Starting Assumptions

One difficulty with proof based courses is the students may be unclear on just what material they can assume. We address this now.

Let $\mathbb{Z}$ be the integers, $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. If $n \in \mathbb{Z}$ then so are $n+1$ and $n-1$, We assume the basic properties of addition, subtraction, multiplication, and division when defined. (Thus, $\mathbb{Z}$ is an example of a *ring*.) We also assume the usual ordering on $\mathbb{Z}$: $\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \ldots$.

Let $\mathbb{N}$ denote the positive integers, $\{1, 2, 3, \ldots...\}$. It is assumed you know how to do induction proofs: If a proposition $P(1)$ is true and if $P(k) \implies P(k+1)$, then $P(n)$ is true for all $n \in \mathbb{N}$ by the Principle of Mathematical Induction.

An element $p \neq 1$ of $\mathbb{N}$ is *prime* if whenever $p = m \cdot n$ for natural numbers m and n either $m = 1$ and $n = p$, or $m = p$ and $n = 1$. An element $c \neq 1$ in $\mathbb{N}$ is *composite* if $\exists$ m and n in $\mathbb{N} - \{1\}$ such that $c = m \cdot n$. Each number in $\mathbb{N}$ is exclusively either 1, prime or composite.

The Prime Factorization Theorem. Every composite number can be written as a product of prime numbers and the *prime decomposition* is unique up to reordering.

Example. $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$.

The Division Algorithm Theorem. If n and d are integers with $d > 0$, then there are unique integers q and r such that

$$n = dq + r \quad \text{with} \quad 0 \leq r < d.$$

We say n divided by d is q remainder r.

Example. For $a = 53$ and $b = 17$ we have $53 = 3 \cdot 17 + 2$. Thus, 53 divided by 17 is 3 remainder 2.

These two theorems are proved in MATH 425, Introduction to Number Theory.

The Rational Numbers

Let $\mathbb{Q}$ be the set of rational numbers, that is

$$\mathbb{Q} = \{(m,n) \,|\, m,n \in \mathbb{Z}, n \neq 0\}/\sim$$

where the equivalence relation $\sim$ is given by

$$(m_1,n_1) \sim (m_2,n_2) \text{ if } m_1n_2 = m_2n_1.$$

We usually write $\frac{m}{n}$ for $[(m,n)]$ (the brackets mean the equivalence class) and $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ when $(m_1,n_1) \sim (m_2,n_2)$. We may write $\frac{n}{1}$ as n and regard $\mathbb{Z}$ as a subset of $\mathbb{Q}$.

Example. $\frac{4}{7} = \frac{-8}{-14}$ since $4(-14) = -56 = -8(7)$.

We say $\frac{a}{b}$ is in *reduced form* if $b > 0$ and a and b have no common prime factors.

We define

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{cd} \quad \& \quad \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

Subtraction, division and powers are defined as usual. Assume b and d are positive. We define $\frac{a}{b} < \frac{c}{d}$ if $ad < cb$. Define $>$, $\leq$ and $\geq$ as usual.

With these definitions $\mathbb{Q}$ is an example of an *ordered field*.

Important Fact. There is no $\frac{p}{q} \in \mathbb{Q}$ such that $\left(\frac{p}{q}\right)^2 = 2$.

It is assumed you can prove this in your sleep.

Theorem. Every rational number can be written in the form

$$\pm\left(n + \sum_{i=1}^{\infty} \frac{a_i}{10^i}\right)$$

where $n \in \mathbb{N} \cup \{0\}$ and each $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$. It can be abbreviated as $\pm n.a_1a_2a_3\ldots$. This is called the *decimal representation*. It is not always unique since, for example, $1.000\cdots = 0.999\ldots$. We will study convergence later.

Theorem. If $n.a_1a_2a_3\cdots \in \mathbb{Q}$ then eventually the a_i's repeat. That is $\exists$ k and j such that for $i \geq k$, $a_i = a_{i+j}$.

Example. $\frac{83515}{1100} = 75.92272727272....$ So, $k = 3$ and $j = 2$. Find k and j for $\frac{579}{17}$.

Optional Project. Write a computer program that finds k and j.

Real Numbers

Let $\mathbb{R} = \{\pm n.a_1a_2a_3\ldots \mid n \in \mathbb{N} \cup \{0\}, a_i \in \{0,1,2,3,4,5,6,7,8,9\}\} / \sim$, where $\sim$ is defined by

$$n.a_1\cdots a_k999... = n.a_1\cdots a_{k-1}(a_k+1)000..., \quad \text{where } a_k \neq 9 \ \&$$

$$n.9999... = n+1.0000...$$

Then $\mathbb{R}$ is called the set of *real numbers.*

It is not obvious how to define the arithmetic operations in $\mathbb{R}$. It can be done using limits. This is done in MATH 452, Introduction to Real Analysis. We assume this for now.

It is easier to define an ordering $<$. Let x and y be distinct nonnegative members of $\mathbb{R}$. Assume

$$x = m.a_1a_2...$$

$$y = n.b_1b_2...$$

are in normal form. Define $x < y$ if $m < n$ or $m = n$ and $a_i < b_i$ where i is the smallest index where $a_i \neq b_i$. This can be extended to pairs of negative real numbers by the rule $x < y$ iff $-y < -x$. We finally agree to define negative real numbers to be less than nonnegative real numbers. One can show, although the details are messy, that this ordering induces the same ordering on the subset of rational numbers as we had before.

Food for Thought. Suppose an intelligent species from another planet used a number system

$$\{...a_3a_2a_1.b_1b_2b_3... \mid a_i, b_i \in \{0,1,2,3,4,5,6,7,8,9\}\}.$$

That is the digits can be infinite in both directions. Would this make them smarter than us?