Aulas 1 e 2

1 Introdução ao curso

Este curso pode ser dividido em dois tópicos principais. Lógica e combinatória. O nome "discreta", usado em contraponto a "contínua", implica que as estruturas e objetos estudados neste ramo da matemática podem ser enumerados com os números inteiros. Exemplos de tais estruturas são fórmulas lógicas, conjuntos finitos e seus subconjuntos, e números racionais.

A parte de lógica deste curso consistirá no estudo de proposições, predicados e quantificados, técnicas de demonstração de proposições, com destaque à indução matemática. A parte de combinatória conterá uma revisão de métodos elementares de contagem, estudo de conjuntos e relações, métodos mais sofisticados de contagem e grafos.

2 Proposições lógicas

Uma proposição é uma sentença que possua um estado definido de verdadeiro ou falso. Considere os exemplos a seguir:

Exemplo 1.

(a) $2 + 2 = 4$.

(b) $\pi + 2 < 5$.

(c) O número 18 é um múltiplo de 3.

(d) Para qualquer número real x, $x^2 - 2x + 10 > 0$.

(e) Para qualquer inteiro positivo n, $n^2 + 1$ não é um quadrado perfeito.

(f) Para qualquer inteiro positivo n, $n^2 + 13$ não é um quadrado perfeito.

Se uma sentença não possui um estado definido de ser verdadeira ou falsa, então ela não é uma proposição. Considere os exemplos

Exemplo 2.

(a) Existe n tal que $90 < n^2 + 10 < 100$?

(b) Ache x tal que $x^2 - 4x + 3 < 0$.

(c) $n^2 > m^3$.

O caso (c) acima é um exemplo de uma *sentença aberta*, muito comum em matemática. Uma vez que valores sejam atribuídos às variáveis n e m, (c) passa a se tornar uma proposição, será portanto verdadeira, ou falsa.

Exercício 1.

1. Determine se as proposições no primeiro exemplo são verdadeiras ou falsas.

2. Ache valores de n and m que tornem a sentença aberta $n^2 > m^3$ verdadeira.

3 Tabela de verdade

Dadas sentenças p, q, r,..., podemos construir uma tabela que expressa o valor de verdade de cada uma delas:

sentença	p	q	r
estado	T	F	T

Por exemplo, se $p =$ " o quadrado de todo número real não é negativo", $q =$ "um dia tem 28 horas" e $r =$ "hoje é quarta feira", então a tabela acima corretamente descreve os valores de verdade destas sentenças.

Alguns símbolos são usados para comporem ou alterarem proposições, criando novas proposições.

(a) Negação: o símbolo $\neg$ modifica a proposição de modo que sempre que esta for verdadeira, a nova proposição seja falsa, e vice-versa. Por exemplo, $\neg p =$ "o quadrado de todo número real é negativo". Note que p originalmente era verdadeira, portanto $\neg p$ é falsa. Precisamente,

	dado	consequência
sentença	p	$\neg p$
estado	T	F
estado	F	T

Novamente: sempre que uma sentença for verdadeira, sua negação será falsa, e sempre que uma sentença for falsa, sua negação será verdadeira. É preciso muito cuidado para se construir a negação de uma sentença.

Por exemplo, qual a negação da sentença: "Todo corvo é preto" ? Será "Nenhum corvo é preto" ?

(b) Conjunção: A conjunção $\wedge$ de duas sentenças é a sentença que se obtém adicionando um "e" entre elas. Por exemplo $p \wedge q =$ "o quadrado de todo número real é não negativo E um dia tem 28 horas". Naturalmente, uma conjunção é verdadeira se ambas as sentenças forem, e falsa se ao menos uma dela for falsa. Em termos da tabela:

dado	dado	consequência
p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

(c) Disjunção: A disjunção $\vee$ de duas sentenças é a sentença que se obtém adicionando um "ou" entre elas. Por exemplo $p \vee q =$ "o quadrado de todo número real é não negativo OU um dia tem 28 horas". Naturalmente, uma disjunção é verdadeira se alguma das sentenças o for, e falsa se ambas forem falsas. Em termos da tabela:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Note que na nossa linguagem, muitas vezes o uso da palavra "ou" indica que desejamos que apenas uma das sentenças seja verdadeira. Em lógica, esse "ou" é chamado de "ou exclusivo", e é denotado por $\oplus$.

Por exemplo, ao chegar em um restaurante, você pode ler a frase "o prato feito inclui um pedaço de carne ou um pedaço de frango". Se este "ou" for uma disjunção, significa que você pode escolher carne, frango, ou ambos. O dono do restaurante por outro lado provavelmente desejou usar o "ou exclusivo", onde não há a possibilidade de "ambos".

Exercício 2. Faça a tabela de verdade do "ou exclusivo".

Exercício 3. Complete a tabela de verdade abaixo

p	q	r	$p \wedge r$	$q \vee r$	$p \wedge (q \vee r)$	$(p \wedge r) \vee q$	$\neg(p \wedge r)$	$\neg(p \wedge r) \wedge (q \vee r)$
T	T	T	T	T	T	T	F	F
T	T	F						T
T	F	T	T				F	
T	F	F		F				F
F	T	T			F			
F	T	F						
F	F	T		T			T	
F	F	F	F					

(d) Implicação: A implicação $\Rightarrow$ estabelece que a proposição à direita precisa ser verdade quando a proposição à esquerda o for. Por exemplo, $p \Rightarrow q$ será "SE o quadrado de todo número real não é negativo, ENTÃO um dia tem 28 horas". Neste exemplo, a primeira proposição era verdadeira e a segunda falsa, tornando esta implicação falsa. Note que se a primeira proposição for falsa, a segunda proposição não possui restrição alguma, e portanto a regra que define a implicação verdadeira não é violada, e daí a implicação é automaticamente verdadeira. "SE o céu é verde, ENTÃO a lua é quadrada" é um exemplo de uma implicação verdadeira.

Note que apesar da sugestividade de uma relação de causa e consequência, uma implicação pode ser verdadeira sem que as proposições tenham aparentemente qualquer relação. "SE o céu é azul, ENTÃO a lua é redonda" é um exemplo de implicação verdadeira.

Note também que a ordem das proposições é extremamente relevante. Implicações também podem ser usadas com sentenças abertas, onde o valor de verdade depende de uma atribuição. Note os exemplos abaixo:

- Se n é múltiplo de 6, então n é par. Implicação verdadeira, independente do valor escolhido para n.

- Se n é par, então n é múltiplo de 6. Implicação falsa, uma vez que haverá valores de n que tornam esta implicação falsa.

Há várias maneiras de se expressar linguisticamente uma implicação:

$p \Rightarrow q$.
p implica q.
Se p, então q.
p é uma condição suficiente para q.
q é uma condição necessária para p.
q se p.
p somente se q.

Por exemplo, substitua p por "n é múltiplo de 6" e q por "n é par", e verifique as proposições equivalentes acima.

Na sentença $p \Rightarrow q$, p é chamado hipótese, e q conclusão. Note a tabela de verdade:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Note que dado o valor de uma implicação e de uma das proposições, pode ou não ser possível inferir o valor da outra proposição.

Dado			Conclusão	
$p \Rightarrow q$	p	q	p	q
F			T	F
T	T			T
T	F			?
T		T	?	
T		F	F	

Entretanto, dizer que uma implicação é falsa automaticamente implica em dizer que a hipótese é verdadeira, enquanto a conclusão é falsa.

4 Equivalência lógica

Duas proposições são chamadas de "equivalências lógicas" se elas possuem o mesmo estado de verdade. O símbolo $\equiv$ é usado para denotar tal fato.

Usando tabelas de verdade, resolva os exercícios abaixo.

Exercício 4. Mostre que independente dos valores de verdade de p e q, as proposições $(\neg p \wedge \neg q)$ e $\neg(p \vee q)$ são equivalentes.
Faça o mesmo para $(\neg p \vee \neg q)$ e $\neg(p \wedge q)$.

As equivalências neste exercício são chamadas de Leis de De Morgan.

Exemplo 3. Suponha agora que a pergunta seja: qual a negação de uma implicação? Ou seja, $\neg(p \Rightarrow q)$? Vamos primeiro achar uma proposição equivalente à $p \Rightarrow q$.

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	
T	T	T	F	F	
T	F	F	T	F	
F	T	T	F	T	
F	F	T	T	T	

Note que $\neg p \vee q$ é logicamente equivalente a $p \Rightarrow q$. A idéia aqui é que se p for verdadeira, então a única maneira em que $\neg p \vee q$ também é verdadeira é se q for, uma vez que $\neg p$ é falsa. Isso reproduz o significado da implicação $p \Rightarrow q$.

Exercício 5. Mostre que $p \Rightarrow q$ e $\neg q \Rightarrow \neg p$ são logicamente equivalentes.

5 Conversa, contrapositiva e inversa, e dupla-implicação

Dada uma implicação $p \Rightarrow q$, define-se três implicações a ela associadas:

(a) Conversa: $q \Rightarrow p$.

(b) Contrapositiva: $\neg q \Rightarrow \neg p$

(c) Inversa: $\neg p \Rightarrow \neg q$.

Exercício 6. Construa a conversa, contrapositiva e inversa, das implicações

- "O time da casa vence sempre que está chovendo."
- "Estar fazendo sol é condição suficiente para eu ir ao clube."

Exercício 7. Usando tabela de verdades, prove que $p \Rightarrow q$ é logicamente equivalente à sua contrapositiva.
Conclua que a conversa e a inversa são logicamente equivalentes.
Mostre que uma implicação e sua conversa não são logicamente equivalentes.

Muitas vezes, tanto a implicação $p \Rightarrow q$ como sua conversa $q \Rightarrow p$ são verdadeiras. Neste caso, escrevemos $p \iff q$, indicando ambos os fatos. Em linguagem natural, dizemos

$p \iff q$.
p é equivalente a q.
p se, e somente se, q.
p é uma condição necessária e suficiente para q.

Note que a ordem não é relevante, e podemos dizer igualmente que $q \iff p$.

6 Aplicação

(retirado de www.brilliant.org)

Há 3 caixas fechadas, e exatamente uma contém uma jóia. Você pode ficar com a jóia se escolher a caixa correta em uma tentativa. Na tampa das caixas tem escrito

caixa 1	a jóia está nesta caixa
caixa 2	a jóia não está nesta caixa
caixa 3	a jóia não está na caixa 1

Você foi informado que APENAS UMA das frases é verdadeira. Você sabe onde está a jóia?

7 Tautologias e contradições

Uma *tautologia* é uma sentença que é sempre verdadeira.

Exemplo 4. Note que $p \vee \neg p$ é uma tautologia, independente do valor de p. Para ver isso, consideremos os dois únicos casos possíveis:

- p é verdadeiro. Neste caso, $\neg p$ é falso, mas ainda assim $p \vee \neg p$ é verdadeiro pois ao menos uma das sentenças é verdadeira.
- p é falso. Neste caso $\neg p$ é verdadeiro, e portanto novamente $p \vee \neg p$ é verdadeiro.

Por exemplo, a frase "ou choveu hoje ou não choveu" é uma tautologia.

Uma *contradição* é uma sentença que é sempre falsa.

Exercício 8. Mostre que, independente do valor de p, a sentença $p \wedge \neg p$ é uma contradição.

Exercício 9. Mostre que $(p \wedge q) \Rightarrow (p \vee q)$ é uma tautologia.

8 Revisão

Listamos abaixo várias equivalências lógicas.

Lei de Dupla negação	$\neg(\neg p) \equiv p$
Lei de Distributividade	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Lei de Distributividade	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Lei de De Morgan	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
Lei de De Morgan	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Lei da Absorção	$p \wedge (p \vee q) \equiv p$
Lei da Absorção	$p \vee (p \wedge q) \equiv p$
Lei da Negação	$p \wedge \neg p \equiv F$
Lei da Negação	$p \vee \neg p \equiv T$
Implicação	$p \Rightarrow q \equiv \neg p \vee q$
Contrapositiva	$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
Negação de implicação	$\neg(p \Rightarrow q) \equiv p \wedge \neg q$

Como revisão da semana, demonstre as equivalências abaixo usando tabelas de verdade.

$$\begin{array}{ccc}
(p \Rightarrow q) \wedge (p \Rightarrow r) & \equiv & p \Rightarrow (q \wedge r) \\
(p \Rightarrow r) \wedge (q \Rightarrow r) & \equiv & (p \vee q) \Rightarrow r \\
(p \Rightarrow q) \vee (p \Rightarrow r) & \equiv & p \Rightarrow (q \vee r) \\
(p \Rightarrow r) \vee (q \Rightarrow r) & \equiv & (p \wedge q) \Rightarrow r \\
p \iff q & \equiv & (p \Rightarrow q) \wedge (q \Rightarrow p) \\
p \iff q & \equiv & \neg p \iff \neg q \\
p \iff q & \equiv & (p \wedge q) \vee (\neg p \wedge \neg q) \\
\neg(p \iff q) & \equiv & p \iff \neg q
\end{array}$$

9 Predicados

Como vimos, muitas sentenças não são proposições pois há variáveis sobre as quais não temos informação na sentença. Por exemplo

$$n^2 > m^3.$$

Para formalizarmos este tipo de sentença, introduzimos o conceito de função proposicional, ou predicado:

$$P(n, m) : \text{“}n^2 > m^3\text{”}.$$

Esta função recebe dois valores, um para n e o outro para m, e devolve T ou F. Por exemplo

$$P(3, 2) = T \quad e \quad P(2, 3) = F.$$

Outro exemplo

$$P(x) : \text{“}x \text{ é um número racional”}.$$

Então

$$P(-1) = T \quad \text{e} \quad P(\pi) = F.$$

Exercício 10. Dado o predicado $P(x, y, z)$: “$x + y = z + 2y$”, descreva todos os números reais x, y e z tais que $P(x, y, z) = T$.

10 Quantificadores

Dado um predicado, por exemplo $P(x)$: “$x^2 \geq x$”, podemos atribuir um valor para x e obtermos um valor para $P(x)$, mas também podemos criar proposições a respeito de $P(x)$ onde os valores de x são descritos como pertencentes a algum intervalo. Por exemplo

$$\text{Para todo } x \in \mathbb{R},\ x^2 \geq x.$$

Esta sentença é verdadeira se $P(x)$ for verdadeira para todo $x \in \mathbb{R}$, e falsa caso $P(x)$ seja falsa para pelo menos um $x \in \mathbb{R}$.

O caso dual ocorre quando desejarmos que a sentença seja verdadeira se ela o for para pelo menos um elemento de um dado conjunto. Observe.

$$\text{Existe algum } x \in \mathbb{R} \text{ tal que } x^2 > x.$$

Esta sentença é verdadeira se existir ao menos um $x \in \mathbb{R}$ tal que $P(x)$ é verdadeira, e será falsa caso $P(x)$ seja falsa para todas as possíveis escolhas de $x \in \mathbb{R}$.

Note que apesar do predicado $P(x)$ ser o mesmo, as sentenças são completamente diferentes. Em particular, neste exemplo, uma delas é falsa, e a outra é verdadeira.

Exercício 11. Qual é qual?

- Observações: "para todo" ou "para qualquer" são sinônimos, e em geral é representado pelo símbolo $\forall$. "Existe" é representado pelo símbolo $\exists$. Estes são exemplos de **quantificadores**.

Definição 1. Uma proposição quantificada é uma proposição da forma

"quantificador" "variável" em "domínio", "predicado contendo variável".

Exercício 12. Determine nas sentenças abaixo as quatro partes que formam uma proposição quantificada:

(i) Existe um inteiro k tal que $k^2 - k$ é um múltiplo de 3.

(ii) Para todo $x \in \mathbb{R}$, $x^2 + x^3 + x^4 > 0$.

(iii) $\forall x \in \mathbb{Q}$, $x^2 \in \mathbb{Q}$.

(iv) $\exists n \in \mathbb{Z} : (n > 1 \ \wedge \ n/n^2 \in \mathbb{Z})$.

(v) A equação $x^2 = 3$ possui uma solução entre os números inteiros.

Determine se as proposições acima são verdadeiras ou falsas. Em cada exemplo, modifique precisamente uma das quatro partes de modo que o estado de verdade seja alterado.

Quando o quantificador $\forall$ é utilizado, pode ser necessário testar todos os elementos do conjunto para obtermos o estado de verdade da proposição.

Exercício 13. Seja $S = \{4, 5, 6\}$. Prove que $\forall x \in S, x^2 > 10$.

As vezes isso não é possível, por exemplo, se o conjunto S for infinito. Neste caso é necessário usar gerais a respeito dos elementos do conjunto.

Exercício 14. Prove que $x^2 \geq x$ para todos os números naturais x.

Para mostrar que uma proposição com o quantificador $\exists$ é verdadeira, é suficiente achar apenas um exemplo no conjunto.

Exercício 15. Seja $S = \{4, 5, 6\}$. Prove que $\exists x \in S, x^2 < 20$.

11 Negação de quantificadores

Exemplo 5. Para todo $n \in \mathbb{Z}$, $n^3 - n > n^2 - 1$. Negar uma proposição como esta significa dizer que a propriedade $n^3 - n > n^2 - 1$ não é verdadeira para todos os números inteiros. Ou seja, é preciso mostrar que "existe um $n \in \mathbb{Z}$ tal que $n^3 - n > n^2 - 1$ é falsa".

Em geral, temos as seguintes regras:

(1) Proposição: "$\forall x \in S, P(x) = T$". Negação: "$\exists x \in S : P(x) = F$".

(2) Proposição: "$\exists x \in S : P(x) = T$". Negação: "$\forall x \in S, P(x) = F$".

Exercício 16. Negue a proposição abaixo sem usar a palavra "não".

$$\text{For all } x \in \mathbb{R}, \text{ se } x^4 + 2x^2 - 2x < 0, \text{ então } 0 < x < 1.$$

Agora decida se é a proposição ou a sua negação que é verdadeira.

12 Quantificadores aninhados

Muitas proposições possuem mais de um quantificador. Isto ocorre quando o predicado de um proposição quantificada é em si uma proposição quantificada a respeito de uma outra variável. É preciso portanto saber aninhar os quantificadores de uma sentença.

Exemplo 6. Para todo $n \in \mathbb{Z}$, existe um $x \in \mathbb{R}$ tal que $n^2 + x^2$ é primo. Vamos separar esta proposição:

(i) Quantificador: "para todo".

(ii) Variável: n.

(iii) Domínio: $\mathbb{Z}$.

(iv) Predicado: $\begin{cases} \text{(a)} & \text{Quantificador: "existe".} \\ \text{(b)} & \text{Variável: } x. \\ \text{(c)} & \text{Domínio: } \mathbb{R}. \\ \text{(d)} & \text{Predicado: } n^2 + x^2 \text{ é primo.} \end{cases}$

Para checar se uma proposição como esta é verdadeira, é preciso começar com um número inteiro arbitrário n e descobrir se é possível achar um número real x (que provavelmente dependerá de n) tal que $n^2 + x^2$ é primo.

Exercício 17. Mostre que a proposição do exemplo acima é verdadeira. Mostre que ela se torna falsa se trocarmos $\mathbb{R}$ por $\mathbb{Z}$.

Note que a ordem em que os quantificadores estão aninhados é extremamente relevante. De fato, ao alterar esta ordem, a proposição pode se tornar falsa. Em

$$\text{Para todo } n \in \mathbb{Z}, \text{ existe um } x \in \mathbb{R} \text{ tal que } n^2 + x^2 \text{ é primo,}$$

é preciso mostrar como achar um x específico que funcione para qualquer n. Por outro lado, na frase

Existe um $x \in \mathbb{R}$ tal que para todo $n \in \mathbb{Z}$, $n^2 + x^2$ é primo,

seria preciso achar um único $x \in \mathbb{R}$ que funcione para todo $n \in \mathbb{Z}$. Esta última proposição é claramente falsa.

Com 2 variáveis, é possível escrever quatro tipos de proposições com quantificadores aninhadas.

(i) $\forall x \in S, \forall y \in T,\ P(x, y)$.

- Para mostrar que tal proposição é verdadeira, é preciso checar que $P(x, y)$ é verdadeira para quaisquer escolhas possíveis de x e y.
- A negação: $\exists x \in S : \exists y \in T : \neg P(x, y)$.

(ii) $\forall x \in S, \exists y \in T,\ P(x, y)$.

- Para mostrar que tal proposição é verdadeira, é preciso começar com o elemento arbitrário $x \in S$ e achar um $y \in T$ que possivelmente dependa de x tal que $P(x, y)$ é verdadeira para eles.
- A negação: $\exists x \in S : \forall y \in T, \neg P(x, y)$.

(iii) $\exists x \in S : \forall y \in T,\ P(x, y)$.

- Para mostrar que tal proposição é verdadeira, é preciso um elemento particular $x \in S$ tal que para qualquer escolha de y, $P(x, y)$ seja verdadeira.
- A negação: $\forall x \in S : \exists y \in T : \neg P(x, y)$.

(iv) $\exists x \in S : \exists y \in T : P(x, y)$.

- Para mostrar que tal proposição é verdadeira, é preciso achar dois elementos particulares $x \in S$ e $y \in T$ tais que $P(x, y)$ seja verdadeira.
- A negação: $\forall x \in S, \forall y \in T, \neg P(x, y)$.

Exercício 18. Neste exercício, expresse a negação da proposição. A seguir prove se a proposição é verdadeira ou falsa usando ela ou sua negação.

(1) Existe um número real x tal que para todos os números inteiros n, $xn^2 = (2^x - 1)n^3$.

(2) Para todos os inteiros n e m, $n^2 > m^3$ ou $n < m$.

(3) Para todos os inteiros positivos n, existe um número real x tal que $n + 1 > x^3 > n$.

(4) Existe um inteiro n e existe um número real x tais que $n^2 > x^2 > (n + 1)^2$ e $x < n$.

Aulas 3 e 4

13 Demonstrações matemáticas

Nesta seção, vamos estudar como se estrutura o conhecimento matemático. Começamos com uma introdução à terminologia:

- Um **axioma (ou postulado)** é afirmação assumida como verdadeira sem a necessidade de uma prova; axiomas são considerados verdades auto-evidentes.
- Um **teorema** é uma afirmação que se pode demonstrar ser verdadeira. Um teorema é um resultado considerado interessante em si mesmo.
- Uma **proposição** é também uma afirmação que se pode demonstrar verdadeira, mas considerada um teorema de menor interesse.
- Um **lema** é uma afirmação auxiliar a ser provada, geralmente para quebrar a prova de um teorema grande em pedaços menores.
- Uma **prova (ou demonstração)** é um argumento que mostra que uma afirmação (teorema, proposição ou lema) segue de um conjunto de premissas.
- Um **corolário** é afirmacão derivável facilmente a partir de um teorema já provado. Colorários são consequências imediatas de outros resultados.
- Uma **conjectura** é suposição bem fundada, porém (ainda) sem prova. Uma vez provada, uma conjectura se torna um teorema ou uma proposição.

Note que para chamarmos algo de prova, é necessário checar que de fato trata-se de um argumento, assim como definido na seção anterior. Ou seja, é preciso que a conclusão possa ser inferida a partir de um conjunto de premissas bem explicitadas. Em contraponto a outras ciências naturais, uma quantidade significativa de evidências é absolutamente irrelevante para determinar se uma proposição é verdadeira. Observe o exemplo.

Exemplo 7.

$$p(n) = n^2 + n + 41$$

Conjectura: $\forall n \in \mathbb{N} : p(n)$ é primo.

Podemos facilmente achar evidências de que a conjectura estaria certa:

Testando valores de $n = 0, 1, \ldots, 39$ a proposição é sempre verdadeira, ou seja, $p(n)$ é primo para $0 \leq n \leq 39$.

n	0	1	2	3	...	20	...	39
$p(n)$	41	43	47	53	...	461	...	1601

Isto não pode ser uma coincidência! A hipótese deve ser verdadeira!

Mas não é: $p(40) = 1681 = 41 \cdot 41$, que não é primo!

Logo, a conjectura é falsa.

Exemplo 8.

- Em 1769, Euler (1707–1783) conjecturou que

$$a^4 + b^4 + c^4 = d^4$$

não tem solução no conjunto dos números inteiros positivos. Durante mais de dois séculos, ninguém conseguiu encontrar valores de a, b, c e d que satisfizessem a equação. O insucesso de todos os matemáticos envolvidos era evidência de que a conjectura poderia ser verdadeira. 218 anos depois, em 1987, Noam Elkies proveu um contra-exemplo, mostrando que

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

Logo, esta conjectura também é falsa.

- Resumindo: Ausência de prova não o mesmo que prova de ausência!

Para escrever uma boa prova matemática, não existe uma receita fechada. O melhor conselho é praticar bastante, mas existe pelo menos uma regra geral a ser seguida:

- Ao se ler a prova em voz alta, substituindo cada símbolo matemático por palavras, a prova deve fazer sentido! Ou seja, é importante definir todas as variáveis usadas, utilizar preposições e pontuação adequada, assim como se certificar que a ordem das proposições faz sentido logicamente.

Uma prova deve estar sempre organizada da seguinte forma:

Teorema. *Proposição que se deseja mostrar. Pode listar algumas hipóteses, e deve estar claro qual a conclusão desejada.*

Demonstração. Argumento utilizando como premissas (1) axiomas (2) proposições conhecidas (3) hipóteses listadas no enunciado do teorema (4) definições, e chegando à conclusão enunciada no teorema. □

Observe o seguinte exemplo. Lembre-se que um número inteiro n é definido como par se existe um número inteiro k tal que $n = 2k$, e é definido como ímpar se existe um número inteiro k tal que $n = 2k + 1$.

Teorema. *Se n é ímpar, então n^2 é ímpar.*

Demonstração. Se n é ímpar, então existe $k \in \mathbb{Z}$ tal que $n = 2k + 1$. Note então que

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1.$$

Por sua vez, podemos reorganizar $4k^2 + 4k + 1$ como $2(2k^2 + 2k) + 1$. Daí concluímos que existe um número inteiro, no caso $m = 2k^2 + 2k$ tal que $n^2 = 2m + 1$. Por definição, n^2 é um número ímpar. □

A seguir, enumeramos uma lista de provas erradas ou impróprias para este teorema.

(a) $n = 2k + 1 \Rightarrow n^2 = 2(2k^2 + 2k) + 1$. Logo n^2 é ímpar. □

Esta prova peca por ser muito concisa. Por mais que esteja claro que o autor sabe como provar o enunciado original, esta prova pula muitos passos e introduz a variável k sem especificar a qual domínio pertence. De fato, caso k seja somente racional, esta prova estaria errada. Uma prova como esta receberia uma nota de 7/10.

(b) Se n é ímpar, então existe k inteiro tal que $n = 2k + 1$. Se n^2 é ímpar, então existe m inteiro tal que $n^2 = 2m + 1$. Como $(2k + 1)^2 = 2(2k^2 + 2k) + 1$, basta escolhermos $m = 2k^2 + 2k$, e vemos que n^2 é ímpar. □

Esta prova cometeu o grave erro de supor como premissa a conclusão que se deseja mostrar. Por mais que as idéias estejam ok, na organização da prova a conclusão jamais poderá ser escrita como uma hipótese. Uma prova como esta receberia uma nota de 2/10.

(c)

$$\begin{aligned}
&n = 2k + 1 \\
&n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \\
&n^2 \text{ é ímpar} \quad \square
\end{aligned}$$

Tente ler esta prova em voz alta. Não está claro o que é definição, o que é hipótese, o que são variáveis, o que é a conclusão. Falta preposições e pontuação nesta prova. Uma prova como esta receberia uma nota de 4/10.

(d) Ímpar vezes ímpar é ímpar, e como $n^2 = n \times n$, então n^2 é ímpar. □

Claramente a pessoa escrevendo esta prova não sabe usar a definição matemática de número ímpar, e acaba quase que supondo a conclusão e fazendo um raciocínio circular. Aqui a nota é 0.

Exercício 19. Prove matematicamente que ímpar vezes ímpar é ímpar.
(note que você está multiplicando dois números ímpares que não são necessariamente iguais).

Exercício 20. Prove que se n^2 é ímpar, então n é ímpar.

Exercício 21. Um número inteiro n é um quadrado perfeito se existe um número inteiro k tal que $n = k^2$. Prove que o produto de quadrados perfeitos é um quadrado perfeito.

Prove que a soma de quadrados perfeitos não é necessariamente um quadrado perfeito.

Exercício 22. Um número real x é racional se existem números inteiros p e q tais que $x = p/q$. Prove que a soma e o produto de dois números racionais é sempre racional.

14 Prova por contrapositiva

A prova por contrapositiva se aplica a situações onde a proposição a ser provada é uma implicação, muitas vezes quantificada, na forma

$$\forall x, P(x) \Rightarrow Q(x). \tag{$*$}$$

Como vimos, $p \Rightarrow q$ e sua contrapositiva $\neg q \Rightarrow \neg p$ são equivalente, portanto uma alternativa para mostrar $(*)$ é mostrar que

$$\forall x, \neg Q(x) \Rightarrow \neg P(x).$$

Por exemplo, considere a seguinte proposição.

Proposição. *Para todo n inteiro, se $3n + 2$ é ímpar, então n é ímpar.*

Note que começar com $3n + 2 = 2k + 1$ e tentar terminar com $n = 2m + 1$ para algum m pode ser um pouco complicado. Entretanto, a contrapositiva desta afirmação é uma proposição fácil de lidar:

Para todo n inteiro, se n é par, então $3n + 2$ é par.

Demonstração. Vamos fazer a demonstração por contrapositiva. Se n é par, então existe k inteiro tal que $n = 2k$. Logo $3n + 2 = 6k + 2 = 2(3k + 1)$. Logo, se $m = 3k + 1$, segue que $3n + 2 = 2m$. Portanto $3n + 2$ é par. □

Exercício 23. Mostre que se $n = ab$, então $n \leq \sqrt{a}$ ou $n \leq \sqrt{b}$. Faça a demonstração pelo método de mostrar a contrapositva.

15 Prova por contradição

A prova por contradição é um dos métodos de demonstração mais úteis em matemática. Basicamente consiste em supor a negação da conclusão, e mostrar que isso leva a uma contradição lógica. Ou seja, se a negação da proposição é uma premissa que, com o uso correto de regras de inferência, leva a uma conclusão falsa, então a premissa deve ser falsa, ou seja, a negação da proposição deve ser falsa, e portanto a proposição deve ser verdadeira.

Numa prova por contradição, a primeira frase da prova sempre deve ser "Suponha com o intuito de chegar a uma contradição que...", e o que se segue é a negação da proposição que se deseja mostrar.

O exemplo clássico de uma prova por contradição é a prova de que $\sqrt{2}$ não é um número racional. Lembre-se que um número é racional se ele pode ser expresso como uma fração p/q onde p e q são inteiros, e que é sempre possível simplificar esta fração de modo que p e q sejam coprimos.

Teorema. $\sqrt{2}$ *não é um número racional.*

Demonstração. Suponha para efeito de chegar a uma contradição que $\sqrt{2}$ é racional. Ou seja, existem inteiros a e b tais que $\sqrt{2} = a/b$. Supomos que esta fração já esteja simplificada, ou seja, que a e b são coprimos. Segue que

$$2 = a^2/b^2,$$

e portanto

$$2b^2 = a^2$$

. Logo a^2 é par, e portanto a é par. Daí, existe um inteiro k tal que $a = 2k$, e portanto $a^2 = 4k^2$. Segue que

$$b^2 = 2k^2,$$

logo b^2 é par, e portanto b é par. Portanto a e b são pares, uma contradição ao fato de que são coprimos. Logo $\sqrt{2}$ não pode ser racional. □

Exercício 24. Prove os seguintes fatos por contradição.

(1) Se p é um número primo, então $\sqrt{p}$ é irracional.

(2) Não existem inteiros p e q tais que $p^2 - q^2 = 10$.

(3) Se $x^3 + x + 1 = 0$, então x não é racional.

Os próximos dois teoremas são muito importantes em matemática, e em geral suas demonstrações são por contradição.

Teorema. *Todo número inteiro maior que* 1 *ou é primo ou é um produto de números primos.*

Demonstração. Suponha com o intuito de chegar a uma contradição que o enunciado é falso, e portanto existem números maiores que 1 que nem são primos e nem são o produto de números primos. Dentre todos eles, seja N o menor deles. Como N não é primo, ele é composto, e portanto existem inteiros a e b, menores que N, tais que $N = ab$. Mas como a e b são menores que N, ou eles são primos ou são o produto de números primos. Logo N é um produto de números primos. Uma contradição lógica, portanto o enunciado do teorema precisa ser verdadeiro. □

Teorema. *Existem infinitos números primos.*

Demonstração. Suponha para chegar a uma contradição que a quantidade de números primos é finita. Seja $\{p_1, ..., p_n\}$ o conjunto de todos eles, e considere o número

$$N = (p_1 \times p_2 \times ... \times p_n) + 1.$$

Em particular N é maior que todos os primos que existem, e nenhum dos números primos p_1,...,p_n pode dividir N. Logo N não pode ser escrito como o produto de números primos. Mas, pelo teorema anterior, segue que N é primo. Uma contradição ao fato que N é maior que todos os primos que existem. Portanto existem infinitos números primos. □

16 Outros exemplos interessantes

Listamos abaixo algumas outras estratégias típicas em matemática para demonstrar fatos.

Proposição. *Existe um número inteiro que pode ser escrito como a soma de dois cubos de inteiros positivos de duas maneiras distintas.*

Prova por exibição de exemplo. Para que esta proposição seja verdadeira, basta acharmos um número inteiro que satisfaça a propriedade.

Demonstração. Note que

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

□

Exercício 25. Mostre por exibição de exemplo que nem todo número inteiro pode ser escrito como a soma de dois quadrados.

Proposição. *Mostre que, dados dois números reais x e y, teremos que*

$$\min\{x, y\} + \max\{x, y\} = x + y.$$

Para demonstrar esta proposição, dividimos em casos.

Demonstração. Se $x < y$, então $\min\{x, y\} = x$ e $\max\{x, y\} = y$, daí

$$\min\{x, y\} + \max\{x, y\} = x + y.$$

Se $x > y$, então $\min\{x, y\} = y$ e $\max\{x, y\} = x$, daí

$$\min\{x, y\} + \max\{x, y\} = x + y.$$

Se $x = y$, então $\min\{x, y\} = x$ e $\max\{x, y\} = x$, daí

$$\min\{x, y\} + \max\{x, y\} = 2x = x + y.$$

Como todos os casos possíveis foram contemplados, a proposição segue. □

Exercício 26. Mostre por divisão em casos que $|xy| = |x||y|$.

Podemos misturar divisão de casos e prova existencial.

Proposição. *Existem números irracionais x e y tais que x^y é racional.*

Aqui novamente somos tentados a acharmos um exemplo. Mas as vezes é possível mostrar que algo existe sem precisamente exibi-lo.

Demonstração. Considere $a = \sqrt{2}$ e $b = \sqrt{2}^{\sqrt{2}}$. Sabemos que a é irracional. Ou b é racional, ou é irracional. Se for racional, note que $b = a^a$, e fazendo $x = y = a$, teremos que x^y é racional. Se b for irracional, então fazemos $x = b$, $y = a$, e teremos

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2,$$

que é racional. □

Note que no exemplo acima, nós não sabemos se $\sqrt{2}^{\sqrt{2}}$ é racional, mas isso não impediu a demonstração da proposição.

Aulas 5 e 6

17 Notação de soma e produto

Como expressar a seguinte soma de uma maneira mais concisa?

$$1^2 + 2^2 + 3^3 + ... + 10^2 \quad ?$$

Note que as parcelas são semelhantes, e que a única coisa que varia é base do expoente. Quando temos uma soma em que a variação de uma parcela para outra depende de uma única variável, que cresce uma unidade a cada parcela, podemos usar a notação de somatório:

$$\sum_{j=1}^{10} j^2.$$

A variável que aparece abaixo de σ indica o que mudará de parcela em parcela. O valor que ela começa é o que aparece ao lado dela, com o sinal de igual. E o valor acima σ é o último que ela atinge.

Exercício 27. Escreva por extenso os seguintes somatórios:

$$\sum_{k=1}^{4} k! \qquad \sum_{n=2}^{6} \sin(n\pi) \qquad \sum_{n=-2}^{0} 4.$$

Muitas vezes a variável não se altera de 1 em 1. Para generalizar, se S é um conjunto, o símbolo

$$\sum_{x \in S} f(x)$$

significa a soma de todos os valores $f(x)$ obtidos quando $x \in S$.

Exercício 28. Seja $S = \{1, 3, 10\}$. Calcule

$$\sum_{x \in S} x^2.$$

Note que é possível fazer alterações na disposição dos índices, ou acrescentar ou remover termos, ou ter restrições explicitadas em outras notações. Considere os exemplos:

(i) $\displaystyle\sum_{k=1}^{n} (k+1) = n + \sum_{k=1}^{n} k = 2n + \sum_{k=1}^{n-1} k.$

(ii) $\displaystyle\sum_{i=1}^{n} i^2 = \sum_{i=2}^{n+1} (i-1)^2.$

(iii) $\displaystyle\sum_{j=2}^{10} j^3 - \sum_{k=1}^{8} k^2 = 10^3 + \sum_{j=1}^{8} (j+1)^3 - \sum_{k=1}^{8} k^2 = 10^3 + \sum_{j=1}^{8} \left[(j+1)^3 - j^2\right]$

Igualmente, se desejarmos representar o produto de vários elementos, poderemos utilizar a notação de produtório:

$$\prod_{k=1}^{3} k^2 = 1^2 \cdot 2^2 \cdot 3^2 = 36.$$

Exercício 29. Expresse o fatorial de n como um produtório.

18 Recorrência

Uma relação de recorrência é uma maneira de definir uma sequência de valores, cada um dos quais definidos a partir de alguns de seus antecessores. Por exemplo

(i) $x_1 = 2$.

(ii) $x_n = 2x_{n-1} + 3$.

Quando $n = 2$, teremos que $x_2 = 2x_1 + 3 = 7$. Agora podemos fazer $n = 3$, e teremos $x_3 = 17$.

Exercício 30. Ache o x_5 acima.

Exercício 31. Expresse

$$x_n = \sum_{k=1}^{n} k^2 + 1$$

como uma relação de recorrência.

Exercício 32. Expresse $x_n = n!$ como uma relação de recorrência.

Exemplo 9. A sequência de Fibonacci é definida como uma relação de recorrência

$$f_n = f_{n-1} + f_{n-2}.$$

Como a definição envolve dois termos anteriores, é preciso dar pelo menos os dois primeiros valores da sequência para podermos definir os demais:

$$f_1 = 1 \qquad f_2 = 1.$$

Mais para frente, voltaremos a falar mais em detalhes de certos tipos de recorrência.

19 Indução

Indução matemática é uma técnica muito poderosa para demonstrar propriedades expressas em termos de números inteiros positivos n. Basicamente, uma prova por indução funciona da seguinte forma:

(i) Primeiro mostra-se que a propriedade é verdadeira para alguns valores pequenos de n.

(ii) E então mostramos que se a propriedade é verdadeira para um valor arbitrário de n, então ela tem que ser verdadeira para $n+1$.

Em outras palavras, imagine que existe uma propriedade P que depende de valores $n \in \mathbb{Z}^+$, e que desejamos mostrar que
$$\forall n \geq 1,\ P(n) = T.$$

Para tal, o caminho é:

(i) Mostrar que $P(1) = T$.

(ii) Mostrar que $P(n) = T \Rightarrow P(n+1) = T$.

Por exemplo, se $n = 1$ no ponto (ii), saberemos que $P(1) \Rightarrow P(2)$. Como $P(1) = T$ pelo ponto (i), segue que $P(2) = T$. Agora que sabemos que $P(2) = T$, olhamos para o ponto (ii) com $n = 2$. Sabemos por (ii) que $P(2) = T \Rightarrow P(3) = T$. Como, de fato, $P(2) = T$, segue que $P(3) = T$. E assim sucessivamente. O relevante de tudo isso é que basta mostrar (i) e (ii) e todos os casos seguirão automaticamente.

A maneira de escrever uma prova por indução é a seguinte:

- Sentença: $\forall n \geq 1$, $P(n)$ é verdadeira.
- Prova:
  (i) "Caso base": demonstra o caso específico que $P(1)$ é verdadeira.
  (ii) "Hipótese indutiva": declare, para um dado k, $P(k)$ é verdadeira.
  (iii) "Conclusão indutiva": Mostra que $P(k+1)$ é verdadeira. Para tal, você pode usar todas as propriedades matemáticas que você está acostumado, mas principalmente, você deve usar a sentença $P(k)$ escrita em (ii) como hipótese.

Sem mais delongas, vamos começar a ver exemplos.

Proposição 1. *Para todo inteiro $n \geq 1$,*
$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

Neste exemplo,
$$P(n) : \text{“}\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.\text{”}$$

Demonstração. Por indução.

(i) Caso base: Se $n = 1$, temos que $\sum_{j=1}^{1} j = 1$, e que $\frac{1(1+1)}{2} = 1$, portanto $P(1) = T$.

(ii) Hipótese indutiva: para um $k \in \mathbb{Z}$ arbitrário, temos que

$$\sum_{j=1}^{k} j = \frac{k(k+1)}{2}.$$

(ou seja, substituimos k por n na expressão que queremos mostrar. Note que o quantificador não é "para todo", e sim "para um".

(iii) Conclusão indutiva: Teremos que

$$\begin{aligned}
\sum_{j=1}^{k+1} j &= 1 + 2 + 3 + ... + k + (k+1) && \text{por definição} \\
&= (1 + 2 + 3 + ... + k) + (k+1) && \text{propriedades da soma} \\
&= \sum_{j=1}^{k} j + (k+1) && \text{definição de somatório} \\
&= \frac{k(k+1)}{2} + (k+1) && \text{POR HIPÓTESE INDUTIVA} \\
&= \frac{k^2 + k + 2k + 2}{2} && \text{manipulação algébrica} \\
&= \frac{(k+1)(k+2)}{2} && \text{manipulação algébrica.}
\end{aligned}$$

Isso encerra a prova.

□

Proposição 2. *Para todo inteiro $n \geq 1$,*

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Demonstração. Por indução.

(i) Caso base: Se $n = 1$, ambos os lados são iguais a 1.

(ii) Hipótese indutiva:

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

(iii) Conclusão: Teremos que

$$\begin{aligned}
\sum_{j=1}^{k+1} j^2 &= 1^2 + 2^2 + 3^2 + ... + k^2 + (k+1)^2 \\
&= (1^2 + 2^2 + 3^2 + ... + k^2) + (k+1)^2 \\
&= \sum_{j=1}^{k} j^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{POR HIPÓTESE INDUTIVA} \\
&= \frac{2k^3 + 3k^2 + k + 6k^2 + 12k + 6}{6} \\
&= \frac{(k+1)(k+2)(2(k+1)+1)}{6}
\end{aligned}$$

Exercício 33. Mostre que para todo $n \geq 0$,

$$\sum_{j=0}^{n} 2^j = 2^{n+1} - 1.$$

Troque 2 por r, $r > 2$. Como a fórmula precisa ser ajustada? Demonstre a nova fórmula por indução.

Você consegue resolver este exercício de um jeito diferente?

Exercício 34. (Desafio) Tente usar uma generalização dos exemplos acima e a idéia da indução pra achar uma fórmula para

$$\sum_{j=1}^{n} j^3.$$

Proposição 3. *Se n é um inteiro positivo, então 5 divide $n^5 - n$.*

Demonstração. Por indução.

1. Caso base: com $n = 1$, $n^5 - n = 0$, e 5 divide 0.

2. Hipótese indutiva: para um $k \in \mathbb{Z}$,

$$5 \text{ divide } k^5 - k.$$

3. Conclusão: Note que

$$(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 4k.$$

Nosso objetivo é usar a hipótese indutiva, e para isso, precisamos fazer $k^5 - k$ aparecer. Manipulamos então para obter

$$(k+1)^5 - (k+1) = (k^5 - k) + 5k^4 + 10k^3 + 10k^2 + 4k + k.$$

Por hipótese indutiva, 5 divide $k^5 - k$. Os demais termos possuem coeficientes múltiplos de 5, portanto 5 divide todos os termos da soma, e logo 5 divide tudo.

Equivalentemente, e de forma mais precisa, por indução, existe ℓ tal que $5\ell = k^5 - k$. Logo

$$(k+1)^5 - (k+1) = 5(\ell + k^4 + 2k^3 + 2k^2 + k).$$

□

Exercício 35. Mostre que para todo $n \geq 0$, 4 divide $5^n - 1$.

Exercício 36. Vamos mostrar que 8 sempre divide 3^{2n}. Nossa hipótese indutiva é $8|3^{2n}$. Para a conclusão, faremos

$$3^{2(n+1)} = 3^{2n+2} = 9 \cdot 3^{2n} = 3^{2n} + 8 \cdot 3^{2n}.$$

Como 8 divide 3^{2n} por hipótese indutiva, e 8 divide $8 \cdot 3^{2n}$, segue que 8 divide $3^{2(n+1)}$. Fim da demonstração.

Tá certo isso aí?

Proposição 4. *Para todo $n \geq 4$, segue que $2^n < n!$.*

Demonstração.

1. Caso base: Se $n = 4$, então $2^n = 16$ e $n! = 24$. Logo $2^n < n!$ para $n = 4$.

2. Hipótese indutiva: para um $k \in \mathbb{Z}$, $2^k < k!$.

3. Conclusão:

$$\begin{aligned} 2^{k+1} &= 2^k \cdot 2 & \\ &< k! \cdot 2 & \text{por hipótese indutiva,} \\ &< k! \cdot (k+1) & \text{porque } 2 < k+1 \text{ para } k \geq 4. \\ &= (k+1)! & \end{aligned}$$

□.

Exercício 37. Prove que 13 sempre divide $3^{n+2} + 4^{2n+1}$, para qualquer $n \geq 0$.

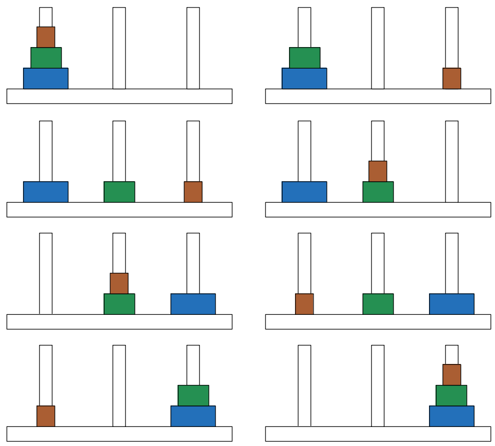
Exercício 38. Ache um inteiro N_0 tal que para todo $n \geq N_0$, $n^2 > 2n + 1$. Prove por indução.

Faça o mesmo para a propriedade $2^n > n^2$.

Exercício 39. Prove que um quadrado perfeito é sempre a soma de números ímpares consecutivos.

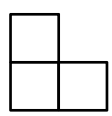
Aulas 7 e 8

Exercício 40. Torres de Hanoi é um jogo em que três peças de tamanhos diferentes são empilhadas em uma das três torres. A maior embaixo, a menor no topo. O objetivo é mover as três peças para a última torre. Para tal, só é permitido mover uma peça por vez, e uma peça nunca pode ficar sobre uma peça menor. Veja o exemplo abaixo de como resolver o jogo:



E se ao invés de 8 peças existirem n peças? É possível? Quantas jogadas serão necessárias para resolver? Faça um chute e depois prove por indução.

Exercício 41. Um triominó é um peça da forma



Prove que um tabuleiro quadricular de $2^n \times 2^n$, $n > 0$, sempre pode ser cobertos por triominós, desde que removamos um único quadrado.

Dica: um tabuleiro de tamanho $2^{n+1} \times 2^{n+1}$ é obtido juntando 4 tabuleiros de tamanho $2^n \times 2^n$.

Exercício 42. Prove que, para todo $n \geq 1$,

$$\sum_{j=1}^{n} \frac{j}{2^j} = 2 - \frac{n+2}{2^n}.$$

Exercício 43. Considere o produto

$$\prod_{j=2}^{n} \left(1 - \frac{1}{j^2}\right).$$

Teste alguns valores, conjecture uma fórmula, e prove esta fórmula por indução.

Exercício 44. Mostre que para todo $n > 1$,

$$1 + \frac{1}{4} + \frac{1}{9} + ... + \frac{1}{n^2} < 2 - \frac{1}{n}.$$

Exercício 45. Considere a seguinte proposição

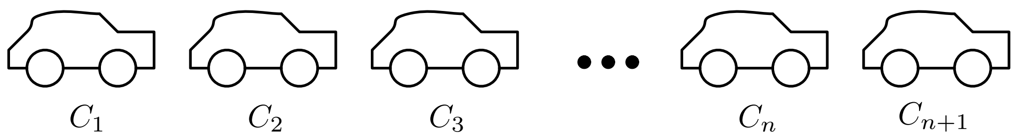
- Todos os carros de Belo Horizonte tem a mesma cor.

Vamos provar este fato por indução.

1. Caso base: Se só houvesse um carro em Belo Horizonte, certamente todos os carros teriam a mesma cor.

2. Hipótese indutiva: Todo conjunto de n carros em Belo Horizonte tem a mesma cor.

3. Conclusão: Considere um conjunto com $n + 1$ carros em Belo Horizonte. Digamos que eles sejam



   Os primeiros n carros, do C_1 ao C_n, tem a mesma cor por hipótese indutiva. Os últimos n carros, do C_2 ao C_{n+1}, também possuem a mesma cor, por hipótese indutiva. Como C_2, por exemplo, está em ambos os conjuntos, segue que C_{n+1} é da mesma cor que os n primeiros, e portanto todos eles tem a mesma cor.

Bem, será que todos os carros de Belo Horizonte tem a mesma cor? Ou será que o princípio da indução matemática está errado? Ou talvez "essas coisas de lógica" não se aplicam ao mundo real?!!

Descubra o que aconteceu.

Exercício 46. Esse é o meu favorito.

Há uma ilha onde mora uma tribo com 1000 pessoas. 100 delas tem olho azul, 900 tem olhos marrons. Entretanto a religião deles proíbe que cada habitante saiba a cor dos seus olhos, ou mesmo que o tema seja discutido. Os portugueses ainda não chegaram nessa ilha, então eles não possuem espelhos, ou qualquer outra superfície refletora. Assim, cada habitante sabe a cor dos olhos de todo mundo, menos a sua.

Se um habitante da tribo descobrir por algum acaso a cor do seus olhos, este habitante precisa cometer suicídio no dia seguinte, ao meio dia, na praça central, para que todos vejam.

Todos os habitante são lógicos, inteligentes, religiosos, e sabem que os outros habitantes também são, e sabem que os outros habitantes sabem que todos são, e assim sucessivamente. É um pessoal bem inteligente mesmo.

Um belo dia um náufrago de olhos azuis foi parar na ilha. A tribo o ajuda, mas ele, sem conhecer os costumes da tribo, comete a gafe de, ao discursar em agradecimento para toda a tribo, fazer o seguinte comentário:

- Que grata surpresa ver outra pessoa de olhos azuis, como eu, nesta ilha tão remota.

O que acontece com a tribo?
(após resolver, ou não, este desafio, vá ler na wikipedia sobre "Common Knowledge").

20 Mais casos bases

Muitas vezes, não basta usar o caso anterior para provarmos o próximo. Pode ser necessário usar alguns ou todos os casos anteriores para provarmos o próximo. Considere primeiramente o exemplo abaixo.

Proposição 5. *Suponha que a sequência $\{x_n\}$ é definida por $x_1 = 0$, $x_2 = 30$, $x_n = x_{n-1} + 6x_{n-2}$, para $n \geq 3$. Mostre que*

$$x_n = 2 \cdot 3^n + 3 \cdot (-2)^n.$$

Demonstração. Vamos primeiro ir como antes:

(i) Caso base: $x_1 = 0$ e $x_2 = 30$ ambos satisfazem a fórmula.

(ii) Hipótese indutiva: para um $k \in \mathbb{Z}$, $x_k = 2 \cdot 3^k + 3 \cdot (-2)^k$.

(iii) Conclusão: Pela recorrência, temos

$$x_{k+1} = x_k + 6x_{k-1}.$$

Usando a hipótese indutiva, o melhor que conseguimos é:

$$x_{k+1} = 2 \cdot 3^k + 3 \cdot (-2)^k + 6x_{k-1}.$$

O que fazemos com x_{k-1} ? A idéia aqui é trocar nossa hipótese indutiva, para que ela contemple todos os valores até o $k + 1$:

(ii) Hipótese indutiva: Para todo $j \leq k$, temos $x_j = 2 \cdot 3^j + 3 \cdot (-2)^j$. Agora voltamos. Temos

$$x_{k+1} = x_k + 6x_{k-1}.$$

Aplicando a hipótese indutiva para $j = k$ e $j = k - 1$, teremos

$$\begin{aligned}
x_{k+1} &= x_k + 6x_{k-1} && \text{definição} \\
&= 2 \cdot 3^k + 3(-2)^k + 6\big(2 \cdot 3^{k-1} + 3(-2)^{k-1}\big) && \left\{ \begin{array}{l} \text{hipótese indutiva} \\ \text{em ambos os termos!!} \end{array} \right. \\
&= 2 \cdot 3^k + 3(-2)^k + \big(4 \cdot 3^k - 9(-2)^k\big) && \left\{ \begin{array}{l} \text{manipulação} \\ \text{(atenção à mudança de sinal)} \end{array} \right. \\
&= 6 \cdot 3^k - 6(-2)^k && \text{manipulação} \\
&= 2 \cdot 3^{k+1} + 3(-2)^{k+1} && \text{manipulação}
\end{aligned}$$

Exercício 47. Definimos $x_1 = 11$, $x_2 = 23$, e $x_n = x_{n-1} + 12x_{n-2}$, para $n \geq 3$. Mostre que, para todo $n \geq 1$, temos

$$x_n = 2 \cdot 4^n - (-3)^n.$$

É preciso tomar muito cuidado com os casos base necessários!!

Proposição 6. *Todo inteiro maior que* 7 *pode ser escrito como a soma de dois múltiplos não negativos de* 3 *e* 5.

Demonstração. (i) Caso base: de fato, $8 = 5 + 3$.

(ii) Hipótese indutiva: Para todo $8 \leq k \leq n$, o número k pode ser escrito como $5x + 3y$, onde x e y são inteiros não-negativos.

(iii) Conclusão: Note que $n + 1 = (n - 7) + 8$. Por hipótese indutiva, há inteiros não negativos x e y tais que

$$n - 7 = 5x + 3y.$$

Então

$$n + 1 = 5x + 3y + 8 = 5x + 3y + 5 + 3 = 5(x + 1) + 3(y + 1).$$

Será que esta prova está OK?

Há um erro relevante na prova acima, ainda que a proposição seja verdeira. Vamos consertar o erro. Note que se $n = 9$, então $n - 7 = 2$. A hipótese indutiva só permite que digamos que números k entre 8 e n podem ser escrito como $5x + 3y$ onde x e y são não-negativos. Então o argumento na conclusão não pode mostrar o caso $n = 9$!!

De fato, ele só se aplica a número n maiores que 15, para que $n - 7 \geq 8$. Então é necessário checar manualmente que o resultado é verdadeiro para todos os número entre 8 e 15. A prova deve ser, portanto, assim:

(i) Casos base: $8 = 5 + 3$, $9 = 0 \cdot 5 + 3 \cdot 3$, $10 = 2 \cdot 5 + 0 \cdot 3$, $11 = 5 + 2 \cdot 3$, $12 = 0 \cdot 5 + 4 \cdot 3$, $13 = 2 \cdot 5 + 3$, $14 = 5 + 3 \cdot 3$, e $15 = 3 \cdot 5 + 0 \cdot 3$.

(ii) Hipótese indutiva: Para todo $8 \leq k \leq n$, o número k pode ser escrito como $5x + 3y$, onde x e y são inteiros não-negativos.

(iii) Conclusão. Seja $n \geq 16$. Note que $n + 1 = (n - 7) + 8$. Note que $n - 7 \geq 8$, então podemos aplicar a hipótese indutiva para $n - 7$. Então existem $x, y \in \mathbb{Z}_{\geq 0}$ tais que

$$n - 7 = 5x + 3y.$$

Então

$$n + 1 = 5x + 3y + 8 = 5x + 3y + 5 + 3 = 5(x + 1) + 3(y + 1).$$

□

Exercício 48. Mostre que todo inteiro ≥ 13 pode ser escrito como $3x + 4y$, com x, y inteiros positivos.

Exercício 49. Considere o jogo em que duas pessoas jogam, uma contra a outra. Há 37 moedas empilhadas. Em cada rodada, uma pessoa remove de 1 a 4 moedas da pilha. Ganha quem remove por último.

Existe uma estratégia sempre vitoriosa? Quem ganha? Quem começa ou quem vai depois?

E se forem n moedas? Qual a estratégia para a vitória? Use indução.

Exercício 50. Relembre a sequência de Fibonacci, dada por $\{f_n\}$ onde $f_1 = 1$, $f_2 = 1$ e $f_n = f_{n-1} + f_{n-2}$ para $n \geq 3$. Use indução para mostrar os resultados abaixo:

(a) Para todo $n \in \mathbb{N}$, $f_{n+1} < \left(\frac{7}{4}\right)^n$.

(b) Para $n \geq 2$, $f_1 + f_2 + ... + f_{n-1} = f_{n+1} - 1$.

(c) Seja $a = \frac{1+\sqrt{5}}{2}$ e $b = \frac{1-\sqrt{5}}{2}$. Para todo $n \in \mathbb{N}$, mostre que $f_n = \frac{a^n - b^n}{\sqrt{5}}$.

Dicas:

(a) Use que, para $n \geq 2$,

$$\left(\frac{7}{4}\right)^n = \frac{49}{16}\left(\frac{7}{4}\right)^{n-2} > \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^{n-2}.$$

(b) Note que

$$\sum_{i=1}^{n-2} f_i + \sum_{i=1}^{n-3} f_i = f_1 + \sum_{i=1}^{n-3} (f_i + f_{i+1}).$$

(c) Tanto a como b satisfazem $x^2 = x + 1$.

Exercício 51. (Desafio) Considere uma longa rodovia circular que possui alguns postos de gasolina no caminho. Todos juntos, os postos contém exatamente a quantidade de gasolina necessária para dar uma volta na rodovia. Seu tanque está vazio, mas cabe muito mais gasolina do que o necessário para dar a volta completa. Mostre que existe um posto onde você pode começar, encher seu tanque com o total do posto, e será possível dar uma volta completa na rodovia.

Aulas 9 e 10

21 Conjuntos

Um *conjunto* é uma coleção de objetos. Estes objetos são chamados de *elementos* do conjunto. A única restrição é que em geral um mesmo elemento não pode contar duas vezes com elemento de um conjunto. Tampouco é relevante a ordem na qual os elementos são apresentados.

Usamos a notação com chaves {...} para denotar um conjunto, separando os elementos por vírgulas. Observe os exemplos:

(i) $\{1, 5, 3, 4, 8\}$ é um conjunto contendo cinco elementos. Estes elementos são números. Os conjuntos $\{3, 5, 8, 4, 1\}$ e $\{1, 1, 5, 5, 5, 3, 8, 4\}$ representam o mesmo conjunto.

(ii) $\{\}$ é o conjunto vazio, que não possui qualquer elemento, também denotado por $\emptyset$.

(iii) $\{\square, 4\}$ é um conjunto que contém dois elementos: $\square$ e 4.

Exercício 52. Quantos conjuntos diferentes você pode construir usando os símbolos "{", "}", ",", "1" e "2" ?

O símbolos $\in$ e $\notin$ são usados para indicar se um elemento pertence ou não a um conjunto, respectivamente. Por exemplo, se $A = \{1, 2, 3\}$, então $1 \in A$, mas $4 \notin A$.

Conjuntos podem ser formados especificando um superconjunto onde estão seus elementos e uma propriedade adicional que separa os elementos deste superconjunto. Por exemplo:

(i) $\{n \in \mathbb{Z} : -11 < n < 11\}$ é o conjunto de todos os inteiros maiores que -11 e menores que 11. Quantos elementos há neste conjunto?

(ii) $\{n \in \mathbb{R} : \ n \text{ é um inteiro primo}\}$. Este é um exemplo de um conjunto com infinitos elementos.

(iii) Também é possível termos uma definição recursiva:

   (a) $1 \in A$.

   (b) Se $x \in A$ e $x + 2 < 10$, então $x + 2 \in A$.

   Descreva os elementos em A.

Conjuntos podem conter outros conjuntos como seus elementos. Por exemplo, se $A = \{1, 2, 3\}$, então $B = \{A, 1, 2, 3\}$ é o conjunto que contém quatro elementos: o conjunto A e os números de 1 a 3.

Exercício 53. Quantos elementos há no conjunto $\{\{\}, \{1, 2, 3\}, 1\}$?

Exercício 54. Seja $A = \{1, 3, \{4, 5\}\}$. É verdade que $4 \in A$?

Exercício 55. Responda o exercício 1 novamente.

Dado um conjunto A, usamos a notação $|A|$ pare representar a quantidade de elementos de A, também chamada de cardinalidade de A.

Exercício 56. Quanto é $|\emptyset|$?

Note que $\emptyset$ e $\{\emptyset\}$ são conjuntos distintos. O primeiro é o conjunto vazio, que não contém elementos. O segundo é o conjunto que contém um elemento - que é o conjunto vazio.

Exercício 57. Quanto é $|\{\{\}\}|$?

Exercício 58. Construa um conjunto com quatro elementos usando apenas os símbolos "{", "}" e ",".

Considere mais alguns exemplos:

(i) $\{n : n \in \mathbb{Z}, 2|n\}$ significa "o conjunto dos n tais que n é um inteiro e 2 divide n". É exatamente o mesmo conjunto que $\{n \in \mathbb{Z} : 2|n\}$, que lemos como "o conjunto dos inteiros n tais que 2 divide n".

(ii) Mesmo que um conjunto seja finito, as vezes a notação indireta é a única possível para expressar os elementos do conjunto:

$$\{x \in \mathbb{C} : x^6 - x^5 + 4x^4 - 2x^2 + 1 = 0\}$$

é um conjunto com 6 elementos, mas que simplesmente não é possível expressá-los de essencialmente outra forma.

Exercício 59. Expresse o conjunto dos números ímpares de 3 formas diferentes usando símbolos. Cada forma deve corresponder a uma frase abaixo.

1. O conjunto das coisas da forma $2k + 1$ onde k é um inteiro.
2. O conjunto dos números naturais n tais que existe um k inteiro tal que $n = 2k + 1$.
3. O conjunto dos números inteiros n tais que $n - 1$ é par.

Para cada um dos conjuntos a seguir, se o conjunto for infinito, descreva com palavras os seus elementos. Se for finitos, liste os elementos:

Exercício 60.

(i) $\{x \in \mathbb{Z} : 1 \leq x^2 \leq 10\}$.

(ii) $\{x^2 : x \in \mathbb{Z}, 1 \leq x^2 \leq 10\}$.

(iii) $\{x \in \mathbb{R} : x^3 - x = 0\}$.

(iv) $\{\frac{p}{q} : p, q \in \mathbb{Z}, q > 0, p < 0\}$.

(v) $\{x \in \mathbb{R} : \frac{1}{5} < 2^x < 10\}$.

(vi) $\{x \in \mathbb{Z} : \frac{1}{5} < 2^x < 10\}$.

22 Subconjuntos e conjunto das partes

Dois conjuntos são *iguais* se eles contém os mesmo elementos. Formalmente, dizemos que $A = B$ se
$$x \in A \iff x \in B.$$
Conforme já vimos acima, há muitas formas de representarmos o mesmo conjunto. As vezes não é óbvio que dois conjuntos são iguais:
$$\{-1, 1, 3, 5\} = \{x \in \mathbb{R} : x^4 - 8x^3 + 14x^2 + 8x - 15 = 0\}.$$

Um *subconjunto* de um conjunto é o conjunto formado por parte de seus elementos. Note que pode conter nenhum elemento ou todos eles, nada impede. Formalmente, dizemos que $A \subseteq B$ se
$$x \in A \Rightarrow x \in B.$$

Exercício 61. Encontre todos os subconjuntos de $\{1, 2\}$.

Como exemplo, note que
$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

Atenção: as vezes se usa a notação $A \subset B$ para indicar que A é um subconjunto de B, e a notação $A \subsetneq B$ para indicar que A é subconjunto de B e diferente de B. Nós entretanto usaremos a convenção a seguir:

1. $A \subset B$ - um subconjunto necessariamente diferente de B.

2. $A \subseteq B$ - qualquer subconjunto de B.

Como já vimos no exercício acima, é possível trabalharmos com o conjunto de todos os subconjuntos de um dado conjunto A. Este é também chamado de *conjunto potência* ou *conjunto das partes*, e é denotado por $\mathcal{P}(A)$.

Exercício 62. Se $A = \{1, 2, 3\}$, denote $\mathcal{P}(A)$.

Exercício 63. Se $|A| = n$, então quanto é $|\mathcal{P}(A)|$?

Exercício 64. Quem é $\mathcal{P}(\emptyset)$?

23 Operações em conjuntos

Uma *n-tupla* ordenada $(a_1, a_2, ..., a_n)$ é uma coleção ordenada de n elementos, em que a_1 é o primeiro, a_2 o segundo, e ... a_n o último ou n-ésimo elemento.

(i) $(1, 4)$ é um par ordenado. Ele é diferente de $(4, 1)$.

(ii) Duas n-tuplas são iguais se os elementos em cada posição são iguais.

O *produto cartesiano* de dois conjuntos, denotado por $A \times B$, é o conjunto de todos os pares ordenados onde o primeiro elemento está em A, e o segundo em B. Formalmente:

$$A \times B = \{(a, b) : a \in A \text{ e } b \in B.\}$$

Exercício 65. Expresse todos os elementos de

$$\{1, 2, 3\} \times \{x, y\}.$$

Exercício 66. Se $|A| = n$ e $|B| = m$, então quanto é $|A \times B|$?

Exercício 67. Dados conjuntos A e B, é verdade que $A \times B = B \times A$? Se não é, quando isso ocorre?

Produtos cartesianos podem ser generalizados para mais de um conjunto:

$$\{1, 2\} \times \{a, b\} \times \{3, 4\} = \{(1, a, 3), (1, a, 4), (1, b, 3), (1, b, 4), (2, a, 3), ...\}$$

Exercício 68. Considere $A = \{n \in \mathbb{Z} : \ n \text{ ímpar}\}$ e $B = \{n \in \mathbb{Z} : 4 \text{ não divide } n^3 + n\}$. Mostre que $A \subset B$. É verdade que $B \subset A$?

A idéia aqui é mostrar que $x \in A \Rightarrow x \in B$. Se $x \in A$, então existe k tal que $x = 2k + 1$. Agora queremos mostrar que 4 não divide $x^3 + x$. Então calculamos:

$$x^3 + x = (2k + 1)^3 + (2k + 1) = 4(2k^3 + 3k^2 + 2k) + 2.$$

E agora?

Dois ou mais conjuntos podem ser combinados de modo a formar novos conjuntos. Já vimos como fazer isso usando o produto cartesiano acima. Vamos ver outras operações:

(i) Interseção: $A \cap B$ é o conjunto de todos os elementos que pertencem tanto a A como a B, ou seja:
$$A \cap B = \{x : x \in A \text{ e } x \in B\}$$

(ii) União: $A \cup B$ é o conjunto de todos os elementos que pertencem a A ou a B, ou seja:
$$A \cup B = \{x : x \in A \text{ ou } x \in B\}$$

(iii) Diferença: $A \backslash B$ é o conjunto de todos os elementos que pertencem a A mas não pertencem a B, ou seja:
$$A \backslash B = \{x : x \in A \text{ e } x \notin B\}$$
Também se denota por $A - B$.

(iv) Diferença simétrica: $A \oplus B$ é o conjunto de todos os elementos que pertencem a A mas não pertencem a B ou que pertencem a B e não pertencem a A, ou seja:
$$A \oplus B = (A \backslash B) \cup (B \backslash A)$$

(v) Se U é um conjunto contendo A, dizemos que o complemento de A em U são os elementos de U que não estão em A, ou seja

$$\overline{A} = U \backslash A.$$

(vi) Se há uma família de conjuntos $A_1, A_2, ..., A_n$, então usamos a notação

$$B = \bigcup_{i=1}^{n} A_i$$

para indicar o conjunto que é a união de todos eles, ou seja, $x \in B$ se, e somente se, existe pelo menos um $i \in \{1, ..., n\}$ tal que $x \in A_i$.

(vii) Analogamente

$$B = \bigcap_{i=1}^{n} A_i$$

indica o conjunto que é a interseção de todos eles, ou seja, $x \in B$ se, e somente se, para todo $i \in \{1, ..., n\}$, temos $x \in A_i$.

.

Note que $A \cap B = B \cap A$, $A \cup B = B \cup A$, e $A \oplus B = B \oplus A$, mas não necessariamente $A \backslash B = B \backslash A$. Aliás, quando é que isso ocorre?

Exercício 69. Seja U um conjunto contendo A e B. Mostre que:

$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Exercício 70. Construímos uma tabela de pertinência para um elemento $x \in U$, com respeito a A, B, seus complementos, interseções e uniões. Usamos 1 para indicar que pertence, 0 que não pertence. Por exemplo:

A	B	$A \cap B$	$A \cup B$	$\overline{A}$	$\overline{B}$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
1	1	1	1	0	0	0	0
1	0	0	1	0	1	1	1
0	1	0	1	1	0	1	1
0	0	0	0	1	1	1	1

Com o que isso se parece? Usando uma tabela semelhante, prove que $\overline{A \cup B}$ é igual a $\overline{A} \cap \overline{B}$.

Exercício 71. Faça a tabela de pertinência para $A \oplus B$ e verifique que

$$A \oplus B = (A \cup B) \backslash (A \cap B).$$

Exercício 72. É verdade que

$$A \oplus (B \oplus C) = (A \oplus B) \oplus C \quad ?$$

Dois conjuntos A e B são *disjuntos* se eles não possuem qualquer elemento em comum, ou seja, se $A \cap B = \emptyset$. Por exemplo, se $A = \{1, 2, 3\}$ e $B = \{4, 5\}$, então A e B são disjuntos. Se $C = \{\{1, 2, 3\}\}$, note que A e C também são disjuntos.

Uma partição de um conjunto A é uma coleção de conjuntos não-vazios $\{A_1, A_2, ..., A_n\}$ tais que

(i) $A = A_1 \cup A_2 \cup ... \cup A_n$, e

(ii) A_i é disjunto de A_j para todos i e j entre 1 e n.

Por exemplo,

$$\{\{1, 2\}, \{5, 7\}, \{4, 3\}\}$$

é uma partição do conjunto

$$\{1, 5, 3, 4, 2, 7\}.$$

Exercício 73. Encontre todas as partições possíveis do conjunto

$$\{1, 2, 3, 4\}.$$

Faça o mesmo para $\{1, 2, 3, 4, 5\}$.

Pesquise sobre “Bell Numbers” e “stirling numbers of the second type”.

24 Correspondência entre subconjuntos e sequências de 0s e 1s

Assuma que há um conjunto universal U com n elementos. Qualquer subconjunto A de U pode ser representado como uma string de n 0s e 1s. Especificamente, definimos uma ordem para U, colocaremos um 1 se o elemento correspondente àquela posição pertencer a A, e 0 caso contrário.

Por exemplo, se $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$, podemos dizer que o subconjunto $A = \{3, 4, 7\}$ corresponde à string 00110010. Seja $B = \{1, 2, 3, 6, 7\}$. Escreva...

1. ...a string correspondente a B.
2. ...a string correspondente a $A \cup B$.
3. ...a string correspondente a $A \cap B$.
4. ...a string correspondente a $A \backslash B$.
5. ...a string correspondente a $A \oplus B$.
6. ...a string correspondente a $\overline{A}$.
7. ...as strings correspondentes aos subconjuntos de A.