Discrete Math Language of

- Sets U, n, C

- Logic ∧, V, ¬, ⇒, ∃, Y, De Morgan Laws {¬(PNQ) = ¬PN¬Q}

- Proofs Direct, Contradiction, Contraposition, Cases

- Induction Weak / Strengthened / Strong

Applications

- Stable Matching

- Improve ment Lemma

- WOP

- Propose and Reject (always terminates w) a Stable Matchins)

- Optimality & Pessimality

- Graph Theory

			Start = End	
_	No Repeats	(Simple) path	cycle	
	Repeated Vertex or Edge	Walk	Tour	J

Eulerian Tours/Walks

- Special Graphs', Complete Graphs, Trees, Hypercubes

- Planarity

- Induction On graph components! V+ 2e > e+2

- Remove / Add Back

3f \(\) 2e

v+ 2e \(\) 2e+2

e \(\) 3v-6

Mod Math

Mod Identities

Suppose a=b (mod m) and C=d (mod m)

Then:

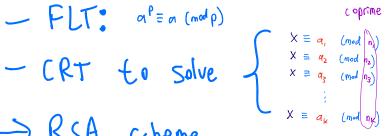
at C = b+d (mod m) a-c= b-d (mod m)

 $ac \equiv bd \pmod{m}$

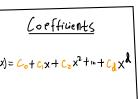
 $\forall \rho \quad \alpha^{\rho} \equiv b^{\rho} \pmod{m}$

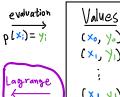
- Residue Classes, Inverses, GCD

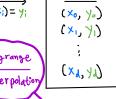
=> RSA scheme



Polynomials







Secret Sharing

- Erasure Errors (Send ntk)
- General Errors
(aka corruptions) (Send nt2k)

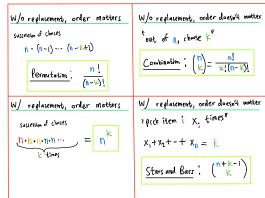
Berlekamp-Welch

(ounting

Combinatorics

- W/ Us, W/o replacement
- order matters us, doesn't matter
- _ Serings, Grid-Walks
- Tricks: Symmetry, PIE
- Combinatorial Proofs

k things out of n



Countability

- Bijections
- Countable;

N Z Z Q

- Uncountable,

P(N) $R \Leftrightarrow Cantor$ Diagonalization

Countable Union of countable Sets is Countable

MXM