

# The Division Theorem

## Reading

Section 3.5

## Practice Problems

**3.5** 1, 5, 6, 7, 8, 10, 11, 12, 15, 27, 28

**Challenge 3.5** (optional) 13, 14, 17, 18, 19, 21, 29, 30

## Notes

The main result in this section is the **Division Theorem**:

For any natural  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}$ , there are unique integers  $q$  and  $r$  such that  $0 \leq r < b$  and:

$$a = qb + r$$

The intuitive idea is that we add together as many  $b$ 's as we can before we reach  $a$ . Then whatever remains cannot have any more  $b$ 's in it, and it will serve as our  $r$ .

Before we look at the proof, let us look at some consequences of the theorem:

- The fact that every integers is odd or even follows directly, by using  $b = 2$ .
- The fact from your homework that every integer was in one of the types A, B, C follows directly, by using  $b = 3$ .

Technical proof:

The proof has two distinct parts. First we prove that there are  $q, r$  satisfying the requirements. Then we will prove that they are unique.

Proof that they exist:

- Consider the set:

$$S = \{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\}$$

- This set  $S$  is always non-empty (WHY?).
- By the Well-Ordering principle, there must be a smallest element, so there is some  $x = q$  that achieves this smallest element in  $S$ .

- Define  $r = a - qb$ , which is this smallest element in  $S$ .
- Then first of all  $r \geq 0$ .
- All that is left is to show that  $r < b$ . We proceed by contradiction.
  - If  $r \geq b$ , then  $r - b \geq 0$ .
  - And  $r - b = a - (q + 1)b$ .
  - So  $r - b$  is a number in  $S$ , and it's smaller than  $r$ , which is a contradiction.
  - So it must be the case that  $r < b$ .
- Essentially the Well-Ordering principle captures the idea to “use as many  $b$ 's as you can fit”.

Proof that they are unique:

- This is a simpler contradiction proof. Suppose that we had two ways, so:

$$a = bq + r = bq' + r'$$

- We can rewrite this as:

$$b(q - q') = r' - r$$

- Now this equation has on the left side the product of  $b$  with an integer. So unless that integer is 0, this product will be either at least  $b$  or at most  $-b$ .
- On the right side it has the difference of two numbers that are  $\geq 0$  and  $< b$ . So this difference must be:

$$-b < r' - r < b$$

- So the only way they can equal each other is if they are both 0. But then  $q = q'$  and  $r = r'$ .

We call  $r$  the *remainder*, and  $q$  the *quotient*.

$b$  divides  $a$  if and only if the remainder of dividing  $a$  by  $b$  is 0.

This is fairly straightforward to see.

Here is one nice consequence of the division theorem:

If  $a|x$  and  $b|x$ , then their least common multiple  $\text{lcm}(a, b)|x$  also must divide  $x$ .

To prove this:

- Define  $M = \text{lcm}(a, b)$ . We will need to show that  $M|x$ .
- Start by doing the division  $x = qM + r$  where  $0 \leq r < M$ .
- It will be enough to show that  $r = 0$ .
- Since  $a|M$ , we can write  $M = ad$ .
- So  $x = qda + r$ .
  - Question: why is that not enough to say that  $r = 0$ , since  $a|x$ ?
  - Make sure to answer this question before proceeding to the next line.
- It must be the case that  $a|r$ , since it divides both  $x$  and  $qda$ .
- With a similar reasoning,  $b|r$ .
- So  $r$  is a common multiple of both  $a$  and  $b$ , so it must be  $\geq M$ . Contradiction.

Another important theorem is an analog of this for the greatest common divisor:

- $\text{gcd}(a, b)$  is an integer linear combination of  $a$  and  $b$ .
- In fact it is the smallest positive number that is an integer linear combination of  $a$  and  $b$ .
- If  $d|a$  and  $d|b$ , then we also have that  $d|\text{gcd}(a, b)$ .

Proof to follow.