

Capítulo 1

Conceitos Básicos

1.1 O Que Provar: Teoremas

O primeiro passo para a resolução de um problema é defini-lo corretamente e precisamente. Tentar encontrar uma solução sem que isso seja feito é receita certa para o insucesso. A definição do problema envolve as seguintes questões:

1. *Qual o objeto (ou quais os objetos) em análise?* Deve-se definir claramente qual o “objeto” sobre o qual se deseja provar algum fato: um triângulo, um conjunto de números inteiros, a trajetória de um projétil.
2. *Quais são as características desse objeto (ou desses objetos)?* Em muitos casos, os objetos identificados possuem características especiais importantes para o problema: o triângulo é retângulo, os números do conjunto são primos, o projétil é arremessado no vácuo próximo à superfície da Terra. Todas as informações sobre o objeto relacionadas ao problema devem ser explicitamente mencionadas.
3. *O que se deseja provar?* Resta agora definir o *problema* em si. Especificados o objeto e suas características conhecidas, qual outra característica se deseja determinar como verdadeira? A soma dos quadrados dos catetos é igual ao quadrado da hipotenusa? O conjunto é infinito? A trajetória é parabólica?

Um *teorema* nada mais é do que uma afirmação apresenta essas três características. Alguns exemplos:

Teorema *Se em um campeonato sem empates todos os times jogam entre si, então é possível, independentemente dos resultados, organizar as equipes em uma “fila” de forma que cada uma (a menos da última) tenha sido vitoriosa sobre a seguinte.*

Teorema *A trajetória de um projétil arremessado no vácuo próximo a superfície da Terra é parabólica.*

Tradicionalmente, um teorema é dividido em duas partes: a *hipótese* apresenta as informações conhecidas sobre o problema; a *tese* representa o que de fato se deseja provar. A forma “padrão” de um teorema, portanto, seria:

Teorema Se *hipótese*, então *tese*.

Essa forma, no entanto, não é obrigatória. É o caso do segundo teorema apresentado como exemplo. Apesar de não haver necessidade, ele pode ser facilmente reescrito no formato “padrão”:

Teorema Se um projétil for arremessado no vácuo próximo à superfície da Terra, então sua trajetória será parabólica.

1.1.1 Lemas, Corolários e Conjecturas

Em algumas situações, teoremas recebem denominações especiais. Quando um teorema é provado apenas para auxiliar na prova de um outro teorema (mais complexo), utiliza-se o termo *lema* para descrevê-lo. Em outros casos, um teorema é consequência imediata de outro teorema mais complexo. Nesse caso, ele recebe a denominação de *corolário*. Considere o seguinte exemplo:

Teorema A soma dos ângulos internos de um triângulo é 180 graus.

Corolário Cada ângulo de um triângulo equilátero tem 60 graus.

Como a prova de um corolário é por definição muito simples, ela é freqüentemente omitida. No entanto, isso deve ser feito com cautela. A decisão de se omitir uma prova (ou mesmo de se considerar que um teorema é de fato um corolário) deve levar em conta não só o teorema em si, mas o público ao qual ele é apresentado. O que é óbvio para alguns pode não sê-lo para outros.

O último caso especial é a *conjectura*, termo usado para descrever teoremas em potencial cuja veracidade ou não ainda está indeterminada. Apesar de freqüentemente ocorrerem abusos de linguagem, uma asserção só poderá ser considerada um teorema se tiver sido provada. Caso contrário, trata-se de uma conjectura. Um exemplo famoso é a seguinte assertiva, formulada pelo matemático francês Pierre de Fermat (1601–1665):

Conjectura Para qualquer valor de n inteiro e maior que 2, não existem três inteiros positivos x , y e z tais que $x^n + y^n = z^n$.

O próprio Fermat provou que a afirmação é verdadeira para $n = 3$, mas uma prova para valores arbitrários de n só foi encontrada em 1995, pelo inglês Andrew Wiles. Portanto, apesar de a proposição acima ser há muito conhecida como o *Último Teorema de Fermat*, a rigor apenas recentemente ela foi alçada à condição de teorema. Antes disso, tratava-se apenas de uma conjectura. A *Última Conjectura de Fermat*.

1.1.2 O Que Não Provar: Axiomas e Definições

A prova de um teorema pode utilizar outros teoremas, desde que eles também tenham sido devidamente provados. É dessa forma que se desenvolvem diversas áreas de conhecimento: resultados cada vez mais complexos podem ser provados a partir de resultados mais simples. Essa cadeia, no entanto, não é infinita. Há dois tipos de enunciados que não precisam (e não podem) ser provados, as *definições* e os *axiomas*. Em última análise, todos os teoremas são provados a partir unicamente deles.

Definição é a enumeração das propriedades que um determinado objeto (matemático ou não) deve obrigatoriamente ter (ou deixar de ter) para pertencer a uma determinada classe de objetos.

Para que um objeto seja considerado um triângulo, por exemplo, ele deve ser um polígono e deve possuir exatamente três lados. Portanto,

Definição *Um triângulo é um polígono de três lados.*

Alguns outros exemplos familiares:

Definição *Um inteiro p é primo se e somente se for divisível por exatamente quatro números: 1, -1 , p e $-p$.*

Definição *O módulo $|r|$ de um número real r é r , se $r \geq 0$, ou $-r$, se $r < 0$.*

Evidentemente, toda definição é correta. Não há necessidade (ou maneira) de prová-la. Há casos, contudo, em que uma mesma entidade recebe duas diferentes definições. Quando isso ocorre, é necessário provar que as definições se equivalem.

Um *axioma* é uma afirmação básica aceita por todos acerca de um algo. Axiomas são normalmente informações óbvias, baseadas no senso comum:

Axioma *Todo número inteiro tem um único sucessor.*

Axioma *Entre dois pontos distintos no plano existe uma única reta.*

Repare que axiomas são distintos de definições. Enquanto os axiomas podem tratar de uma propriedade qualquer de um objeto, definições devem necessariamente descrever *todas* as propriedades que um objeto deve possuir (ou deixar de possuir) para fazer parte de uma classe de objetos.

1.2 Quantificadores e Negação

Um teorema (ou uma assercao qualquer, correta ou incorreta) pode tratar de um objeto fixo. Por exemplo:

Asserção *O número 31.234.971 é divisível por 3.*

A utilidade desse tipo de resultado é limitada, no mínimo. É comum, portanto, que enunciados contenham *quantificadores* para expressar resultados mais gerais:

Asserção *Todo número cuja soma dos dígitos (na base 10) é um múltiplo 3 é divisível por 3.*

Asserção *Existe uma tripla de números inteiros x , y e z tal que $x^2 + y^2 = z^2$.*

O quantificador *todo* é representado por \forall , e muitas vezes utilizamos o termo *qualquer que seja* em seu lugar. Por sua vez, o quantificador *existe* é denotado por \exists . Frequentemente, torna-se necessário encontrar a **negação** de uma asserção. Nesse momento é fundamental compreender perfeitamente o significado dos quantificadores. Por exemplo, a negativa (ou forma complementar) das asserções acima podem ser apresentadas nas formas abaixo.

Asserção *Existe um número que **não** é divisível por 3 cuja soma dos dígitos (na base 10) é um múltiplo de 3.*

Asserção *Toda tripla de números inteiros x , y e z é tal que $x^2 + y^2 \neq z^2$.*

Uma outra forma válida de negar as asserções originais seria:

Asserção *Nem todo número cuja soma dos dígitos (na base 10) é um múltiplo de 3 é divisível por 3.*

Asserção *Não existe uma tripla de números inteiros x , y e z tal que $x^2 + y^2 = z^2$.*

Verifique que todas as negativas das duas primeiras asserções são falsas, visto que suas formas originais são verdadeiras (i.e. são teoremas).

1.3 Tipos de Provas

Uma vez estudadas as características dos teoremas, resta agora determinar como prová-los. Conforme se verá, há diversos tipos de provas, todos igualmente válidos. Cada teorema possui características que tornam mais adequado um ou outro método, ou mesmo uma combinação de métodos.

Independentemente da natureza da prova, deve-se garantir que ela seja inequívoca. Depois de rigorosamente provado, um teorema jamais deixará de ser verdadeiro. Para isso, todas as informações utilizadas para a prova devem ser verdadeiras, de forma absoluta (sempre) ou por hipótese (ou seja, válidas nas condições às quais o teorema se aplica). Isso inclui não só as hipóteses apresentadas no enunciado do teorema, mas também definições, axiomas e até outros teoremas, desde que já devidamente provados e compatíveis com as hipóteses.

Relacionado a isso está o fato de que, se o enunciado trata de um objeto genérico (ou arbitrário), a prova também deve fazê-lo. Ela deve utilizar como propriedades apenas as hipóteses ou o que for derivável a partir delas, de axiomas e de definições. Se uma propriedade não é mencionada, não se pode assumir ela é válida ou que *não* é válida. A prova deve ser completamente independente desse fato. Por exemplo, se o enunciado do teorema é “a soma dos ângulos internos de um triângulo é 180 graus”, a prova não pode usar em momento algum o “fato” de que o triângulo é equilátero, pois ele não é verdadeiro em todos os casos. Se o enunciado nada diz sobre a relação entre os lados do triângulo, deve-se supor que qualquer relação é possível.

1.3.1 Exemplos e Contra-exemplos

Alguns tipos especiais de teoremas prestam-se a provas relativamente simples: a mera apresentação de um exemplo ou contra-exemplo. Quando o enunciado afirma que existe um objeto com determinadas características, apresentar um tal objeto é suficiente para provar o teorema. Por exemplo:

Teorema *Existem três inteiros positivos x , y e z tais que $x^2 + y^2 = z^2$.*

Prova Os números $x = 3$, $y = 4$ e $z = 5$ são inteiros que satisfazem à restrição ($3^2 + 4^2 = 5^2$). \square

Observe que, apesar de haver outros exemplos — (5, 12, 13), (11, 60, 61), (48, 55, 73), etc. — basta apresentar um único para que o teorema seja considerado provado. Da mesma forma, se o enunciado do teorema afirmar a existência não de um, mas de N (uma constante) objetos com uma dada característica, basta apresentar N objetos distintos como prova. Mas cuidado: se o teorema tratar da existência de *infinitos* objetos com uma certa características, apenas apresentar exemplos não é uma prova satisfatória.

Contra-exemplos são usados de forma semelhante aos exemplos, mas para provar que uma determinada conjectura está *errada*. Para isso, é necessário que o enunciado afirme que *todos* os objetos de certo tipo possuam uma determinada propriedade ou que *nenhum* a possui. No primeiro caso, a conjectura será considerada falsa se for apresentado um objeto que *não* possui a propriedade para; no segundo caso, o objeto apresentado deve *possuir* a propriedade. (Na verdade, conforme discutido na seção anterior, os dois casos são equivalentes.) Vejamos um exemplo:

Conjectura *Nenhum número primo é par.*

Contraprova A conjectura está incorreta, pois o número 2 é primo e é par. \square

Esse é um exemplo extremamente simples, mas nem sempre é esse o caso. Há casos em que se passam anos, ou mesmo séculos, entre a formulação de uma conjectura e o surgimento de um contra-exemplo. Considere a seguinte conjectura, também proposta por Pierre de Fermat (como se pode perceber, um matemático muito afeito a conjecturas):

Conjectura *Todos os números da forma $2^{2^n} + 1$ são primos.*

“Prova” Testes triviais mostram que essa afirmação é verdadeira para valores pequenos de n . Os cinco primeiros números com a forma proposta (a partir de $n = 0$) são 3, 5, 17, 257 e 65537. É relativamente simples verificar que todos são primos. No entanto, para o número seguinte, $2^{2^5} + 1 = 4,294,967,297$, a verificação não é tão fácil. Ainda assim, com base na certeza da primalidade dos 5 primeiros termos, Fermat formulou sua conjectura. Em 1732 (quase 70 anos depois da morte de Fermat), entretanto, o matemático suíço Leonhard Euler (1707–1783) conseguiu demonstrar que 4,294,967,297 *não* é um número primo: 641 e 6,700,417 são seus divisores. Portanto, $n = 5$ é um contra-exemplo que torna falsa a conjectura de Fermat. (Ainda assim, os números da forma $2^{2^n} + 1$ são hoje conhecidos como *números de Fermat*.) \square

Como esse problema ilustra, encontrar um contra-exemplo nem sempre é simples. No caso, foi preciso fatorar um número de 10 dígitos. Com os computadores atuais e novos métodos de fatoração, divisores de números dessa magnitude podem ser facilmente determinados. Na verdade, é possível tratar problemas muito maiores; no caso dos números com a forma sugerida por Fermat ($2^{2^n} + 1$), em especial, foram encontrados divisores para todos os valores de n entre 6 ($2^{64} + 1$) e 13 ($2^{8192} + 1$). Em alguns dos casos, contudo, ainda não foi possível realizar a fatoração completa: é possível que um ou mais dos fatores já encontrados não sejam primos. De qualquer forma, o fato de todos os valores de n testados possuírem divisores faz com que atualmente se acredite na conjectura *oposta* à de Fermat:

Conjectura *Para $n > 4$, todos os números da forma $2^{2^n} + 1$ são compostos.*

No entanto, essa conjectura padece do mesmo mal da original: ela se baseia unicamente em alguns poucos exemplos. Um segundo contra-exemplo pode demonstrar que também ela está errada. No entanto, encontrar contra-exemplos é uma tarefa especialmente difícil nesse caso. O número seguinte da seqüência ($2^{16384} + 1$) tem aproximadamente 5000 dígitos!

1.3.2 Força Bruta

Como os problemas apresentados na seção anterior ilustram, exemplos e contra-exemplos são métodos muito simples de se provar um teorema, com uma pequena ressalva: é preciso encontrá-los,

o que nem sempre é fácil.

A estratégia normalmente utilizada para encontrar um contra-exemplo ou exemplo é a verificação de cada um dos objetos sobre os quais trata o teorema. No caso da conjectura proposta por Fermat apresentada na seção anterior, por exemplo, o que se fez foi testar para $n = 0, 1, 2, \dots$. Felizmente, um contra-exemplo foi encontrado para $n = 5$, um valor relativamente pequeno. No caso da conjectura oposta, sabe-se que esta é válida para $n = 5, \dots, 12$ e 13 o que a faz permanecer na condição de conjectura.

Nem sempre é esse o caso. Algumas outras conjecturas podem ter sua validade completamente determinada testando-se cada um dos objetos aos quais elas se aplicam. Para tornar a discussão mais simples, considere que a conjectura seja expressa com o quantificador *todos* (expressões que utilizam quantificadores como *existe* ou *nenhum* podem ser facilmente reescritas usando o quantificador *todos*). Se durante os testes for encontrado pelo menos um objeto que falsifique a conjectura, pode-se afirmar que ela está errada; se, ao contrário, nenhum dos objetos testados tornar falsa a conjectura, ela poderá ser considerada verdadeira.

Repare que, para provar que a conjectura é verdadeira, é necessário enumerar *todos* os objetos possíveis. Por razões óbvias, esse método de prova é denominado *enumeração completa*, *busca exaustiva* ou *força bruta*.

Evidente, o método só poderá se constituir numa prova se o número de objetos for finito. Esse não é o caso, por exemplo, do Último Teorema de Fermat (seção 1.1.1). Para determinar sua validade por enumeração completa, seria necessário testar todas as quádruplas (x, y, z, n) com x, y e z positivos e $n > 2$, o que é claramente impossível. O máximo que se pode esperar de uma busca exaustiva em situações como essa é que seja encontrado um contra-exemplo que invalide a conjectura. Provar que ela está *correta*, no entanto, não é possível por esse método.

Mesmo nos casos em que o número de possibilidades é finito, ele pode ser grande demais para ser analisado. Testes de primalidade de um número inteiro, por exemplo, são normalmente baseados em busca exaustiva. As técnicas atuais permitem que se faorem números com até poucas centenas de dígitos, mesmo se houver um grande poder computacional disponível para a tarefa.

Apesar dessas limitações, provas por enumeração de complexidade cada vez maior têm se tornado possíveis graças ao desenvolvimento dos computadores. Conjecturas há muito propostas têm sido resolvidas graças a esse método. É o caso do seguinte problema, proposto no século XIX:

Conjectura *É impossível colocar em um tabuleiro de xadrez as 8 peças mais poderosas (rainha, torres, bispos, cavalos e rei) de forma que todas as 64 casas estejam sob ataque.*

Esse foi considerado um problema em aberto por mais de um século, pois não havia sido encontrada uma solução que o invalidasse nem havia garantias de que em todas as possíveis configurações pelo menos uma casa está protegida. Em 19??, contudo, Robison, Hafner e Skiena, utilizando um método baseado em busca exaustiva, conseguiram provar que a conjectura está correta: o número máximo de casas simultaneamente sob ataque é 63. A prova, no entanto, requereu quase 24 horas de processamento em computador.

Além desse, há muitos outros problemas — com grande utilidade prática — para os quais a melhor solução conhecida é a busca exaustiva ou uma variação dela. Entre eles, talvez o mais conhecido seja o *Problema do Caixeiro Viajante*, que pode ser enunciado da seguinte forma:

Teorema *Dados um conjunto de n cidades, os comprimentos das estradas existentes entre elas e*

um número positivo D , determinar se é possível sair de uma cidade, passar por todas as demais uma única vez e retornar à origem percorrendo uma distância inferior D quilômetros.

Uma última observação sobre provas baseadas em busca exaustiva: apesar de ser necessário verificar todas os possíveis objetos analisados, muitas vezes isso pode ser feito de forma apenas implícita. Considere, por exemplo, o problema do caixeiro viajante da forma como foi enunciado. O objetivo é determinar se existe uma permutação das n cidades tal que, se elas forem percorridas nessa ordem, a distância total será inferior a D . A solução “óbvia” seria enumerar todas as $n!$ permutações e testar uma a uma. Para $n = 8$, por exemplo, suponha que as primeiras três cidades de uma solução sejam, na ordem, C_1 , C_2 e C_3 . Se a soma dos comprimentos dos caminhos que levam C_1 a C_2 e C_2 a C_3 já for maior que a distância D , pode-se considerar que todas as permutações iniciadas com as três cidades nessa ordem foram devidamente analisadas, mesmo que isso não seja feito explicitamente. Em muitos casos, é possível adotar argumentos de simetria para reduzir ainda mais o número de permutações analisadas. Para o caixeiro viajante, por exemplo, pode-se supor que todos os caminhos começam na cidade C_1 (por quê?).

Essas e outras técnicas, algumas extremamente elaboradas, são rotineiramente utilizadas para tratar de forma mais eficiente problemas práticos. Para muitos deles, isso é tudo o que se pode fazer, pois é pequena a probabilidade de que eles admitam um método que não seja baseado em força bruta.

1.3.3 Prova Direta

Provas diretas são as mais comumente encontradas e, portanto, são extremamente intuitivas. Elas seguem uma seqüência natural: a partir das informações fornecidas (hipóteses), apresentam uma série de passos lógicos interrelacionados até que se chegue ao resultado desejado (tese). Teoremas relativos à Geometria Plana, por exemplo, em geral têm provas diretas:

Teorema A altura h de um triângulo equilátero de lado a é $h = \frac{a\sqrt{3}}{2}$.

Prova Por definição, o segmento \overline{AH} , que representa altura de um triângulo equilátero $\triangle ABC$, forma um ângulo reto com a base \overline{BC} . Forma-se assim o triângulo retângulo $\triangle AHB$, que tem como hipotenusa o segmento AB (que mede a) e como catetos \overline{AH} (que mede h) e \overline{HB} . Como todo triângulo equilátero é isósceles, a altura divide a base em duas partes iguais; portanto, \overline{HB} mede $\frac{a}{2}$. Aplicando o Teorema de Pitágoras ao triângulo $\triangle AHB$, temos:

$$h^2 + \left(\frac{a}{2}\right)^2 = a^2.$$

Resolvendo essa equação, encontramos $h = \frac{a\sqrt{3}}{2}$. □

Nesse caso, foram utilizados apenas argumentos geométricos e algébricos simples para a prova do teorema. Repare que uma prova (não só direta) pode utilizar, além de axiomas e definições, outros teoremas mais básicos. No exemplo, o único mencionado explicitamente é o Teorema de Pitágoras. A rigor, no entanto, o fato de que a altura um triângulo isósceles divide a base em duas partes iguais também necessitaria de uma prova.

1.3.4 Prova Construtiva

Uma *prova construtiva* apresenta um método, procedimento ou fórmula para que se obtenham os objetos sobre os quais trata o teorema. O método é bastante semelhante à apresentação de exemplos (seção 1.3.1), mas sua aplicação é menos restrita. De maneira geral, uma prova construtiva mostra como construir não um único exemplo, mas um conjunto deles (infinitos, possivelmente). Para melhor compreensão do método, considere o seguinte teorema:

Teorema *Existem infinitas triplas (x, y, z) de números inteiros positivos tais que $x^2 + y^2 = z^2$.*

Prova Conjuntos infinitos têm uma propriedade interessante: é possível determinar subconjuntos que também são infinitos. Para provar que o teorema está correto, basta mostrar como construir um conjunto infinito de triplas em que $x^2 + y^2 = z^2$, mesmo esse conjunto não inclua algumas triplas com essa propriedade.

Começemos com a tripla $(3, 4, 5)$. Ela atende à propriedade requerida, pois $3^2 + 4^2 = 5^2$. Consideremos agora as triplas da forma $(3k, 4k, 5k)$, com k assumindo qualquer valor inteiro positivo. Vale a seguinte relação:

$$(3k)^2 + (4k)^2 = 3^2k^2 + 4^2k^2 = (3^2 + 4^2)k^2 = (5^2)k^2 = (5k)^2$$

Portanto, todas as triplas da forma $(3k, 4k, 5k)$ têm a propriedade desejada. Como há infinitos valores de k , há infinitas triplas: $(3, 4, 5)$, $(6, 8, 10)$, $(9, 12, 15)$, e assim por diante. Note que, apesar de não incluir várias (infinitas) triplas válidas, como $(5, 12, 13)$, o conjunto construído é infinito, o que basta para provar o teorema. \square

Em resumo, para provar que um certo conjunto é infinito, apresentou-se uma prova que dá origem a um subconjunto que em si já é infinito. Provas construtivas são úteis também quando o objeto construído é finito, mas arbitrariamente grande.

Teorema *A série harmônica $(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots)$ é divergente.*

Prova Basta provar que, dado um inteiro M qualquer, é possível encontrar um inteiro n tal que:

$$\sum_{i=1}^n \frac{1}{i} > M.$$

Em outras palavras, o valor de n deve ser tal que uma série harmônica terminada em $\frac{1}{n}$ (finita, portanto) tenha soma maior que M , independentemente do valor dessa constante (basta que seja finito). Para que a prova seja mais simples, ignore momentaneamente o primeiro termo da série (1), fazendo-o começar em $\frac{1}{2}$. Com a retirada de um elemento não aumenta o valor da soma (pelo contrário), ela não invalida a prova.

Considere as seqüências em que $n = 2^k$ (k inteiro). Divida uma seqüência desse tipo em subseqüências terminadas por elementos cujos denominadores são potências de 2 ($\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, etc.). É simples verificar que cada uma das subseqüências tem soma pelo menos $1/2$. Para construir uma seqüência cuja soma é maior que M , basta adicionar subseqüências terminadas em potência de 2 até que a soma seja maior que M . O fato de que cada uma delas é finita e tem um valor mínimo (ou *limite inferior*) garante que, após um número finito de operações, a seqüência gerada terá soma maior que M .

$$\begin{aligned}
\frac{1}{2} &\geq 1 \cdot \frac{1}{2} = \frac{1}{2} \\
\frac{1}{3} + \frac{1}{4} &> \frac{1}{4} + \frac{1}{4} = 2 \cdot \frac{1}{4} = \frac{1}{2} \\
\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} &> \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} = 4 \cdot \frac{1}{8} = \frac{1}{2} \\
&\vdots \\
\frac{1}{\frac{n}{2} + 1} + \frac{1}{\frac{n}{2} + 2} + \dots + \frac{1}{n} &> \frac{n}{2} \cdot \frac{1}{n} = \frac{1}{2}
\end{aligned}$$

□

Exercício: determinar o número de termos da seqüência resultante.

Observe que as provas construtivas apresentam uma forma para se obter o objeto referido no teorema, que nos casos acima são: um conjunto infinito de triplas satisfazendo as condições especificadas e para um valor M dado uma série harmônica com valor superior à M .

1.3.5 Prova por Contradição

Conforme vimos até aqui, teoremas podem ser enunciados de diversas formas equivalentes. Do mesmo modo, as respectivas provas também podem ser diferentes. Vimos também que teoremas que podem ser provados por exemplos e conjecturas que podem ser refutadas por contra-exemplos são em geral tarefas mais fáceis que demonstrar a validade de uma asserção para um conjunto infinito de objetos. Assim, matemáticos utilizam frequentemente essa liberdade de representação de uma asserção para facilitar suas respectivas provas.

A prova por contradição consiste provar que a negativa de um teorema é falsa. Consequentemente, esta prova demonstra que o teorema é verdadeiro. Seja \mathcal{T} o teorema a ser provado. O que acabamos de descrever é que se a implicação $\bar{\mathcal{T}} \implies \text{falso}$ for verdadeira, \mathcal{T} é verdadeiro. Exemplo:

Teorema *Existe uma quantidade infinita de números primos.*

Prova Por contradição. Vamos provar que a hipótese *Existe uma quantidade finita de números primos* é falsa. Assumimos então que o conjunto de números primos é finito ou, em outras palavras, que este conjunto pode ser escrito na forma $P = \{p_1, p_2, \dots, p_n\}$, onde p_i é o i -ésimo menor número primo. Para provar que isto é falso, basta apresentarmos um número primo que não pertence a este conjunto. Um tal número primo q pode ser obtido da seguinte forma: $q = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. Bom, falta ainda demonstrarmos que este número é primo. Para isto utilizamos a definição de número primo, i.e. um número que só é divisível por 1 e por ele mesmo (e os simétricos destes). Portanto, números compostos (não primos) são aqueles que são divisíveis por algum número primo. Agora basta verificar que não existe nenhum número em P que divide q , o que permite concluir que q também é primo. Esta conclusão indica que qualquer que seja o conjunto finito exaustivo de números primos que apresentemos, podemos encontrar um outro número primo que não pertence a este conjunto e portanto deve ser acrescentado a este conjunto. Logo a hipótese é falsa e consequentemente o teorema é verdadeiro. □

Portanto, devemos sempre considerar a possibilidade de uma prova por contradição, visto que o trabalho pode ser significativamente simplificado.

1.4 Erros Comuns

Esta seção apresenta erros freqüentemente cometido na tentativa de se provar um teorema. O objetivo é ilustrar a importância de algumas das recomendações e observações feitas no item anterior. Lembre-se: todas as provas desta seção estão **incorretas**.

Teorema Em um triângulo de lados a , b e c , vale a relação $a^2 = b^2 + c^2 - 2bc \cos \alpha$, sendo α o ângulo oposto a a .

“Prova” O enunciado trata de um triângulo arbitrário. Consideremos um triângulo qualquer, portanto; um triângulo retângulo, por exemplo. De acordo com o teorema de Pitágoras, vale a relação $a^2 = b^2 + c^2$. Substituindo o valor de a^2 na equação que se deseja provar, temos:

$$b^2 + c^2 = b^2 + c^2 - 2bc \cos \alpha \implies 2bc \cos \alpha = 0$$

Como os lados de um triângulo têm comprimento estritamente positivo, para que essa equação seja verdadeira devemos ter $\cos \alpha = 0$. No entanto, como se trata de um triângulo retângulo, isso é imediato: $\alpha = 90 \implies \cos \alpha = 0$. Portanto, a relação é válida. \square

Apesar de o teorema estar correto, a prova está completamente equivocada. Ela ilustra uma “interpretação” comum — e errada — da noção de arbitrariedade. Corretamente, a “prova” afirma que se trata de um triângulo arbitrário. Ou seja: o teorema vale para qualquer triângulo. No entanto, o que se faz em seguida é justamente “escolher” o “qualquer”: um triângulo retângulo. Nesse momento, deixa de haver a arbitrariedade, e tudo o que se diz em seguida é válido somente para o caso particular selecionado. Portanto, em vez de se provar que a relação é válida para *todos* os triângulos, provou-se que ela vale para *algum* triângulo (o retângulo).

Em outras palavras, a prova apenas mostra que um ter um ângulo reto é uma condição suficiente para que a relação seja válida em um triângulo. Contudo, essa condição não é necessária.

Exercícios

1. Determine os fatores primos de 4,294,967,297.
2. Calcule o número de tabuleiros de xadrez formados apenas pelas 8 peças mais poderosas (rainha, rei, torres, bispos e cavalos).