1 Basic Notions

Notation:
\[ \mathbb{N} = \{1, 2, \ldots \}, \quad \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots \} \supset \mathbb{Z}_+ = \{0, 1, 2, \ldots \} = \mathbb{N} \cup \{0\} \]
\[ \mathbb{Q} = \{\text{rational numbers}\} \]
\[ \mathbb{R} = \{\text{real numbers}\} \subset \mathbb{C} = \{\text{complex numbers}\}. \]

Principle of Mathematical Induction (PMI): A statement \( P \) about \( \mathbb{Z}_+ \) is true if

(i) \( P \) holds for \( n = 0 \);

and

(ii) If \( P \) holds for all \( m < n \), then \( P \) holds for \( n \). (*)

Inputs for Number Theory:
- Logic
- Algebra
- Analysis (Advanced Calculus)
- Geometry

A slightly different principle from induction:

Well ordering axiom (WOA): Every non-empty subset of \( \mathbb{Z}_+ \) contains a smallest element.

Note: if \( S \) is finite then WOA is obvious and can be checked. Intuitively, we often apply it to infinite sets; this is accepting the WOA.

Lemma: WOA \( \Rightarrow \) PMI (for \( \mathbb{Z}_+ \)).

Proof: Suppose (*) (i), (ii) hold for some property \( P \).

To show: \( P \) is true for all non-negative integers.

Prove by contradiction. Suppose \( P \) is false. Let \( S \) be the subset of \( \mathbb{Z}_+ \) for which \( P \) is false. Since \( P \) is assumed to be false \( S \) is non-empty. By WOA, \( \exists n \geq 0 \) such that \( n \) is in \( S \), and it is the smallest element of \( S \). If \( n = 0 \), we would get a contradiction by (i). So \( n > 0 \). Since \( n \) is the smallest for which \( P \) is false, it is true for all \( m < n \). By (ii), \( P \) holds for \( n \) as well. Contradiction! So \( P \) holds.

Note: First couple of weeks will be very easy, so use them to learn how to write a proof. (People lose more points on easy problems than hard ones.)
Remark: In fact, PMI and WOA are equivalent. Try to show $\text{PMI} \iff \text{WOA}$.

**Theorem: (Euclidean Algorithm)** Let $a, b$ be integers $\geq 1$. Then we can write $a = bq + r$ with $q, r \in \mathbb{Z}$, $0 \leq r < b$.

Proof: Put $S = \{a - bn|n \in \mathbb{Z}\} \cap \mathbb{Z}_+$. Claim: $S \neq \emptyset$. (Easy) Reason: we can take $n$ negative. So by WOA, $S$ has a smallest element $r$. Since $r \in S$, we can write

$$r = a - bq,$$

for some $q \in \mathbb{Z}$

Since $S \subset \mathbb{Z}_+$, $r \geq 0$. Only thing to check: $r < b$. Suppose $r \geq b$. Then let

$$r' = a - b(q + 1) = r - b \geq 0 \text{ since } r \geq b.$$

Thus $r' \in S$ and $r' < r$, a contradiction.

**Definition:** $b$ divides $a$, written $b \mid a$, iff $a = bq$ for some $q \in \mathbb{Z}$. If not, write $b \notmid a$.

**Definition:** An integer $p > 1$ is **prime** iff the only positive integers dividing $p$ are $1$ and $p$.

**Examples:** $2, 3, 5, 7, 11, 13, \ldots 37, \ldots 691, \ldots$

A positive integer which is not a prime is called a **composite** number.

**Theorem:** Every $n \in \mathbb{N}$ is uniquely written as

$$n = \prod_{i=1}^{r} p_i^{m_i},$$

with each $p_i$ prime and $m_i > 0$.

**Proof of unique factorization:**

**Step 1:** Show that any $n \in \mathbb{N}$ is a product of primes.

Proof: If $n = 1$, OK (empty product $= 1$ by convention). So let $n > 1$. If $n$ is a prime, there is nothing to do. So we may assume that $n$ is composite. This means that $\exists$ prime $p$ such that $p \mid n$. So $n = pq$, some $q \geq 1$. Use induction on $n$. Since $q < n$, by induction $q$ is a product of primes. Hence $n$ is a product of primes.

**Step 2:** **Uniqueness of factorization**

Suppose this is false. By WOA, $\exists$ smallest $n$ for which it is false. Write

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

with $p_i, q_j$ primes, $1 \leq i \leq r$, $1 \leq j \leq s$, $p_i \neq q_j$.
for any \((i, j)\). We may assume \(p_1 \leq p_2 \leq \cdots \leq p_r, q_1 \leq q_2 \leq \cdots \leq q_s\) and \(p_1 < q_1\). Now set \(n' = p_1q_2 \cdots q_s < n\). Since \(p_1\) divides \(n\) and \(n'\), it divides \((n - n')\). We can write

\[ n - n' = p_1\ell_1 \ldots \ell_k \]  

(1)

for some primes \(\ell_1, \ldots, \ell_k\) since \(n - n' < n\) and \(n\) is the smallest counterexample. We can also write

\[ q_1 - p_1 = r_1r_2 \ldots r_t \]  

(2)

for primes \(r_1, \ldots, r_t\). On the other hand, \(n - n' = q_1 \cdots q_s - p_1q_2 \cdots q_s\), i.e., \(n - n' = (q_1 - p_1)q_2 \cdots q_s\). Then

\[ n - n' = r_1r_2 \ldots r_tq_2 \cdots q_s \]  

(3)

Since \(n - n' < n\), and since \(n\) is the smallest counterexample, the two factorizations of \(n - n'\) given by (1) and (3) must coincide.

\[ p_1 \in \{r_1, r_3, \ldots, r_t, q_2, \ldots, q_s\} \]

But \(p_1 \neq q_j\); for any \(j\). Thus

\[ p_1 = r_i, \text{ for some } i. \]

Then \(p_1\) divides \((q_1 - p_1) \Rightarrow p_1 | q_1\), contradiction!

Analysis enters when we ask questions about the number and distribution of primes.

**Theorem.** (Euclid) There exist infinitely many primes in \(\mathbb{Z}\).

**Proof:** Suppose not. Then there exist only a finite number of primes; list them as \(p_1, p_2, \ldots, p_m\). Put \(n = p_1p_2 \ldots p_m + 1\). If \(n\) is prime we get a contradiction since \(n > p_m\). So \(n\) cannot be prime. Let \(q\) be a prime divisor of \(n\). Since \(\{p_1, \ldots, p_m\}\) is the set of all primes, \(q\) must equal \(p_j\); for some \(j\). Then \(q\) divides \(n = p_1 \cdots p_m + 1\) and \(p_1 \cdots p_m \Rightarrow q | 1\), a contradiction.

**Euler’s attempted proof.** (This can be made rigorous!) Let \(P\) be the set of all primes in \(\mathbb{Z}\). **Euler’s idea:** If \(P\) were finite, then \(X = \prod_{p \in P} \frac{1}{(1 - \frac{1}{p})} < \infty.\)
Lemma.

Let $s$ be any real number $> 1$. Then

$$\zeta(s) = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

(called the “Riemann” zeta function, though Euler studied it a century earlier).

Proof of Lemma. Recall: If $|x| < 1$, then $\frac{1}{1-x} = 1 + x + x^2 + \ldots$ (geometric series). If $s > 1$, $\frac{1}{p^s} < 1$. So $\frac{1}{1-p^s} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots$. Then

$$\prod_{p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

by unique factorization.

Euler then argued as follows: let $s \to 1$ from right. $X=\lim_{s \to 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s} \to \sum_{n=1}^{\infty} \frac{1}{n}$, which diverges. But if $P$ is finite, then $X$ is a finite rational number, a contradiction. (To make this rigorous, we need to be careful about limits and uniform convergence.)

The Prime Number Theorem (PNT)

For any $x \geq 2$, put

$$\pi(x) = \#\{p: \text{prime} \mid p \leq x\}.$$

What does $\pi(x)$ look like for $x$ very large? The prime number theorem (PNT) says:

$$\pi(x) \sim \frac{x}{\log x}, \text{ as } x \to \infty$$

In other words, the fraction of integers in $[1, x]$ which are prime is roughly $\frac{1}{\log x}$ for $x$ large. (Can’t prove it in this class.)

Twin Primes These are prime pairs $(p, q)$ with $q = p + 2$.

Examples: $(3, 5), (5, 7), (11, 13), \ldots$

Conjecture: There exist infinitely many twin primes.

Stronger conjecture: If $\pi_2(x)$ denotes the number of twin primes $\leq x$, then

$$\pi_2(x) \sim \frac{x}{(\log x)^2} \text{ as } x \to \infty.$$