# 2

# *Methods of Proof*

## 2.1 What is a Proof?

When a chemist asserts that a substance that is subjected to heat will tend to expand, he/she verifies the assertion through experimentation. It is a consequence of the *definition* of heat that heat will excite the atomic particles in the substance; it is plausible that this in turn will necessitate expansion of the substance. However our knowledge of nature is not such that we may turn these theoretical ingredients into a categorical proof. Additional complications arise from the fact that the word "expand" requires detailed definition. Apply heat to water that is at 40° Fahrenheit or above, and it expands—with enough heat it becomes a gas that surely fills more volume than the original water. But apply heat to a diamond and there is no apparent "expansion"—at least not to the naked eye.

Mathematics is a less ambitious subject. In particular, it is closed. It does not reach outside itself for verification of its assertions. When we make an assertion in mathematics, we must verify it using the rules that we have laid down. That is, we verify it by applying our rules of logic to our axioms and our definitions; in other words, we construct a *proof*. Section 1.8 contains some discussion of proofs and the rules of logic.

In modern mathematics we have discovered that there are perfectly sensible mathematical statements that in fact *cannot* be verified in this fashion, nor can they be proven false. This is a manifestation of Gödel's incompleteness theorem: that any sufficiently complex logical system will contain such unverifiable, indeed untestable, statements (see Section 1.8). Fortunately, in practice, such statements are the exception rather than the rule. In this book, and in almost all of university-level mathematics, we concentrate on learning about statements whose truth or falsity *is* accessible by way of proof.

This chapter considers the notion of mathematical proof. We shall concentrate on the three principal types of proof: direct proof, proof by contradiction, and proof by induction. In practice, a mathematical proof may contain elements of several or all of these techniques. You will see all the basic elements here. You should be sure to master each of these proof techniques, both so that you can recognize them in your reading and so that they become tools that you can use in your own work.

## 2.2 Direct Proof

In this section we shall assume that you are familiar with the positive integers, or *natural numbers* (a detailed treatment of the natural numbers appears in Section 6.1). This number system $\{1, 2, 3, \ldots\}$ is denoted by the symbol $\mathbb{N}$. For now we will take the elementary arithmetic properties of $\mathbb{N}$ for granted. We shall formulate various statements about natural numbers and we shall prove them. Our methodology will emulate the discussions in earlier sections. We begin with a definition.

*DEFINITION 2.1* A natural number $n$ is said to be *even* if it can be divided by 2, with integer quotient and no remainder.

*DEFINITION 2.2* A natural number $n$ is said to be *odd* if, when it is divided by 2, the remainder is 1.

You may have never before considered, at this level of precision, what is the meaning of the terms "odd" or "even". But your intuition should confirm these definitions. A good definition should be precise, but it should also appeal to your heuristic idea about the concept that is being defined.

Notice that, according to these definitions, any natural number is either even or odd. For if $n$ is any natural number, and if we divide it by 2, then the remainder will be either 0 or 1—there is no other possibility (according to the Euclidean algorithm—see [HER]). In the first instance, $n$ is even; in the second, $n$ is odd.

In what follows we will find it convenient to think of an even natural number as one having the form $2m$ for some natural number $m$. We will think of an odd natural number as one having the form $2k - 1$ for some natural number $k$. Check for yourself that, in the first instance, division by 2 will result in a quotient of $m$ and a remainder of 0; in the second instance it will result in a quotient of $k - 1$ and a remainder of 1.

Now let us formulate a statement about the natural numbers and prove it. Following tradition, we refer to formal mathematical statements either as *theorems* or *propositions* or sometimes as *lemmas*. A theorem is supposed to be an important statement that is the culmination of some development of significant ideas. A proposition is a statement of lesser intrinsic importance.

Usually a lemma is of no intrinsic interest, but is needed as a step along the way to verifying a theorem or proposition.

*PROPOSITION 2.1*
*The square of an even natural number is even.*

**PROOF** Let us begin by using what we learned in Chapter 1. We may reformulate our statement as "If $n$ is even then $n \cdot n$ is even." This statement makes a promise. Refer to the definition of "even" to see what that promise is:

If $n$ can be written as twice a natural number then $n \cdot n$ can be written as twice a natural number.

The hypothesis of the assertion is that $n = 2 \cdot m$ for some natural number $m$. But then

$$n^2 = n \cdot n = (2m) \cdot (2m) = 4m^2 = 2(2m^2).$$

Our calculation shows that $n^2$ is twice the natural number $2m^2$. So $n^2$ is also even.

We have shown that the hypothesis that $n$ is twice a natural number entails the conclusion that $n^2$ is twice a natural number. In other words, if $n$ is even then $n^2$ is even. That is the end of our proof. ∎

**REMARK 2.2** What is the role of truth tables at this point? Why did we not use a truth table to verify our proposition? One *could* think of the statement that we are proving as the conjunction of infinitely many specific statements about concrete instances of the variable $n$; and then we could verify each one of those statements. But such a procedure is inelegant and, more importantly, impractical.

For our purpose, the truth table *tells us what we must do to construct a proof*. The truth table for $\mathbf{A} \Rightarrow \mathbf{B}$ shows that if $\mathbf{A}$ is false then there is nothing to check whereas if $\mathbf{A}$ is true then we must show that $\mathbf{B}$ is true. That is just what we did in the proof of Proposition 2.1.

Most of our theorems are "for all" statements or "there exists" statements. In practice, it is not usually possible to verify them directly by use of a truth table. ∎

*PROPOSITION 2.3*
*The square of an odd natural number is odd.*

**PROOF** We follow the paradigm laid down in the proof of the previous proposition.

Assume that $n$ is odd. Then $n = 2m - 1$ for some natural number $m$. But then

$$n^2 = n \cdot n = (2m-1) \cdot (2m-1) = 4m^2 - 4m + 1 = 2(2m^2 - 2m + 1) - 1.$$

We see that $n^2$ is $2m' - 1$, where $m' = 2m^2 - 2m + 1$. In other words, according to our definition, $n^2$ is odd. ∎

Both of the proofs that we have presented are examples of "direct proof." A direct proof proceeds according to the statement being proved; for instance, if we are proving a statement about a square then we calculate that square. If we are proving a statement about a sum then we calculate that sum. Here are some additional examples:

**Example 2.3**
Prove that if $n$ is a positive integer, then the quantity $n^2 + 3n + 2$ is even.

**Proof:** Denote the quantity $n^2 + 3n + 2$ by $K$. Observe that

$$K = n^2 + 3n + 2 = (n+1)(n+2).$$

Thus $K$ is the product of two successive integers: $n + 1$ and $n + 2$. One of those two integers must be even. So it is a multiple of 2. Therefore $K$ itself is a multiple of 2. Hence $K$ must be even. □

*PROPOSITION 2.4*
*The sum of two odd natural numbers is even.*

**PROOF** Suppose that $p$ and $q$ are both odd natural numbers. According to the definition, we may write $p = 2r - 1$ and $q = 2s - 1$ for some natural numbers $r$ and $s$. Then

$$p + q = (2r - 1) + (2s - 1) = 2r + 2s - 2 = 2(r + s - 1).$$

We have realized $p + q$ as twice the natural number $r + s - 1$. Therefore $p + q$ is even. ∎

**REMARK 2.5** If we did mathematics solely according to what sounds good, or what appeals intuitively, then we might reason as follows: "If the sum of two odd natural numbers is even then it must be that the sum of two even natural numbers is odd." This is incorrect. For instance 4 and 6 are each even but their sum $4 + 6 = 10$ is *not* odd.

Intuition definitely plays an important role in the development of mathematics, but all assertions in mathematics must, in the end, be proved by rigorous methods. ∎

**Example 2.4**
Prove that the sum of an even integer and an odd integer is odd.

**Proof:** An even integer is divisible by 2, so may be written in the form $e = 2m$, where $m$ is an integer. An odd integer has remainder 1 when divided by 2, so may be written in the form $o = 2k + 1$, where $k$ is an integer. The sum of these is

$$e + o = 2m + (2k + 1) = 2(m + k) + 1 .$$

Thus we see that the sum of an even and an odd integer will have remainder 1 when it is divided by 2. As a result, the sum is odd. □

*PROPOSITION 2.6*
*The sum of two even natural numbers is even.*

**PROOF** Let $p = 2r$ and $q = 2s$ both be even natural numbers. Then

$$p + q = 2r + 2s = 2(r + s).$$

We have realized $p + q$ as twice a natural number. Therefore we conclude that $p + q$ is even. ∎

*PROPOSITION 2.7*
*Let $n$ be a natural number. Then either $n > 6$ or $n < 9$.*

**PROOF** If you draw a picture of a number line then you will have no trouble convincing yourself of the truth of the assertion. What we want to learn here is to organize our thoughts so that we may write down a rigorous proof.

Our discussion of the connective "or" in Section 1.3 will now come to our aid. Fix a natural number $n$. If $n > 6$ then the "or" statement is true and there is nothing to prove. If $n \not> 6$, then the truth table teaches us that we must check that $n < 9$. But the statement $n \not> 6$ means that $n \leq 6$ so we have

$$n \leq 6 < 9.$$

That is what we wished to prove. ∎

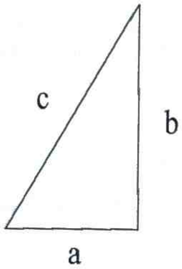


Figure 1

**Example 2.5**
Prove that every even integer may be written as the sum of two odd integers.

**Proof:** Let the even integer be $K = 2m$, for $m$ an integer. If $m$ is odd then we write

$$K = 2m = m + m$$

and we have written $K$ as the sum of two odd integers. If, instead, $m$ is even, then we write

$$K = 2m = (m - 1) + (m + 1) .$$

Since $m$ is even then both $m - 1$ and $m + 1$ are odd. So again we have written $K$ as the sum of two odd integers. □

**Example 2.6**
Prove the Pythagorean theorem.

**Proof:** The Pythagorean theorem states that $c^2 = a^2 + b^2$, where $a$ and $b$ are the legs of a right triangle and $c$ is its hypotenuse. See Figure 1.

Consider now the arrangement of four triangles and a square shown in Figure 2. Each of the four triangles is a copy of the original triangle in Figure 1. We see that each side of the all-encompassing square is equal to $c$. So the area of that square is $c^2$. Now each of the component triangles has base $a$ and height $b$. So each such triangle has area $ab/2$. And the little square in the middle has side $b - a$. So it has area $(b - a)^2 = b^2 - 2ab + a^2$. We write the total area as the sum of its component areas:

$$c^2 = 4 \cdot \left[\frac{ab}{2}\right] + [b^2 - 2ab + a^2] = a^2 + b^2 .$$

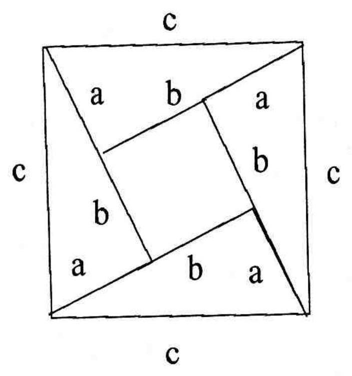


Figure 2

That is the desired equality.

□

In this section and the next two we are concerned with form rather than substance. We are not interested in proving anything profound, but rather in showing you what a proof looks like. Later in the book we shall consider some deeper mathematical ideas and correspondingly more profound proofs.

## 2.3 Proof by Contradiction

Aristotelian logic dictates that every sensible statement has a truth value: TRUE or FALSE. If we can demonstrate that a statement **A** could not possibly be false, then it must be true. On the other hand, if we can demonstrate that **A** could not be true, then it must be false. Here is a dramatic example of this principle. In order to present it, we shall assume for the moment that you are familiar with the system $\mathbb{Q}$ of rational numbers. These are numbers that may be written as the quotient of two integers (without dividing by zero, of course).

*THEOREM 2.8 PYTHAGORAS*

*There is no rational number $x$ with the property that $x^2 = 2$.*

**PROOF** In symbols (refer to Chapter 1), our assertion may be written

$$\sim \big(\exists x, (x \in \mathbb{Q} \wedge x^2 = 2)\big).$$

Let us assume the statement to be false. Then what we are assuming is that

$$\exists x, (x \in \mathbb{Q} \wedge x^2 = 2). \qquad (*)$$

Since $x$ is rational we may write $x = p/q$, where $p$ and $q$ are integers.

We may as well suppose that both $p$ and $q$ are positive and non-zero. After reducing the fraction, we may suppose that it is in lowest terms—so $p$ and $q$ have no common factors.

Now our hypothesis asserts that

$$x^2 = 2$$

or

$$\left(\frac{p}{q}\right)^2 = 2.$$

We may write this out as

$$p^2 = 2q^2. \qquad (**)$$

Observe that this equation asserts that $p^2$ is an even number. But then $p$ must be an even number ($p$ cannot be odd, for that would imply that $p^2$ is odd by Proposition 2.3). So $p = 2r$ for some natural number $r$.

Substituting this assertion into equation $(**)$ now yields that

$$(2r)^2 = 2q^2.$$

Simplifying, we may rewrite our equation as

$$2r^2 = q^2.$$

This new equation asserts that $q^2$ is even. But then $q$ itself must be even.

We have proven that both $p$ and $q$ are even. But that means that they have a common factor of 2. This contradicts our starting assumption that $p$ and $q$ have no common factor.

Let us pause to ascertain what we have established: the assumption that a rational square root $x$ of 2 exists, and that it has been written in lowest terms as $x = p/q$, leads to the conclusion that $p$ and $q$ have a common factor and hence are *not* in lowest terms. What does this entail for our logical system?

We cannot allow a statement of the form $\mathbf{C} = \mathbf{A} \wedge \sim \mathbf{A}$ (in the present context the statement $\mathbf{A}$ is "$x = p/q$ in lowest terms"). For such a statement $\mathbf{C}$ must be false.

But if $x$ exists then the statement $\mathbf{C}$ is true. No statement (such as $\mathbf{A}$) can have two truth values. In other words, the statement $\mathbf{C}$ must be false. The only possible conclusion is that $x$ does not exist. That is what we wished to establish. ∎

**REMARK 2.9** In practice, we do not include the last three paragraphs in a proof by contradiction. We provide them now because this is our first exposure to such a proof, and we want to make the reasoning absolutely clear. The point is that the assertions **A** and $\sim$ **A** cannot both be true. An assumption that leads to this eventuality cannot be valid. That is the essence of proof by contradiction. ▮

Historically, Theorem 2.8 was extremely important. Prior to Pythagoras ($\sim$ 300 B.C.), the ancient Greeks (following Eudoxus) believed that all numbers (at least all numbers that arise in real life) are rational. However, by the Pythagorean theorem, the length of the diagonal of a unit square is a number whose square is 2. And our theorem asserts that such a number cannot be rational. We now know that there are many non-rational, or irrational, numbers. In fact in Section 4.5 we shall learn that, in a certain sense to be made precise, "most" numbers are irrational.

Here is a second example of a proof by contradiction:

*THEOREM 2.10 DIRICHLET*
*Suppose that $n+1$ pieces of mail are delivered to $n$ mailboxes. Then some mailbox contains at least two pieces of mail.*

**PROOF** Suppose that the assertion is false. Then each mailbox contains either zero or one piece of mail. But then the total amount of mail in all the mailboxes cannot exceed

$$\underbrace{1+1+\cdots+1}_{n \text{ times}}.$$

In other words, there are at most $n$ pieces of mail. That conclusion contradicts the fact that there are $n+1$ pieces of mail. We conclude that some mailbox contains at least two pieces of mail. ▮

The last theorem, due to Gustav Lejeune Dirichlet (1805-1859), was classically known as the *Dirichletscher Schubfachschluss.* This German name translates to "Dirichlet's drawer shutting principle." Today, at least in this country, it is more commonly known as "the pigeonhole principle." Since pigeonholes are no longer a common artifact of everyday life, we have illustrated the idea using mailboxes.

**Example 2.7**

Draw the unit interval $I$ in the real line. Now pick 11 points at random from that interval (imagine throwing darts at the interval, or dropping ink drops on the interval). Then some pair of the points has distance not greater than .1 inch.

To see this, write

$$I = [0, .1] \cup [.1, .2] \cup \cdots [.8, .9] \cup [.9, 1].$$

Here we have used standard interval notation. Think of each of these subintervals as a mailbox. We are delivering 11 letters (that is, the randomly selected points) to these ten mailboxes. By the pigeonhole principle, some mailbox must receive two letters.

We conclude that some subinterval of $I$, having length .1, contains two of the randomly selected points. Thus their distance does not exceed .1 inch. $\square$

## 2.4 Proof by Induction

The logical validity of the method of proof by induction is intimately bound up with the construction of the natural numbers, with ordinal arithmetic, and with the so-called well ordering principle (see Section 6.1). However the topic fits naturally into the present chapter. So we shall present and illustrate the method, and worry about its logical foundations later on. As with any good idea in mathematics, we shall be able to make it intuitively clear that the method is a valid and useful one. So no confusion should result.

Consider a statement $P(n)$ about the natural numbers. For example, the statement might be "The quantity $n^2 + 5n + 6$ is always even." If we wish to prove this statement, we might proceed as follows:

*1.* Prove the statement $P(1)$.

*2.* Prove that $P(k) \Rightarrow P(k+1)$ for every $k \in \{1, 2, \ldots\}$.

Let us apply the syllogism *modus ponendo ponens* from the end of Section 1.5 to determine what we will have accomplished. We know $P(1)$ and, from (2) with $k = 1$, that $P(1) \Rightarrow P(2)$. We may therefore conclude $P(2)$. Now (2) with $k = 2$ says that $P(2) \Rightarrow P(3)$. We may then conclude $P(3)$. Continuing in this fashion, we may establish $P(n)$ for every natural number $n$.

Notice that this reasoning applies to any statement $P(n)$ for which we can establish (1) and (2) above. Thus (1) and (2) taken together constitute a method of proof. It is a method of establishing a statement $P(n)$ for every natural number $n$. The method is known as *proof by induction.*

**Example 2.8**
Let us use the method of induction to prove that, for every natural number $n$, the number $n^2 + 5n + 6$ is even.
**Solution:** Our statement $P(n)$ is

The number $n^2 + 5n + 6$ is even.

[*Note:* Explicitly identifying $P(n)$ is more than a formality, as Exercise 2.16 shows. *Always* record carefully what $P(n)$ is before proceeding.]
We now proceed in two steps:

**P(1) is true.** When $n = 1$ then

$$n^2 + 5n + 6 = 1^2 + 5 \cdot 1 + 6 = 12,$$

and this is certainly even. We have verified $P(1)$.

**P(n) ⇒ P(n+1).** We are proving an implication in this step. We *assume* $P(n)$ and *use it* to establish $P(n+1)$. Thus we are assuming that

$$n^2 + 5n + 6 = 2m$$

for some natural number $m$. Then, to check $P(n+1)$, we calculate

$$\begin{aligned}(n+1)^2 + 5(n+1) + 6 &= [n^2 + 2n + 1] + [5n + 5] + 6 \\ &= [n^2 + 5n + 6] + [2n + 6] \\ &= 2m + [2n + 6].\end{aligned}$$

Notice that in the last step we have *used our hypothesis* that $n^2 + 5n + 6$ is even, that is that $n^2 + 5n + 6 = 2m$. Now the last line may be rewritten as

$$2(m + n + 3).$$

Thus we see that $(n+1)^2+5(n+1)+6$ is twice the natural number $m+n+3$. In other words, $(n+1)^2 + 5(n+1) + 6$ is even. But that is the assertion $P(n+1)$.
In summary, assuming the assertion $P(n)$, we have established the assertion $P(n+1)$. That completes Step (2) of the method of induction. We conclude that $P(n)$ is true for every $n$. □

Here is another example to illustrate the method of induction.

*PROPOSITION 2.11*

*If $n$ is any natural number then*

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

**PROOF** The statement $P(n)$ is

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

Now let us follow the method of induction closely.

**P(1) is true.** The statement $P(1)$ is

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

This is plainly true.

$\mathbf{P(n)\Rightarrow P(n+1)}$. We are proving an implication in this step. We *assume* $P(n)$ and *use it* to establish $P(n+1)$. Thus we are assuming that

$$1+2+\cdots+n=\frac{n(n+1)}{2}. \qquad (*)$$

Let us add the quantity $(n+1)$ to both sides of $(*)$. We obtain

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

The left side of this last equation is exactly the left side of $P(n+1)$ that we are trying to establish. That is the motivation for our last step.

Now the right hand side may be rewritten as

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

This simplifies to

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

In conclusion, we have established that

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

This is the statement $P(n+1)$.

Assuming the validity of $P(n)$, we have proved the validity of $P(n+1)$. That completes the second step of the method of induction and establishes $P(n)$ for all $n$. ∎

Some problems are formulated in such a way that it is convenient to begin the induction with some value of $n$ other than $n = 1$. The next example illustrates this notion:

**Example 2.9**
Let us prove that, for $n \geq 4$, we have the inequality

$$3^n > 2n^2 + 3n.$$

**Solution:** The statement $P(n)$ is

$$3^n > 2n^2 + 3n.$$

**P(4) is true.** Observe that the inequality is false for $n = 1, 2, 3$. However for $n = 4$ it is certainly the case that

$$3^4 > 2 \cdot 4^2 + 3 \cdot 4.$$

$\mathbf{P(n) \Rightarrow P(n+1)}$. Now assume that $P(n)$ has been established and let us use it to prove $P(n+1)$. We are hypothesizing that

$$3^n > 2n^2 + 3n.$$

Multiplying both sides by 3 gives

$$3 \cdot 3^n > 3(2n^2 + 3n)$$

or

$$3^{n+1} > 6n^2 + 9n.$$

But now we have

$$\begin{aligned} 3^{n+1} &> 6n^2 + 9n \\ &= 2(n^2 + 2n + n) + (4n^2 + 3n) \\ &> 2(n^2 + 2n + 1) + (3n + 3) \\ &= 2(n+1)^2 + 3(n+1). \end{aligned}$$

This inequality is just $P(n+1)$, as we wished to establish. That completes step two of the induction, and therefore completes the proof. □

We conclude this section by mentioning an alternative form of the induction paradigm which is sometimes called *complete mathematical induction* or *strong mathematical induction*.

*Complete Mathematical Induction:* Let $P$ be a function on the natural numbers. If

1. $P(1)$;
2. $[P(j) \text{ for all } j \leq n] \Rightarrow P(n+1)$ for every natural number $n$;

then $P(n)$ is true for every $n$.

It turns out that the complete induction principle is logically equivalent to the ordinary induction principle enunciated at the outset of this section. But in some instances strong induction is the more useful tool. An alternative terminology for complete induction is "the set formulation of induction".

Complete induction is sometimes more convenient, or more natural, to use than ordinary induction; it finds particular use in abstract algebra. Complete induction also is a simple instance of transfinite induction, which we shall discuss later.

**Example 2.10**
**Theorem:** Every integer greater than 1 is either prime or the product of primes. [Here a prime number is an integer whose only factors are 1 and itself.]

**Proof:** We will use strong induction, just to illustrate the idea. For convenience we begin the induction process at the index 2 rather than at 1.

Let $P(n)$ be the assertion "Either $n$ is prime or $n$ is the product of primes." Then $P(2)$ is plainly true since 2 is the first prime. Now assume that $P(k)$ is true for $2 \leq k \leq n$ and consider $P(n+1)$. If $n+1$ is prime then we are done. If $n+1$ is not prime then $n+1$ factors as $n+1 = k \cdot \ell$, where $k, \ell$ are integers less than $n+1$, but at least 2. By the strong inductive hypothesis, each of $k$ and $\ell$ factors as a product of primes (or is itself a prime). Thus $n+1$ factors as a product of primes.

The complete induction is done, and the proof is complete. $\square$

## 2.5 Other Methods of Proof

We give here a number of examples that illustrate proof techniques other than direct proof, proof by contradiction, and induction.

## Counting Arguments

**Example 2.11**
Show that if there are 23 people in a room then the odds are better than even that two of them have the same birthday.

**Proof:** The best strategy is to calculate the odds that *no two* of the people have the same birthday, and then to take complements.

Let us label the people $p_1, p_2, \ldots, p_{23}$. Then, assuming that none of the $p_j$ have the same birthday, we see that $p_1$ can have his birthday on any of the 365 days in the year, $p_2$ can then have his birthday on any of the remaining 364 days, $p_3$ can have his birthday on any of the remaining 363 days, and so forth. So the number of different ways that these 23 people can all have different birthdays is

$$365 \cdot 364 \cdot 363 \cdots 345 \cdot 344 \cdot 343 .$$

On the other hand, the number of ways that birthdays could be distributed (with no restrictions) among 23 people is

$$\underbrace{365 \cdot 365 \cdot 365 \cdots 365}_{\text{23 times}} = 365^{23} .$$

Thus the probability that these 23 people all have different birthdays is

$$p = \frac{365 \cdot 364 \cdot 363 \cdots 343}{365^{23}} .$$

A quick calculation with a pocket calculator shows that $p \sim 0.4927 < .5$. That is the desired result. $\square$

**Example 2.12**
Show that if there are six people in a room then either three of them know each other or three of them do not know each other. [Here three people know each other if each of the three pairs has met. Three people do not know each other if each of the three pairs has *not* met.]

**Proof:** The tedious way to do this problem is to write out all possible "acquaintance assignments" for fifteen people.

We now describe a more efficient, and more satisfying, strategy. Call one of the people Bob. There are five others. Either Bob knows three of them, or he does not know three of them.

Say that Bob knows three of the others. If any two of those three are acquainted, then those two and Bob form a mutually acquainted threesome. If no two of those three know each other, then those three are a mutually unacquainted threesome.

Now suppose that Bob does not know three of the others. If any two of those three are unacquainted, then those two and Bob form an unacquainted threesome. If all pairs among the three are instead acquainted, then those three form a mutually acquainted threesome.

We have covered all possibilities, and in every instance come up either with a mutually acquainted threesome or a mutually unacquainted threesome. That ends the proof. □

It may be worth knowing that five people are insufficient to guarantee either a mutually acquainted threesome or a mutually unacquainted threesome. We leave it to the reader to provide a suitable counterexample. It is quite difficult to determine the minimal number of people to solve the problem when "threesome" is replaced by "foursome". When "foursome" is replaced by five people, the problem is considered to be grossly intractable. This problem is a simple example from the mathematical subject known as Ramsey theory.

**Example 2.13**
Jill is dealt a poker hand of five cards from a standard deck of 52. What is the probability that she holds four of a kind?

**Proof:** If the hand holds four aces, then the fifth card is any one of the other 48 cards. If the hand holds four kings, then the fifth card is any one of the other 48 cards. And so forth. So there are a total of

$$13 \times 48 = 624$$

possible hands with four of a kind. The total number of possible five-card hands is

$$\binom{52}{5} = 2598960\,.$$

Therefore the probability of holding four of a kind is

$$p = \frac{624}{2598960} = 0.00024\,.$$

□

**Example 2.14**

Let us show that there exist irrational numbers $a$ and $b$ such that $a^b$ is rational.

Let $\alpha = \sqrt{2}$ and $\beta = \sqrt{2}$. If $\alpha^\beta$ is rational then we are done, using $a = \alpha$ and $b = \beta$. If $\alpha^\beta$ is irrational, then observe that

$$\alpha^{\beta^{\sqrt{2}}} = \alpha^{[\beta \cdot \sqrt{2}]} = \alpha^2 = [\sqrt{2}]^2 = 2 .$$

Thus, with $a = \alpha^\beta$ and $b = \sqrt{2}$ we have found two irrational numbers $a, b$ such that $a^b = 2$ is rational. □

---

## Exercises

2.1 Prove that the product of two odd natural numbers must be odd.

2.2 Prove that if $n$ is an even natural number and if $m$ is *any* natural number then $n \cdot m$ must be even.

2.3 Prove that the sum of the squares of the first $n$ natural numbers is equal to

$$\frac{2n^3 + 3n^2 + n}{6}.$$

2.4 Prove that the sum of the first $k$ even natural numbers is $k^2 + k$.

2.5 Prove that the sum of the first $k$ odd natural numbers is $k^2$.

2.6 Prove that if $n$ red letters and $n$ blue letters are distributed among $n$ mailboxes then either some mailbox contains at least two red letters or some mailbox contains at least two blue letters or else some mailbox contains at least one red and one blue letter.

2.7 Prove that if $m$ is a power of 3 and $n$ is a power of 3 then $m + n$ is never a power of 3.

2.8 What is special about the number 3 in Exercise 2.7? What other natural numbers can be used in its place?

2.9 Imitate the proof of Pythagoras's theorem to show that the number 5 does not have a rational square root.

2.10 Prove that if $n$ is a natural number and if $n$ has a rational square root then in fact the square root of $n$ is an integer.

2.11 Complete this sketch to obtain an alternative proof that the number 2 does not have a rational square root:

(a) Take it for granted that it is known that each positive integer has one and only one factorization into prime factors (a prime number is a positive integer, greater than 1, that can be divided evenly only by 1 and itself).