Lesson 1: Intro to proofs and number theory

Tuesday, March 27, 2018 8:44 AM

Theory

- Idea / belief - not necessarily proven
- A model
- Elimination theory
- Theory of relativity
- Theory of evolution
- Theory of gravity
- Quantum / String theory
- Best explanation for observed / experimental results
- May not be possible to prove conclusively true.

Theorem

- More substantial than a theory
  - equations used to help prove other things
- Broad area of mathematics
- Pythagorean Theorem
- a statement / result that can be proven based on logic / axioms / previous results

Proof - an argument based on logic which conclusively demonstrates the truth (or falsehood) of a statement.

- In principle, all proofs of theorems emerge from fundamental axioms that are accepted to be true.

To prove something we need to work with:

- axioms
- definitions
- logic

- mathematical concepts such as numbers, sets, relations & functions

Some important sets (collections) of numbers include:

i) Natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$

ii) Integers $\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

iii) Rationals $\mathbb{Q} = \{x \mid x = p/q,\ p, q \in \mathbb{Z},\ q \neq 0\}$

$\mid$ "such that" $\in$ "is an element of the set"

iv) Real $\mathbb{R}$ = points on the line from $-\infty$ to ∞

= numbers with a (possibly infinite) decimal expansion

= union of the rational & irrational numbers

v) Complex $\mathbb{C} = \{z \mid z = a + bi,\ a, b \in \mathbb{R},\ i^2 = -1\}$

A basic building of any proof is the <u>statement</u> (proposition).
A statement is a claim that is objectively true or false.

<u>Examples</u>:

i) If m and n are odd integers, then mn is also odd.

ii) If n^2 is an even integer, then n must also be even (whenever $n \in \mathbb{Z}$)

iii) Let $n \in \mathbb{N}$. Then $\displaystyle\sum_{i=1}^{n} i^2 = 1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

iv) There are infinitely many prime numbers in $\mathbb{N}$.

v) Let $a, b, c, n \in \mathbb{N}$. Then, the equation $\Big\}$ Fermat's Last Theorem

$a^n + b^n = c^n$ has no solutions if $n > 2$

v) Let $a, b, c, n \in \mathbb{N}$. Then, the equation

$$a^n + b^n = c^n \text{ has no solutions if } n > 2.$$ } Fermat's Last Theorem

vi) Every even integer larger than 2 can be expressed as the sum of two prime numbers } Goldbach's Conjecture

e.g. $100 = 97 + 3 = 11 + 89$.

Exercise Prove statement (i) above: if m and n are odd, then mn is also odd.

Answer 1: $\frac{m}{2}$ and $\frac{n}{2}$ are not integers if m & n are odd.

. . . ?

Answer 2: When you multiply by an even number, you always get an even number. By multiplying two odd integers, we'll get an odd answer since neither is even.

Answer 3: When multiplying m & n, and dividing by two, if the result is not an integer, then mn must be odd.

What do we need?

- Definitions: odd, even, prime, etc.
- Axioms: What is already known to be true?
- Methods: what kind of argument is actually valid?

Basic Number Theory

Axioms - we accept (w/o proof) the following statements:

Let $a, b, c \in \mathbb{Z}$. Then:

1) $a+b \in \mathbb{Z}$
2) $-a \in \mathbb{Z}$
3) $ab \in \mathbb{Z}$
4) $a+b = b+a$ } commutativity
5) $ab = ba$
6) $(a+b)+c = a+(b+c)$ (associativity)
7) $0+a = a$
8) $a+(-a) = 0$
9) $a(b+c) = ab+ac$ (distributivity)

Other well-known facts can be derived from these.

e.g. $a-b \in \mathbb{Z}$ follows from 1) & 2)

$abc \in \mathbb{Z}$ follows from 3) (applied twice)

$a \cdot 0 = 0$ follows from 8) & 9)

$$a \cdot 0 = a(b-b) = ab+(-ab) = 0$$

We also introduce the following definitions:

i) An integer, n, is <u>even</u> if there exists an integer, r, such that $n = 2r$.

ii) Similarly, n is <u>odd</u> if there exists $r \in \mathbb{Z}$ such that
$$n = 2r+1.$$

iii) Let $a, b \in \mathbb{Z}$, with $a \neq 0$. We say that <u>a divides b</u>, written $a \mid b$, if there exists $q \in \mathbb{Z}$ such that

$aq = b$. "a is a factor of b"

"b is a multiple of a".

e.g. $13 \mid 52$ is true since $13 \cdot 4 = 52$, but

$3 \mid 52$ is not true since there is no integer q such that $3 \cdot q = 52$

We write $3 \nmid 52$

Note: $\underbrace{13 \mid 52}_{\text{statement.}}$ is not the same as $\underbrace{13/52}_{\text{number in } \mathbb{Q}}$ or $\frac{13}{52}$.

We can now prove statement (i) from before:

Let m and n be odd.

Then $m = 2r+1$ for some $r \in \mathbb{Z}$, and

$n = 2s+1$ for some $s \in \mathbb{Z}$.

So,
$$\begin{aligned} mn &= (2r+1)(2s+1) \\ &= 4rs + 2s + 2r + 1 \\ &= 2(2rs+s+r) + 1 \end{aligned}$$

Since $2rs+s+r \in \mathbb{Z}$, mn is odd. $\square$

Q.E.D.

This is an example of direct proof.

- Begin with the hypothesis: (m and n are odd).
- Apply definitions, axioms & previously proven results in sequence

to show that the conclusion (mn is odd) is always true.

Sometimes direct proofs aren't convenient.

Example: it is easy to prove the following directly:

"If n is even, then n^2 is also even" (Try!)

What about the converse statement:

"For any integer n, if n^2 is even, then n is also even"?

Using a direct method: n^2 is even, so $n^2 = 2r$ for some $r \in \mathbb{Z}$.

$n = \pm\sqrt{2r}$

... ?