Proposition Every multiple of 4 equals $1+(-1)^n(2n-1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:
If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1+(-1)^n(2n-1)=k$.
What follows is a proof of this conditional statement.
Suppose k is a multiple of 4.
This means $k=4a$ for some integer a.
We must produce an $n \in \mathbb{N}$ for which $1+(-1)^n(2n-1)=k$.
This is done by cases, depending on whether a is zero, positive or negative.
Case 1. Suppose $a=0$. Let $n=1$. Then $1+(-1)^n(2n-1)=1+(-1)^1(2-1)=0$ $=4\cdot 0=4a=k$.
Case 2. Suppose $a>0$. Let $n=2a$, which is in $\mathbb{N}$ because a is positive. Also n is even, so $(-1)^n=1$. Thus $1+(-1)^n(2n-1)=1+(2n-1)=2n=2(2a)=4a=k$.
Case 3. Suppose $a<0$. Let $n=1-2a$, which is an element of $\mathbb{N}$ because a is negative, making $1-2a$ positive. Also n is odd, so $(-1)^n=-1$. Thus $1+(-1)^n(2n-1)=1-(2n-1)=1-(2(1-2a)-1)=4a=k$.

The above cases show that no matter whether a multiple $k=4a$ of 4 is zero, positive or negative, $k=1+(-1)^n(2n-1)$ for some $n \in \mathbb{N}$. ■

4.5 Treating Similar Cases

Occasionally two or more cases in a proof will be so similar that writing them separately seems tedious or unnecessary. Here is an example.

Proposition If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity.
We need to show that $m+n$ is odd. This is done in two cases, as follows.
Case 1. Suppose m is even and n is odd. Thus $m=2a$ and $n=2b+1$ for some integers a and b. Therefore $m+n=2a+2b+1=2(a+b)+1$, which is odd (by Definition 4.2).
Case 2. Suppose m is odd and n is even. Thus $m=2a+1$ and $n=2b$ for some integers a and b. Therefore $m+n=2a+1+2b=2(a+b)+1$, which is odd (by Definition 4.2).

In either case, $m+n$ is odd. ■

The two cases in this proof are entirely alike except for the order in which the even and odd terms occur. It is entirely appropriate to just do one case and indicate that the other case is nearly identical. The phrase "*Without loss of generality...*" is a common way of signaling that the proof is treating just one of several nearly identical cases. Here is a second version of the above example.

Proposition Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof. (Contrapositive) Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$.
By DeMorgan's law, it is not true that $5 \nmid x$ **or** it is not true that $5 \nmid y$.
Therefore $5 \mid x$ or $5 \mid y$. We consider these possibilities separately.
Case 1. Suppose $5 \mid x$. Then $x = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ay)$, and that means $5 \mid xy$.
Case 2. Suppose $5 \mid y$. Then $y = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ax)$, and that means $5 \mid xy$.
The above cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. ■

5.2 Congruence of Integers

This is a good time to introduce a new definition. It is not necessarily related to contrapositive proof, but introducing it now ensures that we have a sufficient variety of exercises to practice all our proof techniques on. This new definition occurs in many branches of mathematics, and it will surely play a role in some of your later courses. But our primary reason for introducing it is that it will give us more practice in writing proofs.

Definition 5.1 Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo n** if $n \mid (a - b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \pmod{n}$.

Example 5.1 Here are some examples:

1. $9 \equiv 1 \pmod{4}$ because $4 \mid (9 - 1)$.
2. $6 \equiv 10 \pmod{4}$ because $4 \mid (6 - 10)$.
3. $14 \not\equiv 8 \pmod{4}$ because $4 \nmid (14 - 8)$.
4. $20 \equiv 4 \pmod{8}$ because $8 \mid (20 - 4)$.
5. $17 \equiv -4 \pmod{3}$ because $3 \mid (17 - (-4))$.

In practical terms, $a \equiv b \pmod{n}$ means that a and b have the same remainder when divided by n. For example, we saw above that $6 \equiv 10 \pmod{4}$ and indeed 6 and 10 both have remainder 2 when divided by 4. Also we saw $14 \not\equiv 8 \pmod{4}$, and sure enough 14 has remainder 2 when divided by 4, while 8 has remainder 0.

To see that this is true in general, note that if a and b both have the same remainder r when divided by n, then it follows that $a = kn + r$ and $b = \ell n + r$ for some $k, \ell \in \mathbb{Z}$. Then $a - b = (kn + r) - (\ell n + r) = n(k - \ell)$. But $a - b = n(k - \ell)$ means $n \mid (a - b)$, so $a \equiv b \pmod{n}$. Conversely, one of the exercises for this chapter asks you to show that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n.

The idea of proof by contradiction is quite ancient, and goes back at least as far as the Pythagoreans, who used it to prove that certain numbers are irrational. Our next example follows their logic to prove that $\sqrt{2}$ is irrational. Recall that a number is rational if it equals a fraction of two integers, and it is irrational if it cannot be expressed as a fraction of two integers. Here is the exact definition.

Definition 6.1 A real number x is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Also, x is **irrational** if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.

We are now ready to use contradiction to prove that $\sqrt{2}$ is irrational. According to the outline, the first line of the proof should be "Suppose that it is not true that $\sqrt{2}$ is irrational." But it is helpful (though not mandatory) to tip our reader off to the fact that we are using proof by contradiction. One standard way of doing this is to make the first line "*Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational.*"

Proposition The number $\sqrt{2}$ is irrational.

Proof. Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational. Then $\sqrt{2}$ is rational, so there are integers a and b for which

$$\sqrt{2} = \frac{a}{b}. \tag{6.1}$$

Let this fraction be fully reduced; in particular, this means that a and b are not both even. (If they were both even, the fraction could be further reduced by factoring 2's from the numerator and denominator and canceling.) Squaring both sides of Equation 6.1 gives $2 = \frac{a^2}{b^2}$, and therefore

$$a^2 = 2b^2. \tag{6.2}$$

From this it follows that a^2 is even. But we proved earlier (Exercise 1 on page 110) that a^2 being even implies a is even. Thus, as we know that a and b are not both even, it follows that b **is odd.** Now, since a is even there is an integer c for which $a = 2c$. Plugging this value for a into Equation (6.2), we get $(2c)^2 = 2b^2$, so $4c^2 = 2b^2$, and hence $b^2 = 2c^2$. This means b^2 is even, so b is even also. But previously we deduced that b is odd. Thus we have the contradiction b is even **and** b is odd. ■

To appreciate the power of proof by contradiction, imagine trying to prove that $\sqrt{2}$ is irrational without it. Where would we begin? What would be our initial assumption? There are no clear answers to these questions.

Proof by contradiction gives us a starting point: Assume $\sqrt{2}$ is rational, and work from there.

In the above proof we got the contradiction (b is even) $\wedge \sim$(b is even) which has the form $C \wedge \sim C$. In general, your contradiction need not necessarily be of this form. Any statement that is clearly false is sufficient. For example $2 \neq 2$ would be a fine contradiction, as would be $4 \mid 2$, provided that you could deduce them.

Here is another ancient example, dating back at least as far as Euclid:

Proposition There are infinitely many prime numbers.

Proof. For the sake of contradiction, suppose there are only finitely many prime numbers. Then we can list all the prime numbers as $p_1, p_2, p_3, \ldots p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and so on. Thus p_n is the nth and largest prime number. Now consider the number $a = (p_1 p_2 p_3 \cdots p_n) + 1$, that is, a is the product of all prime numbers, plus 1. Now a, like any natural number greater than 1, has at least one prime divisor, and that means $p_k \mid a$ for at least one of our n prime numbers p_k. Thus there is an integer c for which $a = cp_k$, which is to say

$$(p_1 p_2 p_3 \cdots p_{k-1} p_k p_{k+1} \cdots p_n) + 1 = cp_k.$$

Dividing both sides of this by p_k gives us

$$(p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n) + \frac{1}{p_k} = c,$$

so

$$\frac{1}{p_k} = c - (p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n).$$

The expression on the right is an integer, while the expression on the left is not an integer. This is a contradiction. ■

Proof by contradiction often works well in proving statements of the form $\forall x, P(x)$. The reason is that the proof set-up involves assuming $\sim \forall x, P(x)$, which as we know from Section 2.10 is equivalent to $\exists x, \sim P(x)$. This gives us a specific x for which $\sim P(x)$ is true, and often that is enough to produce a contradiction. Here is an example:

Proposition For every real number $x \in [0, \pi/2]$, we have $\sin x + \cos x \geq 1$.

Proof. Suppose for the sake of contradiction that this is not true.
Then there exists an $x \in [0, \pi/2]$ for which $\sin x + \cos x < 1$.