1 The Integers

1.1 Numbers and Sequences

This section will set the stage for what's to come. It is primarily about numbers.

Mostly we will be working with the *integers* $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. Additionally, we have the *natural numbers* $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ which are a subset of $\mathbb{Z}^+$.

Definition. We say a set of real numbers is *well-ordered* if every non-empty subset has a smallest element.
Ex. $S = \{1, 2, 3, \cdots\}$ is well-ordered because every subset of S has a least element.
Ex. $S = [0, \infty)$ is *not* well-ordered because every subset does *not* have a least element. Consider the subsets $(0, \infty)$, $(0, 2)$, or $(1, 5]$, none of them have least elements.

Well-Ordering Principle. $\mathbb{Z}^+$ is well-ordered. (This proof involves some serious set theory, far beyond the scope of this course. See this as the proof.)

Definition. A real number is *rational* if it can be expressed as a/b where $a, b \in \mathbb{Z}$ and $b \neq 0$. The set of all rational numbers is denoted as $\mathbb{Q}$.

Ex. Prove $\sqrt{2}$ is irrational (not rational).

Proof. We need to prove that we cannot write $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ and $b \neq 0$. By way of contradiction, suppose $\sqrt{2}$ is rational. That is, suppose

$$\sqrt{2} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}^+$ and $b \neq 0$. Then we have that $a = b\sqrt{2}$. Note that $b \in \mathbb{Z}^+$ and $b\sqrt{2} = a \in \mathbb{Z}^+$.

Let $S = \{k \mid k \in \mathbb{Z}^+ \text{ and } k\sqrt{2} \in \mathbb{Z}^+\}$. Then $S \subset \mathbb{Z}^+$ and $S \neq \emptyset$ because $b \in S$. By the well-ordering principle, S has a least element, denote it m. Consider $m' = m\sqrt{2} - m$. Observe the following:

- $m' = m\sqrt{2} - m = m(\sqrt{2} - 1)$. Therefore $0 < m' < m$.

- Because $m \in S$ and $S \subset \mathbb{Z}^+$, $m, m\sqrt{2} \in \mathbb{Z}^+$. So $m' \in \mathbb{Z}^+$.

- Since $m \in \mathbb{Z}^+$ we have $2m \in \mathbb{Z}^+$, so now consider

$$m'\sqrt{2} = (m\sqrt{2} - m)\sqrt{2} = 2m - m\sqrt{2} \in \mathbb{Z}^+$$

Thus, $m' \in S$, which contradicts the fact that m is the least element in S. $\square$

Definition. A real number is *algebraic* if it is the root of a polynomial with integer coefficients.

Ex.

- Consider $x^3 + 3$. The roots are $x \pm \sqrt{3}$. So $\pm\sqrt{3}$ is algebraic.

- Is 7 algebraic? Yes, $x - 7$.

- Is $3/2$ algebraic? Yes, $3x - 2$.

- Is $\sqrt[3]{2 - \sqrt{7}}$ algebraic? Yes (although a bit more complicated)

$$
\begin{aligned}
x = \sqrt[3]{2 - \sqrt{7}} &\implies x^3 = 2 - \sqrt{7} \\
&\implies x^3 - 2 = \sqrt{7} \\
&\implies (x^3 - 2)^2 = 7 \\
&\implies x^6 - 4x^3 + 4 = 7 \\
&\implies x^6 - 4x^3 - 3 = 0
\end{aligned}
$$

- Is π algebraic? No! So what is it?

Definition. A real number is not algebraic is *transcendental* (it transcends the ability to be expressed as a root of a polynomial). So π is transcendental.

It is not difficult to prove the existence of transcendental numbers, but it is difficult to prove that any given number is transcendental.

Definition. Define $\lfloor x \rfloor$ to be the largest integer $\leq x$. Similarly, define $\lceil x \rceil$ to be the smallest integer $\geq x$.

Ex.

- $\lfloor 5.2 \rfloor = 5$

- $\lfloor -3.8 \rfloor = -4$

- $\lceil 5.2 \rceil = 6$

- $\lceil -3.8 \rceil = -3$

Definition. A set of numbers is *countable* if it is either finite or it can be placed in one-to-one correspondance with the positive integers.

Ex. The positive, even integers are countable, as are the integers and the rationals.

Ex. The real numbers are not countable. This is proved by Cantor's Argument.

Consider all polynomials with integer coefficients. There are countably many of these, each having countably many roots. Thus there are countably many algebraic numbers (the countable union of countable sets is countable). So out of $\mathbb{R}$, which is uncountable, we must have uncountably transcendental numbers (because they are "everything else").

1.2 Sum and Products

Here is a quick review of sums and products.

1. Recall $\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$.

2. Additionally, some useful identities are:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(n+2)}{6}$$

$$\sum_{i=1}^{n} r^i = \frac{r^{n+1}-1}{r-1}$$

3. Telescoping sums (using partial fractions) $\sum_{i=2}^{n} \frac{1}{i(i+1)} = \sum_{i=2}^{n} \frac{1}{i} - \frac{1}{i+1}$.

4. Product notation $\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n$.

1.3 Mathematical Induction

Weak Mathematical Induction. Suppose we wish to prove some statement is true for all $n = 1, 2, 3, \cdots$. Induction works as follows. We prove two things

1. **Base Case:** We prove it for $n = 1$.

2. **Inductive Step:** We prove that *if* it is true for some $k \geq 1$, then it *must* be true for $k + 1$.

Then we can conclude that it is true for $n = 1, 2, 3, \cdots$

Ex. Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all $n = 1, 2, 3, \cdots$.

Proof.

   Base Case:

   Let $n = 1$, $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$ so the base case is valid.

   Inductive Step:

Assume that it is true for some k. That is, assume

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Then consider the sum to $k+1$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} +(k+1)$$
$$= \left[\frac{k(k+1)}{2}\right] + (k+1) \quad \text{by IH}$$
$$= \frac{k(k+1) + 2(k+1)}{2}$$
$$= \frac{(k+1)((k+1)+1)}{2}$$

Thus, by weak induction

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$\square$

Ex. Prove $2^n > n!$ for all $n \geq 4$.

Proof.

Base Case:

Let $n = 4$, $2^4 = 16$ and $4! = 24$ so the base case is valid.

Inductive Step:

Assume that it is true for some $k \geq 4$. That is, assume

$$2^k < k!$$

Then consider the equation to $k+1$

$$2^{k+1} = 2 \cdot 2^k < 2k! < (k+1)k! = (k+1)!$$

Thus, by weak induction
$$2^k < k!$$

$\square$

Strong Mathematical Induction. Here, for the inductive step, instead of just assuming its true for k, we assume it is true for $1, 2, \cdots, k$. Then we show it is true for $k + 1$. (The nice thing is we get to assume more for the inductive hypothesis.)

Why would we need to do this alternative form? Often, to prove it is true for $k + 1$, it is insufficient to assume it is true for k. We may need earlier values.
Ex. Suppose we only have 3 cent and 7 cent stamps. We claim that we can make any cent postage of 12 or more cents. Observe that, for example, knowing we can do 50 cents does not tell us we can do 51 cents! However, we know that if we can do 50 cents we can do 53 cents. Assume we can do $12, \cdots, k$. How can we do $k + 1$? Well, since we can do 12 to k, we know can do $k - 2$. So we just add a 3 cent stamp to $k - 2$. But this only hold if $k - 2 \geq 12$, which is only true if $k \geq 14$. So the inductive step is only valid for $k = 14, 15, 16, \cdots$. So as our base case, we must do 12,13, and 14 as base cases! Thus, for strong induction, you actually would want to do the inductive step first to know how you should setup you base case! In this case we have,

$$12 = 4(\text{3-cent})$$
$$13 = 2(\text{3-cent}) + 1(\text{7-cent})$$
$$14 = 2(\text{7-cent})$$

Thus, by strong induction, we can form any cent postage greater than or equal to 12 with 3 and 7 cent stamps.

1.4 Divisibility

Divisibility underlies much of what is done in number theory.

Definition. Given $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b if there exists $c \in \mathbb{Z}$ such that $ac = b$. When this happens, we say $a \mid b$, otherwise we say $a \nmid b$.
Ex.

- $5 \mid 20$ because $5(4) = 20$.

- $7 \nmid 10$ because $7c \neq 10, \forall c \in \mathbb{Z}$.

Note, we may have $b = 0$. In fact $a \mid 0$ for all a because $a(0) = 0$ for all $a \in \mathbb{Z}$. We don't talk about either $0 \mid b$ nor $0 \nmid b$.

Theorem. If $a \mid b$ and $a \mid c$ then $a \mid (\alpha b + \beta c)$ for any $\alpha, \beta \in \mathbb{Z}$.

Proof. $a \mid b$ so $\exists x \in \mathbb{Z}$ such that $ax = b$. Additionally, $a \mid c$ so $\exists y \in \mathbb{Z}$ such that $ay = c$. Then $\alpha b + \beta c = \alpha(ax) + \beta(ay) = a(\alpha x + \beta y)$. So since $\alpha x + \beta y \in \mathbb{Z}$, we have $a \mid (\alpha b + \beta c)$. $\square$

Theorem. If $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. Since $a \mid b$, there $\exists x \in \mathbb{Z}$ such that $ax = b$. Additionally, $b \mid c$, there $\exists y \in \mathbb{Z}$ such that $by = c$. Then $c = by = axy = a(xy)$. So $a \mid c$. $\square$

The Division Algorithm. If $a, b \in \mathbb{Z}$ and $b > 0$ then $!\exists q, r \in \mathbb{Z}$ with $0 \le r < b$ such that $a = bq + r$.

Proof. First we'll prove that q, r exist. Define the set S as follows,

$$S = \{a - bk \mid k \in \mathbb{Z} \text{ and } a - bk \ge 0\}$$

Then $S \subset \mathbb{Z}^+$, therefore S has a least element. Let r be the least element and q be the k-value which yields it. So $r = a - bq$ is the smallest element in S. Therefore $a = bq + r$. We now need to show $0 \le r < b$.

We know $r \ge 0$ because $r \in S$. Suppose $r \ge b$. Then note $r \ge b$ implies that $r - b \ge 0$. Separately, $r - b < r$ because $b > 0$. Therefore $0 \le r - b = (a - bq) - b = a - b(q + 1)$. Therefore $r - b \in S$, but this means that r is not the least element! This is a contradiction. Therefore $0 \le r < b$.

What remains to be shown is uniqueness. By way of contradiction, assume

$$a = bq_1 + r_1$$

$$a = bq_2 + r_2$$

for $0 \le r_1 < b$ and $0 \le r_2 < b$. Subtracting the equations, we get $0 = b(q_1 - q_2) + (r_1 - r_2)$ which implies $(r_2 - r_1) = b(q_1 - q_2)$. Therefore $b \mid (r_2 - r_1)$ but $-b < r_2 - r_1 < b$. So $r_2 - r_1 = 0$, which means $r_2 = r_1$. Therefore $0 = b(q_1 - q_2)$ which implies $q_1 - q_2 = 0$ because $b > 0$. So $q_1 = q_2$. $\square$

Definition. Suppose $a, b \in \mathbb{Z}$ with at least one nonzero. We define the *greatest common divisor* $\gcd(a, b)$, to be the largest integer dividing both.

Definition. For $a, b \in \mathbb{Z}$, with at least one nonzero. We say that a and b are *relatively prime* (or *coprime*) if $\gcd(a, b) = 1$.

1.5   Problems

---

1. Determine whether each of the following sets is well-ordered. If so, give a proof which relies on the fact that $\mathbb{Z}^+$ is well-ordered. If not, give an example of a subset with no least element.

   (a) $\{a \mid a \in \mathbb{Z}, a > 3\}$
   (b) $\{a \mid a \in \mathbb{Q}, a > 3\}$
   (c) $\{\frac{a}{2} \mid a \in \mathbb{Z}, a \ge 10\}$
   (d) $\{\frac{2}{a} \mid a \in \mathbb{Z}, a > 10\}$

2. Suppose $a, b \in \mathbb{Z}^+$ are unknown. Let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk > 0\}$. Explain why S has a smallest element but no largest element.

3. Use the well-ordering property to show that $\sqrt{5}$ is irrational.

4. Use the identity
$$\frac{1}{k^2 - 1} = \frac{1}{2}\left(\frac{1}{k-1} - \frac{1}{k+1}\right)$$
to evaluate the following:

   (a) $\displaystyle\sum_{k=2}^{10} \frac{1}{k^2-1}$

   (b) $\displaystyle\sum_{k=2}^{n} \frac{1}{k^2-1}$

   (c) $\displaystyle\sum_{k=1}^{n} \frac{1}{k^2+2k}$ Hint: $k^2 + 2k = (???)^2 - 1$

5. Find the value of each of the following:

   (a) $\displaystyle\prod_{j=2}^{7} \left(1 - \frac{1}{j}\right)$

   (b) $\displaystyle\prod_{j=2}^{n} \left(1 - \frac{1}{j}\right)$

   (c) $\displaystyle\prod_{j=2}^{n} \left(1 - \frac{1}{j^2}\right)$ Hint: Be sneaky!

6. Use weak mathematical induction to prove that
$$\sum_{j=1}^{n} j(j+1) = \frac{n(n+1)(n+2)}{3}$$
   for every positive integer n.

7. Use Weak Mathematical Induction to show that $f_n f_{n+2} = f_{n+1}^2 + (-1)^{n+1}$ for all $n \geq 1$.

8. Use weak mathematical induction to show that a $2^n \times 2^n$ chessboard with a corner missing can be tiled with pieces shaped like ⌐ for every integer $n \geq 0$.

9. Define:
$$H_{2^n} = \sum_{j=1}^{2^n} \frac{1}{j}$$
   Use weak mathematical induction to prove that for all $n \geq 1$ we have $H_{2^n} \leq 1 + n$.

10. Use strong mathematical induction to prove that every amount of postage over 53 cents can be formed using 7-cent and 10-cent stamps.