3.1: METHODS OF PROOF

A conjecture is a proposition whose truth value (T/F) is unknown. If it can be proven to be T, it becomes a theorem.

A lemma is a "smaller pre-theorem" used to prove a "larger" theorem.

ˈkȯr-ə-ˌler-ē, ˈkär; Brit: kə-ˈrä-lə-rē

A corollary is a "post-theorem" that follows directly from a previous theorem.

Many conjectures can be written as implications

$$\underset{\text{hypothesis}}{\underset{\uparrow}{p}} \longrightarrow \underset{\text{conclusion}}{\underset{\uparrow}{q}}$$

How can I rewrite this as an if-then stmt?

Ex "All primes are odd" can be rewritten as "If $\underbrace{\text{n is prime}}_{p}$, then $\underbrace{\text{n is odd}}_{q}$."

When $n=2$, p is T and q is F.
So, $n=2$ is a counterexample, and the conjecture is F.
Technically: $\underset{\text{(primes)}}{\forall x}\ \underset{x \text{ is odd}}{O(x)}$ is F.

If such a conjecture is T, we have the theorem

$$p \Longrightarrow q$$

A proof of a theorem can include:

1. Axioms / Postulates
   - statements accepted as true

   underlying assumpt about math. structures

   Ex $0 \neq 1$

2. Other Theorems / Lemmas

3. Definitions

   Another charac'ns mod 2 arithmetic even $\Leftrightarrow 2 \mid n$

   Ex n is an even number $\Leftrightarrow$
   $\exists k \in \mathbb{Z} : n = 2k$

   Ex n is an odd number $\Leftrightarrow$
   $\exists k \in \mathbb{Z} : n = 2k+1$

4. The hypotheses of the theorem
   - assume p is true (show q must be true)
   - used in direct proofs, proofs by cases

5. The negation of the conclusion
   - assume $\neg q$ is true (show $\neg p$ must be true)
   - prove $p \to q$ is T by proving that the contrapositive $\neg q \to \neg p$ is T.
   - used in indirect proofs

⑥ Rules of Inference

- logical rules (Table 1, p.169)
  (Table 2, p.174)

- basic (don't need to memorize names)

<u>Ex</u> A lemma states "$r \Rightarrow s$" ($r \to s$ is T)
We know r is T.
Therefore, s is T.

Shorthand:

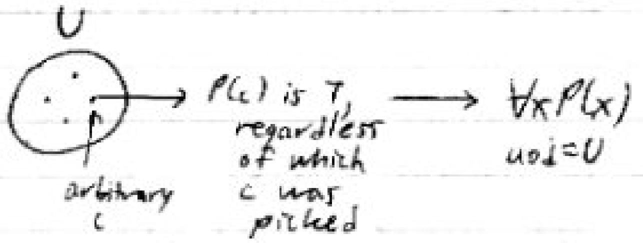
$$\begin{array}{l} \quad r \\ \quad \underline{r \to s} \\ \therefore s \end{array}$$

therefore

"modus ponens" rule
critical in induction
(i.e., $[r \wedge (r \to s)] \to s$ is a tautology)

Ex "Universal Generalization"

$$\frac{P(c) \text{ for an arbitrary } c \in U}{\therefore \forall x\, P(x)}$$



FALLACIES

- incorrect inferences

Affirming the Consequent
John McLaughlin
$p \Rightarrow q \to$ right

Ex $(p \to q) \Leftrightarrow (q \to p)$ Usually wrong!
converse

Ex $(p \to q) \Leftrightarrow (\neg p \to \neg q)$ Usually wrong!
inverse

Descartes' proof of $\exists$God

Ex Begging the question / Circular reasoning
- when a theorem is used to prove itself
- for example, when proving $p \Rightarrow q$ directly, a step in the proof relies on q being true.

$$p \to \ldots r \to \ldots q$$

TYPES OF PROOFS

① Direct Proofs

<u>Ex</u> (#22) Prove that the product of two rational #s is rational. ($\mathbb{Q}$ = set of all rational #s)

(Optional Rewrite)
If m and n are rational #s, then mn is rational.

Assume / Suppose m and n are rational #s. ($m, n \in \mathbb{Q}$)

(By definition)

$$m = \frac{a}{b} \quad \text{and} \quad n = \frac{c}{d}$$

for some $a, b, c, d \in \mathbb{Z}$ where $b, d \neq 0$.

(Sometimes, we assume that the fractions are in reduced form, but not here.)

Then, $mn = \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$

where $ac \in \mathbb{Z}$, $bd \in \mathbb{Z}$, and $bd \neq 0$.

$\therefore$ mn is rational ($mn \in \mathbb{Q}$)

quod erat demonstrandum — QED

Test?: odd even = odd — <u>Ex 14 (p. 175)</u> n odd $\Rightarrow n^2$ odd

See $\S$3.5 ② Indirect Proofs

Ex 15, p. 175 $3n+2$ odd $\Rightarrow n$ odd

Ex If $\underbrace{\underbrace{x \in \mathbb{Z}}_{p_1} \text{ and } \underbrace{y \in \mathbb{Z}}_{p_2}}_{p = p_1 \wedge p_2}$, then $\underbrace{2x + 2y \neq 15}_{q}$

Prove the contrapositive : $\neg q \to \neg p$

Assume $\neg q$: $2x + 2y = 15$

$\Rightarrow x + y = \frac{15}{2}$

Too close to $\ast$

$\Rightarrow \underbrace{x \notin \mathbb{Z} \text{ or } y \notin \mathbb{Z}}_{\neg p}$

Note: If $p = p_1 \wedge p_2 \wedge \ldots$ (conjunctive hypothesis)
to show $\neg p$ is T,
it suffices to show that one of
$p_1, p_2, \ldots$ must be F

② Indirect Proofs

Direct mod 2 proof:

$7n-11 \equiv 1 \ (2)$
$7n \equiv 12 \ (2)$
$n \equiv 0 \ (2)$

Indirect mod 2 proof:

$n \equiv 1 \ (2)$
$7n \equiv 7 \ (2)$
$7n \equiv 1 \ (2)$
$7n-11 \equiv -10 \ (2)$
$7n-11 \equiv 0 \ (2)$
$2 \mid 7n-11$

<u>Ex</u> Prove: If $\underbrace{7n-11 \text{ is odd}}_{p}$, then $\underbrace{n \text{ is even}}_{q}$.

Prove the contrapositive: $\neg q \rightarrow \neg p$

i.e., n is odd $\longrightarrow$ $7n-11$ is even

(n alone is easier to start with)

Assume $\neg q$: n is odd.

Then, $\exists k \in \mathbb{Z}: n = 2k+1$

$$\Rightarrow \exists k \in \mathbb{Z}: 7n-11 = 7(2k+1)-11 = 14k+7-11 = 14k-4 = 2\underbrace{(7k-2)}_{\in \mathbb{Z}}$$

$\Rightarrow 7n-11$ is even $(\neg p)$

QED

③ Proofs by Contradiction / Reductio ad absurdum

Gauss's Zeus

To prove that a conjecture c is true,
show that $\neg c$ leads to a contradiction ($\ast$).

i.e., Show that, for some proposition r,

$$\neg c \longrightarrow \underbrace{(r \wedge \neg r)}_{\text{must be F}} \text{ is T}$$

So, $\neg c$ must be F.
c must be T.

<u>Ex 18, pp. 176-7</u> $\sqrt{2}$ is irrational ($\sqrt{2} \notin \mathbb{Q}$)

<u>Ex</u> If $\underbrace{x \in \mathbb{Z} \text{ and } y \in \mathbb{Z}}_{p}$, then $\underbrace{2x + 2y \neq 15}_{q}$.

Assume p: $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$

Assume $\neg q$: $2x + 2y = 15$

$$\Rightarrow x + y = \tfrac{15}{2}$$

$$\Rightarrow x + y \notin \mathbb{Z}$$

r and $\neg r$ $\ast$

However, $p \Rightarrow x + y \in \mathbb{Z}$ (sum of two integers $\in \mathbb{Z}$)

So, assuming p is T $\Rightarrow \neg q$ is F $\Rightarrow q$ is T

④ Vacuous proof

Show P(0) true if P(n): $(n \geq 1) \to q$

$$p \to q$$

↑ Show p is F.

⑤ Trivial proof

$$p \to q$$

↑ Show q is T

don't worry

<u>Proof by Cases</u>

<u>Ex</u> Prove $\forall n \in \mathbb{Z}\ P(n)$

Can prove $\forall n \in \mathbb{Z}^{\text{even}}\ P(n)$ "Case 1"
<u>and</u> $\forall n \in \mathbb{Z}^{\text{odd}}\ P(n)$ "Case 2"

<u>Ex</u> +, 0, -

<u>Ex</u> Congruence classes (mod m)

<u>Ex</u> $x > y,\ x = y,\ x < y$

<u>To prove $p \leftrightarrow q$</u>

Prove $p \to q$
and $q \to p$

> not necessarily directly

EXISTENCE PROOFS

Ex $\exists n\, P(n)$

Constructive existence proofs indicate how to find a value(s) that make(s) P true.

Sufficient to prove $\forall n \in \mathbb{Z}^+ \ldots n \ldots$

Ex Prove that, for every $n \in \mathbb{Z}^+$ $(n \geq 2)$, there is a sequence of $n-1$ consecutive composite integers.

(This means there are arbitrarily large gaps between the primes.)

Consider: (Assume n big for now.)

$$
\begin{array}{lll}
 & n! & \leftarrow \text{prime if } n=2 \text{, not if } n>2 \\
 & n!+1 & \leftarrow ? \\
\text{sequence of } n-1 \text{ composites} \left\{ \begin{array}{l} \\ \\ \\ \\ \end{array} \right. & n!+2 & \leftarrow 2 \mid n!,\ 2 \mid 2,\ \text{so } 2 \mid (n!+2) \\
 & n!+3 & \leftarrow 3 \mid n!,\ 3 \mid 3,\ \text{so } 3 \mid (n!+3) \\
 & \vdots & \\
 & n!+n & \leftarrow n \mid n!,\ n \mid n,\ \text{so } n \mid (n!+n)
\end{array}
$$

$$\{ (n!+k) \mid k = 2, 3, \ldots, n \}$$

Ex 24 (p. 180) gives a nonconstructive proof showing there are ∞ many primes.

Proof by Contradiction

Assume there are only finitely many primes,
say n of them.

Primes: $\underset{\substack{\parallel \\ 2}}{p_1}, \underset{\substack{\parallel \\ 3}}{p_2}, \ldots, p_n$ ← complete list of all primes

Consider $p_1 p_2 \cdots p_n + 1$ ← M

$p_i \nmid M \quad (1 \leq i \leq n)$

because there is always
a remainder of 1 if
M is divided by any p_i
$(M \equiv 1 \pmod{p_i})$

So, ① M itself is a new prime
not in the list. $*$

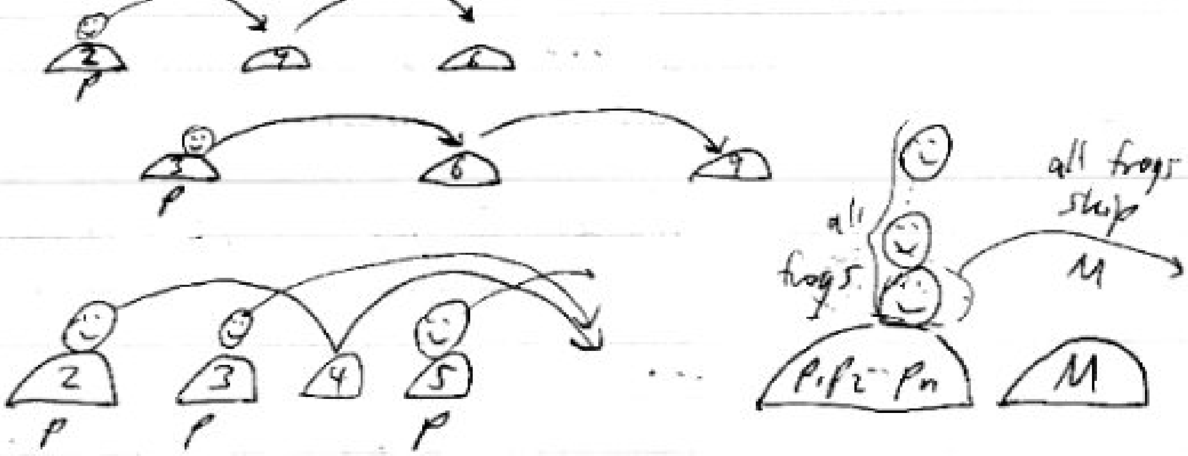
or ② M is divisible by some prime $< M$
that I missed. $*$

$\left.\begin{array}{l}\text{M div} \\ \text{by some} \\ \text{prime not} \\ \text{in my} \\ \text{list (maybe} \\ \text{M itself)}\end{array}\right\}$

In either case, the completeness of my list is contradicted

QED

Picture: frogs correspond to $p_1, p_2, \dots, p_n$



$p_1 \cdots p_n$ is lowest int. + divisible by all p_i, by CRT.
$x \equiv 0\ (p_1)$
$\vdots$
$x \equiv 0\ (p_n)$
!sol: $x \equiv 0\ (p_1 \cdots p_n)$

Either M is prime

or

A frog we missed lands on M