TEORIA DE GRAFOS E COMPUTABILIDADE

PROVA DE TEOREMAS

Técnicas de prova: Introdução

- Uma **prova** é uma demonstração matemática da certeza a respeito de uma afirmação.

- O nível de detalhamento de uma prova pode depender do tipo de leitor ao qual ela se destina, levando em conta fatores como:
  - o conhecimento do leitor sobre o
  - assunto; a maturidade do leitor;
  - o nível de rigor almejado.

- Nesta seção vamos nos focar em provas utilizando o rigor matemático esperado de um profissional em nível de graduação na área de ciências exatas.

- Provas são importantes em várias áreas da Ciência da Computação:
  1. correção de programas;
  2. análise de complexidade de algoritmos;
  3. propriedades de segurança de sistemas;
  4. ...

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.

Evidência versus prova

- Exemplo: Seja a fórmula $p(n) = n^2 + n + 41$.

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

Evidência de que a conjectura está 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 <u>falsa</u>.

- Evidência não é o mesmo que prova!

Evidência versus prova, uma piadinha ;-)

- **Conjectura:** Todos os números ímpares maiores que 1 são primos.

  Como cada profissional "prova" esta conjectura acima?

  - **Matemático**: *"3 é primo, 5 é primo, 7 é primo, mas* $9 = 3^2$ *não é primo, logo a conjectura é falsa."*

  - **Físico**: *"3 é primo, 5 é primo, 7 é primo, 9 não é primo, 11 é primo, 13 é primo. Assim o número* 9 *deve ser um erro experimental, e a conjectura é verdadeira."*

  - **Advogado**: *"Senhoras e senhores do júri: não há duvida de que números ímpares são todos primos. A evidência é clara: 3 é primo, 5 é primo, 7 é primo, 9 é primo, e assim por diante!"*

  - **Professor**: *"3 é primo, 5 é primo, 7 é primo, ... O restante fica para os alunos resolverem na lista de exercícios."*

Técnicas de Provas

- Construir uma prova é uma arte.

  Cada caso é um caso: não existe uma “receita fechada” para construir provas para todas as afirmações.

- Existem, entretanto, técnicas que são úteis para provar uma grande quantidade de afirmações.

  Veremos as seguintes técnicas de prova:

  1. prova direta;
  2. prova por contraposição;
  3. prova por contradição (ou prova por redução ao absurdo).
  4. prova por contra-exemplo;
  5. prova por exaustão e divisão em casos;
  6. prova por indução matemática) serão vistas mais adiante no curso.

Como escrever uma prova

- Escreva claramente qual a afirmação que se deseja provar. (É comum preceder a afirmação com a palavra **Teorema** ou **Lema**.)

- Delimite claramente o escopo da prova.

  Indique o início da prova com a palavra

  Prova.

  Indique o fim da prova com um marcador. Pode-se usar:

  - um quadradinho □ , ou
  - a abreviação **Q.E.D.** (do latim *“quod erat demonstrandum”*), ou
  - sua tradução em português, **C.Q.D.** (*“conforme queríamos demonstrar”*).

- Escreva a prova de tal forma que ela seja autocontida. Use linguagem natural (português) de forma clara, empregando sentenças completas e bem estruturadas. Podem-se utilizar fórmulas matemáticas, equações, etc., quando necessário.

Como escrever uma prova

- Identifique cada variável usada na prova juntamente com seu tipo. Exs.:
    1. Seja x um número real maior que 2.
    2. Suponha que m e n sejam inteiros sem divisores comuns.
- Importante:

  O objetivo principal de uma prova é convencer o leitor de que o resultado (teorema, proposição, lema) é verdadeiro.

  Não basta que você mesmo esteja convencido!

  Certifique-se de que está sendo conciso, mas

  claro.

Prova direta

- Forma geral:

  1. Expresse a afirmação a ser provada na forma:

     $$\forall x \in D : (P(x) \rightarrow Q(x))$$

     Esta etapa às vezes é feita mentalmente.

  2. Comece a prova supondo que x é um elemento específico do domínio D, mas escolhido arbitrariamente, para o qual a hipotese $P(x)$ é verdadeira.

     Normalmente abreviamos esta etapa dizendo *"Assuma que $x \in D$ e $P(x)$ é verdadeiro"* ou *"Seja $x \in D$ tal que $P(x)$"*.

  3. Mostre que a conclusão $Q(x)$ é verdadeira utilizando definições, resultados anteriores e as regras de inferência logica.

- Importante: Como $x \in D$ é escolhido arbitrariamente, ele não depende de nenhuma suposição especial sobre x, e portanto pode ser generalizado para todos os elementos de D.

Prova direta

- Exemplo: Mostre que se n é um inteiro ímpar, então n^2 é ímpar.

(**Obs.** Um inteiro n é par sse existe um inteiro k tal que $n = 2k$. Um inteiro n é ímpar sse existe um inteiro k tal que $n = 2k + 1$.)

Prova. Queremos mostrar que $\forall n : (P(n) \rightarrow Q(n))$, onde $P(n)$ é o predicado *"n é um inteiro ímpar"*, e $Q(n)$ é o predicado *"n^2 é ímpar"*.

Para produzir uma prova direta desta afirmação, assumimos que a hipótese da implicação, $P(n)$, é verdadeira, ou seja, que n é um inteiro ímpar. Então, pela definição de número ímpar, existe um inteiro k tal que $n = 2k + 1$.

Queremos mostrar que a conclusão da implicação, $Q(n)$, é verdadeira, ou seja, que n^2 também é ímpar. Para isto podemos calcular

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Logo, pela definição de número ímpar, n^2 também é ímpar. $\square$

Prova direta

- Exemplo: Mostre que se m e n são quadrados perfeitos, então mn é um quadrado perfeito.

  (**Obs:** Um inteiro a é um quadrado perfeito se existe um inteiro b tal que $a = b^2$.)

  Prova. Para provar esta proposição, vamos assumir que m e n sejam quadrados perfeitos. Pela definição de quadrado perfeito, devem existir inteiros s e t tais que $m = s^2$ e $n = t^2$.

  O objetivo da prova é mostrar que mn será um quadrado perfeito quando m e n o forem. Para ver isto, podemos calcular

$$mn \quad = \quad s^2t^2 \quad = \quad (st)^2.$$

  Mas é claro que st também é um inteiro, logo mn satisfaz a definição de quadrado perfeito (já que $mn = (st)^2$), e a conclusão da implicação também é verdadeira.

  Logo concluímos a prova de que a afirmação é verdadeira. $\square$

Prova por contraposição

- Forma geral:

  1. Expresse a afirmação a ser provada na forma:

  $$\forall x \in D : (P(x) \to Q(x))$$

  Esta etapa às vezes é feita mentalmente.

  2. Encontre a afirmação contrapositiva da afirmação a ser provada:

  $$\forall x \in D : (\neg Q(x) \to \neg P(x))$$

  3. Comece a prova supondo que x é um elemento específico do domínio D, mas escolhido arbitrariamente, para o qual a conclusão $Q(x)$ é falsa.

  4. Mostre que a hipótese $P(x)$ é falsa utilizando definições, resultados anteriores e as regras de inferência logica.

- Importante: Como $x \in D$ é escolhido arbitrariamente, ele não depende de nenhuma suposição especial sobre x, e, portanto, ele ser generalizado para todos os elementos de D.

Prova por contraposição

- Exemplo: Mostre que se n é um inteiro e $3n + 2$ é ímpar, então n é ímpar.

Prova. Queremos mostrar que $\forall n \in \mathrm{N} : (P(n) \rightarrow Q(n))$, onde $P(n)$ é *"$3n + 2$ é ímpar"*, e $Q(x)$ é *"n é ímpar"*. Para produzir uma prova por contraposição, vamos demonstrar que $\forall n \in \mathrm{N} : (\neg Q(n) \rightarrow \neg P(n))$. Ou seja, vamos mostrar que se um número inteiro n não é ímpar, então $3n + 2$ também não é ímpar.

Se n não é ímpar, é porque n é par e, pela definição de número par, $n = 2k$ para algum $k \in \mathrm{N}$. Portanto podemos derivar

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1), \end{aligned}$$

de onde concluímos que $3n + 2$ satisfaz a definição de número par.

Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, a prova por contraposição é concluída com sucesso. □

Prova por contraposição

- Exemplo: Mostre que se $n = ab$ onde a e b são inteiros positivos, então $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.

  Prova. Para produzir uma prova por contraposição, vamos demonstrar que sempre que a conclusão da implicação é falsa, sua hipótese também é falsa.

  A conclusão da implicação pode ser escrita como $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$. Logo, por de Morgan, a negação da conclusão é

$$\neg((a \leq \sqrt{n}) \vee (a \leq \sqrt{n})) \equiv \neg(a \leq \sqrt{n}) \wedge \neg(b \leq \sqrt{n})$$

$$\equiv (a > \sqrt{n}) \wedge (b > \sqrt{n}).$$

  Já a hipótese da implicação pode ser escrita como $n = ab$, e sua negação é $n \mathrel{!}= ab$.

Prova por contraposição

- Exemplo: (Continuação)

Queremos mostrar que se ($a > \sqrt{n}$) $\wedge$ ($b > \sqrt{n}$) então n != ab.

Para isto, note que se ($a > \sqrt{n}$) $\wedge$ ($b > \sqrt{n}$) podemos derivar o seguinte

$$ab > \sqrt{n}\sqrt{n} = n,$$

de onde se conclui que $ab > n$ e, portanto, ab != n.

Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, a prova por contraposição é concluída com sucesso. □

Prova por contradição

- A prova por contradição se baseia no fato de que se partindo de uma premissa *p*, e aplicando regras de infererência corretamente, chegamos a uma conclusão falsa, então a premissa *p* deve ser necessariamente falsa.
- Equivalentemente, se ao tomarmos como premissa a negação $\neg p$ de uma afirmação chegamos a um absurdo (contradição), então a afirmação *p* deve ser necessariamente verdadeira.
- Forma geral:

  1. Para provar que a afirmação *p* é verdadeira, assuma que sua negação $\neg p$ é verdadeira.

  2. Mostre que $\neg p$ leva a uma contradição, ou seja, que $\neg p \rightarrow F$.

Prova por contradição

- Exemplo: Mostre que em um grupo de 22 dias, ao menos 4 dias caem no mesmo dia da semana.

  Prova. Seja p a proposição *"Em um grupo de* 22 *dias, ao menos* 4 *dias caem no mesmo dia da semana"*.

  Suponha que $\neg p$ é verdadeiro, ou seja, que *"Em um grupo de* 22 *dias, no máximo* 3 *dias caem no mesmo dia da semana"*. Neste caso, no máximo 21 dias podem ser escolhidos para fazer parte de um grupo (já que há apenas 7 dias na semana). Mas isso contradiz a premissa de que o grupo tem 22 dias.

  Em outras palavra, se r é a proposição *"22 dias são escolhidos"*, teríamos $\neg p \rightarrow (r \wedge \neg r)$, ou seja, $\neg p \rightarrow F$.

  Logo, $\neg p$ não pode ser verdadeiro, ou seja, p é verdadeiro. $\square$

Prova por contradição

- Exemplo: Mostre que se $3n + 2$ é ímpar, então n é ímpar.

Prova. Queremos mostrar a proposição *"se $3n + 2$ é ímpar, então n é ímpar"*. Podemos escrever esta proposição como $p \rightarrow q$.

Para provar por contradição, vamos assumir que $p \rightarrow q$ é falso. Isso quer dizer que estamos assumindo $p \land \neg q$, ou seja, que *"$3n + 2$ é ímpar e n não é ímpar"*.

Mas se n não é ímpar, é porque n é par e existe um inteiro k tal que $n = 2k$. Podemos, então, derivar

$$3n + 2 \quad = \quad 3(2k) + 2 \quad = \quad 6k + 2 \quad = \quad 2(3k + 1),$$

o que implica que $3n + 2$ é par. Mas isto significa que concluímos exatamente que p é falso, o que contradiz a hipótese de que p é verdadeiro.

Logo, não é possível ter $p \land \neg q$ sem cair em contradição, e, portanto, se $3n + 2$ é ímpar então n é ímpar. $\square$

Prova por contradição

- Exemplo: Vamos mostrar que $\sqrt{2}$ é irracional.

Prova. Suponha o contrário do que queremos provar, ou seja, que 2 é racional.

Neste caso, existem $p, q \in Z$, com $mdc(p, q) = 1$, tais que $\sqrt{2} = p/q$. Elevando os dois lados ao quadrado, obtemos $2 = p^2/q^2$, ou seja, $p^2 = 2q^2$. Note que $2q^2$ é par, portanto pela igualdade acima p^2 também tem que ser par. Isto implica que p deve ser par.

Agora, já que p é par, existe algum $s \in Z$ tal que $p = 2s$. Isso implica que $2q^2 = p^2 = (2s)^2 = 4s^2$, o que resulta em $q^2 = 2s^2$. Note que então q^2 é par, portanto q deve ser par.

Mas se ambos p e q são pares, isto contradiz a suposição de que o $mdc(p, q) = 1$: encontramos uma contradição. Logo podemos concluir que não existem $p, q \in \underline{Z}$, com $q \mathrel{!}= 0$ e $mdc(p, q) = 1$, tais que $\sqrt{2} = p/q$. Portanto $\sqrt{2}$ é irracional $\square$

Prova por contra-exemplo

- Provas por contra-exemplos funcionam para provar que afirmações são falsas.
- Forma geral:
  1. Expresse a afirmação a ser provada na forma:

     $$\forall x \in D : P(x)$$

     Esta etapa às vezes é feita mentalmente.
  2. Encontre um $x \in D$ tal que $P(x)$ seja falso.

Prova por contra-exemplo

- Exemplo: Seja $p(n) = n^2 + n + 41$. Prove que a afirmação "*$\forall n \in$* N *: $p(n)$ é primo*" é falsa.

  Prova. Tome o contra-exemplo $n = 40$. Neste caso temos $p(n) = 1681 = 41 \cdot 41$, que não é primo.

  Logo a afirmação é falsa. □

- Exemplo: Mostre que a afirmação *"Todo inteiro positivo pode ser escrito como a soma do quadrado de dois inteiros"* é falsa.

  Prova. Tome o contra-exemplo 3, que é um inteiro que não pode ser escrito como a soma dos quadrados de dois inteiros.

  Para ver isto, basta ver que os únicos quadrados menores que 3 são 0 e 1, e as somas possíveis destes quadrados são $0 + 0 = 0$, $0 + 1 = 1$, e $1 + 1 = 2$, nenhuma das quais se iguala a 3.

  Logo 3 é um contra-exemplo e a afirmação é falsa. □

Prova por divisão em casos

- Utilizada geralmente para provar que $p \rightarrow q$.
- A prova divide p em casos, e mostra que q segue de qualquer caso possível.
- Forma geral:
  1. Para mostrar que $p \rightarrow q$, primeiro mostre que

     $$p \equiv p_1 \lor p_2 \lor \ldots \lor p_n$$

  2. Mostre, separadamente, cada uma das implicaçoes

     $$\begin{aligned} p_1 &\rightarrow q \\ p_2 &\rightarrow q \\ \ldots &\rightarrow \ldots \\ p_n &\rightarrow q \end{aligned}$$

Prova por divisão em casos

- Exemplo: Mostre que, dados dois números reais x , y , $min(x, y) + max(x, y) = x + y$.

Prova. Há somente três possibilidades para x e y :

$$x < y \quad \text{ou} \quad x = y \quad \text{ou} \quad x > y$$

.
Vamos analisar cada caso separadamente:

- Se $x < y$, então $min(x, y) + max(x, y) = x + y$.
- Se $x = y$, então $min(x, y) + max(x, y) = x + y$.
- Se $x > y$, então $min(x, y) + max(x, y) = y + x = x + y$.

Logo, podemos concluir que sempre teremos $min(x, y) + max(x, y) = x + y$. □

Prova de equivalências

- É muito comum termos que mostrar que um conjunto de afirmações são todas equivalentes.

- Forma geral:

  1. Para mostrar que $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$, mostre, separadamente, cada uma das implicações

$$p_1 \rightarrow p_2$$
$$p_2 \rightarrow p_3$$
$$\ldots \rightarrow \ldots$$
$$p_n \rightarrow p_1$$

- Importante: A prova não está completa se não se fechar o ciclo de implicações, provando que a última proposição implica de volta na primeira: $p_n \rightarrow p_1$.

- <u>Caso especial:</u> Para provar que $p_1 \leftrightarrow p_2$ podemos mostrar, separadamente, que $p_1 \rightarrow p_2$ e que $p_2 \rightarrow p_1$.

Prova de existência

- Uma prova de um teorema do tipo $\exists x : P(x)$ é chamada de **prova de existência**.
- Há duas maneiras de se produzir uma prova existencial:

1. Uma prova **construtiva** produz um elemento a tal que $P(a)$ seja verdadeiro.

   O elemento a é chamado de **testemunha** da prova.

2. Uma prova **não-construtiva** não produz uma testemunha, mas prova $\exists x : P(x)$ de alguma outra forma.

   Uma maneira é produzir, por exemplo, uma prova por contradição.

Prova de existência: construtiva

- Exemplo: Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas maneiras distintas.

  Prova. Após uma busca trabalhosa (por exemplo, usando um programa de computador), encontramos que

$$1\,729 = 10^3 + 9^3 = 12^3 + 1^3.$$

□

- A prova acima é construtiva porque ela produz uma testemunha (o número 1 729 junto com suas decomposições) que atesta a existência desejada.

Prova de existência: não-construtiva

- Exemplo: Existem números irracionais x e y tais que x^y é racional.

  Prova. Sabemos que $\sqrt{2}$ é irracional (já provamos isto). Considere o número $\sqrt{2}^{\sqrt{2}}$. Há duas possibilidades para este número:

  1. Ele é racional. Neste caso temos dois números irracionais $x = \sqrt{2}$ e $y = \sqrt{2}$ tais que x^y é racional.
  2. Ele é irracional. Neste caso podemos calcular que

     $$(\sqrt{2}\,\hat{}\,\sqrt{2})\,\hat{}\,\sqrt{2} = (\sqrt{2})\,\hat{}\,2 = 2$$

     É um número racional. Assim temos dois números irracionais $x = \sqrt{2}\ \hat{}\ \sqrt{2}$ e $y = \sqrt{2}$ tais que x^y é racional. □

- A prova acima é não-construtiva porque ela não produz uma testemunha que atesta a existência desejada. Sabemos que ou $x = \sqrt{2}$ e $y = \sqrt{2}$ ou $x = \sqrt{2}\,\hat{}\,\sqrt{2}$ e $y = \sqrt{2}$ satisfazem a propriedade, mas não sabemos qual destes dois pares é o certo!

Princípio da indução matemática: Introdução

- Muitas proposições matemáticas envolvem quantificações sobre todos os números naturais.
- Por exemplo, as seguintes afirmações são válidas para todos os inteiros positivos n:
  1. $n! \leq n^n$;
  2. $(n^3 - n)$ é divisível por 3;
  3. qualquer conjunto de n elementos tem 2^n subconjuntos distintos.
- Mas se N é um <u>conjunto infinito</u>, como provar que as afirmações acima valem para <u>todos os elementos</u> do conjunto?
- A técnica de **indução matemática** pode ser utilizada para provar afirmativas deste tipo.

Princípio da indução matemática (fraca)

- Para mostrar que uma propriedade $P(n)$ vale para todos os inteiros positivos n, uma **prova** que utilize o **princípio da indução matemática (fraca)** possui duas partes:

  ~~Prova por indução fraca~~:

  - Passo base: Prova-se $P(1)$.
  - Passo indutivo: Prova-se que, para qualquer inteiro k, se $P(k)$ é positivo verdadeiro, então $P(k+1)$ é verdadeiro.

- A premissa do passo indutivo ($P(k)$ é verdadeiro) é chamada de **hipótese de indução** ou **I.H.**

- O princípio da indução matemática pode ser expresso como uma regra de inferência sobre os números inteiros:

$$[\ P(1) \ \wedge \ \forall k : (P(k) \rightarrow P(k+1))] \rightarrow \forall n : P(n)$$

Prova por indução matemática (fraca)

- Exemplo: Se n é um inteiro positivo, então $1 + 2 + \cdots + n = n(n + 1)/2$.

Prova. Seja $P(n)$ a proposição *"a soma dos n primeiros inteiros positivos é* $n(n + 1)/2$*"*.

Passo base: $P(1)$ é verdadeiro porque

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

Passo indutivo: Assuma que $P(k)$ seja verdadeiro para um inteiro positivo arbitrário k. Ou seja, a nossa hipótese de indução é de que, para um inteiro positivo k arbitrário:

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

Prova por indução matemática (fraca)

- Exemplo: (Continuação)

Sob a hipótese de indução, deve-se mostrar que $P(k+1)$ é válido, ou seja:

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

Podemos, então, derivar

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \qquad \text{(pela I.H.)} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

de onde concluímos o passo indutivo.

Como concluímos com sucesso tanto o passo base quanto o passo indutivo, mostramos por indução que $\forall n \in \mathbb{Z}^+ : P(n)$, ou seja, que $1 + 2 + \cdots + n = n(n+1)/2$ para todo inteiro positivo n. $\square$

Prova por indução matemática (fraca)

- Exemplo: A soma dos n primeiros inteiros positivos ímpares é n^2.

Prova. Seja $P(n)$ a proposição *"A soma dos n primeiros inteiros positivos ímpares é n^2"*.

Passo base: $P(1)$ é verdadeiro porque o primeiro inteiro positivo ímpar é 1, o que é igual a 1^2.

Passo indutivo: Assuma que $P(k)$ seja verdadeiro para um inteiro positivo arbitrário k.

Note que o k-ésimo inteiro positivo ímpar é dado por $2k - 1$.

Logo, a hipótese de indução é:

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

Prova por indução matemática (fraca)

- Exemplo: (Continuação)

Queremos mostrar que $\forall k \in Z^+ : (P(k) \rightarrow P(k+1))$, onde $P(k+1)$

é: $1 + 3 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2$.

Logo, podemos derivar

$$
\begin{aligned}
1 + 3 + \cdots + (2k - 1) + (2(k + 1) - 1) &= k^2 + (2(k + 1) - 1) && \text{(pela I.H.)} \\
&= k^2 + 2k + 1 \\
&= (k + 1)^2,
\end{aligned}
$$

de onde concluímos o passo indutivo.

Como concluímos com sucesso o passo base e o passo indutivo, mostramos por indução que $\forall n \in Z^+ : P(n)$, ou seja, que a soma dos n primeiros ímpares positivos é n^2. $\square$

Modelo de prova por indução matemática

1. Expresse a afirmação a ser provada na forma *"para todo inteiro $n \geq b$, $P(n)$"*, onde b é um inteiro fixo.

2. Escreva "Passo base." e mostre que $P(b)$ é verdadeiro, certificando-se de que o valor correto de b foi utilizado. Isto conclui o passo base.

3. Escreva as palavras "Passo indutivo"

4. Escreva claramente a hipótese indutiva, na forma "Assuma que $P(k)$ seja verdadeiro para um inteiro arbitrário fixo $k \geq b$."

5. Escreva o que precisa ser provado sob a suposição de que a hipótese de indução é verdadeira. Ou seja, escreva o que $P(k + 1)$ significa.

6. Prove a afirmação $P(k + 1)$ utilizando o fato de que $P(k)$ é verdadeiro. Certifique-se de que sua prova é válida para qualquer $k \geq b$.

7. Identifique claramente as conclusões do passo indutivo, e conclua-o escrevendo, por exemplo, "isto completa o passo de indução".

8. Completados o passo base e o passo indutivo, escreva a conclusão da prova: que, por indução matemática, $P(n)$ é verdadeiro para todos os inteiros $n \geq b$.

Princípio da indução matemática (forte): Introdução

- O princípio de indução que vimos até agora é conhecido como o **princípio da indução matemática fraca**: Ele recebe este nome de indução “fraca” porque a hipótese de indução (I.H.) é apenas que $P(k)$ seja verdadeiro para algum k.

  Às vezes é complicado usar a indução fraca para provar um teorema, e podemos recorrer ao **princípio da indução matemática forte**.

  Neste princípio, a hipotese de indução é de que $P(j)$ é válido para todo $1 \leq j \leq k$.

Princípio da indução matemática (forte)

- Para mostrar que uma propriedade $P(n)$ vale para todos os inteiros positivos n, uma **prova** que utilize **princípio da indução matemática (forte)** possui duas partes:

  Prova por indução forte:

  Passo base: Prova-se $P(1)$;

  Passo indutivo: Prova-se que, para qualquer inteiro positivo k, se $P(j)$ é verdadeiro para todo $1 \leq j \leq k$, então $P(k + 1)$ é verdadeiro.

- A **hipótese de indução** ou **I.H.** da indução forte é $P(1) \wedge P(2) \wedge . . . \wedge P(k)$ são todos verdadeiros.

- O princípio da indução matemática forte pode ser expresso como uma regra de inferência sobre os números inteiros:

$$[\, P(1) \wedge \forall k : ([P(1) \wedge P(2) \wedge . . . \wedge P(k)] \rightarrow P(k + 1))] \rightarrow \forall n : P(n)$$

Prova por indução matemática (forte)

- Exemplo: Se n é um inteiro maior que 1, então n pode ser escrito como o produto de números primos.

  Prova. Seja $P(n)$ a proposição *“n pode ser escrito como o produto de números primos”*.

  Passo base: $P(2)$ é verdadeiro porque 2 pode ser escrito como o produto de um número primo, ele mesmo.

  Passo indutivo: A hipótese de indução é que $P(j)$ é verdadeiro para todos os inteiros positivos tais que $2 \leq j \leq k$, ou seja, que qualquer inteiro j entre 2 e k pode ser escrito como o produto de primos.

  Para completar o passo indutivo, temos que mostrar que a I.H. de indução implica que $P(k + 1)$ também é verdadeira, ou seja, que o inteiro $k + 1$ também pode ser escrito como o produto de primos.

Prova por indução matemática (forte)

- Exemplo: (Continuação)

Há dois casos a se considerarem: $k + 1$ é primo ou $k + 1$ é composto.

- Caso 1: $k + 1$ é primo. Neste caso $P(k + 1)$ é trivialmente verdadeiro, porque $k + 1$ é o produto de um único primo, ele mesmo.
- Caso 2: $k + 1$ é composto. Neste caso $k + 1$ pode ser escrito como o produto de dois inteiros a e b tais que $2 \leq a \leq b \leq k$. Pela hipótese de indução, tanto a quanto b podem ser escritos como o produto de primos (já que $P(j)$ vale para todo $2 \leq j \leq k$). Logo, $k + 1 = ab$ também pode ser escrito como o produto de primos e assim concluímos o passo indutivo.

Como concluímos com sucesso o passo base e o passo indutivo, mostramos por indução que $\forall n \in Z^+, n \geq 2 : P(n)$, ou seja, que todo inteiro $n \geq 2$ pode ser escrito como o produto de números primos. □

Prova por indução matemática (forte)

- Exemplo: Toda postagem de 12 centavos ou mais pode ser feita usando apenas selos de 4 centavos e selos de 5 centavos.

Prova. Seja $P(n)$ a proposição *“qualquer postagem de n centavos pode ser feita usando apenas selos de* 4 *centavos e selos de* 5 *centavos”*.

Passo base: Vamos precisar de quatro casos base:

- $P(12)$ é verdadeiro porque podemos usar três selos de 4 centavos;
- $P(13)$ é verdadeiro porque podemos usar dois selos de 4 centavos e um selo de 5 centavos;
- $P(14)$ é verdadeiro porque podemos usar um selos de 4 centavos e dois selos de 5 centavos; e
- $P(15)$ é verdadeiro porque podemos usar 3 selos de 5 centavos;

Isto completa o passo base.

Prova por indução matemática (forte)

- Exemplo: (Continuação)

Passo indutivo: A hipótese de indução é que $P(j)$ é verdadeiro para $12 \leq j \leq k$, onde k é um inteiro $k \geq 15$. Ou seja, a I.H. é que toda postagem de valores entre 12 centavos e k centavos pode ser feita usando selos de 4 e 5 centavos apenas.

Para completar o passo indutivo, vamos mostrar que, sob a I.H., $P(k + 1)$ é verdadeiro, ou seja, que uma postagem de $k + 1$ centavos pode ser feita usando-se apenas selos de 4 e 5 centavos.

Pela I.H., $P(k - 3)$ é verdadeiro porque $k - 3 \geq 12$ e para todo $12 \leq j \leq k$ temos $P(j)$ verdadeiro. Logo, existe uma maneira de postar $k - 3$ centavos usando apenas selos de 4 e 5 centavos. Para postar $k + 1$ centavos, basta acrescentar à postagem possível para $k - 3$ centavos um selo de 4 centavos.

Isto conclui o passo indutivo e a prova.

$\square$