Os números naturais $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$

1. Estão definidas as operações de soma $a + b$ e produto ab, ambas comutativas e associativas:

   $$a+b = b+a, \ (a+b)+c = a+(b+c) \qquad ab = ba, \ (ab)c = a(bc)$$

2. Existem os elementos neutros para a soma e para o produto

   $$0 + a = a, \qquad 1a = a \ \forall a \in \mathbb{N}$$

3. Vale a "lei do corte"

   $$ac = bc \wedge c \neq 0 \implies a = b$$

4. $a(b + c) = ab + ac$

Ordem

O conjunto $\mathbb{N}$ está dotado de uma relação de ordem

$$a \leq b \Leftrightarrow \exists n \in \mathbb{N} : a + n = b$$

Usamos a notação $a < b$ se $a \leq b$ e $a \neq b$.

5. $\leq$ é uma **relação de ordem total**: $\forall a, b \in \mathbb{N}$ verifica-se uma e uma só das condições

$$a < b \qquad b < a \qquad a = b$$

6. **Princípio da Boa Ordenação**: Se $X \subset \mathbb{N}$ é não vazio, então X tem um *primeiro elemento*:

$$\exists x_0 \in X : x < x_0 \implies x \notin X$$

Números Inteiros $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$

O conjunto dos inteiros satisfaz as propriedades 1. - 5. e além disso,

- $\forall a \in \mathbb{Z}\ \exists^1 (-a) \in \mathbb{Z} : a + (-a) = 0$
- $\forall a \in \mathbb{Z},\ a \in \mathbb{N} \vee -a \in \mathbb{N}$

$$0a = 0\, \forall a \in \mathbb{Z}$$

$$ab = 0 \implies a = 0 \vee b = 0$$

$$(-a)(-b) = ab$$

Conjuntos finitos e infinitos

Usaremos a notação

$$[m] = \{x \in \mathbb{N} : x < m\} = \{0, \cdots, m-1\}$$

Com esta notação $[0] = \emptyset$.

Um conjunto X diz-se finito se existe $m \in \mathbb{N}$ e uma bijecção

$$f : [m] \to X$$

Diz-se então que X tem m elementos ou que a **cardinalidade** de X é m, usando-se a notação $|X| = m$. Um conjunto X diz-se infinito se não for finito.

Conjuntos finitos e infinitos

Dado um conjunto X, as seguintes afirmações são equivalentes:

i) X é infinito;

ii) Existe uma função $f : \mathbb{N} \to X$ injectiva;

iii) Existe uma função $g : X \to X$ injectiva e não sobrejectiva.

Princípio de Indução Finita

Se $X \subset \mathbb{N}$ satisfaz as condições

$$\begin{array}{rcl} \textbf{(i)} & : & k_0 \in X, \\ \textbf{(ii)} & : & k \geq k_0, k \in X \implies k+1 \in X, \end{array}$$

então

$$X \supset \mathbb{N} \setminus [k_0] .$$

Princípio de Indução Finita: Se $P(n)$ é uma dada afirmação referente aos números naturais $n \in \mathbb{N}$ tal que :

i: *$P(k_0)$ é verdadeira;*

ii: *se $(k \geq k_0 \wedge P(k)) \implies P(k+1)$;*

então $P(n)$ é verdadeira para qualquer $n \geq k_0$.

Se é verdade para os primeiros naturais...

Seja O_n o conjunto dos naturais $k \leq n$ que são produto de um número ímpar de factores primos,
E_n o conjunto dos $k \leq n$ que são o produto de um número par de factores primos.

$|O_n| \geq |E_n| \; \forall \, 2 \leq n \leq 10^6$. Verdade para todo o n?
Falso para $n = 906180352$ e de facto $|O_n| - |E_n|$ troca de sinal infinitas vezes.

Existe algum $y \in \mathbb{N}$, maior que zero, tal que $1141y^2 + 1$ é um quadrado perfeito ? Há infinitas soluções mas a menor delas tem 26 algarismos.

Princípio de Indução Finita (Forte)

Se $P(n)$ é uma dada afirmação referente aos números naturais $n \in \mathbb{N}$ tal que :

i : $P(k_0)$ é verdadeira;

ii : $(k \geq k_0 \wedge P(k_0) \wedge P(k_0+1) \wedge \ldots \wedge P(k)) \implies P(k+1)$;

então $P(n)$ é verdadeira para qualquer $n \geq k_0$.