L01IntroToProofs

January 21, 2017

1 Intro to Proofs

Material for this lecture comes from the Introduction of "How To Prove It" by Daniel J. Velleman.

Let's look at an example. We will need a definition.

Definition 1: A positive integer n is a *prime number* if it has no positive divisors other than 1 and n itself.

Mathematicians have tried for a long time to understand the behavior of prime numbers. - Euclid (circa 350BC) proved that there are infinitely many prime numbers. * But what do they look like?

Two interesting conjectures:

Conjecture 1: Suppose n is an integer larger than 1 and n is prime. Then, $2^n - 1$ is prime.

Conjecture 2:
Suppose n is an integer larger than 1 and n is **not** prime. Then, $2^n - 1$ is **not** prime.

1.0.1 Check your understanding

- What is the relation between Conjecture 1 and 2?
- Specifically, what does one being true or false say about the other?

1.1 Checking a conjecture

Conjecture 1: Suppose n is an integer larger than 1 and n is prime. Then, $2^n - 1$ is prime.

Conjecture 2: Suppose n is an integer larger than 1 and n is **not** prime. Then, $2^n - 1$ is **not** prime.

Let's play around and try a few values.

n	Is n prime?	$2^n - 1$	Is $2^n - 1$ prime?
2	**yes**	3	** yes **
3	**yes**	7	**yes**
4	**no**	15	**no**
5	**yes**	31	**yes**
6	**no**	63	**no**
7	** yes**	127	**yes**
8	**no**	255	**no**
9	**no**	511	**no**
10	**no**	1023	**no**

So far so good, right?

- We haven't proved or disproved any of the conjectures.
- We only know that both are true for $n \leq 10$.

Let's go one more.

n	Is n prime?	$2^n - 1$	Is $2^n - 1$ prime?
11	**yes**	2047	??

No, 2047 is not prime (i.e., it is composite):

$$2047 = 23 \cdot 89$$

- Question: Which conjecture have we disproved?

Whenever we disprove something, we also prove something else. For instance, we have the following *theorem*: ** Theorem 1 ** Conjecture 1 is false.

Proof: * Take n = 11. - We have $n > 1$ and n is prime. * However, $2^n - 1 = 2047$ is not prime, - because $2047 = 23 \cdot 89$.

- This very simple proof is a proof by *counterexample*.
- It just required exhibiting a number ($n = 11$) for which Conjecture 1 was false.

1.2 A More Interesting Proof

Conjecture 2: Suppose n is an integer larger than 1 and n is **not** prime. Then, $2^n - 1$ is **not** prime.

- We still do not know much about the truth of Conjecture 2.
- I will now show you a proof that Conjecture 2 is true.
- This will require more effort, as I need to show that something is true *for all* values of n.

Proof of Conjecture 2: * Since n is not prime, there are positive integers $a, b \geq 1$ such that

$$n = a \cdot b$$

.

- Define:

$$x = 2^b - 1$$

$$y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$$

- Then:

$$xy = (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b})$$

$$= [2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}] - [1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}]$$

$$= 2^{ab} - 1 = 2^n - 1$$

.

Hence, $2^n - 1$ is not prime as $2^n - 1 = xy$.

GOALS FOR THE FIRST PART OF THIS CLASS: 1. Learn to understand proofs 2. Learn to write proofs 3. Learn to **FIND** proofs