2

Induction and the Division Theorem

2.1 The Method of Induction

In the Introduction we discussed a mathematical problem whose solution required the verification of an infinite family of statements. We needed to show, for each integer $n > 43$, that by ordering a suitable number of Chicken McNugget boxes of size 6, 9, or 20 we can buy n Chicken McNuggets. Equivalently, we needed to show that each integer $n > 43$ is $(6, 9, 20)$-accessible. This is an infinite family of statements: 44 is $(6, 9, 20)$-accessible, 45 is $(6, 9, 20)$-accessible, 46 is $(6, 9, 20)$-accessible, 47 is $(6, 9, 20)$-accessible, and so on.

The Chicken McNugget problem is typical of a number of mathematical problems in that the solution consists of an infinite family of statements, indexed by the integers n larger than some fixed integer N. An important means of handling such statements is the *principle of mathematical induction*. We did not discuss this principle explicitly in our treatment of the Chicken McNugget problem, but it was used implicitly, as will become evident. Let us introduce additional problems whose solution can be regarded as an infinite family of statements, and see by example how induction is used.

We begin with the problem of adding all the integers from 1 to a given positive integer n. This problem figures in a familiar story about the childhood of Carl Friedrich Gauss, one of the greatest mathematicians in history. Gauss lived from 1777 to 1855. If you have studied physics, you may be familiar with his name as the unit of measurement of magnetic field strength. In the story, which may be apocryphal, a schoolteacher asked Gauss's class one day to add all the integers from 1 to 100. As the story goes, the teacher did this not because of the mathematical interest of the problem but in order to keep the students busy. To the teacher's astonishment, Gauss produced the correct answer almost instantly.

Gauss may have answered the question by performing addition quickly, but more likely he knew a formula for the sum of all the numbers from 1 to a positive integer n. Let us obtain such a formula ourselves, so we too can answer the teacher's question instantly.

Exercise 2.1. We wish to obtain, for each positive integer n, a formula for the sum of all the numbers from 1 to n. Let us begin by considering a different question that turns out to be simpler. Recall that an integer is *even* if it is divisible by 2 and *odd* otherwise. Thus an even integer can be written in the form $2n$ for some integer n, but an odd integer cannot.

1. Calculate the sums of the first few positive odd integers: 1, 1 + 3, 1 + 3 + 5, 1 + 3 + 5 + 7. Do you recognize the results as familiar numbers?
2. Guess a formula for the sum $1+3+5+\cdots+(2n-1)$ of the first n positive odd integers.
3. Now draw the following sequence of pictures: a single dot, a 2×2 array of four dots, a 3×3 array of 9 dots, and a 4×4 array of 16 dots. How many dots must you add to each array to obtain the next larger array?
4. Using these arrays, explain how each square is built by a sequence of odd numbers, and how this explains the formula that you have guessed.

Exercise 2.2. Suppose n is a positive integer.

1. What can you do to each of the numbers in the sum
$$1 + 3 + 5 + \cdots + (2n - 1)$$
in order to obtain the sum
$$2 + 4 + 6 + \cdots + 2n$$
of the first n positive even integers.
2. Using this idea, and your formula for the sum of the odd integers from 1 to $2n - 1$, obtain a formula for the sum $2 + 4 + 6 + \cdots + 2n$ of the even integers from 2 to $2n$.
3. Using the formula you just obtained for the sum of the first n even integers, perform a simple division to obtain a formula for the sum
$$1 + 2 + 3 + \cdots + n$$
of all the positive integers from 1 to n.
4. Using this formula, calculate Gauss's sum $1 + 2 + \cdots + 100$.

We have succeeded in finding a formula for the sum of the first n positive integers for every positive integer n. However, our approach required a bit of cleverness, and the argument in the last part of Exercise 2.1 is not entirely satisfactory.

Let us develop the notion of mathematical induction and then return to the sum formula. The technique of induction comes in handy when we have an infinite family of statements we wish to prove, one for each positive integer n. For instance, in the example above, the nth statement would say that the sum of the integers from 1 to n is $\left(n^2 + n\right)/2$; that is, the nth statement is the equality

$$1 + 2 + 3 + \cdots + n = \frac{n^2 + n}{2}.$$

The principle of mathematical induction gives us a way to proceed. We can think of it as a technique for climbing a *stairway to heaven*. Suppose there is such a stairway, starting on the ground. Let us label the ground level 0, and let us give each step above the ground a label as well, the first step being level 1, the second level 2, and so on. By climbing all the way to the top, if we can, we will reach heaven. To do so, we need a technique for *getting off the ground* and a technique for *continuing*:

1. First we want a technique that allows us to climb from the ground onto step 1. This is what is meant by "getting off the ground." Getting from the ground onto the first step may be easy, or it may not, depending on how high the step is.
2. Second, we want a technique that allows us to go from each step k to the next step $k + 1$. This is what is meant by "continuing."

Suppose we have these two techniques. Employing the first one, we can get onto step 1. Employing the second, we can get from step 1 to step 2. Employing the second technique again, we can get from step 2 to step 3. Employing it yet again, we can get from step 3 to step 4, and so on. Repeated use of the second technique should allow us to climb all the way to the top. The principle of mathematical induction states that this is true: If we have a technique for getting off the ground and a technique for continuing, we can climb all the way up the stairway and reach heaven.

Let us state this a bit more formally. Suppose we have a family of statements that we wish to prove, one for every positive integer n. Let us call the nth statement Statement(n). The principle of induction says that we can prove all these statements at once if we do the following:

1. First prove Statement(1).
2. Second, show that for every positive integer k, if Statement(k) holds, then so does Statement($k+1$). In doing this, we do not assume that we actually know that Statement(k) holds. We only *assume* it as a hypothesis in our attempt to prove Statement($k + 1$). Continuing the staircase metaphor, we do not assume that we can actually ever reach any of the particular steps $1, 2, 3, \ldots$. We only show that *if* we ever find ourselves on step k, *then* we can get to step $k + 1$.

Suppose we have performed both of these actions. From the first action, we know that Statement(1) is true. From the second action, it follows that Statement(2) is true. Since Statement(2) is true, it follows using the second action again that Statement(3) is true. Since Statement(3) is true, it follows using the second action yet again that Statement(4) is true. By continuing in this way, we can conclude that Statement(n) is true for every positive integer n. This is the method of mathematical induction.

It is important to realize that action one is as important as action two. We may be able to climb from any step of the stairway to the next, but if we cannot get onto the first step, our ability to climb the remaining steps is useless.

Let us use induction in some examples. First, we return to the problem of showing that

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

We had a geometric argument earlier, based on counting dots in square arrays, that was somewhat vague. In particular, it depended too much on intuition. Using induction, one could instead proceed as follows.

Theorem 2.1. *Let n be a positive integer. Then*

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

Proof. We have an infinite family of statements we wish to prove, one for each positive integer n. Statement 1 says that $1 = 1^2$, Statement 2 says that $1 + 3 = 2^2$, and so on. We wish to climb the stairway that says that these infinitely many statements are all true. To get off the ground, we must climb the first step, which means we must show that $1 = 1^2$. This is certainly true, and this obvious equality gets us on the first step successfully, with very little effort.

Suppose we find ourselves on step k. We wish to show that we can get to step $k + 1$. To be standing on step k means that the equality of the theorem is true for $n = k$:

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

In saying that we assume ourselves to be standing on step k we are saying that we can assume that statement k is true. What we must show next is that *under this assumption*, we can get to step $k + 1$. This means that we must show that the equality of the theorem holds for $n = k + 1$, *on the assumption that it holds for* $n = k$. The equality for $n = k + 1$ takes the form

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

which we obtain by substituting $k + 1$ for n.

Since $2(k + 1) - 1 = 2k + 1$, we can rewrite the last equality as

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

To review, we are *assuming* that the equality

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

is true, and we wish to show that the equality

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

is true on that assumption.

One way to proceed is to take the equality that we are assuming to be true and add the odd number $2k+1$ to both sides. We then get

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

But $k^2+2k+1=(k+1)^2$. Therefore,

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

which is exactly what we needed to prove. Thus we have shown that if the equality of the theorem holds when $n=k$, then it holds when $n=k+1$; if we can get to step k, we can get to step $k+1$. The principle of induction allows us to conclude that we have verified our desired statement for all values of n. We have climbed the stairway to heaven, and the proof is complete.

Exercise 2.3. Using the principle of mathematical induction, as above, prove that the following equalities hold for every positive integer n.

1. The sum of the first n integers:

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

2. The sum of the squares of the first n integers:

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

Sometimes a family of statements we wish to prove true is indexed by a sequence of integers that starts not with 1 but with another integer, such as 0 or 2 or 3. The principle of induction still works, with a slight modification. We first show that the lowest-numbered statement holds, and then show that if Statement(k) holds, then Statement($k+1$) holds.

Here is an example. Recall that for a positive integer n the symbol $n!$ (pronounced n *factorial*) represents the product

$$n\times(n-1)\times(n-2)\times\cdots\times 3\times 2\times 1.$$

For instance, 4!, or "four factorial," is the product $4\times 3\times 2\times 1$, which equals 24. Let us prove the following result by induction. Notice that the inequality of the theorem is false if n equals 1, 2, or 3.

Theorem 2.2. *For every integer $n\geq 4$, the inequality $n!>2^n$ holds.*

Proof. We will proceed in two stages, by induction. First we show that the desired inequality $n!>2^n$ holds for $n=4$. This is clear, since it is simply the statement that $24>16$, which is obviously true. We have gotten off the ground onto step number 4. For the second stage, suppose that for some $k\geq 4$,

the inequality $k! > 2^k$ holds. We wish to show that $(k+1)! > 2^{k+1}$. Since we are assuming that $k! > 2^k$ and since it is evident that $(k+1)! = (k+1) \times k!$, we may conclude that

$$(k+1)! = (k+1) \times k! > (k+1) \times 2^k.$$

But since k is at least 4, the number $k+1$ is certainly greater than 2. Hence

$$(k+1) \times 2^k > 2 \times 2^k = 2^{k+1}.$$

Stringing the two sequences of equalities and inequalities together, we conclude that $(k+1)! > 2^{k+1}$, as desired. By the principle of induction, we can conclude that for every integer $n \geq 4$ we have the inequality $n! > 2^n$.

Exercise 2.4. Prove the two statements below:

1. For every integer $n \geq 3$, the inequality $n^2 > 2n + 1$ holds. (Hint: You can prove this by induction if you wish, but alternatively, you can prove it directly, without induction.)
2. For every integer $n \geq 5$, the inequality $2^n > n^2$ holds. (Hint: Use induction and the inequality in the previous part of the exercise.)

One must be careful in using induction that errors do not creep into the argument. Below is a statement and an attempted proof of the statement by induction.

Theorem 2.3. *All cats have the same color.*

Proof. We will show that for every collection of k cats there is a color such that all the cats in the collection have that color. Certainly this is true for $k = 1$: There is a color such that the single cat in the collection has that color. Suppose the statement is true for every collection of k cats and suppose you come upon a collection of $k + 1$ cats. You can line them up in a row and number them, so that cat 1 is on the left, cat 2 is next, and so on, with cat $k + 1$ on the right end. Consider the k cats to the left, cats 1 to k. By assumption, they all have the same color. Consider the k cats to the right, from 2 to $k + 1$. By assumption again, they all have the same color. But then cat 1 has the same color as the cats in the middle, but cat $k + 1$ also has the same color as the cats in the middle, and so all $k + 1$ cats have the same color. We have thus proved, by the principle of mathematical induction, that for every positive integer n, all the cats in a collection of n cats have the same color. Thus, all cats have the same color.

Exercise 2.5. Theorem 2.3 cannot be correct, so there must be an error in the proof. Study the proof, determine where the error lies, and explain what is wrong.

2.2 The Tower of Hanoi

Another illustration of the use of induction arises in analyzing the game called the Tower of Hanoi. There are infinitely many versions of the game, depending on the choice of a positive integer n. The game has three vertical poles, with n disks of different diameters initially stacked on one pole and the other two poles empty. The initial pile of n disks has the largest one at the bottom, the smallest at the top, and the disks in between arranged so that every disk is smaller than the disks below and larger than the disks above. The object of the game is to move the disks one by one from pole to pole, following the rule that no disk may be placed on top of a smaller disk, so that at the end one succeeds in transferring the pile from its initial pole to one of the initially empty poles. Doing so wins the game, or solves the n-disk puzzle.

A little experimentation with small values of n shows that you can solve the puzzle in one move if $n = 1$, in three moves if $n = 2$, and in seven moves if $n = 3$. For instance, with $n = 1$, there is only one disk, and you can simply move it in one step to another pole; with $n = 2$, you can move the smaller disk to pole 2, the larger disk to pole 3, and then the smaller disk to pole 3. You should work out solutions for $n = 3$, 4, and 5 at least, continuing further if you wish, going far enough so that you can make a guess about what is true in general. Do not read on until you have done so.

Did your evidence suggest anything? You might have guessed that for larger n, the puzzle can be solved in $2^n - 1$ moves. Let us verify this by induction, or by climbing the stairway to heaven.

Theorem 2.4. *For each positive integer n, the Tower of Hanoi puzzle with n disks can be solved in $2^n - 1$ moves.*

Proof. We have again an infinite family of statements we wish to prove, one for each positive integer n. Statement 1 says that the puzzle with 1 disk can be solved in $2^1 - 1$ $(= 1)$ move. Statement 2 says that the puzzle with 2 disks can be solved in $2^2 - 1$ moves, or 3 moves. Statement n says that the puzzle with n disks can be solved in $2^n - 1$ moves. The stairway we wish to climb this time is the stairway that says that these infinitely many statements are all true. To get off the ground, we must climb the first step, which means we must show that the puzzle with 1 disk can be solved in 1 move. We can show this just by doing it, as already discussed. This gets us on the first step successfully.

Suppose we have reached step k. We wish to show that we can get to step $k + 1$. To be on step k means that we are assuming that the puzzle with k disks can be solved in $2^k - 1$ moves. In saying that we suppose that we have reached step k, we are saying that we are assuming that statement k is true. What we must show next is that the puzzle with $k + 1$ disks can be solved in $2^{k+1} - 1$ steps *on the assumption that the puzzle with k disks can be solved in $2^k - 1$ steps.*

To proceed, imagine a three-stage approach to solving the $(k+1)$-disk puzzle. In stage one, we move the k smallest disks from the initial pole to another of the poles, which we will call the second pole, leaving the largest disk on the initial pole. Of course, we do this following the rules of the game, never placing a disk upon a smaller disk. In stage two, we move the largest disk to the remaining empty pole, the third pole. In stage three, we complete the solution by moving the k smallest disks, which currently lie on pole two, onto pole three atop the largest disk.

Let us count how many moves it will take for us to do each stage. The first stage, moving k disks from pole 1 to pole 2, is really a version of the k-disk puzzle. We are assuming that we can solve the k-disk puzzle in $2^k - 1$ moves. Hence we can complete the first stage in $2^k - 1$ moves. The second stage, moving the largest disk to pole three, takes one move. The third stage, moving k disks from pole 2 to pole 3, is another version of the k-disk puzzle. Therefore, like the first stage, it can be done in $2^k - 1$ moves. Adding together the $2^k - 1$ moves used for the first stage, the 1 move used for the second, and the $2^k - 1$ moves used for the third, we get a total of

$$\left(2^k - 1\right) + 1 + \left(2^k - 1\right)$$

moves, and this equals $2^{k+1} - 1$.

We have shown that *if* we can solve the k-puzzle in $2^k - 1$ moves, *then* we can solve the $(k+1)$-puzzle in $2^{k+1} - 1$ moves. Thus we have shown that if we can get to step k, we can get to step $k+1$. Since we have also shown that we can obviously get to step 1, the principle of induction allows us to conclude that we have verified our desired statement for all positive integer values of n, and the proof is complete. We have again climbed the stairway to heaven.

To illustrate induction again, let us prove another fact about the Tower of Hanoi puzzle. We have shown that the puzzle with n disks can be solved in $2^n - 1$ moves. Can it be solved in fewer moves? Again, experimentation with small values of n will suggest an answer: It cannot. This is clear for $n = 1$ and $n = 2$. Let us prove it in general.

Theorem 2.5. *For each positive integer n, the Tower of Hanoi puzzle with n disks requires at least $2^n - 1$ moves to be solved.*

Proof. Let Theorem(n) be the statement that the n-disk puzzle requires at least $2^n - 1$ moves to be solved. We will use induction to prove Theorem(n) for each positive integer n. To begin, we must show that Theorem(1) is true. This is the statement that at least one move is required to solve the 1-disk puzzle. Obviously, we cannot solve it with 0 moves; at least 1 move is needed. Thus Theorem(1) is true.

Next we will assume that for some positive integer k, Theorem(k) is true, and show that on that assumption Theorem($k+1$) holds. Theorem(k) states that at least $2^k - 1$ moves are required to solve the k-disk puzzle. This is what we are assuming.

To solve the $(k+1)$-disk puzzle, we must at some point move the largest disk from the initial pole to another pole. In order to do this, we must have already moved the k smallest disks off the largest disk onto the other two poles. If in doing so we split the k disks among the other two poles so each pole has some disk on it, we will not be allowed to move the largest disk, for it cannot be placed on a smaller disk. Thus we must in fact move all k smallest disks from the initial pole to a single other pole before we are free to move the largest disk to another pole. Moving these k disks is a version of the k-puzzle, which by the assumption of Theorem(k) requires at least $2^k - 1$ moves. After performing the necessary moves, we are free to move the largest disk to the vacant pole. This takes 1 move. To complete the puzzle in the fewest possible moves, we want to move onto the largest disk the k smallest disks, which are at this point on a single pole. This again requires at least $2^k - 1$ moves, by Theorem(k). Adding up, we see that we must make at least

$$\left(2^k - 1\right) + 1 + \left(2^k - 1\right)$$

moves to solve the $(k+1)$-puzzle. Since

$$2^k - 1 + 1 + 2^k - 1 = 2^{k+1} - 1,$$

we have proved that if we must make at least $2^k - 1$ moves to solve the k-disk puzzle, then we must make at least $2^{k+1} - 1$ moves to solve the $(k+1)$-disk puzzle. Thus, we have proved Theorem$(k+1)$ under the assumption of Theorem(k). The principle of induction allows us to conclude that we have verified Theorem(n) for all values of n.

Exercise 2.6. Let us introduce a modified version of the Tower of Hanoi game. We place the three poles in a straight line and make a new rule: A disk can be moved only from one pole to an adjacent pole. Suppose the goal of the modified game is to move the usual stack of n disks from a pole at one end to the pole at the other end.

1. Solve the modified puzzle for small values of n, and determine how many moves are required.
2. From these examples, guess a general formula for the number of moves needed to solve the puzzle.
3. Use induction to prove that the puzzle can be solved in the guessed number of moves.

2.3 The Division Theorem

With induction available as a method of proof, we can move on to the study of integers. Recall that an integer a is *divisible* by an integer n if there is another integer m such that $a = mn$. If an integer a is divisible by an integer n, we also say that n *divides* a. Let us begin with some simple facts about divisibility.

Theorem 2.6. *The following divisibility facts hold:*

1. *The integer* 0 *is divisible by every integer.*
2. *Suppose* n*,* a*, and* r *are integers, and* n *divides* a*. Then* n *divides* ra*.*
3. *Suppose* n*,* a*, and* b *are integers, and* n *divides both* a *and* b*. Then* n *divides* $a + b$ *and* $a - b$*.*
4. *Suppose* r *divides* s *and* s *divides* t*. Then* r *divides* t*.*

Proof. For the first part, for every integer r, we have $0 = r \cdot 0$. Thus 0 is divisible by r. For the second part, we can proceed as follows. Since n divides a, by definition there is an integer m such that $a = mn$. Therefore $ra = rmn$. Using the definition of divisibility again, we see that n divides ra.

Exercise 2.7. Prove the third and fourth parts of Theorem 2.6 above. Then use Theorem 2.6 to prove Theorem 2.7 below.

Theorem 2.7. *Suppose* a *and* b *are integers divisible by an integer* n*. Then the integer* $ra + sb$ *is also divisible by* n *for every pair of integers* r *and* s*.*

The key to solving the Chicken McNugget problem in the Introduction was the fact that if a positive integer is divided by 6, a remainder occurs of 0, 1, 2, 3, 4, or 5. This is a special case of a result that may seem so obvious it hardly requires discussion. Nonetheless, discuss it we will, for it underlies much of what we will do in the coming chapters. Let us lead up to it with a question.

Suppose you ask a class of students to do the division below and to state the quotient and the remainder:

$$397 \div 14.$$

If you do this yourself, you will quickly get an answer (what is it?), and you probably expect everyone in the class, assuming that no calculational errors are made, to obtain the same answer as yours. Suppose, however, that one student comes up with a quotient of 27 and a remainder of 19, another a quotient of 28 and a remainder of 5, and yet another a quotient of 26 and a remainder of 33. Are they all correct? It is true, after all, that

$$397 = (14 \times 27) + 19,$$

that

$$397 = (14 \times 28) + 5,$$

and that

$$397 = (14 \times 26) + 33.$$

After some thought, you realize that what is wrong with the answers of the first and third students is that their remainders are too big. The remainder should be smaller than the divisor. This is part of what we mean when we speak of a remainder.

Once everyone agrees on what a remainder is, is it true that the problem of obtaining a quotient and a remainder upon dividing one positive integer by another always has a solution, and is this solution unique? These are really two different questions. Let us begin with the first one. We want the following statement to be true, a statement called the division theorem.

Theorem 2.8 (Division Theorem). *For every two positive integers a and b, there exist nonnegative integers q and r, with $r < a$, such that*

$$b = aq + r.$$

The division theorem asserts the familiar fact that when we divide b by a, we get a nonnegative integer q as the quotient and a nonnegative integer r less than the divisor a as a remainder.

If we fix a to be a specific positive integer, then the division theorem becomes an infinite sequence of statements, one for each positive integer b. It guarantees that for each such b, when we divide b by the given a, a quotient q exists and a remainder r between 0 and $a - 1$ exists. For example, for $a = 6$, the division theorem states that for every positive integer b there exist nonnegative integers q and r, with $r < 6$, such that $b = 6q + r$. Thus when we divide b by 6, we get a quotient q and a remainder r, with r between 0 and 5. This is exactly the result we needed to solve the Chicken McNugget problem. Similarly, the division theorem for $a = 2$ and $a = 3$ underlay our solutions in the Introduction to the simpler nugget problems.

Exercise 2.8. Let us consider the division theorem in the special case $a = 2$.

1. Explain why the division theorem can be restated in this case as follows: For a positive integer b, there exists a nonnegative integer q such that either $b = 2q$ or $b = 2q + 1$.
2. As trivial as this result may seem, let us prove it, using induction. The statement we wish to prove is that every positive integer b can be written either as $2q$ or as $2q+1$ for some nonnegative integer q. Follow the outline below, using induction:
   (a) First show that 1 can be written in the desired form.
   (b) Now suppose an integer b that is greater than or equal to 1 can be written in the desired form. Show that $b + 1$ can also be so written. (Hint: There are two cases here, and they must be dealt with separately. First assume that b has the form $2q$ for some nonnegative integer q and show that $b+1$ can be written in the desired form. Then assume that b has the form $2q + 1$ for some nonnegative integer q and show that $b + 1$ can be written in the desired form.)
   (c) Conclude by the principle of induction that every positive integer b can be written as $2q$ or as $2q + 1$ for some nonnegative integer q.

Next let us see what the division theorem says in the special case that $a = 3$. This is more complicated than the $a = 2$ case.

Exercise 2.9. Explain why the division theorem for $a = 3$ can be restated as follows: For a positive integer b, there exists a nonnegative integer q such that b equals either $3q$, $3q + 1$, or $3q + 2$. Prove this result by induction, following the outline below:

1. First show that 1 can be written in the desired form.
2. Now suppose an integer b that is greater than or equal to 1 can be written in the desired form. Show that $b + 1$ can also be so written. (Hint: There would appear to be three cases here, depending on whether b has the form $3q$, $3q + 1$, or $3q + 2$, but really the first two can be combined into a single case. First assume that b has the form $3q$ or $3q + 1$ for some nonnegative integer q and show that $b + 1$ can be written in one of the three forms. Then assume that b has the form $3q + 2$ for some nonnegative integer q and show that $b + 1$ can be written in one of the three forms.)
3. Conclude by the principle of induction that every positive integer b can be written as $3q$, $3q + 1$, or $3q + 2$ for some nonnegative integer q.

These two examples serve as models for a proof of the division theorem in general.

Exercise 2.10. Prove the division theorem by induction. (Hint: Take a to be a fixed positive integer and let b vary. Prove the theorem for varying b by induction. First treat the case $b = 1$. Then assume that the theorem is true for a given b and show that it holds for $b + 1$.)

The division theorem can be strengthened by adding a statement about the uniqueness of q and r:

Theorem 2.9. *For positive integers a and b, there exists a unique choice of nonnegative integers q and r, with $r < a$, such that*

$$b = aq + r.$$

In Theorem 2.8 we merely asserted that q and r exist; in Theorem 2.9, we are asserting in addition that q and r are unique. What we mean by this is that only one choice of q and one choice of r will work, with the restrictions that q and r are nonnegative integers and that $r < a$. To prove this stronger version, we need only prove the uniqueness statement, since we already know that suitable q and r exist.

Let us discuss further what is meant by "unique." Suppose Ilya divides b by a and comes up with a quotient of q and a remainder of r, with q and r nonnegative and with $r < a$. Suppose Anya divides b by a and comes up with a quotient of s and a remainder of t, with s and t nonnegative integers and $t < a$. We hope that the answers of Ilya and Anya agree. In other words, we hope that Ilya's quotient q equals Anya's quotient s and Ilya's remainder r equals Anya's remainder t. That this must be the case is what uniqueness means. We can formulate this in the following more explicit form:

Theorem 2.10. *For positive integers a and b, suppose q and r are nonnegative integers with $r < a$ such that*

$$b = aq + r$$

and suppose also that s and t are nonnegative integers with $t < a$ such that

$$b = as + t.$$

Then $q = s$ and $r = t$.

Theorem 2.9 should be regarded as two statements, which we can call the existence statement and the uniqueness statement. Theorem 2.8 is the existence statement alone, Theorem 2.10 is the uniqueness statement alone, and Theorem 2.9 is the combination of Theorem 2.8 and Theorem 2.10.

Exercise 2.11. Prove Theorem 2.10. You may find the following outline useful.

1. Assume first that $r \leq t$, so that $t - r \geq 0$.
2. Observe that in this case $t - r < a$ and use the given equalities to show that a divides $t - r$.
3. Conclude, using the fact that $0 \leq t - r < a$, that $t - r = 0$ and $t = r$.
4. Deduce that $q = s$.
5. Assume next that $r \geq t$ and make a similar argument.
6. Conclude that since at least one of $r \leq t$ and $r \geq t$ is true, we have obtained the desired equalities.

http://www.springer.com/978-0-387-40397-7

Integers, Polynomials, and Rings
A Course in Algebra
Irving, R.S.
2004, XVI, 288 p., Hardcover
ISBN: 978-0-387-40397-7