Proof by Cases

You can sometimes prove a statement by:

1. Dividing the situation into cases which exhaust all the possibilities; and
2. Showing that the statement follows in all cases.

It’s important to cover all the possibilities. And don’t confuse this with trying examples; an example is not a proof.

Note that there are usually many ways to divide a situation into cases. For example, if I know that \(x\) is a real number and I’m proving something about \(x\), here are some ways I could take cases:

(a) \(x > 0\), \(x = 0\), or \(x < 0\).

(b) \(|x| > 1\) or \(|x| \leq 1\).

(c) \(x \geq \pi\) or \(x < \pi\)

(d) \(x\) is rational or \(x\) is irrational.

There are an infinite number of ways to divide up the real numbers to take cases; how you do it depends on what you’re trying to prove. In general, you should try to use a small number of cases — and in particular, you should see if you can give a proof without taking cases at all!

I’ll begin with a logic proof. In this situation, your cases are usually \(P\) and \(\neg P\), where \(P\) is a statement.

Example. Premises:

\[
\begin{align*}
A &\rightarrow (B \land \neg D) \\
C &\rightarrow A \\
C &\lor \neg D
\end{align*}
\]

Prove: \(\neg D\).

I can divide the situation into two cases: Either \(C\) is true, or \(\neg C\) is true. These exhaust the possibilities, by the Law of the Excluded Middle. I’ll assume each in turn and show that I can derive \(\neg D\).

1. \(A \rightarrow (B \land \neg D)\) Premise
2. \(C \rightarrow A\) Premise
3. \(C \lor \neg D\) Premise
4. \(C\) Premise - Case 1
5. \(A\) Modus ponens (2,4)
6. \(B \land \neg D\) Modus ponens (1,5)
7. \(\neg D\) Decomposing a conjunction (6)
8. \(\neg C\) Premise - Case 2
9. \(\neg D\) Disjunctive syllogism (3,8)
10. \(\neg D\) Proof by cases (4,7,8,9)

Since both of my cases led to the conclusion \(\neg D\), and since my cases exhausted the possibilities, I’ve proved \(\neg D\).

In logic proofs, cases of the form \(P\) and \(\neg P\) where \(P\) is some statement will cover all possibilities, since one of \(P\) or \(\neg P\) must be true. So these are the natural cases to take in logic proofs.

How did I know to use \(C\) and \(\neg C\) rather than (say) \(B\) and \(\neg B\)? I looked at my premises and noticed that I could do something with each of those assumptions: \(C\) could be used for modus ponens, and \(\neg C\) could
Example. In calculus, you learned Rolle’s theorem. Here’s the statement:

Let $f$ be a function which is continuous on the interval $a \leq x \leq b$ and is differentiable on the interval $a < x < b$. Suppose $f(a) = f(b) = 0$. Then there is a real number $c$ such that $a < c < b$ and $f'(c) = 0$.

In other words (to put it roughly), between two roots there must be a horizontal tangent.

Suppose first that $f$ is never positive or negative on the interval $a \leq x \leq b$, $f$ is positive somewhere on the interval $a \leq x \leq b$, or $f$ is negative somewhere on the interval $a \leq x \leq b$.

Suppose first that $f$ is never positive or negative on the interval $a \leq x \leq b$. Then $f = 0$, a constant function, and $f'(x) = 0$ for all $x$ in the interval $a < x < b$.

Suppose that $f$ is positive at some point of the interval $a \leq x \leq b$. A continuous function on a closed interval attains a maximum value on the interval; since I already know $f$ is positive somewhere, the maximum value of $f$ must be positive. Since $f$ is 0 at the endpoints, it must attain the maximum value at some point $c$ in the open interval $a < x < b$.

Since $a < c < b$, $f$ is differentiable at $c$. But at a point where a differentiable function attains a maximum, the derivative is 0. Therefore, $f'(c) = 0$.

Suppose that $f$ is negative at some point of the interval $a \leq x \leq b$. A continuous function on a closed interval attains a minimum value on the interval; since I already know $f$ is negative somewhere, the minimum value of $f$ must be negative. Since $f$ is 0 at the endpoints, it must attain the minimum value at some point $c$.
c in the open interval $a < x < b$.

Since $a < c < b$, $f$ is differentiable at $c$. But at a point where a differentiable function attains a minimum, the derivative is 0. Therefore, $f'(c) = 0$.

Since the three cases exhaust all the possibilities, this proves that $f'(c) = 0$ for some $c$ in the interval $a < x < b$. 

Many problems involving divisibility of integers use the Division Algorithm. It is a consequence of the Well-Ordering Axiom for the positive integers, which is also the basis for mathematical induction.

**Theorem. (Division Algorithm)** Let $m$ and $n$ be integers, where $n > 0$. Then there are unique integers $q$ and $r$ such that

$$m = nq + r,$$

where $0 \leq r < n$.

(“$q$” stands for “quotient” and “$r$” stands for “remainder”.)

I won’t give a proof of this, but here are some examples which show how it’s used.

**Example.** Apply the Division Algorithm to:

(a) Divide 31 by 8.

(b) Divide $-31$ by 8.

(c) Divide an integer $m$ by 2.

(a) Let $m = 31$ and $n = 8$. Then I have

$$31 = 8 \cdot 3 + 7.$$

In this case, $q = 3$ and $r = 7$. Note that $0 \leq 7 < 8$ holds — when you divide, the remainder should be nonnegative, and less than the number you divided by. 

(b) (a) Let $m = -31$ and $n = 8$. Then I have

$$-31 = 8 \cdot (-4) + 1.$$

In this case, $q = -4$ and $r = 1$. Again, $0 \leq 1 < 8$ holds. Note that if I wrote “$-31 = 8 \cdot (-3) + (-7)$”, the equation is true, but the numbers aren’t the ones produced by the Division Algorithm — $r$ is not allowed to be negative. 

(c) Take $m$ to be an integer, and let $n = 2$. Then

$$m = 2q + r,$$

where $0 \leq r < 2$.

Now since $r$ is an integer and $0 \leq r < 2$, I must have $r = 0$ or $r = 1$. Thus, if $m \in \mathbb{Z}$, then

$$m = 2q \text{ or } m = 2q + 1.$$
Of course, the first case occurs when \( m \) is even, and the second case occurs when \( m \) is odd. *If a problem involves odd or even integers, you might consider taking cases in this way.*

A similar situation occurs when \( n \) is any positive integer. For example, if \( m \in \mathbb{Z} \) and \( n = 5 \), then

\[
m = 5q + r, \quad \text{where} \quad 0 \leq r < 5.
\]

The condition \( 0 \leq r < 5 \) means \( r = 0, r = 1, r = 2, r = 3, \) or \( r = 4 \). So if \( m \in \mathbb{Z} \), the possibilities are

\[
m = 5q, \quad m = 5q + 1, \quad m = 5q + 2, \quad m = 5q + 3, \quad \text{or} \quad m = 5q + 4.
\]

*If a problem involves divisibility by 5 you might consider taking cases in this way.*

(When I discuss modular arithmetic, there will be an easier way to deal with these cases.)

---

**Example.** Prove that if \( n \) is an integer, then \( 3n^2 + n + 14 \) is even.

Let \( n \in \mathbb{Z} \). I’ll consider two cases: \( n \) is even and \( n \) is odd.

**Case 1.** \( n \) is even.

Since \( n \) is even, I can write \( n = 2k \), where \( k \in \mathbb{Z} \). Then

\[
3n^2 + n + 14 = 3(2k)^2 + 2k + 14
\]

\[
= 12k^2 + 2k + 14
\]

\[
= 2(6k^2 + k + 7)
\]

Since \( 6k^2 + k + 7 \) is an integer, \( 3n^2 + n + 14 \) is even if \( n \) is even.

**Case 2.** \( n \) is odd.

Since \( n \) is odd, I can write \( n = 2k + 1 \), where \( k \in \mathbb{Z} \). Then

\[
3n^2 + n + 14 = 3(2k + 1)^2 + (2k + 1) + 14
\]

\[
= 3(4k^2 + 4k + 1) + (2k + 1) + 14
\]

\[
= 12k^2 + 12k + 3 + 2k + 1 + 14
\]

\[
= 12k^2 + 14k + 18
\]

\[
= 2(6k^2 + 7k + 9)
\]

Since \( 6k^2 + 7k + 9 \) is an integer, \( 3n^2 + n + 14 \) is even if \( n \) is odd.

Since in both cases \( 3n^2 + n + 14 \) is even, it follows that if \( n \) is an integer, then \( 3n^2 + n + 14 \) is even.

---

**Example.** Prove that if \( n \) is an integer, then \( 2n^2 + n + 1 \) is not divisible by 3.

When \( n \) is divided by 3, the possible remainders are 0, 1, or 2. I consider these three cases.

**Case 1.** When \( n \) is divided by 3, the remainder is 0.

Then \( n = 3q + 0 = 3q \) for some integer \( q \). So

\[
2n^2 + n + 1 = 2(3q)^2 + (3q) + 1
\]

\[
= 18q^2 + 3q + 1
\]

\[
= 3(6q^2 + q) + 1
\]
The last expression shows that in this case when \(2n^2 + n + 1\) is divided by 3, the remainder is 1. Hence, \(2n^2 + n + 1\) is not divisible by 3.

**Case 2.** When \(n\) is divided by 3, the remainder is 1.

Then \(n = 3q + 1\) for some integer \(q\). So

\[
2n^2 + n + 1 = 2(3q + 1)^2 + (3q + 1) + 1 = 18q^2 + 15q + 4 = 3(6q^2 + 5q + 1) + 1
\]

The last expression shows that in this case when \(2n^2 + n + 1\) is divided by 3, the remainder is 1. Hence, \(2n^2 + n + 1\) is not divisible by 3.

**Case 3.** When \(n\) is divided by 3, the remainder is 2.

Then \(n = 3q + 2\) for some integer \(q\). So

\[
2n^2 + n + 1 = 2(3q + 2)^2 + (3q + 2) + 1 = 18q^2 + 27q + 11 = 3(6q^2 + 9q + 3) + 2
\]

The last expression shows that in this case when \(2n^2 + n + 1\) is divided by 3, the remainder is 2. Hence, \(2n^2 + n + 1\) is not divisible by 3.

Since in every case \(2n^2 + n + 1\) is not divisible by 3, it follows that \(2n^2 + n + 1\) is not divisible by 3 for any integer \(n\).

---

**Example.** Prove that for all \(x \in \mathbb{R}\),

\[-5 \leq |x + 2| - |x - 3| \leq 5.
\]

You often think of taking cases in dealing with absolute values. I have

\[|x + 2| = \begin{cases} 
  x + 2 & \text{if } x + 2 > 0 \\
  -(x + 2) & \text{if } x + 2 \leq 0
\end{cases}
\]

Now \(x + 2 > 0\) means \(x > -2\), and \(x + 2 \leq 0\) means \(x \leq -2\). So

\[|x + 2| = \begin{cases} 
  x + 2 & \text{if } x > -2 \\
  -(x + 2) & \text{if } x \leq -2
\end{cases}
\]

In the same way,

\[|x - 3| = \begin{cases} 
  x - 3 & \text{if } x > 3 \\
  -(x - 3) & \text{if } x \leq 3
\end{cases}
\]

Given the way the functions are broken apart, I’ll consider the cases \(x \leq -2\), \(-2 < x \leq 3\), and \(x > 3\). Notice that all real numbers are in one of the three cases.

**Case 1.** \(x \leq -2\). In this case,

\[|x + 2| - |x - 3| = -(x + 2) - [-(x - 3)] = -5.
\]

Therefore, \(-5 \leq |x + 2| - |x - 3| \leq 5\) holds in this case.
Case 2. $-2 < x \leq 3$. In this case,

$$|x + 2| - |x - 3| = (x + 2) - (-(x - 3)) = 2x - 1.$$  

I have to do some additional work to see whether the target inequality holds. I have

$$\begin{align*}
-2 &< x \leq 3 \\
-4 &< 2x \leq 6 \\
-5 &< 2x - 1 \leq 5
\end{align*}$$

Therefore, $-5 \leq |x + 2| - |x - 3| \leq 5$ holds in this case.

Case 3. $x > 3$. In this case,

$$|x + 2| - |x - 3| = (x + 2) - (x - 3) = 5.$$  

Therefore, $-5 \leq |x + 2| - |x - 3| \leq 5$ holds in this case.

Since $-5 \leq |x + 2| - |x - 3| \leq 5$ holds all three cases, it is true for all $x \in \mathbb{R}$.  

©2020 by Bruce Ikenaga