Ch. 13 - Number Systems

Highlights:
- Rational numbers
- gcd
- coprime/relatively prime
- Irrationality of $\sqrt{2}$

Problem types:
- Prove irrationality
  > from Ch. 11
- Irrationality of certain square roots
Defn: A number $x$ is **rational** if it can be expressed as a fraction $x = \frac{a}{b}$ where $a, b$ are integers ($b \neq 0$).

Defn: Let $a, b \in \mathbb{Z}$ with either $a \neq 0$ or $b \neq 0$. The **greatest common divisor** of $a$ and $b$, denoted $\gcd(a, b)$, is

$$\gcd(a, b) = \max\{n \in \mathbb{Z} : n \text{ divides } a \text{ and } n \text{ divides } b\}$$

**Note:** The set $\{n \in \mathbb{Z} : n \text{ divides } a \text{ and } n \text{ divides } b\}$ is finite because it is a subset of the finite set $\mathbb{N}_a \cup \mathbb{N}_b$, therefore the maximum exists.

Defn: Integers $a, b$, not both zero, are **coprime** (or relatively prime) if $\gcd(a, b) = 1$.

**Lemma:** Let $a, b \in \mathbb{Z}$, not both zero, and set $c = \gcd(a, b)$. Then $\frac{a}{c}, \frac{b}{c} \in \mathbb{Z}$ and $\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = 1$

**Proof:** By definition, $c$ divides $a$ and $b$. So there are $p, q \in \mathbb{Z}$ with $a = pc$ and $b = qc$. Then $\frac{a}{c} = p$ and $\frac{b}{c} = q$ are integers as claimed. Set $m = \gcd(p, q)$ and towards a contradiction suppose $m > 1$. Let $j \in \mathbb{Z}$ with $p = mj$ and $q = mj$. Then

$$a = pc = jm, \quad b = qc = jm.$$ 

So $mc$ divides $a$ and $b$ and therefore $mc \leq \gcd(a, b) = c$. But $mc > c$ because $m > 1$ and $c \geq 0$, a contradiction. We conclude $\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = \gcd(p, q) = 1$. \qed
Corollary: If $x \in \mathbb{R}$ is rational then there are $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $x = \frac{a}{b}$

Proof: Let $x \in \mathbb{R}$ be rational.
So by definition there are $a_0, b_0 \in \mathbb{Z}$ with $x = \frac{a_0}{b_0}$ and $b_0 \neq 0$. Set $c = \gcd(a_0, b_0)$, $a = \frac{a_0}{c} \in \mathbb{Z}$, and $b = \frac{b_0}{c} \in \mathbb{Z}$. Then $a_0 = ac$ and $b_0 = bc$ so

$$x = \frac{a_0}{b_0} = \frac{ac}{bc} = \frac{a}{b}.$$ 

Additionally, $\gcd(a, b) = 1$ by the previous lemma. \qed 

Theorem: $\sqrt{2}$ is not rational

Proof: Towards a contradiction, suppose $\sqrt{2}$ is rational. Then by the corollary above, there are $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $\sqrt{2} = \frac{a}{b}$. Squaring both sides then multiplying by $b^2$ gives $2b^2 = a^2$. So $a^2$ is even and this implies $a$ is even. So there is $a_0 \in \mathbb{Z}$ with $a = 2a_0$. Then $2b^2 = a^2 = (2a_0)^2 = 4a_0^2$ so $b^2 = 2a_0^2$.

It follows $b^2$ is even thus $b$ is even and there is $b_0 \in \mathbb{Z}$ with $b = 2b_0$. Since $a = 2a_0$ and $b = 2b_0$, $2$ divides $a$ and $b$ so $2 \leq \gcd(a, b) = 1$. This is a contradiction since $2 > 1$. We conclude $\sqrt{2}$ is not rational. \qed

Note: This will follow from the Division Theorem we will learn in Chapter 15.