Ken

Today:

- 4.1 Direct Proof and Counterexample I
- 4.2 Direct Proof and Counterexample II

Last time:

- 3.3 Statements with Multiple Quantifiers
- 3.4 Arguments with Quantified Statements
- 4.1 Direct Proof and Counterexample I

Even, Odd, Prime, and Composite Integers

An integer n is **even** if and only if n equals twice some integer. An integer n is **odd** if and only if n equals twice some integer plus 1.

I.e.

(i) n is **even** $\iff n = 2K$ for some integer K

(ii) n is **odd** $\iff n = 2K+1$ for some integer K

We may denote the set of even integers

$2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$

and odd integers

$\mathbb{Z} - 2\mathbb{Z} = \{\pm 1, \pm 3, \pm 5, \pm 7, \ldots\}$

We may formalize (i) & (ii):

(i) $n \in 2\mathbb{Z} \iff \exists K \in \mathbb{Z}\,(n = 2K)$

(ii) $n \in \mathbb{Z} - 2\mathbb{Z} \iff \exists K \in \mathbb{Z}\,(n = 2K+1)$

#4 Assume that $r, s \in \mathbb{Z}$, i.e. r and s are particular integers.

(a) $\forall r \in \mathbb{Z}\ \forall s \in \mathbb{Z}\ (4rs \in 2\mathbb{Z})$?

Is $4rs$ even? Why? Yes

$4rs = 2(2rs)$ where $2rs \in \mathbb{Z}$

(b) $\forall r \in \mathbb{Z}\ \forall s \in \mathbb{Z}\ (6r + 4s^2 + 3 \in \mathbb{Z} - 2\mathbb{Z})$?

Is $6r + 4s^2 + 3$ odd? Why? Yes

$$6r + 4s^2 + 3 = 6r + 4s^2 + 2 + 1$$
$$= 2(3r + 2s^2 + 1) + 1$$

where $t := 3r + 2s^2 + 1$ and $t \in \mathbb{Z}$

Theorem 4.1.1

The sum of any two even integers is even.

$\forall r, s \in 2\mathbb{Z}\ (r + s \in 2\mathbb{Z})$

$\forall r, s \in \mathbb{Z}\ (r \in 2\mathbb{Z} \wedge s \in 2\mathbb{Z} \longrightarrow r + s \in 2\mathbb{Z})$

Proof?

Let $r, s \in 2\mathbb{Z}$ be particular but arbitrarily chosen even integers.

By definition of an even integer, there exist $\ell, k \in \mathbb{Z}$ such that $r = 2\ell$ and $s = 2k$. So

$$r + s = 2\ell + 2k \quad \text{by substitution}$$

$$= 2(\ell + k) \quad \text{by algebra}$$

and define $t := \ell + k$ such that $t \in \mathbb{Z}$ since the set of integers are closed under addition. Thus $r + s = 2t$ and $r + s \in 2\mathbb{Z}$ by definition of an even integer.

example 4.1.9

Fill in the blanks in the proof of the following theorem:

Theorem 4.1.9

For all integers r and s, if r is even and s is odd then $3r+2s$ is even.

$\forall r \in \mathbb{Z}\ \forall s \in \mathbb{Z}\ (r \in 2\mathbb{Z} \wedge s \in \mathbb{Z}-2\mathbb{Z} \rightarrow 3r+2s \in 2\mathbb{Z})$

$\forall r \in 2\mathbb{Z}\ \forall s \in \mathbb{Z}-2\mathbb{Z}\ (3r+2s \in 2\mathbb{Z})$

Proof

Suppose r and s are any (particular but arbitrarily chosen) integers such that r is even and s is odd.

By by definition of even and odd integers $r = 2m$ and $s = 2n+1$ for some integers m and n ($m \in \mathbb{Z}$ and $n \in \mathbb{Z}$). Then

$$3r + 2s = 3(2m) + 2(2n+1) \quad \text{by substitution}$$

$$= 6m + 4n + 2 \quad \text{by multiplication (and distributivity)}$$

$$= 2(3m + 2n + 1) \quad \text{by factoring out 2 (distributivity)}$$

Let $t := 3m + 2n + 1$. Then t is an integer ($t \in \mathbb{Z}$) because $1, 2, 3, m, n$ are integers ($1, 2, 3, m, n \in \mathbb{Z}$) and because integers are closed under products and sums.

Hence $3r + 2s = 2t$ where t is an integer ($t \in \mathbb{Z}$) and so, by definition of even integer, $3r + 2s$ is even.

#27 Fill in the blanks in the following proof.

Theorem

For every odd integer n, n^2 is odd.

Proof: Suppose n is any odd integer.

By definition of odd, $n = 2k+1$ for some integer k.

(By definition of odd, $\exists k \in \mathbb{Z}(n = 2k+1)$.)

Then $n^2 = (2k+1)^2$ by substitution

$= 4k^2+4k+1$ by multiplying out

$= 2(2k^2+2k)+1$ by factoring out 2 (distributivity)

Now $2k^2+2k$ is an integer because it is a sum of products of integers. Therefore n^2 equals 2 multiplied by an integer, plus 1, and so n^2 is odd by definition of odd.

Because we have not assumed anything about n except that it's an odd integer, it follows from the principle of generalization from a generic particular that for every odd integer n, n^2 is odd. □

Definition

An integer n is **prime** if and only if $n > 1$ and, for all positive integers r and s, if $n = rs$ then either r or s equals n.

An integer n is **composite** if and only if $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

More formally: For each integer n where $n > 1$,

(i) n is **prime** $\iff$

$$\forall r \in \mathbb{Z}^+ \, \forall s \in \mathbb{Z}^+ \left(n = rs \Rightarrow (r = 1 \wedge s = n) \veebar (r = n \wedge s = 1) \right)$$

XOR

(ii) n is **composite** $\iff$

$$\exists r \in \mathbb{Z}^+ \, \exists s \in \mathbb{Z}^+ \left(n = rs \wedge (1 < r < n) \wedge (1 < s < n) \right)$$

Sometimes we denote the set of all prime numbers $\mathbb{P}$.

Russell & Whitehead's Principia Mathematica (Abridged)
pg. 360

Proving Existential Statements

Recall for predicate $P(x)$ with domain A

$\exists x \in A\,(P(x))$ if and only if $P(x)$ is true for at least one $x \in A$

To prove such a quantified statement

(i) find an x in A such that $P(x)$ is true

(ii) give a set of directions to find such an x in A

these are called **constructive proofs of existence.**

The underlying logical principle is called **existential generalization.**

e.g. Prove $\exists n \in \mathbb{Z}\,(n^2 = n)$.

Consider $0 \in \mathbb{Z}$. $0^2 = 0$.

Consider $1 \in \mathbb{Z}$. $1^2 = 1$.

A **nonconstructive proof of existence** involves showing either (a) the existence of a value x that makes $P(x)$ true is guaranteed by an axiom or a previously proved theorem or (b) the assumption there is no x such that $P(x)$ leads to a contradiction.

Disproof by Counterexample

Given predicates $P(x), Q(x)$ with domain A, to disprove $\forall x \in A\,(P(x) \to Q(x))$, find at least one $a \in A$, such that $P(x)$ is true and $Q(x)$ is false.

e.g. disprove $\forall x \in \mathbb{R}\,(x \notin \mathbb{Q} \to x \text{ is transcendental})$

$\exists x \in \mathbb{R}\,(x \notin \mathbb{Q} \wedge x \text{ is not transcendental})$

$\sqrt{2} \in \mathbb{R} \wedge \sqrt{2} \notin \mathbb{Q} \wedge \sqrt{2}$ is not transcendental

e.g. disprove $\forall x_1 \in \mathbb{R}\, \forall x_2 \in \mathbb{R}\,(\sin(x_1) = \sin(x_2) \to x_1 = x_2)$

$\exists x_1, x_2 \in \mathbb{R}\,(\sin(x_1) = \sin(x_2) \wedge x_1 \neq x_2)$

Choose $x_1 = 0$, $x_2 = 2\pi$. Then $\sin(0) = 0 = \sin(2\pi)$ and $0 \neq 2\pi$.

Generalizing from a generic particular

To show *all* elements of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Method of Direct Proof

1. express the statement as a universal conditional $\forall x \in A\,(P(x) \rightarrow Q(x))$
2. Suppose $a \in A$ is a particular but arbitrarily chosen element such that $P(a)$ is true.
3. Show $Q(a)$ is true using definitions, theorems, or rules for logical inference.
4. since $a \in A$ was arbitrarily chosen, generalize to x so that $\forall x \in A\,(P(x) \rightarrow Q(x))$

Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced, then it can be given a name, as long as that name is not currently being used to refer to something else in the same discussion.

4.2 Direct Proof and Counterexample II

Directions for Writing Proofs of Universal Statements

1. Copy the statement of the theorem (to be proved) $\forall x \in \mathbb{R}(\ldots)$
2. Clearly mark the beginning of your proof (with the word proof)
3. Make your proof self-contained (e.g. declare quantities or objects) e.g. Let $x \in \mathbb{R}$.
4. Write your proof in complete, grammatically correct sentences
5. Keep your reader informed about the status of each statement in your proof (e.g. assumptions)
6. Give a reason for each assertion in your proof (e.g. by definition, etc)
7. Include words and phrases that make the logic of your arguments clear
8. Display equations and inequalities

Giuseppe Peano

Peano axioms

Common Mistakes

1. arguing from examples
2. using the same letter for distinct objects
3. Jumping to a conclusion
4. Assuming what is to be proved (a circular argument)
5. Confusion between what is known and what is still to be shown
6. Use of any when the correct word some.
7. Misuse of the word "if" instead of "because"

“To beg and assume the original question is a species of failure to demonstrate the problem proposed; but this happens in many ways. A man may not reason syllogistically at all, or he may argue from premisses which are less known or equally unknown, or he may establish the antecedent by means of its consequents; for demonstration proceeds from what is more certain and is prior. Now begging the question is none of these: but since we get to know some things naturally through themselves, and other things by means of something else (the first principles through themselves, what is subordinate to them through something else), whenever a man tries to prove what is not self-evident by means of itself, then he begs the original question. This may be done by assuming what is in question at once; it is also possible to make a transition to other things which would naturally be proved through the thesis proposed, and demonstrate it through them, e.g. if A should be proved through B, and B through C, though it was natural that C should be proved through A: for it turns out that those who reason thus are proving A by means of itself. This is what those persons do who suppose that they are constructing parallel straight lines: for they fail to see that they are assuming facts which it is impossible to demonstrate unless the parallels exist. So it turns out that those who reason thus merely say a particular thing is, if it is: in this way everything will be self-evident. But that is impossible.”
Aristotle, *Prior Analytics*, Book II, Part 16

example 4.2.1

Theorem 4.2.1

The difference of any odd integer and any even integer is odd.

$\forall n \in \mathbb{Z}-2\mathbb{Z}\ \forall m \in 2\mathbb{Z}\ (n-m \in \mathbb{Z}-2\mathbb{Z})$

$\forall n \in \mathbb{Z}\ \forall m \in \mathbb{Z}\ (n \in \mathbb{Z}-2\mathbb{Z} \wedge m \in 2\mathbb{Z} \rightarrow n-m \in \mathbb{Z}-2\mathbb{Z})$

Proof:

Let $n \in \mathbb{Z}-2\mathbb{Z}$ and $m \in 2\mathbb{Z}$.

(Let n be an odd integer and m an even integer.)

$n = 2k+1$ for some integer k and $m = 2l$ for some integer l via definition of odd and even respectively.

$$\begin{aligned} n-m &= 2k+1-2l && \text{by substitution} \\ &= 2k-2l+1 && \text{by commutativity} \\ &= 2(k-l)+1 && \text{by factoring} \end{aligned}$$

where $t := k - l \in \mathbb{Z}$ by closure of the integers under subtraction. So $n - m = 2t + 1$ and $n - m \in \mathbb{Z} - 2\mathbb{Z}$ by definition of odd. □

Showing that an Existential Statement is False

example 4.2.3

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

$\exists n \in \mathbb{Z}^+ (n^2 + 3n + 2 \in \mathbb{P})$ ○

$\neg \exists n \in \mathbb{Z}^+ (n^2 + 3n + 2 \in \mathbb{P}) \equiv \forall n \in \mathbb{Z}^+ (n^2 + 3n + 2 \notin \mathbb{P})$

Proof:

Let $n \in \mathbb{Z}^+$. Then $n^2 + 3n + 2 = (n+1)(n+2)$ via factoring where

$0 < n$ since $n \in \mathbb{Z}^+$

$1 = 0 + 1 < n + 1 < n + 2 < 3n + 2 < n^2 + 3n + 2$

so $1 < n+1 < n^2+3n+2$

$1 < n+2 < n^2+3n+2$

and $n^2+3n+2 = (n+1)(n+2)$ is composite (by definition). Thus $n^2+3n+2 \notin \mathbb{P}$.