Proposition - statement with boolean value; **Propositional Forms** - combining propositions

$P \wedge Q$ - conjunction (and); $P \vee Q$ - disjunction (or); $\neg Q$ - negation (not)

$P \Longrightarrow Q$ - implication (If P, then Q) (equivalent to $\neg P \vee Q$)

Universe - where statement holds true ($\mathbb{N}$ = natural numbers, $\mathbb{Z}$ = integer)

$\neg(\exists x(P(x))) = \forall x(\neg P(x))$; $\neg(\forall x(P(x))) = \exists x(\neg P(x))$ ////

$(\exists x \in N)(\forall y \in N)(x \neq y)$ means there exists x in set. For all y that doesn't equal y in set. (**FALSE**).

-**Direct Proof** of $P \Longrightarrow Q$ - Assume P ... chain of implications ... Therefore Q

-**Contrapositive** of $P \Longrightarrow Q$ - Assume $\neg Q$ ... Therefore $\neg P$... So $P \Longrightarrow Q \equiv \neg Q \Longrightarrow \neg P$

-**Proof by Contradiction** - Assume $\neg P$ ...R ... $\neg R$ (but $R \wedge \neg R$ is false, so $\neg P$ is false) Therefore P

-**Proof by Cases** - prove all the cases must be true, sometimes nonconstructively

a|b - a divides b, b mod a = 0 ***Inference Rules***

modus ponens - $P \wedge (P \Longrightarrow Q) \Longrightarrow Q$ (sufficient); *modus tollens* - $\neg Q \wedge (P \Longrightarrow Q) \Longrightarrow \neg P$ (necessary)

disjunctive elimination - $(P \Longrightarrow Q) \wedge (R \Longrightarrow Q) \wedge (P \vee R) \Longrightarrow Q$; and-elimination - $P \wedge Q \Longrightarrow P$ (or Q)

Induction //(example) - P(k): $0 + 1 + ... + k = k(k+1)(1/2)$ ////**Theorem**: Prove $(\forall x \in \mathbb{N})$ (P(k))

Claim: State. **Base case**: k = 0; **Assume induction hypothesis**: $0 + ... + k = k(k+1)(1/2)$

Induction step: $(0 + ... + k) + (k+1) = (k(k+1)(1/2)) + (k+1) = (k+1)(k+2)(1/2))$ *(true)*

Hence, by the principle of induction, <*claim*>.

simple induction [$P(k) \Longrightarrow P(k+1)$] vs **strong induction** [$P(0) \wedge P(1) \wedge ... \wedge P(k) \Longrightarrow P(k+1)$]

Well Ordering Principle: If $S \subseteq \mathbb{N}$ and $S \neq \varnothing$ then S has a minimal element

(for contradiction proofs) - let **m** be the smallest n for which P(n) is false..P(m-1)=true

Stable Marriage. Propose and Reject - always finds stable pairing (n men + n women):

Each Man proposes to first woman on list; Each Woman: says 'maybe' to best, 'never' to rest of proposals; rejected suitors cross woman off list. ***repeat loop until no rejected suitors***

IMPROVEMENT ***lemma***: If W has M on a string on the kth day, then she will either get him or someone better on a string on each subsequent day. (proof by induction/contradiction)

Sets - Universe U. $B, A \subset U$; $A \equiv \{ x \in U \mid P(x) \}$; $A^C \equiv \{ x \in U \mid \neg P(x) \}$

$A \cup B = \{x \in U \mid x \in A \vee x \in B\} = \{x \in U \mid P(x) \vee Q(x)\}$

$A \cap B = \{x \in U \mid x \in A \wedge x \in B\} = \{x \in U \mid P(x) \wedge Q(x)\}$

Running Time - F(n) = O(g(n)) as n goes to infinity; F(n) is RUNNING TIME eqn (n, n^2, etc)

F(n) exists iff $F(n) \leq Kg(n)$ $\forall n \geq n_0$ (K is worst case scenario). Show $F(n) \leq Kg(n)$ via induction.

"Therefore, F(n) (your running time equation) = O(g(n))."

Euclid algorithm gcd(x,y) ------- if y = 0 then return(x). else return(gcd(y, x mod y))

RSA!!mod arithmetic, p and q are primes; *N = pq*; *message = x mod N; y = E(x) mod N*

Let e be any number that is relatively prime to (p-1)(q-1); e typically is small ~3

Bob's public key = (N, e). //p, q is private. Private key = inverse of [e mod (p-1)(q-1).]

Encryption: $E(x) = x^e \bmod N$. ; **Decryption:** $D(y) = y^d \bmod N$. D(E(x)) = x mod N.

Both E(x) and D(y) are bijections. $x = x^{ed} \bmod N$

Injection: One-to-one. f maps distinct inputs to distinct outputs. $x \neq y \Longrightarrow f(x) \neq f(y)$.

If there is a function $g: B \rightarrow A$, and $(\forall x \in A)(g(f(x)) = x)$; then f must be one-to-one.

Surjection: Onto. Each element in the range has at least one pre-image. $\forall y \, \exists x : f(x) = y$.

Bijections: every element $a \in A$ has unique **image** $b = f(a) \in B$.

every element $b \in B$ has unique **pre-image** $a \in A$: f(a) = B.

If $f: A \rightarrow A$ is one-to-one and A is a finite set, then f is a bijection.

Fermat's Little Theorem: For any prime p and any $a \in \{1,2,...,p-1\}$, $a^{p-1} \equiv 1 \bmod p$. factorial!

Pigeonhole Principle: n elements --> n-1 holes, there must be at least two elements in a hole