Section 2.3 and 2.4

We are asked to prove a statement about a positive odd integer and a positive even integer. Discuss the following beginnings of proofs with your group.

1. Let m be a positive odd integer and let n be a positive even integer. Then m can be written as $2k+1$ and $n$can be written as $2j$ for nonnegative integers k and j.

2. The odd integer can be written as $2k+1$ and the even integer as $2j$ for $k \in \mathbb{N}$ and $j \in \mathbb{P}$.

3. Let m be a positive odd integer and let n be a positive even integer. Then m can be written as $2k+1$ for some nonnegative integer k and n can be written as $2k$.

4. Let m be a positive odd integer and let n be a positive even integer. Then $m{=}2k+1$ and $n = 2j$ for nonnegative integers k and j.

5. The odd integer can be written as $2x+1$ and the even integer as $2y$ for nonnegative integer x and y.

6. Consider the pairs of numbers (1,4), (3,6), (5,2), (3,10), (63, 48). Because these numbers are pretty random, we can just check them and if it works for them it works for all number.

7. So we have $2k+1$ and $2j$.

8. We are trying to prove something about an odd integer and an even integer. We know that since even integers are divisible by 2, we can say that the even number can be written as $2j$. And odd numbers aren't even so then by the division algorithm, we can write the odd integer as $2k+1$. It is important to point out that j and k are positive integers. Also k can be zero. We know they are positive because we said that our numbers were positive to start out with, I didn't write that up there, but they are in the problem. And because for sake of contradiction, assume that j and/or k were negative. But then 2 is positive. And by the rules of algebra we know that the product of a negative and a positive is a positive so then we get that $2j$ is negative, a contradiction. So we have $n = 2j$ and $m = 2k+1$. It's okay that k is 0 because 0+1=1.

Pick your favorite beginning (You can change it a bit if you want/need.) and use it to prove that the product of an even number and an odd number is always even.

Proofs by Cases

Prove that $n^2 + n$ is always even. (Think about how to approach the proof, go as far as you can.)

When trying to prove something(involving one variable) is even, we usually want to consider two cases - either n is even or n is odd. So either $n = 2k$ or $n = 2k + 1$. (Since this is an either/or it is ok to use the variable k twice.) Retry to proof again with these two cases. When we are trying to prove divisibility by another numbers (besides 2) the cases look similar. But you have to make sure you include all of them.

Fact: Set an integer m. Then any integer n can be written as $n = mk + i$ where i is $0, 1, 2, \ldots, m-1$. (For example, if we want to deal with divisibility by 5 - then the cases should be $n = 5k, 5k+1, 5k+2, 5k+3, 5k+4$).

Prove that 3 does not divide $n^2 - 2$ for integers $n \geq 1$.

What should the cases be?

Carryout the proof.

Case 1:

Case 2:

Case 3:

You probably did a lot of the same work over and over again above. You can also use the general from of $3k + i$ where $i = 0, 1, 2$.And do the work first and then plug in the values of i. This is how that would look:

Proof. Let $n = 3k + i$ for $i = 0, 1, 2$. Then

$$n^2 - 2 = (3k + i)^2 - 2 = 9k^2 + 6ki + i^2 - 2.$$

Since 3 divides $9k^2$ and $6ki$, we just need to show that 3 does not divide $i^2 - 2$. When $i = 0$, $i^2 - 2 = -2$. When $i = 1$, $i^2 - 2 = -1$. When $i = 2$, $i^2 - 2 = 2$. Since 3 does not divide $1, -1$ or 2, we can conclude that 3 does not divide $n^2 - 2$. $\square$

Does 7 divide $n^2 - 2$ for integers $n \geq 1$? Do a proof similar to the one above and see what happens. Use this to help construct a counterexample.

Recall that

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

Prove the triangle inequality, i.e. for all real numbers x and y

$$|x + y| \leq |x| + |y|.$$

Proof by Contradiction

The general idea behind proof by contradiction is that we assume the thing we are trying to prove is false. And then we do some work to show that this assumption leads to a contradiction. Therefore, our assumption must have been wrong and what we were trying to prove must have been true all along.

Here is an example of a proof by contradiction:

Theorem 1. *There are infinitely many prime numbers.*

Proof. Assume not, i.e. assume there are finitely many prime numbers. Call the prime numbers $p_1, p_2, \ldots, p_n$, where p_n is the largest prime number. Then consider the number $k = p_1 \cdot p_2 \cdots \cdot p_n + 1$. Since k is one more than a multiple of p_i for all $1 \leq i \leq n$, k is not divisible by any prime number, therefore k must be prime. This is a contradiction since we assumed p_n was the largest prime and k is larger than p_n. Since we have a contradiction, we can conclude there are infinitely many primes. $\square$

Read this proof with your group. Discuss it.

Let's try one.

Theorem 2. $\sqrt{2}$ *is irrational.*

Proof. First, we assume $\sqrt{2}$ is not irrational. If a number is not irrational then

which means (use p and q):

Let's also assume the fraction is in lowest terms. Why can we do this?

Now square both sides.

And multiply through by the common denominator to clear the fractions.

What can we say about p?

Write $p = 2m$. Now, what can we say about q?

Do you see a contradiction? $\square$

Prove that the product of a nonzero rational number and an irrational number is an irrational number.

Proof. For sake of contradiction, assume

□

Sometimes people get a bit too excited about using proof by contradiction and start using it for everything. Read the proof below with your group.

Theorem 3. *The sum of two odd integers is an even integer.*

Proof. For sake of contradiction, assume not. Assume m and n are odd integers and $m + n$ is not even, i.e is odd. There exist integers j and k such that $m = 2j + 1$ and $n = 2k + 1$. Then

$$m + n = 2j + 1 + 2k + 1 = 2(j + k + 1),$$

which is an even number, contradicting our assumption that $m+n$ is odd. Thus the sum of two odd integers is an even integer.

□

We didn't need proof by contradiction above. It would have been much more straight forward to just do a **direct proof**. (Proof by contradiction is a form of indirect proof since we are not just proving what we want, but somehow getting at it another way). On the proof below, cross out the unnecessary steps to turn the proof by contradiction into a direct proof.

Proof. For sake of contradiction, assume not. Assume m and n are odd integers and $m + n$ is not even, i.e is odd. There exist integers j and k such that $m = 2j + 1$ and $n = 2k + 1$. Then

$$m + n = 2j + 1 + 2k + 1 = 2(j + k + 1),$$

which is an even number, contradicting our assumption that $m+n$ is odd. Thus the sum of two odd integers is an even integer.

□

Another form of an indirect proof, which is sometimes more straight forward than a proof by contradiction is a proof by contrapositive.

Proof by Contrapositive

Assume we want to prove $H \implies C$ (H is the hypothesis and C is the conclusion). When we do a proof by contradiction, we assume H and $\neg C$ and see if we can get a contradiction. To do proof by contrapositive, we try to prove $\neg C \implies \neg H$. (Recall that this is logically equivalent to $H \implies C$ and thus if the contrapositive is true the original statement must be true) So we only assume $\neg C$ and see if we can show $\neg H$. This sometimes look quite similar to proof by contradiction.

Below are two examples:

Theorem 4. *If x^2 is irrational, then x is irrational.*

Proof by Contrapositive: (We instead show that if x is rational, then x^2 is rational.) Assume x is rational. Then there exists $m, n \in \mathbb{Z}, n > 0$ such that $x = \frac{m}{n}$. So $x^2 = \frac{m^2}{n^2}$ with $m^2, n^2 \in \mathbb{Z}, n^2 > 0$ and thus x^2 is rational.

Proof by Contradiction: For sake of contradiction, suppose x^2 is irrational and x is rational. Then there exists $m, n \in \mathbb{Z}, n > 0$ such that $x = \frac{m}{n}$. So $x^2 = \frac{m^2}{n^2}$ with $m^2, n^2 \in \mathbb{Z}, n^2 > 0$ and thus x^2 is rational, a contradiction. Thus, if x^2 is irrational, then x is irrational.

Read the two proofs above. As you can see, the proof by contrapositive just makes the proof by contradiction more straight forward. I often find it easier to think in terms of proof by contradiction, but you should always go back at the end and decide if there is a way to make your proof easier.

Another time we use proof by contrapositive if to prove a function is one-to-one.

Remember that a function is one-to-one if $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$. So the way we do a proof by contrapositive is to instead prove that $f(x_1) = f(x_2)$ implies $x_1 = x_2$. Discuss with your group why this is the contrapositive.

Now, let $f : \mathbb{Z} \to \mathbb{Q}$ be defined by $f(n) = \frac{n + \lfloor n \rfloor}{2}$. Use a proof by contrapositive to show f is one-to-one.

Proofs are Tricky

Claim 5. 1 is the largest positive integer.

Proof. Let n be the largest positive integer. Since n^2 is an integer it must be true that

$$n^2 \leq n$$

Dividing through by n, we get that
$$n \leq 1.$$

Since 1 is that only positive integer that satisfies this, we get that $n = 1$. Therefore 1 is the largest positive integer. □

What went wrong and what did we actually prove here?

Claim 6. 1=2

Proof. Let $x = y$. Then
$$xy = y^2$$

$$xy - x^2 = y^2 - x^2$$

$$x(y - x) = (y - x)(y + x)$$

$$x = y + x$$

$$\text{Since } x = y, x = 2x$$

$$1 = 2$$

□

What is we do in each step? Which step is invalid?

Some proofs are pictures (but not in this class...)

Theorem 7. $1 + 3 + 5 + 7 + 9 + \cdots + 2n - 1 = n^2$

First, let's try a few examples.

$$1 + 3 =$$

$$1 + 3 + 5 =$$

$$1 + 3 + 5 + 7 =$$

We will prove this a few different ways to practice using some proof techniques. First, let's convince ourselves it's true using the definition of multiplication.

How can we picture 5x5?

Now, let's change from 5x5 to 6x6. What do you need to add?

Now let's do a geometric proof.

Draw a picture of 4^2. See if you can find a way to view this as $1 + 3 + 5 + 7$.

Use this geometric intuition to prove the claim in general.

Now, we'll do a proof by induction. First, a little example. I have a bag with some numbers in it. I will tell you two facts about these numbers.

1. The number 1 is in the bag.

2. For each number that in the bag, the next number is in the bag.

Which numbers are in the bag?

A related example. Assume I am trying to prove a statement for all integers. I show the following facts:

1. The statement is true for $n = 1$

2. If we assume the statement is true from some integer n, we can show it is true for $n + 1$.

For which integers is the statement true?

This will be the idea behind proof by induction. If we want to prove a statement is true for all integers, we need to do two things.

1. Prove the statement is true for $n = 1$. This is called the base case.

2. Assume the statement is true for some arbitrary n and show this implies it's true for $n + 1$. This is called the inductive step.
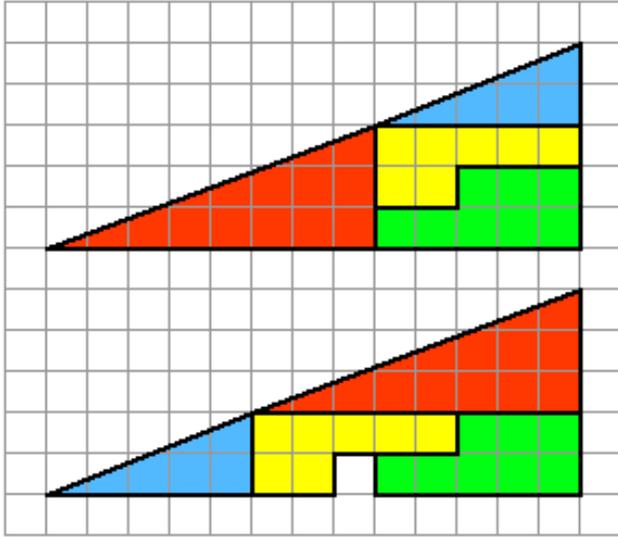
Theorem 8.
$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}$$

Proof:

Now let's look at some sample proofs. We'll begin with a picture proof.

Claim 9. Area can change when you move pieces around.

What do you think?

What does the following picture prove?