9-15-2018

Conditional Proof

A **conditional proof** is a proof of an "if-then" (conditional) statement.

Since any proof makes *some* assumptions, you might say that every proof is a conditional proof. But there are different kinds of assumptions you might make. Consider the following conditional statements:

"If $x \in \mathbb{R}$, then $x^2 + 49 \geq 14x$."

"If $x \in \mathbb{R}$ and $x > 3$, then $x^2 + 5x + 2 > 25$."

There's an obvious sense in which the "if" part of the second statement has more content that the "if" part of the first statement. In the first statement, the "if" part doesn't give you much to go on. In the second statement, you would suspect that the number 7 is somehow related to the "then" part.

In this section, I'll look at proofs of conditional statements where the "if" part carries that kind of significant information.

Example. Prove that if $x \in \mathbb{R}$ and $x > 3$, then $x^2 + 5x + 2 > 25$.

To prove the statement, you *assume* that $x > 3$. Now

$$x > 3, \quad \text{so} \quad x^2 > 9.$$

Likewise,

$$x > 3, \quad \text{so} \quad 5x > 15.$$

If I add $x^2 > 9$ and $5x > 15$, I get $x^2 + 5x > 24$. I compare this inequality to the target inequality, and I see that I'm missing a "2" on the left and a "1" on the right. Well, $2 > 1$, so adding *this* inequality to $x^2 + 5x > 24$, I obtain

$$x^2 + 5x + 2 > 25.$$

Notice the *conditional* nature of the conclusion. It's certainly not true that $x^2 + 5x + 2 > 25$ *for any* real number x. (For example, it's false if $x = 0$.) The conclusion is true *if* the assumption $x > 3$ is true. □

The last example shows how you write a conditional proof. In this situation, you're trying to prove a statement of the form $P \to Q$, where P is the set of assumptions — it may be one statement, or several statements — and Q is the conclusion. You *assume* P and try to derive Q. If you succeed, then $P \to Q$ is true.

Example. (a) Prove that if x is a real number and $x > 2$, then $x^3 - 3x^2 + 2x > 0$.

(b) Give a specific example to show that the converse is false.

(a) Suppose $x > 2$. Then

$$x - 2 > 0, \quad x - 1 > 2 - 1 = 1 > 0, \quad x > 2 > 0.$$

Thus, $x - 2$, $x - 1$, and x are all positive. The product of positive numbers is positive, so

$$x^3 - 3x^2 - 2x = x(x - 1)(x - 2) > 0. \quad \square$$

(b) Take $x = 0.5$. Then

$$(0.5)^3 - 3(0.5)^2 + 2(0.5) = 0.375 > 0.$$

However, $0.5 \not> 2$. □

Example. Premises: $\begin{cases} A \wedge \sim D \\ B \to (C \to D) \end{cases}$

Prove: $(A \to B) \to \sim C$.

To prove the conditional statement $(A \to B) \to \sim C$, I *assume* the "if" part $A \to B$ and try to prove the "then" part $\sim C$.

1.	$A \wedge \sim D$	Premise
2.	$B \to (C \to D)$	Premise
3.	$A \to B$	Premise for conditional proof
4.	A	Decomposing a conjunction (1)
5.	B	Modus ponens (1,3)
6.	$C \to D$	Modus ponens (2,5)
7.	$\sim D$	Decomposing a conjunction (1)
8.	$\sim C$	Modus tollens (6,7)
9.	$(A \to B) \to \sim C$	Conditional proof (3,8)

The *conclusion* $\sim C$ was deduced on line 8. Together with the *assumption* $A \to B$ in line 3, this proves the conditional $(A \to B) \to \sim C$. □

Example. Prove that if n is odd, then n^2 leaves a remainder of 1 when it is divided by 4.

I *assume* that n is an odd number. I want to prove that n^2 leaves a remainder of 1 when it is divided by 4.

An *odd number* is an integer which can be written in the form $2m + 1$ for some integer m. Since n is odd, $n = 2m + 1$ for some m.

Squaring n, I get

$$n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1.$$

Since $4(m^2 + m)$ is divisible by 4, n^2 leaves a remainder of 1 when it is divided by 4.

This proves the conditional statement that if n is odd, then n^2 leaves a remainder of 1 when it is divided by 4. □

Example. (**Proving the contrapositive**) Let n be an integer. Prove that if $3n^2 + 5n + 18$ is not even, then n is not even.

Recall that the conditional $P \to Q$ is logically equivalent to its contrapositive $\sim Q \to \sim P$. In some cases, you use this to prove a conditional statement by replacing it with its contrapositive.

In this example, the given conditional statement is kind of awkward: Both the "if" and "then" parts are negative statements. And if I try to prove this conditional statement by assuming the "if" part — that is, assuming that $3n^2 + 5n + 18$ is not even — it isn't obvious how to proceed.

Instead, I replace the statement with its contrapositive: "If n is even, then $3n^2 + 5n + 18$ is even."

Begin by assuming the "if" part: Suppose n is even. By definition, this means that $n = 2m$, where m is an integer. Then

$$\begin{aligned} 3n^2 + 5n + 18 &= 3(2m)^2 + 5(2m) + 18 \\ &= 12m^2 + 10m + 18 \\ &= 2(6m^2 + 5m + 9) \end{aligned}$$

Now $6m^2+5m+9$ is an integer, so $2(6m^2+5m+9)$ is even (by definition of "even"). Hence, $3n^2+5n+18$ is even.

Since I've proved the contrapositive, this proves the original statement. □

If a and b are integers, a **divides** b means that there is an integer c such that $ac = b$. a divides b is written $a \mid b$ for short.

For example, $6 \mid 18$ because $6 \cdot 3 = 18$, $10 \mid 0$ because $10 \cdot 0 = 0$, and $-6 \mid 6$ since $(-6) \cdot (-1) = 6$.

On the other hand, 3 does not divide 5, since there is no integer c such that $3 \cdot c = 5$. "3 does not divide 5" is written $3 \nmid 5$.

Example. Suppose a, b, and c are integers. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Suppose that $a \mid b$ and $b \mid c$.Since $a \mid b$, there is an integer m such that $am = b$. Since $b \mid c$, there is an integer n such that $bn = c$.

Substitute $am = b$ into $bn = c$ to obtain $(am)n = c$, or $a(mn) = c$. Since mn is an integer, it follows from the definition of divisibility that $a \mid c$. □

Note that when I introduced m and n, I was careful to use different letters than the a, b, and c that were already in use. Note also that after stating my assumptions, I translated those assumptions using the definition of divisibility. I asked myself: "What does it *mean* for a to divide b? What does it *mean* for b to divide c?"

When a proof involves a concept (like *divisibility* in this proof), you *must* have a clear idea of what it means. You should be able to write down a clear, correct definition before proceeding; if you can't remember the definition, look it up in your book or notes and write it down. *Just having a vague idea of what something means is not enough when you're writing proofs.*

Example. Prove: "If $0 = 1$, then $\pi = 100$."

Notice that both the "if" and "then" parts are false!

Assume that $0 = 1$. Multiply both sides by $\pi - 100$, then do some algebra:

$$\begin{aligned} 0 \cdot (\pi - 100) &= 1 \cdot (\pi - 100) \\ 0 &= \pi - 100 \\ \pi &= 100 \end{aligned}$$

Hence, if $0 = 1$, then $\pi = 100$. □

Note that I can do the following as well: Start with $0 = 1$. Differentiate both sides to obtain $0 = 0$. $0 = 0$ is true, even though $0 = 1$ is false.

People sometimes erroneously suppose that they can prove something by starting with what they want to prove, and working until they get a true statement — which they suppose provides "confirmation" that the original statement is true. This example shows that the procedure is invalid, since a true conclusion may come from a false assumption.

Assuming what you want to prove is the most fundamental logical fallacy. It's called *begging the question*. In a formal debate, the *question* was the issue or statement being debated. Thus, *begging the question* referred to arguing for the truth of the statement by assuming that it was true. It's also called *circular reasoning*. Another way to see that this procedure is nonsensical is to observe that if you're trying to prove that P is true and you assume that P is true, then you're done: There's no need for an argument at all! □

Example. An integer is **divisible by** 3 if it can be written in the form $3m$ for some integer m.

Prove that if n is divisible by 3, then $2n^2 + 5n + 12$ is divisible by 3.

Suppose n is divisible by 3. Then $n = 3m$ for some integer m. So

$$2n^2 + 5n + 12 = 2(3m)^2 + 5(3m) + 12 = 18m^2 + 15m + 12 = 3(6m^2 + 5m + 12).$$

The last expression is 3 times an integer. Hence, $2n^2 + 5n + 12$ is divisible by 3. □

Note that I didn't stop with "$18m^2 + 15m + 12$" and say "the sum of integers divisible by 3 must be divisible by 3". That's true, but I haven't proved it. Can you do it?
