Discrete Math Notes (MAT 215)

Dan Wysocki

Fall 2014

Contents

1 Fundamentals

1.1 Joy

1.2 Speaking (and Writing) of Mathematics

1.3 Definition

1.3.1 Integers ($\mathbb{Z}$)

Assumptions:

1) The existance of $\mathbb{Z}$
2) *"Closure properties" for addition, subtraction, and multiplication of $\mathbb{Z}$
3) We will assume the "ordering" of integers, i.e. we can relate integers by using $<$, $\leq$, $>$, and $\geq$.

* **Closure Properties**: $\mathbb{Z}$, is closed under addition, subtraction, and multiplication, i.e. if $p, q \in \mathbb{Z}$, then $p + q, p - q, p \cdot q \in \mathbb{Z}$

Note: $\mathbb{Z}$ are not "closed" with respect to division, e.g. $\frac{3}{2} = 1.5 \notin \mathbb{Z}$

Division: Let $a, b \in \mathbb{Z}$. We say a is divisible by b or that b divides a ($b \mid a$) provided there is an integer x such that $a = b \cdot x$, where a is the dividend, b is the divisor, and x is the quotient.

(1) Is 6 divisible by 3? Yes, because $6 = 3 \cdot 2$

(2) Is 0 divisible by 4? Yes, because $0 = 4 \cdot 0$

(3) Is 4 divisible by 0? No, because $4 \neq 0 \cdot x, x \in \mathbb{Z}$

Even: We say an integer is even, provided it is divisible by 2. i.e. a is even provided there is $x \in \mathbb{Z}$ such that $a = 2x$

(4) Is 0 even? Yes, because $0 = 2 \cdot 0$.

Odd: We say an integer a is odd, provided there is an integer x such that $a = 2x + 1$

(5) Show that 5 is odd. We show there is an integer x such that $5 = 2x + 1$. We know $5 = 2 \cdot 2 + 1$

Prime number: An integer $p > 1$ is said to be prime if it is not divisible by any number other than p and 1.

Composite number: blah

Less than: A natural number a is less than b if $a - b$ is a non-zero natural number

(6) How many positive divisors does each number have? List them all.

a. 8

   4 divisors: 1, 2, 4, 8

b. 32

   6 divisors: 1, 2, 4, 8, 16, 32

c. 2^n

   $n+1$ divisors: 2^0, 2^1, …, 2^n

d. 10

   4 divisors: 1, 2, 5, 10

e. $100 = (2 \cdot 5)^2$

   $3 \cdot 3 = 9$ divisors: $2^0 \cdot 5^0$, $2^0 \cdot 5^1$, $2^0 \cdot 5^2$, $2^1 \cdot 5^0$, $2^1 \cdot 5^1$, $2^1 \cdot 5^2$, $2^2 \cdot 5^0$, $2^2 \cdot 5^1$, $2^2 \cdot 5^2$

f. $1000000 = 10^6 = (2 \cdot 5)^6$

   $(6+1)(6+1) = 7 \cdot 7 = 49$ divisors

g. $10^n = (2 \cdot 5)^n$

   $(n+1)(n+1) = (n+1)^2$ divisors: $(2^0, \dots, 2^n)(5^0, \dots, 5^n)$

```python
#!/usr/bin/python
from sympy import *

def divisor_count(x):
    """Returns the number of divisors for a positive integer `x`"""
    prime_factors = primefactors(x)
    return (log(x, prod(prime_factors))+1)**(len(prime_factors))
```

1.4 Theorem

Theorem: A theorem is a declarative statement in mathematics for which there is a proof.

Proof: An essay that incontrovertibly shows that a statement is true.

Statements:

- If-then statement

  If A, then B, where A, B are conditions. $A \implies B$

  (7) If x, y are even integers, then $x + y$ is an even integer. (could also be stated as: The sum of two even integers is an even integer)

  (8) If you take your medicine (A), you will get well (B)

Condition A	Condition B	$A \implies B$?
True	True	True
True	False	False
False	True	True
False	False	True

- If and only if
  A if and only if B, denoted $A \iff B$
  if A then B **and** if B then A

Condition A	Condition B	$A \implies B$	$B \implies A$	$A \iff B$
True	True	True	True	True
True	False	False	True	False
False	True	True	False	False
False	False	True	True	True

  $A \iff B$ means A and B must either both be true or both be false

- Not A
  $\neg A$, $\sim A$

A	Not A
True	False
False	True

- And statement
  A and B, $A \wedge B$
- Or statement
  A or B, $A \vee B$

A	B	A and B	A or B
True	True	True	True
True	False	False	True
False	True	False	True
False	False	False	False

Theorem $\leftrightarrow$ Proposition $\leftrightarrow$ Result $\leftrightarrow$ Lemma $\leftrightarrow$ Corrolary $\leftrightarrow$ Claim

1.5 Proof

1.5.1 Proving If-Then Statements

Proposition 1: The sum of two even integers is an even integer.
Proof:

1) We want to show: If x, y are even integers, then $x + y$ is an even integer.
2) Let x, y be two even integers

3) a) Since x is even $\implies 2 \mid x$ (definition of even integer) $\implies$ there is an integer a such that $x = 2a$ (2) (definition of divisibility)

   b) Since y is even $\implies 2 \mid y \implies$ there is an integer b such that $y = 2b$ (1), for the same reasons as part a)

   c) Then, $x + y = 2a + 2b$ (from (1) and (2)) $= 2(a + b)$ (from dist. law for integers). Since a, b are integers $\implies a + b$ is also an integer (closure property of addition for $\mathbb{Z}$) $\implies 2 \mid x + y$ (by definition of divisibility)

4) $\implies x + y$ is an even integer

Framework/Template for a direct proof of an If-then statement.

1) Write the first sentence: "We want to show . . . " (If-then statement)

2) a) Write the *last* sentence (at this point, perhaps just in your head)

   b) Assume the *If* part. Instantiate appropriately.

3) "Unravel" the definition from both ends (imagine where you are going).

4) Connect to where you are going ("ravel" the definitions, "aha" moment, "insight")

5) Write the conclusion

Exercise: Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

1) We want to show: For $a, b, c \in \mathbb{Z}$, if $a \mid b$, $b \mid c$, then $a \mid c$.

2) a) $a \mid b \implies \exists x \in \mathbb{Z} : b = ax$ (1). (from definition of divisibility)

   b) $b \mid c \implies \exists y \in \mathbb{Z} : c = by$ (2). (same as above)

3) a) $c = (ax)y$ (3) (from (1) and (2)) $= a(x \cdot y)$

   b) $x, y \in \mathbb{Z} \implies x \cdot y = z \in \mathbb{Z}$ (from closure property of integers)

4) $\exists z \in \mathbb{Z} : c = az$

5) $\implies a \mid c$

1.5.2 Proving $\iff$ Statements

$A \iff B$ means If A, then B **AND** If B, then A.

Structure of proof

1) We want to show: $A \iff B$. We do this by showing $A \implies B$ and $B \implies A$.

2) Identify $A \implies B$, show $A \implies B$.

3) Identify $B \implies A$, show $B \implies A$.

4) Wrap-up, draw your conclusion.

5.14 and 5.22 are good example problems.

1.5.3 Perfect squares

Perfect Square: We say an integer s is a perfect square if there exists an integer $r : r^2 = s$.

(9) Let a be a perfect square. Prove that a is the square of a non-negative integer.

Consecutive Perfect Squares (e.g. 4 and 9, 25 and 36, 49 and 64) are of the form a^2 and $(a+1)^2$. Suppose r and s are consecutive perfect squares, then $\exists\ p, q \in \mathbb{Z} : p^2 = r$ and $q^2 = s$, then $\sqrt{s} - \sqrt{r} = q - p = 1$.

(10) Prove that the difference between distinct, non-consecutive perfect squares is composite.

w.t.s. if d is the difference between two distinct non-consecutive perfect squares, then d is composite.

Let a, b be two distinct non-consecutive perfect squares.

Since a and b are distinct, $a \neq b$.

Without loss of generality, assume $a < b$.

Since a, and b are non-consecutive perfect squares, $\sqrt{a}, \sqrt{b} \in \mathbb{Z}^+, \sqrt{b} - \sqrt{a} > 1$.

Since a, b are perfect squares, $\exists\ r, s \in \mathbb{Z}^+ : r^2 = a,\ s^2 = b$.

Let $d = b - a$, then $d = b - a = s^2 - r^2 = (s - r)(s + r)$.

Check: $s - r,\ s + r \in \mathbb{Z}^+$

Claim: $s - r$ and $s + r$ are both at least 2, so $s - r > 0$.

Since they are the square roots of two non-consecutive, distinct, perfect squares, then $s - r > 1$, so $s - r \geq 2$.

$s - r \geq 2 \implies s \geq r + 2 \implies s + r \geq 2r + 2 \geq 4$, so $s + r \geq 2$.

d has been written as a product of two factors, both of which are at least 2, which implies that both factors are less than d.

$\implies d = b - a$ is composite $(\exists\ t \in \mathbb{Z} : 1 < t < d : t \mid d)$.

1.6 Counter-examples

Statement: All cows are white

If-then statement: If x is a cow, then x is white.

This statement is false.

To disprove it, we show a cow that is not white. Such a cow should be called a counter-example.

Statement: All prime numbers are odd. This statement is false. 2 is a counter-example.

Statement: Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid a$, then $a = b$. False statement. Counter examples: 5 and -5, x and $-x\ \forall\ x \in \mathbb{Z}$.

6.2) If $a, b \in \mathbb{Z}, a, b \geq 0$ with $a \mid b$, then $a \leq b$. Counter-example: choose $b = 0$, and $a > b$.

6.3) Let $a, b, c > 0$ with $a \mid (bc)$, then $a \mid b$ or $a \mid c$. Counter-example: choose $a = 6$, $b = 3$, and $c = 4$.

6.6) If p is prime, then $2^p - 1$ is also prime. Counter-example: choose $p = 11$. p is prime, but $2^11 - 1 = 2047$ is composite. Some more counter examples include $p = 11, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 83, 97$

6.9) Consider the polynomial $n^2 + n + 41$.

a. Calculate the value of this polynomial for $n = 1, 2, 3, \ldots, 10$. Notice that all the numbers you computed are prime.

b. Disprove: If n is a positive integer, then $n^2 + n + 41$ is prime.

Counter-examples include $n = 41, 89, 109, 127$.

1.7 Boolean Algebra

Boolean algebra is a branch of algebra that deals with statements, rather than numbers. The value of the variables is either True or False.

3 main operations:

1) Conjunction/and (denoted by $\wedge$)
2) Disjunction/or (denoted by $\vee$)
3) Not/negation (denoted by $\neg$)

We define these operations as follows:

$x \wedge y$, read as x and y.

$x \vee y$, read as x or y.

$\neg x$, read as not x.

x	y	$x \wedge y$	$x \vee y$	$\neg x$
T	T	T	T	F
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Combining Boolean expressions:

$$\begin{aligned} T \wedge ((\neg F) \vee F) &= T \wedge (T \vee F) \\ &= T \wedge (T) \\ &= T \end{aligned}$$

Logically Equivalent expressions: Two expressions are logically equivalent if they have the same value for all possible values of the variables.

e.g. the expressions and $x \wedge y$ and $y \wedge x$ are logically equivalent, i.e. $x \wedge y = y \wedge x$.

Proposition 7.1: The Boolean expressions $\neg(x \wedge y)$ and $(\neg x) \vee (\neg y)$ are logically equivalent.

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

$\therefore \neg(x \wedge y) = (\neg x) \vee (\neg y)$.

Truth table proof of logical equivalence:

1) We want to show: Two Boolean expressions are logically equivalent.

2) Construct a truth table for all possible values of the variables.

3) Check to see that the value of the Boolean expressions are always equal.

Theorem 7.2:

- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

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

$\therefore x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

- $\neg(x \wedge y) = (\neg x) \vee (\neg y)$

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

$\therefore \neg(x \wedge y) = (\neg x) \vee (\neg y)$

Two more operations:

4) If x, then y: $x \implies y$

5) x if and only if y: $x \iff y$

x	y	$x \implies y$	$x \iff y$
T	T	T	T
T	F	F	F

x	y	$x \implies y$	$x \iff y$
F	T	T	F
F	F	T	T

Proposition 7.3: $x \implies y$ and $(\neg x) \vee y$ are logically equivalent.

x	y	$x \implies y$	$\neg x$	$(\neg x) \vee y$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

7.10. How would you disprove a logical equivalence? Show the following:

a. $x \implies y$ is not logically equivalent to $y \implies x$

x	y	$x \implies y$	$y \implies x$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

b. $x \implies y$ is not logically equivalent to $x \iff y$

c. $x \vee y$ is not logically equivalent to $(x \wedge \neg y) \vee ((\neg x) \wedge y)$

2 Collections

2.8 Lists

A list is an ordered sequence of objects.

Notation: $(x_1, x_2, x_3, \ldots, x_N)$.

Note: The order in which objects appear in the list is important.

(11) $(1, 2, 3) \neq (1, 3, 2)$

Length: The number of objects in a list.

Ordered Pair: Special list of length two, denoted by (x, y).

Note: Ordered pairs are used to specify the position of points in a plane.

(12) $(A, 1, 3)$, where the 1st object is a letter of the alphabet, and 2nd, 3rd objects are numbers.

(13) Write down all lists that can be made given the following conditions:

a) The lists are of length 2
b) The 1st element is drawn from $\{A, B, C, D\}$
c) The 2nd element is drawn from $\{1, 2, 3\}$

$(A, 1)$	$(A, 2)$	$(A, 3)$
$(B, 1)$	$(B, 2)$	$(B, 3)$
$(C, 1)$	$(C, 2)$	$(C, 3)$
$(D, 1)$	$(D, 2)$	$(D, 3)$

(14) How many lists of length 2 can we make when the 1st element is a member of $\{1, 2, \ldots, 8\}$, and the 2nd element is a member of $\{1, 2, \ldots, 10\}$.

Answer: $8 \cdot 10 = 80$.

(15) A club has 10 members. In how many ways can the club elect a President and a Vice-President?

Assumptions:

1) All members of the club are eligible.
2) The President and Vice-President cannot be the same person.

Solution: $\underbrace{10}_{\text{P}} \cdot \underbrace{9}_{\text{VP}} = 90.$

In general:

Theorem 8.2: Consider two element lists (i.e. lists of length 2) for which there are n choices for the 1st element and for each choice of the 1st element, there are m choices for the 2nd element. The number of such lists is $n \cdot m$.

(16) You have a bag that contains 7 red marbles and 5 blue marbles. In how many ways can we draw a set of 2 marbles from the bag?

Solution: $12 \cdot 11 = 132$.

8.2) Airports have names, but they also have three-letter codes. For example, the airport serving Baltimore is `BWI`, adn the code `YYY` is for the airport Mont Joli, Quebec, Canada. How many different airport codes are possible?

Solution: $26 \cdot 26 \cdot 26 = 26^3 = 17576$

(17) How many 3 element lists can be made using the numbers from the set $\{1, 2, 3, 4, 5\}$?

Solution: $5^3 = 125$.

(18) Using the 1st element from $\{A, B, C, D\}$, the 2nd from $\{a, b, c\}$, and the 3rd from $\{1, 2, 3, 4, 5\}$.

Solution: $4 \cdot 3 \cdot 5 = 60$.

8.5) I want to create a playlist on my MP3 player from my collection of 500 songs. One playlist is titled “exercise” for listening in the gym and the other is titled “Relaxing” for leisure time at home. I want 20 different songs on each of these lists.

a) In how many ways can I load songs onto my MP3 player if I allow a song to be on both playlists.

Solution: $(500 \cdot 499 \cdot \ldots \cdot 481)^2 = \left({}_{500}P_{20}\right)^2$

b) And how many ways can I load the songs if I want the two lists to have no overlap?

Solution: $500!/480! \cdot 480!/460! = 500!/460! = {}_{500}P_{460}$

(19)

a) Suppose I toss a coin in the air 6 times. How many possible outcoms are there?

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^6 = 64$

b) Suppose I toss a die 4 times.

c) How many outcomes?
$6 \cdot 6 \cdot 6 \cdot 6 = 6^4$

ii) How many outcomes with an even number on the 2nd toss?
$6 \cdot 3 \cdot 6 \cdot 6 = 6^3 \cdot 3$

(20) Let a set $A = \{1, 2, \ldots, n\}$

a) In how many ways can I make a list of 4 elements from A?

n^4

b) In how many ways can I make a list of k elements from A?

$n \cdot n \cdot \ldots \cdot n = n^k$

(21) The Math Club wants to elect a President, a Vice President, a Secretary, and a Treasurer. In how many ways can they do so if:

a) The club has 10 members.

$10 \cdot 9 \cdot 8 \cdot 7 = 10!/(10-4)!$

b) The club has $n \geq 4$ members.

$n(n-1)(n-2)(n-3) = n!/(n-4)!$

(22) 15 athletes participate in a race. In how many ways can we fill the 1st three positions?
$15 \cdot 14 \cdot 13 = 15!/12!$
n atheletes participate in a race. In how many ways can we fill the 1st k positions?
$n(n-1)\ldots(n-k+1) = n!/(n-k)! = {}_nP_k$

${}_nP_k$ is called a falling factorial.

Theorem 8.6: The number of lists of length k whose elements are chosen from a pool of n possible elements

$$= \begin{cases} n^k, & \text{if repetitions are permitted} \\ {}_nP_k, & \text{if repetitions are forbidden} \end{cases}$$

8.12) A U.S. SSN is a 9-digit number. The first digit(s) may be 0. The numbers are in groups $AAA - BB - CCCC$. No group can be all zeroes.

a) How many SSNs are available?

If nothing was un-allowed, there would be 10^9. Then we can figure out how many of each un-allowed case there are.

8.7) I have 30 photos to post on my website. I'm planning to post these on two web pages, one marked "Friends" and the other marked "Family". No photo may go on both pages, but every photo will end up on one or the other. Conceivably, one of the pages may be empty.

a) In how many ways can I post these photos to the web pages if the order in which the photos appear on those pages matters?

Let's consider a simpler example. Instead of 30 photos, we only have 3. First let's consider all 3 photos posted on the "Friends" page. We would have 3! possible arrangements. We have another 3! possible arrangements if we post them all to the "Family" page. If we post 2 on "Friends", and 1 on "Family", we have another 3! possibilities, and another when we post 2 on "Family" and 1 on "Friends". So altogether we have $4 \cdot 3! = 4!$ possible arrangements.

Now consider 4 photos. There would be $5 \cdot 4! = 5!$ possible arrangements. Extrapolating to 30 photos, we would get $31 \cdot 30! = 31!$ possible arrangements.

b) In how many ways can I post these photos to the web pages if the order in which the photos appear on those pages does not matter?

In the case where we put all the picture on one page, and not the other, since order doesn't matter, each of those counts as 1 arrangement. We can rephrase the problem as the number of possible ways to choose a page for each picture. In the 3 photo situation, it comes out to $2^3 = 8$. In the 30 photo situation, it comes out to 2^30.

Conjecture: For n pages, and m pictures, there are n^m possible arrangements. This works for 1 and 2 pages, but I'm not sure about $n > 2$ pages.

8.9) In how many ways can a black rook and a white rook be placed on different squares of a chess board such that neither is attacking the other? (In other words, they cannot be in the same row or the same column of the chess board. A standard chess board is 8×8.)

Note: We are assuming that the black and white rook are the only pieces on the board.

8.13) Let n be a positive integer. Prove that $n^2 = {}_nP_2 + n$ in two different ways. First (and more simply) show this equation is true algebraically. Second (and more interestingly) interpret the terms n^2, ${}_nP_2$, and n in the context of list counting and use that to argue why the equation must be true.

$$\begin{aligned}
{}_nP_2 + n &= \frac{n!}{(n-2)!} + n \\
&= \frac{n(n-1)(n-2)\cdot\ldots 3\cdot 2\cdot 1}{(n-2)(n-3)\cdot\ldots 3\cdot 2\cdot 1} + n \\
&= n(n-1) + n \\
&= n^2 - n + n = n^2
\end{aligned}$$

In the context of list counting, n^2 is the number of 2-element lists where each entry can be chosen from among n elements and repetitions are allowed.

In the context of list counting, ${}_nP_2$ is the number of 2-element lists where each entry can be chosen from among n elements, and repetitions are *not* allowed.

In the context of list counting, n is the number of 2-element lists where an element (out of $\{1, 2, \ldots, n\}$ objects) is repeated.

Since the ${}_nP_2$ case is just the n^2 case with the repeated elements removed, $n^2 = {}_nP_2 + n$.

8.15) How many 5-digit numbers are there that do not have 2 consecutive digits the same? For example, you would count 12104 and 12397, but not 6321 (it is not 5 digits), or 43356 (it has two consecutive 3s).

The first slot can be $1-9$, so we have 9 possibilities. The remaining 4 slots have 1 less possibility, because they can't include the previous digit, but they also have the possibility of being 0, so there are still 9 possibilities, so we have $9\cdot 9\cdot 9\cdot 9\cdot 9 = 9^5$ possibilities.

2.9 Factorial

Remark: $0! = 1$

1) We would like: $n! = n(n-1)!$.
   - True for all $n > 1, n \in \mathbb{Z}$
   - But would like it to be true for $n = 1$ as well.
   - $1! = 1(1-1)! = 1\cdot 0! = 1 \implies 0! = 1$
2) $n!$ is the number of n-element lists, where each entry is out of n elements
   - $0!$ is the number of 0-element lists, where each entry is chosen out of 0 elements.
   - How many such lists are there?
   - Answer: 1. The empty list, denoted ().
3) Because I said so (definition).

Summation Notation:

$$\sum_{k=1}^{5} k = 1 + 2 + 3 + 4 + 5$$

Product Notation:

$$\prod_{k=1}^{5} k = 1\cdot 2\cdot 3\cdot 4\cdot 5 = 5!$$

$$\frac{50!}{48!} = \frac{50 \cdot 49 \cdot \cancel{48!}}{\cancel{48!}} = 50 \cdot 49 = \prod_{k=49}^{50} k$$

9.2) There are six different French books, eight different Russian books, and five different Spanish books.

a. In how many different ways can these books be arranged on a bookshelf?

   $(6+8+5)! = 19!$

b. In how many different ways can these books be arranged on a bookshelf if all books in the same language are grouped together?

   $3!(6! \cdot 8! \cdot 5!)$

2.10 Sets I: Introduction, Subsets

Set: A set is a repetition-free, unordered collection of objects.

e.g. $\{\text{Mary}, \text{Dan}, \text{Nick}\} = \{\text{Dan}, \text{Mary}, \text{Mary}, \text{Nick}\}$

Notes: 1) An element will not recur in a set. i.e. it does not occur more than once. 2) There is no order in which the elements are listed.

Four of the special sets of numbers:

- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{N} = \{0, 1, 2, \ldots\}$ (book-dependent)
- $\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$
- $\mathbb{R} = \ldots$
- $\imath = \sqrt{-1}$
- $\mathbb{C} = \{a + b\imath : a, b \in \mathbb{R}\}$

Notation:

1) Let A be a given set. $x \in A$ is read as "x belongs to A", or "x is an element of A"
2) $x \notin A$ is read as "x does not belong to A"

Definition: Cardinality of A: The number of elements in the set A; denoted as $|A|$ or $\text{card}(A)$

(23) If $A = \{1, 2, 3\}$, then $|A| = \text{card}(A) = 3$.

Notation: The empty set is denoted by $\emptyset$ or $\{\}$.

$\text{card}(\emptyset) = \text{card}(\{\}) = 0$.

Two ways of specifying a set:

1) List the elements of the set

   e.g. $\mathbb{N} = \{0, 1, 2, \ldots\}$

   Useful when the set is small or when the pattern of elements is clear, and can be expressed with "$\ldots$"

2) Write the set in set builder form

   set name = {dummy variable : conditions}

   e.g. $Q = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$

Let A be the set of all even integers.

$A = \{x : x \in \mathbb{Z} \text{ and } 2 \mid x\}$

$A = \{x : 2r = x \text{ where } r \in \mathbb{Z}\}$

Equality of sets: We say that two given sets A and B are equal, provided A and B contain exactly the same elements.

e.g. If $A = \{1, 2, 3\}$ and $B = \{2, 3, 1\}$, then $A = B$.

Proof Template: Proving two sets are equal:

- Let A, B be the two sets.
- To prove: $A = B$:
  1) Let $x \in A \ldots$ then $x \in B$.
  2) Let $y \in B \ldots$ then $y \in A$.
  3) $\therefore A = B$.

Subset of a set: Suppose A and B are two sets. We say A is a subset of B provided every element of A is an element of B. Notation: $A \subseteq B$.

Notes:

1) $A \subseteq B \implies A$ is either a proper subset of B, or A is equal to B, where a proper subset is one such that there are elements in B that are not in A.
2) $A \subsetneq B \implies A$ is a proper subset of B (i.e. A cannot be equal to B).
   - Some textbooks write this as $A \subset B$. We will not use this notation.
3) $x \in A$ is different from $\{x\} \subseteq A$.
   - $x \in A$ refers to x as a member of A, whereas $\{x\} \subseteq A$ refers to the set containing the single element x being a subset of A.
4) $\emptyset \subseteq A$ for any set A. However, $\{\emptyset\}$ may not be a subset of A.

Proposition 10.3: Let x be any element, and let A be a set. Then, $x \in A \iff \{x\} \subseteq A$. (proof on page 46)

Proof Templates:

1) To show: $A \subseteq B$.
   - Proof: Let $x \in A \ldots$ then, $x \in B$.
   - Conclude: $A \subseteq B$.
2) To show: $A = B$.
   - Show $A \subseteq B$
   - Show $B \subseteq A$
   - Conclude: from steps 1 and 2, $A = B$.
     - This is called a set containment, both directions argument.

10.10 (pg. 51): Let $A = \{x \in \mathbb{Z} : 4 \mid x\}$ and let $B = \{x \in \mathbb{Z} : 2 \mid x\}$. Prove that $A \subseteq B$.

Proof: We want to show: $A \subseteq B$.

Let $r \in A \implies 4 \mid r$ (by definition of A)

$\implies \exists t \in \mathbb{Z} : r = 4t$ (by definition of divisibility)

$\implies r = 2 \cdot 2 \cdot t = 2(2t)$ (by properties of integers)

Now, $2t \in \mathbb{Z}$ (closure property)

$\implies r = 2a$, where $a = 2t \in \mathbb{Z}$

$\implies r \in B$

$\therefore A \subseteq B$.

10.3:

d) Find the cardinality of the set $\{x \in \mathbb{Z} : \emptyset \in x\}$. Answer: 0 (or I would argue: undefined).

e) Find the cardinality of the set $\{x \in \mathbb{Z} : \emptyset \in \{x\}\}$. Answer: ∞.

10.11: Generalization of 10.10

Let $a, b \in \mathbb{Z}$.

Let $A = \{x \in \mathbb{Z} : a \mid x\}$.

Let $B = \{x \in \mathbb{Z} : b \mid x\}$.

Find and prove a necessary and sufficient condition for $A \subseteq B$.

Condition: $A \subseteq B \iff b \mid a$.

Proof:

1) We want to show that if $A \subseteq B$, then $b \mid a$.
   Let $A \subseteq B$. (To show: $b \mid a$)
   Consider $a \in \mathbb{Z}$. Then, $a \mid a$ ($\because a = a \cdot 1$)
   $\implies a \in A$
   But $A \subseteq B \implies a \in B$
   $\implies b \mid a$.

2) We want to show that if $b \mid a$, then $A \subseteq B$.
   Let $r \in A$. (To show: $r \in B$)
   $\implies a \mid r$
   $\implies \exists\, t \in \mathbb{Z} : at = r$. (1)
   Since $b \mid a$
   $\implies \exists\, s \in \mathbb{Z} : bs = a$. (2)
   $bst = r$ (from (1) and (2))
   $\implies b(st) = r$ (3)
   Let $st = u \in \mathbb{Z}$ (closure property) (4).
   $bu = r$ (from (3) and (4))
   $\implies b \mid r$ (from definition of divisibility)
   $\implies r \in B$ (by definition of B)
   $\therefore A \subseteq B$.

3) Therefore, from parts 1) and 2), we conclude that $A \subseteq B \iff b \mid a$.

2.10.1 Counting Subsets

How many subsets for a given, finite set A?

(24) $B = \{x, y\}$. The subsets of B are $\{x, y\}$, $\{x\}$, $\{y\}$, $\emptyset$. $\therefore$ the number of subsets is 4.

(25) $P = \{a, b, c\}$. The subsets of P are $\{a, b, c\}$, $\{a, b\}$, $\{b, c\}$, $\{a, c\}$, $\{a\}$, $\{b\}$, $\{c\}$, $\emptyset$. $\therefore$ the number of subsets is 8.

# elements in subset	subsets	# of subsets
0	$\emptyset$	1
1	$\{a\}$, $\{b\}$, $\{c\}$	3
2	$\{a, b\}$, $\{b, c\}$, $\{a, c\}$	3
3	$\{a, b, c\}$	1
		8

The number of subsets of a set A, containing n elements is $2^n = 2^{|A|} = 2^{\text{card}(A)}$.

2.10.2 Power Set

Power set of a given set A: Let A be a fininte set. Then, the set containing all the subsets of A is called the power set of A.

Notation: $\mathcal{P}(A)$ in most texts, or 2^A in our text.

The reasoning behind the text's notation is: $|\mathcal{P}(A)| = 2^{|A|}$, so in the text's notation it would be written: $|2^A| = 2^{|A|}$. So cardinality is distributed to the exponent.

10.3)

f) Find the cardinality of $2^{2^{\{1,2,3\}}}$.

Solution: $2^{2^{\{1,2,3\}}} = 2^8 = 256$.

g) Find the cardinality of $\{x \in 2^{\{1,2,3,4\}} : \text{card}(x) = 1\}$.

Solution: 4.

2.11 Quantifiers

Two forms of quantifiers

1) There is/exists. Notation: $\exists$.
   - Existential quantifier
2) For all/every/each/any: Notation: $\forall$.
   - Universal quantifier

Proof template for existential quantifier:

To prove: $\exists\ x \in A$ such that (assertion about x).

Proof: Let x be (explicit example).

Then, x satisfies (assertion about x).

$\therefore$ x satisfies the required condition.

(26) There is an integer x whose square is 4.

Proof: Let $x = 2$ (explicit example)

We know: $x^2 = 4$ (x satisfies the assertion)

$\therefore$ $x = 2$ is the required integer.

Proof template for universal quantifier:

To prove: $\forall x \in A$, (some assertion about x).

Proof: Let $x \in A$ (where x can be any element in A).

Then, show that x satisfies (some assertion about x).

$\therefore$ x satisfies (some assertion about x)

$\implies \forall x \in A$, (some assertion about x).

(27) Every integer that is divisible by 6 is divisible by 2.

Proof: Let r be any integer that is divisible by 6. (i.e. $6 \mid r$)

$\implies \exists\ y \in \mathbb{Z} : 6y = r$.

$\implies r = 6y = 2 \cdot 3 \cdot y = 2(3y)$.

We know $3y$ is an integer (closure properties of $\mathbb{Z}$)

$\implies r = 2(3y)$ where $3y \in \mathbb{Z}$

$\implies 2 \mid r$

$\implies r$ is divisible by 2

$\therefore$ every integer that is divisble by 6 is divisible by 2.

Negating quantified statements.

(28) $\exists\ x \in \mathbb{Z}$, x is even and odd.

Read as: There is an integer that is both even and odd.

Negation: There is no integer that is both even and odd.

$\neg(\exists\ x \in \mathbb{Z}$, x is even and odd.)

Taking the negation inside: $\forall x \in \mathbb{Z}$, $\neg$ (x is even and odd).

Read as: Every integer is not even and odd.

(29) $\forall x \in \mathbb{Z}$, x^2 is negative

Read as: The square of all integers are negative.

Negation: $\neg(\forall x \in \mathbb{Z},\ x^2$ is negative$)$

Read as: There is at least one integer whose square is not negative.

Taking the negation inside: $\exists x \in \mathbb{Z},\ \neg(x^2$ is negative$)$

In general:

1) $\neg(\forall x \in A,$ assertions about $x) \equiv \exists x \in A,\ \neg($assertions about $x)$
2) $\neg(\exists x \in A,$ assertions about $x) \equiv \forall x \in A,\ \neg($assertions about $x)$

11.1. Write the sentences in quantifier notation.

a) Every integer is prime.
   $\forall x \in \mathbb{Z},\ x$ is prime
b) There is an integer whose square is 2.
   $\exists x \in \mathbb{Z},\ x^2 = 2$

11.2. Write the negation of the sentences from the previous problem.

a) $\neg(\forall x \in \mathbb{Z},\ x$ is prime$)$
   $\exists x \in \mathbb{Z},\ \neg(x$ is prime$)$
b) $\neg(\exists x \in \mathbb{Z},\ x^2 = 2)$
   $\forall x \in \mathbb{Z},\ \neg(x^2 = 2)$
   $\forall x \in \mathbb{Z},\ x^2 \neq 2$

11.4. *True or false?*

e) $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, xy = 0 =$ false

11.5. For each of the following sentences, write the negation of the sentence, but place the ¬ sybmol as far to the right as possible. Then rewrite the negation in English.

a) $\forall x \in \mathbb{Z}, x < 0$
   $\exists x \in \mathbb{Z} : x \not< 0$
   There exists an integer x such that x is not less than 0.
b) $\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x > y$
   $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x \not> y$

11.7. *True or false?*

a) $\exists! x \in \mathbb{N} : x^2 = 4$ is true
b) $\exists! x \in \mathbb{Z} : x^2 = 4$ is false
c) $\exists! x \in \mathbb{N}, x^2 = 3$ is false
d) $\exists! x \in \mathbb{Z} : \forall y \in \mathbb{Z}, xy = x$ is true
e) $\exists! x \in \mathbb{Z} : \forall y \in \mathbb{Z}, xy = y$ is true

Combining Quantifiers:

Consider: For every integer x, there is an integer y s.t. $x + y = 0$.

1) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z} : x + y = 0$
2) $\exists y \in \mathbb{Z} : \forall x \in \mathbb{Z}, x + y = 0$

These two statements are not equivalent, and in fact the first is true and the second is false.

2.12 Sets II: Operations

2.12.1 Union and Intersection

Definition: Let A, B be two sets.

- *Union*: The union of A and B is the set of all elements that are in A *or* in B.
  - Notation: $A \cup B = \{x : x \in A \vee x \in B\}$
- *Intersection*: The intersection of A and B is the set of all elements that belong to both A *and* B.
  - Notation: $A \cap B = \{x : x \in A \wedge x \in B\}$

(30) Let $A = \{1, 2, 3, 4, 5\}$ and let $B = \{3, 6, 9, 12\}$. Then $A \cup B = \{1, 2, 3, 4, 5, 6, 9, 12\}$, and $A \cap B = \{3\}$.

Definition: Let A, B be sets whose elements are from a universal set $\mathbb{U}$. Then:

1) $A \cup B = \{x \in \mathbb{U} : x \in A \vee x \in B\}$
2) $A \cap B = \{x \in \mathbb{U} : x \in A \wedge x \in B\}$
3) Complement: A' or A^c or $\bar{A} = \{x \in \mathbb{U} : x \notin A\}$
4) Set Difference: $A - B = \{x \in \mathbb{U} : x \in A \wedge x \notin B\}$
5) Symmetric difference of two sets: $A \triangle B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$
6) Cartesian Product: $A \prod B = \{(a, b) : a \in A, b \in B\}$

(31) Let $A = \{1, 2, 3, 4, 5\}$,B = { 4, 5, 6, 7 }$

c) $A - B = \{1, 2, 3\}$
d) $A \triangle B = \{1, 2, 3, 6, 7\}$

Theorem 12.3: Properties of sets.

Let A, B, C denote sets. Then, the following are true:

1) $A \cup B = B \cup A$ and $A \cap B = B \cap A$ (commutative property)
2) $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$ (assocative property)
3) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$
   - $A \cup \mathbb{U} = \mathbb{U}$ and $A \cap \mathbb{U} = A$
4) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributive property)

We want to prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

LHS: $A \cup (B \cap C) = \{x \in \mathbb{U} : x \in A \vee x \in B \cup C\}$

$\implies A \cup (B \cap C) = \{x : x \in A \vee (x \in B \wedge x \in C)\}$ (by definition of intersection)

$\implies A \cup (B \cap C) = \{x : (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\}$ (because $\vee$ distributes over $\wedge$, by Theorem 7.2(6) on pg. 27)

$\implies A \cup (B \cap C) = \{x : x \in (A \cup B) \wedge (x \in A \cup C)\}$ (by definition of union)

$\implies A \cup (B \cap C) = \{x : x \in (A \cup B) \cap (A \cup C)\}$ (by definition of intersection)

$\therefore A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Another way to prove this is via the set containment argument in both directions.

To prove: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

We will show:

1) $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
2) $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

Proof of part 1: Let $x \in A \cup (B \cap C)$

$\implies x \in A \vee x \in B \cup C$ (1) (by definition of union)

Case 1: Let $x \in A \implies x \in A \cup B$ (since $A \subseteq A \cup B$)

Also, $x \in A \cup C$ (since $A \subseteq A \cup C$)

$\implies x \in (A \cup B) \cap (A \cup C)$ (by definition of intersection)

Case 2: Let $x \notin A \implies x \in B \cap C$ (by (1))

$\implies x \in B \wedge x \in C$ (by definition of intersection)

$\implies x \in A \cup B \wedge x \in A \cup C$ ($\because B \subseteq A \cup B \wedge C \subseteq A \cup C$)

$\implies x \in (A \cup B) \cap (A \cup C)$ (by definition of intersection)

$\therefore A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ (2)

Proof of part 2: Let $x \in (A \cup B) \cap (A \cup C)$

$\implies x \in A \cup B \wedge x \in A \cup C$ (by definition of intersection)

$\implies (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ (3) (by definition of union)

Case 1: Let $x \in A \implies x \in A \cup (B \cap C)$

Case 2: Let $x \notin A \implies x \in B \wedge x \in C$ (by (3))

$\implies x \in B \cap C$ (by definition of intersection)

$\implies x \in A \cup (B \cap C)$ (by definition of union)

So in either case, $x \in A \cup (B \cap C)$

$\implies (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ (4)

From (2) and (4), we get: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proposition 12.4:

Let A and B be finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.

(32) Let $|A| = 10$, $|B| = 5$. Find $|A \cap B|$.

$|A \cup B| = (10 - |A \cap B|) + (5 - |A \cap B|) + |A \cap B|$

$|A| + |B| = 10 + 5 = 15$

$|A \cup B| = 15 - |A \cap B|$

$\implies |A \cap B| = 15 - |A \cup B|$.

Definition: Two sets, A and B, are said to be *disjoint* if $A \cap B = \emptyset$, i.e. A and B have no elements in common.

Note: If $A \cap B = \emptyset \implies |A \cap B| = 0$

$\implies |A \cup B| = |A| + |B|$, if $A \cap B = \emptyset$.

Corollary: If A_1, A_2, ..., A_n are finite sets such that $A_i \cap A_j = \emptyset \forall i, j \in \{1, \ldots, n\}$

i.e. A_1, A_2, ..., A_n are pairwise disjoint.

Then, $|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$.

i.e. $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$.

Proposition 12.12 (**DeMorgan's Laws**):

Let A, B, and C be sets. Then

a. $A - (B \cup C) = (A - B) \cap (A - C)$
b. $A - (B \cap C) = (A - B) \cup (A - C)$.

Formal proof of a:

To prove: $A - (B \cup C) = (A - B) \cap (A - c)$.

Proof: $(A - B) \cap (A - C) = \{x \in \mathbb{U} : x \in (A - B) \wedge x \in (A - C)\}$

$= \{x \in \mathbb{U} : (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)\}$

$= \{x \in \mathbb{U} : x \in A \wedge x \notin B \cup C\}$

$= \{x \in \mathbb{U} : x \in (A - (B \cup C))\}$

$= A - (B \cup C)$

$\therefore (A - B) \cap (A - C) = A - (B \cup C)$.

2.12.2 Cartesian Product

$A \times B = \{(a, b) : a \in A, b \in B\}$

(33) Let $A = \{a, b, c\}$, $B = \{2, 3, 4, 5\}$.

Then:

$A \times B = \{(a, 2), (a, 3), (a, 4), (a, 5), (b, 2), (b, 3), (b, 4), (b, 5), (c, 2), (c, 3), (c, 4), (c, 5)\}$.

$B \times A = \{(2, a), (2, b), (2, c), (3, a), (3, b), (3, c), (4, a), (4, b), (4, c), (5, a), (5, b), (5, c)\}$.

Note that $A \times B \neq B \times A$ in general. i.e. the cartesian product of two sets is *not* commutative.

Proposition 12.15: $|A \times B| = |A|\ |B| = |B|\ |A| = |B \times A|$.

Also note that $\forall A \subseteq \mathbb{U}, A \times \emptyset = \emptyset$

2.13 Combinatorial Proof: Two Examples

We'll skip this section for now.

3 Counting and Relations

3.14 Relations

A relation is a set of ordered pairs.

(34) Let $A = \{1, 2, 3\}$, $B = \{4, 5\}$.

Then, let $R = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 5)\}$.

We say R is a relation.

Note that $R \subseteq A \times B$. Here, R is a proper subset of $A \times B$. i.e. $R \subsetneq A \times B$.

Notation:

1. We say $(1, 4) \in R$, or we say 1 is (R) related to 4, (we can include the R or not, depending on context. If there is only the relation R, we can leave it off), and we write it as $1R4$.
2. Here, $(3, 4) \notin R$. We say 3 is not related to 4, and write it as $3 \not R\ 4$.

Formal Definition:

a. *Relation between sets:* Let A, B be any sets. We say R is a relation from A to B provided $R \subseteq A \times B$.

b. *Relation on a set:* Let A be a set. We say R is a relation on A provided $R \subseteq A \times A$.

3.14.1 Properties of Relations

Definition 14.7: Let R be a relation defined on a set A.

- If $\forall x \in A$ we have xRx, we say R is *reflexive.*
- If $\forall x \in A$ we have $x \not R\ x$, we say R is *irreflexive.*
- If $\forall x, y \in A$ we have $xRy \implies yRx$, we say R is *symmetric.*
- If $\forall x, y \in A$ we have $(xRy \wedge yRx) \implies x = y$, we say R is *antisymmetric.*
- If $\forall x, y, z \in A$ we have $(xRy \wedge yRz) \implies xRz$, we say R is *transitive.*

(35) Consider the relation $\leq$ on $\mathbb{Z}$.

a. $\leq\ = \{(x, y) : x, y \in \mathbb{Z} \wedge x \leq y\}$
$\leq\ = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \leq y\} \subseteq \mathbb{Z} \times \mathbb{Z}$
$\therefore \leq$ is a relation.

b. Reflexive? Yes, $\because x \leq x \forall x \in \mathbb{Z}$.
Irreflexive? No, $\because \neg(x \not\leq x) \forall x \in \mathbb{Z}$
Symmetric? No, ...
Antisymmetric? Yes, $\because x \leq y \wedge y \leq x \implies x = y$.
Transitive? Yes, $\because x \leq y \wedge y \leq z \implies x \leq z$.

(36) Consider the relation $<$ on $\mathbb{Z}$. (answer the same questions…)

(37) Consider the relation: "is the child of".

- reflexive?
  - No, x is the child of $x \forall x \in P$ is not true.
- irreflexive?
  - Yes, x is not the child of $x \forall x \in P$ is true.
- symmetric?
  - No, x is the child of $y \implies y$ is the child of x $\forall x, y \in P$ is false
- antisymmetric?
  - Yes, it is vacuously antisymmetric, as the if condition can never happen.
- transitive?
  - No, your parent's parent is your grandparent, not your parent.

Definition 14.4: **(Inverse relation)** Let R be a relation. The *inverse* of R, denoted R^{-1}, is the relation formed by reversing the order of all the ordered pairs in R.

i.e. Let $R = \{(a,b) : (a \in A) \wedge (b \in B)\}$, then $R^{-1} = \{(b,a) : (a \in A) \wedge (b \in B)\}$.

1) If R is a relation from A to B, then R^{-1} is a relation from A to B, then R^{-1} is a relation from B to A. (If R is a relation on A, then so is R^{-1})
2) $R^{-1} \neq \frac{1}{R}$

Proposition 14.6: $(R^{-1})^{-1} = R$

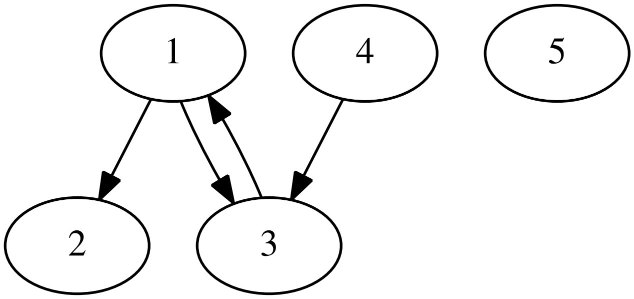
Problem 14.9: Let R be a relation on a set A. Prove or disprove: If R is antisymmetric, then R is irreflexive.

(Recall: If R is antisymmetric, then $(xRy) \wedge (yRx) \implies x = y$. If R is irreflexive, then $x \not R x, \forall x \in A$.)

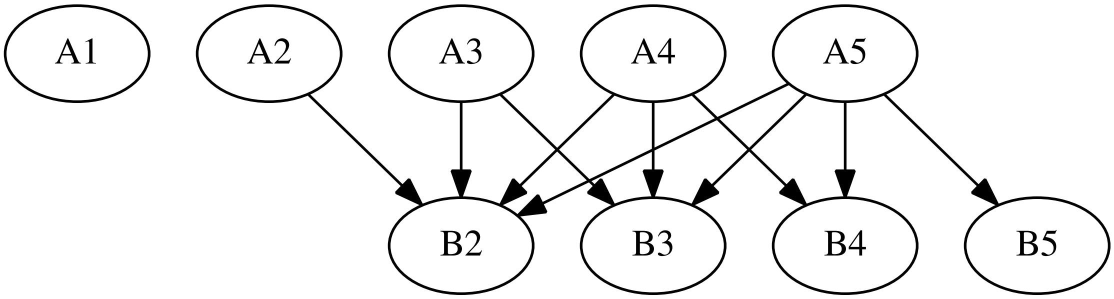
Counter-example: $\leq$ is antisymmetric, but not irreflexive. $=$ is another counter-example, as is $\geq$.

Problem 14.17: Drawing pictures of relations.

Let $A = \{1,2,3,4,5\}$. Let $R = \{(1,1),(1,2),(1,3),(4,3),(3,1)\}$



Let $A = \{1,2,3,4,5\}$, $B = \{2,3,4,5\}$. Let $R = \geq$ from A to B.



Problem 14.11: Consider the relation $\subseteq$ on $2^{\mathbb{Z}}$ (i.e., the is-a-subset-of relation defined on all sets of integers). Which of the properties on Definition 14.7 does $\subseteq$ have? Prove your answers.

$2^{\mathbb{Z}} = \mathcal{P}(\mathbb{Z}) = \{\{1\}, \{1, 2\}, \{-1, -2\}, \ldots\}$.

3.15 Equivalence Relations

Definition 15.1: **(Equivalence relation)** Let R be a relation on a set A. We say R is an *equivalence relation* provided it is reflexive, symmetric, and transitive.

e.g. congruence on $\triangle$'s (two $\triangle$'s are congruent provided they can be superimposed completely on one another, i.e. the 3 sides and 3 angles are exactly equal)

Let A = the set of all $\triangle$'s congruent to a given $\triangle$. Show that congruence is reflexive, symmetric, and transitive.

Definition 15.3: **(Congruence modulo *n*)** Let $n \in \mathbb{N}$. We say x and y are congruent modulo n, provided $n \mid (x - y)$. Notation: $x \equiv y \mod n$

(38) Let $n = 5$. Let $x = 10, y = 5$. Then $5 \mid (x - y) = 10 - 5$. Let $x = 9, y = 4$. Then $5 \mid (9 - 4) = 5$.

We have $x \equiv y \mod 5$, provided $x - y$ is a multiple of 5. $\therefore 9 \equiv 4 \mod 5$. $10 \not\equiv 4 \mod 5$.

$\forall x \in \mathbb{Z},\ 2x + 1 \equiv -1 \mod 2$.

$\forall x \in \mathbb{Z},\ 0 \equiv 2x \mod 2$.

Note: Two numbers are congruent modulo 2 provided they are both even, or they are both odd.

Is "congruence modulo 2":

- reflexive?
  - Yes, because $\forall x \in \mathbb{Z},\ x \equiv x \mod 2$.
- symmetric?
  - Yes, because $x \equiv y \mod 2 \implies y \equiv x \mod 2$.
- transitive?
  - Yes, because $(x \equiv y \mod 2) \wedge (y \equiv z \mod 2) \implies x \equiv z \mod 2$.

Thus, congruence mod 2 is an *equivalence relation*.

Theorem 15.5: Let n be a positive integer. The is-congruent-to-mod-n relation is an equivalence relation on the set of integers.

(39) Let A = the set of all students in class. Let R = the relation "born in the same month".

Is R:

- reflexive?
  - Yes, because $\forall x \in A, xRx$.
- symmetric?
  - Yes, because $\forall x, y \in A, xRy \implies yRx$.
- transitive?
  - Yes, because $\forall x, y, z \in A, (xRy) \wedge (yRz) \implies (xRz)$.

3.15.1 Equivalence Classes

Definition 15.6: **(Equivalence class)** Let R be an equivalence relation on a set A and let $a \in A$. The *equivalence class of* a, denoted $[a]$, is the set of all elements of A related (by R) to a; that is,

$$[a] = \{x \in A : xRa\}.$$

Note that R is reflexive, so xRa could be written as aRx as well.

(40) Let $n = 2$, and let $R =$ congruence mod 2. Then:

$[0] = \{x \in \mathbb{Z} : x \equiv 0 \mod 2\} = \{x \in \mathbb{Z} : 2 \mid x\}$.

$[1] = \{x \in \mathbb{Z} : x \equiv 1 \mod 2\} = \{x \in \mathbb{Z} : 2 \mid (x + 1)\}$.

We note: $\mathbb{Z} = [0] \cup [1]$, and $\emptyset = [0] \cap [1]$.

(41) Let $n = 3$, and let $R =$ congruence mod 3.

Is R an equivalence relation? Yes.

Then,

$[0] = \{x \in \mathbb{Z} : x \equiv 0 \mod 3\} = \{x \in \mathbb{Z} : 3 \mid x\}$.

$[1] = \{x \in \mathbb{Z} : x \equiv 1 \mod 3\} = \{x \in \mathbb{Z} : 3 \mid (x - 1)\}$.

$[2] = \{x \in \mathbb{Z} : x \equiv 2 \mod 3\} = \{x \in \mathbb{Z} : 3 \mid (x - 2)\}$.

We note: $\mathbb{Z} = [0] \cup [1] \cup [2]$, and $\emptyset = [0] \cap [1] \cap [2]$.

(42) Let $R =$ congruence mod n.

Then,

$[0] = \{x \in \mathbb{Z} : x \equiv 0 \mod n\} = \{x \in \mathbb{Z} : n \mid x\}$.

$\vdots$

$[n - 1] = \{x \in \mathbb{Z} : x \equiv (n - 1) \mod n - 0\} = \{x \in \mathbb{Z} : n \mid x - (n - 1)\}$.

$\mathbb{Z} = \bigcup_{m=0}^{n-1} [m]$, and $\emptyset = \bigcap_{m=0}^{n-1} [m]$.

So $[0] \ldots [n - 1]$ are pairwise disjoint, non-empty sets such that their union is the set of integers.

Definition: **Partition of a set** A

Let A be a set. A partition of A is a set of non-empty, pairwise disjoint, subsets of A such that the union of those subsets is A itself.

(43) Consider $\mathbb{Z}$, with the relation of congruence modulo 3. Then $\{[0],[1],[2]\}$ is a partition of $\mathbb{Z}$.

(44) Consider $\mathbb{Z}$, with the relation congruence modulo 2. Then $\{[0],[1]\}$ is a partition of $\mathbb{Z}$.

(45) Let $A=\{1,2,3,4,5\}$. Let $P=\{\{1,2\},\{3,4\},\{5\}\}$. P is a partition of A.

Proposition 15.9:

Let R be an equivalence relation on A. Then $a \in [a]$.

Proof:

We know $[a]=\{x \in A : xRA\}$, and aRa (since R is an equivalence relation, and R is reflexive).

$\therefore a \in [a]$.

Proposition 15.10:

Let R be an equivalence relation on A. Then $aRb \iff [a]=[b]$.

Proof:

Part 1: $aRb \implies [a]=[b]$.

Let aRb. To prove: $[a]=[b]$.

Let $x \in [a] \implies xRa$. But aRb (given) $\implies xRb$ (since R is transitive) $\implies x \in [b] \implies [a] \subseteq [b]$ (1).

Conversely, let $x \in [b]$. To show: $x \in [a]$.

Let $x \in [b] \implies xRb$. But bRa (given) $\implies xRa$ (since R is transitive) $\implies x \in [a] \implies [b] \subseteq [a]$ (2).

From (1) and (2): $[a]=[b]$.

Part 2: $[a]=[b] \implies aRb$.

Let $[a]=[b]$, to show aRb.

Let $x \in [a] \implies xRa$ and $x \in [b]$ ($\because [a]=[b]$).

Since $x \in [b] \implies xRb$. (3)

Since $xRa \implies aRx$ ($\because R$ is symmetric) (4).

From (3) and (4): aRx and $xRb \implies aRb$ ($\because R$ is transitive).

Proposition 15.11:

Let R be an equivalence relation on A. Let $a,x,y \in A$.

If $x,y \in [a]$, then xRy.

Proposition 15.12:

Let R be an equivalence relation on A. Let $[a]\cap[b] \neq \emptyset$, where $a,b \in A$. Then $[a]=[b]$.

Proof:

Let $[a]\cap[b] \neq \emptyset$. To prove: $[a]=[b]$.

(Note: We could use a set containment argument, however, instead we are going to use Proposition 15.10.)

Since $[a]\cap[b] \neq \emptyset$, let $x \in [a]\cap[b]$.

$\implies x \in [a]$ and $x \in [b]$.

$\implies xRa$ and xRb.

$xRa \implies aRx$. (since R is symmetric)

$\implies aRb$. (since R is transitive)

$aRb \iff [a]=[b]$ (from Proposition 15.10).

$\therefore [a]=[b]$.

Corrolary 15.13:

Let R be an equivalence relation on A. The equivalence classes of R are non-empty, pairwise disjoint subsets of A, whose union is A.

Problem 15.1 (a): $53 \equiv 23 \mod N$, where $N \in \mathbb{Z}$ and $N > 1$. Find all N.

$N \mid (53-23) = N \mid 30$. $N \mid 30 \implies N \in \{2,3,5,6,10,15,30\}$.

Problem 15.6: Prove that congruence modulo n is transitive.

To prove: If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

Let $a \equiv b \mod n$ and $b \equiv c \mod n$

$\implies n \mid (a-b) \wedge n \mid (b-c)$

$\implies \exists x, y \in \mathbb{Z} : a-b = nx \wedge b-c = ny$.

Then, $(a-b)+(b-c) = nx+ny$

$\implies a-c = n(x+y)$.

Let $z = x+y \implies z \in \mathbb{Z}$.

$\implies a-c = nz \implies n \mid (a-c)$

$\therefore a \equiv c \mod n$.

3.16 Partitions

Definition 16.1: **(Partition)** Let A be a set. A *partition of* (or *on*) A is a set of nonempty, pairwise disjoint sets whose union is A.

The equivalence classes of A form a partition of A.

Note: The subsets in a partition of A are called *parts* or *blocks* of A.

So, given an equivalence relation, we form a partition of A.

(46) $\equiv \mod 2$ and $\equiv \mod 3$.

What about the reverse situation? i.e. Given a partition $\mathcal{P}$, can we construct an equivalence relation using the partition?

(47) Let $A = \{1,2,3,4,5,6\}$ and let $\mathcal{P} = \{\{1,2\},\{3,4,5\},\{6\}\}$.

Notation: Let $\mathcal{P}$ be a partition of A. We will use $\mathcal{P}$ to form a relation on A. We call this relation the "is-in-the-same-part-as" relation, and denote it by $\overset{\mathcal{P}}{\equiv}$.

Theorem: Congruence modulo N is an equivalence relation.

Proof: We would like to show: $\equiv \mod n$ is reflexive, symmetric, and transitive.

Claim: $\equiv \mod n$ is reflexive.

To show: $a \equiv a \mod n \forall a \in \mathbb{Z}$, i.e. $n \mid a-a$.

But $a-a=0$ and $n \mid 0 \forall n \in \mathbb{Z}$ ($\because 0 = n \cdot 0$).

$\implies a \equiv a \mod n$

$\therefore$ it is reflexive.

Claim: $\equiv \mod n$ is symmetric.

To show: If $a \equiv b \mod n$, then $b \equiv a \mod n$.

Let $a \equiv b \mod n \implies n \mid a - b$.

$\implies \exists x \in \mathbb{Z} : a - b = nx$

$\implies b - a = n(-x)$ (note that $(-x) \in \mathbb{Z}$)

$\implies n \mid b - a$

$\implies b \equiv a \mod n$

$\therefore$ it is symmetric.

Claim: $\equiv \mod n$ is transitive.

To show: If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

Proof: Let $a \equiv b \mod n$ and $b \equiv c \mod n$

$\implies n \mid a - b$ (by definition of $\equiv \mod n$) and $n \mid b - c$

$\implies \exists x \in \mathbb{Z} : a - b = nx$ and $n \mid b - c$ (1)

$\exists y \in \mathbb{Z} : b - c = ny$ (2)

$\implies (a - b) + (b - c) = nx + ny$ (from (1) and (2))

$\implies a - c = n\underbrace{(x + y)}_{\in \mathbb{Z}} \implies n \mid a - c$

$\implies a \equiv c \mod n$

$\therefore$ it is transitive.

We have shown that $\equiv \mod n$ is reflexive, symmetric, and transitive, $\therefore \equiv \mod n$ is an equivalence relation.

Proposition 16.3: Let A be a set and let $\mathcal{P}$ be a partition on A. The relation $\overset{\mathcal{P}}{\equiv}$ is an equivalence relation on A.

Proof: We want to show that $\overset{\mathcal{P}}{\equiv}$ is reflexive, symmetric, and transitive.

Claim: $\overset{\mathcal{P}}{\equiv}$ is reflexive, i.e. to show $a \overset{\mathcal{P}}{\equiv} a \forall a \in A$.

Proof: Let $a \in A \implies \exists P \in \mathcal{P} : a \in P$ (by definition of partition)

Then, $a \overset{\mathcal{P}}{\equiv} a \forall a \in A$ (Note: there is only one part that a can belong to).

Claim: $\overset{\mathcal{P}}{\equiv}$ is symmetric.

i.e. to show if $a \overset{\mathcal{P}}{\equiv} b$, then $b \overset{\mathcal{P}}{\equiv} a$.

Let $a, b \in A$ and let $a \overset{\mathcal{P}}{\equiv} b$

$\implies \exists P \in \mathcal{P} : a, b \in P$ (i.e. a, b are in the same part P of $\mathcal{P}$)

$\implies b \overset{\mathcal{P}}{\equiv} a,$

$\therefore \overset{\mathcal{P}}{\equiv}$ is symmetric.

Claim: $\overset{\mathcal{P}}{\equiv}$ is transitive, i.e. to show if $a \overset{\mathcal{P}}{\equiv} b$ and $b \overset{\mathcal{P}}{\equiv} c$, then $a \overset{\mathcal{P}}{\equiv} c$.

Proof: Let $a \overset{\mathcal{P}}{\equiv} b$ and $b \overset{\mathcal{P}}{\equiv} c$.

Since $a \overset{\mathcal{P}}{\equiv} b \implies \exists P \in \mathcal{P} : a, b \in P$ (1)

Since $b \overset{\mathcal{P}}{\equiv} c \implies \exists Q \in \mathcal{P} : b, c \in Q$ (2)

From (1) and (2), $b \in P \cap Q$.

We know either two parts are pairwise disjoint, or they must be identical, so $P \cap Q \neq \emptyset \implies P = Q$

$\implies a, b, c \in P$

$\implies a \overset{\mathcal{P}}{\equiv} c$

$\therefore \overset{\mathcal{P}}{\equiv}$ is transitive.

We have shown that that $\overset{\mathcal{P}}{\equiv}$ is reflexive, symmetric, and transitive, $\therefore$ $\overset{\mathcal{P}}{\equiv}$ is an equivalence relation.

Proposition 16.4: Let $\mathcal{P}$ be a partition of A and let $\overset{\mathcal{P}}{\equiv}$ be the "in the same part as" relation. Then, we know (Prop. 16.3) that $\overset{\mathcal{P}}{\equiv}$ is an equivalence relation.

The equivalence classes of $\overset{\mathcal{P}}{\equiv}$ are exactly the parts of $\mathcal{P}$.

Proof: We want to show:

Part 1) Every equivalence class of $\mathcal{P}$ is a part of $\mathcal{P}$.

Part 2) Every part of $\mathcal{P}$ is an equivalence class of $\mathcal{P}$.

Proof of 1) Let $a \in A$. Consider $[a] = \{x \in A : x \overset{\mathcal{P}}{\equiv} a\}$.

Since $a \in A \implies \exists P \in \mathcal{P} : a \in P$.

To show: $[a] = P$.

Let $x \in [a] \implies x \overset{\mathcal{P}}{\equiv} a \implies x \in P$ ($\because$ $a \in P$)

$\therefore$ $[a] \subseteq P$.

Let $x \in P \implies x \overset{\mathcal{P}}{\equiv} a \implies x \in [a] \implies P \subseteq [a]$

$\implies [a] = P$.

Proof of 2) Let P be a part of $\mathcal{P}$. We will show: $\exists$ an equivalence class of $\overset{\mathcal{P}}{\equiv}$ equal to P.

Since P is a part, $P \neq \emptyset \implies \exists a \in P$.

Claim: $P = [a]$. **(complete for homework)**

Question: In how many ways can you arrange the letters of the word TAP? (anagrams of TAP)

Answer: $6 = 3!$.

How many anagrams of the word TELL?

Suppose we consider the two L's as separate characters. Then there are 4! anagrams.

Now when we consider them as the same character, each anagram in the 4! anagrams has one duplicate, so there are 4!/2 anagrams.

Consider: Let A be the set of all anagrams of TELL (including duplicates). Then, $|A| = 4! = 24$.

Let $a, b \in A$ (i.e. a, b are anagrams of TELL).

Define a relation R on A as follows: aRb provided a and b give the same arrangement of the letters in TELL, when duplicates are considered equal. Then, R is reflexive, symmetric, and transitive. i.e. R is an equivalence relation.

What are the equivalence classes of R?

$[\mathrm{TELL'}] = \{\mathrm{TELL'}, \mathrm{TEL'L}\}$

$[\mathrm{ELTL'}] = \{\mathrm{ELTL'}, \mathrm{EL'TL}\}$

$\implies \mathrm{card}([\mathrm{TELL'}]) = 2.$

In fact, the cardinality of every equivalence class of R is 2.

How many equivalence classes?

We know $A = [\mathrm{TELL'}] \cup \ldots \cup [\mathrm{L'LET}]$,

$\implies \mathrm{card}(A) = \mathrm{card}([\mathrm{TELL'}]) \cup \ldots \cup \mathrm{card}([\mathrm{L'LET}])$

$\implies 24 = 2 + \ldots + 2 = 2N$, where N is the number of equivalence classes.

$\implies N = 24/2 = 12.$

$\therefore$ there are 12 anagrams of TELL.

In general, the number of anagrams is equal to the number of equivalence classes, multiplied by the cardinality of each equivalence class.

Now consider the anagrams of STATISTICS. Note that it has 3 T's, 3 S's, and 2 I's.

Let A be all the anagrams of the word $S_1T_1AT_2I_1S_2T_3I_2CS_3 = 10!$.

3.17 Binomial Coefficients

How many subsets of size k does an n-element set have?

Notation: $\binom{n}{k}$, "n choose k".

Definition 17.1: **(Binomial coefficient)** Let $n, k \in \mathbb{N}$. The symbol $\binom{n}{k}$ denotes the number of k-element subsets of an n-element set.

We call $\binom{n}{k}$ a binomial coefficient.

(48) Consider set A with 5 elements: $A = \{a, b, c, d, e\}$. Calculate the number of 0-element subsets, 1-element subsets, ..., 5-element subsets of A.

Solution:

$\binom{5}{0}$ denotes the *number* of 0-element subsets of A. A has just one – $\emptyset$ – as a 0-element subset. $\therefore$ $\binom{5}{0} = 1$ (Note: in fact, $\binom{n}{0} = 1 \ \forall n \in \mathbb{N}$)

$\binom{5}{1}$ denotes the number of 1-element subsets. A has 5: $\{a\}, \{b\}, \{c\}, \{d\}, \{e\}$. $\therefore$ $\binom{5}{1} = 5$. (Note: in fact, $\binom{n}{1} = n \ \forall n \in \mathbb{N}$)

$\binom{5}{2} = 10$ ($\{a, b\}$, $\{b, c\}$ ...)

$\binom{5}{3}$ denotes the number of 3-element subsets, and equals 10.

$\binom{5}{4} = 5.$

$\binom{5}{5} = 1.$

Note: We had coefficients $1, 5, 10, 10, 5, 1$, which are the coefficients in the expansion:

$$(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.$$

$$\begin{array}{ccccccccccccc|l}
 & & & & & & 1 & & & & & & & (x+y)^0 \\
 & & & & & 1 & & 1 & & & & & & (x+y)^1 \\
 & & & & 1 & & 2 & & 1 & & & & & (x+y)^2 \\
 & & & 1 & & 3 & & 3 & & 1 & & & & (x+y)^3 \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & & (x+y)^4 \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & (x+y)^5 \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & (x+y)^6
\end{array}$$

Also note that $\binom{5}{0} = \binom{5}{5} = 1$, $\binom{5}{1} = \binom{5}{4} = 5$, $\binom{5}{2} = \binom{5}{3} = 10$.

Proposition 17.7: Let $n, k \in \mathbb{N}$ with $0 \leq k \leq n$. Then

$$\binom{n}{k} = \binom{n}{n-k}.$$

What is $\binom{5}{6}$? It's zero, because there do not exist any 6-element subsets of a 5-element set. So in general, $k > n \iff \binom{n}{k} = 0$.

Likewise, n and k must not be negative, because you cannot have a set with a negative number of elements.

Theorem 17.8: **(Binomial Theorem)** Let $n \in \mathbb{N}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proposition:

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

Proposition 17.5: Let n be an integers with $n \geq 2$. Then

$$\binom{n}{2} = 1 + 2 + 3 + \ldots + (n-1) = \sum_{k=1}^{n-1} k.$$

3.17.1 Pascal's Triangle

Theorem 17.10: **(Pascal's Identity)** Let n and k be integers with $0 < k < n$. Then

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

Proof: We shall provide a combinatorial proof.

Template: *We ask a question. Then, we show that the left hand side and the right hand side of the equation we are trying to prove are correct answers to the question we asked. Since both LHS and RHS are correct answers to the same question, they are identical, and therefore the equation must be true.*

In this case, we ask the following question (motivated by the LHS): How many k-element subsets of an n-element set?

The LHS, which is $\binom{n}{k}$ is one answer to this question (by definition of $\binom{n}{k}$). (1)

Now, consider the RHS: Consider any set of n elements, so let $A = \{1, 2, \ldots, n\}$.

Designate any one element of the set A by $*$. For any k-element subset of A, there are two possibilities:

Case 1: The k-element subset includes $*$.

Then, the remaining $(k-1)$ elements of the subset must be chosen from the remaining $(n-1)$ elements of A.

$\therefore$ the number of k-element subsets from the $(n-1)$ element subset (which excludes $*$) is equal to $\binom{n-1}{k-1}$.

Case 2: The k-element subset does not include $*$.

Then, all k elements must be chosen from the remaining $(n-1)$ elements in A. The number of k-element subsets of of an $(n-1)$ element set is equal to $\binom{n-1}{k}$.

We note: Cases 1 and 2 account for all k-element subsets of A, and all subsets that contain $*$ are disjoint from all subsets that do not contain $*$.

$\therefore$ the number of k-element subsets of A is equal to $\binom{n-1}{k-1}+\binom{n-1}{k}$. (2)

From statements (1) and (2), we find that $\binom{n}{k}$ and $\binom{n-1}{k-1}+\binom{n-1}{k}$ are both correct answers to the question: How many k-element subsets of an n-element set exist?

$\therefore$ the two must be equal, so we have

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

Theorem 17.12: **(Formula for $\binom{n}{k}$)** Let n and k be integers with $0 \leq k \leq n$. Then

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

Exercise 17.3: What is the coefficient of:

a. x^4 in $(1+x)^6$? Using Pascal's triangle, it is 15.

b. x^5 in $(2x-3)^8$. Using the Binomial Theorem, it's

$$\binom{8}{5}(2x)^5(-3)^3=-48384x^5.$$

Exercise 17.6:

a. How many n-digit binary (0,1) sequences contain exactly k 1's? $\binom{n}{k}$.

Sum of the first n natural numbers is

$$\begin{aligned}\sum_{i=1}^{n} n &= 1+2+\ldots+n-1+n\\ &= \underbrace{(n+1)+(n-1)+2+\ldots}_{n/2 \text{ times}}\\ &= \frac{n}{2}\cdot(n+1)\end{aligned}$$

The number of lists of length k drawn from n elements is $n(n-1)(n-2)\ldots(n-k+1)=(n)_k={}_nP_k$.

Define an equivalence relation R on the lists of length k drawn from n elements as follows:

aRb provided a and b give rise to the same k subsets.

The number of elements in equivalence class of $R = k!$.

The number of equivalence classes (i.e. the number of k-element subsets drawn from an n-element set) is

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

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

4 More Proof

4.20 Contradiction

4.20.1 Proof by Contrapositive

That statement "If A, then B" (1) is logically equivalent to "If not B, then not A" (2). (can be shown using truth table)

Proof: To prove "If A, then B", we prove:

Assume (not B), and go on to prove "then (not A)".

Proposition 20.1: Let R be an equivalence relation on a set A, and let $a, b \in A$. If $a \not R b$, then $[a] \cap [b] = \emptyset$.

Proof by contrapositive:

Contrapositive statement: If $[a] \cap [b] \neq \emptyset$, then aRb.

Proof: Let $[a] \cap [b] \neq \emptyset$

$\implies \exists x \in [a] \cap [b]$

$\implies x \in [a] \land x \in [b]$ (by defn of intersection)

$\implies xRa \land xRb$ (by defn of equivalence class)

$\implies aRx \land xRb$ ($\because$ R is symmetric)

$\implies aRb$ ($\because$ R is transitive).

We have proven: If $[a] \cap [b] \neq \emptyset$, then aRb.

$\therefore$ the contrapositive statement: If $a \not R b$, then $[a] \cap [b] = \emptyset$ has been proven.

4.20.2 Reductio Ad Absurdum

Reduction to the absurd, or proof by contradiction.

To prove: If A, then B.

We show: It is impossible for A to be true when B is false.

We do this by supposing the impossible statement is true, and then show that this leads to an absurd statement.

Proof template:

To prove: If A, then B, we assume the conditions in A, and suppose – for the sake of contradiction – "not B".

Follow this up with a series of logical statements, until you reach an absurd conclusion.

(49) “No integer is both odd and even.”

Equivalent if-then statement: “If x is an integer, then x is not both even and odd.”

Proof: We will prove the above statement by contradiction.

Let x be an integer. For the sake of contradiction, let x be both even and odd.

x is even, $\therefore\ \exists k \in \mathbb{Z} : x = 2k$.

x is odd, $\therefore\ \exists r \in \mathbb{Z} : x = 2r + 1$.

So $x = 2k = 2r + 1$

$\implies 2(k - r) = 1 \implies k - r = \frac{1}{2}$.

Since $k, r \in \mathbb{Z} \implies k - r \in \mathbb{Z}$, but $\frac{1}{2} \notin \mathbb{Z}$.

$\therefore$ our assumption was false, i.e. x cannot be both even and odd.

Exercise 20.7: Prove by contradiction: If the sum of two primes is prime, then one of the primes must be 2. You may assume that every integer is either even or odd, but never both.

Proof: We will prove the statement by contradiction. Let x, y be two prime numbers, such that $x + y$ is prime. For the sake of contradiction, we assume that $x \neq 2$ and $y \neq 2$.

Since x, y are prime, that implies $x, y > 1$, and if they're not 2, then $x, y > 2$. Neither x nor y is even, because the only even prime number is 2. Both x and y are odd

$\implies \exists\ r, s \in \mathbb{Z} : x = 2r + 1, y = 2s + 1$

Then, $x + y = 2r + 2s + 1 + 1 = 2(r + s) + 2 = 2(r + s + 1)$

$\implies 2 \mid x + y$, where both $x, y > 2$

$\implies x + y$ is not prime.

But, this is a contradiction ($\because\ x + y$ is prime)

$\therefore$ our assumption was false, i.e. either $x = 2$ or $y = 2$.

$\therefore$ if the sum of two primes is prime, then one of the primes is 2.

4.21 Smallest Counterexample

Statement 21.6: **(Well Ordering Principle)** Every nonempty set of natural numbers contains a least element.

Note: For $\mathbb{Z}$, the WOP applies only in specific cases (e.g. finite sets). The same goes for $\mathbb{Q}$ and $\mathbb{R}$. Also, the WOP is an axiom, and need not be proved.

4.22 Induction

Theorem 22.2: **(Principle of Mathematical Induction)** Let A be a set of natural numbers. If

1. $0 \in A$, and
2. $\forall k \in \mathbb{N},\ k \in A \implies k + 1 \in A$,

then $A = \mathbb{N}$.

Analogy: You are trying to climb a ladder. If you can prove that you can climb the first rung, and that you can always climb the rung which succeeds the rung you're on, then you have proven that you can climb the whole ladder.

Proof of Theorem 22.2 (Using the WOP)

Let A be a set of natural numbers (i.e. $A \subseteq \mathbb{N}$). Let A satisfy conditions (1) and (2). For the sake of contradiction, assume that $A \neq \mathbb{N}$, i.e. $\mathbb{N} - A \neq \emptyset$.

Let $X = \mathbb{N} - A$. Then, by our assumption, $X \neq \emptyset$. i.e. X is a nonempty set of natural numbers.

By the WOP, X must contain a least element, say x (3).

Claim: $x \neq 0$

Because: $x \in X = \mathbb{N} - A$, i.e. $x \notin A \implies x \neq 0$ ($\because$ $0 \in A$, by (1)).

$\therefore$, $x > 0 \implies x - 1 \geq 0 \implies x - 1 \in \mathbb{N}$.

We note: $x - 1 < x$. Also, x is the samllest element in $X = \mathbb{N} - A$ (by the WOP) $\implies x - 1 \notin X$. $\implies x - 1 \in A$.

By (2): if $x - 1 \in A \implies (x-1) + 1 = x \in A$, i.e. $x \in A$.

But, this is a contradiction to (3), because $x \in X = \mathbb{N} - A$.

$\therefore$ our assumption was false.

i.e. $A \neq \mathbb{N}$ is not true $\implies A = \mathbb{N}$.

This proves our theorem.

Proposition 22.1: Let n be a positive integer. The sum of the first n odd natural numbers is n^2.

Note: PMA can be modified so as to ignore the first j natural numbers by re-phrasing it as:

Let A be a set of natural numbers $n \in \mathbb{N}$. If

1. $j + 1 \in A$
2. $\forall k \in \mathbb{N},\ k \in A \implies k + 1 \in A$,

then $A = \{x \in \mathbb{N} : x \geq j + 1\}$.

Proof of Proposition 22.1:

We prove the result using the PMI. Let A be the set of natural numbers for which equality holds in $1 + 3 + \ldots + (2n - 1) = n^2$ (1).

i.e. $r \in A \iff 1 + 3 + \ldots + (2r - 1) = r^2$.

Basic step: Is the equality true for 1?

For $r = 1$, LHS of (1) is 1, and RHS of (1) is $1^2 = 1$

$\implies 1 \in A$.

Induction hypothesis: Let us assume that $r \in A$.

i.e. we assume that (1) holds for r.

i.e. $1 + 3 + \ldots + (2r - 1) = r^2$ (2)

Induction step: To prove: for $r \in A$, $r + 1 \in A$.

Consider LHS of (1) for $r + 1$:

$$\text{LHS} = 1 + 3 + \ldots + (2(r) - 1) + (2(r + 1) - 1)$$

$$= \underbrace{(1+3+\ldots+(2r-1))}_{r^2}+(2r+1)$$

$$= r^2+(2r+1)=(r+1)^2$$

The RHS of 1 for $r+1$ is $(r+1)^2$.

$\therefore$ the LHS of (1) is equal to the RHS of (1) for $(r+1)$

i.e. equality holds in (1) for $r+1$

i.e. $r+1 \in A$.

We have shown that $\forall r \in A,\ r+1 \in A$.

$\therefore$ by the PMI, we have

1. $1 \in A$
2. $\forall r \in A,\ (r+1) \in A$

$\therefore\ A=\{1,2,\ldots\}=\mathbb{Z}^+$

Exercise 22.5: Prove the following inequalities by induction. In each case, $n \in \mathbb{Z}^+$.

e. $n! \leq n^n$ (1)

Proof: Let A be the set of positive integers for which inequality (1) holds.

i.e. $r \in A \iff r! \leq r^r$

Basic step: The inequality holds for $n=1$, i.e. $1! \leq 1^1$.

Induction hypothesis: Let us assume that the inequality holds for some $k \in \mathbb{Z}^+$, i.e. $k! \leq k^k$ (2)

Induction step: To prove $k+1 \in A$

i.e. $(k+1)! \leq (k+1)^{k+1}$.

LHS: $(k+1)!=(k+1)k! \leq (k+1)k^k \leq (k+1)(k+1)^k=(k+1)^{k+1}$

(by the binomial theorem $k^k \leq (k+1)^k$)

5 Functions

5.24 Functions

Definition 24.1: **(Function)** A relation f is called a *function* provided $(a,b) \in f$ and $(a,c) \in f$ imply $b=c$.

(50) Let $f=\{(0,1),(1,3),(3,5),(7,9)\}$, f is a function.

(51) Let $g=\{(1,2),(2,4),(2,7),(3,5)\}$, g is not a function. (However, g is still a relation)

Definition 24.5: **(Domain, image)** Let f be a function. The set of all possible first elements of the ordered pairs in f is called the *domain* of f and is denoted $\operatorname{dom} f$. The set of all possible second elements of the ordered pairs in f is called the *image* of f and is denoted $\operatorname{im} f$.

$\operatorname{dom} f=\{a : \exists b,\ (a,b) \in f\}$,

$\operatorname{im} f=\{b : \exists a,\ (a,b) \in f\}$.

(52) Consider $f = \{(x, y) : x, y \in \mathbb{Z}, y = x^2\}$. $\operatorname{dom} f = \mathbb{Z}$, $\operatorname{im} f = \{x^2 : x \in \mathbb{Z}\}$.

Definition 24.8: ($f : A \to B$) Let f be a function and let A and B be sets. We say that f is a *function from A to B* provided $\operatorname{dom} f = A$, and $\operatorname{im} f \subseteq B$. In this case, we write $f : A \to B$. We also say that f is a *mapping from A to B*.

(53) Let $f(x) = x^2$. We can say $f : \mathbb{R} \to \mathbb{R}$. Here, $\operatorname{dom} f = \mathbb{R}$, and $\operatorname{im} f = [0, \infty) \subseteq \mathbb{R}$. We call the superset of the $\operatorname{im} f$ its co-domain.

(54) Consider the sine function. We can write $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = \sin(x)$.

$\operatorname{dom} f = \mathbb{R}$. $\operatorname{im} f = [-1, 1]$.

We might even write $\sin : \mathbb{R} \to \mathbb{R}$.

Definition 24.18: **(Onto)** Let $f : A \to B$. We say that f is *onto* B provided that for every $b \in B$ there is an $a \in A$ so that $f(a) = b$. In other words, $\operatorname{im} f = B$, or the image and co-domain are equal.

If we consider $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = \sin(x)$, then f is *not* onto.

e.g. $2 \notin \operatorname{im} f$, i.e. $\nexists\, x : \sin(x) = 2$.

However, $f : \mathbb{R} \to [-1, 1]$ defined as $f(x) = \sin(x)$ is onto. Here, $\forall y \in [-1, 1],\ \exists x \in \mathbb{R} : \sin(x) = y$.

If we consider $f(x) = x^2 + 1$ and consider $f : \mathbb{R} \to \mathbb{R}$. Then, f is *not* onto.

Definition 24.13: **(One-to-one)** A function f is called *one-to-one* provided that, whenever $(x, b), (y, b) \in f$, we must have $x = y$. In other words, if $x \neq y$, then $f(x) \neq f(y)$.

(55) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 1,\ \forall x \in \mathbb{R}$

Proof: f is one-to-one:

A. Direct Method: We will prove that $\forall x_1, x_2 \in \mathbb{R}$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Let $x_1, x_2 \in \mathbb{R} : f(x_1) = f(x_2)$

$\implies 2x_1 + 1 = 2x_2 + 1$ (by definition of f)

$\implies 2x_1 = 2x_2$ (subtracting 1 from both sides)

$\implies x_1 = x_2$ (by dividing both sides by 2)

We have shown that $\forall x_1, x_2 \in \mathbb{R}$, if $f(x_1) = f(x_2) \implies x_1 = x_2$

$\therefore$ f is one-to-one (by definition of a one-to-one function).

B. By contrapositive: We will prove that $\forall x_1, x_2 \in \mathbb{R}$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

Let $x_1, x_2 \in \mathbb{R} : x_1 \neq x_2$

$\implies 2x_1 \neq 2x_2$

$\implies 2x_1 + 1 \neq 2x_2 + 1$

$\implies f(x_1) \neq f(x_2)$.

We have shown: If $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)\ \forall x_1, x_2 \in \mathbb{R}$

$\therefore$ by definition, f is one-to-one.

To prove: f is onto: We want to show:

$\forall y \in \mathbb{R},\ \exists x \in \mathbb{R}$ such that $f(x) = y$ (by definition of onto)

Let $x = \frac{y-1}{2}$, then $f\left(\frac{y-1}{2}\right) = 2\left(\frac{y-1}{2}\right) + 1 = y$ (by definition of f)

$\therefore$ given $y \in \mathbb{R}$, we found $x = \frac{y-1}{2} \in \mathbb{R}$ such that $f(x) = y$

$\therefore$ f is onto.

Definition 24.22: **(Bijection)** Let $f : A \to B$. We call f a *bijection* provided it is both one-to-one and onto.

Proposition 24.14: Let $f : A \to B$. The inverse relation f^{-1} is a function if and only if f is one-to-one.

Proposition 24.15: Let $f : A \to B$, and suppose f^{-1} is also a function. Then $\operatorname{dom} f = \operatorname{im} f^{-1}$ and $\operatorname{im} f = \operatorname{dom} f^{-1}$.

Theorem 24.21: Let A and B be sets and let $f : A \to B$. The inverse relation f^{-1} is a function from B to A if and only if f is one-to-one and onto B (i.e. f is a bijection).

Proposition 24.24: **(Pigeonhole Principle)** Let A and B be finite sets and let $f : A \to B$.

1. If $|A| > |B|$, then f is not one-to-one.
2. If $|A| < |B|$, then f is not onto.

Contrapositive statements:

1. If f is one-to-one, then $|A| \leq |B|$.
2. If f is onto, then $|A| \geq |B|$.

This leads to the following proposition:

Proposition 24.25: Let A and B be finite sets and let $f : A \to B$. If f is a bijection, then $|A| = |B|$.

If there are n letters to be delivered to m pigeonholes and $n > m$, then some pigeonholes must receive more than one letter.

7 Number Theory

7.35 Dividing

Theorem 35.1: **(Division)** Let $a, d \in \mathbb{Z}$ with $d > 0$. There exist integers q and r such that

$$a = qd + r \text{ and } 0 \leq r < d.$$

Moreover, there is only one such pair of integers (q, r) that satisfies these conditions.

Terminology: We call a the dividend, d the divisor, q the quotient, and r the remainder.

Proof:

1. Consider $A = \{a - dk : k \in \mathbb{Z}\}$ and consider $B = A \cap \mathbb{N} = \{a - dk : k \in \mathbb{Z} \text{ and } a - dk \geq 0\}$

   Claim: $B \neq \emptyset$

   Case 1: If $a \geq 0$, then $a \in B \implies B \neq \emptyset$ ($\because\ a = a - d \cdot 0 \geq 0$)

   Case 2: If $a < 0$, then choose $k < \frac{a}{d}$, then $dk < a \implies a - dk > 0 \implies a - dk \in B \implies B \neq \emptyset$

   In either case, $B \neq \emptyset$, $\therefore$ B is a non-empty set of natural numbers.

   $\therefore$ by the well-ordering principle: B must contain a least element. We call this least element r. i.e. $r \in B \implies \exists q \in \mathbb{Z} : r = a - dq$. Further, $r \geq 0$.

   We will show: $r < d$.

   Assume for the sake of contradiction that $r \not< d$, i.e. $r \geq d$

$\implies r = a - dq \geq d$

$\implies a - dq - d \geq 0$

$\implies a - d(q+1) \geq 0$

$\implies a - d(q+1) \in B$.

But, $a - d(q+1) < a - dq = r$.

$\therefore$ we have found an element in B that is smaller than r. This is a contradiction, since r is the least element of B.

$\therefore$ our assumption was false, and thus $r < d$.

$\therefore$ given $a, d \in \mathbb{Z},\ d > 0$, we have found $q, r \in \mathbb{Z} : a = dq + r$ where $0 \leq r < d$.

2. We will show the uniqueness of (q, r) (by contradiction).

   Suppose that there exist another $q', r' \in \mathbb{Z}$ such that $a = q'd + r'$, where $0 \leq r' < d$. (1)

   We already have $\exists q, r \in \mathbb{Z}$ such that $a = qd + r$, where $0 \leq r < d$. (2)

   From (1) and (2), $a = qd + r = q'd + r'$.

   $\implies d(q - q') = r' - r$ (3), where $(q - q') \in \mathbb{Z}$ (by closure of $\mathbb{Z}$)

   $\implies d \mid (r' - r)$

   But $0 \leq r, r' < d$, $\therefore$ if $d \mid (r' - r)$, then $r' - r = 0$

   $\implies r = r'$.

   From (3), $d(q - q') = 0$, but $d > 0$

   $\implies q - q' = 0 \implies q = q'$.

   $\therefore$ our assumption was false and q, r must exist uniquely.

   $\therefore$ given $a, d \in \mathbb{Z}$, $d > 0$, $\exists$ unique $q, r \in \mathbb{Z} : a = dq + r$, where $0 \leq r < d$.

Corollary 35.4: Every integer is either even or odd, but not both.

Proof: Let n be any integer. Then, by the division theorem, $\exists! q, r \in \mathbb{Z} : n = 2q + r$ where $0 \leq r < 2$.

Since $0 \leq r < 2$, $r \in \mathbb{Z}$, $\therefore\ r = 0$ or $r = 1$.

If $r = 0 \implies n = 2q \implies 2 \mid n \implies n$ is even.

If $r = 1 \implies n = 2q + 1 \implies n$ is odd.

We now prove n cannot be both even and odd (by contradiction).

Do this as an exercise

Corollary 35.5: Let $n, m \in \mathbb{Z}$. Then $n \equiv m \mod 2$ iff either n and m are both even, or n and m are both odd.

Proof: Let $n, m \in \mathbb{Z}$. Let $n \equiv m \mod 2$. To prove: Either n, m are both even, or n, m are both odd.

Since $n \equiv m \mod 2 \implies 2 \mid (n - m)$ (by definition of $\equiv \mod n$)

$\implies \exists k \in \mathbb{Z} : n - m = 2k$. (1)

Case 1: Suppose m is even $\implies m = 2r$ for some $r \in \mathbb{Z}$. Then, $n - 2r = 2k \implies n = 2\underbrace{(k + r)}_{\in \mathbb{Z}}$, $\therefore\ 2 \mid n \implies n$ is even.

Case 2: Suppose m is odd $\implies m = 2t + 1$ for some $t \in \mathbb{Z}$. $\therefore\ n - (2t + 1) = 2k$ (substitute $m = 2t + 1$ into (1))

$\implies n = 2(k + t) + 1$

$\therefore$ n is odd.

Conversely, let n, m be both odd or both even, to prove $n \equiv m \mod 2$.

Proof:

Case 1: Let n, m be both odd

$\implies n = 2k+1$ and $m = 2r+1$ for some $k, r \in \mathbb{Z}$.

$\implies n - m = (2k+1) - (2r+1) = 2(k-r)$

$\implies 2 \mid n - m \implies n \equiv m \mod 2$.

Case 2: Let n, m both be even.

Do as an exercise

Definition 35.6: **(div and mod)** Let $a, d \in \mathbb{Z}$, and $d > 0$. By the division theorem, $\exists! q, r \in \mathbb{Z} : a = dq + r$, where $0 \leq r < d$. We define the operations div and $\mod$ as follows:

$$a \operatorname{div} d = q, \text{ and } a \mod d = r.$$

Earlier, we defined $a \equiv b \mod m \iff m \mid a - b$. For example $53 \equiv 2 \mod 3$, where 2 was one of many possible answers. Now, we will think of this operation as $53 \mod 3 = 2$.

Thus, we have a new definition of the "congruence mod m" relation. It is the (non-negative) remainder that we get when a is divided by d.

7.36 Greatest Common Divisor

Definition 36.1: **(Common divisor)** Let $a, b \in \mathbb{Z}$. An integer d is called a *common divisor* of a and b if $d \mid a$ and $d \mid b$.

Definition 36.2: **(Greatest common divisor)** Let $a, b \in \mathbb{Z}$. An integer d is called the *greatest common divisor* of a and b provided

1. d is a common divisor of a and b and
2. if e is a common divisor of a and b, then $e \leq d$.

The greatest common divisor of a and b is denoted $\gcd(a, b)$.

Does every pair of integers have a gcd? Almost. Every pair except $\gcd(0, 0)$, as all numbers divide 0.

For $a, b \in \mathbb{Z}$, is the $\gcd(a, b)$ unique? Yes. One could prove it by contradiction through Definition 36.2, by assuming there are two greatest common divisors, d_1 and d_2, but finding that $d_1 \leq d_2$ and $d_2 \leq d_1$, and therefore $d_1 = d_2$.

Proposition 36.3: Let a and b be positive integers, and let $c = a \mod b$. Then

$$\gcd(a, b) = \gcd(b, c).$$

Theorem 36.6: Let a and b be integers, not both zero. The smallest positivve integer of the form $ax + by$, where x and y are integers, is $\gcd(a, b)$.

Note: The theorem states that if $d = \gcd(a, b)$, then $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$, i.e. d is a linear combination of a and b.

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

Let $D = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$.

Claim: $D \neq \emptyset$.

If we choose $x = a$, and $y = b$, then $a^2 + b^2 > 0$, meaning $a^2 + b^2 \in D$.

$\therefore$ D is a non-empty set of natural numbers.

$\therefore$ by the WOP, D must have a least element, d.

Show that: $d = \gcd(a, b)$.

Definition 36.8: Let a and b be integers. We call a and b *relatively prime* provided $\gcd(a, b) = 1$.

7.39 Factoring

Theorem 39.1: **(Fundamental Theorem of Arithmetic)** Let n be a positive integer > 1. Then n can be factored into a product of primes. Furthermore, the factorization of n into primes is unique up to the order of the primes.

Lemma 39.2: Suppose $a, b, p \in \mathbb{Z}$ and p is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Let $a, b, p \in \mathbb{Z}$ and let p be prime. By way of contradiction (BWoC), assume that $p \nmid a$ and $p \nmid b$. Now, p is prime, $\therefore$ p has factors ± 1 and $\pm p$ only. Also, $p \nmid a$. $\therefore$ $\gcd(p, a) = 1$. Therefore, by Theorem 36.6 ($\gcd(a, b) = ax + by,\ x, y \in \mathbb{Z}$), $\exists x, y \in \mathbb{Z} : px + ay = 1$. (1)

Similarly, $p \nmid b \implies \gcd(p, b) = 1 \implies \exists r, s \in \mathbb{Z} : px + bs = 1$. (2)

From (1) and (2), we get $1 = (px + ay)(pr + bs)$ (by multiplying (1) and (2))

$\implies 1 = p^2xr + pxbs + bayr + abys$

$\implies 1 = \underbrace{p(pxr + xbx + ayr)}_{\alpha} + \underbrace{(ab)ys}_{\beta}$.

Now, $p \mid \alpha$ and $p \mid \beta$ ($\because p \mid p$ and $p \mid ab$)

$\therefore p \mid p(pxr + xbx + ayr) + (ab)ys$.

$\therefore p \mid 1$, $\therefore$ we have a contradiction, and $\therefore$ our assumption was false.

$\therefore p \mid a$ or $p \mid b$.

Lemma 39.3: Suppose $p, q_1, q_2, \ldots, q_t$ are prime numbers. If

$$p \mid (q_1 q_2 \ldots q_t),$$

then $p = q_i$ for some $1 \leq i \leq t$.

Try this proof by induction, using Lemma 39.2.

Proof of the Fundamental Theorem of Arithmetic (FToA):

First, 1 can be written as an empty product of primes. $\therefore$ the result is true for $n = 1$.

BWoC, assume that not all positive integers can be written as a product of primes.

i.e. X, the set of all positive integers that cannot be factored as a product of primes is non-empty. i.e. $X \neq \emptyset$.

$\therefore$, by the WOP, X has a least element, say x.

i.e. x is the least positive integer that cannot be factored into a product of primes. Also, x is not prime (since it can be expressed as a product of just itself, which would mean it could be factored into a product of a single prime, namely x, and therefore $x \notin X$).

i.e. x is composite

$\implies \exists a \in \mathbb{Z}, 1 < a < x : a \mid x$

$\therefore\ \exists b \in \mathbb{Z} : x = ab$.

Now, $1 < b < x$, and therefore we have $1 < a,\ b < x$.

Since x is the least element of X, $\therefore a, b \notin X$

$\implies$ a and b can be factored into a product of primes.

$\implies \exists$ primes $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ such that $a = p_1 p_2 \dots p_r$ and $b = q_1 q_2 \dots q_s$

$\implies x = ab = (p_1 p_2 \dots p_r)(q_1 q_2 \dots q_s)$

i.e. x has been written as a product of primes.

This is a contradiction ($\because$ we had $x \in X$)

$\therefore$ our assumption was false, i.e. $X = \emptyset$.

i.e. every positive integer can be written as a product of primes.

Uniqueness of the prime factorization upto order.

BWoC, assume that there are positive integers for which the prime factorization is not unique. Let Y be the set of all positive integers for which the prime factorization is not unique. We are assuming that $Y \neq \emptyset$.

$\therefore$ by the WOP, Y has a least element, say y. i.e. $y \in Y$.

$\therefore$ we can write $y = \prod_{i=1}^{s} p_i = \prod_{j=1}^{t} q_j$ (3), where $\forall i, j, p_i$ and q_j are prime, and $p_i \neq q_j$. ($\because$ if $p_r = q_u$, for some r, $1 \leq r \leq s$, and some u, $1 \leq u \leq t$, then divide both sides of (3) by $p_r = q_u = w$. Then, we have $\frac{y}{w} \in \mathbb{Z}$ and $\frac{y}{w} \in Y$, but $\frac{y}{w} < y$, and y is the least element of Y $\therefore$ we have a contradiction $\implies \forall r, u, p_r \neq q_u$)

Now, $\prod_{i=1}^{s} p_i = \prod_{i=1}^{t} q_i \implies p_1 \mid \prod_{i=1}^{t} q_i$

$\therefore$ by lemma 39.3, $p_1 = q_r$ for some r, $1 \leq r \leq t$. Thus, we have a contradiction (because we assumed that $p_i \neq q_j$ for any i, j) and therefore our assumption was false,

$\therefore Y = \emptyset$, i.e. there are no positive integers that have two different prime factorizations. i.e. the prime factorization of any positive integer is unique upto order.

7.39.1 Infinitely Many Primes

Theorem 39.4: **(Infinitude of primes)** There are infinitely many primes.

Proof: (due to Euclid $\sim$ 300 B.C.E.) BWoC, assume that there are only a finite number of primes. Then, we can list them as $2, 3, 5, \dots, p$ (i.e. there is a largest prime number, p).

Let $q = (2 \cdot 3 \cdot 5 \cdot \dots \cdot p) + 1$. (1) There are two possibilities for q, i.e. q is either prime or composite.

Case 1: q is prime. Then, q must be a prime larger than p, and we have a contradiction. Therefore, q cannot be prime, i.e. q must be composite.

Case 2: q is composite.

$\implies \exists$ some prime p', $1 < p' < q$ such that $p' \mid q$. (2)

But p' must be in the list $2, 3, 5, \dots, p$, as all primes are contained in that list. $\therefore p' \mid 2 \cdot 3 \cdot 5 \cdot \dots \cdot p$. (3)

$\implies p' \mid q - 2 \cdot 3 \cdot 5 \cdot \dots \cdot p$ (because if $y \mid x_1$ and $y \mid x_2$, then $\exists r, q \in \mathbb{Z} : x_1 = yr, x_2 = ys$. And so $x_1 - x_2 = y(r - s)$, which means that $y \mid x_1 - x_2$)

$\implies p' \mid 1$ (from (1)), which is a contradiction, because p' is prime and therefore greater than 1.

$\therefore$ our assumption was false, and there is no greatest prime, i.e. there are infinitely many primes.

7.39.2 Irrationality of $\sqrt{2}$

Proposition 39.6: There is no rational number x such that $x^2 = 2$.

Proof: BWoC, assume that $\sqrt{2}$ is rational. Then, we can write $\sqrt{2} = \frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $q \neq 0$. In addition, we may assume that p and q are relatively prime, i.e. $\gcd(p, q) = 1$ (this is because we assume the fraction is fully simplified).

Since $\sqrt{2} = \frac{p}{q} \implies 2 = \frac{p^2}{q^2}$ (by squaring both sides).

$\implies 2q^2 = p^2$ (multiply by q^2)

$\implies 2 \mid p^2 \implies 2 \mid p$ (by Lemma 39.2)

$\implies \exists r \in \mathbb{Z} : p = 2r$

$\implies p^2 = 4r^2$, but $p^2 = 2q^2 \implies 2q^2 = 4r^2$

$\implies q^2 = 2r^2$

$\implies 2 \mid q^2 \implies 2 \mid q$

$\therefore$ we have $2 \mid p$ and $2 \mid q$, but this is a contradiction, because they are coprime. Therefore our assumption was false, and $\sqrt{2}$ is irrational.