Theorems

Theorem (Principle of Mathematical Induction). *Let $P(n)$ be a statement for each integer $n \geq m$. Suppose the following conditions are satisfied,*

1. $P(m)$ is true, and

2. $P(k) \Rightarrow P(k+1)$ for every $k \geq m$.

Then $P(n)$ is true for every $n \geq m$.

Theorem (Another Induction Principle). *Let $P(n)$ be a statement for each integer $n \geq m$. Suppose the following conditions are satisfied,*

1. $P(m)$ amd $P(m+1)$ are true, and

2. If $k \geq m$ and both $P(k)$ and $P(k+1)$ are true then $P(k+2)$ is true.

Then $P(n)$ is true for every $n \geq m$.

Theorem 1.2.1 (The Division Algorithm). *Let $n \in \mathbb{Z}$ and $d \geq 1$ be an integer. Then there exists uniquely determined $q, r \in \mathbb{Z}$ such that*

$$n = qd + r \text{ and } 0 \leq r < d.$$

Theorem 1.2.2 (Bézout's Identity). *Let a and b be integers, not both zero. Then there exist $r, s \in \mathbb{Z}$ such that $\gcd(a, b) = ra + sb$.*

Theorem 1.2.4. *Let $m, n \in \mathbb{Z}$ not both zero. Then*

$$m, n \text{ relatively prime} \Leftrightarrow \exists r, s \in \mathbb{Z} \text{ such that } 1 = rm + sn$$

Theorem 1.2.4. *Let $m, n \in Z$ not both zero. Then*

$$m, n \text{ relatively prime} \Leftrightarrow \exists r, s \in \mathbb{Z} \text{ such that } 1 = rm + sn$$

Theorem (Euclid's Lemma). *Let p be a prime number.*

1. If $p \mid mn$ where $m, n \in \mathbb{Z}$, then $p \mid m$ or $p \mid n$.

2. If $p \mid m_1 m_2 \cdots m_r$ where $m_i \in \mathbb{Z}$ for all i, then $p \mid m_i \; \exists i$.

Theorem 1.2.7 (Prime Factorization Theorem).   *1. Every integer $n \geq 2$ is a product of (one or more) primes.*

2. This factorization is unique (up to order of the factors).
   That is, if
$$n = p_1 p_2 \cdots p_r \text{ and } n = q_1 q_2 \cdots q_2,$$
then $r = s$ and the q_j can be relabeled so that $p_i = q_i$ for $i = 1, 2, \ldots, r$.

Corollary. *Two integers are relatively prime if there exists no prime that divides them both.*

Corollary. *Every $n \in \mathbb{Z}_{\geq 2}$ can be written uniquely as*

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

where the p_i are distinct primes and $n_i \geq 1$ for all i.

Theorem 1.2.8. *Let $n \geq 2$ be an integer with prime factorization*

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

where the p_i are all distinct primes and $n_i \geq 1$ for all i. Then

$$d \mid n \Rightarrow d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \text{ where } 0 \leq d_i \leq n_i \; \forall i.$$

Theorem 1.2.9. *Let $\{a, b, c, \ldots\}$ be a finite set of positive integers and write*

$$
\begin{aligned}
a &= p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \\
b &= p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} \\
c &= p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}
\end{aligned}
$$

where there is an exponent of zero if the prime is not a factor.
Then

$$\gcd(a, b, c, \ldots) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where $k_i = \min(a_i, b_i, c_i, \ldots)$ for each i, and

$$\operatorname{lcm}(a, b, c, \ldots) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

where $m_i = \max(a_i, b_i, c_i, \ldots)$ for each i.

Theorem 1.3.1. *Congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Theorem 1.3.2. *Given $n \geq 2$, $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{n}$.*

Theorem 1.3.4. *Let $n \geq 2$ be a fixed modulus and let a, b and c denote arbitrary integers. Then the following hold in $\mathbb{Z}_n$.*

1. $\bar{a} + \bar{b} = \bar{b} + \bar{a}$ *and* $\bar{a}\bar{b} = \bar{b}\bar{a}$.

2. $\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$ *and* $\bar{a}(\bar{b}\bar{c}) = (\bar{a}\bar{b})\bar{c}$.

3. $\bar{a} + \bar{0} = \bar{a}$ *and* $\bar{a}\bar{1} = \bar{a}$.

4. $\bar{a} + \overline{-a} = \bar{0}$.

5. $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$.

Theorem 1.3.5. *Let $a, n \in \mathbb{Z}$ with $n \geq 2$. Then $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.*

Theorem 1.3.6 (The Chinese Remainder Theorem)**.** *Let m and n be relatively prime integers. If s and t are arbitrary integers, then there is an integer b for which*

$$b \equiv s \pmod{m} \text{ and } b \equiv t \pmod{n}.$$

Theorem 1.3.7. *The following are equivalent for any integer $n \geq 2$.*

    1. *Every element $\bar{a} \neq \bar{0}$ in $\mathbb{Z}_n$ has a multiplicative inverse.*

    2. *If $\bar{a}\bar{b} = \bar{0}$ in $\mathbb{Z}_n$, then either $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$.*

    3. *The integer n is prime.*

Theorem (Wilson's Theorem)**.** *If p is prime then $(p-1)! \equiv -1 \pmod{p}$.*

Theorem 1.3.8 (Fermat's Theorem)**.** *If p is prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Moreover, if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem . *Disjoint cycles commute. That is if σ and τ are disjoint cycles then $\sigma\tau = \tau\sigma$.*

Theorem 1.4.5 (Cycle Decomposition Theorem)**.** *Every $\sigma \in S_n$ with $\sigma \neq \varepsilon$ can be written as a product of disjoint cycles.*

Theorem 1.4.6. *If $n \geq 2$, then every cycle in S_n can be written as a product of transpositions.*

Theorem 1.4.7 (The Parity Theorem)**.** *If a permutation has two factorizations*

$$\sigma = \gamma_n \cdots \gamma_2 \gamma_1 = \mu_m \cdots \mu_s \mu_1,$$

where each of γ_i and μ_j are transpositions, then $m \equiv n \pmod{2}$ (m and n have the same parity).

Definitions

Definition. For $a, b, d \in \mathbb{Z}$:

    • We write $a \mid b$ to mean a *divides* b, which is defined formally as

$$a \mid b \Leftrightarrow b = ak \text{ for some } k \in \mathbb{Z}.$$

    • We say d is *a common divisor of a and b* if $d \mid a$ and $d \mid b$.

    • The *greatest common divisor of a and b* is the largest integer that is a common divisor of a and b. Denote this value by $\gcd(a, b)$.

Definition. Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. We say that a and b are *congruent modulo n* if

$$n \mid (a - b).$$

In that case, we write $a \equiv b \pmod{n}$.

Definition. If $a \in \mathbb{Z}$, then its equivalence class, $[a]$, with respect to congruence modulo n is called its *residue class modulo n* and we write $\bar{a}$ for convenience.

$$\bar{a} = \{x \in \mathbb{Z} | x \equiv a \pmod{n}\}.$$

Definition. The *set of integers modulo n* is denoted $\mathbb{Z}_n$ and is given by

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

Definition. We call an element $\bar{a} \in \mathbb{Z}_n$ *invertible* if there is some $\bar{b} \in \mathbb{Z}_n$ for which $\overline{ab} = \bar{1}$. We call such a $\bar{b}$ an *inverse* of $\bar{a}$.

We call the set of all units, $\mathbb{Z}_n^\times$ the *group of units* in $\mathbb{Z}_n$.

Definition. A *permutation* of $T_n = \{1, 2, \ldots, n\}$ is a mapping $\sigma : T_n \to T_n$ that is both one-to-one and onto (a bijection).

We call the collection of all permutations of T_n the *symmetric group of order n*, and we write

$$S_n := \{\sigma : T_n \to T_n \mid \sigma \text{ is a permutation}\}.$$

Definition. A *permutation* matrix A is an $n \times n$ matrix that has exactly one 1 in each row and column and every other entry is 0.

Definition. The *r-cycle* $(x_1 \ x_2 \ \ldots \ x_r)$ in S_n is the permutation that sends

$$
\begin{aligned}
x_1 &\mapsto x_2 \\
x_2 &\mapsto x_3 \\
x_3 &\mapsto x_4 \\
&\vdots \\
x_{r-1} &\mapsto x_r \\
x_r &\mapsto x_1.
\end{aligned}
$$

Definition. Two cycles $(x_1 \ x_2 \ \ldots \ x_r)$ and $(y_1 \ y_2 \ \ldots \ y_s)$ are *disjoint* if

$$\{x_1, x_2, \ldots, x_r\} \cap \{y_1, y_2, \ldots, y_s\} = \emptyset.$$

Definition. A *transposition* is a cycle of length 2.

Definition. A permutation $\sigma \in S_n$ is called *even* if it can be written as a product of an even number of transpositions.

Similarly, permutations can be called *odd*.

Definition. The *alternation group of degree n* is the set of even permutations in S_n. We call it A_n.

Definition. The *order* of a permutation, $\sigma \in S_n$ is the smallest positive integer k such that $\sigma^k = \varepsilon$.