## 1. The Set $\mathbb{N}$ of Natural Numbers

- Last time, we covered the **Peano Axioms**, which tells that the set $\mathbb{N}$ satisfies:

  **(N1)** $1 \in \mathbb{N}$.

  **(N2)** For any $n \in \mathbb{N}$, we have $\mathsf{Suc}(n) \in \mathbb{N}$.

  **(N3)** $\mathsf{Suc}(n) \neq 1$ for any $n \in \mathbb{N}$.

  **(N4)** For any $m, n \in \mathbb{N}$, if $\mathsf{Suc}(m) = \mathsf{Suc}(n)$, then $m = n$.

  **(N5)** Suppose $S \subseteq \mathbb{N}$ satisfies the properties:

  (i) $1 \in S$; (ii) if $n \in S$, then $n + 1 \in S$.

  Then $S = \mathbb{N}$.

- Axiom (N5) deserves particular attention, because it serves the basis of one of the most powerful machinery in mathematics, called the **principle of mathematical induction**.[1]

> **Principle of Mathematical Induction (PMI).** Consider a list of statements $P_1, P_2, P_3, \dots$ so that each $P_n$ may or may not be true, possibly depending on the value of $n$. Suppose the following properties hold:
>
> **(I1)** $P_1$ is true, (Base Case)
>
> **(I2)** For each $n \in \mathbb{N}$, if $P_n$ is true, then $P_{n+1}$ is true. (Inductive Step)
>
> Then all the statement $P_1, P_2, P_3, \dots$ are true.

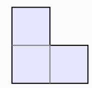
*Proof.*

[1] Despite its name, this is actually a form of deductive reasoning. This should not be confused with inductive reasoning.

**Example 1.1.** Prove that $1+2+\cdots+n=\dfrac{n(n+1)}{2}$ holds for any positive integer $n$.

*Proof.*

**Example 1.2.** Show that a $2^n \times 2^n$ grid with one square at the corner removed can be tiled with L-triominoes. Here, an L-triomino is a shape consisting of three squares joined in an 'L'-shape:



*Proof.*

- If we instead have a list of statements $P_m, P_{m+1}, P_{m+2}, \ldots$ that starts at the index $m$ instead of $1$, a version of PMI still works for an obvious reason.

**Example 1.3.** Prove that $2^n > n^2$ holds for any integer $n \geq 5$.

*Proof.*

- Here is an important remark. In (I2), the inductive step, we are not required to verify the truth of any of $P_n$ and $P_{n+1}$ at all. We are merely required to prove:

  "If we assume that $P_n$ is true, then under that assumption $P_{n+1}$ is also true."

  In particular, it is possible that the inductive step holds true even when all of $P_n$'s are false!

**Example 1.4.** Consider the statement

$$P_n \,:\, n^2 + 5n + 1 \text{ is an even integer.}$$

**(a)** Verify that the inductive step is true for this $P_n$.

**(b)** Show that $P_n$ is actually *false* for any $n \in \mathbb{N}$.

*Proof.*

- Concluding, we introduce another well-known property of $\mathbb{N}$:

**Well-Ordering Principle.** Every non-empty subset $T$ of $\mathbb{N}$ has a least element. That is, there is $m \in T$ such that $m \leq n$ for all $n \in T$.

Although this principle may look trivial, it is at least as powerful as PMI, in the sense that one implies the other. Here, we will only prove that PMI implies the well-ordering principle.

*Proof.*

## 2. The Set $\mathbb{Q}$ of Rational Numbers

- After subtraction is introduced, we are able to define $0$ and negative integers. By adding them to $\mathbb{N}$, we obtain the **set $\mathbb{Z}$ of integers**:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

- After division is introduced, we are led to enlarge $\mathbb{Z}$ by adding numbers of the form $m/n$ for integers $m, n \in \mathbb{Z}$ with $n \neq 0$. This gives rise to the **set $\mathbb{Q}$ of rational numbers**. That is,

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z} \text{ and } n \neq 0 \right\}.$$

- The set $\mathbb{Q}$ is very satisfactory in that it is closed under the basic operations (addition, subtraction, multiplication, and division).

- On the other hand, the set $\mathbb{Q}$ is often not large enough, having "gaps". One class of such gaps arise when we try to solve polynomial equations, such as $x^2 - 2 = 0$.

**Definition 2.1.** A number is called an **algebraic number** if it satisfies a polynomial equation

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

where $n \geq 1$, the coefficients $c_0, c_1, \dots, c_n$ are integers, and $c_n \neq 0$.

**Example 2.1.** Show that any rational numbers are algebraic numbers.

*Solution.*

**Example 2.2.** Show that $a = \sqrt{\frac{1}{3}(4 - \sqrt[3]{5})}$ is an algebraic number.

*Solution.*

- The following theorem tells that there are only handful of rational candidates for solutions of an integer polynomial equation.

**Theorem 2.2. (Rational Zeros Theorem)** Consider the polynomial equation

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

where $n \geq 1$ and $c_0, c_1, \ldots, c_n$ are integers with $c_0 \neq 0$ and $c_n \neq 0$. Suppose $r = p/q$ is a rational solution of this equation, where $p, q$ are integers having no common factors and $d \neq 0$. Then $p$ divides $c_0$, and $q$ divides $c_n$.

*Proof.*

**Corollary 2.3.** Consider the polynomial equation

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

where $n \geq 1$ and $c_0, c_1, \ldots, c_{n-1}$ are integers with $c_0 \neq 0$. Then any rational solution of this equation must be an integer that divides $c_0$.

*Proof.*

- Using the Rational Zeros Theorem and its corollary, we can establish irrationality of many algebraic numbers.

**Example 2.3.** Prove that each of the following numbers is not a rational number.

**(a)** $\sqrt{2}$ **(b)** $\sqrt[3]{5}$

*Solution.*

**Example 2.4.** Prove that $a = \sqrt{\frac{1}{3}(4 - \sqrt[3]{5})}$ is not a rational number.

*Solution.*