ &= 1. && \text{(Proposição 74)} \end{aligned}$$

Isto conclui a demonstração. ■

Proposição 77:
Sejam $a, b \in \mathbb{Z}$. *Valem as seguintes propriedades:*

i. $(-a) \cdot (-b) = a \cdot b$;

ii. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$. □

Demonstração:

$$
\begin{aligned}
(-a)\cdot(-b) &= (-1\cdot a)\cdot(-1\cdot b)\,, && \text{(Lema 75)}\\
&= (a\cdot(-1))\cdot(-1\cdot b)\,, && \text{(P.4)}\\
&= a\cdot(-1\cdot(-1\cdot b))\,, && \text{(P.1)}\\
&= a\cdot((-1\cdot(-1))\cdot b)\,, && \text{(P.1)}\\
&= a\cdot(1\cdot b)\,, && \text{(Lema 76)}\\
&= a\cdot b. && \text{(P.6)}
\end{aligned}
$$

Isto demonstra a primeira afirmação. Para provar a segunda, basta fazermos

$$
\begin{aligned}
(-a)\cdot b &= (-1\cdot a)\cdot b, && \text{(Lema 75)}\\
&= -1\cdot(a\cdot b)\,, && \text{(P.1)}\\
&= -(a\cdot b)\,, && \text{(Lema 75)}
\end{aligned}
$$

o que prova a segunda parte da segunda afirmação, e

$$
\begin{aligned}
(-a)\cdot b &= (-1\cdot a)\cdot b, && \text{(Lema 75)}\\
&= (a\cdot(-1))\cdot b, && \text{(P.4)}\\
&= a\cdot(-1\cdot b)\,, && \text{(P.1)}\\
&= a\cdot(-b)\,, && \text{(Lema 75)}
\end{aligned}
$$

que prova a primeira parte da segunda afirmação, concluindo a prova. ■

Definição 34 [Quadrado]**:**
Seja $a \in \mathbb{Z}$. Definimos o *quadrado* de a, denotado a^2, como o número inteiro que satisfaz $a^2 = a \cdot a$. ♠

Lema 78:
Seja $a \in \mathbb{Z}$. *É verdade que* $a^2 = 0 \Leftrightarrow a = 0$. □

Demonstração:
Suponhamos que $a^2 = a \cdot a = 0$. Pela Proposição 72, é preciso que $a = 0$. ■

Lema 79:
Seja $a \in \mathbb{Z}$. *Se* $a^2 = a$, *então* $a = 0$ *ou* $a = 1$. □

Demonstração:
Suponhamos, primeiramente, que $a = 0$. Então $0 \cdot 0 = 0$ e, pela Proposição 71, a equação realmente é satisfeita.

Suponhamos agora que $a \neq 0$. Então segue que:

$$
\begin{aligned}
a\cdot a &= 1\cdot a, && \text{(P.6)}\\
a &= 1. && \text{(P.7)}
\end{aligned}
$$

Assim vemos que, de fato, $a^2 = a \Rightarrow (a = 0 \vee a = 1)$. ■

Proposição 80:
A equação $a + x = b$ *possui solução única em* $\mathbb{Z}$. □

Demonstração:
Suponha que x e y, ambos inteiros, satisfaçam a equação. Então vale que $a + x = b$ e que $a + y = b$. Logo, $a + x = a + y$. Pela Proposição 68, $x = y$. ■

§6: Propriedades do Ordenamento

Proposição 81:
Seja $a \in \mathbb{Z}$. *Então* $a \leqslant 0 \Leftrightarrow 0 \leqslant (-a)$. □

Demonstração:

$$\begin{aligned} a &\leqslant 0, \\ -a + a &\leqslant -a + 0, && \text{(P.14)} \\ 0 &\leqslant -a + 0, && \text{(P.3)} \\ 0 &\leqslant -a. && \text{(P.2)} \end{aligned}$$

A volta é provada de maneira análoga, somando a aos dois lados da desigualdade e desenvolvendo a expressão para obter que $a \leqslant 0$. ■

Observação:
Note que, devido à Proposição 74, a Proposição 81 também implica que $0 \leqslant a \Leftrightarrow -a \leqslant 0$. ♣

Lema 82:
Seja $a \in \mathbb{Z}$. *Vale que* $a^2 = (-a)^2$. □

Demonstração:

$$\begin{aligned} (-a)^2 &= (-a) \cdot (-a), \\ &= (-1 \cdot a) \cdot (-1 \cdot a), && \text{(Lema 75)} \\ &= (a \cdot (-1)) \cdot (-1 \cdot a), && \text{(P.8)} \\ &= a \cdot ((-1) \cdot (-1 \cdot a)), && \text{(P.5)} \\ &= a \cdot ((-1 \cdot (-1)) \cdot a), && \text{(P.5)} \\ &= a \cdot (1 \cdot a), && \text{(Lema 76)} \\ &= a \cdot a, && \text{(P.6)} \\ &= a^2. \end{aligned}$$
■

Proposição 83:
Seja $a \in \mathbb{Z}$. *Se* $a = 0$, *então* $0 = a^2$. *Se não,* $0 < a^2$. □

Demonstração:
Se $a = 0$ o resultado é verdadeiro pela Proposição 71.
Suponhamos que $0 < a$. Então, usando P.15, sabemos que $0 \cdot a < a^2$ e, pela Proposição 71, obtemos que $0 < a^2$.
Finalmente, suponhamos que $a < 0$. Pela Proposição 81 temos que $0 < (-a)$. Conhecendo o Lema 82, percebe-se que caímos no caso em que $0 < a$, o que conclui a demonstração. ■

Proposição 84:
$0 < 1$. □

Demonstração:
Por P.6, $1 \cdot 1 = 1$, *i.e.*, $1^2 = 1$. Pela Proposição 83, $0 < 1^2$ e, portanto, $0 < 1$. ■

Lema 85:
Dados $a, b, c \in \mathbb{Z}$ *e* $d \in \mathbb{Z}_+^*$, *valem:*

i. $(a < b \wedge b < c) \Rightarrow a < c$;

ii. $a < b \Rightarrow a + c < b + c$;

iii. $a < b \Rightarrow a \cdot d < b \cdot d$. □

Demonstração: i. Sabemos que $(a < b \wedge b < c) \Rightarrow (a \leqslant b \wedge b \leqslant c)$. Logo, por P.12, $a \leqslant c$. É preciso que $a \neq c$, pois, caso contrário, ter-se-ia que $a \leqslant b \wedge b \leqslant a \Rightarrow b = a$, o que é falso por hipótese. Logo, $a < c$.

ii. Se $a < b$, então $a \leqslant b$. Por P.14 sabemos então que $a+c \leqslant b+c$. É preciso que $a+c \neq b+c$ pois, caso contrário, 68 nos daria que $a = b$, o que é falso por hipótese. Logo, $a+c < b+c$.

iii. Se $a < b$, então $a \leqslant b$. Por P.15 sabemos então que $a \cdot d \leqslant b \cdot d$. É preciso que $a \cdot d \neq b \cdot d$, pois, caso contrário, P.7 forneceria que $a = b$. Conclui-se que $a \cdot d < b \cdot d$. ■

Corolário 86:
Seja $a \in \mathbb{Z}$. *Vale que* $a < a + 1$. □

Demonstração:

$$\begin{aligned} 0 &< 1, && \text{(Proposição 84)} \\ a + 0 &< a + 1, && \text{(Lema 85.ii)} \\ a &< a + 1. \end{aligned}$$
■

Corolário 87:
$0 = \min \mathbb{Z}_+$. □

Demonstração:
Pela Proposição 84, $0 < 1$ e, portanto, $0 \leqslant 1$. Logo, por P.15, $0 \leqslant a, \forall\, a \in \mathbb{Z}_+$, o que nos fornece diretamente que $0 = \min \mathbb{Z}_+$. ■

Proposição 88:
Sejam $a, b \in \mathbb{Z}$; $a < b$. *Vale que* $-b < -a$. □

Demonstração:

$$\begin{aligned} a &< b, \\ -a - b + a &< -a - b + b, && \text{(Lema 85.ii)} \\ -b + 0 &< -a + 0, \\ -b &< -a. \end{aligned}$$
■

Corolário 89:
Sejam $a, b \in \mathbb{Z}$ *e* $c \in \mathbb{Z}_-^*$. *Então* $a < b \Rightarrow bc < ac$. □

Demonstração:
Como $c < 0$, seguirá da Proposição 81 que $-c > 0$. Pelo Lema 85.iii, vale então que $a < b \Rightarrow -ac < -bc$ (por Proposição 77). Aplicando a Proposição 88, concluímos que $bc < ac$. ■

Corolário 90:
Sejam $a, b \in \mathbb{Z}$; $a \leqslant b$. *Vale que* $-b \leqslant -a$. □

Demonstração:
Se $a < b$, então a afirmação é verdadeira pela Proposição 88. Se $a = b$, então a afirmação é trivialmente verdadeira. ■

Observação:

Nas últimas demonstrações foram emitidas as menções a algumas propriedades que devem ser familiares agora. ♣

Proposição 91:

Sejam $a, b \in \mathbb{Z}$. *Se* $a > 0$ *e* $ab > 0$, *então* $b > 0$. *O mesmo vale para a relação* $\leqslant$. □

Demonstração:

Suponha que $b = 0$. Então $ab = 0$, o que contraria a hipótese. Logo, $b \in \mathbb{Z}^*$. Suponha que $b < 0$. Então, pelo Corolário 89, $ab < 0$. Absurdo. Logo, por 31 P.13, $b > 0$.

A demonstração para a relação $\leqslant$ é análoga. ■

Corolário 92:

Sejam $a, b, c \in \mathbb{Z}$. *Se* $c > 0$ *e* $ac > bc$, *então* $a > b$. □

Como $ac > bc$, sabemos pelo Lema 85.ii que $(a - b)\,c > 0$. Como $c > 0$, vem da Proposição 91 que $a - b > 0$. Logo, usando o Lema 85.ii novamente, temos que $a > b$.

Notação:

Sejam $a, b \in \mathbb{Z}$. Como feito na demonstração da Proposição 88, utilizaremos a notação $b - a \equiv b + (-a)$ para nos referir à soma de b com o oposto de a. ♣

Lema 93:

Sejam $a, b, c, d \in \mathbb{Z}; a < b, c < d$. *Então* $a + c < b + d$. *Analogamente, se* $a \leqslant b, c \leqslant d$, *então* $a + c \leqslant b + d$. □

Demonstração:

Primeiramente, note que, como $c < d$, vem do Lema 85.ii que $0 < d - c$. Dito isso, veja que

$$
\begin{aligned}
&0 < 1, && \text{(Proposição 84)}\\
&0 < d - c, && \text{(Lema 85.iii)}\\
&b < b + d - c. && \text{(Lema 85.ii)}
\end{aligned}
$$

Como $a < b$, vale por P.12 que $a < b + d - c$. Usando Lema 85.ii, obtemos que $a + c < b + d$. A demonstração para $\leqslant$ é análoga e parte do fato de que $0 < 1 \Rightarrow 0 \leqslant 1$. ■

Teorema 94 [Propriedade Arquimediana em $\mathbb{Z}$]**:**

Sejam $a, b \in \mathbb{Z}_+^*$. $\exists\, n \in \mathbb{Z}_+^*; n \cdot a > b$. □

Demonstração:

Suponhamos, por absurdo, que existam $a, b \in \mathbb{Z}_+^*; \forall\, n \in \mathbb{Z}_+^*, na \leqslant b$. Por P.14, tem-se que $0 \leqslant b - na, \forall\, n \in \mathbb{Z}_+^*$, e, portanto, $\varnothing \subset S := \left\{b - na; n \in \mathbb{Z}_+^*\right\} \subseteq \mathbb{Z}_+$. Logo, por P.16, S possui mínimo. Seja $m \equiv \min S$.

Como $m \in S$, $m = b - pa$, para algum $p \in \mathbb{Z}_+^*$. Note que, como $a \in \mathbb{Z}_+^*$, decorre do Corolário 87 que $0 < a$. Considere o elemento de S dado por $m' = b - (p + 1)a$:

$$
\begin{aligned}
m' &= b - (p + 1)a,\\
&= b - pa - a,\\
&= m - a.
\end{aligned}
$$

Sabemos de P.10 que $m \leqslant m$ e do Lema 93 vem que $m \leqslant m + a$ (se $0 < a, 0 \leqslant a$). Usando o Lema 85.iii obtemos que $m - a \leqslant m$. Como $m - a = m' \in S$, obtemos que existe um elemento em S menor que o mínimo de S (pois sabemos que $m' \neq m$). Absurdo. ■

Teorema 95:

Todo conjunto não-vazio de números inteiros limitado inferiormente admite mínimo. □

Demonstração:

Seja A um tal conjunto. Seja m um minorante de A (sabemos que existe um tal m, pois A é limitado inferiormente). Então $m \leqslant a, \forall\, a \in A$ e, por P.14, $0 \leqslant a - m$.

Consideremos então o conjunto $S := \{a - m, a \in A\}$. Como $0 \leqslant a - m, \forall\, a \in A$, sabemos que $S \subseteq \mathbb{Z}+$. Logo, por P.16, sabemos que S admite mínimo. Como $\min S \in S$, podemos escrever $\min S = a_0 - m$, onde $a_0 \in A$.

É claro que $\min S \leqslant a - m, \forall\, a \in A$ e, portanto, $a_0 - m \leqslant a - m, \forall\, a \in A$. Usando P.14, temos que $a_0 \leqslant a, \forall\, a \in A$. Logo, como $a_0 \in A$, $a_0 = \min A$. ■

Teorema 96:

Todo conjunto não-vazio de números inteiros limitado superiormente admite máximo. □

Demonstração:

Seja A um tal conjunto. Seja m um majorante de A (sabemos que existe um tal m, pois A é limitado superiormente). Então $m \geqslant a, \forall\, a \in A$ e, por P.14, $0 \leqslant m - a$.

Consideremos então o conjunto $S := \{m - a, a \in A\}$. Como $0 \leqslant m - a, \forall\, a \in A$, sabemos que $S \subseteq \mathbb{Z}+$. Logo, por P.16, sabemos que S admite mínimo. Como $\min S \in S$, podemos escrever $\min S = m - a_0$, onde $a_0 \in A$.

É claro que $\min S \leqslant m - a, \forall\, a \in A$ e, portanto, $m - a_0 \leqslant m - a, \forall\, a \in A$. Usando P.14, temos que $-a_0 \leqslant -a, \forall\, a \in A$. Pelo Corolário 90, $a_0 \geqslant a, \forall\, a \in A$. Logo, como $a_0 \in A$, $a_0 = \max A$. ■

Lema 97:

Seja $n \in \mathbb{Z}$. *Se* $0 \leqslant n \leqslant 1$, *então ou* $n = 0$ *ou* $n = 1$. □

Demonstração:

Primeiramente, ressalta-se que há sentido em escrever $0 \leqslant n \leqslant 1$, visto que $0 < 1$ pelo Proposição 84.

Dito isso, suponhamos por absurdo que $0 \neq n \neq 1$. Então o conjunto S, definido segundo

$$S := \{p \in \mathbb{Z}; 0 < p < 1\},$$

é não-vazio e, por P.16, possui mínimo, visto que 0 é minorante de S. Seja $m \equiv \min S$.

Como $m \in S$, vale que $0 < m < 1$. Usando P.15, temos que $0 < m^2 < m$. Como $m < 1$, por P.12 sabemos que $0 < m^2 < 1$ e, portanto, $m^2 \in S$. Contudo, isso nos diz que existe um elemento em S, m^2, que é menor que o mínimo de S. Absurdo. ■

Teorema 98:

Sejam $a, b \in \mathbb{Z}$. *Se* $a \leqslant b \leqslant a + 1$, *então ou* $b = a$ *ou* $b = a + 1$. □

Demonstração:

Se $a \leqslant b \leqslant a + 1$ (note que essa expressão faz sentido, pois $a < a + 1$ pelo Corolário 86), então P.14 nos fornecerá que $0 \leqslant b - a \leqslant 1$. Do Lema 97 segue que

$$(b - a = 0 \vee b - a = 1) \Rightarrow (b = a \vee b = a + 1)\,. \quad ■$$

Notação:

Seja S um conjunto finito. Denotaremos a cardinalidade, *i.e.*, o número de elementos, de S por $|S|$. ♣

Corolário 99:

Seja $A \subset \mathbb{Z}$ *um conjunto não-vazio limitado superiormente por* a *e inferiormente por* b. *Então* A *contém no máximo* $a - b + 1$ *elementos.* □

Demonstração:

Pelo Teorema 95 e pelo Teorema 96, sabemos que A admite máximo e mínimo. Como

a é majorante de A, é maior ou igual A todo elemento de A e, em particular, $a \geqslant \max A$. Analogamente, $b \leqslant \min A$.

Seja $S := \{n \in \mathbb{Z}; b \leqslant n \leqslant a\}$. Claramente, $A \subset S$ e, portanto, $|A| \leqslant |S|$.

$b \in S$ e, portanto, $|S| \geqslant 1$. Pelo Teorema 98, o próximo possível elemento de S é $b+1$, se este for menor ou igual a a. Supondo que seja, teremos que $|S| \geqslant 1+1$, pois $|\{b, b+1\}| = 1+1$, e este conjunto é subconjunto de S. Prosseguindo com esta sequência lógica, tem-se que se $b \leqslant b+n \leqslant a$, então $b+n \in S$, tal como todos os seus antecessores maiores ou iguais a b, e segue que $|S| \geqslant n+1$.

Como $a = b + a - b \in S$, valerá então que $|S| \geqslant a - b + 1$. No entanto esta precisa ser a cardinalidade de S pois, ao chegar em a, teremos passado por todos os elementos de S. Caso contrário, isto implicaria na existência de um elemento c de S que obedece $b+n < c < b+n+1$, visto que contamos todos os elementos da forma $b+n$ para $0 \leqslant n \leqslant a-b$. Como isso é impossível pelo Teorema 98, concluímos que $|S| = a - b + 1$. Como $|A| \leqslant |S|$, concluímos que $|A| \leqslant a - b + 1$. ■

Definição 35 [Inteiros Consecutivos]**:**

Seja $\{a_i\}_{i=1}^{n}$, $n \in \mathbb{Z}_+^*$ um conjunto de números inteiros. Diremos que os inteiros a_i são *consecutivos* se, e somente se, $a_{i+1} = a_i + 1, \forall\, i \in \{i\}_{i=1}^{n-1}$. ♠

§7: Valor Absoluto

Definição 36 [Valor Absoluto]**:**

Seja $a \in \mathbb{Z}$. Definimos o *valor absoluto* de a, denotado por $|a|$, da seguinte maneira:

$$|a| := \begin{cases} a, \text{se } a \geqslant 0 \\ -a, \text{se } a < 0 \end{cases}.$$

Também usaremos a nomenclatura *módulo* de a ao falar sobre $|a|$. ♠

Proposição 100:

Seja $a \in \mathbb{Z}$. *Então* $|a| \geqslant 0$ *e* $|a| = 0 \Leftrightarrow a = 0$. □

Demonstração:

Suponhamos primeiramente que $a > 0$. Então $|a| = a$ e, portanto, $|a| > 0$.

Suponhamos então que $a < 0$. Então $|a| = -a$ e, pelo Corolário 90 ter-se-á que $|a| > 0$.

Se $a = 0$, então $|0| = 0$. Sabemos que $|0| \Rightarrow a = 0$, pois, caso a não fosse nulo, ter-se-ia pelo início desta demonstração que $|a| \neq 0$. Assim concluímos a prova. ■

Proposição 101:

Seja $a \in \mathbb{Z}$. *Então vale que* $-|a| \leqslant a \leqslant |a|$. □

Demonstração:

Primeiramente, note que a Proposição 100, em conjunto com o Corolário 90 e P.12, faz com que o enunciado faça sentido, visto que, de fato, $-|a| \leqslant |a|$.

Suponhamos $a \geqslant 0$. Então $|a| = a$ e, portanto, $|a| \geqslant a$. Além disso, ter-se-á pelo Corolário 90 que $-|a| \leqslant 0$. Logo, por P.12, vale que $-|a| \leqslant a$.

Suponhamos então que $a < 0$. Vale que $|a| = -a$ e, pelo Corolário 90, que $|a| > 0$. Por P.12 temos que $|a| \geqslant a$. Além disso, como $-|a| = -a$, é simples constatar qie $-|a| \leqslant a$, o que conclui a demonstração. ■

Proposição 102:

$|-a| = |a|, \forall\, a \in \mathbb{Z}$. □

Demonstração:

Sem perda de generalidade, suponhamos $a \geqslant 0$. Então $|a| = a$. Pelo Corolário 90, sabemos que $-a \leqslant 0$ e, portanto, $|-a| = -(-a) = a$, pela Proposição 74. Logo, $|a| = |-a|$. ■

Notação:

Escreveremos a expressão $(a = b \vee a = -b)$ numa forma compactada como $a = \pm b$. ♣

Corolário 103:

Sejam $a, b \in \mathbb{Z}$. $|a| = |b| \Leftrightarrow a = \pm b$. □

Demonstração:

A volta decorre trivialmente da Proposição 102.

Tem-se, por hipótese, que $|a| = |b|$. Suponhamos que a e b são ambos não-negativos ou ambos negativos. Então ou $a = b$ ou $-a = -b$. De qualquer forma, resultará que $a = b$, provando o enunciado.

Suponhamos, sem perda de generalidade, que a seja negativo e b seja não-negativo. Então $-a = b$ e, portanto $a = -b$. Assim concluímos a demonstração. ■

Proposição 104:

$|a \cdot b| = |a| \cdot |b|, \forall\, a, b \in \mathbb{Z}$. □

Demonstração:

Se a ou b for nulo, tem-se que o enunciado é trivialmente verdadeiro devido à Proposição 71. Logo, provaremos os casos em que nenhum dos dois é nulo.

A princípio, suponhamos sem perda de generalidade que $a > 0$ e $b < 0$. Então, pelo Corolário 89, $ab < 0$. Logo, segue que

$$\begin{aligned} |ab| &= -ab, && \text{(Definição 36)} \\ &= a(-b), && \text{(Proposição 77)} \\ &= |a||b|. && \text{(Definição 36)} \end{aligned}$$

Suponhamos a seguir que a e b são ambos positivos. É simples constatar que

$$\begin{aligned} |ab| &= ab, && \text{(Definição 36)} \\ &= |a||b|, && \text{(Definição 36)} \end{aligned}$$

pois o Lema 85.iii garante que $ab > 0$.

Finalmente, suponhamos que a e b são negativos. Pelo Corolário 89, sabemos que $ab > 0$. Veja então que

$$\begin{aligned} |ab| &= ab, && \text{(Definição 36)} \\ &= (-|a|)(-|b|), && \text{(Definição 36)} \\ &= |a||b|. && \text{(Proposição 77)} \end{aligned}$$

Assim concluímos a demonstração. ■

Teorema 105 [Desigualdade Triangular]**:**

Sejam $a, b \in \mathbb{Z}$. *Então vale que* $|a + b| \leqslant |a| + |b|$. □

Demonstração:

Da Proposição 101, sabemos que $-|a| \leqslant a \leqslant |a|$ e que $-|b| \leqslant b \leqslant |b|$. Com estas duas expressões, podemos utilizar Lema 93 para obter que

$$-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|.$$

Se $(a+b) \geqslant 0$, então
$$|a+b| = a+b \leqslant |a|+|b|.$$

Se $(a+b) < 0$, então podemos usar o Corolário 89 para multiplicar a desigualdade por -1 e obter que
$$|a|+|b| \geqslant -(a+b) \geqslant -(|a|+|b|)\,.$$

Como $|a+b| = -(a+b)$, está provado que
$$|a+b| = -(a+b) \leqslant |a|+|b|.$$ ■

Proposição 106:
Sejam $a, b \in \mathbb{Z}$. $||a|-|b|| \leqslant |a-b|$. □

Demonstração:
Sabemos, do Teorema 105, que dados $b, a-b \in \mathbb{Z}$ vale que
$$\begin{aligned} |a-b+b| &\leqslant |a-b|+|b|, \\ |a|-|b| &\leqslant |a-b|. \end{aligned}$$

Se $|a|-|b| \geqslant 0$, então $||a|-|b|| = |a|-|b|$ e a demonstração está concluída.

Se $|a|-|b| < 0$, então $||a|-|b|| = |b|-|a|$. Perceba que o mesmo argumento utilizado anteriormente fornecerá que $|b|-|a| \leqslant |b-a|$. Pelo Corolário 89, $|b|-|a| > 0$, o que nos leva ao caso anterior e mostra que
$$\begin{aligned} ||a|-|b|| &\leqslant |b-a|, \\ ||a|-|b|| &\leqslant |a-b|. && \text{(Proposição 102)} \end{aligned}$$

Isso conclui a demonstração. ■

§8: Princípío de Indução

Teorema 107 [Princípio de Indução Fraco]**:**
Seja $a \in \mathbb{Z}$ *e* $S \subset \mathbb{Z}$ *um conjunto tal que* $a \leqslant x, \forall\, x \in S$. *Se forem verdadeiras ambas as propriedades*

i. $a \in S$,

ii. $k \in S \Rightarrow k+1 \in S, \forall\, k \geqslant a$,

então $S = \{k \in \mathbb{Z}; a \leqslant k\}$. □

Demonstração:
Suponhamos que a afirmação seja falsa. Então o conjunto S', definido segundo
$$S' := \{k \in \mathbb{Z}; a \leqslant k\} \setminus S,$$
é não-vazio e limitado inferiormente (por a). Logo, pelo Teorema 95, S' admite mínimo. Denotemos $m \equiv \min S'$.

Como $a \in S$, $a \notin S'$. Visto que a é minorante de S', mas não pertence ao conjunto, sabemos que $a < m$. Sabemos do Corolário 86 que $m-1 < m$ e, portanto, sabemos do Teorema 98 que $a \leqslant m-1 < m$, o que fornece o fato de que ou $m-1 \in S'$ ou $m-1 \in S$. Como $m-1 < m = \min S'$, vemos que $m-1 \in S$. Usando a segunda hipótese do enunciado, temos que $m-1 \in S \Rightarrow m-1+1 = m \in S$. Como $m \in S'$, isso é absurdo. ■

Corolário 108:
Seja $a \in \mathbb{Z}$ *e* $P(n)$ *uma proposição acerca de um número inteiro* n. *Se forem verdadeiras ambas as propriedades*

i. $P(a)$,

ii. $P(k) \Rightarrow P(k+1), \forall\, k \geqslant a$,

então $P(k)$ *é verdadeira* $\forall\, k \geqslant a$. □

Demonstração:
Considere o conjunto $P := \{k \in \mathbb{Z}; P(k) \text{ é verdadeira}\}$. Pelo Teorema 107,

$$P = \{k \in \mathbb{Z}; a \leqslant k\}$$

e, portanto, $P(k)$ é verdadeira $\forall\, k \geqslant a$. ■

Teorema 109 [Princípio de Indução Forte]**:**
Seja $a \in \mathbb{Z}$ *e* $S \subset \mathbb{Z}$ *um conjunto tal que* $a \leqslant x, \forall\, x \in S$. *Se forem verdadeiras ambas as propriedades*

i. $a \in S$,

ii. $\{i\}_{i=a}^{k} \subset S \Rightarrow k+1 \in S, \forall\, k \geqslant a$,

então $S = \{k \in \mathbb{Z}; a \leqslant k\}$. □

Demonstração:
Seja $S' := \left\{k \in \mathbb{Z}, k \geqslant a; \{i\}_{i=a}^{k} \subset S\right\}$. Como $a \in S$ por hipótese, $\{a\} \subset S$ e, portanto, $a \in S'$.

Suponhamos que um dado inteiro $k \in S'$. Então $\{i\}_{i=a}^{k} \subset S$. Por hipótese, isso implica que $k+1 \in S$. Logo, vale que $\{i\}_{i=a}^{k+1} \subset S$ e, portanto, que $k+1 \in S'$.

Pelo Teorema 107, isso implica que $S' = \{k \in \mathbb{Z}; a \leqslant k\}$. Logo, $\{i\}_{i=a}^{k} \subset S, \forall\, k \geqslant a$, implicando que $S = \{k \in \mathbb{Z}; a \leqslant k\}$. ■

Escólio:
O fato de que o Teorema 107 implica o Teorema 109 é notável. Provar-se-á adiante que, além disso, ambos os Princípios são equivalentes entre si e ao Princípio da Boa Ordem. Isto é, assumindo-se um destes três princípios, pode-se deduzir os outros dois. ♣

Fazer esta demonstração

Corolário 110:
Seja $a \in \mathbb{Z}$ *e* $P(n)$ *uma proposição acerca de um número inteiro* n. *Se forem verdadeiras ambas as propriedades*

i. $P(a)$,

ii. $(P(m), \forall\, m; a \leqslant m \leqslant k) \Rightarrow P(k+1), \forall\, k \geqslant a$,

então $P(k)$ *é verdadeira* $\forall\, k \geqslant a$. □

Demonstração:
Considere o conjunto $P := \{k \in \mathbb{Z}; P(k) \text{ é verdadeira}\}$. Pelo Teorema 109,

$$P = \{k \in \mathbb{Z}; a \leqslant k\}$$

e, portanto, $P(k)$ é verdadeira $\forall\, k \geqslant a$. ■

Definição 37 [Potências]**:**
Seja $a \in \mathbb{Z}$. Definimos as *potências* de a com expoente positivo por

i. $a^1 := a$;

ii. $a^{n+1} := a \cdot a^n, \forall n \geqslant 0$.

Ademais, se $a \neq 0$, definimos $a^0 := 1$ por conveniência. ♠

Lema 111:
Todas as potências de 0 *são nulas.* □

Demonstração:
A $n+1$-ésima potência de 0 é dada por $0 \cdot 0^n, \forall n \in \mathbb{Z}_+^*$. Logo, pela Proposição 71, $0^{n+1} = 0$ independentemente do valor de 0^n. Conclui-se que $0^n = 0, \forall n > 1$. Como $0^1 = 0$ por definição, está concluída a demonstração. ■

Proposição 112:
Sejam $a, b \in \mathbb{Z}$ *e sejam* $m, n \in \mathbb{Z}_+$. *Então valem as seguintes propriedades, excluindo os casos em que ter-se-ia elementos da forma* 0^0*:*

i. $a^m a^n = a^{m+n}$;

ii. $(a^m)^n = a^{mn}$;

iii. $(ab)^m = a^m b^m$. □

Demonstração:
Para o caso em que a ou b é nulo (e m e n não o são), temos que todas as propriedades enunciadas são verdadeiras pelo Lema 111 e pela Proposição 71.

i. Fixe $a \in \mathbb{Z}^*$ e $m \in \mathbb{Z}_+$. Queremos provar que, $\forall n \in \mathbb{Z}_+$, vale a seguinte propriedade: $a^m a^n = a^{m+n}$. Prosseguiremos por indução.

   Tomemos $n = 0$. Então $a^m a^0 = a^m$ pela Definição 37. Suponhamos agora que a propriedade vale para um inteiro não-negativo n. Então seguirá que:

$$\begin{aligned} a^m a^{n+1} &= a^m a^n a^1, && \text{(Definição 37)} \\ &= a^{m+n} a^1, && \text{(hipótese de indução)} \\ &= a^{m+n+1}. && \text{(Definição 37)} \end{aligned}$$

   Segue do Corolário 108 que a propriedade vale para todo inteiro não-negativo n., concluindo a demonstração do primeiro enunciado.

ii. Fixe $a \in \mathbb{Z}^*$ e $m \in \mathbb{Z}_+$. Queremos provar que, $\forall n \in \mathbb{Z}_+$, vale a seguinte propriedade: $(a^m)^n = a^{mn}$. Prosseguiremos por indução.

   Tomemos $n = 0$. Então $(a^m)^0 = 1 = a^{0 \cdot m}$ pela Definição 37 e pela Proposição 71. Suponhamos então que vale a propriedade para um inteiro não-negativo n. Seguirá então que

$$\begin{aligned} (a^m)^{n+1} &= (a^m)^n (a^m)^1, && \text{(Definição 37)} \\ &= (a^{mn})(a^m)^1, && \text{(hipótese de indução)} \\ &= a^{mn} a^m, && \text{(Definição 37)} \\ &= a^{mn+m}, && \text{(provado acima)} \\ &= a^{m(n+1)}. \end{aligned}$$

   Novamente, segue do Corolário 108 que a propriedade é valida para todo inteiro não-negativo, o que encerra a prova do segundo enunciado.

iii. Fixe $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}_*$. Queremos provar que, $\forall\, m \in \mathbb{Z}_+$, vale a seguinte propriedade: $(ab)^m = a^m b^m$. Prosseguiremos por indução. Tomando $m = 0$, o enunciado decorre trivialmente da Definição 37. Suponhamos então que ele é válido para um m inteiro não-negativo. Decorre que

$$\begin{aligned}
(ab)^{m+1} &= (ab)^m (ab)^1, && \text{(Definição 37)}\\
&= a^m b^m (ab)^1, && \text{(hipótese de indução)}\\
&= a^m b^m ab, && \text{(Definição 37)}\\
&= a^m a b^m b, &&\\
&= a^{m+1} b^{m+1},. && \text{(Definição 37)}
\end{aligned}$$

Finalmente, o Corolário 108 nos fornece mais uma vez que o enunciado é válido para todo m inteiro não-negativo, concluindo a prova.

■

Observação: o fim precoce deste capítulo se deve ao fato de que a bibliografia [4] trata, após a seção sobre o PIF, do Teorema do Binômio, que obviamente depende da definição de divisão. É portanto um tema que deve ser tratado a posteriori, bem como as somas de PA e PG, que também resultam em identidades expressíveis apenas com notação fracionária. Além disso, não se deve ignorar o fato de que toda a construção feita até cá foi abstrata, ignorando, por exemplo, o número 2 em notação decimal, usando-o apenas na definição de quadrado.

Capítulo 3

Divisão de Inteiros

Um número primo é aquele que é medido apenas pela unidade.

Os Elementos, Livro VII
Euclides

§9: Características Elementares da Divisão

Definição 38 [Divisibilidade]**:**
Sejam $a, b \in \mathbb{Z}$. Diremos que b é *divisível* por a, ou que a *divide* b, se, e somente se, existir $x \in \mathbb{Z}$ tal que $a \cdot x = b$. Neste caso, escreveremos $a \mid b$. Se a não dividir b, escreveremos $a \nmid b$. ♠

Proposição 113:
Sejam $a, b \in Z; a \mid b$. *Se* $a \neq 0, \exists!\, x \in \mathbb{Z}; a \cdot x = b$. □

Demonstração:
Suponha que x e y, ambos inteiros, satisfaçam a equação, *i.e.*, $a \cdot x = b$ e $a \cdot y = b$. Então segue que

$$\begin{aligned} a \cdot x &= a \cdot y, \\ x &= y. \end{aligned} \tag{P.7}$$

Isto conclui a demonstração. ■

Observação:
Perceba que $0 \mid b \Leftrightarrow b = 0$, devido à Proposição 71. Além disso, esta mesma Proposição faz com que todos os inteiros sejam solução da equação $0 \cdot x = 0$. ♣

Definição 39 [Divisor]**:**
Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$. Diremos que a é *divisor* de b se, e somente se, $a \mid b$. ♠

Proposição 114:
Sejam $a, b \in \mathbb{Z}^*$. *Se* $a \mid b$, *então* $|a| \leqslant |b|$. □

Demonstração:
Como $a \mid b, \exists!\, c \in \mathbb{Z}; a \cdot c = b$, pela Proposição 113. Logo, $|ac| = |b|$. Pela Proposição 104, $|a||c| = |b|$.

Sabemos que $|c| \neq 0$ pois, se o fosse, $|b|$ também o seria, mas isso é falso por hipótese. Logo, segue da Proposição 100 que $|c| > 1$. Devido à mesma Proposição, podemos aplicar o Lema 85.iii para multiplicar os dois lados da inequação por $|a|$. Logo, $|c||a| > |a|$. Como $|c||a| = |b|$, vemos que $|b| > |a|$, encerrando a demonstração. ■

Corolário 115:

Os únicos divisores de 1 *são* 1 *e* -1. □

Demonstração:

Suponha que um inteiro não-nulo a divide 1. Então, pela Proposição 114, $|a| \leqslant |1|$. Da Proposição 100, sabemos que $0 < |a| \leqslant |1|$. Logo, pelo Lema 97, teremos que $|a| = 1 = |1|$. Conclui-se então, do Corolário 103, que $a = \pm 1$. ■

Corolário 116:

Sejam $a, b \in \mathbb{Z}^*$. *Se* $a \mid b$ *e* $b \mid a$, *então* $a = \pm b$. □

Demonstração:

Basta fazer

$$\begin{aligned} a \mid b &\Rightarrow |a| \leqslant |b|, && \text{(Proposição 114)} \\ b \mid a &\Rightarrow |b| \leqslant |a|, && \text{(Proposição 114)} \\ (|b| \leqslant |a| \wedge |a| \leqslant |b|) &\Rightarrow |b| = |a|, && \text{(P.11)} \\ |b| = |a| &\Rightarrow a = \pm b. && \text{(Corolário 103)} \end{aligned}$$

Isto conclui a demonstração. ■

Definição 40 [Quociente]**:**

Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$ tais que $a \mid b$. Definimos o *quociente* de b, que será dito o *dividendo*, por a, que será dito o *divisor*, como o número inteiro c que resolve a equação $a \cdot c = b$. Em geral, denotaremos o quociente de b por a como

$$b/a \equiv \frac{b}{a}.$$ ♠

Observação:

A noção de quociente de dois inteiros é bem definida devido à Proposição 113. ♣

Proposição 117:

Sejam $a \in \mathbb{Z}^*, b, c, d \in \mathbb{Z}$. *Valem as seguintes propriedades:*

i. $a \mid a$;

ii. *para* $b \neq 0$, $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$;

iii. *para* $c \neq 0$, $(a \mid b \wedge c \mid d) \Rightarrow ac \mid bd$;

iv. $(a \mid b \wedge a \mid c) \Rightarrow a \mid (b + c)$;

v. $a \mid b \Rightarrow a \mid mb, \forall\, m \in \mathbb{Z}$. □

Demonstração:

Far-se-á a demonstração item a item:

i. $a \cdot 1 = a \Rightarrow a \mid a$;

ii. de $a \mid b$, temos que $a \cdot x = b$, para algum x inteiro. De $b \mid c$, temos que $b \cdot y = c$, para algum y inteiro. Substituindo a primeira expressão na segunda, segue que $a \cdot xy = c$. Logo, $a \mid c$;

iii. de $a \mid b$, sabemos que $a \cdot x = b$, para algum $x \in \mathbb{Z}$. De $c \mid d$, sabemos que $c \cdot y = d$, para algum $y \in \mathbb{Z}$. É simples ver que $ac \cdot xy = bd$ e, portanto, $ac \mid bd$;

iv. de $a \mid b$, sabemos que $a \cdot x = b$, para algum $x \in \mathbb{Z}$. De $a \mid c$, sabemos que $a \cdot y = c$, para algum $y \in \mathbb{Z}$. Somando as duas expressões, segue que $a \cdot (x + y) = (b + c)$ e, portanto, $a \mid (b + c)$;

v. de $a \mid b$, sabemos que $a \cdot x = b$, para algum $x \in \mathbb{Z}$. Multiplicando por m em ambos os lados, tem-se que $a \cdot mx = mb$. Logo, $a \mid mb$. ■

Corolário 118:
Sejam $a, b, c \in \mathbb{Z}$, $a \neq 0$, *tais que* $a \mid b$ *e* $a \mid c$. *Então* $a \mid (mb + nc)\,, \forall\, m, n \in \mathbb{Z}$. □

Demonstração:
Perceba que

$$a \mid b \Rightarrow a \mid mb, \forall\, m \in \mathbb{Z}, \qquad \text{(Proposição 117.v)}$$
$$a \mid c \Rightarrow a \mid nc, \forall\, n \in \mathbb{Z}, \qquad \text{(Proposição 117.v)}$$
$$(a \mid mm \wedge a \mid nc) \Rightarrow a \mid (mb + nc)\,. \forall\, n \in \mathbb{Z}, \qquad \text{(Proposição 117.iv)}$$

Isto conclui a prova. ■

Corolário 119:
Sejam $a \in \mathbb{Z}^*, b, c, d \in \mathbb{Z}$. *Valem as seguintes propriedades:*

i.
$$\frac{a}{a} = 1;$$

ii. *para* $b \neq 0$,
$$\frac{b}{a} \cdot \frac{c}{b} = \frac{c}{a};$$

iii. *para* $c \neq 0$,
$$\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac};$$

iv.
$$\frac{b}{a} + \frac{c}{a} = \frac{b + c}{a};$$

v.
$$m \cdot \frac{b}{a} = \frac{mb}{a}, \forall\, m \in \mathbb{Z}.$$ □

Demonstração:
Cada enunciado decorre da demonstração do enunciado de número equivalente na Proposição 117. ■

Proposição 120:
Sejam $a, b \in \mathbb{Z}^*$, $c \in \mathbb{Z}$. *Então vale que* $a \mid c \Leftrightarrow ab \mid cb$. □

Demonstração:

$\Rightarrow$: se $a \mid c$, sabemos que $a \cdot x = c$, para algum $x \in \mathbb{Z}$. Multiplicando em ambos os lados por b, temos que $ab \cdot x = cb$ e, portanto, $ab \mid cb$. $\Leftarrow$: basta reverter o argumento com auxílio de P.7. ■

Corolário 121:

Sejam $a, b \in \mathbb{Z}^*$, $c \in \mathbb{Z}$. *Então vale que*

$$\frac{c}{a} = \frac{b}{b} \cdot \frac{c}{a}. \qquad \square$$

Demonstração:

Foi provado na demonstração da Proposição 120. Além disso, o Corolário 119.i garante que $b/b = 1$, o que torna fornece um argumento alternativo. ■

Proposição 122:

Sejam $a, b \in \mathbb{Z}$, $a \neq 0$. *Se* $a \mid b$, *então* $(-a) \mid b$, $a \mid (-b)$ *e* $(-a) \mid (-b)$. □

Demonstração:

Como $a \mid b$, sabemos que $a \cdot x = b$, para algum $x \in \mathbb{Z}$. Teremos então que

$$\begin{aligned} -a \cdot (-x) = b &\Rightarrow (-a) \mid b, \\ a \cdot (-x) = -b &\Rightarrow a \mid (-b)\,, \\ -a \cdot (x) = -b &\Rightarrow (-a) \mid (-b)\,. \end{aligned} \qquad ■$$

§10: O Algoritmo da Divisão

Lema 123:

Sejam $a, b \in \mathbb{Z}_+$, $a \neq 0$. *Então existem inteiros* q *e* r *que satisfazem* $qa + r = b$, *com* $0 \leqslant r < a$. □

Demonstração:

Seja $S := \{b - ax; x \in \mathbb{Z}, b - ax \geqslant 0\}$. Perceba que S é não vazio, pois $x = 0$ implica que $b - ax = b \geqslant 0$.

Podemos então aplicar P.16 para obter que S admite mínimo. Seja $r = \min S$. Visto que $r \in S$, sabemos que $r = b - aq \geqslant 0$, para algum $q \in \mathbb{Z}$.

Resta provar que $0 \leqslant r < a$. Como $r \in S$, sabemos que r é não-negativo, sendo apenas necessário provar que $r < a$. Suponhamos que não. Então $r = b - aq \geqslant a \Rightarrow b - a(q+1) = r - a \geqslant 0$. Logo, $r - a \in S$. Como $a > 0$, vale pela Proposição 88 que $-a < 0$ e, portanto $-a \leqslant 0$. Seguirá então que:

$$\begin{aligned} r &\leqslant r, \\ r - a &\leqslant r, \\ r - a &\leqslant \min S. \end{aligned}$$

Visto que $a \neq 0$, existe um elemento em S estritamente menor que o mínimo de S. Absurdo. Logo, é preciso que $r < a$. ■

Teorema 124 [Algoritmo da Divisão]**:**

Sejam $a, b \in \mathbb{Z}$, $a \neq 0$. *Existem inteiros* q, r *únicos, com* $0 \leqslant r < |a|$, *satisfazendo* $b = aq + r$. □

Demonstração:

Provar-se-á a princípio a existência de tais inteiros q e r. Tendo-a em mãos, será demonstrada a unicidade.

Tomemos primeiramente o caso em que $a > 0$. Se $b \geqslant 0$, a existência de q e r é garantida pelo Lema 123. Consideremos então o caso em que $b < 0$. Pelo Lema 123, existem inteiros q' e r' que satisfazem

$$|b| = q'a + r', 0 \leqslant r' < a.$$

Se $r' = 0$, teremos que

$$\begin{aligned} -b &= q'a, \\ b &= -q'a. \end{aligned}$$

Logo, vale o enunciado. Se $r' > 0$, segue então que

$$\begin{aligned} -b &= q'a + r', \\ b &= -q'a - r', \\ b &= -\left(q' + 1\right) a + \left(a - r'\right). \end{aligned}$$

Perceba que $0 < a - r' < a$, sendo que a primeira relação segue de que $r' < a$ e a segunda de que $r' > 0$. Desta forma, o enunciado também se verifica para este caso.

Abordemos então o caso em que $a < 0$. Independentemente de b, a primeira parte desta demonstração garante a existência de q' e r' inteiros respeitando a equação

$$b = q'|a| + r', 0 \leqslant r' < |a|.$$

Segue então que

$$\begin{aligned} b &= q'\left(-a\right) + r', \\ b &= -q'a + r'. \end{aligned}$$

Logo, o enunciado também se sustenta neste caso.

Resta por fim demonstrar a unicidade de q e r. Suponha que os pares ordenados (q, r) e (q', r') satisfazem as condições anteriormente explicitadas para a e b fixados. Logo, vale que

$$\begin{cases} b = qa + r, 0 \leqslant r < |a| \\ b = q'a + r', 0 \leqslant r' < |a| \end{cases} \Rightarrow qa + r = q'a + r'.$$

Suponhamos, sem perda de generalidade, que $r' \geqslant r$. Da equação anterior, sabemos que $\left(q - q'\right) a = r' - r$. Além disso, como $0 \leqslant r, r' < |a|$, sabemos também que $r' - r < |a|$. È claro, então, que $\left(q - q'\right) a < |a|$.

Como, por hipótese, $r' \geqslant r$, é claro que $r' - r = \left(q - q'\right) a \geqslant 0$. Logo, tem-se que

$$\begin{aligned} 0 &\leqslant \left(q - q'\right) a < |a|, && \\ 0 &\leqslant |\left(q - q'\right) a| < |a|, && \text{(Definição 36)} \\ 0 &\leqslant |\left(q - q'\right)||a| < |a|, && \text{(Proposição 104)} \\ 0 &\leqslant |\left(q - q'\right)| < 1, && \text{(Corolário 92)} \\ \left(q - q'\right) &= 0. && \text{(Lema 97)} \end{aligned}$$

Assim, vemos que $q = q'$. Vemos também que $r' - r = 0 \cdot a = 0$. Logo, $r = r'$ e, portanto, os inteiros q e r definidos no enunciado são, de fato, únicos. ■

Definição 41 [Resto]:

Sejam $a, b \in \mathbb{Z}, a \neq 0$. Os números q e r que satisfazem $b = aq + r$ são chamados, respectivamente, de *quociente* e *resto* da divisão de b por a. Note que isso estende a definição de quociente dada na Definição 40. ♠

Notação:

Usaremos as notações a/b e $\frac{a}{b}$ para o quociente da divisão de a por b apenas quando o resto da divisão de a por b for nulo. ♣

Proposição 125:

Sejam $a, b \in \mathbb{Z}$, $a \neq 0$. a *dividirá* b *se, e somente se, o resto da divisão de* b *por* a *for nulo.* □

Demonstração:

Suponhamos que $a \mid b$. Então $\exists\, q \in \mathbb{Z}; aq = b$. Pelo Teorema 124, vale que o resto e o quociente da divisão de b por a são únicos e, portanto, vemos que tal resto é, de fato, nulo.

Suponhamos agora que o resto da divisão de b por a é nulo. Então $b = qa + 0 = qa$ para algum $q \in \mathbb{Z}$. Logo, da Definição 38, vale que $a \mid b$. ■

Lema 126:

Sejam $a, b \in \mathbb{Z}$, $a \neq 0$, *e seja* r *o resto da divisão de* b *por* a. *Se* $r \neq a - 1$, *então o resto da divisão de* $b + 1$ *por* a *é* $r + 1$. *Se* $r = a - 1$, $a \mid b + 1$. □

Demonstração:

Suponhamos, a princípio, que $r \neq a - 1$. Então vale que

$$\begin{aligned} b &= qa + r, \\ b + 1 &= qa + (r + 1)\,. \end{aligned}$$

Como $0 \leqslant r < a - 1$, é claro que $1 \leqslant r + 1 < a$. Pelo Teorema 124, o quociente e o resto de uma divisão são únicos. Logo, $r + 1$ é, de fato, o resto da divisão de $b + 1$ por a.

Suponhamos que $r = a - 1$. Então teremos que

$$\begin{aligned} b &= qa + a - 1, \\ b + 1 &= (q + 1)\, a. \end{aligned}$$

Logo, vemos que $a \mid b + 1$, encerrando a demonstração. ■

Proposição 127:

Seja $\{a_i\}_{i=1}^{n}$, $n \in \mathbb{Z}, n \geqslant 1$ *um conjunto de inteiros consecutivos. Então* $\exists!\, i \in \{i\}_{i=1}^{n}; n \mid a_i$. □

Demonstração:

Pelo Teorema 124, sabemos que,

$$\forall\, i \in \{i\}_{i=1}^{n}, \exists!\, q_i, r_i \in \mathbb{Z}, 0 \leqslant r_i < n; a_i = q_i n + r_i.$$

Consideremos a princípio o caso em que r_1 é nulo. Então, pela Proposição 125, vemos que $n \mid a_1$, provando a validade do enunciado neste caso.

Consideremos agora os casos em que $0 < r_1 \leqslant n - 1$. Pelo Lema 126, $r_{1+1} = r_1 + 1$. Reiterando o processo, teremos que ou $n \mid a_{1+1}$, ou $0 < r_{1+1} \leqslant n - 1$. Prosseguindo com este método, eventualmente atingiremos que $r_m = r_1 + m - 1 = n - 1$. Afinal, definindo $m := n - r_1$, é claro que teremos $m \in \{i\}_{i=1}^{n}$ (pois $0 < r_1 \leqslant n - 1$). Logo, pelo Lema 126, valerá que $n \mid r_{m+1}$, concluindo a demonstração. ■

Lema 128:

Sejam $a, b \in \mathbb{Z}_+$, $a \neq 0$. *Seja* q *o quociente da divisão de* b *por* a. *Vale que* $0 \leqslant q \leqslant b$. *Além disso, se o resto,* r, *da divisão de* b *por* a *for não-nulo ou* $a \neq 1$, *vale que* $0 \leqslant q < b$. □

Demonstração:

Suponhamos primeiramente que $b = 0$. Então $b = 0a + 0$ e, pelo Teorema 124, sabemos que tanto o quociente quanto o resto da divisão de b por a são nulos, o que confirma o enunciado para este caso.

Suponhamos então que $b \neq 0$ e que $a \mid b$. Como tanto a quanto $b = qa$ são não-negativos, a Proposição 91 garante que $q \geqslant 0$. Como $b = qa$, vale que $q \mid b$ e, pela Proposição 114, $|q| \leqslant |b|$. Como ambos são não-negativos, concluímos que $0 \leqslant q \leqslant b$.

Consideremos o caso especial em que $a \neq 1$. Pelo Lema 97, sabemos que $a > 1$ (pois, por hipótese, a é positivo). Então teremos que

$$\begin{aligned} |a| &> 1, \\ |a||q| &> |q|, \\ |aq| &> |q|, \\ |b| &> |q|, \\ b &> q. \end{aligned}$$

Consideremos a seguir o caso em que $r \neq 0$. Logo, pelo Teorema 124, $0 < r < a$. Suponhamos, por absurdo, que $q < 0$. Então $-qa > 0$ e, por consequência, $b - qa > 0$. Mas como $a \mid -qa$, a Proposição 114 garante que $|a| \leqslant |-qa|$. Logo, sendo ambos positivos, temos que $a < b + a \leqslant b - qa = r$. Absurdo. Logo, $q \geqslant 0$.

Resta ainda provar, no caso em que $r \neg 0$, que $q < b$. Como $b - r = qa$, sabemos que $q \mid b - r$, e é evidente que $b - r < b$, visto que r é positivo. Além disso, sabemos que $b - r \geqslant 0$, pois $qa \geqslant 0$ pelo argumento anterior. Da Proposição 114, sabemos que $|q| \leqslant |b - r| < |b|$. Como todos os números envolvidos são não-negativos, conclui-se que $0 \leqslant q < b$, encerrando a demonstração. ■

Notação [Somatório]:

Antes de enunciar e provar o Teorema 129, far-se-á um breve comentário sobre o uso da notação de somatório ($\sum$).

A notação de somatório expressa somas consecutivas que dependem de um índice de forma compacta. O índice que está sob o sigma maiúsculo expressa qual é o índice sobre o qual se dá a soma e o seu valor inicial. O índice que está sobre o sigma maiúsculo denota quando a soma para. O índice, pressuposto natural, varia sempre sob a adição de uma unidade.

Por exemplo, podemos escrever as expressões abaixo:

$$\sum_{k=0}^{n} k = 0 + 1 + \cdots + (n-1) + n,$$

$$\sum_{i=1}^{m} r_i + k = (r_1 + k) + (r_{1+1} + k) + \cdots + (r_{m-1} + k) + (r_m + k)\,. \qquad ♣$$

Teorema 129:

Seja $b > 1$ um inteiro. Todo inteiro positivo a pode ser escrito de modo único na forma

$$a = \sum_{k=0}^{n} r_k b^k,$$

em que $n \geqslant 0, r_n \neq 0$ e, para cada índice inteiro i, $0 \leqslant i \leqslant n$, tem-se que $0 \leqslant r_i < b$. □

Demonstração:

Provaremos, a princípio, a existência de uma representação de a na forma citada no enunciado. Tendo feito isso, demonstrar-se-á que tal representação é única. Deste já elucidamos que todos os quocientes e restos das divisões que serão efetuadas nesta demonstração existem e são únicos, devido ao Teorema 124.

$$\begin{aligned}
a &= q_0 b + r_0,\\
q_0 &= q_1 b + r_1,\\
q_1 &= q_{1+1} b + r_{1+1},\\
&\vdots
\end{aligned}$$

Como $b > 1$ e $a > 0$, pelo Lema 128 teremos que

$$a > q_0 > q_1 > q_{1+1} > \cdots \geqslant 0.$$

Considere o conjunto $S := \{a, 0\} \cup \{q_i, \forall\, i \in \mathbb{Z}_+\}$. Como a é claramente majorante de S e 0 é minorante, vale pelo Corolário 99 que $|S| \leqslant a + 1$. Como os quocientes são distintos, a menos que sejam nulos, é claro que existe $n \in \mathbb{Z}_+$ tal que $q_n = 0$. Logo, temos que

$$\begin{aligned}
a =& q_0 b + r_0, 0 \leqslant r_0 < b,\\
q_0 =& q_1 b + r_1, 0 \leqslant r_1 < b,\\
q_1 =& q_{1+1} b + r_{1+1}, 0 \leqslant r_{1+1} < b,\\
&\vdots\\
q_{n-1-1} =& q_{n-1} b + r_{n-1}, 0 \leqslant r_{n-1} < b,\\
q_{n-1} =& 0 \cdot b + r_n, 0 \leqslant r_n < b.
\end{aligned}$$

Substituindo cada equação na que lhe antecede teremos

$$\begin{aligned}
a &= q_0 b + r_0,\\
&= (q_1 b + r_1)\, b + r_0 = q_1 b^2 + r_1 b + r_0,\\
&= (q_{1+1} b + r_{1+1})\, b^2 + r_1 b + r_0 = q_{1+1} b^{1+1+1} + r_{1+1} b^2 + r_1 b + r_0,\\
&\vdots\\
&= (q_{n-1} b + r_{n-1})\, b^{n-1} + \sum_{k=0}^{n-1-1} r_k b^k = q_{n-1} b^n + \sum_{k=0}^{n-1} r_k b^k,\\
&= (0 + r_n)\, b^n + \sum_{k=0}^{n-1} r_k b^k = \sum_{k=0}^{n} r_k b^k.
\end{aligned}$$

Esta é uma expressão de a na forma prevista pelo enunciado. Suponhamos agora que existem dois conjuntos ordenados de inteiros, $\{r_i\}_{i=1}^n$ e $\{r_i'\}_{i=1}^m$, satisfazendo as condições do enunciado para representar a. Ou seja, tais que

$$\sum_{k=0}^{n} r_k b^k = a = \sum_{k=0}^{m} r_k' b^k.$$

Note que

$$\begin{aligned}
\sum_{k=0}^{n} r_k b^k =& a = \sum_{k=0}^{m} r_k' b^k,\\
\left(\sum_{k=1}^{n} r_k b^{k-1}\right) b + r_0 =& a = \left(\sum_{k=1}^{m} r_k' b^{k-1}\right) b + r_0'.
\end{aligned}$$

Sabemos então, do Teorema 124, que $r_0 = r'0$ e que $\sum_{k=1}^{n} r_k b^{k-1} = \sum_{k=1}^{m} r'_k b^{k-1}$.

Suponhamos, para indução, que $r_k = r'_k, \forall\, k \in \mathbb{Z}; 0 \leqslant k \leqslant l$. Queremos mostrar que então vale que $r_{l+1} = r'_{l+1}$. Teremos que: Note que

$$\begin{aligned}
\sum_{k=0}^{n} r_k b^k &= \sum_{k=0}^{m} r'_k b^k,\\
\sum_{k=l+1}^{n} r_k b^k + \sum_{k=0}^{l} r_k b^k &= \sum_{k=l+1}^{m} r'_k b^k + \sum_{k=0}^{l} r'_k b^k,\\
\sum_{k=l+1}^{n} r_k b^k &= \sum_{k=l+1}^{m} r'_k b^k,\\
\left(\sum_{k=l+1}^{n} r_k b^{k-l-1}\right) b^{l+1} &= \left(\sum_{k=l+1}^{m} r'_k b^{k-l-1}\right) b^{l+1},\\
\sum_{k=l+1}^{n} r_k b^{k-l-1} &= \sum_{k=l+1}^{m} r'_k b^{k-l-1},\\
\left(\sum_{k=l+1+1}^{n} r_k b^{k-l-1-1}\right) b + r_{l+1} &= \left(\sum_{k=l+1+1}^{m} r'_k b^{k-l-1-1}\right) b + r'_{l+1},\\
r_{l+1} &= r'_{l+1}. && \text{(Teorema 124)}
\end{aligned}$$

Logo, teremos que $r_i = r'_i, \forall\, i \in \mathbb{Z}$, concluindo que a representação é, de fato, única. ■

Notação [Base Decimal]:

De agora em diante, representaremos, segundo a conveniência, inteiros na base decimal. Usaremos os símbolos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ para representar os primeiros inteiros não-negativos (cada símbolo denota o anterior acrescentado de 1, *e.g.*, $3 = 2+1$ e $7 = 4+1+1+1 = 4+3$). Pelo Teorema 129, poderemos representar $d := 9+1$ na forma $1 \cdot d + 0$, $d^2 = 1 \cdot d^2 + 0 \cdot d + 0$ e assim por diante. Utilizaremos uma notação posicional, *i.e.*, emitiremos os d's e escreveremos $d = 10$, $d^2 = 100$ e assim por diante, *e.g.*, $d^2 + 3 \cdot d + 4 = 134$, $d^4 + 0d^3 + 5d^2 + 2d + 3 = 10523$. ♣

§11: Máximo Divisor Comum

Definição 42 [Ideal de $\mathbb{Z}$]**:**

Seja $J \subseteq \mathbb{Z}$ não-vazio. Diremos que J é um *ideal* de $\mathbb{Z}$ se satisfizer as seguintes condições:

Ideais são definidos sobre anéis. Definir de forma mais geral no capítulo abstrato?

i. $a, b \in J \Rightarrow a + b \in J$;

ii. $a \in J, x \in \mathbb{Z} \Rightarrow a \cdot x \in J$. ♠

Definição 43 [Múltiplo]**:**

Seja a um inteiro não-nulo. Diremos que um inteiro m é um *múltiplo* de a se, e somente se, existir um inteiro q tal que $m = a \cdot q$, *i.e.*, se $a \mid m$. ♠

Notação:

Seja $m \in \mathbb{Z}$. Denotaremos o conjunto de todos os múltiplos inteiros de m por $m\mathbb{Z} \equiv \{m \cdot n, n \in \mathbb{Z}\}$. ♣

Proposição 130:

Seja $m \in \mathbb{Z}$. *Então* $m\mathbb{Z}$ *é um ideal de* $\mathbb{Z}$. □

Demonstração:

Primeiramente, notemos que $m\mathbb{Z} \neq \varnothing$. Afinal, $m \cdot 0 \in m\mathbb{Z}$.

Sejam $m_1, m_2 \in m\mathbb{Z}$. Então $m_1 = m \cdot a$ e $m_2 = m \cdot b$, com $a, b \in \mathbb{Z}$. Logo, $m_1 + m_2 = m \cdot (a+b)$ e, portanto, $m_1 + m_2 \in m\mathbb{Z}$.

Seja $x \in \mathbb{Z}$. Então $m_1 \cdot x = m \cdot ax$ e, portanto, $m_1 \cdot x \in m\mathbb{Z}$.

Logo, concluímos que $m\mathbb{Z}$ é um ideal de $\mathbb{Z}$. ■

Teorema 131:

Seja J *um ideal de* $\mathbb{Z}$. *Então ou* $J = \{0\}$ *ou existe um único* $n \in \mathbb{Z}_+^*$ *tal que* $J = n\mathbb{Z}$. □

Demonstração:

Se $J = \{0\}$, o enunciado vale trivialmente. Consideremos então o caso em que $J \neq \{0\}$.

Se $J \neq \{0\}, \exists\, a \in J; a \neq 0$. É preciso que exista ao menos um elemento positivo em J, afinal, se $a > 0$, a afirmação é claramente verdadeira. Se $a < 0$, a Definição 42 garante que $-a \in J$, e $-a > 0$. Logo, o conjunto $J_+ := \{a \in J; a > 0\}$ é um subconjunto não vazio de $\mathbb{Z}$. Por P.16, S admite mínimo. Seja $n = \min J_+$. Clamo que $J = n\mathbb{Z}$.

Da Definição 42, sabemos que $nx \in J, \forall\, x \in \mathbb{Z}$. Logo, $n\mathbb{Z} \subseteq J$. Resta provar que $J \subseteq n\mathbb{Z}$.

Seja $m \in J$. Sabemos do Teorema 124 que existem q e r, $0 \leqslant r < n$, únicos tais que $m = qn + r$. Como $n \in J, qn \in J$ e como $m \in J, m - qn = r \in J$. Se $r > 0, r \in J_+$. Contudo, $r < n = \min J_+$, o que impede que $r \in J_+$. Logo, $r = 0$ e, pela Proposição 125, $n \mid m$. Logo, $m = nq \Rightarrow m \in n\mathbb{Z} \Rightarrow J \subseteq n\mathbb{Z}$. Assim concluímos que, de fato, $J = n\mathbb{Z}$.

A unicidade de n decorre do Corolário 116. Se n_1 e n_2 forem tais que $J = n_1\mathbb{Z} = n_2\mathbb{Z}$, n_1 será múltiplo de n_2 e vice-versa. Logo, $n_1 \mid n_2$ e $n_2 \mid n_1$, implicando que $n_1 = n_2$ (pois ambos são positivos.) ■

Definição 44 [Divisor Comum]**:**

Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Diremos que um inteiro c é um *divisor comum* de a e b se, e somente se, $c \mid a \wedge c \mid b$. Denotamos o conjunto de todos os divisores comuns de a e b por $D(a, b) := \{c \in \mathbb{Z}; c \mid a \wedge c \mid b\}$. ♠

Proposição 132:

Sejam $a, b \in \mathbb{Z}$, *não ambos nulos.* $D(a, b)$ *admite máximo.* □

Demonstração:

Primeiramente, notemos que $D(a, b) \neq \varnothing$, pois $a \cdot 1 = a, \forall\, a \in \mathbb{Z} \Rightarrow 1 \mid a$. Logo, $1 \in D(a, b)$.

Seja $c \in D(a, b)$. Então $c \mid a$. Pela Proposição 114, $|c| \leqslant |a| = a$. Logo, a é majorante de $D(a, b)$. Pelo Teorema 96, $D(a, b)$ admite máximo. ■

Definição 45 [Máximo Divisor Comum]**:**

Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Diremos que $\max D(a, b)$, *i.e.*, o máximo dos divisores comuns de a e b, é o *máximo divisor comum* de a e b. Além disso, utilizaremos a notação $\mathrm{mdc}\,(a, b) \equiv \max D(a, b)$. ♠

Teorema 133 [Teorema de Bézout]**:**

Sejam $a, b \in \mathbb{Z}$, *não ambos nulos, e seja* $d = \mathrm{mdc}\,(a, b)$. *Então existem* $r, s \in \mathbb{Z}$ *tais que* $d = ar + bs$. □

Demonstração:

Considere o conjunto $J := \{ax + by; x, y \in \mathbb{Z}\}$. J é não-vazio e distinto de $\{0\}$, pois, sem perda de generalidade, $a = a \cdot 1 + b \cdot 0 \in J$. Dados $ax_1 + by_1, ax_2 + by_2 \in J$, segue que $a(x_1 + x_2) + b(y_1 + y_2) \in J$. Finalmente, se $z \in \mathbb{Z}$, $a(zx_1) + b(zy_1) \in J$. Logo, J é um ideal de $\mathbb{Z}$. Pelo Teorema 131, existe $d \in \mathbb{Z}_+^*; J = d\mathbb{Z}$. Clamo que $d = \mathrm{mdc}\,(a, b)$

Como $a \in J$, $a = kd$ para algum $k \in \mathbb{Z}$. Logo, $d \mid a$. Por argumentação análoga temos que $d \mid b$ e, portanto, $d \in D(a, b)$. Considere agora algum $d' \in D(a, b)$. Como $d \in J, d = ar + bs$, com $r, s \in \mathbb{Z}$. Logo, vale pelo Corolário 118 que $d' \mid d$ e, pela Proposição 114, $|d'| \leqslant |d| = d$. Concluímos que $d = \operatorname{mdc}(a, b)$. ■

Lema 134:
Sejam $a, b, c, d, e \in \mathbb{Z}$*, com* a *e* b *não ambos nulos,* c *e* d *não ambos nulos e* $e \neq 0$*. Se* $(e \mid a \wedge e \mid b) \Leftrightarrow (e \mid c \wedge e \mid d)$*, então* $\operatorname{mdc}(a, b) = \operatorname{mdc}(c, d)$. □

Demonstração:
Se $(e \mid a \wedge e \mid b) \Leftrightarrow (e \mid c \wedge e \mid d)$, então $e \in D(a, b) \Leftrightarrow e \in D(c, d)$. Logo, $D(a, b) = D(c, d)$ e, portanto,

$$\operatorname{mdc}(a, b) = \max D(a, b) = \max D(c, d) = \operatorname{mdc}(cd).$$ ■

Proposição 135:
$\operatorname{mdc}(a, b) = \operatorname{mdc}(b, a), \forall\, a, b \in \mathbb{Z}$*, não ambos nulos.* □

Demonstração:
Note que, se $d \mid a$ e $d \mid b$, é claro que $d \mid b$ e $d \mid a$ e vice-versa. Concluímos do Lema 134 que $\operatorname{mdc}(a, b) = \operatorname{mdc}(b, a)$. ■

Proposição 136:
$\operatorname{mdc}(\operatorname{mdc}(a, b), c) = \operatorname{mdc}(a, \operatorname{mdc}(b, c)), \forall\, a, b, c \in \mathbb{Z}$*, com no máximo um destes nulo.* □

Demonstração:

$$\begin{aligned}
&\operatorname{mdc}(a, \operatorname{mdc}(b, c)) \mid a, \qquad \operatorname{mdc}(a, \operatorname{mdc}(b, c)) \mid \operatorname{mdc}(b, c), \\
&\operatorname{mdc}(a, \operatorname{mdc}(b, c)) \mid a, \quad \operatorname{mdc}(a, \operatorname{mdc}(b, c)) \mid b, \quad \operatorname{mdc}(a, \operatorname{mdc}(b, c)) \mid c, && \text{(Proposição 117.ii)} \\
&\operatorname{mdc}(a, \operatorname{mdc}(b, c)) \mid xa + yb + zc, \forall\, x, y, z \in \mathbb{Z}.. && \text{(Corolário 118)}
\end{aligned}$$

Com isso em mente, note que

$$\begin{aligned}
\operatorname{mdc}(\operatorname{mdc}(a, b), c) &= x' \cdot \operatorname{mdc}(a, b) + zc = xa + yb + zc, && \text{(Teorema 133)} \\
\operatorname{mdc}(a, \operatorname{mdc}(b, c)) &\mid \operatorname{mdc}(\operatorname{mdc}(a, b), c). && \text{(primeira parte)}
\end{aligned}$$

Por argumentação análoga, obter-se-á que $\operatorname{mdc}(\operatorname{mdc}(a, b), c) \mid \operatorname{mdc}(a, \operatorname{mdc}(b, c))$. Logo, vem do Corolário 116 que

$$\begin{aligned}
\operatorname{mdc}(\operatorname{mdc}(a, b), c) &= \pm \operatorname{mdc}(a, \operatorname{mdc}(b, c)), \\
\operatorname{mdc}(\operatorname{mdc}(a, b), c) &= \operatorname{mdc}(a, \operatorname{mdc}(b, c)),
\end{aligned}$$

pois ambos são números positivos. ■

Proposição 137:
Seja $a \in \mathbb{Z}$*. Então* $\operatorname{mdc}(a, 1) = 1$. □

Demonstração:
Pelo Corolário 115, é preciso que $D(a, 1) \subseteq \{-1, 1\}$. Como $-1 < 0$ e o máximo divisor comum é sempre positivo, temos que os candidatos a $\operatorname{mdc}(a, 1)$ são os elementos do conjunto $\{1\}$. Logo, $\operatorname{mdc}(a, 1) = 1$. ■

Proposição 138:
Seja $a \in \mathbb{Z}^*$*. Vale que* $\operatorname{mdc}(a, a) = |a|$. □

Demonstração:
Sabemos, de Proposição 117.i, que $a \in D(a, a)$. É claro que $|a| \in D(a, a)$, pois, se $a < 0$, ainda teremos que $a = -1 \cdot |a|$.

Da Proposição 114, sabemos que $|d| \leqslant |a|, \forall\, d \in D(a,a)$. É trivial constatar que $-|d| \leqslant |a|, \forall\, d \in D(a,a)$, devido à Proposição 100. Logo, $\max D(a,a) = \text{mdc}\,(a,a) = |a|$. ■

Proposição 139:
Sejam $a, b \in \mathbb{Z}, b \neq 0$. *É verdade que* $b \mid a \Leftrightarrow \text{mdc}\,(a,b) = |b|$. □

Demonstração:
Sabemos que $|b|$ é divisor de b e, pelo Proposição 114, sabemos que $|d| \leqslant |b|, \forall\, d \in D(b,b)$. Seguirá da Proposição 122 que $|b| \mid a$ e, como nenhum número maior que $|b|$ divide b, concluímos que $\text{mdc}\,(a,b) = |b|$.
Se $\text{mdc}\,(a,b) = |b|$, $|b| \mid a$. Pela Proposição 122, $b \mid a$. ■

Proposição 140:
Sejam $a, b \in \mathbb{Z}$, *não ambos nulos.* $\text{mdc}\,(a,b) = \text{mdc}\,(-a,b) = \text{mdc}\,(a,-b) = \text{mdc}\,(-a,-b)$. □

Demonstração:
Segue da Proposição 122 que

$$\begin{aligned} D(a,b) &= D(-a,b) = D(a,-b) = D(-a,-b), \\ \max D(a,b) &= \max D(-a,b) = \max D(a,-b) = \max D(-a,-b), \\ \text{mdc}\,(a,b) &= \text{mdc}\,(-a,b) = \text{mdc}\,(a,-b) = \text{mdc}\,(-a,-b). \end{aligned}$$ ■

Teorema 141:
Sejam $a, b \in \mathbb{Z}$, *não ambos nulos. Um inteiro positivo* d *é o máximo divisor comum de* a *e* b *se, e somente se, verificar as seguintes condições:*

i. $d \mid a \wedge d \mid b$;

ii. $(c \mid a \wedge c \mid b) \Rightarrow c \mid d$. □

Demonstração:
$\Rightarrow$: seja $d = \text{mdc}\,(a,b)$. A primeira condição é trivialmente verificada. A segunda condição decorre do Teorema 133 e do Corolário 118.
$\Leftarrow$: se valer a primeira condição, então $d \in D(a,b)$. Se valer a segunda, teremos, pela Proposição 114, que $|c| \leqslant d, \forall\, c \in D(a,b)$ (usamos o fato de que d é positivo por hipótese). Logo, valerá que $d = \max D(a,b) = \text{mdc}\,(a,b)$. ■

Proposição 142:
Sejam $a, b \in \mathbb{Z}$, *não ambos nulos, e seja* $c \in \mathbb{Z}^*$. *Então valem as seguintes propriedades:*

i. $\text{mdc}\,(ac, bc) = \text{mdc}\,(a,b) \cdot |c|$;

ii. $(c \mid a \wedge c \mid b) \Rightarrow \text{mdc}\,(a/c, b/c) = \text{mdc}\,(a,b)/|c|$. □

Demonstração:
Faremos a demonstração item a item. Usaremos a notação $d \equiv \text{mdc}\,(a,b)$.

i. Sabemos, do Teorema 141, que $d \mid a \wedge d \mid b$. Pela Proposição 120, $d|c| \mid ac \wedge d|c| \mid bc$.
   Pelo Teorema 133, $d = ra + sb$, para $r, s \in \mathbb{Z}$. Logo, $d|c| = r(a|c|) + s(b|c|)$. Logo, segue do Corolário 118 que $(e \mid ac \wedge e \mid bc) \Rightarrow e \mid d|c|$. Pelo Teorema 141, $d|c| = \text{mdc}\,(ac, bc)$.

ii. Do Corolário 119 sabemos que vale que

$$\begin{aligned} \text{mdc}\,(a,b) &= \text{mdc}\left(\frac{a \cdot c}{c}, \frac{b \cdot c}{c}\right), \\ &= \text{mdc}\left(\frac{a}{c}, \frac{b}{c}\right) \cdot |c|. \qquad \text{(primeira parte)} \end{aligned}$$

É simples perceber que $|c| \mid \text{mdc}(a, b)$ e, portanto podemos tomar o quociente. Fazendo isso, obteremos, usando o Corolário 119 novamente, que

$$\text{mdc}\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\text{mdc}(a, b)}{|c|}. \qquad \blacksquare$$

Teorema 143 [Teorema de Euclides]**:**
Sejam $a, b, c \in \mathbb{Z}$, $a \neq 0$, *tais que* $a \mid bc$. *Se* $\text{mdc}(a, b) = 1$, *então* $a \mid c$. □

Demonstração:
Suponha que $c = 0$. Então $c = 0 \cdot a$ e $a \mid c$.
Consideremos a seguir o caso em que $c \neq 0$. Como $\text{mdc}(a, b) = 1$, a Proposição 142 implica que $\text{mdc}(ac, bc) = |c|$. A Proposição 142 ainda garante que

$$\text{mdc}\left(ac\frac{a}{a}, bc\frac{a}{a}\right) = |c|,$$
$$\text{mdc}\left(\frac{ac}{a}, \frac{bc}{a}\right) \cdot |a| = |c|,$$
$$a \mid c. \qquad \blacksquare$$

Escólio:
Podemos fazer outra demonstração para o Teorema 143 usando o Teorema 133.
Sabemos do Teorema 133 que $1 = \text{mdc}(a, b) = ar + bs$, com $r, s \in \mathbb{Z}$. Logo, para estes r, s, tem-se que

$$(ar + bs)\,c = c,$$
$$arc + bsc = c.$$

Como $a \mid a$, pela Proposição 117, e $a \mid bc$ por hipótese, o Corolário 118 nos permite concluir que $a \mid (arc + bsc)$ e, portanto, $a \mid c$. ♣

Definição 46 [Relativamente Primos]**:**
Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Diremos que a e b são *relativamente primos*, ou *primos entre si*, se, e somente se, $\text{mdc}(a, b) = 1$. ♠

Proposição 144:
Sejam $a, b \in \mathbb{Z}$, *não ambos nulos, com* $\text{mdc}(a, b) = d$. *Se, para um inteiro* c, $a \mid c \wedge b \mid c$, *então* $(ab/d) \mid c$. □

Demonstração:
Sejam $a = a'd$ e $b = b'd$. Então $\text{mdc}(a', b') = \text{mdc}(a/d, b/d) = d/d = 1$, pela Proposição 142. Segue portanto que $c = a'dq$, para algum inteiro q e, portanto, $b'd \mid a'dq$. Usando a Proposição 120 e o Teorema 143, $b' \mid q$.
Ter-se-á então que $q = b'r$. Substituindo na expressão para c, isto indica que $c = a'db'r = ab'r$. Pelo Corolário 119, teremos que $c = (abr)/d$ e, portanto, vale que $(ab)/d \mid c$. ■

Proposição 145:
Sejam $a, b, c \in \mathbb{Z}$, $a \neq 0$, *com* b *e* c *não mutuamente nulos. Se* a *for divisor de* b *e* b *e* c *forem relativamente primos, então* a *e* c *também são relativamente primos.* □

Demonstração:
Como a é divisor de b, sabemos que existe um inteiro q tal que $b = aq$. Seja $\text{mdc}(a, c) = d$. Então temos que $a = a'd$ e $c = c'd$, com $r, s \in \mathbb{Z}$. Logo, teremos que

$$\begin{aligned} \text{mdc}(b, c) &= \text{mdc}(aq, c), \\ &= \text{mdc}(a'dq, c'd), \\ &= \text{mdc}(a'q, c') \cdot d, \qquad \text{(Proposição 142)} \end{aligned}$$

Logo, $d \mid \mathrm{mdc}\,(b, c)$. Pela Proposição 114, $d \leqslant \mathrm{mdc}\,(b, c)$ e, como tanto a quanto c são divisíveis por 1, temos que $1 \leqslant d \leqslant 1$. Logo, $\mathrm{mdc}\,(a, c) = 1$. ■

Proposição 146:
Sejam $a, b, c \in \mathbb{Z}$ *tais que* a *e* c *não sejam ambos nulos e* b *e* c *não sejam ambos nulos. Vale que* $\mathrm{mdc}\,(a, c) = \mathrm{mdc}\,(b, c) = 1 \Leftrightarrow \mathrm{mdc}\,(ab, c) = 1$. □

Demonstração:
$\Leftarrow$: seja $\mathrm{mdc}\,(a, c) = d$. Vale que $d \mid a$ e $d \mid c$. Pela Proposição 117, $d \mid ab$. Logo, $d \in D(ab, c)$. Como $1 = \mathrm{mdc}\,(ab, c) = \max D(ab, c)$, conclui-se que $d \leqslant 1$. Como 1 é divisor de todo número inteiro, $1 \leqslant d \leqslant 1$, e concluímos que $\mathrm{mdc}\,(a, c) = 1$. Por argumentação análoga obter-se-á que $\mathrm{mdc}\,(b, c) = 1$.
$\Rightarrow$: seja $\mathrm{mdc}\,(ab, c) = d$. Pelo Teorema 133 sabemos que $1 = \mathrm{mdc}\,(a, c) = ar + sc$, para certos inteiros r, s. Daí segue que $abr + sbc = b$. Como sabemos que $d \mid ab$ e $d \mid c$, podemos concluir do Corolário 118 que $d \mid b$. Logo, sabemos que $d \mid b$ e $d \mid c$, o que significa que $d \in D(b, c)$. Como $\max D(b, c) = \mathrm{mdc}\,(b, c) = 1$ e 1 divide todo inteiro (e portanto divide ab e c), concluímos que $1 \leqslant d \leqslant 1$ e, portanto, $d = 1$. ■

Proposição 147:
Sejam $a \in \mathbb{Z}, n \in \mathbb{Z}_+^*$ *e* $d = \mathrm{mdc}\,(a, a+n)$. *Então* $d \mid n$. □

Demonstração:
Sabemos que $d \mid a$ e que $d \mid a + n$. Logo, existem inteiros q, r tais que $a = qd$ e $a + n = rd$. Substituindo a primeira equação na segunda, temos que $qd + n = rd$. Logo, $n = d(r - q)$ e, portanto, $d \mid n$. ■

Lema 148:
Seja $a \in \mathbb{Z}^*$. $\mathrm{mdc}\,(a, 0) = |a|$. □

Demonstração:
Sabemos que todo inteiro divide 0. Logo, mdc $a, 0$ nada mais é do que o maior divisor de a. Pela Proposição 114, sabemos que todos os divisores de a são menores ou iguais a $|a|$, e sabemos que este divide a. Logo, $\mathrm{mdc}\,(a, 0) = |a|$. ■

Lema 149 [Algoritmo de Euclides]**:**
Sejam $a, b \in \mathbb{Z}, b \neq 0$ *e sejam* q *e* r *o quociente e o resto, respectivamente, da divisão de* a *por* b. *Então valerá que* $D(a, b) = D(b, r)$ *e, consequentemente, que* $\mathrm{mdc}\,(a, b) = \mathrm{mdc}\,(b, r)$. □

Demonstração:
Sabemos que $a = qb + r$. Logo, pelo Corolário 118, $d \mid a, \forall\, d \in D(b, r)$ e, portanto, $D(b, r) \subseteq D(a, b)$. Além disso, podemos escrever $r = a - qb$ e, também pelo Corolário 118, $d \mid r, \forall\, d \in D(a, b)$, implicando que $D(a, b) \subseteq D(b, r)$. Segue do Lema 134 que $\mathrm{mdc}\,(a, b) = \mathrm{mdc}\,(b, r)$. ■

Escólio:
Perceba que, escolhendo os números a e b de forma que $a \geqslant b$, *i.e.*, o primeiro argumento de mdc seja maior ou igual ao segundo, o Lema 149 fornece um algoritmo para o cálculo recursivo de máximos divisores comuns. Afinal, ter-se-á que

$$\begin{aligned}
a &= q_0 b + r_0, & r_0 &\leqslant |b|,\\
b &= q_1 r_0 + r_1, & r_1 &\leqslant r_0,\\
r_0 &= q_2 r_1 + r_2, & r_2 &\leqslant r_1,\\
r_1 &= q_3 r_2 + r_3, & r_3 &\leqslant r_2,\\
&\vdots & &\vdots
\end{aligned}$$

Eventualmente, atingir-se-á $r_n = 0$ e, pelo Lema 148, concluir-se-á que

$$\mathrm{mdc}(a, b) = \mathrm{mdc}(r_{n-1}, 0) = r_{n-1}.$$

Além disso, o Lema 149 permite determinar inteiros r, s que satisfaçam as condições do Teorema 133. Usando r_i da mesma forma como feito nas equações anteriores, perceba que

$$\begin{aligned}
r_0 &= q_0 b - a,\\
r_1 &= q_1 q_0 b - q_1 a - b,\\
r_2 &= q_2 q_1 q_0 b - q_2 q_1 a - q_2 b - q_0 b + a,\\
&\vdots
\end{aligned}$$

Continuando este processo até atingir r_{n-1}, teremos uma expressão para $\mathrm{mdc}(a, b)$ em termos de múltiplos de a e b. ♣

§12: Mínimo Múltiplo Comum

Definição 47 [Múltiplo Comum]**:**
Sejam $a, b \in \mathbb{Z}^*$. Diremos que um inteiro c é um *múltiplo comum* de a e b se, e somente se, $a \mid c \wedge b \mid c$. Denotaremos o conjunto de todos os múltiplos comuns de a e b por $M(a, b) := \{c \in \mathbb{Z}; a \mid c \wedge b \mid c\}$. Indicaremos por o conjunto de todos os múltiplos comuns positivos de a e b por $M^+(a, b) := \{m \in M(a, b); m > 0\}$. ♠

Proposição 150:
Sejam $a, b \in \mathbb{Z}^*$. $M^+(a, b)$ *admite mínimo.* □

Demonstração:
É claro que $M^+(a, b) \subset \mathbb{Z}^+$. Além disso, é simples constatar que é um conjunto não-vazio. Afinal, $|ab| \in M^+(a, b)$. Logo, por 32 P.16, $M^+(a, b)$ admite máximo. ■

Definição 48 [Mínimo Múltiplo Comum]**:**
Sejam $a, b \in \mathbb{Z}^*$. Diremos que $\min M^+(a, b)$, *i.e.*, o mínimo dos múltiplos comuns positivos de a e b, é o *mínimo múltiplo comum* de a e b. Além disso, utilizaremos a notação $\mathrm{mmc}(a, b) \equiv \min M^+(a, b)$. ♠

Lema 151:
Sejam $a, b \in \mathbb{Z}^*$. *Então* $\mathrm{mmc}(a, b) \mid m, \forall\, m \in M(a, b)$. □

Demonstração:
Como $\mathrm{mmc}(a, b) \in M(a, b)$, é claro que $M(a, b)$ é não-vazio.

Considere $m_1, m_2 \in M(a, b)$. Então é claro que $(a \mid m_1 \wedge b \mid m_1) \wedge (a \mid m_2 \wedge b \mid m_2)$. Logo, concluímos da Proposição 117 que $(a \mid m_1 + m_2 \wedge b \mid m_1 + m_2)$. Logo, $m_1 + m_2 \in M(a, b)$. Além disso, concluímos também da Proposição 117 que $(a \mid xm_1 \wedge b \mid xm_1), \forall x \in \mathbb{Z}$. Logo, $xm_1 \in M(a, b)$. Demonstramos desta forma que $M(a, b)$ é um ideal.

Como $\mathrm{mmc}(a, b) = \min M^+(a, b)$, segue do Teorema 131 que $M(a, b) = \mathrm{mmc}(a, b)\mathbb{Z}$. Logo, todo múltiplo comum de a e b é divisível pelo mínimo múltiplo comum de a e b. ■

Teorema 152:
Sejam $a, b \in \mathbb{Z}^*$ *e seja* $m \in \mathbb{Z}^*_+$. *Vale que* $m = \mathrm{mmc}(a, b)$ *se, e somente se, valerem as seguintes propriedades:*

i. $a \mid m, b \mid m$;

ii. $(a \mid c \wedge b \mid c) \Rightarrow m \mid c$. □

Demonstração:

A ida decorre trivialmente da Definição 48 e do Lema 151. Para a volta, suponha que um inteiro positivo m satisfaz as propriedades enunciadas. Como $a \mid m$ e $b \mid m$, $m \in M^+(a,b)$. Como $m \mid c, \forall c \in M(a,b)$, segue da Proposição 114 que $m \leqslant |c|, \forall c \in M(a,b)$. Logo, $m = \min M^+(a,b)$ e, portanto, $m = \mathrm{mmc}\,(a,b)$. ■

Teorema 153:

Sejam $a, b \in \mathbb{Z}^*$. *Sejam* $m = \mathrm{mmc}\,(a,b)$ *e* $d = \mathrm{mdc}\,(a,b)$. *Vale que* $md = |ab|$. □

Demonstração:

Seja $x \in \mathbb{Z}$ o número inteiro definido por

$$x = \frac{|ab|}{d}.$$

Como $d \mid a$ e $d \mid b$, sabemos que $x = |a|(|b|/d) = |b|(|a|/d)$. Logo, $a \mid x$ e $b \mid x$. Isso significa que podemos escrever $|a| = d(x/|b|)$.

Como $d \mid a$ e $d \mid b$, podemos escrever $a = a'd$ e $b = b'd$. Seja $c \in M(a,b)$. Então podemos escrever $c = aq$, para algum q inteiro e, por consequência, $c = a'dq$. Sabemos também que $b'd = b \mid c$ e, pela Proposição 142, sabemos que $\mathrm{mdc}\,(a', b') = 1$. Logo, pelo Teorema 143 sabemos que $b'd \mid a'dq \Rightarrow b' \mid q$ e, portanto, podemos escrever $q = b'r$. Substituindo na expressão original de c, temos que

$$c = |a'|d|b'|r' = |ab'|r' = (|ab|/d)r' = xr'.$$

Logo, $x \mid c$ e, pelo Teorema 152, $x = \mathrm{mmc}\,(a,b)$. Acima, definimos implicitamente r' como o inteiro que satisfaz $|a'||b'|r' = abr$. ■

Proposição 154:

Sejam $a, b \in \mathbb{Z}^*$. *Vale que* $\mathrm{mmc}\,(a,b) = \mathrm{mdc}\,(a,b) \Leftrightarrow |a| = |b|$. □

Demonstração:

$\Rightarrow$: suponhamos que $\mathrm{mmc}\,(a,b) = \mathrm{mdc}\,(a,b)$. Segue da Proposição 114 que $\mathrm{mdc}\,(a,b) \leqslant |a| \leqslant \mathrm{mmc}\,(a,b)$. No entanto, como $\mathrm{mmc}\,(a,b) = \mathrm{mdc}\,(a,b)$, isso implicará que $\mathrm{mdc}\,(a,b) = \mathrm{mmc}\,(a,b) = |a|$. Com argumentação análoga, obtém-se que $\mathrm{mdc}\,(a,b) = \mathrm{mmc}\,(a,b) = |b|$ e, portanto, $|a| = |b|$.

$\Leftarrow$: se $|a| = |b|$, é claro, pela Proposição 138 e pela Proposição 140 que $\mathrm{mdc}\,(a,b) = |a|$. Além disso, é evidente que $|a| = |a| \cdot 1 = |b| \in M^+(a,b)$ e este há de ser o menor múltiplo comum positivo dos dois. Afinal, pela Proposição 114 vale que $|a| \leqslant m, \forall m \in M^+(a,b)$. Logo, $|a| = \mathrm{mmc}\,(a,b)$ e, portanto, $\mathrm{mdc}\,(a,b) = \mathrm{mmc}\,(a,b)$. ■

Proposição 155:

Sejam $a, b \in \mathbb{Z}^*$. $\mathrm{mmc}\, ka, kb = |k|\,\mathrm{mmc}\,(a,b), \forall k \in \mathbb{Z}^*$. □

Demonstração:

Pelo Teorema 153 vale que

$$\begin{aligned}
\mathrm{mmc}\,(ka,kb)\,\mathrm{mdc}\,(ka,kb) &= |kakb|, \\
\mathrm{mmc}\,(ka,kb)\,\mathrm{mdc}\,(a,b)|k| &= |k||akb|, && \text{(Proposição 142)} \\
\mathrm{mmc}\,(ka,kb) &= |k|\frac{|ab|}{\mathrm{mdc}\,(a,b)}, \\
\mathrm{mmc}\,(ka,kb) &= |k|\,\mathrm{mmc}\,(a,b). && \text{(Teorema 153)}
\end{aligned}$$

Isto conclui a demonstração. ■

Proposição 156:

Sejam $a, b \in \mathbb{Z}^*$. $\operatorname{mmc}(a/k, b/k) = \operatorname{mmc} a, b/|k|, \forall\, k \in D(a, b)$. $\square$

Demonstração:

Pelo Teorema 153 vale que

$$\begin{aligned}
\operatorname{mmc}\left(\frac{a}{k}, \frac{b}{k}\right) \operatorname{mdc}\left(\frac{a}{k}, \frac{b}{k}\right) &= \left|\frac{a}{k}\frac{b}{k}\right|, \\
\operatorname{mmc}\left(\frac{a}{k}, \frac{b}{k}\right) \frac{\operatorname{mdc}(a, b)}{|k|} &= \frac{|a|}{|k|}\frac{|b|}{|k|}, && \text{(Proposição 142)} \\
\operatorname{mmc}\left(\frac{a}{k}, \frac{b}{k}\right) &= \frac{|a||b|}{|k| \operatorname{mdc}(a, b)}, \\
\operatorname{mmc}\left(\frac{a}{k}, \frac{b}{k}\right) &= \frac{\operatorname{mmc}(a, b)}{|k|}. && \text{(Teorema 153)}
\end{aligned}$$

Isto conclui a demonstração. $\blacksquare$

§13: Números Primos

Definição 49 [Número Primo]**:**

Seja $p \in \mathbb{Z}$. Diremos que p é *primo* se, e somente se, tiver exatamente dois divisores positivos: 1 e $|p|$. Seja $c \in \mathbb{Z}^* \setminus \{-1, 1\}$. Se c for não-primo, diremos que c é um número *composto*. Além disso, diremos que um inteiro b tal que $b \mid c$ e $1 < |b| < |c|$ é um *divisor próprio* de c. ♠

Proposição 157:

Seja p *um número primo e sejam* $a, b \in \mathbb{Z}$. *Vale que:*

i. $p \nmid a \Rightarrow \operatorname{mdc}(p, a) = 1$;

ii. $p \mid ab \Rightarrow (p \mid a \vee p \mid b)$. $\square$

Demonstração:

Faremos a demonstração item a item.

i. sabemos que os únicos divisores positivos de p são 1 e $|p|$. Como $p \nmid a$, $|p| \nmid a$ e, portanto, o único divisor positivo de p que divide a é 1. Logo, não há outra opção que não $\operatorname{mdc}(p, a) = 1$.

ii. se $p \mid a$, a demonstração se encerra. Se não, o primeiro trecho garante que $\operatorname{mdc}(p, a) = 1$ e, pelo Teorema 143, vale que $p \mid b$. $\blacksquare$

Notação [Produtório]:

A notação de produtório expressa multiplicações consecutivas que dependem de um índice de forma compacta. O índice que está sob o pi maiúsculo expressa qual é o índice sobre o qual se dá a multiplicação e o seu valor inicial. O índice que está sobre o pi maiúsculo denota quando a multiplicação para. O índice, pressuposto natural, varia sempre sob a adição de uma unidade.

Por exemplo, podemos escrever as expressões abaixo:

$$\prod_{k=1}^{n} k = 1 \cdot 2 \cdots (n-1) \cdot n,$$

$$\prod_{i=1}^{m} r_i + k = (r_1 + k) \cdot (r_{1+1} + k) \cdots (r_{m-1} + k) \cdot (r_m + k)\,.$$ ♣

Corolário 158:

Se um número primo p *divide um produto* $a_1 \cdots a_n$*, então* $p \mid a_k$*, para algum* k *tal que* $1 \leqslant k \leqslant n$. □

Demonstração:

Pela Proposição 157, sabemos que a tese vale para o caso $n = 2$. Para demonstrar por indução, suponhamos que valha para um inteiro positivo n. Queremos provar que então ela há de valer para $n + 1$.

Se $p \mid a_1 \cdots a_n \cdot a_{n+1}$, podemos escrever $p \mid (a_1 \cdots a_n) \cdot a_{n+1}$. Pela Proposição 157, sabemos então que ou $p \mid a_{n+1}$ ou $p \mid (a_1 \cdots a_n)$. Se valer a primeira condição, vale a tese. Se não, segue da hipótese de indução que $p \mid a_k$, para algum k tal que $1 \leqslant k \leqslant n$. Logo, também vale a tese.

Pelo Corolário 108, o enunciado se sustenta para todo caso $n \geqslant 2$. Como o caso $n = 1$ é trivialmente verdadeiro, vale para todo caso $n \geqslant 1$. ■

Teorema 159:

Seja $p \in \mathbb{Z}^* \setminus \{-1, 1\}$. p *é primo se, e somente se,* $p \mid ab \Rightarrow (p \mid a \vee p \mid b), \forall a, b \in \mathbb{Z}$. □

Demonstração:

$\Rightarrow$: provado na Proposição 157.

$\Leftarrow$: suponhamos, por absurdo, que p satisfaça a condição, mas seja composto. Então podemos escrever $|p| = qr$ para certos inteiros q, r que são divisores próprios de p, *i.e.*, $1 < q, r < |p|$. É claro que $p \mid qr$. Contudo, devido à Proposição 114, vemos que $p \nmid q$ e $p \nmid r$, contrariando a hipótese de que p satisfaz as condições do enunciado. Logo, p há de ser primo. ■

Lema 160:

Todo número inteiro a *que satisfaça* $a > 1$ *pode ser escrito como produto de números primos.* □

Demonstração:

Como 2 é primo, sabemos que o enunciado se sustenta para o caso $a = 2$. Suponhamos que ele se sustente para todo caso $2 \leqslant a \leqslant n$ e provemos que, então, ele há de se sustentar para o caso $n + 1$.

Se $n + 1$ for primo, o produto é trivial e a tese se sustenta. Consideremos então o caso em que $n + 1$ é composto. Por hipótese, $n + 1 = qr$ para certos inteiros q e r satisfazendo $1 < q, r < n + 1$, *i.e.*, q e r são divisores próprios de $n + 1$. Pela Proposição 114, sabemos que $2 \leqslant q, r \leqslant n$. Assim, a hipótese de indução nos fornece que tanto q quanto r podem ser escritos como produtos de números primos e, por consequência, seu produto, $qr = a$, também pode. Logo, pelo Corolário 110 a tese se sustenta para todo inteiro positivo $a > 1$. ■

Definição 50 [Decomposição em Fatores Primos]**:**

Seja $a > 1$ um inteiro e seja $p_1 \cdots p_n = a$, com $p_i, i = 1, \ldots, n$, números primos. Diremos que $p_1 \cdots p_n$ é uma *decomposição em fatores primos* de a e diremos que n, *i.e.*, o número de elementos usados na decomposição, é o *comprimento da decomposição*. ♠

Teorema 161:

Seja $a > 1$ *um inteiro. Então existem primos* $p_i, i = 1, \ldots, n$*, tais que* $a = p_1 \cdots p_n$ *e* $p_1 \leqslant \cdots \leqslant p_n$*, sendo que esta decomposição é única.* □

Demonstração:

A existência de tal decomposição é garantida pelo Lema 160. Provaremos então a unicidade usando indução sobre o comprimento da decomposição.

Seja a um inteiro que admita uma decomposição da forma $a = p_1$, com p_1 primo. Seja $q_1 \cdots q_n$ outra decomposição de a. Então temos que $a = p_1 = q_1 \cdots q_n$. Logo, $q_1 \mid p_1$. Como tanto q_1 quanto p_1 são primos, ambos são diferentes de 1 e não admitem divisores próprios. Logo, conclui-se que $q_1 = p_1$ e teremos que $1 = q_2 \cdots q_n$. Como nenhum dos q_i pode ser 1, pois todos são primos, é preciso que $n = 1$. Caso contrário, $q_2 \cdots q_n$ seria da forma $ab = 1$ com

$a, b > 1$, o que é absurdo. Logo, concluímos que $a = p_1 = q_1$ e, portanto, a decomposição é única se for possível decompor o inteiro de forma que o comprimento da decomposição seja 1.

Suponhamos que a tese valha para inteiros que admitem decomposições de comprimento $k \geqslant 1$. Queremos provar que, nesse caso, ela também vale para decomposições de comprimento $k + 1$.

Seja $a = p_1 \cdots p_{k+1} = q_1 \cdots q_n$, com $p_1 \leqslant \cdots \leqslant p_{k+1}$ e $q_1 \leqslant \cdots \leqslant q_{k+1}$. É claro que $q_1 \mid p_1 \cdots p_{k+1}$. Logo, pelo Corolário 158, $p_1 \mid q_i$, para algum $1 \leqslant i \leqslant k+1$. Como os q_i estão ordenados, isso implica que $p_1 \geqslant q_1$. Com raciocínio análogo obtém-se que $q_1 \geqslant p_1$ e, portanto, $q_1 = p_1$.

Temos então que $p_2 \cdots p_{k+1} = q_2 \cdots q_n$. Como a primeira decomposição tem comprimento k, a hipótese de indução garante a unicidade, fornecendo que $n = k$ e $p_i = q_i, 1 \leqslant i \leqslant k+1$. Logo, pelo Corolário 108, a tese vale para todo inteiro maior que 1. ■

Notação:

A função sign recebe um número inteiro e retorna $+1$, -1 ou 0 a depender do número ser positivo, negativo ou nulo. A rigor, sua definição é

$$\operatorname{sign} a := \begin{cases} \frac{a}{|a|}, \text{se } a \neq 0 \\ 0, \text{se } a = 0 \end{cases} .$$

Usaremos essa notação no Teorema 162. ♣

Teorema 162 [Teorema Fundamental da Aritmética]**:**

Seja $a \in \mathbb{Z}^* \setminus \{-1, 1\}$*. Então existem primos positivos* $p_1 < \cdots < p_r$ *e inteiros* $n_1, \ldots, n_r$ *tais que* $a = \operatorname{sign}(a) \cdot p_1^{n_1} \cdots p_r^{n_r}$*. Ademais, esta decomposição é única.* □

Demonstração:

Sabemos, do Teorema 161 que

$$|a| = \prod_{i=1}^{m} p_i, \; p_1 \leqslant \cdots \leqslant p_m,$$

onde os p_i são primos e esta decomposição é única. Logo, podemos escrever

$$a = \operatorname{sign} a \cdot \prod_{i=1}^{m} p_i, \; p_1 \leqslant \cdots \leqslant p_m.$$

Podemos juntar os p_i iguais em potências de forma a obter que

$$a = \operatorname{sign} a \cdot \prod_{i=1}^{r} p_i^{n_i}, \; p_1 < \cdots < p_r.$$

Assim concluímos a demonstração. ■

Corolário 163:

Sejam $a, b \in \mathbb{Z}^* \setminus \{-1, 1\}$*. Então existem primos positivos* $p_1 < \cdots < p_t$ *e inteiros não negativos* $n_1, \ldots, n_t, m_1, \ldots, m_t$ *tais que*

$$a = \operatorname{sign} a \cdot \prod_{i=1}^{t} p_i^{n_i},$$
$$b = \operatorname{sign} b \cdot \prod_{i=1}^{t} p_i^{m_i},$$

sendo que os n_i *e os* m_i *podem ser nulos, se necessário.* □

Demonstração:

Sejam $p_1 < p_2 < \cdots < p_t$ números primos positivos. Sejam $I, J \subseteq \{i\}_{i=1}^t$ e sejam $n_1, \ldots, n_t, m_1, \ldots, m_t$ tais que as decomposições

$$a = \operatorname{sign} a \cdot \prod_{i \in I} p_i^{n_i},$$
$$b = \operatorname{sign} b \cdot \prod_{j \in J} p_i^{m_j},$$

sejam as descritas no Teorema 162. É claro que, se $k \in I^c = \{i\}_{i=1}^t \setminus I$, ainda valerá que

$$a = \operatorname{sign} a \cdot p_k^0 \cdot \prod_{i \in I} p_i^{n_i},$$

dado que $z^0 = 1, \forall z \in \mathbb{Z}$. Fazendo isso para todo $k \in I^c$ e definindo $n_k = 0, \forall k \in I^c$, teremos que

$$a = \operatorname{sign} a \cdot \prod_{i=1}^{t} p_i^{n_i}.$$

Analogamente, obtemos para b que

$$b = \operatorname{sign} b \cdot \prod_{i=1}^{t} p_i^{m_i},$$

o que conclui a demonstração. Observe que se $I = \varnothing$ ou $J = \varnothing$ a prova tornar-se-ia trivial. ■

Lema 164:

Sejam $p_1 < \cdots < p_t$ *primos positivos. Sejam*

$$a = \operatorname{sign} a \cdot \prod_{i=1}^{t} p_i^{n_i}, b = \operatorname{sign} b \cdot \prod_{i=1}^{t} p_i^{m_i} \in \mathbb{Z},$$

com $a \mid b$ *e* $n_1, \ldots, n_t, m_1, \ldots, m_t \in \mathbb{Z}_+$. *Então vale que* $c = b/a$ *pode ser escrito na forma*

$$c = \operatorname{sign} c \cdot \prod_{i=1}^{t} p_i^{q_i}.$$ □

Demonstração:

Suponha que na decomposição de c exista um certo primo positivo s. Então é claro que $b = s \cdot ak$, onde k é o quociente da divisão de c por s. Pelo Teorema 162, teremos que s necessariamente aparece na decomposição de b em fatores primos. Como isso há de valer para todos os números que aparecem na decomposição de c, do Corolário 163 segue a tese. ■

Lema 165:

Sejam $p_1 < \cdots < p_t$ *primos positivos. Sejam*

$$a = \prod_{i=1}^{t} p_i^{n_i}, b = \prod_{i=1}^{t} p_i^{m_i} \in \mathbb{Z}_+^*,$$

onde $n_1, \ldots, n_t, m_1, \ldots, m_t \in \mathbb{Z}_+$. *Então vale que* $b \mid a$ *se, e somente se,* $m_i \leqslant n_i, \forall i \in \{i\}_{i=1}^t$. □

Demonstração:

$\Rightarrow$: suponhamos que $b \mid a$. Então existe um inteiro c tal que $a = bc$ e, pelo Lema 164, podemos escrever $c = \prod_{i=1}^{t} p_i^{q_i}$. Logo, ter-se-á que

$$\begin{aligned} \prod_{i=1}^{t} p_i^{n_i} &= \prod_{i=1}^{t} p_i^{m_i} \cdot \prod_{i=1}^{t} p_i^{q_i}, \\ &= \prod_{i=1}^{t} p_i^{m_i+q_i}, && \text{(Proposição 112)} \\ \therefore n_i &= m_i + q_i, \forall\, i \in \{i\}_{i=1}^{t}. && \text{(Teorema 162)} \end{aligned}$$

Como os q_i são não-negativos, segue que $m_i \leqslant n_i, \forall\, i \in \{i\}_{i=1}^{t}$.

$\Leftarrow$: tome $r_i := n_i - m_i$. Então seguirá que

$$\begin{aligned} \prod_{i=1}^{t} p_i^{n_i} &= \prod_{i=1}^{t} p_i^{m_i+q_i}, \\ &= \prod_{i=1}^{t} p_i^{m_i} \cdot \prod_{i=1}^{t} p_i^{q_i}, && \text{(Proposição 112)} \\ &= b \cdot \prod_{i=1}^{t} p_i^{q_i}. \\ \therefore b &\mid a. \end{aligned}$$

■

Teorema 166:

Sejam $p_1 < \cdots < p_t$ *primos positivos. Sejam*

$$a = \prod_{i=1}^{t} p_i^{n_i}, b = \prod_{i=1}^{t} p_i^{m_i} \in \mathbb{Z}_+^*,$$

onde $n_1, \ldots, n_t, m_1, \ldots, m_t \in \mathbb{Z}_+$. *Vale que*

$$d = \operatorname{mdc}(a, b) = \prod_{i=1}^{t} p_i^{\alpha_i}; \alpha_i = \min n_i, m_i, \forall\, i \in \{i\}_{i=1}^{t},$$

$$m = \operatorname{mmc}(a, b) = \prod_{i=1}^{t} p_i^{\beta_i}; \beta_i = \max n_i, m_i, \forall\, i \in \{i\}_{i=1}^{t}.$$

□

Demonstração:

Do Lema 165 sabemos que $(d \mid a \wedge d \mid b)$ e que $(c \mid a \wedge c \mid b) \Rightarrow c \mid d$. Logo, pelo Teorema 141 vale que $d = \operatorname{mdc}(a, b)$.

Analogamente, do Lema 165 sabemos que $(a \mid m \wedge b \mid m)$ e que $(a \mid n \wedge b \mid n) \Rightarrow n \mid m$. Logo, pelo Teorema 152 vale que $m = \operatorname{mmc}(a, b)$. ■

Escólio:

Note que o Teorema 166 nos permite obter outra definição para o máximo divisor comum e para o mínimo múltiplo comum, visto que estes são invariantes pelo sinal dos seus argumentos (Proposição 140 e Teorema 153). ♣

Definição 51 [Progressão Geométrica]**:**

Se uma sequência de inteiros for tal que $a_{i+1} = a_i \cdot r$, para algum $r \neq 1$ inteiro, diremos que tal sequência é uma *progressão geométrica* (abreviada como PG) de razão r. ♠

Lema 167 [Soma de Progressões Geométricas Finitas]**:**
Vale que a soma dos n *primeiros termos de uma PG de razão* r *com valor inicial* a_1*,* S_n*, é dada por*

$$S_n = a_1 \frac{r^n - 1}{r - 1}.$$ □

Demonstração:
Primeiramente, note que

$$\begin{aligned} S_n &= \sum_{i=1}^{n} a_i, \\ &= \sum_{i=1}^{n} a_1 \cdot r^{i-1}, \\ &= a_1 \cdot \sum_{i=1}^{n} r^{i-1}. \end{aligned}$$

Além disso,

$$\begin{aligned} r \cdot S_n &= a_1 \cdot \sum_{i=1}^{n} r^{i}, \\ &= a_1 \cdot \sum_{i=2}^{n+1} r^{i-1}, \\ &= a_1 \cdot \sum_{i=1}^{n} r^{i-1} - a_1 + a_1 \cdot r^n, \\ &= S_n - a_1 + a_1 \cdot r^n. \end{aligned}$$

Logo, teremos que

$$S_n\left(r-1\right) = a_1\left(r^n - 1\right).$$

Perceba que $r^n - 1 = (r-1)\left(\sum_{i=0}^{n-1} r^i\right)$ e, portanto, $r - 1 \mid r^n - 1$. Logo, podemos finalmente escrever que

$$S_n = a_1 \frac{r^n - 1}{r - 1}.$$

Assim concluímos a prova. ■

Proposição 168:
Seja $a \in \mathbb{Z}_+^*$*,* $a > 1$*, com sua decomposição*

$$a = \prod_{i=1}^{t} p_i^{m_i}$$

nas condições do Teorema 162*. Então o número de divisores positivos de* a*,* $n(a)$*, e a soma desses divisores,* $s(a)$*, são dados respectivamente pelas seguintes identidades:*

$$n(a) = \prod_{i=1}^{t} \left(m_i + 1\right),$$

$$s(a) = \prod_{i=1}^{t} \frac{p_i^{m_i+1} - 1}{p_i - 1}.$$ □

Demonstração:

Devido ao Lema 165, sabemos que todos os divisores de a são da forma $d = \prod_{i=1}^{t} p_i^{l_i}; 0 \leqslant l_i \leqslant m_i, 1 \leqslant i \leqslant t$. Além disso, todos os números dessa forma dividem a. Logo, vale que os divisores de a são exatamente os termos do desenvolvimento do produto dado por

$$S = \prod_{i=1}^{t} \left(\sum_{j=0}^{m_i} p_i^j \right).$$

Como cada termo do produtório é uma soma de $m_i + 1$ fatores, com $1 \leqslant i \leqslant t$, teremos que o número de divisores de a é dado por

$$n(a) = \prod_{i=1}^{t} (m_i + 1).$$

Ao somar todos os divisores de a, é claro que obteremos S. Logo, $S = s(a)$. Sabemos, pelo Lema 167, que $\sum_{j=0}^{m_i} p_i^j = \frac{p_i^{m_i+1}-1}{p_i-1}, \forall i \in \{i\}_{i=1}^{n}$. Logo, concluímos que

$$s(a) = \prod_{i=1}^{n} \frac{p_i^{m_i+1} - 1}{p_i - 1},$$

encerrando a demonstração. ■

Proposição 169:

Sejam $n \in \mathbb{Z}$ e q um primo. Então podemos escrever n na forma $n = q^k m$, com $k \in \mathbb{Z}_+$ e $m \in \mathbb{Z}; q \nmid m$. □

Demonstração:

Sabemos, do Corolário 163, que $n = \operatorname{sign} n \cdot \prod_{i=1}^{t} p_i^{m_i}$ com $p_1 < \cdots < p_t$ primos positivos e $m_i \geqslant 0, 1 \leqslant i \leqslant t$. Se $q \in \{p_i\}_{i=1}^{t}$, teremos que $q = p_k$ para algum $1 \leqslant k \leqslant t$. Logo, teremos que

$$\begin{aligned} n &= \operatorname{sign} n \cdot \prod_{i=1}^{t} p_i^{m_i}, \\ &= p_k^{m_k} \cdot \operatorname{sign} n \cdot \prod_{\substack{1 \leqslant i \leqslant t \\ i \neq k}} p_i^{m_i}, \\ &= q^{m_k} \cdot \left(\operatorname{sign} n \cdot \prod_{\substack{1 \leqslant i \leqslant t \\ i \neq k}} p_i^{m_i} \right). \end{aligned}$$

Se $q \notin \{p_i\}_{i=1}^{t}$, basta fazermos $n = q^0 \cdot n$. ■

Omite-se aqui o trecho sobre o Crivo de Eratóstenes por depender do conceito de raiz quadrada, que ainda não foi adequadamente formalizado no anel dos inteiros.

Notação:

Doravante, denotaremos o conjunto dos números primos por $\mathcal{P}$. ♣

Teorema 170:

O conjunto dos números primos é infinito. □

Demonstração:

Suponha que $\mathcal{P}$ seja finito. Então $\mathcal{P} = \{p_i\}_{i=1}^{n}$, para algum $n \in \mathbb{Z}_+$. Considere o número dado por $q = \prod_{i=1}^{n} p_i + 1$. Pelo Teorema 162, sabemos que, se q for composto, $\exists\, p_k \in \mathcal{P}; p_k \mid q$. Contudo, é claro que $p_k \mid \prod_{i=1}^{n} p_i$. Logo, do Corolário 118, temos que $p_k \mid 1 = \prod_{i=1}^{n} p_i - q$, o que contradiz o Corolário 115. Logo, q não pode ser composto e, portanto é primo. Mas $q \notin \mathcal{P}$, contradizendo a hipótese inicial de que o conjunto dos números primos é finito. Logo, por absurdo, $\mathcal{P}$ é infinito. ■

Definição 52 [Fatoriais]**:**
Seja $n \in \mathbb{Z}_+$. Definimos o fatorial de n por

i. $0! := 1$;

ii. $(n+1)! := (n+1) \cdot n!$.

♠

Proposição 171:
Seja $n \in \mathbb{Z}_+^*$. Então é possível determinar n inteiros compostos consecutivos. □

Demonstração:
Fixado n, perceba que o conjunto $\{(n+1)! + i\}_{i=2}^{n+1}$ é formado por números compostos consecutivos, visto que todo número da forma $a_m = (n+1)! + m, 2 \leqslant m \leqslant n+1$ pode ser escrito como

$$\begin{aligned} a_m &= \prod_{1 \leqslant k \leqslant n+1} k + m \\ &= m \cdot \prod_{\substack{1 \leqslant k \leqslant n+1 \\ k \neq m}} k + m \\ &= m \cdot \left(\prod_{\substack{1 \leqslant k \leqslant n+1 \\ k \neq m}} k + 1 \right) \end{aligned}$$

Logo, $m \mid a_m$ e, como $1 \neq m \neq a_m$, a_m é composto. Como existem n números a_m consecutivos, encontramos n números compostos consecutivos. ■

Corolário 172:
Seja $n \in \mathbb{Z}_+^*$. Então existem primos consecutivos p_h e p_{h+1} satisfazendo $p_{h+1} - p_h \geqslant n$. □

Demonstração:
Considere o conjunto $\mathscr{P} = \{p \in \mathcal{P}; p < (n+1)! + 2\}$. Pelo Teorema 96, sabemos que existe $p_h = \max \mathscr{P}$. É claro então que $p_h \leqslant (n+1)! + 1$. Sabemos, da demonstração da Proposição 171, que todos os números de $(n+1)! + 2$ a $(n+1)! + (n+1)$ são compostos e, portanto, $p_{h+1} > (n+1)! + (n+1)$. Tomando a diferença das desigualdades, conclui-se que $p_{h+1} - p_h > n$. ■

§14: Binômios

Lema 173:
Sejam $m, n \in \mathbb{Z}, n \geqslant 1$. Vale que $n! \mid \prod_{k=1}^{n} m + k$, i.e., o fatorial de n divide o produto de n inteiros consecutivos. □

Demonstração:
Faremos a demonstração por indução sobre n. Para $n = 1$, tem-se um caso trivial, visto que todo inteiro a pode ser escrito como $a = 1 \cdot a$ e, portanto, $1 \mid a$.

Suponhamos que o enunciado valha para um inteiro positivo n. Queremos provar que vale para $n+1$. Faremos esta demonstração por indução sobre m. Se $m = 0$, teremos que $n! = \prod_{k=1}^{n} k$. Multiplicando ambos os lados por $(n+1)$, temos que $(n+1)! = \prod_{k=1}^{n+1} k$ e, portanto, $(n+1)! \mid \prod_{k=1}^{n+1} k$.

Suponhamos agora que, para um dado $m \in \mathbb{Z}$, o enunciado ser verdadeiro para n implica em sua veracidade para $n+1$. Mostraremos que, sob estas condições, a implicação também vale para $m+1$.

$$\begin{aligned}
\prod_{k=1}^{n+1} m+1+k &= (m+1+n+1)\cdot \prod_{k=1}^{n} m+1+k, \\
&= (m+1)\cdot\left(\prod_{k=1}^{n} m+1+k\right) + (n+1)\cdot\left(\prod_{k=1}^{n} m+1+k\right), \\
&= (m+1)\cdot\left(\prod_{k=2}^{n+1} m+k\right) + (n+1)\cdot\left(\prod_{k=1}^{n} m+1+k\right), \\
&= \left(\prod_{k=1}^{n+1} m+k\right) + (n+1)\cdot\left(\prod_{k=1}^{n} m+1+k\right), \\
&= (n+1)!\cdot q + (n+1)\cdot\left(\prod_{k=1}^{n} m+1+k\right), && \text{(hip. ind. sobre } m) \\
&= (n+1)!\cdot q + (n+1)\cdot(p\cdot n!), && \text{(hip. ind. sobre } n) \\
&= (n+1)!\cdot q + (n+1)!\cdot p, \\
&= (n+1)!\cdot(q+p).
\end{aligned}$$

Acima, $p, q \in \mathbb{Z}^*$. Concluímos desse desenvolvimento que $(n+1)! \mid \prod_{k=1}^{n+1} m+1+k$ e, pelo Corolário 108, sabemos que

$$n! \mid \prod_{k=1}^{n} m+k \Rightarrow (n+1)! \mid \prod_{k=1}^{n+1} m+k, \forall\, m \in \mathbb{Z}_+.$$

Logo, pelo mesmo Corolário, concluímos que a tese é verdadeira para todo $n \in \mathbb{Z}_+^*$.

Por uma argumentação análoga, obtém-se que se, para um dado $m \in \mathbb{Z}$, o enunciado ser verdadeiro para n implica em sua veracidade para $n+1$, a implicação também vale para $m-1$.

Note que, pelo Teorema 96, teremos que o enunciado precisa ser válido para todo $m \in \mathbb{Z}$. Caso contrário, o conjunto dos m que não satisfazem a propriedade seria majorado pelo 0 e, pelo Teorema 96, teria um máximo. No entanto, acabamos que provar que, como a propriedade é válida para o inteiro que sucede o máximo, ela precisa ser válida para o máximo, que portanto não está no conjunto de que é máximo. Por absurdo, conclui-se que o enunciado é, de fato, válido para todo inteiro m e todo inteiro positivo n. ■

Proposição 174:

Sejam $n, k \in \mathbb{Z}_+, k \leqslant n$. *Então vale que* $k!\,(n-k)! \mid n!$. □

Demonstração:

Sabemos, do Lema 173, que $(n-k)! \mid \prod_{l=k+1}^{n} l$. Logo, segue de Proposição 120 que $k!\,(n-k)! \mid k! \cdot \prod_{l=k+1}^{n} l$ e, portanto, $k!\,(n-k)! \mid n!$. ■

Definição 53 [Números Combinatórios]**:**

Sejam $n, k \in \mathbb{Z}_+, k \leqslant n$. Seja A um conjunto tal que $|A| = n$. Denotaremos o números de subconjuntos de A com k elementos por $\binom{n}{k}$ e leremos *combinações de* n *elementos tomados* k *a* k, ou ainda n *escolhe* k. Trataremos estes números como inteiros[1]. ♠

Proposição 175 [Fórmula de Stieffel]**:**
Sejam $n, k \in \mathbb{Z}_+^*, 1 \leqslant k \leqslant n-1$. *Então vale a seguinte identidade:*

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \qquad \square$$

Demonstração:
Seja A um conjunto tal que $|A| = n$. Então existem $\binom{n}{k}$ conjuntos $B_i \subseteq A$ tais que $|B_i| = k$.

Seja $a \in A$. O número de subconjuntos de A com cardinalidade k que incluem a é dado por $\binom{n-1}{k-1}$. Afinal, o problema é equivalente a obter o número de subconjuntos de $A \setminus \{a\}$ com cardinalidade $k-1$ e então unir cada um destes subconjuntos a $\{a\}$. Perceba ainda que o número de subconjuntos de A com cardinalidade k que não incluem a é dado por $\binom{n-1}{k}$, pois o problema nada mais é do que obter o número de subconjuntos de $A \setminus \{a\}$ com cardinalidade k.

Visto que $\binom{n}{k}$ precisa ser o número de subconjuntos de A com cardinalidade k que incluem a somado ao número de subconjuntos de A com cardinalidade k que não o fazem, conclui-se que, de fato,

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \qquad \blacksquare$$

Notação:
Seja A um conjunto. Denotaremos o conjunto das partes de A, *i.e.*, o conjunto dos subconjuntos de A, por $\mathbb{P}(A)$. ♣

Proposição 176:
Sejam $n, k \in \mathbb{Z}_+, k \leqslant n$. *Então vale a seguinte identidade:*

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}. \qquad \square$$

Demonstração:
Primeiramente, para $n = 0$, teremos que se um conjunto A for tal que $|A| = n$, então $A = \varnothing$. Logo, é claro que o único subconjunto de A será o próprio $\varnothing$, que tem cardinalidade 0. Logo, $\binom{0}{0} = 1$ e é elementar constatar que não há outros valores possíveis para k, visto que $0 \leqslant k \leqslant n = 0$. Como $\frac{0!}{0!0!} = \frac{1}{1} = 1$, vale a tese.

Para $n = 1$, temos que $|A| = n \Rightarrow \mathbb{P}(A) = \{\varnothing, A\}$. Como $|\varnothing| = 0$ e $|A| = 1$, é claro que $\binom{1}{0} = \binom{1}{1} = 1$ e, visto que $\frac{0!}{1!0!} = \frac{0!}{0!1!} = 1$, vale a tese.

Suponhamos agora que a tese seja verdadeira $\forall\, k \in \mathbb{Z}_+^*, k \leqslant n$, onde $n \in \mathbb{Z}_+^*$ é dado. Note

[1]O autor esforçou-se para obter uma maneira de deduzir que os números combinatórios precisam ser inteiros, mas não a encontrou. Para poder operar com estes números, parece ser necessário saber como se comportam e isso só se mostra possível assumindo de antemão que eles pertencem a uma álgebra universal (para definição de álgebra universal, ver [1]) específica. No caso, escolheu-se os inteiros, e não os naturais, por mera conveniência.

que, pela Proposição 175,

$$\begin{aligned}
\binom{n+1}{k} &= \binom{n}{k-1} + \binom{n}{k}, \\
&= \frac{n!}{(k-1)!\,(n-k+1)!} + \frac{n!}{k!\,(n-k)!}, && \text{(hipótese de indução)} \\
&= \frac{n!}{(k-1)!\,(n-k+1)!} \cdot \frac{k!\,(n-k)!}{k!\,(n-k)!} + \frac{n!}{k!\,(n-k)!} \cdot \frac{(k-1)!\,(n-k+1)!}{(k-1)!\,(n-k+1)!}, \\
& && \text{(Corolário 119.i)} \\
&= \frac{n!k!\,(n-k)!}{(k-1)!\,(n-k+1)!k!\,(n-k)!} + \frac{n!\,(k-1)!\,(n-k+1)!}{k!\,(n-k)!\,(k-1)!\,(n-k+1)!}, \\
& && \text{(Corolário 119.iii)} \\
&= \frac{n!k!\,(n-k)! + n!\,(k-1)!\,(n-k+1)!}{k!\,(n-k)!\,(k-1)!\,(n-k+1)!}, && \text{(Corolário 119.iv)} \\
&= \frac{n!\,[k!\,(n-k)! + (k-1)!\,(n-k+1)!]}{k!\,(k-1)!\,(n-k)!\,(n-k+1)!}, \\
&= \frac{n!\,(k-1)!\,(n-k)!\,[k + (n-k+1)]}{k!\,(k-1)!\,(n-k)!\,(n-k+1)!}, \\
&= \frac{n!\,[n+1]}{k!\,(n-k+1)!}, && \text{(Corolário 119.ii)} \\
&= \frac{(n+1)!}{k!\,(n+1-k)!}.
\end{aligned}$$

Logo, conclui-se por indução que, $\forall\, n \in \mathbb{Z}_+^*$, a tese vale $\forall\, k < n$. Para $k = n$, temos que $\binom{n}{n} = 1$ (o mesmo subconjunto de A com a mesma cardinalidade de A é o próprio A) e que $\frac{n!}{n!0!} = 1$. Além disso, $\binom{n}{0} = 1$, pois o único subconjunto de A com cardinalidade nula é o conjunto vazio. Como $\frac{n!}{n!0!} = 1$, vale a tese e concluímos a demonstração. ■

Lema 177:
$\binom{n}{0} = \binom{n}{n} = 1, \forall\, n \in \mathbb{Z}_+$. □

Demonstração:
Segue da Proposição 176 que

$$\frac{n!}{0!n!} = \frac{n!}{n!0!} = 1, \forall\, n \in \mathbb{Z}_+.$$ ■

Corolário 178:
$\binom{a}{0} = \binom{a}{a} = \binom{b}{b} = \binom{b}{0}, \forall\, a, b \in \mathbb{Z}_+$. □

Demonstração:

$$\binom{a}{0} = \binom{a}{a} = 1 = \binom{b}{b} = \binom{b}{0}, \forall\, a, b \in \mathbb{Z}_+. \qquad \text{(Lema 177)}$$

Isto encerra a demonstração. ■

Teorema 179 [Teorema do Binômio]**:**
Sejam $a, b, n \in \mathbb{Z}, n \geqslant 1$. *Então*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Além disso, se a *e* b *forem não ambos nulos, a identidade acima é válida para* $n = 0$. □

Demonstração:

Faremos a prova via indução sobre n. Para $n = 1$, temos que

$$\begin{aligned}
(a+b)^1 &= a + b,\\
&= \binom{1}{0} a^{1-0} b^0 + \binom{1}{1} a^0 b^1,\\
&= \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k.
\end{aligned}$$

Dado $n \geqslant 1$, suponhamos que a tese seja verdadeira $\forall\, a, b \in \mathbb{Z}$. Então perceba que

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^n,\\
&= a(a+b)^n + b(a+b)^n,\\
&= a\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k + b\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k,\\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1},\\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k,\\
&= \binom{n}{0} a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] a^{n+1-k} b^k + \binom{n}{n} b^{n+1},\\
&= \binom{n}{0} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + \binom{n}{n} b^{n+1}, && \text{(Proposição 175)}\\
&= \binom{n+1}{0} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n+1-k} b^k + \binom{n+1}{n+1} b^{n+1}, && \text{(Corolário 178)}\\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.
\end{aligned}$$

Assim, concluímos por indução que vale a tese para todo inteiro positivo n. ■

Teorema 180:

Não existe nenhum polinômio $p(n)$ em apenas uma variável, não-constante e com coeficientes inteiros tal que $p(n)$ seja primo, para todo $n \in \mathbb{Z}_+$. □

Escrever demonstração!

Demonstração:

Suponhamos que $f(x) = \sum_{k=0}^{n} a_k x^k$, com os $a_k \in \mathbb{Z}$, seja tal que $f(n)$ é primo para todo inteiro $n \geqslant 0$.

Seja $n_0 \in \mathbb{Z}_+$ e seja $p = f(n_0)$. Perceba que, sendo t um inteiro arbitrário, teremos que

$$
\begin{aligned}
f(n_0 + tp) &= \sum_{k=0}^{n} a_k \cdot (n_0 + tp)^k\,, \\
&= \sum_{k=0}^{n} a_k \cdot \sum_{l=0}^{k} \binom{k}{l} n_0^{k-l} t^l p^l, && \text{(Teorema 179)} \\
&= \sum_{k=0}^{n} a_k n_0^k + a_k \cdot \sum_{l=1}^{k} \binom{k}{l} n_0^{k-l} t^l p^l, \\
&= f(n_0) + \sum_{k=0}^{n} \sum_{l=1}^{k} a_k \binom{k}{l} n_0^{k-l} t^l p^l, \\
&= p + \psi(t),
\end{aligned}
$$

onde $\psi(t) = \sum_{k=0}^{n} \sum_{l=1}^{k} a_k \binom{k}{l} n_0^{k-l} t^l p^l$. Perceba que $p \mid \psi(t), \forall\, t \in \mathbb{Z}$, pois

$$
\begin{aligned}
\psi(t) &= \sum_{k=0}^{n} \sum_{l=1}^{k} a_k \binom{k}{l} n_0^{k-l} t^l p^l, \\
&= \sum_{k=0}^{n} p \cdot \sum_{l=1}^{k} a_k \binom{k}{l} n_0^{k-l} t^l p^{l-1}, \\
&= p \cdot \sum_{k=0}^{n} \sum_{l=1}^{k} a_k \binom{k}{l} n_0^{k-l} t^l p^{l-1}.
\end{aligned}
$$

Isso nos permite definir a função $\phi(t) = \sum_{k=0}^{n} \sum_{l=1}^{k} a_k \binom{k}{l} n_0^{k-l} t^l p^{l-1}$, que satisfaz $\psi(t) = p \cdot \phi(t)$. Logo, teremos que $f(n_0 + tp) = p + p \cdot \phi(t) = p \cdot (1 + \phi(t))$ e, portanto, $p \mid f(n_0 + tp)$.

Como, por hipótese, $f(n_0 + tp)$ é primo, é preciso que $f(n_0 + tp) = \pm p$. Caso contrário, teríamos que $f(n_0 + tp)$ possui um divisor próprio ou que $p = \pm 1$ (e portanto p não seria primo). Segue então que $\pm p = p + \psi(t)$, o que implica que $\psi(t) = \pm p - p$. Seguirá que $\phi(t) = 0$ ou $\phi(t) = -2$, para todo t.

Como concluir a prova sem utilizar o Teorema Fundamental da Álgebra?

■

CAPÍTULO 4

Congruências

§15: Equações Diofantinas Lineares

Definição 54 [Equação Diofantina]**:**
Diremos que uma equação polinomial a coeficientes inteiros em uma ou mais variáveis é uma *equação diofantina* quando nos interessarmos apenas por suas soluções inteiras. Em especial, diremos que uma equação diofantina é linear se for uma soma de monômios de grau 1 ou 0 igualada a um inteiro. ♠

Observação:
Consideraremos aqui apenas as equações diofantinas lineares da forma $ax + by = c$. ♣

Proposição 181:
Sejam $a, b, c \in \mathbb{Z}$*, com* a *e* b *não ambos nulos. A equação diofantina* $ax + ay = c$ *admite soluções se, e somente se,* $\text{mdc}(a, b) \mid c$. □

Demonstração:
Conforme feito na demonstração do Teorema de Bézout, sabemos que $J = \{ax + by, x, y \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$ e, portanto, vale que $J = d\mathbb{Z}$, onde $d = \text{mdc}(a, b)$.

É trivial constatar que a equação possui solução se, e somente se, $c \in J$ e, portanto, se, e somente se, $d \mid c$. ■

Teorema 182:
Sejam $a, b, c \in \mathbb{Z}$*, com* a *e* b *não ambos nulos e tais que* $d = \text{mdc}(a, b) \mid c$*. Sejam* $r, s \in \mathbb{Z}$ *tais que* $d = ra + sb$*. Então* $x_0 = r \cdot \frac{c}{d}$ *e* $y_0 = s \cdot \frac{c}{d}$ *solucionam a equação* $ax + by = c$*. Além disso, toda outra solução desta equação é da forma*

$$x = r \cdot \frac{c}{d} + t \cdot \frac{b}{d}, \quad y = s \cdot \frac{c}{d} - t \cdot \frac{a}{d}, \quad t \in \mathbb{Z},$$

sendo que todo inteiro t *fornece uma solução da equação.* □

Demonstração:
Visto que $d = ra + sb$, basta multiplicar a equação por c/d para constatar que

$$ra \cdot \frac{c}{d} + sb \cdot \frac{c}{d} = c.$$

Veja ainda que ao substituir $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$ obtém-se

$$\begin{aligned} ax + by &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t, \\ &= ax_0 + by_0, \\ &= c. \end{aligned}$$

Por fim, suponha que x' e y' solucionem a equação. Então perceba que

$$\begin{aligned} ax' + bx' = c &= ax_0 + by_0, \\ \therefore a\,(x' - x_0) + b\,(y' - y_0) &= 0. \end{aligned}$$

Denotando $a_1 = \frac{a}{d}$ e $b_1 = \frac{b}{d}$, temos que

$$\begin{aligned} \mathrm{mdc}\,(a_1, b_1) &= \mathrm{mdc}\,(\frac{a}{d}, \frac{b}{d}), \\ &= \frac{\mathrm{mdc}\, a, b}{d}, && \text{(Proposição 142)} \\ &= 1. \end{aligned}$$

Como podemos escrever $a_1\,(x' - x_0) = b_1\,(y_0 - y')$, vemos que $b_1 \mid a_1\,(x' - x0)$ e, pelo Teorema de Euclides, $b_1 \mid (x' - x_0)$. Dessa forma, sabemos que existe $t \in \mathbb{Z}$ tal que $x' - x_0 = b_1 t$ e segue que

$$\begin{aligned} x' &= x_0 + \frac{b}{d}t, \\ &= r\frac{c}{d} + \frac{b}{d}t. \end{aligned}$$

Substituindo $x' - x_0 = b_1 t$, obtemos que

$$\begin{aligned} a_1\,(x' - x_0) &= b_1\,(y_0 - y')\,, \\ a_1 b_1 t &= b_1\,(y_0 - y')\,, \\ a_1 t &= y_0 - y', \\ y' = s\frac{c}{d} - \frac{a}{d}t. \end{aligned}$$

Assim concluímos a demonstração. ■

§16: Congruências Módulo m

Definição 55 [Congruência Módulo m]**:**
Sejam $m, a, b \in \mathbb{Z}, m \neq 0$. Diremos que a e b são *congruentes módulo* m, e escreveremos $a \equiv b \pmod{m}$, se, e somente se, $m \mid a - b$. Se a e b não forem congruentes módulo m, *i.e.*, $m \nmid a - b$, escreveremos $a \not\equiv b \pmod{m}$. ♠

Observação:
Perceba que a Definição 55 é equivalente a afirmar que $a \equiv b \pmod{m} \Leftrightarrow a = b + mq, q \in \mathbb{Z}$. Além disso, como $m \mid a - b \Leftrightarrow |m| \mid a - b$, pode-se tratar sem perda de generalidade apenas o caso $m > 0$. ♣

Proposição 183:
Seja $m \in \mathbb{Z}_+^*$. Dois inteiros a e b são congruentes módulo m se, e somente se, ambos tem como resto o mesmo inteiro ao serem divididos por m. □

Demonstração:
Suponhamos que $a \equiv b \pmod{m}$. Sabemos do Algoritmo da Divisão que existem q_1, q_2, r_1, r_2 únicos tais que

$$a = mq_1 + r_1,\ 0 \leqslant r_1 < m,$$
$$b = mq_2 + r_2,\ 0 \leqslant r_2 < m.$$

Subtraindo a segunda equação da primeira, segue que

$$a - b = m(q_1 - q_2) + (r_1 - r_2),$$
$$r_1 - r_2 = m(q_2 - q_1) + (a - b),$$
$$\therefore m \mid r_1 - r_2 \Leftrightarrow m \mid a - b.$$

No entanto, como sabemos que $0 \leqslant r_i < m$, vem que

$$0 \leqslant r_i < m,$$
$$-m < -r_i \leqslant 0,$$
$$-m < r_1 - r_2 < m, \qquad -m < r_2 - r_1 < m,$$
$$\therefore 0 \leqslant |r_1 - r_2| < m.$$

Logo, $\nexists\, q' \in \mathbb{Z}^*; q'm = |r_1 - r_2|$. Afinal, pelo Lema 97,

$$0 \leqslant q'm < m \Rightarrow 0 \leqslant q' < 1 \Rightarrow q' = 0.$$

Assim vemos que $r_1 - r_2 = 0$ e, portanto, $r_1 = r_2$. Como $m \mid r_1 - r_2 \Leftrightarrow m \mid a - b$ e todo inteiro m divide 0, concluímos que $a \equiv b \pmod{m} \Leftrightarrow r_1 = r_2$. ■

Proposição 184:
Seja $m \in \mathbb{Z}_+^*$ *e sejam* $a, b \in \{i\}_{i=1}^{m-1}$. *Então* $a \equiv b \pmod{m} \Leftrightarrow a = b$. □

Demonstração:
Pelo Algoritmo da Divisão, sabemos que existem inteiros q_1, q_2, r_1, r_2 únicos tais que

$$a = mq_1 + r_1,\ 0 \leqslant r_1 < m,$$
$$b = mq_2 + r_2,\ 0 \leqslant r_2 < m.$$

Logo, como $a = 0 \cdot q_1 + a, 0 \leqslant a < m$ e $b = 0 \cdot q_2 + b, 0 \leqslant b < m$, vemos que a e b são os restos de suas respectivas divisões por m. Logo, pela Proposição 183, conclui-se que $a \equiv b \pmod{m} \Leftrightarrow a = b$. ■

Definição 56 [Sistema Completo de Resíduos Módulo m]**:**
Seja $\mathcal{A} = \{a_i\}_{i=1}^{m} \subset \mathbb{Z}$. Diremos que $\mathcal{A}$ é um *sistema completo de resíduos módulo* m se, e somente se, cada inteiro é congruente módulo m a um, e apenas um, dos elementos de $\mathcal{A}$. ♠

Proposição 185:
Seja $m \in \mathbb{Z}_+^*$. *O conjunto* $\mathcal{A} = \{n\}_{n=0}^{m-1}$ *é um sistema completo de resíduos módulo* m. □

Demonstração:
Tome $n \in \mathcal{A}$. Conforme a demonstração da Proposição 184, n é o resto da sua divisão por m. Pelo Algoritmo da Divisão, um inteiro qualquer z, ao ser dividido por m, terá um único resto r tal que $0 \leqslant r < m$, *i.e.*, um único resto em $\mathcal{A}$. Pela Proposição 183, z será congruente ao único $n \in \mathcal{A}$ ao qual seu resto se iguala. ■

Proposição 186:
Seja $m \in \mathbb{Z}_+^*$. *A congruência módulo* m *constitui uma relação de equivalência em* $\mathbb{Z}$. □

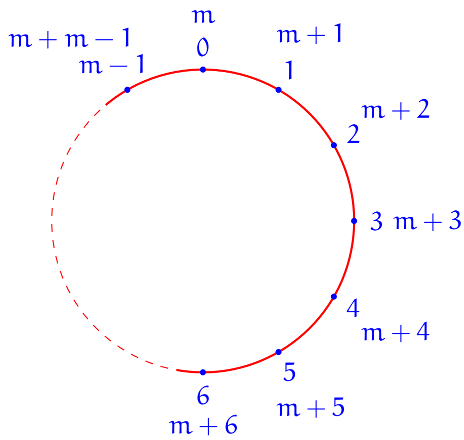

Figura 4.1: *Cada inteiro é congruente a um, e apenas um, dos números dispostos no círculo, de forma que podemos associar cada inteiro a um ponto. Note que isso é devido à Proposição* 185.

Demonstração:

Sejam $a, b, c \in \mathbb{Z}$. Como $a - a = 0$ e todo inteiro m divide 0, é claro que $a \equiv a \pmod{m}$. Além disso, como $m \mid a-b \Leftrightarrow m \mid b-a$, temos também que $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$.

Suponha que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$. Então o resto da divisão de a por m é igual ao resto da divisão de b por m (pela Proposição 183), que por sua vez é igual ao resto da divisão de c por m (pela mesma Proposição). Como o Algoritmo da Divisão garante a unicidade da divisão de um inteiro por outro, temos que o resto das divisões de a e c por m são iguais. Pela Proposição 183, $a \equiv c \pmod{m}$. ■

Teorema 187:

Sejam $a, b, c, d, , m \in \mathbb{Z}, m \neq 0$. *Valem as propriedades:*

i. $[a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}] \Rightarrow a + c \equiv b + d \pmod{m}$;

ii. $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$;

iii. $[a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}] \Rightarrow ac \equiv bd \pmod{m}$;

iv. $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$;

v. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{Z}_+^*$;

vi. $a + c \equiv b + c \pmod{m} \Rightarrow a \equiv b \pmod{m}$. □

Demonstração:

Faremos a demonstração item a item.

i.

$$\begin{aligned}
[a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}] &\Leftrightarrow [m \mid a - b \wedge m \mid c - d]\,, \\
&\Rightarrow (a = b + mq \wedge c = d + mp)\,, \\
&\Rightarrow a + c = b + d + m(p + q)\,, \\
&\Rightarrow a + c \equiv b + d \pmod{m}\,.
\end{aligned}$$

ii. Como, pela Proposição 186, $c \equiv c \pmod{m}$, segue do item i.

iii.

$$\begin{aligned}[a \equiv b \pmod m \wedge c \equiv d \pmod m] &\Rightarrow (a = b + mq \wedge c = d + mp)\,,\\ &\Rightarrow ac = (b + mq)(d + mp)\,,\\ &\Leftrightarrow ac = bd + m(qd + pb + mqp)\,,\\ &\Rightarrow ac \equiv bd \pmod m\,.\end{aligned}$$

iv. Como, pela Proposição 186, $c \equiv c \pmod m$, segue do item iii.

v. Para $n = 1$, vale trivialmente. Suponha que vale para algum $n \in \mathbb{Z}_+^*$. Então, por iii, $a^n \equiv b^n \pmod m \Rightarrow a^{n+1} \equiv b^{n+1} \pmod m$. Por indução, vale para todo inteiro positivo n.

vi.

$$\begin{aligned}a + c \equiv b + c \pmod m &\Leftrightarrow m \mid [(a + c) - (b + c)]\,,\\ &\Leftrightarrow m \mid (a - b)\,,\\ &\Leftrightarrow a \equiv b \pmod m\,.\end{aligned}$$

■

Proposição 188:
Sejam $a, b, c, m \in \mathbb{Z}, m \neq 0$. *Se* $\mathrm{mdc}(c, m) = 1$, *então* $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod m$. □

Demonstração:
$ac \equiv bc \pmod m \Leftrightarrow m \mid c(a - b)$. Como $\mathrm{mdc}(c, m) = 1$, o Teorema de Euclides garante que $m \mid a - b$. Logo, $a \equiv b \pmod m$. ■

Proposição 189:
Sejam $c, m \in \mathbb{Z}, m \neq 0$. *Se* $d = \mathrm{mdc}(c, m) \neq 1$, *existem inteiros* a, b *tais que* $ac \equiv bc \pmod m$, *mas não é necessário que* $a \equiv b \pmod m$. □

Demonstração:
Há dois casos: como $d \mid m$, é preciso que $d \leqslant m$. Logo, ou $d = m$ ou $d < m$.

Se $d = m$, então $m \mid c$. Logo, o resto da divisão de c por m é nulo e, portanto, $c \equiv 0 \pmod m$. Assim, dados $a, b \in \mathbb{Z}$ quaisquer, $m \mid c(a - b)$ e segue que $ac \equiv bc \pmod m$.

Se $d < m$, então sabemos que existem inteiros p e q tais que $m = pd$ e $c = qd$. Tem-se então que $m \mid cp$, visto que $cp = qdp = qm$ e $m \mid m$. Logo, $cp \equiv 0 \pmod m$, embora em geral não valha que $p \equiv 0 \pmod m$. ■

Observação:
Note que, dados $a, b \in \mathbb{Z}, b \neq 0$, podemos determinar o resto da divisão de a por b buscando o inteiro r tal que $0 \leqslant r < b$ e $a \equiv r \pmod m$. ♣

Observação:
Dada uma base numérica de $\mathbb{Z}$ (*e.g.*, a decimal), podemos determinar o algarism odas unidades de $a = \sum_{k=0}^{n} a_k m^k$ buscando o inteiro a_0 que satisfaz $0 \leqslant a_0 < m$ e $a \equiv a_0 \pmod m$. ♣

Exemplo [Critério de Divisibilidade]**:**
Seja $a \in \mathbb{Z}$, com $a = \sum_{k=0}^{m} a_k 10^k, 0 \leqslant a_k \leqslant 9$. Pode-se obter um critério para determinar se $3 \mid a$.

Note que $10 \equiv 1 \pmod 3$. Logo, $10^k \equiv 1 \pmod 3$ pelo Teorema 187. Pelo mesmo Teorema, $a_k 10^k \equiv a_k \pmod 3$. Temos então que $\sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} a_k \pmod 3$ e, portanto, $a \equiv$

$\sum_{k=0}^{m} a_k \pmod 3$. Vemos assim que existe $q \in \mathbb{Z}$ tal que

$$a = \sum_{k=0}^{m} a_k + 3q.$$

Logo, $3 \mid a \Leftrightarrow 3 \mid \sum_{k=0}^{m} a_k$. ♢

Proposição 190:

Sejam $a, b, r, s \in \mathbb{Z}, r, s \neq 0$. *Então* $a \equiv b \pmod r \Leftrightarrow as \equiv bs \pmod{rs}$. □

Demonstração:

Se $a \equiv b \pmod r$, então $a - b = rq$, para algum inteiro q. Logo, $as - bs = rsq$ e segue que $as \equiv bs \pmod{rs}$. Perceba que o argumento é inversível. ■

Proposição 191:

Sejam $m_1, m_2 \in \mathbb{Z}^*$ *relativamente primos e seja* a *um inteiro. Então*

$$a \equiv 0 \pmod{m_1 m_2} \Leftrightarrow a \equiv 0 \pmod{m_1} \wedge a \equiv 0 \pmod{m_2}.$$ □

Demonstração:

$\Rightarrow$:

$$\begin{gathered} a \equiv 0 \pmod{m_1 m_2}, \\ a = m_1 m_2 q, \quad q \in \mathbb{Z}, \\ \therefore m_1 \mid a \Rightarrow a \equiv 0 \pmod{m_1}, \\ \therefore m_2 \mid a \Rightarrow a \equiv 0 \pmod{m_2}. \end{gathered}$$

$\Leftarrow$:

$$\begin{gathered} a \equiv 0 \pmod{m_1} \wedge a \equiv 0 \pmod{m_2}, \\ a = m_1 q \wedge a = m_2 p. \end{gathered}$$

Como $\mathrm{mdc}(m_1, m_2) = 1$ e $m_2 \mid m_1 q = a$, vem do Teorema de Euclides que $m_2 \mid q$. Logo, existe $k \in \mathbb{Z}$ tal que $q = m_2 k$. Assim, $a = m_1 m_2 k$ e segue que $a \equiv 0 \pmod{m_1 m_2}$. ■

Proposição 192:

Seja $\{a_i\}_{i=1}^{m}$ *um sistema completo de resíduos módulo* m *e seja* $a \in \mathbb{Z}$ *tal que* $\mathrm{mdc}(a, m) = 1$. *Então valerá que* $\{a \cdot a_i\}_{i=1}^{m}$ *é um sistema completo de resíduos módulo* m. □

Demonstração:

Como $\{a_i\}_{i=1}^{m}$ é um sistema completo de resíduos módulo m, sabemos que $\forall\, i \,\exists\, j; a \cdot a_i \equiv a_j \pmod m$. Além disso, $a \cdot a_i \equiv a_j \pmod m \wedge a \cdot a_k \equiv a_j \pmod m \Rightarrow i = j$. Caso contrário, teríamos da Proposição 186 que $a \cdot a_i \equiv a \cdot a_k \pmod m$ e, do Teorema 187, vem que $a_i \equiv a_k \pmod m$. Como a_i e a_k são elementos de um sistema completo de resíduos módulo m, conclui-se que $a_i = a_k$.

Como todo inteiro é congruente módulo m a um, e apenas um, a_i e cada a_i é congruente módulo m a um, e apenas um, $a \cdot a_j$, percebe-se que cada inteiro há de ser congruente módulo m a um, e apenas um, $a \cdot a_j$, o que nos leva à conclusão de que $\{a \cdot a_j\}_{j=1}^{m}$ é, de fato, um sistema completo de resíduos módulo m. ■

Observação:

Dados $a, b, m \in \mathbb{Z}, m \neq 0$, diremos que uma solução da congruência $ax \equiv b \pmod m$ é um inteiro x que a satisfaça. ♣

Teorema 193:

A congruência $ax \equiv b \pmod m$ *tem solução se, e somente se,* $d = \mathrm{mdc}(a, m) \mid b$. □

Demonstração:

$ax \equiv b \pmod{m} \Leftrightarrow \exists\, y \in \mathbb{Z}; ax = b - my$. Ou seja, um certo inteiro x resolverá a congruência $ax \equiv b \pmod{m}$ se, se somente se, houver $y \in \mathbb{Z}$ tal que x e y resolvam a equação diofantina $ax + my = b$. Pela Proposição 181, isso ocorrerá se, e somente se, $\mathrm{mdc}\,(a, m) \mid b$. ■

Proposição 194:

Sejam $a, b, m \in \mathbb{Z}, m \neq 0$. *As soluções da congruência* $ax \equiv b \pmod{m}$ *são*

$$x = r\frac{b}{d} + \frac{m}{d}t, \qquad t \in \mathbb{Z},$$

onde $r \in \mathbb{Z}$ *é algum inteiro tal que* $\mathrm{mdc}\,(a, m) = ra + sm$ *(cuja existência é garantida pelo Teorema de Bézout).* □

Demonstração:

$x_0 \in \mathbb{Z}$ resolve $ax \equiv b \pmod{m}$ se, e somente se, houver $y_0 \in \mathbb{Z}$ que resolva $ax + my = b$. Como todas as soluções desta equação diofantina são

$$x = r\frac{b}{d} + \frac{m}{d}t,\ y = s\frac{b}{d} - \frac{a}{d}t, \qquad t \in \mathbb{Z},$$

segue que as soluções da congruência são

$$x = r\frac{b}{d} + \frac{m}{d}t, \qquad t \in \mathbb{Z}.$$ ■

Teorema 195:

Sejam $a, b, m \in \mathbb{Z}, m \neq 0$, *com* $d = \mathrm{mdc}\,(a, m) \mid b$. *Escrevendo* $d = ra + sm$, *com* $r, s \in \mathbb{Z}$, *a congruência* $ax \equiv b \pmod{m}$ *admite* d *soluções não congruentes, duas a duas, módulo* m. *Estas soluções são*

$$x = r\frac{b}{d} + \frac{m}{d}t, \qquad t \in \{i\}_{i=0}^{d-1}.$$

Além disso, toda outra solução da congruência é congruente a uma dessas. □

Demonstração:

Sabemos, da Proposição 194, que toda solução é da forma

$$x_t = r\frac{b}{d} + \frac{m}{d}t, \qquad t \in \mathbb{Z}.$$

Mostremos que toda solução é congruente a uma com $t \in \{i\}_{i=0}^{d-1}$. Como, pela Proposição 185, $\{i\}_{i=0}^{d-1}$ é um sistema completo de resíduos módulo d, sabemos que $\forall\, t \in \mathbb{Z}, \exists!\, k \in \{i\}_{i=0}^{d-1}; t \equiv k \pmod{m}$. Usando reiteradamente o Teorema 187, teremos que

$$\begin{aligned} t &\equiv k \pmod{m}, \\ \frac{m}{d}t &\equiv \frac{m}{d}k \pmod{m}, \\ r\frac{b}{d} + \frac{m}{d}t &\equiv r\frac{b}{d} + \frac{m}{d}k \pmod{m}. \end{aligned}$$

Assim vemos que, de fato, toda solução da congruência é congruente módulo m a uma das apresentadas. Resta provarmos que existem realmente d soluções distintas módulo m. Para tanto, suponhamos que existam x_h, x_k tais que $x_h \equiv x_k \pmod{m}$, com $0 \leqslant h \leqslant k < d$. Perceba que

$$
\begin{aligned}
r\frac{b}{d} + \frac{m}{d}h &\equiv r\frac{b}{d} + \frac{m}{d}k \pmod{m}, \\
\frac{m}{d}h &\equiv \frac{m}{d}k \pmod{m}, && \text{(Teorema 187)} \\
m \cdot \alpha &= \frac{m}{d}h - \frac{m}{d}k, \\
m &\mid \frac{m}{d}(k-h).
\end{aligned}
$$

Como, por hipótese, $0 \leqslant k - h < d$, teremos então que $0 \leqslant \frac{m}{d}(k-h) < \frac{m}{d}d = m$. Contudo, visto que $m \mid \frac{m}{d}(k-h)$, sabemos que ou $m \leqslant \frac{m}{d}(k-h)$ (o que é impossível pela desigualdade anterior) ou $\frac{m}{d}(k-h) = 0$. Segue que $h = k$. Portanto, concluímos que duas soluções distintas dentre as apresentadas não podem ser congruentes módulo m entre si e, como $\left|\{i\}_{i=0}^{d-1}\right| = d$, concluímos que existem d soluções não congruentes, duas a duas, módulo m e que toda outra solução é congruente módulo m a uma destas, provando a tese. ■

Corolário 196:

Sejam $a, m \in \mathbb{Z}$ relativamente primos e seja $b \in \mathbb{Z}$. A congruência $ax \equiv b \pmod{m}$ tem sempre solução. Ademais, escrevendo $1 = ra + sm$, ter-se-á que $x = rb$ é a única solução congruente módulo m, i.e., *toda outra solução é congruente módulo m a esta.* □

Demonstração:

Do Teorema 195, sabemos que a congruência admite uma única solução congruente módulo m, que será dada por $x = r\frac{b}{1} = rb$. Isso conclui a demonstração. ■

Teorema 197:

Sejam $a, b, m \in \mathbb{Z}$, $m \neq 0$, com $d = \mathrm{mdc}(a, m) \mid b$. Escrevendo $d = ra + sm$, a congruência $ax \equiv b \pmod{m}$ é equivalente à congruência $x \equiv r\frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$, i.e., *ambas tem as mesmas soluções.* □

Demonstração:

Como $d = \mathrm{mdc}(a, m) \mid b$, sabemos que existem $a', b' \in \mathbb{Z}$ tais que

$$a = a'd, \quad b = b'd.$$

Tem-se então que

$$
\begin{aligned}
ax &\equiv b \pmod{m}, \\
a'xd &\equiv b'd \pmod{m'd}, \\
a'x &\equiv b' \pmod{m'}. && \text{(Proposição 190)}
\end{aligned}
$$

Pelo Teorema 187, sabe-se então que $ra'x \equiv rb' \pmod{m'}$. Contudo, como $d = ra + sm = ra'd + sm'd$, tem-se que $1 = ra' + sm'$. Portanto, $ra' \equiv 1 \pmod{m'}$ e segue do Teorema 187 que $ra'x \equiv x \pmod{m'}$. Logo, pela Proposição 186 obtemos que $x \equiv rb' \pmod{m'}$.

Como $\mathrm{mdc}(m', r) = 1$ (pois caso contrário $1 = ra' + sm'$ teria um divisor maior que 1), o argumento é reversível, o que conclui a prova. ■

Teorema 198 [Teorema Chinês do Resto]**:**

Sejam $n_1, \ldots, n_k \in \mathbb{Z}^*$ relativamente primos dois a dois e sejam $c_1, \ldots, c_k \in \mathbb{Z}$. Então o sistema de congruências lineares

$$
\begin{cases}
x \equiv c_1 \pmod{n_1} \\
x \equiv c_2 \pmod{n_2} \\
\qquad \vdots \\
x \equiv c_k \pmod{n_k}
\end{cases}
$$

admite uma solução única módulo $n = \prod_i n_i$. □

Demonstração:

Para cada índice i, denotaremos $N_i = \frac{\prod_j n_j}{n_i}$. Pela hipótese de serem relativamente primos dois a dois, teremos que $\mathrm{mdc}\,(N_i, n_i) = 1$. Logo, existem $r_i, s_i \in \mathbb{Z}$ tais que $1 = r_i N_i + s_i n_i, 1 \leqslant i \leqslant k$.

Como $i \neq j \Rightarrow n_i \mid N_j, N_j \equiv 0 \pmod{n_i}$. Pelo Teorema 187, ter-se-á que $c_j r_j N_j \equiv 0 \pmod{n_i}$, para $i \neq j$. Usando Teorema 187 novamente, obtemos que

$$\sum_{j=0}^{k} c_j r_j N_j \equiv c_i r_i N_i \pmod{n_i}.$$

Contudo, como $r_i N_i + s_i n_i = 1$, vale que $r_i N_i \equiv 1 \pmod{n_i}$ e, novamente pelo Teorema 187, $c_i r_i N_i \equiv c_i \pmod{n_i}$ e, da Proposição 186, tem-se que $\sum_{j=0}^{k} c_j r_j N_j \equiv c_i \pmod{n_i}$. Portanto, $x_0 = \sum_{j=0}^{k} c_j r_j N_j$ soluciona o sistema. Resta provar que esta solução é única módulo $n = \prod_i n_i$.

Seja x solução do sistema, *i.e.*, $x \equiv c_i \pmod{n_i}, 1 \leqslant i \leqslant k$. Como $x_0 \equiv c_i \pmod{n_i}$, a Proposição 186 garante que $x \equiv x_0 \pmod{n_i} \Rightarrow n_i \mid (x - x_0)$. Como os n_i são dois a dois primos entre si, segue da Proposição 144 que $\prod_i n_i \mid (x - x_0)$ e, portanto, $x \equiv x_0 \pmod{n}$. ■

Observação:

A hipótese feita no Teorema 198 de que $\mathrm{mdc}\,(n_i, n_j) = 1$, para $i \neq j$, é usada para garantir a existência de solução para o sistema. Sua ausência requer a análise caso a caso. ♣

Proposição 199:

Sejam $a, b \in \mathbb{Z}$ *e* $m, n \in \mathbb{Z}^*$. *O sistema de congruências*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

admite solução se, e somente se, $\mathrm{mdc}\,(m, n) \mid (a - b)$. *Ademais, esta solução é única módulo* $\mathrm{mmc}\,(m, n)$. □

Demonstração:

$\Rightarrow$: suponhamos que o sistema tenha solução. Então veja que

$$\begin{gathered} x \equiv a \pmod{m} \Rightarrow x = a + my, \\ x \equiv b \pmod{n} \Rightarrow a + my \equiv b \pmod{n}, \\ \therefore my \equiv b - a \pmod{n}. \end{gathered}$$

Como o sistema, por hipótese, admite solução, sabemos que $\mathrm{mdc}\,(m, n) \mid (b - a)$ e, por consequência, $\mathrm{mdc}\,(m, n) \mid (a - b)$.

$\Leftarrow$: suponha que $\mathrm{mdc}\,(m, n) \mid (a - b)$. Então a congruência $my \equiv b - a \pmod{n}$ admite solução. Vê-se assim que existe $y \in \mathbb{Z}$ tal que $a + my \equiv b \pmod{n}$.

Ao definir $x := a + my$, podemos escrever $x \equiv b \pmod{n}$. É simples constatar que também vale que $x \equiv a \pmod{m}$. Assim provamos que o sistema

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

admite uma solução. Resta provarmos que esta é única módulo $\mathrm{mmc}\,(m, n)$.

Sejam x e x' soluções do sistema. Então

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \\ x' \equiv a \pmod{m} \\ x' \equiv b \pmod{n} \end{cases},$$
$$\begin{cases} x \equiv x' \pmod{m} \\ x \equiv x' \pmod{n} \end{cases},$$
$$\begin{cases} m \mid (x - x') \\ n \mid (x - x') \end{cases},$$
$$\frac{mn}{\operatorname{mdc}(m, n)} \mid (x - x'), \qquad \text{(Proposição 144)}$$
$$\frac{|m| \cdot |n|}{\operatorname{mdc}(m, n)} \mid (x - x'),$$
$$\operatorname{mmc}(m, n) \mid (x - x'), \qquad \text{(Teorema 153)}$$
$$\therefore x \equiv x' \pmod{\operatorname{mmc}(m, n)}. \qquad \blacksquare$$

Teorema 200 [Pequeno Teorema de Fermat]**:**
Sejam p *um primo e* $a \in \mathbb{Z}$ *tais que* $p \nmid a$. *Então* $p \mid a^{p-1} - 1$. □

Escrever demonstração!

Demonstração:
Primeiramente, perceba que $p \mid a^{p-1} - 1 \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$. ■

Glossário de Definições

Adição ($\mathbb{N}$)

Seja m um número natural dado. Então definimos a soma, também chamada de adição e denotada por $+$, de m com outro número natural por

i. $m + 0 = m$;
ii. $m + \sigma(n) = \sigma(m + n), \forall\, n \in \mathbb{N}$.

Adição ($\mathbb{Z}$)

Sejam $\alpha = [(a, b)], \beta = [(c, d)] \in \mathbb{Z}$. Definimos a adição, ou soma, de α e β, por $\alpha + \beta := [(a + c, b + d)]$.

Antecessor ($\mathbb{N}$)

Seja $n \in \mathbb{N}^*$. Dizemos que o número natural m que satisfaz $m = \sigma(n)$ é o antecessor de n e que n é o sucessor de m. Também dizemos que m antecede n e que n sucede m.

Boa Ordem

Seja A um conjunto e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que $\preccurlyeq$ é uma boa ordem se, e somente se, todo subconjunto não-vazio de A admitir mínimo. Ou seja,

$$\forall\, B \subseteq A, B \neq \varnothing, \exists\, x \in B; \forall\, y \in B, x \preccurlyeq y.$$

Classe de Equivalência

Sejam A um conjunto, $\sim$ uma relação de equivalência em A e $x \in A$. Denominaremos classe de equivalência de x, denotada por $[x]$, o conjunto definido por

$$[x] := \{y \in A; y \sim x\}.$$

Congruência Módulo m

Sejam $m, a, b \in \mathbb{Z}, m \neq 0$. Diremos que a e b são congruentes módulo m, e escreveremos $a \equiv b \pmod{m}$, se, e somente se, $m \mid a - b$. Se a e b não forem congruentes módulo m, *i.e.*, $m \nmid a - b$, escreveremos $a \not\equiv b \pmod{m}$.

Conjunto Limitado

Seja A um conjunto, $B \subseteq A$ e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que B é limitado superiormente (inferiormente) se admitir majorante (minorante).

Conjunto Quociente

Seja A um conjunto e $\sim$ uma relação de equivalência em A. Definimos o conjunto quociente de A por $\sim$, denotado por $A/\!\sim$, como o conjunto formado por todas as classes de equivalência determinadas por $\sim$ em A, *i.e.*,

$$A/\!\sim\, := \{[x]; x \in A\}.$$

Contradomínio de uma Função

Sejam A, B conjuntos e $f: A \to B$ uma função. Diremos que B é o contradomínio de f.

Decomposição

Seja A um conjunto. Uma decomposição, ou partição, de A é uma família $\mathscr{A}$ de subconjuntos não-vazios de A, dois a dois disjuntos, cuja união é o próprio A. Isto é, uma família de subconjuntos de A satisfazendo:

i. $\forall\, S, T \in \mathscr{A}, S \neq T \Rightarrow S \cap T = \varnothing$;
ii. $\bigcup \mathscr{A} = A$;
iii. $\forall\, S \in \mathscr{A}, S \neq \varnothing$.

Decomposição em Fatores Primos

Seja $a > 1$ um inteiro e seja $p_1 \cdots p_n = a$, com $p_i, i = 1, \ldots, n$, números primos. Diremos que $p_1 \cdots p_n$ é uma decomposição em fatores primos de a e diremos que n, *i.e.*, o número de elementos usados na decomposição, é o comprimento da decomposição.

Divisibilidade

Sejam $a, b \in \mathbb{Z}$. Diremos que b é divisível por a, ou que a divide b, se, e somente se, existir $x \in \mathbb{Z}$ tal que $a \cdot x = b$. Neste caso, escreveremos $a \mid b$. Se a não dividir b, escreveremos $a \nmid b$.

Divisor

Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$. Diremos que a é divisor de b se, e somente se, $a \mid b$. Ver também *Quociente*, *Divisibilidade*.

Divisor Comum

Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Diremos que um inteiro c é um divisor comum de a e b se, e somente se, $c \mid a \wedge c \mid b$. Denotamos o conjunto de todos os divisores comuns de a e b por $D(a, b) := \{c \in \mathbb{Z}; c \mid a \wedge c \mid b\}$. Ver também *Divisor*.

Divisor Próprio

Seja c um número composto. Diremos que um inteiro b tal que $b \mid c$ e $1 < |b| < |c|$ é um divisor próprio de c. Ver também *Número Composto*.

Domínio de uma Relação

Sejam A, B conjuntos e R uma relação entre A e B. Definimos o domínio de R, $\operatorname{Dom} R$, da maneira seguinte:

$$\operatorname{Dom} R := \{a \in A; (a, b) \in R, b \in B\}.$$

Elemento Nulo ($\mathbb{N}$)

Devido à Proposição 7 diremos que 0 é o elemento neutro aditivo, ou elemento nulo, de $\mathbb{N}$.

Equação Diofantina

Diremos que uma equação polinomial a coeficientes inteiros em uma ou mais variáveis é uma equação diofantina quando nos interessarmos apenas por suas soluções inteiras. Em especial, diremos que uma equação diofantina é linear se for uma soma de monômios de grau 1 ou 0 igualada a um inteiro.

Estritamente Menor ($\mathbb{N}$)

Sejam $m, n \in \mathbb{N}$. Diremos que m é menor (ou estritamente menor) que n, e escreveremos $m < n$, se valerem simultaneamente as seguintes condições:

i. $m \leqslant n$;

ii. $m \neq n$.

Se $m < n$, também dizemos que n é maior (ou estritamente maior) que m e escrevemos $n > m$, onde $>$ denota a relação inversa de $<$.

Estritamente Menor ($\mathbb{Z}$)

Definimos a relação $<$ em $\mathbb{Z}$ como a ordem correspondente de $\leqslant$. Pela Proposição 31 e pela Proposição 27, $<$ é uma relação de ordem total estrita em $\mathbb{Z}$.

Fatoriais ($\mathbb{Z}$)

Seja $n \in \mathbb{Z}_+$. Definimos o fatorial de n por

i. $0! := 1$;

ii. $(n+1)! := (n+1) \cdot n!$.

Função

Sejam A, B dois conjuntos e f uma relação binária entre A e B. Diremos que f é uma função de A em B se satisfizer:

i. $\operatorname{Dom} f = A$;

ii. $\forall\, a \in A, ((a,b) \in f \wedge (a,b') \in f) \Rightarrow b = b'$.

Função Bijetora

Sejam A, B conjuntos e $f\colon A \to B$ uma função. Diremos que f é uma função bijetora se, e somente se, f for injetora e sobrejetora.

Função Injetora

Sejam A, B conjuntos e $f\colon A \to B$ uma função. Diremos que f é uma função injetora se $f(a) = f(a') \Rightarrow a = a'$.

Função Inversível

Sejam A, B conjuntos e $f\colon A \to B$ uma função. Diremos que f é inversível se sua relação inversa for uma função.

Função Sobrejetora

Sejam A, B conjuntos e $f\colon A \to B$ uma função. Diremos que f é uma função sobrejetora se sua imagem coincidir com o seu contradomínio, *i.e.*, $\operatorname{Ran} f = B$.

Ideal de $\mathbb{Z}$

Seja $J \subseteq \mathbb{Z}$ não-vazio. Diremos que J é um ideal de $\mathbb{Z}$ se satisfizer as seguintes condições:

i. $a, b \in J \Rightarrow a + b \in J$;

ii. $a \in J, x \in \mathbb{Z} \Rightarrow a \cdot x \in J$.

Identidade ($\mathbb{N}$)

Devido à Proposição 15 diremos que 1 é o elemento neutro multiplicativo, ou identidade, de $\mathbb{N}$.

Imagem de uma Relação

Sejam A, B conjuntos e R uma relação entre A e B. Definimos a imagem de R, $\operatorname{Ran} R$, da maneira seguinte:

$$\operatorname{Ran} R := \{b \in B; (a,b) \in R, a \in A\}.$$

Incomparabilidade

Seja A um conjunto e R uma relação sobre A. Dizemos que dois elementos $x, y \in A, x \neq y$, são incomparáveis por R, e escrevemos $x \parallel y$, se, e somente se, $(x, y), (y, x) \notin R$. Se dois elementos não são incomparáveis por R, dizemos que são comparáveis por R e escrevemos $x \nparallel y$.

Inteiros Consecutivos

Seja $\{a_i\}_{i=1}^{n}$, $n \in \mathbb{Z}_+^*$ um conjunto de números inteiros. Diremos que os inteiros a_i são consecutivos se, e somente se, $a_{i+1} = a_i + 1, \forall\, i \in \{i\}_{i=1}^{n-1}$.

Mínimo

Seja A um conjunto e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que um elemento $x \in A$ é um mínimo ou primeiro elemento de A se, e somente se, $x \preccurlyeq y, \forall\, y \in A$.

Mínimo Múltiplo Comum

Sejam $a, b \in \mathbb{Z}^*$. Diremos que $\min M^+(a, b)$, *i.e.*, o mínimo dos múltiplos comuns positivos de a e b, é o mínimo múltiplo comum de a e b. Além disso, utilizaremos a notação $\text{mmc}\,(a, b) \equiv \min M^+(a, b)$. Ver também *Múltiplo Comum*, *Múltiplo*.

Majorante

Seja A um conjunto, $B \subseteq A$ e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que um elemento $z \in A$ é um majorante, ou uma cota superior, de B se, e somente se, $y \preccurlyeq z, \forall\, y \in B$.

Máximo

Seja A um conjunto e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que um elemento $z \in A$ é um máximo ou último elemento de A se, e somente se, $y \preccurlyeq z, \forall\, y \in A$.

Máximo Divisor Comum

Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Diremos que $\max D(a, b)$, *i.e.*, o máximo dos divisores comuns de a e b, é o máximo divisor comum de a e b. Além disso, utilizaremos a notação $\text{mdc}\,(a, b) \equiv \max D(a, b)$. Ver também *Divisor Comum*, *Divisor*.

Menor ou Igual ($\mathbb{N}$)

Sejam $m, n \in \mathbb{N}$. Diremos que m é menor ou igual a n, e escreveremos $m \leqslant n$, se existir $p \in \mathbb{N}$ tal que $m + p = n$. Se $m \leqslant n$, também dizemos que n é maior ou igual a m e escrevemos $n \geqslant m$, onde $\geqslant$ denota a relação inversa de $\leqslant$.

Menor ou Igual ($\mathbb{Z}$)

Sejam $\alpha = [(a, a')]$ e $\beta = [(b, b')]$ números inteiros. Diremos que α é menor ou igual a β, e escreveremos $\alpha \leqslant \beta$, se $a + d \leqslant b + c$. Neste caso, também diremos que β é maior ou igual a α e escreveremos $\beta \geqslant \alpha$, onde $\geqslant$ denota a relação inversa de $\leqslant$.

Minorante

Seja A um conjunto, $B \subseteq A$ e $\preccurlyeq$ uma relação de ordem parcial ampla sobre A. Diremos que um elemento $x \in A$ é um minorante, ou uma cota inferior, de B se, e somente se, $x \preccurlyeq y, \forall\, y \in B$.

Módulo ($\mathbb{Z}$)

Ver *Valor Absoluto ($\mathbb{Z}$)*.

Multiplicação ($\mathbb{N}$)

Seja $m \in \mathbb{N}$ um número natural dado. Então definimos o produto, também chamado de multiplicação e denotado por $\cdot$, de m com outro número natural por

i. $m \cdot 0 = 0$;

ii. $m \cdot \sigma(n) = (m \cdot n) + m, \forall\, n \in \mathbb{N}$.

Multiplicação ($\mathbb{Z}$)

Sejam $\alpha = [(a, b)]\,, \beta = [(c, d)] \in \mathbb{Z}$. Definimos a multiplicação, ou produto, de α e β, por $\alpha \cdot \beta := [(ac + bd, ad + bc)]$.

Múltiplo

Seja a um inteiro não-nulo. Diremos que um inteiro m é um múltiplo de a se, e somente se, existir um inteiro q tal que $m = a \cdot q$, *i.e.*, se $a \mid m$.

Múltiplo Comum

Sejam $a, b \in \mathbb{Z}^*$. Diremos que um inteiro c é um múltiplo comum de a e b se, e somente se, $a \mid c \wedge b \mid c$. Denotaremos o conjunto de todos os múltiplos comuns de a e b por $M(a, b) := \{c \in \mathbb{Z}; a \mid c \wedge b \mid c\}$. Indicaremos por o conjunto de todos os múltiplos comuns positivos de a e b por $M^+(a, b) := \{m \in M(a, b); m > 0\}$. Ver também *Múltiplo*.

Número Composto

Seja $c \in \mathbb{Z}^* \setminus \{-1, 1\}$. Se c for não-primo, diremos que c é um número composto. Ver também *Número Primo*.

Número Negativo ($\mathbb{Z}$)

Seja $\alpha \in \mathbb{Z}$. Diremos que α é negativo se, e somente se, $0 > \alpha$.

Número Positivo ($\mathbb{Z}$)

Seja $\alpha \in \mathbb{Z}$. Diremos que α é positivo se, e somente se, $0 < \alpha$.

Número Primo

Seja $p \in \mathbb{Z}$. Diremos que p é primo se, e somente se, tiver exatamente dois divisores positivos: 1 e $|p|$. Ver também *Número Composto*.

Números Combinatórios

Sejam $n, k \in \mathbb{Z}_+, k \leqslant n$. Seja A um conjunto tal que $|A| = n$. Denotaremos o números de subconjuntos de A com k elementos por $\binom{n}{k}$ e leremos combinações de n elementos tomados k a k, ou ainda n escolhe k. Trataremos estes números como inteiros.

Números Inteiros

Doravante utilizaremos a notação $\mathbb{Z} \equiv \mathbb{N} \times \mathbb{N}/\sim$ e iremos nos referenciar aos elementos de $\mathbb{Z}$ como números inteiros, ou simplesmente inteiros.

Oposto ($\mathbb{Z}$)

Dado $\alpha = [(a, a')] \in \mathbb{Z}$, definimos o oposto de α, denotado por $-\alpha$, segundo $-\alpha := [(a', a)]$. A motivação para esta definição flui da demonstração da Proposição 59.iii.

Ordem Correspondente

Seja A um conjunto com uma relação de ordem parcial ampla ou estrita. Definimos a ordem correspondente à primeira segundo

i. se $\preccurlyeq$ é uma relação de ordem parcial ampla sobre A, sua ordem correspondente $\prec$ é definida por $x \prec y \Leftrightarrow (x \preccurlyeq y \wedge x \neq y), \forall x, y \in A$;

ii. se $\prec$ é uma relação de ordem parcial estrita sobre A, sua ordem correspondente $\preccurlyeq$ é definida por $x \preccurlyeq y \Leftrightarrow (x \prec y \vee x = y), \forall x, y \in A$.

Ordem Parcial Ampla

Seja A um conjunto e $R \subseteq A \times A$ uma relação binária em A. Diremos que R é uma relação de ordem parcial ampla em A se satisfizer as seguintes condições:

i. $\forall x \in A, (x, x) \in R$, *i.e.*, todo elemento de A está relacionado consigo mesmo (reflexividade);

ii. $\forall x, y \in A, ((x, y) \in R \wedge (y, x) \in R) \Rightarrow x = y$ (antissimetria);

iii. $\forall x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$ (transitividade).

Ordem Parcial Estrita

Seja A um conjunto e $R \subseteq A \times A$ uma relação binária em A. Diremos que R é uma relação de ordem parcial estrita em A se satisfizer as seguintes condições:

i. $\forall x \in A, (x, x) \notin R$, *i.e.*, nenhum elemento de A está relacionado consigo mesmo (irreflexividade);

ii. $\forall x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$ (transitividade).

Ordem Total

Seja A um conjunto e R uma relação de ordem parcial, estrita ou ampla, sobre A. Diremos que R é uma relação de ordem total (ampla ou estrita) sobre A se todos os elementos de A foram comparáveis por R. De forma mais específica,

i. se A é um conjunto e $\preccurlyeq$ é uma relação de ordem parcial ampla sobre A, diremos que $\preccurlyeq$ é uma relação de ordem total ampla sobre A se, e somente se, valer a dicotomia:

$$\forall x, y \in A, (x \preccurlyeq y \vee y \preccurlyeq x);$$

ii. se A é um conjunto e $\prec$ é uma relação de ordem parcial estrita sobre A, diremos que $\prec$ é uma relação de ordem total estrita sobre A se, e somente se, valer a tricotomia:

$$\forall x, y \in A, (x = y \vee x \prec y \vee y \prec x).$$

Potências ($\mathbb{Z}$)

Seja $a \in \mathbb{Z}$. Definimos as potências de a com expoente positivo por

i. $a^1 := 0$;

ii. $a^{n+1} := a \cdot a^n, \forall n \geqslant 0$.

Ademais, se $a \neq 0$, definimos $a^0 := 1$ por conveniência.

Progressão Geométrica

Se uma sequência de inteiros for tal que $a_{i+1} = a_i \cdot r$, para algum $r \neq 1$ inteiro, diremos que tal sequência é uma progressão geométrica (abreviada como PG) de razão r.

Quadrado ($\mathbb{Z}$)

Seja $a \in \mathbb{Z}$. Definimos o quadrado de a, denotado a^2, como o número inteiro que satisfaz $a^2 = a \cdot a$.

Quociente

Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$ tais que $a \mid b$. Definimos o quociente de b, que será dito o dividendo, por a, que será dito o divisor, como o número inteiro c que resolve a equação $a \cdot c = b$. Em geral, denotaremos o quociente de b por a como

$$b/a \equiv \frac{b}{a}.$$

Ver também *Resto*, *Divisibilidade*.

Relação Binária

Sejam A e B conjuntos e seja o seu produto cartesiano $A \times B$. Diremos que um subconjuntos $R \subseteq A \times B$ é uma relação binária, ou simplesmente uma relação, entre A e B.

Relação de Equivalência

Seja A um conjunto e $R \subseteq A \times A$ uma relação. Diremos que R é uma relação de equivalência em A se satisfizer as seguintes condições:

i. $\forall x \in A, (x, x) \in R$ (reflexividade);
ii. $\forall x, y \in A, (x, y) \in R \Rightarrow (y, x) \in R$ (simetria);
iii. $\forall x, y, z \in A, ((x, y) \in R \wedge (y, z) \in R) \Rightarrow (x, z) \in R$ (transitividade).

Relação de Equivalência em $\mathbb{N} \times \mathbb{N}$

Considere o conjunto

$$\mathbb{N} \times \mathbb{N} = \{(m, n); m, n \in \mathbb{N}\}.$$

Definimos a relação $\sim$ em $\mathbb{N} \times \mathbb{N}$ de forma que, dados dois elementos $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$.

Relação Inversa

Sejam A e B conjuntos e R uma relação entre A e B. Definimos a relação inversa de R, R^{-1}, por

$$R^{-1} := \{(b, a) \in B \times A; (a, b) \in R\}.$$

Relativamente Primos

Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Diremos que a e b são relativamente primos, ou primos entre si, se, e somente se, $\text{mdc}\,(a, b) = 1$. Ver também *Número Primo*.

Resto

Sejam $a, b \in \mathbb{Z}, a \neq 0$. Os números q e r que satisfazem $b = aq + r$ são chamados, respectivamente, de quociente e resto da divisão de b por a. Note que isso estende a definição de quociente dada na Definição 40. Ver também *Quociente*.

Sistema Completo de Resíduos Módulo m

Seja $\mathcal{A} = \{a_i\}_{i=1}^{m} \subset \mathbb{Z}$. Diremos que $\mathcal{A}$ é um sistema completo de resíduos módulo m se, e somente se, cada inteiro é congruente módulo m a um, e apenas um, dos elementos de $\mathcal{A}$.

Um ($\mathbb{N}$)

Chamaremos de *um*, e indicaremos por 1, o sucessor de 0, *i.e.*, $1 \equiv \sigma(0)$.

Um ($\mathbb{Z}$)

Como o elemento $[(\sigma(m), m)] \in \mathbb{Z}$ herda a propriedade multiplicativa do um natural, denotamos esse número inteiro por 1 e também o denominamos um.

Valor Absoluto ($\mathbb{Z}$)

Seja $a \in \mathbb{Z}$. Definimos o valor absoluto de a, denotado por $|a|$, da seguinte maneira:

$$|a| := \begin{cases} a, \text{se } a \geqslant 0 \\ -a, \text{se } a < 0 \end{cases} .$$

Também usaremos a nomenclatura módulo de a ao falar sobre $|a|$.

Zero ($\mathbb{Z}$)

Como o elemento $[(a, a)] \in \mathbb{Z}$ herda a propriedade aditiva do zero natural, denotamos esse número inteiro por 0 e também o denominamos zero.

Bibliografia

1. Barata, J. C. A. *Notas para um Curso de Física-Matemática* http://denebola.if.usp.br/ (2018).
2. Deskins, W. E. *Abstract Algebra* ISBN: 9780486158464 (Dover Publications, 2013).
3. Herstein, I. N. *Topics in Algebra* 2nd Edition. ISBN: 9780471010906 (John Wiley & Sons, 1975).
4. Polcino Milies, C. & Coelho, S. P. *Números: Uma Introdução à Matemática* 248 pp. ISBN: 8531404584 (Edusp, São Paulo, 1998).
5. ProofWiki. *Definition:Partition (Set Theory)* [Acesso em 11 de julho de 2018]. https://proofwiki.org/w/index.php?title=Definition:Partition_(Set_Theory)&oldid=342420.
6. ProofWiki. *Equivalence of Well-Ordering Principle and Induction* [Acesso em 16 de julho de 2018]. https://proofwiki.org/wiki/Equivalence_of_Well-Ordering_Principle_and_Induction.
7. Tao, T. *Analysis I* ISBN: 9788185931623 (Hindustan Book Agency, 2006).
8. Wikipedia. *Integers* [Acesso em 14 de julho de 2018]. https://en.wikipedia.org/w/index.php?title=Integer&oldid=849675860.
9. Wikipédia. *Equação Diofantina* [Acesso em 21 de agosto de 2018]. https://pt.wikipedia.org/wiki/Equa%C3%A7%C3%A3o_diofantina.
10. Wikipédia. *Relação de Ordem* [Acesso em 28 de junho de 2018]. https://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o_de_ordem.

Adicionar Índice Remissivo?