Contradiction and Contraposition

Method of Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Theorem: There is no greatest integer.

Proof:

Suppose not. That is, suppose there is a greatest integer N.

Then $N \geq n$ for every integer n.

Let $M = N + 1$. Now M is an integer since it is a sum of integers. Also $M > N$ since $M = N + 1$. Thus M is an integer that is greater than N. So N is the greatest integer and N is not the greatest integer, which is a contradiction. [This contradiction shows that the supposition is false and, hence, that the theorem is true.]

Theorem: There is no integer that is both even and odd.

Proof:

Suppose not. That is, suppose there is at least one integer n that is both even and odd. [We must deduce a contradiction.] By definition of even, $n = 2a$ for some integer a, and by definition of odd, $n = 2b + 1$ for some integer b. Consequently, by equating the two expressions for n

$$2a = 2b + 1$$

and so

$$2a - 2b = 1$$
$$2(a - b) = 1$$
$$a - b = 1/2 \qquad \text{by algebra.}$$

Now since a and b are integers, the difference $a - b$ must also be an integer. But $a - b = 1/2$, and $1/2$ is not an integer. Thus $a - b$ is an integer and $a - b$ is not an integer, which is a contradiction. [This contradiction shows that the supposition is false and, hence, that the theorem is true.]

Theorem: The sum of any rational number and any irrational number is irrational.

Proof: [We take the negation of the theorem and suppose it to be true.] Suppose not. That is, suppose there is a rational number r and an irrational number s such that $r + s$ is rational. [We must deduce a contradiction.] By definition of rational, $r = a/b$ and $r + s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. By substitution,

$$\frac{a}{b} + s = \frac{c}{d},$$

and so

$$s = \frac{c}{d} - \frac{a}{b}$$ by subtracting a/b from both sides

$$s = \frac{cb - ad}{bd}$$ by the laws of algebra.

Now $bc - ad$ and bd are both integers [since a, b, c, and d are integers and since products and differences of integers are integers], and $bd \neq 0$ [by the zero-product property]. Hence s is a quotient of the two integers $bc - ad$ and bd with $bd \neq 0$. Thus, by definition of rational, s is rational, which contradicts the supposition that s is irrational. [Hence the supposition is false, and the theorem is true.]

Method of Proof by Contraposition

1. Express the statement to be proved in the form
   $\forall x\ in\ D$, if $P(x)$ then $Q(x)$. (This step may be done mentally.)
2. Rewrite this statement in the contrapositive form
   $\forall x\ in\ D$, if $Q(x)$ is false then $P(x)$ is false. (This step may also be done mentally.)
3. Prove the contrapositive by a direct proof.
   a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.
   b. Show that $P(x)$ is false.

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

Proof (by contraposition):

$$\forall\, n \in \mathbb{Z}, \text{if } n \text{ is odd then } n^2 \text{ is odd}$$

Suppose n is any odd integer. [We must show that n^2 is odd.] By definition of odd, $n = 2k + 1$ for some integer k. By substitution and 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,

$n^2 = 2.\text{(an integer)} + 1$, and thus, by definition of odd, n^2 is odd [as was to be shown].

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

Proof (by contradiction):

[We take the negation of the theorem and suppose it to be true.] Suppose not. That is, suppose there is an integer n such that n^2 is even and n is not even. [We must deduce a contradiction.] 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, by definition of odd, $n = 2k + 1$ for some integer k. By substitution and 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 $n^2 = 2 \cdot (\text{an integer}) + 1$, and thus, by definition of odd, n^2 is odd. Therefore, n^2 is both even and odd. This contradicts the result that: no integer can be both even and odd. [This contradiction shows that the supposition is false and, hence, that the proposition is true.]

Theorem: $\sqrt{2}$ is irrational.

Proof (by contradiction): *[We take the negation and suppose it to be true.]* Suppose not. That is, suppose $\sqrt{\mathbf{2}}$ is rational. Then there are integers *m* and *n* with no com- mon factors such that

$$\sqrt{\mathbf{2}} = \frac{\boldsymbol{m}}{\boldsymbol{n}}$$

[by dividing m and n by any common factors if necessary]. *[We must derive a contradiction.]* Squaring both sides of equation gives

$$2 = \frac{m^2}{n^2}.$$

Or, equivalently,

$$m^2 = 2n^2$$

(1)

Note that equation implies that m^2 is even (by definition of even). It follows that *m* is even (by Proposition). We file this fact away for future reference and also deduce (by definition of even) that

$$m = 2k \text{ for some integer } k. \qquad (2)$$

Substituting equation (2) into equation (1), we see that

$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Dividing both sides of the right-most equation by 2 gives

$$n^2 = 2k^2.$$

Consequently, n^2 is even, and so *n* is even (by Proposition). But we also know that *m* is even. *[This is the fact we filed away.]* Hence both *m* and *n* have a common factor of 2. But this contradicts the supposition that *m* and *n* have no common factors. *[Hence the supposition is false and so the theorem is true.]*

Proposition:

For any integer a and any prime number p, if $p|a$ then $p \nmid (a+1)$.

Proposition: The set of primes is infinite.

Proof (by contradiction): Suppose not. That is, suppose the set of prime numbers is finite. *[We must deduce a contradiction.]* Then some prime number *p* is the largest of all the prime numbers, and hence we can list the prime numbers in ascending order:

$$2, 3, 5, 7, 11, \ldots, p.$$

Let *N* be the product of all the prime numbers plus 1:

$$N = (2.3.5.7.11 \ldots p) + 1$$

Then $N > 1$, and so, by theorem, *N* is divisible by some prime number *q*. Because *q* is prime, *q* must equal one of the prime numbers $2, 3, 5, 7, 11, \ldots, p$. Thus, by definition of divisibility, *q* divides $2.3.5.7.11 \ldots p$, and so, by Proposition, *q* does not divide $(2.3.5.7.11 \ldots p) + 1$, which equals *N*. Hence *N* is divisible by *q* and *N* is not divisible by *q*, and we have reached a contradiction. *[Therefore, the supposition is false and the theorem is true.]*