MATH 267 Fall 2026 - Class Notes

09/14/2026

Scribe: Virginia

Summary: We began with an in-class warm-up reviewing how to select an appropriate proof method (direct, contrapositive, contradiction, or cases) for different kinds of statements. The lecture then covered proofs by contradiction in detail. We worked a full contradiction proof showing there are no positive integers a, b with $a^2 - b^2 = 1$, then introduced proof by cases and used it to show that $3 \mid (n^3 - n)$ for every integer n. We ended by setting up contradiction proofs for two more statements, including the irrationality of $\sqrt{2}$.

Notes: Warm-up: choosing a proof method.

1. *"If $a + b$ is odd, then a is even or b is even."* A direct proof is harder than the contrapositive here. Trying a direct proof, we would start with $a + b$ odd, i.e. $a + b =$ 2k+1. This is problematic for two main reasons:

   - It is one equation with many variables (one equation with two unknowns), so we can't easily solve it
   - We would need to prove an OR statement

   For a proof using the contrapositive, the starting point is the negation of the conclusion: *a is odd and b is odd.* That is a lot to work with since we already have two known facts.

2. *"There do not exist integers m and n with $6m + 3n = 100$."* The phrase "do not exist" hints that a proof by contradiction might be a good choice. Your starting point should be to negate the statement you're trying to prove.

3. *"For ever real number x, $|x| \geq x$."* The absolute value is naturally defined as a piecewise function, so you can't just plug it in. Since $|x|$ is defined piecewise, this is a good hint to do a proof by cases.

4. *"There is no integer n such that n is even and n^2 is odd."* The statements starts out with $\neg\exists$, so its negation starts with $\exists$. A contradiction proof therefore has the *existence* as something to work with.

Start of lecture: proofs by contradiction. To prove a statement S, we start by supposing $\neg S$.

- We are negating the *entire* statement, not just the conclusion.

- The "goal" is to derive a false statement. We build a list of true statements, each following from what came before, until we reach a contradiction. You don't know ahead of time what the false statement will be. This is why proofs by contradiction are hard. In the beginning you don't know what the false statement is; you have to go find it.

Setting up the example below. For the statement "there do not exist positive integers a, b such that $a^2 - b^2 = 1$," the phrase "do not exist" is a hint to try a proof by contradiction. Formally (with $a > 0$, $b > 0$):

$$S: \neg\big(\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}\,(a^2 - b^2 = 1)\big), \qquad \neg S: \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}\,(a^2 - b^2 = 1).$$

We always start proofs by contradiction with *"Suppose for contradiction that…"* Two ways to indicate the end of a proof by contradiction are the symbol $\rightarrow\leftarrow$, or a lightning bolt ("struck down your false supposition"). A direct proof instead ends with a tombstone symbol ($\square$) or "Therefore, …".

Choosing methods - General:

- "If …, then …" statements: direct proof or contrapositive.
- Statements with $\forall$, $\exists$ lend themselves better to proof by contradiction.

Proof by cases. This one can be missed with direct/contrapositive or contradiction proofs.

- Use proof by cases any time we want to make additional assumptions that simplify the problems.
- By using different assumptions we cover all possibilities.
- Proof by cases has a tendency to be tedious.

End-of-class setup exercises. We practiced *setting up* proofs by contradiction.

1. *Set up a proof by contradiction for: "There is no integer n such that $2n+1$ is even." Proof 1 (setup).* Suppose for contradiction there exists an integer n where $2n+1$ is even. Then there exists an integer k such that $2n+1 = 2k$ …
2. *Start a proof by contradiction that $\sqrt{2}$ is irrational." Proof (setup).* Suppose for contradiction that $\sqrt{2}$ is rational. Then, $\sqrt{2} = \frac{p}{q}$ for some integers p, q where $q \neq 0$. (Equivalently: $\sqrt{2} \in \mathbb{Q}$, so $\sqrt{2} = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$, and then $2 = \frac{a^2}{b^2}$.)

Definitions:

Definition 1. *The absolute value $|x|$ is defined piecewise:*

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

Theorems and Proofs: Use theorem environments for important results:

Theorem 1. *There do not exist positive integers a, b such that $a^2 - b^2 = 1$.*

Proof. Suppose for contradiction there exist positive integers a, b with $a^2 - b^2 = 1$. Then $a^2 - b^2 = (a+b)(a-b)$, so

$$(a+b)(a-b) = 1.$$

Since a and b are positive, $a+b$ is positive. Since $(a+b)$ is positive and 1 is positive, $(a-b)$ must also be positive.

Since $(a+b)$ is positive and $(a-b)$ is positive and they multiply to 1, we must have $a+b = 1$ and $a-b = 1$ Add the equations:

$$2a + \underbrace{b - b}_{0} = 2$$

so $2a = 2$ and $a = 1$. But if $a = 1$ then $1 + b = 1$. So $b = 0$, which is not positive, a contradiction. We contradicted something we assumed to be true (we derived that b had to be 0 following true statements, which contradicts what we assumed to be true). $\rightarrow\leftarrow$ One of the ways to get our contradiction is to contradict something we are assuming. $\square$

Theorem 2. $3 \mid (n^3 - n)$ *for any integer n.*

Proof. We prove this by cases depending on the remainder when n is divided by 3. (Can we make assumptions about n that simplify this? Note this is easy when n is divisible by 3. The remaining integers have remainder 1 or 2 when divided by 3, so there are 3 cases, and we have to handle each separately: $n = 3k$, i.e. n is divisible by 3; $n = 3k+1$, i.e. n has remainder 1 when divided by 3; and $n = 3k+2$, i.e. n has remainder 2.) First suppose $3 \mid n$. Then $n = 3k$ for some integer k. Then

$$n^3 - n = (3k)^3 - 3k = 27k^3 - 3k = 3(9k^3 - k).$$

Since $(9k^3 - k)$ is an integer, $n^3 - n$ is divisible by 3. Now, suppose n has remainder 1 when divided by 3. Then $n = 3k+1$ for some integer k. (We can reuse k, because the proof for the 2nd case is completely separate/different). Using $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$:

$$n^3 - n = (3k+1)^3 - (3k+1) = (27k^3 + 27k^2 + 9k + 1) - (3k+1) = 27k^3 + 27k^2 + 6k = 3(9k^3 + 9k^2 + 2k).$$

So $n^3 - n$ is divisible by 3. Finally, suppose the remainder when n is divided by 3 is 2. Then $n = 3k+2$ for some integer k. Then

$$\begin{aligned} n^3 - n &= (3k+2)^3 - (3k+2) \\ &= 27k^3 + 3(3k)^2(2) + 3(3k)(2^2) + 2^3 - (3k+2) \\ &= (27k^3 + 54k^2 + 36k + 8) - (3k+2) \\ &= 27k^3 + 54k^2 + 33k + 6 \\ &= 3(9k^3 + 18k^2 + 11k + 2). \end{aligned}$$

So again $n^3 - n$ is divisible by 3 In every case, $n^3 - n$ was divisible by 3. $\square$

Questions raised in class:

- When formalizing "there exist positive integers a, b with $a^2 - b^2 = 1$," can you write $\exists a \in \mathbb{Z}$, $b \in \mathbb{Z}$ (with only one ($\exists$)? **No.** We need both $\exists$'s because we need to formally state that there exist 2 different integers.
- The two setup exercises at the end of class (the contradiction for "no integer n makes $2n + 1$ even," and the irrationality of $\sqrt{2}$) were only set up, not finished. The full arguments were left for next time.