151 Midterm 3

① Modular Arithmetics.

→ $\forall n \in \mathbb{N}, a, b \in \mathbb{Z}$, $a \equiv b \mod n$

$\Leftrightarrow$ (i) $n \mid a-b$

(ii) a, b leaves the same remainder when divided by n

(iii) $a = b + kn$, $k \in \mathbb{Z}$

→ given $a \equiv b \mod n$, ① $c \equiv d \mod n \Rightarrow a+c \equiv b+d \mod n \wedge ac \equiv bd \mod n$

③ $a^c \equiv b^c \mod n$

→ finding multiplicative inverse of a mod b: $1 = ax + by \Rightarrow ax + \overset{0}{\cancel{by}} \equiv 1 \mod b$

→ Wilson: if p is a positive prime, then $(p-1)! \equiv -1 \mod p$

→ FLT: if p is a positive prime and $a \in \mathbb{Z}$ s.t. $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$

→ Euler: if $n \in \mathbb{N}^+$, $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$

↳ totient function ϕ: # of ints in $[n]$ that are coprime with n

② Finite Sets

→ S is finite if $\exists\, n \in \mathbb{N}$ and a bij $f : [n] \to S$

→ let $f : X \to Y$ if f is inj, $|X| \le |Y|$ and if Y finite, X finite

if f is surj, $|X| \ge |Y|$, and if X finite, Y finite

if f is bij, $|X| = |Y|$

→ X finite $\wedge$ $U \subseteq X \Rightarrow U$ finite.

→ every non-empty finite set of $\mathbb{N}$ has a greatest element.

③ Counting

→ Addition Principle: if a finite set S is partitioned into $S_1, \dots, S_k$, s.t.

1. $\bigcup_{i=1}^{k} S_i = S$ (partition is exhaustive), and
2. $S_i \cap S_j = \emptyset$ for $i \neq j$ (partition is disjoint), then $|S| = \sum_{i=1}^{k} |S_i|$

→ Multiplication Principle: if S consists of k-tuples s.t. the i^{th} coordinate is selected from n_i elements, then $|S| = \prod_{i=1}^{k} n_i$

→ The # of k-tuples chosen ($\bar{c}$ replacement) with each coordinate from $\overset{n\text{ elements}}{\overset{\downarrow}{S}}$ is n^k

↳ equiv. $f: [k] \to S$, $f(i)$ is the i^{th} coordinate.

→ The # of arrangements (w/o replacement) of k from S is $n(n-1)\cdots(n-(k-1)) = \frac{n!}{(n-k)!} = \binom{n}{k} \cdot k!$

↳ equiv: $\overset{\text{func. w/o repeats}}{\text{inj}}$ $f: [k] \to S$ 2-step process: select then permute ↑

→ The # of permutations of S is $n!$ ← arrangement of all n elements.

↳ equiv. bij $f: S \to S$

→ S is a finite set, event $E \subseteq S$. if all outcomes in S are equally likely, then $P(E) = \frac{|E|}{|S|}$

→ Binomial Theorem: $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$