Divisibility

Learning Objectives. By the end of class, students will be able to:

- Define "divisible" and "factor"
- Prove basic facts about divisibility .

Read: Read Ernst Chapter 1 and Section 2.1. Also read Strayer Introduction and Section 1.1 through the proof of Proposition 1.2 (that is, pages 1-5).

Turn in: From Ernst: Problem 2.6 and 2.8

Definition (a divides b)**.** Let $a, b \in \mathbb{Z}$. The a *divides* b, denoted $a \mid b$, if there exists an integer c such that $b = ac$. If $a \mid b$, then a is said to be a *divisor* or *factor of* b. The notation $a \nmid b$ means a does not divide b.

Note that 0 is not a divisor of any integer other than itself, since $b = 0c$ implies $a = 0$. Also all integers are divisors of 0, as weird as that sounds at first. This is because for any $a \in \mathbb{Z}$, $0 = a0$.

Proposition 1. *Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Since this is the first result in the chapter, the only tool we have is the definition of "$a \mid b$".

Proof Since $a \mid b$ and $b \mid c$, there exist $d, e \in \mathbb{Z}$ such that $b = ae$ and $c = bf$. Combining these, we see

$$c = bf = (ae)f = a(ef),$$

so $a \mid c$. ∎

This means that division is *transitive*.

Proposition 2. *Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.*

Proof *Let $a, b, c, m, n \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. Then by definition of divisibility, there exists $j, k \in \mathbb{Z}$ such that $cj = a$ and $ck = b$. Thus,*

$$ma + nb = m(cj) + n(ck) = c(mj + nk).$$

Therefore, $c \mid ma + nb$ by definition. ∎

Definition. The expression $ma + nb$ in Proposition 2 is called *an (integral) linear combination of a and b.*

Proposition 2 says that an integer dividing each of two integers also divides any integral linear combination of those integers. This fact will be extremely valuable in establishing theoretical results. But first, let's get some more practice with proof writing

Break into three groups. Using the proofs of Proposition 1 and Proposition 2 as examples, prove the following facts. Each group will prove one part.

In-class Problem 1 Prove or disprove the following statements.

(a) If a, b, c, and d are integers such that if $a \mid b$ and $c \mid d$, then $a + c \mid b + d$.

(b) If a, b, c, and d are integers such that if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Learning outcomes:
Author(s): Claire Merriman

(c) If a, b, and c are integers such that if $a \nmid b$ and $b \nmid c$, then $a \nmid c$.

Solution: Problem on Homework.