3. Mathematical induction

The general setup where the method of mathematical induction may be applicable is as follows. Suppose that for every $n \in \mathbb{N}$ we are given some statement $P(n)$, depending on n, e.g.

$$1 + \ldots + n = \frac{n(n+1)}{2} \qquad P(n).$$

The statement may have the form of an equality, inequality or something more involved. We wish to prove that $P(n)$ is true for all $n \in \mathbb{N}$. The method of mathematical induction asserts that this can be accomplished in two stages:

(i) (Induction base) Prove that $P(1)$ is true
(ii) (Induction step) For every $n \in \mathbb{N}$ prove the implication "$P(n) \Rightarrow P(n+1)$", that is, assume that $P(n)$ is true and deduce that $P(n+1)$ is true.

Indeed, if we verified (i) and (ii), then the following sequence of implications shows that $P(n)$ must be true for all $n \in \mathbb{N}$:

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \ldots$$

Example 3.1. *Prove that* $1 + \ldots + n = \frac{n(n+1)}{2}$ *for all* $n \in \mathbb{N}$.

For simplicity of notation in this example we let $s_n = 1 + \ldots + n$. Thus the statement $P(n)$ we have to prove in this problem can be rewritten as

$$s_n = \frac{n(n+1)}{2} \qquad P(n)$$

Note that by definition $s_1 = 1$ and $s_{n+1} = (1 + \ldots + n) + (n+1) = s_n + (n+1)$. The conditions $s_1 = 1$ and $s_{n+1} = s_n + (n+1)$ for all $n \in \mathbb{N}$ completely determine the sequence $\{s_n\}$, so from this point on we can forget about the original definition of s_n and work with this recursive definition.

Base case: $n = 1$. We need to check that $s_1 = \frac{1(1+1)}{2}$. This is true since $s_1 = 1$ by definition and $\frac{1(1+1)}{2} = 1$ as well.

Induction step. "$P(n) \Rightarrow P(n+1)$". Now we fix n and assume that $s_n = \frac{n(n+1)}{2}$. Our goal is to show that $s_{n+1} = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$.

We shall compute both s_{n+1} and $\frac{(n+1)(n+2)}{2}$ and show that they are equal to each other. Multiplying out, we have $\frac{(n+1)(n+2)}{2} = \frac{n^2+3n+2}{2} = \frac{n^2}{2} + \frac{3n}{2} + 1$. On the other hand, using the recursive relation $s_{n+1} = s_n + (n+1)$ and the inductive hypothesis $s_n = \frac{n(n+1)}{2}$, we get

$$s_{n+1} = s_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2}{2} + \frac{n}{2} + n + 1 = \frac{n^2}{2} + \frac{3n}{2} + 1.$$

Thus, we proved that $s_{n+1} = \frac{(n+1)(n+2)}{2}$, so $P(n+1)$ is true. This completes the induction step.

Example 3.2. *Prove that for every* $n \in \mathbb{N}$

$$\text{there exist } a_n, b_n \in \mathbb{Z} \text{ such that } (1+\sqrt{2})^n = a_n + b_n\sqrt{2}. \qquad P(n)$$

In this problem the statement $P(n)$ is more complicated as it does not specify the values of a_n and b_n (they are for us to choose; all we have to make sure is that $a_n, b_n \in \mathbb{Z}$). We shall solve this problem by induction as follows: first we will define $a_1, b_1 \in \mathbb{Z}$ so that $P(1)$ is true. Then, for every $n \in \mathbb{N}$, we will assume that $P(n)$ is true and then define a_{n+1} and b_{n+1} recursively in terms of a_n and b_n so that $P(n+1)$ is true.

Base case: $n = 1$. We set $a_1 = b_1 = 1$. Then $a_1 + b_1\sqrt{2} = 1 + \sqrt{2} = (1+\sqrt{2})^1$, so $P(1)$ is true.

Induction step. Now assume that $P(n)$ is true, so that $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$ for some $a_n, b_n \in \mathbb{Z}$. Before defining a_{n+1} and b_{n+1}, we compute $(1+\sqrt{2})^{n+1}$ using the above formula for $(1+\sqrt{2})^n$. We have

$$(1+\sqrt{2})^{n+1} = (1+\sqrt{2})^n \cdot (1+\sqrt{2}) = (a_n + b_n\sqrt{2})(1+\sqrt{2}) = (a_n + 2b_n) + (a_n + b_n)\sqrt{2}.$$

Now it is clear how to define a_{n+1} and b_{n+1}: we set $a_{n+1} = a_n + 2b_n$ and $b_{n+1} = a_n + b_n$. Then $(1+\sqrt{2})^{n+1} = a_{n+1} + b_{n+1}\sqrt{2}$ by the above computation. Also, since $a_n, b_n \in \mathbb{Z}$ by inductive hypothesis and since integers are closed under addition and multiplication by 2, we conclude that $a_{n+1}, b_{n+1} \in \mathbb{Z}$. Thus, we verified that $P(n+1)$ is true.

Here are a few standard variations one sometimes needs to make when doing an induction proof.

(i) Sometimes it is technically more convenient to do the induction step in the form "$P(n-1) \Rightarrow P(n)$" (instead of $P(n) \Rightarrow P(n+1)$). Of course, in this case we assume that $n \geq 2$ in the induction step.

(ii) We may be asked to prove that certain statement $P(n)$ holds for all integers $n \geq a$ for some $a \neq 1$. In this case proof by induction works the same except that in the base case we verify $P(a)$, not $P(1)$.

(iii) It is possible that the statement $P(n)$ holds for all $n \in \mathbb{N}$, but the natural argument for the induction step does not work for some small values of n (say, it only works for $n \geq 3$). In this case we verify $P(1), P(2)$ and $P(3)$ separately as part of the base case.

(iv) Finally, sometimes we need to use the *complete induction.* In this case, for the induction step we assume not only that $P(n)$ is true but that $P(k)$ is true for all $k \leq n$ (that is, $P(1), P(2), \ldots, P(n)$ are all true) and deduce that $P(n+1)$ is true. Note that the logical justification of a proof by complete induction remains the same.

We finished the lecture by proving the theorem about division with remainder for integers.

Theorem 3.3. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r \leq |b| - 1$.*