3.3.1 Direct proof

A **direct proof** is a simple chain of implications, starting with what's known and ending with the statement of the theorem one wanted to prove. For example:

Theorem 2 *The sum of two odd integers is an even integer.*

Proof. An integer is odd if it can be written in the form $2n+1$ for some $n \in \mathbb{Z}$. So the sum of two odd integers is of the form $(2n+1)+(2m+1)$, for some $n, m \in \mathbb{Z}$. Now $(2n+1)+(2m+1) = 2n+2m+2 = 2(n+m+1)$, which is even. □

3.3.2 Proof by contradiction

A **proof by contradiction** (also called *redactio ad absurdum*) starts by assuming that the statement you want to prove is false, and then deducing from this a contradiction. In other words, if we want to prove a statement P, we show that $\neg P$ implies a statement which is false. Hence $\neg P$ is false, and so P must be true.

We used this technique in our proof of Theorem 1: We assumed that $A \neq \emptyset$ (i.e. that there exist positive integers greater than 1 which are not divisible by prime numbers), and deduced a contradiction from this. Thus $A = \emptyset$ must hold.

Here is another example:

Theorem 3 $\sqrt{2}$ *is irrational.*

Proof. Suppose that $\sqrt{2}$ is rational, i.e. that $\sqrt{2} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$, $n \neq 0$. We may write $\frac{m}{n}$ in lowest terms, i.e. we can choose m, n such that m and n do not share any common factor besides 1. Squaring both sides give $2 = \frac{m^2}{n^2}$, so $m^2 = 2n^2$. This means that m^2 is even, and so m itself is also even (if m were odd, then m^2 would also be odd). Hence we can write $m = 2k$ for some $k \in \mathbb{Z}$, and so $2n^2 = m^2 = (2k)^2 = 4k^2$. Divide both side by 2, and we get $n^2 = 2k^2$. This means that n^2 is even, which in turn implies that n itself is also even. So now we have shown that m and n are both even (are both divisible by 2), which is impossible since m and n have no common factor. This contradiction shows that our assumption (that $\sqrt{2}$ is rational) is wrong. Hence $\sqrt{2}$ is irrational. □

Here is yet another example (which dates back to Euclid, some 2300 years ago):

Theorem 4 *There are infinitely many prime numbers.*

Proof. Suppose that there are only finitely many prime numbers, and let $p_1, p_2, \ldots, p_n$ be all of them. Consider the number $N := p_1 \cdot p_2 \cdots p_n + 1$, the product of all primes, plus one. Then N is not divisible by any of the p_i's, because it leaves a remainder of 1 when divided by any p_i. But this means that N is not divisible by any prime number, and certainly $N > 1$. However, Theorem 1 asserts that any integer greater than 1 is divisible by a prime. This is a contradiction, hence our assumption (that there are only finitely many primes) must be false. It follows that there are infinitely many primes. □

3.3.3 Mathematical induction

A proof by **mathematical induction** is a clever way of using Axiom 1 (the **well-ordering principle**).

If we want to prove a statement S_n that depends on a natural number n, then it suffices to prove the following two statements:

(i) S_1 is true, i.e. our statement is true when $n = 1$, and