Lecture I

Primary objects in math
- Statements: sentence w/ a defined true/false values
  ex. $2+2=5$ (false) $5 \times 3 = 25$ (true)
- Proof: mathematical argument that communicates truth

- Make observations (may help w/ proof)

Proof tips (of (statement))
- Start w/ Proof: at beginning of proof
- Write □ to indicate end of proof
- Complete english sentences
- Keep audience in mind
  → What depth / detail do I need (don't need to prove $1+1=2$)
- Use math notation to help argument
- Counterexample only needs to be provided, not explained
- Contradiction: prove something true by assuming it to be false, then finding a contradiction from that statement

- Some statements have a definite value, but can't be proved
- Negation: Sentence w/ the opposite truth value
  → Symbol: If A is a statement, $\neg A$ is its negation
  → $\neg(\neg A) = A$
  → $\neg$ false = true, $\neg$ true = false

Lecture II

A set: A well-defined collection of objects
- → Element: member of that set
- → Can contain numbers, letters, words, etc etc, including sets
- → Denoted $S = \{e_1, e_2, e_3, e_4 \ldots\}$
- → Sets can be nested $\{2, 4, 5, \{36, 8\}\} = S$, $8 \notin S$
- → NOTATION
  - → x is a member of S: $x \in S$, x is in S
  - → x is not a member of S: $x \notin S$, x is not in S
- → IMPORTANT SETS (0? disagreement)
  - → $\mathbb{N}$: natural numbers: $\{0, 1, 2, 3 \ldots\}$ (also counting numbers)
  - → $\mathbb{Z}$: integers: $\{\ldots -2, -1, 0, 1, 2 \ldots\}$
  - → $\mathbb{Q}$: rational numbers $\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$
  - → $\mathbb{R}$: real numbers: {the whole f'ing number line}
- → colon [:] means for all → vertical line means for all
  - → $S = \{n^2 : n \in \mathbb{Z}\}$ → $S = \{n^2 \mid n \in \mathbb{Z}\}$

Empty set: set w/ no elements $\{\}$ or $\emptyset$

NOT the empty set: $\{\emptyset\}$ (Set that contains empty set)

Statements
- → Definite T/F value
- → all elements/variables are defined
  - → "n^2+1 is not a perfect square" is not a statement.
  - → "n^2+1 is never a perfect square for $n \in \mathbb{N}$" is a statement
  - → Open sentence: sentence w/ undeclared variables (can become statement when variables are declared)
- → Statements/sentences can be represented and manipulated symbolically
  - → ex. $P(x)$ for a statement about x
- → Statements and open sentences can be negated
  - → $Q(x) = x^2 \geq 0$ → $\neg Q(x) = x^2 < 0$ (two ways)
- → Open sents are turned into statements by quantifying the variables
  - → "For all positive $n \in \mathbb{Z}$, $P(n)$" (quantifies $P(n)$)
    - → Symbolically: $\forall n \in \mathbb{Z}$ with $n > 0$, $P(n)$
  - → "There exists an integer $k \in \mathbb{Z}$ such that $4^k = 3$"
    - → Symbolically: $\exists k \in \mathbb{Z}, T(k) : 3$

"I haven't rigorously defined what love means"

-> $\forall$: universal quantifier : means "for all..."
-> $\exists$: existential quantifier : means "there exists"
-> Parts of a quantified statement

quantifier $\forall x \in S, \boxed{P(x)}$ open sentence
variable ↑ domain (a set)

-> Example : for all integers n, n^2+14 is not square
  -> $\forall n \in \mathbb{Z}, \forall m \in \mathbb{Z}, n^2+14 \neq m^2$
-> Logically equivalence symbol : $\equiv$
  -> Used to relate logical statements that are equivalent.
  -> $(\forall n \in \mathbb{Z}, \forall m \in \mathbb{Z}, n^2+14 \neq m^2) \equiv (\forall n \in \mathbb{Z}, \sqrt{n^2+14} \notin \mathbb{Z})$
-> Negation of quantified statements
  S = "All students love MATH 135"
  $\neg S \equiv$ "At least one student doesn't love MATH 135"
  R = "There are perfect squares greater than 1000"
  $R \equiv \exists n \in \mathbb{Z}, n^2 > 1000$
  $\neg R \equiv \forall n \in \mathbb{Z}, n^2 \leq 1000$
  In general terms
  $\neg(\exists x \in S, P(x) \equiv \forall x \in S, \neg P(x)$
  $\neg(\forall x \in S, P(x) \equiv \exists x \in S, \neg P(x)$
-> Nested quantifiers

Lecture III

Fermat's last theorem

Exercise 1. The equation $x^n + y^n = z^n$ has no positive integer solutions for $n \geq 3$

$\forall x, y, z, n \in \mathbb{N}\ x^n + y^n \neq z^n$ (?)

- Instead of writing $n \in \mathbb{N}$, $n \geq 3$, write $n+2 \in \mathbb{N}$

Solution: $\forall x, y, z, n \in \mathbb{N}, x^{n+2} + y^{n+2} \neq z^{n+2}$

Statement variable: "bodeau" variable that can be true of false

→ Usually denoted w/ capital letter, ex. A, C, etc

→ Functions can operate on statement variables

→ Define by a truth table: every combination of inputs is given an output

A	¬A
T	F
F	T

A	B	A ∧ B
T	T	T
T	F	F
F	T	F
F	F	F

← conjunction operator (AND)

A	B	A ∨ B
T	T	T
T	F	T
F	T	T
F	F	F

disjunction operator (

$A \wedge B$: A and B $A \vee B$: A or B

De Morgan's laws

$\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$ $!(A \,\&\&\, B) == !A \,||\, !B$

$\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$ $!(A \,||\, B) == !A \,\&\&\, !B$

Proving logical laws: make a truth table for each to show they're the same

disproving logical laws: only one counterexample necessary

Commutative laws

$A \vee B \equiv B \vee A$ $A \wedge B \equiv B \wedge A$ } same as integers

Associative laws

$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$ } Disjunction like addition

$A \vee (B \vee C) \equiv (A \vee B) \vee C$ } Conjunction like multiplication

Distributive laws → try to prove

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

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

→ These laws can be used to prove logical statements instead (or in addition to) truth tables

Exercise 2: Prove $\neg(A \wedge (\neg B \wedge C)) \equiv \neg(A \wedge C) \vee B$

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

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

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

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

Lecture IV

Implication operator: $A \Rightarrow B$ (read A implies B)

$\equiv \neg A \vee B$

A	B	$A \Rightarrow B$	
T	T	T	A false statement cannot follow from a true statement (hypothesis true, conclusion false)
T	F	F	
F	T	T	← vacuously true statements because hypothesis is false
F	F	T	←

$A \Rightarrow B$ — both statements

hypothesis → if (hypothesis) then (conclusion) ← conclusion

Lecture IV

Vacuous statements

-> "Every unicorn is pink" $\equiv \forall x \in U, P(x)$

-> Problem: set of unicorns is an empty set ($\emptyset$)

-> Negation -> There exists a unicorn that is not pink (false)

-> The negation is false, so $\forall x \in U, P(x)$ is vacuously true

-> The hypothesis is never fulfilled

Implication example

-> $\forall x \in C, (x \in U) \Rightarrow P(x)$

-> If a creature is a unicorn, it must be pink

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

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

The negation of an implication is not another implication

Construct a truth table:

A	B	C	$B \wedge C$	$A \Rightarrow (B \wedge C)$
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F

A	B	C	$B \wedge C$	$A \Rightarrow B \wedge C$
F	T	T	T	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

↗ not always true

Converse Implication

A	B	A ⇒ B	B ⇒ A
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

The converse implication of $A \Rightarrow B$ is $B \Rightarrow A$

$\forall x \in \mathbb{R}\ (x > 0) \Rightarrow (x^2 > 0)$

converse: $\forall x \in \mathbb{R}\ (x^2 > 0) \Rightarrow (x > 0$

Contrapositive Implication

A	B	A ⇒ B	¬B ⇒ ¬A
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

The contrapositive implication of $A \Rightarrow B$ is $\neg B \Rightarrow \neg A$

If you're in ON, you're in CA

contrapositive: if you're not in CA, you're not

★ Contrapositive is always the same as the implication

If and only if

A	B	A ⇒ B	B ⇒ A	B ⇔ A
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

$A \Leftrightarrow B$ if both $A \Rightarrow B$ and $B \Rightarrow A$

Can be written A iff B (A if and only if B)

Lecture 5

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

CHAPTER 3: PROOFS

How to read and write proofs

→ A written proof needs to be formal and direct (and convincing)

Proving universally quantified statements (∀)

→ Could check all members of a set (if S is finite)

→ Usually better to prove in general, not using specific elements

→ Proof: Let x be an arbitrary element of S..... □

→ Start with what you know, work toward conclusion

→ At each step, show/explain that L = R (left side = right side)

Proof example: claim: $\forall \theta \in \mathbb{R}, \sin(3\theta) = 3\sin\theta - 4\sin^3\theta$

Proof: Let θ be a real number, now:

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

$= \sin(2\theta)\cos(\theta) + (1 - 2\sin^2(\theta))\sin(\theta)$

$= 2\sin(\theta)\cos^2(\theta) + \sin(\theta) - 2\sin^3(\theta)$

$= 2\sin(\theta)(1 - \sin^2\theta) + \sin(\theta) - 2\sin^3(\theta)$

$= 3\sin\theta - 4\sin^3(\theta)$ □

Identities and simplifications should be explained

should be able to be read as sentence

→ A similar strategy can be used to prove inequalities

→ Method 2: proof by cases

→ Splitting a statement into multiple cases, and proving each case individually

Proving Existentially quantified statements

→ $\exists x \in S, P(x)$

→ All you need to do is find an example of $x \in S$ that satisfies $P(x)$ (showing work is not required)

→ Ex. Claim: $\exists m \in \mathbb{Z}, \frac{m-7}{2m+4} = 5$

Proof: Let $m = -3$, which is an integer. $\frac{m-7}{2m+4} = \frac{-3-7}{2(-3)+4} = \frac{-10}{-2} = 5$ □

→ Ex Claim: $\exists k, m \in \mathbb{Z}\ (k^2 - \frac{31}{2}k = 8) \wedge (m^2 = k)$

Proof: Let $k = 16$, which is a square. Now $k^2 - \frac{31}{2}k =$ $16^2 - \frac{31}{2}(16) = 8$

Disproving Statements

→ Proving a statement false ≡ proving its negation is true

→ This is how statements are proved false

→ Prove or disprove: $\forall x \in \mathbb{R}, (x^2-1)^2 \geq 0$

→ Negation: $\exists x \in \mathbb{R}, (x^2-1)^2 \leq 0$

→ Let $x = 1$, then $(x^2-1)^2 = 0 \leq 0$.

→ Negation is true $\Rightarrow$ statement is false

→ Disprove: $\exists \theta \in \mathbb{R}, \sin(2\theta) + \cos(2\theta) = 3$

→ Negation: $\forall \theta \in \mathbb{R}, \sin(2\theta) + \cos(2\theta) \neq 3$

→ Proof: note that $-1 \leq \sin(\alpha) \leq 1$ and $-1 \leq \cos(\alpha) \leq 1$ for all $\alpha \in \mathbb{R}$. Thus, $\sin(\alpha) + \cos(\alpha) \leq 2$ for all $\alpha \in \mathbb{R}$

Proving Nested Quantifiers

→ Case: $\forall x \in S, \exists y \in S, P(x,y)$
- → First define x as a member of S (any member)
- → Then find an expression for y that satisfies $P(x,y)$
- → Prove as you would any other $\forall$

→ Case $\exists x \in S, \forall y \in S, P(x,y)$
- → Provide an example of x!
- → Show that for all $y \in S$, $P(x,y)$ is true (regular $\forall$ proof)
- → OR: Negate and prove other statement

Proving Implications

→ Ex. $\forall x \in S, P(x) \Rightarrow Q(x)$
- → Assume the hypothesis is true
- → Using what you know to be true, prove the conclusion
  - → i.e. work your way from $P(x)$ to $Q(x)$
- → Ex. Claim: for $k \in \mathbb{Z}$, if k^5 is a perfect square, so is $9k^{14}$
  - → Proof: Suppose that k^5 is square. Thus, there is an integer m such that $m^2 = k^5$. Now $9k^{14} = 3^2 \cdot k^{14} \cdot k^5 = 3^2 \cdot k^{14} \cdot m^2 = (3 \cdot k^7 \cdot m)^2$ where $3 \cdot k^7 \cdot m \in \mathbb{Z}$ □

Rigorous Definitions for common statements

→ "n is square" $\equiv \exists m \in \mathbb{Z}, m^2 = n$
→ "n is even" $\Leftrightarrow \exists m \in \mathbb{Z}, n = 2m$
→ "n is odd" $\Leftrightarrow \exists m \in \mathbb{Z}, n = 2m+1$

→ Ex. $\forall k \in \mathbb{Z}$, if k is even then $7k^2 + 5$ is odd
- → Proof: Let k be an integer. Assume k is even. Thus, there is an integer a where $k = 2a$. Now, $7k^2 + 5 = 7(2a)^2 + 5 = 28a^2 + 5 = 2(14a^2 + 2) + 1$ where $14a^2 + 2$ is an integer

→ Ex. $\forall n \in \mathbb{Z}$, if 2^{2n} is odd, then 2^{-2n} is odd, vice versa
- → Proof: The hypothesis is only true when $n = 0$. Assume $n = 0$. Then $2^{2n} = 2^{-2n} = 2^0 = 1$. Case 2: assume $n \geq 0$. Then $2^{2n} = 2^{2n-2+2} = 2^2(2^{2(n-1)}) = 2(2 \cdot 2^{2(n-1)})$ which is even, so the hypothesis is false. If $n < 0$, then 2^{2n} is not an integer. □

Definition: For $a, b \in \mathbb{Z}$, we say "a divides b" whenever there exists an $m \in \mathbb{Z}$ such that $a = mb$. notation: $a|b$, $a \nmid b$

Symbolically: $a|b \Leftrightarrow \exists m \in \mathbb{Z}, am = b$

- Facts: $\forall a \in \mathbb{Z}, a|a$ $\forall a \in \mathbb{Z}, 1|a$ $\forall a \in \mathbb{Z}, a|0$

Transitivity of Divisibility

$\forall a, b, c \in \mathbb{Z}, ((a|b) \wedge (b|c)) \Rightarrow (a|c)$

Proof: Let $a, b, c \in \mathbb{Z}$. Assume that $a|b$ and $b|c$. Thus, there exist integers k and n such that $ak = b$ and $bn = c$.

Now, $a(kn) = (ak)n = bn = c$. So $a|c$ as kn is an integer

Types of Statements we will prove

Theorem: Particularly important proposition

Lemma: Small proposition that acts as a stepping stone to a theorem

Corollary: Small proposition that is easily proven after proving a theorem

Splitting one statement into two

$\forall a, b, c \in \mathbb{Z}$, if $a|b$ or $a|a$, then $a|bc$ hard to prove

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

$\forall a, b, c \in \mathbb{Z}$: if $a|b$ then $a|bc$ and if $a|c$ then $a|bc$ easier to prove

Proof: Let $a, b, c \in \mathbb{Z}$. We can prove the claim by instead proving the two statements:

(1) $a|b \Rightarrow a|bc$

(2) $a|c \Rightarrow a|bc$

To prove (1), assume $a|b$ such that there is an integer m satisfying $a = mb$. Now mc is an integer and $a(mc) = bc$, so $a|bc$. To prove (2), assume $a|c$ such that there is an integer n satisfying $a = nc$. Now $a(nb) = b(an) = c$, so $a|bc$. This proves the proposition. □

→ In the future, instead of repeating these same steps for a statement like "the proof of (2) is similar" instead

Divisibility of Integer combinations

$\forall$ and $\exists$ can be used in a hypothesis or conclusion

$\forall a,b \in \mathbb{Z}$, if $a|b$ and $a|c$, then $\forall x,y \in \mathbb{Z}$ $a|(bx+cy)$

Proof: Let a, b, and $c \in \mathbb{Z}$, assume $a|b$ and $a|c$. There are integers m and n such that $am = b$ and $an = c$. Let x and y be integers. Now, $mx+ny$ is an integer and $a(mx+ny) = amx + any = bx + cy$ (QED)

$$\forall a,b,c \in \mathbb{Z}, \left[(a|b) \wedge (a|c) \Rightarrow (\forall x,y \in \mathbb{Z}, a|(bx+cy))\right]$$

CONVERSE: $$\forall a,b,c \in \mathbb{Z}, \left[(\forall x,y \in \mathbb{Z}, a|(bx+cy)) \Rightarrow ((a|b) \wedge (a|c))\right]$$

CONTRAPOSITIVE: $$\forall a,b,c \in \mathbb{Z}, \left[(\exists x,y \in \mathbb{Z}, a \nmid (bx+cy)) \Rightarrow (a \nmid b \vee a \nmid c)\right]$$

Proof by Contrapositive

Proving $\forall x \in S, \neg Q(x) \Rightarrow \neg P(x)$ instead of $\forall x \in S, P(x) \Rightarrow Q(x)$

-> Ex. Claim: $\forall x \in \mathbb{R}, (x^3 - 5x^2 + 3x \neq 15) \Rightarrow (x \neq 5)$

-> Proof: We prove the contrapositive $(x = 5) \Rightarrow (x^3 - 5x^2 + 3x = 15)$

Assume $x = 5$, via algebra... $(5)^3 - 5(5)^2 + 3(5) = 15$ □

-> Ex. Claim: $\forall k \in \mathbb{Z}$, ($k^2 + 4k - 2$ is odd) $\Rightarrow$ (k is odd)

-> Proof: Assume k is even. Then there is $n \in \mathbb{Z}$ such that $2n = k$.

Now $k^2 + 4k - 2 = (2n^2) + 8n - 2 = 2(2n^2 + 4n - 1)$ which is even, as $(2n^2 + 4n - 1)$ is an integer □

Irrational numbers

For a number $x \in \mathbb{R}$, $\left[x \in \mathbb{Q}\right] \Leftrightarrow \left[\exists a,b \in \mathbb{Z},\ b \neq 0 \wedge x = \frac{a}{b}\right]$

If x is irrational, it is not rational ($x \notin \mathbb{Q}$)

-> Rationality is easier to prove than irrationality, so proof by contrapositive useful

-> Ex. Claim: $\forall xy \in \mathbb{R}$, $xy \notin \mathbb{Q} \Rightarrow x \notin \mathbb{Q} \vee y \notin \mathbb{Q}$

-> Proof: We prove the contrapositive. Let x and y be rational numbers.

Thus, $\exists a,b,m,n \in \mathbb{Z}$ such that $b,n \neq 0$ and $x = \frac{a}{b}$ and $y = \frac{m}{n}$.

$xy = \frac{a}{b} \cdot \frac{m}{n} = \frac{am}{bn}$ where $a,m,b,n \in \mathbb{Z}$ and $b,n \neq 0$.

So, xy is rational. □

Proof by Elimination (elimination method)

-> Useful for implications where the conclusion has an OR statement

-> $A \Rightarrow (B \vee C) \equiv \neg A \vee (B \vee C) \equiv (\neg A \vee B) \vee C \equiv$
$(\neg(A \wedge \neg B)) \vee C \equiv \boxed{(A \wedge \neg B) \Rightarrow C}$

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

-> Ex. Claim: $\forall x \in \mathbb{R},\ (|2x-6| = 4) \Rightarrow (x \geq 3 \vee x = 1)$

-> Proof: We'll prove this by elimination. Let $x \in \mathbb{R}$, assume $\underbrace{|2x-6| = 4}_{P(x)}$. Assume further that $\underbrace{x \leq 3}_{\neg Q(x)}$, Now $2x \leq 6$, $\rightarrow R(x)$

and thus $2x - 6 \leq 0$. Hence, $|2x-6| = 6 - 2x$. Now,

$x = -\left(\frac{-2x}{2}\right) = -\left(\frac{6-2x}{2} + 3\right) = -\left(\frac{|2x-6|}{2}\right) + 3$

$= -4/2 + 3 = -2 + 3 = 1$ [R(x)] $\square$.

Proving "if and only if" ($\Leftrightarrow$) statements

-> $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A) \equiv \boxed{(A \Rightarrow B) \wedge (\neg A \Rightarrow \neg B)}$

-> Ex. Suppose $x, y \geq 0$. Prove $(x+y)/2 = \sqrt{xy}) \Leftrightarrow (x = y)$

-> Proof: Assume $x, y \geq 0$, $x = y$. Then, $(x+y)/2 = x = \sqrt{x \cdot x} = \sqrt{xy}$

For the other direction, assume instead that $(x+y)/2 = \sqrt{xy}$. This is equivalent to $x + y = 2\sqrt{xy}$. Squaring yields $x^2 + 2xy + y^2 = 4xy$. Rearranging, we find $x^2 - 2xy + y^2 = 0$, or $(x-y)^2 = 0$. Thus, $(x-y)$ must be 0, and thus $x = y$ $\square$.

-> Claim: $2 \mid a \Leftrightarrow 2 \mid a^2$

Proof: Let $a \in \mathbb{Z}$, so $2 \mid a$. note that $a \mid a^2$. By transitivity of division, $2 \mid a^2$. To prove $2 \mid a^2 \Rightarrow 2 \mid a$, we will prove the contrapositive. Assume $1 \nmid 2$, so $a = 2k+1$, $k \in \mathbb{Z}$. So, $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so a^2 must also be odd. Thus, $2 \mid a \Leftrightarrow 2 \mid a^2$

Proof by Contradiction

-> A statement A can't be both true and false ($A \wedge \neg A$ is always false)

-> If you come to logically deduce A and $\neg A$, your initial statement must be false

-> If you want to prove P as true, you can assume P is false and find a contradiction from that assumption

-> Ex. $\forall a, b \in \mathbb{Z}$, $a \geq 2 \Rightarrow a \nmid b \vee a \nmid (b+1)$.

-> Proof: Assume that $a|b$ and $a|(b+1)$. Then, there must exist $m, n \in \mathbb{Z}$ such that $b = ma$ and $b+1 = na$. Then, $a(n-m) = 1$. Because $(n-m) \in \mathbb{Z}$, a must divide 1. So, $a = -1$ or $a = 1$. Contradiction: we assumed $a \geq 2$, but a must be -1 or 1. Thus, our initial claim must be false, so $a \nmid b \vee a \nmid (b+1)$ must be true.

-> Ex. Claim: $\sqrt{2} \notin \mathbb{Q}$

Proof: assume $\sqrt{2}$ is rational. Then, there exist $a, b \in \mathbb{Z}$, $b \neq 0$ where $\sqrt{2} = \frac{a}{b}$. Thus, $\frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2$. But $a^2 = 2b^2$ means a^2 is even, and thus a is even. If a is even, for some $k \in \mathbb{Z}$ $a = 2k$, so $2b^2 = (2k)^2 \Rightarrow 2b^2 = 4k^2 \Rightarrow b^2 = 2k^2$, so b^2 must also be even. Contradiction: We know that either a or b must be odd (or $\frac{a}{b}$ can be further reduced), but we've shown that a and b are both even.

Proving Uniqueness

-> Ex. For all integers a, there exists a unique integer k such that $a = 2k+1$

-> Two things to prove:

1) $\exists a, k \in \mathbb{Z}$ such that $a = 2k+1$
2) $\forall m, n, (2m+1 = a) \Rightarrow (m = k)$

-> Proof: Let a be an odd integer. By definition, $\exists k \in \mathbb{Z}$ such that $2k+1 = a$ (i). Suppose there is another integer m such that $2m+1 = a$. Thus $2m+1 = 2k+1$, so $m = k$. □

-> General strategy:

1) Prove $\exists x \in S$, $P(x)$
2) Prove $\forall y \in S$, if $P(y)$ then $y = x$

Base case: $f(0) = k$

Inductive hypothesis: $f(n) \Rightarrow f(n+1)$, $n \in \mathbb{N}$, $n \geq k$

Inductive conclusion: proof of inductive hypothesis

Mathematical Induction (POMI)

-> Axiom: suppose you have statements $P(1), P(2), P(3)\ldots$ where $P(n)$ is an open sentence for all $n \in \mathbb{N}$.

-> If you can prove

-> $P(1)$

-> $\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$

Then you can conclude that $\forall n \in \mathbb{N}, P(n)$.

-> Example: prove that for all $n \in \mathbb{N}$, $4 \mid (5^n - 1)$.

-> Proof: For this proof, we will use POMI. Base case: $4 \mid (5^1 - 1) \Rightarrow 4 \mid (5-1) \Rightarrow 4 \mid 4$, so $4 \mid 5^n - 1$ is true for $n = 1$.

Inductive step: Let $k \in \mathbb{N}$. Assume $P(k)$ is true, meaning $\exists m \in \mathbb{Z}$ such that $4m = 5^k - 1 \Rightarrow 4m = 5(5^k) - 1 \Rightarrow 4m = 5(4m+1) - 1$ $\Rightarrow 20m + 5 - 1 \Rightarrow 20m + 4 \Rightarrow 4m = 4(5m+1)$, which is divisible by 4 as $5m + 1 \in \mathbb{Z}$. So, $P(k+1)$ is true. Therefore by POMI, $P(n)$ is true for all $n \in \mathbb{N}$. □

-> Example: consider the sums $\sum_{i=1}^{n} i(i+1)$ for $n \in \mathbb{N}$.

Prove that $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$ for all $n \in \mathbb{N}$

-> Proof: The proof is by induction. The base case is true: $1(1+1) = \frac{1(1+1)(1+2)}{3} \Rightarrow 1(2) = \frac{1(2)(3)}{3} \Rightarrow 2 = 2$. Inductive step: Let $k \in \mathbb{N}$ be arbitrary. Assume $P(k)$. That is, $\sum_{i=1}^{k} i(i+1) = \frac{k(k+1)(k+2)}{3}$

Now, $\sum_{i=1}^{k+1} i(i+1) = 1(1+1) + 2(2+1) + \ldots + k(k+1) + (k+1)(k+2)$

$= \sum_{i=1}^{k} i(i+1) + (k+1)(k+2) = \frac{k(k+1)(k+2)}{3} + (k+1)(k+2)$

$= (k+1)(k+2)\left(\frac{k}{3} + 1\right) = \frac{(k+1)(k+2)(k+3)}{3} = \frac{(k+1)((k+1)+1)((k+1)+2)}{3}$

Thus, $P(k+1)$ is true for all $n \in \mathbb{N}$. By POMI, $P(n)$ is true □

Summation notation $\sum$

upper bound ↘

lower bound →

$$\sum_{k=0}^{n} f(k) = f(0) + f(1) + f(2) \ldots + f(n-1) + f(n)$$

$$\sum_{i=m}^{n} c f(i) = c \sum_{i=m}^{n} f(i), \quad \sum_{i=m}^{n} f(i) + \sum_{i=m}^{n} g(i) = \sum_{i=m}^{n} f(i) + g(i)$$

$$\sum_{i=m}^{n} f(i) = \sum_{i=m+k}^{n+k} f(i-k)$$ ← use to change bounds to add two expressions

The Binomial Theorem

$\binom{n}{m} = 0$ if $m > n$

$\binom{n}{m}$ is defined as $\frac{n!}{m!(n-m)!}$, also known as n choose m (nC_m)

This is called a binomial coefficient

→ Ex: $\binom{7}{3} = \frac{7!}{3!4!} = \frac{7\times6\times5\times4!}{3!4!} = \frac{7\times5\times3}{3!} = 35$

Pascal's law: For $n, m \in \mathbb{Z}$, we have $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Proof:

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!}$$

inhibin?

$$= (n-1)!\left[\frac{k}{k!(n-k)} + \frac{n-k}{k!(n-k)!}\right]$$

$$= \frac{(n-1)!}{k!(n-k)!}[n]$$

$$= \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

For this to work $0!$ must be 1 (for combinatorics)

Binomial theorem: For all $x \in \mathbb{R}$, $n \in \mathbb{N}$, $(x+1)^n = \sum_{m=0}^{n} \binom{n}{m} x^m$

Proof by induction. Let $x \in \mathbb{R}$, and for each $n \in \mathbb{N}$, let $P(x, n)$ be the statement $(x+1)^n = \sum_{m=0}^{n} \binom{n}{m} x^m$

Base case: For $n=1$, $(x+1)^1 = 1+x = \binom{1}{0}x^0 + \binom{1}{1}x^1 = \sum_{m=0}^{1}\binom{1}{m}x^m$ so $P(1)$ is true

Inductive step: let $k \in \mathbb{N}$ and assume $P(x,k)$ is true, meaning

$$(x+1)^k = \sum_{m=0}^{k}\binom{k}{m}x^m$$

Now,

$$(x+1)^{k+1} = (x+1)(x+1)^k = (x+1)\sum_{m=0}^{k}\binom{k}{m}x^m =$$

$$\sum_{m=0}^{k}\binom{k}{m}x^m + x\cdot\sum_{m=0}^{k}\binom{k}{m}x^m = \left[1 + \sum_{m=1}^{k}\binom{k}{m}x^m\right] + \left[\sum_{m=0}^{k-1}\binom{k}{m}x^{m+1} + x^{k+1}\right] =$$

let $j = m+1 = k$ (change of vars)

$$1 + \sum_{m=1}^{k}\binom{k}{m}x^m + \sum_{j=1}^{k}\binom{k}{j-1}x^j + x^{k+1} \longrightarrow \text{by addition} \rightarrow$$

$= 1 + \sum_{m=1}^{k} \left[\binom{k}{m} + \binom{k}{m-1} \right] x^m + x^{k+1}$ by pascal's identity:

$= \binom{k+1}{0} x^0 + \sum_{m=1}^{k} \binom{k+1}{m} x^m + \binom{k+1}{k+1} x^{k+1} = \sum_{m=0}^{k+1} \binom{k+1}{m} x^m$

so, $P(x, k+1)$ is true and by induction, $P(x,n)$ is true for all n and x

Binomial theorem part 2: $(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m}$

Proof: Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$.

Case 1: $y = 0$: $(x+y)^n = (x)^n = \overbrace{\binom{n}{0} x^0 0^n}^{0} + \overbrace{\binom{n}{1} x^1 0^{n-1}}^{0} + \dots + \overbrace{\binom{n}{n} x^n 0^0}^{1}$

$= \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m}$ →

Case 2: Suppose $y \neq 0$, then

$(x+y)^n = y^n \left(\frac{x}{y} + 1\right)^n = y^n \sum_{m=0}^{n} \binom{n}{m} \left(\frac{x}{y}\right)^m$ by binomial theorem I

$= \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m}$ ∎.

Principle of Strong Induction (POSI)

Let $P(n)$ be an open statement for $n \in \mathbb{N}$. Strong induction is when:

$P(1) \wedge (\forall k \in \mathbb{N},\ P(1) \wedge P(2) \dots \wedge P(k) \Rightarrow P(k+1)) \Rightarrow \forall n \in \mathbb{N},\ P(n)$

Basically, multiple base cases must be true for the statement to be true:

1) Prove $P(0) \wedge P(1) \wedge \dots \wedge P(k)$ are all true (base case)

2) Prove $P(0) \wedge P(1) \wedge \dots \wedge P(k) \Rightarrow P(k+1)$ (inductive case)

Example POSI proof:

Let $\{x_k\}$ be defined by $x_1 = 0$, $x_2 = 30$, and $x_m = x_{m-1} + 6x_{m-2}$ $m \geq 3$. Prove that for all integers $n \geq 1$, $x_n = 2 \cdot 3^n + 3 \cdot (-2)^n$

Base cases: $P(1) = 0 = 2 \cdot 3^1 + 3(-2)^1 = 6 - 6 = 0$ ✓

$P(2) = 30 = 2 \cdot 3^2 + 3(-2)^2 = 18 + 12 = 30$ ✓

Inductive hypothesis: $2 \cdot 3^i + 3 \cdot (-2)^i$ for all integers $i = 1, 2 \ldots k$

$\equiv P(k+1) \equiv x_{k+1} = 2 \cdot 3^{k+1} + 3 \cdot (-2)^{k+1}$

Inductive conclusion: since $k+1 \geq 3$ because $k \geq 2$, we have

$$x_{k+1} = x_k + 6x_{k-1}$$

$$= (2 \cdot 3^k + 3(-2)^k) + 6(2 \cdot 3^{k-1} + 3(-2)^{k-1})$$

$$= 3^{k-1}(2 \cdot 3 + 6 \cdot 2) + (3(-2) + 6 \cdot 3)(-2)^{k-1}$$

by inductive hypothesis $= (18)(3^{k-1}) + (12)(-2)^{k-1}$

using $i = k$ and $i = k-1$, $= 2 \cdot 3^2 \cdot 3^{k-1} + 3 \cdot (-2)^2 \cdot (-2)^{k-1}$

which is valid because $= 2 \cdot 3^{k+1} + 3 \cdot (-2)^{k+1}$

$k-1 \geq 1$ when $k \geq 2$

By POSI, $P(n)$ is true for all $n \in \mathbb{N}$

Sets

Set Builder Notation: Rules that define what is in a set

-> Given a universal set (U) and a property P(x), for each $x \in U$, $\{x \in U : P(x)\}$ is the set of all elements of U for which P(x) is true

-> ex. $S = \{n \in \mathbb{N} : n \mid 12\}$ = divisors of 12 = $\{1, 2, 3, 4, 6, 12\}$

-> ex. $\{x \in \mathbb{R}, 0 \leq x \leq 1\} = [0, 1]$

-> Given a universal set (U) and a function f(x), apply f(x) to each element of U : $\{f(x) : x \in U\}$

-> Combination: $\{f(x) : x \in U, P(x)\}$

-> Ex. $\{m^2 : m \in \mathbb{Z}, 2 \nmid m\} = \{1, 9, 25, 49 \ldots\} = \{(2k+1)^2 : k \in \mathbb{Z}\}$

notation $A \times B$

Cartesian product: for sets S and T, it is the set of all the ordered pairs of the elements of S and T. $\{(x, y) : x \in S, y \in T\}$

-> Ex. $S = \{1, 2\}$, $T = \{3, 4\}$, $S \times T = \{(1,3), (1,4), (2,3), (2,4)\}$

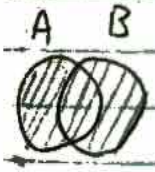
-> $\mathbb{R}^2$ (the real plane) is defined as $\{(x, y), x \in \mathbb{R}, y \in \mathbb{R}\}$

-> Ex. $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 4\}$ set of points 2 units from (0,0)

Cardinality: the number of elements in a finite set (notation: $|S|$)

-> $A = \{1, 2, 4, 8\}$, $|A| = 4$

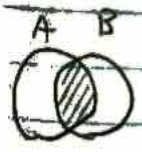
-> $|\emptyset| = 0$



Union: The set of elements in either A or B (or both). Notation: $A \cup B$

-> $A \cup B = \{x : x \in A \vee x \in B\}$

-> $\{1, 3, 5\} \cup \{7, 6, 5\} = \{1, 3, 5, 7, 6\}$



Intersection: the set of elements in both A and B. Notation: $A \cap B$

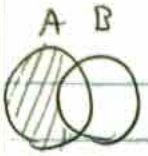
-> $A \cap B = \{x : x \in A \wedge x \in B\}$

-> $\{1, 3, 5\} \cap \{7, 6, 5\} = \{5\}$

-> If $A \cap B = \emptyset$, A and B are <u>disjoint</u>

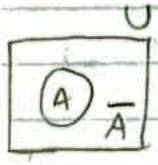
-> $\{2k+1 : k \in \mathbb{N}\}$ and $\{2k : k \in \mathbb{N}\}$ are disjoint

-> Every set is disjoint with $\emptyset$ because $\emptyset$ has no elements

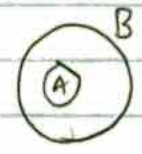


A − B

Difference: For sets A and B, their difference $(A - B)$ is the set $A - B = \{x \in A : x \notin B\}$
- → Elements in A that aren't in B
- → $\{1, 2, 3\} - \{5, 4, 3\} = \{1, 2\}$
- → $\{5, 4, 3\} - \{1, 2, 3\} = \{4, 5\}$



Complement: Given a universal set U and a set A that is a subset of U, its complement ($\overline{A}$) is the set $\overline{A} = \{x \in U : x \notin A\}$
- → With respect to $\mathbb{Z}$, the complement of the set of even numbers is the set of odd numbers
- → Can be defined as $U - A$



Subset: A is a subset of B ($A \subseteq B$) if every element of A is also in B. $A \subseteq B \Leftrightarrow \forall x \in A, x \in B$
- → Conversely, B is a superset of A
- → If A and B are both subsets of a superset U ($A \subseteq U \wedge B \subseteq U$), then $A \subseteq B \Leftrightarrow \forall x \in U, (x \in A \Rightarrow x \in B)$

Proving Subsets: Proving $A \subseteq B$ means proving $\forall x \in A, x \in B$. Thus,
1) Let $x \in A$ be arbitrary 2) Using $x \in A$, prove $x \in B$

If $A, B \subseteq U$ (universal set), proving $A \subseteq B$ is the same as proving $\forall x \in U, x \in A \Rightarrow x \in B$
- → Example: prove $S = \{x : x \in \mathbb{Z}, 6 | x\} \subseteq T = \{y : y \in \mathbb{Z}, 2 | y\}$
- → Proof: Let $x \in \mathbb{Z}$ be arbitrary. Assume $x \in S$. Then, $6 | x$, meaning $\forall m \in \mathbb{Z}$ such that $x = 6m$. Now $x = 2(3m)$, where $3m \in \mathbb{Z}$, so $2 | x$. Thus, $x \in T$.
- → To prove $C \not\subseteq D$, find one $x \in C$ where $x \notin D$
  - → $A \not\subseteq B \Leftrightarrow \exists x \in A, x \notin B$.

→ For all sets A:
- → $A \subseteq A$ (trivially true)
- → $\emptyset \subseteq A$ (vacuously true because there are no counterexamples)

Set equality: Given two sets, $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$.
-> Two sets are equal if they contain the same elements.

Proving Set equality. To prove $A = B$, we must prove that:
1) $A \subseteq B$ and 2) $B \subseteq A$
-> Example: prove $S = \{-1, 0, 1\} = T = \{x : x \in \mathbb{R}, x^3 = x\}$
-> 1): $S \subseteq T$ (show that $x^3 = x$ for $-1, 0, 1$)
-> 2): $T \subseteq S$: factor $x^3 = x$ into $x(x-1)(x+1) = 0$
-> Thus, $S = T$
-> Example: Prove $A = \{s \in \mathbb{R} : |s^2 - 2| = 1\} = B = \{t \in \mathbb{R} : t^4 - 4t^2 + 3 = 0\}$
-> 1) $A \subseteq B$: Turn $|x^2 - 2| = 1$ into $x^4 - 3x^2 + 3 = 0$
-> 2) $B \subseteq A$: Turn $x^4 - 3x^2 + 3 = 0$ into $|x^2 - 2| = 1$.
-> Thus, $S = T$

Proper Subset: Given sets A and B, A is a proper subset of B ($A \subsetneq B$) if $A \subseteq B$ and $A \neq B$.
-> $A \subsetneq B \Leftrightarrow (A \subseteq B \wedge A \neq B)$
-> Ex. $\mathbb{N} \subsetneq \mathbb{Z}$, $\mathbb{Z} \subsetneq \mathbb{Q}$, $\mathbb{Q} \subsetneq \mathbb{R}$
-> $A \subsetneq B \Leftrightarrow (A \subseteq B \wedge \exists x \in B, x \notin A)$

Proving claims about arbitrary sets
-> Claim: for all sets A, B, $(A \cap B = A \cup B) \Rightarrow A = B$
-> Proof: of $A \subseteq B$: let $x \in A$.

Bounds of Divisibility

-> $\forall a,b \in \mathbb{Z}, (a \neq 0 \wedge b|a) \Rightarrow b \leq |a|$

-> Proof: let $a,b \in \mathbb{Z}$, and assume $a \neq 0$ and $b|a$. Then there exists a $k \in \mathbb{Z}$ such that $kb = a$. because $a \neq 0$ and $kb \neq 0$, $k \neq 0$ and $b \neq 0$. So, $k \leq -1$ or $k \geq 1$, meaning $|k| \geq 1$. Now $b \leq |b|$ so $b \leq |b| \cdot 1$, so $b \leq |b||k|$, so $b \leq |kb| \leq a$.

Division Theorem

-> $\forall a,b \in \mathbb{Z}$, $b > 0$ => there exist unique integers $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r \leq b$

-> $a = 20$, $b = 7$ => $q = 2$, $r = 6$

-> Proof: let $a,b \in \mathbb{Z}$, assume $b > 0$. Suppose for now there exist $q, r \in \mathbb{Z}$, such that $a = qb + r$ and $0 \leq r < b$. Assume $q_1, r_1, q_0, r_0 \in \mathbb{Z}$ and $a = q_1 b + r_1 = q_2 b + r_2$. Since $0 \leq r < b$ and $-b < -r \leq 0$, we have $-b < r - r_0 < b \Rightarrow |r - r_0| < b$. Also, since $qb + r = q_0 b + r_0 = a$, we have $r - r_0 = (q_0 - q)b$. Hence, $b|(r - r_0)$. Now, suppose $r \neq r_0$. Since $b|(r - r_0)$, $b \leq |r - r_0|$ by BBD. However, we know $b > |r - r_0|$, so $r = r_0$ by contradiction. Now, $(q_0 - q)b = (r - r_0) = 0$. Since $b \neq 0$, we have $q_0 - q = 0$ $\Rightarrow q_0 = q$. $\square$

Greatest Common Divisor

-> let $a,b \in \mathbb{Z}$ such that a and b are not both 0. $d = \gcd(a,b)$ if:

I) $d|a \wedge d|b$ (common divisor)

II) $\forall k \in \mathbb{Z}$, $(k|a \wedge k|b) \Rightarrow k \leq d$ (largest common divisor)

-> Remark: $\forall n \in \mathbb{Z}$, $n|0$

-> Remark: $\forall a \in \mathbb{Z}$, $a \neq 0 \Rightarrow \gcd(a,0) = \gcd(a,a) = |a|$

-> $\forall a,b \in \mathbb{Z}$, $\gcd(a,b) = \gcd(b,a)$

-> We define $\gcd(0,0) = 0$ for convenience (even though it's wrong lol)

-> Prop: $\gcd(3a+b, a) = \gcd(a,b)$

-> Proof: Let $d = \gcd(a,b)$. Then, $d|a \wedge d|b$. By DIC, we have $d|3a + b$. Thus, d is common divisor of $3a+b$ and b. Imagine k also divides $3a+b$ and b. By DIC, $k|a$. By the definition of GCD, $k \leq \gcd(a,b) = d$, so $d = \gcd(3a+b, b)$. $\square$

Corollaries

-> Existence: let $a, b \in \mathbb{Z}$ and assume $b > 0$. Define q as $\left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - qb$, where $q \in \mathbb{Z}$. Now, $\frac{a}{b} - 1 < q \leq \frac{a}{b} \Rightarrow$ $a - b < qb \leq a \Rightarrow -b < qb \leq 0 \Rightarrow 0 \leq a - qb < b$. So, $a = qb + r$ and $0 \leq r < b$. □

GCDWR

Euclid's Algorithm: $\forall a, b, q, r \in \mathbb{Z}, a = qb + r \Rightarrow [\gcd(a,b) = \gcd(b,r)]$

-> ex. $\gcd(63, 18) = \gcd(18, 9) = 9$

-> This makes it easy to compute the gcd of large numbers

-> Recall: $\gcd(0, n)$ is n

-> Proof: let $a, b, q, r \in \mathbb{Z}$ and assume $a = qb + r$. Consider 2 cases:

-> $b = 0$: then $a = r$, so $\gcd(a,b) = \gcd(r,b) = \gcd(b,r)$

-> $b \neq 0$: define $d = \gcd(a,b)$. Then $d|a \wedge d|b$, so $\exists m, n \in \mathbb{Z}$ such that $a = md$ and $b = nd$. Now, $r = a - qb = md - qnd = d(m - qn)$, so $d|r$. Hence $d|b \wedge d|r$. Let $k \in \mathbb{Z}$ be some common divisor of b and r. Since $k|b \wedge k|r$, $k|a$ $(= qb + 1(r))$ by the DIC. Thus, $k|a \wedge k|b$. By the definition of gcd, $k \leq d$ since $d = \gcd(a,b)$. Hence, $d = \gcd(b,r)$. □

GCD of adjacent numbers: $\forall n \in \mathbb{Z}, \gcd(n, n+1) = 1$

-> Proof: let $n \in \mathbb{Z}$. Note that $n + 1 = n \cdot 1 + 1$. By GCDWR, $\gcd(n+1, n) = \gcd(n, 1)$. Since $\gcd(n, 1) = 1$ $\forall n \in \mathbb{Z}$, we have $\gcd(n+1, n) = \gcd(n, n+1) = 1$.

GCD Characterization Theorem: $\forall a, b, d \in \mathbb{Z}$, if $d \geq 0 \wedge d|a \wedge d|b \wedge (\exists x, y \in \mathbb{Z}\ ax + by = d)$, then $\gcd(a,b) = d$.

-> Ex. we can show $\gcd(30, 42) = 6$ because $6 \geq 0 \wedge 6|30 \wedge 6|42 \wedge (3)30 + (-2)(42) = 6$.

-> We say that x and y (in this case 3 and -2) are a certificate of correctness for $\gcd(30, 42) = 6$ because they allow that to be shown easily.

-> Proof: Let $a, b, d \in \mathbb{Z}$. Assume $d \geq 0$, $d|a$, $d|b$, $\exists x, y \in \mathbb{Z}$, $ax + by = d$.

-> Case: $a = b = 0$. Then, $d = 0x + 0y = 0 = \gcd(0,0) = \gcd(a,b)$

-> Case (else): Let $k \in \mathbb{Z}$ and assume $k|a \wedge k|b$. By DIC, $k|ax + by$, so $k|d$ (from hypothesis), and thus $k \leq |d| = d$. Hence, $d = \gcd(a,b)$.

Coprimes: $a, b \in \mathbb{Z}$ are coprime if $\gcd(a,b) = 1$.

→ Ex. Prove that if $ax + by = \gcd(a,b)$, either $a = b = 0$ or $\gcd(x, y) = 1$.

→ Proof: If $a = b = 0$, $0 = \gcd(0,0)$, which is base. Otherwise: Let $d = \gcd(a,b)$. So, $d|a \wedge d|b$. So $\exists m, n \in \mathbb{Z}$ such that $md = a \wedge nd = b$. Now, since $d = ax + by$, we have $d = mdx + ndy \Rightarrow 1 = mx + ny$. Since $1|x$ and $1|y$, by GCD-CT we can conclude that $\gcd(x,y) = 1$. □

Bézout's Lemma: $\forall a, b, d \in \mathbb{Z}$, $\gcd(a,b) = d \Rightarrow [\exists x, y \in \mathbb{Z}, ax + by = d]$

→ Converse of the GCD-CT

Extended Euclidian Algorithm

→ For computing $\gcd(a,b)$ and finding $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a,b)$

→ Instructions:

→ Initialize a table w/ columns x, y, r, q

→ Row 1: $[1, 0, a, 0]$

→ Row 2: $[0, 1, b, 0]$

→ For $i > 3$, repeat $q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$ and $\text{Row}_i = \text{Row}_{i-2} - q_i \text{Row}_{i-1}$

→ Stop when $r_i = 0$. $\gcd(a,b) = r_{i-1}$, and x_{i-1} and y_{i-1} form the certificate of correctness.

x	y	r	q
1	0	1386	0
0	1	322	0
1	-4	98	4
-3	13	28	3
10	-43	14	3
-23	99	0	2

Further properties of GCD

→ $(c|a \wedge c|b) \Rightarrow c|\gcd(a,b)$ } GCD-GCD $(\forall a, b, c \in \mathbb{Z})$

(common divisor divides gcd)

→ Proof: Let $a, b, c \in \mathbb{Z}$. Assume $c|a$ and $c|b$. Let $d = \gcd(a,b)$. By Bézout's Lemma, $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$. By DIC, $c|ax + by$, so $c|d$. Thus, $c|\gcd(a,b)$.

→ $\forall a, b \in \mathbb{Z}$, $\gcd(a,b) = 1 \Rightarrow \gcd(a, b^n) = 1$ for all $n \in \mathbb{N}$

→ Proof: Let $a, b \in \mathbb{Z}$ and assume $\gcd(a,b) = 1$. By Bézout, $\exists s, t \in \mathbb{Z}$ such that $as + bt = 1$. We prove $\gcd(a, b^n) = 1$ by induction

→ Base case: $\gcd(a, b^1) = \gcd(a,b) = 1$.

→ IC: Let $\gcd(a, b^k) = 1$ for some $k \in \mathbb{N}$. By Bézout, $\exists x, y \in \mathbb{Z}$, $ax + b^k y = 1$. Since $as + bt = 1$, we have $1 = 1 \cdot 1 = (as + bt)(ax + b^k y) = \ldots = au + bv$ where $u = asx + b^k sy + btx$ and $v = ty \in \mathbb{Z}$. By the GCT-CT, $\gcd(a, b^{k+1}) = 1$.

→ $\forall a,b,d \in \mathbb{Z}$, $(d = \gcd(a,b) \wedge d \neq 0) \Rightarrow \gcd(\frac{a}{d}, \frac{b}{d}) = 1$

→ Proof: $d = \gcd(a,b) \Rightarrow d|a \wedge d|b$, so $\exists m,n \in \mathbb{Z}$ such that $md = a$ and $nd = b$. So, $\frac{a}{d} = m$ and $\frac{b}{d} = n$. Our assumption is $\gcd(m,n) = 1$. By Bézout's lemma, $\exists x,y \in \mathbb{Z}$ such that $ax + by = d$, thus $\frac{a}{d}x + \frac{b}{d}y = 1$. By the GCD-CT, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Coprimeness Characterization Theorem

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

→ Proof. By Bezout's lemma, $\exists s,t \in \mathbb{Z}$ such that $as + bt = 1$. Assume such integers exist. Now $1|a \wedge 1|b$ for all $a,b \in \mathbb{Z}$, so by the GCD-CT, $\gcd(a,b) = 1$

→ Showing $\gcd(a,b)\gcd(b,c)|a$: since $e|a$, $e|b$, $f|a$, $f|b$, $ef|ac \wedge ef|ab$. $\gcd(b,c) = 1 \Rightarrow \exists x,y \in \mathbb{Z}$, $bx + cy = 1$, so $abx + acy = a \Rightarrow ef|a$.

Prime Numbers

→ for $p \in \mathbb{N}$, if $p > 1$; p is prime $\Leftrightarrow [\forall k \in \mathbb{N}, k|p \Rightarrow k \in \{1, p\}]$

→ for $p \in \mathbb{N}$, p is composite (not prime) $\Leftrightarrow$
$\exists a,b \in \mathbb{N}$, $a,b > 1 \wedge ab = p$

→ Shorthand: $\mathbb{P} = \{\mathbb{N} : \forall k \in \mathbb{N}, k|p \Rightarrow k \in \{1,p\}\}$

→ Define this before using it on assignments, etc.

Prime Factorization Theorem

→ Every $n \in \mathbb{N}$ such that $n \geq 2$ can be written as a product of prime numbers.

→ Ex. $12 = (2)(3)(2)$, $2021 = (43)(47)$

→ $\prod_{i=1}^{1} q_i = 2$, where $q_1 = 2$ (example: 2)

product notation can be used

→ Proof: Proceed by strong induction. For each $n \in \mathbb{N}$. Let $P(n)$ be "n can be written as a product of primes."

→ Base case: 2 is prime

→ IS: Let $k \in \mathbb{N}$ and assume $k \geq 2$. Assume for each $r \in \mathbb{N}$ satisfying $2 \leq r \leq k$, that $P(r)$ is true, that is, each $r \in \{2, 3, 4 \ldots k\}$ can be written as a product of primes. Now consider $k+1$. If $k+1 \in \mathbb{P}$, then it is a product of primes. Suppose k is composite. (since $k+1 > 1$, it must be this if not prime). So, $\exists a, b \in \mathbb{N}$ such that $1 < a < k+1$ and $1 < b < k+1$ such that $ab = k+1$. By IH, a and b can be written as the product of primes: let $a = p_1 p_2 \ldots p_s$ and $b = q_1 q_2 \ldots q_t$. As such, $k = q_1 q_2 \ldots q_t p_1 p_2 \ldots p_s$ so $P(k+1)$ is true. Since we've shown $P(2) \wedge P(3) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)$, $P(n)$ must be true for all $N \in \mathbb{N}$ by POSI.

Unique Factorization Theorem

→ Every $n \in \mathbb{N}$, $n \geq 2$ can be expressed as a unique product of primes.

→ $\forall n \in \mathbb{N}, n \geq 2 \Rightarrow \exists! \{p_1, p_2 \ldots\} \in \mathbb{P}, p_1 p_2 \ldots = n$

Euclid's Theorem

→ Are there a finite amount of primes? ($|\mathbb{P}| \in \mathbb{N}$?) No.

→ Euclid's theorem: there are infinitely many primes.

→ Proof: suppose for the sake of obtaining a contradiction that there are a finite amount of primes. So, $\mathbb{P} = \{p_1, p_2 \ldots p_n\}$. Consider $N = p_1 p_2 \ldots p_n + 1$. By the FTA, N has to be written as a product of prime numbers, so there is at least one $i \in \{1, 2 \ldots n\}$ such that $p_i | N$. But, $N = (\prod_{j \neq i} p_j) p_i + 1$. By the GCD with remainders theorem, it must be that $\gcd(q p_i + 1, p_i) \Rightarrow \gcd(p_i, 1) = 1$, so $p_i \nmid N$. This is a contradiction of $p_i | N$, so our assumption must be false. Thus, there are infinitely many primes. □

Euclid's Lemma: $\forall a, b \in \mathbb{Z}, \forall p \in \mathbb{P}, p | ab \Rightarrow p | a \vee p | b$.

CAD: $\forall a, b, c \in \mathbb{Z}, (a | c \wedge \gcd(a, b) = 1) = a | c$

Finding Prime Factors

→ $\forall n \in \mathbb{N}$, if $n \geq 2$, n is either prime or $\exists p \in \mathbb{P}$, $1 < p \leq \sqrt{n}$, $p \mid n$

→ Example: Show 89 is prime

→ $9^2 < 89 < 100^2$, so we must check if 2, 3, 5, or 7 divides 89

→ Proof: Let $n \in \mathbb{N}$, $n \geq 2$. Assume n is not prime. By Prime Factorization, $\exists p_1, p_2 \dots p_k$ such that $n = p_1 p_2 \dots p_k$ ($k \geq 2$). Define $p = \min\{p_1, p_2 \dots p_k\}$ so that $p \leq p_i$ for all $i \in \{1 \dots k\}$. We have $p^2 \leq p^k \leq p_1 p_2 \dots p_k$, so $p^2 \leq n$, hence $p \leq \sqrt{n}$.

Divisors from prime factorization

→ Let $n \in \mathbb{N}$, $n \geq 2$, having prime factors $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$.
$\forall c \in \mathbb{N}$, $c \mid n \Leftrightarrow c = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \dots q_k^{\beta_k}$ for some $\beta_1 \dots \beta_k \in \mathbb{Z}$ satisfying $0 \leq \beta_i \leq \alpha_i$ for all $i \in \{1, \dots k\}$

→ Example: $98 \mid 2940$ because $98 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^2$ and $2940 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^2$

→ In general, $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$: total number of distinct positive divisors is $(a_1+1)(a_2+1)\dots(a_k+1)$ (because each power [starting at 0] can contribute $a+1$ powers of p as factors)

→ Ex. $2940 = 2^2 3^1 5^1 7^2$ has $3 \cdot 2 \cdot 2 \cdot 3 = 36$ distinct pos divisors

→ Ex. How many divisors of 2940 are multiples of 12? $12 = 2^2 \cdot 3^1$, so $2940/12 = (2^2 \cdot 3^1 \cdot 5^1 \cdot 7^2)/(2^2 \cdot 3^1) = 5^1 \cdot 7^2$, so it has $(1+1)(2+1) = 6$ factors. So, 2940 has 6 factors that are multiples of 12.

Problem: Prove $a^2 \mid b^2 \Rightarrow a \mid b$

→ By UFT, $b = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ for some distinct $p_1, \dots, p_k \in \mathbb{P}$ and $a_1 \dots a_k \in \mathbb{N}$. So, $b^2 = p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}$. Since $a \mid a^2$ and $a^2 \mid b^2$ (from hypothesis), we have $a \mid b^2$. By DFPF, $a = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ for some $\beta_1 \dots \beta_k \in \mathbb{Z}$, $0 \leq \beta_i \leq \alpha_i$ $\forall i \in \{1 \dots k\}$. Now, $a^2 = p_1^{2\beta_1} p_2^{2\beta_2} \dots p_k^{2\beta_k}$, but $a^2 \mid b^2$, so $0 \leq 2\beta_i \leq 2\alpha_i$ $\forall i \in \{1 \dots k\}$, so $0 \leq \alpha_i \leq \beta_i$ $\forall i \in \{1 \dots k\}$. So, by DFPF, $a \mid b$.

Using Prime Factorization to Find GCD

-> The gcd of two numbers is the product of all the prime factors of both numbers to their smallest powers.

-> If $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$,
$\gcd(m,n) = p_1^{\min(a_1,\beta_1)} p_2^{\min(a_2,\beta_2)} \dots p_k^{\min(a_k,\beta_k)}$

CHAPTER 7 Linear Diophantine Equations

-> Meaning: Linear Integer equations

-> Named for Diophantus, an ancient Greek mathematician

-> Exercise: compute gcd(15, 80) using the EEA

R_0	1	0	80
R_1	0	1	15
R_2	1	-5	5
R_3	-3	16	0

R_2

Q1) Are there any other solutions other than $(1,-15)$ to $80x + 15y = 5$

A1) If $80x + 15y = 5$ is true $(\exists x,y \in \mathbb{Z})$, (x,y) is a solution. So, we wish to find the cardinality of the solution set: $|\{(x,y) \in \mathbb{Z}^2 : 80x + 15y = 5\}|$

R_2 shows us that $80(-3) + 15(16) = 0$, so $80(1-3) + 15(-5+16) = 5$. We can also multiply $(-3,16)$ by a constant, and it will hold. So, for all $[x = 1-3n,\ y = -5+16n]\ (n \in \mathbb{Z})$, (x,y) is a solution. So, if any one solution exist, an infinite number of other solutions can be generated. Our solution set is $S = \{(x_0 - 3n,\ y_0 + 16n),\ n \in \mathbb{Z}\}$

Q2) For which $d \in \mathbb{Z}$ does the equation $80x + 15y = d$ have integer solutions?

A2) If $d = 1$, there are no solutions because 80 and 15 are not coprime.

If $5 \mid d$, we can just multiply both sides of the equation by $\frac{d}{5}$. So, $\exists k \in \mathbb{Z}$ so that $d = 5k$; $80(kx) + 15(ky) = d$. (point: $5 = \gcd(80,15)$).

If $5 \nmid d$, there are not [integer] solutions

Proof: Let $d \in \mathbb{Z}$. Suppose there is one solution, meaning $\exists x,y \in \mathbb{Z}$ $80x + 15y = d$. Since $5 \mid 80$ ^ $5 \mid 15$, by DLC $5 \mid (80x + 15y) \equiv 5 \mid d$. So, we must have $5 \mid d$.

-> Examples of LDEs: $7a + 7 = 3b$, $18v + 5v - 6w + 7 = 0$.

-> Non-examples: $x^2 + y^2 = 1$ (not linear), $\cos(x) = y + z$ (not linear), $\frac{7}{2}x + y = \pi$ (non-integer coefficients), $3x + 2y$ (not an equation)

LDE Theorem I:

→ For all $a, b, c \in \mathbb{Z}$

$$\left[\text{The equation } \boxed{ax+by=c} \text{ (*) has an integer solution}\right] \iff \left[\gcd(a,b) \mid c\right]$$

→ Proof: Let $a, b, c \in \mathbb{Z}$.

→ ($\Rightarrow$). By the hypothesis, assume $\exists x, y \in \mathbb{Z}$, $ax+by=c$. Since $\gcd(a,b) \mid a$ ↑ $\gcd(a,b) \mid b$, by DLC $\gcd(a,b) \mid c$

→ ($\Leftarrow$) Assume $\gcd(a,b) \mid c$. Such, $\exists k \in \mathbb{Z}$, $c = k \cdot \gcd(a,b)$. By Bézout's lemma, $\exists s, t \in \mathbb{Z}$, $as+bt = \gcd(a,b)$, so $kas + kbt = k\gcd(a,b)$. Let $x = ks$ and $y = kt$. As such, $ax+by=c$. □

LDE Theorem II

→ For all $a, b, c \in \mathbb{Z}$, if $\gcd(a,b) \neq 0$ and $ax+by=c$ has at least one integer solution, it has infinitely many solutions. Moreover, it must have the form $x = x_0 - \frac{b}{d}n$, $y = y_0 + \frac{a}{d}n$, where $d = \gcd(a,b)$ for some $n \in \mathbb{Z}$.

→ Solution set: $\{(x,y) \in \mathbb{Z}^2 : ax+by=c\} = \{(x_0 - \frac{b}{d}n,\ y_0 + \frac{a}{d}n) : n \in \mathbb{Z}\}$

→ If $ax+by=c$ has a solution (x_0, y_0)

→ Solutions lie on the line $y = \frac{c-ax}{b}$ (integer solutions are evenly spaced)

→ Ex. $21x + 18y = 6$

→ $\gcd(21,18) = 3$ and $3 \mid 6$, so solutions exist

→ We have $21(2) + 18(-2) = 6$, so $x_0 = 2$ and $y_0 = -2$

→ Solutions set: $\{(2 - \frac{18}{3}n,\ -2 + \frac{21}{3}n) : n \in \mathbb{Z}\}$

$= \{(2-6n,\ 7n-2) : n \in \mathbb{Z}\}$

Modular Arithmetic

-> Like doing math with time: what comes 123 hours before 09:00?

06:00 ← 12 hours on a clock

-> $9 + 123 \equiv 6 \pmod{12}$

Congruence

-> Let $m \in \mathbb{N}$. For integers $a, b \in \mathbb{Z}$:

a is congruent to b modulo $m \iff m \mid (a-b)$ ← equivalent: $\iff \exists k \in \mathbb{Z}, mk = a-b$

-> Expressed $a \equiv b \pmod{m}$

-> Otherwise, we have $a \not\equiv b \pmod{m}$ $(m \nmid (a-b))$

-> Ex. $17 \equiv 2 \pmod{15}$, $17 \not\equiv 2 \pmod{4}$

Equivalence Relations

-> Properties of $=$ (The equals sign):

-> Reflexive: $\forall a \in \mathbb{Z}, a = a$

-> Symmetric: $\forall a, b \in \mathbb{Z}, a = b \Rightarrow b = a$

-> Transitive: $\forall a, b, c \in \mathbb{Z}, (a = b \wedge b = c) \Rightarrow a = c$

-> Not all relationships have these properties

-> $\mid$ (divides by) is not symmetric

-> $<$ (less than) is not symmetric and not transitive

-> However, congruence does have these properties

-> Let $m \in \mathbb{N}$, $\forall a, b, c \in \mathbb{Z}$

(R) -> $a \equiv a \pmod{m}$

(S) -> $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(T) -> $(a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$

-> Proof: Let $a, b, c \in \mathbb{Z}$

(R) -> $a - a = 0$ and $m \mid 0$, so $a \equiv a \pmod{m}$

(S) -> assume $a \equiv b \pmod{m}$. Thus, $m \mid (a-b)$, so $\exists k \in \mathbb{Z}, mk = a-b$

now $-k \in \mathbb{Z}$ and $m(-k) = b-a$, so $m \mid (b-a)$ so $b \equiv a \pmod{m}$

-> Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Thus,

$m \mid (a-b) \wedge m \mid (b-c)$. By DIC, $m \mid (a-b)+(b-c) \iff m \mid a-c$,

so $a \equiv c \pmod{m}$

Modular Arithmetic

-> We can add, subtract, and multiply like normal

CAM: -> Congruence add and multiply): For all $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ if $a_1 \equiv b_1 \pmod m$ and $b_1 \equiv b_2 \pmod m$, then

1) $a_1 + a_2 \equiv b_1 + b_2 \pmod m$
2) $a_1 - a_2 \equiv b_1 - b_2 \pmod m$
3) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m$

-> Proof:

1) By DIC, $m \mid [(a_1 - a_2) + (b_1 - b_2)]$, so $m \mid [(a_1 + b_1) - (a_2 + b_2)]$ hence $a_1 + b_1 \equiv a_2 + b_2 \pmod m$
2) Similar proof to 1)
3) $\exists k, l \in \mathbb{Z}$ such that $a_1 - b_1 = km$ and $a_2 - b_2 = lm$
$a_1 a_2 = (b_1 + km)(b_2 + lm) = b_1 b_2 + m(lb_1 + kb_2 + klm)$
so $m \mid (a_1 a_2 - b_1 b_2)$ hence $a_1 a_2 \equiv b_1 b_2 \pmod m$

proofs follow from CAM from induction

-> Proposition: adding or multiplying any number of terms is always fine (per CAM)

-> Proposition: let $m \in \mathbb{Z}$, $\forall a, b \in \mathbb{Z}$, if $a \equiv b \pmod m$ then $\forall n \in \mathbb{N}$, $a^n \equiv b^n \pmod m$

-> Example: what is the remainder of $(5^9 + 62^{2021})/7$?

-> $5^3 \equiv -1 \pmod 7$, so $(5^3)^3 = 5^9 \equiv (-1)^3 = -1 \pmod 7$

-> $62 \equiv -1 \pmod 7$, so $62^{2021} \equiv -1 \pmod 7$

-> So $5^3 + 62^{2021} \equiv -1 - 1 \equiv -2 \equiv 5 \pmod 7$

-> Division: Let $m \in \mathbb{N}$. $\forall a, b, c \in \mathbb{Z}$:

$ac \equiv bc \pmod m \wedge \gcd(c, m) = 1 \Rightarrow a \equiv b \pmod m$

-> Proof: we have $m \mid ac - bc$ so $m \mid c(a-b)$. Since $\gcd(m, c) = 1$, by Coprimeness and Divisibility (CAD), we have $m \mid (a-b)$, so $a \equiv b \pmod m$

-> Congruent iff same remainder:

$a \equiv b \pmod m \Leftrightarrow a/m$ and b/m have the same remainder

$0 \le a < 10,\ a \in \mathbb{Z}$

Fun Problems

-> **Last digit** of a number n : $n \equiv a \pmod{10}$

-> Ex. last digit of $3^{10} \cdot 4^{45}$.

-> $3^2 \equiv +1 \pmod{10}$, so $3^{10} \equiv (3^2)^5 \equiv (-1)^5 \equiv -1 \pmod{10}$

-> $4^n \pmod{10}$ alternates between 4 and 6 (show by showing $4 \Rightarrow 6$ and $6 \Rightarrow 4$), so $4^{45} \equiv 4 \pmod{10}$

-> $-1 \cdot 4 \equiv -4 \equiv 6 \pmod{10}$

Divisibility Rules

-> Any $n \in \mathbb{Z}$ can be represented as

$d_0 \cdot 10^0 + d_1 \cdot 10^1 + d_2 10^2 + \dots d_k 10^k$

where $d_0, d_1, d_2 \dots$ are the digits of that number

-> Divisibility by 3

-> For all $n \in \mathbb{N}$, $3 \mid n \Leftrightarrow$ sum of n's digits is divisible by 3

-> Proof: $10 \equiv 1 \pmod 3$. Thus $10^k \equiv 1^k \equiv 1 \pmod 3$ for all $k \in \mathbb{N}$. Also, $3 \mid n \Leftrightarrow n \equiv 0 \pmod 3$. Now.

$d_0 10^0 + d_1 10^1 + d_2 10^2 \dots \equiv d_0 + d_1 + d_2 \dots \pmod 3$, so

$d_0 10^0 + d_1 10^1 + d_2 10^2 \equiv 0 \pmod 3 \Rightarrow d_1 + d_2 + d_3 \equiv 0 \pmod 3$

$\Rightarrow 3 \mid d_1 + d_2 + d_3 \dots$

-> Divisibility by 11

-> $10 \equiv -1 \pmod{11}$, and $10^2 \equiv 1 \pmod{11}$.

-> Similar to 3, but the odd powers of 10 evaluate to $-d_k$ (while the positive ones still evaluate to d_k)

-> So, the alternating sum of digits must be divisible by 11 if the number is divisible by 11

-> 9 has the same rule as 3 for the same reason ($10 \equiv 1 \pmod 9$)

Linear Congruences

-> A linear congruence is an open sentence in the form:
$ax \equiv c \pmod{m}$ for $a, c, m \in \mathbb{Z}$

LCT

-> A linear congruence has a solution if and only if $\gcd(a,m) \mid c$
(derived from LDET 1 and def of congruence)
-> If there is one solution, there are an infinite number of them

-> Proof: $ax_0 \equiv c \pmod{m} \Leftrightarrow m \mid (ax_0 - c) \Leftrightarrow \exists y_0 \in \mathbb{Z},\ my_0 = ax_0 - c$
$\Leftrightarrow \exists y_0 \in \mathbb{Z}\ \ ax_0 - my_0 = c \Leftrightarrow \exists y_0 \in \mathbb{Z}\ \ ax_0 + (-m)y_0 = c$
(LDET 1 and 2 can be applied)

-> Solution set: $S = \{x_0 + \frac{m}{d}n : n \in \mathbb{Z}\}$

-> Strategy for finding solutions: convert to $ax + my = c$, solve using EEA

Non-Linear Congruences

-> EEA can't be used

-> For small m, guess and check (every integer is congruent to one of $0, 1, 2 \ldots m-1 \pmod{m}$)
-> for $x^2 \equiv 3 \pmod{6}$, we check $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ mod 6 (and find $3^3 \equiv 3 \pmod{6}$ is a solution
-> One solution => Infinite solutions $(a + mn)$ for all $n \in \mathbb{Z}$

Congruency Classes

may be written as $[a]$ if m is clear

-> Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. The congruency class of a mod m, denoted $[a]_m$, is the set $\{x \in \mathbb{Z};\ x \equiv a \pmod{m}\}$
-> set of all integers that equal a mod m
-> Ex. for $m = 5$, $[1] = [6] = [2021]$ since $1 \equiv 6 \equiv 2021 \pmod{5}$

-> $\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots [m-1]_m\}$
-> Set of distinct congruency classes mod m
-> $[0] \cup [1] \cup [2], \ldots \cup [m-1] = \mathbb{Z}$
-> $[a] \cap [b] \neq \emptyset \Leftrightarrow a \equiv b \pmod{m} \Leftrightarrow [a] = [b]$

subtraction works similarly

Operations on $\mathbb{Z}_m$

-> Addition: $[a] + [b] = [a+b]$

-> $[3]_5 + [2]_5 = [5]_5 = [0]_5$ $(3+2 \equiv 0 \equiv 5 \pmod 5)$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

-> An addition table summarizes all possible additions in a given modulus

-> Ex. addition table for $\mathbb{Z}_3$

-> Here, $[1]+[2] = [3] = [0]$, etc

-> Multiplication: $[a] \cdot [b] = [ab]$

-> $[3]_5 \cdot [2]_5 = [6]_5 = [1]_5$ $(3 \cdot 2 \equiv 1 \equiv 6 \pmod 5)$

-> $3 = 5k+3$, $2 = 5k+2$ -> $3 \cdot 2 = (5k+3)(5k+2) =$

$25k^2 + 25k + 5 = 5(5k^2 + 5k + 1) + 1 = 5n + 1$

-> We can create a multiplication table in a similar way

Properties of Modular Arithmetic

Let $m \in \mathbb{Z}$, for all $a \in \mathbb{Z}$

- $[0] + [a] = [a] + [0] = [a+0] = [a]$ ← $[0]$ is the additive identity
- $[0] \cdot [a] = [a] \cdot [0] = [0]$
- $[a] + [-a] = [-a] + [a] = [0]$ ← $[-a]$ is the additive inverse of $[a]$
- $[a] \cdot [1] = [1] \cdot [a] = [a]$ ← $[1]$ is the multiplicative identity

Multiplicative Inverses

-> If there exists a $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1]$, then $[b]$ is the multiplicative inverse of $[a]$

-> This is denoted $[a]^{-1}$

-> A given congruency class has at most one multiplicative inverse

-> ex. $[2]_5^{-1} = [3]_5$ since $[2]_5 \cdot [3]_5 = [2 \cdot 3]_5 = [6]_5 = [1]_5$

-> There may not exist a multiplicative inverse for some cases

-> $p \in \mathbb{Z}$ is prime, for every $a \in \mathbb{Z}$, $1 \leq a < p$, $[a]^{-1}$ exists in $\mathbb{Z}_p$

-> Follows from gcd rule

-> $[0]$ never has a multiplicative inverse for $\mathbb{Z}_2$ or higher

Finding Multiplicative Inverses

-> We are looking for $x \in \mathbb{Z}$ such that $[a]_m [x]_m = [1]_m$

-> This is equivalent to $ax = 1 \pmod m$

-> This can be solved using the LCT

Modular Arithmetic Theorem

-> let $m \in \mathbb{Z}$. Let $a, c \in \mathbb{Z}$ and consider $[a][x] = [c]$ in $\mathbb{Z}_m$

(1) A solution exists in $\mathbb{Z}_m \iff \gcd(a,m) \mid c$

(2) If a solution exists, the others are $[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}]$ ... $[x_0 + (d-1)\frac{m}{d}]$ where $d = \gcd(a,m)$

Fermat's Little Theorem (FLT)

$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z}, \; p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

-> $[a]^{p-1}$ is a multiplicative inverse of $[a] \bmod p$ (if conditions are met)

-> Let p be prime and $a \in \mathbb{Z}$ such that $\gcd(a,p) = 1$. Now $[a][a^{p-2}] = [a^{p-1}] = [a]^{p-1} = 1$ (by FLT).

-> So, $[a]^{-1} = [a^{p-2}]$ in $\mathbb{Z}_p$ (!)

Chinese Remainder Theorem (CRT)

-> problem: solve $\begin{cases} a \equiv 4 \pmod 5 & (1) \\ a \equiv 3 \pmod 9 & (2) \end{cases}$ (assume a exists)

-> By (1), we have $\exists x \in \mathbb{Z}, a = 5x + 4$, so we have $5x + 4 \equiv 3 \pmod 9$

$\Rightarrow -5x = -1 \pmod 9$, $\Rightarrow$ By LDET $x = 2 + 9n$ and $y = -1 - 5n$,

So $a = 5x + 4 = 5(2 + 9n) + 4 = 10 + 45n + 4 = 14 + 45n$

-> Theorem: $\forall m_1, m_2 \in \mathbb{N}$ and $\forall a_1, a_2 \in \mathbb{Z}$, if $\gcd(m_1, m_2) = 1$

Then $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ has a solution. If that solution is x_0,

then all other solutions are $\{x_0 + m_1 m_2 n : n \in \mathbb{Z}\}$.

$= \{x \in \mathbb{Z} : x \equiv x_0 \pmod{m_1, m_2}\}$

Generalized CRT

-> Applies to any number of equations in the system

-> If every set of two a are coprime, solution mod $m_1 m_2 m_3 \ldots$

-> Solving: feed solution to two into the next one

Splitting the Modulus

-> Suppose $m_1, m_2 \in \mathbb{N}$ and $\gcd(m_1, m_2) = 1$ and $a \in \mathbb{Z}$. $\forall x \in \mathbb{Z}$,

$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases} \iff x$ is a solution to $x \equiv a \pmod{m_1 m_2}$

-> Proof: uses CRT

-> Ex: find solutions to $x^2 \equiv 34 \pmod{99}$

-> Equivalent to (1) $x^2 \equiv 34 \pmod{9}$ and (2) $x^2 \equiv 34 \pmod{11}$

equivalent to $x^2 \equiv 7 \pmod{9}$

Equivalent to $x^2 \equiv 7 \pmod{11}$

-> Solutions to one (inspection): $x \equiv 4 \pmod{9}$ or $x \equiv 5 \pmod{9}$

-> Solutions to two (inspection): $x \equiv 1 \pmod{11}$ or $x \equiv 10 \pmod{11}$

-> So, there are four combination that yield solutions:

-> $x \equiv 4 \pmod{9}$ and $x \equiv 1 \pmod{11} \Rightarrow x = 67 \pmod{99}$

-> $x \equiv 4 \pmod{9}$ and $x \equiv 10 \pmod{11} \Rightarrow x = 76 \pmod{99}$ etc

-> Four solutions: $[67]_{99}, [76]_{99}, [23]_{99}, [32]_{99}$

Cryptography

-> How to communicate securely

-> Steps for secure communication

-> A wants to send a message to B

-> A encodes message into a number -> the plaintext

-> A encrypts the message using an encryption key (encrypted message: ciphertext)

-> A sends ciphertext to B

-> B decrypts it using a decryption key

-> Symmetric encryption: encryption and decryption keys are the same

-> Otherwise, asymmetric encryption

RSA Encryption

→ Asymmetric encryption method
→ B generates a public and private key
  → Everyone knows the public key, only bob knows the private key
→ A encrypts message using public key, B uses private key to decrypt

Generating Public and Private Keys

→ B picks two large primes p and q
→ Let $n = p \cdot q$
→ B picks some $e \in \{1, 2, 3 \dots (p-1)(q-1)\}$ where $\gcd(e, (p-1)(q-1)) = 1$
→ Because $\gcd(e, (p-1)(q-1)) = 1$, there exists a unique $d \in \mathbb{Z}$ such that $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

B's public key: (n, e)	B's private key: (n, d)

only B knows p, q, so only they can find d

→ Someone can't just guess p and q because factoring numbers is an incredibly hard task [2048-bit number → longer than universe age]

How RSA encryption actually plays out

→ Alice chooses message $M \in \{0, 1, 2 \dots n-1\}$
  → Can encode whatever (probably ASCII text)
→ Alice encrypts M using the public key e by solving $C \equiv M^e \pmod{n}$ where $0 \leq C \leq n-1$
  → C is the encrypted message (the ciphertext)
  → This is sent to Bob
→ Bob recives message C and solves for $R \equiv C^d \pmod{n}$ for $R \in \{0 \dots n\}$
  → R is the received message, and is equal to M

Proof that $R = M$

→ We have $R \equiv C^d \equiv M^{ed} \pmod{pq}$
→ $\exists k \in \mathbb{Z}$ such that $ed = 1 + k(p-1)(q-1)$ ①
→ By splitting the modulus, we have $R \equiv M^{ed} \pmod{p}$ ∧ $R \equiv M^{ed} \pmod{q}$ ②

similar proof for ②

① If $p \mid M$, $M \equiv 0 \pmod{p}$, so $R \equiv 0^{ed} \equiv 0 \equiv M \pmod{p}$
  If $p \nmid M$, then $M^{p-1} \equiv 1 \pmod{p}$, so $R \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)}$
  $\equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot (1)^{k(q-1)} \equiv M \cdot 1 \equiv M \pmod{p}$

By ⑤M, $R \equiv M \pmod{p}$ ∧ $R \equiv M \pmod{q} \Rightarrow R \equiv M \pmod{pq}$

Types of Numbers

-> $\mathbb{N}$: counting numbers (invented to count items)
-> $\mathbb{Z}$: integers: includes negative numbers
-> $\mathbb{Q}$: ratios between integers (accepted since antiquity)
-> $\mathbb{R}$: solutions to problems like $x^2 = 2$
-> $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$
-> But $x^2 + 1 = 0$ has no solution in $\mathbb{R}$, we need new numbers...

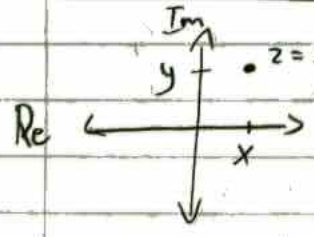
Complex Numbers

-> For some $x, y \in \mathbb{R}$, $x + yi$ is a complex number ($i = \sqrt{-1}$) ($z =$)
-> $z \in \mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$
-> Since $0 \in \mathbb{R}$, any complex number of the form $x + 0i$ is also a real number, so $\mathbb{R} \subset \mathbb{C}$
-> Real part of z: $\mathrm{Re}(z)$ $\quad \mathrm{Re}(2+3i) = 2$] $\in \mathbb{R}$
-> Imaginary Part of z: $\mathrm{Im}(z)$ $\quad \mathrm{Im}(2+3i) = 3$ (not $3i$)]
-> $z = \mathrm{Re}(z) + \mathrm{Im}(z) \cdot i$
-> A complex number can be purely real or imaginary (x or $y = 0$)
-> $\forall z, w \in \mathbb{C}$, $z = w \iff [\mathrm{Re}(z) = \mathrm{Re}(w) \wedge \mathrm{Im}(z) = \mathrm{Im}(w)]$

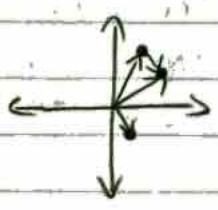
Complex Arithmetic

-> for $z = a + bi$ and $w = c + di$ $(a, b, c, d \in \mathbb{R})$
-> $z + w = a + bi + c + di = (a + c) + (b + d)i$
-> $z \cdot w = (a + bi)(c + di) = ac + abi + bic + bdi = (ac - bd) + (ad + bc)i$
-> we can use this to show $i = \sqrt{-1}$

The Complex Plane...



-> Since complex numbers have two dimensions, they are represented in the complex plane
-> Horizontal axis: real axis
-> Vertical axis: vertical axis



-> Adding two points is like adding two vectors (tip to tail)

Multiplicative Inverses

→ For $z, w \in \mathbb{C}$, w is a multiplicative inverse of z if $w \cdot z = 1$

→ Exists as long as $z \neq 0$. Moreover, it is unique and defined by

$$z^{-1} = \frac{x}{x^2+y^2} + \frac{-y}{x^2+y^2}i \quad \text{where } z = x+yi$$

→ This is of course equal to $\frac{1}{z}$ as well

Exponents

→ We define $z^0 = 1$, $z^1 = z$ and $z^{k+1} = z^k z^1$ for all $k \in \mathbb{N}$

Properties of Complex Arithmetic

→ For all $v, w, z \in \mathbb{C}$

(1) $(v+w)+z = v+(w+z)$	Associativity of addition
(2) $w+z = z+w$	Commutativity of addition
(3) $z+0 = z$	Additive Identity: 0
(4) $z+(-z) = 0$	Additive Inverse: $-z$
(5) $(v \cdot w) \cdot z = v \cdot (w \cdot z)$	Associativity of multiplication
(6) $w \cdot z = z \cdot w$	Commutativity of multiplication
(7) $1 \cdot z = z$	Multiplicative Identity: 1
(8) If $z \neq 0$, $z \cdot z^{-1} = 1$	Multiplicative inverse: z^{-1}
(9) $z(v+w) = zv + zw$	Distributivity

→ Regular exponent rules also hold

Polynomials in $\mathbb{C}$

→ Let $f(z) = az^2 + bz + c$, $a, b, c \in \mathbb{C}$

→ $f(z)$ has a real solution if $\exists x \in \mathbb{R}$ such that $f(x) = 0$

→ Strategy: Distribute complex number coefficients over x, split into complex and imaginary polynomials, solve each for 0, pick overlapping values

→ Ex. $6z^3 + (1+3\sqrt{2}i)z^2 - (11-2\sqrt{2}i)z - 6 = 0 \Rightarrow$

$6x^3 + x^2 - 11x - 6 + (3\sqrt{2}x^2 + 2\sqrt{2}x)i = 0$, which implies both parts are 0

$3\sqrt{2}x^2 + 2\sqrt{2}x = 0 \Rightarrow x = 0$ or $x = -\frac{2}{3}$. $x = 0$ is not a solution to $6x^3 + x^2 - 11x - 6 = 0$, and $x = -\frac{2}{3}$ is, so $x = -\frac{2}{3}$ is the only solution

Conjugate

→ Given $z \in \mathbb{C}$ and $z = x + yi$, the conjugate $\overline{z}$ of z is $x - yi$

→ Normal real part, negative complex part

(1) $\overline{(\overline{z})} = z$ (2) $\overline{z+w} = \overline{z} + \overline{w}$

(3) $z + \overline{z} = 2 \cdot Re(z)$ ^ $z - \overline{z} = 2\,Im(z)i$

(4) $\overline{zw} = \overline{z} \cdot \overline{w}$ (5) $z \neq 0 \Rightarrow \overline{z^{-1}} = (\overline{z})^{-1}$

→ All of these can be proven by breaking z into $x + yi$

→ Corollary: $z = \overline{z} \Leftrightarrow z$ is purely real $\Leftrightarrow Im(z) = 0$

→ We also have $z \cdot \overline{z} = x^2 + y^2 = |z|^2$

→ Trick for dividing complex numbers: multiply top and bottom by conjugate

→ $\frac{3-2i}{(4+i)(i)} = \frac{3-2i}{(4+i)(i)} \cdot \frac{4-i}{4-i} \cdot \frac{-i}{-i} = \frac{(3-2i)(4-i)(-i)}{(4+i)(4-i)\cdot(i)(-i)} = \frac{(14-11i)(-i)}{17} = \dots$

Modulus

→ If $x \in \mathbb{R}$ and $x \geq 0$, $\sqrt{x}$ is defined as the unique non-negative number such that $(\sqrt{x})^2 = x$.

→ Not defined for non-purely-real complex numbers

→ Given $z \in \mathbb{C}$, the modulus $|z|$ of z is $\sqrt{z\overline{z}}$

→ If $z = x + yi$, $|z| = \sqrt{x^2+y^2}$

→ Denotes the number's distance from the origin on the complex plane

(1) $|z| \neq 0 \Leftrightarrow z = 0$ (2) $|\overline{z}| = |z|$

(3) $z\overline{z} = |z|^2$ (4) $|zw| = |z||w|$

(5) $z \neq 0 \Rightarrow |z^{-1}| = |z|^{-1}$

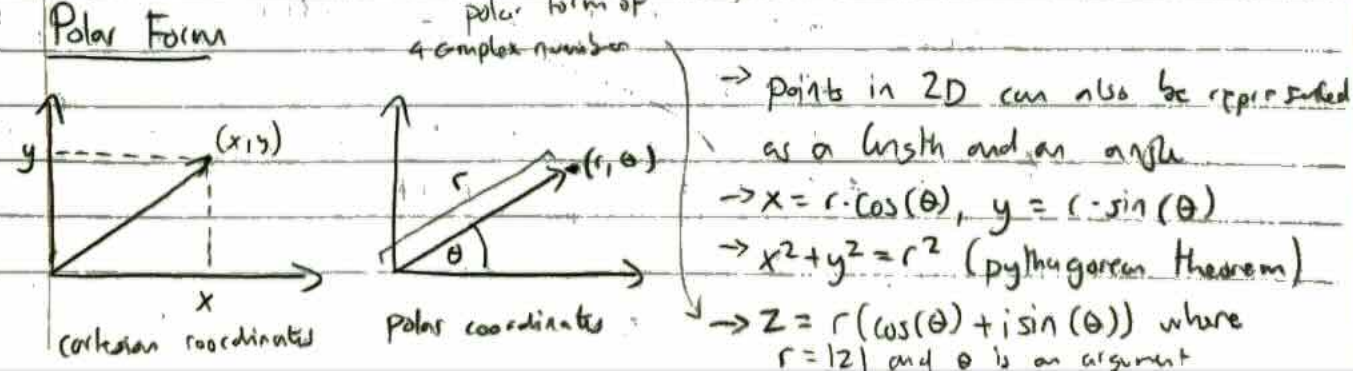
→ If $x \in \mathbb{R}$, the modulus of x is the same as the absolute value of x

→ From triangle inequality: $|z+w| \leq |z| + |w|$

→ Since both end at $z+w$ but $|z|+|w|$ takes a longer path unless either z or w is a multiple of the other

→ The set $\{z \in \mathbb{C} : |z| = 1\}$ denotes the unit circle

Polar Form



→ Points in 2D can also be represented as a length and an angle

→ $x = r \cdot \cos(\theta)$, $y = r \cdot \sin(\theta)$

→ $x^2 + y^2 = r^2$ (pythagorean theorem)

→ $z = r(\cos(\theta) + i\sin(\theta))$ where $r = |z|$ and θ is an argument

Converting from Cartesian to Polar Form

- Step 1: Find r (the modulus)
- Step 2: Find θ
- Ex: convert $z = -\sqrt{3} + i$
  - $r = \sqrt{(-\sqrt{3})^2 + 1^2} = \sqrt{4} = 2$
  - $z = 2\left(-\frac{\sqrt{3}}{2} + \frac{1}{2}i\right)$ we need to find θ such that $\cos\theta = -\frac{\sqrt{3}}{2}$ and $\sin\theta = \frac{1}{2}$ (look familiar)
  - $\sin\left(\frac{5}{6}\pi\right) = \frac{1}{2}$ and $\cos\left(\frac{5}{6}\pi\right) = -\frac{\sqrt{3}}{2}$, so $\theta = \frac{5\pi}{6}$
  - $z = 2\left(\cos\left(\frac{5}{6}\pi\right) + i\sin\left(\frac{5}{6}\pi\right)\right)$
- Ex. $z = -\sqrt{3} - 3i$
  - $r = \sqrt{(-\sqrt{3})^2 + (-3)^2} = \sqrt{3+9} = \sqrt{12} = 2\sqrt{3}$
  - $z = 2\sqrt{3}\left(-\frac{1}{2} - i\left(\frac{\sqrt{3}}{2}\right)\right) \longrightarrow \theta = \frac{4\pi}{3}$
  - $z = 2\sqrt{3}\left(\cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right)\right)$

Multiplication in Polar Form

- Uses trig identities
  - $\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$
  - $\sin(\alpha+\beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)$
- Let $z_1, z_2 \in \mathbb{C}$, where $z_1 = r_1(\cos(\theta_1) + i\sin(\theta_1))$, $z_2 \ldots$
  - $z_1 z_2 = r_1 r_2 (\cos\theta_1 + i\sin\theta_2)(\cos\theta_2 + i\sin\theta_2)$
    $= r_1 r_2 [(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_2\cos\theta_2 + \cos\theta_1\sin\theta$
    $= r_1 r_2 (\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$
  - When multiplying two complex numbers, multiply their moduli and add their angles (in polar form).
  - $zw = |z||w|(\cos(\theta_z+\theta_w) + i\sin(\theta_z+\theta_w))$
  - some notation: $\mathrm{cis}(\theta) = \cos(\theta) + i\sin(\theta)$
    - $zw = |z||w|\,\mathrm{cis}(\theta_z+\theta_w)$
- Ex. $z_1 = 1+i$, $z_2 = 3i$. Calculate $z_1 z_2$ in polar form
  - $z_1 = \sqrt{2}(\mathrm{is}(\frac{\pi}{4})$, $z_2 = 3\,\mathrm{cis}(\frac{\pi}{2})$
  - $z_1 z_2 = 3\sqrt{2}\,\mathrm{cis}(\frac{\pi}{4}+\frac{\pi}{2}) = 3\sqrt{2}\,\mathrm{cis}(\frac{3\pi}{4}) = 3\sqrt{2}\left(-\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right)$
    $= -3 + 3i$
- $z^{-1} = \frac{r\cdot\cos(\theta) - ir\sin\theta}{r^2\cos^2\theta + r^2\sin^2\theta} = \frac{r(\cos\theta - i\sin\theta)}{r^2(1)} = \frac{\cos\theta - i\sin\theta}{r}$

$= \frac{1}{r}(\cos(-\theta) + i\sin(-\theta)) = \boxed{\frac{1}{r}\,\mathrm{cis}(-\theta)}$

De Moivre's Theorem

-> For all $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, $\text{cis}(\theta)^n = \text{cis}(n\theta)$

↳ Corollary: For all $z \in \mathbb{C}$, $z = r\text{cis}(\theta)$, and all $n \in \mathbb{Z}$,

$z^n = r^n \text{cis}(n\theta)$

-> unless $r = 0$ and $n < 0$

-> $z = \text{cis}\left(\frac{3\pi}{4}\right)$. (alculate $z^{-1000} = \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right)^{-1000} =$

$\text{cis}\left(\frac{3\pi}{4}\right)^{-1000} = \text{cis}\left(-1000 \cdot \frac{3\pi}{4}\right) = \text{cis}(-750\pi) =$

$\text{cis}(-375 \cdot 2\pi)$ (since multiple of 2π, we have $= \text{cis}(2\pi)$

$= \cos(2\pi) + i\sin(2\pi) = 1 + 0i = 1$

-> $z = 1 + \sqrt{3}i = r \cdot \text{cis}(\theta)$. (alculate $z^8 = r^8 \text{cis}(8\theta)$ ->

$r = |z| = 2$, $z = 2\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 2\,\text{cis}\left(\frac{\pi}{3}\right)$ ->

$z^8 = 2^8 \text{cis}\left(8 \cdot \frac{\pi}{3}\right) = 256 \cdot \text{cis}\left(2\pi + \frac{2\pi}{3}\right) = 256 \cdot \text{cis}\left(\frac{2\pi}{3}\right)$

-> Proof:

-> Case one: true for $n \in \mathbb{N}$. We will prove by induction.

$P(n)$: $\forall \theta \in \mathbb{R}$, $\text{cis}(\theta)^n = \text{cis}(n\theta)$. Base case: $n = 1$.

Let $\theta \in \mathbb{R}$. $\text{cis}(\theta)^1 = \text{cis}\theta = \text{cis}(1 \cdot \theta)$, so $P(1)$ is true.

IC: Let $k \in \mathbb{N}$ be arbitrary and assume $P(k)$. Let $\theta \in \mathbb{R}$ be arbitrary. Now $\text{cis}(\theta)^{k+1} = \text{cis}(\theta)\text{cis}(\theta)^k =$

$\text{cis}(k\theta)\text{cis}(\theta)$ [by IH] $= \text{cis}(k\theta + \theta) = \text{cis}((k+1)(\theta))$

-> Case two: $n = 0$. Let $\theta \in \mathbb{R}$. $\text{cis}(0)^0 = 1 = \text{cis}(0) = \text{cis}(0\theta)$

-> Case three: Let $n \in \mathbb{Z}$ be negative and let $\theta \in \mathbb{R}$. Because $n < 0$, $n = (-1)|n|$, where $|n| \in \mathbb{N}$. We have already proved $P(|n|)$. Now, $\text{cis}(\theta)^n = \text{cis}(\theta)^{-|n|} = (\text{cis}(\theta)^{-1})^{|n|}$

$= \text{cis}(-\theta)^{|n|} = \text{cis}(-|n|\theta)$ (since we've proved DMT for $|n|$)

$= \text{cis}((-n)(\theta))$

-> Proven in all cases, so it must be true

Conjugate Root Theorem

-> Suppose $f(x) = a_0 + a_1x + a_2x^2 + \dots a_nx^n$. Suppose $c \in \mathbb{C}$ is a root, meaning $f(c) = 0$. Then, $\overline{c}$ is also a root

-> Super helpful for factoring polynomials in $\mathbb{C}$