

2. The Division Theorem

This Theorem is central to our study of Number Theory. To give a proof, we begin by discussing a useful function which relates real numbers and integers.

The Integer Part Function.

Definition

Let $x \in \mathbf{R}$. The *integer part* of x is the largest integer less than or equal to x . It is denoted by $[x]$.

For example : $[3] = 3$, $[3.2] = 3$, $[2.9] = 2$, $[-2.1] = -3$, $[\pi] = 3$.

The definition can be expressed in formal terms as $[x] = \max \{ n \in \mathbf{Z} : n \leq x \}$.

Now $[x] + 1$ is an integer *greater than* $[x]$, so cannot belong to $\{ n \in \mathbf{Z} : n \leq x \}$ as $[x]$ is the *largest* member. Thus we have

Lemma 1 $[x] \leq x < [x] + 1$.

If we subtract $[x]$ from each term, we get

$$0 \leq x - [x] < 1.$$

Thus, $x = [x] + \theta$, where $0 \leq \theta < 1$.

In some texts, θ is called *the fractional part of x*.

Long Division

Before calculators, division by a number greater than 10 was laid out as follows.

Suppose that we are dividing 583 by 17.

$$\begin{array}{r} 34 \\ 17 \overline{) 583} \\ \underline{51} \\ 73 \\ \underline{68} \\ 5 \end{array}$$

We say that 34 is the *quotient*, and 5 the *remainder* when 583 is divided by 17.

The result can be written as $583/17 = 34 + 5/17$,

or (multiplying through by 17) as $583 = 34 \cdot 17 + 5$.

Note that the final version uses only *integers*. It *motivates* the next result.

Theorem 1 - The Division Theorem

Let a and b be integers with $a > 0$. Then there are *unique* integers q, r such that

$$b = qa + r, \text{ and } 0 \leq r < a.$$

Note. The integers q and r are the *quotient* and *remainder* when b is divided by a .

Proof

Let q be the integer $[b/a]$.

From Lemma 1 we get

$$q \leq b/a < q + 1.$$

Then $qa \leq b < qa + a$, so that

$$0 \leq b - qa < a. \quad (*)$$

Now put $r = b - qa$. Then $r \in \mathbf{Z}$ (as b, q, a are themselves in \mathbf{Z}). Also

$$b = qa + r \text{ (from the definition of } r), \text{ and } 0 \leq r < a \text{ (from } (*))$$

So far, we have shown that suitable integers q and r *exist*. But the theorem asserts that they are also *unique*.

Suppose we can find a pair of integers q', r' which are such that

$$b = q'a + r', \text{ and } 0 \leq r' < a.$$

Then $0 \leq b - q'a < a$, so that $q'a \leq b < q'a + a$. It follows that $q' = [b/a]$.
Now $b = q'a + r'$ so $r' = b - q'a$.

Thus q', r' must *always* be the values found in the first part of the proof.

Example Find the quotient and remainder when -583 is divided by 17 .

Solution In the notation of the Theorem, $a = 17, b = -583$

The quotient, q , is $[-583/17] = -35$.

The remainder is $r = b - qa = 12$.

NB We do NOT expect you to remember these formulae!

We stated the theorem for a positive integer a , and any integer b . Our example shows a case with b negative. Since we are dividing by a , we cannot allow $a = 0$. If we allow a negative, we have to amend the statement somewhat.

Theorem 2 - The Generalized Division Theorem

Let a and b be integers with $a \neq 0$. Then there are *unique* integers q, r such that

$$b = qa + r, \text{ and } 0 \leq r < |a|.$$

Proof (Optional)

The original proof deals with the case $a > 0$.

Now consider the case $a < 0$.

We can apply the Division Theorem to b and $-a$, as $-a > 0$. This yields unique integers q' and r' such that

$$b = q'(-a) + r', \text{ and } b = qa + r, \text{ and } 0 \leq r < |a|.$$

Rearranging this, and using the fact that $a < 0$, so that $|a| = -a$, we get

$$b = (-q')a + r', \text{ and } 0 \leq r' < |a|.$$

Thus, we get quotient $-q'$, remainder r' .

Odd and Even Integers

Suppose we have $a = 2$ in the Division Theorem. For a given b , we have

$$k, r \in \mathbf{Z}, \text{ with } b = 2k + r \text{ and } 0 \leq r < 2$$

As $0 \leq r < 2$, the only possible values for r are 0 and 1.

Integers b for which $r = 0$ are called *even integers*.

These have the form $b = 2k + 0$, i.e. $b = 2k$, with $k \in \mathbf{Z}$.

Integers b for which $r = 1$ are called *odd integers*.

These have the form $b = 2k + 1$, with $k \in \mathbf{Z}$.

Fact 1 If b is an even integer and c is any integer, then bc is even.

Proof

As b is even, $b = 2k$, with $k \in \mathbf{Z}$. Then $bc = (2k)c = 2(kc)$.

Now, as $k, c \in \mathbf{Z}$, $kc \in \mathbf{Z}$. Thus bc is even.

Fact 2 If b, c are odd integers, then bc is odd.

Proof

As b is odd, $b = 2k + 1$, with $k \in \mathbf{Z}$.

As c is odd, $c = 2m + 1$, with $m \in \mathbf{Z}$.

Then $bc = (2k + 1)(2m + 1) = 4km + 2k + 2m + 1 = 2(2km + k + m) + 1$

As $k, m \in \mathbf{Z}$, $n = 2km + k + m \in \mathbf{Z}$, so $bc = 2n + 1$, with $n \in \mathbf{Z}$. Thus, bc is odd.

Fact 3 If b is even, then b^2 is of the form $4k$, with $k \in \mathbf{Z}$.

Proof

As b is even, $b = 2q$, with $q \in \mathbf{Z}$. Then $b^2 = 4q^2$.

As $q \in \mathbf{Z}$, $k = q^2 \in \mathbf{Z}$, so b^2 is of the form $4k$, with $k \in \mathbf{Z}$.

Fact 4 If b is odd, then b^2 is of the form $4k + 1$, with $k \in \mathbf{Z}$.

Proof

As b is odd, $b = 2q + 1$, with $q \in \mathbf{Z}$. Then $b^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$.

As $q \in \mathbf{Z}$, $k = q^2 + q \in \mathbf{Z}$, so b^2 is of the form $4k + 1$, with $k \in \mathbf{Z}$.

Indeed, we can sharpen the result in Fact 4. This relies on an observation which is often useful in its own right. For the moment, we postpone the proof.

Fact 5 For any integer q , $q(q + 1)$ is even.

Fact 4a If b is odd, then b^2 is of the form $8m + 1$, with $m \in \mathbf{Z}$.

Proof

As in the proof of Fact 4, $b = 2q + 1$, with $q \in \mathbf{Z}$ and $b^2 = 4(q^2 + q) + 1$.

By Fact 5, $q^2 + q = q(q + 1)$ is even. It is therefore of the form $2m$, with $m \in \mathbf{Z}$.

Thus, $b^2 = 4(2m) + 1 = 8m + 1$, with $m \in \mathbf{Z}$, as required.

Proof (of Fact 5)

We know that the integer q is either even or odd. We consider each case in turn.

If q is even, then $q(q + 1)$ is even by Fact 1.

If q is odd, then $q + 1$ is even, so $q(q + 1) = (q + 1)q$ is even by Fact 1 again.

Thus in any case $q(q + 1)$ is even.

Observe that, taking $a = 4$ in the Division Theorem, each integer b can be written in one of the forms $4k + r$, with $r = 0, 1, 2$ or 3 .

Example 1

Show that any integer of the form $4K + 3$ cannot be written as the sum of two integer squares, i.e. cannot be written as $a^2 + b^2$, with $a, b \in \mathbf{Z}$.

Deduce that none of the integers $11, 111, 1111, 11111, \dots$ is the sum of two integer squares.

Solution

We consider the various possibilities for a and b , and use Facts 3, 4.

a and b both even : then $a^2 + b^2 = 4k + 4m = 4K$, with $K = k + m$

a and b both odd : then $a^2 + b^2 = 4k + 1 + 4m + 1 = 4K + 2$, with $K = k + m$

one of a, b even, one odd : then $a^2 + b^2 = 4k + 4m + 1 = 4K + 1$ with $K = k + m$.

Thus $a^2 + b^2 = 4K + r$, with $r = 0, 1$ or 2 , is cannot have the form $4K + 3$.

For the second part, note that $1\dots 111 = 1\dots 1.100 + 11 = 4.(1\dots 1.25 + 2) + 3$.

Thus no such integer is a sum of squares, by the first part.

Exercise to reader

Show that an integer of the form $4K + 2$ cannot be written as $a^2 - b^2$, with $a, b \in \mathbf{Z}$.

Hints

(a) unlike Example 1, we must distinguish “ a odd, b even” from “ a even, b odd”.

(b) an integer of the form $4L - 1$ is of the form $4K + 3$, with $K = L - 1$.