Set → a well-defined collection of distinct objects.

Element / Member → a thing in the set.

Example: $\{1, 3, 5\}$ (a set of 3 numbers)

↳ $3 \in \{1, 3, 5\}$

↳ "Is an element of"

↳ $4 \notin \{1, 3, 5\}$

↳ "Is NOT an element of"

Example: $\{1, 3, \{1, 3, 5\}\}$ → $5 \notin S$, but $5 \in \{1,3,5\} \in S$.

Canonical Sets:

- $\mathbb{N} = \{1, 2, 3, \dots\}$ → sometimes includes 0 — natural
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ — integers
- $\mathbb{Q} = \{ a/b \mid a, b \in \mathbb{Z}, b \neq 0 \}$ — rational
  - ↳ "such that"
- $\mathbb{R}$ = Real numbers.

Statement: $A = (\pi = \frac{22}{7})$.

↳ the negation of A, $\neg A$, is the statement which has the opposite truth.

↳ $\neg A = (\pi \neq \frac{22}{7})$ aka, $\neg A = \neg(\pi = \frac{22}{7})$

- $\neg A = \neg(\neg A)$ — double negation!

Quantifiers & Quantified Statements

- A quantified statement is a statement with 4 parts:
  1) a quantifier
  2) a variable (symbol representing a math object)
  3) a domain (a set)
  4) an open sentence involving the variable.

quantifiers → universal ("for all", "for every").
↳ existential ("there exists", "there is").

Eg: $\frac{2m+1}{m-7} = 5$ — open sentence! → not statement bc not definitive

so, $\exists\, m \in \mathbb{Z},\ \frac{2m+1}{m-7} = 5$

∃ = quantifier; "there exists"; m = variable; $\mathbb{Z}$ = domain.

$\forall$ = "for all".

Example: 64 is a perfect square

↳ $\exists\, m \in \mathbb{Z},\ 64 = m^2$

m = variable; ∃ = quantifier; $\mathbb{Z}$ = domain; $64 = m^2$ = open sentence P(m)

Example: the graph $y = x^2 - 2x + 1$ has an x-intercept.

↳ $\exists x \in \mathbb{R}, \quad 0 = x^2 - 2x + 1$ } no occurance of y.

Quantified Statement	True	False
$\forall x \in S, P(x)$	$P(x)$ ✓ for All x	$P(x)$ ✗ for at least one x in S.
$\exists x \in S, P(x)$	$P(x)$ ✓ for at least 1 x	$P(x)$ ✗ for all x in S.

Consequence : Negation of a quantifcaiton statement

↳ $\neg(\forall x \in S, P(x)) \equiv (\exists x \in S, \neg P(x))$

↳ is equal to

Example: $\neg(\forall x \in \mathbb{R}, x^2 > 0)$
$\equiv (\exists x \in \mathbb{R}, \neg(x^2 > 0))$
$\equiv (\exists x \in \mathbb{R}, x^2 \not> 0)$
$\equiv (\exists x \in \mathbb{R}, x \leq 0)$.

Similarly: $\neg(\exists x \in S, P(x)) \equiv (\forall x \in S, \neg P(x))$

Nested Quantifiers

Example: $x^3 - y^3 = 1$

↳ $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ S.T. $x^3 - y^3 = 1$ ✓

↳ for every x, there is a y that statisfies $x^3 - y^3 = 1$

↳ $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}$ S.T $x^3 - y^3 = 1$ ✓

└ same as → two exististential quantifiers can be in either order!

↳ $\exists y \in \mathbb{R}, \exists x \in \mathbb{R}$ s.t $x^3 - y^3 = 1$ ✓

Negating $\forall x \in S, \exists y \in T$ s.t $Q(x,y)$

↳ $\neg(\forall x \in S, \exists y \in T$ s.t $Q(x,y))$.

↳ $\equiv \exists x \in S, \neg(\exists y \in T$ st $Q(x,y))$

↳ $\equiv \exists x \in S, \forall y \in T,$ st $\neg(Q(x,y))$.

Chapter 2: Logical Analysis (of Statements)

- Use letters A, B, C for abstract statements
  ↳ eg, A = (4 > 7) = false.

2.1 truth tables:

- Negation table:

A	¬A	¬(¬A)
T	F	T
F	T	F

2.2 The Junctions

- A, B each statements.
  ↳ compound statement including A and B:

- Conjunction = "and" = $\wedge$ (wedge) (eg: $A \wedge B$ = "a and b").
- disjunction = "or" = $\vee$ (vee) (eg: $A \vee B$ = "a or b").

- Conjunction Table :

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

- disjunction Table :

A	B	$A \wedge B$
T	T	T
T	F	T
F	T	T
F	F	F

2.3 Negation and the Junctions

A	B	$A \wedge B$	$\neg(A \wedge B)$	$A \vee B$	$\neg(A \vee B)$	$(\neg A) \vee (\neg B)$	$(\neg A) \wedge (\neg B)$
T	T	T	F	T	F	F	F
T	F	F	T	T	F	T	F
F	T	F	T	T	F	T	F
F	F	F	T	F	T	T	T

De Morgan's Law (DML)

↳ $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$

$\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$

Commulative Law (CL)

↳ $A \wedge B \equiv B \wedge A$

$A \vee B \equiv B \vee A$

Distributive Law (DL)

↳ $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

Assosciative Law (AL)

↳ $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$

$A \vee (B \vee C) \equiv (A \vee B) \vee C$

Example: Applications of "Logical Algebra/Arithmetic"

↳ Prove $\neg(A \wedge (\neg B \wedge C)) \equiv \neg(A \wedge C) \vee B$

↳ $(\neg A) \vee (\neg(\neg B \wedge C))$ DML

↳ $\neg A \vee B \vee \neg C$

↳ $(\neg A) \vee (\neg C) \vee B$

↳ $\neg(A \wedge C) \vee B$

2.4 Implication:

↳ $A \Rightarrow B$, "a implies b"

A	B	A⇒B
T	T	T
T	F	F
F	T	T
F	F	T

↳ example: $A = (\exists x \in \mathbb{R},\ (x > 2) \Rightarrow (x^2 > 4))$.

↳

$x > 2$	$x^2 > 4$	A
T	T	T
T	F	F
F	T	T
F	F	T

true!

↳ example: $B = (\exists x \in \mathbb{R},\ (x \geq 2),\ (x^2 > 4))$.

$x \geq 2$	$x^2 > 4$	B
T	F	T

A	B	C	A∨B	(A∨B)⇒C	A⇒C	B⇒C	(A⇒C)∧(B⇒C)
T	T	T	T	T	T	T	T
T	F	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	F	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	F	F	T	T	T	T

↳ $(A \vee B \Rightarrow C) \equiv ((A \Rightarrow C) \wedge (B \Rightarrow C))$

2.5: Converse and Contrapositive

↳ Converse of $(A \Rightarrow B)$ is $(B \Rightarrow A)$

↳ Contrapositive $(\neg B) \Rightarrow (\neg A)$.

↳ Truth table:

A	B	$A \Rightarrow B$	$\neg B$	$\neg A$	$(\neg B) \Rightarrow (\neg A)$	$B \Rightarrow A$
T	T	T	F	F	T	T
T	F	F	F	T	F	T
F	T	T	T	F	T	F
F	F	T	T	T	T	T

↳ $(A \Rightarrow B) \equiv (\neg B \Rightarrow \neg A)$ ✓

$(\neg B \Rightarrow \neg A) \not\equiv (B \Rightarrow A)$ ✗

Example: $\forall x \in \mathbb{R}, \quad x = 0 \Rightarrow \sin x = 0$

↳ contrapositive → $\forall x \in \mathbb{R}, \neg(\sin x = 0) \Rightarrow \neg(x = 0)$

↳ $\forall x \in \mathbb{R}, \sin x \neq 0 \Rightarrow x \neq 0$.

↳ converse → $(\forall x \in \mathbb{R}, (\sin x = 0) \Rightarrow x = 0)$.

2.6 If and only if

$A \Leftrightarrow B$ → "A if and only if B"

↳

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

p31

$(A \Leftrightarrow B) \equiv ((A \Rightarrow B) \wedge (B \Rightarrow A))$

Chapter 3 - proving statements

↳ basically a statement

Proposition → a mathematical statement which must be argued or proved to be true or false.

Theorem → a proposition that is deemed important.

Lemma → proposition used to support proof of a theorem. ↳ subroutine

Corollary → proposition which follows easily from another.

3.1 (Dis) proving universally-quantified statements

↳ $\forall x \in S,\ P(x)$.

Art/science of proof

- Let x denote an arbitrary element of S
- Using valid rules associated with S

→ often $P(x)$ is a relational statement (eg $f(x) < g(x)$)
→ Begin w/ one side and then work towards the other.

- discovery: you may need to find/devise a helpful rule.

Example: Prove $\forall \theta \in \mathbb{R}$, $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$.

↳ $\sin(3\theta) = \sin(2\theta + \theta)$

↳ $\sin(2\theta)\cos\theta + \cos(2\theta)\sin\theta$

↳ $2\sin\theta\cos\theta\cos\theta + (\cos^2\theta - \sin^2\theta)\sin\theta$

↳ $2\sin\theta(1-\sin^2\theta) + (1-\sin^2\theta-\sin^2\theta)\sin\theta$

↳ $3\sin\theta - 4\sin^3\theta$

3.2) Proving existentially quantified statements:

$\exists n \in \mathbb{Z},\ n^2+9n+5 = 0$

Proof: $n=-1$: $(-1)^2+9(-1)+5 = -3 < 0$

Search:

$n=$	-1	-2	-3	....
n^2+9n+5	-3	-9	-18	

Example: $\exists x \in \mathbb{R},\ \cos(2x)+\sin(2x)=3$

- Searching would be hopeless
- So try negation:

$\forall x \in \mathbb{R},\ \cos(2x)+\sin(2x) \neq 3.$

- $a \in \mathbb{R},\ |\cos a| \leq 1,\ |\sin a| \leq 1.$
- $z, w \in \mathbb{R},\ |z+w| \leq |z|+|w|.$ (triangle law)

Proof, take an arbitrary x in $\mathbb{R}$, notice $2x \in \mathbb{R}$.

↳ $|\cos(2x) + \sin(2x)| \leq |\cos 2x| + |\sin 2x|$

↳ $|\cos(2x) + \sin(2x)| \leq 1 + 1 \Rightarrow \leq 2$.

$2 \neq 3$, so $\cos(2x) + \sin(2x)$ is never 3, so fdp!

3.3) Proving implications:

Prove $A \Rightarrow B$ → assume A is true
using allowed rules to verify B
DO NOT assume that B is true

Proving quantified

$\forall x \in S, P(x) \Rightarrow Q(x)$ → assume $P(x)$
using rules of S, try to deduce $Q(x)$
Use $Q(x)$ as reference goal
↳ but DO NOT assume it.

Example: if m is an even integer, then $7m^3 + 4$ is even

$\exists k \in \mathbb{Z}, m = 2k$.

↳ $\forall m \in \mathbb{Z}, (\exists k \in \mathbb{Z}, m = 2k) \Rightarrow (\exists l \in \mathbb{Z}, 7m^3 + 4 = 2l)$.

Proof: Let $m \in \mathbb{Z}$, assume $m = 2k, k \in \mathbb{Z}$.

$7m^3 + 4 = 7(2k)^3 + 4 = 2(\underbrace{7 \cdot 4k^3 + 2}_{= l \in \mathbb{Z}})$ □

Example: if k^5 is a perfect square, then $9k^{19}$ is a perfect square.

$\exists n \in \mathbb{Z},\ m = n^2.$

Proof: $\exists n \in \mathbb{Z},\ k^5 = m^2$

$$9k^{19} = 9(k^{14} + k^5) = 3^2(k^{7^2} + k^5) = 3^2(k^{7^2} + m^2)$$

$$\hookrightarrow (3(k^7 + m))^2.$$

↳ let $n = 3(k^7 + m)$. Perfect square!

$(A \Rightarrow B) \equiv (\neg A) \vee B$

↳ therefore, $\neg(A \Rightarrow B) \equiv A \wedge (\neg B).$

Another Application: $A \Rightarrow (B \Rightarrow C) \equiv (A \wedge B) \Rightarrow C$

↳ Proof: $A \Rightarrow (B \Rightarrow C) \equiv (\neg A) \vee (B \Rightarrow C)$

$\equiv (\neg A) \vee ((\neg B) \vee C)$

Example: proving universally quantified statements:

↳ if $x \in \mathbb{R}$ ST 2^{2x} is odd then $2^{2x+3} + 6$ is even.

↳ aka:

hypothesis, "$2k$ is odd"

$\forall x \in \mathbb{R}, (\exists k \in \mathbb{Z}, 2^{2x} = 2k+1) \Rightarrow (\exists l \in \mathbb{Z}, 2^{2x+3}+6 = 2l)$

conclusion, "$2^{2x+3}+6$ is even"

↳ Proof: The hypothesis states $2^{2x} = 2k+1$ for some k in $\mathbb{Z}$.

- $2^{2x+3} + 6 \rightarrow 8 \cdot 2^{2x} + 6$
- $8 \cdot (2k+1) + 6$
- $2(8k+4+3)$

call this l

↳ ∴ if $l = 8k+7$, then $l \in \mathbb{Z}$ and $2^{2k+3}+6 = 2l$.

Definition: $a, b \in \mathbb{Z}$. a divides b, written as $a \mid b$ if $\exists k \in \mathbb{Z}$ ST $ak = b$.

Examples: $8 \mid 56$, as $8 \cdot 7 = 56$.
$8 \mid -56$, as $8 \cdot -7 = 56$
$56 \nmid 8$, as no $k \in \mathbb{Z}$ ST $56k = 8$.

Example: If $14 \mid m$, then $7 \mid m$.

↳ $\forall m \in \mathbb{Z}, (\exists k \in \mathbb{Z}, 14k = m) \Rightarrow (\exists l \in \mathbb{Z}, 7l = m)$.

↳ Proof: $14k = m$

$14 = 7 \cdot 2$

$m = 14k \rightarrow m = 7 \cdot 2k$

call this l.

Proposition: Transitivity of Division (TD)

↳ For all integers a, b, c, if $a \mid b$ and $b \mid c$, then $a \mid c$. → proof on plus lec notes pdf.

Corollary: For all integers a, b, c, if $a \mid b$, then $a \mid bc$.

Proposition: Divisibility of integer combinations (DIC)
↳ For all integers a, b, c, if $a \mid b$ and $a \mid c$, then for all integers x, y, $a \mid (bx + cy)$.

↳ symbolic form: hypothesis conclusion.

$\forall a, b, c \in \mathbb{Z}, (a \mid b) \wedge (a \mid c) \Rightarrow (\forall x, y \in \mathbb{Z}, a \mid (bx + cy))$

Proof:
Hypothesis: $\exists k, l \in \mathbb{Z}$ so $ak = b$, $al = c$.
Now if $x, y \in \mathbb{Z}$, let's consider $bx + cy$.

↳ $bx + cy = akx + aly = a(kx + ly)$

Thus, if $m = kx + ly$, then $m \in \mathbb{Z}$ and $bx + cy = am$.

Universally Quantified Statements:

↳ $\forall x \in S, P(x) \Rightarrow Q(x) \equiv \forall x \in S, \neg Q(x) \Rightarrow \neg P(x)$.

Proving $\forall x \in S, P(x) \Rightarrow (Q(x) \vee R(x))$
↓
Elimination Method: assume $P(x)$ is TRUE.

↳ case 1: assume $Q(x)$ is FALSE, determine truth of $R(x)$

↳ case 2: assume $R(x)$ is FALSE, determine truth of $Q(x)$.

↓

contrapositive method:

↳ $\forall x \in S,\ P(x) \Rightarrow (Q(x) \vee R(x))$

$\equiv \forall x \in S,\ \neg(Q(x) \vee R(x)) \Rightarrow \neg P(x)$

$\equiv \forall x \in S,\ (\neg Q(x) \wedge \neg R(x)) \Rightarrow \neg P(x)$.

Example: prove for real x that if $x^2 - 7x + 12 \geq 0$, then $x \leq 3$ or $x \geq 4$.

Discovery: $x^2 - 7x + 12 = x^2 - 2\frac{7}{2}x + 12 = x^2 - 2\frac{7}{2}x + \left(\frac{7}{2}\right)^2 - \left(\frac{7}{2}\right)^2 + 12$

$= \left(x - \frac{7}{2}\right)^2 - \frac{1}{4}$

↳ $x^2 - 7x + 12 = 0 \iff \left(x - \frac{7}{2}\right)^2 \geq \frac{1}{4}$

$\iff (2x - 7)^2 \geq 1$

symbolically: $\forall x \in \mathbb{R},\ (x^2 - 7x + 12 \geq 0) \Rightarrow (x \leq 3) \wedge (x \geq 4)$

Elimination Method:

Case 1: $\neg(x < 3) \equiv x > 3$

hypothesis: $(2x - 7)^2 \geq 1$ and $x > 3$

↳ sqrt → $|2x - 7| \geq 1 \rightarrow 2x \geq 8 \rightarrow x \geq 4$

Contrapositive Method:

$\forall x \in \mathbb{R},\ (x > 3) \wedge (x < 4) \Rightarrow (x^2 - 7x + 12 < 0)$

hypothesis: $3 < x < 4$.

$6 < 2x < 8$ ↓ $\times 2$

$-1 < 2x - 7 < 1$ ↓ -7

↳ $|2x - 7| < 1$

↳ $(2x-7)^2 < 1$

Proof by Contradiction:

↳ If A is a statement, then $A \wedge (\neg A)$ is always FALSE. The statement "$A \wedge (\neg A)$ is TRUE" is called a contradiction.

Method of Proof: step 1: existence

↳ show such x exists

Step 2: Uniqueness

2 submethods

↳ a) show that if $P(x)$ is true and $P(y)$ is true, then $x = y$. $(x, y \in S)$.

↳ b) contradiction → suppose $x \neq y$ so $P(x) \wedge P(y)$ is TRUE, establish contradiction.

Example: for $a, b \in \mathbb{Z}$, $a \neq 0$.

if $a|b$, then there is unique $k \in \mathbb{Z}$ s.t. $ak = b$.

PF: Existence: this is from definition

Uniqueness: a) let $k, l \in \mathbb{Z}$ and satisfy $ak = b$ and $al = b$. Hence $al = b = ak$

so $al - ak = a(l-k)$. $\therefore a \neq 0$, so $l = k$.

b) contradiction: suppose we had $k \neq l$ in $\mathbb{Z}$ so $ak : b$ and $al = b$. Then $ak = al$, so $0 : ak - ak : a(k-l)$. Since $k \neq l$ we must have $k - l \neq 0$, so $a : 0$. But this violates the hypothesis that $a \neq 0$.

Example: any two non-vertical, non-parallel lines have a unique intersection.

4.1 : Induction

Sum and Product Notation

↳ let $m \leq n$ in $\mathbb{N}$; $x_m, x_{m+1}, \ldots, x_n \in \mathbb{R}$. ($x_m \in \mathbb{R}$ if $m = n$)

Sum: $\sum_{i=m}^{n} x_i = x_m + x_{m+1} + \ldots + x_n$

Product: $\prod_{i=m}^{n} x_i = x_m \cdot x_{m+1} \cdot \ldots \cdot x_n$

Note: if $m > n$:

↳ sum: $\sum_{i=m}^{n} x_i = 0$ "empty sum"

↳ product: $\prod_{i=m}^{n} x_i = 1$ "empty product"

Sum Rules:

1) $\sum_{i=m}^{n} a x_i = a \sum_{i=m}^{n} x_i$ (distributive law)

↳ a: some constant

2) $\sum_{i=m}^{n} x_i + \sum_{i=m}^{n} y_i = \sum_{i=m}^{n} (x_i + y_i)$

3) **Breaking Sums**: $(m \le n \le p)$:

↳ $\sum_{i=m}^{p} x_i = \sum_{i=m}^{n} x_i + \sum_{i=n+1}^{p} x_i$

4) **Index Shift**: $0 \le m \le n$, $r \in \mathbb{N}$.

↳ $\sum_{i=m}^{n} x_i = \sum_{i=m+r}^{n+r} x_{i-r}$

Product Rules:

1) $\prod_{i=m}^{n} a x_i = a^{n-m+1} \prod_{i=m}^{n} x_i$

2) $\prod_{i=m}^{n} x_i \cdot \prod_{i=m}^{n} y_i = \prod_{i=m}^{n} (x_i \cdot y_i)$

3) **Breaking Products**: $(m \le n \le p)$:

↳ $\prod_{i=m}^{p} x_i = \prod_{i=m}^{n} x_i \cdot \prod_{i=n+1}^{p} x_i$

4) **Index Shift**: $0 \le m \le n$, $r \in \mathbb{N}$.

↳ $\prod_{i=m}^{n} x_i = \prod_{i=m+r}^{n+r} x_{i-r}$

Example:

↳ $\sum_{i=2}^{n} \ln\left(1-\frac{1}{i}\right) = \sum_{i=2}^{n} \ln\left(\frac{i-1}{i}\right) = \sum_{i=2}^{n} \left(\ln(i-1) - \ln(i)\right)$

$= \sum_{i=2}^{n} \ln(i-1) - \sum_{i=2}^{n} \ln(i)$

$= \sum_{i=1}^{n-1} \ln((i+1)-1) - \sum_{i=2}^{n} \ln(i)$

$= \ln(1) + \sum_{i=2}^{n-1} \ln(i) - \sum_{i=2}^{n-1} \ln(i) + \ln(n)$

↳ $\ln(1) - \ln(n) = -\ln(n) = \ln(1/n)$.

4.2: Proof By Induction:

↳ aka, principle of mathematical induction (POMI).

let for $n \in \mathbb{N}$, $P(n)$ be an open sentence.

if ① $P(1)$ is TRUE (base case)
② $P(n) \Rightarrow P(n+1)$ is true (induction step),

then $\forall n \in \mathbb{N}$, $P(n)$ is true!

Example: prove that $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

↳ base case: $\sum_{i=1}^{n} i(i+1) = 1(1+1) = 2$.

base case is true!

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

↳ inductive step:

↳ the induction hypothesis: assume $\sum_{i=m}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

↳ $\sum_{i=1}^{n+1} i(i+1) = \sum_{i=1}^{n} i(i+1) + (n+1)(n+2)$

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

$= \left(\frac{n}{3} + 1\right)(n+1)(n+2)$, factoring

↳ $\frac{(n+3)(n+1)(n+2)}{3}$

↳ $\frac{(n+1)((n+1)+1)((n+1)+2)}{3}$ ✓

Example: Does $6 \mid (2n^3+3n^2+n)$ for all n?

↳ base case: $n=1 \rightarrow 6 \mid (2+3+1) \rightarrow 6 \mid 6$ ✓.

↳ Induction step: $2(n+1)^3 + 3(n+1)^2 + (n+1)$

↳ $= 2(n^3+3n^2+3n+1) + 3(n^2+2n+1) + (n+1)$

$= (2n^3+6n^2+6n+2) + 3n^2+6n+3+n+1$

$= (2n^3+3n^2+n) + (6n^2+12n+6)$

$= 6k + 6(n^2+2n+1)$, $k \in \mathbb{Z}$, $(n^2+2n+1) \in \mathbb{Z}$

inductive hypothesis: $6 \mid (2n^3+3n^2+n)$.

Thus by DJC, $6 \mid (2(n+1)^3 + 3(n+1)^2 + n)$ $\forall n \in \mathbb{N}$

By POMI, $6 \mid (2n^3 + 2n^2 + n)$ $\forall n \in \mathbb{N}$.

Set Theory:

5.1: Set construction:

· Empty set: $\emptyset = \{\}$ the set of no elements.

· Cardinality of sets (size): $|S|$ (the # of elements in S)

↳ $A = \{1, 2, 3, \dots, 1001\} \rightarrow |A| = 1001$

⇢ $\{\emptyset\}$ → the set of the empty set.

$\{1, 2, \{1, 2\}\} \rightarrow |S| = 3$ → $|\mathbb{Z}| = |\mathbb{R}| = \infty$!

Set builder notation:

↳ U → universe in which we want the set (eg $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{N}$).

Type 1: $P(x)$, an open sentence, $x \in U \rightarrow \{x \in U : P(x)\}$ (⇢ x in U ST P(x) is true!)

Type 2: Function $f : U \to U$ (U another universe, usually $U : U$).

Type 3: $\{f(x) : x \in U, P(x)\}$ (⇢ range of f for those x s.t. P(x) is true.)

Example: $U = \mathbb{R}^2$, consider points of distance 8 from the origin

type 1: $\{(x,y) \in \mathbb{R}^2 : \underbrace{x^2+y^2=64}_{P(x)}\}$

Eg 2: The set of integers divisible by 7:

type 1: $\{z \in \mathbb{Z},\ 7 \mid z\}$

type 2: $\{7k : k \in \mathbb{Z}\}$

Eg 3: the set of odd integers divisible by 7

type 1: $\{n \in \mathbb{Z} : (7 \mid n) \wedge (2 \nmid n)\}$

type 2: $\{7(2n+1) : k \in \mathbb{Z}\}$

type 3: $\{7h : h \in \mathbb{Z}, 2 \nmid h\}$

5.3 Set operations:

S, T are sets $\in U$.

Union $S \cup T \to \{x \in U : (x \in S) \vee (x \in T)\}$

Intersection: $S \cap T \to \{x \in U : (x \in S) \wedge (x \in T)\}$

Difference: $S - T \to \{x \in U : (x \in S) \wedge (x \notin T)\}$

↳ $= S - (S \cap T)$

Complement: $S = \{x \in U ; x \notin S\} = (U - S)$

The art of proof

↳ $\forall x \in U, P(x) \Rightarrow Q(x)$

- Make sure to identify hypothesis ($P(x)$) and conclusion ($Q(x)$).
- Discovery: find out what is required

$(A <=> B) = A \Rightarrow B \wedge B \Rightarrow A$

↳ contrapositive → $(\neg B \Rightarrow \neg A) \wedge (\neg A \Rightarrow \neg B)$

$\equiv (\neg A) <=> (\neg B)$

↳ $(A <=> B) \equiv (\neg A) <=> (\neg B)$

Example: show for real x that $x^2 - x > 0 <=> x \notin [0,1]$

↳ $\forall x \in \mathbb{R}, (x^2 - x > 0) <=> (x \notin [0,1])$

$\equiv \forall x \in \mathbb{R}, (x^2 - x \leq 0) <=> (x \in [0,1])$

- hypothesis: $x^2 - x \leq 0 = x(x-1) \leq 0$

$\Rightarrow ((x \leq 0) \wedge (x - 1 \geq 0)) \vee ((x \geq 0) \wedge (x - 1 \leq 0))$

cannot be true → empty set

↳ $(x \in \emptyset) \vee (0 \leq x \leq 1)$

↳ $x \in [0,1]$

Example: if S is a set, then there is a unique set T such that $T \subseteq S$ and $S \cap T = S$.

let $T = S$

↳ $S \subseteq S$ and $S \cap S = S$.

Example: Show that there are no integers p, q for which $p^2 - q^2 = 10$

↳ $(p+q)(p-q) = 10$ → divisors: $\pm 1, \pm 2, \pm 5, \pm 10$

$p+q = p-q+2q$ → both odd or both even

case 1: both odd: $p-q = 2k+1 \rightarrow p+q = 2l+1$, $k, l \in \mathbb{Z}$.

↳ even = odd · odd = false!

case 2: $p-q = 2k$, $p+q = 2l$, $k, l \in \mathbb{Z}$.

↳ $(p-q)(p+q) = (2k)(2l) = 4kl$

↳ $4kl = 10 \rightarrow 4 \nmid 10$, so contradiction!

∴ no p, q exist!

Example: prove for $n \geq 2$ that $\underbrace{\prod_{j=2}^{n}\left(1-\frac{1}{j^2}\right)=\frac{n+1}{2n}}_{P(n)}$

base case: $n=2$.

↳ $\prod_{j=2}^{2}\left(1-\frac{1}{j^2}\right)=\left(1-\frac{1}{2^2}\right)=1-\frac{1}{4}=\frac{3}{4}$.

$\frac{n+1}{2n}=\frac{2+1}{4}=\frac{3}{4}$ ← base case holds!

Inductive step:

↳ Inductive hypothesis: $\prod_{j=2}^{n}\left(1-\frac{1}{j^2}\right)=\frac{n+1}{2n}$ holds for $n \geq 2$.

Compute: $\prod_{j=2}^{n+1}\left(1-\frac{1}{j^2}\right)$

↳ $=\prod_{j=2}^{n}\left(1-\frac{1}{j^2}\right)\left(1-\frac{1}{(n+1)^2}\right)$

inductive hypothesis

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

↳ $\frac{n+1}{2n}\left(\frac{(n+1)^2-1}{(n+1)^2}\right)$

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

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

$=\frac{1}{2}\left(\frac{n+2}{n+1}\right) \rightarrow \frac{(n+1)+1}{2(n+1)}$ ▨

Example: let $f_1=1$, $f_2=1$. → $f_{n+2}=f_n+f_{n+1}$.

↳ show that $f_n < \left(\frac{7}{4}\right)^n$ for all n.

base case: $f_1 = 1 < \frac{7}{4}$

$f_2 = 1 < \frac{49}{16}$ } base case holds!

Inductive Step: (POSI) $k = 1, \dots, n$.

↳ Inductive Hypothesis: $n \geq 2$ and $f_k < \left(\frac{7}{4}\right)^k$

Now: $f_{n+1} = f_{n-1} + f_n < \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^n$

$= \left(\frac{7}{4}\right)^{n-1}\left(1 + \frac{7}{4}\right) = \left(\frac{7}{4}\right)^{n+1}\left(\frac{11}{4}\right)$

$= \left(\frac{7}{4}\right)^{n-1} \cdot \frac{44}{16} < \left(\frac{7}{4}\right)^{n+1} \frac{49}{16} = \left(\frac{7}{4}\right)^{n+1}$ ▨

Chapter 6: Greatest Common Divisor

6.1: Division algorithm:

↳ Proposition: if $a, b \in \mathbb{Z}$, $a \neq 0$ and $b \mid a$, then $|b| \leq |a|$.

BBD (Bound by divisibility):

Proof: $a \neq 0$, $b \mid a$. $\in \mathbb{Z}$.

∴ there is $k \in \mathbb{Z}$ so $bk = a$

↳ $|b||k| = |bk| = |a|$ since $|a| \neq 0$, $k \neq 0$ $|k| \geq 1$.

∴ $|b| \leq |b||k| = |a|$ ie $|b| \leq |a|$ □

Corollary: For a, b as above $b \leq |a|$

↳ $-|b| \leq b \leq |b|$, so $b \leq |b|$ where $|b| \leq |a|$ □

Proposition: Division Algorithm: (DA)

↳ if a, b are integers and $b > 0$ then there are unique $q, r \in \mathbb{Z}$ so that

$a = qb + r$, where $0 \leq r < b$

Proof Uniqueness:

we suppose that $a = qb + r$, $0 \leq r < b$, $q, r \in \mathbb{Z}$.

$a = q_1 b + r_1$, $0 \leq r_1 < b$, $q_1, r_1 \in \mathbb{Z}$.

$0 = a - a = (qb + r) - (q_1 b + r_1) = (q - q_1)b + (r - r_1)$

↳ $-(r - r_1) = (q - q_1)b$

↳ $|r - r_1| = |q - q_1| b$ → $b > 0$ anyways.

↳ $|r - r_1| < b$

$\therefore |q - q_1| b = |r - r_1| < b$

↳ $|q - q_1| < 1$ as $b > 0$

↳ as $q_1, q \in \mathbb{Z}$, $|q - q_1| \in \{0\} \cup \mathbb{N}$.
with $|q - q_1| < 1$, so $q = q_1$.

$\therefore qb + r = q_1 b + r_1, q = q_1$.

↳ $qb + r = qb + r_1 \rightarrow r = r_1$. □.

$q \rightarrow$ quotient
$r \rightarrow$ remainder.

Proposition: Division Algorithm. (DA).

Let a, b be integers with $b > 0$.

Then there exists unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.

↳ eg: $a = 17, b = 3$: $17 = 5 \cdot 3 + 2$.

Proof (existence):

define floor function $\lfloor x \rfloor$ as the greatest integer less than or equal to x.

↳ assume : $\lfloor x \rfloor = m \in \mathbb{Z}$.
↳ $m \leq x < m + 1$

↳ $0 \leq x - m < 1$.

Given $a, b \in \mathbb{Z}$, $b > 0 \rightarrow \frac{a}{b} \in \mathbb{R}$.

Claim: $q = \lfloor \frac{a}{b} \rfloor \in \mathbb{Z}$, $r = a - qb \in \mathbb{Z}$

It remains to show that $0 \leq r < b$:

↳ $0 \leq \frac{a}{b} - \lfloor \frac{a}{b} \rfloor < 1$

| multiply by b

↳ $0 \leq a - b\lfloor \frac{a}{b} \rfloor < b$ ☒.

($q = \lfloor \frac{a}{b} \rfloor$, $r = a - b\lfloor \frac{a}{b} \rfloor$)

Greatest Common Divisor (GCD):

↳ Let $a, b \in \mathbb{Z}$. A common divisor of a and b is $c \in \mathbb{Z}$ such that $c|a$ and $c|b$.

GCD rules:

↳ 1) $GCD(0, 0) = 0$
2) $GCD(a, a) = |a|$
3) $GCD(a, 0) = |a|$
4) $GCD(a, 1) = GCD(a, -1) = 1$.

Proposition: GCD w/ remainder $a - bq = r$

↳ For all $a, b, q, r \in \mathbb{Z}$ with $a = qb + r$ we have $\gcd(a, b) = \gcd(b, r)$.

Proof: Divisibility integer combinations: $\forall a, b \in \mathbb{Z}$, $a \mid b$ and $a \mid c \Rightarrow a \mid (bx + cy)$ $\forall x, y \in \mathbb{Z}$.

Let $\gcd(a, b) = d$. $\Rightarrow d \mid a$, $d \mid b$.

↳ goal: Show that $d = \gcd(b, r)$

(i) d is $\gcd(b, r)$, so show $d \mid b$ and $d \mid r$.
(ii) for any common divisors c of b and r, $c \leq d$.

(i) already know $d \mid b$ because $d = \gcd(a, b)$.

Using DIC: $d \mid \underbrace{a(1) + b(-q)}_{r = a - bq} \Rightarrow d \mid r$. ($x = 1$, $y = -q$)

(ii) if $c \mid b$ and $c \mid r$, then show $c \leq d$.

↳ if $c \mid a$, then c is a common divisor of a and b. But, since $d = \gcd(a, b)$, $c \leq d$.

↳ $c \mid qb + r \Rightarrow c \mid a$.

Example: Find $\gcd(84, 120)$

↳ $120 = 1 \cdot \underbrace{84}_{b} + \underbrace{36}_{r}$ (form of $a = qb + r$).

↳ $\gcd(84, 120) = \gcd(84, 36)$.

↳ $84 = 1 \cdot 36 + 48$

↳ $\gcd(84, 36) = \gcd(36 + 48)$

↳ $48 = 36 + 12$

↳ $\gcd(36, 48) = \gcd = (36, 12)$

↳ obviously, $\gcd(12, 36) = 12$!

Bounds By Divisibility (BBD):

↳ $\forall a, b \in \mathbb{Z}$, if $b \mid a$ and $a \neq 0$, then $b \leq |a|$.

Division Algorithm (DA):

↳ $\forall a \in \mathbb{Z}, \forall a \in \mathbb{N}, \exists q, r \in \mathbb{Z}$ st $\underbrace{a = qb + r}_{0 \leq r < b}$

GCD With Remainders (GCD WR)

↳ $\forall a, b, q, r \in \mathbb{Z}$, if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

↳ Example: $\gcd(1386, 322)$:

the euclidean algorithm

$1386 = 4(322) + 98 \quad = \gcd(322, 98)$

$322 = 3(98) + 28 \quad = \gcd(98, 28)$

$98 = 3(28) + 14 \quad = \gcd(28, 14)$

$28 = 2(14) + 0 \quad = \gcd(14, 0)$

since $\gcd(14, 0) = 14$, $\gcd(1386, 322) = 14$.

Example 2: show that $\gcd(22a + 7, 3a + 1) = 1$:

$22a + 7 = 7(3a+1) + a \quad = \gcd(3a+1, a)$

$3a + 1 = 3(a) + 1 \quad = \gcd(a, 1)$.

since $\gcd(a, 1) = 1$, $\gcd(22a + 7, 3a + 1) = 1$.

Example 3: show that $\gcd(a^2, a+1) = 1$

$a^2 = (a-1)(a+1) + 1 \quad = \gcd(a+1, 1)$.

since $\gcd(a+1, 1) = 1$, $\gcd(a^2, a+1) = 1$.

GCD Characterization Theorem (GCD CT):

$\forall a, b \in \mathbb{Z}$, $\forall d \in \mathbb{N}$, if:

- $d \mid a$ and $d \mid b$,
- $\exists s, t \in \mathbb{Z}$ ST $as + bt = d$,

then $d = \gcd(a, b)$.

↳ Example: gcd(1386, 322)

↳ since $14 \mid 1386$ and $14 \mid 322$,
and since $1386(10) + 322(-43) = 14$,

$\gcd(1386, 322) = 14$.

↳ aka, Beizout's Identity

Beizout's Lemma (BL):

↳ $\forall a, b \in \mathbb{Z}$, $\exists s, t \in \mathbb{Z}$ st $as + bt = \gcd(a, b) = d$.

The Extended Euclidean Algorithm (EEA):

↳ table with 4 columns: x, y, q, r.
the first row is: $(1, 0, a, 0)$
the second row is: $(0, 1, b, 0)$.
$q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$

$\text{row}_i \leftarrow \text{row}_{i-2} - q_i \, \text{row}_{i-1}$

Stop when $r_i = 0$.

↳ $\gcd(a, b) = r_{i-1}$
$s = x_{i-1}$, $t = y_{i-1}$

↳ Example: gcd(2172, 423)

↳

x	y	r	q
1	0	2172	0
0	1	423	0
1	-5	57	5
-7	36	24	7
15	-77	9	2
-37	190	6	2
52	-267	3	1
-141	724	0	2

$\gcd(2172, 423) = 3$

$s = 52, \quad t = -267$

↳ certificate of correctness

↳ $2172(52) + 423(-267) = 3$

Common Divisor Divides GCD (CODGCD):

↳ $\forall a, b, c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.

Coprime Characterization Theorem (CCT):

↳ $\forall a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$ iff $\exists s, t \in \mathbb{Z}$ ST $as + bt = 1$.

Division by the GCD (DBGCD):

↳ $\forall a, b \in \mathbb{Z}$, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ where $d = \gcd(a, b)$.

$a \neq 0$
$b \neq 0$.

Coprimeness and Divisibility (CAD):

↳ $\forall a, b, c \in \mathbb{Z}$, if $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

Prime Factorization (PF):

↳ Every natural number can be written as a product of primes.

Euclid's Lemma (EL):

↳ $\forall a, b \in \mathbb{Z}$, and prime numbers p, if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Unique Factorization Theory (UFT)

↳ every natural number can be written as a product of prime factors uniquely.

Finding a Prime Factor (FPF)

↳ Every natural number $n > 1$ is either prime or has a prime factor $\leq \sqrt{n}$.

Divisors From Prime Factorization (DFPF):

↳ let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

the integer c is a positive divisor of n iff:

↳ $c = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ where $0 \leq b_i \leq a_i$.

GCD From Prime Factorization (GCD PF):

↳ let $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, and $b = p_1^{b_1} p_2^{b_1} \cdots p_k^{b_k}$

$\gcd(a,b) = p_1^{y_1} p_2^{y_1} \cdots p_k^{y_k}$ where $y_i = \min(a_i, b_i)$.

Linear Diophantine Equation Theorem, Part 1 (LDET 1):

↳ $\forall a, b, c \in \mathbb{Z}$, $ax + by = c$ has an integer solution iff $\gcd(a,b) \mid c$.

↳ Example: $84x + 35y = 63$

x	y	r	q
1	0	84	0
0	1	35	0
1	-14	14	2
-2	5	7	2
5	-12	0	2

since $\gcd(84,35) = 7 \mid 63$, there is a solution.

from the table, $s = -2$, $t = 5$.

↳ $84(-2) + 35(5) = 7$

$84(-2 \cdot 9) + 35(5 \cdot 9) = 63$

$84(-18) + 35(45) = 63$

↳ $x = -18, \quad y = 45$.

Linear Diophantine Equation Theorem, Part 2 (LDET 2):

↳ if $x = x_0$ and $y = y_0$ is one particular integer solution to the linear diophantine equation $ax + by = c$, then the set of all solutions is given by:

↳ $\{(x, y) \mid x = x_0 + \frac{b}{\gcd(a,b)} n, \; y = y_0 - \frac{a}{\gcd(a,b)} n, \; n \in \mathbb{Z}\}$.

↳ Previous Example continued:

↳ $\{(x,y) \mid x = -18 + \frac{35}{7} n, \; y = 45 - \frac{84}{7} n, \; n \in \mathbb{Z}\}$.

↳ $\{(x,y) \mid x = -18 + 5n, \; y = 45 - 12n, \; n \in \mathbb{Z}\}$.

Congruence is Equivelence Relation (CER):

↳
- $a \equiv a \pmod{m}$
- if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Congruence Add and Multiply (CAM):

↳ if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$:

↳ $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

$a_1 a_2 = b_1 b_2 \pmod m$.

Congruence Power (CP):

↳ $\forall n \in \mathbb{N}, \forall a, b \in \mathbb{Z}$, if $a \equiv b \pmod m$, then $a^n \equiv b^n \pmod m$

Congruence Divide (CD):

↳ $\forall a, b, c \in \mathbb{Z}$, if $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod m$.

Congruent Iff Same Remainder (CISR):

↳ $\forall a, b \in \mathbb{Z}$, $a \equiv b \pmod m$ iff a and b have the same remainder when divided by m.

Congruent to Remainder (CTR):

↳ $\forall a, b \in \mathbb{Z}$ with $0 \leq b < m$, $a \equiv b \pmod m$ iff a has a remainder b when divided by m.

Example: what is the remainder when 3^{47} is divided by 7?

$3^3 = 27 = -1 \pmod 7$

$3^{47} \equiv 3^{45+2} \pmod 7$

$\equiv 9\,(3^{45}) \pmod 7$

$\equiv 9\,(3^3)^{15} \pmod 7$

$\equiv 9(-1)^{15} \pmod 7$

$\equiv -9 \pmod 7$

$\equiv -2 \pmod 7$

$\equiv 5 \pmod 7$. → remainder is 5.

Linear Congruence Theorem (LCT):

↳ $ax \equiv c \pmod m$ has a solution iff $\gcd(a, m) \mid c$.

if x_0 is one particular solution to this congruence, then the set of all solutions is given by:

↳ $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{\gcd(a,m)}}\}$, or, equivalently,

$\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod m\}$.

$m_1 = 0.11$

$r = 0.121$

$\omega = 5.49$

$I = 3.29 \cdot 10^{-4}$

$m_2 = 0.0444$

$I_1 \omega_1 = I_2 \omega_2$

$I_1 \omega_1 = (I_1 + m_2 R^2)\omega_2$

$$\frac{3.29 \times 10^{-4} \times 5.49}{3.29 \times 10^{-4} + 0.0444(0.121^2)} = \omega_2$$

$M = 23.8$

$R = 0.761$

$I = 380$

$m = 0.695$

$v = 7.25$

$0.0693 + m_2 L^2 + m_3 L^2$