Proof p -> q:

1 direct: assume p is true, show q is true

2: contraposition: assume q is false, show p is false

3: if and only if: first prove p -> q, then prove q -> p

4: contradiction: assume p is false, find a contradiction that must be false, so p is true

Proof by induction:

Proof Template VII: Induction to prove $\forall n \geq 1 : P(n)$.

Proof. We use induction to prove $\forall n \geq 1 : P(n)$.

1: Show that $P(1)$ is T. (Usually a simple verification.) **[base case]**

2: Show $P(n) \to P(n+1)$ for $n \geq 1$ **[induction step]**

Prove *the implication* using direct proof or contraposition.	
Direct	Contraposition
Assume $P(n)$ is T.	Assume $P(n+1)$ is F.
(valid derivations)	(valid derivations)
must show for any $n \geq 1$	must show for any $n \geq 1$
must use $P(n)$ here	must use $\neg P(n+1)$ here
Show $P(n+1)$ **is** T.	**Show** $P(n)$ **is** F.

3: Conclude: by induction, $\forall n \geq 1 : P(n)$. ■

Recursive definition of Rooted Binary Trees (RBT).

1. *The empty tree ε is an RBT.*
2. *If T_1, T_2 are disjoint RBTs with roots r_1 and r_2, then linking r_1 and r_2 to a new root r gives a new RBT with root r.*

1. A single root-node ● is an RFBT.
2. If T_1, T_2 are disjoint RFBTs with roots r_1 and r_2, then linking r_1 and r_2 to a a new root r gives a new RFBT with root r.

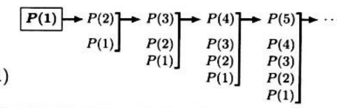
Set

1. *Associative:* $(A \cap B) \cap C = A \cap (B \cap C)$;
$(A \cup B) \cup C = A \cup (B \cup C)$.
2. *Commutative:* $A \cap B = B \cap A$;
$A \cup B = B \cup A$.
3. *Complements:* $\overline{(\overline{A})} = A$;
$\overline{A \cap B} = \overline{A} \cup \overline{B}$;
$\overline{A \cup B} = \overline{A} \cap \overline{B}$.
4. *Distributive:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

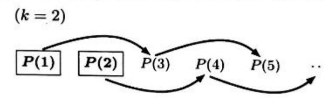
Ordinary (Weak) Induction
Base Case: $P(1)$
Induction: $P(n) \to P(n+1)$

$\boxed{P(1)} \to P(2) \to P(3) \to P(4) \to P(5) \to \cdots$

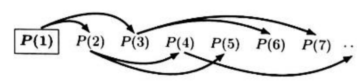
Strong Induction
Base Case: $P(1)$
Induction: $P(1) \wedge \cdots \wedge P(n) \to P(n+1)$



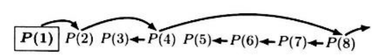
k-Leaping Induction
Base Cases: $P(1), P(2), \ldots, P(k)$
Induction: $P(n) \to P(n+k)$



Exponential Induction
Base Case: $P(1)$
Induction: $P(n) \to P(2n) \wedge P(2n+1)$



Backward Induction
Base Case: $P(1)$
Induction: $P(n) \to P(2n) \wedge P(n-1)$



Sum calculation:

$$\sum_{i=k}^{n} 1 = n+1-k \qquad \sum_{i=1}^{n} i = \tfrac{1}{2}n(n+1) \qquad \sum_{i=0}^{n} 2^i = 2^{n+1}-1$$

$$\sum_{i=1}^{n} f(x) = nf(x) \qquad \sum_{i=1}^{n} i^2 = \tfrac{1}{6}n(n+1)(2n+1) \qquad \sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$$

$$\sum_{i=0}^{n} r^i = \frac{1-r^{n+1}}{1-r} \ (r \neq 1) \qquad \sum_{i=1}^{n} i^3 = \tfrac{1}{4}n^2(n+1)^2 \qquad \sum_{i=1}^{n} \log i = \log n!$$

$\sum_{i=0}^{n} i2^{i+1} = 0 + \sum_{i=1}^{n} i2^{i+1}$

$= (n-1)2^{n+1} + 2$

1. *Associative:* $(p \wedge q) \wedge r \overset{\text{eqv}}{\equiv} p \wedge (q \wedge r)$;
$(p \vee q) \vee r \overset{\text{eqv}}{\equiv} p \vee (q \vee r)$.
2. *Commutative:* $p \wedge q \overset{\text{eqv}}{\equiv} q \wedge p$;
$p \vee q \overset{\text{eqv}}{\equiv} q \vee p$.
3. *Negations:* $\neg(\neg p) \overset{\text{eqv}}{\equiv} p$;
$\neg(p \wedge q) \overset{\text{eqv}}{\equiv} \neg p \vee \neg q$;
$\neg(p \vee q) \overset{\text{eqv}}{\equiv} \neg p \wedge \neg q$.
4. *Distributive:* $p \vee (q \wedge r) \overset{\text{eqv}}{\equiv} (p \vee q) \wedge (p \vee r)$;
$p \wedge (q \vee r) \overset{\text{eqv}}{\equiv} (p \wedge q) \vee (p \wedge r)$.
5. *Implication:* $p \to q \overset{\text{eqv}}{\equiv} \neg q \to \neg p$;
$p \to q \overset{\text{eqv}}{\equiv} \neg p \vee q$.

$$\frac{T(n)}{f(n)} \xrightarrow[n \to \infty]{} \begin{cases} \infty & T \in \omega(f); \\ \text{constant}>0 & T \in \Theta(f); \\ 0 & T \in o(f). \end{cases}$$

(More formally, $T \in \Theta(f)$ if $cf(n) \leq T(n) \leq Cf(n)$.)

$T \in o(f)$	$T \in O(f)$	$T \in \Theta(f)$	$T \in \Omega(f)$	$T \in \omega(f)$
"$T < f$"	"$T \leq f$"	"$T = f$"	"$T \geq f$"	"$T > f$"

Harmonic Sum: $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{i=1}^{n} \frac{1}{i}$. Use $f(x) = 1/x$ to get that

$$H_n = 1 + \sum_{i=2}^{n} \frac{1}{i} \leq 1 + \int_1^n dx\, \frac{1}{x} = 1 + \ln n.$$

Approximation via Integration

Theorem 9.3. Let f be a monotonically increasing function. Then,

$$\boxed{\int_{m-1}^{n} dx\ f(x) \leq \sum_{i=m}^{n} f(i) \leq \int_{m}^{n+1} dx\ f(x).}$$

(If f is monotonically decreasing instead, the inequalities are reversed.)

GCD facts:

(i) $\gcd(m,n) = \gcd(m, \text{rem}(n,m))$.

(ii) Every common divisor of m, n divides $\gcd(m,n)$.

(iii) For $k \in \mathbb{N}$, $\gcd(km, kn) = k \cdot \gcd(m,n)$.

(iv) IF $\gcd(l,m) = 1$ AND $\gcd(l,n) = 1$, THEN $\gcd(l, mn) = 1$.

(v) IF $d|mn$ AND $\gcd(d,m) = 1$, THEN $d|n$.

gcd(6,15)	15-2x6=3
=gcd(3,6)	6-2x(15-2x6)
	= 5x6-2x15=0
=gcd(0,3)	15-2x6-(5x6-2x15)
=3	=3x15-7x6=3

So gcd(6,15)= 3 =3x15-7x6

Modular Equivalence Properties:

$a \equiv b\ (mod\ d)$ and $r \equiv s\ (mod\ d)$

① $ar \equiv bs\ (mod\ d)$

② $a + r \equiv b + s\ (mod\ d)$

③ $a^n \equiv b^n\ (mod\ d)$

the inverse of **k** exists modulo **d** if and only **gcd(k,d)=1**

Big Q is all rational numbers
Big N is all positive integers
Big Z is all integers
E is all positive evens
R is all real numbers

Binomial Distribution. Let $\mathbf{X}$ be the number of successful trials in an experiment with n independent trials, each trial having success probability p; $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$ is a sum of n independent Bernoullis, with $\mathbb{P}[\mathbf{X}_i = 1] = p$. The PDF of $\mathbf{X}$ is a Binomial distribution, $P_{\mathbf{X}}(k) = B(k; n, p)$, where

$$B(k; n, p) = \binom{n}{k} p^k (1-p)^{n-k}.$$

$$b^y = x$$

Then the base b logarithm of x is equal to y:

$$\log_b(x) = y$$

For example when:

$$2^4 = 16$$

Then

$$\log_2(16) = 4$$

$A \subseteq B$	A *is a subset of* B	*Every element of* A *is in* B
$A \subset B$	A *is a proper subset of* B	*Every element of* A *is in* B *and at least* 1 *element of* B *is not in* A
$A = B$	A *is equals to* B	*All elements in* A *are in* B, *same with* B

	No repetition	With repetition
K sequence (order matters)	N!/(n-k)!	N^k
K subset (order does not matter)	$\binom{n}{k}$	$\binom{k+n-1}{n-1}$