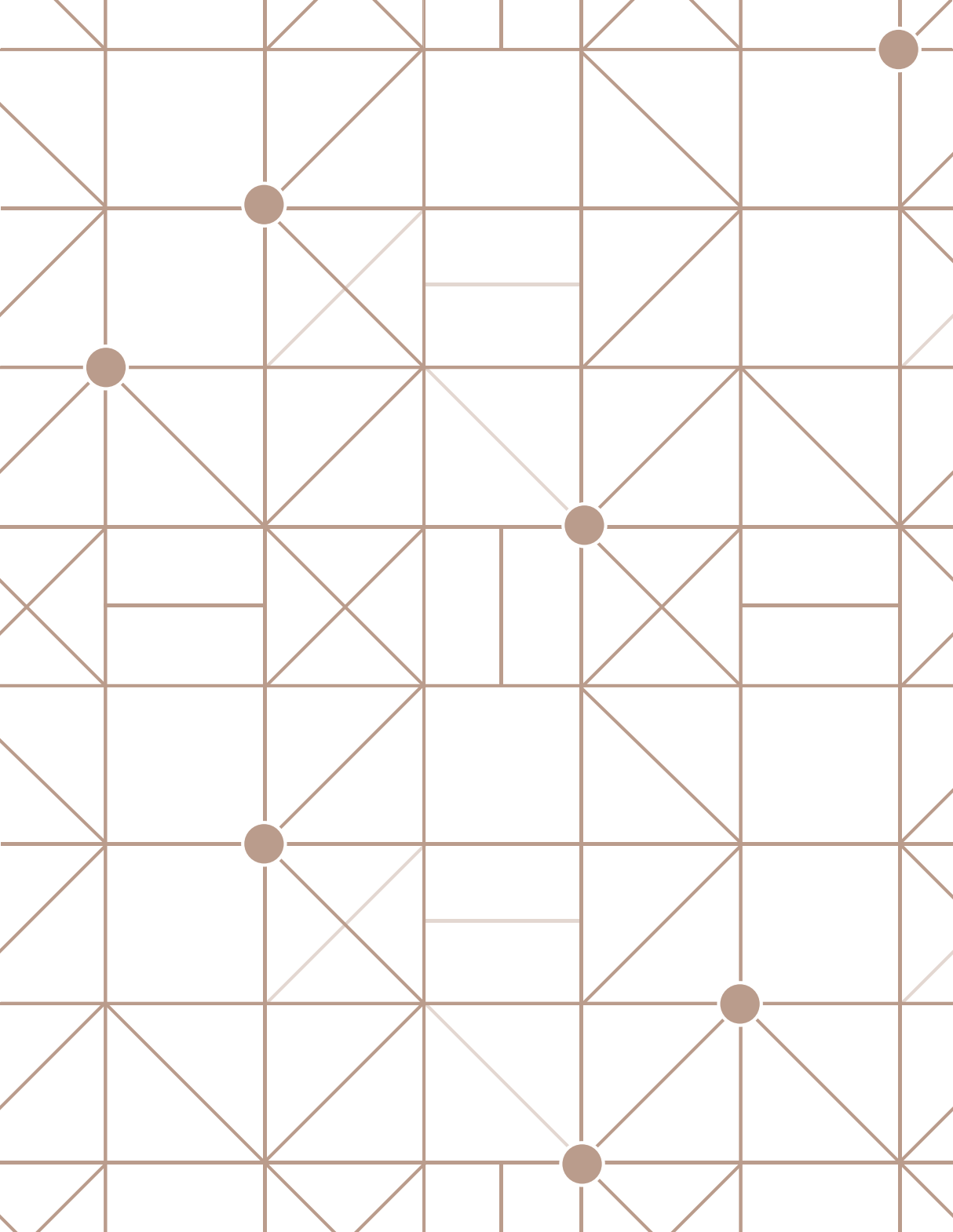

september 8

COURSE OUTLINE

- 10 Mobius quizzes (every Tues): 10%
  - ↳ 1hr time limit
  - ↳ best 9/10 will count
  - ↳ final attempt (out of 3) is counted
- 10 written assignments (every Wed): 40%
  - ↳ best 9/10 will count
  - ↳ Crowdmark assignments
- midterm: 20%
- final exam: 30%

week 1

SETS

- **set** is well-defined, unordered collection of distinct objects
  - ↳ each object is **element / member**
  - ↳ put btwn {}
  - ↳ e.g. $\mathbb{N} = \{1, 2, 3, \dots\}$
  - ↳ if $T = \{0, 1, \{0, 1\}, \{1, 2\}\}$, then T is set containing 2 #s & 2 sets
    - NOTE: $2 \notin T$ (2 is not part of set T)
- special sets:
  - ↳ $\mathbb{N}$: natural #s
  - ↳ $\mathbb{Z}$: integers
  - ↳ $\mathbb{Q}$: rational #s
    - form of $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ & $b \neq 0$
  - ↳ $\mathbb{R}$: real #s

QUANTIFIED STATEMENTS

- **statement** is sentence that has definite state of being T or F
  - ↳ if A is statement, then **negation** of A (denoted as $\neg A$) is statement w/opposite truth value of A
- **quantified statement** must have 4 parts:
  - ↳ quantifier (universal → "for all" or existential → "there exists")
  - ↳ variable
  - ↳ domain (any set)
  - ↳ open sentence involving variable (determine if statement is T or F when value from domain is assigned to variable)
- **universally quantified** statement: $\forall x \in S, P(x)$
  - ↳ for all x is S, P(x) is true
  - ↳ to prove, start w/ "Let $x \in S$"
- **existentially quantified** statement: $\exists x \in S, P(x)$
  - ↳ there exists at least one value of x in S for which P(x) is true
  - ↳ to prove, find only one particular $x \in S$ for which P(x) is true

- negation for quantified statements:
  - ↳ $\neg(\forall x \in S, P(x)) \equiv (\exists x \in S, \neg P(x))$
    - for all $x \in S$, P(x) is T $\xrightarrow{\text{negation}}$ there exists some $x \in S$ for which P(x) is F
  - ↳ $\neg(\exists x \in S, P(x)) \equiv (\forall x \in S, \neg P(x))$
    - there exists some $x \in S$ for which P(x) is T $\xrightarrow{\text{negation}}$ for all $x \in S$, P(x) is F
  - ↳ NOTE: $\equiv$ means **logically equivalent**

NESTED QUANTIFIERS

nested quantifiers contain more than one quantifier
- ↳ read from left to right

- order matters & can change truth value of statement
  - ↳ e.g. $\forall s \in \mathbb{R}, \exists t \in \mathbb{R}, t > s$ is true b/c it states there's no largest real # but $\exists t \in \mathbb{R}, \forall s \in \mathbb{R}, t > s$ is false b/c it states that there exists a largest real #
  - ↳ when nested quantifiers are of same type, order makes no difference in resulting truth value
- $\exists x \in \mathbb{R}, \exists y \in \mathbb{R}, (x \leq y)$ is T
- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} (x \leq y)$ is F

- $\exists x \in X, \forall y \in Y, \exists z \in Z, R(x,y,z)$ can be written as $\exists x \in X, P(x)$
  where $P(x)$ is $\forall y \in Y, Q(x,y)$
  where $Q(x,y)$ is $\exists z \in Z, R(x,y,z)$
- when negating nested quantifiers, switch each type of quantifier to the opposite one

week 2

TRUTH TABLES AND NEGATION

- truth values for $\neg A$ ("not A") is defined by truth table:

A	¬A
T	F
F	T

  - ↳ $\neg A$ also referred to as **negation** of A
  - ↳ A is known as statement variable
    - has a definite truth value
- $\neg(\neg A) \equiv A$ means that A & $\neg(\neg A)$ are logically equivalent

CONJUNCTION AND DISJUNCTION

- **compound statement** is composed of several individual statements called **component statements**
- truth value for $A \wedge B$ ("A and B") is defined by truth table:

A	B	A ∧ B
T	T	T
T	F	F
F	T	F
F	F	F

  - ↳ $A \wedge B$ also referred to as **conjunction** of A & B
- truth value for $A \vee B$ ("A or B") is defined by truth table:

A	B	A ∨ B
T	T	T
T	F	T
F	T	T
F	F	F

  - ↳ $A \vee B$ also referred to as **disjunction** of A & B
  - ↳ logical operator "or" is inclusive

LOGICAL OPERATORS AND ALGEBRA

- **De Morgan's Laws** state logical equivalences:
  - ↳ $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$
  - ↳ $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$
- for statement variables A, B, & C, rules hold for logical operators $\wedge$ & $\vee$:
  - ↳ **commutative**:
    - $A \wedge B \equiv B \wedge A$
    - $A \vee B \equiv B \vee A$
  - ↳ **associative**:
    - $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
    - $A \vee (B \vee C) \equiv (A \vee B) \vee C$
  - ↳ **distributive**:
    - $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
    - $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
- **transivity** of logical equivalence means "≡" for logical expressions is treated like "=" for algebraic expressions

IMPLICATION

- truth value for $A \Rightarrow B$ ("A implies B") is defined by truth table:

A	B	A⇒B
T	T	T
T	F	F
F	T	T
F	F	T

  - ↳ also referred to as implication
    - A is hypothesis
    - B is conclusion
  - ↳ in English:
    - if A is true, then B is true
    - if A then B
- $A \Rightarrow B \equiv (\neg A) \vee B$
- $\neg (A \Rightarrow B) \equiv A \wedge (\neg B)$
- 3rd & 4th row in table are irrelevant b/c when hypothesis doesn't hold, there's no need to determine whether the conclusion holds or not
  - ↳ assuming the hypothesis means only considering situations where hypothesis holds
- for statement variables A, B, & C: $((A \vee B) \Rightarrow C) \equiv ((A \Rightarrow C) \wedge (B \Rightarrow C))$

CONVERSE AND CONTRAPOSITIVE

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

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

- implication of $(\neg B) \Rightarrow (\neg A)$ is contrapositive of $A \Rightarrow B$

A	B	A⇒B	¬B	¬A	(¬B)⇒(¬A)
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

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

IF AND ONLY IF

- truth value for $A \Leftrightarrow B$ ("A if & only if B") is defined by truth table:

A	B	A⇔B
T	T	T
T	F	F
F	T	F
F	F	T

  - ↳ concisely written as "A iff B"
  - ↳ only T when A & B have same truth values
- $(A \Leftrightarrow B) \equiv ((A \Rightarrow B) \wedge (B \Rightarrow A))$
- logical equivalence for universally quantified statements:

$$(\forall x \in X, P(x) \Leftrightarrow Q(x)) \equiv ((\forall x \in X, P(x) \Rightarrow Q(x)) \wedge (\forall x \in X, Q(x) \Rightarrow P(x)))$$

week 3

PROVING UNIVERSALLY QUANTIFIED STATEMENTS

- to prove $\forall x \in S, P(x)$, choose rep mathematical object $x \in S$ & show that P must be true for rep x, using known facts about elements of S
  - ↳ state "let x be arbitrary element of S" or "let $x \in S$"
  - ↳ referred to as **direct proof**
  - ↳ **never assume** the truth of $P(x)$
- if unable to find single line of reasoning that works for all elements in a domain, use **case analysis**
  - ↳ different lines of reasoning used for different parts of domain
- to disprove $\forall x \in S, P(x)$, find an element $x \in S$ for which $P(x)$ is false
  - ↳ aka find **counter-example**
  - ↳ prove $\exists x \in S, \neg P(x)$

PROVING EXISTENTIALLY QUANTIFIED STATEMENTS

- to prove $\exists x \in S, P(x)$, provide explicit value of x from domain S that satisfies P & makes it true
- when equations are transformed, **extraneous solutions** may be created
  - ↳ can try subbing values into original equation to check
  - ↳ another method is to check all transformations are **invertible**, meaning that the solutions to original are exactly same as solutions to transformed
- to disprove existentially quantified statement $\exists x \in S, P(x)$, prove the universally quantified statement $\forall x \in S, \neg P(x)$

PROVING IMPLICATIONS

- to prove implication $A \Rightarrow B$, assume A is true & use this to show B is true
  - ↳ to prove universally quantified implication $\forall x \in S, P(x) \Rightarrow Q(x)$
    - let x be arbitrary element of S
    - assume hypothesis $P(x)$ is true
    - use assumption to show conclusion $Q(x)$ is true
- can also use **definitions** in proofs
  - ↳ e.g. integer is even if it can be written as $2k$ where k is integer; otherwise integer can be written as $2k+1$ where k is integer & that integer is odd
    - "if" means "if & only if" in definition
- statement is **vacuously true** when hypothesis is proven to be false

DIVISIBILITY OF INTEGERS

- an integer m divides an integer n, write $m \mid n$, if there exists integer k so that $n = km$
  - ↳ if $m \mid n$, m is divisor/factor of n & n is multiple of/divisible by m
  - ↳ if m doesn't divide n, write $m \nmid n$
  - ↳ for all integers a, $a \mid 0$ since $0 = 0 \cdot a$
    - $0 \mid 0$ is true
  - ↳ for all non-zero integers a, $0 \nmid a$ since there's no integer k so that $k \cdot 0 = a$
  - ↳ for all integers b, $1 \mid b$ & $-1 \mid b$
- **divisibility is transitive**: for all integers a, b, c, if $a \mid b$ & $b \mid c$, then $a \mid c$
- for all integers a, b, c, if $a \mid b$ or $a \mid c$, then $a \mid bc$

- divisibility of integer combinations (DIC): for all integers $a, b, \& c$, if $a|b$ & $a|c$, then for all integers $x \& y$, $a \mid (bx+cy)$

- when working w/ universal quantifiers in proofs of implications
  - ↳ if hypothesis is of form $\forall x \in S, P(x)$, can assume hypothesis & sub any value(s) of x into $P(x)$ & use the fact it's true to prove conclusion

PROOF BY CONTRAPOSITIVE

- to prove implication using contrapositive:
  - ↳ replace $A \Rightarrow B$ w/ $(\neg B) \Rightarrow (\neg A)$
    - assume $\neg B$ is true & deduce $\neg A$ must be also true
  - ↳ to prove $\forall x \in S, P(x) \Rightarrow Q(x)$, replace w/ $\forall x \in S, (\neg Q(x)) \Rightarrow (\neg P(x))$
- can use when hypothesis seems more complicated than conclusion
- can use when conclusion is a disjunction
  - ↳ i.e. $A \Rightarrow (B \vee C)$ becomes $(\neg B) \wedge (\neg C) \Rightarrow A$
- method of elimination to prove $A \Rightarrow (B \vee C)$
  - ↳ $A \Rightarrow (B \vee C) \equiv (A \wedge (\neg B)) \Rightarrow C$
    - in hypothesis, assume $\neg B$ is true so B is false & eliminate from conclusion
    - prove C is true

week 4

PROOF BY CONTRADICTION

- if A is statement, then either A or $\neg A$ must be false
  - ↳ compound statement $A \wedge (\neg A)$ is always false
  - ↳ contradiction is "$A \wedge (\neg A)$ is true"
- to use proof by contradiction to prove "$A \Rightarrow B$ is true", assume "$A \Rightarrow B$ is false"
  - ↳ if assumption of $\neg(A \Rightarrow B) \equiv A \wedge (\neg B)$ leads to contradiction, implication of "$A \Rightarrow B$" is proven true
  - ↳ e.g. prove that for all integers a, b, & c, if $a \mid (b+c)$ and $a \nmid b$, then $a \nmid c$

    SOLUTION

    Assume that there exists integers a, b, & c such that $a \mid (b+c)$, $a \nmid b$, and $a \mid c$

    Since $a \mid (b+c)$ & $a \mid c$, then by DIC $\cdot$ $a \mid (1(b+c) + (-1)(c)) = a \mid b$

    ↳ in initial assumptions, $a \nmid b$ & now we've concluded $a \mid b$ so it's a contradiction

    ↳ thus, original implication is proven to be true

- to prove "there's unique element $x \in S$ such that $P(x)$ is true"
  - ↳ prove there exists at least one element $x \in S$ such that $P(x)$ is true (i.e prove "$\exists x \in S, P(x)$")
  - ↳ then, prove uniqueness:
    - assume $P(x)$ & $P(y)$ are true for $x, y \in S$ & prove this assumption leads to $x = y$
    - assume $P(x)$ & $P(y)$ are true for distinct $x, y \in S$ (i.e $x \neq y$) & prove this assumption leads to a contradiction

PROVING IF AND ONLY IF STATEMENTS

- to prove iff statement:
  - ↳ equivalent to proving "$(A \Rightarrow B) \wedge (B \Rightarrow A)$"
  - ↳ to prove universally quantified iff statement "$\forall x \in S, P(x) \Leftrightarrow Q(x)$"
    - let $x \in S$ & prove both implication "$P(x) \Rightarrow Q(x)$" & converse "$Q(x) \Rightarrow P(x)$"
    - prove both "$\forall x \in S, P(x) \Rightarrow Q(x)$" & "$\forall x \in S, Q(x) \Rightarrow P(x)$"

NOTATION FOR SUMMATIONS, PRODUCTS, AND RECURRENCES

- for integers n & m w/ $n \geq m$, summation notation is $\sum_{i=m}^{n} x_i$
  - ↳ rep sum $x_m + x_{m+1} + \cdots + x_{n-1} + x_n$
  - ↳ i is index of summation
  - ↳ m is lower bound
  - ↳ n is upper bound
- properties of summations:
  - ↳ $\sum_{i=m}^{n} c x_i = c \sum_{i=m}^{n} x_i$ where c is constant
  - ↳ $\sum_{i=m}^{n} x_i \pm \sum_{i=m}^{n} y_i = \sum_{i=m}^{n} (x_i \pm y_i)$
  - ↳ changing bounds: $\sum_{i=m}^{n} x_i = \sum_{i=m+k}^{n+k} x_{i-k}$
- summation is linear

- for integers n & m w/ $n \geq m$, product notation is $\prod_{i=m}^{n} x_i$
  - ↳ rep product $x_m x_{m+1} \cdots x_{n-1} x_n$

- recurrence relation defines a sequence of values by giving it initial terms w/ an equation each subsequent term in terms of earlier ones

↳ e.g. Fibonacci sequence is $f_n = f_{n-1} + f_{n-2}$, for $n \geq 3$
- initial 2 terms are $f_1 = 1$ & $f_2 = 1$

PROOF BY INDUCTION

- an **axiom** of a mathematical system is statement that's assumed to be true
  ↳ no proof given
- **Principle of Mathematical Induction (POMI)** is axiom
  ↳ let $P(n)$ be statement that depends on $n \in \mathbb{N}$
  ↳ if statements 1 & 2 are true:
    1) $P(1)$
    2) for all $k \in \mathbb{N}$, if $P(k)$, then $P(k+1)$
  ↳ then statement 3 is true:
    3) for all $n \in \mathbb{N}$, $P(n)$
- to prove "for all $n \in \mathbb{N}$, $P(n)$" by induction on n
  ↳ **base case**: prove/verify "$P(1)$"
  ↳ **inductive step**:
    - let $k \in \mathbb{N}$
    - assume $P(k)$, which is inductive hypothesis
    - prove $P(k+1)$, which is inductive conclusion, using assumption $P(k)$
    - end proof by stating that result is true for $n = k+1$, & hence holds for all $n \geq 1$ by POMI
- e.g. prove $\forall n \in \mathbb{N}$, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

SOLUTION

Base case: $P(1)$ is $\sum_{i=1}^{1} i^2 = \frac{1(1+1)(2(1)+1)}{6}$

LS: $\sum_{i=1}^{1} i^2 = 1^2 = 1$ RS: $\frac{1(1+1)(2(1)+1)}{6} = 1$ Since LS=RS, $P(1)$ is true

Inductive step: let $k \in \mathbb{N}$
↳ assume $P(k)$ which is $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$
↳ wish to prove $P(k+1)$ which is $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \left(\sum_{i=1}^{k} i^2\right) + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad \leftarrow \text{by inductive hypothesis} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)(k(2k+1) + 6(k+1))}{6} \\
&= \frac{(k+1)(2k^2+k+6k+6)}{6} \\
&= \frac{(k+1)(2k^2+7k+6)}{6} \\
&= \frac{(k+1)(2k^2+4k+3k+6)}{6} \\
&= \frac{(k+1)(2k(k+2)+3(k+2))}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}
\end{aligned}$$

∴ The result is true for $n = k+1$, hence holds for all $n \geq 1$ by POMI.

- for statement "for all integers $n \geq b$, $P(n)$" where b is fixed integer but $b \neq 1$, use **induction w/base case b**
  ↳ prove $P(b)$ for base case
  ↳ for inductive step, assume $k \in \mathbb{Z}$ where $k \geq b$

BINOMIAL THEOREM

- for +ve integer m, define m factorial as $m! = \prod_{i=1}^{m} i$
  ↳ $0! = 1$

- for non-negative integer n & non-negative integer $m \leq n$, define **binomial coeff** as $\binom{n}{m} = \frac{n!}{(n-m)!\,m!}$
  - ↳ if $m > n$, define $\binom{n}{m} = 0$
  - ↳ e.g. $\binom{n}{2} = \frac{n!}{(n-2)!\,2!} = \frac{n(n-1)}{2}$
- **Pascal's Identity (PI)**: for all +ve integers n & m w/ $m < n$, $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$
  - ↳ recurrence that allows us to calculate value $\binom{n}{m}$ for all non-negative integers n & m
    - ° initial values are $\binom{n}{0} = 1$ for all non-negative integers n & $\binom{0}{m} = 0$ for all +ve integers m (since $\binom{n}{m} = 0$ for $m > n$)

NOTE: $\binom{n}{n-i} = \binom{n}{i}$

- **Binomial Theorem Version 1 (BT1)**: for all integers $n \geq 0$ & all $x \in \mathbb{R}$, $(1+x)^n = \sum_{m=0}^{n} \binom{n}{m} x^m$
  - ↳ e.g. coeff of x^3 in $(1+x)^6$ is $\binom{6}{3} = 20$
- **Binomial Theorem Version 2 (BT2)**: for all integers $n \geq 0$ & all $a, b \in \mathbb{R}$, $(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^{n-m} b^m$

PROOF BY STRONG INDUCTION

- Principle of Strong Induction (POSI) is axiom
  - ↳ if statements 1 & 2 are both true:
    1) $P(1)$
    2) for all $k \in \mathbb{N}$, if $P(1) \wedge P(2) \wedge \ldots \wedge P(k)$, then $P(k+1)$
  - ↳ then statement 3 is true:
    3) for all $n \in \mathbb{N}$, $P(n)$
- to prove "for all integers $n \geq b$, $P(n)$"
  - ↳ prove "$P(b) \wedge P(b+1) \wedge \ldots \wedge P(B)$" for some integer $B \geq b$
    - ° b is smallest base case & B is largest
  - ↳ prove implication "for all integers $k \geq B$, if $P(b) \wedge P(b+1) \wedge \ldots \wedge P(k)$, then $P(k+1)$"

week 5

INTRODUCTION

- empty set $\{\}$ contains no elements
  - ↳ commonly denoted by $\emptyset$
  - ↳ $\{\emptyset\} \neq \emptyset$ b/c $\{\emptyset\}$ is not an empty set
- # of elements in set S is cardinality of S
  - ↳ denoted by $|S|$
  - ↳ e.g. $|\emptyset| = 0$ ≠ $|\{\emptyset\}| = 1$

SET-BUILDER NOTATION

- 2 parts of set-builder notation:
  - ↳ universe of discourse, denoted by $\mathcal{U}$, is very large set that contains all objects we might encounter in given situation
    - e.g. in divisibility, assume set of integers $\mathbb{Z}$ is universe
  - ↳ open sentence $P(x)$, whose value is defined for every $x \in \mathcal{U}$
- type 1 set-builder notation: $\{x \in \mathcal{U} : P(x)\}$
  - ↳ describes set consisting of all x such that $x \in \mathcal{U}$ & $P(x)$ is true
  - ↳ i.e. "set of all x in $\mathcal{U}$ w/ property P"
  - ↳ explicit mention of universe might be omitted: $\{x : P(x)\}$
  - ↳ e.g. set of all even integers can be written as $\{n \in \mathbb{Z} : 2 \mid n\}$

type 2 set-builder notation: $\{f(x) : x \in \mathcal{U}\}$
- ↳ describes set consisting all objects of form $f(x)$ such that $x \in \mathcal{U}$
- ↳ e.g. set of all even integers can be written as $\{2k : n \in \mathbb{Z}\}$
  - $f(k) = 2k$

type 3 set-builder notation: $\{f(x) : x \in \mathcal{U}, P(x)\}$ or $\{f(x) : P(x), x \in \mathcal{U}\}$
- ↳ describes set consisting all objects of form $f(x)$ such that $x \in \mathcal{U}$ & $P(x)$ is true
- ↳ e.g. set of all integers that are +ve powers of 5 can be written as $\{5^k : k \in \mathbb{Z}, k > 0\}$

- in notation, expressions are separated by single colon
  - ↳ expression on left gives typical element of set, in terms of single variable
  - ↳ expression on right gives list of conditions that variable must satisfy
    - each comma is "AND"
  - ↳ set of rational #s can be written as $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}$

SET OPERATIONS

- union of 2 sets S & T is set of all elements belonging to either set S, set T, or both
  - ↳ $S \cup T = \{x : x \in S \text{ OR } x \in T\} = \{x : (x \in S) \vee (x \in T)\}$
- intersection of 2 sets S & T is set of all elements belonging to both S & T
  - ↳ $S \cap T = \{x : x \in S \text{ AND } x \in T\} = \{x : (x \in S) \wedge (x \in T)\}$
- set-difference of 2 sets S & T is set of all elements belonging to S but not T
  - ↳ $S - T = \{x : (x \in S) \wedge (x \notin T)\} = \{x : (x \in S) \wedge (\neg (x \in T))\}$
  - ↳ also denoted by $S \setminus T$
- complement of set S is set of all elements not in S
  - ↳ $\overline{S} = \{x : x \notin S\}$
  - ↳ w/explicit mention of universe $\mathcal{U}$, $\overline{S} = \{x \in \mathcal{U} : x \notin S\}$
    - in terms of set-difference notation, $\overline{S} = \mathcal{U} - S$

SUBSETS OF A SET

- 2 sets S & T are **disjoint** when $S \cap T = \emptyset$
  - ↳ $S \cap \emptyset = \emptyset \cap S = \emptyset$
  - ↳ $S \cap \overline{S} = \emptyset$
- set S is **subset** of set T when every element of S belongs to T
  - ↳ written as $S \subseteq T$
  - ↳ S is **proper subset** of set T, written as $S \subsetneq T$, when S is subset of T & there exists element in T which doesn't belong to S
  - ↳ when S is not subset of T, write $S \not\subseteq T$
  - ↳ when $S \subseteq T$, T is superset of S
- for all integers $n \geq 1$, $S_n = \{1, 2, 3, \ldots, n\}$ has 2^n subsets

SUBSETS, SET EQUALITY, AND IMPLICATIONS

- to prove $S \subseteq T$, prove implication: $\forall x \in \mathcal{U}, (x \in S) \Rightarrow (x \in T)$
  - ↳ to prove $S \not\subseteq T$, disprove implication
  - ↳ e.g. in an arbitrary universe $\mathcal{U}$, prove for all sets A & B, $\overline{A \cup B} \subseteq \overline{A}$

    SOLUTION

    We prove "$\forall x \in \mathcal{U}, (x \in \overline{A \cup B} \Rightarrow x \in \overline{A})$". Let $x \in \mathcal{U}$, let $A, B \subseteq \mathcal{U}$, & assume $x \in \overline{A \cup B}$

    $\overline{A \cup B} = \{x \in \mathcal{U} : \neg(x \in A \cup B)\}$
    $= \{x \in \mathcal{U} : \neg(x \in A \vee x \in B)\}$
    $= \{x \in \mathcal{U} : x \notin A \wedge x \notin B\}$
    $= \overline{A} \cap \overline{B}$

    Since $x \in \overline{A \cup B}$ which is $x \in \overline{A} \cap \overline{B}$. This means $x \in \overline{A}$ & $x \in \overline{B}$ so it's proven that $x \in \overline{A}$.
- 2 sets S & T are **equal**, written as $S = T$, when $S \subseteq T$ & $T \subseteq S$
  - ↳ i.e. 2 sets have exactly the same elements
  - ↳ to prove via universally quantified statements: $\forall x \in \mathcal{U}, (x \in S) \Leftrightarrow (x \in T)$
    $\equiv (\forall x \in \mathcal{U}, (x \in S) \Rightarrow (x \in T)) \wedge (\forall x \in \mathcal{U}, (x \in T) \Rightarrow (x \in S))$

midterm notes

Prove for $\forall n \in \mathbb{N}$, that $\sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} = 2^{n-1}$

NOTE. $\sum_{j=0}^{n} t_j$
- ↳ n is even: $\sum_{j=0}^{\lfloor n/2 \rfloor} t_{2j}$ for some $j \in \mathbb{Z}$
- ↳ n is odd: $\sum_{j=0}^{\lfloor n/2 \rfloor} t_{2j+1}$ for some $j \in \mathbb{Z}$

$$(1+x)^n + (1-x)^n$$
$$= \sum_{m=0}^{n} \binom{n}{m} x^m + \sum_{m=0}^{n} \binom{n}{m} (-x)^m$$
$$= \sum_{m=0}^{n} \binom{n}{m} x^m + \sum_{m=0}^{n} \binom{n}{m} (-1)^m (x)^m$$
$$= \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} x^{2j} + \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j+1} x^{2j+1} + \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} (-1)^{2j} x^{2j} + \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j+1} (-1)^{2j+1} x^{2j+1}$$
$$= 2 \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} x^{2j}$$

This means $(1+x)^n - (1-x)^n = 2 \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} x^{2j}$ for any $x \in \mathbb{R}$. Choose $x = 1$.

$$(1+1)^n - (1-1)^n = 2 \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j} 1^{2j}$$
$$2^n = 2 \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j}$$
$$2^{n-1} = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{2j}$$

Thus, we've proven the statement.

Prove there's no $a, b, c \in \mathbb{Z}^+$ such that $a^3 + 8b + 6c^2 = 20$.

We know for $x, y, z \in \mathbb{Z}^+$: $x < x+y+z$, $y < x+y+z$, and $z < x+y+z$

We'll prove by contradiction. Assume there exists $a, b, c \in \mathbb{Z}^+$ such that $a + 8b + 6c^2 = 20$.

$$6c^2 < 20$$
$$c^2 < \frac{20}{6}$$

Since $1^2 < \frac{20}{6} < 2^2$, then $1^2 \leq c^2 < \frac{20}{6} < 2^2$

$$1^2 \leq c^2 < 2^2$$
$$1 \leq c < 2 \quad \longleftarrow \text{this only holds true b/c } c \in \mathbb{Z}^+$$

c must be an integer so we see that $c = 1$.

$$a^3 + 8b + 6c^2 = 20$$
$$a^3 + 8b + 6 = 20$$
$$a^3 + 8b = 14$$
$$8b < 14$$
$$b < \frac{7}{4}$$

$1 \leq b < 2 \longrightarrow$ b must be an integer so $b = 1$

$$a^3 + 8b = 14$$
$$a^3 + 8 = 14$$
$$a^3 = 6$$
$$a = \sqrt[3]{6}$$

Since a is not a +ve integer, there's a contradiction. Thus, we've proven the original statement.

Prove / disprove $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, 3 \mid (xy + x^2 - y^2)$.

We will disprove using contradiction. Assume the statement is true.

$$x = \begin{cases} 3a \\ 3a+1 \\ 3a+2 \end{cases} \text{ for some } a \in \mathbb{Z} \qquad y = \begin{cases} 3b \\ 3b+1 \\ 3b+2 \end{cases} \text{ for some } b \in \mathbb{Z}$$

Consider the case $x = 3a+1$ for some $a \in \mathbb{Z}$.

$$xy + x^2 - y^2$$
$$= (3a+1)y + (3a+1)^2 - y^2$$
$$= 3ay + y + 9a^2 + 6a + 1 - y^2$$
$$= 3ay + 9a^2 + 6a + 1 + y - y^2$$
$$= 3(ay + 3a^2 + 2a) + 1 + y - y^2$$

We now assume $3 \mid (1+y-y^2)$

CASE 1: $y = 3b$

$$\frac{(1+3b-(3b)^2)}{3}$$

$$= \frac{1+3b-9b^2}{3}$$

$$= \frac{1}{3} + b - 3b^2 \quad \longleftarrow \text{ there's no } b \in \mathbb{Z} \text{ that will make the result an integer}$$

CASE 2: $y = 3b+1$

$$\frac{(1+3b+1-(3b+1)^2)}{3}$$

$$= \frac{2+3b-9b^2-6b-1}{3}$$

$$= \frac{1-3b-9b^2}{3}$$

$$= \frac{1}{3} - b - 3b^2 \quad \longleftarrow \text{ there's no } b \in \mathbb{Z} \text{ that will make the result an integer}$$

CASE 3: $y = 3b+2$

$$\frac{(1+3b+2-(3b+2)^2)}{3}$$

$$= \frac{3+3b-9b^2-12b-4}{3}$$

$$= \frac{-1-9b-9b^2}{3}$$

$$= -\frac{1}{3} - 3b - 3b^2 \quad \longleftarrow \text{ there's no } b \in \mathbb{Z} \text{ that will make the result an integer}$$

Since there doesn't exist a $y \in \mathbb{Z}$ that makes $(1+y-y^2)$ by 3, then $3 \nmid (xy+x^2-y^2)$ when $x = 3a+1$ for some $a \in \mathbb{Z}$. We've found a contradiction and thus, we've proven the statement false.

week 6

DIVISIBILITY AND BOUNDS

- proposition: $\forall x \in \mathbb{R}$, $x \leq |x|$
  - ↳ i.e. $\forall x \in \mathbb{R}, (x < |x|)$ or $(x = |x|)$
  - ↳ proof: let $x \in \mathbb{R}$
    - case 1: x is -ve so $x < 0 < |x|$; $x < |x|$ so $x \leq |x|$
    - case 2: x is not -ve so $x = |x|$ so $x \leq |x|$
- Bounds By Divisibility (BBD): for all integers a & b, if $b \mid a$ and $a \neq 0$ then $b \leq |a|$
- when dividing integer a by +ve integer b, there exist integers q (quotient) & r (remainder)
- Division Algorithm (DA): for all integers a & +ve integers b, there exist unique integers q & r such that $a = qb + r$, $0 \leq r < b$

GREATEST COMMON DIVISOR

- let a & b be integers; integer c is defined as common divisor of a & b if $c \mid a$ and $c \mid b$
- let a & b be integers:
  - ↳ if $a, b \neq 0$, an integer $d > 0$ is greatest common divisor of a & b, written $d = \gcd(a,b)$ when:
    - d is common divisor of a & b
    - $\forall c \in \mathbb{Z}$, if c is common divisor of a & b, then $c \leq d$
  - ↳ if $a = b = 0$, $\gcd(a,b) = \gcd(0,0) = 0$

properties of gcd when a is arbitrary integer:

- ↳ $\gcd(a,a) = \gcd(a,-a) = |a|$
  - when $a = 0$, this gives $\gcd(0,0) = 0$
- ↳ $\gcd(a,1) = \gcd(a,-1) = 1$
- ↳ $\gcd(a,0) = |a|$
  - when $a = 0$, also gives $\gcd(0,0) = 0$

- GCD With Remainders (GCD WR): for all integers $a, b, q,$ & r, if $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$
  - ↳ does not have condition $0 \leq r < b$
  - ↳ i.e. express $\gcd(8n+3, 5n-2)$ as function of integer n

SOLUTION

Let $n \in \mathbb{Z}$. Using GCD WR:

$8n+3 = 1(5n-2) + (3n+5)$

$5n-2 = 1(3n+5) + (2n-7)$

$3n+5 = 1(2n-7) + (n+12)$

$2n-7 = 2(n+12) + (-31)$

It follows that $\gcd(8n+3, 5n-2) = \gcd(n+12, -31) = \gcd(n+12, 31)$. Since 1 & 31 are only +ve divisors of 31, then $\gcd(n+12, 31) = 31$ or $\gcd(n+12, 31) = 1$.

- CASE 1: Suppose $\gcd(n+12, 31) = 31$, then $31 \mid (n+12)$. Conversely, if $31 \mid (n+12)$, then 31 is common divisor of $n+12$ & 31. Thus, $31 \leq \gcd(n+12, 31)$. On another hand, $\gcd(n+12, 31) \leq \min(|n+12|, 31) \leq 31$ so $\gcd(n+12, 31) = 31$. We can conclude $\gcd(n+12, 31) = 31 \iff 31 \mid (n+12)$.
- CASE 2: Suppose $\gcd(n+12, 31) = 1$. By contrapositive to statement in case 1, $\gcd(n+12, 31) \neq 31 \iff 31 \nmid (n+12)$. Since $\gcd(n+12, 31) = \{1, 31\}$, then we conclude $\gcd(n+12, 31) = 1 \iff 31 \nmid (n+12)$

Thus, $\gcd(n+12, 31) = \begin{cases} 31, & \text{if } 31 \mid (n+12) \\ 1, & \text{if } 31 \nmid (n+12) \end{cases}$

- **Euclidean Algorithm** uses GCD WR & DA iteratively until we get $\gcd(c,0)$ for some $c \in \mathbb{Z}^+$
  - ↳ use fact that $\gcd(c,0)=c$ to conclude $\gcd(a,b)=c$
  - ↳ i.e. determine $\gcd(1386,322)$

    SOLUTION

    1) $1386 = 4 \times 322 + 98 \longrightarrow \gcd(1386,322) = \gcd(322,98)$

    2) $322 = 3 \times 98 + 28 \longrightarrow \gcd(322,98) = \gcd(98,28)$

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

    4) $28 = 2 \times 14 + 0 \longrightarrow \gcd(28,14) = \gcd(14,0)$

    Since $\gcd(14,0)=14$, then $\gcd(1386,322)=14$.
  - ↳ i.e. prove $\forall a \in \mathbb{Z}$, $\gcd(a^2, a+1) = 1$

    SOLUTION

    Let $a \in \mathbb{Z}$. Using GCD WR:

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

    Since $\gcd(a+1,1)=1$ for all $a \in \mathbb{Z}$, we can conclude $\gcd(a^2, a+1) = 1$.

CERTIFICATE OF CORRECTNESS AND BÉZOUT'S LEMMA

- **GCD Characterization Theorem (GCD CT)**: for all $a,b \in \mathbb{Z}$ & not -ve integer d, if d is common divisor of a & b, and there exist $s,t \in \mathbb{Z}$ such that $as+bt=d$, then $d=\gcd(a,b)$
  - ↳ i.e. for all $a,b,d \in \mathbb{Z}$, if:
    - $d \geq 0$
    - $d \mid a$
    - $d \mid b$
    - $\exists s,t \in \mathbb{Z}$, $as+bt=d$

    then $d=\gcd(a,b)$
  - ↳ s & t are providing a **certificate of correctness** for d as $\gcd(a,b)$

e.g. find s & t for $a=1386$ & $b=322$ whose gcd was $d=14$

SOLUTION

1) $1386 - 4(322) = 98$

2) $322 - 3(98) = 28$

3) $98 - 3(28) = 14$

Sub 2) into 3):

$98 - 3(322 - 3(98)) = 14$

$-3(322) + 10(98) = 14$

Sub 1) in:

$-3(322) + 10(1386 - 4(322)) = 14$

$-3(322) + 10(1386) - 40(322) = 14$

$10(1386) - 43(322) = 14$

Thus $s=10$ & $t=-43$ provide certificate of correctness for $\gcd(1386,322)=14$.

- **Bézout's Lemma (BL)**: for all $a,b \in \mathbb{Z}$, there exist $s,t \in \mathbb{Z}$ such that $as+bt=d$, where $d=\gcd(a,b)$
  - ↳ converse of GCD CT
- we've only described how to apply Euclidean Algorithm when $a \geq b > 0$ but domain of BL isn't restricted to $a \geq b > 0$
  - ↳ if $a < b$, $\gcd(a,b) = \gcd(b,a)$
  - ↳ if $a < 0$, $b < 0$, or both are -ve, $\gcd(a,b) = \gcd(|a|, |b|)$
  - ↳ if $a=0$ or $b=0$, $\gcd(a,0) = a$ for all $a \in \mathbb{Z}$

EXTENDED EUCLIDEAN ALGORITHM

given integers $a \geq b > 0$, Extended Euclidean Algorithm (EEA) computes both $d=\gcd(a,b)$ & pair

of integers s & t that provide certificate of correctness for d w/o substitution of equations

- floor of $x \in \mathbb{R}$, written $\lfloor x \rfloor$, is largest integer $\leq x$
  - e.g. $\lfloor \frac{7}{2} \rfloor = \lfloor \frac{18}{5} \rfloor = \lfloor \frac{18}{6} \rfloor = \lfloor \frac{1007}{329} \rfloor = 3$
- formal statement of EEA:
  1) input integers a & b w/ $a \geq b > 0$
  2) construct table w/ 4 columns:
     - labelled x, y, r, & q
     - 1st row is (1, 0, a, 0)
     - 2nd row is (0, 1, b, 0)
  3) repeat for $i \geq 3$:
     - $q_i \leftarrow \lfloor \frac{r_{i-2}}{r_{i-1}} \rfloor$
     - $\text{Row}_i \leftarrow \text{Row}_{i-2} - q_i \text{Row}_{i-2}$
  4) stop when $r_i = 0$
  5) set $n = i-1$ (i.e. look at 2nd last row)
     - $\gcd(a,b) = r_n$
     - $s = x_n$ & $t = y_n$ are certificate of correctness

↳ for each row of table, $ax_i + by_i = r_i$

- e.g. let $d = \gcd(2172, 423)$, compute d & give certificate of correctness for d

SOLUTION

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

We can see $d = \gcd(2172, 423) = 3$. The certificate of correctness is $s = 52$ & $t = -267$.

$2172 \times 52 + 423 \times (-267) = 3$

For $d_1 = \gcd(423, -2172) = \gcd(2172, 423) = 3$. The certificate of correctness is $s = -267$ & $t = -52$.

$423 \times (-267) + (-2172) \times (-52) = 3$

FURTHER PROPERTIES OF GCD

- common divisor divides GCD (CDD GCD): for all integers a, b, & c, if $c \mid a$ and $c \mid b$, then $c \mid \gcd(a,b)$

PROOF

Let $a, b, c \in \mathbb{Z}$ & assume $c \mid a$ and $c \mid b$. By BL, there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$, where $d = \gcd(a,b)$. Since $c \mid a$ & $c \mid b$, by DIC we get $c \mid (as + bt)$ so $c \mid d$.

- 2 integers a & b are coprime if $\gcd(a,b) = 1$
  - ↳ coprime characterization theorem (CCT): for all $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ iff there exist $s, t \in \mathbb{Z}$ such that $as + bt = 1$

division by the GCD (DB GCD): for all integers a & b (not both zero), $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ where $d = \gcd(a,b)$

coprimeness and divisibility (CAD): for all $a, b, c \in \mathbb{Z}$, if $c \mid ab$ and $\gcd(a,c) = 1$, then $c \mid b$

week 7

PRIME NUMBERS

- natural # $p > 1$ is called **prime** if its only +ve divisors are 1 & p itself
  - ↳ otherwise, p is **composite**
  - ↳ 1 is neither prime nor composite
- **Prime Factorization (PF)**: every natural # $n > 1$ can be written as product of primes
- **Euclid's Theorem (ET)**: # of primes is infinite

UNIQUE FACTORIZATION THEOREM

- **Euclid's Lemma (EL)**: for all $a, b \in \mathbb{Z}$ & prime #s p, if $p \mid ab$, then $p \mid a$ or $p \mid b$
  - ↳ let p be prime #, n be natural #, & $a_1, a_2, \ldots, a_n \in \mathbb{Z}$; if $p \mid (a_1 a_2 \ldots a_n)$, then $p \mid a_i$ for some $i = 1, 2, \ldots, n$
    - known as generalized EL
- **Unique Factorization Theorem (UFT)**: every natural # $n > 1$ can be written as product of prime factors uniquely, apart from order of factors
- **Finding a Prime Factor (FPF)**: every natural # $n > 1$ is either prime or has prime factor $\leq \sqrt{n}$
  - ↳ e.g. is 73 a prime #?

    SOLUTION

    Either 73 is prime or has prime factor $\leq \sqrt{73}$.

    $\sqrt{73} < \sqrt{81} = 9$ so check prime factors ≤ 8. Since 2, 3, 5, & 7 all don't divide 73, 73 is prime.

PRIME FACTORIZATIONS AND THE GCD

- **Divisors From Prime Factorization (DFPF)**: let $n \geq 2$ & $c \geq 1$ be +ve integers, & let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be unique rep of n as product of distinct primes $p_1, p_2, \ldots, p_k$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are +ve integers; c is +ve divisor of n iff c can be rep as $c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ where $0 \leq \beta_i \leq \alpha_i$ for $i = 1, 2, \ldots, k$
  - ↳ # of +ve divisors of integer n w/prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$
- **GCD From Prime Factorization (GCD PF)**: let $a, b \in \mathbb{Z}^+$ & let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ & $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ be ways to express a & b as products of distinct primes $p_1, p_2, \ldots, p_k$, where some/all of exponents may be 0; $\gcd(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $r_i = \min\{\alpha_i, \beta_i\}$ for $i = 1, 2, \ldots, k$

LINEAR DIOPHANTINE EQUATIONS IN 2 VARIABLES

- **Diophantine equation** is where both coeffs & variables are integers
  - ↳ **linear** if each term is a constant or a constant times a single variable

Linear Diophantine Equation Theorem, Part 1 (LDET 1): for all $a, b, c \in \mathbb{Z}$ w/ $a \neq 0$ & $b \neq 0$, the linear Diophantine equation $ax + by = c$ has integer solution iff $d \mid c$, where $d = \gcd(a, b)$

- to find integer solution to $ax + by = c$ when $d \mid c$, where $d = \gcd(a, b)$:
  1) find certificate of correctness s & t for d, which gives $as + bt = d$
  2) multiply equation by $k = \frac{c}{d}$ to get $a(ks) + b(kt) = kd = c$
     - solutions are $x = ks$ & $y = kt$
  - ↳ e.g. give integer solution to $61x + 140y = 189$

    SOLUTION

    Find $\gcd(61, 140) = \gcd(140, 61)$

x	y	r	q
1	0	140	0
0	1	61	0
1	-2	18	2
-3	7	7	3
7	-16	4	2
-10	23	3	1
17	-39	1	1
-61	140	0	3

$d = \gcd(140, 61) = 1$

$1 \mid 189$ so integer solution exists

$140(17) + 61(-39) = 1$

$\downarrow$

$d = \gcd(61, 140) = 1$

$61(-39) + 140(17) = 1$

$61(-7371) + 140(3213) = 189$ ← multiply by $\frac{c}{d} = \frac{189}{1} = 189$

An integer solution is $x = -7371$ & $y = 3213$

FINDING ALL SOLUTIONS IN 2 VARIABLES

- Linear Diophantine Equation Theorem, Part 2 (LDET 2): let $a, b, c \in \mathbb{Z}$ w/ $a \neq 0$ & $b \neq 0$ & define $d = \gcd(a, b)$; if $x = x_0$ & $y = y_0$ is a particular solution to linear Diophantine equation $ax + by = c$, then set of all solutions is given by $\{(x, y) : x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n, n \in \mathbb{Z}\}$
- by LDET 1, if $d \nmid c$, then $ax + by = c$ has no solutions
- by LDET 1 & 2, if $d \mid c$, then $ax + by = c$ has infinitely many solutions
  - ↳ if $c = d$, then there's infinitely many certificates of correctness for $d = \gcd(a, b)$
- e.g. find all solutions to $175x + 41y = 12$

SOLUTION

Find $\gcd(175, 41)$

x	y	r	q
1	0	175	0
0	1	41	0
1	-4	11	4
-3	13	8	3
4	-17	3	1
-11	47	2	2
15	-64	1	1
-41	175	0	2

$d = \gcd(175, 41) = 1$

$1 \mid 12$ & let $k = \frac{c}{d} = \frac{12}{1} = 12$

$175(15) + 41(-64) = 1$

$175(180) + 41(-768) = 12$ ← multiply by k

$b = \frac{41}{1} = 41$

$d = \frac{175}{1} = 175$

All solutions are $\{(x, y) : x = 180 + 41n, y = -768 - 175n, n \in \mathbb{Z}\}$

week 8

CONGRUENCE

- let m be fixed +ve integer; for $a, b \in \mathbb{Z}$, $a \equiv b \pmod m$ means a is congruent to b modulo m
  - ↳ write this when $m \mid (a-b)$
  - ↳ for $a, b \in \mathbb{Z}$ st $m \nmid (a-b)$, then write $a \not\equiv b \pmod m$
  - ↳ $\equiv$ is congruence & m is its modulus
  - ↳ e.g. $41 \equiv 41 \pmod 3$ but $-41 \not\equiv 41 \pmod 3$

ELEMENTARY PROPERTIES OF CONGRUENCE

- Congruence is an Equivalence Relation (CER): for all $a, b, c \in \mathbb{Z}$ & m is fixed +ve integer:
  - ↳ reflexivity: $a \equiv a \pmod m$
  - ↳ symmetry: if $a \equiv b \pmod m$, then $b \equiv a \pmod m$
  - ↳ transivity: if $a \equiv b \pmod m$ & $b \equiv c \pmod m$, then $a \equiv c \pmod m$
- for all $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, if $a_1 \equiv b_1 \pmod m$ & $a_2 \equiv b_2 \pmod m$, then
  - ↳ $a_1 + a_2 \equiv b_1 + b_2 \pmod m$
  - ↳ $a_1 - a_2 \equiv b_1 - b_2 \pmod m$
  - ↳ $a_1 a_2 \equiv b_1 b_2 \pmod m$
- e.g. $-32 \equiv 3 \bmod 7$ & $-44 \equiv 5 \bmod 7$; what value of X, $0 \leq X \leq 6$, satisfies $X \equiv ((-32) + (-44)) \bmod 7$?

  SOLUTION

  $3 + 5 \equiv ((-32) + (-44)) \bmod 7$

  $7 \mid (X - (3+5))$

  $\Rightarrow 7 \mid (X - 8)$

  $X = 1$

NOTE: apply CAM to subtraction by adding -ve

- Congruence Add and Multiply (CAM): for all +ve integers n, for all integers $a_1, \ldots, a_n$ & $b_1, \ldots, b_n$, if $a_i \equiv b_i \pmod m$ for all $1 \leq i \leq n$, then:
  - ↳ $a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \pmod m$
  - ↳ $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod m$
- Congruence Power (CP): for all +ve integers n & $a, b \in \mathbb{Z}$, if $a \equiv b \pmod m$, then $a^n \equiv b^n \pmod m$
- Congruence Divide (CD): for all $a, b, c \in \mathbb{Z}$, if $ac \equiv bc \pmod m$ & $\gcd(c, m) = 1$, then $a \equiv b \pmod m$

CONGRUENCE AND REMAINDERS

- Congruent Iff Same Remainder (CISR): for all $a, b \in \mathbb{Z}$, $a \equiv b \pmod m$ iff a & b have same remainder when divided by m
- Congruent to Remainder (CTR): for all $a, b \in \mathbb{Z}$ w/ $0 \leq b < m$, $a \equiv b \pmod m$ iff a has remainder b when divided by m
- e.g. determine remainder when 3^{47} is divided by 7

  SOLUTION

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

  $3^2 \equiv 9 \equiv 2 \pmod 7$

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

  $\equiv 3^2 (3^{45}) \pmod 7$

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

$\equiv 2(-1)^{15} \pmod 7$

$\equiv -2 \pmod 7$

$\equiv 5 \pmod 7$

Since $0 \leq 5 < 7$, use CTR to conclude that 3^{47} divided by 7 has remainder 5.

· square-and-multiply algorithm used to compute remainder of integer a^n when divided by m:

1) write n as sum of powers of 2
   - $n = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_k}$
2) compute $a \pmod m$, $a^2 \pmod m$, $a^4 \pmod m$, $a^8 \pmod m$, ...
3) use data from 1 & 2 to compute $a^n \pmod m$

↳ e.g. compute last 2 decimal digits of 211^{90}

SOLUTION

Find integer r such that $0 \leq r < 100$ & $r \equiv 211^{90} \pmod{100}$.

$211 \equiv 11 \pmod{100}$ so $211^{90} \equiv 11^{90} \pmod{100}$

1) $90 = 2^6 + 26$
   $= 2^6 + 2^4 + 10$
   $= 2^6 + 2^4 + 2^3 + 2$
   $= 64 + 16 + 8 + 2$

2) $11 \equiv 11 \pmod{100}$
   $11^2 \equiv 121 \equiv 21 \pmod{100}$
   $11^4 \equiv (11^2)^2 \equiv 21^2 \equiv 441 \equiv 41 \pmod{100}$
   $11^8 \equiv (11^4)^2 \equiv 41^2 \equiv 1681 \equiv 81 \pmod{100}$
   $11^{16} \equiv (11^8)^2 \equiv 81^2 \equiv 6561 \equiv 61 \pmod{100}$
   $11^{32} \equiv (11^{16})^2 \equiv 61^2 \equiv 3721 \equiv 21 \pmod{100}$
   $11^{64} \equiv (11^{32})^2 \equiv 21^2 \equiv 441 \equiv 41 \pmod{100}$

3) $11^{90} \equiv 11^{64} \cdot 11^{16} \cdot 11^8 \cdot 11^2 \pmod{100}$
   $\equiv 41 \cdot 61 \cdot 81 \cdot 21 \pmod{100}$
   $\equiv 41 \cdot 61 \cdot 1701 \pmod{100}$
   $\equiv 41 \cdot 61 \cdot 1 \pmod{100}$
   $\equiv 2501 \pmod{100}$
   $\equiv 1 \pmod{100}$

Last 2 digits of 211^{90} are 01.

· for all not -ve $a \in \mathbb{Z}$, a is divisible by 3 iff sum of digits in decimal rep of a is divisible by 3

· for all not -ve $a \in \mathbb{Z}$, a is divisible by 11 iff $S_e - S_o$ is divisible by 11:

↳ S_e is sum of digits of even powers of 10 in decimal rep of a

↳ S_o is sum of digits of odd powers of 10 in decimal rep of a

LINEAR CONGRUENCES

· a relation of form $ax \equiv c \pmod m$ is called linear congruence in variable x

↳ solution is integer x_0 such that $ax_0 \equiv c \pmod m$

· Linear Congruence Theorem (LCT): for all $a, c \in \mathbb{Z}$ w/ $a \neq 0$, linear congruence $ax \equiv c \pmod m$ has solution iff $d \mid c$, where $d = \gcd(a, m)$

↳ if $x = x_0$ is particular solution, then set of all solutions is $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$ or $\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \pmod m\}$

↳ to find solutions to $ax \equiv c \pmod m$, use linear Diophantine equation $ax + my = c$ & apply EEA

NON-LINEAR CONGRUENCES

- e.g. solve $x^2 + x \equiv 2 \pmod 8$

SOLUTION

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1
$x^2 + x \pmod 8$	0	2	6	4	4	6	2	0

The solution is given by all $x \in \mathbb{Z}$ such that $x \equiv 1 \pmod 8$ or $x \equiv 6 \pmod 8$.

week 9

CONGRUENCE CLASSES AND MODULAR ARITHMETIC

- congruence class modulo m of integer a is set of integers $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod m\}$
  - ↳ by proposition Congruent Iff Same Remainder, there's exactly m different congruence classes modulo m b/c there are m choices 0, 1, ..., m-1 of remainder when dividing by m
  - ↳ e.g. for m = 3, 3 congruence classes:
    - $[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\} = \{..., -6, -3, 0, 3, 6, ...\} = \{3k : k \in \mathbb{Z}\}$
    - $[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\} = \{..., -5, -2, 1, 4, 7, ...\} = \{3k+1 : k \in \mathbb{Z}\}$
    - $[2] = \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\} = \{..., -4, -1, 2, 5, 8, ...\} = \{3k+2 : k \in \mathbb{Z}\}$
  - ↳ can have more than 1 rep
    - e.g. for m = 3, $[-3] = [0] = [3] = [6]$
    - $[0]$ has infinitely many rep of form $[a]$ for $a \in \mathbb{Z}$
- define $\mathbb{Z}_m$ to be set of m congruence classes $\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}$
  - ↳ can do modular arithmetic on $\mathbb{Z}_m$:
    - addition: $[a] + [b] = [a+b]$
    - multiplication: $[a][b] = [ab]$
- properties of modular arithmetic for all $[a] \in \mathbb{Z}_m$:
  1) $[a] + [0] = [0] + [a] = [a]$
     - $[0]$ is additive identity
  2) $[a][0] = [0][a] = [0]$
  3) $[a] + [-a] = [-a] + [a] = [0]$
     - $[-a]$ is additive inverse of $[a]$
  4) $[a][1] = [1][a] = [a]$
     - $[1]$ is multiplicative identity
- for $[a] \in \mathbb{Z}_m$, if there exists $b \in \mathbb{Z}_m$ such that $[a][b] = [b][a] = 1$, then $[b] = [a]^{-1}$ is multiplicative inverse of a
  - ↳ not every $[a]$ has multiplicative inverse

NOTE: when multiplying both sides of equation by $[k]$, make sure $\gcd(k, m) = 1$

- Modular Arithmetic Theorem (MAT): for all $a, c \in \mathbb{Z}$ w/ $a \neq 0$, equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has solution iff $d \mid c$, where $d = \gcd(a, m)$
  - ↳ when $d \mid c$, there's d solutions as given by $[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}], ..., [x_0 + (d-1)\frac{m}{d}]$
    - $[x] = [x_0]$ is one particular solution
  - ↳ to find solutions, consider $ax + my = c$
- Inverses in $\mathbb{Z}_m$ (INV $\mathbb{Z}_m$): let $a \in \mathbb{Z}$ w/ $1 \leq a \leq m-1$; element $[a]$ in $\mathbb{Z}_m$ has multiplicative inverse iff $\gcd(a, m) = 1$
  - ↳ multiplicative inverse is unique
- Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$): for all prime #s p & non-zero elements $[a]$ in $\mathbb{Z}_p$, multiplicative inverse $[a]^{-1}$ exists & is unique

FERMAT'S LITTLE THEOREM

- Fermat's Little Theorem (FLT): for all prime #s p & integers a not divisible by p, $a^{p-1} \equiv 1 \pmod p$
  - ↳ using INV $\mathbb{Z}_p$ when $[a]$ is non-zero element in $\mathbb{Z}_p$ & p is prime:
    - $[a][a]^{p-2} = [1]$

      $[a]^{-1} = [a^{p-2}]$
  - ↳ corollary of FLT: for all prime #s p & integers a, $a^p \equiv a \pmod p$

e.g. what's remainder when 3167^{2531} is divided by 17?

SOLUTION

$3167 \equiv 5 \pmod{17}$

$17 \nmid 5$ so by FLT, we have:

$5^{16} \equiv 1 \pmod{17}$

Using CAM & CP:

$3167^{2531} \equiv 5^{2531} \equiv 5^{158(16)+3} \equiv (5^{16})^{158}(5^3) \equiv 1^{158}(125) \equiv 6 \pmod{17}$

Since $0 \leq 6 < 17$, conclude from CTR that remainder is 6

CHINESE REMAINDER THEOREM

- Chinese Remainder Theorem (CRT): for all integers a_1 & a_2, & +ve integers m_1 & m_2, if $\gcd(m_1, m_2) = 1$, then simultaneous linear congruences $n \equiv a_1 \pmod{m_1}$ & $n \equiv a_2 \pmod{m_2}$ have a unique solution modulo $m_1 m_2$
  - ↳ if $n = n_0$ is one particular solution, then solutions are given by set of all $n \in \mathbb{Z}$ such that $n \equiv n_0 \pmod{m_1 m_2}$
- Generalized Chinese Remainder Theorem (GCRT): for all +ve integers k & $m_1, m_2, \ldots, m_k$, & integers $a_1, a_2, \ldots, a_k$, if $\gcd(m_i, m_j) = 1$ for all $i \neq j$, then simultaneous congruences $n \equiv a_1 \pmod{m_1}$, $n \equiv a_2 \pmod{m_2}$, $\vdots$, $n \equiv a_k \pmod{m_k}$ have unique solution modulo $m_1 m_2 \cdots m_k$
  - ↳ if $n = n_0$ is particular solution, then solutions are given by set of all $n \in \mathbb{Z}$ such that $n \equiv n_0 \pmod{m_1 m_2 \cdots m_k}$

SPLITTING A MODULUS

- Splitting Modulus Theorem (SMT): for all integers a & +ve integers m_1 & m_2, if $\gcd(m_1, m_2) = 1$, then simultaneous congruences $n \equiv a \pmod{m_1}$ & $n \equiv a \pmod{m_2}$ have exactly same solutions as $n \equiv a \pmod{m_1 m_2}$

week 10

PUBLIC-KEY ENCRYPTION

- objective of any secret communications scheme is to allow 2 parties, Alice (person A) & Bob (person B), to achieve **confidentiality** when communicating over insecure channel like the internet
  - ↳ i.e. eavesdropper Eve who observes exchanged messages wouldn't understand actual meaning of them
- Alice wants to communicate **plaintext** that needs to be transformed into unintelligible **ciphertext** using **encryption**
  - ↳ needs encryption key (EK)
  - ↳ transforming ciphertext into plaintext is called **decryption**
    - needs decryption key (DK)
- in traditional **symmetric-key encryption schemes**, encryption & decryption keys are identical (same key k)
  - ↳ key distribution problem is issue of securely transporting k
  - ↳ key management problem is managing huge # of secret keys
- **public-key cryptography** separates encryption from decryption keys
  - ↳ each participant B has secret DK & related EK they share in public repository
  - ↳ if user A wants to send message M to B, A obtains authentic copy of B's public EK & encrypts M to send ciphertext C to B
    - B is only person w/private DK so only B can decrypt C to recover M

IMPLEMENTING THE RSA SCHEME

in RSA (popular public-key encryption scheme), plaintexts are integers & assign # to each letter of alphabet

- **3 stages of RSA implementation**, in which Alice sends message to Bob:
  - ↳ setting up RSA: Bob does the following:
    1) randomly choose 2 large, distinct primes p & q & let $n = pq$
    2) select arbitrary integer e so $\gcd(e, (p-1)(q-1)) = 1$ & $1 < e < (p-1)(q-1)$
    3) solve congruence $ed \equiv 1 \pmod{(p-1)(q-1)}$ for integer d where $1 < d < (p-1)(q-1)$
    4) publish public key (e, n)
    5) keep secret private key (d, n) & primes p & q
  - ↳ RSA encryption: to encrypt message as ciphertext & send securely to Bob, Alice does following:
    1) obtain authentic copy of Bob's public key (e, n)
    2) construct plaintext message M, an integer st $0 \leq M < n$
       - if M is too long, may need to be broken into parts
    3) encrypt M as ciphertext C, given by $C \equiv M^e \pmod{n}$
       - $0 \leq C < n$
    4) send C to Bob
  - ↳ RSA decryption: to decrypt ciphertext received from Alice, Bob does following:
    1) use private key (d, n) to decrypt C as received message R, given by $R \equiv C^d \pmod{n}$
       - $0 \leq R < n$
    2) claim: $R = M$
- for RSA to be secure, must be computationally infeasible for adversary to compute Bob's private key (d, n) from public key (e, n)
  - ↳ n can't be factored so rec p & q be at least 300 digits each so that n is at least 600 digits

PROVING RSA SCHEME WORKS

- for all integers $p, q, n, e, d, M, C,$ & R, if

↳ p & q are distinct primes

↳ $n = pq$

↳ e & d are +ve integers st $ed \equiv 1 \pmod{(p-1)(q-1)}$ & $1 < e, d < (p-1)(q-1)$

↳ $0 \leq M < n$

↳ $M^e \equiv C \pmod{n}$, where $0 \leq C < n$

↳ $C^d \equiv R \pmod{n}$, where $0 \leq R < n$

then $R = M$

STANDARD FORM

· complex # z in standard form is expression of form $z = x + yi$ where $x, y \in \mathbb{R}$

↳ real # x is real part of z, written as $\mathrm{Re}(z)$

↳ real # y is imaginary part of z, written as $\mathrm{Im}(z)$

↳ set of all complex #s is $\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$

↳ $z = x + yi$ & $w = u + vi$ are equal (i.e. $z = w$) iff $x = u$ & $y = v$

↳ e.g. complex # $0 = 0 + 0i = 0i$ is both purely real & purely imaginary

· let $z = a + bi$ & $w = c + di$ be complex #s

↳ addition is defined by $z + w = (a + c) + (b + d)i$

↳ multiplication is defined by $zw = (ac - bd) + (ad + bc)i$

· $i^2 = -1$

· properties of complex #s where $z \in \mathbb{C}$:

↳ $z + 0 = 0 + z = z$

- 0 is additive identity in $\mathbb{C}$

↳ $z0 = 0z = 0$

↳ $z + (-1)z = (-1)z + z = 0$

- $(-1)z = -z$ is additive inverse of z

↳ $z1 = 1z = z$

- 1 is multiplicative identity in $\mathbb{C}$

· for all $z \in \mathbb{C}$, multiplicative inverse of z exists iff $z \neq 0$

↳ for $z = a + bi \neq 0$, multiplicative inverse is unique & given by $z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i = \frac{a - bi}{a^2 + b^2}$

properties of complex arithmetic (PCA) where $u, v, z \in \mathbb{C}$:

↳ $(u + v) + z = u + (v + z)$

- associativity of addition

↳ $u + v = v + u$

- commutativity of addition

↳ $0 = 0 + 0i$ has property that $z + 0 = z$

- additive identity

↳ if $z = a + bi$, then there exists additive inverse of z, written $-z$ w/property $z + (-z) = 0$

- additive inverse of $z = a + bi$ is $-z = -a - bi$

↳ $(uv)z = u(vz)$

- associativity of multiplication

↳ $uv = vu$

- commutativity of multiplication

↳ $1 = 1 + 0i$ has property $z1 = z$

- multiplicative identity

↳ if $z = a + bi \neq 0$, then there exists a multiplicative inverse of z, written z^{-1} w/property $zz^{-1} = 1$

- multiplicative inverse of $z = a + bi \neq 0$ is $z^{-1} = \frac{a - bi}{a^2 + b^2}$

↳ $z(u + v) = zu + zv$

- distributivity

· Binomial Theorem (BT): for all integers $n \geq 0$ & for all $a, b \in \mathbb{C}$, $(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^{n-m} b^m$

CONJUGATE AND MODULUS

· complex conjugate of complex # $z = x+yi$ is complex # $\overline{z} = x-yi$

· properties of conjugate (PCJ) where $z, w \in \mathbb{C}$:

↳ $\overline{(\overline{z})} = z$

↳ $\overline{z+w} = \overline{z} + \overline{w}$

↳ $z + \overline{z} = 2\text{Re}(z)$

- z is purely imaginary iff $z+\overline{z} = 0$ or $z = -\overline{z}$

↳ $z - \overline{z} = 2\text{Im}(z)i$

- z is purely real iff $z - \overline{z} = 0$ or $z = \overline{z}$

↳ $\overline{zw} = \overline{z}\,\overline{w}$

↳ if $z \neq 0$, then $\overline{(z^{-1})} = (\overline{z})^{-1}$

· modulus of complex # $z = x+yi$ is not -ve real # $|z| = \sqrt{x^2+y^2}$

· properties of modulus (PM) where $z, w \in \mathbb{C}$:

↳ $|z| = 0$ iff $z = 0$

↳ $|\overline{z}| = |z|$

↳ $\overline{z}z = |z|^2$

↳ $|zw| = |z||w|$

↳ if $z \neq 0$, then $|z^{-1}| = |z|^{-1}$

· e.g. write $z = \frac{3+4i}{2+5i}$ in standard form

SOLUTION

$$z = \frac{3+4i}{2+5i}\left(\frac{2-5i}{2-5i}\right)$$
$$= \frac{(6+20)+(-15+8)i}{2^2+5^2}$$
$$= \frac{26-7i}{29}$$
$$= \frac{26}{29} - \frac{7}{29}i$$

for all +ve $n \in \mathbb{Z}$ & $z_1, z_2, \ldots, z_n \in \mathbb{C}$ ·

↳ $\overline{z_1+z_2+\ldots z_n} = \overline{z_1} + \overline{z_2} + \ldots \overline{z_n}$

↳ $\overline{z_1 z_2 \ldots z_n} = \overline{z_1}\,\overline{z_2} \ldots \overline{z_n}$

↳ $|z_1 z_2 \ldots z_n| = |z_1||z_2| \ldots |z_n|$

· Triangle Inequality (TIQ): for all $z, w \in \mathbb{C}$, $|z+w| \leq |z| + |w|$

week 11

COMPLEX PLANE AND POLAR FORM

- complex # $z = x+yi$ can be rep by point (x,y) in plane whose axes are **real axis** (x-values) & **imaginary axis** (y-values)
  - ↳ called **complex / Argand plane**
- conjugate $\bar{z} = x-yi$ is rep by point $(x,-y)$
  - ↳ in geometric terms, reflection abt real axis
- modulus given by $|z| = \sqrt{x^2+y^2}$
  - ↳ in geometric terms, distance from origin to point
- Triangle Inequality becomes equality when A, B, & C are collinear

- **polar form** for complex # z is $z = r(\cos\theta + i\sin\theta)$
  - ↳ $r \geq 0$ is $|z|$
  - ↳ angle $\theta \in \mathbb{R}$ is **argument** of z
    - argument can be $\theta + 2\pi k$ for any $k \in \mathbb{Z}$
  - ↳ e.g. write $z = 5-5i$ in polar form

SOLUTION

$|z| = \sqrt{5^2+(-5)^2}$
$= \sqrt{50}$
$= 5\sqrt{2}$

$z = 5\sqrt{2}\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i\right)$
$z = 5\sqrt{2}\left(\cos\frac{7\pi}{4} - i\sin\frac{7\pi}{4}\right)$
Since $\frac{7\pi}{4} - 2\pi = -\frac{\pi}{4}$, another polar form is:
$z = 5\sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) - i\sin\left(-\frac{\pi}{4}\right)\right)$

- sum of angle formulas for sine & cosine:
  - ↳ $\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$
  - ↳ $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$

Polar Multiplication in $\mathbb{C}$ (PMC): for all complex #s $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ & $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$, $z_1 z_2 = r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$
  - ↳ $z_1 z_2 = z_2 z_1$

DE MOIVRE'S THEOREM

- **De Moivre's Theorem (DMT)**: for all $\theta \in \mathbb{R}$ & $n \in \mathbb{Z}$, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$
  - ↳ corollary: for all complex #s $z = r(\cos\theta + i\sin\theta)$ & $n \in \mathbb{Z}$, except when $|z| = r = 0$ & $n < 0$, $z^n = r^n(\cos n\theta + i\sin n\theta)$
- can use $\text{cis}\theta$ to rep $\cos\theta + i\sin\theta$
- when $\alpha, \beta \in \mathbb{R}$ & $n \in \mathbb{Z}$:
  - ↳ $\text{cis}\,0 = 1$
  - ↳ $\text{cis}\alpha\,\text{cis}\beta = \text{cis}(\alpha+\beta)$
  - ↳ $(\text{cis}\alpha)^n = \text{cis}(n\alpha)$
- $\text{cis}\theta = e^{i\theta}$ also written as $\cos\theta + i\sin\theta = e^{i\theta}$
  - ↳ special case $\theta = \pi$ gives $e^{i\pi} + 1 = 0$

COMPLEX n-TH ROOTS

- for complex # a & $n \in \mathbb{Z}^+$, complex #s z that satisfy equation $z^n = a$ are complex n-th roots of a
- **Complex n-th Roots Theorem (CNRT)**: for all complex #s $a = r(\cos\theta + i\sin\theta)$ & $n \in \mathbb{N}$, complex n-th roots of a are $\sqrt[n]{r}\left(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right)$, $k = 0, 1, 2, \ldots, n-1$
  - ↳ $\sqrt[n]{r}$ is n-th not -ve real root of r (unique)

↳ every non-zero complex # has exactly n diff complex n-th roots

↳ n-th roots of non-zero complex # of modulus r are equally spaced around circle of radius $\sqrt[n]{r}$ in complex plane, centred at origin

SQUARE ROOTS AND QUADRATIC FORMULA

- for all complex #s $a, b, \& c$ w/ $a \neq 0$, solutions to $az^2 + bz + c = 0$ are $z = \frac{-b \pm w}{2a}$ where w is solution to $w^2 = b^2 - 4ac$
- e.g express solutions to $2z^2 + 3z + 2 = 0$ in standard form

SOLUTION

$z = \frac{-3 \pm w}{4}$ where $w^2 = 3^2 - 4(2)(2)$

$= -7$

One solution to $w^2 = -7$ is $w = \sqrt{7}\,i$ so 2 solutions are $z = -\frac{3}{4} \pm \frac{\sqrt{7}}{4}i$

POLYNOMIALS INTRODUCTION

- a field is a set of #s which has an addition & multiplication satisfying 9 properties in PCA
  - ↳ e.g. rational #s $\mathbb{Q}$, real #s $\mathbb{R}$, complex #s $\mathbb{C}$, & integers modulo a prime $\mathbb{Z}_p$
  - ↳ integers $\mathbb{Z}$ aren't a field b/c only -1 & 1 have a multiplicative inverse
  - ↳ $\mathbb{Z}_6$ isn't a field b/c [3] doesn't have a multiplicative inverse

for all fields $\mathbb{F}$ & all $a, b, c \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$

  - ↳ i.e. $\mathbb{F}$ has no zero divisors

- polynomial in x over field $\mathbb{F}$ is expression of form $a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$
  - ↳ $n \geq 0$ & $n \in \mathbb{Z}$
  - ↳ x is indeterminate
  - ↳ $a_0, a_1, \dots, a_n$ are elements of $\mathbb{F}$
  - ↳ each a_i is coefficient & each $a_i x^i$ is term of polynomial
  - ↳ use $\mathbb{F}[x]$ to denote set of all polynomials over field $\mathbb{F}$
- let $a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ be polynomial in $\mathbb{F}[x]$, where $n \geq 0$ is integer & $a_n \neq 0$
  - ↳ has degree n, written as $\deg f(x) = n$
  - ↳ zero polynomial has all coeffs = 0 & degree is undefined
  - ↳ constant polynomial is either zero polynomial or has degree 0
- polynomials $a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ & $b_n x^n + b_{n-1}x^{n-1} + \dots + b_1 x + b_0$ in $\mathbb{F}[x]$ are equal iff $a_k = b_k$ for all $k = 0, 1, \dots, n$

ARITHMETIC WITH POLYNOMIALS

$f(x)$ in summation notation is $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k$

let $f(x) = \sum_{i=0}^{m} a_i x^i$ & $g(x) = \sum_{j=0}^{n} b_j x^j$ be polynomials in $\mathbb{F}[x]$

  - ↳ addition of $f(x)$ & $g(x)$ is $f(x) + g(x) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) x^k$
    - $a_k = 0$ for $k > m$ & $b_k = 0$ for $k > n$
  - ↳ multiplication of $f(x)$ & $g(x)$ is $f(x)g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j} = \sum_{\ell=0}^{m+n} c_\ell x^\ell$
    - $c_\ell = a_0 b_\ell + a_1 b_{\ell-1} + \dots + a_{\ell-1} b_1 + a_\ell b_0 = \sum_{i=0}^{\ell} a_i b_{\ell-i}$ for $\ell = 0, 1, \dots, m+n$

- Degree of Product (DP) Lemma: for all fields $\mathbb{F}$ & all non-zero polynomials $f(x)$ & $g(x)$ in $\mathbb{F}[x]$, $\deg f(x)g(x) = \deg f(x) + \deg g(x)$
- Division Algorithm for Polynomials (DAP): for all fields $\mathbb{F}$ & all polynomials $f(x)$ & $g(x)$ in $\mathbb{F}[x]$ w/ $g(x)$ not being zero polynomial, there exist unique polynomials st $f(x) = q(x)g(x) + r(x)$
  - ↳ $r(x)$ is zero polynomial or $\deg r(x) < \deg g(x)$
- for polynomials $f(x)$ & $g(x)$ over $\mathbb{F}$, $g(x)$ divides / is a factor of $f(x)$, written $g(x) \mid f(x)$, if there exists polynomial $q(x)$ st $f(x) = q(x)g(x)$
  - ↳ i.e. $g(x) \mid f(x)$ when $r(x)$ from DAP is zero polynomial or $f(x)$ & $g(x)$ are both zero polynomials

week 12

ROOTS OF COMPLEX POLYNOMIALS

- polynomial equation has form $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$
  - ↳ often written as $f(x) = 0$ where $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{F}[x]$
  - ↳ element $c \in \mathbb{F}$ is root of polynomial $f(x)$ if $f(c) = 0$
    - i.e. c is solution of $f(x) = 0$
- Remainder Theorem (RT): for all fields $\mathbb{F}$, all polynomials $f(x) \in \mathbb{F}[x]$, & all $c \in \mathbb{F}$, remainder polynomial when $f(x)$ is divided by $x - c$ is constant polynomial $f(c)$
- Factor Theorem (FT): for all fields $\mathbb{F}$, all polynomials $f(x) \in \mathbb{F}[x]$, & all $c \in \mathbb{F}$, linear polynomial $x - c$ is factor of $f(x)$ iff $f(c) = 0$

Fundamental Theorem of Algebra (FTA): for all complex polynomials $f(z)$ w/ $\deg f(z) \geq 1$, there exists a $z_0 \in \mathbb{C}$ st $f(z_0) = 0$

- Complex Polynomials of Degree n Have n Roots (CPN): for all integers $n \geq 1$ & all complex polynomials $f(z)$ of degree $n \geq 1$, there exist complex #s $c \neq 0$ & $c_1, c_2, \dots, c_n$ st $f(z) = c(z - c_1)(z - c_2) \cdots (z - c_n)$
  - ↳ roots of $f(z)$ are $c_1, c_2, \dots, c_n$
- multiplicity of root c of polynomial $f(x)$ is largest +ve integer k st $(x - c)^k$ is factor of $f(x)$
- for all fields $\mathbb{F}$, all integers $n \geq 1$, & all $f(x) \in \mathbb{F}[x]$ of degree n, polynomial $f(x)$ has at most n roots
- polynomial in $\mathbb{F}[x]$ of +ve degree is reducible polynomial in $\mathbb{F}[x]$ when it can be written as product of 2 polynomials in $\mathbb{F}[x]$ of +ve degree
  - ↳ otherwise, it's irreducible polynomial in $\mathbb{F}[x]$
    - using DP, all linear polynomials are irreducible over any field
    - by CPN, linear polynomials are the only irreducible polynomials over $\mathbb{C}$
    - for all primes p, there are irreducible polynomials of any given +ve degree so there's no upper bound on degree of irreducible polynomials in $\mathbb{Z}_p[x]$
- monic polynomials have coeff of largest power of x equal to 1 (multiplicative identity in $\mathbb{F}$)
  - ↳ unique factorization result for polynomials is that every monic polynomial in $\mathbb{F}[x]$ can be written as product of monic irreducible polynomials uniquely (apart from order of factors)
    - if $f(x)$ isn't monic polynomial, write $f(x) = cg(x)$ where $g(x)$ is monic polynomial

REAL POLYNOMIALS AND CONJUGATE ROOTS THEOREM

Conjugate Roots Theorem (CJRT): for all polynomials $f(x)$ w/ real coeffs, if $c \in \mathbb{C}$ is root of $f(x)$, then $\bar{c} \in \mathbb{C}$ is root of $f(x)$

- Real Quadratic Factors (RQF): for all polynomials $f(x)$ w/ real coeffs, if $c \in \mathbb{C}$ is root of $f(x)$ & $\mathrm{Im}(c) \neq 0$, then there exists a real quadratic polynomial $g(x)$ & real polynomial $q(x)$ st $f(x) = g(x)q(x)$
  - ↳ quadratic factor $g(x)$ is irreducible in $\mathbb{R}[x]$
- Real Factors of Real Polynomials (RFRP): for all real polynomials $f(x)$ of +ve degree, $f(x)$ can be written as product of real linear & real quadratic factors
  - ↳ irreducible polynomials over $\mathbb{R}$ have only degrees of 1 or 2

INTEGER POLYNOMIALS AND RATIONAL ROOTS THEOREM

- Rational Roots Theorem (RRT): for all polynomials $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$ w/ integer coeffs & $n \geq 1$, if $\frac{p}{q}$ is rational root of $f(x)$ w/ $\gcd(p, q) = 1$, then $p \mid a_0$ & $q \mid a_n$
  - ↳ result can be applied to any rational polynomial
  - ↳ provides list of rational #s that are candidates to be roots (i.e. not guaranteed)
- there are irreducible polynomials of every +ve degree in $\mathbb{Q}$ so there's no upper bound on degree of irreducible

polynomials over $\mathbb{Q}$

- e.g. factor $f(x) = x^4 + [1]$ in $\mathbb{Z}_2[x]$

SOLUTION

Since $[1] = [-1]$ in $\mathbb{Z}_2$:

$$\begin{aligned} x^4 + [1] &= x^4 - [1] \\ &= (x^2 - [1])(x^2 + [1]) \\ &= (x^2 - [1])(x^2 - [1]) \\ &= (x^2 - [1])^2 \\ &= (x + [1])^2 (x - [1])^2 \\ &= (x + [1])^2 (x + [1])^2 \\ &= (x + [1])^4 \end{aligned}$$

Thus, $x^4 + [1] = (x + [1])^4$.

PRIME NUMBERS AND RIEMANN HYPOTHESIS

- for an integer $x \geq 2$, # of primes in interval $[2, x]$ is denoted by prime counting function $\pi(x)$
  - ↳ values of $\pi(x)$ for $2 \leq x \leq 20$:

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\pi(x)$	1	2	2	3	3	4	4	4	4	5	5	6	6	6	6	6	7	8	8

- for all $n \in \mathbb{Z}^+$, $p_n \leq 2^{2^{n-1}}$
  - ↳ gives upper bound for p_n
- for all integers $x \geq 2$, $\pi(x) > \log(\log x)$
  - ↳ gives lower bound for prime counting function $\pi(x)$
- for all integers $x \geq 2$, $\pi(x) \geq \log x / (2 \log 2)$
  - ↳ gives better lower bound for prime counting function $\pi(x)$
- Prime Number Theorem: $\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$
- Riemann Hypothesis: let $Li(x) = \int_2^x \frac{dt}{\log t}$ for $x \geq 2$; for all integers $x \geq 3000$, $|\pi(x) - Li(x)| < (\sqrt{x} \log x)/8\pi$