Math 8: Integers

Spring 2011; Helena McGahagan

We now assume that, in addition to basic logic and set theory, we understand the set of integers, denoted by $\mathbb{Z}$. The integers include the positive numbers, the negative numbers, and 0. We know how to add and multiply integers, and we can compare two integers using inequalities. Important properties of an inequality are that, when multiplied by a negative number on both sides, the inequality changes direction; also multiplying two positive numbers together always yields another positive number. (You can glance at Chapter 4 if you want to see these rules written down explicitly.)

Definitions

Let $a, b \in \mathbb{Z}$. We say that a **divides** b (denoted $a \mid b$, also sometimes read as "a is a factor of b") if there exists an integer c such that $b = ca$.

Let $p \in \mathbb{Z}$. We say that p is **prime** if $p \geq 2$ and the only postive factors of p are 1 and p itself.

Let $a, b \in \mathbb{Z}$. An integer d is called a **common factor** of a and b if both $d \mid a$ and $d \mid b$.

Let $a, b \in \mathbb{Z}$. The **highest common factor** of a and b (denoted by $\text{hcf}(a, b)$)is the largest positive integer that divides both a and b. (In other words, it is the largest common factor of a and b.)

Let $a, b \in \mathbb{Z}$. The **least common multiple** of a and b (denoted by $\text{lcm}(a, b)$) is the smallest positive integer that is divisible by both a and b.

Let $a, b \in \mathbb{Z}$. We say that a and b are **coprime** if $\text{hcf}(a, b) = 1$.

Fix $a \in \mathbb{N}$. For any $b \in \mathbb{Z}$, we can define the **quotient** and the **remainder** as in the Division Algorithm (see below).

Examples We can easily see that $-3 \mid 12$ (use the integer $c = -4$ to see that the definition is satisfied). Similarly, $7 \mid 7$ and $1 \mid -3$ and $4 \mid 0$ – what is an integer c that works for each example?

Examine the definition of divides to see why $n \mid 0$ is true for any integer n. Is $0 \mid n$ ever true? (Hint: It's only true for one value of n...)

PROPOSITION Let $a, b, d \in \mathbb{Z}$.

(i) If $a \mid b$ and $b \mid d$, then $a \mid d$.

(ii) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

(iii) If $a \mid b$ and $a, b \in \mathbb{N}$, then $a \leq b$.

The proof of each of these is a straightforward exercise in applying the definition of divides. See if you can repeat the arguments on your own; see your class notes if you get stuck. The proof of the next proposition is also straightforward:

PROPOSITION 10.2 Let $a, b, d \in \mathbb{Z}$. Suppose $d \mid a$ and $d \mid b$. Then $d \mid (ma + nb)$ for any $m, n \in \mathbb{Z}$.

The proof of the next proposition, however, is more involved since we do not assume we know how to divide integers!

THE DIVISION ALGORITHM (Proposition 10.1)
Let $a \in \mathbb{N}$. Then for any $b \in \mathbb{Z}$, there exist unique integers q, r such that

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

The integer q is called the *quotient* and r is called the *remainder*.

THE EUCLIDEAN ALGORITHM Let $a, b \in \mathbb{Z}$ and $a \neq 0$. The highest common factor hcf(a, b) can be found by repeatedly using the Division Algorithm:

$$\begin{array}{rcll}
b & = & q_1 a + r_1 & \text{where} \quad 0 < r_1 < |a| \\
a & = & q_2 r_1 + r_2 & \text{where} \quad 0 < r_2 < r_1 \\
r_1 & = & q_3 r_2 + r_3 & \text{where} \quad 0 < r_3 < r_2 \\
 & \vdots & & \\
r_{n-2} & = & q_n r_{n-1} + r_n & \text{where} \quad 0 < r_n < r_{n-1} \\
r_{n-1} & = & q_{n+1} r_n + 0 &
\end{array}$$

The last nonzero remainder $r_n = \text{hcf}(a, b)$.

Notice that the Euclidean algorithm guarantees that the hcf(a, b) exists whenever $a \neq 0$. Can you use the definition of highest common factor directly to find hcf$(b, 0)$ for any integer $b \neq 0$? (Notice that, with the definition given in your book, hcf$(0, 0)$ is undefined.) The Euclidean Algorithm is used in the proof of the following important proposition:

PROPOSITION 10.3 If $a, b \in \mathbb{Z}$ and $d = \text{hcf}(a, b)$, then there exist integers s and t such that

$$d = sa + tb.$$

Proof. Using the equations given in the Euclidean algorithm, we know that $d_n = r_n$ where $r_n = r_{n-2} - q_n r_{n-1}$. Continuing to work backwards, solve each equation for r_j in terms of earlier remainders. Eventually, we'll find that $d = sa + tb$ for some integers s and t. (Write down a few steps of this to see how it works!)

Using Proposition 10.3, we can prove the next two propositions. The first is the simple statement that factors of a and b must of course divide the *highest* factor of a and b. The second gives results on what happens when a prime number divides a product (or a number coprime to one of the others divides the product).

PROPOSITION 10.4 If $a, b \in \mathbb{Z}$, then any common factor of a and b also divides $\mathrm{hcf}(a, b)$.

PROPOSITION 10.5 Let $a, b \in \mathbb{Z}$

(a) Suppose $c \in \mathbb{Z}$ is coprime to a and suppose $c \mid ab$. Then $c \mid b$.

(b) Suppose p is a prime number and $p \mid ab$. Then either $p \mid a$ or $p \mid b$.

See if you can reproduce these proofs! Remember that you'll need Proposition 10.3 to prove both 10.4 and 10.5(a). Look back at your notes or the book if you get stuck.

EXAMPLES.

- For Proposition 10.4, consider a = 100 and b = 150. We could compute that the highest common factor is $d = 50$ (use the Euclidean algorithm to do this!) Other common factors of a and b include $\pm 2, \pm 5, \pm 10$, and ± 25, and we see that these all divide d.

- For Proposition 10.5(b), consider $a = -15$ and $b = 28$. Think of primes that divide $ab = -420$ such as $2, 3, 5$, and 7. Of course, all of these either divide either a or b! (*On the other hand, there are numbers that are* not *prime such as* 10 *that divide* -420*, but do not divide either* a *or* b*. This shows that it is necessary to assume* p *is a prime for the conclusion of this statement to be true.*)

When you read theorems, always try to think of examples (including examples where the result of the theorem is false to see why the assumptions are needed)!! (By the way, when you're reading this section in your book, you can skip the proof of Proposition 10.6 for now; we'll come back to it later.)