Wednesday, January 17: Introduction and Divisibility

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

- Understand the course structure
- Formally define even and odd
- Formally define "divides"
- Complete basic algebraic proofs .

Introduction

What is number theory?

Elementary number theory is the study of integers, especially the positive integers. A lot of the course focuses on prime numbers, which are the multiplicative building blocks of the integers. Another big topic in number theory is integer solutions to equations such as the Pythagorean triples $x^2+y^2=z^2$ or the generalization $x^n+y^n=z^n$. Proving that there are no integer solutions when $n>2$ was an open problem for close to 400 years.

The first part of this course reproves facts about divisibility and prime numbers that you are probably familiar with. There are two purposes to this: 1) formalizing definitions and 2) starting with the situation you understand before moving to the new material.

Go over syllabus highlights: Deadlines, make-up policy, in-class work, reading assignments.

Mathematical definitions, mathematical notation

Definition. We will use the following number systems and abbreviations:

- The *integers,* written $\mathbb{Z}$, is the set $\{\dots,-3,-2,-1,0,1,2,3,\dots\}$.
- The *natural numbers,* written $\mathbb{N}$. Most elementary number theory texts either define $\mathbb{N}$ to be the positive integers or avoid using $\mathbb{N}$. Some mathematicians include 0 in $\mathbb{N}$.
- The *real numbers,* written $\mathbb{R}$.
- The *integers modulo n,* written $\mathbb{Z}_n$. We will define this set in Strayer Chapter 2, although Strayer does not use this notation.

We will also use the following notation:

- The symbol $\in$ means "element of" or "in." For example, $x\in\mathbb{Z}$ means "x is an element of the integers" or "x in the integers."

This first section will cover results in both Strayer and Ernst.

Definition (Ernst, Definition 2.1)**.** An integer n is *even* if $n=2k$ for some $k\in\mathbb{Z}$. An integer n is odd if $n=2k+1$ for some $k\in\mathbb{Z}$.

Now, this definition is standard in an introduction to proofs course, but it is not the only definition of even/odd.

Definition (Strayer, Definition 4)**.** Let $n\in\mathbb{Z}$. Then n is said to be *even* if 2 divides n and n is said to be *odd* if 2 does not divide n.

Note that we need to define *divides* in order to use Strayer's definition. We will formally prove that these definitions are *equivalent,* but for now, let's use Ernst definition.

In-class Problem 1

Theorem 1. *If n is an even integer, then n^2 is even.*

Prove this theorem.

Solution: *If n is an even integer, then by definition, there is some $k \in \mathbb{Z}$ such that $n = 2k$. Then*

$$n^2 = (2k)^2 = 2(2k^2).$$

Since $2(k^2)$ is an integer, we have written n^2 in the desired form. Thus, n^2 is even.

Crowd Sourced Proof.

Theorem 2. *The sum of two consecutive integers in odd.*

For this problem, we need to figure out how to write two consecutive integers.

Solution: Let $n, n+1$ be two consecutive integers. Then their sum is $n+n+1 = 2n+1$, which is odd by definition.

Divisibility

The goal of this chapter is to review basic facts about divisibility, get comfortable with the new notation, and solve some basic linear equations.

We will also use this material as an opportunity to get used to the course.

Definition. 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 odd as that sounds at first. This is because for any $a \in \mathbb{Z}$, $0 = a0$.

Friday, January 19: Division algorithm, divisibility

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

- Prove facts about divisibility
- Prove basic mathematical statements using definitions and direct proof
- Use truth tables to understand compound propositions
- Prove statements by contradiction
- Use the greatest integer function .

Reading 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. For $n, m \in \mathbb{Z}$, how are the following mathematical expressions similar and how are they different? In particular, is each one a sentence or simply a noun?

  (a) $n \mid m$

(b) $\frac{m}{n}$

(c) m/n

- Problem 2.8 Let $a, b, n, m \in \mathbb{Z}$. Determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

  (a) If $a \mid n$, then $a \mid mn$

- Problem 2.12. Determine whether the converse of each of Corollary 2.9, Theorem 2.10, and Theorem 2.11 is true. That is, for $a, n, m \in \mathbb{Z}$, determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

  (a) If a divides n^2, then a divides n. (Converse of Corollary 2.9)

  (b) If a divides $-n$, then a divides n. (Converse of Theorem 2.10)

  (c) If a divides $m + n$, then a divides m and a divides n. (Converse of Theorem 2.11)

Divisibility practice

Proposition (Strayer, Proposition 1.1)**.** *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 course, 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 (Strayer, Proposition 1.2)**.** *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 1.2 is called *an (integral) linear combination of a and b.*

Proposition 1.2 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 Propositions 1.1 and 1.2 as examples, prove the following facts. Each group will prove one part.

In-class Problem 2 *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 $ac \mid bd$.

(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 1.

Logic, proof by contradiction, and biconditionals

We will begin by working through Ernst Section 2.2 through Example 2.21. Discuss Problem 2.17 as a class, and note that Problem 2.19 is on Homework 1.

In-class Problem 3 *Construct a truth table for $A \Rightarrow B, \neg(A \Rightarrow B)$ and $A \wedge \neg B$*

Solution:

A	B	$A \Rightarrow B$	$\neg(A \Rightarrow B)$	$A \wedge \neg B$
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	F	F

This is the basis for *proof by contradiction.* We assume both A and $\neg B$, and proceed until we get a contradiction. That is, A and $\neg B$ cannot both be true.

Definition (Proof by contradiction)**.** Let A and B be propositions. To prove A implies B by contradiction, first assume the B is false. Then work through logical steps until you conclude $\neg A \wedge A$.

First, let's define a *lemma.* A lemma is a minor result whose sole purpose is to help in proving a theorem, although some famous named lemmas have become important results in their own right.

Definition. Let $x \in \mathbb{R}$. The *greatest integer function of x,* denoted $[x]$ or $\lfloor x \rfloor$, is the greatest integer less than or equal to x.

Lemma 3 (Strayer, Lemma 1.3)**.** *Let $x \in \mathbb{R}$. Then $x - 1 < [x] \leq x$.*

Proof By the definition of the greatest integer function, $[x] \leq x$.

To prove that $x - 1 < [x]$, we proceed by contradiction. Assume that $x - 1 \geq [x]$ (the negation of $x - 1 < [x]$). Then, $x \geq [x] + 1$. This contradicts the assumption that $[x]$ is the greatest integer *less than or equal to* x. Thus, $x - 1 < [x]$. ■