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, the preceding definition is standard in an introduction to proofs course, but it is not the only definition of even/odd. We also have the following definition that is closer to the definition you are probably used to:

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.

Theorem (Ernst, Theorem 2.2)**.** *If n is an even integer, then n^2 is even.*

In-class Problem 1 *Prove this theorem.*

Proof *If n is an even integer, then by Ernst, Definition 2.1, 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. ■

Theorem (Ernst, Theorem 2.3)**.** *The sum of two consecutive integers in odd.*

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

Proof Let $n, n+1$ be two consecutive integers. Then their sum is $n + n + 1 = 2n + 1$, which is odd by Ernst, Definition 2.1. ■

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

Reminding students about the reading for Friday.

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) $\dfrac{m}{n}$

  (c) ${}^{m}/_{n}$

Solution: The first means "n divides m," which is a relationship between n and m. This is a sentence. The other two are nouns, that is, the rational number $\frac{m}{n}$.

- 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 $a \mid mn$

Solution: Let $a \mid n$. Then by Definition (a divides b), there exists $k \in \mathbb{Z}$ such that $ak = n$. Multiplying both sides of the equation by m gives

$$a(km) = mn,$$

so $a \mid mn$ by definition of a divides b.

(b) If 6 divides n, then 2 divides n and 3 divides n.

Solution: Let $6 \mid n$. Then by definition of a divides b, there exists $k \in \mathbb{Z}$ such that $6k = n$. By factoring out 6, we see that $2(3k) = 3(2k) = n$, so $2 \mid n$ and $3 \mid n$.

(c) If ab divides n, then a divides n and b divides n.

Solution: Let $ab \mid n$. Then by definition of a divides b, there exists $k \in \mathbb{Z}$ such that $abk = n$. Thus, we see that $a(bk) = b(ak) = n$, so $a \mid n$ and $b \mid n$.

- 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)

Solution: False; $4 \mid 4$ but $4 \nmid 2$.

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

Solution: True. If $a \mid -n$, then by definition of a divides b, there exists $k \in \mathbb{Z}$ such that $ak = -n$. Multiplying both sides by -1 gives

$$-ak = a(-k) = n.$$

Therefore, $a \mid n$.

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

Solution: False; $3 \mid 2 + 1$ but $3 \nmid 2$ and $3 \nmid 1$.

Reminders and Homework Guide Review

Updated In Class Work logistics: if I am able to give individual feedback during class or have pairs/groups present the answers during class, then I will not collect the work.

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

Proof By the definition of the greatest integer (floor) 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, $x - 1 < [x]$. ■