CHAPTER 4

ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

4.5 Direct Proof and Counterexample V: Division into Cases and the Quotient-Remainder Theorem

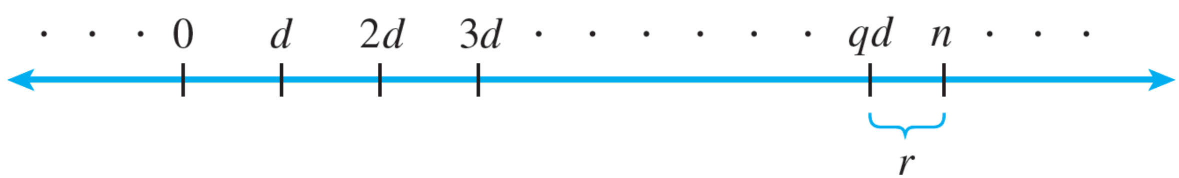
Direct Proof and Counterexample V: Division into Cases and the Quotient-Remainder Theorem

Theorem 4.5.1 The Quotient-Remainder Theorem

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

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

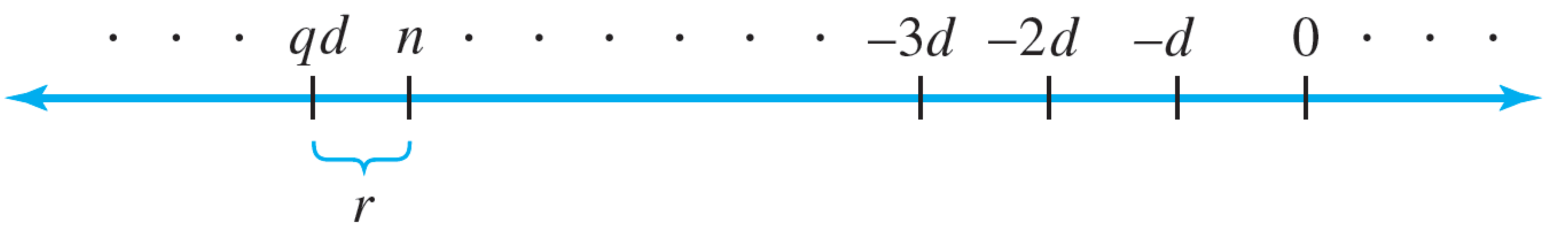
If *n* is positive, the quotient-remainder theorem can be illustrated on the number line as follows:



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

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 bring dq either exactly to n (in which case $r = 0$) or to a point below n (in which case the positive integer r is added to bring $dq + r$ back up to n).

This is illustrated as follows:



Example 4.5.1 – *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. $n = 54$, $d = 70$

Example 4.5.1 – *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

div and mod

Definition

Given an integer n and a positive integer d,

$$\begin{aligned} \boldsymbol{n\ div\ d} &= \text{the integer quotient obtained} \\ &\quad\ \text{when } n \text{ is divided by } d \text{, and} \\ \boldsymbol{n\ mod\ d} &= \text{the nonnegative integer remainder obtained} \\ &\quad\ \text{when } n \text{ is divided by } d. \end{aligned}$$

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 $0 \leq r < d$.

Example 4.5.2 – *Computing div and mod by Hand or with a Four-Function Calculator*

Compute 32 *div* 9 and 32 *mod* 9 by hand or with a four-function calculator.

Example 4.5.2 – *Solution*

Performing the division by hand gives the following results:

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

To use a four-function calculator to compute *n div d* for a nonnegative integer *n* and a positive integer *d*, just divide *n* by *d* and ignore the part of the answer to the right of the decimal point.

Example 4.5.2 – *Solution*

continued

To compute *n mod d*, substitute *n div d* in place of *q* and *n mod d* in place of *r* in the equation $n = dq + r$. The result is

$$n = d \cdot (n \textit{ div } d) + n \textit{ mod } d.$$

Solving for *n mod d* gives

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

Thus, when 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

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

Example 4.5.4 – *Solving Problems about mod*

a. Prove that if n is a positive integer, then n *mod* 10 is the digit in the ones place in the decimal representation for n.

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

Example 4.5.4 – *Solution*

a. **Proof:** Suppose n is any positive integer. The decimal representation for n is $d_k\, d_{k-1} \ldots d_2\, d_1\, d_0$, where $d_0, d_1, d_2, \ldots, d_k$ are integers from 0 to 9 inclusive, $d_k \neq 0$ unless $n = 0$ and $k = 0$.

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0,$$

and d_0 is the digit in the ones place. Factoring out 10 from all but the final term gives

$$n = 10 \cdot (d_k \cdot 10^{k-1} + d_{k-1} \cdot 10^{k-2} + \cdots + d_2 \cdot 10^1 + d_1) + d_0.$$

Thus $n = 10 \cdot$(an integer) $+ d_0$, and so $n \bmod 10 = d_0$, which is the digit in the ones place in the decimal representation for n.

Example 4.5.4 – *Solution*

continued

b. Because $m \text{ mod } 11 = 6$, 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,

$$4m \text{ mod } 11 = 2.$$

Representations of Integers

Representations of Integers

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.

Note The fact that any integer is either even or odd is called the **parity property**.

Example 4.5.5 – *Consecutive Integers Have Opposite Parity*

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

Example 4.5.5 – *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, you can divide the analysis into two cases: case 1, where the smaller of the two integers is even, and case 2, where the smaller of the two integers is 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.

Example 4.5.5 – *Solution*

continued

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.*]

Representations of Integers

Theorem 4.5.2 The Parity Property

Any two consecutive integers have opposite parity.

Representations of Integers

Method of Proof by Division into Cases

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

$$\begin{gathered}\text{If } A_1, \text{ then } C,\\ \text{If } A_2, \text{ then } C,\\ \vdots\\ \text{If } A_n, \text{ then } C.\end{gathered}$$

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

Example 4.5.6 – *Representing Integers mod 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.

Example 4.5.6 – *Solution*

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

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

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. In other words, n *mod* 4 equals 0, 1, 2, or 3.

Example 4.5.7 – *The Square of an Odd Integer*

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

Example 4.5.7 – *Solution*

Formal Restatement: ∀ odd integer n, ∃ an integer m such th$n^2 = 8m + 1.$

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

Example 4.5.7 – *Solution*

continued

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

To Show: ∃ 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 $n^2 - 1 = (n - 1)(n + 1).$

Example 4.5.7 – *Solution*

continued

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.

You could try another approach by arguing that since n is odd, you can represent it 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 $8m + 1$.

Example 4.5.7 – *Solution*

continued

Yet another possibility is to use the result of Example 4.5.6. 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.

Representations of Integers

Theorem 4.5.3

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 4*q* and 4*q* + 2 are even, *n* must have one of the forms

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

Example 7 – *Solution*

cont'd

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

Since $n = 4q + 1$,

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

Example 7 – *Solution*

cont'd

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,

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

Example 7 – *Solution*

cont'd

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

Since $n = 4q + 3$,

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

Example 7 – *Solution*

cont'd

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,

$n^2 = 8m + 1$ where *m* is an integer.

Example 7 – *Solution*

cont'd

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.]*

Absolute Value and the Triangle Inequality

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** $\boldsymbol{x}$, denoted $|x|$, is defined as follows:

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

Absolute Value and the Triangle Inequality

Lemma 4.5.4

For every real number r, $-|r| \leq r \leq |r|$.

Lemma 4.5.5

For every real number r, $|-r| = |r|$.

Theorem 4.5.6 The Triangle Inequality

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