Language of Discrete Math

- Sets $\cup, \cap, \subseteq$
- Logic $\wedge, \vee, \neg, \Rightarrow, \exists, \forall$, De Morgan Laws $\begin{cases} \neg(P \wedge Q) \equiv \neg P \vee \neg Q \\ \neg(P \vee Q) \equiv \neg P \wedge \neg Q \end{cases}$
- Proofs Direct, Contradiction, Contraposition, Cases
- Induction Weak / Strengthened / Strong

Applications

- Stable Matching
  - Improvement Lemma
  - WOP
  - Propose and Reject (always terminates w/ a Stable Matching)
  - Optimality & Pessimality
- Graph Theory
  -

		Start = End
No Repeats	(Simple) path	Cycle
Repeated vertex or Edge	Walk	Tour

 / Eulerian Tours/Walks
  - Special Graphs', Complete Graphs, Trees, Hypercubes
  - Planarity → $3f \leq 2e$; $v+f = e+2$; $v + \frac{2e}{3} \geq e+2$; $e \leq 3v-6$
  - Induction on graph components!
    - Remove / Add Back

Mod Math

Mod Identities

Suppose $a \equiv b \pmod m$ and $c \equiv d \pmod m$

Then:

$a+c \equiv b+d \pmod m$

$a-c \equiv b-d \pmod m$

$ac \equiv bd \pmod m$

$\forall p \quad a^p \equiv b^p \pmod m$

- Residue Classes, Inverses, GCD
- FLT: $a^p \equiv a \pmod p$
- CRT to solve (coprime)

$$\begin{cases} X \equiv a_1 \pmod{n_1} \\ X \equiv a_2 \pmod{n_2} \\ X \equiv a_3 \pmod{n_3} \\ \vdots \\ X \equiv a_k \pmod{n_k} \end{cases}$$

$\Rightarrow$ RSA scheme

Polynomials

Coefficients: $p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_d x^d$

evaluation: $p(x_i) = y_i$

Values: $(x_0, y_0), (x_1, y_1), \ldots, (x_d, y_d)$

Lagrange interpolation

- Secret Sharing
- Erasure Errors (send ntk)
- General Errors (aka corruptions) (send $nt2k$) $\rightarrow$ Berlekamp-Welch

Counting

Combinatorics

- w/ vs. w/o replacement
- order matters vs. doesn't matter
- Strings, Grid-Walks
- Tricks: Symmetry, PIE
- Combinatorial Proofs

k things out of n

w/o replacement, order matters	w/o replacement, order doesn't matter
succession of choices: $n \cdot (n-1) \cdots (n-k+1)$ Permutation: $\frac{n!}{(n-k)!}$	"out of n, choose k" Combination: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
w/ replacement, order matters	**w/ replacement, order doesn't matter**
succession of choices: $\underbrace{n \cdot n \cdot n \cdot n \cdots}_{k \text{ times}} = n^k$	"pick item i x_i times" $x_1 + x_2 + \cdots + x_n = k$ Stars and Bars: $\binom{n+k-1}{k}$

Countability

- Bijections
- Countable: $\mathbb{N}$ $\mathbb{Z}$ $\mathbb{Z}^+$ $\mathbb{Q}$ $\mathbb{N} \times \mathbb{N}$
- Uncountable: $\mathcal{P}(\mathbb{N})$ $\mathbb{R}$ $\Leftrightarrow$ Cantor Diagonalization

A Countable union of countable Sets is Countable