Proofs
A Long-Form Mathematics Textbook
by
Jay Cummins

Deepak Kar

June 5, 2025

Chapter 1

Intuitive Proofs

Principle 1.1 (The Pigeonhole Principle)**.** *If $kn + 1$ objects are placed into n boxes, then at least one box has at least $k + 1$ objects.*

Proposition 1.1. *Given any* 101 *integers frrom* $1, 2, 3, ..., 200$*, at least one of these numbers will divide another.*

Scratch Work. Since there are 101 items, we can consider the pigeon hole principle with $k = 1$ and $n = 100$.

Let us consider the following boxes. Create a box for each of the odd numbers $1, 3, 5, ..., 199$ and for any number x if x is of the form $x = 2^k \cdot m$, where m is odd and $k >= 0$, we can put x in the box m.

There are 100 odd numbers in the set so we have 100 boxes. And any two numbers in a box only differ by 2^k for some k. Thus, for any two numbers in one box, the smaller number divides the larger one.

For any odd number larger than 101, it will be the only number in that box.

Proof. For each number n from the set $1, 2, 3, ..., 200$, write it in the form of $n = 2^k \cdot m$ where $k >= 0$ and m is an odd number.

Now, create a box for each odd number from 1 to 199. There will be 100 such boxes. For each of the given 101 integers,

If $n = 2^k \cdot m$ then put n in the box numbered m.

Since 101 integers are placed in 100 boxes, there must be at least one box with more than 1 integer by 1.1.

Suppose the box m contains two numbers of the form $n_1 = 2^k \cdot m$ and $n_2 = 2^l \cdot m$ where without loss of generality $k > l$. Then we can show that

$$\frac{n_1}{n_2} = \frac{2^k \cdot m}{2^l \cdot m} = 2^{k-l}$$

Here, 2^{k-l} is an integer since $k > l$, thus, n_2 divides n_1.

Thus, proved. □

Proposition 1.2. *Suppose G is a graph with $n \geq 2$ vertices. Then, G contains two vertices which have the same degree.*

Proof Idea. The possible degrees of a vertex is any number between 0 and $n-1$. Thus, there are n boxes for each possible value for the degree of a vertex and n vertices.

We can show that at least one box must be empty. Therefore, we need to put n vertices in $n-1$ boxes and by The Pigeonhole Principle (1.1), there must be at least two vertices in the same box, i.e., have the same degree.

We can show that both box 0 and box $n-1$ cannot have a vertex because if vertex v_1 is in box $n-1$ then it has an edge connecting it to every other vertex.

Thus, every other vertex has an edge connecting it to v_1 which implies that every other vertex has at least a degree of 1 and box 0 must be empty.

If there is no vertex in box $n-1$ then we have box $n-1$ that is empty.

Thus, at least one box is empty in both scenarios.

Proof. Let G be a graph with $n \geq 2$ vertices. Create boxes numbered from 0 to $n-1$.

Now, for each vertex, let us say it's degree is d, then put that vertex in box d. Let us take box 0 and $n-1$. Both of these boxes are either empty or have some vertex in them.

Case 1. Box $n-1$ is empty.
Since box $n-1$ is empty, we have n vertices being placed into $n-1$ boxes. Therefore, by The Pigeonhole Principle (1.1), there are at least one box with at least two vertices.

Thus, there are at least two vertices with the same degrees.

Case 2. Box $n-1$ is not empty.
The vertex in box $n-1$ must have a degree of $n-1$ which implies it has an edge connecting to $n-1$ vertices.
Therefore, all n vertices have at least one edge connecting them to another edge and all n vertices have a degree of at least 1.

This implies that box 0 must be empty since all vertices have a degree of at least 1.

Since box 0 is empty, there are n vertices placed into $n-1$ boxes.

Therefore, by The Pigeonhole Principle (1.1), there are at least two vertices in the same box and have the same degree.

Thus, proved.

□

Proposition 1.3. *If you draw five points on the surface of an orange in marker, then there is always a way to cut the orange in half so that four points (or some part of each of those points) all lie on one of the halves.*

Scratch Work. There are two subtle statements in the propsition. First it asserts that "always a way to cut the orange in half so that...". If doesn't assert that *any* such cut has this property.

Second, it is important that we say "or some part of each of those points". When you use a marker to make the points, the points are big enough that when you slice through any point, part of the point appears on *both* halves.

Classical Geometry Theorem. Given any two points on the sphere, there is a great circle that passes through those two points.

Proof. Take 2 out of 5 given points. By Classical Geometry Theorem, there is a great circle passing through these points. Thus, this great circle divides that sphere in two halves.

The remaining three points are placed among these two halves. Thus, by The Pigeonhole Principle (1.1), there are at least two points on one of the havles.

Adding the two initially chosen points to both halves, we have one half with atleast four points.

Hence, proved. □

Exercises

Problem 1.1. *Skipped.*

Problem 1.2. *Explain the error in the following "proof" that* $2 = 1$.
Let $x = y$. *Then,*

$$x^2 = xy \tag{1.1}$$
$$x^2 - y^2 = xy - y^2 \tag{1.2}$$
$$(x + y)(x - y) = y(x - y) \tag{1.3}$$
$$x + y = y \tag{1.4}$$
$$2y = y \tag{1.5}$$
$$2 = 1 \tag{1.6}$$

Solution. Since $x = y$, $x - y = 0$ and therefore, we cannot divided by $x - y$ in step 3 to get $x + y = y$ from $(x + y)(x - y) = y(x - y)$. Thus, solved.

Problem 1.3. *Suppose that* m *and* n *are positive odd integers. Using* 2×1 *dominos,*

(a) Does there exist a perfect cover of the $m \times n$ *chessboard?*

(b) If I remove 1 square from the $m \times n$ *chessboard, will it have a perfect cover?*

Solution (a)**.** In this case, there are $m \times n$ cells on the board which is an odd number. Since each domino covers only 2 cells, the total number of cells covered will always be even.

Hence, no perfect cover exists.

Scratch Work (b)**.** Let us take 3×3 chessboard. There are 9 cells on the board. Without loss of generality, let us say there are 4 white cells and 5 black cells.

Since a domino always covers 1 white and 1 black cell, the number of white and black cell must be equal for a perfect cover.

Let us remove a black cell from the above chessboard. Now there are 4 white cells and 4 black cells.

Checking all 5 black squares for removal, we find that we have a cover in every case.

Solution (b)**.** Let us assume that the board has x white cells and $x + 1$ black cells. Note: If it is not the case, we can always swap the colors and have the same setup.

Since each domino must cover exactly 1 white and 1 black cell, we must remove a black cell to have a perfect cover.

In this scenario, all the corners will have black cells since there are more black cells than white.

Now, the question is, whether we can remove any black cell.

Lemma 1.1. *For every chessboard of size $m \times n$, there exists a cover if either m or n is even.*

Proof. Let us assume that m is even. We can always turn the board if n is even.

For every column, we have an even number of cells in that column as m is even. Hence, we can cover that column with dominos.

Hence, proved. □

Let us say we removed a black cell from row r. Now, there are two cases:

Case 1. r is odd.

In this case, we can divide the remaining chessboard into $(r-1) \times n$ and $(m-r) \times n$ and cover them by Lemma 1.1.

Note: In case $r = 1$ or $r = m$, we only have one remaining part. The second part is empty and thus, requires no cover.

Since the corners are black, the left most cell of every odd row must be black because the colors are alternating. That is, all the cells in first column and rows $1, 3, 5, ..., m$ must be black.

Since r is odd, the left most cell in it must be black. Thus, the columns containing black cells in row r are odd, i.e., cells in columns $1, 3, 5, ..., n$ and row r are black.

Thus, if we remove any black cell from row r we will have divided the row into two even sized pieces, which can be covered by the dominos by Lemma 1.1.

Case 2. r is even.

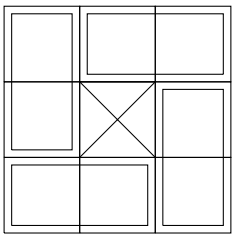
In this case, we can take rows $r-1, r, r+1$ and divide the remaining chess board in $(r-2) \times n$ and $(m-r-1) \times n$ and cover them by Lemma 1.1.

Since r is even, all the cells in row r and columns $2, 4, 8, ..., n-1$ are black.

Let us say we remove the cell in column c. Now, we can take column $c-1, c$ and $c+1$, and divide the rest of cells into chess boards of sizes $(c-2) \times 3$ and $(n-c-1) \times 3$. Since c is even, therefore, $c-2$ and $n-c-1$ are even as well.

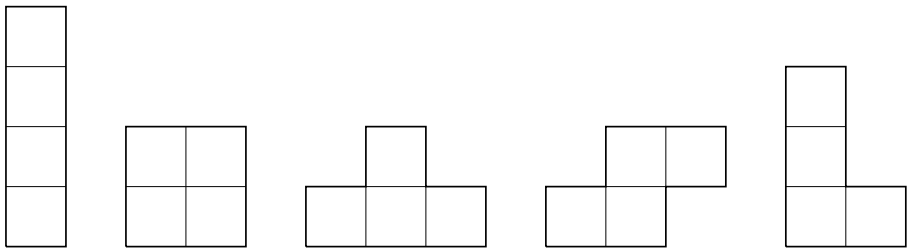
Thus, we can cover these boards using Lemma 1.1.

Now, for the remainig 3×3 board without its center, we can cover it like this:



Hence, proved.

Problem 1.4. *The game **Tetris** is played with five different shapes – the five shapes that can be obtained by piecing together four squares.*



For the questions below, we also allow these pieces to be "flipped over".

(a) Is it possible to perfectly cover a 4×5 chessboard using each of these shapes exactly once? Prove that it is impossible, or show by example that it is possible.

(b) Is it possible to perfectly cover an 8×5 chessboard using each of these shapes exactly twice? Prove that it is impossible, or show by example that it is possible.

Scratch Work. Let's color the chessboard in black and white. Here, we can see that all the shapes will cover 2 black cells and 2 white cells except the third shape.

The third shape will cover either 3 black and 1 white cell or 1 black and 3 white cells.

Therefore, if we use each shape exactly once, we will get either get a total of 11 black and 9 white cells or 9 black and 11 white cells.

Solution (a)**.** Let's assume that it is possible to cover a 4×5 chessboard using these shapes exactly once.

The chess board has exactly 10 black and 10 white cells in it. Each shape will take up exactly 2 white and 2 black cells except the third shape.

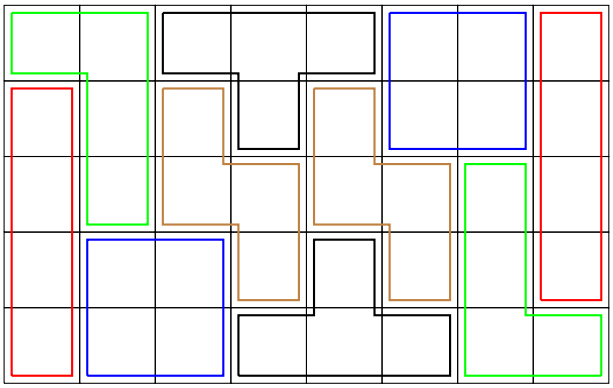
The third shape will either take up 3 black and 1 white cell or 3 white or 1 black cell. This is because all adjacent cells must be different color so if the center of the third shape is white, all the rest 3 cells of that shape must be black and vice versa.

Let's place each shape one by one.
After placing the first shape, we will have 8 black and 8 white cells.
After placing the second shape, we will have 6 black and 6 white cells.
After placing the fourth shape, we will have 4 black and 4 white cells.
After placing the fifth shape, we will have 2 black and 2 white cells.

Now, we don't have enough white or black cells to place the third shape. This is a contradiction. Therefore, it is impossible to cover a 4×5 chessboard using each of these shapes exactly once.

Hence, proved.

Solution (b)**.** Giving an example:



Hence, proved.

Problem 1.5. *If I remove two squares of different colors from an 8×8 chessboard, must the result have a perfect square?*

Solution. TODO

Problem 1.6. *If I remove four squares – two white, two black – from an 8×8 chessboard, must the result have a perfect cover?*

→ If you believe a perfect cover exists, justify why.

→ If you belive a perfect cover does not need to exist, give an example of four squares that you could remove for which the result does not have a perfect cover.

Solution. TODO

Problem 1.7. *In chess, a **knight** is a piece that can move two squares vertically and one square horizontally, or two squares horizontall and one square vertically.*

*A **knight** can legally move to any square provided there is not another piece on that same square.*

(a) Suppose there is a knight on every square of a 7×7 chessboard. Is it possible for every one of those knights to simultaneously make a legal move?

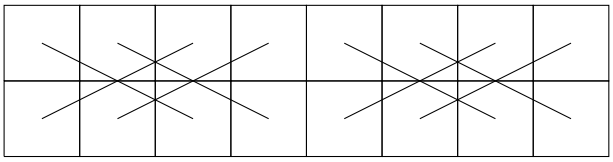
(b) Suppose there is a knight on every square of a 8×8 chessboard. Is it possible for every one of those knights to simultaneously make a legal move?

Solution (a)**.** Let us color the chessboard such that there are 24 white squares and 25 black squares without loss of generality.

In one move, a **knight** on a white square moves to a black square and vice-verse.

Since there are more black squares than white squares, we cannot move all the knight simultaneuosly such that all of them occupy different squares after the move by Principle 1.1.

Solution (b)**.** In the first two rows of the 8×8 chessboard, there are 8 white squares and 8 black squares. We can pair them up like so:



This pattern can be repeat by every two rows of the board. And the knights in these places can swap positions.

Hence, proved.

Problem 1.8. *Prove that if one chooses $n+1$ numbers from $\{1, 2, 3, ..., 2n\}$, it is guaranteed that two of the numbers that they choose are consecutive.*

Also, before the proof, write 2 example for $n = 3$, $n = 4$ and $n = 5$.

Scratch Work. For $n = 3$, we can choose 4 numbers from $\{1, 2, 3, 4, 5, 6\}$. Let them be $1, 3, 5, 6$. Here, 5 and 6 are consecutive.

For $n = 4$, we can choose 5 numbers from $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Let them be $1, 3, 5, 7, 8$. Here, 7 and 8 are consecutive.

For $n = 5$, we can choose 6 numbers from $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Let them be $1, 3, 5, 7, 9, 10$. Here, 9 and 10 are consecutive.

Solution. Let us define the n boxes numbered 1 to n. For each selected x, if $x = 2k - 1$ or $x = 2k$, put it in the box k.

Thus, box k will only contain two numbers: $2 \cdot k - 1$ and $2 \cdot k$. Both these numbers are consecutive.

Since there are $n + 1$ selected numbers atleast two numbers must be in the same box by Principle 1.1 which implies that they are consecutive.

Hence, proved.

Problem 1.9. *Assume that n is a positive integer. Prove that if one selects any $n+1$ numbers from the set $\{1, 2, 3, ..., 2n\}$, then two of the selected numbers will sum to $2n + 1$.*

Solution. Let us define n boxes numbered 1 to n such that box i contains the numbers i and $2n + 1 - i$.

Thus, we will get boxes with numbers $(1, 2n), (2, 2n - 1), ...(n, n + 1)$. Note that the numbers in a box add up to $2n + 1$.

Now, since there are $n+1$ selected numbers atleast two numbers must be in the same box by Principle 1.1 which implies that they add up two $2n + 1$.

Problem 1.10. *Explain in your own words what the general pigeonhole princple says.*

Solution. If there are n objects that are placed into m boxes then there is atleast one box with atleast $\lfloor \frac{n}{m} \rfloor$ items in it.

Problem 1.11. *Prove that there are atleast two U.S. residents that have the same weight when rounded to the nearest **millionth** of a pound.*

Solution. A quick google search tells us that there are only 3.2 million people over 300 pounds in the U.S. and the population of the U.S. is 340 million people.

Thus, there are more than 330 million people that weigh between 0 and 300 pounds.

Let us create box for each weight with a millionth of a pound of precision. This will give us 300 million boxes each denoting a weight with a precision of a millionth of a pound.

Since there are more than 300 million people in the U.S. who weigh between 0 and 300 pounds, by Principle 1.1, we can conclude that there are atleast two people with the exact same weight when rounded to a millionth of a pound.

Problem 1.12. *Determine whetehr or not the pigeonhole principle guarantees that two students at your school have the exact three leter initials.*

Solution. My school had 1000 students in each year so a total of 4000 students.

There are $26 \cdot 26 \cdot 26 = 17576$ unique three letter initials.

Therefore, the pigeonhole principle doesn't guarantee that two students at my school have the same three letter initial.

Problem 1.13. *Find your own real-world example of the pigeonhole principle.*

Solution. There are $10,000$ engineers at my workplace. But there are only 366 days in the year.

Therefore, atleast $\lfloor 10000/366 \rfloor = 27$ employees have the exact same joining anniversary.

Definition. Two integers m and n are said to be *relatively prime* if there is no integer larger than 1 which divides both m and n.

This definition will be used in the following exercise.

Problem 1.14. *Prove that if one chooses* 31 *numbers from the set* $\{1, 2, 3, ..., 60\}$*, that two of the numbers must be relatively prime.*

Solution. We can use the same method as last one. We can create 30 boxes where each box k will contain the numbers $2k - 1$ and $2k$. Thus, we will get boxes that contain the numbers $(1, 2), (3, 4), (5, 6)..., (59, 60)$.

Here, it is obvious that both numbers in a box are relatively prime.

Thus, putting 31 selected numbers in these boxes, we will get atleast one box which has atleast two numbers.

Therefore, there are two numbers that are relatively prime.

Hence, proved.

Problem 1.15. *Assume that* n *is a positive integer. Prove that if one chooses* $n+1$ *distince odd integers from* $\{1, 2, 3, ..., 3n\}$*, then atleast one of these numbers will divide another.*

Also, before your proof, check all possible selection of 4 *odd numbers from* $\{1, 2, 3, ..., 9\}$*, and for each selection locate two of the numbers for which one divdes the other.*

Scratch Work. The following are the selections:

- $\{1, 3, 5, 7\}$: 1 divides 3.
- $\{1, 3, 5, 9\}$: 1 divides 3.
- $\{1, 3, 7, 9\}$: 1 divides 3.
- $\{1, 5, 7, 9\}$: 1 divides 5.
- $\{3, 5, 7, 9\}$: 3 divides 9.

Since there are $\lfloor \frac{3n+1}{2} \rfloor$ odd numbers in the given setand we are choosing $n+1$, we need to put these numbers in n boxes.

Now, we want to choose n boxes such that in each box the smaller number divides the larger number or the box has only one number.

Let us say that for any selected number x, it can be written in the format $x = 3^k \cdot m$ where $k \geq 0$ and m is not divisible by 3.

Now there are two cases:

Case 1. n is odd.

Now if n is odd, The odd numbers are $\{1, 3, 5, 7, 9, ..., 3n\}$. There are $\frac{3n+1}{2}$ odd numebrs out of which $\frac{n+1}{2}$ are divisible by 3. Now,

$$\frac{3n+1}{2} - \frac{n+1}{2} = \frac{2n}{2} = n$$

Thus, there are n numbers not divisble by 3.

Case 2. n is even.

Now, the odd numbers are $\{1, 3, 5, 7, 9, ..., 3n-1\}$. There are $\frac{3n}{2}$ odd numbers out of which $\frac{n}{2}$ are divisble by 3.

Therefore, n numbers are not divisble by 3.

Thus, if we create a box of n numbers that are not divisble by 3. And place $n+1$ numbers in those boxes, such that if $x = 3^k \cdot m$ then put x in box m.

Then by Principle 1.1, we will have atleast one box with two numbers in it.

Let us say $x_1 = 3^{k_1} \cdot m$ and $x_2 = 3^{k_2} \cdot m$ are both in box m such that $k_1 < k_2$. Then,

$$\frac{x_1}{x_2} = \frac{3^{k_1} \cdot m}{3^{k_2} \cdot m} = 3^{k_1 - k_2}$$

Since $k_1 > k_2$, we have shown that x_2 divides x_1.

Thus, if we have two numbers in the same box, the smaller one divides the larger one.

With that, let us move on to the solution.

Solution. There are two cases that we define:

Case 1. n is even.

In this case, the odd numbers are as follows: $\{1, 3, 5, ..., 3n-1\}$. By counting them, we can say that there are $\frac{3n}{2}$ odd numbers.

The numbers in the above set that are divisible by 3 are as follows: $\{3, 9, 15, ..., 3n-3\}$. This ends at $3n-3$ because $3n$ is even. This set contains all the numbers

from the set $\{1, 3, 5, ..., n-1\}$ multiplied by 3. Thus, by counting them, we get that there are $\frac{n}{2}$ numbers divisble by 3.

Subtracting the first two counts, we get,

$$\frac{3n}{2} - \frac{n}{2} = \frac{2n}{2} = n$$

Thus, there are n numbers in the set of odd numbers between 1 to $3n$ such that they are not divisble by 3.

Case 2. n is odd.

Since n is odd $3n$ is also odd.

In this case, the odd numbers are as follows: $\{1, 3, 5, ..., 3n\}$. By counting them, we can say that there are $\frac{3n+1}{2}$ odd numbers.

The numbers in the above set that are divisible by 3 are as follows: $\{3, 9, 15, ..., 3n\}$. This set contains all the numbers from the set $\{1, 3, 5, ..., n\}$ multiplied by 3. Thus, by counting them, we get that there are $\frac{n+1}{2}$ numbers divisble by 3.

Subtracting the first two counts, we get,

$$\frac{3n+1}{2} - \frac{n+1}{2} = \frac{2n}{2} = n$$

Thus, there are n numbers in the set of odd numbers between 1 to $3n$ such that they are not divisble by 3.

Hence, we have proved that for any n, the count of odd numbers not divisble by 3 in the set $\{1, 2, 3, ..., 3n\}$ is n.

Now, let us take any number x from the set of selected $n+1$ numbers. We can write x in the form of $x = 3^k \cdot m$ where $k \geq 0$ and m is an odd number which is not divisble by 3.

Since x is an odd number, therefore, all its factors must be odd as well. This implies that we can take out all the factors that are 3 and will be left with an odd number m.

Now, let us define n boxes for each odd number in $\{1, 2, 3, ..., 3n\}$ which is not divisible by 3.

Now, we can put all $n+1$ numbers of the format $x = 3^k \cdot m$ in box m since m is not divisble by 3.

By Principle 1.1, since there are n boxes and $n+1$ numbers, there must be a box m with atleast two numbers.

Let us say that the numbers are $x_1 = 3^{k_1} \cdot m$ and $x_2 = 3^{k_2} \cdot m$ such that $k_1 > k_2$. (Note: Since they are in the same box they have the same m.)

Now, we can show that,

$$\frac{x_1}{x_2} = \frac{3^{k_1} \cdot m}{3^{k_2} \cdot m} = 3^{k_1 - k_2}$$

Since $k_1 > k_2$, we can say that x_1 is divisble by x_2.

Hence, proved.

Problem 1.16. *Give an example of* 100 *numbers from* $\{1, 2, 3, ..., 200\}$ *such that none of your selected numbers divides any of the others.*

Solution.

$$\{101, 102, 103, ..., 200\}$$

In the above set, none of the numbers divide another since any multiple for a number greater than 100 will be greater than 200.

Problem 1.17. *Prove that any set of seven integers contains a pair whose sum or difference is divisible by* 10*.*

Also, give three examples of this before your proof. Have your sets contain a diverse set collection of integers.

Scratch Work. Examples:

- $\{1, 4, 5, 9, 19, 38, 42\}$: $38 + 42 = 80$ is divisble by 10.
- $\{786, 124, 213, 468, 109, 309, 5876\}$: $786 + 124 = 910$ is divisble by 10.
- $\{16, 27, 12, 70, 29, 45, 74\}$: $16 + 74 = 90$ is divisble by 10.

Solution. Let us define 6 boxes as follows: $(0), (1, 9), (2, 8), (3, 7), (4, 6), (5)$.

Now, for each selected number we take its remainder when divided by 10. For negative numbers, we can add 10 until the remainder isn't positive.

Now, since there are 7 boxes atleast one box must have 2 or more numbers by Principle 1.1

Now, we can show that we any box contains two or more numbers then those two numbers must either add or subtract to give a number divisible by 10. We have the following cases for the box that contains two or more numbers:

Case 1. Box is (0).
Both numbers are divisble by 10 so their sum is also divisible by 10.

Case 2. Box is one of $(1, 9), (2, 8), (3, 7), (4, 6)$.
If both numbers have the same remainder then their difference is divisble by 10. If they have different remainders, then in all the cases, their remainders will add to make 10, so their sum will be divisible by 10.

Case 3. Box is (5).
Here, they both have a same remainder so their difference will be divisible by 10.

Hence, proved.

Problem 1.18. *Prove that if one chooses any* 19 *points from the interior of a* 6×4 *rectangle such that no three points are colinear, then there must exit four of these points which form a quadilateral of area at most* 4*.*

Solution. The area of the rectangle is 24. Let us divide it into 6 rectangles of are 4 and dimensions 1×4. And let us define that if a point lies on a line that is shared between two rectangles then that point is part of the upper rectangle that has a line as its edge.

Since we are choosing 19 points and we have 6 rectangles that they can be placed in. By Principle 1.1 (The Pigoenhole Principle), there must be a rectangle with at least 4 points.

Since these four points lie inside the rectangle of an areaa 4 and no three of them are colinear, therefore, they form a quadilateral and their area is at most 4.

Hence, proved.

Problem 1.19. *Assume that* 9 *points are choses from the right triangle with base and height of* 2*. Assume that no three points are colinear. Prove that there exists three points which form a triangle whose area is less than* $\frac{1}{2}$*.*

Solution. Here, the total area of the triangle is 2.

In this, the base is 2, which can be divided into 4 segments of $\frac{1}{2}$ each and we can connect them to the opposite vertex.

Here, we have 4 triangles with the same base and height. Note: Height is same because they will all have the same perpendicular from the opposite vertex. Thus, the area of these triangles is $\frac{1}{2}$.

Now, selecting 9 points that can be placed in these trianges, we will have atleast 1 triangle with 3 or more points by Principle 1.1.

Since no 3 points are colinear, these 3 points form a triangle within another triangle of area $\frac{1}{2}$. Thus, the area of this triangle is less than or equal to $\frac{1}{2}$.

The area is equal to $\frac{1}{2}$ only when the three points lie on the vertices of the triangle that they contain in.

Problem 1.20. *At a party, each person is acquainted with a certain number of others at the party and is a stranger to everyone else. Suppose there are* $n \geq 2$ *people at a party. Prove that atleast two people at this party have the same number of acquaintances at the party.*

Note: Being Acquaintances is symmetric. Every person is acquainted with atleast one person at the party.

Solution. Since every person is acquainted with atleast one person at the party and no person can obviously be acquainted with themselves, therefore, the number of acquaintances of each person must lie between 1 and $n-1$.

Let us create $n-1$ boxes and put each person in the box with the number of acquaintances that they have.

By Principle 1.1, since there are n people and $n-1$ boxes, there is atleast 1 box with atleast 2 people in it.

Therefore, there are atleast 2 people at the party with the same number of acquaintances.

Problem 1.21. *(a) Determine the population of your hometown and how many non-balding people in your homwtown, if any, are guaranteed to have the same number of hairs on their head, according to the pigeonhole principle.*

(b) Determine, as best you can, the number of students who attended your high school while you were a senior. Then, determine how many of them, if any, are guaranteed to have the same birthday according to the pigeonhole principle.

Solution. Not Interested. Not Valueable.

Problem 1.22. *The following conjectures are all false. Prove that they are false by finding a counter example to each.*

(a) Conjecture 1: If x and y are real numbers, then $|x+y| = |x| + |y|$.

Solution. $x = 1, y = -1 \implies |x+y| = 0 \neq |x| + |y| = 2$

(b) Conjecture 2: If x is a real number, then $x^2 < x^4$.

Solution. $x = 0.1 \implies x^2 = 0.01, x^4 = 0.00001 \implies x^2 > x^4$

(c) Conjecture 3: Suppose x and y are real numbers. If $|x+y| = |x-y|$, then $y = 0$.

Solution. $x = 0, y = 1, |x+y| = 1 = |x-y|$

Problem 1.23. *Suppose you deal a pile of cards, face down, from a shuffled deck of cards (only 13 cards of each suit). How many must you deal out until you are guaranteed...*

(a) five of the same suit?

Solution. By Principle 1.1, we have $n = 4$ boxes as suits. We want atleast $k + 1 = 5 (\implies k = 4)$ in some box/suit.

Thus, we must atleast have $kn + 1 = 17$ cards.

(b) two of the same rank?

Solution. By Principle 1.1, we have $n = 13$ boxes as ranks. We want atleast $k + 1 = 2 (\implies k = 1)$ in some box/rank.

Thus, we must atleast have $kn + 1 = 14$ cards.

(c) three of the same rank?

Solution. By Principle 1.1, we have $n = 13$ boxes as ranks. We want atleast $k + 1 = 3 (\implies k = 2)$ in some box/rank.

Thus, we must atleast have $kn + 1 = 27$ cards.

(d) four of the same rank?

Solution. By Principle 1.1, we have $n = 13$ boxes as ranks. We want atleast $k + 1 = 4 (\implies k = 3)$ in some box/rank.

Thus, we must atleast have $kn + 1 = 40$ cards.

(e) two of one rank and three of another?

Solution. For 3 cards of the same rank, we need atleast 40 cards.

In this case, we will already have another rank having two cards. In the worst case, scenario, there will be 2 cards in each rank/box for us to get to 40 cards for 3 cards in some rank/box.

Thus, we need atleast 40 cards.

Problem 1.24. *Determine the U.S. population at the time you are reading this.*

(a) Does the pigeonhole principle guarantee that 1 million U.S. residents have the same birthday?

Solution. There are 340 million people in the U.S. There are 366 days in the year.

Thus, $n = 366$ and $k = 1000000$ which means we only need 366 million and 1 people ($kn + 1$) for atleast one day where 1 million people have thier birthday.

We clearly have more people than neeeded for this to be guaranteed. Hence, yes.

(b) If the principle does not guarantee this, how many people are neede until that miltsone is reached? If the USA grows by 2 million people per year, in what year will this occur?

Solution. The current population does guarantee it.

Problem 1.25. *Imagine a friend gives you a deck of cards (a standard 52-card deck) and lets you shuffle it a few times. They then ask you to slowly deal out the cards, one at a time, into a new pile on the table. The entire time the cards are face-down, so they have no idea which cards you are deailing.*

At a certain point thisn procedure, they ask you to stop, and declare with confidence that the two stacks (hand and table) are in perfect balance. They say the number of red cards in the stack in your hand is equal to the number of black cards in the stack on the table. They let you count, and sure enough, they were correct.

There were no gimmicks in this procedure – no trick cards or hidden cameras or outside help. How did your friend do it?

Solution. There are 23 red and black cards each in a standard deck. Let us divide the deck randomly into two decks of 23 each and say that the first deck has r red cards and b black cards.

Now, since there are 23 red and black cards each, we have $23 - r$ red and $23 - b$ black cards in the second deck.

Now, since each deck size is 23, we know that

$$r + b = 23 \implies r = 23 - b$$

Thus, number of red cards, r, in the first deck is the same as number of black cards, $23 - b$, in the second deck.

Thus, he only had to wait till I had dealt 23 cards and stop me to make the claim.

Problem 1.26. *An alien creature has three legs, and on each o fhis three alien feet he wears an alien sock. Suppose he just washed n triplets of alien socks (3n individual socks), and each triplet is a different color. If this alien pulls out his alien socks out of his alien dryer one-at-a-time, how many must he pull out to be guaranteed to have a matching triplet?*

Solution. Here, we have n colored triplets or boxes. We want atleast one box/color to have atleast $k + 1 = 3$ socks which implies $k = 2$

Thus, by Principle 1.1, we need atleast $kn + 1 = 2n + 1$ socks.

Problem 1.27. *A magic square is an $n \times n$ matrix where teh sum of the entries in each row, column and diagonal equal the same value.*

*An **anitmagic square** is an $n \times n$ matrix where each row, column and diagonal sums to a distinct value.*

Prove that, for every n, there does not exist an $n \times n$ antimagic square where each entry is $-1, 0$ or 1.

Solution. For each $n \times n$ matrix with entries $-1, 0$ or 1, the sum of its rows, columns and diagonals can only be between $-n$ and n.

Let us create $2n + 1$ boxes labelled from $-n$ to n.

Now, there are n rows, n columns and 2 diagonals. Therefore, there are $2n + 2$ sums that need to be distinct.

But each sum must be placed in one of the $2n + 1$ boxes. Therefore, by Principle 1.1, there must be a box with two sums in it. This implies that the square cannot have distinct sum of rows, columns and diagonals.

Thus, the antimagic square of size $n \times n$ with entries $-1, 0$ or 1 is not possible.

Chapter 2

Direct Proofs

Definition 2.1. A nonzero integer a is said to *divide* an integer b if $b = ak$ for some integer k. When a divides b, we write $a \mid b$ and when a does not divide b, we write $a \nmid b$.

Proposition 2.1. *Let a, b and c be intgers. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Theorem 2.1 (The Division Algorithm)**.** *For all integers a and m witht $m > 0$, there exist unique integers q and r such that*

$$a = mq + r$$

where $0 \leq r < m$.

Definition 2.2. Let a and b be integers. If $c \mid a$ and $c \mid b$, then c is said to be a *common divisor* of a and b.

The *greatest common divisor* of a and b is the largest d such that $d \mid a$ and $d \mid b$. This number is denoted $\gcd(a, b)$.

Theorem 2.2 (Bezout's Identity)**.** *If a and b are positive integers, then there exist integers k and l such that*

$$\gcd(a, b) = ak + bl$$

Scratch Work. Let's jot down an example. Let $a = 12$ and $b = 20$, making $\gcd(a, b) = 4$. Then indeed we get,

$$4 = 12 * 2 + 20 * (-1)$$

Or maybe

$$4 = 12 * (-3) + 20 * 2$$

Proof. Assume a and b are fixed positive integers. Then the expression $ax + by$ can take infinitely many integer values for any integers x and y. It can even be 0 for $x = y = 0$.

Let d be the smallest positive integers that the expression $ax + by$ can take. And let k and l be integers for which

$$d = ak + bl \tag{2.1}$$

Now, we need to prove that $d = \gcd(a, b)$. We will do this in two parts. First, we will show that d is a common divisor of a and b. Then, we will show that $d = \gcd(a, b)$.

Part 1: d is a common divisor of a and b.

Since $d > 0$, therefore, by Theorem 2.1, there exists integers q and r such that

$$a = dq + r$$

with $0 \leq r < d$. By rewriting this, we get,

$$\begin{aligned} r &= a - dq && (2.2)\\ &= a - (ak + bl)q && (2.3)\\ &= a - akq - blq && (2.4)\\ &= a(1 - kq) + b(-lq) && (2.5) \end{aligned}$$

Since $1 - kq$ and $-lq$ are integers, we have found another expression of the form $ax + by$. But since $0 \leq r < d$ and d was the smallest posititve integer of the form $ax + by$ then it must be true that $r = 0$.

Therefore, we have the equation $a = dq + r$ which simplifies to $a = dq$. And thus, by Definition 2.1, $d \mid a$.

Similarly, we can also prove that $d \mid b$. Thus, d is a common divisor of a and b.

Part 2: d is the greatest common divisor of a and b.

Suppose that d' is another common divisor of a and b. Here, we must show that $d' \leq d$ for all such d'.

By Definition 2.1, we have

$$a = d'm \text{ and } b = d'n$$

for some integers m and n. Then, applying the above to Equation 2.1,

$$\begin{aligned} d &= ak + bl && (2.6)\\ &= d'mk + d'nl && (2.7)\\ &= d'(mk + nl) && (2.8)\\ \implies d' &= \frac{d}{mk + nl} && (2.9) \end{aligned}$$

Since $mk + nl$ is an integer and d is positive, this implies that $d' \leq d$.

Note: If $mk + nl$ is negative then d' is negative and it is trivial that $d' \leq d$. If $mk + nl$ is positive then $d' = \frac{d}{mk+nl}$ implies that $d' \leq d$.

Thus, d is in fact the greatest common divisor of a and b, i.e.,

$$\gcd(a, b) = d = ak + bl$$

Hence, proved. □

Definition 2.3. For integers a, r and m, we say that a *is congruent to* r *modulo* m, and we write $a \equiv r \pmod{m}$, if $m \mid (a - r)$.

Proposition 2.2 (Properties of Modular Arithmetic)**.** *Assume that a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,*

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $a \cdot c \equiv b \cdot d \pmod{m}$

Definition 2.4. An integer $p \geq 2$ is *prime* if its only positive divisors are 1 and p. An integer $p \geq 2$ is *composite* if it is not prime.

Equivalently, n is composite if it can be written as $n = st$, where s and t are integers and $1 < s, t < n$.

Lemma 2.1. *Let a, b and c be integers, and let p be a prime.*

1. *If $p \nmid a$, then $\gcd(p, a) = 1$.*
2. *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*
3. *If $p \mid bc$, then $p \mid b$ or $p \mid c$.*

Proposition 2.3 (Modular Cancellation Law)**.** *Le a, b, k and m be integers, with $k \neq 0$. If $ak \equiv bk \pmod{m}$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod{m}$.*

Scratch Work. Here, we have the following:

$$ak \equiv bk \pmod{m} \tag{2.10}$$
$$\implies (ak - bk) = mq \tag{2.11}$$
$$\implies (a - b)k = mq \tag{2.12}$$
$$\implies k \mid mq \tag{2.13}$$

By Lemma 2.1(2), since $\gcd(k, m) = 1$, we get $k \mid q$, therefore, $q = kl$ for some integer l.

$$(a - b)k = mkl \implies a - b = ml \implies m \mid (a - b) \implies a \equiv b \pmod{m}$$

Proof. Since $ak \equiv bk \pmod{m}$, by Definition 2.3 and 2.1, we have, $ak - bk = mp$ for some integer p.

$$ak - bk = mp \implies (a - b)k = mp \implies k \mid mp$$

Now, since $\gcd(k, m) = 1$, by Lemma 2.1(2), we get $k \mid p \implies p = kq$ for some integer q.

$$(a-b)k = mp \implies (a-b)k = mkq \implies (a-b) = mq \implies m \mid (a-b)$$

Now, by Definition 2.3, we can say that $a \equiv b \pmod{m}$.

Hence, proved. □

Theorem 2.3 (Fermat's Little Theorem)**.** *If a is an integer and p is a prime which does not divide a, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Scratch Work. The all-important observation is the following, which we explain through the example $a = 4$ and $p = 7$. Consider two sets:

$$\{a, 2a, 3a, 4a, 5a, 6a\} \text{ and } \{1, 2, 3, 4, 5, 6\}$$

In this example, since $a = 4$, this is the same as

$$\{4, 8, 12, 16, 20, 24\} \text{ and } \{1, 2, 3, 4, 5, 6\}$$

These look like completely different sets. But look what happens when you consider each of the numbers module p; the second set stays the same but the numbers in the first set change.

$$\{4, 1, 5, 2, 6, 3\} \text{ and } \{1, 2, 3, 4, 5, 6\}$$

Now, these two sets are the same. Since the order doesn't matter in multiplication, this means that

$$a \cdot 2a \cdot 3a \cdot 4a \cdot 5a \cdot 6a \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}$$

Proof. Assume that a is an integer and p is prime which does not divide a. We begin by proving that when taking module p

$$\{a, 2a, 3a, ..., (p-1)a\} \equiv \{1, 2, 3, ..., p-1\} \pmod{p}$$

To do this observe that set on the right has every module except 0. Thus, if we can show that no number on the left hand side is 0 module p and all of them are unique module p, then both sets must have the same elements module p.

Step 1. No element in the set $\{a, 2a, 3a, ..., (p-1)a\}$ is congruent to 0 module p.

Let us take an element ia from the set and assume that it is congruent to 0 modulo p. By Definition 2.3, we get that $p \mid ia$.

Since $p \nmid a$, by Lemma 2.1, we get that $\gcd(p, a) = 1$.

By Lemma 2.1(2), we get that $p \mid i$. This is a contradiction since for all $i \in \{1, 2, 3, ..., p-1\}$, $p \nmid i$.

Thus, our initial assumption that $ia \equiv 0 \pmod{p}$ must be wrong.

Hence, proved.

Step 2. All elements in the set $\{a, 2a, 3a, ..., (p-1)a$ are unique modulo p.

Let us take two elements ia and ja from the above set such that $ia \equiv ja \pmod{p}$.

Since $\gcd(a, p) = 1$ as shown before, by Proposition 2.3, we get that $i \equiv j \pmod{p}$.

Since i and j are in the set $\{1, 2, 3, ..., (p-1)\}$, we can say that $i = j$ since no two elements in the set are congruent to each other module p.

Thus, we get that $ia \equiv ja \pmod{p} \implies i = j$ and that all the elements are unique in the given set module p.

These two steps complete the proof that

$$\{a, 2a, 3a, ..., (p-1)a\} \equiv \{1, 2, 3, ..., p-1\} \pmod{p}$$

Now, since the order doesn't matter in multiplication we can say that

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \pmod{p}$$

Since for each i such that $2 \leq i \leq p-1$, we know that $p \nmid i$, we get that $\gcd(p, i) = 1$. Therefore, by Proposition 2.3, we get

$$\underbrace{a \cdot a \cdot a \cdot ... \cdot a}_{p-1 \text{ times}} \equiv 1 \pmod{p}$$

$$\implies a^{p-1} \equiv 1 \pmod{p}$$

Hence, proved. □

Theorem 2.4 (Euler's Theorem)**.** *If a and N are positive integers which are relatively prime then*

$$a^{\phi(N)} \equiv 1 \pmod{N}$$

Exercises

Problem 2.1. *Skipped.*

Problem 2.2. *The following are the squares of four numbers, each ending in* 5.

$$15^2 = 225, 25^2 = 625, 35^2 = 1225, 45^2 = 2025$$

Lookiung at these four squares, do you see anythign interesting about their answers. Once you have noticed a pattern, answer the following.

(a) Write down a conjecture that explains that the answer is for the square of any integer ending in 5*.*

Solution.

Conjecture. Any integer ending in 5 has a square which ends in 25.

(b) Give four more examples illustrating your conjecture.

Solution.

$$5^2 = 25, 55^2 = 3025, (-15)^2 = 225, (-25)^2 = 625$$

(c) Prove your conjecture.

Solution. For any integer ending in 5 would be of the form $10a + 5$ for some integer a. Now, we can show that,

$$\begin{aligned}(10a + 5)^2 &= (10a)^2 + 2 \cdot 10a \cdot 5 + 5^2 && (2.14)\\ &= 100a^2 + 100a + 25 && (2.15)\\ &= 100(a^2 + a) + 25 && (2.16)\end{aligned}$$

Since a is an integer, therefore, $a^2 + a$ is also an integer. Thus, the square is of the form $100k + 25$ where $k = a^2 + a$ is an integer.

This proves that the square of the number ends in 25.

Hence, proved.

Problem 2.3. *For each of the following, prove that it is true.*

(a) The sum of an even integer and an odd integer is odd.

Solution. Let a be an even integer and b be an odd integer. By definition, there exist some integers k and l such that $a = 2k$ and $b = 2l + 1$.

Now,

$$a + b = 2k + 2l + 1 = 2(k + l) + 1$$

Since k and l are integers, therefore, $k + l$ is also an integer. Thus, for $a + b$ there exist an integer $m = k + l$ such that $a + b = 2m + 1$. This proves that $a + b$ is odd.

Hence, proved.

(b) The product of two even integers is even.

Solution. Let $a = 2k$ and $b = 2l$ be two even integers such that k and l are integers. Now,

$$a \cdot b = 2k \cdot 2l = 4kl = 2 \cdot (2kl)$$

Since k and l are integers, therefore, $2kl$ is also an integers. This proves that $a \cdot b = 2m$ for some integer m. Hence, proved.

(c) The product of two odd integers is odd.

Solution. Let $a = 2k + 1$ and $b = 2l + 1$ be two odd integers for some integers k and l. Now,

$$\begin{aligned} a \cdot b &= (2k + 1) \cdot (2l + 1) && (2.17)\\ &= 2k \cdot 2l + 2k \cdot 1 + 1 \cdot 2l + 1 \cdot 1 && (2.18)\\ &= 4kl + 2k + 2l + 1 && (2.19)\\ &= 2(2kl + k + l) + 1 && (2.20) \end{aligned}$$

Here, $2kl + k + l$ is an integer since k and l are integers. This proves that $a \cdot b = 2m + 1$ for some integer m and thus, $a \cdot b$ is odd.

Hence, proved.

(d) The product of an even integer and an odd integer is even.

Solution. Let $a = 2k$ and $b = 2l + 1$ be an even and odd integer respectively for some integers k and l. Now,

$$a \cdot b = 2k \cdot b = 2 \cdot (kb)$$

Here, since k and b are integers, we have shown that $a \cdot b = 2m$ for some integer m and thus, $a \cdot b$ is even.

Hence, proved.

(e) An even integer squaredd is an even integer.

Solution. Let $a = 2k$ be an even integer for some integer k. Now,

$$a^2 = a \cdot a = 2k \cdot 2k = 2 \cdot (2k^2)$$

Here $2k^2$ is an integer since k is an integer. Thus, we have shown that $a^2 = 2m$ for some integer m and thus, a^2 is even.

Hence, proved.

Problem 2.4. *For each of the following, prove that it is true.*

(a) If n is an even integer, then $-n$ is an even integer.

Solution. Let $n = 2k$ be an even integer for some integer k. Now, $-n = -2k = 2 \cdot (-k)$. Since k is an integer, $-k$ is also an integer. Thus, we have shown that $-n$ is an even integer. Hence, proved.

(b) If n is an odd integer, then $-n$ is an odd integer.

Solution. Let $n = 2k + 1$ be an odd integer for some integer k. Now, $-n = -(2k + 1) = -2k - 1 = -2k - 2 + 1 = 2(-k - 1) + 1$.

Since k is an integer, $-k - 1$ is also an integer. Thus, we have shown that $-n$ is an odd integer. Hence, proved.

(c) If n is an even integer, then $(-1)^n = 1$.

Solution. Let $n = 2k$ be an even ingger for some integer k. Now,

$$(-1)^n = (-1)^{2k} = ((-1)^2)^k = 1^k = 1$$

Hence, proved.

Problem 2.5. *Prove the following:*

(a) If n is odd, then $n^2 + 4n + 9$ is even.

Solution. Let $n = 2k + 1$ be an odd integer for some integer k.

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$

$$4n = 4(2k + 1) = 8k + 4$$

$$n^2 + 4n + 9 = 4k^2 + 4k + 1 + 8k + 4 + 9 = 4k^2 + 12k + 10 = 2(2k^2 + 6k + 5)$$

Since k is an integer, therefore, $2k^2 + 6k + 5$ is also an integer. Thus, we have shown that $n^2 + 4n + 9 = 2m$ for some integer m and therefore, $n^2 + 4n + 9$ is even.

Hence, proved.

(b) If n is odd, then n^3 is odd.

Solution. Let $n = 2k + 1$ for some integer k. Then,

$$n^3 = (2k + 1)^3 = (2k + 1)(4k^2 + 4k + 1)$$

$$n^3 = 8k^3 + 8k^2 + 2k + 4k^2 + 4k + 1 = 8k^3 + 12k^2 + 6k + 1$$

$$n^3 = 2(4k^3 + 6k^2 + 3k) + 1$$

Hence, proved.

(c) If n is even, then $n + 1$ is odd.

Solution. Let $n = 2k$ for some integer k, then $n + 1 = 2k + 1$ which is odd by definition. Hence, proved.

Problem 2.6. *Prove the following. For each m and n are integers.*

(a) If m and n are odd, then $5m - 3n$ is even.

Solution. Let $m = 2k + 1$ and $n = 2l + 1$ by definition of odd numbers.

$$5m-3n = 5(2k+1)-3(2l+1) = 10k+5-6l-3 = 10k-6l+2 = 2(5k-3l+1)$$

Hence, proved.

(b) If m and n are even, then $3mn$ is divisible by 4.

Solution. Let $m = 2k$ and $n = 2l$ by definition of even numbers.

$$3mn = 3 \cdot 2k \cdot 2l = 12kl = 4 \cdot 3kl$$

By Definition 2.1, $4 \mid 3mn$. Hence, proved.

Problem 2.7. *Skipped.*

Problem 2.8. *Skipped.*

Problem 2.9. *Skipped.*

Problem 2.10. *Prove the following. For each m, n and l are integers.*

(a) If $m \mid n$, then $m^2 \mid n^2$

Solution. By Definition 2.1, since $m \mid n$, there exists an integer k such that $n = mk$ which implies that $n^2 = m^2 \cdot k^2$. Again by definition 2.1, $m^2 \mid n^2$. Hence, proved.

(b) If $m \mid n$, then $m \mid (7n^3 + 13n^2 - n)$

Solution. We can show that $7n^3 + 13n^2 - n = n \cdot (7n^2 + 13n - 1)$ which by definition 2.1 implies that $n \mid (7n^3 + 13n^2 - n)$. Now, by Proposition 2.1, since $n \mid n$, we can say that $m \mid (7n^3 + 13n^2 - n)$

(c) If $m \mid n$ and $m \mid l$, then $m \mid (n + l)$.

Solution. By Definition 2.1, we get $n = ma$ and $l = mb$ for some integers a and b. Therefore, $n + l = ma + mb = m(a + b)$ which by definition 2.1 implies that $m \mid (n + l)$. Hence, proved.

(d) If $3 \mid 2n$, then $3 \mid n$

Solution. Since $\gcd(3, 2) = 1$, then by Lemma 2.1(2), $3 \mid n$.

(e) If $9 \mid 6n$, then $3 \mid n$.

Solution. By Definition 2.1, for some integer a, $6n = 9a \implies 2n = 3a$. Thus, by (d), $3 \mid n$.

(f) If $m^3 \mid n$ and $n^4 \mid t$ then $m^12 \mid t$.

Solution. By Definition 2.1, $t = n^4 \cdot k$ and $n = m^3 \cdot l$ for some integers k and l. This implies that $t = (m^3 \cdot l)^4 \cdot k = m^1 2 \cdot l^4 \cdot k$. Thus, by Definition 2.1, $m^1 2 \mid t$. Hence, proved.

Problem 2.11. *Skipped.*

Problem 2.12. *Prove that if m and n are positive real numbers and $m < n$, then $m^2 < n^2$. You may use the fact that if $a < b$ and c is positive, then $ac < bc$.*

Solution.

$$m < n, m > 0 \implies m^2 < mn \tag{2.21}$$

$$m < n, n > 0 \implies mn < n^2 \tag{2.22}$$

$$m^2 < mn, mn < n^2 \implies m^2 < n^2 \tag{2.23}$$

Problem 2.13. *Define the absolute value of a real number x in this way:*

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

Prove that $|xy| = |x| \cdot |y|$.

Solution. Let us take 4 cases:

Case 1. $x = 0$ or $y = 0$.

Without loss of generality, let us assume that $x = 0$.

This implies that $xy = 0$. Thus, $|xy| = 0$ and $|x| = 0$, therefore, $|x| \cdot |y| = 0 = |xy|$. Hence, proved.

Case 2. $x > 0$ and $y > 0$.

This implies that $xy > 0$ so $|xy| = xy, |x| = x$ and $|y| = y$. Thus, $|xy| = xy = |x| \cdot |y|$. Hence, proved.

Case 3. $x < 0$ and $y < 0$.

This implies that $xy > 0$ so $|xy| = xy, |x| = -x$ and $|y| = -y$. Thus, $|x| \cdot |y| = (-x) \cdot (-y) = xy = |xy|$. Hence, proved.

Case 4. Without loss of generality, $x < 0$ and $y > 0$.

This implies that $xy < 0$. Here, $|xy| = -xy, |x| = -x$ and $|y| = y$. Therefore, $|x| \cdot |y| = (-x) \cdot y = -xy = |xy|$. Hence, proved.

Problem 2.14. *Prove that if m, n and t are integers, then at least one of $m-n$, $n-t$ and $m-t$ is even. Also write down three example, and show which of $m-n$, $n-t$ or $m-t$ are even.*

Scratch Work.

$m = 1, n = 2, t = 3 \implies m-n = -1, n-t = -1, m-t = -2 \implies m-t$ is even.

$m = 54, n = 29, t = 20 \implies m-n = 25, n-t = 9, m-t = 34 \implies m-t$ is even.

$m = 19, n = 45, t = 77 \implies m-n = -26, n-t = -32, m-t = -58 \implies m-n$ is even.

Proof. Since all integers are either even or odd, by The Pigeonhole Principle (1.1), we know that atleast two of m, n or t have the same parity, i.e., two of them are either both odd or both even.

Lemma 2.2. *If a and b are integers that have the same parity then $a - b$ is even.*

Lemma Proof. Case 1. a and b are even.

By definition, $a = 2k$ and $b = 2l$ then $a - b = 2k - 2l = 2(k - l)$. Thus, $a - b$ is even by definition.

Case 2. a and b are odd.

By definition, $a = 2k + 1$ and $b = 2l + 1$ then $a - b = (2k + 1) - (2l + 1) = 2k - 2l = 2(k - l)$. Thus, $a - b$ is even by definition.

Hence, proved. □

Since atleast two of m, n or t have the same parity then there is atleast one even number in $m - n$, $n - t$ and $m - t$ by Lemma **??**. □

Problem 2.15. *Prove the following:*

(a) Prove that if n is a positive integer, then 4 divides $1 + (-1)^n(2n - 1)$.

Solution. Given $n > 0$, we know that n is either even or odd. Let us define two cases:

Case 1. n is even.

By Definition, $n = 2k$ for some integer k. Therefore, we know that $(-1)^n = (-1)^{2k} = ((-1)^2)^k = (1)^k = 1$. Thus,

$$1 + (-1)^n(2n - 1) = 1 + 2n - 1 = 2n = 2 \cdot 2k = 4k$$

Thus, by Defintion 2.1, $4 \mid 1 + (-1)^n(2n - 1)$

Case 2. n is odd.

By Definition, $n = 2k + 1$ for some integer k. Therefore, we know that $(-1)^n = (-1)^{2k+1} = (-1)^{2k} \cdot (-1) = -1$ since $(-1)^{2k} = 1$. Thus, we get,

$$\begin{aligned} 1 + (-1)^n(2n - 1) &= 1 + (-1)(2n - 1) && (2.24)\\ &= 1 - 2n + 1 = 2 - 2n && (2.25)\\ &= 2 - 2(2k + 1) && (2.26)\\ &= 2 - 4k - 2 = -4k && (2.27) \end{aligned}$$

Thus, by Defintion 2.1, $4 \mid 1 + (-1)^n(2n - 1)$

Hence, proved.

(b) Prove that every multiple of 4 is equal to $1 + (-1)^n(2n - 1)$ for some positive integer n.

Solution. Let us take a multiple of 4 as $4k$. We have two cases:

Case 1. $k \geq 0$

Since $(-1)^{2k} = 1$, we can show,

$$4k = 2 \cdot 2k = 1 + 2 \cdot 2k - 1 = 1 + (-1)^{2k}(2 \cdot 2k - 1)$$

If we substitute, $n = 2k$, we get,

$$4k = 1 + (-1)^n(2n - 1)$$

Thus, $k \geq 0$ satisfies the condition.

Case 2. $k < 0$ Let us define $l = -k$ which implies that $l > 0$.

$$4k = -4l = 2 - 4l - 2 = 2 - 2(2l + 1)$$

Let us substitute $n = 2l + 1$.

$$4k = 2 - 2n = 1 - 2n + 1 = 1 - (2n - 1) = 1 + (-1)(2n - 1)$$

Since $(-1)^{2l} = 1 \implies (-1)^{2l+1} = (-1)^n = -1$, we get that

$$4k = 1 + (-1)^n(2n - 1)$$

Thus, proved.

Problem 2.16. *Skipped.*

Problem 2.17. *Skipped.*

Problem 2.18. *Skipped.*

Problem 2.19. *Let a and b be positive integers, and suppose r is the nonzero remainder when b is divided by a. Prove that when $-b$ is divided by a, the remainder is $a - r$.*

Solution. By Theorem 2.1, we can say that $b = aq + r$ such that $0 \leq r < a$. But we are given that r is nonzero, therefore, $0 < r < a$. Now,

$$-b = -aq - r = -a - aq + a - r = a(-1 - q) + (a - r)$$

Since $0 < r < a$, we can show that

$$r < a \implies a - r > 0, r > 0 \implies r > a - a \implies a > a - r$$

Thus, we have $0 < a - r < a$. By applying Theorem 2.1, we get that the remainder on dividing $-b$ by a is $a - r$.

Hence, proved.

Problem 2.20. *Determine the remainder when 3^302 is divided by 28, and show without a calculator how you found the answer.*

Solution.

$$3^{302} = 3^2 \cdot 3^{300} \pmod{28} \tag{2.28}$$
$$= 9 \cdot (3^3)^{100} \pmod{28} \tag{2.29}$$
$$= 9 \cdot 27^{100} \pmod{28} \tag{2.30}$$
$$\tag{2.31}$$

Since $27 \equiv -1 \pmod{28}$, then by Proposition 2.2(3), we get that $27^{100} \equiv (-1)^{100} \pmod{28}$ since exponentiation is just repeated multiplication.

$$3^{302} = 9 \cdot (-1)^{100} \pmod{28} \tag{2.32}$$
$$3^{302} = 9 \cdot 1 \pmod{28} \tag{2.33}$$
$$3^{302} = 9 \pmod{28} \tag{2.34}$$

Thus, the answer is 9.

Problem 2.21. *Assume that a, b, c, d and n are integers. Also assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Prove the following*

(i) $a - c \equiv b - d \pmod{n}$

Solution. By Definition 2.3, we get that $n \mid (a-b)$ and $n \mid (c-d)$ which implies that $a - b = nk$ and $c - d = nl$ for some integers k and l. Now,

$$(a - c) - (b - d) = a - c - b + d = (a - b) - (c - d) = nk - nl = n(k - l)$$

Thus, $n \mid ((a - c) - (b - d))$ and by Definition 2.3, $a - c \equiv b - d \pmod{n}$

(ii) $a \cdot c \equiv b \cdot d \pmod{n}$

Solution. As shown above, we have $a - b = nk$ and $c - d = nl$ for some integers k and l. This gives us $a = b + nk$ and $c = d + nl$. Now,

$$a \cdot c = (b + nk) \cdot (d + nl) \tag{2.35}$$
$$= bd + bnl + dnk + n^2kl \tag{2.36}$$
$$= bd + n(bl + dk + nkl) \tag{2.37}$$
$$\implies (ac - bd) = n(bl + dk + nkl) \tag{2.38}$$
$$\implies n \mid (ac - bd) \tag{2.39}$$

Thus, by Definition 2.3, $ac \equiv bd \pmod{n}$.

Problem 2.22. *Assume that a is an integer and p and q are distint primes. Prove that if $p \mid a$ and $q \mid a$, then $pq \mid a$.*

Solution. By Definition 2.1, we get that $a = pk$ for some integer k. Now, $q \mid a \implies q \mid pk$.

Since p and q are distinct primes their only factors are $1, p$ and $1, q$ respectively. Therefore, $\gcd(p, q) = 1$. Thus, by Lemma 2.1(2), we get $q \mid k$.

Thus, by Definition 2.1, $k = ql$ for some integer l and we get that $a = pql$ which by Definiton 2.1 implies that $pq \mid a$.

Hence, proved.

Problem 2.23. *Prove that if abc is a multiple of 10 then atleast one of ab, bc or ac is a multiple of 10.*

Solution. By Proposition 2.1, since $2 \mid 10$ and $5 \mid 10$, we get that $2 \mid abc$ and $5 \mid abc$.

Now, by Lemma 2.1(3), we get that atleast one of the following is true: $2 \mid a$ or $2 \mid b$ or $2 \mid c$ since 2 is a prime.

Similarly, since 5 is a prime atleast one of these is true: $5 \mid a$ or $5 \mid b$ or $5 \mid c$.

There are two cases:

Case 1. 2 and 5 divide the same number among a, b or c.

Without loss of generality, let us assume that $2 \mid a$ and $5 \mid a$. Then by previous problem, we can say that $10 \mid a$ which implies $a = 10k$ for some integer k.

Since $a = 10k$, we have $ab = 10kb$ which by Definition 2.1 means $10 \div ab$.

Case 2. 2 and 5 divide different numbers among a, b or c.

Without loss of generality, let us assume that $2 \mid a$ and $5 \mid b$. Thus, by Definition 2.1, we have $a = 2k$ and $b = 5l$ for some integers k and l.

Now, $ab = 10kl$ which by Definition 2.1 means $10 \mid ab$.

Thus, in both cases there exists atleast one number among ab, bc or ac divisible by 10.

Hence, proved.

Problem 2.24. *Assume that a, b and c are integers and $a^2 \mid b$ and $b^3 \mid c$. Prove that $a^6 \mid c$.*

Solution. By Definition 2.1, we have $b = a^2 \cdot k$ and $c = b^3 \cdot l$ for some integers k and l. Thus,

$$c = b^3 \cdot l = (a^2 \cdot k)^3 \cdot l = a^6 \cdot k^3 \cdot l$$

Hence, by Definiton 2.1, $a^6 \mid c$. Hence, proved.

Problem 2.25. *Prove that for every integer n, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.*

Scratch Work.

$$n^2 = 4k \implies 4 \mid n^2 \implies 2 \mid n \implies n = 2l$$

$$n^2 = 4k + 1 \implies 4 \mid (n^2 - 1) \mid 4 \mid (n-1)(n+1)$$

Since $n - 1$ and $n + 1$ are 2 apart, they are either both odd or both even. Since product of odd numbers is always odd, they must be even. Thus, n is odd.

Here, we see that if $n^2 \equiv 0 \pmod 4$ then n must be even. And otherwise n must be odd.

Solution. Let us take two cases:

Case 1. n is even.

By Definition, $n = 2k$ for some integer k. Thus, $n^2 = 4k^2$ which by Definition 2.1 and 2.3 means that $4 \mid n^2 \implies n^2 \equiv 0 \pmod 4$.

Case 2. n is odd.
By Definition, $n = 2k + 1$ for some integer k. Thus,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

$$\implies n^2 - 1 = 4(k^2 + k)$$

Thus, by Definition 2.3, we get that $n^2 \equiv 1 \pmod 4$.
Hence, proved.

Problem 2.26. *Skipped.*

Problem 2.27. *The Pythagorean theorem involves integers a, b and c for which $a^2 + b^2 = c^2$. Prove that if three integers satisfy this relationship, then either a or b will be divisible by 3.*

Scratch Work. For every integer n, we know $n \pmod 3$ is either $0, 1$ or 2. This implies that $n^2 \pmod 3$ is either $0, 1$ or 4 which is the same as 0 or 1.

Thus, a^2, b^2 and c^2 are either 0 or 1 modulo 3.

Let us assume that both a^2 and b^2 are 1 modulo 3. Then, c^2 must be 2 modulo 3 which is a contradiction. Therefore, either a^2 or b^2 must be divisible by 3 which implies either a or b must be divisible by 3.

Solution.

Lemma 2.3. *For any integer n, either $n^2 \equiv 0 \pmod 3$ or $n^2 \equiv 0 \pmod 3$.*

Proof. For any integer n, we have 3 cases:
Case 1. $n \equiv 0 \pmod 3 \implies n^2 \equiv 0 \pmod 3$ by Proposition 2.2(3).
Case 2. $n \equiv 1 \pmod 3 \implies n^2 \equiv 1 \pmod 3$ by Proposition refmodprop(3).
Case 3. $n \equiv 2 \pmod 3 \implies n^2 \equiv 4 \equiv 1 \pmod 3$ by Proposition 2.2(3).
Hence, proved. □

Since a and b are integers, by Lemma **??**, a^2 and b^2 are either 0 or 1 modulo 3.

Let us assume both a^2 and b^2 are 1 modulo 3. Thus, by Proposition 2.2(3), we get that $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 3$.

But by Lemma **??**, we know that $c^2 \not\equiv 2 \pmod 3$. This is a contradiction. Therefore, either a^2 or b^2 is congruent to 0 modulo 3 which by Definition 2.3 means that either $3 \mid a^2$ or $3 \mid b^2$.

Without loss of generality, let us assume that $3 \mid a^2$. By Lemma 2.1(3), since $3 \mid a \cdot a$ and 3 is prime, we get either $3 \mid a$ or $3 \mid a$ which impiles $3 \mid a$.

Therefore, either a or b must be divisible by 3. Hence, proved.

Problem 2.28. *Skipped.*

Problem 2.29. *Suppose that a and b are positive integers, and $\gcd(a, b) = d$. Prove that $a \mid b$ if and only if $d = a$. To do this, here are the two things you should prove:*
(i) If $a \mid b$, then $d = a$.

Solution. Since $a \mid a$ and $a \mid b$, a is a common divisor of a and b.

For any other common divisor $d' > 0$, we must have $d' \mid a$. Thus, $a = d'k$ for some integer k. Since a and d' are positive, then k must be positive as well. This implies that $d' = \frac{a}{k}$ where k is a positive intger. Hence, $d' \leq a$.

Thus, a is greater than any other common divisor of a and b which by Definition 2.2 implies that $d = a$.

Hence, proved.

(ii) If $d = a$, then $a \mid b$.

Solution. Since a is the greatest common divisor of a and b, then by Definition 2.2, $a \mid b$.

Hence, proved.

Problem 2.30. *Prove that $m \equiv n \pmod{15}$ if and only if $m \equiv n \pmod 3$ and $m \equiv n \pmod 5$. To do that, prove the following,*

(a) If $m \equiv n \pmod{15}$, then $m \equiv n \pmod 3$ and $m \equiv n \pmod 5$

Solution. By Defintion 2.3, we have

$$15 \mid (m-n) \implies m - n = 15k \tag{2.40}$$
$$\implies m - n = 5 \cdot 3k \implies 5 \mid (m-n) \tag{2.41}$$
$$\implies m - n = 3 \cdot 5k \implies 3 \mid (m-n) \tag{2.42}$$

By Definition 2.3, $m \equiv n \pmod 3$ and $m \equiv n \pmod 5$.

(b) If $m \equiv n \pmod 3$ and $m \equiv n \pmod 5$, then $m \equiv n \pmod{15}$.

Solution. By Definition 2.3, we have

$$3 \mid (m-n) \implies m - n = 3k \tag{2.43}$$
$$5 \mid (m-n) \implies 5 \mid 3k \tag{2.44}$$

By Lemma 2.1, since $\gcd(3,5) = 1$, we get $5 \mid k$. Therefore, $k = 5l$ for some integer l and $m - n = 15l \implies 15 \mid (m-n)$.

Thus, by Definition 2.3, $m \equiv n \pmod{15}$.

Hence, proved.

Problem 2.31. *Suppose that a and b are positive integers and $d = \gcd(a,b)$.*

(a) Prove that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Solution. Let $g = \gcd(\frac{a}{d}, \frac{b}{d})$. Now, since g is a divisor, we get

$$\frac{a}{d} = gk \implies a = dgk$$

$$\frac{b}{d} = gl \implies b = dgl$$

for some integers k and l.

Now, by Definition 2.1, we know that $dg \mid a$ and $dg \mid b$. Therefore, dg is a common divisor of a and b.

Since d is the *greatest common divisor* of a and b, we can say that

$$dg \leq d \implies g \leq 1$$

Since g is a *greatest common divisor* for $\frac{a}{d}$ and $\frac{b}{d}$, it must be atleast 1 which means $g \geq 1$.

The only number that satisfies both these conditions is $g = 1$.

Hence, proved.

(b) Prove that $\gcd(an, bn) = dn$ *for every positive integer* n.

Solution. Since d is the *greatest common divisor* of a and b, we know that $a = dk$ and $b = dl$ for some integers k and l.

This implies that $an = dnk$ and $bn = dnl$. Therefore, by Definition 2.1 and 2.2, dn is a common divisor of an and bn.

Let us say $g = \gcd(an, bn)$. Now, by Theorem 2.2, we know that $g = anx + any$ for some integers x and y. This implies that

$$g = n \cdot (ax + ay) \implies n \mid g$$

Thus, we can say that $g = nq$ for some integer q. Now, by Definition 2.1 anb 2.2, we have

$$an = nqk', bn = nql' \implies a = qk', b = ql'$$

Thus, q is a common divisor of a and b. Since d is the *greatest common divisor* of a and b, we have

$$q \leq d \implies qn \leq dn \implies g \leq dn$$

But also, dn is a common divisor of an and bn, therefore, $dn \leq \gcd(an, bn)$. The only way both these conditions are satisified is when $dn = \gcd(an, bn)$.

Hence, proved.

Problem 2.32. *Assume that* a, b *and* c *are integers for which* $\gcd(a, b) = 1$ *and* $\gcd(a, c) = 1$. *Prove that* $\gcd(a, bc) = 1$.

Solution. Let $g = \gcd(a, bc)$. Now, by Definition 2.1 and 2.2, we have $g \mid a$ and $g \mid bc$.

By Bezout's Identity (2.2), we know that for some integers k, l, m and n, we have

$$ak + bl = 1 \implies bl = 1 - ak \tag{2.45}$$

$$am + cn = 1 \implies cn = 1 - am \tag{2.46}$$

$$\implies bl \cdot cn = (1 - ak) \cdot (1 - am) \tag{2.47}$$

$$\implies bc \cdot ln = 1 - ak - am + a^2km \tag{2.48}$$

$$\implies a \cdot (k + m - akm) + bc \cdot ln = 1 \tag{2.49}$$

Thus, we have $ax + bcy = 1$ for some integers x and y. Since $\gcd(a, bc)$ must be the smallest positive integer with this property, by Bezout's Identity (2.2 , See Proof), we get $\gcd(a, bc) \leq 1$.

But also, since 1 is a common divisor of a and bc, we have $\gcd(a, bc) \geq 0$.

The only value that satisfies this is $\gcd(a, bc) = 1$.

Hence, proved.

Problem 2.33. *Skipped.*

Problem 2.34. *If* $\gcd(a, b) = 1$*, then we say that* $\frac{a}{b}$ *is in* reduced form. *Prove that if* n *is an integer then*

$$\frac{21n + 4}{14n + 3}$$

is in reduced form.

Solution. Here, we only need to show that $\gcd(21n + 4, 14n + 3) = 1$.

We can easily show that

$$3 \cdot (14n + 3) + (-2) \cdot (21n + 4) = 42n + 9 - 42n - 8 = 1$$

But since $\gcd(21n + 4, 14n + 3)$ is the smallest positive integer of the form $(21n + 4)x + (14n + 3)y$, we get that $\gcd(21n + 4, 14n + 3) \leq 1$.

But also, 1 is a common divisor of both so $\gcd(21n + 4, 14n + 3) \geq= 1$.

This implies that $\gcd(21n + 4, 14n + 3) = 1$.

Hence, proved.

Problem 2.35. *Prove that* $3 \mid (4^n - 1)$ *for any* $n \in \mathbb{N}$ *in two different ways.*

(a) First, prove it using modular arithmetic.

Solution. Since $4 \equiv 1 \pmod 3$ and n is an integer greater than or equal to 1, we can say that $4^n \equiv 1^n \pmod 3$ by repeated application of Proposition 2.2(3) as exponentiation is just repeated multiplication.

This gives us $4^n \equiv 1 \pmod 3$ for any $n \in \mathbb{N}$. By Definition 2.3, we get that $3 \mid (4^n - 1)$. Hence, proved.

(b) Second, prove it using the fact

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + ... + xy^{n-2} + y^{n-1})$$

for any real numbers x *and* y.

Solution. Since 4 and 1 are real numbers, we can show that

$$4^n - 1^n = (4 - 1)(4^{n-1} + 4^{n-2} \cdot 1 + ... + 4 \cdot 1^{n-2} + 1^{n-1}) \tag{2.50}$$

$$\implies 4^n - 1 = 3 \cdot (4^{n-1} + 4^{n-2} \cdot 1 + ... + 4 \cdot 1^{n-2} + 1^{n-1}) \tag{2.51}$$

Since 4 and 1 are integers, the expression in parenthesis is also an integer. Thus, by Definition 2.1, we have $3 \mid (4^n - 1)$. Hence, proved.

Problem 2.36. *Prove that every odd integer is a difference of two squares.*

Scratch Work.

$$5 = 3^2 - 2^2$$
$$7 = 4^2 - 3^2$$
$$9 = 5^2 - 4^2$$

Here, we see a pattern that $2k + 1 = (k + 1)^2 - k^2$.

Solution. Let $2k + 1$ be an odd integer. Here, we can show that

$$(k + 1)^2 - k^2 = k^2 + 2k + 1 - k^2 = 2k + 1$$

Thus, $2k + 1$ is difference of squares of $k + 1$ and k. Hence, proved.

Problem 2.37. *Prove that for every positive integer n, there exist a string of n consecutive intgers none of which are prime.*

Solution. If we take the following numbers:

$$(n + 1)! + 2, (n + 1)! + 3, (n + 1)! + 4, ..., (n + 1)! + (n + 1)$$

Here, the first number must be divisible by 2, the second number must be divisible by 3 and so on. There are in total n integers in this sequence, all of which have a divisor other than 1 and itself.

Hence, proved.

Problem 2.38. *Skipped.*

Problem 2.39. *Suppose n is an integer. Prove that if $n^2 \mid n$, then n is either $-1, 0$ or 1.*

Solution. Since $n^2 \mid n$, we get that $n = kn^2$ for some integer k. Thus,

$$n = kn^2 \implies kn^2 - n = 0 \implies n(kn - 1) = 0$$

Therefore, either $n = 0$ or $k = \frac{1}{n}$. Since k is an integer, the only value of n for which $\frac{1}{n}$ is an integer is 1 and -1.

Thus, n is either $-1, 0$ or 1.

Hence, proved.

Problem 2.40. *As Evelyn Lamb pointed out,*

Every prime larger than 3 is precisely 1 off from a multiple of 3!.

The above statement is true whether the "!" symbol is an exclamation or a factorial. Prove this.

Solution. For every prime $p > 3$, we must have $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$ since it cannot be divisible by 3.

Case 1. $p \equiv= 1 \pmod 3 \implies 3 \mid (p - 1)$ by Definition 2.3.

Case 2. $p \equiv= 2 \pmod 3 \implies p + 1 \equiv 3 \equiv 0 \implies 3 \mid (p + 1)$ by Definition 2.3.

Hence, proved.

For every $p > 3$, we must have $p \in 1, 2, 3, 4, 5 \pmod 6$ since $p \pmod 6$ cannot be zero.

Case 1. $p \equiv 1 \pmod 6 \implies 6 \mid (p-1) \implies 3 \mid (p-1)$ by Definition 2.3 and Proposition 2.1 since $3 \mid 6$.

Case 2. $p \equiv 2 \implies 6 \mid (p-2) \implies 2 \mid (p-2) \implies 2 \mid p$ by Definition 2.3 and Proposition 2.1 and Lemma 2.2(1), thus, p is not prime.
This case is not possible.

Case 3. Similar to Case 2, $p \equiv 3 \implies 6 \mid (p-3) \implies 3 \mid (p-3) \implies 3 \mid p$, thus, p is not prime.
This case is not possible.

Case 4. $p \equiv 4 \implies 6 \mid (p-4) \implies 4 \mid (p-4) \implies 4 \mid p$, thus, p is not prime.
This case is not possible.

Case 5. $p \equiv 5 \pmod 6 \implies 6 \mid (p-5) \implies 6 \mid (p+1) \implies 3 \mid (p+1)$ by Definition 2.3 and Lemma 2.2(1).

Problem 2.41. *Prove that $n \geq 2$ is not prime if and only if $n = st$ for some integers s and t where $1 < s, t < n$.*

Solution. Case 1. If $n \geq 2$ is not prime, then $n = st$ for some integers s and t where $1 < s, t < n$.

Since n is not prime, there must be a positive integer s such that $s \mid n$, $s \neq 1$ and $s \neq n$ by Definition 2.4.

Now, since s is a positive integer and $s \neq 1$, we must have $s > 1$.

Since $s \mid n$, by Definition 2.1, we have $n = st$ for some integer t. Since both s and n are positive, t must be positive as well.

Now, since $s \neq n$, therefore, $t \neq 1$ which implies $t > 1$. Also, since $t > 1$, we must have $s = \frac{n}{t} < n$. Similarly, since $s > 1$, we must have $t = \frac{n}{s} < n$.

Thus, we have $n = st$ for some integers s and t such that $1 < s, t < n$.

Case 2. If for some $n \geq 2$, $n = st$ for some integers s and t where $1 < s, t < n$, then n is not prime.

By Definition 2.1, we have $s \mid t$, $s > 0$, $s \neq 1$ and $s \neq n$. Therefore, by Definition 2.4, n is not a prime number.

Hence, proved.

Problem 2.42. *Skippped.*

Chapter 3

Sets

Definition 3.1. A *set* is ann unordered collection of distinct objects, which are called *elements*. If x is an element of a set S, we write $x \in S$. This is read "x in S".

Definition 3.2. Common Sets:

- The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\{1, 2, 3, ...\}$.
- The set of *integers*, denoted $\mathbb{Z}$, is the set $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.
- The set without any elements, denoted ϕ or $\{\}$, is called the *empty set*.

Definition 3.3. The set

$$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$$

is called the set of *rational numbers*.

The set of real numbers, denoted $\mathbb{R}$, is more difficult to define, so for now rely on your intuition. (Note to Self: We will define this in Real Analysis.)

Definition 3.4. Suppose A and B are sets. If every element in A is also an element of B, then A is *subset* of B, which is denoted $A \subseteq B$.

Strategy To Prove $A \subseteq B$: We can start with some element $x \in A$ and the condition for A. Now, we can apply logic and reasoning to show that this is the same as condition for B. Therefore, $x \in B$.

Since we chose a arbitrary element of A, therefore, this is true for all elements of A. Hence, proved. Moreover, we are not allowed to assume anything about x beyond that it is in A. This is the reason that we can say that since it applies to an *arbitrary* element of A, therefore, it applies to every element of A.

Notice that if $A = B$ then $A \subseteq B$. In the case, $A \subseteq B$ and $A \neq B$, we say that A is a *proper subset* of B, denoted by $A \subset B$. But we will not use this notation in this text.

Strategy To Prove $A = B$: To prove this, you will have to show that:

1. Every element of A is also in B which means $A \subseteq B$.
2. Every element of B is also in A which means $B \subseteq A$.

Definition 3.5. Set Operations:

- The *union* of sets A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
- The *intersection* of sets A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
- Likewise, if $A_1, A_2, A_3, ..., A_n$ are all sets, then the union of all of them is the set $A_1 \cup A_2 \cup A_3 \cup ... \cup A_n = \{x : x \in A_i \text{ for some } i\}$. This set is also denoted as
$$\bigcup_{i=1}^{n} A_i$$
- Likewise, if $A_1, A_2, A_3, ..., A_n$ are all sets, then the intersection of all of them is the set $A_1 \cap A_2 \cap A_3 \cap ... \cap A_n = \{x : x \in A_i \text{ for all } i\}$. This set is also denoted as
$$\bigcap_{i=1}^{n} A_i$$

Definition 3.6 (Subtraction and Complements)**.** Assume A and B are sets and $x \notin B$means that x is not an element of B.

- The *subtraction* of B from A is $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.
- If $A \subseteq U$, then U is called a *universal set* of A. The *complement* of A in U is $A^c = U \setminus A$.

Definition 3.7 (Power Sets and Cardinality)**.** Assume A is a set:

- The *power set* of A is $\mathcal{P}(A) = \{X : X \subseteq A\}$.
- The *cardinality* of A is the number of elements ion A, and is denoted $|A|$.

Definition 3.8 (Cartesian Product)**.** Assume A and B are sets. The *Cartesian Product* of A and B is $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

Proposition 3.1. *Suppose A and B are sets. If $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.*

Proof. Assume $x \in A$ be an arbitrary element of A.

Then by Definition **??**, $\{x\} \subseteq A$ and $\{x\} \in \mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, by Definition **??**, we get that $\{x\} \in \mathcal{P}(B)$. Now, by Definition **??**, we get that $\{x\} \subseteq B$. And finally, by Definition **??**, we get that $x \in B$.

Hence, proved that any arbitrary element of A is also in B. Therefore, $A \subseteq B$. □

Theorem 3.1 (De Morgan's Laws)**.** *Suppose A and B are subsets of a universal set U. Then,*

$$(A \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c$$

Exercises

Problem 3.1. *Skipped.*

Problem 3.2. *Suppose A and B are two boxes. Describe the following in terms of boxes: A*
B, $\mathcal{P}(A)$ and $|A|$.

Solution. A
B: This is a box with all the objects in A that are not in B.

$\mathcal{P}(A)$: This is a box with many boxes such that each box in this box has objects from A.

$|A|$: Number of objects in A.

Problem 3.3. *Skipped.*

Problem 3.4. *Skipped.*

Problem 3.5. *Skipped.*

Problem 3.6. *Skipped.*

Problem 3.7. *Skipped.*

Problem 3.8. *Skipped.*

Problem 3.9. *Skipped.*

Problem 3.10. *The set $\{5a + 3b : a, b \in \mathbb{Z}\}$ is equal to a familiar set. By examining which elements are possible, determine the familiar set.*

Solution. For $a = b = 0$, we get $5a + 3b = 0$.
For $a = -1$ and $b = 2$, we get $5a + 3b = -5 + 6 = 1$.

Since we have 0 and 1, we can build any integers k by setting $a = -1 \cdot k$ and $b = 2 \cdot k$ which gives us $-5k + 6k = k$.

Thus, our set is the set of integers, $\mathbb{Z}$.

It is trivial that all elements of the given set are integers to the given set is a subset of integers.

Now, for any $x \in \mathbb{Z}$, we can take $a = -x$ and $b = 2x$ since $-x, 2x \in \mathbb{Z}$ and get $5a + 3b = -5x + 6x = x$ which is an element of the given set. Thus, $\mathbb{Z}$ is a subset of the given set.

Therefore, both sets are equal.

Problem 3.11. *Suppose A, B and C are sets. Is there a difference between $(A \times B) \times C$ and $A \times (B \times C)$? Explain your answer.*

Solution. Let $(a, b, c) \in (A \times B) \times C$ such that $a \in A$, $b \in B$ and $c \in C$. All elements of $(A \times B) \times C$ are like this by Definition **??**.

Also, by defintion **??**, $(a, b, c) \in A \times (B \times C)$.

Therefore, $(A \times B) \times C \subseteq A \times (B \times C)$. Similarly, we can show that $A \times (B \times C) \subseteq (A \times B) \times C$.

Hence, proved that these two sets are the same.

Problem 3.12. *Prove the second identity in De Morgan's Law (Theorem* **??** *). That is, suppose A and B are subsets of U. Using U as our universal set, show that*

$$(A \cap B)^c = A^c \cup B^c$$

Solution. Let $x \in (A \cap B)^c$ be any arbitrary element. By Definition **??**, we have that

$$x \in (A \cap B)^c \tag{3.1}$$
$$x \notin A \cap B \tag{3.2}$$
$$x \notin A \text{ or } x \notin B \tag{3.3}$$
$$x \in A^c \text{ or } x \in B^c \tag{3.4}$$
$$x \in A^c \cup B^c \tag{3.5}$$

Hence, proved that $(A \cap B)^c \subseteq A^c \cup B^c$.

Now, let $x \in A^c \cup B^c$ be any arbitrary element.

$$x \in A^c \cup B^c \tag{3.6}$$
$$x \in A^c \text{ or } x \in B^c \tag{3.7}$$
$$x \notin A \text{ or } x \notin B \tag{3.8}$$
$$x \notin A \cap B \tag{3.9}$$
$$x \in (A \cap B)^c \tag{3.10}$$

Hence, proved that $A^c \cup B^c \subseteq (A \cap B)^c$.

Therefore, these two sets must be equal.

Problem 3.13. *Skipped.*

Problem 3.14. *Skipped.*

Problem 3.15. *Suppse A and B are sets. Prove that*

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$$

Solution. Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$ be any arbitrary element. Then by Definition of union, we have

$$X \in \mathcal{P}(A) \cup \mathcal{P}(B) \tag{3.11}$$
$$X \in \mathcal{P}(A) \text{ or } X \in \mathcal{P}(B) \tag{3.12}$$
$$X \subseteq A \text{ or } X \subseteq B \tag{3.13}$$

By definition of union, we have $A \subseteq A \cup B$. Therefore, we can show that

$$X \subseteq A \cup B \implies X \in \mathcal{P}(A \cup B)$$

Thus, proved that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Problem 3.16. *Let $A = \{n \in \mathbb{Z} : 2 \mid n\}$, $B = \{n \in \mathbb{Z} : 3 \mid n\}$ and $C = \{n \in \mathbb{Z} : 6 \mid n\}$.*

Show that $A \cap B = C$.

Solution. Let $n \in A \cap B$ be any arbitrary element. Then, we have

$$n \in A \cap B \tag{3.14}$$
$$n \in A \text{ and } n \in B \tag{3.15}$$
$$2 \mid n \text{ and } 3 \mid n \tag{3.16}$$
$$6 \mid n \tag{3.17}$$
$$n \in C \tag{3.18}$$

Hence, proved that $A \cap B \subseteq C$.

Let $n \in C$ be any arbitrary element. Then, we have

$$n \in C \implies 6 \mid n \implies n = 6k \text{ for some } k \in \mathbb{Z} \tag{3.19}$$
$$n = 2(3k) \text{ and } n = 3(2k) \tag{3.20}$$
$$2 \mid n \text{ and } 3 \mid n \tag{3.21}$$
$$n \in A \text{ and } n \in B \tag{3.22}$$
$$n \in A \cap B \tag{3.23}$$

Hence, proved that $C \subseteq A \cap B$.

Therefore, $A \cap B = C$.

Problem 3.17. *Let A and B are two sets. Prove that if $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.*

Solution. Let us assume that A and B are two sets such that $A \subseteq B$.

Now, let $X \in \mathcal{P}(A)$ be any arbitrary element. By Definiton **??**, we have $X \subseteq A$.

Since $A \subseteq B$, we get that $X \subseteq B$. Thus, by Definition **??**, we get that $X \in \mathcal{P}(B)$.

Hence, proved.

Problem 3.18. *Suppose A, B and C are sets with $C \neq \phi$.*

1. *Prove that if $A \times C = B \times C$, then $A = B$.*

   Solution. Let $a \in A$ be any arbitrary element. Since $C \neq \phi$, there exists $c \in C$. Thus, by Definition **??**, $(a, c) \in A \times C$.

   This implies that $(a, c) \in B \times C$ which means $a \in B$. Therefore, $A \subseteq B$.

   Similarly, for any arbitrary element $b \in B$, we have $(b, c) \in B \times C \implies (b, c) \in A \times C \implies b \in A$. Therefore, $B \subseteq A$.

   Hence, proved that $A = B$.

2. *Explain why the condition $C \neq \phi$ is necessary.*

Solution. If $C = \phi$ then catesian product is always ϕ and thus, any two sets can have equal cartesian products with C and not be equal.

Also, if $C = \phi$, then there exists no element $c \in C$ and the argument above doesn't work.

Problem 3.19. *Suppose A, B and C are sets. Prove that*

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

Solution. Let $x \in A \cap (B \cup C)$ be any arbitrary element. Then, we have,

$$x \in A \cap (B \cup C) \tag{3.24}$$
$$x \in A \text{ and } x \in B \cup C \tag{3.25}$$
$$x \in A \text{ and } (x \in B \text{ or } x \in C) \tag{3.26}$$
$$(x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \tag{3.27}$$
$$x \in A \cap B \text{ or } x \in A \cap C \tag{3.28}$$
$$x \in (A \cap B) \cup (A \cap C) \tag{3.29}$$

Hence, proved that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Since all the above steps are reversible, we can show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Hence, proved.

Problem 3.20. *Skipped.*

Problem 3.21. *Skipped.*

Problem 3.22. *Skipped.*

Problem 3.23. *Skipped.*

Problem 3.24. *Prove the following*

1. $\{5k + 1 : k \in \digamma\} = \{5k + 6 : k \in \mathbb{Z}\}$

   Solution. For any element $5k + 1$ in the first set, we have

   $$5k + 1 = 5k + 6 - 5 = 5(k - 1) + 6$$

   Now, by definition $5(k - 1) + 6$ is in the second set. Therfore, the first set is a subset of the second set.

   For any element $5k + 6$ in the second set, we have

   $$5k + 6 = 5k + 5 + 1 = 5(k + 1) + 1$$

   Now, by definition $5(k + 1) + 1$ is in the first set. Therfore, the second set is a subset of the first set.

   Hence, proved.

2. $\{12a + 3b : a, b \in \mathbb{Z}\} = \{3k : k \in \mathbb{Z}\}$

   Solution. Since $\gcd(12, 3) = 3$, by Theorem 2.2, there exists $m, n \in \mathbb{Z}$ such that $12m + 3n = 3$.

   Now, let $3k$ be any element in the second set. Since $3 = 12m + 3n$, we get $3k = (12m + 3n)k = 12mk + 3nk$ which by definition is in the first set. Thus, the second set is a subset of the first set.

   Now, let $12a + 3b$ be any element in the first set. Then, we get $12a + 3b = 3(4a + b)$ which by definition is in the second set. Thus, the first set is a subset of the second set.

   Hence, proved.

3. $\{8a + 17b : a, b \in \mathbb{Z}\} = \mathbb{Z}$

   Solution. Since $\gcd(8, 17) = 1$, by Theorem 2.2, there exists $m, n \in \mathbb{Z}$ such that $8m + 17n = 1$.

   Now, let $k \in \mathbb{Z}$. Since $1 = 8m+17n$, we get $k = (8m+17n)k = 8mk+17nk$ which by definition is in the first set. Thus, the second set is a subset of the first set.

   Now, since every element in the first set is an integer, we know that, the first set is a subset of the second set.

   Hence, proved.

Problem 3.25. *Prove or find counterexample for the following:*

1. *If $A \subseteq B \cup C$, then $A \cup B = B$ or $A \cup C = C$.*

   Solution. Let $A = \{1, 2, 3\}$ and $B = \{1, 3, 5\}$ and $C = \{2, 4, 6\}$.

   Here, $B \cup C = \{1, 2, 3, 4, 5, 6\}$ and $A \subseteq B \cup C$.

   But, $A \cup B = \{1, 2, 3, 5\} \neq B$ and $A \cup C = \{1, 2, 3, 4, 6\} \neq C$.

2. *If $A \subseteq B \cup C$, then $A \cap B \subseteq B \cap C$.*

   Solution. Let us take the example from the previous problem.

   Here, $A \cap B = \{1, 3\}$ and $B \cap C = \phi$. Thus, $A \cap B \nsubseteq B \cap C$.

3. *If $A \subseteq B \cup C$, then $A \cap B \subseteq C$.*

   Solution. Let us take the example from the previous problem.

   Here, $A \cap B = \{1, 3\} \nsubseteq C$.

4. *If $A = B \setminus C$, then $B = A \cup C$.*

   Solution. Let $B = \{1, 2, 3\}$ and $C = \{2, 3, 4\}$. Therefore, $A = B \setminus C = \{1\}$.

   Here, $A \cup C = \{1, 2, 3, 4\} \neq B$.

5. $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$

Solution. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{2\}$ and $C = \{2, 3\}$.

Here, $B \cap C = \{2\}$, $A \setminus B = \{1, 3, 4, 5\}$ and $A \setminus C = \{1, 4, 5\}$.

Thus, $A \setminus (B \cap C) = \{1, 3, 4, 5\}$ and $(A \setminus B) \cap (A \setminus C) = \{1, 4, 5\}$ are not the same.

6. $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$

Solution. Let $A = \{1\}, B = \{2\}, C = \{3\}$ and $D = \{4\}$.

Here, $A \times B = \{(1, 2)\}, C \times D = \{(3, 4)\}, A \cup C = \{1, 3\}$ and $B \cup D\{2, 4\}$.

Thus, $(A \times B) \cup (C \times D) = \{(1, 2), (3, 4)\}$ and $(A \cup C) \times (B \cup D) = \{(1, 2), (1, 4), (3, 2), (3, 4)\}$.

Hence, proved that these are not the same.

7. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

Solution. Let $(x, y) \in (A \times B) \cap (C \times D)$ be an arbitrary element. Thus, we can show that

$$
\begin{aligned}
& (x, y) \in (A \times B) \cap (C \times D) && (3.30)\\
\implies & (x, y) \in A \times B \text{ and } (x, y) \in C \times D && (3.31)\\
\implies & x \in A, y \in B, x \in C \text{ and } y \in D && (3.32)\\
\implies & x \in A \cap C \text{ and } y \in B \cap D && (3.33)\\
\implies & (x, y) \in (A \cap C) \times (B \cap D) && (3.34)
\end{aligned}
$$

This proves that the first set is the subset of the second. Now, to prove the inverse, let $x \in (A \cap C) \times (B \cap D)$ be an arbitrary element. Then, we can show,

$$
\begin{aligned}
& (x, y) \in (A \cap C) \times (B \cap D) && (3.35)\\
\implies & x \in A \cap C \text{ and } y \in B \cap D && (3.36)\\
\implies & x \in A, x \in C, y \in B \text{ and } y \in D && (3.37)\\
\implies & x \in A, y \in B \text{ and } x \in C, y \in D && (3.38)\\
\implies & (x, y) \in A \times B \text{ and } (x, y) \in C \times D && (3.39)\\
\implies & (x, y) \in (A \times B) \cap (C \times D) && (3.40)
\end{aligned}
$$

Hence, proved.

8. $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$

Solution.

Lemma 3.1. *For any sets X, A and B, if $X \subseteq A$ and $X \subseteq B$, then $X \subseteq A \cap B$.*

Proof. Let $x \in X$ be any arbitrary element. Since $X \subseteq A$, we know that $x \in A$. Similarly, we know that $x \in B$.

Thus, by definition of intersection, $x \in A \cap B$. Therefore, $X \subseteq A \cap B$. Hence, proved. □

Now, let $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ be an abitrary element. Then we have

$$X \in \mathcal{P}(A) \cap \mathcal{P}(B) \tag{3.41}$$
$$X \in \mathcal{P}(A) \text{ and } X \in \mathcal{P}(B) \qquad \text{(Definition ??)} \tag{3.42}$$
$$X \subseteq A \text{ and } X \subseteq B \qquad \text{(Lemma ??)} \tag{3.43}$$
$$X \subseteq A \cap B \tag{3.44}$$
$$X \in \mathcal{P}(A \cap B) \tag{3.45}$$

Thus, proved that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

Now, let $X \in \mathcal{P}(A \cap B)$ be an abitrary element. Then by Definition **??**, we have

$$X \in \mathcal{P}(A \cap B) \implies X \subseteq A \cap B$$

Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, we have,

$$X \subseteq A \text{ and } X \subseteq B \tag{3.46}$$
$$X \in \mathcal{P}(A) \text{ and } X \in \mathcal{P}(B) \tag{3.47}$$
$$X \in \mathcal{P}(A) \cap \mathcal{P}(B) \tag{3.48}$$

Thus, proved that $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

Hence, proved.

9. $\mathcal{P}(A) \setminus \mathcal{P}(B) = \mathcal{P}(A \setminus B)$

Solution. Let $A = B = \phi$. Now, $\mathcal{P}(A) = \mathcal{P}(B) = \{\phi\}$ and $A \setminus B = \phi$.

Therefore, $\mathcal{P}(A) \setminus \mathcal{P}(B) = \phi$ and $\mathcal{P}(A \setminus B) = \{\phi\}$ are not the same set.