TURING 图灵原版数学·统计学系列 35

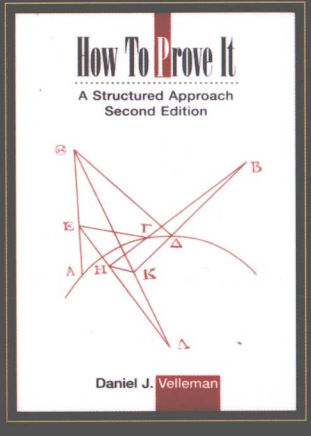
CAMBRIDGE

How to Prove It

怎样证明数学题

（英文版·第2版）

[美] Daniel J. Velleman 著



人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵原版数学·统计学系列

How to Prove It

怎样证明数学题

（英文版·第2版）

[美] Daniel J. Velleman 著

人民邮电出版社
北京

图书在版编目（CIP）数据

怎样证明数学题：第2版＝How to Prove It: A Structured Approach, Second Edition: 英文/（美）费林曼（Velleman, D. J.）著. —北京：人民邮电出版社，2009.7
（图灵原版数学·统计学系列）
ISBN 978-7-115-20968-9

I. 怎… II. 费… III. 数学－证明－方法 IV. O1-0

中国版本图书馆CIP数据核字（2009）第088996号

内 容 提 要

本书介绍了数学证明的基本要点，内容通俗而不失严谨，可以帮助高中以上程度的学生熟悉数学语言，迈入数学殿堂．新版添加了200多个练习题，附录中给出部分练习的答案或提示．

本书适用于任何对逻辑和证明感兴趣的人，数学、计算机科学、哲学、语言学专业的读者都可以从中获益匪浅．

图灵原版数学·统计学系列

怎样证明数学题（英文版·第2版）

◆ 著 [美] Daniel J. Velleman
责任编辑 明永玲
◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
◆ 开本：700×1000 1/16
印张：24.75
字数：394千字 2009年7月第1版
印数：1-2 000册 2009年7月北京第1次印刷
著作权合同登记号 图字：01-2009-2895号
ISBN 978-7-115-20968-9/O1

定价：59.00元

读者服务热线：（010）51095186 印装质量热线：（010）67129223
反盗版热线：（010）67171154

版 权 声 明

To Shelley

Preface to the Second Edition

I would like to thank all of those who have sent me comments about the first edition. Those comments have resulted in a number of small changes throughout the text. However, the biggest difference between the first edition and the second is the addition of more than 200 new exercises. There is also an appendix containing solutions to selected exercises. Exercises for which solutions are supplied are marked with an asterisk. In most cases, the solution supplied is a complete solution; in some cases, it is a sketch of a solution, or a hint.

Some exercises in Chapters 3 and 4 are also marked with the symbol ℞. This indicates that these exercises can be solved using Proof Designer. Proof Designer is computer software that helps the user write outlines of proofs in elementary set theory, using the methods discussed in this book. Further information about Proof Designer can be found in an appendix, and at the Proof Designer Web site: `http://www.cs.amherst.edu/~djv/pd/pd.html`.

Preface

Students of mathematics and computer science often have trouble the first time they're asked to work seriously with mathematical proofs, because they don't know the "rules of the game." What is expected of you if you are asked to prove something? What distinguishes a correct proof from an incorrect one? This book is intended to help students learn the answers to these questions by spelling out the underlying principles involved in the construction of proofs.

Many students get their first exposure to mathematical proofs in a high school course on geometry. Unfortunately, students in high school geometry are usually taught to think of a proof as a numbered list of statements and reasons, a view of proofs that is too restrictive to be very useful. There is a parallel with computer science here that can be instructive. Early programming languages encouraged a similar restrictive view of computer programs as numbered lists of instructions. Now computer scientists have moved away from such languages and teach programming by using languages that encourage an approach called "structured programming." The discussion of proofs in this book is inspired by the belief that many of the considerations that have led computer scientists to embrace the structured approach to programming apply to proof-writing as well. You might say that this book teaches "structured proving."

In structured programming, a computer program is constructed, not by listing instructions one after another, but by combining certain basic structures such as the if-else construct and do-while loop of the Java programming language. These structures are combined, not only by listing them one after another, but also by *nesting* one within another. For example, a program constructed by

nesting an if-else construct within a do-while loop would look like this:

```
do
  if [condition]
    [List of instructions goes here.]
  else
    [Alternate list of instructions goes here.]
while [condition]
```

The indenting in this program outline is not absolutely necessary, but it is a convenient method often used in computer science to display the underlying structure of a program.

Mathematical proofs are also constructed by combining certain basic proof structures. For example, a proof of a statement of the form "if P then Q" often uses what might be called the "suppose-until" structure: We *suppose* that P is true *until* we are able to reach the conclusion that Q is true, at which point we retract this supposition and conclude that the statement "if P then Q" is true. Another example is the "for arbitrary x prove" structure: To prove a statement of the form "for all x, $P(x)$," we *declare x to be an arbitrary object* and then *prove P(x)*. Once we reach the conclusion that $P(x)$ is true we retract the declaration of x as arbitrary and conclude that the statement "for all x, $P(x)$" is true. Furthermore, to prove more complex statements these structures are often combined, not only by listing one after another, but also by nesting one within another. For example, to prove a statement of the form "for all x, if $P(x)$ then $Q(x)$" we would probably nest a "suppose-until" structure within a "for arbitrary x prove" structure, getting a proof of this form:

```
Let x be arbitrary.
  Suppose P(x) is true.
    [Proof of Q(x) goes here.]
  Thus, if P(x) then Q(x).
Thus, for all x, if P(x) then Q(x).
```

As before, we have used indenting to make the underlying structure of the proof clear.

Of course, mathematicians don't ordinarily write their proofs in this indented form. Our aim in this book is to teach students to write proofs in ordinary English paragraphs, just as mathematicians do, and not in the indented form. Nevertheless, our approach is based on the belief that if students are to succeed at writing such proofs, they must understand the underlying structure that proofs have. They must learn, for example, that sentences like "Let x be arbitrary" and "Suppose P" are not isolated steps in proofs, but are used to introduce the "for arbitrary x prove" and "suppose-until" proof structures. It is not uncommon for beginning students to use these sentences inappropriately in other ways.

Such mistakes are analogous to the programming error of using a "do" with no matching "while."

Note that in our examples, the choice of proof structure is guided by the logical form of the statement being proven. For this reason, the book begins with elementary logic to familiarize students with the various forms that mathematical statements take. Chapter 1 discusses logical connectives, and quantifiers are introduced in Chapter 2. These chapters also present the basics of set theory, because it is an important subject that is used in the rest of the book (and throughout mathematics), and also because it serves to illustrate many of the points of logic discussed in these chapters.

Chapter 3 covers structured proving techniques in a systematic way, running through the various forms that mathematical statements can take and discussing the proof structures appropriate for each form. The examples of proofs in this chapter are for the most part chosen, not for their mathematical content, but for the proof structures they illustrate. This is especially true early in the chapter, when only a few proof techniques have been discussed, and as a result many of the proofs in this part of the chapter are rather trivial. As the chapter progresses the proofs get more sophisticated and more interesting, mathematically.

Chapters 4 and 5, on relations and functions, serve two purposes. First, they provide subject matter on which students can practice the proof-writing techniques from Chapter 3. And second, they introduce students to some fundamental concepts used in all branches of mathematics.

Chapter 6 is devoted to a method of proof that is very important in both mathematics and computer science: mathematical induction. The presentation builds on the techniques from Chapter 3, which students should have mastered by this point in the book.

Finally, in Chapter 7 many ideas from throughout the rest of the book are brought together to prove some of the most difficult and most interesting theorems in the book.

I would like to thank all those who read earlier drafts of the manuscript and made many helpful suggestions for improvements, in particular Lauren Cowles at Cambridge University Press, my colleague Professor Duane Bailey and his Discrete Mathematics class, who tried out earlier versions of some chapters, and finally my wife, Shelley, without whose constant encouragement this book would never have been written.

Contents

Introduction

What is mathematics? High school mathematics is concerned mostly with solving equations and computing answers to numerical questions. College mathematics deals with a wider variety of questions, involving not only numbers, but also sets, functions, and other mathematical objects. What ties them together is the use of *deductive reasoning* to find the answers to questions. When you solve an equation for x you are using the information given by the equation to *deduce* what the value of x must be. Similarly, when mathematicians solve other kinds of mathematical problems, they always justify their conclusions with deductive reasoning.

Deductive reasoning in mathematics is usually presented in the form of a *proof*. One of the main purposes of this book is to help you develop your mathematical reasoning ability in general, and in particular your ability to read and write proofs. In later chapters we'll study how proofs are constructed in detail, but first let's take a look at a few examples of proofs.

Don't worry if you have trouble understanding these proofs. They're just intended to give you a taste of what mathematical proofs are like. In some cases you may be able to follow many of the steps of the proof, but you may be puzzled about why the steps are combined in the way they are, or how anyone could have thought of the proof. If so, we ask you to be patient. Many of these questions will be answered later in this book, particularly in Chapter 3.

All of our examples of proofs in this introduction will involve prime numbers. Recall that an integer larger than 1 is said to be *prime* if it cannot be written as a product of two smaller positive integers. For example, 6 is not a prime number, since $6 = 2 \cdot 3$, but 7 is a prime number.

Before we can give an example of a proof involving prime numbers, we need to find something to prove – some fact about prime numbers whose correctness can be verified with a proof. Sometimes you can find interesting

patterns in mathematics just by trying out a calculation on a few numbers. For example, consider the table in Figure 1. For each integer n from 2 to 10, the table shows whether or not both n and $2^n - 1$ are prime, and a surprising pattern emerges. It appears that $2^n - 1$ is prime in precisely those cases in which n is prime!

n	Is n prime?	$2^n - 1$	Is $2^n - 1$ prime?
2	yes	3	yes
3	yes	7	yes
4	no: $4 = 2 \cdot 2$	15	no: $15 = 3 \cdot 5$
5	yes	31	yes
6	no: $6 = 2 \cdot 3$	63	no: $63 = 7 \cdot 9$
7	yes	127	yes
8	no: $8 = 2 \cdot 4$	255	no: $255 = 15 \cdot 17$
9	no: $9 = 3 \cdot 3$	511	no: $511 = 7 \cdot 73$
10	no: $10 = 2 \cdot 5$	1023	no: $1023 = 31 \cdot 33$

Figure 1

Will this pattern continue? It is tempting to guess that it will, but this is only a guess. Mathematicians call such guesses *conjectures*. Thus, we have the following two conjectures:

Conjecture 1. *Suppose n is an integer larger than 1 and n is prime. Then $2^n - 1$ is prime.*

Conjecture 2. *Suppose n is an integer larger than 1 and n is not prime. Then $2^n - 1$ is not prime.*

Unfortunately, if we continue the table in Figure 1, we immediately find that Conjecture 1 is incorrect. It is easy to check that 11 is prime, but $2^{11} - 1 = 2047 = 23 \cdot 89$, so $2^{11} - 1$ is not prime. Thus, 11 is a *counterexample* to Conjecture 1. The existence of even one counterexample establishes that the conjecture is incorrect, but it is interesting to note that in this case there are many counterexamples. If we continue checking numbers up to 30, we find two more counterexamples to Conjecture 1: Both 23 and 29 are prime, but $2^{23} - 1 = 8{,}388{,}607 = 47 \cdot 178{,}481$ and $2^{29} - 1 = 536{,}870{,}911 = 2{,}089 \cdot 256{,}999$. However, no number up to 30 is a counterexample to Conjecture 2.

Do you think that Conjecture 2 is correct? Having found counterexamples to Conjecture 1, we know that this conjecture is incorrect, but our failure to find a

counterexample to Conjecture 2 does not show that it is correct. Perhaps there are counterexamples, but the smallest one is larger than 30. Continuing to check examples might uncover a counterexample, or, if it doesn't, it might increase our confidence in the conjecture. But we can never be sure that the conjecture is correct if we only check examples. No matter how many examples we check, there is always the possibility that the next one will be the first counterexample. The only way we can be sure that Conjecture 2 is correct is to *prove* it.

In fact, Conjecture 2 *is* correct. Here is a proof of the conjecture:

Proof of Conjecture 2. Since n is not prime, there are positive integers a and b such that $a < n$, $b < n$, and $n = ab$. Let $x = 2^b - 1$ and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$. Then

$$\begin{aligned} xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= 2^b \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

Since $b < n$, we can conclude that $x = 2^b - 1 < 2^n - 1$. Also, since $ab = n > a$, it follows that $b > 1$. Therefore, $x = 2^b - 1 > 2^1 - 1 = 1$, so $y < xy = 2^n - 1$. Thus, we have shown that $2^n - 1$ can be written as the product of two positive integers x and y, both of which are smaller than $2^n - 1$, so $2^n - 1$ is not prime. □

Now that the conjecture has been proven, we can call it a *theorem*. Don't worry if you find the proof somewhat mysterious. We'll return to it again at the end of Chapter 3 to analyze how it was constructed. For the moment, the most important point to understand is that if n is any integer larger than 1 that can be written as a product of two smaller positive integers a and b, then the proof gives a method (admittedly, a somewhat mysterious one) of writing $2^n - 1$ as a product of two smaller positive integers x and y. Thus, if n is not prime, then $2^n - 1$ must also not be prime. For example, suppose $n = 12$, so $2^n - 1 = 4095$. Since $12 = 3 \cdot 4$, we could take $a = 3$ and $b = 4$ in the proof. Then according to the formulas for x and y given in the proof, we would have $x = 2^b - 1 = 2^4 - 1 = 15$, and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b} = 1 + 2^4 + 2^8 = 273$. And, just as the formulas in the proof predict, we have $xy = 15 \cdot 273 = 4095 = 2^n - 1$. Of course, there are other ways of factoring 12 into a product of two smaller integers, and these might lead to other ways of

factoring 4095. For example, since $12 = 2 \cdot 6$, we could use the values $a = 2$ and $b = 6$. Try computing the corresponding values of x and y and make sure their product is 4095.

Although we already know that Conjecture 1 is incorrect, there are still interesting questions we can ask about it. If we continue checking prime numbers n to see if $2^n - 1$ is prime, will we continue to find counterexamples to the conjecture – examples for which $2^n - 1$ is not prime? Will we continue to find examples for which $2^n - 1$ is prime? If there were only finitely many prime numbers, then we might be able to investigate these questions by simply checking $2^n - 1$ for every prime number n. But in fact there are infinitely many prime numbers. Euclid (circa 350 B.C.) gave a proof of this fact in Book IX of his *Elements*. His proof is one of the most famous in all of mathematics:

Theorem 3. *There are infinitely many prime numbers.*

Proof. Suppose there are only finitely many prime numbers. Let $p_1, p_2, \ldots, p_n$ be a list of all prime numbers. Let $m = p_1 p_2 \cdots p_n + 1$. Note that m is not divisible by p_1, since dividing m by p_1 gives a quotient of $p_2 p_3 \cdots p_n$ and a remainder of 1. Similarly, m is not divisible by any of $p_2, p_3, \ldots, p_n$.

We now use the fact that every integer larger than 1 is either prime or can be written as a product of primes. (We'll see a proof of this fact in Chapter 6.) Clearly m is larger than 1, so m is either prime or a product of primes. Suppose first that m is prime. Note that m is larger than all of the numbers in the list $p_1, p_2, \ldots, p_n$, so we've found a prime number not in this list. But this contradicts our assumption that this was a list of *all* prime numbers.

Now suppose m is a product of primes. Let q be one of the primes in this product. Then m is divisible by q. But we've already seen that m is not divisible by any of the numbers in the list $p_1, p_2, \ldots, p_n$, so once again we have a contradiction with the assumption that this list included all prime numbers.

Since the assumption that there are finitely many prime numbers has led to a contradiction, there must be infinitely many prime numbers. □

Once again, you should not be concerned if some aspects of this proof seem mysterious. After you've read Chapter 3 you'll be better prepared to understand the proof in detail. We'll return to this proof then and analyze its structure.

We have seen that if n is not prime then $2^n - 1$ cannot be prime, but if n is prime then $2^n - 1$ can be either prime or not prime. Because there are infinitely many prime numbers, there are infinitely many numbers of the form $2^n - 1$ that, based on what we know so far, *might* be prime. But how many of them *are* prime?

Prime numbers of the form $2^n - 1$ are called *Mersenne primes*, after Father Marin Mersenne (1588–1647), a French monk and scholar who studied these numbers. Although many Mersenne primes have been found, it is still not known if there are infinitely many of them. Many of the largest known prime numbers are Mersenne primes. As of this writing (April 2005), the largest known prime number is the Mersenne prime $2^{25,964,951} - 1$, a number with 7,816,230 digits.

Mersenne primes are related to perfect numbers, the subject of another famous unsolved problem of mathematics. A positive integer n is said to be *perfect* if n is equal to the sum of all positive integers smaller than n that divide n. (For any two integers m and n, we say that m *divides* n if n is divisible by m; in other words, if there is an integer q such that $n = qm$.) For example, the only positive integers smaller than 6 that divide 6 are 1, 2, and 3, and $1 + 2 + 3 = 6$. Thus, 6 is a perfect number. The next smallest perfect number is 28. (You should check for yourself that 28 is perfect by finding all the positive integers smaller than 28 that divide 28 and adding them up.)

Euclid proved that if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect. Thus, every Mersenne prime gives rise to a perfect number. Furthermore, about 2000 years after Euclid's proof, the Swiss mathematician Leonhard Euler (1707–1783), the most prolific mathematician in history, proved that every even perfect number arises in this way. (For example, note that $6 = 2^1(2^2 - 1)$ and $28 = 2^2(2^3 - 1)$.) Because it is not known if there are infinitely many Mersenne primes, it is also not known if there are infinitely many even perfect numbers. It is also not known if there are any odd perfect numbers.

Although there are infinitely many prime numbers, the primes thin out as we look at larger and larger numbers. For example, there are 25 primes between 1 and 100, 16 primes between 1000 and 1100, and only six primes between 1,000,000 and 1,000,100. As our last introductory example of a proof, we show that there are long stretches of consecutive positive integers containing no primes at all. In this proof, we'll use the following terminology: For any positive integer n, the product of all integers from 1 to n is called n *factorial* and is denoted $n!$. Thus, $n! = 1 \cdot 2 \cdot 3 \cdots n$. As with our previous two proofs, we'll return to this proof at the end of Chapter 3 to analyze its structure.

Theorem 4. *For every positive integer n, there is a sequence of n consecutive positive integers containing no primes.*

Proof. Suppose n is a positive integer. Let $x = (n + 1)! + 2$. We will show that none of the numbers $x, x + 1, x + 2, \ldots, x + (n - 1)$ is prime. Since this is a sequence of n consecutive positive integers, this will prove the theorem.

To see that x is not prime, note that

$$\begin{aligned} x &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n+1) + 1). \end{aligned}$$

Thus, x can be written as a product of two smaller positive integers, so x is not prime.

Similarly, we have

$$\begin{aligned} x + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n+1) + 1), \end{aligned}$$

so $x + 1$ is also not prime. In general, consider any number $x + i$, where $0 \le i \le n - 1$. Then we have

$$\begin{aligned} x + i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + (i+2) \\ &= (i+2) \cdot (1 \cdot 2 \cdot 3 \cdots (i+1) \cdot (i+3) \cdots (n+1) + 1), \end{aligned}$$

so $x + i$ is not prime. □

Theorem 4 shows that there are sometimes long stretches between one prime and the next prime. But primes also sometimes occur close together. Since 2 is the only even prime number, the only pair of consecutive integers that are both prime is 2 and 3. But there are lots of pairs of primes that differ by only two, for example, 5 and 7, 29 and 31, and 7949 and 7951. Such pairs of primes are called *twin primes*. It is not known whether there are infinitely many twin primes.

Exercises

*1. (a) Factor $2^{15} - 1 = 32{,}767$ into a product of two smaller positive integers.
   (b) Find an integer x such that $1 < x < 2^{32767} - 1$ and $2^{32767} - 1$ is divisible by x.

2. Make some conjectures about the values of n for which $3^n - 1$ is prime or the values of n for which $3^n - 2^n$ is prime. (You might start by making a table similar to Figure 1.)

*3. The proof of Theorem 3 gives a method for finding a prime number different from any in a given list of prime numbers.
   (a) Use this method to find a prime different from 2, 3, 5, and 7.
   (b) Use this method to find a prime different from 2, 5, and 11.

4. Find five consecutive integers that are not prime.