CSCI 2824 - CU Boulder, 2019 Summer

Lecture 7: Proof by cases, contradiction, and contrapositive

12 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications and Andrew Altomare's notes.

1 Review

We talked about rational numbers and divisibility.

2 Proof by Cases

Another very natural direct way of proving something is to consider general cases to think about. We kind of saw this with the proof that "any integer $n > 1$ is divisible by a prime number" since we considered each number to be prime or not.

You know that if 3 is odd then 3+1=4 is even and so forth. This is called alternating parity.

Theorem 2.1. *Any two consecutive integers have opposite parity.*

Proof. Suppose that two consecutive integers are given m and $m + 1$. By the parity property, m is either even or odd.

Case 1: m **is even**. In this case $m = 2k$ for some integer k so $m + 1 = 2k + 1$ which is odd by definition. They have opposite parity.

Case 2: m **is odd**. In this case $m = 2k + 1$ for some integer k and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer and $m + 1$ is even. They have opposite parity.

It follows that regardless of which case, for a particular m and $m + 1$ then m and $m + 1$ have opposite parity. $\square$

In general, we call this the Method of Proof by Division into Cases.

Definition: *Method of Proof by Division into Cases*
To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C prove all the following:

$$\text{If } A_1, \text{ then } C$$
$$\text{If } A_2, \text{ then } C$$
$$\dots$$
$$\text{If } A_n, \text{ then } C.$$

This process shows that C is true regardless of which $A_1, A_2, \ldots A_n$ happens to be the case.

Theorem 2.2. *The square of any odd integer has the form $8m + 1$ for some integer m.*

Proof. Suppose n is an odd integer. By the quotient-remainder theorem, n can be written in one of the forms: $4q$ or $4q + 1$ or $4q + 2$ or $4q + 3$ for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of two forms: $4q + 1$ and $4q + 3$.

Case 1, $n = 4q + 1$. Since $n = 4q + 1$

$$\begin{aligned} n^2 &= (4q+1)^2 \\ &= (4q+1)(4q+1) \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 \end{aligned}$$

Let $m = 2q^2 + q$. Then, m is an integer since 2 and q are integers and sums and products of integers are integers. Thus substitution yields $n^2 = 8m + 1$.

Case 2, $n = 4q + 3$

$$\begin{aligned} n^2 &= (4q+3)^2 \\ &= (4q+3)(4q+3) \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8 + 1) \\ &= 8(2q^2 + 3q + 1) + 1 \end{aligned}$$

Let $m = 2q^2 + 3q + 1$. Then, m is an integer since $1, 2, 3$, and q are integers and sums and products of integers are integers. Thus, by substitution $n^2 = 8m + 1$.

Cases 1 and 2 show that for any odd integer, $n^2 = 8m + 1$ for some integer m. □

3 Proof by Contradiction

There are indirect forms of proof too. Suppose you were accused of robbing a bank. You might prove that you didn't by saying, "Suppose I did commit the crime. Then at the time of the crime, I would have had to be at the scene of the crime. In fact, at the time of the crime I was in a meeting with 20 people far from the crime scene, as they will testify. This contradicts the assumption that I committed the crime since it is impossible to be in two places at one time. Hence that assumption is false." Assuming your claims can be verified, any reasonable jury will accept this alibi. This is proof by contradiction since you supposed that the statement was not true and showed the result was absurd.

Definition: *Method of proof by contradiction*

1. Suppose the statement to be proved is false.

2. Show that this supposition leads logically to a contradiction.

3. Conclude that the statement to be proved must actually be true.

We can use this idea to prove that there is no biggest integer.

Theorem 3.1. *There is no greatest integer.*

Proof. Suppose that N is the greatest integer. Then, $N \geq n$ for every integer n. Let $M = N + 1$. Now M is an integer because it is a sum of integers. Also, $M > N$. Thus, M is an integer greater than N, a contradiction. Therefore, there is no greatest integer. □

Exercise
Prove: There is not integer that is both even and odd.

Exercise
The sum of any rational number and any irrational number is irrational.

4 Proof by Contrapositive

A more complicated form of proof relies on the idea of contraposition. Remember that a conditional statement is logically equivalent to its contrapositive. We exploit that here:

Definition: *Method of proof by contraposition*

1. Express the statement to be proved in the from $\forall x \in D, P(x) \rightarrow Q(x)$.

2. Rewrite this in the contrapositive form $\forall x \in D, \not Q(x) \rightarrow \not P(x)$

3. Prove the contrapositive by direct proof, i.e. suppose $x \in D$ such that $Q(x)$ is false and show that $P(x)$ is false.

It may seem weird and silly to prove things like this. But, there are times that it is easier.

Theorem 4.1. *For all integers n, if n^2 is even then n is even.*

Proof. **[By contraposition]**. Suppose n is any odd integer. By definition of odd $n = 2k + 1$ for some integer k. Then,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

. But $2k^2 + 2k$ is an integer because products and sums of integers are integers. So $n^2 = 2q + 1$ where $q = 2k^2 + 2k$ and thus by definition is odd. □

We could have also proved this with contradiction.

Proof. **[By contradiction]** Suppose not, i.e. suppose there is an integer n such that n^2 is even but n is not event. By the quotient remainder theorem with $d = 2$, any integer is even or odd. Hence, since n is not even it is odd and thus $n = 2k + 1$ for some integer k. By algebra:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

But $2k^2 + 2k$ is an integer because products and sums of integers are integers. So, $n^2 = 2q + 1$ where $q = 2k^2 + 2k$ and thus by definition, it is odd. Therefore, n^2 is both odd and event. This contradicts our previous theorem that no integer can be both even and odd. $\square$