Portfolio

Math 300: Introduction to Mathematical Proof

California State University, East Bay

Fall 2024

Mark Brautigam

11 Dec 2024

Table of Contents

Introduction 3

Examples of Proof Techniques

1. Direct Proof 4
   If *x* is an even integer and *y* is an odd integer, then *xy* is an even integer.

2. Proof Using Contrapositive 5
   For all integers a and b, if ab is even, then a is even or b is even.

3. Proof Using Contradiction 6
   For each positive real number r, if r2 = 18, then r is irrational.

4. Proof of If and Only If Statement 8
   For integers k, 4 divides k^2 if and only if k is even.

5. Proof Using Induction 10
   For each natural number n, 3 divides $(n^3 - n)$.

6. Proof that Two Sets Are Equal 12
   Let A, B, and C be subsets of some universal set U. Then, A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C).

7. Proof that a Relation is an Equivalence Relation 14
   Consider the relation $\sim$ on the set of integers defined by: For a, b, integers, $a \sim b$ if and only if 2 divides $(a + b)$. Prove that this relation is an equivalence relation.

8. Proof that shows a function is injective 16
   Let A, B, and C, be nonempty sets and assume that $f: A \rightarrow B$ and g: B → C.
   If f and g are both injections, then $(g \circ f)$: A → C is an injection.

9. Proof that is beautiful, interesting, or elegant 17
   Consider the relation on the set of real numbers defined by: $x \sim y$ if there exists a nonzero rational number q such that $x = qy$. This relation is an equivalence relation.

10. Proof that I struggled with 19
    There are no integers a and b such that $b^2 = 4a + 2$.

11. Proof that classmates collaborated on 21
    Let A, B, and C be subsets of some universal set U. Then, $A - (B \cap C) = (A - B) \cup (A - C)$.

12. A Proof that I feel proud of 23
    For n an integer, n is odd if and only if n^3 is odd.

Final Reflection 25

Introduction

After a long career in high tech as a software engineer, I spent the last several years teaching computer programming to high school students in San Jose, California. In that class, we used algebra and geometry every single day. I don't know how to do any kind of user interface programming without mathematics. The programmer must precisely place objects on the screen, create icons and logos, even come up with color combinations using hexadecimal math.

When I was in high school, math was my strongest subject. But when I got to university, things didn't work out so well in the more advanced calculus courses. I still had to use trigonometry and even basic calculus in my career as a software engineer, but nothing beyond that.

I am fortunate that my computer science courses included digital logic, combinatorics, graph theory, and applied algebra, which prepared me for this course to some degree.

One reason I chose to pursue this study of mathematics is because of my experience with high school students. During my years at that job, I honestly don't think I did a good job of communicating mathematics to the students. Communicating even elementary math ideas to younger people takes a lot of preparation and the lessons must be meticulously designed. It is possible for a teacher to understand math *too* well, which actually makes it harder to communicate the basic concepts, because they come so easily to the more experienced teacher. This makes it tempting to gloss over small points that are critical to a learner. So, an important part of what I'm learning in this class is how to effectively communicate mathematics to students who want to learn. Participation in the small groups is an important part of this process.

I am currently teaching computer science in the community college setting. I hope to put to use what I've learned in this course about communication and group work.

1. Direct Proof

A direct proof of a proposition is a demonstration that the conclusion of the proposition follows logically from the hypothesis. We use definitions, previously proven propositions, and mathematical properties to justify each step in the proof.

Proposition: If x is an even integer and y is an odd integer, then xy is an even integer.

Some propositions, like this one, seem obvious at first, because we feel almost instinctively that the product of any even integer and any other integer must be an even integer. But, to prove it rigorously, we must pay attention to the definitions and make sure we don't skip a step. The temptation might be to skip something we think is trivial. In a more complicated proof, this might end up with errors. The challenge for me is to make sure I stay on track and make no assumptions.

Proof. Assume we have an even integer x and an odd integer y. We will prove that xy is then an even integer.

If x is an even integer, then, by definition, there exists an integer k such that $x = 2k$. If y is an odd integer, then, by definition, there exists an integer q such that $y = 2q + 1$.

Then, by algebra and substitution,

$$\begin{aligned} xy &= (2k)(2q+1) \\ &= 4kq + 2k \\ &= 2(2kq + k) \end{aligned}$$

So, $xy = 2r$ for some integer $r = 2kq + k$. We know $2kq + k$ is an integer, because the integers are closed under multiplication and addition. So, by definition, xy is an even integer. We have proven that if x is an even integer and y is an odd integer, then xy is an even integer. 🐾

2. Proof using Contrapositive

The contrapositive of a conditional statement P → Q is the conditional statement ¬Q → ¬P.

P → Q means "P implies Q" or "If P, then Q."
¬Q → ¬P means "Not Q implies Not P" or "If not Q, then not P."

Sometimes we find it easier to prove the contrapositive statement than to prove the original conditional statement. If we can prove either statement, this also proves the other. That is, if we can prove the original statement, this also proves the contrapositive. If we can prove the contrapositive, this also proves the original statement.

Proposition. For all integers a and b, if ab is even, then a is even or b is even.

I chose this proof because it is a counterpart to the direct proof on the previous page. For me, the challenge with contrapositive is that it is not that intuitive to me. Logic dictates that it works, but sometimes I still have to convince myself. This simple example is not that challenging, which makes it a good introduction to contrapositive.

Proof. We will approach this by contrapositive: If a is odd and b is odd, then ab is odd. Assume we have odd integers a and b. Since a is odd, there exists an integer k such that $a = 2k + 1$. Since b is odd, there exists an integer q such that $b = 2q + 1$. By algebra and substitution,

$$\begin{aligned} ab &= (2k+1)(2q+1) \\ &= 4kq + 2k + 2q + 1 \\ &= 2(2kq + k + q) + 1 \\ &= 2r + 1 \end{aligned}$$

for some integer r. We know r is an integer because the integers are closed under addition and multiplication. So $2r + 1$ is odd by definition, hence ab is also an odd integer. We have shown that if a and b are odd integers, then ab is an odd integer. By contrapositive, we conclude that if ab is even, then either a is even or b is even (or both). 🐾

3. Proof Using Contradiction

A contradiction is a compound statement that is false for all possible combinations of truth values of the individual statements. If we can start with a statement P and from it, prove something we know to be false, then we have a contradiction. We might even be able to prove a statement to be both true and false, which is a contradiction.

Proposition. For each positive real number r, if $r^2 = 18$, then r is irrational.

This proof proceeds by contradiction. The proof relies on some lemmas we proved in class. One reason I like this proof a lot is just because I was never before exposed to a proof that a number is irrational, so this is something new to me. I also like fractions, and proofs of rationality and irrationality seem to be full of fractions.

This proof will rely on the following Lemmas, which we proved previously in class.

Lemma 1. If m is an integer, then $m/1$ is rational.

Lemma 2. Any rational number can be expressed in least terms m/n where $n \neq 0$ and m and n have no common factors greater than 1.

Lemma 3. If n is an integer, if n^2 is even, then n is even.

Proof. We will show that if r is a real number and $r^2 = 18$, then r is irrational. We will proceed by contradiction. Assume r is a positive real number, $r^2 = 18$ and r is rational. By definition, $r = m/n$ for some integers m and n, and m and n do not share factors greater than 1, and $n \neq 0$. By substitution and algebra,

$$r = \frac{m}{n}$$

$$18 = \left(\frac{m}{n}\right)^2$$

$$18 = \frac{m^2}{n^2}$$

$$m^2 = 18n^2$$

$$m^2 = 2(9n^2)$$

Continued on next page →

We know m^2 is an even integer. By Lemma 3, m is an even integer. By definition, there exists an integer k such that $m = 2k$. So

$$m^2 = (2k)^2 = 2(9n^2)$$

$$m^2 = (2k)(2k) = 2(9n^2)$$

$$m^2 = 2(2k^2) = 2(9n^2)$$

So now we know that $2k^2 = (3n)^2$. By definition, $(3n)^2$ is an even number. By Lemma 3, we see that $3n$ is an even number. So we know that n is an even number. So m is even and n is even. This is a contradiction because by Lemma 2, m and n have no common factors greater than 1. ↮

Thus our original assumption must have been false. So if a real number $r^2 = 18$, then r is irrational. 🐾

4. Proof of If and Only If Statement

To prove an "if and only if" statement, we need to prove both directions. That is, in order to prove "P if and only if Q," we need to prove both "If P, then Q" and also "If Q, then P." In other words, P → Q and Q → P.

Proposition. For integers k, 4 divides k^2 if and only if k is even.

This is an interesting proof because not only do we have to prove both directions, but in one direction, we proceed by contradiction. In the other direction, we use a direct proof. When constructing the proof of an "if and only if" statement, we do not have to use the same strategy for both directions. We can use whatever strategy works best in each case, and this may be two different strategies.

Proof. To demonstrate that 4 divides k^2 if and only if k is even, we will show that if 4 divides k^2, then k is even. We will also show that if k is even, then 4 divides k^2.

Part 1. (→) We will show that for an integer k, if 4 divides k^2, then k is even. We will demonstrate this by contradiction. Assume 4 divides k^2 and k is odd. Since k is odd, there exists an integer q such that $k = 2q + 1$. By substitution and algebra,

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

which is an odd number by definition. We know that $2q^2 + 2q$ is an integer, because the integers are closed under multiplication and addition.

If 4 divides k^2, then there exists a number r such that $4r = k^2$. By substitution and algebra,

$$\begin{aligned} k^2 &= 4r \\ &= 2(2r) \end{aligned}$$

which is an even number by definition. So, we arrive at a contradiction, since k^2 cannot be both an odd number and an even number. We conclude that if 4 divides k^2, then k must be even.

Continued on next page →

Part 2. (←) We will show that for an integer k, if k is even, then 4 divides k^2. We assume k is even, therefore there exists an integer s such that $k = 2s$. By substitution and algebra,

$$k = 2s$$
$$k^2 = (2s)^2$$
$$= 4s^2$$

If 4 divides k^2, then there exists an integer t such that $4t = k^2$. In this case, $t = s^2$. So, 4 divides k^2. This means that if k is even, then 4 divides k^2.

Conclusion. Since we have shown that if 4 divides k^2, then k must be even, and if k is even, then 4 divides k^2, we conclude that 4 divides k^2 if and only if k is even. 🐾

5. Proof Using Induction

Induction is a technique we use to prove statements about the natural numbers,

$$n \in 1, 2, 3, \ldots$$

We cannot use direct proof to prove a proposition is true for every natural number n, because there are infinitely many of them. Instead, we use a recursive technique to demonstrate that the proposition is true for every n. We do this in two steps:

1. Show that the statement is true for $n = 1$.
2. Show that if the statement is true for some natural number k, it is also true for $k + 1$.

The first step is called the **basis step**. The second step is called the **inductive step**.

Proposition. For each natural number n, 3 divides $(n^3 - n)$.

I chose this proof because it is one of the longer inductive proofs we have done. It was satisfying to work on. In the process of copying this from a previous assignment to here, I corrected a few typos and added some clarifying statements. It seems that no matter how much I pore over the text, there is always something to tweak.

Proof. We proceed by the principle of mathematical induction. For each natural number n, we let $P(n)$ be the statement

$$3 \text{ divides } (n^3 - n).$$

Basis step. We first prove that $P(1)$ is true. Let $n = 1$.

$$n^3 - n = 1^3 - 1 = 1 - 1 = 0.$$

3 divides 0, so $P(1)$ is true.

Inductive step. We will prove that for each natural number k, if $P(k)$ is true, then $P(k + 1)$ is true. We assume that $P(k)$ is true, that is,

$$3 \text{ divides } (k^3 - k).$$

The goal now is to prove that $P(k + 1)$ is true. So we will prove that

$$3 \text{ divides } (k + 1)^3 - (k + 1).$$

Continued on next page →

By algebra, we see that

$$\begin{aligned}(k+1)^3-(k+1) &= k^3+3k^2+3k+1-(k+1)\\ &= k^3+3k^2+2k\\ &= k(k+1)(k+2)\\ &= k(k+1)(k-1+3)\\ &= k(k+1)(k-1)+3k(k+1)\\ &= (k^3-k)+3k(k+1)\end{aligned}$$

We know that 3 divides k^3-k because that is our initial assumption. So we can rewrite the previous equation as follows:

$$(k+1)^3-(k+1)=3q+3r$$

where $q=k^3-k$ and $r=k(k+1)$. We know q is an integer by the definition of divides. We know r is an integer because the integers are closed under multiplication and addition. By distribution, we see that

$$\begin{aligned}(k+1)^3-(k+1) &= 3(q+r)\\ &= 3s\end{aligned}$$

Where $s=q+r$. We know that s is an integer because the integers are closed under addition. So we know that 3 divides $(k+1)^3-(k+1)$ by the definition of divides. So we have shown that if $P(k)$ is true, then $P(k+1)$ is true. By the principle of mathematical induction, we conclude that for each natural number n, 3 divides (n^3-n). 🐾

6. Proof that Two Sets Are Equal

This is a perhaps somewhat longer proof that two sets are equal. In order to prove set equality, we show that each set is a subset of the other set. There is another proof of set equality in Proof 11, a collaboration with other students in my group.

Proposition.
Let A, B, and C be subsets of some universal set U. Then, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

This proof is not difficult. But like some other proofs involving sets, putting it together was a little tedious. The symbols for set notation are not easy to access. I found myself copying and pasting a lot. This introduced the possibility of copy and paste errors, especially substituting ∩ for ∪ and vice versa.

Proof. In order to show set equality, we will prove that each set is a subset of the other set.

[⊆] We will first prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Let x be an element chosen arbitrarily from $A \cap (B \cup C)$. By definition of set intersection, $x \in A$ and also $x \in B \cup C$. By definition of set union, since $x \in B \cup C$, then $x \in B$ or $x \in C$.

In the first case, if $x \in B$ and $x \in A$, then by definition of set intersection, $x \in A \cap B$. In the second case, if $x \in C$ and $x \in A$, then by definition of set intersection, $x \in A \cap C$.

So $x \in A \cap B$ or $x \in A \cap C$. By definition of set union, $x \in (A \cap B) \cup (A \cap C)$. Since an element x chosen arbitrarily from $A \cap (B \cup C)$ is also an element of $(A \cap B) \cup (A \cap C)$, by definition of subset, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

[⊇] We will now prove that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Let x be an element chosen arbitrarily from $(A \cap B) \cup (A \cap C)$. By definition of set union, $x \in A \cap B$ or $x \in A \cap C$. In the first case, by definition of set intersection, if $x \in A \cap B$, then $x \in A$ and $x \in B$. In the second case, if $x \in A \cap C$, then $x \in A$ and $x \in C$. In either case $x \in A$.

If $x \in A \cap B$, since we already know that $x \in A$, it must also be that $x \in B$. If $x \in A \cap C$, since we know that $x \in A$, it must also be that $x \in C$. So $x \in B$ or $x \in C$. By definition of set union, $x \in B \cup C$. Since we already know that $x \in A$, by definition of set intersection, $x \in A \cap (B \cup C)$.

Continued on next page →

Since an element *x* chosen arbitrarily from (A ∩ B) ∪ (A ∩ C) is also an element of A ∩ (B ∪ C), by definition of subset, (A ∩ B) ∪ (A ∩ C) ⊆ A ∩ (B ∪ C).

Since we have shown that A ∩ (B ∪ C) ⊆ (A ∩ B) ∪ (A ∩ C) and (A ∩ B) ∪ (A ∩ C) ⊆ A ∩ (B ∪ C), we conclude that A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C). 🐾

7. Proof that a Relation is an Equivalence Relation

A relation is an equivalence relation if the relation is reflexive, symmetric, and transitive.

- A relation R is **reflexive** on the set A if for every element $x \in A$, $(x, x) \in R$.
- A relation R is **symmetric** if for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
- A relation R is **transitive** if for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Proposition.
Consider the relation $\sim$ on the set of integers defined by:
For a, b, integers, $a \sim b$ if and only if 2 divides $(a + b)$.
Prove that this relation is an equivalence relation.

This is not a difficult proof. I like it because it clearly shows the reflexive, symmetric, and transitive properties in use.

Proof. To show that this relation is an equivalence relation, we must show that the relation is reflexive, symmetric, and transitive.

1. Reflexive.

The relation R is reflexive on A if for each x in A, x R x, or (x, x) is an element of A.

Let x be an element chosen arbitrarily from A. R is reflexive if (x, x) is an element of A. 2 divides $(x + x)$. $x + x = 2x$, and 2 divides $2x$ by definition of divides. By definition, R is reflexive. So we have shown that R is reflexive.

2. Symmetric.

Let x and y be two elements chosen arbitrarily from A. Assume 2 divides $(x + y)$. $x + y = y + x$ (by the symmetric property of addition). We know 2 divides $(y + x)$ because 2 divides $(x + y)$. So both $(x \sim y)$ and $(y \sim x)$ are in the relation. By definition, R is symmetric. So we have shown that R is symmetric.

Continued next page →

3. Transitive.

Let x, y, and z be three elements chosen arbitrarily from A. Assume 2 divides $(x + y)$ and 2 divides $(y + z)$. By definition of divides, $x + y = 2q$ where q is an integer. Also by definition of divides, $y + z = 2r$ where r is an integer. Then by substitution and algebra,

$$x + y + y + z = 2q + 2r$$
$$x + 2y + z = 2q + 2r$$
$$x + z = 2q + 2r - 2y$$
$$x + z = 2(q + r - y)$$
$$x + z = 2s$$

Where $s = q + r - y$. We know s is an integer because the integers are closed under addition and subtraction. So, we see 2 divides $x + z$ by definition of divides. Since we know 2 divides $x + y$ and 2 divides $y + z$, and we have shown that 2 divides $x + z$, by definition, the relation R is transitive.

Conclusion. Since we have shown that the relation R is reflexive, symmetric, and transitive, we conclude that R is an equivalence relation.

8. Proof that shows a function is injective

A function $f: A \rightarrow B$ from the set A to the set B is an injection (or is injective) if

For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.

Another way to say this is that f is one-to-one; each element $f(x)$ in B (called an *image*) has its own unique corresponding element x in A (called a *preimage*).

Proposition. Let A, B, and C, be nonempty sets and assume that $f: \mathrm{A} \rightarrow \mathrm{B}$ and $g: \mathrm{B} \rightarrow \mathrm{C}$. If f and g are both injections, then $(g \circ f) : \mathrm{A} \rightarrow \mathrm{C}$ is an injection.

This proof concerns the composition of functions. $(g \circ f) = g(f(x))$. This is a concept that is familiar to programmers, especially those with a background in functional programming. We apply one function, then we apply the second function to the output of the first function.

Proof. Assume we have nonempty sets A, B, and C, and $f: \mathrm{A} \rightarrow \mathrm{B}$ and $g : \mathrm{B} \rightarrow \mathrm{C}$ are both injections.

By definition of injection, for all x, y in A, if $x \neq y$, then $f(x) \neq f(y)$. Let a and b be two elements chosen arbitrarily from A, and let $a \neq b$. Then $f(a) \neq f(b)$. Let $c = f(a)$ and $d = f(b)$. c and d are elements of B. We know $c \neq d$ because f is an injection. So c and d are two different elements of B. c and d are not selected arbitrarily, but they are not equal.

By definition of injection, for all x, y in B, if $x \neq y$, then $g(x) \neq g(y)$. Since $c \neq d$, then $g(c) \neq g(d)$. Let $e = g(c)$ and $f = g(d)$. e and f are elements of C. $e \neq f$. So e and f are two different elements of C.

So we have a and b, two elements of A, and $a \neq b$. By applying the two functions f and g, we find e and f, two elements of C, and $e \neq f$.

So we have $a \neq b$, and $(g \circ f)(a) \neq (g \circ f)(b)$. So By definition of injection, the two functions applied together $(g \circ f)$ is an injection. 🐾

9. Proof that is beautiful, interesting, or elegant

I have to be honest and say that I love the rational numbers and I love fractions. This proof makes use of fractions, not in a clever or even interesting way, but in a way that I think is beautiful and maybe elegant. There is a certain symmetry to the way the fractions resolve.

Proposition. Consider the relation on the set of real numbers defined by: $x \sim y$ if there exists a nonzero rational number q such that $x = qy$. This relation is an equivalence relation.

This is a proof about an equivalence relation. We discussed equivalence relations in Proof #7 on page 13.

Proof. To show that this relation is an equivalence relation, we must show that the relation is reflexive, symmetric, and transitive.

Reflexive. The relation $\sim$ is reflexive if for all x in A, (x, x) is in A. Let x be an arbitrarily selected element of A. Then

$$x = x$$
$$x = 1 \cdot x$$
$$x = q \cdot x$$

where $q = 1$, a rational number. We have shown that the relation ~ is reflexive.

Symmetric. The relation $\sim$ is symmetric if for all x in A, if $x{\sim}y$, then $y{\sim}x$. Let x and y be arbitrarily selected elements of A such that $x \sim y$. Then

$$x = q \cdot y \qquad \text{by proposition}$$

$$x = \frac{a}{b} \cdot y \qquad \text{by def. of rational number}$$

where a and b are integers and a and b are non-zero.

$$\frac{b}{a} \cdot x = \frac{b}{a} \cdot \frac{a}{b} \cdot y \qquad \text{multiply both sides by } \frac{b}{a}$$

$$\frac{b}{a} \cdot x = y \qquad \frac{b}{a} \cdot \frac{a}{b} = 1$$

Therefore $y \sim x$ by definition. We have shown that the relation $\sim$ is symmetric.

Continued next page →

Transitive. The relation $\sim$ is transitive if for all x, y, and z in A, if $x \sim y$ and $y \sim z$, then $x \sim z$. Let x, y, and z be arbitrarily selected elements of A such that $x \sim y$ and $y \sim z$. Then by definition of the relation,

$$x = q \cdot y \text{ and } y = r \cdot z$$

where q and r are non-zero rational numbers. By definition of rational numbers,

$$x = \tfrac{a}{b} \cdot y \text{ and } y = \tfrac{c}{d} \cdot z$$

where a, b, c, and d are non-zero integers. By substitution and algebra,

$$x = \frac{a}{b} \cdot y$$

$$= \frac{a}{b} \cdot (\frac{c}{d} \cdot z)$$

$$= \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) z$$

$$= \frac{ac}{bd} \cdot z$$

$$= \frac{e}{f} \cdot z$$

where $e = ac$ and $f = bd$. We know e and f are integers because the integers are closed under multiplication. We know e and f are non-zero because a, b, c, and d are non-zero.

$$x = \frac{e}{f} \cdot \ z$$

$$= s \cdot z$$

where $s = \frac{e}{f}$. We know s is a rational number by definition, because e and f are non-zero integers. So we have shown that $x \sim z$ by definition. So we have shown that the relation $\sim$ is transitive.

Conclusion. Since we have shown that the relation $\sim$ is reflexive, symmetric, and transitive, we conclude that $\sim$ is an equivalence relation. 🐾

10. Proof that I struggled with

Proposition. There are no integers a and b such that $b^2 = 4a + 2$.

This proof should probably proceed by contradiction. When I first wrote the proof, it seemed that two cases were necessary. The instructor pointed out that I had not completely covered the second of the two cases. I went back and split the second case into two sub-cases, which resulted in a correct but overly long proof. It turns out the two sub-cases were not really necessary, and the second case can proceed without sub-cases. This is a situation where I moved too quickly to fix an initial error without looking at the bigger picture.

Proof. We will proceed by contradiction. We will look at two separate cases.

- Case 1: b is odd
- Case 2: b is even

Case 1. b is odd. Assume a and b are integers, $b^2 = 4a + 2$, and b is odd. By definition of odd, $b = 2k + 1$ for some integer k. By substitution and algebra, we have

$$\begin{aligned} b^2 &= 4a + 2 && \\ (2k+1)^2 &= 4a + 2 && \text{substitution} \\ 4k^2 + 2k + 1 &= 4a + 2 && \text{expansion} \\ 2(k^2 + k) + 1 &= 2(a + 1) && \text{factoring} \\ 2q + 1 &= 2r && \text{substitution} \end{aligned}$$

for some integer q and some integer r. The left-hand side is odd, by definition, and the right-hand side is even, by definition. But an odd integer cannot equal an even integer, so we have a contradiction. So we conclude there are no such integers a and b that satisfy the equation if b is odd.

Continued next page →

Case 2. b is even. Assume a and b are integers, $b^2 = 4a + 2$, and b is even. By definition of even, $b = 2k$ for some integer k, and $a = 2q$ for some integer q. By substitution and algebra, we have

$b^2 = 4a + 2$	
$(2k)^2 = 4a + 2$	substitution
$4k^2 = 4a + 2$	expansion
$2k^2 = 2a + 1$	divide both sides by 2
$2s = 2a + 1$	substitution

for some integer $s = k^2$. We know that s is an integer because the integers are closed under multiplication. The left-hand side is even, by definition, and the right-hand side is odd, by definition. But an even integer cannot equal an odd integer, so we have a contradiction. So we conclude that there are no such integers a and b that satisfy the equation if b is even.

Conclusion. Since we have demonstrated that $b^2 \neq 4a + 2$ whether b is odd or even, we conclude that there are no integers a and b such that $b^2 = 4a + 2$. 🐾

11. Proof that classmates collaborated on

Group effort: Mark Brautigam, Regan Peri, Ericka Reyes, Jinbiao Tan

Proposition:
Let A, B, and C be subsets of some universal set U. Then, $A - (B \cap C) = (A - B) \cup (A - C)$.

Ericka chose to present this proof to our group. Part A proceeded smoothly, but Ericka herself had some questions about Part B and we agreed that something was not quite right. After consulting with the instructor, all of us worked together to flesh out the various pieces of Part B. We were all pleased with the result. We were glad that our collaboration helped us understand these set concepts better.

Proof. To show set equality, we first show that the left-hand side is a subset of the right-hand side. Then we show that the right-hand side is a subset of the left-hand side.

A. ⊆ We first show $A - (B \cap C) \subseteq (A - B) \cup (A - C)$.

Let x be an arbitrarily chosen element of $A - (B \cap C)$. By definition of set difference, $x \in A$ but $x \notin B \cap C$. Since $x \notin B \cap C$, by definition of intersection, $x \notin B$ or $x \notin C$.

If $x \in A$ and $x \notin B$, then $x \in A - B$. If $x \in A$ and $x \notin C$, then $x \in A - C$. By definition of union, since $x \in A - B$ or $x \in A - C$, $x \in (A - B) \cup (A - C)$. By definition of subset, $A - (B \cap C) \subseteq (A - B) \cup (A - C)$.

So, we have shown $A - (B \cap C) \subseteq (A - B) \cup (A - C)$.

B. ⊇ We will now show $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

Let x be an arbitrarily chosen element of $(A - B) \cup (A - C)$. By definition of union, $x \in A - B$ or $x \in A - C$. By definition of set difference, $x \in A$ but $x \notin B$. Similarly, $x \in A$ but $x \notin C$.

Either way, we know $x \in A$. We also know that $x \notin B$ or $x \notin C$. By definition of intersection, either $x \in B$ and $x \notin C$, or $x \in C$ and $x \notin B$, or $x \notin B$ and $x \notin C$.

By definition of intersection, if $x \in B$ and $x \notin C$, then $x \notin B \cap C$. By definition of intersection, if $x \in C$ and $x \notin B$, then $x \notin B \cap C$. Finally, if $x \notin B$ and $x \notin C$, then $x \notin B \cap C$.

Continued next page →

Either way, $x \notin B \cap C$. Since we have already established that $x \in A$, by definition of set difference, $x \in A - (B \cap C)$. By definition of subset, $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

So, we have shown $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

Conclusion. Since we have shown that $A - (B \cap C) \subseteq (A - B) \cup (A - C)$ and $(A - B) \cup (A - C) \subseteq A - (B \cap C)$, by definition of set equality, we conclude that $A - (B \cap C) = (A - B) \cup (A - C)$. 🐾

12. A Proof that I feel proud of

This is an example of an "if and only if" proof. There is another example of an "if and only if" proof at Proof 4 on page 8. With such a proof, we need to prove both directions. So the proof ends up being twice as long as a direct proof. In this particular proof, each direction is a direct proof, with nothing particularly special.

Proposition. For n an integer, n is odd if and only if n^3 is odd.

There wasn't any one proof that I was particularly proud of. I was proud to be able to draw up any of the proofs that were non-trivial. If I were to choose one, it would probably be Proof 11 on the previous page, because I was proud of the collaboration with classmates.

One reason I chose this proof here is that I may have a bit of a phobia about exponents higher than two. Factoring is harder, and polynomials get squiggly. I don't mind differentiating them because it reduces their degree. So I was proud to successfully address an exponent of 3.

Proof. To show if and only if, we need to prove two propositions: ↔

[1] → If an integer n is odd, then n^3 is odd.

[2] ← For an integer n, if n^3 is odd, then n is odd.

Part 1. → We will show that if n is an integer, and n is odd, then n^3 is odd.
If n is odd, then there exists an integer k such that $n = 2k + 1$. By substitution and algebra,

$$\begin{aligned} n^3 &= (2k+1)^3 \\ &= 8k^3 + 12k^2 + 6k + 1 \\ &= 2(4k^3 + 6k^2 + 3k) + 1 \\ &= 2q + 1 \end{aligned}$$

for some integer $q = 4k^3 + 6k^2 + 3k$. We know q is an integer because the integers are closed under multiplication and addition. So, by definition, n^3 is an odd number.

Continued next page →

Part 2. ← We will show that for an integer n, if n^3 is odd, then n is odd. We will approach this statement by contradiction. That is, we will assume that n^3 is odd and n is even. By definition, if n is even, there exists an integer k such that $n = 2k$. By substitution and algebra,

$$\begin{aligned} n^3 &= (2k)^3 \\ &= 8k^3 \\ &= 2(4k^3) \\ &= 2q \end{aligned}$$

for some integer $q = 4k^3$. We know q is an integer because the integers are closed under multiplication and addition. So, by definition, n^3 is an even integer. But this contradicts our assumption that n^3 is an odd integer. So, it is not possible that n^3 is odd and n is even. So, if n^3 is odd, then n must be an odd integer.

Conclusion. We have shown that if n is an odd integer, then n^3 is odd. We have also shown that if n^3 is odd, then n is an odd integer. So, we conclude that for an integer n, n is odd if and only if n^3 is odd. 🐾

Final Reflection

How I grew as a mathematician. I learned how to write proofs more rigorously than I've been used to. I've had to write proofs before, but they were more math-y (lots of equations) and less thought-y (text with explanations).

We first learned the idea of proofs when we were in Geometry class in high school (freshman year). I really hated proofs because while I could visualize the answer (similar triangles, for example) I had a hard time putting into words the ideas I was seeing in my head. It seemed that others in my high school class had similar difficulties. In this present class, I have learned to hate proofs less and actually appreciate them. That is purely an emotional process, but I think it is an important step in the mathematical journey.

Mentally, I resisted the group work because as a very introverted person, I'm uncomfortable in groups. But I think the group work helped me grow as a potential teacher because it gave me new insights into teaching techniques. (I teach computer science but there is the possibility of teaching math in the future or incorporating these group techniques into my computer science courses.)

If we had time, it might have been good to have a brief review of all the topics at the end, spread out over two to three days, with a few topics each day.

My perception from working in the groups is that contrapositive might have given other students some pause. Also, the discussion of functions and relations at the end seemed rushed. I wish we had one or two more days to discuss those topics in more detail, perhaps with more examples. There was a homework problem regarding function composition, and while this was in the textbook, I don't remember ever discussing it in class. (See Proof #8.)

What I hope to remember and use from this class. I would hope that what I learned in this class would help me to succeed more in my future mathematics courses.

I appreciate what we learned about proof by mathematical induction and the use of natural numbers and rational numbers. I am interested in number theory and I think those topics will come in handy in the future.

I would want to remember the instructor's use of group work and other techniques for helping students learn. I may be able to utilize some of these techniques in my own courses in the future. 🐾