Math 2000 Writing Assignment #2

Sean Fitzpatrick

November 27, 2015

Due Date: Friday, December 4th, by 4:30 pm, in the assignment drop-box across from the Math & CS Department office.

Here is your second writing assignment. The guidelines and grading rubric are the same as for the first assignment, but with a new set of topics. Note that you can ask me for help figuring out any of the mathematics involved: I'm more interested in your ability to understand the material well enough to organize it into a readable paper.

The topics below are all borrowed from (or based upon) projects from the textbook *Reading, Writing, and Proving – A Closer Look at Mathematics*, 2nd ed., by U. Daepp and P. Gorkin, Undergraduate Textbooks in Mathematics, Springer, 2011.

Topic #1: A Set Theoretic Construction of the Natural Numbers

This topic will require you to be comfortable with elements of set theory, including indexed families of sets. This construction is usually attributed to John von Neumann.

Let x be a set. Define the successor of x to be the set $x^+ = x \cup \{x\}$.

1. Determine the successors of $\emptyset$, $\{\emptyset\}$, and $\{a, b, c\}$.

We now introduce the following notation: Let $0 = \emptyset$, $1 = 0^+$, $2 = 1^+$, and so on.

2. Write down 0, 1, 2, 3, and 4 as sets in two different ways: first, using the definitions made above, and then using only the symbol $\emptyset$, set brackets, and appropriate set notation.

It may seem intuitively obvious that if we "do this forever", then we will have defined the natural numbers. However, as simple and attractive as this approach may be, it is not what we call mathematically rigorous. What we need is a statement that explains that we can do this forever. We take this statement as an axiom, an thus it will not be proved.

Axiom (Axiom of infinity). There exists a set containing 0 and the successor of each of its elements.

3. Let I be a nonempty set, and $\{A_k : k \in I\}$ an indexed collection of sets. Suppose that for each $k \in I$, the set A_k has the following two properties: (i) $0 \in A_k$, and (ii) if

$x \in A_k$, then $x^+ \in A_k$. Show that the set $\bigcap_{k \in I} A_k$ also has these two properties. We will call a set with these two properties a successor set.[1]

4. The axiom of infinity guarantees the existence of a successor set. So let A be an arbitrary successor set. Define the set $\boldsymbol{\omega}_A$ to be the intersection of all the subsets of A that are also successor sets. In symbols, we might write

$$\boldsymbol{\omega}_A = \bigcap_{B \in I} B,$$

where $I = \{B : B \subseteq A, \text{ and } B \text{ is a successor set}\}$.
By paert 3, $\boldsymbol{\omega}_A$ is a successor set. Show that $\boldsymbol{\omega}_A = \boldsymbol{\omega}_B$ for all successor sets A and B. Perhaps surprisingly, our definition does not depend on the initial choice of successor set, and therefore we can write $\boldsymbol{\omega}$ rather than $\boldsymbol{\omega}_A$. We call $\boldsymbol{\omega}$ the set of natural numbers. Thus far we know that $\boldsymbol{\omega}$ is a successor set, and it is the only successor set that is contained in every other successor set.

5. Prove the following statement. Suppose $S \subseteq \boldsymbol{\omega}$ satisfies the two properties (i) $0 \in S$ and (ii) if $x \in S$, then $x^+ \in S$. Show that $S = \boldsymbol{\omega}$. (This is the Principal of Mathematical Induction.)

6. Prove that $0 \neq x^+$ for any $x \in \boldsymbol{\omega}$. (Hint: use proof by contradiction, and argue that if this is not true, then $\boldsymbol{\omega}$ cannot be the only successor set that is contained in every other successor set.)

Note: This topic is fairly abstract, and should be challenging for most of you. If you decide to go with this topic, and make it through the problems above, you can see me for a couple of extra credit problems related to defining addition of natural numbers in this set-theoretic framework.

Topic #2: Rational and Irrational Numbers

For this topic, you need to be comforatable with proof by cases, and be familiar with the basic concepts of rational and irrational numbers. You may use without proof the fact that $\sqrt{2}$ is irrational.

We proved in class that the sum and product of any two rational numbers is a rational number: we say that the set of rational numbers is *closed under addition and multiplication.* However, the set of irrational numbers is not so well-behaved.

1. Give an example of two irrational numbers a and b such that $a + b$ is irrational.

2. Give an example of two irrational numbers a and b such that $a + b$ is rational.

[1] This probably sounds a lot like the Principle of Mathematical Induction, and it should. What's different is that we haven't yet constructed $\mathbb{N}$, so we can't assume any of these sets are subsets of $\mathbb{N}$: they may contain more than what we want in the natural numbers.

You must be able to explain why your examples are valid, including proofs, if necessary, that your choices of a and b are irrational, and that $a + b$ is either rational or irrational, as required.

3. Give an example of two rational numbers a and b such that a^b is rational.

4. Give an example of two rational numbers a and b such that a^b is irrational.

We now want to show that it's possible for an irrational number raised to a irrational power to be rational.

Theorem 1. *There exist irrational numbers a and b such that a^b is rational.*

5. Give a *constructive* proof of this theorem. You will need to prove that your numbers a and b are indeed irrational.

   (Hint: try constructing an example involving $\sqrt{2}$ and $\log_2 9$.)

6. Complete a *non-constructive* of this theorem, using appropriate choices for a and b and the two cases below:

   Case 1: $\sqrt{2}^{\sqrt{2}}$ is a rational number.

   Case 2: $\sqrt{2}^{\sqrt{2}}$ is an irrational number.

The interesting (or perhaps, annoying) thing about the second proof above is that you don't need to know (and indeed, *don't* know) whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational!

7. Finally, prove the following theorem:

   Theorem 2. *There exist irrational numbers a and b such that a^b is irrational.*

   (Hint: consider a proof by cases, where $\sqrt{2}^{\sqrt{2}}$ is one of your cases. Hint for the hint: if $\sqrt{2}^{\sqrt{2}}$ is rational, the product of $\sqrt{2}^{\sqrt{2}}$ and any irrational number is irrational.)

Topic 3: Pascal's Triangle

This topic requires you to be comforatble with proof by induction.

Pascal's Triangle was "introduced" in a paper by Blaise Pascal in 1654 (although attributed to Pascal, the triangle had been discovered by others before him) that he wrote to answer a problem about gambling. The triangle is given below. Each row has one more entry than the previous row. All entries along the left and right edges are one. Every other entry in a row is the sum of the two numbers in the row above that lie immediately to the left and to the right. The triangle goes on forever (there is one row for every natural number).

$$\begin{array}{ccccccccccccccc}
&&&&&&&1&&&&&&& \\
&&&&&&1&&1&&&&&& \\
&&&&&1&&2&&1&&&&& \\
&&&&1&&3&&3&&1&&&& \\
&&&1&&4&&6&&4&&1&&& \\
&&1&&5&&10&&10&&5&&1&& \\
&.&&.&&.&&.&&.&&.&&.& \\
.&&.&&.&&.&&.&&.&&.&&.
\end{array}$$

Recall that the *binomial coefficient* $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

We begin by understanding the relationship between the binomial coefficients and Pascal's Triangle:

1. Compute each of the following:

$$\binom{6}{0}, \binom{6}{1}, \binom{6}{2}, \binom{6}{3}, \binom{6}{4}, \binom{6}{5}, \binom{6}{6}.$$

2. Prove that for all $k, n \in \mathbb{N}$ with $1 \leq k \leq n$, we have

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

   (Hint: this is an algebra problem, not an induction problem.)

3. Use the definition of Pascal's Triangle given above to show tha tall entries in Pascal's Triangle are binomial coefficients and find a familiar mathematical expression for the kth entry from the left in the nth row. (The first row corresponds to $n = 0$ and the first entry from the left corresponds to $k = 0$.) Use induction to prove that oyur familiar expression is correct.

4. Prove the *Binomial Theorem*: for each $n \in \mathbb{N}$, and for any real numbers a and b,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

   (Hint: use proof by induction. This is an important result, so there are plenty of sources with the proof. Feel free to look it up, as long as you cite your source.)

5. Consider the statement

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

   (a) Check this formula for a few small values of n.

   (b) Prove the statement using the Binomial Theorem.

   (c) Show how you can obtain this result using Pascal's Triangle.

6. For each $n \in \mathbb{N}$, consider the statement

$$\sum_{k=1}^{n} \binom{k}{k-1} = \binom{n+1}{n-1}.$$

   (a) Do something clever for a few n (as you did in part (a) of the previous problem).

   (b) Prove the statement.

   (c) Show how you can obtain this sum using Pascal's Triangle.

7. Find one more pattern in Pascal's Triangle, and state and prove the formula corresponding to this pattern as you did in the previous two problems. (There are many patterns to choose from.)

Topic 4: RSA Cryptography

For this topic, you will need to read Chapter 8 in our textbook, on elementary Number Theory. In particular, you will need to read (and summarize) the definitions and results related to the following: greatest common divisors, relatively prime integers, Fermat's Little Theorem, Euler's φ-function, and Euler's Theorem. (Not all of these are covered in our textbook, so you'll have to do some additional research.) Provide examples for each definition and theorem.

You will then need to find a source that explains the method behind RSA cryptography, and explain how the results from Number Theory above are relevant. In particular, you should explain (a) how a message is encoded, and (b) how it is decoded. Provide several examples showing how the process works. To keep things manageable, your examples should involve relatively small two-digit prime numbers. (By the time you get to this point, you should understand why prime numbers are relevant.)

If you want further guidance on this topic, you should drop by to discuss it with me.