Proofs: divisibility.

Friday, October 2, 2015 11:11 AM

In the previous lecture we saw more examples of conditional propositions, and, as I expected, there were some confusions on why we should say "$P \Rightarrow Q$ is true when P is false."

"What is the difference between $P \wedge Q$ and $P \Rightarrow Q$?"

Of course your friend could see the difference in the truth table. What he meant was how one should think about them.

Maybe the example that we discussed at the end of the previous lecture can clarify the issue a little better:

For any integer n, $n \neq 0 \Rightarrow |n| \geq 1$.

All of you agree that this is a true statement. Now what do you think about this one:

For any integer n, $n \neq 0 \wedge |n| \geq 1$.

You are right! This is a false statement.

When we are proving a conditional proposition, (in a direct proof) we assume the hypothesis holds; and we try to deduce the conclusion. This does NOT mean that we claim the hypothesis always hold.

always hold.

Let's continue the study of divisibility. So far we have seen

. For any non-zero integers a and b, $a \mid b \Rightarrow |a| \le |b|$.

Lemma. For any integers d, n_1, and n_2,

$$d \mid n_1 \wedge d \mid n_2 \Rightarrow d \mid n_1 + n_2.$$

Pf. $d \mid n_1 \Rightarrow$ for some integer k_1, $n_1 = d k_1$

$d \mid n_2 \Rightarrow$ for some integer k_2, $n_2 = d k_2$

$\Rightarrow n_1 + n_2 = d(k_1 + k_2)$

Since $k_1 + k_2$ is an integer, $n_1 + n_2$ is a multiple of d.

So $d \mid n_1 + n_2$. ∎

Biconditional propositions: $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

. P if and only if Q

. P is necessary and sufficient for Q

. $P \Leftrightarrow Q$ is true exactly when P and Q are equivalent.

Lemma. For any integer n, n is odd if and only if for some integer k

$$n = 2k + 1.$$

Pf. We have to prove two implications.

($\Rightarrow$) If n is odd, then $n = 2k+1$ for some integer.

Pf. (a little bit of cheating. Can you find where?)

Suppose k is the largest integer so that $2k \le n$. ⊛

Step 1. $n-2k$ is an integer.

Pf of step 1. Since n and k are integers, $n-2k$ is an integer.

Step 2. $n-2k \neq 0$.

Pf of step 2. Suppose to the contrary that $n-2k=0$. Then $n=2k$, which implies $2 \mid n$. So n is even, which contradicts the assumption that n is odd.

Step 3. $n-2k<2$.

Pf of step 3. Suppose to the contrary that $n-2k \ge 2$. Then $n \ge 2k+2 = 2(k+1)$. This contradicts ⊛ where we assumed k is the largest integer so that $n \ge 2k$.

So $n-2k$ is an integer (by step 1), it is at least 0 ⊛, it is NOT 0 (by step 2), it is less than 2 (by step 3). Altogether $n-2k=1$, which implies $n=2k+1$. ∎

($\Leftarrow$) $n=2k+1 \Rightarrow n$ is odd.

Pf. Suppose to the contrary that n is even. So for some integer k' we have $n = 2k'$. Hence

$$2k' = 2k+1.$$

Therefore $1 = 2(k'-k)$, which implies $2 \mid 1$.

And so $|2| \leq |1|$ (we have proved this earlier.) which is a contradiction. ∎