

Os números inteiros

Abordaremos algumas propriedades dos números inteiros, sendo de destacar o Algoritmo da Divisão e o Teorema Fundamental da Aritmética. Falaremos de algumas aplicações como sejam a detecção de erros e o sistema de encriptação de dados RSA.

Começamos por fixar alguma notação.

Conjunto dos números inteiros:

$$\mathbb{Z} = \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, \dots\}$$

Conjunto dos números inteiros positivos ou naturais:

$$\mathbb{Z}^+ = \mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

Conjunto dos números inteiros não negativos:

$$\mathbb{Z}_0^+ = \mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

Relembramos agora diversas noções importantes.

Um número inteiro t , diferente de zero, diz-se **divisor** de um inteiro s se existe um inteiro u tal que $s = tu$. Escreve-se $t \mid s$ e lê-se “ t divide s ”. Se t não divide s escreve-se $t \nmid s$.

Um número inteiro s diz-se **múltiplo** de um número inteiro t se existe um inteiro u tal que $s = tu$. Note-se que s é múltiplo de t se e só se t divide s .

Um número inteiro positivo, maior do que 1, diz-se **primo** se os seus únicos divisores positivos são o 1 e ele próprio.

Da definição de divisor resulta imediatamente a seguinte observação.

Lema

Sejam a , b e c inteiros.

- (i) *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*
- (ii) *Se $a \mid b$, então $a \mid bc$.*
- (iii) *Se $a \mid b$ e $a \mid c$, então $a \mid b + c$.*
- (iv) *Se $a \mid b$ e $b \mid a$, então $a = \pm b$.*
- (iv') *Se $a \mid 1$, então $a = \pm 1$.*
- (v) *Se $a, b \in \mathbb{N}$ e $a \mid b$, então $a \leq b$.*

Princípio de Boa Ordenação

Para o estudo das propriedades dos números inteiros vamos admitir como axioma o Princípio de Boa Ordenação em $\mathbb{Z}$, dado que não é possível provar este princípio a partir das propriedades aritméticas elementares dos inteiros.

Axioma (Princípio de Boa Ordenação)

Qualquer conjunto P não-vazio de inteiros positivos tem mínimo m , isto é, $\exists m \in P$ tal que $\forall x \in P \quad m \leq x$.

O conjunto P mencionado no Axioma anterior pode não consistir somente de números inteiros positivos, como se afirma na proposição seguinte.

Proposição

Qualquer conjunto não-vazio de inteiros tem mínimo (respectivamente, máximo) desde que seja minorado (respectivamente, majorado).

O Princípio de Boa Ordenação é equivalente a qualquer uma das formas do Princípio de Indução Matemática que se apresentam a seguir.

Proposição (Princípio de Indução Matemática - Primeira forma)

Sejam S um conjunto de inteiros e a um número inteiro. Se

(i) $a \in S$ e

(ii) se $n \in S$ e $n \geq a$, então $n + 1 \in S$,

então S contém todos os inteiros maiores ou iguais a a .

Demonstração. Seja S um conjunto de inteiros e a um elemento de S . Suponhamos que S tem a seguinte propriedade: Se um qualquer inteiro $n \geq a$ pertence a S , então o inteiro $n + 1$ pertence a S . Queremos provar que qualquer inteiro $m \geq a$ pertence a S .
Seja $A = \{m \in \mathbb{Z} \mid m \geq a \wedge m \notin S\}$. Suponhamos, com vista a chegar a um absurdo, que $A \neq \emptyset$. Sendo $A \neq \emptyset$ e minorado (a é um minorante), pelo Princípio de Boa Ordenação, $\exists x_0 \in A$ tal que $\forall m \in A$ $x_0 \leq m$. Visto que por hipótese $a \in S$, então $a \notin A$ e portanto $x_0 \geq a + 1$. Assim, $x_0 - 1 \geq a$, mas como $x_0 - 1 \notin A$ (porque x_0 é mínimo de A) então $x_0 - 1 \in S$. Ora, aplicando a propriedade de S admitida por hipótese, $x_0 \in S$, o que não pode ser pois $x_0 \in A$. Chegámos a um absurdo pelo facto de ter suposto que $A \neq \emptyset$, logo $A = \emptyset$, ou seja, S contém todos os inteiros maiores ou iguais a a . □

O Princípio de Indução é utilizado com frequência para provar que determinada afirmação é verdadeira para todos os inteiros positivos, ou seja, utilizando a notação da proposição, que $S = \mathbb{N}$. Numa prova deste tipo, primeiro é necessário verificar que a afirmação é verdadeira para o inteiro 1, isto é, que $1 \in S$. Depois, assumindo que a afirmação é verdadeira para o inteiro n , isto é, que $n \in S$, prova-se que a afirmação é verdadeira para o inteiro $n + 1$, isto é, que $n + 1 \in S$.

Exemplo

Vamos provar que para qualquer n inteiro positivo,

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

Seja S o conjunto de todos os inteiros k tais que $1 + 2 + \dots + k = \frac{k(k+1)}{2}$. Ora, $1 \in S$, pois $1 = \frac{1+1}{2}$. Suponhamos que existe um inteiro $n \in S$, então $1 + 2 + \dots + n = \frac{n(n+1)}{2}$. Assim $1 + 2 + \dots + n + (n + 1) = \frac{n(n+1)}{2} + (n + 1) = \frac{(n+1)(n+2)}{2}$, donde podemos afirmar que $(n + 1) \in S$. Logo, por indução, $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ para todos os inteiros positivos n .

Exercício

Escreva duas funções GAP para calcular a soma de todos os números inteiros positivos até n inclusive, uma usando a fórmula dada no exemplo anterior e a outra usando um ciclo *for*.

Compare a sua eficiência usando a função `time` para o efeito.

Em alguns casos torna-se mais conveniente utilizar uma outra forma do Princípio de Indução equivalente à que foi anteriormente referida.

Proposição (Princípio de Indução Matemática - Segunda forma)

Sejam S um conjunto de inteiros e a um inteiro. Se

- (i) $a \in S$ e*
- (ii) se $k \in S$, para qualquer $a \leq k < n$, então $n \in S$,*
então, S contém todos os inteiros maiores ou iguais a a .