4.4 Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Be especially critical of any statement following the word "obviously."
— Anna Pell Wheeler 1883–1966

When you divide 11 by 4, you get a quotient of 2 and a remainder of 3.

$$\begin{array}{r} 2 \leftarrow \text{quotient} \\ 4\overline{)\,11} \\ \underline{8} \\ 3 \leftarrow \text{remainder} \end{array}$$

Another way to say this is that 11 equals 2 groups of 4 with 3 left over:

$$\boxed{xxxx}\ \boxed{xxxx}\ xxx$$

2 groups of 4 — 3 left over

Or,

$$11 = 2 \cdot 4 + 3.$$

2 groups of 4 — 3 left over

Of course, the number left over (3) is less than the size of the groups (4) because if 4 or more were left over, another group of 4 could be separated off.

The quotient-remainder theorem says that when any integer n is divided by any positive integer d, the result is a quotient q and a nonnegative remainder r that is smaller than d.

Theorem 4.4.1 The Quotient-Remainder Theorem

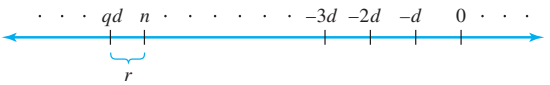
Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

The proof that there exist integers q and r with the given properties is in Section 5.4; the proof that q and r are unique is outlined in exercise 18 in Section 4.7.

If n is positive, the quotient-remainder theorem can be illustrated on the number line as follows:

If n is negative, the picture changes. Since $n = dq + r$, where r is nonnegative, d must be multiplied by a negative integer q to go below n. Then the nonnegative integer r is added to come back up to n. This is illustrated as follows:



Example 4.4.1 The Quotient-Remainder Theorem

For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

a. $n = 54,\ d = 4$ b. $n = -54,\ d = 4$ c. $n = 54,\ d = 70$

Solution

a. $54 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$.

b. $-54 = 4 \cdot (-14) + 2$; hence $q = -14$ and $r = 2$.

c. $54 = 70 \cdot 0 + 54$; hence $q = 0$ and $r = 54$. ■

div and mod

A number of computer languages have built-in functions that enable you to compute many values of q and r for the quotient-remainder theorem. These functions are called **div** and **mod** in Pascal, are called / and % in C and C++, are called / and % in Java, and are called / (or \) and **mod** in .NET. The functions give the values that satisfy the quotient-remainder theorem when a *nonnegative* integer n is divided by a positive integer d and the result is assigned to an integer variable. However, they do not give the values that satisfy the quotient-remainder theorem when a negative integer n is divided by a positive integer d.

• Definition

Given an integer n and a positive integer d,

$$\textbf{\textit{n div d}} = \text{the integer quotient obtained when } n \text{ is divided by } d, \text{ and}$$

$$\textbf{\textit{n mod d}} = \text{the nonnegative integer remainder obtained when } n \text{ is divided by } d.$$

Symbolically, if n and d are integers and $d > 0$, then

$$n \ div \ d = q \quad \text{and} \quad n \ \ mod \ \ d = r \quad \Leftrightarrow \quad n = dq + r$$

where q and r are integers and $0 \leq r < d$.

Note that it follows from the quotient-remainder theorem that $n \ mod \ d$ equals one of the integers from 0 through $d - 1$ (since the remainder of the division of n by d must be one of these integers). Note also that a necessary and sufficient condition for an integer n to be divisible by an integer d is that $n \ mod \ d = 0$. You are asked to prove this in the exercises at the end of this section.

You can also use a calculator to compute values of *div* and *mod*. For instance, to compute $n \ div \ d$ for a nonnegative integer n and a positive integer d, you just divide n by d and ignore the part of the answer to the right of the decimal point. To find $n \ mod \ d$, you can use the fact that if $n = dq + r$, then $r = n - dq$. Thus $n = d \cdot (n \ div \ d) + n \ mod \ d$, and so

$$n \ mod \ d = n - d \cdot (n \ div \ d).$$

Hence, to find $n \ mod \ d$ compute $n \ div \ d$, multiply by d, and subtract the result from n.

Example 4.4.2 Computing *div* and *mod*

Compute 32 *div* 9 and 32 *mod* 9 by hand and with a calculator.

Solution Performing the division by hand gives the following results:

$$\begin{array}{r} 3 \\ 9\overline{)\,32} \\ \underline{27} \\ 5 \end{array} \quad \begin{array}{l} \leftarrow 32\ div\ 9 \\ \\ \\ \leftarrow 32\ mod\ 9 \end{array}$$

If you use a four-function calculator to divide 32 by 9, you obtain an expression like 3.555555556. Discarding the fractional part gives $32\ div\ 9 = 3$, and so

$$32\ mod\ 9 = 32 - 9 \cdot (32\ div\ 9) = 32 - 27 = 5.$$

A calculator with a built-in integer-part function iPart allows you to input a single expression for each computation:

$$32\ div\ 9 = \text{iPart}(32/9)$$

and $$32\ mod\ 9 = 32 - 9 \cdot \text{iPart}\ (32/9) = 5.$$ ■

Example 4.4.3 Computing the Day of the Week

Suppose today is Tuesday, and neither this year nor next year is a leap year. What day of the week will it be 1 year from today?

Solution There are 365 days in a year that is not a leap year, and each week has 7 days. Now

$$365\ div\ 7 = 52 \quad \text{and} \quad 365\ mod\ 7 = 1$$

because $365 = 52 \cdot 7 + 1$. Thus 52 weeks, or 364 days, from today will be a Tuesday, and so 365 days from today will be 1 day later, namely Wednesday.

More generally, if *DayT* is the day of the week today and *DayN* is the day of the week in N days, then

$$DayN = (DayT + N)\ mod\ 7, \tag{4.4.1}$$

where Sunday $= 0$, Monday $= 1, \ldots,$ Saturday $= 6$. ■

Example 4.4.4 Solving a Problem about *mod*

Suppose m is an integer. If $m\ mod\ 11 = 6$, what is $4m\ mod\ 11$?

Solution Because $m\ mod\ 11 = 6$, the remainder obtained when m is divided by 11 is 6. This means that there is some integer q so that

$$m = 11q + 6.$$

Thus $$4m = 44q + 24 = 44q + 22 + 2 = 11(4q + 2) + 2.$$

Since $4q + 2$ is an integer (because products and sums of integers are integers) and since $2 < 11$, the remainder obtained when $4m$ is divided by 11 is 2. Therefore,

$$4m\ mod\ 11 = 2.$$ ■

Representations of Integers

In Section 4.1 we defined an even integer to have the form twice some integer. At that time we could have defined an odd integer to be one that was not even. Instead, because it was more useful for proving theorems, we specified that an odd integer has the form twice some integer plus one. The quotient-remainder theorem brings these two ways of describing odd integers together by guaranteeing that any integer is either even or odd. To see why, let n be any integer, and consider what happens when n is divided by 2. By the quotient-remainder theorem (with $d = 2$), there exist unique integers q and r such that

$$n = 2q + r \quad \text{and} \quad 0 \leq r < 2.$$

But the only integers that satisfy $0 \leq r < 2$ are $r = 0$ and $r = 1$. It follows that given any integer n, there exists an integer q with

$$n = 2q + 0 \quad \text{or} \quad n = 2q + 1.$$

In the case that $n = 2q + 0 = 2q$, n is even. In the case that $n = 2q + 1$, n is odd. Hence n is either even or odd, and, because of the uniqueness of q and r, n cannot be both even and odd.

The *parity* of an integer refers to whether the integer is even or odd. For instance, 5 has odd parity and 28 has even parity. We call the fact that any integer is either even or odd the **parity property.**

Example 4.4.5 Consecutive Integers Have Opposite Parity

Prove that given any two consecutive integers, one is even and the other is odd.

Solution Two integers are called *consecutive* if, and only if, one is one more than the other. So if one integer is m, the next consecutive integer is $m + 1$.

To prove the given statement, start by supposing that you have two particular but arbitrarily chosen consecutive integers. If the smaller is m, then the larger will be $m + 1$. How do you know for sure that one of these is even and the other is odd? You might imagine some examples: 4, 5; 12, 13; 1,073, 1,074. In the first two examples, the smaller of the two integers is even and the larger is odd; in the last example, it is the reverse. These observations suggest dividing the analysis into two cases.

Case 1: The smaller of the two integers is even.

Case 2: The smaller of the two integers is odd.

In the first case, when m is even, it appears that the next consecutive integer is odd. Is this always true? If an integer m is even, must $m + 1$ necessarily be odd? Of course the answer is yes. Because if m is even, then $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd.

In the second case, when m is odd, it appears that the next consecutive integer is even. Is this always true? If an integer m is odd, must $m + 1$ necessarily be even? Again, the answer is yes. For if m is odd, then $m = 2k + 1$ for some integer k, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$, which is even.

This discussion is summarized on the following page.

Theorem 4.4.2 The Parity Property

Any two consecutive integers have opposite parity.

Proof:

Suppose that two *[particular but arbitrarily chosen]* consecutive integers are given; call them m and $m + 1$. *[We must show that one of m and $m + 1$ is even and that the other is odd.]* By the parity property, either m is even or m is odd. *[We break the proof into two cases depending on whether m is even or odd.]*

Case 1 (m is even): In this case, $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd *[by definition of odd]*. Hence in this case, one of m and $m + 1$ is even and the other is odd.

Case 2 (m is odd): In this case, $m = 2k + 1$ for some integer k, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer, and thus $m + 1$ is even. Hence in this case also, one of m and $m + 1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular m and $m + 1$ that are chosen, one of m and $m + 1$ is even and the other is odd. *[This is what was to be shown.]*

■

The division into cases in a proof is like the transfer of control for an **if-then-else** statement in a computer program. If m is even, control transfers to case 1; if not, control transfers to case 2. For any given integer, only one of the cases will apply. You must consider both cases, however, to obtain a proof that is valid for an arbitrarily given integer whether even or not.

There are times when division into more than two cases is called for. Suppose that at some stage of developing a proof, you know that a statement of the form

$$A_1 \text{ or } A_2 \text{ or } A_3 \text{ or } \ldots \text{ or } A_n$$

is true, and suppose you want to deduce a conclusion C. By definition of *or,* you know that at least one of the statements A_i is true (although you may not know which). In this situation, you should use the method of division into cases. First assume A_1 is true and deduce C; next assume A_2 is true and deduce C; and so forth until you have assumed A_n is true and deduced C. At that point, you can conclude that regardless of which statement A_i happens to be true, the truth of C follows.

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or . . . or A_n, then C," prove all of the following:

If A_1, then C,
If A_2, then C,
⋮
If A_n, then C.

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Proof by division into cases is a generalization of the argument form shown in Example 2.3.7, whose validity you were asked to establish in exercise 21 of Section 2.3. This method of proof was combined with the quotient-remainder theorem for $d = 2$ to prove Theorem 4.4.2. Allowing d to take on additional values makes it possible to obtain a variety of other results. We begin by showing what happens when $a = 4$.

Example 4.4.6 Representations of Integers Modulo 4

Show that any integer can be written in one of the four forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q.

Solution Given any integer n, apply the quotient-remainder theorem to n with $d = 4$. This implies that there exist an integer quotient q and a remainder r such that

$$n = 4q + r \quad \text{and} \quad 0 \le r < 4.$$

But the only nonnegative remainders r that are less than 4 are 0, 1, 2, and 3. Hence

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q. ■

The next example illustrates how the alternative representations for integers modulo 4 can help establish a result in number theory. The solution is broken into two parts: a discussion and a formal proof. These correspond to the stages of actual proof development. Very few people, when asked to prove an unfamiliar theorem, immediately write down the kind of formal proof you find in a mathematics text. Most need to experiment with several possible approaches before they find one that works. A formal proof is much like the ending of a mystery story—the part in which the action of the story is systematically reviewed and all the loose ends are carefully tied together.

Example 4.4.7 The Square of an Odd Integer

Note Another way to state this fact is that if you square an odd integer and divide by 8, you will always get a remainder of 1. Try a few examples!

Prove: The square of any odd integer has the form $8m + 1$ for some integer m.

Solution Begin by asking yourself, "Where am I starting from?" and "What do I need to show?" To help answer these questions, introduce variables to represent the quantities in the statement to be proved.

Formal Restatement: $\forall$ odd integers n, $\exists$ an integer m such that $n^2 = 8m + 1$.

From this, you can immediately identify the starting point and what is to be shown.

Starting Point: Suppose n is a particular but arbitrarily chosen odd integer.

To Show: $\exists$ an integer m such that $n^2 = 8m + 1$.

This looks tough. Why should there be an integer m with the property that $n^2 = 8m + 1$? That would say that $(n^2 - 1)/8$ is an integer, or that 8 divides $n^2 - 1$. Perhaps you could make use of the fact that $n^2 - 1 = (n - 1)(n + 1)$. Does 8 divide $(n - 1)(n + 1)$? Since n is odd, both $(n - 1)$ and $(n + 1)$ are even. That means that their product is divisible by 4. But that's not enough. You need to show that the product is divisible by 8. This seems to be a blind alley.

You could try another tack. Since n is odd, you could represent n as $2q + 1$ for some integer q. Then $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$. It is clear from this

analysis that n^2 can be written in the form $4m + 1$, but it may not be clear that it can be written as $8m + 1$. This also seems to be a blind alley.*

Yet another possibility is to use the result of Example 4.4.6. That example showed that any integer can be written in one of the four forms $4q$, $4q + 1$, $4q + 2$, or $4q + 3$. Two of these, $4q + 1$ and $4q + 3$, are odd. Thus any odd integer can be written in the form $4q + 1$ or $4q + 3$ for some integer q. You could try breaking into cases based on these two different forms.

Note Desperation can spur creativity. When you have tried all the obvious approaches without success and you really care about solving a problem, you reach into the odd corners of your memory for *anything* that may help.

It turns out that this last possibility works! In each of the two cases, the conclusion follows readily by direct calculation. The details are shown in the following formal proof:

Theorem 4.4.3

The square of any odd integer has the form $8m + 1$ for some integer m.

Proof:

Suppose n is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem, n can be written in one of the forms

$$4q \quad \text{or} \quad 4q + 1 \quad \text{or} \quad 4q + 2 \quad \text{or} \quad 4q + 3$$

for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms

$$4q + 1 \quad \text{or} \quad 4q + 3.$$

Case 1 ($n = 4q + 1$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q + 1)^2 && \text{by substitution} \\ &= (4q + 1)(4q + 1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Case 2 ($n = 4q + 3$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{by substitution} \\ &= (4q + 3)(4q + 3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8 + 1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

[The motivation for the choice of algebra steps was the desire to write the expression in the form $8 \cdot$(some integer) $+ 1$.]

*See exercise 18 for a different perspective.

Let $m = 2q^2 + 3q + 1$. Then m is an integer since 1, 2, 3, and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. *[This is what we needed to show.]*

■

Note that the result of Theorem 4.4.3 can also be written, "For any odd integer n, n^2 *mod* $8 = 1$."

In general, according to the quotient-remainder theorem, if an integer n is divided by an integer d, the possible remainders are 0, 1, 2, . . ., $(d - 1)$. This implies that n can be written in one of the forms

$$dq,\ dq + 1,\ dq + 2,,\ \ldots,\ dq + (d - 1) \qquad \text{for some integer } q.$$

Many properties of integers can be obtained by giving d a variety of different values and analyzing the cases that result.

Absolute Value and the Triangle Inequality

The triangle inequality is one of the most important results involving absolute value. It has applications in many areas of mathematics.

• Definition

For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

The triangle inequality says that the absolute value of the sum of two numbers is less than or equal to the sum of their absolute values. We give a proof based on the following two facts, both of which are derived using division into cases. We state both as lemmas. A **lemma** is a statement that does not have much intrinsic interest but is helpful in deriving other results.

Lemma 4.4.4

For all real numbers r, $-|r| \leq r \leq |r|$.

Proof:

Suppose r is any real number. We divide into cases according to whether $r \geq 0$ or $r < 0$.

Case 1 ($r \geq 0$): In this case, by definition of absolute value, $|r| = r$. Also, since r is positive and $-|r|$ is negative, $-|r| < r$. Thus it is true that

$$-|r| \leq r \leq |r|.$$

continued on page 188

Case 2 ($r < 0$): In this case, by definition of absolute value, $|r| = -r$. Multiplying both sides by -1 gives that $-|r| = r$. Also, since r is negative and $|r|$ is positive, $r < |r|$. Thus it is also true in this case that

$$-|r| \leq r \leq |r|.$$

Hence, in either case,

$$-|r| \leq r \leq |r|$$

[as was to be shown].

Lemma 4.4.5

For all real numbers r, $|-r| = |r|$.

Proof:

Suppose r is any real number. By Theorem T23 in Appendix A, if $r > 0$, then $-r < 0$, and if $r < 0$, then $-r > 0$. Thus

$$|-r| = \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ -(-r) & \text{if } -r < 0 \end{cases} \quad \text{by definition of absolute value}$$

$$= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } -r < 0 \end{cases} \quad \text{because } -(-r) = r \text{ by Theorem T4 in Appendix A}$$

$$= \begin{cases} -r & \text{if } r < 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } r > 0 \end{cases} \quad \text{because, by Theorem T24 in Appendix A, when } -r > 0, \text{ then } r < 0, \text{ when } -r < 0, \text{ then } r > 0, \text{ and when } -r = 0, \text{ then } r = 0$$

$$= \begin{cases} r & \text{if } r \geq 0 \\ -r & \text{if } r < 0 \end{cases} \quad \text{by reformatting the previous result}$$

$$= |r| \quad \text{by definition of absolute value.}$$

Lemmas 4.4.4 and 4.4.5 now provide a basis for proving the triangle inequlity.

Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

Proof:

Suppose x and y, are any real numbers.

Case 1 ($x + y \geq 0$): In this case, $|x + y| = x + y$, and so, by Lemma 4.4.4,

$$x \leq |x| \quad \text{and} \quad y \leq |y|.$$

Hence, by Theorem T26 of Appendix A,

$$|x + y| = x + y \leq |x| + |y|.$$

Case 2 ($x + y < 0$): In this case, $|x + y| = -(x + y) = (-x) + (-y)$, and so, by Lemmas 4.4.4 and 4.4.5,

$$-x \leq |-x| = |x| \quad \text{and} \quad -y \leq |-y| = |y|.$$

It follows, by Theorem T26 of Appendix A, that

$$|x + y| = (-x) + (-y) \leq |x| + |y|.$$

Hence in both cases $|x + y| \leq |x| + |y|$ *[as was to be shown]*.

Test Yourself

1. The quotient-remainder theorem says that for all integers n and d with $d \geq 0$, there exist _____ q and r such that _____ and _____.
2. If n and d are integers with $d > 0$, n *div* d is _____ and n *mod* d is _____.
3. The parity of an integer indicates whether the integer is _____.
4. According to the quotient-remainder theorem, if an integer n is divided by a positive integer d, the possible remainders are _____. This implies that n can be written in one of the forms _____ for some integer q.
5. To prove a statement of the form "If A_1 or A_2 or A_3, then C," prove _____ and _____ and _____.
6. The triangle inequality says that for all real numbers x and y, _____.

Exercise Set 4.4

For each of the values of n and d given in 1–6, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

1. $n = 70, d = 9$ 2. $n = 62, d = 7$

3. $n = 36, d = 40$ 4. $n = 3, d = 11$

5. $n = -45, d = 11$ 6. $n = -27, d = 8$

Evaluate the expressions in 7–10.

7. a. 43 *div* 9 b. 43 *mod* 9

8. a. 50 *div* 7 b. 50 *mod* 7

9. a. 28 *div* 5 b. 28 *mod* 5

10. a. 30 *div* 2 b. 30 *mod* 2

11. Check the correctness of formula (4.4.1) given in Example 4.4.3 for the following values of *DayT* and *N*.
    a. *DayT* = 6 (Saturday) and $N = 15$
    b. *DayT* = 0 (Sunday) and $N = 7$
    c. *DayT* = 4 (Thursday) and $N = 12$

★ 12. Justify formula (4.4.1) for general values of *DayT* and *N*.

13. On a Monday a friend says he will meet you again in 30 days. What day of the week will that be?

***H* 14.** If today is Tuesday, what day of the week will it be 1,000 days from today?

15. January 1, 2000, was a Saturday, and 2000 was a leap year. What day of the week will January 1, 2050, be?

16. Suppose d is a positive integer and n is any integer. If $d \mid n$, what is the remainder obtained when the quotient-remainder theorem is applied to n with divisor d?

17. Prove that the product of any two consecutive integers is even.

18. The result of exercise 17 suggests that the second apparent blind alley in the discussion of Example 4.4.7 might not be a blind alley after all. Write a new proof of Theorem 4.4.3 based on this observation.

19. Prove that for all integers n, $n^2 - n + 3$ is odd.

20. Suppose a is an integer. If a *mod* 7 = 4, what is 5a *mod* 7? In other words, if division of a by 7 gives a remainder of 4, what is the remainder when 5a is divided by 7?

21. Suppose b is an integer. If b *mod* 12 = 5, what is 8b *mod* 12? In other words, if division of b by 12 gives a remainder of 5, what is the remainder when 8b is divided by 12?

22. Suppose c is an integer. If c *mod* 15 = 3, what is 10c *mod* 15? In other words, if division of c by 15 gives a remainder of 3, what is the remainder when 10c is divided by 15?

23. Prove that for all integers n, if n *mod* 5 = 3 then n^2 *mod* 5 = 4.

24. Prove that for all integers m and n, if m *mod* 5 = 2 and n *mod* 3 = 6 then mn *mod* 5 = 1.

25. Prove that for all integers a and b, if a *mod* 7 = 5 and b *mod* 7 = 6 then ab *mod* 7 = 2.

***H* 26.** Prove that a necessary and sufficient condition for a nonnegative integer n to be divisible by a positive integer d is that n *mod* $d = 0$.

27. Show that any integer n can be written in one of the three forms

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2$$

for some integer q.

28. a. Use the quotient-remainder theorem with $d = 3$ to prove that the product of any three consecutive integers is divisible by 3.

b. Use the *mod* notation to rewrite the result of part (a).

H 29. a. Use the quotient-remainder theorem with $d = 3$ to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.

b. Use the *mod* notation to rewrite the result of part (a).

30. a. Use the quotient-remainder theorem with $d = 3$ to prove that the product of any two consecutive integers has the form $3k$ or $3k + 2$ for some integer k.

b. Use the *mod* notation to rewrite the result of part (a).

In 31–33, you may use the properties listed in Example 4.2.3.

31. a. Prove that for all integers m and n, $m + n$ and $m - n$ are either both odd or both even.

b. Find all solutions to the equation $m^2 - n^2 = 56$ for which both m and n are positive integers.

c. Find all solutions to the equation $m^2 - n^2 = 88$ for which both m and n are positive integers.

32. Given any integers a, b, and c, if $a - b$ is even and $b - c$ is even, what can you say about the parity of $2a - (b + c)$? Prove your answer.

33. Given any integers a, b, and c, if $a - b$ is odd and $b - c$ is even, what can you say about the parity of $a - c$? Prove your answer.

H 34. Given any integer n, if $n > 3$, could n, $n + 2$, and $n + 4$ all be prime? Prove or give a counterexample.

Prove each of the statements in 35–46.

35. The fourth power of any integer has the form $8m$ or $8m + 1$ for some integer m.

H 36. The product of any four consecutive integers is divisible by 8.

37. The square of any integer has the form $4k$ or $4k + 1$ for some integer k.

H 38. For any integer n, $n^2 + 5$ is not divisible by 4.

H 39. The sum of any four consecutive integers has the form $4k + 2$ for some integer k.

40. For any integer n, $n(n^2 - 1)(n + 2)$ is divisible by 4.

41. For all integers m, $m^2 = 5k$, or $m^2 = 5k + 1$, or $m^2 = 5k + 4$ for some integer k.

H 42. Every prime number except 2 and 3 has the form $6q + 1$ or $6q + 5$ for some integer q.

43. If n is an odd integer, then n^4 *mod* $16 = 1$.

H 44. For all real numbers x and y, $|x| \cdot |y| = |xy|$.

45. For all real numbers r and c with $c \geq 0$, if $-c \leq r \leq c$, then $|r| \leq c$.

46. For all real numbers r and c with $c \geq 0$, if $|r| \leq c$, then $-c \leq r \leq c$.

47. A matrix $\mathbf{M}$ has 3 rows and 4 columns.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

The 12 entries in the matrix are to be stored in *row major* form in locations 7,609 to 7,620 in a computer's memory. This means that the entries in the first row (reading left to right) are stored first, then the entries in the second row, and finally the entries in the third row.

a. Which location will a_{22} be stored in?

b. Write a formula (in i and j) that gives the integer n so that a_{ij} is stored in location $7{,}609 + n$.

c. Find formulas (in n) for r and s so that a_{rs} is stored in location $7{,}609 + n$.

48. Let $\mathbf{M}$ be a matrix with m rows and n columns, and suppose that the entries of $\mathbf{M}$ are stored in a computer's memory in row major form (see exercise 47) in locations N, $N + 1$, $N + 2$, . . . , $N + mn - 1$. Find formulas in k for r and s so that a_{rs} is stored in location $N + k$.

★ 49. If m, n, and d are integers, $d > 0$, and m *mod* $d = n$ *mod* d, does it necessarily follow that $m = n$? That $m - n$ is divisible by d? Prove your answers.

★ 50. If m, n, and d are integers, $d > 0$, and $d \mid (m - n)$, what is the relation between m *mod* d and n *mod* d? Prove your answer.

★ 51. If m, n, a, b, and d are integers, $d > 0$, and m *mod* $d = a$ and n *mod* $d = b$, is $(m + n)$ *mod* $d = a + b$? Is $(m + n)$ *mod* $d = (a + b)$ *mod* d? Prove your answers.

★ 52. If m, n, a, b, and d are integers, $d > 0$, and m *mod* $d = a$ and n *mod* $d = b$, is (mn) *mod* $d = ab$? Is (mn) *mod* $d = ab$ *mod* d? Prove your answers.

53. Prove that if m, d, and k are integers and $d > 0$, then $(m + dk)$ *mod* $d = m$ *mod* d.

Answers for Test Yourself

1. integers; $n = dq + r$; $0 \leq r < d$ 2. the quotient obtained when n is divided by d; the nonnegative remainder obtained when n is divided by d 3. odd or even 4. 0, 1, 2, . . . , $(d - 1)$; dq, $dq + 1$, $dq + 2$, . . . , $dq + (d - 1)$ 5. If A_1, then C; If A_2, then C; If A_3, then C 6. $|x + y| \leq |x| + |y|$