Final Basic Fact Sheet

You may use, with reference, any of the theorem or definitions given in lecture. Some of these theorems and definitions are below for your reference. **Everything** else must be clearly justified from definitions and appropriate logic.

- **even**: $n \in \mathbb{Z}$ is even $\Leftrightarrow n = 2k$ for some $k \in \mathbb{Z}$.
- **odd**: $n \in \mathbb{Z}$ is odd $\Leftrightarrow n = 2k + 1$ for some $k \in \mathbb{Z}$.
- **divisibility**: For $a, b \in \mathbb{Z}$ with $b \neq 0$, if there exists $k \in \mathbb{Z}$ such that $a = kb$, then we write $b|a$.
- **prime**: If $n \in \mathbb{N}$ with $n \neq 1$ and the only positive divisors of n are 1 and n, then we say n is a prime number.
- **greatest common divisor**: If $a, b \in \mathbb{Z}$ with not both zero, then gcd(a, b)='the largest positive integer that divides both a and b'.
- **congruence**: $x \equiv y \pmod{n}$ if and only if $n|(x - y)$.
- **Triangle Inequality Theorem**: $\forall x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$.
- **AGM Inequality Theorem**: $\forall x, y \in \mathbb{R}$,
  (a) $2xy \leq x^2 + y^2$,
  (b) $xy \leq \left(\frac{x+y}{2}\right)^2$, and
  (c) if $x, y \geq 0$, then $\sqrt{xy} \leq \frac{x+y}{2}$.
- Basic Logic Facts:

Rule	For Logic	For Sets
de Morgan's Law	$\neg(P \wedge Q) = \neg P \vee \neg Q$	$(A \cap B)^c = A^c \cup B^c$
de Morgan's Law	$\neg(P \vee Q) = \neg P \wedge \neg Q$	$(A \cup B)^c = A^c \cap B^c$
Distributive Laws	$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Distributive Laws	$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- **The Binomial Theorem**: For all $\forall x, y \in \mathbb{R}$ and $\forall n \in \mathbb{N}$, $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.
- **Pascal's Identity**: $\forall k, n \in \mathbb{N}$ with $1 \leq k < n$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.
- **Division Algorithm**: If $a, b \in \mathbb{N}$ with $a \geq b > 0$, then there exists $q, r \in \mathbb{N}$ such that $a = qb + r$ with $0 \leq r < b$.
- **Euclidean Algorithm**: Let $a, b \in \mathbb{N}$ with $a \geq b > 0$ and define $r_0 = a$, $r_1 = b$ and $r_i = q_{i+1}r_{i+1} + r_{i+2}$, where $0 \leq r_{i+2} < r_{i+1}$.
  If $r_n \neq 0$ and $r_{n+1} = 0$ for some n, then $\gcd(a, b) = r_n$.
- **Linear Diophantine Equation (LDE) Theorem**: For $a, b, c \in \mathbb{N}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b)|c$.
- **Replacement Theorem**: If $x \equiv y \pmod{n}$ and $w \equiv z \pmod{n}$, then $x + w \equiv y + z \pmod{n}$, $xw \equiv yz \pmod{n}$, and $x^k \equiv y^k \pmod{n}$ for all $k \in \mathbb{N}$.