Mathematical Proof

What is a proof? To explain, let us consider an example.

THEOREM 1.1. *There is no rational number* r *which is a square root of* 2.

This theorem was already known to the ancient Greeks. It was very important to them since they were particularly interested in geometry, and, as follows from the Theorem of Pythagoras, a segment of length $\sqrt{2}$ can be constructed as the hypotenuse of a right triangle with both sides of length 1.

Before we prove this theorem, in fact before we prove any theorem, we must understand its statement. To understand its statement, we must understand each of the terms used. For instance: what is a *rational number*? For this we need a *definition*.

DEFINITION 1.1. A number r is *rational* if it can be represented as the ratio of two integers:

$$r = \frac{n}{m} \tag{1.1}$$

where $m \neq 0$.

Of course, in this definition, we are using other terms that need to be defined, such as *number*, *ratio*, *integer*. We will not dwell on this point, and instead assume for now that these have been defined previously. However, already one point is clear. If we wish to be absolutely rigorous, we must begin from some given assumptions. We will call these *axioms*. They do not require proof. We will discuss this point further later. For the time being, let us assume that we have a system of numbers where the usual operations of arithmetic are defined.

Next we need to define what we mean by a *square root* of 2.

DEFINITION 1.2. Let y be a number. The number x is a *square root* of y if $x^2 = y$.

Again, we assume that the meaning of x^2 is understood. Note that we have said *a* square root, and not *the* square root. Indeed if $x \neq 0$ is a square root of y, then $-x$ is another one. Note that then, one of the two numbers x and $-x$ is positive. Now, we may give the proof of Theorem 1.1.

PROOF. The proof is by contradiction. Suppose that x is a square root of 2, and that x is rational. Clearly, $x \neq 0$, hence we may assume that $x > 0$. Then, $x^2 = 2$, and there are integers n, $m \neq 0$, such that

$$x = \frac{n}{m}. \tag{1.2}$$

Of course there are many such pairs n, and m. In fact, if n and m is any such pair, then $2n$ and $2m$ is another pair. Also, there is one pair in which $n > 0$. Among all these pairs, with $n > 0$, pick one for which n is the smallest positive integer possible, i.e., $x = n/m$, $n > 0$, and if $x = k/l$ then $n \leqslant k$. We have:

$$\left(\frac{n}{m}\right)^2 = 2, \tag{1.3}$$

or equivalently

$$n^2 = 2m^2. \tag{1.4}$$

Thus, 2 divides $n^2 = n \cdot n$. It follows that 2 divides n, i.e. n is even. We may therefore write $n = 2k$ and thus

$$n^2 = 4k^2 = 2m^2, \tag{1.5}$$

or equivalently

$$2k^2 = m^2. \tag{1.6}$$

Now, 2 divides m^2, hence m is even. Write $m = 2l$. We obtain

$$x = \frac{n}{m} = \frac{2k}{2l} = \frac{k}{l}. \tag{1.7}$$

But k is positive and clearly $k < n$, a contradiction. Thus no such x exists, and the theorem is proved. □

A close examination of this proof will be instructive. The first observation is that the proof is by contradiction. We assumed that the statement to be proved is false, and we reached an absurdity. Here the statement to be proved was that *there is no rational x for which $x^2 = 2$*, so we assumed there is one such x. The absurdity was that we could certainly take $x = n/m$, with $n > 0$ and as small as possible, but we deduced $x = k/l$ with $0 < k < n$. Next, we see that each step follows from the previous one, and possibly some additional information. Take for example, the argument immediately following (1.4). If 2 divides n^2 then 2 divides n. This seemingly obvious fact requires justification. We will not do this here; it is done in algebra, and relies on the unique factorization by primes of the integers. It is extremely important to identify the information which you import into your proof from outside. Usually, this is done by quoting a known theorem. Remember that before you quote a theorem, you must check its hypotheses.

Read this proof again and again during the term. Try to find its weak points, those points which could use more justification. Try to improve it. Try to imagine how it was discovered.