Self-paced Example: There are Infinitely Many Primes

Module 3

MCIT Online - CIT592 - Professor Val Tannen

This is a segment that contains material meant to be learned *at your own pace*. We are trying to assist you in this endeavor by organizing the material in a manner similar to the way it is outlined in the recorded segments, however with one additional suggestion. When you see the following marker:

we suggest that you stop and make sure you thoroughly understood the material presented so far before you proceed further.

Euclid's Proof of Infinitely Many Primes

Recall from an earlier module that we have defined a prime number as follows:

An integer m is **prime** when m has exactly two (positive) factors: 1 and itself, and moreover $m \geq 2$.

In this segment we explore an ancient proof (from Euclid) which shows that **there are infinitely many prime numbers**. It is a beautiful example of proof by contradiction and it illustrates how old mathematical reasoning really is.

Assume, for the sake of contradiction, that there are only finitely many primes. Let p be the largest prime number. Then all the prime numbers can be listed in increasing order as

$$2, 3, 5, 7, 11, 13, \ldots, p$$

In particular, no integer strictly bigger than p can be prime.

Our proof by contradiction aims to show that $2, 3, 5, 7, 11, 13, \ldots, p$ **cannot be all** the primes.

Consider an integer n that is formed by multiplying all these prime numbers and then adding 1. That is,

$$n = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$$

Observe that n is **not divisible** by any of $2, 3, 5, 7, \ldots p$ because the remainder for the division of n by each of these is 1.

(CONTINUED)

Euclid's Proof of Infinitely Many Primes

To continue the proof we use the following:

Proposition. Every integer has at least one prime factor only for integers > 1.

We omit the proof of this fact, except to note that it follows, for example, from the *Unique Prime Factorization Theorem* also known as the *Fundamental Theorem of Arithmetic* which is discussed in an optional segment in this module. Direct proofs are also possible, using concepts that we learn later in the course such as induction.

Therefore, in particular, the integer that we defined earlier, $n = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$ has a prime factor.

Since, as we have shown, n is not divisible by any of $2, 3, 5, 7, \ldots p$, these cannot be all the prime numbers. Contradiction, and this ends Euclid's proof.

By the way, a common mistake when trying to reproduce this proof is to claim that n must be prime and the contradiction is that n is bigger than the biggest assumed prime, p.

However, it does not follow from the definition of n that it must be prime. In fact, in general it is not a prime:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 \;=\; 30031 \quad \text{which is divisible by } \; 59$$

Luckily, we do not need the primality of n to reach a contradiction. We just needed that n has a prime factor, like any integer.