Aula 2 – Os Números Naturais e o Princípio da Indução

Metas da aula: Apresentar os números naturais e suas propriedades básicas. Apresentar o Princípio da Indução Matemática e algumas de suas aplicações.

Objetivos: Ao final desta aula, você deverá ser capaz de:

- Saber a definição dos números naturais através dos axiomas de Peano, bem como o seu uso na demonstração das propriedades elementares das operações com esses números;
- Saber usar o Princípio da Indução Matemática na demonstração de proposições elementares envolvendo os números naturais.

Introdução

Nesta aula vamos estudar o conjunto dos números naturais que é a base fundamental para a construção do conjunto dos números reais. Vamos aprender o Princípio da Indução Matemática que é um instrumento fundamental para a demonstração de proposições sobre os números naturais e será utilizado frequentemente ao longo de todo o curso.

Os números naturais

O conjunto dos números naturais, $\mathbb{N} = \{1, 2, 3, \dots\}$, é definido a partir dos seguintes axiomas:

1. $\mathbb{N}$ possui um elemento que denotamos por 1; isto é, postula-se que $1 \in \mathbb{N}$.
2. Existe uma função $s : \mathbb{N} \to \mathbb{N}$ satisfazendo:

   (a) s é *injetiva*, isto é, dados $j, k \in \mathbb{N}$, $s(j) = s(k)$ se e somente se $j = k$;

   (b) $s(\mathbb{N}) = \mathbb{N} \setminus \{1\}$.

   Para cada número natural k, $s(k)$ é chamado sucessor de k e denota-se $s(k) = k + 1$. Portanto, (b) afirma que 1 é o único elemento de $\mathbb{N}$ que não é sucessor de nenhum outro número natural.

3. Se $A \subset \mathbb{N}$ é tal que $1 \in A$ e $s(A) \subset A$, isto é, $k \in A$ implica $k+1 \in A$, então $A = \mathbb{N}$.

Os 3 axiomas acima são conhecidos como *Axiomas de Peano* em homenagem ao matemático italiano GIUSEPPE PEANO (1858 - 1932), criador, entre outras coisas, da lógica simbólica, que foi quem primeiro os formulou. O terceiro axioma é conhecido como *Princípio da Indução Matemática*. Ele pode ser traduzido para o seguinte enunciado mais diretamente utilizado nas aplicações.

Teorema 2.1 (Princípio da Indução Matemática)
Seja P uma proposição acerca dos números naturais. Suponhamos que P seja tal que:

1. $P[1]$ vale, isto é, 1 verifica a proposição P;

2. Se $P[k]$ vale, então vale $P[k+1]$, isto é, se k verifica a proposição P, então seu sucessor $k+1$ também a verifica.

Então, P é válida para todos os números naturais.

Prova: Denotemos por A o conjunto dos números naturais satisfazendo P. Então, por hipótese, temos $1 \in A$; e se $k \in A$ então $k+1 \in A$. Pelo terceiro axioma de Peano temos que $A = \mathbb{N}$, que é o que teríamos que demonstrar.$\square$

As provas matemáticas em que se aplica o Teorema 2.1 são chamadas *provas por indução*. Em 2, no enunciado do Teorema 2.1, a hipótese de que $P[k]$ é válida é chamada *hipótese de indução*. Como primeiro exemplo de prova por indução, vamos demonstrar que, para todo $k \in \mathbb{N}$, vale $s(k) \neq k$. Neste caso, a propriedade $P[k]$ é $s(k) \neq k$. Com efeito, $1 \neq s(1)$, pois 1 não é sucessor de nenhum número natural; em particular, 1 não é sucessor de si próprio. Logo vale $P[1]$. Além disso, se, para um certo $k \in \mathbb{N}$, vale $s(k) \neq k$, então, pela injetividade da função s, $s(s(k)) \neq s(k)$, isto é, $s(k+1) \neq k+1$, e, portanto, vale $P[k+1]$, o que conclui a prova por indução de que $s(k) \neq k$, para todo $k \in \mathbb{N}$.

Como $s : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ é uma bijeção, existe a sua função inversa $s^{-1} : \mathbb{N} \setminus \{1\} \to \mathbb{N}$ que a cada $k \in \mathbb{N} \setminus \{1\}$ associa o número $s^{-1}(k)$ cujo sucessor é k. Denotamos $s^{-1}(k) = k - 1$, para $k \in \mathbb{N} \setminus \{1\}$.

O terceiro axioma de Peano implica, em particular, que todos os números naturais podem ser obtidos a partir de 1 tomando-se reiteradamente sem cessar (começando-se pelo próprio 1) a aplicação sucessor s que também denotamos $\cdot + 1$, obtendo sucessivamente $1 + 1$, $1 + 1 + 1$, $1 + 1 + 1 + 1$ etc. Os nomes e as notações para a seqüência de sucessores de 1 no sistema decimal usual são bastante familiares a todos nós:

$$
\begin{aligned}
&2 := 1 + 1,\\
&3 := 1 + 1 + 1,\\
&4 := 1 + 1 + 1 + 1,\\
&5 := 1 + 1 + 1 + 1 + 1,\\
&6 := 1 + 1 + 1 + 1 + 1 + 1,\\
&7 := 1 + 1 + 1 + 1 + 1 + 1 + 1,\\
&8 := 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1,\\
&9 := 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1,\\
&10 := 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

A adição de números naturais

Por meio da aplicação $\cdot + 1$ podemos facilmente definir a operação de adição ou soma de dois números naturais quaisquer. Intuitivamente, podemos estabelecer que a soma do natural j com o natural k é obtida aplicando-se k vezes a transformação $\cdot + 1$ a j, isto é,

$$j + k = j \underbrace{+1 + 1 + \cdots + 1}_{k \text{ vezes}}. \tag{2.1}$$

A rigor, a definição de soma de dois números naturais que acabamos de dar está imprecisa do ponto de vista lógico, já que recorremos à expressão "k vezes" cujo significado matemático ainda não foi definido. O procedimento mais correto é definir essa operação "passo a passo" fazendo uso do princípio da indução. Assim, primeiro definimos

$$j + 1 := s(j), \tag{2.2}$$

o que está de acordo com a notação $j+1$ que adotamos para o sucessor de j, $s(j)$. Uma vez que já temos a definicão de $j + k$ para $k = 1$, podemos definir recursivamente

$$j + (k + 1) := (j + k) + 1. \tag{2.3}$$

Isto significa que se já tivermos definido, para um certo $k \in \mathbb{N}$, quem é $j+k$, resultará também imediatamente definido, através de (2.3), quem é $j+(k+1)$. Chama-se esse procedimento de definição por indução (indutiva) ou definição por recorrência (recursiva).

Usando o Princípio da Indução podemos provar que a operação de adição de números naturais definida acima tem as propriedades de *associatividade*, *comutatividade* e a *lei do corte*. Mais especificamente, para todos $j, k, l \in \mathbb{N}$, valem:

1. $(j+k)+l = j+(k+l)$; (associatividade)
2. $j+k = k+j$; (comutatividade)
3. se $j+l = k+l$, então $j = k$. (lei do corte)

Por exemplo, para provar a associatividade basta uma simples indução em $l \in \mathbb{N}$. Para $l = 1$ a propriedade decorre diretamente de (2.3). Supondo a propriedade válida para um certo $l \in \mathbb{N}$, temos $(j+k)+(l+1) = ((j+k)+l)+1$ (por (2.3)) e $((j+k)+l)+1 = (j+(k+l))+1$ (pois vale $P[l]$) e, de novo por (2.3), $(j+(k+l))+1 = j+((k+l)+1) = j+(k+(l+1))$, onde na última igualdade usamos $P[1]$. Logo, se vale $(j+k)+l = j+(k+l)$, vale também $(j+k)+(l+1) = j+(k+(l+1))$, o que conclui a prova por indução da associatividade da adição.

Para provar a propriedade da comutatividade, provamos primeiro que, para todo $j \in \mathbb{N}$, vale $j+1 = 1+j$, fazendo indução em j. Para $j = 1$ a igualdade é trivial. Supondo que vale para um certo $j \in \mathbb{N}$, prova-se facilmente que vale para $j+1$, usando-se a definição de adição e a hipótese de indução, $P[j]$. Em seguida, fixando $j \in \mathbb{N}$ arbitrário, fazemos uma nova indução em $k \in \mathbb{N}$ para provar que $j+k = k+j$, para todo $k \in \mathbb{N}$. Você certamente será capaz de dar agora os detalhes da demonstração da propriedade da comutatividade.

Finalmente, a prova da lei do corte também decorre de uma indução simples em $l \in \mathbb{N}$. Com efeito, fixados $j, k \in \mathbb{N}$, arbitrários, se tivermos $j+1 = k+1$ então, decorre da injetividade da função s que $j = k$ e, portanto, vale $P[1]$. Supondo que valha $P[l]$, para um certo $l \in \mathbb{N}$, isto é, que $j+l = k+l \Rightarrow j = k$, temos $j+(l+1) = k+(l+l) \Rightarrow (j+l)+1 = (k+l)+1$ (pela associatividade) e, como vale $P[1]$, $(j+l)+1 = (k+l)+1 \Rightarrow j+l = k+l \Rightarrow j = k$, onde a última implicação é a hipótese de indução $P[l]$. Logo temos que se vale $P[l]$ vale $P[l+1]$, o que conclui a prova por indução da lei do corte para a adição de números naturais.

$\square$

A propriedade da associatividade nos permite escrever simplesmente $j + k + l$ em lugar de $(j + k) + l$ ou $j + (k + l)$.

A ordem entre os números naturais

O resultado seguinte exibe uma propriedade da adição dos números naturais que dá origem à noção de ordem usual entre os mesmos.

Teorema 2.2
Dados dois números naturais quaisquer, m e n, uma, e somente uma, das possibilidades abaixo é válida:

1. $m = n$;

2. Existe $d \in \mathbb{N}$ tal que $m + d = n$;

3. Existe $d' \in \mathbb{N}$ tal que $m = n + d'$.

Prova: Se um dos dois números, m ou n, é igual a 1, digamos $m = 1$, então a terceira possibilidade é vazia, já que se tivermos $1 = n + d'$, para certos $n, d' \in \mathbb{N}$, então 1 seria sucessor de $n + (d' - 1)$, ou de n, caso $d' = 1$, o que é impossível.

Além disso, vemos que se $m = 1$, então as duas primeiras possibilidades são mutuamente excludentes, isto é, no máximo uma delas ocorre, já que se $1 = n$, então não pode valer $1 + d = n$, para nenhum $d \in \mathbb{N}$, pois neste caso 1 seria sucessor de d o que é impossível.

Agora, supondo que para um $m \in \mathbb{N}$ qualquer, fixado, as três possibilidades acima são mutuamente excludentes, qualquer que seja $n \in \mathbb{N}$ (essa é a hiótese de indução $P[m]$), podemos provar que o mesmo deve valer quando tomamos $m + 1$ em lugar de m.

Com efeito, para isso supomos por absurdo que duas delas ocorram simultaneamente, usamos a associatividade da adição e/ou a lei do corte, para provar que isso implicaria a negação da hipótese de indução $P[m]$, chegando assim a uma contradição. Concluímos então que vale $P[m + 1]$, o que prova que as possibilidades 1, 2 e 3 do enunciado são sempre mutuamente excludentes.

Para concluir a prova do teorema devemos provar que uma dessas possibilidades sempre ocorre. Para tanto, dado um $n \in \mathbb{N}$ arbitrário, definimos o conjunto $X(n)$ por

$$X(n) = X^-(n) \cup \{n\} \cup X^+(n),$$

com

$$X^-(n) = \{m \in \mathbb{N} \, : \, m + d = n, \text{ para algum } d \in \mathbb{N}\},$$
$$X^+(n) = \{m \in \mathbb{N} \, : \, m = n + d', \text{ para algum } d' \in \mathbb{N}\}.$$

Observe que, pelo que ficou provado acima, a interseção de quaisquer dois entre os três conjuntos, $X^-(n)$, $\{n\}$ e $X^+(n)$, é vazia. O objetivo então é mostrar que $X(n) = \mathbb{N}$ para todo $n \in \mathbb{N}$. Provamos primeiro que $X(1) = \mathbb{N}$. Neste caso, como observado acima, temos $X^-(1) = \emptyset$. Claramente, temos $1 \in X(1)$. Além disso, supondo $k \in X(1)$, para um certo $k \in \mathbb{N}$, provamos que $k + 1 \in X(1)$. Com efeito, se $k \in X(1)$ então, ou $k = 1$, e nesse caso $k+1 \in X^+(1)$, ou $k \in X^+(1)$, e nesse caso $k = 1+d'$, para algum $d' \in \mathbb{N}$. No último caso, temos $k+1 = (1+d')+1 =$(pela associatividade)$= 1+(d'+1)$, e assim fica provado que $k \in X(1) \Rightarrow k + 1 \in X(1)$. Pelo terceiro axioma de Peano (Princípio da Indução) segue que $X(1) = \mathbb{N}$. A prova de que $X(n) = \mathbb{N}$, para todo $n \in \mathbb{N}$, decorrerá novamente do Princípio da Indução se mostrarmos que $X(k) = \mathbb{N} \Rightarrow X(k+1) = \mathbb{N}$. Deixamos isso como exercício para você fazer. □

Definição 2.1
Dizemos que o natural m é menor que o natural n, ou que n é maior que n, e denotamos $m < n$, se existe $d \in \mathbb{N}$ tal que $m + d = n$. A notação $n > m$ equivale a $m < n$ e a notação $m \leq n$ significa $m < n$ ou $m = n$. Se $m < n$, o número natural d tal que $m + d = n$ é denotado $n - m$. Observe que essa notação é coerente com a notação $n - 1$ para o antecessor de n.

A relação $<$ tem as propriedades:

1. Se $m < n$ e $n < p$ então $m < p$; (transitividade)
2. Se $m < n$ e $p \in \mathbb{N}$ então $m + p < n + p$; (monotonicidade)
3. Dados dois números quaisquer $m, n \in \mathbb{N}$ vale uma, e somente uma, das seguintes possibilidades: ou $m < n$, ou $m = n$, ou $n < m$. (tricotomia)

A terceira propriedade é o próprio Teorema 2.2 reescrito de forma distinta. A primeira e a segunda propriedade decorrem diretamente da definição de $<$.

Com efeito, se $m < n$ e $n < p$ então existem d_1 e d_2 tais que $m + d_1 = n$ e $n + d_2 = p$. Decorre daí que $(m + d_1) + d_2 = p$, isto é, $m + (d_1 + d_2) = p$ e, portanto, $m < p$. Quanto à segunda, se $m < n$, então $m + d = n$, para algum $d \in \mathbb{N}$, assim $n + p = (m + d) + p = (m + p) + d$ e, portanto, $m + p < n + p$.

$\square$

O seguinte resultado é uma conseqüência imediata do Teorema 2.1.

Teorema 2.3 (Princípio da Indução Matemática (segunda versão)) Seja $n_0 \in \mathbb{N}$ e seja $P[n]$ uma proposição acerca dos números naturais $n \geq n_0$. Suponhamos que:

1. A proposição $P[n_0]$ é verdadeira;

2. Para todo $k \geq n_0$, a proposição $P[k]$ implica $P[k + 1]$.

Então, $P[n]$ é válida para todo $n \geq n_0$.

Prova: Se $n_0 = 1$, então o enunciado acima é o próprio Teorema 2.1. Se $n_0 > 1$, então, para cada $n \in \mathbb{N}$, consideramos a proposição $Q[k] = P[(n_0 - 1) + k]$.

Então, a hipótese 1 do enunciado afirma que vale $Q[1]$, ao passo que a hipótese 2 afirma que $Q[k]$ implica $Q[k+1]$. Pelo Teorema 2.1 segue que vale $Q[k]$, para todo $k \in \mathbb{N}$, isto é, vale $P[n]$ para todo $n \geq n_0$. $\square$

O produto de números naturais

O produto de dois números naturais, $m \cdot n$, $m, n \in \mathbb{N}$, pode ser definido recursivamente, como já foi feito para a adição, da seguinte forma:

$$m \cdot 1 = m,$$
$$m \cdot (n + 1) = m \cdot n + m.$$

As duas linhas acima constituem o modo rigoroso de expressar a definição informal bastante conhecida:

$$m \cdot n := \underbrace{m + m + \cdots + m}_{n \text{ vezes}}.$$

No que segue, frequentemente, denotaremos $m \cdot n$ simplesmente por mn, como é usual.

Usando o Princípio da Indução, como fizemos para o caso da adição, podemos provar as seguintes propriedades bem conhecidas satisfeitas pelo produto de números naturais. Deixamos a você, como exercício, a demonstração de tais propriedades. Para todos $m, n, p \in \mathbb{N}$ temos:

1. $(mn)p = m(np)$; (associatividade)
2. $mn = nm$; (comutatividade)
3. Se $mn = mp$ então $n = p$; (lei do corte)
4. Se $m < n$ então $mp < np$; (monotonicidade)
5. $m(n + p) = mn + mp$. (distributividade)

Dado qualquer $m \in \mathbb{N}$, definimos m^k, para todo $k \in \mathbb{N}$, estabelecendo que $m^1 = m$ e $m^{k+1} = m \cdot m^k$. Analogamente, o fatorial de um número natural n é definido indutivamente pondo-se $1! = 1$ e $(n+1)! = (n+1) \cdot n!$. Expresso de modo menos formal, temos

$$m^k = \underbrace{m \cdot m \cdots m}_{k \text{ vezes}}, \quad n! = n(n-1) \cdots 2 \cdot 1.$$

O Princípio da Boa Ordenação

Dado um conjunto $A \subset \mathbb{N}$, dizemos que m_0 é o *menor elemento de* A, ou é o *elemento mínimo de* A, se $m_0 \leq m$, para todo $m \in A$. É imediato verificar que o elemento mínimo, quando existe, é único. Com efeito, se m_0 e m_1 são dois elementos mínimos de A, então $m_0 \leq m_1$, pois m_0 é mínimo, e $m_1 \leq m_0$, pois m_1 também é mínimo. Logo, $m_0 = m_1$.

Se considerarmos o próprio conjunto $\mathbb{N}$, vemos que 1 é o elemento mínimo de $\mathbb{N}$, já que, para todo $m \in \mathbb{N}$, ou $m = 1$, ou m é o sucessor de algum outro número natural, o qual é menor que m.

Analogamente, $M_0 \in A$ é chamado o *maior elemento de* A, ou o *elemento máximo de* A, se $m \leq M_0$, para todo $m \in A$. A prova de que o elemento máximo de $A \subset \mathbb{N}$ é único, quando existe (!), é feita de modo idêntico ao que foi feito para provar a unicidade do mínimo. Nem sempre um subconjunto não-vazio de $\mathbb{N}$ possui elemento máximo. O próprio $\mathbb{N}$ não o possui, já que para todo $m \in \mathbb{N}$, $m + 1 \in \mathbb{N}$ e $m < m + 1$.

No entanto, em relação ao mínimo, vale o seguinte princípio fundamental.

Teorema 2.4 (Princípio da Boa Ordenação)
Se $A \subset \mathbb{N}$ e $A \neq \emptyset$ então A possui um menor elemento.

Prova: Dado $n \in \mathbb{N}$, denotemos $J_n := \{k \in \mathbb{N} : 1 \leq k \leq n\}$. Seja A um subconjunto não-vazio de $\mathbb{N}$. Como A é não-vazio, $\mathbb{N} \backslash A \neq \mathbb{N}$. Se $1 \in A$, então

1 é o elemento mínimo de A, já que 1 é o elemento mínimo de $\mathbb{N}$. Suponhamos, então, que $1 \notin A$, isto é, $1 \in \mathbb{N} \setminus A$. Seja $X := \{n \in \mathbb{N} : J_n \subset \mathbb{N} \setminus A\}$. Como $J_1 = \{1\}$, temos $1 \in X$, já que estamos supondo que $1 \in \mathbb{N} \setminus A$. Se para todo $m \in X$ tivermos $m + 1 \in X$ então, pelo Princípio da Indução, teremos $X = \mathbb{N}$, o que implicará $\mathbb{N} \setminus A = \mathbb{N}$ e daí $A = \emptyset$, contrariando a hipótese de que A é não-vazio. Assim, deve existir $m_0 \in X$ tal que $m := m_0 + 1 \notin X$. Afirmamos que m, assim definido, é o elemento mínimo de A.

Com efeito, se $p < m$, então $p \in J_{m_0} \subset \mathbb{N} \setminus A$, e, portanto, $p \notin A$. Logo, para todo $p \in A$ devemos ter $m \leq p$, o que demonstra que m é o elemento mínimo de A e conclui a prova. □

A seguir damos alguns exemplos mais práticos de demonstrações por indução. Neles faremos livre uso das propriedades dos números reais já bastante conhecidas por você (uma exposição mais formal sobre essas propriedades será feita mais adiante).

Exemplos 2.1

(a) Para cada $n \in \mathbb{N}$, a soma dos n primeiros números naturais é dada por

$$1 + 2 + \cdots + n = \frac{1}{2} n(n+1). \tag{2.4}$$

Com efeito, chamemos $P[n]$ esta fórmula. Nesse caso, $P[1]$ é $1 = \frac{1}{2} \cdot 1 \cdot 2$ que, portanto, é verdadeira. Suponhamos agora que valha $P[k]$, isto é,

$$1 + 2 + \cdots + k = \frac{1}{2} k(k+1).$$

Somando $(k+1)$ a ambos os membros desta equação, obtemos uma nova equação cujo o membro esquerdo é $1+2+\cdots+(k+1)$, que é o membro esquerdo da fórmula $P[k+1]$. Por outro lado, após somarmos $(k+1)$ à equação $P[k]$, o membro direito da nova equação é $\frac{1}{2}k(k+1)+(k+1) = \frac{1}{2}(k+1)(k+2)$. Assim, somando $(k+1)$ à equação $P[k]$ obtemos

$$1 + 2 + \cdots + (k+1) = \frac{1}{2}(k+1)(k+2),$$

que nada mais é que $P[k+1]$. Assim, pelo Princípio da Indução Matemática (Teorema 2.1), segue que $P[n]$, isto é, a equação (2.4), é verdadeira para todo $n \in \mathbb{N}$.

(b) Para cada $n \in \mathbb{N}$, a soma dos quadrados dos n primeiros números naturais é dada por

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1). \tag{2.5}$$

De novo, chamando $P[n]$ esta fórmula, vemos que $P[1]$ é $1 = \frac{1}{6} \cdot 1 \cdot 2 \cdot 3$ e, portanto, é verdadeira. Suponhamos que valha $P[k]$:

$$1^2 + 2^2 + \cdots + k^2 = \frac{1}{6}k(k+1)(2k+1).$$

Somando $(k+1)^2$ a ambos os membros da equação $P[k]$ obtemos

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\ &= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\ &= \frac{1}{6}(k+1)(2k^2 + 7k + 6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3). \end{aligned}$$

O membro esquerdo da primeira equação desta cadeia de equações e o membro direito da última equação coincidem com os membros esquerdo e direito de $P[k+1]$. Portanto, temos que $P[k]$ implica $P[k+1]$. Logo, pelo Princípio da Indução Matemática, concluímos que (2.5) vale para todo $n \in \mathbb{N}$.

(c) Dados dois números $a, b \in \mathbb{N}$, $a > b$, provaremos que $a - b$ é um fator de $a^n - b^n$, para todo $n \in \mathbb{N}$. Com efeito, para $n = 1$ a afirmação é óbvia. Suponhamos então que valha $P[k]$: $a - b$ é um fator de $a^k - b^k$. Então temos

$$\begin{aligned} a^{k+1} - b^{k+1} &= a^{k+1} - ab^k + ab^k - b^{k+1} \\ &= a(a^k - b^k) + (a-b)b^k. \end{aligned}$$

Pela hipótese de indução (vale $P[k]$), concluímos então que vale $P[k+1]$. De novo, pelo Princípio da Indução, vemos que a afirmação vale para todo $n \in \mathbb{N}$. Como aplicação, deduzimos, por exemplo, que $13^n - 8^n$ é divisível por 5, $17^n - 13^n$ é divisível por 4, etc., qualquer que seja $n \in \mathbb{N}$.

(d) A desigualdade $2^n > 2n + 1$ é verdadeira para $n \geq 3$ (observe que ela não vale para $n = 1, 2$). De fato, chamando de $P[n]$ a desigualdade, vemos que vale $P[3]$ já que $2^3 = 8 > 7 = 2 \cdot 3 + 1$. Suponhamos que valha $P[k]$: $2^k > 2k + 1$. Levando em conta que $2k + 2 > 3$ para todo $k \in \mathbb{N}$, após multiplicar $P[k]$ por 2, temos

$$2^{k+1} > 2(2k + 1) = 4k + 2 = 2k + (2k + 2) > 2k + 3 = 2(k + 1) + 1,$$

e assim obtemos $P[k + 1]$. Portanto, pelo Teorema 2.3 concluímos que a desigualdade vale para todo $n \geq 3$.

(e) A desigualdade $2^n \leq (n + 1)!$ pode ser estabelecida pelo Princípio da Indução Matemática. De fato, inicialmente observemos que vale $P[1]$, já que $2^1 = 2 = 2 \cdot 1 = 2!$. Supondo que valha $P[k]$, isto é, $2^k \leq (k+1)!$, multiplicando $P[k]$ por 2, e usando o fato que $2 \leq k + 2$, segue que

$$2^{k+1} \leq 2(k + 1)! \leq (k + 2)(k + 1)! = (k + 2)!,$$

o que nos dá que vale $P[k + 1]$. Portanto, o Teorema 2.1 implica que a desigualdade vale para todo $n \in \mathbb{N}$.

A seguinte versão do Princípio da Indução Matemática é, às vezes, bastante útil. Alguns autores a chamam "Princípio da Indução Forte". Usamos a notação habitual $\{1, 2, \ldots, k\}$ para denotar o conjunto $J_k = \{j \in \mathbb{N} : 1 \leq j \leq k\}$.

Teorema 2.5 (Princípio da Indução Forte)
Seja S um subconjunto de $\mathbb{N}$ tal que

(1) $1 \in S$.

(2) Para todo $k \in \mathbb{N}$, se $\{1, 2, \ldots, k\} \subset S$, então $k + 1 \in S$.

Então $S = \mathbb{N}$.

Prova: Consideremos o conjunto $X = \mathbb{N} \setminus S$. Provaremos por contradição que $X = \emptyset$. Suponhamos então que $X \neq \emptyset$. Então, pelo Princípio da Boa Ordenação, X possui um elemento mínimo m_0. Como, por (1), $1 \in S$, temos $m_0 > 1$. Por outro lado, como m_0 é o menor elemento de $X = \mathbb{N} \setminus S$, temos que $\{1, \ldots, m_0 - 1\} \subset S$. Decorre então de (2) que $m_0 \in S$, o que nos dá uma contradição e conclui a prova. $\square$

Exercícios 2.1

1. Prove que $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\cdots+\dfrac{1}{n(n+1)}=\dfrac{n}{n+1}$ para todo $n\in\mathbb{N}$.

2. Prove que $1^3+2^3+\cdots+n^3=\left[\frac{1}{2}n(n+1)\right]^2$ para todo $n\in\mathbb{N}$.

3. Prove que $3+11+\cdots+(8n-5)=4n^2-n$ para todo $n\in\mathbb{N}$.

4. Prove que $1^2+3^2+\cdots+(2n-1)^2=(4n^3-n)/3$ para todo $n\in\mathbb{N}$.

5. Prove que $1^2-2^2+3^2+\cdots+(-1)^{n+1}n^2=(-1)^{n+1}n(n+1)/2$ para todo $n\in\mathbb{N}$.

6. Prove que n^3+5n é divisível por 6 para todo $n\in\mathbb{N}$.

7. Prove que $5^{2n}-1$ é divisível por 8 para todo $n\in\mathbb{N}$.

8. Prove que $n^3+(n+1)^3+(n+2)^3$ é divisível por 9 para todo $n\in\mathbb{N}$.

9. Prove que vale o binômio de Newton: dados $a,b\in\mathbb{R}$, para todo $n\in\mathbb{N}$, vale
$$(a+b)^n=a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\cdots+\binom{n}{n-1}ab^{n-1}+b^n,$$
onde $\binom{n}{k}=n!/k!(n-k)!$. (Sugestão: verifique que $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$.)

10. Prove a desigualdade de Bernoulli: dado $x\in\mathbb{R}$, $x>-1$, para todo $n\in\mathbb{N}$ vale
$$(1+x)^n\geq 1+nx.$$

11. Prove que $n<2^n$ para todo $n\in\mathbb{N}$.

12. Prove que $2^n<n!$ para todo $n\geq 4$, $n\in\mathbb{N}$.

13. Prove que $2n-3\leq 2^{n-2}$ para todo $n\geq 5$, $n\in\mathbb{N}$.

14. Prove que $1/\sqrt{1}+1/\sqrt{2}+\cdots+1/\sqrt{n}>\sqrt{n}$ para todo $n>2$, $n\in\mathbb{N}$.

15. Sejam os números x_n definidos do seguinte modo: $x_1:=1$, $x_2:=2$ e $x_{n+2}:=\frac{1}{2}(x_{n+1}+x_n)$ para todo $n\in\mathbb{N}$. Use o Princípio da Indução Forte (Teorema 2.5) para mostrar que $1\leq x_n\leq 2$ para todo $n\in\mathbb{N}$.

Prossiga: Números Inteiros e Racionais

Vamos descrever sucintamente como o conjunto dos números inteiros $\mathbb{Z}$ e o conjunto dos números racionais $\mathbb{Q}$ são definidos a partir de $\mathbb{N}$ e como são definidas a adição, a multiplicação e a ordem entre esses números. Mencionaremos, omitindo as provas, algumas propriedades satisfeitas pelas operações e pela ordem definidas para os inteiros. Abordaremos mais detalhadamente essas propriedades em breve, quando estivermos estudando os números reais.

O conjunto $\mathbb{Z}$ é definido adicionando-se a $\mathbb{N}$ o elemento 0, chamado "zero", e, para cada $k \in \mathbb{N}$, o elemento $-k$, chamado "menos k". Define-se a adição entre dois inteiros quaisquer estabelecendo que a mesma coincide com a adição em $\mathbb{N}$, quando ambos os números pertencem a $\mathbb{N}$, e pondo-se além disso:

$$\begin{aligned}
&0 + s = s + 0 := s, \quad \text{para todo } s \in \mathbb{Z},\\
&(-j) + j = j + (-j) := 0, \quad \text{para todo } j \in \mathbb{N},\\
&(-j) + (-k) := -(j + k), \quad \text{para todos } j, k \in \mathbb{N},\\
&(-j) + k = k + (-j) := k - j \quad \text{se } j, k \in \mathbb{N} \text{ e } j < k,\\
&(-j) + k = k + (-j) := -(j - k) \quad \text{se } j, k \in \mathbb{N} \text{ e } j > k,
\end{aligned}$$

onde denotamos $-(j - k) := -d$, com $d = j - k$.

Verifica-se facilmente que a adição de inteiros assim definida satisfaz: $r + s = s + r$ (comutatividade) e $(r + s) + t = r + (s + t)$ (associatividade).

A ordem em $\mathbb{Z}$ é definida estabelecendo-se que $r < s$ se $r + d = s$ para algum $d \in \mathbb{N}$. Em particular, $0 < n$ e $-n < 0$, para todo $n \in \mathbb{N}$. A transitividade ($r < s$ e $s < t \Rightarrow r < t$), a monotonicidade ($r < s \Rightarrow r + t < s + t$) e a tricotomia (uma e só uma das alternativas é válida: $r < s$, $r = s$, ou $r > s$) valem quaisquer que sejam $r, s, t \in \mathbb{Z}$ como é fácil verificar.

A multiplicação em $\mathbb{Z}$ é definida estabelecendo-se que ela coincide com a multiplicação em $\mathbb{N}$, quando ambos os números pertencem a $\mathbb{N}$, e pondo

$$\begin{aligned}
&0 \cdot s = s \cdot 0 := 0, \quad \text{para todo } s \in \mathbb{Z},\\
&(-j) \cdot (-k) = (-k) \cdot (-j) := j \cdot k, \quad \text{para todos } j, k \in \mathbb{N},\\
&(-j) \cdot k = j \cdot (-k) := -j \cdot k, \quad \text{para todos } j, k \in \mathbb{N}.
\end{aligned}$$

Pode-se provar sem dificuldade que a multiplicação em $\mathbb{Z}$, assim definida, é comutativa, associativa e distributiva em relação à adição: $r \cdot s = s \cdot r$

(comutatividade), $(rs)t = r(st)$ (associatividade), $r(s+t) = rs + rt$ (distributividade).

Além disso, não é difícil verificar que se $r < s$ então $r \cdot t < s \cdot t$, se $t > 0$ (isto é, se $t \in \mathbb{N}$) e $r \cdot t > s \cdot t$, se $t < 0$ (isto é, se $(-1) \cdot t \in \mathbb{N}$).

Finalmente, se, para todo $s \in \mathbb{Z}$, definirmos $-s = (-1) \cdot s$, temos que valem as equações $s + (-s) = (-s) + s = 0$ e $-(-s) = s$.

O conjunto $\mathbb{Q}$ dos números racionais é formado por objetos da forma $\dfrac{p}{q}$ onde $p, q \in \mathbb{Z}$ e $q \neq 0$, convencionando-se que $\frac{p}{q} = \frac{r}{s}$ se e somente se $p \cdot s = r \cdot q$. Definem-se a soma e a multiplicação de números racionais como você já conhece bem:

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}, \qquad \frac{p}{q} \cdot \frac{r}{s} = \frac{p \cdot r}{q \cdot s}.$$

As operações assim definidas são comutativas e associativas, e vale também a distributividade da multiplicação em relação à adição. Denota-se

$$-\frac{p}{q} := (-1) \cdot \frac{p}{q} = \frac{-p}{q} \quad \text{e} \quad \frac{p}{q} - \frac{r}{s} := \frac{p}{q} + \left(-\frac{r}{s}\right) = \frac{p}{q} + \frac{-r}{s}.$$

Define-se a ordem entre os racionais estabelecendo-se que $\dfrac{p}{q} > 0$ se $p \cdot q > 0$ e $\dfrac{p}{q} > \dfrac{r}{s}$ se $\dfrac{p}{q} - \dfrac{r}{s} > 0$.

Se $x, y, z \in \mathbb{Q}$, verifica-se sem muita dificuldade que: (i) $x < y$ e $y < z$ implica $x < z$; (ii) $x < y$ então $x + z < y + z$; (iii) $x < y$ então $xz < yz$ se $z > 0$ e $xz > yz$ se $z < 0$; (iv) uma e só uma das alternativas é válida: $x < y$, $x = y$, ou $x > y$.

Se $x \in \mathbb{Q} \setminus \{0\}$ e $x = \dfrac{p}{q}$ define-se x^{-1}, chamado o inverso de x, por $x^{-1} := \dfrac{q}{p}$. Verifica-se sem dificuldade que x^{-1} é o único racional satisfazendo $x \cdot x^{-1} = 1$.