Quantifiers

- $\forall x \forall y, P(x,y) \equiv \forall y \forall x, P(x,y)$
- $\exists x \exists y, P(x,y) \equiv \exists y \exists x, P(x,y)$
- $\forall x \exists y, P(x,y) \not\equiv \exists y \forall x, P(x,y)$
  - $\forall x \exists y, P(x,y) \not\Longrightarrow \exists y \forall x, P(x,y)$
  - $\exists y \forall x, P(x,y) \Longrightarrow \forall x \exists y, P(x,y)$
- $\forall x \big(P(x) \wedge Q(x)\big) \equiv \big(\forall x, P(x)\big) \wedge \big(\forall x, Q(x)\big)$
- $\forall x \big(P(x) \vee Q(x)\big) \not\equiv \big(\forall x, P(x)\big) \vee \big(\forall x, Q(x)\big)$
  Let $P(1) = Q(2) = True, P(2) = Q(1) = False$, then LHS $= True$, RHS $= False$.
- $\exists x \big(P(x) \wedge Q(x)\big) \not\equiv \big(\exists x, P(x)\big) \wedge \big(\exists x, Q(x)\big)$
  Let $P(1) = Q(2) = True$, all other cases $= False$, then LHS $= False$, RHS $= True$.
- $\exists x \big(P(x) \vee Q(x)\big) \equiv \big(\exists x, P(x)\big) \vee \big(\exists x, Q(x)\big)$

Note 2

(Direct Proof, Proof by Contraposition, Proof by Contradiction, Proof by Cases)

- Theorem 2.1: For any $a, b, c \in \mathbb{Z}$ if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
- Theorem 2.2. Let $0 < n < 1000$ be an integer. If the sum of the digits of n is divisible by 9, then n is divisible by 9.
- Theorem 2.3 (Converse of Theorem 2.2). Let $0 < n < 1000$ be an integer. If n is divisible by 9, then the sum of the digits of n is divisible by 9.
- Theorem 2.4. Let $n \in \mathbb{Z}^+$ and let $d \mid n$. If n is odd then d is odd.
- Theorem 2.5 (Pigeonhole Principle). Let $n, k \in \mathbb{Z}^+$ be positive integers. Place n objects into k boxes. If $n > k$, then at least one box must contain more than one object.
- Theorem 2.6. There are infinitely many prime numbers.
- Lemma 2.1. Every natural number greater than one is either prime or has a prime divisor.
- Theorem 2.7. $\sqrt{2}$ is irrational.
- Lemma 2.2. If a^2 is even, then a is even.
- Theorem 2.8. There exist irrational numbers x and y such that x^y is rational.

Note 3

(Base Case, Inductive Hypothesis, Inductive Step)

- Theorem 3.1: $\forall n \in \mathbb{N}, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- Theorem 3.2: $(\forall n \in \mathbb{N})\ \big(3 \mid (n^3 - n)\big)$
- Theorem 3.3: Let $P(n)$ denote the statement "Any map with n lines is two-colorable". Then, it holds that $(\forall n \in \mathbb{N})\ \big(P(n)\big)$

- Theorem 3.4: $\forall n \geq 1$, the sum of the first n odd numbers is n^2.
- Theorem 3.5: $(\forall n \geq 1)\ \left(\sum_{i=1}^{n} \frac{1}{i^2} \leq (2 - \frac{1}{n})\right)$
- Theorem 3.6: For every natural number $n \geq 12$, it holds that $n = 4x + 5y$ for some $x, y \in \mathbb{N}$.
- Theorem 3.7: Every natural number $n > 1$ can be written as a product of primes.

Note 4
(Stable Marriage Algorithm)

- Lemma 4.1: The stable marriage algorithm always halts.
- Lemma 4.2 (Improvement Lemma): If man M proposes to woman W on the k^{th} day, then on every subsequent day W has someone on a string whom she likes at least as much as M.
- Definition 4.1 (Well-ordering principle): If $S \subseteq N$ and $S \neq \emptyset$, then S has a smallest element.
- Lemma 4.3: The stable marriage algorithm always terminates with a pairing.
- Theorem 4.1: The pairing produced by the algorithm is always stable.
- Definition 4.2 (Optimal woman for a man): For a given man M, the optimal woman for M is the highest woman on M's preference list that M is paired with in any stable pairing.
- Theorem 4.2: The pairing output by the Stable Marriage algorithm (with relaxed proposal as well) is male optimal, and (Proved in HW:) no two men can have the same optimal partner.
- Theorem 4.3: If a pairing is male optimal, then it is also female pessimal.
- There always exists some woman who receives a single proposal, and she always receives it on the last day of the algorithm. (Proved both in discussion and homework)
- Extra (need proof by induction on exam): The most rejections that can occur on k^{th} day is $n-k$.
- Extra (good as counterexample): Consider rotational preferences, Man $A : 1 > 2 > 3; B : 2 > 3 > 1; C : 3 > 1 > 2$ and Woman $1 : B > C > A; 2 : C > A > B; 3 : A > B > C$, which has 3 stable pairings.

Note 5
(Planar Graph, Tree, Complete Graph, Hypercube)

- path - simple (no repeating vertex)
- cycle - closed path
- walk - path w/ possibly repeating vertex
- tour - closed walk with NO repeating edge
- Eulerian - every edge once
- Hamiltonian - every vertex once
- Theorem 5.1 (Euler's Theorem): An undirected graph $G = (V, E)$ has an Eulerian tour $\iff G$ is even degree, and connected (except possibly for isolated vertices).

Function $EULER(G, s)$:
$T = FINDTOUR(G, s)$;
Let $G_1, ..., G_k$ be the connected components when the edges in T are removed from G, and let s_i be the first vertex in T that intersects G_i;
Output $SPLICE(T, EULER(G_1, s_1), ..., EULER(G_k, s_k))$
end $EULER$

- Theorem 5.2 (Euler's formula): For every connected planar graph, $v + f = e + 2$ ($\equiv e \leq 3v - 6$)
- Theorem 5.3: A graph is non-planar $\iff$ it contains K_5 or $K_{3,3}$.
- (Prove tree properties with induction.) $G = (V, E)$ is a Tree $\iff$:
  1. G is connected and contains no cycles.
  2. G is connected and has $n - 1$ edges (where $n = |V|$ is the number of vertices).
  3. G is connected, and the removal of any single edge disconnects G.
  4. G has no cycles, and the addition of any single edge creates a cycle.
- Theorem 5.4: The statements "G is connected and contains no cycles" and "G is connected and has $n - 1$ edges" are equivalent.
- Lemma 5.1: The total number of edges in an n-dimensional hypercube is $n2^{n-1}$.
- Theorem 5.5: Let $S \subseteq V$ be such that $|S| \subseteq |V - S|$ (i.e., that $|S| \leq 2^{n-1}$), and let E_S denote the set of edges connecting S to $V - S$, (i.e., $E_S := \big\{\{u, v\} \in E \mid (u \in S) \land (v \in V - S)\big\}$). Then, it holds that $|E_S| \geq |S|$.
- $\sum\limits_{v \in V} deg(v) = 2|E|$ (sum of all degrees = twice the number of edges) (Proved earlier in class)
- Extra (Proved in HW): A graph is bipartite $\iff$ it has no tours of odd length, and $\forall n \in \mathbb{Z}^+$, the n-dimensional hypercube is bipartite (so a hypercube has no tours of odd length and can be two-colored).
- Extra (need proof): A graph with k edges has $\geq |V| - k$ connected components.
- Extra (proof by PHP): In any (simple) graph, there are always two vertices of the same degree.
- Extra (need proof): K_n can be vertex colored with n colors.

Note 6, 7

(Modular and FLT)

- Theorem 6.1: If $a \equiv c$ and $b \equiv d \pmod m$, then $(a + b) \equiv (c + d)$ and $(ab) \equiv (cd) \pmod m$
- Theorem 6.2: Let m, x be positive integers such that $\gcd(m, x) = 1$. Then x has a multiplicative inverse, $x^{-1} \pmod m$, and it is unique (mod m).
- Theorem 6.3: Let $x \geq y > 0$. Then $\gcd(x, y) = \gcd(y, x \bmod y)$.
- Theorem 7.2 [Fermat's Little Theorem]: For any prime p and any $a \in \{1, 2, ..., p - 1\}$, we have $a^{p-1} \equiv 1 \pmod p$. (Extra: and so, $a^y = a^{y \pmod{p-1}} \pmod p$)
- Extra (need proof by ???): If $ax + bm = d$, $\gcd(x, m) = d, xu \equiv v \pmod m$, then it has a solution $\iff$ $d \mid v$; if so, one such solution is $u \equiv \frac{va}{d} \pmod{\frac{m}{d}}$, (in essence, $a = (\frac{x}{d})^{-1} \pmod{\frac{m}{d}}$,) and there are exactly d-many solutions (of the form $u = \frac{va}{d} + i \cdot \frac{m}{d} \pmod m$).

- Extra (Proved in HW): If $a \equiv b \pmod{m_1 \wedge m_2}$ and $\gcd(m_1, m_2) = 1$, then $a \equiv b \pmod{m_1 m_2}$.
- Extra (Proved in HW, FLT entended to composite): If $n = p_1 p_2 \cdots p_k$ where p_i are distinct primes and $(p_i - 1) \mid (n - 1)\ \forall i$, then $a^{n-1} \equiv 1 \pmod{n}\ \forall a \in \{i \mid 1 \leq i \leq n \wedge \gcd(n, i) = 1\}$.
- Extra: $(p-1)! \equiv (p-1) \pmod{p}$: Proof by the fact that $2, ..., p-2$ will pair up with their own inverse, and only ones that map back to themselves are $1, -1$.