

MA 299 ~ MATHEMATICAL PROOFS  
CLASS ASSIGNMENTS

December 4, 2025

CONTENTS

0	General Process 8/28/25	1
1	Vector Proofs 9/4/25	4
2	Limits using the Definition 9/11/25	6
3	Derivative Power Rule 9/18/25	10
4	Triangle Inequality for Vectors 9/25/25	13
5	Density Functions 10/2/25	15
6	Annuities 10/23/25	18
7	Algebraic Groups 10/30/25	20
8	Euclid's Lemma 11/6/25	22
9	DeMoivre's Theorem 11/13/25	24
10	Archimedean Property 11/20/25	26
11	Properties of Sets 12/4/25	28

Anything repeatable follows a process - learn the process, and you can repeat it too

Describe all ideas in your own words - do NOT use jargon until you can explain the jargon in your own words without preparing/looking anything up

1. determine the style of proof needed: 2 most common types are direct and inductive proof (with cases, contrapositive, and contradiction also showing up as subsets of direct proof)

2. follow the general process for each style:

- direct: start with relevant definitions and already proven theory; building stepping stones (logical consequence of one of more of the above)
  - (a) start with givens and definitions
  - (b) identify what you need to show (but don't start here)
  - (c) consider any other definitions, already proven theory, logic, algebra, etc that relates
  - (d) devise a path from start to end
  - (e) fill in the details of the path

**cases:** enumerate all the possibilities of something related and then address each case (usually using a direct proof)

**contrapositive:** if trying to prove  $a \implies b$ , then use another proof technique on  $\neg b \implies \neg a$

**contradiction:** suppose what you are trying to prove is wrong, then use another proof technique (with the above assumption as part of the givens, usually direct)

**uniqueness** is a special case of contradiction: suppose two distinct and show they must be the same

- induction:
  - (a) show it's true for a base case (often  $n = 1$ )
  - (b) show you can get from one step to the next: suppose it's true for a general  $n$  then show you can get from true for  $n$  to true for  $n + 1$  (usually use direct proof techniques here)

3. focus on the process of the proofs - this is how you learn them for tests and this is how you develop the skill of doing them

4. don't forget bi-directional proofs (either both ways always, or do the proof twice)

**Theorem.** Given  $\lim_{x \rightarrow c} f(x) = L$  and  $\lim_{x \rightarrow c} g(x) = K$ , then  $\lim_{x \rightarrow c} f(x) + g(x) = L + K$

*Proof.* Let  $\frac{\epsilon}{2} > 0$ , then there exists  $\delta_f, \delta_g$  such that

if  $0 < |x - c| < \delta_f$  then  $|f(x) - L| < \frac{\epsilon}{2}$ , and if  $0 < |x - c| < \delta_g$  then  $|g(x) - K| < \frac{\epsilon}{2}$ .

Let  $\delta = \min\{\delta_f, \delta_g\}$ ,

then  $|(f(x) + g(x)) - (L + K)| = |(f(x) - L) + (g(x) - K)| \leq |f(x) - L| + |g(x) - K|$  by the triangle inequality  
and  $|f(x) - L| + |g(x) - K| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$  by the given

$$\implies |(f(x) + g(x)) - (L + K)| < \epsilon$$

$$\implies \lim_{x \rightarrow c} f(x) + g(x) = L + K \quad \square$$

**Theorem.**  $x^2 \geq 0$  for all  $x \in \mathbb{R}$

*Proof.* Case 1: let  $x \geq 0$ , then

$$\begin{aligned} x &\geq 0 \\ \implies x \cdot x &\geq 0 \cdot x \quad \text{by the multiplication property of inequalities} \\ \implies x^2 &\geq 0 \end{aligned}$$

Case 2: let  $x < 0$ , then

$$\begin{aligned} x &< 0 \\ \implies x \cdot x &> 0 \cdot x \quad \text{by the multiplication (reversal) property of inequalities} \\ \implies x^2 &\geq 0 \end{aligned} \quad \square$$

**Theorem.** Let  $f$  be a real-valued continuous function, then  $\frac{d}{dx} x^n = nx^{n-1}$  for  $n \in \mathbb{Z}^>$

*Proof.* Let  $n \in \mathbb{Z}^>$ . Consider an inductive argument:

Base  $n = 1$       $\frac{d}{dx} x^1 = \lim_{h \rightarrow 0} \frac{(x+h)^1 - x^1}{h} = 1 = 1x^{1-1}$

Suppose      $\frac{d}{dx} x^k = kx^{k-1}$  holds for some  $k \in \mathbb{Z}^>$

Show      $\frac{d}{dx} x^{k+1} = (k+1)x^{(k+1)-1} = (k+1)x^k$  holds.

$$\frac{d}{dx} x^{k+1} = \frac{d}{dx} (x^k \cdot x) = \frac{d}{dx} x^k \cdot x + x^k \cdot \frac{d}{dx} x = kx^{k-1} \cdot x + x^k \cdot 1 = kx^k + x^k = (k+1)x^k$$

Therefore      $\frac{d}{dx} x^n = nx^{n-1}$  holds for  $n \in \mathbb{Z}^>$       $\square$

**Theorem.** *If  $a^2 + b^2$  is odd, then exactly one of the numbers  $a$  or  $b$  is odd.*

*Proof.* Consider the contrapositive statement:

if either both  $a$  and  $b$  are odd or both even then  $a^2 + b^2$  is even

Case 1: let  $a$  and  $b$  both be even, then

there exists  $p \in \mathbb{Z}$  such that  $a = 2p$  and there exists  $q \in \mathbb{Z}$  such that  $b = 2q$

$\implies a^2 = 4p^2 = 2(2p^2)$  and since  $p \in \mathbb{Z} \implies 2p^2 \in \mathbb{Z}$  by closure of  $\mathbb{Z}$  over multiplication  
and  $b^2 = 4q^2 = 2(2q^2)$  and since  $q \in \mathbb{Z} \implies 2q^2 \in \mathbb{Z}$  by closure of  $\mathbb{Z}$  over multiplication

therefore  $a^2 + b^2 = 2(2p^2 + 2q^2)$  where  $2p^2 + 2q^2 \in \mathbb{Z}$  by closure of  $\mathbb{Z}$  over addition

$\implies a^2 + b^2$  is even.

Case 2: let  $a$  and  $b$  both be odd, then

there exists  $p \in \mathbb{Z}$  such that  $a = 2p + 1$  and there exists  $q \in \mathbb{Z}$  such that  $b = 2q + 1$

$\implies a^2 = 4p^2 = 2(2p^2 + 2p) + 1$  and since  $p \in \mathbb{Z} \implies 2p^2 + 2p \in \mathbb{Z}$  by closure of  $\mathbb{Z}$  over  $+$  and  $\cdot$   
and  $b^2 = 4q^2 = 2(2q^2 + 2q) + 1$  and since  $q \in \mathbb{Z} \implies 2q^2 + 2q \in \mathbb{Z}$  by closure of  $\mathbb{Z}$  over  $+$  and  $\cdot$

therefore  $a^2 + b^2 = 2(2p^2 + 2p + 2q^2 + 2q + 1)$

where  $2p^2 + 2p + 2q^2 + 2q + 1 \in \mathbb{Z}$  by closure of  $\mathbb{Z}$  over  $+$

$\implies a^2 + b^2$  is even.

□

**Theorem 1.1.** *Let  $\mathbf{v} \in \mathbb{R}^n$ , then  $\|\mathbf{v}\| = 0$  iff  $\mathbf{v} = \mathbf{0}$ .*

**Theorem 1.2.** *Let  $\mathbf{u}$  and  $\mathbf{v}$  be orthogonal unit vectors. Then  $\mathbf{u} \times \mathbf{v}$  is also a unit vector.*

**Definitions.** Let  $\mathbf{v} \in \mathbb{R}^n$ , then  $\|\mathbf{v}\| = \left(\sum_{i=1}^n v_i^2\right)^{\frac{1}{2}}$ , and  $\mathbf{v}$  is a unit vector iff  $\|\mathbf{v}\| = 1$ .

Let  $\mathbf{u}$  and  $\mathbf{v} \in \mathbb{R}^3$ , then  $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^3 u_i v_i = u_1 v_1 + u_2 v_2 + u_3 v_3$  and  $\mathbf{u} \times \mathbf{v} = \langle u_2 v_3 - u_3 v_2, -u_1 v_3 + u_3 v_1, u_1 v_2 - u_2 v_1 \rangle$ .

The vectors  $\mathbf{u}$  and  $\mathbf{v}$  are said to be orthogonal if the angle between them is  $90^\circ$ .

**Theorem.** Given non-zero vectors,  $\vec{u}$  and  $\vec{v}$ , let  $\theta$  be the angle between them. Then

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\| \cos \theta \quad \text{and} \quad \|\mathbf{u} \times \mathbf{v}\| = \|\mathbf{u}\| \|\mathbf{v}\| \sin \theta.$$

**Theorem.** Let  $\mathbf{v} \in \mathbb{R}^n$ , then  $\|\mathbf{v}\| = 0$  iff  $\mathbf{v} = \mathbf{0}$ .

*Proof.* Consider both directions:

( $\implies$ ) Let  $\mathbf{v} \in \mathbb{R}^n$ , such that  $\|\mathbf{v}\| = 0$ .

$$\implies 0 = \left(\sum_{i=1}^n v_i^2\right)^{1/2} \implies 0^2 = 0 = \sum_{i=1}^n v_i^2$$

Suppose  $\mathbf{v} \neq \mathbf{0} \implies \exists k \in \{1, \dots, n\} \ni v_k \neq 0$

$\implies v_i \geq 0$  for all  $i \in \{1, \dots, n\}$  and  $v_k > 0$

$$\implies \sum_{i=1}^n v_i^2 > 0 \implies \Leftarrow$$

Therefore if  $\|\mathbf{v}\| = 0$ , then  $\mathbf{v} = \mathbf{0}$ .

( $\Leftarrow$ ) Let  $\mathbf{v} \in \mathbb{R}^n$ , such that  $\mathbf{v} = \mathbf{0}$ .

$\implies v_i = 0$  for all  $i \in \{1, \dots, n\}$

$$\|\mathbf{v}\| = \left(\sum_{i=1}^n v_i^2\right)^{1/2} = \left(\sum_{i=1}^n 0^2\right)^{1/2} = 0$$

Therefore if  $\mathbf{v} = \mathbf{0}$ , then  $\|\mathbf{v}\| = 0$ .

Therefore  $\|\mathbf{v}\| = 0$  iff  $\mathbf{v} = \mathbf{0}$ . □

**Theorem.** Let  $\mathbf{u}$  and  $\mathbf{v}$  be orthogonal unit vectors. Then  $\mathbf{u} \times \mathbf{v}$  is also a unit vector.

*Proof.* The hard way ... Let  $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$ , and let  $\mathbf{u}$  and  $\mathbf{v}$  be orthogonal unit vectors  $\implies \|\mathbf{u}\| = \|\mathbf{v}\| = 1$  and  $\theta = 90^\circ$  is the angle between  $\mathbf{u}$  and  $\mathbf{v}$ . Then  $\|\mathbf{u}\| = \|\mathbf{v}\| = 1$  and  $\mathbf{u} \cdot \mathbf{v} = 0$ .

Consider  $\mathbf{u} \times \mathbf{v} = \langle u_2 v_3 - v_2 u_3, -u_1 v_3 + u_3 v_1, u_1 v_2 - u_2 v_1 \rangle$ .

$$\begin{aligned} \implies \|\mathbf{u} \times \mathbf{v}\|^2 &= u_2^2 v_3^2 - 2u_2 u_3 v_2 v_3 + v_2^2 u_3^2 + u_1^2 v_3^2 - 2u_1 u_3 v_1 v_3 + u_3^2 v_1^2 + u_1^2 v_2^2 - 2u_1 u_2 v_1 v_2 + u_2^2 v_1^2 \\ &= u_1^2 (v_1^2 + v_2^2 + v_3^2) - u_1^2 v_1^2 + u_2^2 (v_1^2 + v_2^2 + v_3^2) - u_2^2 v_2^2 + u_3^2 (v_1^2 + v_2^2 + v_3^2) - u_3^2 v_3^2 \\ &\quad - 2(u_2 u_3 v_2 v_3 + u_1 u_3 v_1 v_3 + u_1 u_2 v_1 v_2) \\ &= u_1^2 + u_2^2 + u_3^2 - u_1^2 v_1^2 - u_2^2 v_2^2 - u_3^2 v_3^2 - 2(u_2 u_3 v_2 v_3 + u_1 u_3 v_1 v_3 + u_1 u_2 v_1 v_2) \\ &= 1 - (u_1^2 v_1^2 + 2u_2 u_3 v_2 v_3 + u_2^2 v_2^2 + 2u_1 u_3 v_1 v_3 + u_3^2 v_3^2 + 2u_1 u_2 v_1 v_2) \\ &= 1 - (u_1 v_1 + u_2 v_2 + u_3 v_3)^2 = 1 - (\mathbf{u} \cdot \mathbf{v})^2 = 1 - 0^2 = 1 \end{aligned}$$

Therefore  $\|\mathbf{u} \times \mathbf{v}\| = 1$ , and  $\mathbf{u} \times \mathbf{v}$  is a unit vector. □

*Proof.* The easy way ... Let  $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$ , and let  $\mathbf{u}$  and  $\mathbf{v}$  be orthogonal unit vectors

$\implies \|\mathbf{u}\| = \|\mathbf{v}\| = 1$  and  $\theta = 90^\circ$  is the angle between  $\mathbf{u}$  and  $\mathbf{v}$ .

$\implies \|\mathbf{u} \times \mathbf{v}\| = \|\mathbf{u}\| \|\mathbf{v}\| \sin \theta = 1 \cdot 1 \cdot \sin \frac{\pi}{2} = 1 \implies \mathbf{u} \times \mathbf{v}$  is a unit vector. □

**Definition.** Let  $f : \mathbb{R} \rightarrow \mathbb{R}$  be defined on an open interval containing  $c$  (except possibly at  $c$ ) and let  $L \in \mathbb{R}$ . Then  $\lim_{x \rightarrow c} f(x) = L$  iff for every  $\epsilon > 0$ ,  $\exists \delta > 0$  such that if  $0 < |x - c| < \delta$ , then  $|f(x) - L| < \epsilon$ .

Prove

**Theorem 2.3.** Let  $f(x) = x^3 - 8x + 1$ , then  $\lim_{x \rightarrow 3} f(x) = 4$ .

Prove

**Theorem 2.4.** Let  $f(x) = mx + b$  where  $m, b \in \mathbb{R}$  and  $m \neq 0$ , then  $\lim_{x \rightarrow c} f(x) = mc + b$ .

**Definition.** Let  $r : \mathbb{R} \rightarrow \mathbb{R}^n$  be defined on an open interval containing  $c$  (except possibly at  $c$ ) and let  $\mathbf{L} \in \mathbb{R}^n$ . Then  $\lim_{t \rightarrow c} \mathbf{r}(t) = \mathbf{L}$  iff for every  $\epsilon > 0$ ,  $\exists \delta > 0$  such that

if \_\_\_\_\_, then \_\_\_\_\_.

Prove

**Theorem 2.5.** Let  $\mathbf{r}(t) = \mathbf{r}_0 + t\mathbf{v}$  where  $t \in \mathbb{R}$ ,  $\mathbf{r}_0, \mathbf{v} \in \mathbb{R}^n$  and  $\mathbf{v} \neq \mathbf{0}$ , then  $\lim_{t \rightarrow c} \mathbf{r}(t) = \mathbf{r}_0 + c\mathbf{v}$ .

**Theorem.** Let  $f(x) = x^3 - 8x + 1$ , then  $\lim_{x \rightarrow 3} f(x) = 4$ .

*Proof.* Observe:  $f(x) - L = x^3 - 8x - 3 = (x - 3)(x^2 + 3x + 1)$  and  $0 \leq x^2 + 3x + 1 \leq 29$  for all  $x \in [2, 4]$ .

Let  $\epsilon > 0$ , and consider  $|f(x) - L| = |x^3 - 8x - 3| = |(x - 3)(x^2 + 3x + 1)| = |x - 3| \cdot |x^2 + 3x + 1|$ .

$$\text{Let } \delta = \min\left\{\frac{\epsilon}{29}, 1\right\} \implies 3 - 1 \leq 3 - \delta < x < 3 + \delta \leq 3 + 1 \implies [3 - \delta, 3 + \delta] \subseteq [2, 4]$$

$$\implies 0 \leq x^2 + 3x + 1 \leq 29 \text{ for all } x \in [3 - \delta, 3 + \delta].$$

Case 1: let  $\frac{\epsilon}{29} < 1$ , then

$$\begin{aligned} 0 < |x - 3| < \delta &\implies |x - 3| < \frac{\epsilon}{29} \\ &\implies 29|x - 3| < \epsilon \\ &\implies |(x^2 + 3x + 1)| \cdot |x - 3| < \epsilon \\ &\implies |f(x) - 4| < \epsilon \end{aligned}$$

Case 2: let  $\frac{\epsilon}{29} \geq 1$ , then

$$\begin{aligned} 0 < |x - 3| < \delta &\implies |x - 3| < 1 \leq \frac{\epsilon}{29} \\ &\implies 29|x - 3| < \epsilon \\ &\implies |(x^2 + 3x + 1)| \cdot |x - 3| < \epsilon \\ &\implies |f(x) - 4| < \epsilon \end{aligned}$$

Therefore since

$$\text{for every } \epsilon > 0, \exists \delta = \min\left\{\frac{\epsilon}{29}, 1\right\} > 0$$

$$\text{such that when } 0 < |x - 3| < \delta, \text{ then } |f(x) - 4| < \epsilon,$$

$$\text{then } \lim_{x \rightarrow 3} x^3 - 8x + 1 = 4.$$

□

**Theorem.** Let  $f(x) = mx + b$  where  $m, b \in \mathbb{R}$  and  $m \neq 0$ , then  $\lim_{x \rightarrow c} f(x) = mc + b$ .

*Proof.* Let  $\epsilon > 0$ , and consider  $|f(x) - (mc + b)| = |mx + b - (mc + b)| = |m(x - c)| = |m| \cdot |x - c|$

$$\begin{aligned} \text{Let } \delta = \frac{\epsilon}{|m|}, \text{ then } 0 < |x - c| < \delta &\implies |x - c| < \frac{\epsilon}{|m|} \\ &\implies |m| \cdot |x - c| < \epsilon \\ &\implies |f(x) - (mc + b)| < \epsilon \end{aligned}$$

Therefore since

$$\text{for every } \epsilon > 0, \exists \delta = \frac{\epsilon}{|m|} > 0$$

$$\text{such that when } 0 < |x - c| < \delta, \text{ then } |f(x) - (mc + b)| < \epsilon,$$

$$\text{then } \lim_{x \rightarrow c} f(x) = mc + b.$$

□

**Definition.** Let  $r : \mathbb{R} \rightarrow \mathbb{R}^n$  be defined on an open interval containing  $c$  (except possibly at  $c$ ) and let  $\mathbf{L} \in \mathbb{R}^n$ . Then  $\lim_{t \rightarrow c} \mathbf{r}(t) = \mathbf{L}$  iff for every  $\epsilon > 0$ ,  $\exists \delta > 0$  such that

$$\text{if } \underline{0 < |t - c| < \delta}, \text{ then } \underline{\|\mathbf{r}(t) - \mathbf{L}\| < \epsilon}.$$

**Theorem.** Let  $\mathbf{r}(t) = \mathbf{r}_0 + t\mathbf{v}$  where  $t \in \mathbb{R}$ ,  $\mathbf{r}_0, \mathbf{v} \in \mathbb{R}^n$  and  $\mathbf{v} \neq \mathbf{0}$ , then  $\lim_{t \rightarrow c} \mathbf{r}(t) = \mathbf{r}_0 + c\mathbf{v}$ .

*Proof.* Let  $\epsilon > 0$ , and consider  $\|\mathbf{r}(t) - (\mathbf{r}_0 + c\mathbf{v})\| = \|\mathbf{r}_0 + t\mathbf{v} - (\mathbf{r}_0 + c\mathbf{v})\| = \|(t - c)\mathbf{v}\| = |t - c|\|\mathbf{v}\|$ .

$$\begin{aligned} \text{Let } \delta = \frac{\epsilon}{\|\mathbf{v}\|}, \text{ then } 0 < |t - c| < \delta &\implies |t - c| < \frac{\epsilon}{\|\mathbf{v}\|} \\ &\implies \|\mathbf{v}\| \cdot |t - c| < \epsilon \\ &\implies \|\mathbf{r}(t) - (\mathbf{r}_0 + c\mathbf{v})\| < \epsilon \end{aligned}$$

Therefore since

$$\text{for every } \epsilon > 0, \exists \delta = \frac{\epsilon}{\|\mathbf{v}\|} > 0$$

$$\text{such that when } 0 < |t - c| < \delta, \text{ then } \|\mathbf{r}(t) - (\mathbf{r}_0 + c\mathbf{v})\| < \epsilon,$$

$$\text{then } \lim_{t \rightarrow c} \mathbf{r}(t) = \mathbf{r}_0 + c\mathbf{v}.$$

□

Recall the definition of derivative: Let  $f : \mathbb{R} \rightarrow \mathbb{R}$ , then  $f'(x) = D_x(f(x)) = \lim_{\Delta x \rightarrow 0} \frac{f(x + \Delta x) - f(x)}{\Delta x}$ .

Recall the derivative of the natural log function: Let  $y$  be a function of  $x$ , then  $D_x(\ln y) = \frac{D_x(y)}{y}$ .

Recall the product rule for derivatives:

$$\text{Let } f : \mathbb{R} \rightarrow \mathbb{R} \text{ and } g : \mathbb{R} \rightarrow \mathbb{R}, \text{ then } D_x(f(x)g(x)) = D_x(f(x))g(x) + f(x)D_x(g(x)).$$

Recall the chain rule for derivatives:

$$\text{Let } f : \mathbb{R} \rightarrow \mathbb{R} \text{ and } g : \mathbb{R} \rightarrow \mathbb{R}, \text{ then } D_x(f(g(x))) = D_{g(x)}(f(g(x)))D_x(g(x)).$$

By the way, what is  $D_{3 \sin y}(9 \sin^2 y)$ ?

**Theorem 3.6.** *Let  $x = 0$ ,  $n \in \mathbb{R}^>$ , then  $D_x(x^n) = \begin{cases} nx^{n-1} & \text{if } n > 1 \\ 0 & \text{if } 0 < n \leq 1 \end{cases}$ .*

**Theorem 3.7.** *Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n \in \mathbb{Z}$ , then  $D_x(x^n) = nx^{n-1}$ .*

**Theorem 3.8.** *Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n$  be rational, then  $D_x(x^n) = nx^{n-1}$ .*

**Lemma 3.1.** *Let  $x \in \mathbb{R}$ ,  $x \neq 0$ , then  $D_x(|x|) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \end{cases}$ .*

**Theorem 3.9.** *Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n \in \mathbb{R}$ , then  $D_x(x^n) = nx^{n-1}$ .*

By the way, what is  $D_{3 \sin y}(9 \sin^2 y)$ ? Let  $x = 3 \sin y$ , then  $D_{3 \sin y}(9 \sin^2 y) = D_x(x^2) = 2x = 6 \sin y$ .

**Theorem.** Let  $x = 0$ ,  $n \in \mathbb{R}^>$ , then  $D_x(x^n) = \begin{cases} nx^{n-1} & \text{if } n > 1 \\ 0 & \text{if } 0 < n \leq 1 \end{cases}$ .

*Proof.* Let  $x = 0$ ,  $n \in \mathbb{R}$ .

**Case 1:** Consider  $n > 1$ , then  $D_x(x^n) = D_x(0^n) = D_x(0) = 0 = n0^{n-1}$ .

**Case 2:** If  $0 < n \leq 1$ , then  $D_x(x^n) = D_x(0^1) = D_x(0) = 0$ . □

**Theorem.** Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n \in \mathbb{Z}$ , then  $D_x(x^n) = nx^{n-1}$ .

*Proof.* Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n \in \mathbb{Z}$ , and consider proof by cases:

**Case 1:** Let  $n \in \mathbb{Z}^>$ . Consider an inductive argument:

Base Case Let  $n = 1$ , then  $D_x(x^1) = 1 = 1x^{1-1}$

Suppose  $D_x(x^k) = kx^{k-1}$  holds for some  $k \in \mathbb{Z}^>$

Show  $D_x(x^{k+1}) = (k+1)x^{(k+1)-1} = (k+1)x^k$  holds.

$$D_x(x^{k+1}) = D_x(x^k \cdot x) = D_x(x^k) \cdot x + x^k \cdot D_x(x) = kx^{k-1} \cdot x + x^k \cdot 1 = kx^k + x^k = (k+1)x^k$$

Therefore  $D_x(x^n) = nx^{n-1}$  holds for  $n \in \mathbb{Z}^>$

**Case 2:** Let  $n = 0$ , then  $D_x(x^0) = 0 = 0x^{0-1}$  since  $x \neq 0$

**Case 3:** Let  $n \in \mathbb{Z}^<$ . Consider a direct argument:

$$\begin{aligned} \text{Recall } D_x(x^{-1}) &= D_x\left(\frac{1}{x}\right) = \lim_{\Delta x \rightarrow 0} \frac{f(x+\Delta x) - f(x)}{\Delta x} = \lim_{\Delta x \rightarrow 0} \frac{\frac{1}{x+\Delta x} - \frac{1}{x}}{\Delta x} = \lim_{\Delta x \rightarrow 0} \frac{\frac{x-(x+\Delta x)}{x(x+\Delta x)}}{\Delta x} \\ &= \lim_{\Delta x \rightarrow 0} \frac{-1}{x(x+\Delta x)} = \frac{-1}{x^2} \end{aligned}$$

Note that since  $n < 0$ , we have  $n = -|n|$

Then  $D_x(x^n) = D_x(x^{-|n|}) = D_x((x^{-1})^{|n|})$ , and since  $x \in \mathbb{R}$ ,  $x \neq 0$  then  $x^{-1} \in \mathbb{R}$  and since  $|n| \in \mathbb{Z}^>$ , then the result from case 1 holds.

$$D_x((x^{-1})^{|n|}) = |n|(x^{-1})^{|n|-1} \cdot D_x(x^{-1}) = |n|(x^{-1})^{|n|-1} \cdot (-x^{-2}) = -|n|x^{-|n|-1} = nx^{n-1}$$

Therefore  $D_x(x^n) = nx^{n-1}$  holds for  $n \in \mathbb{Z}^<$

Therefore  $D_x(x^n) = nx^{n-1}$  holds for  $n \in \mathbb{Z}$  □

**Theorem.** Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n$  be rational, then  $D_x(x^n) = nx^{n-1}$ .

*Proof.* Let  $x \in \mathbb{R}$ ,  $x \neq 0$ . Given  $D_x(x^n) = nx^{n-1}$  for all  $n \in \mathbb{Z}$ , let  $n$  be rational.

$$\implies \exists a, b \in \mathbb{Z} \text{ where } n = \frac{a}{b}, \text{ therefore we must show } D_x\left(x^{\frac{a}{b}}\right) = \frac{a}{b}x^{\frac{a}{b}-1}.$$

Consider  $\left(x^{\frac{a}{b}}\right)^b = x^a$ , then  $D_x\left(\left(x^{\frac{a}{b}}\right)^b\right) = D_x(x^a)$ , and since  $a \in \mathbb{Z}$ , then  $D_x(x^a) = ax^{a-1}$ .

$$\text{Since } b \in \mathbb{Z} \text{ and by the chain rule, } D_x\left(\left(x^{\frac{a}{b}}\right)^b\right) = b\left(x^{\frac{a}{b}}\right)^{b-1} D_x\left(x^{\frac{a}{b}}\right).$$

Therefore  $ax^{a-1} = b\left(x^{\frac{a}{b}}\right)^{b-1} D_x\left(x^{\frac{a}{b}}\right)$

$$\implies D_x\left(x^{\frac{a}{b}}\right) = \frac{a}{b}x^{a-1}\left(x^{\frac{a}{b}}\right)^{-b+1} = \frac{a}{b}x^{a-1}\left(x^{-a+\frac{a}{b}}\right) = \frac{a}{b}x^{\frac{a}{b}-1} \quad \square$$

**Lemma.** Let  $x \in \mathbb{R}$ ,  $x \neq 0$ , then  $D_x(|x|) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \end{cases}$ .

*Proof.* Recall  $|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$ .

If  $x > 0$ , then  $D_x(|x|) = D_x(x) = 1$ .

If  $x < 0$ , then  $D_x(|x|) = D_x(-x) = -1$ . □

**Theorem.** Let  $x \in \mathbb{R}$ ,  $x \neq 0$ ,  $n \in \mathbb{R}$ , then  $D_x(x^n) = nx^{n-1}$ .

*Proof.* Let  $x \in \mathbb{R}$ ,  $x \neq 0$ , and  $n \in \mathbb{R}$ .

**Case 1:** Let  $x > 0$  and  $y = x^n$ , then show  $y' = nx^{n-1}$ . Then  $\ln y = n \ln x$ .

$$\begin{aligned} D_x(\ln y) &= D_x(n \ln x) \\ \frac{y'}{y} &= n \cdot \frac{1}{x} \\ y' &= y \cdot nx^{-1} = x^n nx^{-1} = nx^{n-1} \end{aligned}$$

**Case 2:** Let  $x < 0$ , then  $x = -|x|$ .

Since  $x < 0$ , then  $|x| > 0$ , case 1 applies to  $|x|$ , so  $D_{|x|}(|x|^n) = n|x|^{n-1}$  where  $|x| = -x$ .

Then by the chain rule for  $x < 0$  and since  $|x| = -x \implies D_x(|x|) = -1$ , we have

$$D_x(|x|^n) = D_{|x|}(|x|^n) \cdot D_x(|x|) = n|x|^{n-1} D_x(|x|) = -n|x|^{n-1}.$$

$$\begin{aligned} \implies D_x(x^n) &= D_x((-1)^n(|x|^n)) = (-1)^n D_x(|x|^n) = (-1)^n (-n|x|^{n-1}) \\ &= n(-1)^{n+1}|x|^{n-1} = n(-1)^2(-|x|)^{n-1} = nx^{n-1} \end{aligned}$$

□

**Theorem.** *MVT: If  $f$  is continuous on the closed interval  $[a, b]$  and differentiable on the open interval  $(a, b)$ , then there exists a number  $c \in (a, b)$  such that  $f'(c) = \frac{f(b) - f(a)}{b - a}$ .*

**Theorem 4.10.** *Prove that if  $f'(x) > 0$  for all  $x \in (a, b)$  then  $f$  is increasing on  $(a, b)$ .*

**Theorem 4.11.** *Prove that  $f(x) = \sqrt{x}$  for  $x > 0$  is an increasing function.*

**Theorem 4.12.** *Prove that for any  $a, b, c \geq 0$ ,  $c \leq a + b$  iff  $c^2 \leq (a + b)^2$ .*

**Theorem 4.13.** *Given non-zero vectors  $\mathbf{u}$  and  $\mathbf{v}$  in a plane, let  $\theta$  be the acute angle between them (notice that  $\mathbf{v} - \mathbf{u}$  becomes the third side of the triangle), then*

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\| \cos \theta \quad \text{or} \quad \cos \theta = \frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\| \|\mathbf{v}\|}.$$

**Theorem 4.14.** *Prove that  $\mathbf{u} \cdot \mathbf{v} \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$ .*

**Theorem 4.15.** *Prove the triangle inequality,  $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ .*

**Theorem.** Prove that if  $f'(x) > 0$  for all  $x \in (a, b)$  then  $f$  is increasing on  $(a, b)$ .

*Proof.* Let  $f'(x) > 0$  for all  $x \in (a, b)$  and let  $a < x_1 < x_2 < b$ .

By MVT there exists  $c \in (x_1, x_2) \subset (a, b)$  such that

$$f'(c) = \frac{f(x_2) - f(x_1)}{x_2 - x_1}.$$

Since  $f'(c) > 0$  and  $x_2 - x_1 > 0$ , then  $f(x_2) - f(x_1) > 0$ , and we have that if  $x_1 < x_2$  then  $f(x_1) < f(x_2)$  and  $f$  is increasing on  $(a, b)$ .  $\square$

**Theorem.** Prove that  $f(x) = \sqrt{x}$  for  $x > 0$  is an increasing function.

*Proof.* Let  $f(x) = \sqrt{x}$  for  $x > 0$ . Then  $f'(x) = \frac{1}{2\sqrt{x}} > 0$  for all  $x > 0$ , therefore  $f(x) = \sqrt{x}$  is increasing for all  $x > 0$ .  $\square$

**Theorem.** Prove that for any  $a, b, c \geq 0$ ,  $c \leq a + b$  iff  $c^2 \leq (a + b)^2$ .

*Proof.* ( $\implies$ ) Let  $a, b, c \geq 0$  and  $c \leq a + b$ , then

$$c^2 \leq (a + b)c \leq (a + b)(a + b) = (a + b)^2.$$

( $\impliedby$ ) Let  $a, b, c \geq 0$  and  $c^2 \leq (a + b)^2$ , then since  $f(x) = \sqrt{x}$  is an increasing function and since  $a, b, c > 0$ , we have that

$$c = |c| = f(c^2) \leq f((a + b)^2) = |a + b| = a + b.$$

$\square$

**Theorem.** Given non-zero vectors  $\mathbf{u}$  and  $\mathbf{v}$  in a plane, let  $\theta$  be the acute angle between them (notice that  $\mathbf{v} - \mathbf{u}$  becomes the third side of the triangle), then

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\| \cos \theta \quad \text{or} \quad \cos \theta = \frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\| \|\mathbf{v}\|}.$$

*Proof.* Recall the Law of Cosines:  $\|\mathbf{v} - \mathbf{u}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\| \|\mathbf{v}\| \cos \theta$

Consider LHS:  $\|\mathbf{v} - \mathbf{u}\|^2 = (\mathbf{v} - \mathbf{u}) \cdot (\mathbf{v} - \mathbf{u}) = \mathbf{v} \cdot \mathbf{v} - \mathbf{u} \cdot \mathbf{v} - \mathbf{v} \cdot \mathbf{u} + \mathbf{u} \cdot \mathbf{u} = \|\mathbf{v}\|^2 - 2\mathbf{u} \cdot \mathbf{v} + \|\mathbf{u}\|^2$

$$\|\mathbf{v}\|^2 - 2\mathbf{u} \cdot \mathbf{v} + \|\mathbf{u}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\| \|\mathbf{v}\| \cos \theta \implies \mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\| \cos \theta$$

$\square$

**Theorem.** Prove that  $\mathbf{u} \cdot \mathbf{v} \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$ .

*Proof.* Recall  $\cos \theta \leq 1$  for any  $\theta$ . Then

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\| \cos \theta \leq \|\mathbf{u}\| \|\mathbf{v}\|$$

$\square$

**Theorem 4.16.** Prove the triangle inequality,  $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ .

*Proof.* Given above theorems,  $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$  iff  $\|\mathbf{u} + \mathbf{v}\|^2 \leq (\|\mathbf{u}\| + \|\mathbf{v}\|)^2$ .

$$\begin{aligned} \|\mathbf{u} + \mathbf{v}\|^2 &= (\mathbf{v} + \mathbf{u}) \cdot (\mathbf{v} + \mathbf{u}) = \mathbf{v} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{u} + \mathbf{u} \cdot \mathbf{u} = \|\mathbf{v}\|^2 + 2\mathbf{u} \cdot \mathbf{v} + \|\mathbf{u}\|^2 \\ &\leq \|\mathbf{v}\|^2 + 2\|\mathbf{u}\| \cdot \|\mathbf{v}\| + \|\mathbf{u}\|^2 = (\|\mathbf{u}\| + \|\mathbf{v}\|)^2 \end{aligned}$$

Therefore  $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ .  $\square$

**Definition.**  $n! = 1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$  for any  $n \in \mathbb{Z}$

**Definition.** Let  $n, r \in \mathbb{Z}$ , then 
$$\binom{n}{r} = \begin{cases} \frac{n!}{r!(n-r)!} & \text{for } 0 \leq r \leq n \\ 0 & \text{else} \end{cases}$$

**Theorem.**

Recall the binomial theorem: 
$$(x+y)^n = \sum_{r=0}^n \binom{n}{r} x^{n-r} y^r \quad \forall n \in \mathbb{Z}^>$$

Given the following for a probability density function (something that kind of describes the probability of taking on that value):

**Theorem.** A function,  $f(x)$ , can be a density function of a RV  $X$  iff it satisfies

1.  $f(x) \geq 0$  for all  $x$ , and

2.  $\sum_{\text{all } x} f(x) = 1$  for discrete variables  $\left( \text{or } \int_{\text{all } x} f(x) dx = 1 \text{ for continuous variables} \right)$ .

Consider the binomial distribution (counts the number of successes in a fixed number of trials,  $n$ , where the probability of success for each try,  $p \in (0, 1)$ , stays the same): then we say  $X$  is distributed  $Bin(n, p)$  and the density function,  $f(x) = P(X = x)$ , is given by

$$f(x) = \binom{n}{x} p^x (1-p)^{n-x} \text{ for } x = 0, 1, \dots, n,$$

which is interpreted as the probability of getting  $x$  successes in  $n$  tries if we have a  $p$  probability of success on any single try. (Note  $X$  is a random variable and  $x$  is a certain value the random variable can take.)

**Theorem 5.17.** Given fixed values for  $n$  and  $p$ ,  $f(x) = \binom{n}{x} p^x (1-p)^{n-x}$  for  $x = 0, 1, \dots, n$  is a valid density function.

**Question.** What is  $\sum_{x=0}^{n-1} \binom{n-1}{x} p^x (1-p)^{(n-1)-x} = \underline{\hspace{2cm}}$ ?

**Definition.** If  $X$  is a RV with density function  $f(x)$ , then the expected value (aka mean) of a function of  $X$ ,  $g(X)$ , is given by

$$E[g(X)] = \sum_x g(x) \cdot f(x) \text{ (if } X \text{ is discrete)} \left( \text{or } E[g(X)] = \int_{-\infty}^{\infty} g(x) \cdot f(x) dx \text{ (if } X \text{ is continuous)} \right)$$

**Theorem 5.18.** The mean, aka  $E[X]$ , of a binomial random variable is  $np$  (aka, the number of tries \* probability of success).

**Theorem.** Given fixed values for  $n$  and  $p$ ,  $f(x) = \binom{n}{x}p^x(1-p)^{n-x}$  for  $x = 0, 1, \dots, n$  is a valid density function.

*Proof.* Since  $p \in (0, 1)$  and  $\binom{n}{x} > 0$  for  $0 \leq x \leq n$ ,  $x, n \in \mathbb{Z}$ , then  $\binom{n}{x}p^x(1-p)^{n-x} \geq 0 \quad \forall x \in \mathbb{Z}^{\geq}$ .

Now we need to show  $\sum_{x=0}^n \binom{n}{x}p^x(1-p)^{n-x} = 1$ .

$$\begin{aligned} \sum_{x=0}^n \binom{n}{x}p^x(1-p)^{n-x} &= (p + (1-p))^n && \text{by the binomial theorem} \\ &= 1^n = 1 \end{aligned}$$

□

**Question.** What is  $\sum_{x=0}^{n-1} \binom{n-1}{x}p^x(1-p)^{(n-1)-x} = \underline{p + (1-p) = 1}$  (by the binomial theorem)

**Theorem.** The mean of a binomial random variable is  $np$ .

*Proof.* (Try to get what we start with to look like what we know from the previous theorem).

$$\begin{aligned} E[X] &= \sum_{x=0}^n x \binom{n}{x}p^x(1-p)^{n-x} = \sum_{x=1}^n x \binom{n}{x}p^x(1-p)^{n-x} && \text{since the first term in the sum} = 0 \\ &= \sum_{x=1}^n x \frac{n!}{(n-x)!x!}p^x(1-p)^{n-x} && \text{recall } \binom{n}{x} = \frac{n!}{(n-x)!x!} \text{ for } n, x \in \mathbb{Z} \text{ where } 0 \leq x \leq n \\ &= \sum_{x=1}^n \frac{n!}{(n-x)!(x-1)!}p^x(1-p)^{n-x} \\ &= \sum_{x=1}^n \frac{n(n-1)!}{(n-x)!(x-1)!}p^{x-1}(1-p)^{n-x} \\ &= np \sum_{x=1}^n \frac{(n-1)!}{(n-x)!(x-1)!}p^{x-1}(1-p)^{n-x} \\ &= np \sum_{x=1}^n \binom{n-1}{x-1}p^{x-1}(1-p)^{(n-1)-(x-1)} && \text{let } y = x - 1, \text{ then} \\ &= np \sum_{y=0}^{n-1} \binom{n-1}{y}p^y(1-p)^{(n-1)-y} && x = 1 \implies y = 0 \text{ and } x = n \implies y = n - 1 \end{aligned}$$

Since  $\binom{n-1}{y}p^y(1-p)^{(n-1)-y}$  fits the form of a density function when there are  $n-1$  tries with  $p$  probability of success, we know by the previous theorem that  $\sum_{y=0}^{n-1} \binom{n-1}{y}p^y(1-p)^{(n-1)-y} = 1$ .

Therefore

$$E[X] = np \sum_{y=0}^{n-1} \binom{n-1}{y}p^y(1-p)^{(n-1)-y} = np(1) = np$$

□

**Definition.** *An annuity certain is a contract that provides regular payments in exchange for a lump sum assuming a fixed interest rate.*

**Definition.** *An account that accrues interest at  $i\%(m)$  can be valued using the compound interest formula:  $FV = PV \left(1 + \frac{i}{m}\right)^n$  where  $i$  is the decimal version of a percentage,  $FV$  is the future value  $n$  periods into the future (where there are  $m$  equal periods per year), and  $PV$  is the present value (when the money is deposited).*

Derive the results of the following theorem:

**Theorem 6.19.** *Depositing  $m$  payments per year (evenly throughout the year) of \$100 for 5 years will accrue at  $i\%(m)$  and have value immediately after the last payment of*

$$100 \left( \frac{\left(1 + \frac{i}{m}\right)^{5m} - 1}{\frac{i}{m}} \right).$$

**Theorem 6.20.** *Depositing  $m$  payments per year (evenly throughout the year) of \$100 for 5 years will accrue at  $i\%$ ( $m$ ) and have value immediately after the last payment of*

$$100 \left( \frac{\left(1 + \frac{i}{m}\right)^{5m} - 1}{\frac{i}{m}} \right).$$

*Proof.* There will be  $5m$  equally spaced payments made of \$100 each.

Consider the  $k^{\text{th}}$  payment. Since there are  $5m - k$  periods in which the  $k^{\text{th}}$  payment can accrue interest, the future value of the  $k^{\text{th}}$  payment is given by

$$FV_k = 100 \left( 1 + \frac{i}{m} \right)^{5m-k}.$$

Therefore the value of all  $5m$  \$100-payments immediately after the last payment is

$$\begin{aligned} \sum_{k=1}^{5m} FV_k &= \sum_{k=1}^{5m} 100 \left( 1 + \frac{i}{m} \right)^{5m-k} \\ &= 100 \left( 1 + \frac{i}{m} \right)^{5m} \sum_{k=1}^{5m} \left( 1 + \frac{i}{m} \right)^{-k} \\ &= 100 \left( 1 + \frac{i}{m} \right)^{5m} \sum_{k=1}^{5m} \left( \left( 1 + \frac{i}{m} \right)^{-1} \right)^k \\ &= 100 \left( 1 + \frac{i}{m} \right)^{5m} \left( \left( 1 + \frac{i}{m} \right)^{-1} \right) \sum_{k=1}^{5m} \left( \left( 1 + \frac{i}{m} \right)^{-1} \right)^{k-1} \\ &= 100 \left( 1 + \frac{i}{m} \right)^{5m} \left( 1 + \frac{i}{m} \right)^{-1} \left( \frac{1 - \left( \left( 1 + \frac{i}{m} \right)^{-1} \right)^{5m}}{1 - \left( 1 + \frac{i}{m} \right)^{-1}} \right) \\ &= 100 \frac{\left( 1 + \frac{i}{m} \right)^{5m}}{\left( 1 + \frac{i}{m} \right)} \left( \frac{1 - \left( 1 + \frac{i}{m} \right)^{-5m}}{1 - \left( 1 + \frac{i}{m} \right)^{-1}} \right) \\ &= 100 \left( \frac{\left( 1 + \frac{i}{m} \right)^{5m} - 1}{\left( 1 + \frac{i}{m} \right) - 1} \right) = 100 \left( \frac{\left( 1 + \frac{i}{m} \right)^{5m} - 1}{\frac{i}{m}} \right) \end{aligned}$$

□

**Definition.** A nonempty set  $G$  on which there is defined a binary operation “ $\circ$ ” is called a group (with respect to this operation) provided the following properties are satisfied:

1. If  $a, b, c \in G$ , then  $a \circ (b \circ c) = (a \circ b) \circ c$ . (associative law)

2. There exists an element  $e \in G$  such that  $e \circ a = a \circ e = a$  for all  $a \in G$ . (identity)

3. If  $a \in G$ , there exists an element  $x \in G$  such that  $a \circ x = x \circ a = e$ . (inverse)

Prove the following theorem:

**Theorem 7.21.** The set of all integers with an operation,  $\circ$ , defined by  $a \circ b = a + b + 1$  is a group.

**Theorem.** *The set of all integers with an operation,  $\circ$ , defined by  $a \circ b = a + b + 1$  is a group.*

*Proof.* Let  $a, b, c \in \mathbb{Z}$ . then

$$a \circ (b \circ c) = a \circ (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2$$

$$(a \circ b) \circ c = (a + b + 1) \circ c = (a + b + 1) + c + 1 = a + b + c + 2$$

Therefore the associative law holds.

Let  $a \in \mathbb{Z}$  and consider  $e = -1 \in \mathbb{Z}$ , then

$$e \circ a = -1 + a + 1 = a$$

$$a \circ e = a - 1 + 1 = a$$

Therefore there exists an identity for all  $a \in \mathbb{Z}$ .

Let  $a \in \mathbb{Z}$  and consider  $x = -a - 2 \in \mathbb{Z}$ , then

$$a \circ x = a + (-a - 2) + 1 = -1 = e$$

$$x \circ a = (-a - 2) + a + 1 = -1 = e$$

Therefore there exists an inverse for all  $a \in \mathbb{Z}$ .

Therefore  $\mathbb{Z}$  under  $a \circ b = a + b + 1$  is a group. □

**Definition.** Let  $s, t \in \mathbb{Z}$ , then  $t \neq 0$  is a divisor of  $s$  iff  $\exists u \in \mathbb{Z}$  such that  $s = tu$  and we write  $t|s$ .

**Theorem.** For any nonzero  $a, b \in \mathbb{Z}$ , the greatest common divisor of  $a$  and  $b$  is a linear combination of  $a$  and  $b$ , meaning that there exists  $s, t \in \mathbb{Z}$  such that  $\gcd(a, b) = as + bt$ .

**Theorem 8.22.** *Euclid's Lemma:* If  $p$  is a prime such that  $p|ab$  where  $a, b \in \mathbb{Z}$ , then  $p|a$  or  $p|b$ .

**Definition.** Let  $s, t \in \mathbb{Z}$ , then  $t \neq 0$  is a divisor of  $s$  iff  $\exists u \in \mathbb{Z}$  such that  $s = tu$  and we write  $t|s$ .

**Theorem.** For any nonzero  $a, b \in \mathbb{Z}$ , the greatest common divisor of  $a$  and  $b$  is a linear combination of  $a$  and  $b$ , meaning that there exists  $s, t \in \mathbb{Z}$  such that  $\gcd(a, b) = as + bt$ .

**Theorem.** Euclid's Lemma: If  $p$  is a prime such that  $p|ab$  where  $a, b \in \mathbb{Z}$ , then  $p|a$  or  $p|b$ .

*Proof.* Let  $p$  be prime such that  $p|ab$  where  $a, b \in \mathbb{Z}$ . Then there exists  $k \in \mathbb{Z}$  such that  $pk = ab$ .

Consider cases, either  $p$  divides  $a$  or it does not:

1. Suppose  $p | a$ . Then  $p|a$  or  $p|b$  holds.
2. Suppose  $p \nmid a$ . Then  $\gcd(a, p) = 1$ .

From the above theorem, there exists  $s, t \in \mathbb{Z}$  such that

$$\begin{aligned}
 & 1 = \gcd(a, p) = as + pt \\
 \implies & 1(b) = (as + pt)(b) \\
 \implies & b = abs + pbt \\
 \implies & b = pks + pbt \text{ since } p|ab \\
 \implies & b = p(ks + bt) \text{ where } k, b, s, t \in \mathbb{Z} \\
 \implies & \text{there exists } n = (ks + bt) \in \mathbb{Z} \text{ such that } b = pn
 \end{aligned}$$

Therefore  $p|b$ , and the result,  $p|a$  or  $p|b$ , holds.

□

**Theorem.** Recall sine and cosine addition formulas:

$$\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta$$

$$\sin(\alpha + \beta) = \cos \alpha \sin \beta + \sin \alpha \cos \beta$$

Prove the following theorem:

**Theorem 9.23.** If  $u$  and  $v$  are complex numbers with trigonometric forms  $u = r(\cos \theta + i \sin \theta)$  and  $v = s(\cos \phi + i \sin \phi)$ , then  $uv = rs(\cos(\theta + \phi) + i \sin(\theta + \phi))$ .

Prove the following theorem:

**Theorem 9.24.** If  $n$  is a positive integer and  $u = r(\cos \theta + i \sin \theta)$  is the trigonometric form of the complex number  $u$ , then  $u^n = r^n(\cos n\theta + i \sin n\theta)$ .

**Theorem.** If  $u$  and  $v$  are complex numbers with trigonometric forms  $u = r(\cos \theta + i \sin \theta)$  and  $v = s(\cos \phi + i \sin \phi)$ , then  $uv = rs(\cos(\theta + \phi) + i \sin(\theta + \phi))$ .

*Proof.*

$$\begin{aligned}
 uv &= r(\cos \theta + i \sin \theta) \cdot s(\cos \phi + i \sin \phi) \\
 &= rs(\cos \theta \cos \phi + i \sin \theta \cos \phi + i \cos \theta \sin \phi + i^2 \sin \theta \sin \phi) \\
 &= rs(\cos \theta \cos \phi - \sin \theta \sin \phi + i(\sin \theta \cos \phi + \cos \theta \sin \phi)) \\
 &= rs(\cos(\theta + \phi) + i \sin(\theta + \phi))
 \end{aligned}$$

□

**Theorem.** If  $n$  is a positive integer and  $u = r(\cos \theta + i \sin \theta)$  is the trigonometric form of the complex number  $u$ , then  $u^n = r^n(\cos n\theta + i \sin n\theta)$ .

*Proof.* Note that  $u^1 = r(\cos \theta + i \sin \theta) = r^1(\cos(1 \cdot \theta) + i \sin(1 \cdot \theta))$  holds.

Suppose that for some  $k \in \mathbb{Z}$ ,  $k > 1$ ,  $u^k = r^k(\cos k\theta + i \sin k\theta)$  holds.

$$\begin{aligned}
 \text{Consider } u^{k+1} &= u^k \cdot u \\
 &= r^k(\cos k\theta + i \sin k\theta) \cdot r(\cos \theta + i \sin \theta) \\
 &= r^k \cdot r(\cos(k\theta + \theta) + i \sin(k\theta + \theta)) \\
 &= r^{k+1}(\cos((k+1)\theta) + i \sin((k+1)\theta))
 \end{aligned}$$

Therefore since  $u^n = r^n(\cos n\theta + i \sin n\theta)$  holds for  $n = 1$  and

if  $u^n = r^n(\cos n\theta + i \sin n\theta)$  holds then  $u^{n+1} = r^{n+1}(\cos(n+1)\theta + i \sin(n+1)\theta)$  holds,

then we know that  $u^n = r^n(\cos n\theta + i \sin n\theta)$  holds for all  $n \in \mathbb{Z}^{\geq}$ .

□

Prove the following theorem:

**Theorem 10.25.** *If  $r$  and  $s$  are any positive rational numbers, there is a positive integer  $n$  such that  $nr > s$ .*

**Theorem.** *If  $r$  and  $s$  are any positive rational numbers, there is a positive integer  $n$  such that  $nr > s$ .*

*Proof.* Let  $r, s$  be positive rational numbers.

Then  $\exists a, b, c, d \in \mathbb{Z}^>$  such that  $r = \frac{a}{b}$  and  $s = \frac{c}{d}$ .

$$\implies nr > s \text{ holds iff } nr = n\frac{a}{b} > \frac{c}{d} = s$$

which holds iff  $nad > bc$  since  $a, b, c, d > 0$

Therefore  $\exists n \in \mathbb{Z}^>$  such that  $nr > s$  iff  $\exists n \in \mathbb{Z}^>$  such that  $nad > bc$ .

Since  $a, d \in \mathbb{Z}^>$ , then  $a, d \geq 1$ .

$$\implies ad \geq 1$$

$$\implies ad + ad \geq 2 > 1$$

$$\implies 2ad > 1$$

$$\implies 2ad(bc) > bc$$

$$\implies (2bc)(ad) > bc$$

Since  $b, c \in \mathbb{Z}^>$  then  $n = 2bc \in \mathbb{Z}^>$  and there exists  $n \in \mathbb{Z}$  such that  $nad > bc$ .

Therefore there exists  $n \in \mathbb{Z}^>$  such that  $nr > s$  holds. □

**Definition.**  $A - B = \{x|x \in A \text{ and } x \notin B\}$

$A \cap B = \{x|x \in A \text{ and } x \in B\}$

$A \cup B = \{x|x \in A \text{ or } x \in B\}$

$A^c = \{x : x \notin A\}$ , and let  $S$  be the universal set

$\implies A \cup A^c = \{x|x \in A \text{ or } x \in A^c\} = S$ , and  $A \cap A^c = \{x|x \in A \text{ and } x \in A^c\} = \emptyset$

$A \subseteq B$  iff  $\forall x \in A$  then  $x \in B$

Prove the following theorems:

**Theorem 11.26.** *If  $A \subseteq B$ , then  $B^c \subseteq A^c$ .*

**Theorem 11.27.** *Let  $A$  and  $B$  be subsets of some universal set,  $S$ . Then  $A - B = A \cap B^c$ .*

**Theorem 11.28.** *Let  $A$  and  $B$  be subsets of some universal set,  $S$ . Then  $A - (A - B) = A \cap B$ .*

**Definition.**  $A - B = \{x | x \in A \text{ and } x \notin B\}$

$A \cap B = \{x | x \in A \text{ and } x \in B\}$

$A \cup B = \{x | x \in A \text{ or } x \in B\}$

$A^c = \{x : x \notin A\}$ , and let  $S$  be the universal set

$\implies A \cup A^c = \{x | x \in A \text{ or } x \in A^c\} = S$ , and  $A \cap A^c = \{x | x \in A \text{ and } x \in A^c\} = \emptyset$

$A \subseteq B$  iff  $\forall x \in A$  then  $x \in B$

**Theorem 11.29.** If  $A \subseteq B$ , then  $B^c \subseteq A^c$ .

*Proof.* Let  $A \subseteq B \implies$  for any  $x \in A$ , then  $x \in B$ .

Negating this logic yields, that if  $x \notin B$ , then  $x \notin A$ .

Consider any  $x \in B^c \implies x \notin B$ , therefore  $x \notin A$ .

Therefore if  $A \subseteq B$  then  $B^c \subseteq A^c$  by the definition of subsets. □

**Theorem 11.30.** Let  $A$  and  $B$  be subsets of some universal set,  $S$ . Then  $A - B = A \cap B^c$ .

*Proof.* Since each step can go both ways, we will use a bi-directional proof (so we can show both directions at the same time).

$$\begin{aligned} \text{Let } x \in A - B &\iff x \in A \text{ and } x \notin B \\ &\iff x \in A \text{ and } x \in B^c \\ &\iff x \in A \cap B^c \end{aligned}$$

□

**Theorem.** Let  $A$  and  $B$  be subsets of some universal set,  $S$ . Then  $A - (A - B) = A \cap B$ .

*Proof.* If  $x \notin (A - B)$ , then  $x \in (A - B)^c$ , so consider  $(A - B)^c = (A \cap B^c)^c = A^c \cup B$

or  $(A - B)^c = \{x : x \notin (A - B)\} = \{x : x \notin \{x | x \in A \text{ and } x \notin B\}\} = \{x : x \notin A \text{ or } x \in B\}$ .

$$\begin{aligned} (\implies) \quad \text{Let } x \in A - (A - B) &\implies x \in A \text{ and } x \notin (A - B) \\ &\implies x \in A \text{ and } [x \notin A \text{ or } x \in B] \\ &\implies [x \in A \text{ and } x \notin A] \text{ or } [x \in A \text{ and } x \in B] \\ &\implies x \in \emptyset \text{ or } x \in A \cap B \\ &\implies x \in A \cap B \end{aligned}$$

$$\begin{aligned} (\impliedby) \quad \text{Let } x \in A \cap B &\implies x \in A \text{ and } x \in B \\ &\implies [x \in A \text{ and } x \in B] \text{ or } [x \in A \text{ and } x \notin A] \text{ (since the added set is the empty set)} \\ &\implies x \in A \text{ and } [x \in B \text{ or } x \notin A] \\ &\implies x \in A \text{ and } x \notin (A - B) \\ &\implies x \in A - (A - B) \end{aligned}$$

□