Lista 2

1) Prove as seguintes afirmações:

a) (Lei do cancelamento) Sejam m, n e p números naturais, então:

$$m+n=m+p \Rightarrow n=p$$

Vamos provar por indução em m, isto é, vamos demonstrar que:

(i) Para quaisquer n e p naturais, temos que $1+n=1+p \Rightarrow n=p$;

(ii) Se $(m+n=m+p \Rightarrow n=p)$, então $(S(m)+n=S(m)+p \Rightarrow n=p)$.

Demonstração:

(i) $1+n=1+p \underset{\text{Soma é comutativa}}{\Longrightarrow} n+1=p+1 \underset{\text{Definição de soma}}{\Longrightarrow} S(n)=S(p) \underset{\text{função S é injetora}}{\Longrightarrow} n=p$ ∎

(ii) $S(m)+n=S(m)+p \underset{\text{Soma é comutativa}}{\Longrightarrow} n+S(m)=p+S(m) \underset{\text{Definição de soma}}{\Longrightarrow} S(n+m)=S(p+m) \Rightarrow$

$\underset{\text{função S é injetora}}{\Longrightarrow} n+m=p+m \underset{\text{Soma é comutativa}}{\Longrightarrow} m+n=m+p \underset{\text{Hipótese de indução}}{\Longrightarrow} n=p$ ∎

b) (Tricotomia) Dados m e n naturais, vale uma, e somente uma, das três afirmações:

(i) $m=n$;

(ii) $\exists\, p \in \mathbb{N}$ tq. $m=n+p$;

(iii) $\exists\, q \in \mathbb{N}$ tq. $n=m+q$;

Vamos provar por indução em n, isto é, vamos demonstrar que:

(α) (Base de indução) Vale a tricotomia para $n=1$, isto é, dado qualquer $m \in \mathbb{N}$, vale uma, e somente uma, das afirmações:

(i) $m=1$; (ii) $\exists\, p \in \mathbb{N}$ tq. $m=1+p$; (iii) $\exists\, q \in \mathbb{N}$ tq. $1=m+q$.

(β) (Passo de indução) Vale a tricotomia para $n \Rightarrow$ Vale a tricotomia para $S(n)$, isto é, se dado qualquer $m \in \mathbb{N}$, vale uma, e somente uma, das afirmações: (i) $m=n$; (ii) $\exists\, p \in \mathbb{N}$ tq. $m=n+p$; (iii) $\exists\, q \in \mathbb{N}$ tq. $n=m+q$; então dado qualquer $m \in \mathbb{N}$, vale uma, e somente uma, das afirmações: (i) $m=S(n)$; (ii) $\exists\, p \in \mathbb{N}$ tq. $m=S(n)+p$; (iii) $\exists\, q \in \mathbb{N}$ tq. $S(n)=m+q$.

Demonstração:

/ /

(α) É claro que não é possível que valha (iii), pois $\forall m \in \mathbb{N}$, $\nexists q \in \mathbb{N}$ tq. $1 = m + q$, pois $1 \notin Im(S)$. Portanto, basta mostrarmos a dicotomia: (i) $m = 1$; (ii) $\exists p \in \mathbb{N}$ tq. $m = 1 + p$.

Se vale (i), não pode valer (ii), pois se o fosse, teríamos $1 = 1 + p = p + 1 = S(p)$ o que é um absurdo, já que $1 \notin Im(S)$.

Se não vale (i), então temos que $m \neq 1$, donde $m \in Im(S)$, isto é, $\exists p \in \mathbb{N}$ tq. $m = S(p) = p + 1 = 1 + p$ e, portanto, valeria (ii). ∎

(β) Supondo a tricotomia para n, vamos mostrar a tricotomia para $S(n)$. Para isso, mostraremos que (i), (ii) e (iii) não valem, duas a duas, simultaneamente e, além disso, a negação de duas afirmações implica na terceira:

- (i) e (ii) não valem simultaneamente: suponha $m = S(n)$ e a existência de $p \in \mathbb{N}$ tq. $m = S(n) + p$. Então, teríamos que $S(n) = S(n) + p \Rightarrow n + 1 = (n+1) + p = n + (1+p) = n + (p+1) = n + (S(p)) \Rightarrow 1 = S(p)$. Absurdo pois $1 \notin Im(S)$ ∎
- (i) e (iii) não valem simultaneamente: suponha $m = S(n)$ e a existência de $q \in \mathbb{N}$ tq. $S(n) = m + q$. Então, teríamos que $S(n) = S(n) + q \Rightarrow 1 = S(q)$ ζ ∎
- (ii) e (iii) não valem simultaneamente: suponha a existência de $p \in \mathbb{N}$ e $q \in \mathbb{N}$ tais que $m = S(n) + p$ e $S(n) = m + q$. Então, teríamos que $S(n) = S(n) + p + q \Rightarrow 1 = S(p + q)$. Absurdo, pois $1 \notin Im(S)$ ∎
- a negação de (i) e (ii) implica em (iii): suponha que $m \neq S(n)$ e $m \neq S(n) + p, \forall p \in \mathbb{N}$. Então, $m \neq n + 1$ e $m \neq n + S(p), \forall p \in \mathbb{N}$, logo, temos que $m \neq n + p, \forall p \in \mathbb{N}$. Portanto, pela hipótese de indução, vale a seguinte dicotomia: (i) $m = n$; ou (iii) $\exists q \in \mathbb{N}$ tq. $n = m + q$; Se vale (i), temos que $S(n) = m + 1$ e se vale (iii), temos que $S(n) = S(m+q) = m + S(q)$, algum $q \in \mathbb{N}$. De qualquer forma, $\exists q \in \mathbb{N}$ tq. $S(n) = m + q$ ∎

2. (Transitividade do "menor que" (<)) Sejam m, n e p naturais. Mostre que:

$$(m < n \text{ e } n < p) \Rightarrow m < p$$

$\exists q_1$ tq. $n = m + q_1$ e $\exists q_2$ tq. $p = n + q_2$, logo $p = n + q_2 = (m + q_1) + q_2 = m + (q_1 + q_2)$

$\therefore m < p$ ∎

③ Sejam m, n e p naturais. Mostre que: $m+p<n+p \Leftrightarrow m<n$

Vamos provar por indução em p, isto é, vamos demonstrar que:

(i) $m+1<n+1 \Leftrightarrow m<n$;

(ii) $(m+p<n+p \Leftrightarrow m<n) \Rightarrow (m+S(p)<n+S(p) \Leftrightarrow m<n)$;

Demonstração:

(i) $m+1<n+1 \Leftrightarrow \exists q \in \mathbb{N}$ tq. $n+1=(m+1)+q \Leftrightarrow \exists q \in \mathbb{N}$ tq. $n+1=(m+q)+1 \Leftrightarrow \exists q \in \mathbb{N}$ tq. $n=m+q \Leftrightarrow m<n$ ∎

(ii) $m+S(p)<n+S(p) \Leftrightarrow \exists q \in \mathbb{N}$ tq. $n+S(p)=(m+S(p))+q \Leftrightarrow \exists q \in \mathbb{N}$ tq. $(n+p)+1=[(m+p)+q]+1 \Leftrightarrow \exists q \in \mathbb{N}$ tq. $n+p=(m+q)+p$ $\underset{\text{Hipótese de indução}}{\Longleftrightarrow} \exists q \in \mathbb{N}$ tq. $n=m+q \Leftrightarrow m<n$ ∎

④ Sejam m, n e p naturais. Mostre que:

$$(m<n \text{ e } n \leq p) \Rightarrow m<p$$

$n \leq p$ significa $n<p$ ou $n=p$. Se $n<p$, pelo ex. 2, temos que $m<p$ e se $n=p$, temos $m<n=p$ e, portanto, $m<p$ ∎

⑤ Prove as seguintes propriedades da multiplicação em $\mathbb{N}$

a) Mostre que a multiplicação está bem definida para quaisquer m e n naturais através de (i) e (ii)

b) (Associatividade) Mostre que para quaisquer m, n e p naturais temos $(m \cdot n) \cdot p = m \cdot (n \cdot p)$

c) (Comutatividade) Mostre que para quaisquer m e n naturais vale $m \cdot n = n \cdot m$

d) (Cancelamento) Mostre que para quaisquer m, n e p naturais temos que:

(d1) $(m \cdot p = n \cdot p) \Rightarrow m=n$

(d2) (Distributividade) $m \cdot (n+p) = m \cdot n + m \cdot p$

(d3) (Monotonicidade) $m<n \Rightarrow m \cdot p < n \cdot p$

——— // ——— // ———

a) Dado $m \in \mathbb{N}$, temos que está definido o produto $m \cdot 1$ e, se está definido o produto $m \cdot n$, então o produto $m \cdot S(n)$ está definido, já que $m \cdot S(n) = m \cdot n + m$

Logo, o conjunto $A_m = \{n \in \mathbb{N} : \text{o produto } m \cdot n \text{ está definido}\} = \mathbb{N}$ ∎

Vamos resolver os próximos ítens em outra ordem, que consideramos mais conveniente. Antes de tudo, vamos provar o seguinte lema:

Lema: (α) $1 \cdot n = n, \forall n \in \mathbb{N}$

(β) $S(m) \cdot n = m \cdot n + n, \forall m \in \mathbb{N}, \forall n \in \mathbb{N}$

Dem: (α) Vamos provar por indução em n, isto é, vamos demonstrar que:

(i) $1 \cdot 1 = 1$;

(ii) $(1 \cdot n = n) \Rightarrow (1 \cdot S(n) = S(n))$.

Demonstração: (i) $1 \cdot 1 = 1$, por definição;

(ii) $1 \cdot S(n) = 1 \cdot n + 1 \underset{\text{Hipótese de indução}}{=} n + 1 = S(n)$. ∎

(β) Vamos provar por indução em n, isto é, vamos demonstrar que:

(i) $S(m) \cdot 1 = m \cdot 1 + 1, \forall m \in \mathbb{N}$;

(ii) $(S(m) \cdot n = m \cdot n + n, \forall m \in \mathbb{N}) \Rightarrow (S(m) \cdot S(n) = m \cdot S(n) + S(n), \forall m \in \mathbb{N})$

Demonstração: (i) Dado $m \in \mathbb{N}$, temos que $S(m) \cdot 1 = S(m) = m + 1 = m \cdot 1 + 1$ ∎

(ii) Dado $m \in \mathbb{N}$, temos que $S(m) \cdot S(n) = S(m) \cdot n + S(m) \underset{\text{Hipótese de indução}}{=}$

$(m \cdot n + n) + S(m) = (m \cdot n + n) + (m + 1) \underset{\text{Associatividade e Comutatividade da Soma}}{=} (m \cdot n + m) + (n + 1) = m \cdot S(n) + S(n)$ ∎

(d2) Vamos provar por indução em m, isto é, vamos demonstrar que:

(i) $1 \cdot (n + p) = 1 \cdot n + 1 \cdot p, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}$;

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

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

Demonstração: (i) $1 \cdot (n + p) \underset{\text{Lema}(\alpha)}{=} n + p \underset{\text{Lema}(\alpha)}{=} 1 \cdot n + 1 \cdot p, \forall n \in \mathbb{N}, \forall p \in \mathbb{N}$ ∎

(ii) $S(m) \cdot (n + p) \underset{\text{Lema}(\beta)}{=} m \cdot (n + p) + (n + p) \underset{\text{Hipótese de Indução}}{=} (m \cdot n + m \cdot p) + (n + p) \underset{\text{Associatividade e Comutatividade da Soma}}{=}$

$= (m \cdot n + n) + (m \cdot p + p) \overset{\text{Lema}(\beta)}{=} S(m) \cdot n + S(m) \cdot p$ ∎

(d3) $m < n \Rightarrow \exists q \in \mathbb{N}$ tq. $n = m + q \Rightarrow \exists q \in \mathbb{N}$ tq. $n \cdot p = (m + q) \cdot p \overset{(d2')}{\Longrightarrow}$

$\exists q \in \mathbb{N}$ tq. $n \cdot p = m \cdot p + q \cdot p \underset{q \cdot p \in \mathbb{N}}{\Longrightarrow} m \cdot p < n \cdot p, \forall p \in \mathbb{N}$ ∎

(d2') Claro que $(m + n) \cdot p = m \cdot p + n \cdot p$. Basta proceder por indução em p, como em (d2).

(d1) Sendo $m \cdot p = n \cdot p$, suponha $m \neq n$. Então, pela tricotomia, temos que $m < n$ ou $n < m$. Em ambos os casos, usando (d3), obteríamos que $m \cdot p < n \cdot p$ ou $n \cdot p < m \cdot p$ e, de qualquer forma, temos $m \cdot p \neq n \cdot p$ ∎

(c) Vamos provar por indução em m, isto é, vamos demonstrar que:

(i) $1 \cdot n = n \cdot 1, \forall n \in \mathbb{N}$;

(ii) $(m \cdot n = n \cdot m, \forall n \in \mathbb{N}) \Longrightarrow (S(m) \cdot n = n \cdot S(m), \forall n \in \mathbb{N})$

Demonstração: (i) $n \cdot 1 = n$, por definição e $1 \cdot n = n$, pela parte (α) do Lema ∎

(ii) $S(m) \cdot n \underset{\text{Lema}(\beta)}{=} m \cdot n + n \underset{\substack{\text{Hipótese de} \\ \text{Indução}}}{=} n \cdot m + n = n \cdot S(m)$ ∎

(b) Vamos provar por indução em m, isto é, vamos demonstrar que:

(i) $(1 \cdot n) \cdot p = 1 \cdot (n \cdot p)$, $\forall n \in \mathbb{N}, \forall p \in \mathbb{N}$;

(ii) $[(m \cdot n) \cdot p = m \cdot (n \cdot p), \forall n \in \mathbb{N}, \forall p \in \mathbb{N}] \Longrightarrow$
$[(S(m) \cdot n) \cdot p = S(m) \cdot (n \cdot p), \forall n \in \mathbb{N}, \forall p \in \mathbb{N}]$

Demonstração: (i) $(1 \cdot n) \cdot p \underset{\text{Lema}(\alpha)}{=} n \cdot p \underset{\text{Lema}(\alpha)}{=} 1 \cdot (n \cdot p)$ ∎

(ii) Dado $n \in \mathbb{N}, p \in \mathbb{N}$, temos que: $(S(m) \cdot n) \cdot p \underset{\text{Lema}(\beta)}{=} (m \cdot n + n) \cdot p \underset{(d2)}{=}$

$= (m \cdot n) \cdot p + n \cdot p \overset{\substack{\text{Hipótese de} \\ \text{Indução}}}{=} m \cdot (n \cdot p) + n \cdot p \overset{\text{Lema}(\beta)}{=} S(m) \cdot (n \cdot p)$ ∎

6 Discuta se valem ou não as propriedades do cancelamento e da monotonicidade da multiplicação quando consideramos os naturais incluindo o zero.

O cancelamento e a monotonicidade não valem com o zero:

– Tome $m = 1$ e $n = S(1)$. Então, pela definição, temos que $m \cdot 0 = n \cdot 0 = 0$ e $m \neq n$, pois $m < n$. Logo, não vale o cancelamento

– Usando o mesmo exemplo acima, vemos que também não vale a monotonicidade.

7 Prove o seguinte resultado, sabendo que $\mathbb{N}$ contém o zero:

Seja $X \subseteq \mathbb{N}$ tal que (i) $a \in X$; e (ii) $n \in X \Rightarrow n+1 \in X$

Mostre que $\{a, a+1, a+2, \ldots\} = \{a + m \mid m \in \mathbb{N}\} \subseteq X$

Para mostrarmos que $A=\{a+m \mid m \in \mathbb{N}\} \subseteq X$, vamos demonstrar que $M=\{m \in \mathbb{N} \mid a+m \in X\}$ é igual ao conjunto $\mathbb{N}$ dos números naturais (com zero)

Para isso, pela Axiomática de Peano, basta provarmos que:

(α) $0 \in M$; e (β) $m \in M \Rightarrow S(m) \in M$.

Demonstração: (α) $a+0=a \in X$ por (i), logo $0 \in M$;

(β) $m \in M \Rightarrow a+m \in X \underset{\text{por (ii)}}{\Longrightarrow} (a+m)+1 = a+(m+1) = a+S(m) \in X \Rightarrow S(m) \in M$ ∎

(8) Sejam a e b naturais fixados. Prove que para quaisquer m e n naturais, temos que:

(a) $a^m \cdot a^n = a^{m+n}$;

(b) $(a^m)^n = a^{m \cdot n}$;

(c) $(a \cdot b)^n = a^n \cdot b^n$

(a) Vamos provar por indução em n, isto é, vamos demonstrar que:

(i) $a^m \cdot a^1 = a^{m+1}, \forall m \in \mathbb{N}$;

(ii) $(a^m \cdot a^n = a^{m+n}, \forall m \in \mathbb{N}) \Longrightarrow (a^m \cdot a^{n+1} = a^{m+(n+1)}, \forall m \in \mathbb{N})$;

Demonstração: (i) $a^m \cdot a^1 = a^1 \cdot a^m = a^{1+m} = a^{m+1}, \forall m \in \mathbb{N}$

(ii) $a^m \cdot a^{n+1} = a^m \cdot (a \cdot a^n) = (a^m \cdot a^n) \cdot a \underset{\substack{\text{Hipótese de} \\ \text{Indução}}}{=} a^{m+n} \cdot a = a \cdot a^{m+n} = a^{1+(m+n)} =$

$= a^{m+(n+1)}, \forall m \in \mathbb{N}$ ∎

(b) Vamos provar por indução em n, isto é, vamos demonstrar que:

(i) $(a^m)^1 = a^{m \cdot 1}, \forall m \in \mathbb{N}$;

(ii) $[(a^m)^n = a^{m \cdot n}, \forall m \in \mathbb{N}] \Longrightarrow [(a^m)^{n+1} = a^{m \cdot (n+1)}, \forall m \in \mathbb{N}]$

Demonstração: (i) $(a^m)^1 = a^m = a^{m \cdot 1}, \forall m \in \mathbb{N}$

(ii) $(a^m)^{n+1} = a^m \cdot (a^m)^n \underset{\substack{\text{Hipótese de} \\ \text{Indução}}}{=} a^m \cdot a^{m \cdot n} \underset{(a)}{=} a^{m+m \cdot n} = a^{m \cdot (n+1)}, \forall m \in \mathbb{N}$ ∎

(c) Vamos provar por indução em n, isto é, vamos demonstrar que:

(i) $(a \cdot b)^1 = a^1 \cdot b^1$; e (ii) $(a \cdot b)^n = a^n \cdot b^n \Rightarrow (a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}$.

Demonstração: (i) $(a \cdot b)^1 = a \cdot b = a^1 \cdot b^1$ ∎

(ii) $(a \cdot b)^{n+1} = (a \cdot b) \cdot (a \cdot b)^n \underset{\substack{\text{Hipótese de} \\ \text{Indução}}}{=} (a \cdot b) \cdot (a^n \cdot b^n) = (a \cdot a^n) \cdot (b \cdot b^n) = a^{n+1} \cdot b^{n+1}$ ∎

(9) Mostre que, para todo $n \geq 4$ natural, temos que:

(a) $2^n < n!$ (Antes de fazer a prova, defina recursivamente a função $n!$)

Fat: $\mathbb{N} \to \mathbb{N}$ é definida por: $\begin{cases} i. \ Fat(1) = 1 \\ ii. \ Fat(n+1) = (n+1) \cdot Fat(n) \end{cases}$

Obs: Da mesma forma, podemos definir em (i) que $Fat(0) = 1$

Vamos mostrar que $2^n < n! \ \forall n \geq 4$, por indução, isto é, vamos demonstrar que:

(i) $2^4 < 4!$ e (ii) $(2^n < n!) \Rightarrow (2^{n+1} < (n+1)!)$

Demonstração: (i) $2^4 = 16 < 24 = 4!$ ∎

(ii) $2^{n+1} = 2 \cdot 2^n \underset{\text{Hipótese de Indução}}{<} 2 \cdot n! \underset{4 \leq n}{<} (n+1) \cdot n! = (n+1)!$ ∎

(b) $2n^3 > 3n^2 + 3n + 1$

Vamos mostrar por indução em n, isto é, vamos demonstrar que:

(i) $2 \cdot 4^3 > 3 \cdot 4^2 + 3 \cdot 4 + 1$;

(ii) $(2 \cdot n^3 > 3n^2 + 3n + 1) \Rightarrow (2 \cdot (n+1)^3 > 3 \cdot (n+1)^2 + 3 \cdot (n+1) + 1)$

Demonstração: (i) $2 \cdot 4^3 = 128 > 61 = 3 \cdot 4^2 + 3 \cdot 4 + 1$

(ii) $3 \cdot (n+1)^2 + 3 \cdot (n+1) + 1 = 3 \cdot n^2 + 6 \cdot n + 3 + 3 \cdot n + 3 + 1 =$

$= (3 \cdot n^2 + 3 \cdot n + 1) + (6n + 6) \underset{\text{Hipótese de Indução}}{<} 2 \cdot n^3 + 6n + 6 \underset{\boxed{n > 1}}{<} 2 \cdot n^3 + 6 \cdot n + 6 \cdot n^2 <$

$< 2 \cdot n^3 + 6 \cdot n^2 + 6 \cdot n + 2 = 2 \cdot (n^3 + 3 \cdot n^2 + 3 \cdot n + 1) = 2 \cdot (n+1)^3$ ∎

(10) (Divisão Euclidiana) Dados $n \in \mathbb{N} \cup \{0\}$ e $d \in \mathbb{N}$, mostre que existem naturais q e r tais que:

$$n = d \cdot q + r, \text{ com } 0 \leq r < d$$

Mostre também que fixados n e d, q e r são únicos.

Vamos mostrar por indução em n, isto é, vamos demonstrar que fixado $d \in \mathbb{N}$:

(i) existem naturais q_0 e r_0 tais que $0 = d \cdot q_0 + r_0$ e $0 \leq r_0 < d$;

(ii) Se existem naturais q_n e r_n tais que $n = d \cdot q_n + r_n$ e $0 \leq r_n < d$, então existem naturais q_{n+1} e r_{n+1} tais que $n+1 = d \cdot q_{n+1} + r_{n+1}$ e $0 \leq r_{n+1} < d$

Demonstração:

Tome $q_0 = 0 = r_0$ e teremos que $0 = d \cdot q_0 + r_0$ e $0 \leq r_0 < d$. ∎

(ii) $n+1 \underset{\substack{\text{Hipótese de} \\ \text{Indução}}}{=} d \cdot q_n + r_n + 1$. Então, como $0 \leqslant r_n < d$, temos a seguinte dicotomia: $r_n + 1 < d$ ou $r_n + 1 = d$:

- Se $r_n + 1 < d$, basta tomar $q_{n+1} = q_n$ e $r_{n+1} = r_n + 1$ e assim, teremos que $n+1 = d \cdot q_{n+1} + r_{n+1}$ e $0 \leqslant r_{n+1} < d$.
- Se $r_n + 1 = d$, basta tomar $q_{n+1} = q_n + 1$ e $r_{n+1} = 0$ e assim, teremos que $n+1 = d \cdot q_n + r_n + 1 = d \cdot q_n + d = d \cdot q_n + d \cdot 1 = $
$= d \cdot (q_n + 1) = d \cdot q_{n+1} + 0 = d \cdot q_{n+1} + r_{n+1}$ e $0 \leqslant 0 = r_{n+1} < d$

De qualquer forma, existem os naturais pedidos ∎

Para demonstrarmos a unicidade de q e r, suponha que, fixados n e d naturais, existam naturais q, q', r e r' tais que $n = d \cdot q + r$ e $n = d \cdot q' + r'$. Agora suponha por absurdo que $q < q'$ (sem perda de generalidade), então teríamos que $n = d \cdot q + r \underset{\boxed{r<d}}{<}$
$< d \cdot q + d = d \cdot (q+1) \underset{q<q'}{\leqslant} d \cdot q' \underset{0 \leqslant r'}{\leqslant} d \cdot q' + r' = n$, isto é, $n < n$, absurdo.

Portanto, temos que $q = q'$, donde $\cancel{d \cdot q} + r = \cancel{d \cdot q'} + r'$ implica que $r = r'$ e, portanto, q e r são únicos ∎