Portfolio Project

Dor Rondel

Due May 5, 2017

1.1 Demonstrating Growth

Prompt: Show that given any rational integer x, and any positive integer k, there exists an integer y such that $x^k y$ is an integer.

Proof: To prove that an integer y exists to satisfy the requirements of the prompt, we will first rewrite x^k in a different form. Recall that a rational number is one that can be expressed in terms of a fraction. Let x be a rational number represented as $\frac{m}{n}$, where m and n are both integers and $n \neq 0$, and the fraction $\frac{m}{n}$ cannot be further reduced. Raising $\frac{m}{n}$ to the power of a positive integer k, would yield $(\frac{m}{n})^k = \frac{m^k}{n^k}$. Since k is a positive integer, and m is an integer, m^k is equivalent to $(m)(m)...(m)$ k times, which would mean that m^k is still an integer, as the integers are closed under multiplication. The same argument can be used for justifying that n^k is still an integer. Now that we've established that $x^k = \frac{m^k}{n^k}$ and that both m^k and n^k are integers, we can proceed to define y. Let $y = n^k$ making y an integer, $x^k y = \frac{m^k(n^k)}{n^k} = m^k$. Recall that m^k is an integer. This proves that given a rational number, raised to a positive power, multiplied by the denominator raised to the same positive integer - leaves you with the numerator alone, which has already been established to be an integer, effectively deeming the prompt true.

1.2 Demonstrating Growth cont.

Coming into class at the beginning of the semester, the only proof writing experience I had, was that which was covered in my high school geometry class. The proof writing we did at the time was not very rigorous, just stating a series of deductive steps until we reached a conclusion. After completing about a semester's worth of proof writing, I can honestly say that my views on what a proof is, and how to go about writing a proof have changed. As far as what a proof is, the role of proof project made me realize that not all proofs are used simply for justification purposes; rather, that there is far more thought that goes into the reasons for writing proofs, than simply verification alone. Additionally, as far as learning how to write proofs, I believe that I have added more proof techniques to my proof writing arsenal, than that which I had on the first day of class. I can prove propositions in a myriad of ways, some of which will be demonstrated in section 2. I learned about how to phrase mathematical jargon better, and the notation associated with it for writing mathematical proofs. Most importantly however, I am now more capable of judging the validity of proofs, which I think is an integral part of being a good proof writer.

2.1 Demonstrating Breadth - Direct Proof

Prompt: Given any arbitrary positive integer a, b, and c, show that if $a|c$, $b|c$, and $gcd(a, b) = 1$, then $ab|c$.

Proof: Assume that given any arbitrary integers a, b, c such that $a, b, c \in \mathbb{N}$, $a|c$, $b|c$, and $gcd(a, b) = 1$. If the $gcd(a, b) = 1$, then by $Bézout's$ identity, $\exists s, t \in \mathbb{Z}$ such that $as + bt = 1$. Multiplying the equation on both sides by c yields $c(as + bt) = c(1)$. Additionally, by the definition of divisibility, under the assumption that $a|c$ and $b|c$, we can say that $c = aj$ and $c = bk$ for some $j, k \in \mathbb{Z}$. Substituting the different values of c with the equation derived above yields:

$$\begin{aligned} c &= c(as + bt) \\ &= cas + cbt \\ &= bkas + ajbt \\ &= abks + abjt \\ &= ab(ks + jt) \end{aligned}$$

Since $ks+jt$ is an integer, as k, s, j and t are integers, and integers are closed under both multiplication and addition, it is clear that $ab|c$. This shows that if $a|c, b|c$, and the $gcd(a, b) = 1$, then $ab|c$.

2.2 Demonstrating Breadth - Proof by Contradiction

Prompt: Prove that $\sqrt{2}$ is irrational.

Proof: Suppose $\sqrt{2}$ is rational, that means it can be written as a ratio of two integers $p, q \in \mathbb{Z}$, such that $\sqrt{2} = \frac{p}{q}$ where p and q have no common factors and $q \neq 0$. Squaring both sides of the equation yields $2 = \frac{p^2}{q^2}$, which can algebraically manipulated to, $p^2 = 2q^2$. Thus we know that p^2 is even, as it can be expressed in terms of $2k$ for some $k \in \mathbb{Z}$, where in our case $k = q^2$. The square of a number can only be even if the number itself is even, so we know that p must be even, as p^2 is even. Since we know that p is even, we can rewrite is as $2r$ for some $r \in \mathbb{Z}$. Going back to out original equation and substituting $2r$ for p:

$$\begin{aligned} 2 &= \frac{p^2}{q^2} \\ &= \frac{(2r)^2}{q^2} \\ &= \frac{4r^2}{q^2} \end{aligned}$$

This time, multiplying by q^2 on both sides yields:

$$\begin{aligned} 2q^2 &= 4r^2 \\ q^2 &= 2r^2 \end{aligned}$$

Since q^2 can be expressed in terms of $2j$ for some $j \in \mathbb{Z}$ where $j = 2r^2$, we can conculde that q^2 is even. As previously established, if the square of a number is even, then the number itself is also even, so q is even. Since p and q are both even, that means they share a common factor, which contradicts our original assumption that $\sqrt{2} = \frac{p}{q}$ where p and q are both integers which don't share a common factor. Therefore, by contradiction, $\sqrt{2}$ must be irrational.

2.3 Demonstrating Breadth - Proof by Induction

Prompt (from Board Work #6): Prove by induction that $n(n+1)(n+2)$ is a multiple of 3, for all integers $n \geq 1$.

Proof: We will prove that $\forall n \in \mathbb{N}, n(n+1)(n+2)$ is a multiple of 3 by induction. For the base case, let $n = 1$, $1(1+1)(1+2) = 6 = 3(2)$. Since $1(1+1)(1+2) = 3(2)$ where 2 is an integer, the basis is true.

For our inductive hypothesis, assume that for some $k \in \mathbb{N}$, $k(k+1)(k+2) = 3j$ for some $j \in \mathbb{Z}$. We will prove that $k+1$ is also a multiple of 3.

$$\begin{aligned}(k+1)(k+2)(k+3) &= k(k+1)(k+2) + 3(k+1)(k+2) \\ &= 3j + 3(k+1)(k+2) && \text{Substituting Inductive Hypothesis} \\ &= 3[j + (k+1)(k+2)]\end{aligned}$$

Since j and k are integers and the integers are closed under both addition and multiplication, $(k+1)(k+2)(k+3)$ can be expressed in terms of $3q$ for some $q \in \mathbb{Z}$ as shown, making it divisible by 3. Therefore, $\forall n \in \mathbb{N}, n(n+1)(n+2)$ is a multiple of 3, proven by induction.

2.4 Demonstrating Breadth - Explanation

The three preceding proofs are all proven using a different proof methodology. They are mathematically sound, and utilize appropriate notations while adhering to established conventions. The wording is very specific, to not only make mathematical sense, but also syntactic and semantic sense as far as language is concerned. While they are probably not fully understandable to all audiences, the proofs don't make too many assumptions regarding the reader, and as such don't skip many steps while arriving to the conclusion. They display a good degree of proof-writing proficiency by not being overly redundant as well. All the proofs followed the appropriate template corresponding to the methodology used. The direct proof assumed the antecedent and arrived at the conclusion. The proof by contradiction assumed the inverse and showed how it must be false implying the original form is true. And the induction proof has a base case, followed by an inductive hypothesis, capped off by an incremented inductive step.

3 Reflection

As previously mentioned, prior to taking Introduction to Discrete Mathematics, the only mathematical proofs I've written were in geometry class. The proofs in that class were not even formatted as essays, rather were simply a list of logical deductions for arriving from an assumption to a conclusion. After having taken the course, my perception of what a proof looks like changed. A proof can either be a series of steps as we did in that class, it can be paragraph, or even a visual. In essence, a valid proof can take almost any form, as long as it establishes some absoluteness regarding the proposition being scrutinized. Aside from learning the different types of appearances proofs can manifest, I also learned about different motivations for writing proofs, which gave me a different perspective on their roles in computer science and mathematics. Proofs aren't always written to demonstrate conviction, but also to spark conversations and set a foundation for deriving corollaries from theorems. As mentioned in the role of proof project, many times mathematicians are already convinced of the truth of a theorem prior to formally proving it. As far as computer science is concerned, an example of proof writing would be proofs regarding turing machines for example. An application of proof writing in computing, I'd imagine would be a proof deeming an encryption unbreakable for example, and other cryptography related proofs. Another area of computer science I can see proofs used for would be for dealing with data representations such as trees, or even using graph theory proofs for making a claim regarding an artificial neural network, among other tree abstractions.

For a proof to be good, first and foremost it must be valid. That is, that the reasoning used for claiming the conclusion reached must be logically sound. Personally, the scope of my proof writing capabilities is quite limited, as currently, my mathematical knowledge does not go past calculus. As far as reasoning is concerned, I often have the correct approach for proving a proposition, but occasionally have difficulties translating my ideas into words. Aside from having good reasoning to support its claims, a good proof must also be understood by its readers. While that does mean not skipping too many subjectively obvious steps along the way, it also means that the syntax and grammar used must adhere to the given language's guidelines. I have less of a problem with the former, but often have difficulty with the latter. Additionally, another problem I have when writing proofs, is not taking all possible cases of a theorem into account. That takes on two forms: the first discredits the proof as a whole, as it's completely wrong as the solution doesn't work for that case, and the second is not mentioning exceptions I've taken for granted, such as not making a note regarding division by zero, for example. Another area I can develop in as far as proof writing is concerned, is knowing exactly which proof technique to use simply based of reading a prompt. While for some propositions, such as proving an idea is true for all positive integers, induction immediately comes to mind, that is not always the case. I'd like to get to a level, such as with integrals for example, where I know which technique to use to solve the problem simply by looking at it. Although it may seem trivial, I think I need to use certain phrases more responsibly, namely: let, arbitrary, and given. Finally, the last area of proof writing I think I can improve on is decreasing the redundancy in my writing. For example, not saying something like "let positive integers $x, y \in \mathbb{N}$," since by saying that x and y are positive integers, it is already implied that they are members of the set $\mathbb{N}$.