Primes

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

- Prove every integer greater than 1 has a prime divisor.
- Prove that there are infinitely many prime numbers .

Read Strayer, Section 1.2

Turn in
- The proof method for Euclid's infinitude of primes is an important method. Summarize this method in your own words.

  Solution: Summaries will vary

- Identify any other new proof methods in this section

  Solution: Proof by construction may be new to some students. Students also identified:

  – Introducing a variable to aid in proof

  – Without loss of generality

- Exercise 22. Prove that 2 is the only even prime number.

Definition (prime and composite)**.** An integer $p > 1$ is *prime* if the only positive divisors of p are 1 and itself. An integer n which is not prime is *composite*.

Why is 1 not prime?

Lemma 1. Every integer greater than 1 has a prime divisor.

Proof Assume by contradiction that there exists $n \in \mathbb{Z}$ greater than 1 with no prime divisor. By the **??**, we may assume n is the least such integer. By definition, $n \mid n$, so n is not prime. Thus, n is composite and there exists $a, b \in \mathbb{Z}$ such that $n = ab$ and $1 < a < n$, $1 < b < n$. Since $a < n$, then it has a prime divisor p. But since $p \mid a$ and $p \mid n$, $p \mid n$. This contradicts our assumption, so no such integer exists. ■

We will not go over this proof in class.

Theorem 1 (Euclid's Infinitude of Primes)**.** There are infinitely many prime numbers.

Proof Assume by way of contradiction, that there are only finitely many prime numbers, so $p_1, p_2, \ldots, p_n$. Consider the number $N = p_1p_2 \cdots p_n + 1$. Now N has a prime divisor, say, p, by **??**. So $p = p_i$ for some i, $i = 1, 2, \ldots, n$. Then $p \mid N - p_1p_2 \ldots p_n$, which implies that $p \mid 1$, a contradiction. Hence, there are infinitely many prime numbers. ■

One famous open problem is the Twin Primes Conjecture. A *conjecture* is a proposition you (or in this case, the mathematical community) believe to be true, but have not proven.

Conjecture 1 (Twin Prime Conjecture)**.** There are infinitely many prime number p for which $p + 2$ is also prime number.

Learning outcomes:
Author(s): Claire Merriman

Another important fact is there are arbitrarily large sequences of composite numbers. Put another way, there are arbitrarily large gaps in the primes. Another important proof method, which is a *constructive proof*:

Theorem 2. For any positive integer n, there are at least n consecutive positive integers.

Proof Given the positive integer n, consider the n consecutive positive integers

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1.$$

Let i be a positive integer such that $2 \leq i \leq n+1$. Since $i \mid (n+1)!$ and $i \mid i$, we have

$$i \mid (n+1)!+i, \quad 2 \leq i \leq n+1$$

by linear combination. So each of the n consecutive positive integers is composite. ■

In-class Problem 1 Let n be a positive integer with $n \neq 1$. Prove that if n^2+1 is prime, then n^2+1 can be written in the form $4k+1$ with $k \in \mathbb{Z}$.

Solution: Assume that n is a positive integer, $n \neq 1$, and n^2+1 is prime. If n is odd, then n^2 is odd, which would imply $n^2+1=2$, the only even prime. However, $n \neq 1$ by assumption. Thus, n is even.

By definition of even, there exists $j \in \mathbb{Z}$ such that $n=2k$ and $n^2=4j^2$. Thus, $n^2+1=4k+1$ when $k=j^2$.

In-class Problem 2 Prove or disprove the following conjecture, which is similar to **??**:

Conjecture 2. There are infinitely many prime number p for which $p+2$ and $p+4$ are also prime numbers.