

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.

^{!kör-ə-tér-ē}
^{'när}
Brit: kə-tə-rəm

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

Many conjectures can be written as implications

$$\begin{array}{ccc} p & \longrightarrow & q \\ \uparrow & & \uparrow \\ \text{hypothesis} & & \text{conclusion} \end{array}$$

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

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

When $n=2$, p is T and q is F.
So, $n=2$ is a counterexample, and
the conjecture is F.

Technically: $\forall x \underset{\substack{\text{(primes)} \\ x \text{ is odd}}}{\text{O}(x)}$ 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

Ex $0 \neq 1$

② Other Theorems / Lemmas

③ Definitions

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 $p \rightarrow q$ is T by proving that the
contrapositive $\neg q \rightarrow \neg p$ 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)

Ex A lemma states " $r \Rightarrow s$ " ($r \rightarrow s$ is T)
We know r is T.
Therefore, s is T.

Shorthand:

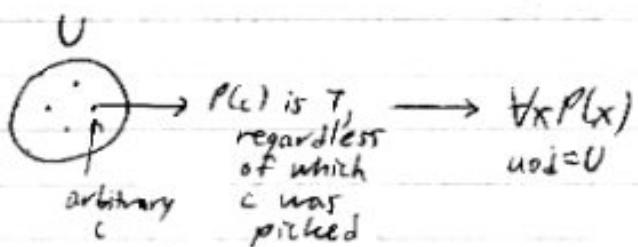
$$\frac{r}{\therefore s}$$

↑
therefore

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

Ex "Universal Generalization"

$P(c)$ for an arbitrary $c \in U$
 $\therefore \forall x P(x)$



FALLACIES

- incorrect inferences

Affirming the
consequent
John McLaughlin
 $p \Rightarrow q$ is right

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

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

Descartes'
proof of
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.

$$p \rightarrow \dots \overbrace{r}^{\leftarrow} \rightarrow \dots q$$

TYPES OF PROOFS

① Direct Proofs

Ex (#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)

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

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.)

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

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

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

QED

quod erat
demonstrandum

Test? odd even = odd

Ex 14 (p. 175) $n \text{ odd} \Rightarrow n^2 \text{ odd}$

See (3-3.5) ② Indirect Proofs

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

Ex If $\underbrace{x \in \mathbb{Z}}_{P_1}$ and $\underbrace{y \in \mathbb{Z}}_{P_2}$, then $\underbrace{2x+2y=15}_q$
 $P = P_1 \wedge P_2$

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

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

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

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

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

② Indirect Proofs

Direct mod 2 proof:

$$\begin{aligned}7n-11 &\equiv 1 \pmod{2} \\7n &\equiv 12 \pmod{2} \\n &\equiv 0 \pmod{2}\end{aligned}$$

Indirect mod 2 proof:

$$\begin{aligned}n &\equiv 1 \pmod{2} \\7n &\equiv 7 \pmod{2} \\7n &\equiv 1 \pmod{2} \\7n-11 &\equiv -10 \pmod{2} \\7n-11 &\equiv 0 \pmod{2} \\2 \mid 7n-11\end{aligned}$$

Ex Prove: If $\underbrace{7n-11}_{P}$ is odd, then \underbrace{n}_{q} is even.

Prove the contrapositive: $\neg q \rightarrow \neg p$
 i.e., n is odd $\rightarrow 7n-11$ is even
 (n alone is easier to start with)

Assume $\neg q$: n is odd.

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

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

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

QED

③ Proofs by Contradiction / Reductio ad absurdum

Gangarzew
%

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

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

$$\neg c \rightarrow (r \wedge \neg r) \text{ is T}$$

V
must be F

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

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

Ex If $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, then $2x + 2y \neq 15$.

p q

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

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

$$\begin{aligned} &\Rightarrow x + y = \frac{15}{2} \\ &\Rightarrow x + y \notin \mathbb{Z} \quad r \text{ and } \neg r \text{ ---} \end{aligned}$$

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 is true
if $P(n); (n \geq 1) \rightarrow q$

$$p \rightarrow q$$

↑
Show p is F.

don't
worry

(5) Trivial proof

$$p \rightarrow q$$

↑
Show q is T

Proof by Cases

Ex Prove $\forall n \in \mathbb{Z} \ P(n)$

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

Ex +, 0, -

Ex Congruence classes ($a \bmod m$)

Ex $x > y, x = y, x < y$

To prove $p \leftrightarrow q$

Prove $p \rightarrow q$ > not necessarily
 and $q \rightarrow p$ 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 $\exists n P(n)$

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.)

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

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

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: p_1, p_2, \dots, p_n ← list of all primes
 $\frac{1}{2}, \frac{1}{3}$

Consider $p_1 p_2 \cdots p_n + 1 \leftarrow M$

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

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. *

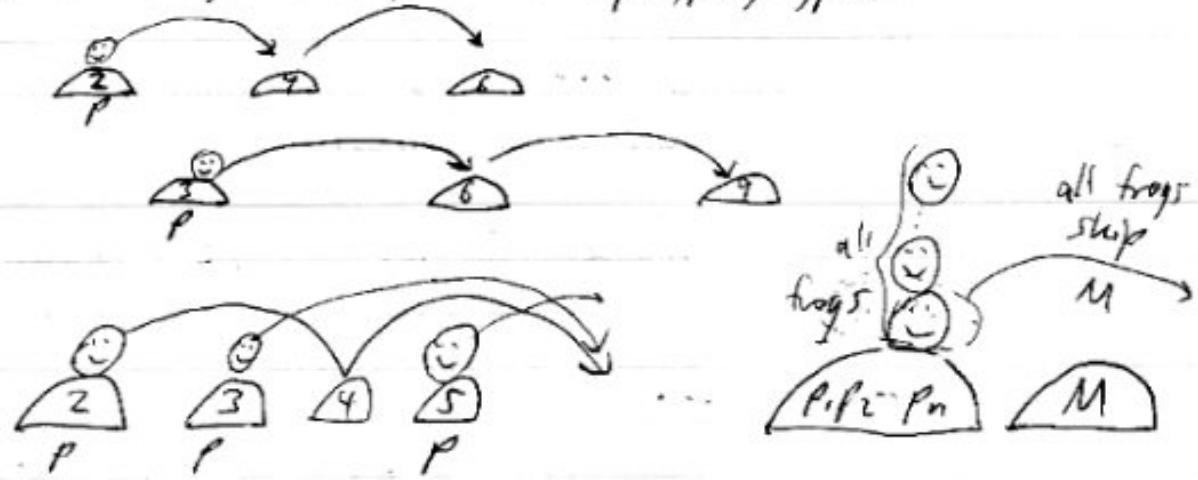
or ② M is divisible by some prime (M
that I missed). *

In either case, the completeness of my list is
contradicted

M divides
by some
prime not
in my
list (except
 M itself)

QED

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



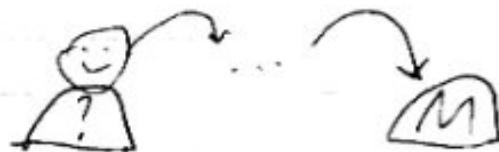
$P_1 \dots P_n$ is
invertible
divisible by
all p_i ,
by CRT.
 $x \equiv 0 \pmod{p_1}$
 $x \equiv 0 \pmod{p_2}$
 \vdots
 $x \equiv 0 \pmod{p_n}$

Either M is prime

or

$$\frac{M}{P}$$

A frog we missed lands on M



3.2: MATHEMATICAL INDUCTION

Not used to derive formulas or make discoveries.
Is used to prove guesses.

Ex 2 (pp. 189-190)

What is the sum of the first n odd positive integers?

<u>n</u>		<u>Sum</u>	
1	1	1	□
2	1+3	4	□
3	1+3+5	9	□

Guess: n^2

Ex 2 proves this.

$\forall n \ P(n)$

$\text{odd } \mathbb{Z}^+$ $\underbrace{\text{sum of first}}_{\text{is } n^2} \text{ odd pos. ints}$

!//
remain later:

$$\begin{aligned} 1+2+\dots+n &= \frac{n(n+1)}{2} \\ &\approx \frac{n^2}{2} \\ (\text{+ correction}) \end{aligned}$$

What you'd expect,

WEAK INDUCTION

$P(0)$ or $P(1)$
etc.
 $P(n) \rightarrow P(n+1)$
 $\therefore \forall x P(x)$

To prove propositions of the form $\forall n P(n)$, $n \in \mathbb{Z}^+$.

① Basis step: Show $P(1)$ is true.

② Inductive step:

Show that, for any arbitrary $n \in \mathbb{Z}^+$,
 $\underbrace{P(n)}_{\text{inductive hypothesis}} \rightarrow P(n+1)$ is true!

i.e., If we assume $P(n)$ is true,
show that $P(n+1)$ must also
be true. (NOT circular reasoning!)

Falling dominoes



Inductive step guarantees
that each falling
domino makes the
next domino fall.

Makes up the ying-yang!

Read Exs 2-5, 8-11

#8, p. 200 Ex Prove: $\forall n \in \mathbb{Z}^+ \quad \overbrace{1^3 + 2^3 + \dots + n^3}^{P(n)} = \left[\frac{n(n+1)}{2} \right]^2$

Note: $= (1+2+\dots+n)^2$

① Basis Step
 $P(1): 1^3 = \left[\frac{1(1+1)}{2} \right]^2 \quad (\text{plug in } n=1)$

$1 = 1$

$\therefore P(1)$ is true.

② Inductive Step

Let n be any arbitrary positive integer.
 Assume $P(n)$ is true.

(Inductive Hypothesis:)

$$1^3 + 2^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2$$

Show $P(n+1)$ is true.

$$\text{Show: } 1^3 + 2^3 + \dots + (n+1)^3 = \underbrace{\left[\frac{(n+1)(n+2)}{2} \right]^2}_{\text{Replace } n \text{ with } n+1}$$

$$1^3 + 2^3 + \dots + n^3 + (n+1)^3$$

by the I.H.,
this equals

$$\left[\frac{n(n+1)}{2} \right]^2$$

$$= \left[\frac{n(n+1)}{2} \right]^2 + (n+1)^3$$

$$= \frac{n^2(n+1)^2}{4} + (n+1)^3$$

$$= \frac{n^2(n+1)^2}{4} + \frac{4(n+1)^3}{4}$$

$$= \frac{n^2(n+1)^2 + 4(n+1)^3}{4}$$

We want: $\left[\frac{(n+1)(n+2)}{2} \right]^2$

Factor out $(n+1)^2$

$$= (n+1)^2 \left[\frac{n^2 + 4(n+1)}{4} \right]$$

$$= \frac{(n+1)^2(n^2 + 4n + 4)}{4}$$

$$= \frac{(n+1)^2(n+2)^2}{4}$$

$$= \left[\frac{(n+1)(n+2)}{2} \right]^2$$

$\therefore \forall n \in \mathbb{Z}^+ P(n)$
QED

Note To prove $P(n)$ for all nonnegative integers:
Base step: Show $P(0)$ is true.

OK
because
such a set is
well-ordered

To prove $P(n)$ is true for all integers $\geq a$ ($a \in \mathbb{Z}$)
Base step: Show $P(a)$ is true.

Ex 14 (Rosen pp. 198-9)

Prove that every amt. of postage of ≥ 12 ¢ can be formed using just 4¢ and 5¢ stamps.

Intuit $\mathbb{Z}^{>0}$
 $4m + 5n$
 $\rightarrow \text{get } \geq 12$

Let $P(n) =$ postage of n cents can be formed from 4¢ and 5¢ stamps

① Basis Step
 $P(12)$: 3 4¢ stamps $\rightarrow 12$ ¢

 4 4 4
12

② Inductive Step

Let n be any integer ≥ 12 .

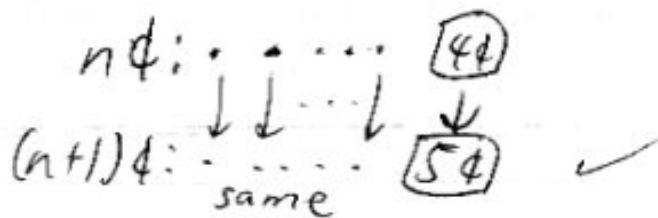
Assume $P(n)$ is true.

(maybe) some 4¢
(maybe) some 5¢ $\rightarrow n$ ¢

Show $P(n+1)$ is true

Case 1 ≥ 1 4¢ stamp can be used
to form n ¢.

Then, replace 1 4¢ stamp with 1 5¢ stamp.



In fact only
 $n=15$ is in
this case.
 $n=20: 4+4+4+4+4$
and any higher
multiple of 5
can build on
this.

Case 2 No 4¢ stamp can be used
to form n ¢.

Then, all stamps used to form n ¢
are 5¢ stamps.



QED

STRONG INDUCTION

To prove $\forall n P(n)$, $n \in \mathbb{Z}^+$

① Basis Step: Show $P(1)$ is true.

You may have to show $P(2), P(3), \dots$, some $P(k)$ are true.

② Inductive Step:

Show that, for any arbitrary $n \in \mathbb{Z}^+$,
 $(P(1) \wedge P(2) \wedge \dots \wedge P(n)) \rightarrow P(n+1)$

IH: Assume that

all previous
cases are true.

Sometimes you need
more than just
 $P(n)$ to prove
 $P(n+1)$.

Ex 13 (Kosen p. 98)

Prove that every integer greater than 1
can be written as the product of primes.

① $P(2)$ is true : $2 = 2$, prime

② Assume $P(2), P(3), \dots, P_n$ are true.)_{IH}
i.e., $\forall k (2 \leq k \leq n) P(k)$ is true.

Show Pn+1) is true

Case 1 $n+1$ is prime ✓
 $n+1 = n+1$

Case 2 $n+1$ is composite

$\Rightarrow \exists r, s \in \mathbb{Z} (2 \leq r \leq s \leq n); r \neq s$
say r is
larger

By IH, r and s can be written
as the product of primes.

So, $n+1$ can be written as a product
of primes

$p_1 p_2 \cdots p_r p_{r+1} p_{r+2} \cdots p_n$ ← can have repetitions

QED

This proves the existence part of FTA.
The uniqueness proof is on p. 139 (2e5)

Ex 14 (again)

(maybe) some 4¢ stamps \geq anything $\geq 12¢$

Proof by strong induction

① Base step

$$P(12) \text{ is } T : 4+4+4=12$$

$$P(13) \text{ is } T : 4+4+5=13$$

$$P(14) \text{ is } T : 4+5+5=14$$

$$P(15) \text{ is } T : 5+5+5=15$$

② Inductive step

Let $n \in \mathbb{Z}$, $n \geq 15$

Assume $\forall k (12 \leq k \leq n) P(k)$ is true,
 $P(12), P(13), \dots, P(n)$

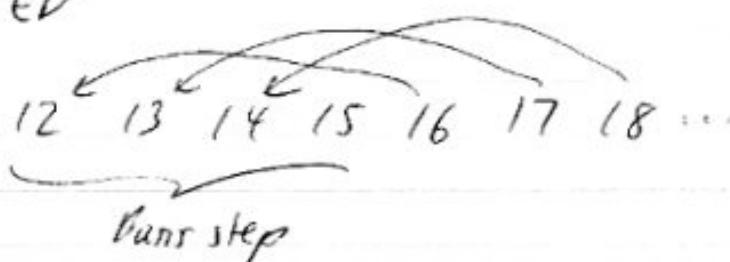
Show $P(n+1)$ is true.

By IH and $n \geq 15$, we know
 $P(n-3)$ must be true.

$$n-3 \notin \sim$$

$$n+1 \notin \sim \quad \boxed{44} \quad \checkmark$$

QED



Verify
only 15
needed all
std.

3.3: RECURSIVE DEFINITIONS

Ex Give a recursive definition of the sequence $\{a_n\}$, $n \in \mathbb{Z}^+$, if $a_n = 7n - 3$.

define terms by referring to previous terms!

Method 1

List some values:

$$a_1 = 7(1) - 3 = 4$$

$$a_2 = 7(2) - 3 = 11$$

$$a_3 = 7(3) - 3 = 18$$

Method 2 (slope)

Arithmetic
Geometric

$$a_{n+1} - a_n = [7(n+1) - 3] - (7n - 3)$$

$$= 7n + 7 - 3 - 7n + 3$$

$$= 7$$

$$\Rightarrow a_{n+1} = a_n + 7$$

Method 3

Think! What happens when $n+1$ replaces n ?

$$7n - 3 \xrightarrow{a_n} 7(n+1) - 3$$

\checkmark
effect of adding 7

Recursive / Inductive defin:

$$a_1 = 4$$

$$a_{n+1} = a_n + 7 \quad \text{for } \underbrace{n \in \mathbb{Z}}_{n \in \mathbb{Z}^+}, n \geq 1$$

$$\text{If } f(n) = 7n - 3$$

$$f(1) = 4$$

$$f(n+1) = f(n) + 7$$

$$\underline{z \rightarrow b \rightarrow n \in \mathbb{Z}, n \geq 1}$$

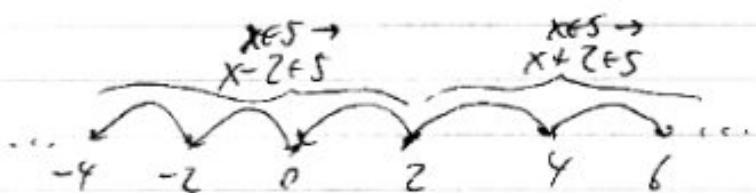
Read Exs 1-5 (203-5)

RECURSIVELY DEFINED SETS

Basic building
blocks(s)
 $f(x,y) \in S$
ambiguous!
or func.
values
? = BBS

Ex ① $Z \in S$

② $\begin{cases} x-y \in S & \text{if } x \in S \text{ and } y \in S \\ x+y \in S & \text{if } \end{cases}$ } recursive /
inductive step



Not in lossing
in transients

③ Extremal clause, If something can't be included in S after a finite # of applications of ① and ②, then it is $\notin S$.

Ex The set S of bit strings with exactly one "1".

① $1 \in S$

② $\begin{cases} 0x \in S & \text{if } x \in S \\ x0 \in S & \text{if } x \in S \end{cases}$

③ Extremal clause

3.4: RECURSIVE ALGORITHMS

Pro
Shorter

Cons

Twice as

base cases, critical

Memory space considerations
lead to repeat work