Solutions to "Proofs" by Jay Cummings

Jannes Kleinau

November 2024

Contents

1 Chapter 1: Intuitive Proofs

1.1 Exercise 1.1.

Task: Read *The Secret To Raising Smart Kids* by Carol Dweck
`https://www.scientificamerican.com/article/the-secret-to-raising-smart-kids1/`
and write a few paragraphs about what you learned and how it may help you be successful in a proof-based math class.

Solution

The article *The Secret to Raising Smart Kids* discusses how students who believe intelligence is a fixed trait tend to perform worse when faced with difficult problems. In contrast, students who understand that problem-solving is a skill that improves with practice are more successful. Intelligence is not a static, innate quality; rather, it can be developed through learning and hard work. The brain functions like a muscle: when it is challenged, it improves.

Surprisingly, one study showed that students who adopt a growth mindset not only achieve better grades, but they also enjoy their schoolwork more and place higher value on it.

Dweck explains that great accomplishments, and even what we commonly call "genius," are typically the result of years of passion and dedication, rather than a natural-born gift. Historical figures such as Mozart, Edison, Curie, Darwin, and Cézanne were not simply born with extraordinary talent; they developed their abilities through tremendous and sustained effort. Similarly, hard work and discipline contribute more to academic achievement than innate intelligence.

What are the implications of this article for this proof-writing book?

In essence, you should seek out challenging exercises. Struggling with difficult problems is a crucial part of learning. A mistake is not a sign of low intelligence, but often a lack of effort or persistence. When you encounter a tough problem, don't give up! Write down everything you know (and what you don't know) about the problem, your goal, and every method you've tried. If you're completely stuck, take a break: go outside, meet a friend, or sleep on it, and come back to it the next day.

Embrace the struggle, because that's when you truly learn and build your mathematical *mind castle*.

1.2 Exercise 1.2.

Task: Explain the error in the following "proof" $2 = 1$.
Let $x = y$. Then,

$$\begin{aligned} x^2 &= xy \\ x^2 - y^2 &= xy - y^2 \\ (x+y)(x-y) &= y(x-y) \\ x + y &= y \\ 2y &= y \\ 2 &= 1 \end{aligned}$$

Official Solution

The error is moving from the third line to the fourth. We had assumed that $x = y$, which means that $x - y = 0$. It's true that

$$(x + y) * 0 = y * 0,$$

no matter what $(x + y)$ and y are. But you are never allowed to divide by zero, which is what's done to move to the next step. So indeed, $x + y$ and y could be anything at all in line 3, and certainly do not have to be equal to each other as asserted in line 4.

Note: There could also be a problem in the final step. If $2y = y$, then you can not necessarily cancel a y from each side; again, what if $y = 0$? In fact, the only way that $2y = y$ is possible is if y does equal 0!

1.3 Exercise 1.3.

Task: Suppose that m and n are positive odd integers.
(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) The solution to this exercise is similar to the example in the first chapter: *Is it possible to perfectly cover a* 8×8 *chessboard by dominoes if we cross out the top-left square?*

Proof. Since each domino covers 2 squares and the dominoes are non-overlapping, if one places our k dominoes on the board, then they will cover $2k$ squares, which is always an even number. Therefore, a perfect cover can only cover an *even* number of squares. Notice, though, that the product of 2 odd numbers *(in our case m and n)* always results in an *odd* number. Thus, it cannot be perfectly covered. □

(b) Since the $m \times n$ chessboard always has an *odd* number of squares, there will be one more square of one color than the other. This fact is crucial to solving the problem because it matters whether we remove a square from the color that appears more often or the one that appears less often. We need to consider these cases separately:

Case 1: A square with the color that appears **more** often is crossed out:
In this case, the remaining squares are evenly split between black and white, meaning there are the same number of each color. Since each domino covers one black and one white square, it is possible to find a perfect cover.

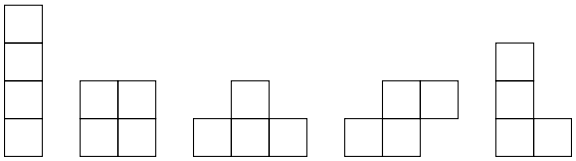
Proof. The chessboard alternates between black and white squares, and after removing one square of the more frequent color, there will be an equal number of black and white squares. Since each domino covers exactly one square of each color, it is always possible to cover the entire board perfectly. This is true for all test cases and can be reasoned by considering the symmetry of the board and the arrangement of dominoes. □

Case 2: A square with the color that appears **less** often is crossed out:
This case is similar to the example from the first chapter, where we remove the top-left and bottom-right squares of an 8×8 chessboard.

Proof. When we remove a square of the less frequent color, we are left with two more squares of the more frequent color. Since each domino covers one black and one white square, it is impossible to perfectly cover the remaining squares. After covering all squares of the less frequent color, two squares of the more frequent color will remain, and these two squares cannot be covered by a domino. Therefore, a perfect cover is not possible. □

1.4 Exercise 1.4.

Task: The game *Tetris* is played with five different shapes − the five shapes that can be obtained by piecing together four unit squares:



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

(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.

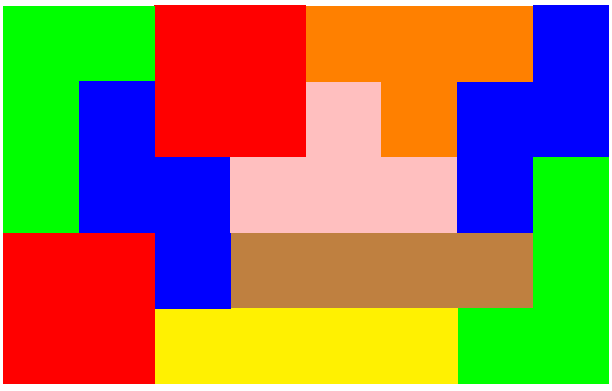
(b) Is it possible to perfectly cover an 8×5 chessboard using each of these shapes exactly twice? Prove that it is impossible, or show by example that it is possible.

Solution

(a)

Proof. Note that a 4×5 chessboard has 10 squares of each color. To perfectly cover the chessboard, the pieces must cover exactly 10 squares of each color. However, upon closer inspection of the shapes, we observe that they will always cover 11 squares of one color and only 9 squares of the other. This imbalance arises due to the small pyramid shape, which covers 3 squares of one color and only 1 square of the other. Hence, it is impossible to achieve a perfect cover. □

(b)



1.5 Exercise 1.5.

Task: If I remove two squares of different colors from an 8×8 chessboard, must the result have a perfect cover?

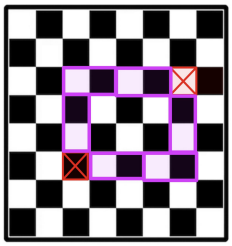
Official Solution

Jay Cummings' solution to this exercise is wonderful! It is very long and I wanted to conclude my own proof, but you can look it up in "Chapter 1 Solutions to Selected Exercises" - Question 2.

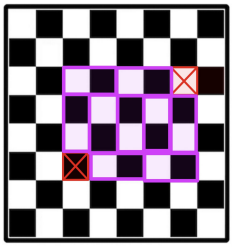
Solution

Proof. Observe that the amount of squares between two opposite-colored squares on a chessboard is always an *even* number, which can be perfectly covered using dominoes since each domino covers two squares.

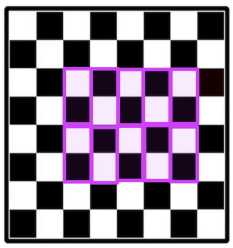
To solve this problem, we connect the two removed squares and form a rectangle using dominoes, ensuring that the removed squares are located at opposite corners of this rectangle.



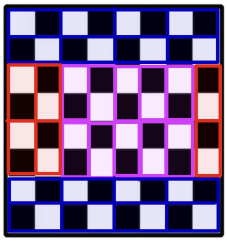
Since the horizontal or vertical distance between the two removed squares is always *even*, we can fill the interior of the rectangle with dominoes by aligning them in rows or columns.



Now, we have an $m \times n$ rectangle on the chessboard, where m is an *even* number and n is an *odd* number. Because one of the rectangle's dimensions is even, the rectangle with the crossed-out squares can be viewed as a complete rectangle filled with dominoes, we can proceed to operate on it as such.



If we place dominoes in columns to fill the rectangle in the step before, the squares to the left and right of the rectangle can be filled with vertical dominoes, while the rest of the chessboard is covered with horizontal dominoes.
If the dominoes in the rectangle are arranged in rows, we can simply rotate the chessboard by 90° and proceed as described for the column arrangement.



Therefore, when two squares of different colors are removed from an 8×8 chessboard, it is always possible to cover the remaining squares perfectly with dominoes. □

1.6 Exercise 1.6.

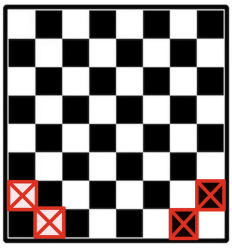
Task: If I remove four squares − two black, two white − from an 8×8 chess board, must the result have a perfect cover?

$\longrightarrow$ If you believe a perfect cover must exist, justify why.

$\longrightarrow$ If you believe 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

The result does not need to have a perfect cover, as demonstrated by the example below. The bottom-left and bottom-right squares can no longer be covered by a domino because they are boxed in.



This chessboard can not be perfectly covered because no 2-square-long domino can cover a1 without also covering one of the crossed-out squares a2 or b1.

1.7 Exercise 1.7.

Task: In chess, a *knight* is a piece that can move two squares vertically and one square horizontally, or two squares horizontally and one square vertically. A knight can legally move to any one of these squares, provided there is not another piece on that same square.

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

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

Solution

(a)

Proof. Consider that a 7×7 chessboard has 49 squares, meaning there are 25 squares of one color and 24 squares of the opposite color. Thus, 25 knights are positioned on squares of one color, and 24 knights are on squares of the other color.
Whenever a knight moves, it always lands on a square of the opposite color, as its move covers an odd number of squares. Therefore, all 25 knights that are on the more frequent color must move to the 24 squares of the less frequent color. However, by the pigeonhole principle, it is impossible to place 25 knights onto only 24 squares without at least one square being occupied by more than one knight, which is not allowed.
Hence, it is impossible for all the knights on a 7×7 chessboard to make a legal move simultaneously. □

(b)

Proof. We start by demonstrating that this is possible on a 4×2 chessboard. In the diagram below, there are four pairs of knights, each pair occupying different colors. These knights can swap positions simultaneously.

Since the 4×2 chessboard fits exactly eight times within a standard 8×8 chessboard, we can apply this same swapping pattern across all the 4×2 sections of the larger board. Therefore, it is indeed possible for all knights on an 8×8 chessboard to make a legal move at the same time.

□

1.8 Exercise 1.8.

Task: Prove that if one chooses $n+1$ numbers from $\{1, 2, 3, \ldots, 2n\}$, it is guaranteed that two of the numbers they chose are consecutive. Also, before your proof, write down an example of 4 numbers from $\{1, 2, 3, 4, 5, 6\}$ and locate two of them which are consecutive. Then, repeat for 5 numbers from $\{1, 2, 3, \ldots, 8\}$ and 6 numbers from $\{1, 2, 3, \ldots, 10\}$.

Solution

Proof. This problem can be addressed using the pigeonhole principle. To demonstrate the guarantee of selecting consecutive numbers, we can categorize the numbers from the set $\{1, 2, 3, \ldots, 2n\}$ into n pairs, each representing a box of consecutive numbers:

$$\boxed{\text{1 and 2}} \quad \boxed{\text{3 and 4}} \quad \boxed{\text{5 and 6}} \quad \ldots \quad \boxed{\text{2n-1 and 2n}}$$

By organizing the numbers in this manner, we create n distinct pairs. When we choose $n+1$ numbers from the set, the pigeonhole principle asserts that at least one pair (or box) must contain two numbers. Consequently, these two numbers must be consecutive.

Therefore, it follows that if one chooses $n+1$ numbers from $\{1, 2, 3, \ldots, 2n\}$, at least two of the chosen numbers will be consecutive. □

1.9 Exercise 1.9.

Task: Assume that n is a positive integer. Prove that if one selects any $n+1$ numbers from the set $\{1, 2, 3, \ldots, 2n\}$, then two of the selected numbers will sum to $2n+1$. Also, before your proof, write down an example of 4 numbers from $\{1, 2, 3, 4, 5, 6\}$ and locate two of them which sum to 7. Then, repeat for 5 numbers from $\{1, 2, 3, \ldots, 8\}$ and 5 numbers from $\{1, 2, 3, \ldots, 10\}$.

Solution

Proof. This problem can be addressed using the pigeonhole principle. To demonstrate the guarantee of selecting numbers, that sum up to $2n+1$, we can categorize the numbers from the set $\{1, 2, 3, \ldots, 2n\}$ into n pairs:

$$\boxed{\text{1 and } 2n} \quad \boxed{\text{2 and } 2n-1} \quad \boxed{\text{3 and } 2n-2} \quad \ldots \quad \boxed{n \text{ and } n+1}$$

By organizing the numbers in this manner, we create n distinct pairs. When we choose $n+1$ numbers from the set, the pigeonhole principle asserts that at least one pair (or box) must contain two numbers. Consequently, these two numbers must sum up to $2n+1$.

Therefore, it follows that if one chooses $n+1$ numbers from $\{1, 2, 3, \ldots, 2n\}$, at least two of the chosen numbers will must sum up to $2n+1$. □

1.10 Exercise 1.10.

Task: Explain in your own words what the general pigeonhole principle says.

Solution

The pigeonhole principle states that if you place more objects than there are boxes, at least one box must contain more than one object. Specifically, if you place $n+1$ objects into n boxes, then at least one box will contain at least two objects, because there are simply more objects than boxes.
The general form of the pigeonhole principle extends this idea: If you place $kn+1$ objects into n boxes, then at least one box will contain at least $k+1$ objects This is because there are more objects than can be evenly distributed among the boxes, so at least one box must contain more than k objects.

1.11 Exercise 1.11.

Task: Prove that there are at least two U.S. residents that have the same weight when rounded to the nearest *millionth* of a pound. Hint: Do a Google search for how many U.S. residents weigh over 300 pounds.

Solution

Proof. The United States had an official estimated resident population of 335,893,238 on Jan 1, 2024, according to the U.S. Census Bureau. Given that 1.5% of U.S. adults weigh over 300 pounds, approximately 5 million residents fall into this category. Thus, about 330 million U.S. residents weigh between 0 and 300 pounds.
Since there are only 300 million distinct weights when rounded to the nearest millionth of a pound in this range, by the pigeonhole principle, it is impossible to assign all 330 million residents distinct weights. Therefore, at least two residents must share the same weight when rounded to the nearest millionth of a pound. □

1.12 Exercise 1.12.

Task: Determine whether or not the pigeonhole principle guarantees that two students at your school have the exact same 3-letter initials. (Include first, middle and last name in the initials. For instance, Natalie Laura Hobson = NLH).

Solution

Proof. Currently, approximately 14,600 students are enrolled at my university. There are $26 \times 26 \times 26$ (17,576) possible 3-letter initials. Therefore, it is possible for each student to have a unique 3-letter initial. □

1.13 Exercise 1.13.

Task: Find your own real-world example of the pigeonhole principle.

Solution

Consider a table tennis club with 30 players and a maximum of 20 possible racket brands. By the pigeonhole principle, since there are more players than brands, at least two players must be using the same brand of racket. Thus, it is impossible for all 30 players to use distinct racket brands, ensuring that at least two share a brand.

1.14 Exercise 1.14.

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

Solution

Proof. Notice, that all consecutive numbers are always relatively prime. Using that fact, we can prove this proposition the same way we proved **Exercise 1.8**: To demonstrate the guarantee of selecting relatively prime numbers, we can categorize the numbers from the set $\{1, 2, 3, \ldots, 60\}$ into 31 pairs, each representing a box of relatively prime numbers:

$$\boxed{1 \text{ and } 2} \quad \boxed{3 \text{ and } 4} \quad \boxed{5 \text{ and } 6} \quad \ldots \quad \boxed{59 \text{ and } 60}$$

By organizing the numbers in this manner, we create 31 distinct pairs. When we choose 31 numbers from the set, the pigeonhole principle asserts that at least one pair (or box) must contain two numbers.
Consequently, these two numbers must be relatively prime.
Therefore, it follows that if one chooses 31 numbers from $\{1, 2, 3, \ldots, 60\}$, at least two of the chosen numbers will be relatively prime. □

1.15 Exercise 1.15.

Task: Assume that n is a positive integer. Prove that if one chooses any $n+1$ distinct odd integers from $\{1, 2, 3, \ldots, 3n\}$, then at least on of these numbers will divide another. Also, before your proof, check all possible selections of 4 odd numbers from $\{1, 2, 3, \ldots, 9\}$, and for each selection locate two of the numbers for which one divides another.

Solution

Proof. To prove that when selecting $n+1$ distinct odd numbers from the set $\{1, 2, 3, \ldots, 3n\}$, at least one number will divide another, we can group the numbers into n pairs, where each box contains odd numbers that divide each other. First, we remove the number 1 from the set, as it divides any other odd number. This is not an issue, because if 1 is selected along with any other odd number, then 1 will divide that number. Therefore, it suffices to focus on the remaining odd numbers.
We define the boxes as groups containing numbers of the form $k \cdot 3^m$, where k is an odd positive integer greater than 1 and m is a non-negative integer.

Case 1: n is an **odd** positive integer

$\boxed{3,\ 9,\ 27,\ldots,3*3^m}$ $\boxed{5,\ 15,\ 45,\ldots,5*3^m}$ $\ldots$ $\boxed{n,n*3^1,\ n*3^2,\ \ldots,n*3^m}$

Case 2: n is an **even** positive integer

$\boxed{3,\ 9,\ 27,\ldots,3*3^m}$ $\boxed{5,\ 15,\ 45,\ldots,5*3^m}$ $\ldots$ $\boxed{(n-1),(n-1)*3^1,\ \ldots,(n-1)*3^m}$

Notice that in both cases, there are n boxes, and we are selecting $n+1$ numbers from the set $\{1, 2, 3, \ldots, 3n\}$. By the pigeonhole principle, at least one box must contain two numbers after selecting $n+1$ numbers. Since the numbers within a box are of the form $k \cdot 3^m$, one of them must divide the other.
Thus, if one chooses any $n+1$ distinct odd integers from $\{1, 2, 3, \ldots, 3n\}$, at least one of these numbers will divide another.

□

1.16 Exercise 1.16.

Task: Give an example of 100 numbers from $\{1, 2, 3, \ldots, 200\}$ such that none of your selected numbers divides any of the others. By doing so, this proves that Proposition 1.11 is optimal.

Solution

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

1.17 Exercise 1.17.

Task: Prove that any set of seven integers contains a pair whose sum or difference is divisible by 10. Also, before your proof, write down three different sets of seven integers, and for each set locate a pair whose sum or difference is divisible by 10. Have your sets contain a diverse collection of integers - some bigger, some smaller, some positive, some negative.

Solution

Proof. Observe that every integer ends in a digit between 0 and 9. A pair whose sum or difference is divisible by 10 is formed from two integers that either share the same last digit (Example: 56 and -36, where $56+(-36) = 20$ and $20 \div 10 = 2$) or whose last digits add up to 10 (Example: 82 and 8, where $82 + 8 = 90$ and $90 \div 10 = 9$). With this in mind, we can categorize integers into the following six groups based on their last digit:

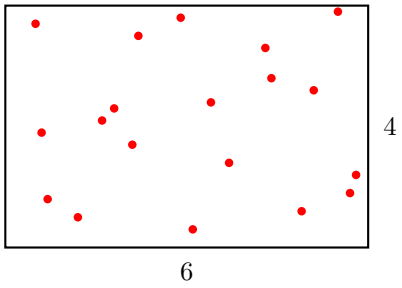
1 and 9	2 and 8	3 and 7	4 and 6	5	0

Now, if we select 7 random integers and sort them by their last digit, placing them into the corresponding group, the pigeonhole principle guarantees that at least one group will contain two numbers. As demonstrated above, these two numbers will either have the same last digit or their last digits will sum to 10, ensuring that their sum or difference is divisible by 10.

□

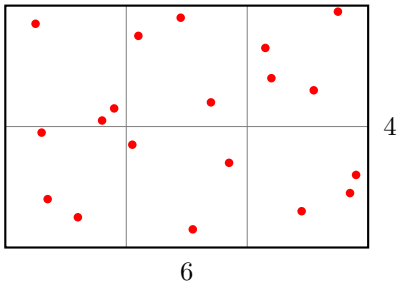
1.18 Exercise 1.18.

Task: Prove that if one chooses any 19 points from the interior of a 6×4 rectangle and no three form a straight line, then there must exist four of these points which form a quadrilateral area of at most 4.

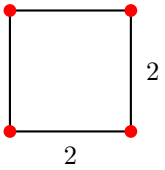


Solution

Proof. Take the 6×4 rectangle and divide it into 6 (2×2) boxes as follows:



As for the points on the lines between squares, consider them part of the square above and/or to the right. Doing this, each of the points in the 6×4 rectangle is assigned to one of the 6 boxes. By the pigeonhole principle, by placing 19 points into these 6 boxes, at least one box has at least 4 points in it. The maximum quadrilateral area of four points in a (2×2) square is 4.

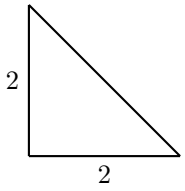


Hence, we are guaranteed that there is at least one (2×2) square with at least 4 points in it, there must exist four points which form a quadrilateral area of at most 4.

□

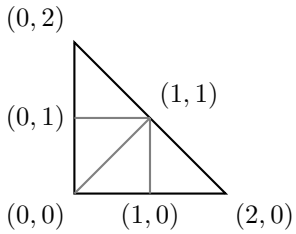
1.19 Exercise 1.19.

Task: Assume that 9 points are chosen from the right triangle below and that no three of them form a straight line. Prove that there exist three of these points which form a triangle whose area is less than 1/2.



Solution

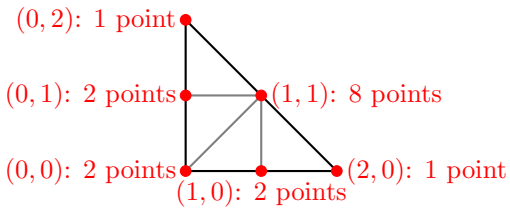
Proof. Take the triangle and divide it into 4 triangles with a area of 1/2 each:



Now, consider the placement of 9 points within this large triangle. By the pigeonhole principle, if we place 9 points into these 4 smaller triangles, at least one of the smaller triangles must contain 3 or more points.

Since the area of each smaller triangle is 1/2, and the maximum possible area of a triangle formed by three points within such a region is 1/2, we are guaranteed that the area of any triangle formed by three points inside this small triangle will either be less than or equal to 1/2.

Moreover, if the three points happen to lie on a straight line, which must be the case when in the small triangles the area of the 3 points is exactly 1/2 as shown below, their area is exactly 0. Thus, we conclude that there must exist three points among the chosen 9 that form a triangle whose area is less than 1/2.



□

1.20 Exercise 1.20.

Task: At a party, each person is *acquainted* with a certain number of others at the party (and is a stranger to everyone else). For example, Jessica may be acquainted with six people at the party while Fara is acquainted with eight. Suppose that there are ≥ 2 people at a party. Prove that at least two people at this party have the same number of acquaintances at the party.
You may also assume the following two things:
(1) Being acquaintances is symmetric (if John is acquainted with Heidi, then Heidi is also acquainted with John - no stalkers allowed at this party) and
(2) Every person is acquainted with at least one person at the party (no party crashers allowed).

Solution

Proof. Since every person is acquainted with at least one person at the party, the possible number of acquaintances are $1, 2, 3, \ldots, (n-1)$, where n is the total number of people at the party. Therefore, there are n people and $n-1$ possible numbers of acquaintances.
We can think of assigning each person to a "box" corresponding to the number of people they know, with the possible boxes being labeled $1, 2, 3, \ldots, (n-1)$. This gives us:

$$\boxed{1} \quad \boxed{2} \quad \boxed{3} \quad \ldots \quad \boxed{(n-2)} \quad \boxed{(n-1)}$$

Since we have n people being placed into $n-1$ boxes, by the simple form of the pigeonhole principle two people must be placed into the same box, which means they have the same number of acquaintances.

□

1.21 Exercise 1.21.

Task:
(a) Determine the population of your hometown and how many non-balding people in your hometown, 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

(a)

- The average person has between 100,000 and 150,000 hairs on their head, and essentially everyone has under 200,000 hairs. So we will focus on people with at most 199,999 hairs.
- For the sake of this problem, we'll define "non-balding" to mean they have at least 50,000 strands of hair.
- On the 31.05.2024, there were 3,790,590 people living in Berlin. Assuming that 25% of Berlin residents are balding, there are 947,647 non-balding people in Berlin.

Proof. By the above facts, there are 2,842,943 non-balding people in Berlin. We can use the pigeonhole principle and imagine a box for every hair count between 50,000 and 199,999:

$$\boxed{50{,}000} \quad \boxed{50{,}001} \quad \boxed{50{,}002} \quad \dots \quad \boxed{199,998} \quad \boxed{199,999}$$

Therefore there are 150,000 (n) boxes in which we put all names of the 2,842,943 ($kn + 1$) people living in Berlin in the box with their hair count on it. By the pigeonhole principle we are guaranteed that there is at least one box with at least 18 ($k + 1$) names on it, meaning they have the same number of hairs on their head.

□

(b)

Proof. Assume that there were 900 students at my high school during my senior year and there are 366 possible birthdays. According to the pigeonhole principle, it is guaranteed that at least two students must share the same birthday, since the number of students exceeds the number of possible birthdays. □

1.22 Exercise 1.22.

Task: The following conjectures are all false. Prove that they are false by finding a counterexample to each.

(a) Conjecture 1: If x and y are real numbers, then $|x + y| = |x| + |y|$
(b) Conjecture 2: If x is a real number, then $x^2 < x^4$
(c) Conjecture 3: Suppose x and y are real numbers. If $|x + y| = |x - y|$, then $y = 0$.

Solution

(a) $x := 1$ and $y := -1$
(b) $x := 0.1$
(c) $x := 0$ and $y := 1$

1.23 Exercise 1.23.

Task: Suppose you deal a pile of cards, face down, from a shuffled deck of cards (this is a standard 52-card deck, where each card is one of 4 suits and of 13 ranks). How many must you deal out until you are guaranteed ...

(a) five of the same suit?
(b) two of the same rank?
(c) three of the same rank?
(d) four of the same rank?
(e) two of one rank and three of another?

Solution

By applying the pigeonhole principle, we get:
(a) 17
(b) 14
(c) 27
(d) 40
(e) $4 + 13 = 17$

1.24 Exercise 1.24.

Task: Determine the U.S. population at the time you are reading this.
(a) Does the pigeonhole principle guarantee that 1 million U.S. residents all have the same birthday?
(b) If the principle does not guarantee this, how many people are needed until that milestone is reached? If the USA grows 2 million people per year, in what year will this occur?

Solution

The United States had an official estimated resident population of 335,893,238 on Jan 1, 2024, according to the U.S. Census Bureau.

(a) To be guaranteed that 1 million U.S. residents all have the same birthday, there would have to be at least 366,000,001 U.S. residents. Since 335,893,238 $<$ 366,000,001, it's not guaranteed that 1 million U.S. residents all have the same birthday.

(b) To guarantee that 1 million U.S. residents all share the same birthday, we need a total population of 366,000,001. Assuming a growth rate of 2 million residents per year, we can determine the number of years required to reach this population by solving the following equation:

$$366,000,001 = 335,893,238 + 2x$$

Solving for x, we find $x = 15,053,381.5$. Thus, it would take approximately 15,053,382 years to ensure that 1 million U.S. residents share the same birthday.

1.25 Exercise 1.25.

Task: 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 dealing.

At a certain point this procedure, they ask you to stop, and declare with confidence that the two stacks - the one still in your hand, and the one on the table - are in perfect balance. They say that 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 outside help. How did your friend do it?

Solution

My friend always stops me after I've dealt the 26th card. To understand why this trick works, let's define the number of black cards on the table as b and the number of red cards on the table as a. The total number of cards dealt on the table is $c = a + b$. Notice that the number of black cards is $b = c - a$.
The number of red cards remaining in my hand is always $26 - a$, because we start with 26 red cards and subtract the number of red cards dealt so far. Since the goal is for the number of black cards on the table to be equal to the number of red cards in my hand, we can set up the following equation:

$$26 - a = c - a$$

Simplifying this gives:

$$26 = c$$

Thus, when 26 cards have been dealt, the number of red cards remaining in my hand will always equal the number of black cards on the table. That's why my friend can confidently stop me after the 26th card!

1.26 Exercise 1.26.

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

Solution

To guarantee that the alien has pulled out a complete triplet of matching socks, the alien must pull out at least $2n+1$ individual socks. This result follows from the pigeonhole principle. The principle states that if we place $kn+1$ objects (in this case, $2n+1$ individual socks) into n boxes (where each box represents a different color), at least one box will contain at least $k+1$ objects (in this case, at least 3 socks of the same color). Therefore, after pulling out $2n+1$ socks, the alien is guaranteed to have a matching triplet.

1.27 Exercise 1.27.

Task: A *magic square* is an $n \times n$ matrix where the sum of the entries in each row, column or diagonal equal the same value. For example,

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$$

is a 3×3 matrix whose three rows, three columns, and two diagonals each sum up to 15. Thus, this is a magic square.

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

$$\begin{bmatrix} 9 & 4 & 5 \\ 10 & 3 & -2 \\ 6 & 9 & 7 \end{bmatrix}$$

is a 3×3 matrix, whose rows sum to 18, 11 and 22, columns sum to 25,16 and 10 and diagonals sum to 19 and 14. Notice that all eight of these numbers is different than the rest, showing that this is an antimagic square.

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

Solution

Proof. Observe that every $n \times n$ matrix has n rows, n columns, and 2 diagonals. Therefore, an antimagic square of size $n \times n$ has $2n + 2$ sums (one for each row, column, and diagonal). To show that it is impossible for all these sums to be distinct when the matrix entries are $-1, 0$, or 1, we can create a box for each possible result of adding n entries, where each entry is $-1, 0$, or 1. These possible results are:

$$\boxed{\text{-n}} \quad \boxed{\text{-n+1}} \quad \boxed{\text{-n+2}} \quad \dots \quad \boxed{\text{n-1}} \quad \boxed{\text{n}}$$

Notice that there are $2n + 1$ such boxes, meaning there are $2n + 1$ possible sums for all rows, columns, and diagonals. Since we need to place $2n + 2$ sums into one of these $2n + 1$ boxes, by the pigeonhole principle, at least one box must contain more than one sum. This implies that at least two rows, columns, or diagonals must have the same sum.

Therefore, there cannot exist an $n \times n$ antimagic square where each entry is $-1, 0$, or 1. □

1.28 Exercise 1.28.

Task: Read the *Introduction to Ramsey Theory* following this chapter. Then, let $r(n, m)$ be the smallest value N for which every red/blue coloring of K_N contains either a red K_n or a blue K_m. Prove that $r(n, 2) = n$.

Solution

Proof. To prove this proposition, we need to show that $r(n, 2) = n$, meaning that for any red/blue coloring of the edges of a complete graph K_N, there is always either a red complete subgraph K_n or a blue edge K_2, and the smallest such N is n.

First, observe that any complete graph K_N for $N \geq 2$ must have at least one edge, which corresponds to a K_2 (a connection between two vertices). In a red/blue coloring of the edges, this K_2 will either be red or blue.

Next, let's consider the case when $N = 1$. Notice that a K_2 cannot exist within a K_1, as the latter has only one vertex. Therefore, n cannot be 1 and must be at least 2.

Finally, to show that $r(n, 2) = n$, consider a complete graph K_N for $N \geq 2$. As demonstrated earlier, the smallest possible subgraph in this K_N is a K_2. Therefore, any other subgraph K_n within this complete graph must also be at least a K_2 or larger.

This completes the proof that $r(n, 2) = n$. □

2 Chapter 2: Direct Proofs

2.1 Exercise 2.1.

Task: List 5 skills that are important for someone to be successful in a college math class. Which skills seem most important for an upper-division math class? Which skills do you want to work to improve?

Solution

5 skills that are important for success in a college math class:
- understanding the solution process for various types of problems
- minimizing computational mistakes
- staying organized and managing time effectively
- thoroughly reviewing and understanding prerequisite concepts
- consistently practicing and solving similar types of problems

5 skills that are important for success in an upper-division math class:
- writing clear and rigorous proofs
- effectively communicating mathematical ideas
- analyzing abstract concepts and definitions in detail
- integrating different areas of mathematics
- applying creativity in proof-writing and problem-solving

I want to work on improving my communication skills, especially in written form. I would also love to approach some problems in this book with creative solutions.

2.2 Exercise 2.2.

Task: The following are the squares of four numbers, each ending in a 5.

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

Looking at these four squares, do you see anything interesting about their answers? Once you have noticed a pattern, answer the following:

(a) Write down a conjecture that explains what the answer is for the square of any integer ending in a 5.
(b) Give four more examples illustrating your conjecture.
(c) Prove your conjecture.

Solution

(a)

Conjecture

If a number is ending in a 5, the square of this number will always end in a 25.

(b)

$$85^2 = 7225$$
$$125^2 = 15625$$
$$232813785^2 = 54202258486026225$$
$$3184712894812745^2 = 10142396222386574198728614435025$$

(c)

Proof. Let's consider any number that ends in 5. Such a number can always be expressed in the form $10n + 5$, where n is an integer. Now, let's square this number:

$$(10n + 5)^2 = 100n^2 + 100n + 25 = 100(n^2 + n) + 25.$$

Notice that $100(n^2+n)$ is always a multiple of 100, which means it ends in two zeros. Adding 25 to this result gives a number that ends in 25, since $0+25=25$.

Thus, the square of any number ending in 5 will always end in 25, as required. □

2.3 Exercise 2.3.

Task: For each of the following, give three examples of this property. Then, prove that it is true.
(a) The sum of an even integer and an odd integer is odd;
(b) The product of two even integers is even;
(c) The product of two odd integers is odd;
(d) The product of an even integer and an odd integer is even;
(e) An even integer squared is an even integer

Solution

(a)

Proof. Assume that n is an even integer and m is an odd integer. By Definition 2.2, this means that $n=2a$ and $m=2b+1$, for some integers a and b. Then,

$$n+m=(2a)+(2b+1)=2a+2b+1=2(a+b)+1.$$

And since, by Fact 2.1, $(a+b)$ is an integer too, we have shown that $n+m=2k+1$, where $k=a+b$ is an integer. Therefore, by Definition 2.2, this means that $n+m$ is odd. □

(b)

Proof. Assume that n and m are even integers. By Definition 2.2, this means that $n=2a$ and $m=2b$, for some integers a and b. Then,

$$n\cdot m=(2a)\cdot(2b)=4ab=2(2ab)$$

And since, by Fact 2.1 $2ab$ is an integer too, we have shown that $n\cdot m=2k$, where $k=2ab$ is an integer. Therefore, by Definition 2.2, this means that $n\cdot m$ is even. □

(c)

Proof. Assume that n and m are odd integers. By Definition 2.2, this means that $n=2a+1$ and $m=2b+1$, for some integers a and b. Then,

$$n\cdot m=(2a+1)\cdot(2b+1)=4ab+2a+2b+1=2(2ab+a+b)+1$$

And since, by Fact 2.1 $2ab+a+b$ is an integer too, we have shown that $n\cdot m=2k+1$, where $k=2ab+a+b$ is an integer. Hence, by Definition 2.2, this means that $n\cdot m$ is odd. □

(d)

Proof. Assume that n is an even integer and m is an odd integer. By Definition 2.2, this means that $n = 2a$ and $m = 2b + 1$, for some integers a and b. Then,

$$n \cdot m = (2a) \cdot (2b + 1) = 4ab + 2a = 2(2ab + a).$$

And since, by Fact 2.1 $2ab+a$ is an integer too, we have shown that $n \cdot m = 2k$, where $k = 2ab + a$ is an integer. Therefore, by Definition 2.2, this means that $n \cdot m$ is even. □

(e)

Proof. Assume that n is an even integer. By Definition 2.2, this means that $n = 2a$, for some integer a. Then,

$$n^2 = (2a)^2 = 4a^2 = 2(2a^2)$$

And since, by Fact 2.1, $2a^2 = 2 \cdot a \cdot a$ is an integer too, we have shown that $n^2 = 2k$, where $k = 2a^2$ is an integer. Therefore, by Definition 2.2, this means that n^2 is even. □

2.4 Exercise 2.4.

Task: For each of the following give three examples of this property. Then, prove that it is true.
(a) If n is an even integer then, $-n$ is an even integer.
(b) If n is an odd integer then, $-n$ is an odd integer.
(c) If n is an even integer, then $(-1)^n = 1$. You may use standard properties of exponents.

Solution

(a)

Proof. Assume that n is an even integer. By Definition 2.2, this means that $n = 2a$, for some integer a. Then,

$$(-n) = -(2a) = 2(-a)$$

And since $-a$ is an integer too, we have shown that $(-n) = 2k$, where $k = -a$ is an integer. Therefore, by Definition 2.2, this means that $(-n)$ is even.

□

(b)

Proof. Assume that n is an odd integer. By Definition 2.2, this means that $n = 2a + 1$, for some integer a. Then,

$$(-n) = -(2a + 1) = 2(-a - 1) + 1$$

And since, by Fact 2.1, $-a-1$ is an integer too, we have shown that $(-n) = 2k + 1$, where $k = (-a - 1)$ is an integer. Therefore, by Definition 2.2, this means that $(-n)$ is odd. □

(c)

Proof. Assume that n is an even integer. By Definition 2.2, this means that $n = 2a$, for some integer a. Then,

$$(-1)^n = (-1)^{(2a)} = ((-1)^2)^a = 1^a = 1 \cdot 1 \cdot 1 \ldots 1 = 1.$$

Therefore, if n is an even integer, then $(-1)^a = 1$, as required. □

2.5 Exercise 2.5.

Task: Prove the following. For each, n is an integer.
(a) If n is odd, then $n^2 + 4n + 9$ is even.
(b) If n is odd, then n^3 is odd.
(c) If n is even, them $n + 1$ is odd.

Solution

(a)

Proof. Assume that n is an odd integer. By Definition 2.2, this means that $n = 2a + 1$, for some integer a. Then,

$$n^2+4n+9 = (2a+1)^2+4(2a+1)+9 = 4a^2+4a+1+8a+8+9 = 4a^2+12a+18 = 2(2a^2+6a+9)$$

.

And since, by Fact 2.1, $(2a^2 + 6a + 9)$ is an integer too, we have shown that $(n^2 + 4n + 9) = 2k$, where $k = (2a^2 + 6a + 9)$ is an integer. Therefore, by Definition 2.2, this means that $(n^2 + 4n + 9)$ is even. □

(b)

Proof. Assume that n is an odd integer. By Definition 2.2, this means that $n = 2a + 1$, for some integer a. Then,

$$n^3 = (2a + 1)^3 = 8a^3 + 12a^2 + 6a + 1 = 2(4a^3 + 6a^2 + 3a) + 1$$

.

And since, by Fact 2.1, $(4a^3+6a^2+3a)$ is an integer too, we have shown that $n^3 = 2k + 1$, where $k = (4a^3 + 6a^2 + 3a)$ is an integer. Therefore, by Definition 2.2, this means that n^3 is odd. □

(c)

Proof. Assume that n is an even integer. By Definition 2.2, this means that $n = 2a$, for some integer a. Then,

$$n + 1 = (2a) + 1 = 2(a) + 1$$

.

And since a is an integer too, we have shown that $n+1 = 2k+1$, where $k = a$ is an integer. Therefore, by Definition 2.2, this means that $n + 1$ is odd. □

2.6 Exercise 2.6.

Task: Prove the following. For each, m and n are integers.
(a) If m and n are odd, then $5m - 3n$ is even.
(b) If m and n are even, then $3mn$ is divisible by 4.

Solution

(a)

Proof. Assume that n and m are odd integers. By Definition 2.2, this means that $n = 2a + 1$ and $m = 2b + 1$, for some integers a and b. Then,

$$5m-3n = 5(2b+1)-3(2a+1) = 10b+5-6a-3 = 10b-6a+2 = 2(5b-3a+1)$$

.

And since, by Fact 2.1, $(5b - 3a + 1)$ is an integer too, we have shown that $5m - 3n = 2k$, where $k = (5b - 3a + 1)$ is an integer. Therefore, by Definition 2.2, this means that $5m - 3n$ is even. □

(b)

Proof. Assume that n and m are even integers. By Definition 2.2, this means that $n = 2a$ and $m = 2b$, for some integers a and b. Then,

$$3mn = 3(2b)(2a) = 3(4ab) = 4(3ab)$$

.

And since, by Fact 2.1, $(3ab)$ is an integer too, we have shown that $3mn = 4k$, where $k = (3ab)$ is an integer. Therefore, by Definition 2.8, this means that 4 divides $3mn$. □

2.7 Exercise 2.7.

Task: Provide a second proof of Proposition 2.7 in which you first prove that $n(n + 1)$ is even, and then you apply Proposition 2.4.

Solution

Proof. Assume that n is an integer. To prove that $n^2 + n + 6$ always results in an even number, we will first show that $n(n + 1)$ is even. Since n can be either odd or even, we consider both cases:

Case 1: n is an **even** number.
If n is even, by Definition 2.8, we can write $n = 2a$ for some integer a. Then,

$$n(n + 1) = (2a)((2a) + 1) = 4a^2 + 2a = 2(2a^2 + a).$$

Since $2a^2+a$ is an integer, we conclude that $n(n+1) = 2k$, where $k = 2a^2+a$ is an integer. Therefore, by Definition 2.2, $n(n + 1)$ is even.

Case 2: n is an **odd** number.
If n is odd, by Definition 2.8, we can write $n = 2a+1$ for some integer a. Then,

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

Since $2a^2 + 3a + 1$ is an integer, we conclude that $n(n + 1) = 2k$, where $k = 2a^2 + 3a + 1$ is an integer. Therefore, by Definition 2.2, $n(n + 1)$ is even.

This shows that $n(n + 1)$ is even for all integers n, since every integer is either even or odd.

Now, observe that $n(n + 1) = n^2 + n$, which is always even as shown above. By Proposition 2.4, the sum of two even integers is always even. Since both $n^2 + n$ and 6 are even, their sum $n^2 + n + 6$ is also even. □

2.8 Exercise 2.8.

Task: Give an example of each of the following properties. Then, prove that it is true.
(a) If n is an integer, then $n^2 + n$ is even.
(b) If n is an integer, then $3n^2 + 5n + 1$ is odd.
(c) If n is an integer, then $n^2 + 3n - 6$ is even.
(d) If m and n are integers of the same parity, them $7m - 3n$ is even.

Solution

(a) Since $n(n + 1) = n^2 + n$, this task is shown first in Exercise 2.7.
(b)

Proof. Assume that n is an integer. Since n can be either odd or even, we consider both cases:

Case 1: n is an **even** number.
If n is even, by Definition 2.8, we can write $n = 2a$ for some integer a. Then,

$$3n^2 + 5n + 1 = 3(2a)^2 + 5(2a) + 1 = 12a^2 + 10 + 1 = 2(6a^2 + 5) + 1$$

.

And since, by Definition 2.2, $(6a^2 + 5)$ is an integer too, we have shown that $3n^2 + 5n + 1 = 2k + 1$, where $k = (6a^2 + 5)$ is an integer. Therefore, by Definition 2.2, this means that $3n^2 + 5n + 1$ is odd.

Case 2: n is an **odd** number.
If n is even, by Definition 2.8, we can write $n = 2a + 1$ for some integer a. Then,

$$\begin{aligned} 3n^2 + 5n + 1 &= 3(2a + 1)^2 + 5(2a + 1) + 1 \\ &= 3(4a^2 + 4a + 1) + 10a + 5 + 1 \\ &= 12a^2 + 14a + 7 \\ &= 2(6a^2 + 7a + 3) + 1 \end{aligned}$$

And since, by Fact 2.1, $(6a^2 + 7a + 3)+$ is an integer too, we have shown that $3n^2 + 5n + 1 = 2k + 1$, where $k = (6a^2 + 7a + 3)+$ is an integer. Therefore, by Definition 2.2, this means that $3n^2 + 5n + 1$ is odd.

This shows that $3n^2 + 5n + 1$ is odd for all integers n. □

(c)

Proof. Assume that n is an integer. Since n can be either odd or even, we consider both cases:

Case 1: n is an **even** number.
If n is even, by Definition 2.8, we can write $n = 2a$ for some integer a. Then,

$$n^2 + 3n - 6 = (2a)^2 + 3(2a) - 6 = 2(2a^2 + 3a - 3)$$

.

And since, by Fact 2.1, $(2a^2 + 3a - 3)$ is an integer too, we have shown that $n^2+3n-6 = 2k$, where $k = (2a^2+3a-3)$ is an integer. Therefore, by Definition 2.2, this means that $n^2 + 3n - 6$ is even.

Case 2: n is an **odd** number.
If n is even, by Definition 2.8, we can write $n = 2a+1$ for some integer a. Then,

$$n^2+3n-6 = (2a+1)^2+3(2a+1)-6 = 4a^2+4a+1+6a+3-6 = 2(2a^2+5a-1)$$

.

And since, by Fact 2.1, $(2a^2 + 5a - 1)$ is an integer too, we have shown that $n^2+3n-6 = 2k$, where $k = (2a^2+5a-1)$ is an integer. Therefore, by Definition 2.2, this means that $n^2 + 3n - 6$ is even.

This shows that $n^2 + 3n - 6$ is even for all integers n. □

(d)

Proof. Assume that m and n are integers of the same parity. Since m and n can be either both odd or even, we consider both cases:

Case 1: m and n are **even** integers.
If m and n are even, by Definition 2.8, we can write $m = 2a$ and $n = 2b$ for some integers a and b. Then,

$$7m - 3n = 7(2a) - 3(2b) = 2(7a - 3b)$$

.

And since, by Fact 2.1, $(7a - 3b)$ is an integer too, we have shown that $7m - 3n = 2k$, where $k = (7a - 3b)$ is an integer. Therefore, by Definition 2.2, this means that $7m - 3n$ is even.

Case 2: m and n are **odd** integers.
If m and n are even, by Definition 2.8, we can write $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b. Then,

$$7m - 3n = 7(2a + 1) - 3(2b + 1) = 2(7a - 3b + 2)$$

.

And since, by Fact 2.1, $(7a - 3b + 2)$ is an integer too, we have shown that $7m - 3n = 2k$, where $k = (7a - 3b + 2)$ is an integer. Therefore, by Definition 2.2, this means that $7m - 3n$ is even.

This shows that $7m - 3n$ is even for all integers n. □

2.9 Exercise 2.9.

Task: Determine conditions on integers m and n for which mn is even. Write down your conditions as a conjecture, and then prove that your conjecture is correct.

Solution

Conjecture

If m or n is even (or both), then also mn is even.

Proof. To prove this conjecture, we need to consider three cases:
Case 1: *m is even and n is odd.*

If m is even and n is odd, then by Definition 2.8, we can express $m = 2a$ and $n = 2b + 1$ for some integers a and b. Thus,

$$mn = (2a)(2b + 1) = 4ab + 2a = 2(2ab + a).$$

Since $2ab + a$ is an integer by Fact 2.1, we have shown that $mn = 2k$, where $k = 2ab + a$ is an integer. Therefore, by Definition 2.2, mn is even.
Case 2: *m is odd and n is even.*

If m is odd and n is even, then by Definition 2.8, we can write $m = 2a + 1$ and $n = 2b$ for some integers a and b. Therefore,

$$mn = (2a + 1)(2b) = 4ab + 2b = 2(2ab + b).$$

Since $2ab + b$ is an integer by Fact 2.1, we have shown that $mn = 2k$, where $k = 2ab + b$ is an integer. Therefore, by Definition 2.2, mn is even.
Case 3: *Both m and n are even.*

If both m and n are even, then by Definition 2.8, we can express $m = 2a$ and $n = 2b$ for some integers a and b. Thus,

$$mn = (2a)(2b) = 4ab = 2(2ab).$$

Since $2ab$ is an integer by Fact 2.1, we have shown that $mn = 2k$, where $k = 2ab$ is an integer. Therefore, by Definition 2.2, mn is even.

Thus, we have shown that mn is even whenever at least one of m or n is an even integer. □

2.10 Exercise 2.10.

Task: Prove the following. For each, m, n and t are integers.
(a) If $m \mid n$, then $m^2 \mid n^2$.
(b) If $m \mid n$, then $m \mid (7n^3 + 13n^2 - n)$.
(c) If $m \mid n$ and $m \mid t$, then $m \mid (n + t)$.
(d) If $3 \mid 2n$, then $3 \mid n$.
(e) If $9 \mid 6n$, then $3 \mid n$.
(f) If $m^3 \mid n$ and $n^4 \mid t$, then $m^{12} \mid t$.

Solution

(a)

Proof. Assume that $m \mid n$. By Definition 2.8, this means that $n = mk$ for some integer k. Thus,

$$n^2 = (mk)^2 = m^2(k^2)$$

We have shown that $n^2 = m^2(k^2)$, and $(k^2 = k \cdot k)$ is an integer. So it is indeed true that $n^2 = m^2p$ for the integer $p = (k^2)$, which by the definition of divisibility (Definition 2.8) means $m^2 \mid n^2$. □

(b)

Proof. Assume that $m \mid n$. By Definition 2.8, this means that $n = mk$ for some integer k. Thus,

$$7n^3 + 13n^2 - n = 7(mk)^3 + 13(mk)^2 - (mk) = m(7m^2k^3 + 13mk^2 - k)$$

We have shown that $7n^3+13n^2-n = m(7m^2k^3+13mk^2-k)$, and $(7m^2k^3 + 13mk^2 - k)$ is an integer. So it is indeed true that $7n^3 + 13n^2 - n = mp$ for the integer $p = (7m^2k^3+13mk^2-k)$, which by the definition of divisibility (Definition 2.8) means $m \mid 7n^3 + 13n^2 - n$. □

(c)

Proof. Assume that $m \mid n$ and $m \mid t$. By Definition 2.8, this means that $n = mk$ and $t = ms$ for some integers k and s. Thus,

$$n + t = mk + ms = m(ks)$$

We have shown that $n + 1 = m(ks)$, and since k and s are integers, so is ks by Fact 2.1. So it is indeed true that $n+1 = mp$ for the integer $p = (ks)$, which by the definition of divisibility (Definition 2.8) means $m \mid n + 1$. □

(d)

Proof. Assume that $3 \mid 2n$ and observe that 3 is a prime number. By Lemma 2.17, we know that if $p \mid bc$, where $p = 3$ is a prime and $b = 2$ and $c = n$ are integers, then $p \mid b$ or $p \mid c$ (or both). Since $3 \nmid 2$, it must follow that $3 \mid n$. □

(d)

Proof. Assume that $3 \mid 2n$. By Definition 2.8, this means that $2n = 3k$ for some integer k. By Exercise 2.3(c), we know that the product of two odd numbers is odd. Since 3 is an odd number and, by Definition 2.1, $2n$ is an even number, k must be even. Hence, $k = 2s$ for some integer s, because the product of 3, which is odd, and an odd number would be odd, which contradicts the fact that $2n$ is even. Thus,

$$n = \frac{3k}{2} = \frac{3(2s)}{2} = 3s$$

We have shown that $n = 3s$, where s is an integer. Therefore, $n = 3k$ for some integer $k = s$, and by the definition of divisibility (Definition 2.8), this proves that $3 \mid n$. □

(e)

Proof. Assume that $9 \mid 6n$. By Definition 2.8, this means that $6n = 9k$ for some integer k. Dividing both sides of this equation by 3, we get: $2n = 3k$, which means $3 \mid 2n$. As shown in Exercise 2.10. (d) $3 \mid 2n$ implies $3 \mid n$. □

(f)

Proof. Assume that $m^3 \mid n$ and $n^4 \mid t$. By Definition 2.8, this means that $n = m^3k$ and $t = n^4s$ for some integers k and s. Thus,

$$t = n^4s = (m^3k)^4s = m^{12}k^4s = m^{12}(k^4s)$$

We have shown that $t = m^{12}(k^4s)$, where (k^4s) is an integer. Therefore, $t = m^{12}p$ for some integer $p = k^4s$, and by the definition of divisibility (Definition 2.8), this proves that $m^{12} \mid t$. □

2.11 Exercise 2.11.

Task: Prove the following. For each, m, n and t are integers.
(a) $1 \mid n$.
(b) $n \mid n$.
(c) If $mn \mid t$, them $m \mid t$.
(d) If $mn \mid tn$, then $m \mid t$.

Solution

(a)

Proof. Assume that n is an integer. Thus,

$$n = 1(n)$$

We have shown that $n = 1(n)$, where (n) is an integer. Therefore, $n = 1k$ for some integer $k = n$, and by the definition of divisibility (Definition 2.8), this proves that $1 \mid n$. □

(b)

Proof. Assume that n is an integer. Thus,

$$n = n(1)$$

We have shown that $n = n(1)$, where (1) is an integer. Therefore, $n = nk$ for some integer $k = 1$, and by the definition of divisibility (Definition 2.8), this proves that $n \mid n$. □

(c)

Proof. Assume that $mn \mid t$. By Definition 2.8, this means that $t = mn(k)$ for some integer k. Thus,

$$t = mn(k) = m(nk)$$

We have shown that $t = m(nk)$, where (nk) is an integer. Therefore, $t = mp$ for some integer $p = nk$, and by the definition of divisibility (Definition 2.8), this proves that $m \mid t$. □

(d)

Proof. Assume that $mn \mid tn$. By Definition 2.8, this means that $tn = mn(k)$ for some integer k. Thus,

$$t = \frac{mn(k)}{n} = m(k)$$

We have shown that $t = m(k)$, where (k) is an integer. Therefore, $t = mp$ for some integer $p = k$, and by the definition of divisibility (Definition 2.8), this proves that $m \mid t$. □

2.12 Exercise 2.12.

Task: 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

Proof. Assume that $m < n$. Thus,

$$m < n \tag{1}$$
$$m \cdot m < n \cdot m \tag{2}$$
$$m^2 < n \cdot m < n \cdot n \tag{3}$$
$$m^2 < n^2 \tag{4}$$

Observe, that in line (3) that $m < n$ implies that $n \cdot m < n \cdot n$. Hence, we have shown that if m and n are positive real numbers and $m < n$, then $m^2 < n^2$. □

2.13 Exercise 2.13.

Task: Define the absolute value of a real number x in this way:

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

Give three examples showing that if x and y are real numbers, then $|xy| = |x| \cdot |y|$. Then, prove that this is true.

Solution

Proof. Assume that x and y are real numbers. To show that $|xy| = |x| \cdot |y|$, we consider the following cases:

Case 1: One of x or y is ≥ 0, and the other is < 0.

In this case, $xy < 0$, so $|xy| = -(xy)$. Since either $x < 0$ and $y \geq 0$, or $x \geq 0$ and $y < 0$. If for example $x < 0$ and $y \geq 0$, we get:

$$|xy| = -(xy) = (-x) \cdot y = |x| \cdot |y|.$$

Case 2: Both x and y are ≥ 0.

Here, $xy \geq 0$, so $|xy| = xy$. Thus,

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

Case 3: Both x and y are < 0.

In this case, $xy \geq 0$, and we have $|xy| = xy$. Since $x < 0$ and $y < 0$, we get:

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

Therefore, we have shown that $|xy| = |x| \cdot |y|$ in all cases.

□

2.14 Exercise 2.14.

Task: Prove that if m, n and t are integers, then at least one of $m-n$, $n-t$ and $m-t$ is even. Also, before your proof, write down three examples of integers m, n and t, and show which of $m-n$, $n-t$ and $m-t$ are even.

Solution

Proof. We start by showing that the difference between two odd integers or two even integers is always an even number.

Assume that m and n are both odd integers. By Definition 2.2, this means that we can write $m = 2k+1$ and $n = 2s+1$ for some integers k and s. Then,

$$m - n = (2k+1) - (2s+1) = 2k - 2s = 2(k-s).$$

Since $k-s$ is an integer, we have shown that $m-n = 2p$, where $p = k-s$ is also an integer. Therefore, by Definition 2.2, $m-n$ is even. The order of subtraction does not matter here, as swapping k and s would yield the same result.

Next, suppose that x and y are both even integers. By Definition 2.2, this means we can write $x = 2k$ and $y = 2s$ for some integers k and s. Then,

$$x - y = (2k) - (2s) = 2(k-s).$$

Since $k-s$ is an integer, we have shown that $x-y = 2p$, where $p = k-s$ is also an integer. Therefore, by Definition 2.2, $x-y$ is even. Again, the order of subtraction does not affect the result.

With these facts, we can use the pigeonhole principle to complete the proof. Suppose we categorize integers into two types, "even" and "odd." Since any integer is either even or odd, placing the three integers m, n, and t into these two categories means, by the pigeonhole principle, that at least two of the integers must have the same parity. The difference between any two integers of the same parity, as shown above, will always be even. Thus, we conclude that at least one of $m-n$, $n-t$, or $m-t$ is even. □

2.15 Exercise 2.15.

Task:
(a) Prove that if n is a positive integer, then 4 divides $1 + (-1)^n(2n - 1)$.
(b) Prove that every multiple of 4 is equal to $1+(-1)^n(2n-1)$ for some positive integer n.

Solution

(a)

Proof. To show this proposition, we consider the cases n is even and n is odd:
Case 1: n is an even number.
Assume that n is an even number. By Definition 2.2, this means that we can write $n = 2k$ for some integer k. Then,

$$\begin{aligned} 4k &= 4k \\ 1 + (4k - 1) &= 4k. \end{aligned}$$

Since we showed in Exercise 2.4 that if n is an even integer, then $(-1)^n = 1$, we can multiply by 1 on both sides of the equation:

$$\begin{aligned} 1 + (-1)^n(4k - 1) &= 4k \\ 1 + (-1)^n(2n - 1) &= 4k. \end{aligned}$$

We have shown that $1 + (-1)^n(2n - 1) = 4k$, where k is an integer. Therefore, $1 + (-1)^n(2n - 1) = 4p$ for some integer $p = k$, and by the definition of divisibility (Definition 2.8), this proves that $4 \mid 1 + (-1)^n(2n - 1)$.

Case 2: n is an odd number.
Assume that n is an odd number. By Definition 2.2, this means that we can write $n = 2k+1$ for some integer k. For this case, we define an integer $m = -k$. Then,

$$\begin{aligned} 4k &= -4m \\ 1 + (-4k - 1) &= -4m \\ 1 + (-4k - 2 + 1) &= 4(-m) \\ 1 + (-2n + 1) &= 4(-m). \end{aligned}$$

Since we showed in Exercise 2.4 that if n is an odd integer, then $(-1)^n = -1$, we can rewrite $(-2n + 1)$ as $-1(2n - 1)$:

$$1 + (-1)^n(2n - 1) = 4(-m).$$

We have shown that $1 + (-1)^n(2n-1) = 4(-m)$, where $(-m)$ is an integer. Therefore, $1 + (-1)^n(2n-1) = 4p$ for some integer $p = (-m)$, and by the definition of divisibility (Definition 2.8), this proves that $4 \mid 1 + (-1)^n(2n-1)$.

Therefore, we have shown that $4 \mid 1 + (-1)^n(2n-1)$ in all cases. □

(b)

Proof. Consider an arbitrary multiple of 4, which we write as $4k$ for some integer k. We proceed by considering the two cases, $k > 0$ and $k \leq 0$.

Case 1: $k > 0$
For this case, let $n = 2k$. Then, observe that:

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

Thus, we have found a positive integer $n = 2k$ for which $1+(-1)^n(2n-1) = 4k$, matching our arbitrary multiple of 4.

Case 2: $k \leq 0$
For this case, let $n = -2k + 1$, which is positive since k is non-positive. Then we observe:

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

So here, we have also found a positive integer $n = -2k + 1$ for which $1 + (-1)^n(2n-1) = 4k$.

In either case, we have shown that for any multiple of 4, there exists a positive integer n such that $1 + (-1)^n(2n-1)$ equals this multiple. This completes the proof. □

2.16 Exercise 2.16.

Task: For each pair of integers, find the unique quotient and remainder when a is divided by m.

(a) $a = 15$, $m = 4$ (c) $a = -7$, $m = 3$ (e) $a = -1$, $m = 15$
(b) $a = 4$, $m = 15$ (d) $a = 65$, $m = 11$ (f) $a = 0$, $m = 4$

Solution

(a) unique quotient: 3, remainder: 3, because $15 = 3 \cdot 4 + 3$
(b) unique quotient: 0, remainder: 4, because $4 = 0 \cdot 15 + 4$
(c) unique quotient: -3, remainder: 2, because $-7 = -3 \cdot 3 + 2$
(d) unique quotient: 5, remainder: 10, because $65 = 5 \cdot 11 + 10$
(e) unique quotient: -1, remainder: 14, because $-1 = -1 \cdot 15 + 14$
(f) unique quotient: 0, remainder: 0, because $0 = 0 \cdot 4 + 0$

2.17 Exercise 2.17.

Task: For each of the following pairs of numbers, list all their common divisors (positive and negative!), and find $\gcd(a, b)$.

(a) $a = 12$, $b = 330$ (b) $a = -36$, $b = 64$ (c) $a = 7$, $b = -27$

Solution

(a) ordered common divisors: -6,-3,-2,-1,1,2,3,6
(b) ordered common divisors: -4,-2,-1,1,2,4
(c) ordered common divisors: -1,1

2.18 Exercise 2.18.

Task: For each pair of integers, find gcd(a,b) and integers k and l such that $gcd(a, b) = ak + bl$. (Note: We know that such integers exist by Theorem 2.13.)

(a) $a = 3$, $b = 13$ (c) $a = -25$, $b = 40$ (e) $a = 62$, $b = 48$
(b) $a = 13$, $b = 3$ (d) $a = -22$, $b = -14$ (f) $a = 13$, $b = -50$

Solution

(a) $gcd(3, 13) = 1 = 3 \cdot (-4) + 13 \cdot 1$
(b) $gcd(13, 3) = 1 = 13 \cdot 1 + 3 \cdot (-4)$
(c) $gcd(-25, 64) = 1 = -25 \cdot 23 + 64 \cdot 9$
(d) $gcd(-22, -14) = 2 = (-22) \cdot (-2) + (-14) \cdot 3$
(e) $gcd(62, 48) = 2 = 62 \cdot 7 + 48 \cdot (-9)$
(f) $gcd(13, -50) = 1 = 13 \cdot 77 + (-50) \cdot 20$

2.19 Exercise 2.19.

Task: 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

Proof. To prove the statement, we use the division algorithm for positive integers.

Since r is the remainder when b is divided by a, we can write

$$b = q \cdot a + r,$$

where $a > r \geq 0$ and q is an integer.

Now, we multiply both sides of this equation by -1:

$$-b = -q \cdot a - r.$$

To express $-b$ in a form that matches the division algorithm (a multiple of a plus a remainder that lies between 0 and a), we rewrite the equation as follows. Let $p = -q - 1$ so that p is an integer. Then we can write

$$-b = p \cdot a + (a - r).$$

Since $0 \leq a - r < a$, we see that when $-b$ is divided by a, the remainder is indeed $a - r$. □

2.20 Exercise 2.20.

Task: Determine the remainder when 3^{302} is divided by 28, and show how you found your answer (without a calculator!).

Solution

To find the remainder when 3^{302} is divided by 28, we need to determine the value of x such that $3^{302} \equiv x \pmod{28}$. Here's how we can approach this:
First, observe that $3^3 = 27$, and $27 \equiv -1 \pmod{28}$. This congruence will help us simplify the expression for 3^{302} by using powers of -1.
Since $3^3 \equiv -1 \pmod{28}$, we can apply Proposition 2.15, part (iii) repeatedly. By raising both sides of the congruence to the 100th power, we get:

$$(3^3)^{100} \equiv (-1)^{100} \pmod{28}$$

which simplifies to:

$$3^{300} \equiv 1 \pmod{28}$$

Now, we can write 3^{302} as:

$$3^{302} = 3^{300} \cdot 3^2$$

Since $3^{300} \equiv 1 \pmod{28}$ and $9 \equiv 9 \pmod{28}$, we get by Proposition 2.15(iii):

$$3^{302} \equiv 3^{300} \cdot 9 \equiv 1 \cdot 9 \equiv 9 \pmod{28}$$

Therefore, we have shown that $3^{302} \equiv 9 \pmod{28}$, which means the remainder when 3^{302} is divided by 28 is 9.

2.21 Exercise 2.21.

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

Solution

Proof. Part (i). Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By the definition of modular congruence (Definition 2.14),

$$n \mid (a - b) \qquad \text{and} \qquad n \mid (c - d).$$

Then by the definition of divisibility (Definition 2.8),

$$a - b = nk \qquad \text{and} \qquad c - d = np$$

for some integers k and p. Subtracting the second equation from the first, we have:

$$(a - b) - (c - d) = nk - np.$$

Regrouping,

$$(a - c) - (b - d) = n(k - p)$$

Since $k - p$ is an integer, by the definition of divisibility (Definition 2.8),

$$n \mid (a - c) - (b - d)$$

which then by the definition of modular congruence (Definition 2.14) means that

$$a - c \equiv b - d \pmod{n},$$

completing the proof of (i).

Part (ii).

Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By the definition of modular congruence (Definition 2.14),

$$n \mid (a - b) \qquad \text{and} \qquad n \mid (c - d).$$

Then by the definition of divisibility (Definition 2.8),

$$a - b = nx \qquad \text{and} \qquad c - d = ny$$

for some integers k and p. We get,

$$\begin{aligned} a \cdot c - b \cdot d &= a \cdot c - b \cdot d \\ &= (nx + b) \cdot (ny + d) - b \cdot d \\ &= n^2xy + nxd + nyb + bd - bd \\ &= n^2xy + nxd + nyb \\ &= n(nxy + xd + yb) \end{aligned}$$

Since $nxy + xd + yb$ is an integer, by the definition of divisibility (Definition 2.8),

$$n \mid (a \cdot c) - (b \cdot d)$$

which then by the definition of modular congruence (Definition 2.14) means that

$$a \cdot c \equiv b \cdot d \pmod{n},$$

completing the proof of (ii). □

2.22 Exercise 2.22.

Task: Assume that a is an integer and p and q are distinct primes. Prove that if $p \mid a$ and $q \mid a$, then $pq \mid a$. Also, before your proof, give three examples for this property.

Solution

Proof. Assume that $p \mid a$ and $q \mid a$. By the definition of divisibility (Definition 2.8), this implies that there exist integers k and s such that

$$a = pk \qquad \text{and} \qquad a = qs.$$

Since $a = qs$, it follows that $p \mid qs$. By Lemma 2.17 (iii), and the fact that $p \nmid q$ (since p and q are distinct primes), we conclude that $p \mid s$. Therefore, we can write

$$s = pm$$

for some integer m. Substituting this expression for s into the equation $a = qs$, we get

$$a = q(pm) = (pq)m.$$

Since m is an integer, this shows that $pq \mid a$, which completes the proof. □

2.23 Exercise 2.23.

Task: Prove that if abc is a multiple of 10 (,where a, b, c are integers!), then at least one of ab, ac or bc is a multiple of 10. Also, before your proof, give three examples of this property.

Solution

Proof. First, note that since $2 \mid 10$ and $5 \mid 10$ and both 2 and 5 are prime, any number divisible by 10 must have both 2 and 5 as factors. Since we are given that $10 \mid abc$, Proposition 2.10 implies that both $2 \mid abc$ and $5 \mid abc$. Applying Lemma 2.17 (iii) to both $2 \mid abc$ and $5 \mid abc$, we conclude that:

$$5 \mid a, \qquad 5 \mid b \qquad \text{or} \qquad 5 \mid c$$

and

$$2 \mid a, \qquad 2 \mid b \qquad \text{or} \qquad 2 \mid c.$$

This result shows that at least one of a, b, or c is divisible by 5, and at least one of a, b, or c is divisible by 2. This leads us to consider two possible cases to complete the proof:

Case 1: One number is divisible by 5 and a different number is divisible by 2.

Let's consider the case where $5 \mid a$ and $2 \mid b$. By the definition of divisibility (Definition 2.8), we can write $a = 5x$ and $b = 2y$ for some integers x and y. Then:

$$ab = (5x)(2y) = 10(xy),$$

where xy is an integer. By Definition 2.8, this shows that $10 \mid ab$ in this case. By similar reasoning, any pairing of one factor divisible by 5 and another by 2 will result in a product divisible by 10, ensuring that at least one of ab, ac, or bc is divisible by 10.

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

Assume, for instance, that $5 \mid a$ and $2 \mid a$. This implies $a = 5k$ and $a = 2p$ for some integers k and p. Substituting, we get $2 \mid 5k$. Since $\gcd(2, 5) = 1$, by Lemma 2.17 (ii), it follows that $2 \mid k$. Thus, $k = 2s$ for some integer s, and we can rewrite a as:

$$a = 5(2s)$$
$$a = 10s$$
$$ab = 10(bs)$$

By Definition 2.8, this means $10 \mid ab$, or any other pair of a, b and c.
Thus, $10 \mid$ (pair of a, b and c) holds in both cases. □

2.24 Exercise 2.24.

Task: Assume that a, b and c are integers, where $a^2 \mid b$ and $b^3 \mid c$. Prove that $a^6 \mid c$. Also, before your proof, give three examples of this property.

Solution

Proof. Let a, b, and c be integers, and suppose $a^2 \mid b$ and $b^3 \mid c$. By the definition of divisibility (Definition 2.8), we know that there exist integers x and y such that:

$$b = a^2 x \quad \text{and} \quad c = b^3 y.$$

Now, let's expand b^3 in terms of a:

$$b^3 = (a^2 x)^3 = a^6 x^3.$$

Since x^3 is an integer, we see that $a^6 \mid b^3$ by Definition 2.8.
Now that we know $a^6 \mid b^3$ and $b^3 \mid c$, Proposition 2.10 implies $a^6 \mid c$. □

2.25 Exercise 2.25.

Task: Prove that for every integer n, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Solution

Proof. We will prove that for any integer n, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$. To do this, we consider the two cases where n is either even or odd.

Case 1: n is an even integer

If n is even, then by Definition 2.2, we can write $n = 2k$ for some integer k. Then,

$$n^2 = (2k)^2 = 4k^2 = 4(k^2).$$

Since k^2 is an integer, this shows that n^2 is a multiple of 4, or $n^2 = 4p$ for some integer $p = k^2$. By Definition 2.8, this means $4 \mid n^2$. Using the definition of congruence (Definition 2.14), we conclude that $n^2 \equiv 0 \pmod 4$.

Case 2: n is an odd integer

If n is odd, then by Definition 2.2, we can write $n = 2k + 1$ for some integer k. Then,

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

Since $k^2 + k$ is an integer, we have shown that $n^2 - 1$ is a multiple of 4, or $n^2 - 1 = 4p$ for some integer $p = k^2 + k$. By Definition 2.8, this means $4 \mid (n^2 - 1)$. Therefore, $n^2 \equiv 1 \pmod 4$ by Definition 2.14.

Since $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$ in both cases, the proof is complete. □

2.26 Exercise 2.26.

Task: Prove that if a, b and n are positive integers and $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$. Also, before your proof, write down three examples of this property.

Solution

Proof. Assume that if a, b and n are positive integers and $a \equiv b \pmod{n}$. Since $a \equiv b \pmod{n}$, we have that $a \cdot a \equiv b \cdot b \pmod{n}$ by Proposition 2.15(iii), giving us $a^2 \equiv b^2 \pmod{n}$. This completes the proof. □

2.27 Exercise 2.27.

Task: 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, b or c will be divisible by 3.

Solution

Proof. Assume that a, b, and c are integers such that $a^2 + b^2 = c^2$. We want to prove that at least one of a, b, or c is divisible by 3.

To do this, let's use the contrapositive approach by assuming the opposite: suppose that none of a, b, or c is divisible by 3. This implies that each of a, b, and c must be congruent to either 1 or 2 modulo 3. Thus:

$$a \equiv 1 \text{ or } 2 \pmod{3}, \quad b \equiv 1 \text{ or } 2 \pmod{3}, \quad c \equiv 1 \text{ or } 2 \pmod{3}.$$

Now, by applying Proposition 2.15(iii), we find that:

$$a^2 \equiv 1 \pmod{3}, \quad b^2 \equiv 1 \pmod{3}, \quad c^2 \equiv 1 \pmod{3}.$$

Using Proposition 2.15(i) we get:

$$a^2 + b^2 \equiv 1 + 1 = 2 \pmod{3}.$$

However, since $a^2 + b^2 = c^2$, we also have $c^2 \equiv a^2 + b^2 \equiv 2 \pmod{3}$. This leads to a contradiction, because we previously determined that $c^2 \equiv 1 \pmod{3}$.

Therefore, our assumption that none of a, b, or c is divisible by 3 is incorrect. This proves that at least one of a, b, or c must be divisible by 3.

This completes the proof. □

2.28 Exercise 2.28.

Task: Prove that n is even if and only if n^2 is even. To do this, here are the two things you should prove:
(a) If n is even, then n^2 is even.
(b) If n^2 is even, then n is even.

Solution

Proof. To prove that n is even if and only if n^2 is even, we'll show two parts:

Part 1: if n is even, then n^2 is even:
Assume that n is an even integer, which means by Definition 2.2, $n = 2k$ for some integer k. Thus,

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

And since, by Fact 2.1, $2k^2$ is an integer too, we have shown that $n^2 = 2(p)$ for some integer $p = 2k^2$. This shows, by Definition 2.2, that n^2 is an even integer.

Part 2: If n^2 is even, then n is even:
We are given that n^2 is an even number, and we need to prove that n must also be even. To do this, let us assume the opposite: suppose n is odd.

If n is odd, then by definition, n can be written as $n = 2k + 1$ for some integer k. Thus,

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

And since, by Fact 2.1, $2k^2 + 2k$ is an integer too, we have shown that $n^2 = 2(p) + 1$ for some integer $p = 2k^2 + 2k$. This shows, by Definition 2.2, that n^2 is an even integer.

This is a contradiction because we assumed at the beginning that n^2 is even. Therefore, our assumption that n is odd must be incorrect, and n must be even.

Hence, n is even if and only if n^2 is even. □

2.29 Exercise 2.29.

Task: 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:
(a) If $a \mid b$, then $d = a$.
(b) If $d = a$ is even, then $a \mid b$.

Solution

Proof. Suppose that a, and b are positive integers, and $\gcd(a, b) = d$. To prove that $a \mid b$ if and only if $d = a$, we'll show two parts:

Part 1: If $a \mid b$, then $d = a$:
Assume that $a \mid b$. By Definition 2.8, this means $b = ak$ for some integer $k \geq 0$. Substituting this expression for b into the equation $\gcd(a, b) = d$, we get

$$\gcd(a, ak) = d.$$

Notice though, that the $\gcd(a, ak)$ equals a, because $a \mid ak$ and $a \leq ak$. Therefore, we conclude that.

$$a = d.$$

Part 2: If $d = a$, then $a \mid b$:
Assume that $d = a$. Substituting this expression for d into the equation $\gcd(a, b) = d$, we get

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

Since a is a divisor if the greatest common divisor, it must also divide b. Thus, we have

$$a \mid b.$$

This completes the proof, showing that $a \mid b$ if and only if $d = a$. □

2.30 Exercise 2.30.

Task: Prove that $m \equiv n \pmod{15}$ if and only if $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$. To do this, here are the two things that you should prove:
(a) If $m \equiv n \pmod{15}$, then $m \equiv n \pmod{3}$ 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

Proof. To prove that $m \equiv n \pmod{15}$ if and only if $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$, we'll show two parts:

Part 1: If $m \equiv n \pmod{15}$, then $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$:
Assume that $m \equiv n \pmod{15}$, which means, by Definition 2.14, $15 \mid (m-n)$. Notice that $3 \mid 15$ and $5 \mid 15$, and 3 and 5 are prime numbers. Given that, Proposition 2.10. implies $3 \mid (m-n)$ and $5 \mid (m-n)$, which can be written as $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$.

Part 2: If $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$, then $m \equiv n \pmod{15}$
Assume that $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$. Since 3 and 5 are distinct primes, Exercise 2.22 implies $15 \mid (m-n)$, which, by Definition 2.14, is the same as $m \equiv n \pmod{15}$.

This completes the proof, showing that $m \equiv n \pmod{15}$ if and only if $m \equiv n \pmod{3}$ and $m \equiv n \pmod{5}$. □

2.31 Exercise 2.31.

Task: Suppose that a and b are positive integers and $d = \gcd(a, b)$.
(a) Prove that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.
(b) Prove that $\gcd(an, bn) = dn$ for every positive integer n.

Solution

(a)

Proof. Suppose that $c = gcd(\frac{a}{d}, \frac{b}{d})$. We want to show that $c = 1$. We will do this by showing that $c \leq 1$ and $c \geq 1$. The latter inequality follows from the fact that c is the greatest common divisor of two integers, and as we noted, every greatest common divisor is greater or equal to 1. To show that $c \leq 1$, we use the fact that $c \mid \frac{a}{d}$ and $c \mid \frac{b}{d}$. We then know that there are integers q and r such that $cq = \frac{a}{d}$ and $cr = \frac{b}{d}$. Thus,

$$(cd)q = a \qquad\qquad (cd)r = b.$$

These equations show that cd is a divisor of a and b. It is thus not greater than the greatest common divisor of a and b, because this is $d = gcd(a, b)$. Hence $cd \leq d$, which implies $c \leq 1$.

Since $c \leq 1$ and $c \geq 1$, $c = 1$, which completes the proof. □

(b)

Proof. Assume that $\gcd(a, b) = d$. We want to show that $\gcd(an, bn) = dn$ for any positive integer n. To do this, we'll show that $\gcd(an, bn) \geq dn$ and $\gcd(an, bn) \leq dn$, which will imply that $\gcd(an, bn) = dn$.

Part 1: showing $\gcd(an, bn) \geq dn$:
Since $\gcd(a, b) = d$, we know $d \mid a$ and $d \mid b$, so we can write $a = dx$ and $b = dy$ for some integers x and y. Now multiplying both a and b by an positive integer n, we get

$$an = (dn)x \qquad and \qquad bn = (d)y.$$

Definition 2.8 tells us that this means $dn \mid an$ and $dn \mid bn$. Hence dn is a common divisor of an and bn, which implies that $\gcd(an, bn) \geq dn$.

Part 2: showing $\gcd(an, bn) \leq dn$
Since $\gcd(a, b) = d$, we know $d \mid a$ and $d \mid b$. This implies $d \leq a$ and $d \leq b$. Note that $\gcd(an, bn) \leq an$ and $\gcd(an, bn) \leq bn$. Since $d \leq a, b$, it follows that $\gcd(an, bn) \leq an, bn \leq dn$. Therefore $\gcd(an, bn) \leq dn$.

Since we have shown both that $\gcd(an, bn) \geq dn$ and $\gcd(an, bn) \leq dn$, we conclude that $\gcd(an, bn) = dn$, as required.

This completes the proof. □

2.32 Exercise 2.32.

Task: 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

Proof. Assume that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. By Bezout's Identity,there exist integers m, n, x and y such that $1 = am + bn$ and $1 = ax + cy$. Since both expressions equal 1, we can multiply both equations together and obtain:

$$\begin{aligned}(am + bn)(ax + cy) &= 1\\ a^2mc + amcy + bnax + bncy &= 1\\ a(amc + mcy + bnx) + bc(ny) &= 1.\end{aligned}$$

Since there exist integers k and p such that $a(k) + bc(p) = 1$, where $k = (amc + mcy + bnx)$ and $p = (ny)$, we conclude that $\gcd(a, bc) = 1$. Note that this conclusion is valid only because we showed that $\gcd(a, bc) = 1$. For any greater common divisor, we would first have to show that no smaller integer can be represented as $a(k) + bc(p)$. □

2.33 Exercise 2.33.

Task: For the pairs of numbers in parts (a)-(d), determine $\gcd(a, b), \mathrm{LCM}(a, b)$, and ab.
(a) $a = 6, b = 8$
(b) $a = 3, b = 6$
(c) $a = 4, b = 6$
(d) $a = 5, b = 6$
(e) Based on your answers to parts (a)-(d), conjecture a relationship between $\gcd(a, b), \mathrm{LCM}(a, b)$ and ab. Then, prove that your conjecture is correct.

Solution

(a) $\gcd(a, b) = 2$, $\mathrm{LCM}(a, b) = 24$, $ab = 48$
(b) $\gcd(a, b) = 3$, $\mathrm{LCM}(a, b) = 6$, $ab = 18$
(c) $\gcd(a, b) = 2$, $\mathrm{LCM}(a, b) = 12$, $ab = 24$
(d) $\gcd(a, b) = 1$, $\mathrm{LCM}(a, b) = 30$, $ab = 30$
(e)

Conjecture

If a and b are both positive non-zero integers, then

$$\mathrm{LCM}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Proof. First notice that

$$\frac{ab}{\gcd(a,b)} = a(\frac{b}{\gcd(a,b)}) = b(\frac{a}{\gcd(a,b)}).$$

is a common multiple of a and b. Thus $\text{LCM}(a,b) \leq \frac{ab}{\gcd(a,b)}$.

By the division algorithm, we can express ab as:

$$ab = q \cdot \text{LCM}(a,b) + r,$$

where $0 \leq r < \text{LCM}(a,b)$. Thus,

$$\begin{aligned} r &= q \cdot \text{LCM}(a,b) - ab \\ &= a(q \cdot x - b) \\ &= b(q \cdot y - a) \end{aligned}$$

for some integers x and y. As the equation above shows, r is also a common multiple of a and b. Since $0 \leq r < \text{LCM}(a,b)$, $r = 0$. This implies that $\text{LCM}(a,b) \mid ab$.

Now notice that

$$(\frac{ab}{\text{LCM}(a,b)}) \cdot \frac{\text{LCM}(a,b)}{b} = a$$

and

$$(\frac{ab}{\text{LCM}(a,b)}) \cdot \frac{\text{LCM}(a,b)}{a} = b.$$

By the definition of divisibility, and the fact that $\frac{\text{LCM}(a,b)}{a}$ and $\frac{\text{LCM}(a,b)}{b}$ are integers, this means $\frac{ab}{\text{LCM}(a,b)}$ is a common divisor of a and b. Since $\gcd(a,b)$ is the greatest common divisor of a and b, we get $\frac{ab}{\text{LCM}(a,b)} \leq \gcd(a,b)$, which implies $\text{LCM}(a,b) \geq \frac{ab}{\gcd(a,b)}$, because $\gcd(a,b), \text{LCM}(a,b) \geq 0$.

Since $\text{LCM}(a,b) \leq \frac{ab}{\gcd(a,b)}$ and $\text{LCM}(a,b) \geq \frac{ab}{\gcd(a,b)}$, $\text{LCM}(a,b) = \frac{ab}{\gcd(a,b)}$.
This completes the proof. □

2.34 Exercise 2.34.

Task: 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

Proof. To show that $\frac{21n+4}{14n+3}$ is in reduced form, we'll prove that $\gcd(21n + 4, 14n + 3) = 1$, which will imply that $\frac{21n+4}{14n+3}$ is indeed in reduced form.
By Bezout's Identity (Theorem 2.13), there exist integers x and y such that

$$\gcd(21n + 4, 14n + 3) = (21n + 4)x + (14n + 3)y.$$

We now choose $x = -2$ and $y = 3$, which gives us

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

Since we have found integers x and y such that $(21n+4)x+(14n+3)y = 1$, it follows from Bezout's Identity that $\gcd(21n + 4, 14n + 3) = 1$.
Therefore, since we have shown that $\gcd(21n + 4, 14n + 3) = 1$, $\frac{21n+4}{14n+3}$ is in reduced form, which completes the proof. □

2.35 Exercise 2.35.

Task: Prove that $3 \mid (4^n - 1)$ for every $n \in \mathbb{N}$ in two different ways.
(a) First, prove is using modular arithmetic.
(b) Second, prove it using the fact (which you do not have to prove) that

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

for any real numbers x and y.

Solution

(a)

Proof. First, observe that $4 \equiv 1 \pmod 3$. By applying Proposition 2.15 (iii) repeatedly n times, we obtain

$$4^n \equiv 1^n \equiv 1 \pmod 3.$$

Therefore, by the definition of modular congruence (Definition 2.14), we have $3 \mid (4^n - 1)$, which completes the proof. □

(b)

Proof. By applying the fact from the task (b) with $x = 4$ and $y = 1$, we obtain

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

Notice that $(4 - 1) = 3$, and the product and sum of the integers 4 and 1 will always result in an integer. Therefore, we can write

$$4^n - 1 = 3k,$$

where $k = (4^{n-1} + 4^{n-2} \cdot 1 + 4^{n-3} \cdot 1^2 + \cdots + 4 \cdot 1^{n-2} + 4^{n-1})$ is an integer. This shows, by Definition 2.8, that $3 \mid (4^n - 1)$. This completes the proof. □

2.36 Exercise 2.36.

Task: Prove that every odd integer is the difference of two squares. (For example, $11 = 6^2 - 5^2$)

Solution

Proof. Let k be a non-negative integer. Consider the difference of the squares of $(k+1)$ and k:

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

This shows that $(k+1)^2 - k^2 = 2k+1$, which is an odd number since $2k+1$ is always odd for any integer k. Therefore, we have shown that the difference of the squares of two integers $(k+1)$ and k is always an odd number.

Hence, every odd integer can be expressed as the difference of two squares. □

2.37 Exercise 2.37.

Task: Prove that for every positive integer n, there exist a string of n consecutive integers none of which are prime.

Solution

Proof. First, observe that for any positive integer n, we can construct a sequence of n consecutive integers as follows:

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

To prove that none of these integers is prime, we use the fact that

$$(n+1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n \cdot (n+1).$$

Since we are adding an integer t where $2 \leq t \leq n+1$, we can always factor out t from each term in the sequence as follows:

$$\begin{aligned}(n+1)! + t &= 1 \cdot 2 \cdot 3 \cdots t \cdots (n-1) \cdot n \cdot (n+1) + t \\ &= t\left(\frac{(n+1)!}{t} + 1\right).\end{aligned}$$

By Definition 2.8, this implies that $(n+1)! + t$ is divisible by t, since $\frac{(n+1)!}{t}$ is an integer (as t divides $(n+1)!$). Therefore, each integer in the sequence is divisible by some integer t greater than 1, meaning none of them is prime.

Hence, we have constructed a sequence of n consecutive integers, none of which are prime. This completes the proof. □

2.38 Exercise 2.38.

Task: The following Conjectures are all false, Prove that they are false by finding a counterexample to each.
(a) Conjecture 1: Let $f(n) = n^2 - n + 5$. If n is an integer, then $f(n)$ is a prime number.
(b) Conjecture 2: Suppose a, b and c are positive integers. If $a \mid bc$ then $a \mid b$ or $a \mid c$.
(c) Conjecture 3: Suppose a and b are integers. If $a \mid b$ and $b \mid a$, then $a = b$.

Solution

(a)

Proof. Let $n = 5$. Then

$$f(5) = 5^2 - 5 + 5 = 25 = 5 \cdot 5,$$

which is not a prime number. Thus, Conjecture 1 is false. □

(b)

Proof. Let $a = 6$, $b = 2$, and $c = 3$. Then $6 \mid (3 \cdot 2)$, but neither $6 \mid 2$ nor $6 \mid 3$. Therefore, Conjecture 2 is false. □

(c)

Proof. Let $a = 1$ and $b = -1$. Then $1 \mid -1$ and $-1 \mid 1$, but $1 \neq -1$. Therefore, Conjecture 3 is false. □

2.39 Exercise 2.39.

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

Solution

Proof. Suppose n is an integer and that $n^2 \mid n$. By Definition 2.8, this implies that there exists an integer k such that

$$n = n^2 \cdot k.$$

To proceed, we divide both sides of this equation by n. However, we must first consider the case when $n = 0$ separately, since division by zero is undefined. If $n = 0$, then the statement is trivially true.

Now assume $n \neq 0$. Dividing the equation by n, we obtain

$$1 = n \cdot k.$$

According to Definition 2.14, this implies that $n \mid 1$. Since 1 is only divisible by 1 and -1, it follows that $n = 1$ or $n = -1$.

Therefore, we have shown that if $n^2 \mid n$, then n must be either -1, 0, or 1, which completes the proof. □

2.40 Exercise 2.40.

Task: As Evelyn Lamb pointed out,

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

The cool thing about this statement is that it is true whether the "!" symbol is an exclamation or a factorial! Prove this.

Solution

Proof. Let p be a prime number such that $p > 3$. Any integer can be written in one of the following forms:

$$p = 6k, \quad p = 6k + 1, \quad p = 6k + 2, \quad p = 6k + 3, \quad p = 6k + 4, \quad p = 6k + 5,$$

where k is an integer.

Now, since p is prime and greater than 3, it cannot be divisible by 2 or 3. We examine each case:

Expression	Divisibility
$6n = 2(3n) = 3(2n)$	Divisible by 2 and 3
$6n + 1$	Not divisible by 2 or 3
$6n + 2 = 2(3n + 1)$	Divisible by 2
$6n + 3 = 3(2n + 1)$	Divisible by 3
$6n + 4 = 2(3n + 2)$	Divisible by 2
$6n + 5$	Not divisible by 2 or 3

This leaves only two cases:

- **Case 1:** $p = 6k + 1$: Here, p is 1 more than a multiple of 6.
- **Case 2:** $p = 6k + 5$: This can be rewritten as $p = 6(k + 1) - 1$, showing that p is 1 less than a multiple of 6.

Thus, any prime $p > 3$ is either 1 more or 1 less than a multiple of 6. Additionally, since $6 = 3 \cdot 2$ is a multiple of 3, this argument also holds for any multiple of 3, completing the proof. □

2.41 Exercise 2.41.

Task: After defining a prime number, Definition 2.16 stated that an integer $n \geq 2$ being not prime was equivalent to n being able to be written as $n = st$, where s and t are integers and $1 < s, t < n$. Prove that these are indeed equivalent. That is, prove that if $n \geq 2$ is not prime, then $n = st$ for some integers s and t where $1 < s, t < n$. And then prove that if $n = st$ for some integers s and t where $1 < s, t < n$, then n is not prime.

Solution

Proof. To prove the equivalence, we need to show both directions:

Part 1: If $n \geq 2$ is not prime, then $n = st$, where s and t are integers and $1 < s, t < n$.

Suppose $n \geq 2$ is not prime. By Definition 2.16, this is equivalent to $t \mid n$ for an integer t, where $n > t > 1$. This implies, by Definition 2.14, $n = st$ for some integer s. Since $n > t > 1$ and $n = st$, also $n > s > 1$.

Part 2: If $n = st$, where s and t are integers and $1 < s, t < n$, then $n \geq 2$ is not prime.

Suppose $n = st$, where s and t are integers and $1 < s, t < n$. Definition 2.14 tells us that this is equivalent to $t \mid n$. Since $1 < t < n$, n is divided by a number greater than 1, which is not itself. This means it is not prime and greater or equal to 2.

Thus, we have shown that n being able to be written as $n = st$, where s and t are integers and $1 < s, t < n$ and $n \geq 2$ being not prime are equivalent. This completes the proof. □

2.42 Exercise 2.42.

Task: Read the *Introduction to Number Theory* following this chapter. Then, encrypt your first name using the RSA algorithm, and then show how to decrypt it. Show every step of your procedure, including what you used for your encryption key, what your numerical message is, and every calculation along the way.

Solution

In this example of encryption and decryption using the RSA algorithm, I will use my first name "jannes".

1. First, I pick two small prime numbers p and q, and let N be their product:

$$p = 5, \quad q = 17, \quad N = pq = 85$$

2. Now, I compute totient(N): If $N = pq$, then totient$(N) = (p-1)(q-1)$.

$$\text{totient}(N) = (5-1)(17-1) = 4 \cdot 16 = 64$$

3. Choose any number t in $\{2, 3, \ldots, \text{totient}(N)\}$ that is relatively prime to N *and* totient(N); this will always be possible. I choose:

$$t := 7$$

4. The numbers in Steps 3 and 1 give the encryption key: (t, N).

$$\text{The encryption key is } (7, 85)$$

5. Choose the smallest d in $\{1, 2, 3, \ldots, \text{totient}(N)\}$ such that $t \cdot d \equiv 1 \pmod{\text{totient}(N)}$. Using the extended Euclidean algorithm:

$$d = 55, \quad t \cdot d = 7 \cdot 55 = 385 \equiv 1 \pmod{64}$$

6. The numbers in Steps 5 and 1 give the decryption key: (d, N).

$$\text{The decryption key is } (55, 85)$$

It is important to note that finding totient(N) is extremely difficult if p and q are large prime numbers. Since $N = p \cdot q$, this results in a very large number that is the product of two primes. To calculate totient(N), one would need to factorize N into p and q. However, for sufficiently large prime numbers, factorizing N is computationally infeasible with current technology and algorithms.

On the next page, you find the steps for encryption and decryption:

Encryption

Each letter of my name is converted to a number (e.g., $\mathrm{j} = 10, \mathrm{a} = 1, \mathrm{n} = 14, \mathrm{e} = 4, \mathrm{s} = 19$), then encrypted using $c = m^t \pmod{N}$, where m is the numeric value of the letter.

$$\begin{aligned}
\mathrm{j} &\implies 10 \implies 10^7 \pmod{85} = 15 \\
\mathrm{a} &\implies 1 \implies 1^7 \pmod{85} = 1 \\
\mathrm{n} &\implies 14 \implies 14^7 \pmod{85} = 49 \\
\mathrm{n} &\implies 14 \implies 14^7 \pmod{85} = 49 \\
\mathrm{e} &\implies 4 \implies 4^7 \pmod{85} = 79 \\
\mathrm{s} &\implies 19 \implies 19^7 \pmod{85} = 51
\end{aligned}$$

The encrypted message is: $15, 1, 49, 49, 79, 51$.

Decryption

Each encrypted value c is decrypted using $m = c^d \pmod{N}$, where $d = 55$.

$$\begin{aligned}
15 &\implies 15^{55} \pmod{85} = 10 \implies \mathrm{j} \\
1 &\implies 1^{55} \pmod{85} = 1 \implies \mathrm{a} \\
49 &\implies 49^{55} \pmod{85} = 14 \implies \mathrm{n} \\
49 &\implies 49^{55} \pmod{85} = 14 \implies \mathrm{n} \\
79 &\implies 79^{55} \pmod{85} = 4 \implies \mathrm{e} \\
51 &\implies 51^{55} \pmod{85} = 19 \implies \mathrm{s}
\end{aligned}$$

The decrypted message is: "jannes".

This demonstrates the RSA encryption and decryption process with every step calculated explicitly.

3 Chapter 3: Sets