CSE 311: Foundations of Computing I

Parity/Rationals Annotated Proofs

Relevant Definitions

a is even
There exists an $\ell \in \mathbb{Z}$ such that $a = 2\ell$.

a is odd
There exists an $\ell \in \mathbb{Z}$ such that $a = 2\ell + 1$.

Our First Proof

Prove that if $x \in \mathbb{Z}$ is odd, then x^2 is odd.

Proof	Commentary & Scratch Work
Suppose a be an arbitrary odd number.	*Remove the $\forall$. . . . Note that we combined the steps for removing the $\forall$ and the $\rightarrow$ by saying "suppose" and "arbitrary" in the same phrase.*
Then, note that, since a is odd, it follows that $a = 2j + 1$ for some $j \in \mathbb{Z}$.	*The only thing left to do is apply definitions.*
Note that $a^2 = (2j + 1)^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1$ by our characterization of a above, multiplying out the square, and factoring out the 2.	*Our result is in terms of a^2; so, we need to introduce it. We must be careful to actually justify our steps. Saying "by math" is not acceptable.*
Then, since we have found an integer (namely, $2j^2 + 2j$) that satisfies the definition of odd, it follows that a^2 is odd.	*We found the "form" we wanted; so, we "appeal" to the definition to conclude.*

Example Contradition Proof

Prove that no integer is both even and odd.

Proof	Commentary & Scratch Work
Let x be an arbitrary integer.	*For our own consideration, it helps to translate the claim into logical notation: $\forall x\ \neg(\text{Even}(x) \land \text{Odd}(x))$. Then, we clearly see that it's a "forall" claim. So, define our variables. . .*
We go by contradiction.	*We're left with trying to prove the claim "$\neg(\text{Even}(x) \land \text{Odd}(x))$". Our first thought should be "try deMorgan" which gets us "$\neg\text{Even}(x) \lor \neg\text{Odd}(x)$". Notice how this didn't help! We still have a bunch of extra "negations" in our claim. When a claim is phrased "in the negative" like this, and we're trying to prove it, that's often a "clue" that contradiction makes sense.* *So, alert our proof reader that this is what we're doing.*
Suppose, for contradition, that x is even and odd.	*Since we've decided to go by contradition, we assert exactly the opposite of the claim.*

Then, $x = 2k$ for some $k \in \mathbb{Z}$ and $x = 2\ell + 1$ for some $\ell \in \mathbb{Z}$.	*Now, we proceed like normal. We use all of our definitions and attempt to make them contradict each other.* *It is extremely tempting to use the "same" variable for k and ℓ. Don't be fooled!!! These are $\exists$ Elim applications which means they always need to be NEW variables!!!*
Putting these together, we see $2k = 2\ell + 1$. So, $k = \ell + \frac{1}{2}$.	*Put all of our definitions together into as few statements as possible. In this case, the common piece is x.*
Since ℓ is an integer, and $\frac{1}{2}$ is not, it must be the case that $\ell + \frac{1}{2}$ is also not an integer.	*Okay. We can "see" that something is wrong now (intuitively, $\frac{1}{2}$ does not belong here, since we're working with integers).* *The hard part here is explicitly explaining it. Our approach is to show one side of the equation* must *be an integer and the other side* must not be an integer *which is clearly bogus.*
It follows that k is not an integer, which is a contradiction, because we assumed it was one!	*Explain what the actual contradiction is.*
So, no integer is both even and odd!	*Conclude our proof with what we just showed!*

Rationals!

Prove that if $x, y \in \mathbb{Q}$, then $xy \in \mathbb{Q}$.

Proof	Commentary & Scratch Work
Let $x, y \in \mathbb{Q}$ be arbitrary.	*Remove the $\forall$. . . .*
Then, choose $p_x, q_x, p_y, q_y \in \mathbb{Z}$ where $q_x \neq 0$ and $q_y \neq 0$ such that $x = \frac{p_x}{q_x}$ and $y = \frac{p_y}{q_y}$.	*Blindly apply the definitions that we get from our instantiation of the variables.*
Then, $xy = \left(\frac{p_x}{q_x}\right)\left(\frac{p_y}{q_y}\right) = \frac{p_x p_y}{q_x q_y}$, multiplying together the fractions.	*We are interested in a property of xy; so, we should introduce it and start manipulating it.*
Then, since the product of two integers is an integer, $p_x p_y$ is an integer. Also, since the product of two non-zero integers is an integer, $q_x q_y$ is a non-zero integer. It follows that xy is rational, by definition.	*Conclude what we want by using the definition.*