Proof Portfolio
Math 210

Quang Nguyen
Wittenberg University

Fall 2018

Contents

Chapter 1

Midterm Reflection

Which of your proof drafts to date do you feel has been your best? Why do you think that is?

By far, I'm most satisfied with my drafts for problems 1 and 3. Problem 1 consists of proofs about numbers, and problem 3 is a proof by mathematical induction, and I've had chances working on these types of problems as in-class and homework exercises. In addition, these 2 kinds of proofs did appear on our last quiz and test, for which I spent a fair amount of time studying for. Furthermore, the proofs to these 2 problems are pretty straightforward, as they involve very basic terms like the definition of even and odd numbers, the division theorem and the principle of mathematical induction.

What do you feel is your greatest strength when preparing proof portfolio drafts?

I think my greatest strength is my ability to work independently. This skill really helps me in the process of self-brainstorming, finding needed concepts, definitions, theorems... from class notes and our textbook and reviewing errors. Moreover, I also taught myself how to use LaTeX to write up proofs.

Which of the proof portfolio problems has been your favorite to work on so far? Which one was the hardest? Why?

Problem 2 has been my favorite to work on so far and also the one I think was the toughest. This problem requires some knowledge of algebra - in particular, quadratic factorization. Figuring out the right technique to prove this problem (whether to use direct proof, proof by contradiction, proof by contrapositive, or some other method) is another aspect that makes Problem 2 interesting and a little hard. Furthermore, cases needed to be used in order to prove this problem. Therefore, in order to have a complete proof, a fair amount of work is required for problem 2.

What do you think is the area in which you most need to improve in preparing proof portfolio drafts? Why? What plans do you have for making this improvement?

I think the area that I can improve is being more organized . For one of the problems (I think it's one of the contradiction proofs), I first did some brainstorming, but forgot to write down what I was thinking. Therefore, when I wrote my proof, I got stuck quite a bit because I did not remember what to do. So I had to do the brainstorming part again, and after all, I managed to get on the right track. But had the notes been taken before, I would have saved my time and this would make have made the proof-writing process easier. So what I learned from this is to always write down some notes, because you never know when you'll need them.

What insights ("Aha!" moments) have you had about the process of proving results and writing up your proofs for the portfolio?

I experienced this moment when I was working on problem 4A - a problem involving the Pigeonhole principle. After several attempts, I finally figured out the key to solve the problem, which are the number of boxes to distribute the numbers into, the boxes labels and the least amount of items each box must have.

What changes to how the instructor provides feedback could make it more useful for you as you finish your portfolio?

For the moment, I do not have any suggestions for changes.

Chapter 2

Final Reflection

Which of your proofs do you feel is the best? Why do you think this is?

I'm most content with my proofs for problems 1 and 3 (the same 2 problems I said I feel most satisfied with in my midterm reflection). Problem 1 features 3 proofs about numbers, and problem 3 is a proof by mathematical induction, and I've done plenty of assignments on these types of proof this semester. Additionally, the proofs to these 2 problems are relatively straightforward, as they involve very basic terms like the definition of odd and even integers, the division theorem and the principle of mathematical induction.

Which of your proofs do you feel least confident about? Why do you think this is?

I feel least confident about the very last proof (8B), which is the problem about function. I think this proof is very challenging because there are lots of information given in the problem statement, and we have to know how to utilize all those information to come up with the right proof. Another reason is that I started working on this proof at the very last place, and I only turned in one draft for this proof prior to my final submission, therefore the amount of feedback I get for problem 8B is not a lot.

What do you feel is your greatest strength when writing proofs for this portfolio?

Just like what I mentioned in my midterm reflection, I feel that my ability to work independently is my best strength. I have successfully utilized this skill in the process of self-brainstorming, finding needed concepts, definitions, theorems... from class notes and our textbook and reviewing errors. Moreover, I also taught myself how to use LaTeX to write up proofs.

Reflect on the entire semester and comment on how you feel you have progressed in writing proofs. You should specifically address what you think has been your biggest improvement and what insights ("Aha!" moments) you have had about the process of proving results and writing up your proofs for your portfolio.

I've learned different proof techniques such as direct proof, proof by contrapositive, contradiction and induction. Since there are many proof methods, sometimes it's hard to know which one is the correct method to use to solve a problem. Therefore figuring out the right technique to use is crucial, and so I've had a few "Aha!" moments after I discovered the right approach.

For instance, I experienced this moment when I was working on problem 4A - a problem involving the Pigeonhole principle. After several attempts, I finally figured out the key to solve the problem, which are the number of boxes to distribute the numbers into, the boxes labels and the least amount of items each box must have.

Do you think that the proof portfolio was valuable in helping you improve your skills in writing proofs? If so, please indicate which parts were most helpful. If not, please comment on why you feel it was not valuable. In both cases, please give any suggestions you might have on how the instructor could improve the implementation of the project in the future.

This project really helps me improve my proof-writing skills. It allows me to practice writing proofs using different techniques and receive feedback in order to improve my work. The proof portfolio also gives me a chance to demonstrate what I've learned throughout the semester. All the skills I've gained from this project and this course (writing, brainstorming, reviewing errors...) will definitely help me in the future when I take upper level math courses.

One thing I would change about the project is the start date. I would give students an earlier date to begin working on the portfolio (probably one month into the semester, after the first test).

Chapter 3

Problems

3.1

Problem Statement: Let $n \in \mathbb{Z}$.

(a) Prove that if n is even, then $n^3 + 2n$ is divisible by 4.

(b) Prove that if a is an integer, then $a^3 - a$ is divisible by 3.

(c) Prove or give a counterexample:

(i) For every positive integer n, $n^2 + 5n + 6$ is even.

(ii) For every positive integer n, $n^2 + 6n + 4$ is even.

Proof. (a) Let n be an even integer. This means $n = 2k$, for some $k \in \mathbb{Z}$. Hence

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

Since $2k^3 + k$ is an integer, this shows that $n^3 + 2n$ is divisible by 4.

(b) Let an integer a be given. By the Division Theorem, when a is divided by 3, it leaves a remainder of $0, 1$ or 2. That is, one of the following cases must be true:

- Case 1: It might be that $a = 3k$, for some $k \in \mathbb{Z}$. In this case,

$$a^3 - a = (3k)^3 - 3k = 3(9k^3 - k).$$

Since $9k^3 - k$ is an integer, $a^3 - a$ is divisible by 3 in this case.

- Case 2: It might be that $a = 3k + 1$, for some $k \in \mathbb{Z}$. In this case,

$$a^3 - a = (3k+1)^3 - (3k+1) = 3(9k^3 + 9k^2 + 2k).$$

Since $9k^3 + 9k^2 + 2k$ is an integer, $a^3 - a$ is divisible by 3 in this case.

- <u>Case 3</u>: It might be that $a = 3k+2$, for some $k \in \mathbb{Z}$. In this case,
$$a^3 - a = (3k+2)^3 - (3k+2) = 3(9k^3 + 18k^2 + 11k + 2).$$
Since $9k^3 + 18k^2 + 11k + 2$ is an integer, $a^3 - a$ is divisible by 3 in this case.

Hence, in every possible case, $a^3 - a$ is divisible by 3.
Therefore the statement "If a is an integer, then $a^3 - a$ is divisible by 3" is true.

(c)

(i) Let a positive integer n be given. Since every positive integer is either even or odd, we have two cases to consider for n:

- <u>Case 1</u>: Suppose n is even. This means $n = 2k$, for some $k \in \mathbb{Z}$, and
$$n^2 + 5n + 6 = (2k)^2 + 5(2k) + 6 = 2(2k^2 + 5k + 3).$$
Since $2k^2 + 5k + 3$ is an integer, we have that $n^2 + 5n + 6$ is even in this case.

- <u>Case 2</u>: Suppose n is odd. This means $n = 2h+1$, for some $h \in \mathbb{Z}$, and
$$n^2 + 5n + 6 = (2h+1)^2 + 5(2h+1) + 6 = 2(2h^2 + 7h + 6).$$
Since $2h^2 + 7h + 6$ is an integer, we have that $n^2 + 5n + 6$ is even in this case.

Thus, in either case we have shown that $n^2 + 5n + 6$ is even. Therefore, for every positive integer n, $n^2 + 5n + 6$ is even.

(ii) Let $n = 1 \in \mathbb{Z}^+$. Then $n^2 + 6n + 4 = 1^2 + 6 \cdot 1 + 4 = 11 = 2 \cdot 5 + 1$. Therefore by definition, $n^2 + 6n + 4$ is not even when $n = 1$, and we have a counterexample to show that the statement "For every positive integer n, $n^2 + 6n + 4$ is even." is false .

■

3.2

Problem Statement: Prove that if a and b are both odd integers, then the polynomial $x^2 + ax + b$ cannot be factored.

Proof. We prove the contrapositive "If the polynomial $x^2 + ax + b$ is factorable, then either a or b is an even integer". Suppose we can factor the quadratic $x^2 + ax + b$ where a and b are integers. This means there exists integers c and d such that

$$\begin{aligned} x^2 + ax + b &= (x+c)(x+d) \\ &= x^2 + cx + dx + c \cdot d \\ &= x^2 + (c+d)x + c \cdot d \end{aligned}$$

Therefore $a = c + d$ and $b = c \cdot d$. Since c and d are integers, each one of them can be either even or odd. Thus we have three cases to consider:

- <u>Case 1</u>: Both c and d are odd.
  Let odd integers c and d be given. This means $c = 2h+1$ and $d = 2k+1$ for some h and $k \in \mathbb{Z}$. Then we have

$$\begin{cases} a = c+d = (2h+1)+(2k+1) = 2(h+k+1) \\ b = c \cdot d = (2h+1)(2k+1) = 2(2hk+h+k)+1 \end{cases}$$

  Since $h+k+1$ and $2hk+h+k$ are integers, this shows that a is even and b is odd in this case.

- <u>Case 2</u>: Both c and d are even.
  Let even integers c and d be given. This means $c = 2m$ and $d = 2n$ for some m and $n \in \mathbb{Z}$. Then we have

$$\begin{cases} a = c+d = 2m+2n = 2(m+n) \\ b = c \cdot d = 2m \cdot 2n = 2(2mn) \end{cases}$$

  Since $m+n$ and $2mn$ are integers, this shows that a and b are both even in this case.

- <u>Case 3</u>: One of c and d is odd and the other is even.
  Without loss of generality, assume c is odd and d is even. This means $c = 2p+1$ and $d = 2q$ for some p and $q \in \mathbb{Z}$. Then we have

$$\begin{cases} a = c+d = (2p+1)+2q = 2(p+q)+1 \\ b = c \cdot d = (2p+1) \cdot 2q = 2(2pq+q) \end{cases}$$

  Since $p+q$ and $2pq+q$ are integers, this shows that a is odd and b is even in this case.

Thus, in all three cases, we have shown that either a or b is even when x^2+ax+b can be factored. So we have proved the contrapositive of our original statement. Therefore the proposition "If a and b are both odd integers, then the polynomial x^2+ax+b cannot be factored" is also true. ■

3.3

Problem Statement: Prove that $2+5+8+\cdots+(3n-1) = \dfrac{n(3n+1)}{2}$ for all $n \geq 1$.

Proof by induction. Let $P(n)$ be the statement $2+5+8+...+(3n-1) = \dfrac{n(3n+1)}{2}$.

Using sigma notation, we can rewrite $P(n)$ as $\sum_{k=1}^{n}(3k-1) = \dfrac{n(3n+1)}{2}$.

We know that $P(1)$ is true since $\sum_{k=1}^{1}(3k-1) = 3(1)-1 = 2 = \dfrac{1(3 \cdot 1+1)}{2}$.

Now suppose that $P(m)$ is true, for some $m \geq 1$. This means $\sum_{k=1}^{m}(3k-1) = \frac{m(3m+1)}{2}$.

Then we have

$$\begin{aligned}
\sum_{k=1}^{m+1}(3k-1) &= \left[\sum_{k=1}^{m}(3k-1)\right] + [3(m+1)-1] \\
&= \frac{m(3m+1)}{2} + (3m+2)) \\
&= \frac{m(3m+1)+2(3m+2)}{2} \\
&= \frac{3m^2+7m+4}{2} \\
&= \frac{(m+1)(3m+4)}{2} \\
&= \frac{(m+1)[(3(m+1)+1]}{2}
\end{aligned}$$

So $P(m+1)$ is true. Thus $P(n)$ is true for all $n \geq 1$ by induction. ■

3.4

Problem Statement A: Given any seven integers, there will be four for which the sum of the squares of those integers is divisible by 4.

Proof. Let seven integers be given. By definition, we know that every integer is either even or odd. Accordingly, we define two boxes labeled "even" and "odd", and then distribute our seven integers into those two boxes. By the Pigeonhole Principle, we know that one of the two boxes must contain at least four integers. Let's refer to these four integers as a, b, c and d. We consider two cases based on which box they are in:

- Case 1: If a, b, c and d are in the box labeled "even", then by definition, we have $a = 2k$, $b = 2l$, $c = 2m$ and $d = 2n$ for some integers k, l, m and n. Hence

$$a^2+b^2+c^2+d^2 = (2k)^2+(2l)^2+(2m)^2+(2n)^2 = 4(k^2+l^2+m^2+n^2).$$

  Since $k^2+l^2+m^2+n^2$ is an integer, this shows that $a^2+b^2+c^2+d^2$ is divisible by 4 in this case.

- Case 2: If a, b, c and d are in the box labeled "odd", then by definition, we have $a = 2p+1$, $b = 2q+1$, $c = 2r+1$ and $d = 2s+1$ for some integers p, q, r and s. Hence

$$\begin{aligned}
a^2+b^2+c^2+d^2 &= (2p+1)^2+(2q+1)^2+(2r+1)^2+(2s+1)^2 \\
&= 4(p^2+q^2+r^2+s^2+p+q+r+s+1)
\end{aligned}$$

Since $p^2+q^2+r^2+s^2+p+q+r+s+1$ is an integer, this shows that $a^2+b^2+c^2+d^2$ is divisible by 4 in this case.

Thus, in either case we have shown that $a^2+b^2+c^2+d^2$ is divisible by 4. Therefore if we are given any seven integers, there will be four for which the sum of the squares of those integers is divisible by 4. ■

3.5

Problem Statement: Prove that 4 does not divide n^2+2 for any integer n.

Proof by contradiction. Suppose there is a counterexample to the statement above. That is, an integer n exists such that 4 divides n^2+2. This means $n^2+2=4k$ for some $k \in \mathbb{Z}$. Since an integer is either even or odd, we have two cases to consider for n:

- Case 1: Suppose n is even. This means $n=2h$, for some $h \in \mathbb{Z}$, and

$$\begin{aligned} & n^2+2 = (2h)^2+2 \\ \Leftrightarrow \quad & 4k = 4h^2+2 \\ \Leftrightarrow \quad & 4(k-h^2) = 2 \\ \Leftrightarrow \quad & k-h^2 = \frac{1}{2} \end{aligned}$$

  Since $k-h^2 \in \mathbb{Z}$ and $\frac{1}{2} \notin \mathbb{Z}$, we have a contradiction. Therefore, no counterexample to the original statement exists in this case.

- Case 2: Suppose n is odd. This means $n=2m+1$, for some $m \in \mathbb{Z}$, and

$$\begin{aligned} & n^2+2 = (2m+1)^2+2 \\ \Leftrightarrow \quad & 4k = 4m^2+4m+3 \\ \Leftrightarrow \quad & 4(k-m^2-m) = 3 \\ \Leftrightarrow \quad & k-m^2-m = \frac{3}{4} \end{aligned}$$

  Since $k-m^2-m \in \mathbb{Z}$ and $\frac{3}{4} \notin \mathbb{Z}$, we have a contradiction. Therefore, no counterexample to the original statement exists in this case.

So in every case, a contradiction arises. Thus, no counterexample exists for the original statement. Therefore the statement "4 does not divide n^2+2 for any integer n" is true. ■

3.6

Problem Statement A: Let n be a positive integer (ie. $n \in \mathbb{N}$). Prove that if $n \equiv 3 \pmod 4$ (ie. $\exists\, q \in \mathbb{Z}$ such that $n = 4q+3$), then n is not the sum of two square integers. That is, there do not exist integers, $a,\ b \in \mathbb{Z}$ such that $n = a^2 + b^2$.

Proof by contradiction. Suppose a counterexample to the statement above exists.
That is, $\exists q \in \mathbb{Z}$ such that $n = 4q+3$ and $n = a^2 + b^2$ for some a and $b \in \mathbb{Z}$. Since a and b are integers, each one of them can be either even or odd. Thus we have three cases to consider:

- Case 1: Both a and b are odd.
  Let odd integers a and b be given. This means $a = 2h+1$ and $b = 2k+1$ for some h and $k \in \mathbb{Z}$. Then we have

$$\begin{aligned} & a^2 + b^2 = n \\ \Leftrightarrow \quad & (2h+1)^2 + (2k+1)^2 = 4q+3 \\ \Leftrightarrow \quad & 4h^2 + 4k^2 + 4h + 4k + 2 = 4q+3 \\ \Leftrightarrow \quad & 4(h^2 + k^2 + h + k - q) = 1 \\ \Leftrightarrow \quad & h^2 + k^2 + h + k - q = \frac{1}{4} \end{aligned}$$

  Since $h^2 + k^2 + h + k - q \in \mathbb{Z}$ and $\frac{1}{4} \notin \mathbb{Z}$, we have a contradiction. Therefore, no counterexample to the original statement exists in this case.

- Case 2: Both a and b are even.
  Let even integers a and b be given. This means $a = 2l$ and $b = 2m+1$ for some l and $m \in \mathbb{Z}$. Then we have

$$\begin{aligned} & a^2 + b^2 = n \\ \Leftrightarrow \quad & (2l)^2 + (2m)^2 = 4q+3 \\ \Leftrightarrow \quad & 4l^2 + 4m^2 = 4q+3 \\ \Leftrightarrow \quad & 4(l^2 + m^2 - q) = 3 \\ \Leftrightarrow \quad & l^2 + m^2 - q = \frac{3}{4} \end{aligned}$$

  Since $l^2 + m^2 - q \in \mathbb{Z}$ and $\frac{3}{4} \notin \mathbb{Z}$, we have a contradiction. Therefore, no counterexample to the original statement exists in this case.

- Case 3: One of a and b is odd and the other is even.
  Without loss of generality, assume a is odd and b is even. This means $a = 2s+1$ and $b = 2t$

for some s and $t \in \mathbb{Z}$. Then we have

$$\begin{aligned} & a^2+b^2=n \\ \Leftrightarrow \quad & (2s+1)^2+(2t)^2=4q+3 \\ \Leftrightarrow \quad & 4s^2+4s+1+4t^2=4q+3 \\ \Leftrightarrow \quad & 4(s^2+t^2+s-q)=2 \\ \Leftrightarrow \quad & s^2+t^2+s-q=\frac{1}{2} \end{aligned}$$

Since $s^2+t^2+s-q \in \mathbb{Z}$ and $\frac{1}{2} \notin \mathbb{Z}$, we have a contradiction. Therefore, no counterexample to the original statement exists in this case.

Thus, in all cases we have shown that there's no counterexample to our proposition.
Therefore our statement "If n mod $4=3$, then n is not the sum of two square integers." is true. ■

3.7

Problem Statement B: Let A and B be sets. Show that $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

Definition. The power set of a set X is the set of all subsets of X and is denoted as:

$$\mathscr{P}(X)=\{Y \mid Y \subseteq X\}$$

Proof. Let sets A and B be given, and suppose $S \in \mathscr{P}(A) \cup \mathscr{P}(B)$.
This means $S \in \mathscr{P}(A)$ or $S \in \mathscr{P}(B)$. By definition, we know that $S \subseteq A$ or $S \subseteq B$.
Thus, $S \subseteq (A \cup B)$, and so $S \in \mathscr{P}(A \cup B)$. Therefore $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$. ■

3.8

Problem Statement: Let $f: A \to B$ and $g: B \to C$ be functions.

(a) Show that if f and g are onto, then $g \circ f: A \to C$ is also onto.

(b) Define the following subsets:

- If $C \subseteq A$, define $f(C)=\{f(x) \mid x \in C\}$. $f(C)$ is a subset of B, called the image of C in B.
- If $D \subseteq B$, define $f^{-1}(D)=\{x \in A \mid f(x) \in D\}$. $f^{-1}(D)$ is a subset of A, called the pre-image of D in A. (Note that f^{-1} may not exist as a function.)

Assume f is onto and that $C = f^{-1}(D)$. Prove that $f(C) = D$.

Proof. (a) Let onto functions $f : A \to B$ and $g : B \to C$ be given, and let $z \in C$.
Since $g : B \to C$ is onto, we know that there is an element $y \in B$ such that $g(y) = z$.
Similarly, since $f : A \to B$ is onto, we know that there is an $x \in A$ such that $f(x) = y$.
Then we have

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

Hence, any chosen element in the codomain C is an output of the function $g \circ f$.
Therefore $g \circ f : A \to C$ is onto.

(b) To prove that $f(C) = D$, we must show that $f(C) \subseteq D$ and $D \subseteq f(C)$.

- Property 1: $f(C) \subseteq D$
  Let $u \in f(C)$. Then by definition of $f(C)$, we know that there exists $v \in C$ such that $u = f(v)$.
  Since $v \in C$ and $C = f^{-1}(D)$, we have that $v \in f^{-1}(D)$.
  Also since $v \in C$ and $C \subseteq A$, this implies that $v \in A$.
  Therefore by definition of $f^{-1}(D)$, we conclude that $f(v) \in D$.
  And since $u = f(v)$, this means that $u \in D$.
  Thus every element of $f(C)$ is also in D, and so $f(C) \subseteq D$.

- Property 2: $D \subseteq f(C)$
  Let $y \in D$. Then by definition of $f^{-1}(D)$, we know that there exists $x \in A$ such that $f(x) = y$.
  Hence $f(x) \in D$. So $x \in f^{-1}(D)$, which also means $x \in C$, since $C = f^{-1}(D)$.
  Therefore by definition of $f(C)$, we conclude that $f(x) \in f(C)$.
  And since $f(x) = y$, this means that $y \in f(C)$.
  Thus every element of D is also in $f(C)$, and so $D \subseteq f(C)$.

So we have shown that $f(C) \subseteq D$ and $D \subseteq f(C)$. Therefore $f(C) = D$. ■