Section 3.6: Indirect Argument: Contradiction and Contraposition

So far, we have only considered so called "direct proofs" of mathematical statements. Specifically, we have been given a statement to prove, and then we have used the definitions and previous results to logically derive the statement. In this section we consider "indirect proofs" - proofs which do not focus on proving the statement we want to prove, but rather closely related statements whose truth is related to the truth of the statement we want to prove. In mathematics, such proofs are very common place (indeed, we shall see two classic examples in the next section). However, as we discussed previously, some people take issue with the validity of such an approach since it invokes the law of the excluded middle.

1. Proof by Contradiction

The first indirect proof we shall consider is proof by contradiction. Suppose you are given a statement that you want to prove. The general steps to take when trying to prove this statement by contradiction is the following:

- (i) Suppose that the statement is false i.e. assume the negation of the statement is true
- (ii) Show that this leads logically to a contradiction using standard logical reasoning
- (iii) Conclude that the statement to be proved is true (since its negations leads to a contradiction)

We illustrate proof by contradiction through a number of examples. We shall present a couple of examples taken from the book as well as some examples from the homework problems. To emphasis the notation we specified in Section 3.1, we shall write each of the statement as theorems and follow the general directions for proving theorems.

Theorem 1.1. *There is no greatest integer*

Proof. Suppose the negation of the theorem i.e. suppose there is a greatest integers. Then there exists an integer N such that for all integers n, $n \leqslant N$. Consider the number $N+1$. Since N is an integer and 1 is an integer, the sum $N+1$ is an integer. However, $N+1 > N$. Therefore, N is not the greatest integer. Therefore, we have supposed that N is the greatest integer and derived that N is not the greatest integer which is clearly a contradiction (i.e. we have shown $P \wedge \sim P$). Therefore, this shows that the assumption that there is a greatest integer is false, and hence there is no greatest integer.

$\square$

Theorem 1.2. *For any integer n, $n^2 - 2$ is not divisible by* 4

Proof. Suppose the negation of the theorem i.e. $\exists n \in \mathbb{Z}, 4$ divides $n^2 - 1$. Let n be an integer such that 4 divides $n^2 - 2$. Then there exists an integer k such that $n^2 - 2 = 4k$ (by definition of 4 dividing $n^2 - 2$). It follows that

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

so n^2 is even and hence n is even (since if n were odd, n^2 would have to be odd). Therefore, there exists a number l such that $n = 2l$. Then

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

and so

$$2l^2 = 2k+1$$

using the simple rules of arithmetic. However, $2l^2$ is even and $2k+1$ is odd (by definition) and hence we have exhibited a number which is both even and odd. This is not possible (by a result in the book) and hence we have a contradiction. Thus the initial assumption is not true and thus for any integer n, $n^2 - 2$ is not divisible by 4. $\square$

The next example is a little more difficult since we shall use contradiction a number of different times.

Theorem 1.3. *For all prime numbers a, b and c, $a^2 + b^2 \neq c^2$.*

Proof. Suppose the negation of the theorem. Specifically, let P denote the set of prime integers. Then the negation would be

$$\exists a, b, c \in P, a^2 + b^2 = c^2.$$

We shall prove this by considering the different parities of a, b and c.
(New contradiction proof) First assume that a and b are both odd. Then a^2 and b^2 will each be odd and therefore $a^2 + b^2$ will be even, so c^2 will be even. Since c^2 is even, c must be even, and therefore, $c = 2$ and $c^2 = 4$. Since a and b are odd, we know $a, b \geqslant 3$ and so $a^3 + b^2 \geqslant 9$. In particular, we could not have $a^2 + b^2 = 4$, and thus our assumption that both a and b are odd must be false. Therefore, at least one of a or b is even.
(New contradiction proof) Assume a and b are both even. Then since a and b are prime, we have $a = b = 2$ and this $a^2 + b^2 = 4 + 4 = 8 = c^2$. Since 8 is even and $c^2 = 8$, it follows that c is even, and thus $c = 2$. However, these choices of a, b and c do not satisfy $a^2 + b^2 = c^2$, and thus we have a contradiction. Therefore our assumption that a and b were both even was false. Therefore, we must have one even and one odd.
(New contradiction proof) Suppose that a is even and b is odd and that $a^2 + b^2 = c^2$. Then c^2 will be odd since it is the sum of an odd integer and an even integer and therefore c is odd. As noted before, since a is even and prime, we must have $a = 2$. Also, since c and b are odd,

there exists integers k and l such that $c = 2k+1$ and $d = 2l+1$. Then we have

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

so

$$4 + 4l^2 + 4l = 4k^2 + 4k$$

giving

$$1 + l + l^2 = k^2 + k.$$

Notice that regardless of whether k is odd or even, $k^2 + k$ is even, and likewise, if l is odd or even, $l^2 + l + 1$ is odd. Thus we have an even odd number equal to an even number which is not possible. Thus our initial assumption must be false, so a cannot be even with b odd.
Putting all these arguments together, we assumed that there existed primes a, b and c such that $a^2 + b^2 = c^2$, and we showed that for all possible choices for a, b and c, this equality is not satisfied, so we have shown there exists and there doesn't exist such integers - a contradiction. Thus our original assumption must be wrong and thus for all prime numbers a, b and c, $a^2 + b^2 \neq c^2$.

$\square$

Note that when we use contradiction a number of different times, we need to be very careful to make sure we know which hypothesis is being contradicted.

2. Proof by Contraposition

We know that the the contrapositive of a conditional is equivalent to a conditional. Therefore, to prove a conditional statement, we can instead prove the contrapositive of that statement. This method of indirect proof is called "proof by contraposition". To use proof by contraposition, we take the following steps:

(i) Express the statement to be proved in the form

$$\forall x, P(x) \rightarrow Q(x)$$

(ii) Rewrite the contrapositive of the statement

$$\forall x, \sim Q(x) \rightarrow \sim P(x)$$

(iii) Prove the contrapositive via a direct proof (as previously learned)

Since the general technique of contraposition is similar to contradiction, we shall illustrate with just two examples.

Theorem 2.1. *If a product of two positive real numbers is greater than* 100*, then at least on of the numbers is greater than* 10*.*

Proof. Formally, this statement reads:

$$\forall x, y \in \mathbb{R}^+, xy > 100 \to (x > 10) \vee (y > 10).$$

The contrapositive reads

$$\forall x, y \in \mathbb{R}^+, (x \leqslant 10) \wedge (y \leqslant 10) \to xy \leqslant 100.$$

Suppose x and y are two arbitrary positive real numbers less than or equal to 10. Then using simple arithmetic and inequalities, we have

$$xy \leqslant 10 \cdot 10 = 100$$

so $xy \leqslant 100$. Thus the contrapositive is true and hence the original statement is true.

□

The next theorem we have already used a number of times, so for completion, we shall write a complete proof.

Theorem 2.2. *For all integers n, if n^2 is odd then n is odd*

Proof. If O denotes the set of all odd integers, then formally, this statement reads:

$$\forall x \in O, x^2 \text{ odd } \to x \text{ odd}.$$

The contrapositive reads

$$\forall x \in O, x \text{ even } \to x^2 \text{ even}.$$

Suppose x is an even integer. Then $x \cdot x$ is a product of even integers and so is itself an even integer. Therefore, we have proved the contrapositive, and thus the original statement must hold.

□

Homework

(i) From the book, pages 178-179: Questions: 1, 2, 3, 5, 10, 14, 16, 19, 20, 22, 25, 27