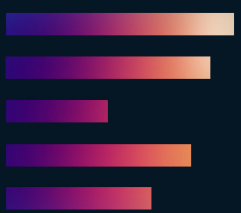
FALL 2024

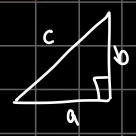
MATH 230: Abstract & Discrete Mathematics



Pythagorean Theorem:

Friday, August 23

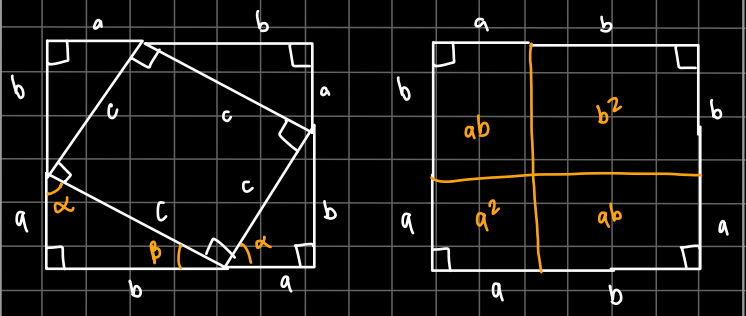
$a^2+b^2=c^2$



sidelength opposite the angle between a & b

theorem: given a right triangle with side lengths a, b and c, where c is the length of the hypotenuse. (longest side)

$a^2+b^2=c^2$



$A=(a+b)^2=a^2+2ab+b^2$

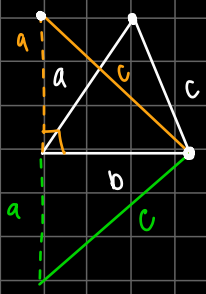
$A=4\left(\frac{ab}{2}\right)+c^2=2ab+c^2$

$a^2+2ab+b^2=2ab+c^2$

$\therefore a^2+b^2=c^2$

Converse of Pythagorean Theorem:

- Suppose we have a triangle with side lengths a, b, and c such that $a^2+b^2=c^2$.
- then, the triangle is a right triangle.



$a^2+b^2=c^2$

$c^2=a^2+b^2=e^2$

$\therefore c=e$

"If A then B":

- only valuable is A is true
- if A is false, we have a vacuous truth.

- Pythagoras' Theorem is both an

"if A, then B" $\iff A \Rightarrow B$

"if B, then A" $\iff B \Rightarrow A$

$\therefore$ "A if and only if B" $\iff A \Leftrightarrow B$

Generalized Pythagorean Theorem:

- Suppose we have a triangle $\uparrow$ with side lengths a, b, and c, with c being the longest of the three.
- Then $\uparrow$ is a right triangle if and only if $a^2+b^2=c^2$.

Find a general solution to

$ax^2+bx+c=0$ when $a\neq 0$ $\Big\}$ $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

Since $a\neq 0$, we can divide both sides by a.

$\therefore \frac{ax^2+bx+c}{a}=\frac{0}{a}$

$x^2+\frac{b}{a}x+\frac{c}{a}=0$

complete the square

$\left(x+\frac{b}{2a}\right)^2=x^2+\frac{b}{a}+\frac{b^2}{4a^2}$

$\therefore \left(x+\frac{b}{2a}\right)^2+\frac{c}{a}=\frac{b^2}{4a^2}$

$\left(x+\frac{b}{2a}\right)^2=\frac{b^2}{4a^2}-\frac{c}{a}$

$\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$

take the square root

$x+\frac{b}{2a}=\pm\sqrt{\frac{b^2-4ac}{4a^2}}=\pm\frac{\sqrt{b^2-4ac}}{2a}$

$\therefore x=-\frac{b}{2a}\pm\frac{\sqrt{b^2-4ac}}{2a}$

Law of Cosines:

- Then $c^2=a^2+b^2-2ab\cos\theta$
- $\cos\theta=\frac{m}{a}$ - $m=a\cos\theta$
- $m=b-n$ - $b=n+m$
- $n=b-m$

By pythagoras:

$m^2+h^2=a^2$

$n^2+h^2=c^2$

$\therefore c^2=n^2+(a^2-m^2)$

$=(n^2-m^2)+a^2$

$=(n-m)(n+m)+a^2$

$=b(n-m)+a^2$

$=b(b-2m)+a^2$

$=b^2-2bm+a^2$

$=a^2+b^2-2ab\cos\theta$

5. Proof

Monday, 26 August

Proof Template 1 Direct proof of an if-then theorem.

- Write the first sentence(s) of the proof by restating the hypothesis of the result. Invent suitable notation (e.g., assign letters to stand for variables).
- Write the last sentence(s) of the proof by restating the conclusion of the result.
- Unravel the definitions, working forward from the beginning of the proof and backward from the end of the proof.
- Figure out what you know and what you need. Try to forge a link between the two halves of your argument.

definition: An integer n is even if there exists an integer k such that $n = 2k$.

theorem: The sum of two even integers is even

proof:
- let x, y be even.
- we want to show that $x+y$ is even
- since x, y are even, there exist m, n integers such that:

$x = 2m$, $y = 2n$ } $x+y = 2c$ } the sum of two integers is an integer

$x+y = 2(m+n)$

let $c = m+n$

$\therefore x+y = 2c$ where c is an integer

$\therefore x+y$ is even □

definition: let a, b be integers. We say $a \mid b$ ("a divides b") if there exists an integer k such that $b = ak$.

↓ allows $\frac{0}{0}$

theorem: If a, b, d are integers such that $d \mid a$ and $d \mid b$, then $d \mid a+b$.

proof:
- Since $d \mid a$ and $d \mid b$, there exist integers m and n such that:

$a = dm$

$b = dn$

- Therefore $a+b = d(m+n)$

let $c = m+n$

$\therefore a+b = dc$

- c is an integer and $a+b = dc$

$\therefore d \mid a+b$ □

definition: An integer n is odd if there exists an integer k such that $n = 2k+1$

theorem:
- let n be an integer.
- n is even if and only if $n+1$ is odd.

proof: WTP: "If n is even, $n+1$ is odd" ($\Rightarrow$) sufficient

WTP: "If $n+1$ is odd, n is even" ($\Leftarrow$) necessary

($\Rightarrow$):
- Suppose n is even so $n = 2k$ for some integer k.
- Then $n+1 = 2k+1$, so $n+1$ is odd.

($\Leftarrow$):
- Suppose $n+1$ is odd so $n+1 = 2k+1$ for some integer k.
- Then $n = (2k+1)-1 = 2k$, so n is even. □

definition: An integer $p > 1$ is prime if the only divisors of p are 1 and p

proposition: If $n > 1$ is an integer, then n^3+1 is not prime

proof: $n^3+1 = (n+1)(n^2-n+1)$

so $n+1 \mid n^3+1$

NTS: $n+1 \neq 1$, $n+1 \neq n^3+1$

$n > 1$ so $n+1 > 1$

$n > 1$ so $n^3 > n$ so $n^3+1 > n+1$

$\therefore n+1 \neq 1$, $n+1 \neq n^3+1$ □

definition: A positive integer a is called composite provided there is an integer b such that $1 < b < a$ and $b \mid a$.

proposition: Let x be an integer. If $x > 1$, then x^3+1 is composite.

proof:

1. Let x be an integer and suppose that $x > 1$.
2. Note that $x^3+1 = (x+1)(x^2-x+1)$
3. Since x is an integer, both $(x+1)$ and (x^2-x+1) are integers.
4. Therefore $x+1 \mid x^3+1$
   - Since $x > 1$, $x+1 > 1+1 = 2 > 1$.
   - Also, since $x > 1$, $x < x^3$. Adding 1 to both sides, $x+1 < x^3+1$.
   - Thus, $x+1$ is an integer with $1 < x+1 < x^3+1$.
5. Since $1 < x+1 < x^3+1$ and $x+1 \mid x^3+1$, x^3+1 is composite.

□

6. Counterexample

Proof Template 3 Refuting a false if-then statement via a counterexample.

To disprove a statement of the form "If A, then B":
Find an instance where A is true but B is false.

disprove: If $a|b$ and $b|a$, then $a = b$.

proof:
1. since $a|b$, $b = ka$ for some integer k.
2. Likewise, since $b|a$, $a = mb$ for some integer m.
3. Substituting b from step 1 into the equation in step 2: $a = m(ka)$
   $a = (mk)a$
4. If $a > 0$, $mk = 1$
   $\therefore m = k = 1$ or $m = k = -1$
5. If $m = k = 1$, $a = (1)b$, $a = b$
6. If $m = k = -1$, $a = (-1)b$, $a = -b$
7. Therefore $a = \pm b$ □

disprove: If a and b are integers with $a|b$, $a \leq b$.

proof: NTS: $a|b$ but $a \not\leq b$
1. Let $a = 2$, $b = 0$
2. First, we show that $a|b$: $2|0$ is true because there exists an integer $k = 0$ such that $b = ka$: $0 = (0)2$
3. However $a \not\leq b$ does not hold: $2 \not\leq 0$ because $2 > 0$. □

disprove: If p and q are prime, then $p+q$ is composite.

proof:
1. Let $p = 2$, $q = 3$
2. First, we show that p and q are prime.
   - 2 is prime as its only factors are 1 and 2.
   - 3 is prime as its only factors are 1 and 3.
3. Now we evaluate $p+q$:
   - $p+q$: $2+3 = 5$
4. We need to show that 5 is not composite (i.e., 5 is prime).
   - The factors of 5 are only 1 and 5
   therefore, 5 is prime, not composite. □

7. Boolean Algebra

Wed, Aug 28

Proof Template 4 Truth table proof of logical equivalence

To show that two Boolean expressions are logically equivalent:
Construct a truth table showing the values of the two expressions for all possible values of the variables.
Check to see that the two Boolean expressions always have the same value.

theorem: $x \vee \neg x = T$

"$\vee$": or
"$\wedge$": and
"$\neg$": not

proof:

x	$\neg x$	$x \vee \neg x$
T	F	T
F	T	T

□

OR

proof:- If x is true, then $\neg x$ is false, so $x \vee \neg x = T$.
- If x is false, then $\neg x$ is true,
so $x \vee \neg x = T$. □

"$\rightarrow$": implies

"$\leftrightarrow$": if & only if

x	y	$x \rightarrow y$	
T	T	T	
T	F	F	
F	T	T	vacuously true
F	F	T	vacuously true

x	y	$x \leftrightarrow y$
T	T	T
T	F	F
F	T	F
F	F	T

proposition: $(x \rightarrow y) \wedge (y \rightarrow x) = x \leftrightarrow y$

proof:

x	y	$x \rightarrow y$	$y \rightarrow x$	$(x \rightarrow y) \wedge (y \rightarrow x)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

□

Theorem 7.2:

① $x \wedge y = y \wedge x$, $x \vee y = x \wedge y$ } commutative properties

② $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$ } associative properties

③ $\underbrace{x \wedge T}_{x \times 1} = x$, $\underbrace{x \vee F}_{x+0} = x$ } identity elements

④ $\neg(\neg x) = x$ } involution

⑤ $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ } distributive properties

⑥ $x \wedge (\neg x) = F$, $x \vee (\neg x) = T$

⑦ $\neg(x \wedge y) = (\neg x) \vee (\neg y)$, $\neg(x \vee y) = (\neg x) \wedge (\neg y)$ } DeMorgan's Laws

proposition: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

proof:

x	y	z	$y \wedge z$	$x \vee (y \wedge z)$	$x \vee y$	$x \vee z$	$(x \vee y) \wedge (x \vee z)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

□

OR

proof:
- if $x = T$, then $x \vee (y \wedge z) = T$, likewise both $(x \vee y)$ and $(x \vee z) = T$.
- so, $(x \vee y) \wedge (x \vee z) = T$
- if $x = F$, then $x \vee (y \wedge z) = y \wedge z$
  likewise $x \vee y = y$
  $x \vee z = z$
- so, $(x \vee y) \wedge (x \vee z) = y \wedge z$ □

---

8. Lists

Fri, Aug 30

definition: A list is an ordered collection of elements in a sequence.

$(1,2,3)$, $((1,2),(1,2,3))$

$(1,2,3) \neq (3,2,1)$

1. How many lists with 2 elements exist if the elements are $(1,2,3,4)$.
   $4 \times 4 = 16$ //

Multiplication Principle: The number of list with 2 elements where the first element is one of m things and the second element is one of n things is $m \times n$.

Ex: count the divisors of 10^n
if $d \mid 10^n$, then $d = 2^a \cdot 5^b$
where $0 \leq a \leq n$
and $0 \leq b \leq n$
The # of such divisors is the number of lists of the form (a,b) where $0 \leq a \leq n$, $0 \leq b \leq n$
answer: $(n+1)(n+1) = (n+1)^2$

- A list with k elements and each element is one of n possibilities.
  - # of lists $= n^k$.
- what if we don't allow repeats?
  - $n(n-1)(n-2)\dots(n-k+1) = (n)_k$

Ex: 100m final, 8 lanes, 3 winners
# of possible podiums $= 8(8-1)(8-2)$
$= 8 \times 7 \times 6$

$n! = n(n-1)(n-2)\dots(1)$ for $n \geq 1$
$= \frac{n!}{(n-k)!}$ if $0 \leq k \leq n$

---

10. Sets I: Introduction, Subsets

Definition: A set is an unordered collection of elements.

$\{1,2\}, \{1,\mathbb{Z}\}, \{\{1,2\},\{1,2,3\}\}$

$\mathbb{Z} = \{\dots,-2,-1,0,1,2,\dots\}$
$\mathbb{N} = \{1,2,3,\dots\} = \mathbb{Z}^+$
$\mathbb{N}_0 = \{0,1,2,3,\dots\}$

$\{1,2,3\} = \{3,2,1\}$

- Two sets are equal if they have the same elements.

$A = \{(a,b,c) \mid a,b,c \in \mathbb{Z} \text{ and } a^2+b^2=c^2\}$

$B = \{(a,b,c) \mid a = x^2-y^2, b = 2xy, c = x^2+y^2 \text{ for some } x,y,z\}$

$C = \{\frac{a}{b} \mid a,b \in \mathbb{Z} \text{ and } b \neq 0\}$

$d = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$

Suppose: $(a,b,c) \in B$,
then, there exist $x,y \in \mathbb{Z}$ s.t.
$a = x^2-y^2$
$b = 2xy$
$c = x^2+y^2$
Note: $a,b,c \notin \mathbb{Z}$

$\therefore a^2+b^2 = (x^2-y^2)^2 + (2xy)^2$
$= x^4 - 2x^2y^2 + y^4 + 4x^2y^2$
$= x^4 + 2x^2y^2 + y^4 = (x^2+y^2)^2 = c^2$

- since $a, b, c \in \mathbb{Z}$ and $a^2 + b^2 = c^2$

$$(a, b, c) \in A$$

$\therefore B \subseteq A$

- However, $A \not\subseteq B$.

- For example, $(4, 3, 5) \in A$

- For $(4, 3, 5) \in B$, we need $3 = 2xy$ for some $x, y \in \mathbb{Z}$.

- However $xy = \frac{3}{2} \notin \mathbb{Z}$.

- given 2 sets S and T.
  To prove $S = T$.
- You need:
  (1) $S \subseteq T$ ($s \in S$, $s \in T$)
  (2) $T \subseteq T$ ($t \in T$, $t \in T$)

- show that $C = D$

- suppose $d \in D$:
  - so $d = \frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$
  - so $a, b \in \mathbb{Z}$ and $b \neq 0$
  - hence $\frac{a}{b} \in C$
  - so $D \subseteq C$.

- suppose $c \in C$:
  - so $c = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$
  - so $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ & $b \neq 0$
  - if $b \in \mathbb{N}$, then $\frac{a}{b} \in D$
  - if $b \notin \mathbb{N}$, b is a negative integer so $b \neq 0$

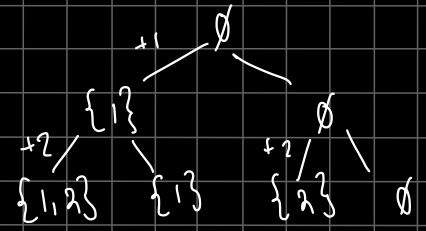
$$\frac{a}{b} : \frac{a(-1)}{b(-1)} = \frac{-a}{-b}$$

  - $b \in \mathbb{N}$ and $b \neq 0$ so $-b \in \mathbb{N}$
  - $-a \in \mathbb{Z}$

  - $\therefore \frac{-a}{-b} \in D$, so $C \subseteq D$.

$A = \{1, 2\}$

Subsets: $\emptyset, \{1\}, \{2\}, \{1, 2\}$



$A = \{1, 2, 3\}$

Subsets: $\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$

$A = \{1, 2, 3, \ldots n\}$
Subsets $= 2^n$

definition: The power set of A is the sets of all sets of A
$pow(A) = 2^A$

---

11. Quantifiers

Wed, Sep 4

- $\exists$ - there exists - $!$ - unique

- Existential statement: To prove them, you need an example
- Example: There is an even integer that is prime.
- Proof: 2 is even and 2 is prime

- $\forall$ - for all → Proof: Negate the prove

- Example: The sum of two even integers is an even integer.
- Example: $A \subseteq B \rightarrow \forall x \in A, \forall x \in B$

"Every integer is prime"

logic: $\forall n \in \mathbb{Z}$, n is prime.
negate: $\exists n \in \mathbb{Z}$, n is not prime
sentence: "There is an integer that is not prime"

"There is an integer x such that for all integers y, $x+y = 0$"

1. $\exists x \in \mathbb{Z},\ \forall y \in \mathbb{Z},\ x+y=0$
2. $\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ x+y \neq 0$
3. "For all integers x, there exists an integer y such that $x+y \neq 0$."

"Some integer is divisible by 7"

1. $\exists n \in \mathbb{Z},\ 7 \mid n$
2. $\forall n \in \mathbb{Z},\ 7 \nmid n$
3. "All integers are not divisible by 7"

"There is no line that goes through all 3 line segments (unless it goes through a vertex)"

Negation: "there is a line that goes through all 3 line segments without going through a vertex."

---

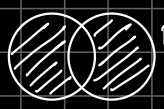
12. Sets II : Operations

union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

difference: $A \setminus B = A - B = \{x \mid x \in A \text{ and } x \notin B\}$

sym. diff.: $A \triangle B = (A-B) \cup (B-A)$



cartesian product: $A \times B = \{(x,y) \mid x \in A \text{ and } y \in B\}$

DeMorgan's Laws:
$A-(B \cup C) = (A-B) \cap (A-C)$
$A-(B \cap C) = (A-B) \cup (A-C)$

Theorem: If A and B are finite and $|A|=m$ and $|B|=n$, then $|A \times B| = m \cdot n$

NTS: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

1. let $x \in A \cup (B \cap C)$
   so $(x \in A)$ or $(x \in B$ and $x \in C)$
   (a) if $(x \in A)$ or $(x \in B)$, $x \in (A \cup B)$
   (b) if $(x \in A)$ or $(x \in C)$, $x \in (A \cup C)$
   $\therefore x \in (A \cup B) \cap (A \cup C)$

2. let $y \in (A \cup B) \cap (A \cup C)$
   so $y \in^{(a)} (A \cup B)$ and $y \in^{(b)} (A \cup C)$
   - if $y \in A$, $y \in A$ for both conditions
   - if $y \notin A$, $y \in B$
     if $y \notin A$, $y \in C$
   - if $y \in B$ and $y \in C$, $y \in B \cap C$
   $\therefore y \in A \cup (B \cap C)$

Theorem (Principle of Inclusion-Exclusion):
Suppose A, B are finite sets:
$$|A \cup B| = |A| + |B| - |A \cap B|$$

Proof:
- Let $a_1, a_2, \ldots, a_n$ be the elements of A not in B.
- Let $b_1, b_2, \ldots, b_m$ be the elements of B not in A.
- Let $c_1, c_2, \ldots, c_r$ be the elements of $A \cap B$.

then $|A \cup B| = n+m+r$
$|A| = n+r$
$|B| = m+r$
$\therefore |A|+|B| - |A \cap B| = (n+r)+(m+r)-(r) = n+m+r$

$$|A \cup B \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$$
$$= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cup C)|$$
$$= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

How many positive integers ≤ 1000 are even, mult. of 3 or mult. of 5?

A: even integers between 1 & 1000 (incl.)
B: Mult of 3 between 1 & 1000
C: Mult of 5 between 1 & 1000 (incl.)

(mult. of 6; mult. of 15; mult. of 10)

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|$$
$$= 500 + 333 + 200 - 166 - 100 - 66 + 33$$

Combinations with repetition

Dozen donuts, 3 flavors, how many ways? $n=12$, $r=3$

14 choices for the 2 seperators $r-1$ $\binom{14}{2}$

14. Relations — Mon, Sep 9

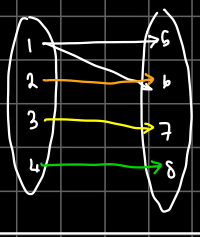
- A relation R on A×B is a subset of A×B.

Ex: $A = \{1,2,3,4\}$
$B = \{5,6,7,8\}$

$R = \{(1,5), (1,6), (2,6), (3,7), (4,7)\}$

"1 is related to 5"
"1 R 5"
"$(1,5) \in R$"
if $(x,y) \in R$, xRy.

1R5, 1R6, 2R6, 3R7, 4R8
1R7, 1R8, 2R5, 2R7, 3R8



- R is a relation on a set A if $R \subseteq A \times A$

$A = \{1,2,3,4\}$

1. Let R_1 be the relation "is equal to"
$R_1 = \{(1,1), (2,2), (3,3), (4,4)\}$
2. Let R_2 be the relation "is less than"
$R_2 = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$
3. Let R_3 be the relation such that:
$R_3 = \{(1,1), (1,2), (2,2), (3,1), (3,2), (4,4)\}$

- Some types of relations:

- Reflexive
- Irreflexive
- Transitive
- Symmetric
- Antisymmetric

Let R be a relation on A.

① Reflexive: (=)

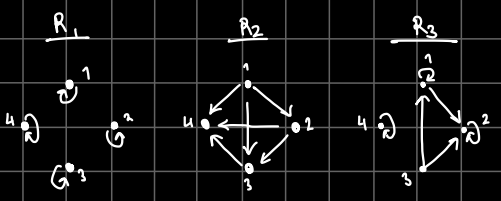
- R is reflexive if $\forall a \in A, (a,a) \in R$. or aRa

② Irreflexive: No loops
- R is irreflexive if $\forall a \in A, (a,a) \notin R$. $a \not R a$.

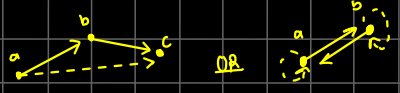
③ Symmetric: (≠)

- R is symmetric if whenever $(a,b) \in R$, $(b,a) \in R$. $aRb \Rightarrow bRa$

④ Antisymmetric: (≤) [any arrows go 1 way]
- R is antisymmetric if $(a,b) \in R$ and $(b,a) \in R$ implies $a = b$ → $(aRb \wedge bRa) \Rightarrow x = y$



⑤ Transitive: (<)



- R is transitive if $(a,b) \in R$ and $(b,c) \in R$ implies $(a,c) \in R$. $(xRy \wedge yRz) \Rightarrow xRz$

Theorem:
- Let R be a relation on a non-empty set A
- Then R is symmetric and antisymmetric if and only if $R \subseteq \{(a,a) \mid a \in A\}$

Proof:

(<=):
- Suppose $(a,b) \in R$
- Since $R \subseteq \{(a,a) \mid a \in A\}$,
  $\therefore a = b$
  so $(b,a) \in R$
- Therefore R is symmetric.
- Suppose $(a,b) \in R$ and $(b,a) \in R$.
- Since $(a,b) \in R$, $a = b$.
- So, it's antisymmetric.

$\Rightarrow$:

- Suppose R is symmetric and antisymmetric.
- Let $(a,b) \in R$.
- Since R is symmetric, $(b,a) \in R$.
- Since R is antisymmetric and $(a,b) \in R$ and $(b,a) \in R$.
  so, $a = b$.
- Therefore $(a,b) \in \{(x,x) \mid x \in A\}$

$A = \{1,2,3,4\}$

- How many relations of A are symmetric and antisymmetric.

$2^4 = 32$ // (Power sets)

- # of relations: 2^{n^2} (diagonals / off-diagonals) $\rightarrow R \subseteq A \times A$
- # of symmetric: $2^n \cdot 2^{\frac{n^2-n}{2}} = 2^{\frac{n^2+n}{2}}$
- # of antisymmetric: $2^n \cdot 3^{\frac{n^2-n}{2}}$ (3 choices when $a \neq b$: include (a,b) but not (b,a); include (b,a) but not (a,b); exclude both)
- # of reflexive: 2^{n^2-n}
- # of irreflexive: 2^{n^2-n}
- # of transitive: open problem.

---

15. Equivalence Relations — Wed, Sep 18

- We say a relation R on set A is an equivalence relation if R is reflective, symmetric, and transitive.

$\{(1,1),(2,2),(3,3)\}$ on $\{1,2,3\}$ is an equiv. relation.

- Let R be the relation on $\mathbb{Z}$ where a is related to b if they both have the same parity.

Prove it's an equivalence relation:

Reflective: A number a has the same parity as itself—so $(a,a) \in R$ $\therefore$ R is reflective.

Symmetric: Suppose $(a,b) \in R$.
case 1: a and b are both even, then $(b,a) \in R$.
case 2: a and b are both odd, then $(b,a) \in R$.
$\therefore$ R is symmetric

Transitive: Suppose $(a,b) \in R$ and $(b,c) \in R$.
Case 1: a is even
Since $(a,b) \in R$, b is even
Since $(b,c) \in R$, c is even.
a and c have the same parity $\therefore (a,c) \in R$
case 2: a is odd.
Since $(a,b) \in R$, b is odd.
Since $(b,c) \in R$, c is odd.
Since a and c have the same parity, $(a,c) \in R$.
$\therefore$ R is transitive.

Congruence mod n: (→ equivalence relation)

- We say $a \equiv b \bmod n$ iff $n \mid (b-a)$ (they differ by a multiple of n.)

a is congruent to $b \pmod n$, $a \equiv b \pmod n \Rightarrow a \pmod n = b \pmod n$

Consider the relation R_n: $\{(a,b) \mid a \equiv b \bmod n\}$
$\therefore (a,b) \in R_n$ if $n \mid b-a$

Prove equivalence relation on $\mathbb{Z}$

Reflexive: Let $a \in \mathbb{Z}$

- NTS: $(a,a) \in R_n$, $a \equiv a \bmod n$
  $n \mid a-a$
  - $a-a = 0$, $n \mid 0$ because $0 = 0 \cdot n$
  $\therefore n \mid a-a$
  $\therefore a \equiv a$.
- Thus, R_n is reflexive.

Symmetric: Let $(a,b) \in R_n$

- NTS: $(b,a) \in R_n$, $b \equiv a \bmod n$, $n \mid a-b$, $a-b = kn$
- Since $(a,b) \in R_n$, $a \equiv b \bmod n$,
  so $n = b-a$
- There $\exists k \in \mathbb{Z}$ s.t. $b-a = k \cdot a$
  $a-b = (-k)n$
- Since $-k \in \mathbb{Z}$, $n \mid a-b$ $\therefore (b,a) \in R_n$.
- Thus, R_n is symmetric.

Transitive: suppose $(a,b) \in R_n$ and $(b,c) \in R_n$

- NTS: $(a,c) \in R_n$, $a \equiv c \bmod n$, $n \mid c-a$.
- Since $(a,b) \in R_n$, $n \mid b-a$
- Since $(b,c) \in R_n$, $n \mid c-b$
- Since $n \mid b-a$ and $n \mid c-b$,
  $n \mid (b-a)+(c-b) = c-a$
- So, $(a,c) \in R_n$ $\therefore$ R_n is transitive.

$[x]_n = \{\ldots, x-2n, x-n, x, x+n, x+2n, \ldots\}$ (equivalence class of $x \bmod n$ = $[x]_n$)

Ex: What is the equivalence class of 2 with respect to congruence modulo 5?

- $[2] = \{x \in \mathbb{Z} : (x,2) \in R\}$
  $\therefore x \equiv 2 \bmod 5 \Rightarrow x \bmod 5 = 2 \bmod 5 = 2$
  $\therefore [2] = \{\ldots -8, -3, 2, 7, 12, \ldots\}$ (−5, −5; +5, +5)

Equivalence Classes

- Let R be an equivalence relation on A.
- Let $a \in R$

$[a] = \{x \in A : (x,a) \in R\}$

the subset of some equivalence relation R which includes all elements that are equivalent to each other.

- In the relation with parity, there are 2 equivalence classes.
  - $[0]$ - set of even numbers
  - $[1]$ - set of odd numbers

- Ex: $A = \{1,2,3,4,5\}$, $R = \{(a,b) : a+b \text{ is even}\}$

$[1] = \{1,3,5\}$ $[3] = \{1,3,5\}$ $[5] = \{1,3,5\}$

$[2] = \{2,4\}$ $[4] = \{2,4\}$

$[1] = [3] = [5] \neq [2] = [4]$ ∴ there are only 2 equivalence classes

---

- Theorem: Let R be an equivalence relation on A
  1. If $(a,b) \in R$, $[a] = [b]$
  2. If $[a] = [b]$, $(a,b) \in R$
  3. $(a,b) \notin R$, $[a] \cap [b] = \emptyset$
  4. $\bigcup_{a \in A} [a] = A$

↳ union of all equivalence classes

Proof:

① $(a,b) \in R$ NTS: $[a] = [b]$

(⇒) - Let $x \in [a]$ NTS: $[a] \subseteq [b]$ → $x \in [b]$
- Then $(a,x) \in R$
- R is symmetric so $(x,a) \in R$. → $(b,x) \in R$
- $(x,a) \in R$ and $(a,b) \in R$
  so by transitivity, $(x,b) \in R$,
  by symmetry, $(b,x) \in R$.
- So, $x \in [b]$
- Thus $[a] \subseteq [b]$ NTS: $[b] \subseteq [a]$ → $y \in [a]$

(⇐) - Let $y \in [b]$, so $(b,y) \in R$. → $(a,y) \in R$
- Since $(a,b) \in R$ and $(b,y) \in R$, $(a,y) \in R$,
- Hence, $y \in [a]$
- So $[b] \subseteq [a]$

Therefore $[a] = [b]$.

② $[a] = [b]$ NTS: $(a,b) \in R \rightarrow b \in [a]$

- By reflexivity $a \in [a]$, $b \in [b]$.
- $b \in [b] \Rightarrow b \in [a]$ because $[a] = [b]$
- Since $b \in [a]$, $(a,b) \in R$ □

④ $\bigcup_{a \in A} [a] = A$

- Let $x \in A$, then $x \in [x]$
- So, $x \in \bigcup_{a \in A} [a]$
- Therefore $A \subseteq \bigcup_{a \in A} [a]$
- $[a] = \{b \in A \mid (a,b) \in R\} \subseteq A$,
  so $\bigcup_{a \in A} = A$

③ $(a,b) \notin R$, $[a] \cap [b] = \emptyset$

We'll prove the contrapositive $(x \Rightarrow y = \neg y \Rightarrow \neg x)$

- If $[a] \cap [b] \neq \emptyset$, $(a,b) \in R$.
- Let $x \in [a] \cap [b]$.
- So $(a,x) \in R$ and $(b,x) \in R$
- By symmetry, $(x,b) \in R$
- By transitivity, since $(a,x) \in R$ and $(x,b) \in R$, $(a,b) \in R$ □

---

16. Partitions

- Let R be an equivalence relation on a set A.
- The equivalence classes of R form a partition of the set of A

(Partition) Let A be a set. A partition of (or on) A is a set of nonempty pairwise disjoint sets whose union is A.

① A partition is a set of sets: each member of a partition is a subset of A. The members are called parts.

② The parts of a partition are nonempty.

③ The parts of a partition are pairwise disjoint. No two sets of a partition may have any element in common.
- if $[a] \neq [b]$, $[a] \cap [b] = \emptyset$

④ The union of the parts is the original set.

$\bigcup_{[a] \in A} [a] = A$

(Counting Equivalence Classes) Let R be an equivalence class on a finite set A. If all the equivalence classes of R have the same size, m, then the number of equivalence classes is $\frac{|A|}{m}$.

17. Binomial Coefficients — Fri, Sep 20

Pascal's Triangle

			1				$n=0$
		1		1			$n=1$
	1		2		1		$n=2$
1		3		3		1	$n=3$
	1		4		6		1	$n=4$
1		5		10		10		5		1	$n=5$

(Binomial Coefficient): $\binom{n}{k} = {}_nC_k$
= "n choose k"

- number of ways of choosing k elements from a set of n elements (if the order doesn't matter)
- number of k-element subsets of an n-element set

(Pascal's Identity): $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k(k-1)(k-2)\cdots(2)(1)}$ → enforces an order
→ to remove ordering

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

Why is it true that:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \; ?$$

Newton's Binomial Theorem

Ex. $(a+b)^5 = (a+b)(a+b)(a+b)(a+b)(a+b)$

↓

two choices when expanding

$\therefore 2^5 = 32$

↓

sum of row $n=5$ of Δ

Proving Pascal's Identity:

- Let n, k be nonnegative integers with $k+1 \leq n$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Algebraic Proof:

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

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

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

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

Combinatorial Proof:

- Let's count the number of subsets of $\{1, 2, \ldots, n+1\}$ with $k+1$ elements
  - ① it's $\binom{n+1}{k+1}$
  - ② Consider whether the subsets have $n+1$ or not.
    - There are $\binom{n}{k}$ subsets that contain $n+1$.
    - There are $\binom{n}{k+1}$ subsets that don't contain $n+1$.

(Theorem) Let $0 \leq k \leq n$ are integers
Then $\binom{n}{k} = \binom{n}{n-k}$

Proof: Algebraic

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

same! ←

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

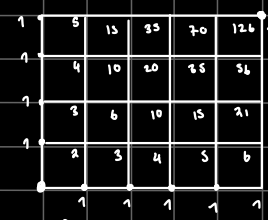
Proof: Combinatorial

- If you choose a subset with k elements of $\{1, 2, \ldots, n\}$
- It's complement is a subset with $n-k$ elements.

e.g. the # of subsets of $\{1,2,3,4,5\}$ with 2 elements = # of subsets with 3 elements.

Counting Lattice Paths:

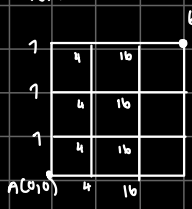
① How many paths from A → B if you can only move → ↑ ? N-E lattice path



- to get to B, you need 5 right arrows & 4 up arrows, in total 9 arrows.
- $\binom{9}{4}$

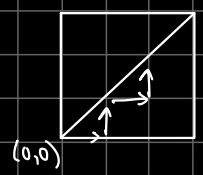
- In general, the number of paths from (0,0) to (n,k) is $\binom{n+k}{n}$ or $\binom{n+k}{k}$ → this is because once we choose the N's, the E's are given, and vice versa.

② Now what if we allow → ↑ ↓, but you can't repeat a vertex?



- In general : $(b+1)^a$

③ Now, you can't cross the diagonal, only → ↑.
↳ Dyck Path



(Catalan number : C_n) number of paths from (0,0) to (n,n) with only → ↑.

Note, you can never have more ↑'s than →'s.

$\frac{1}{n+1}\binom{2n}{n}$

Poker Hands:

- Deck has 52 numbers, 13 numbers, 4 suits.
- Pair : same number
- 3-of-a-Kind : same number
- 4-of-a-Kind : same number
- Full House : 3-of-a-Kind + Pair
- Straight : 5 consecutive numbers
- Flush : 5 in same suit
- Straight Flush : Straight + Flush

1. How many poker hands?

$\binom{52}{5}$

2. How many poker hands are there with just one pair?

$\underbrace{\binom{13}{1}\binom{4}{2}}_{\text{pair}}\underbrace{\binom{12}{3}\binom{4}{1}\binom{4}{1}\binom{4}{1}}_{\text{last three}}$

3. How many poker hands are there with two pairs?

$\underbrace{\binom{13}{2}\binom{4}{2}\binom{4}{2}}_{\text{two pair}}\underbrace{\binom{11}{1}\binom{4}{1}}_{\text{last one}}$

4. How many poker hands are there with three of a kind? ↗ and not a full house

$\underbrace{\binom{13}{1}\binom{4}{3}}_{\text{three of a kind}}\underbrace{\binom{12}{2}\binom{4}{1}\binom{4}{1}}_{\text{last two}}$

5. How many poker hands are there with four of a kind?

$\underbrace{\binom{13}{1}\binom{4}{4}}_{\text{four of a kind}}\underbrace{\binom{12}{1}\binom{4}{1}}_{\text{last one}}$

6. How many poker hands are a full house?

$\underbrace{\binom{13}{1}\binom{4}{3}}_{\text{three of a kind}}\underbrace{\binom{12}{1}\binom{4}{2}}_{\text{pair}}$

7. How many poker hands are a straight flush?

$10 \times \binom{4}{1} = 40$

↓ from A 2 3 4 5
⋮
10 J Q K A

8. How many poker hands are a flush? ↗ but not a straight

$\binom{13}{5}\binom{4}{1} - 40$

9. How many poker hands are a straight? ↗ but not a flush

$10 \times \binom{4}{1}^5 - 40$ ← suit selection

10. How many poker hands are a royal flush?

$\underbrace{\binom{4}{1}}_{\text{suit}}\underbrace{\binom{5}{5}}_{\text{royalty}} = 4$

22. Induction

- We have some statement that depends on a variable n which is a positive integer.
  $S(n)$.
- NTS: $S(n)$ is true $\forall n \geq n_0$.

- Steps:
  1. Prove $S(n_0)$ is true. ← Base case
  2. Prove $S(k)$ implies $S(k+1)$ → Inductive step
  - You can conclude that it's true $\forall n \geq n_0$.

Ex: Prove $1+2+\dots+n = \frac{n(n+1)}{2}$ for some $n \geq 1$

Base case: $n=1$

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1 \quad \square$$

Inductive hypothesis:
- Suppose $1+2+\dots+k = \frac{k(k+1)}{2}$ for some $k \geq 1$. (1)

Inductive step: (NTS) $1+2+\dots+k+(k+1) = \frac{(k+1)(k+2)}{2}$

- Adding $k+1$ to both sides of (1):

$$1+2+\dots+k+(k+1) = \frac{k(k+1)}{2} + (k+1)$$
$$= \frac{k^2+k+2k+2}{2}$$
$$= \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2} \quad \square$$

Ex: Hockey Stick Identity

$$\binom{r}{r} + \binom{r+1}{r} + \dots + \binom{n}{r} = \binom{n+1}{r+1} \text{ for } n \geq r.$$

Base case: $n=r$

$$\binom{r}{r} = \binom{r+1}{r+1} \Rightarrow 1 = 1$$

Induction hypothesis:

- Suppose $\binom{r}{r} + \binom{r+1}{r} + \dots + \binom{k}{r} = \binom{k+1}{r+1}$

Inductive case:

NTS: $\underbrace{\binom{r}{r} + \binom{r+1}{r} + \dots + \binom{k}{r}}_{\binom{k+1}{r+1}} + \binom{k+1}{r} = \binom{k+2}{r+1}$

$\therefore \binom{k+1}{r+1} + \binom{k+1}{r} = \binom{k+2}{r+1} \quad \square$

Theorem: Let $n \in \mathbb{Z} : n \geq 0$
Then $2^n \geq 1+n$

Base case: $n=0$

$$2^0 \geq 1+0$$
$$1 \geq 1$$

Inductive hypothesis: Suppose $2^k \geq 1+k$

Inductive case: $2^{k+1} \geq k+2$

$\therefore \underbrace{2^k}_{\geq 1+k} 2 \geq k+2$

$(k+1)2 \geq k+2$

$2k+2 \geq k+2 \quad \forall k \geq 0 \quad \square$

Prove. $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$, for $n \geq 0$

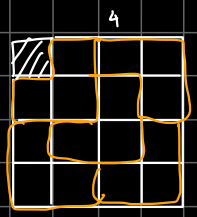
Base case: $n=0$

$$\frac{1}{2^0} \geq 1 + \frac{0}{2} \Rightarrow 1 \geq 1$$

Inductive hypothesis: Suppose $\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{2^k} \geq 1 + \frac{k}{2}$

Inductive case: $\underbrace{\frac{1}{1} + \frac{1}{2} \dots + \frac{1}{2^k}}_{\geq 1 + \frac{k}{2}} + \frac{1}{2^{k+1}} \geq 1 + \frac{k+1}{2} \geq 1 + \frac{k}{2} + \frac{1}{2}$

$$1 + \frac{k}{2} + \frac{1}{2^{k+1}} \geq 1 + \frac{k}{2} + \frac{1}{2}$$
$$\frac{1}{2^{k+1}} \geq \frac{1}{2} \quad \forall k \geq 0 \quad \square$$

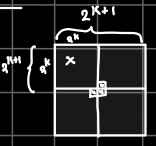


Theorem: Let $n \geq 1$. A $2^n \times 2^n$ grid with a unit square removed can be tiled with L-triominoes.

Base case: $n=1$

Inductive hypothesis: Suppose any $2^k \times 2^k$ grid with a square removed can be tiled with L-triominoes.

Inductive step:



Prove: $f_1 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$

$1, 1, 2, 3, \ldots$

$$f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Base case: $n = 1$

$$f_1 = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1}{\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1$$

$n = 2$

$$f_2 = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}} = \frac{\frac{6+2\sqrt{5}}{4} - \frac{6-2\sqrt{5}}{4}}{\sqrt{5}} = \frac{\frac{4\sqrt{5}}{4}}{\sqrt{5}} = 1$$

Inductive hypothesis:

Suppose $f_K = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^K - \left(\frac{1-\sqrt{5}}{2}\right)^K}{\sqrt{5}}$

and $f_{K+1} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{K+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{K+1}}{\sqrt{5}}$

Induction case:

NTS: $f_{K+2} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{K+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{K+2}}{\sqrt{5}}$

$f_{K+2} = f_K + f_{K+1}$

$$\therefore f_{K+2} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^K - \left(\frac{1-\sqrt{5}}{2}\right)^K}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{K+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{K+1}}{\sqrt{5}}$$

(Proposition) Let n be a positive integer. Then

$2^0 + 2^1 + \ldots + 2^{n-1} = 2^n - 1$

Proof.

- **Base case:** $n = 1 \Rightarrow 2^{1-1} = 2^1 - 1 \Rightarrow 2^0 = 2 - 1 = 1$
- **Induction hypothesis:** Suppose $2^0 + 2^1 + \ldots + 2^{K-1} = 2^K - 1$ (1)
- **Induction case:** NTS $2^0 + 2^1 + \ldots + 2^{K-1} + 2^K = 2^{K+1} - 1$

Adding 2^K to both sides of (1):

$2^0 + 2^1 + \ldots + 2^{K-1} + 2^K = 2^K - 1 + 2^K$

$= 2 \cdot 2^K - 1 = 2^{K+1} - 1$ □

(Proposition) Let n be a natural number.

Then $4^n - 1$ is divisible by 3.

(Proof) For each n, let $P(n)$ be the statement $3 \mid 4^n - 1$

- **Base case:**
  - $P(0)$ is true because $4^0 - 1 = 0 = 0 \cdot 3$
- **Inductive hypothesis:**
  - Suppose $P(k)$ is true $\forall k = n$:
  - $3 \mid 4^k - 1 \therefore 4^k - 1 = 3m$ for some $m \in \mathbb{Z}$.

    $\therefore 4^k = 3m + 1$ (1)
- **Inductive case:**
  - We must show that $4^{k+1} - 1$ is also divisible by 3.
  - Multiply both sides of eq. (1) by 4:

    $4 \cdot 4^k = 4(3m+1)$

    $4^{k+1} = 12m + 4$
  - Subtract 1 from both sides:

    $4^{k+1} - 1 = 12m + 3$

    $4^{k+1} - 1 = 3(4m+1) = 3n$ where $n = 4m+1$
  - Thus $P(k+1)$ is true.
- Therefore, $P(n)$ is true $\forall n \in \mathbb{N}$. □

Chicken McNugget Theorem:

- If a and b are positive integers such that $\gcd(a, b) = 1$ (i.e., relatively prime)
- Then any number $n > ab - a - b + 1$ can be written as $ax + by$ with $(x, y) \in \mathbb{Z} : x \geq 0, y \geq 0$.

- Let $a = 4$, $b = 9$
- $24 = 6 \cdot 4$
- $25 = 4 \cdot 4 + 1 \cdot 9$
- $26 = 2 \cdot 4 + 2 \cdot 9$
- $27 = 0 \cdot 4 + 3 \cdot 9$
- $28 = 7 \cdot 4$
- $29 = 5 \cdot 4 + 1 \cdot 9$
- $30 = 3 \cdot 4 + 2 \cdot 9$
- $31 = 1 \cdot 4 + 3 \cdot 9$
- $32 = 8 \cdot 4$
- $33 = 6 \cdot 4 + 1 \cdot 9$
- $34 = 4 \cdot 4 + 2 \cdot 9$
- $35 = 2 \cdot 2 + 3 \cdot 9$
- $36 = 9 \cdot 4$

largest number we can't write in the form $ax + by$ is $ab - a - b$

If $n = 4a + 9b$

Then, $n + 4 = 4(a+1) + 9b$

5-step induction

$n \to n + 5$

Base cases:

$S(1), S(2), \ldots, S(5)$

$\therefore$ By 4-step induction, every number ≥ 24 can be written as $4a + 9b$ with $a, b \geq 0$.

- So, what's the largest amount of nuggets we can't buy with boxes of 4 and 9?

$n = 4 \cdot 9 - 4 - 9 + 1$

$= 36 - 4 - 9 + 1 =$

Strong Induction:

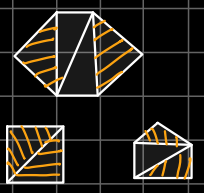
1. Base case:
   - $S(n_0)$ is true
2. Strong induction hypothesis:
   - Suppose $S(m)$ is true for all $n_0 \leq m \leq k$.
3. Induction step:
   - Show $S(k+1)$ is true.

(Fundamental Theorem of Arithmetic):
- Any positive integer $n \geq 1$ can be factored as a product of primes in a unique way up to ordering.

- We'll prove that they can all be factored, we want prove factorization is unique.

Proof:
- $P(2)$ is true because 2 is itself a prime.
- Assume $P(k)$ is true $\forall k : 2 \leq k \leq n$.
- We need to prove $P(k+1)$, i.e, $k+1$ has a prime factorization
- Consider $k+1$, there are 2 cases:
  1. If $k+1$ is prime:
     - Then $k+1$ is already expressed as a product of prime factors (itself), and $P(k+1)$ holds.
  2. If $k+1$ is composite:
     - Then $\exists\, a, b \in \mathbb{Z}^+$ such $2 \leq a, b \leq k$ and $k+1 = a \times b$
     - By the inductive hypothesis, $P(a)$ and $P(b)$ are true.
     - Therefore, $a = p_1 \times p_2 \times \ldots \times p_m$ and $b = q_1 \times q_2 \times \ldots \times q_n$ where p_i and q_j are prime.
     - Hence $k+1 = a \times b = (p_1 \times p_2 \times \ldots \times p_m)(q_1 \times q_2 \times \ldots \times q_n)$
     - This expresses $k+1$ as a product of prime factors, proving $P(k+1)$.
- By the principle of strong induction, $P(n)$ holds for all integers $n \geq 2$ $\therefore$ every positive integer greater than 1 can be expressed as a product of prime factors.

- Any polygon can be triangulated
- An external triangle is a triangle in the triangulation that uses two sides.



- (Theorem): Any triangulation of a polygon with $n \geq 4$ sides has at least 2 external triangles.

- Strong induction hypothesis: Suppose any triangulation of an n-sided polygon has at least 2 ext. triangles.
- Induction case:
  - Take a $k+1$ sided polygon. Triangulated, the triangulation consists of drawing diagonals.
  - Since $k+1 > 4$, it must have at least one diagonal.
  - Isolate a diagonal d.

  - Case 1:
    - A or B is a triangle. The other one has at least 4 sides.
    - The one with 4 sides by S.I.H has at least 2 external sides.
  - Case 2: A and B have at least 4 sides

20. Proof by Contradiction

↗ if a claim is about something "not" being something else

- If we want to prove an "If A, then B" statement.
- Direct proof: Assume A is true, prove B is true.
- Contrapositive: Assume B is false, prove B is false.
- Contradiction: Assume A is true and B is false ($\neg B$ is true)

↓

① Assume $\neg p$
② Find contradiction $p \wedge \neg p$
③ Claim $\neg\neg p = p$

- Then you reach a contradiction.
- "reductio ad absurdum"
- which proves B was to be true.

(Theorem) There are infinitely many primes

Proof: Suppose, for the sake of contradiction, there are finitely many primes.

- Let $p_1, p_2, \ldots, p_n$ be the complete list of primes.
- Let $N = p_1 p_2 \ldots p_{n+1}$
- $N > p_1, p_2, \ldots, p_n$ so N is not prime because it can be factored as a product of primes.
- Let p be a prime divisor of N.
- Then $p = p_i$ for some $i = 1, 2, \ldots, n$
- So $p \mid p_1 p_2 \ldots p_n$ and $p \mid N = p_1 p_2 \ldots p_{n+1}$
- So $p \mid N - p_1 p_2 \ldots p_n = 1$ ↯
- Thus, our assumption that there are infinitely many primes is false. □

(Theorem) $\sqrt{2}$ is irrational

Note: A number is rational if it can be written as a ratio (fraction) of two integers.

Proof:

- Assume, for contradiction, that $\sqrt{2} = \frac{p}{q}$ where p and q are integers in lowest terms.
- In particular, both p and q cannot be even.
- Square both sides: $2 = \frac{p^2}{q^2}$
- Multiply by q^2: $2q^2 = p^2$
- p^2 is even, so p is even (since odd · odd = odd)
- Let $p = 2k$
- Substitute: $2q^2 = (2k)^2 = 4k^2$
- q^2 is even, so q is even.
- Both p and q are even, contradicting that they're in lowest terms. ↯
- Thus, $\sqrt{2}$ cannot be rational and must be irrational. □

Prove that $(A-B) \cap (B-A) = \emptyset$

1. Assume, for contradiction, that $(A-B) \cap (B-A) \neq \emptyset$
2. This means $\exists x$ such that $x \in (A-B) \cap (B-A)$
3. So, $x \in A-B$ and $x \in B-A$
4. $x \in (A-B)$ means $x \in A$ and $x \notin B$
5. $x \in (B-A)$ means $x \in B$ and $x \notin A$
6. From steps 4 and 5, we have:
   - $x \in A$ and $x \notin A$
   - $x \in B$ and $x \notin B$ ↯ 0
7. Both statements in step 6 are contradiction.
8. Therefore, our initial assumption must be false and we conclude that $(A-B) \cap (B-A) = \emptyset$.

(Theorem) No integer is both even and odd.

Proof:

1. Assume, for contradiction, that $\exists n \in \mathbb{Z}$ that is both even and odd.
2. This means $n = 2k$ and $n = 2m+1$ for some integers k, m.
3. Therefore, $2k = 2m+1$
4. Subtracting 2m from both sides:
   $2k - 2m = 1$
   $2(k-m) = 1$
   $k-m = \frac{1}{2}$
5. Since $k-m$ is the subtraction of integers, $\frac{1}{2}$ is an integer. ↯ 0
6. Therefor, our initial assumption must be false and we conclude that no integer is both even and odd.

(Theorem) e is irrational

Recall, $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \ldots = \sum_{k=0}^{\infty} \frac{1}{k!}$

Proof:

1. Assume, for contradiction, that $e = \frac{p}{q}$ where p and q are integers in lowest terms
2. Multiply by $q!$:
   $e \cdot q! = \frac{p \cdot q!}{q}$
   $e \cdot q! = p \cdot (q-1)!$
3. Since p and q are integers, $e \cdot q!$ is an integer.
4. $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{(q-1)!} + \frac{1}{q!} + \frac{1}{(q+1)!} + \ldots$
   $e \cdot q! = \underbrace{q! + q! + \frac{q!}{2!} + \frac{q!}{3!} + \ldots + \frac{q!}{q!}}_{} + \frac{q!}{(q+1)!} + \ldots$

- $\sqrt{2}$ is a root of x^2-2
- $\sqrt[3]{2}$ is a root of x^3-3
- i is a root of x^2+1

when α is a root of a polynomial with integer coefficients, we say α is **algebraic**.

- If there is no polynomial with integer coefficients with root α, we say α is **transcendental**.

- **Examples**: e (proved in 1850s), π (proved in 1880s (Hermite)), Liouville's number (first to be discovered (1840s))
  - proved that if α is algebraic,
  - e^{α} is not algebraic

---

21. Smallest Counter-Example

Steps:
1. Negation: Assume the formula fails for some smallest K.
2. Base case: Verify the base case (typically $n=1$)
3. Use the assumption for $n=K-1$
   - Since K is the smallest counterexample, the theorem must hold for all values $n < K$, including $n=K-1$.
4. Express the quantity for $n=K$ using $n=K-1$.
5. Simply the expression and check if it contradicts the assumption that the theorem fails at K.
6. Contradiction: Since we have shown that the proposition holds for $n=k$, this contradicts the assumption that the theorem fails at the smallest counterexample K. Therefore, no such smallest counterexample can exist.

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

Theorem: For all $n \in \mathbb{N}$:

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

Proof:

- Assume $S(n)$ is false for some $n \in \mathbb{N}$. Let K be the smallest counterexample such that:

$$S(K) \neq 1+2+\dots+K = \frac{K(K+1)}{2} \quad (1)$$

- $S(1)$ holds because $1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$, so $K > 1$.
- Since K is the smallest counterexample, $S(K-1)$ holds such that:

$$S(K-1) = 1+2+\dots+(K-1) = \frac{(K-1)K}{2}$$

- Notice that

$$S(K) = S(K-1)+K$$
$$= \frac{(K-1)K}{2} + K$$
$$= \frac{(K-1)K}{2} + \frac{2K}{2}$$
$$S(K) = \frac{K(K-1+2)}{2} = \frac{K(K+1)}{2}$$

contradicting (1) ↯ □.

(Well-Ordering Principle): If S is a non-empty subset of $\mathbb{N}$, then S has a smallest element.

(Theorem) Division Algorithm.

Let a and b be integers

Then, there exist unique integers q, r such that

① $a = bq + r$

② $0 \leq r < b$

Proof:

- Suppose $b \nmid a$.
- Let $S = \{ x \in \mathbb{N} \mid x = a - bq \text{ for } q \in \mathbb{Z} \}$
- S is non-empty because $a \in S$.
- $S \subseteq \mathbb{N}$.
- By WOP, there is a smallest element r in S.
- $r = a - bq$ so $a = bq + r$
- Assume, for contradiction, that $r \geq b$.
- Now, consider $r-b$.
- Since $b \nmid a$, $r - b \neq 0$ so $r-b>0$ so $r-b \in \mathbb{N}$
- $r - b < r$, so $r-b \notin S$.
- If $r = a - bq \Rightarrow r-b = a - bq - b$
  $= a - b(q+1)$
- so $r-b \in S$ ↯
- so $r < b$.

- We proved existence, now let's prove uniqueness.
- Assume, for contradiction that $a = bq_1 + r_1$ with $0 \leq r_1 < b$ and $a = bq_2 + r_2$ with $0 \leq r_2 < b$ with $(q_1, r_1) \neq (q_2, r_2)$
- $bq_1 + r_1 = bq_2 + r_2$
  $b(q_1 - q_2) = r_2 - r_1$
  so $b \mid r_2 - r_1$
- Since $0 \leq r_1 < b$ and $0 \leq r_2 < b$,
  $-b < r_2 - r_1 < b$
- so $r_2 - r_1 = 0$

- so $r_2 = r_1$
- Therefore, $bq_1 + r_1 = bq_2 + r_2$
  $bq_1 = bq_2$
  $\therefore q_1 = q_2$

(Euclidean Algorithm)

Let a, b be positive integers.

$$\log_2 n \begin{cases} a = bq_1 + r_1 & 0 < r_1 < b \\ b = r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ \vdots & \\ r_{n-2} = r_{n-1} q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} + 0 & \end{cases}$$

$r_n \rightarrow \gcd(a,b)$

(Bezout's Identity): Given $a, b \in \mathbb{N}$, there exist $(x,y) \in \mathbb{Z}$ such that

$$ax + by = \gcd(a,b)$$

(Euclid's Lemma): If $p \mid ab$ where p is prime, $(a,b) \in \mathbb{N}$, then, $p \mid a$ or $p \mid b$.

(Proposition) Every natural number is even or odd.

$P(n) = \forall n \in \mathbb{N}$, n is even or odd.

Proof:

- Assume, for contradiction, that $P(n)$ is false.
  Let k be the smallest counterexample such that:
  $\exists k \in \mathbb{N}$, k is neither even nor odd
  i.e., $k \neq 2m$ or $k \neq 2m+1$ where $m \in \mathbb{Z}$.
- $P(1)$ holds because $1 = 2(0)+1$, so $k > 1$.
- Since k is the smallest counterexample, assume $P(k-1)$ holds s.t:
  $\exists k-1 \in \mathbb{N}$, $k-1$ is either odd or even.
- If $k-1$ is odd: $k-1 = 2m+1$
  $k = 2m+2 = 2(m+1)$
  so k is even ↯ (k is neither even or odd)
- If $k-1$ is even: $k-1 = 2m$
  $k = 2m+1$
  so k is odd ↯ (k is neither even or odd).
- Either way, we have a contradiction. Therefore
  $\forall n \in \mathbb{N}$, n has to be even or odd. □

(Proposition) Every $n \geq 2$ is a product of one or more primes

(Proof):

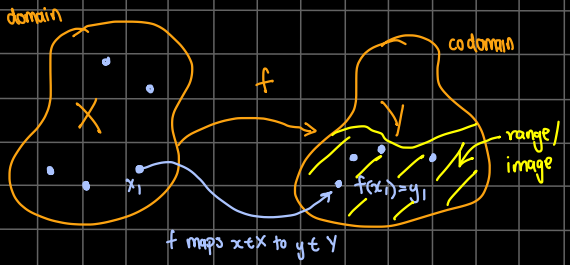
- Assume, for contradiction, that $P(n)$ is false.
  Then, let k be the smallest counterexample s.t:
  $\exists k \geq 2$ that is not a product of primes.
  So, $k = a \cdot b$ where $1 < a, b < k$
- $P(2)$ holds because 2 is itself a prime. So $k > 2$.
- k is the smallest counterexample so $P(n)$ holds for $2 \geq n > k$.
- Since $1 < a, b < k$, $P(a)$ and $P(b)$ hold.
  That is, a and b are a product of primes
- Since $k = a \cdot b$, k is a product of primes ↯
- Thus, $\forall n \geq 2$, n is a product of primes. □

2.4. Functions:

- $f: X \xrightarrow{\text{maps}} Y$ (domain: X, codomain: Y)
- f is a function from X to Y if
  - $\forall x \in X$ there exists a unique $y \in Y$ s.t. $f(x) = y$.
    OR
- A relation f is called a function provided
  $(a,b) \in f$ and $(a,c) \in f \Rightarrow b = c$

Vertical line test

range/image $= \{y \in Y : f(x) = y\}$



Examples:

1. $f(x) = x^2$
   Notice that this is a $f: \mathbb{R} \rightarrow \mathbb{R}^+$
   - $f(2) = 4$ & $f(-2) = 4$
   - codomain $= \mathbb{R}^+$

   Range: $\{x^2 \mid \sqrt{x}$ is an integer$\}$
   - $3 \notin$ im f.

Useful Functions to Know:

Characteristic Function:

$$f(x) = \begin{cases} 0 & \text{if } x \notin A \\ 1 & \text{if } x \in A \end{cases}$$ like thumb tacks

$f: \mathbb{R} \rightarrow \{0,1\}$

Identity Function:

- $id_A: A \rightarrow A$
  where $id_A(a) = a$ → example: $f(x) = x$

Floor & Ceiling Functions:

Floor: $f(x) = \lfloor x \rfloor$ → $\lfloor 2.xyz \rfloor = 2$

Ceiling: $f(x) = \lceil x \rceil$ $\lceil 2.xyz \rceil = 3$,

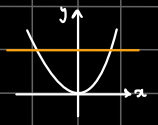
Injective, Surjective & Bijective Functions:

Injective: $f: X \to Y$ is injective (one-to-one)
if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
or if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$
↓ every value in the range corresponds to exactly one element in the domain.
no two inputs can share an output.
horizontal line test

Examples:

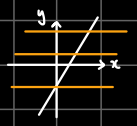
1. $f: \mathbb{R} \to \mathbb{R}$
$f(x) = 2x+1$
$f(x) = f(y) \Rightarrow 2x+1 = 2y+1 \Rightarrow x = y$ ∴ f is 1-1.

---

2. Is $f(x) = x^2$ injective?


- Suppose $f(a) = f(b)$
$a^2 = b^2$
$\pm a = \pm b$
- Let $a = 2$ and $b = -2$.
- So $f(a) = f(2) = 4$
$f(b) = f(-2) = 4$.
- Thus $f(a) = f(b)$ but $a \neq b$ ∴ $f(x) = x^2$ is not injective. □

---

3. Show $f(x) = 3x-2$ is injective.


NTS $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
- Direct: Suppose $f(a) = f(b)$
$3a-2 = 3b-2$
$3a = 3b$
∴ $a = b$ □ injective

Surjective: $f: X \to Y$ is onto or surjective
iff $\forall y \in Y, \exists x \in X$ s.t. $f(x) = y$.
im(f) = codomain of f (range)
every element in the codomain maps to at least one element in the domain.

- Examples:

1. $f: \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x+1$, is f onto?
- NTS $\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}$ s.t. $f(x) = y$
- That is, $y = 2x+1$
- Rearranging: $x = \frac{y-1}{2}$
- $x \notin \mathbb{Z}$ $\forall x = 2k$ for some $k \in \mathbb{Z}$ (x has to be odd)
- Since even integers are not in the image of f, f is not onto (the codomain has to = the image)

2a. Show $f(x) = 5x+2$ is surjective when $f: \mathbb{R} \to \mathbb{R}$
- NTS $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}: 5x+2 = y$
- Solving for x: $x = \frac{y-2}{5}$
- Since $y \in \mathbb{R}$, $x \in \mathbb{R}$ because subtraction & division by a non-zero constant (5) preserves real numbers. □

b. What about when $f: \mathbb{Z} \to \mathbb{R}$?
- In this case, $x = \frac{y-2}{5} \notin \mathbb{Z}$ $\forall y \in \mathbb{R}$
- For example, if $y = 3$, $x = \frac{1}{5} \notin \mathbb{Z}$.
- Thus $\exists y \in \mathbb{R}$ s.t. $\nexists x \in \mathbb{Z}$ with $f(x) = y$.
when $f: \mathbb{Z} \to \mathbb{R}$, f is not surjective.

c. What is the image of f?
- $\text{Im}(f) = \{ y \in \mathbb{R} \mid y \equiv 2 \bmod 5 \}$

d. What about when $f: \mathbb{R} \to \mathbb{Z}$
- NTS $\forall y \in \mathbb{Z}$, $\exists x \in \mathbb{R}$ s.t. $f(x) = 5x+2$
- $x = \frac{y-2}{5}$
- Since $y \in \mathbb{Z}$ and subtraction, and division by a non-zero constant (5) yields a real number, $x \in \mathbb{R}$ and f is onto □.

Bijective: A function is bijective (one-to-one correspondence) if it is both injective & surjective.
- For $f: X \to Y$, each $x \in X$ maps to exactly one unique $y \in Y$.
- As a result $|X| = |Y|$

Function Proofs:

- $f: A \to B$

1. Is f 1-1?
① To prove: Assume $f(x) = f(y)$
Prove $x = y$
② To disprove: Find $x \neq y$ s.t. $f(x) = f(y)$

2. Is f onto? → 1. let $f(x) = y$ 2. find $y = f^{-1}(x)$ 3. range of y 4. check range = codom
① To prove: Let $b \in B$
Find $a \in A$ s.t. $f(a) = b$.
② To disprove: Find $b \in B$ s.t. there is no $a \in A$ with $f(a) = b$.

Inverse Functions:

- Let f be a bijection from set A to B
- The inverse of f, f^{-1}, is the function from $B \to A$ defined as $f^{-1}(y) = x$ iff $f(x) = y$.
- In order for a function to be invertible, it must be a bijection.

(Theorem): Let $f: A \to B$
$f^{-1}: \text{Im} f \to A$
f^{-1} is a function iff f is 1-1.

(=>):
- Let's prove if f is not 1-1, then f^{-1} is not a function.
- $\exists a_1, a_2 : a_1 \neq a_2$ s.t. $f(a_1) = f(a_2) = b$.
- So $(a_1, b), (a_2, b) \in f$.
- Thus, $(b, a_1), (b, a_2) \in f^{-1}$.
- Since $a_1 \neq a_2$, f^{-1} is not a function.

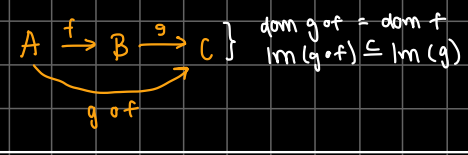
(<=):
- Suppose f is 1-1. WTS: f^{-1} is a function.
- Suppose $(b, a_1), (b, a_2) \in f^{-1}$.
- (Goal): Show $a_1 = a_2$.
- Therefore $(a_1, b), (a_2, b) \in f$.
- $f(a_1) = b$, $f(a_2) = b$, so $f(a_1) = f(a_2)$.
- Since f is 1-1, $a_1 = a_2$.

---

26. Composition:

- $f: A \to B$
- $g: B \to C$
- $g \circ f: A \to C$ — $g \circ f$ is defined if $\text{dom}(f) \subseteq \text{codom}(g)$ i.e.) $(A \subseteq C)$

where $g \circ f(a) = g(f(a))$



$\text{dom } g \circ f = \text{dom } f$
$\text{Im}(g \circ f) \subseteq \text{Im}(g)$

(Theorem) If $f: A \to B$ and $g: B \to C$ are injective (1-1) functions, then $g \circ f$ is injective.

(Proof): Suppose $g \circ f(a) = g \circ f(b)$. NTS $a = b$,
- $g(f(a)) = g(f(b))$
- Since g is 1-1, $f(a) = f(b)$ ← we can cancel out the functions, leaving the inputs
- Since f is 1-1, $a = b$. □

(Theorem) If $f: A \to B$ and $g: B \to C$ are surjective (onto) functions, then $g \circ f$ is onto.

(Proof): $g \circ f: A \to C$
- Let $c \in C$. NTS $\exists a \in A$ s.t. $g(f(a)) = c$.
- Since g is onto, $\exists b \in B$ s.t. $g(b) = c$.
- Since f is onto, $\exists a \in A$ s.t. $f(a) = b$
- So $g \circ f(a) = g(f(a)) = g(b) = c$. □

(Theorem) $f: A \to B$, $g: B \to C$, $h: C \to D$
Then,
$h \circ (g \circ f) = (h \circ g) \circ f$

(Proof): NTS: 1. $\text{dom}(h \circ (g \circ f)) = \text{dom}((h \circ g) \circ f)$
2. $h \circ (g \circ f)(a) = (h \circ g) \circ f(a)$

1. $\text{dom}(h \circ (g \circ f)) = \text{dom}(g \circ f) = \text{dom}(f)$
$\text{dom}((h \circ g) \circ f) = \text{dom}(f)$ ✓

2. $h \circ (g \circ f)(a) = h(g(f(a)))$ ✓
$(h \circ g) \circ f(a) = h \circ g(f(a))$
$= h(g(f(a)))$ ✓

- Suppose f and f^{-1} are bijections, $f: A \to B$, $f^{-1}: B \to A$.
$f \circ f^{-1} = id_B$
$f^{-1} \circ f = id_A$

↓ if functions (i.e., f is not onto), then $f^{-1}: \text{Im}(f) \to A$
$\therefore f \circ f^{-1} = \text{Im} f$

Counting Functions:

- $A = \{1, a_1, \ldots, n\}$
- $B = \{1, a_1, \ldots, m\}$

in a function, every element in the domain maps to something in the codomain.

① How many functions $f: A \to B$ exist?

$f(1)$ has m possibilities
$f(a_1)$ has m "
$f(n)$ has m "

$\Big\}\ m^n$ //

$|B|^{|A|}$ — options ↓, elements to map ↓

② How many 1-1 functions $f: A \to B$?

$f(1)$ has m
$f(a_1)$ has $m-1$
⋮
$f(n)$ has $(m-n)+1$

$\Big\}\ \binom{m}{n} \cdot n!$ if $m \geq n$ (map n elements onto m elements; ways of arranging)

0 if $m < n$ (we don't have enough elements in the domain to map to every element in the codomain.)

③ How many onto functions $f: A \to B$? → inclusion-exclusion

all functions − functions that aren't onto

$$m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n - \binom{m}{3}(m-3)^n + \ldots (-1)^m \binom{m}{m}(m-m)^n$$

$\binom{m}{1}$: each missing value; $(m-1)^n$: missing a value; $\binom{m}{2}$: pair; $\binom{m}{3}$: triple

$$\sum_{k=0}^{m-1} (-1)^k \binom{m}{k} (m-k)^n = \begin{cases} 0 & \text{when } m > n \\ n! & \text{when } m = n \end{cases}$$

- (Theorem) Let A, B be finite sets and $f: A \to B$.
- If 2 of the following 3 are true, the third is also true.
  1) $|A| = |B|$
  2) f is one-to-one
  3) f is onto

1. Prove ①+② ⇒ ③:
   - Let $A = \{a_1, a_2, \ldots a_n\}$
   - $f(a_1) = b_1$
   - $f(a_2) = b_2$
     ⋮
     $f(a_n) = b_n$.
   - Since f is 1-1, $b_1, b_2, \ldots b_n$ are all distinct
   - $\{b_1, b_2, \ldots b_n\} \subseteq B$.
   - But $|B| = |A| = n$
     and $|\{b_1, b_2, \ldots, b_n\}| = n$
   - so $B = \{b_1, b_2, \ldots, b_n\}$.
   - Take $b \in B$ so $b = b_i$ for some i.
   - Then $f(a_i) = b_i$, so f is onto.

2. Prove ①+③ ⇒ ②:
   - Let $B = \{b_1, b_2, \ldots, b_n\}$, so $|B| = n$
   - Since f is onto for each b_i, there exists $a_i \in A$ such that $f(a_i) = b_i$.
   - From the definition of a function, $a_1, a_2, \ldots, a_n$ are all distinct.
   - $\{a_1, a_2, \ldots, a_n\} \subseteq A$
   - $|\{a_1, a_2, \ldots, a_n\}| = n = |A|$
   - So, $A = \{a_1, a_2, \ldots, a_n\}$.
   - Suppose $f(x) = f(y)$ so $x = a_i$ for some i
     $y = a_j$ for some j.
   - $f(x) = b_i$, $f(y) = b_j$ so $b_i = b_j \Rightarrow i = j \Rightarrow a_i = a_j$ so f is 1-1.

3. Prove ②+③ ⇒ ①:
   - Let $A = \{a_1, a_2, \ldots a_n\}$.
   - Let $b_1 = f(a_1) \in B$.
     $b_2 = f(a_2) \in B$
     ⋮
     $b_n = f(a_n) \in B$
   - Since f is 1-1, $b_1, b_2, \ldots, b_n$ are all distinct.
   - We know f is onto, so there is no other output.
   - So $B = \{b_1, b_2, \ldots, b_n\}$
   - $|A| = n = |B|$

25. Pigeonhole Principle:

if A & B are finite sets and $|A| > |B|$, there can be no 1-1 functions $f: A \to B$

- If you have $n+1$ pigeons flying towards n pigeonholes, at least 2 pigeons will share a pigeonhole.

Generalized Pigeonhole Principle:

- Given n items and k boxes, if $m > n$, there is at least one box with $\lceil \frac{n}{k} \rceil$ items.

Examples:

1. 25 students, 12 months

- $\lceil \frac{25}{12} \rceil = \lceil 2.xyz... \rceil = 3$

∴ At least 3 people have a birthday in 1 month.

---

2. 50,000 people, 366 possible birthdays (n)

- $\lceil \frac{50{,}000}{366} \rceil = \lceil 136.xyz... \rceil = 137$

∴ At least 137 people share a birthday.

---

3. Show that at a party at least 2 people have the same number of acquaintances.

- Ex: 7 people

0, 1, 2, 3, 4, 5, 6 } 7 options

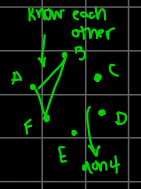
↓ Know noone ↓ Know everyone => can't both exist

∴ there are actually only 6 options.

---

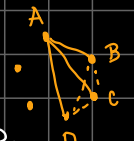
4. Given 6 people at a party, show you can find either
   a) 3 of them that all know each other,
   b) 3 of them that don't know each other.

Ramsey Number $R(3,3) = 6$

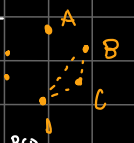


Proof:

1. First, let's model this:
   - Let's represent people as vertices.
   - An edge between two people means they know each other, no edge means they don't.
   - So, we're looking for either: a) A triangle (3 mutual edges) or b) an anti-triangle (3 vertices with no edges between them.)
2. Let's focus on one person, call them A.
   - Looking at the other 5 people, each of these 5 must either know or not know A.
   - By pigeonhole, at least $\lceil \frac{5}{2} \rceil = 3$ people either know or don't know A.
3. Let's consider the cases:
   - Case 1: 3 know A (call them B, C, D)
     - Now look at edges between B, C, and D.
       - If any 2 of them know each other, we get a triangle ABC or ABD or ACD.
       - If none of them do, we get an anti-triangle BCD.



   - Case 2: 3 don't know A (call them B, C, D)
     - If any 2 don't know each other, we get an anti-triangle ABC or ACD.
     - If all 3 know each other, we get triangle BCD.



4. In either case:
   - We find 3 people who all know each other or 3 people who don't. □

---

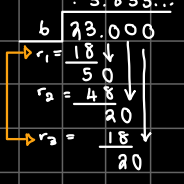
5. Suppose we have 5 points in the plane with integer coordinates
   - Show there is a point with integer coordinates in at least one segment connecting the original 5 points.
   - I'll show that the midpoint of at least one pair has integer coordinates.
     - $m = \left(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2} \right)$
     - For $m \in \mathbb{Z}$, x_1+x_2 and y_1+y_2 need to be even. Thus, x_1 and x_2 need to have the same parity. Same for y_1 and y_2.
     - For each midpoint (x_1+x_2, y_1+y_2) can be (even, even), (even, odd), (odd, odd), or (odd, even). So 4 possibilities.
     - From the pigeonhole principle, there are at least $\lceil \frac{5}{4} \rceil = 2$ coordinates with the same parity.

---

6. Rational numbers are numbers of the form $\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$.
   - Prove that every rational number must have a repeating decimal representation.

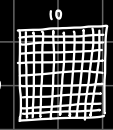
Proof:

- Given a rational number $\frac{a}{b}$, when we perform long division, we multiply the remainder and divide by b. Each step gives us the next digit and a new remainder.



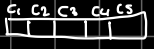
- When dividing by b, the possible remainders are $0, 1, 2, \ldots, b-1$. So there are only b possibilities.
- After $b+1$ steps of long division, we have $b+1$ remainders but since there are only b possibilities, some remainder must repeat (by pigeonhole principle).
- When a remainder repeats, the next digits will be the same as what came after the first occurrence.
- Thus, every rational number must have a repeating decimal expansion. □

7. Given a 10×10 chessboard and 41 rooks, prove you can find 5 rooks that are not attacking each other.

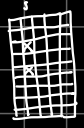


Proof:

- Since we have 41 rooks and 10 rows, one row has at least $\lceil \frac{41}{10} \rceil = 5$ rooks. This is the row with the most rooks.
  - Let's call this row R_5
- Each of the 5 rooks are in a different column.
  - Mark the C_1, C_2, C_3, C_4, C_5.



- Now we remove R_5 and consider the sub board:
  - So, now we have a 9×5 board with 36 rooks.
  - 45 spaces, 36 rooks, so 9 squares must be empty. By pigeonhole, 1 columns must have at least $\lceil \frac{9}{5} \rceil = 2$ empty spaces



① - Choose 1 of these empty spaces and remove the row.

- Now, we have a 8×5, so 40 spaces, 32 rooks
  - So there are 8 empty spaces. So one row has at least $\lceil \frac{8}{5} \rceil = 2$ empty spaces, choose 1. ②
- 7×5 → 35 spaces, 28 rooks, 7 empty. So, 1 row has at least $\lceil \frac{7}{5} \rceil = 2$ empty, choose 1. ③
- 6×5 → 30 spaces, 24 rooks, 6 empty. So, 1 row has at least $\lceil \frac{6}{5} \rceil = 2$ empty, choose 1. ④
- 5×5 → 25 spaces, 20 rooks, 5 empty. So, 1 row has at least $\lceil \frac{5}{5} \rceil = 1$ empty, choose it ⑤
- We've chosen 5 empty spaces in different rows and columns, essentially selecting 5 non attacking rooks □.

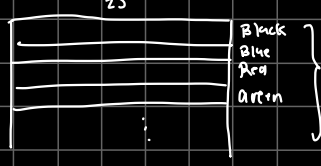
---

8. Given a 21×25 chessboard with an integer written on each square, show there is a rectangle (with width, length ≥ 2) in the board, whose 4 corner numbers sum to a multiple of 4.

Proof:

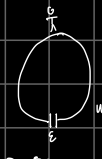
- We will color a square black if it's a multiple of 4, Blue if it's 1 mod 4, Red if 2 mod 4, Green if it's 3 mod 4.
- If we find a rectangle with corners of the same color, when we add them up, we will get a multiple of 4.

- We have 4 colors, so by pigeonhole, 1 color appears at least 7 times.



- There is a color that appears as the "winner" in the most rows. By pigeonhole, it will be the winner in at least 6 rows.

9.



step size = α, $\alpha \notin \mathbb{Q}$

hole size $\varepsilon > 0$

- Prove that the person will fall through eventually.
- Proof:
  - We need to find i and j such that $|\{(j-i)\alpha\}| < \varepsilon$
    - $\{a.a\} = 0.a$
  - $\varepsilon > 0$, $\lim_{n\to\infty} \frac{1}{n} = 0$ so $\exists N \in \mathbb{N}$ s.t. $\frac{1}{N} < \varepsilon$.

- N arcs of the circle.
- If you have N+1 steps, 2 of them land on the same arc.
- Since $\alpha \notin \mathbb{Q}$, two step sizes can't fall on the same point: $i\alpha = N_i + \{i\alpha\}$

$$j\alpha = N_j + \{j\alpha\}$$
$$(j-i)\alpha = N_j - N_i$$
$$\therefore \alpha = \frac{N_j - N_i}{j-i} \in \mathbb{Q}$$

---

10. Let $S = \{1, 2, \ldots, 20\}$

- If we pick 11 numbers, we are guaranteed that the sum of two picked numbers is 21.
- Pairs that equal 21:

$$\left.\begin{matrix}(1,20), (2,19), (3,18), (4,17), (5,16), \\ (6,15), (7,14), (8,13), (9,12), (10,11)\end{matrix}\right\} \text{10 pairs}$$

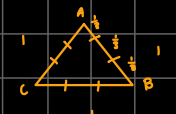
- Suppose you pick the first number in each pair such that none of the numbers you choose sum up to 21:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

- You've picked 10 numbers, so you need to pick 1 more. No matter which number you pick, you'll complete a pair that sums to 21. □

---

11. Let $\triangle ABC$ be an equilateral triangle with $AB = 1$. Show that by selecting 10 points on the perimeter, there are at least two with distance $\leq \frac{1}{3}$ apart.



Proof:

- If we divide the perimeter into sections of length $\frac{1}{3}$, we get 9 sections (including vertices A, B, C).
- By pigeonhole, at least $\lceil \frac{10}{9} \rceil = 2$ points must be in the same section.
- For two points in the same section, their arc length distance $\leq \frac{1}{3}$. □

(Erdős-Szekeres): Let n be a positive integer. Every sequence of n^2+1 distinct integers must contain a monotone subsequence of length $n+1$.

Cardinality:

- The cardinality of a set A, denoted by $|A|$ is the number of elements in A when A is a finite set.

- For infinitite sets:
  - Let A and B be sets.
  - $|A| = |B|$ if there exists a bijection $f: A \to B$
  - $|A| \leq |B|$ if there exists a 1-1 function $f: A \to B$.
  - $|A| \geq |B|$ if there exists an onto function $f: A \to B$.

---

1. Let's show $|2\mathbb{Z}| = |\mathbb{Z}|$:

$f: \mathbb{Z} \to 2\mathbb{Z}$, $f(n) = 2n$.

injective:	surjective:
$f(a) = f(b)$	Let $y = f(x)$
$2a = 2b$	$x = \frac{y}{2}$
$a = b$	$f(x) = \frac{2y}{2} = y$ □

---

2. Show $|\mathbb{N}| = |\mathbb{Z}|$

$$f: \mathbb{N} \to \mathbb{Z}: \quad 1 \to 0,\ 2 \to 1,\ 3 \to -1$$

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{1-n}{2} & \text{if } n \text{ is odd} \end{cases}$$

- Prove $f(n)$ is bijective:

- Injectivity: Suppose $f(a) = f(b)$
  - Case 1: both odd
    - $\frac{1-a}{2} = \frac{1-b}{2}$
    - $1-a = 1-b$
    - $a = b$.
  - Case 2: both even:
    - $\frac{a}{2} = \frac{b}{2}$
    - $a = b$
  - Case 3: different parity
    - $\frac{a}{2} = \frac{1-b}{2}$
    - $a = 1-b$
    - $a+b = 1$ $\Rightarrow\Leftarrow$ $a, b \in \mathbb{N}$ so $a+b \geq 1+1 = 2$
    - So $f(a) \neq f(b)$
  - Therefore, f is injective. □

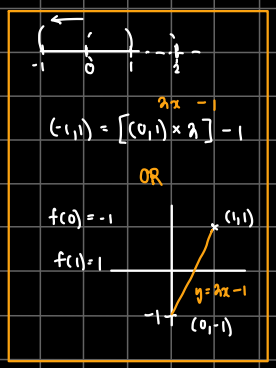
- Surjectivity. Let $y = f(x)$
  - Case 1: x is even
    - $y = \frac{x}{2}$
    - $x = 2y$
    - $f(2y) = \frac{2y}{2} = y$
  - Case 2: x is odd
    - $y = \frac{1-x}{2}$
    - $x = 1+2y$
    - $f(1+2y) = \frac{1-1-2y}{2} = y$
  - Therefore, f is surjective. □

---

3. Show $|(0,1)| = |(-1,1)|$

$f: (0,1) \to (-1,1)$

$f(x) = 2x-1$



- Injective: Suppose $f(a) = f(b)$
  - $2a-1 = 2b-1$
  - $2a = 2b \Rightarrow a = b$ □
- Surjective: Let $y = f(x)$
  - $y = 2x-1$
  - $x = \frac{y+1}{2}$ $\quad f\left(\frac{y+1}{2}\right) = \frac{2(y+1)}{2} - 1 = y$
  - NTS $\frac{y+1}{2} \in (0,1)$:
    - So $0 < \frac{y+1}{2} < 1$
    $0 < y+1 < 2$
    $\therefore\ -1 < y < 1$ □

(Theorem) Two open intervals have the same cardinality

i.e., $|(a,b)| = |(c,d)|$

- $f(a) = c$
- $f(b) = d$

$\Big\}$ $(a,c) \longleftrightarrow (b,d)$, $m = \frac{d-c}{b-a}$

(Proof): $f(x) = \left(\frac{d-c}{b-a}\right)x + \left[c - \left(\frac{d-c}{b-a}\right)a\right]$

$f(a) = \left(\frac{d-c}{b-a}\right)a + c - \left(\frac{d-c}{b-a}\right)a = c$

$f(b) = \left(\frac{d-c}{b-a}\right)b + c - \left(\frac{d-c}{b-a}\right)a = c + \frac{d-c}{b-a}(b-a)$

Injective: Suppose $f(r) = f(s)$

- $\frac{d-c}{b-a} \cdot r + c - a\frac{d-c}{b-a} = \frac{d-c}{b-a} \cdot s + c - a\frac{d-c}{b-a}$

$\frac{d-c}{b-a} \cdot r = \frac{d-c}{b-a} \cdot s$

- Since $b-a > 0$ and $d-c > 0$, we can multiply by both sides.
- Thus: $r = s$ □

(Theorem): Equality of cardinality is an equivalence relation.

(Proof): We need to prove the relation is reflexive, symmetric, and transitive.

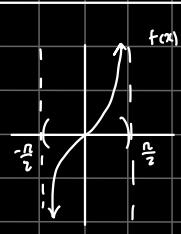
- Reflexive: Let A be a set. NTS $|A| = |A|$
  - Take $f: A \to A$ defined by $f(x) = x$.
  - $f(a) = f(b)$: $a = b$ □ injective
  - Let $y = x$. □ surjective.

- Symmetric: Suppose $|A| = |B|$, NTS $|B| = |A|$
  - $f: A \to B$ is a bijection. NTF $g: B \to A$.
  - Take $g: B \to A$ defined by $g = f^{-1}$.
  - Since f is a bijection, f^{-1} is also a bijection
  - So, $|B| = |A|$ □

- Transitive: Suppose $|A| = |B|$ and $|B| = |C|$, NTS $|A| = |C|$
  - There is a bijection $f: A \to B$.
  - There is a bijection $g: B \to C$.
  - Then, $g \circ f : A \to C$ is a bijection. □

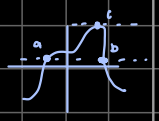
---

4. Show $|(-\frac{\pi}{2}, \frac{\pi}{2})| = |\mathbb{R}|$



- $f: (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$
  defined by $f(x) = \tan(x)$
- Injective:
  - Suppose $\tan(a) = \tan(b)$ for some $a, b \in (-\frac{\pi}{2}, \frac{\pi}{2})$.
  - For contradiction, assume $a \neq b$, and $a < b$.
  - $\tan(x)$ is cont. on $[a, b]$ and diff. on (a, b)
  - By Rolle's Theorem, $\exists c \in (a, b)$ such that $f'(c) = 0$.
  - $f'(c) = \sec^2(c) = 0$
    $\tan(x)$ is increasing on $(-\frac{\pi}{2}, \frac{\pi}{2})$
  - Since our assumption that $a \neq b$ led to a contradiction, we conclude $a = b$.
  - Thus, f is injective.

Rolle's Theorem:
- If f is cont. on $[a, b]$ and f is diff on (a, b), and $f(a) = f(b)$, $\exists c \in (a, b)$ s.t. $f'(c) = 0$.



- Surjective:
  - Let $y = f(x)$ $\therefore y = \tan x$
    $x = \tan^{-1}(y)$ $\therefore f(\tan^{-1}(y)) = \tan(\tan^{-1}(y)) = y$ □

Countable:

- A set A is countable if $|A| = |\mathbb{N}| = \aleph_0$ [aleph not] → smallest infinity
- A set is countable if there is a bijection between that set and the natural numbers.

---

1. Show that $\{0, 2, 4, 6, 8\}$ is countable.

NTS: $\{0, 2, 4, 6, 8, \ldots\} \mapsto \{0, 1, 2, 3, \ldots\}$

$2n \mapsto n$

$n \mapsto \frac{n}{2}$

$\therefore f(n) = \frac{n}{2}$

Verifying Bijectivity:

1. Injectivity:
   - Suppose $f(a) = f(b)$
     $\frac{a}{2} = \frac{b}{2}$ $\therefore a = b$ $\therefore$ f is injective. □

2. Surjectivity:
   - Let $y = f(x)$
     $y = \frac{x}{2}$ $\therefore x = 2y$
   - $f(2y) = \frac{2y}{2} = y$ $\therefore$ f is surjective. □

---

2. Show that $\{1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \ldots\}$ is countable.

Let $S = \{1, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \ldots\}$

Let $f: \mathbb{N} \mapsto S$

$\therefore f(n) = \frac{1}{n^2}$

Injectivity:
- Suppose $f(a) = f(b)$
  $\frac{1}{a^2} = \frac{1}{b^2}$
  $a^2 = b^2 \Rightarrow a = b$ $\therefore$ f is injective. □

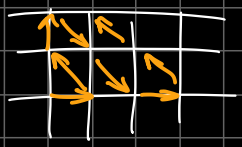
Surjectivity:
- Let $y = f(x)$
  $\therefore y = \frac{1}{x^2}$
  $x = \pm\frac{1}{\sqrt{y}}$
- $f(\pm\frac{1}{\sqrt{y}}) = y$ $\therefore$ f is surjective.

(Theorem) If A and B are countable, then $A \cup B$ is countable

(Proof):
- Since A and B are countable, we can write $A = \{a_1, a_2, \ldots\}$ and $B = \{b_1, b_2, \ldots\}$
- Thus, $A \cup B = \{a_1, b_1, a_2, b_2, \ldots\}$
- If $A \cap B \neq \emptyset$, don't list duplicates.

(Theorem) If A and B are countable, $A \times B$ is countable.

(Proof):
- $A = \{a_1, a_2, \ldots\}$
- $B = \{b_1, b_2, \ldots\}$
- $A \times B = \{(a_1, b_1), (a_2, b_2)$

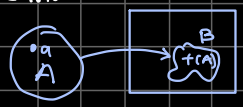


(Theorem) $|2^{\mathbb{N}}| > |\mathbb{N}|$ ← Cantor's Theorem

(Proof): $|2^{\mathbb{N}}| = |\mathbb{R}|$
so $|\mathbb{R}| \neq |\mathbb{N}|$
↓ $\mathbb{R}$ is uncountable.

Cantor's Theorem:

- Recall, $|A| \leq |B|$ if there exists $f: A \to B$ that is one-to-one. Equivalently, if there exists $g: B \to A$ that is onto.
- $f: A \to B$ is 1-1
- $g: B \to A$ $\quad g(x) = \begin{cases} f^{-1}(x) & \text{if } x \in \text{im}(f) \\ a & \text{if } x \notin \text{im}(f) \end{cases}$



- $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$

(Cantor's Theorem): $|A| < |2^A|$

Rephrase: there exist no onto functions from A to 2^A.

To show $|A| \leq |2^A|$ is easy:

- $f: A \to 2^A$
  $f(a) = \{a\}$

Example: $A = \{1, 2, 3\}$

$f(1) = \{1\}$
$f(2) = \{2\}$
$f(3) = \{3\}$

$2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

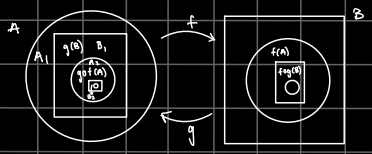
Prove $|A| \neq |2^A|$:

- Assume, for contradiction, that they have the same size.
  $\therefore |A| = |2^A|$.
- Let $f: A \to 2^A$.
- Let's show that f is not onto. [let's create a set $\notin$ im(f)]
- Let $B = \{x \in A \mid x \notin f(x)\}$
- Claim: $B \notin \text{im}(f)$
  - Suppose, for contradiction, that $B \in \text{im}(f)$.
  - So, $\exists\, a \in A$ s.t. $f(a) = B$
  - Is $a \in B$?
    - If $a \in B$, then $a \notin f(a) = B$ ↯
    - If $a \notin B$, then $a \notin f(a)$, so $a \in B$. ↯
- Thus, $|A| < |2^A| < |2^{2^A}| < \ldots$

Cantor-Bernstein-Schroeder Theorem:

(Theorem) If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$

(Proof): We have $f: A \to B$ that is 1-1.
We have $g: B \to A$ that is 1-1.
Goal: Find a bijection $h: A \to B$.



- $A_1 = A - g(B)$
- $B_1 = g(B) - g \circ f(A)$
- $A_2 = g \circ f(A) - g \circ f \circ g(B)$
- $B_2 = g \circ f \circ g(B) - g \circ f \circ g \circ f(A)$

- $A_{n+1} = g \circ f(A_n)$
- $B_{n+1} = g \circ f(B_n)$

- Let $C = A_1 \cup A_2 \cup \ldots$
  $D = A - C$
- $h(x) = \begin{cases} f(x) & \text{if } x \in C \\ g^{-1}(x) & \text{if } x \in D \end{cases}$ $\qquad h: A \to B$

- Claim: h is a bijection
  - Injectivity: Suppose $h(a) = h(b)$
    - Case 1: $a, b \in C$
      - $h(a) = h(b) \Rightarrow f(a) = f(b)$
      - f is 1-1 $\therefore a = b$.
    - Case 2: $a, b \in D$
      - $h(a) = h(b) \Rightarrow g^{-1}(a) = g^{-1}(b)$
      - g is 1-1 $\therefore a = b$.
    - Case 3: $a \in C$, $b \in D$
      - $h(a) = h(b) \Rightarrow f(a) = g^{-1}(b)$
      - $a \in C$, so $a \in A_i$ for some i
      - $\Rightarrow g \circ f(a) \in A_{i+1}$ (apply g to both sides)
      - $g \circ f(a) = b \in A_{i+1} \Rightarrow b \in C$ ↯
  - Surjectivity: NTS $\forall b \in B, \exists\, a \in A$.
    - Let $b \in B$.
    - Let $E = f(A_1) \cup f(A_2) \cup \ldots$
      $F = B - E$
    - If $b \in E$:
      - $b \in f(A_i)$ for some i, so $\exists\, a \in A_i$ s.t. $f(a_i) = b$.
      - So, $h(a_i) = f(a_i) = b$
    - If $b \in F$:
      - $b \notin f(A_i)$ for any i.
      - So, $g(b) \notin g \circ f(A_i)$ so $g(b) \notin A_{i+1}$.
      - $A_1 = A - g(B)$ so $g(b) \notin A_1$.
      - So $g(b) \in A_1 \cup A_2 \cup \ldots \Rightarrow g(b) \in D$
      - Thus, $h(g(b)) = g^{-1}(g(b)) = b$, so $b \in \text{im}(h)$.
      - Therefore, h is onto □.

(Corollary) $|(0,1)| = |(0,1]|$

- We showed that $|(0,1)| = |\mathbb{R}|$.

Proof:

- We know $|(0,1]| \leq |\mathbb{R}|$ since $f(x) = x$ where $f: (0,1] \to \mathbb{R}$
- Since $|(0,1)| = |\mathbb{R}|$, $|\mathbb{R}| \leq |(0,1)|$

$\therefore |(0,1)| = |(0,1]|$.

(Theorem) $|\mathbb{R}| = |2^{\mathbb{N}}|$

Proof: We'll show $|(0,1]| = |2^{\mathbb{N}}|$

- Let $f: 2^{\mathbb{N}} \to (0,1]$

$f(A) = \sum_{a \in A} \frac{1}{2^a}$ → $f(\emptyset) = 0$, $f(\mathbb{N}) = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 1$

- Claim: f is onto.
  - Let $x \in (0,1]$
  - WTS: $\exists A \in \mathbb{N}$ s.t. $f(A) = x$.

$x = 0.b_1b_2b_3\dots$

Example: $x = 0.001001001\overline{001}_2$

$= \frac{1}{2^3} + \frac{1}{2^6} + \frac{1}{2^9} + \frac{1}{2^{12}} + \dots$

$A = \{3, 6, 9, 12, \dots\}$

$f(A) = \frac{1}{2^3} + \frac{1}{2^6} + \frac{1}{2^9} + \frac{1}{2^{12}} + \dots = x$

  - So f is onto.
- Thus, $|2^{\mathbb{N}}| \geq |(0,1]|$

- Now, consider $g: 2^{\mathbb{N}} \to (0,1]$

$g(A) = \sum_{a \in A} \frac{1}{10^a}$

- $g(\{1,2,3\}) = 0.111$

$g(\{3,4,6\}) = 0.0011101$

- Thus, g is 1-1
- So, $|2^{\mathbb{N}}| \leq |(0,1]|$
- Since $|2^{\mathbb{N}}| \geq |(0,1]|$ and $|2^{\mathbb{N}}| \leq |(0,1]|$,

$|2^{\mathbb{N}}| = |(0,1]|$

Using the Cantor-Bernstein-Schroeder Theorem, prove $|2^{\mathbb{N}}| = |\mathbb{R}|$.

- $f: 2^{\mathbb{N}} \to (0,1]$

$f(A) = \sum_{a \in A} \frac{1}{2^a}$ (e.g. $f(\{2,5,6\}) = 0.010011$)

- $g: (0,1] \to 2^{\mathbb{N}}$

$g(A) = \sum_{a \in A} \frac{1}{10^a}$

$0.0101110011\dots$

$= 0.1011001$

- $A_1 = A - g(a)$, where a is the smallest that ends with $\{n, n+1, \dots\}$
- $A_2 = g$ of (A_1)

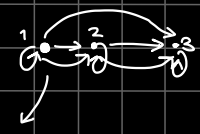
§4. Fundamentals of Partially Ordered Sets

- A partially ordered set is a pair $P = (X, R)$ (ground set, partial order relation) where X is a nonempty set and R is a relation on X that satisfies the following conditions:
  - R is reflexive: $\forall x \in X,\ x R x$.
  - R is antisymmetric: $\forall x, y \in X,\ x R y$ and $y R x \Rightarrow x = y$.
  - R is transitive: $\forall x, y, z \in X$, if $x R y$ and $y R z$, then $x R z$.

---

1. $X = \{1,2,3\}$, $R = \{(x,y) \mid x \leq y\}$

$R = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$



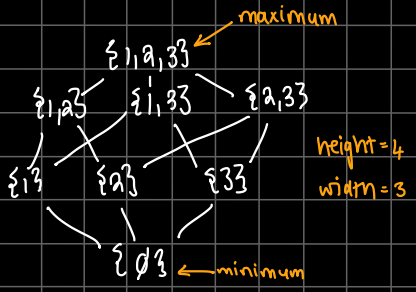
  - Since R is reflexive, we don't have to draw the loops.
  - Since R is transitive, we don't have to draw 1R3.
  - The result is a Hasse Diagram:
    - If $x R y$ in the poset, we draw y above x.

Total Order →

---

2. $X = 2^{\{1,2,3\}} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

$R = \{(x,y) \mid x \subseteq y\}$



Definitions:

- Suppose $P = (X, \preceq)$ ("is below") is a poset.

(Incomparable): $a, b \in X$ are called incomparable if $a \not\preceq b$ and $b \not\preceq a$. ($a \not\parallel b$) (they are not connected by a path that respects the order.)

(Chain): $C \subseteq X$ is a chain if for any $a, b \in C$, a, b are comparable.

(Anti-chain): $A \subseteq X$ is an antichain if for any $a, b \in A$, a, b are incomparable.

(Height): The height of P is the maximum size of a chain. (depth-first)
- It is also the longest path from the minimals to the maximals.

(width): The width of P is the maximum size of an antichain. (breadth-first)

width = max (longest antichain at each level)

comparable	$\lessgtr$
incomparable	$\not\lessgtr$
below	$\preceq$
above	$\succeq$

55. Max and Min

(Maximum): An element $m \in X$ is a maximum if for every $x \in X$, $x \leq m$.

(Minimum): An element $m \in X$ is a minimum if for every $x \in X$, $m \leq x$.

(Maximal): An element $m \in X$ is maximal if for every x that is comparable to m, $x \leq m$. (no successor)

(Minimal): An element $m \in X$ is minimal if for every x that is comparable to m, $m \leq n$. (no predecessor)

---

1. $X = \{1, 2, \dots, 50\}$
   $R = \{(x,y) : x \mid y\}$

   maximals = 26, 50 → for any number x, $m > x$ if $m \geq 2x$.
   minimum = 1
   height = 6
   width = 25

---

2. $X = \{1, 2, \dots, n\}$
   $R = \{(x,y) : x \mid y\}$

   height = $\lfloor \log_2 n \rfloor + 1$ (accounts for the 1)
   width = $\lceil \frac{n}{2} \rceil$
   maximals = $\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + 2, \dots \lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil$ (n of them)
   minimum = 1

(Theorem): Given a set with $n+1$ positive integers $\leq 2n$, at least two of them divide each other.

(Proof):

- Every positive integer can be written as:
  $m = 2^k \cdot b$ where b is odd.
- How many odd numbers are there between 1 and $2n$?
  $\frac{2n}{2} = n$
- By the pigeonhole principle, at least 2 numbers have the same odd part.
  $2^i \cdot b$ and $2^j \cdot b$
- If $i < j$ => $2^i b \mid 2^j b$.
- If $j < i$ => $2^j b \mid 2^i b$. ☒

---

3. $X = 2^{\{1, 2, \dots, n\}}$
   $R = \{(x,y) : x \subseteq y\}$

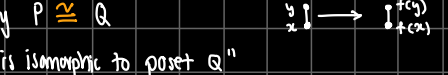
   height = $n+1$
   width = $\binom{n}{\lfloor \frac{n}{2} \rfloor}$
   maximum = $\{1, 2, \dots, n\}$
   minimum = $\emptyset$

---

56. Linear Orders

(Total / Linear Order): Let $P = (X, \leq)$ be a partially ordered set. We call P a total or linear order provided P does not contain incomparable elements.

(Isomorphic): We say $P \cong Q$ ("poset P is isomorphic to poset Q") if:



1. there exists a bijection $f: P \to Q$ (isomorphism → bijective invertible.)
2. the bijection f is "order-preserving" such that $\forall x, y \in P$, $x \leq_P y \iff f(x) \leq_Q f(y)$

---

1. Given $f: P \to Q$ (isomorphism)
   Prove x is a minimum in P iff $f(x)$ is a minimum in Q.

Proof:

(=>) Suppose x is minimum in P. (NTS: $f(x) \leq_Q z \ \forall z \in Q$)

1. By definition, $\forall y \in P$, $x \leq_P y$.
2. For any $z \in Q$, since f is surjective, $\exists y \in P$ such that $f(y) = z$.
3. By the isomorphism property of f, $\forall y \in P$, $f(x) \leq_Q f(y) = z$
4. Therefore $\forall z \in Q$, $f(x) \leq_Q z$, making $f(x)$ minimum.

(<=) Suppose $f(x)$ is minimum in Q. (NTS: $x \leq_P y \ \forall y \in P$)

1. By definition, $\forall z \in Q$, $f(x) \leq_Q z$
2. Let $z = f(y)$
3. Therefore $y = f^{-1}(z)$
4. Since f is an isomorphism, there exists an order preserving $f^{-1}: Q \to P$.
5. Applying f^{-1} to both sides of 1: $x \leq_P f^{-1}(z) = y$.
6. Since f^{-1} is surjective, this covers all the elements in P. □

For what n do we get a linear order?

$n = p^k$ for some prime p and nonnegative integer k.