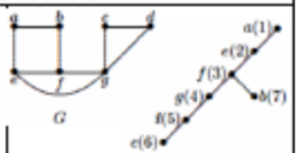
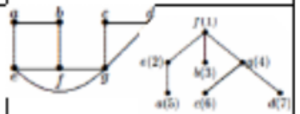
Algorithm	Example

Base b Expansion:
$int[\,]\ baseExpansion(int\ b, int\ n)$ {
int[ ]arr = new int[ ];
int i = 0;
while($n > 0$) {
arr[i]=n Mod b;
$n = \lfloor n/b \rfloor$;
i++;
}
}
	$b=8, n=250$
	
	$250 = 31.8+2$
	$(n=31, a_0=2)$
	$31 = 3.8+7$
	$(n=3, a_1=7)$
	$3 = 0.8+3$
	$(n=0, a_2=3)$

Find b^n Mod m (1) Compute $n = (a_k \ldots a_1 a_0)_2$ (2) Compute $r_k = b^k$ Mod m (3) b^n Mod $m =$ $r_0^{a_0} r_1^{a_1} \ldots r_k^{a_k}$ Mod m	Find 3^{101} Mod 100 (1) $101 = (1100101)_2$ $= 2^6+2^5+2^2+2^0$ $= 64+32+4+1$ $\therefore 3^{101} = 3^{64}3^{32}3^4 3^1$ (2) All congruence modulo 100 $3^2 \equiv 9$ $3^4 \equiv 9^2 \equiv 81$ $3^8 \equiv 81^2 \equiv 61$ $3^{16} \equiv 61^2 \equiv 21$ $3^{32} \equiv 21^2 \equiv 41$ $3^{64} \equiv 41^2 \equiv 81$ (3) $3^{101} \equiv 3^{64}3^{32}3^4 3^1$ $\equiv 81.41.81.3$ $\equiv 3 \pmod{100}$

Euclidean Algorithm
int gcd(int a, int b) {
Int temp ;
while(b != 0) {
$temp = b$;
$b = a \% b$;
$a = temp$;
}
}
	gcd(414,1076)
	
	$1076\ Mod\ 414 = 248$
	$414\ Mod\ 248 = 166$
	$248\ Mod\ 166 = 82$
	$166\ Mod\ 82 = 2$
	$82\ Mod\ 2 = 0$
	By extension,
	if $d = \gcd(a,b) \rightarrow d = as + bt$

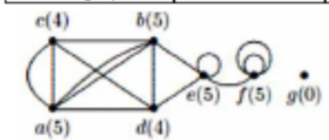
Reverse Euclidean $\gcd(414,1076) = 2 = 166 - 82\cdot 2$ $= 166 - (248-166\cdot 1)\cdot 2$ $= -248\cdot 2 + 166\cdot 3$ $= -248\cdot 2 + (414-248\cdot 1)\cdot 3$ $= 414\cdot 3 - 248\cdot 5$ $= 414\cdot 3 - (1076-414\cdot 2)\cdot 5$ $= 414\cdot 13 - 1076\cdot 5$	
Depth First Search: Spanning Trees (1) Randomly choose one vertex (2) Add its neighbors that has not been searched until the end (3) Backtrack to search unmarked for neighbors	
Breadth First Search (1) Randomly choose one vertex (2) Add in all its adjacent vertices (3) Repeat for all vertices until all vertices are marked	

Vert.	Adj.Vert.
a	bbccd
b	aacde
c	aabd
d	abce
e	bde

Prim's Algorithm (1) Choose any edge with min weight (2) Among adjacent vertices, choose one of minimum weight (3) Stop when we have $n-1$ edges		$bf, ab, if,$
Kruskal's Algorithm (1) Sort all edges in order of increasing weight (2) Select the edges s.t. it joins two distinct components (3) Stop when after $n-1$ edges	*Same as Prim's Algorithm* (1) $bf, cd, kl, ab, cg, fj, bc, ae$, $fg, hl, ij, jk, ef, gh, ei, gk, dh$ (2) Select from the list and reject any that closes a circuit or overlaps	

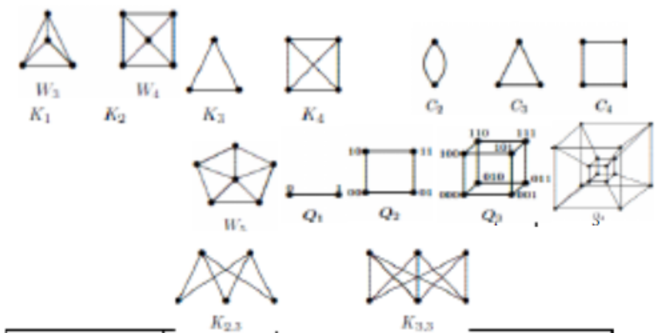
Chapter 7: Graphs

Type	Edges	Multiple Edges?	Loops?
Simple Graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes



a is **ADJACENT** to d
a is **INCIDENT** to edge ab
g is **ISOLATED**
A **LEAF** has degree 1
Degree sum=2×edges

INDEGREE	$deg^-(u)$	Edges with u as terminal vertex



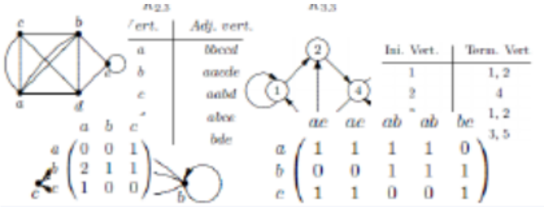
OUTDEGREE	$deg^+(u)$	Edges with u as initial vertex

$|\mathbf{E}(\mathbf{K_n})| = \binom{n}{2}$

COMPLETE BIPARTITE GRAPH denoted $K_{m,n}$, $no.edges = mn$

incidence	ac	ac	ab	ab	bc
a	1	1	1	1	0
b	0	0	1	1	1
c	1	1	0	0	1

LIST

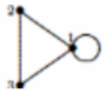


No. of paths from i to j

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} A^2 = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} A^3 = \begin{pmatrix} 7 & 5 & 5 \\ 5 & 3 & 4 \\ 5 & 4 & 3 \end{pmatrix}$$

An **EULER CIRCUIT** is a simple circuit that contains every vertex edge
→ A connected graph has Euler circuit iff every vertex is of even deg

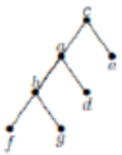
An **EULER PATH** is a simple path which is not a circuit and contains all the edges and vertices → A graph has an Euler path iff it is connected



$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad A^2 = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix} \quad A^3 = \begin{pmatrix} 7 & 5 & 5 \\ 5 & 3 & 4 \\ 5 & 4 & 3 \end{pmatrix}$$

and all vertices, but two, have even degrees.

Chapter 8: Trees - A TREE is a connected graph with **NO** cycles



T_2 With root at c

b and d are **CHILDREN** of a
b and d are **SIBLINGS**
f, g, d, e are **LEAVES**
c, b, a are **INTERNAL VERTICES**
a, c are **ANCESTORS** of d
b, d, f, g are **DESCENDANTS** of a

An m-ary is **FULL** if every internal vertex has exactly m children.

An **ORDERED ROOTED TREE** is a rooted tree in which children of each vertex are ordered. E.g. for T2, the left subtree of c is the subtree rooted at a while the right subtree if a single vertex e

- A tree with $n \geq 2$ vertices has at least two vertices of deg(1)
- A tree with n vertices has $n-1$ edges
- A full m-ary tree ẃ i internal vertex has $n = m\,i + 1$ vertices
- Suppose full m-ary tree with n vertices, i internal vertices and l leaves, then

Chapter 3: The Integers

<u>Divisibility</u>

Write $d \mid n$ if d divides n if $n = dk$ for some $k \in \mathbb{Z}$

if $a \mid b, b \mid c$ ➔ $a \mid c$ if $a \mid b, a \mid c$ ➔ $a \mid mb + nc$

a is Congruent to b *modulo* m if $m \mid (a - b)$

$$a \equiv b \ (mod\ m) \to m \mid (a - b)$$
$$a \equiv b \ (\text{mod } m) \text{ iff } a \text{ Mod m} = b \text{ Mod } m$$

$$\text{if } a \equiv b \ (mod\ m)\ \&\ c \equiv d\ (mod\ m)$$
$$➔\ a + c \equiv b + d\ (mod\ m)\ \&\ ac = bd\ (mod\ m)$$
$$q = n\ Div\ d \qquad r = n\ Mod\ d$$

<u>Prime Numbers and GCD</u>

A positive integer is:

- PRIME if it has exactly 2 +ve divisors, 1 and itself;
- COMPOSITE if it has more than 2 +ve divisors

If n is composite, then it has a divisor d with $1 < d \leq \sqrt{n}$

➔if n does not have a divisor with $1 < d \leq \sqrt{n}$, n is prime

Fundamental Theorem of Arithmetic:

Every +ve integer > 1 has a divisor which is prime

➔ every +ve integer greater than 1 can be written uniquely as a product of primes. E.g. $100 = 2^2 5^5; 999 = 3^3 37$

➔ $\gcd(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \ldots p_n^{\min\{a_n, b_n\}}$

➔ $\operatorname{lcm}(a, b) = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \ldots p_n^{\max\{a_n, b_n\}}$

An integer $\bar{a}$ s.t. $\bar{a}a \equiv 1\ (mod\ m)$ is called an inverse of a modulo m.

The inverse of a modulo m exists iff $\gcd(a, m) = 1$

➔ if c,d are inverses, $c \equiv d\ (mod\ m)$

Chapter 4: Mathematical Induction

Let $P(n)$ be the proposition that …

Basis Step: $P(1)$ is true since…

Inductive Step: Assumer that $P(1), \ldots, P(k)$ are true. Then ….

Working here to prove that $P(k + 1)$ is true

Thus $P(k+1)$ is true.

Therefore, by Mathematical Induction, **proposition** for all **domain**

Chapter 5: Counting

$$P(n, r) = n(n-1) \ldots (n - r + 1) = \frac{n!}{(n-r)!}$$

$$\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!} \cdot \frac{1}{r!} = \binom{n}{n-r}$$

With Repetition:

$$Permu: \frac{n!}{k_1! k_2! \ldots} \qquad Combi: \frac{(r+n-1)!}{r!\,(n-1)!} = \binom{n+r-1}{r}$$

<u>Binomial</u>

$$(a+b)^n = a^n + \binom{n}{1} a^1 b^1 + \cdots + \binom{n}{i} a^{n-i} b^i$$
$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$
$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n} = 0$$
$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$$

Pascal's Identity: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

- Tree with $n \geq 2$ vertices has at least two vertices of degree 1
- Tree with n vertices has $n - 1$ edges ➔ sum of deg$= 2n - 2$
- A full m-ary tree ẃ i internal vertex has $n = mi + 1$ vertices
- Suppose full m-ary tree with n vertices, i internal vertices and l leaves, then

$$n = mi + 1 = \frac{ml - 1}{m - 1}$$
$$i = \frac{n-1}{m} = \frac{l-1}{m-1}$$
$$l = \frac{n(m-1)+1}{m} = i(m-1) + 1$$

- A rooted m-ary tree of height h is **BALANCED** if all leaves are at level h or $h - 1$
- In an m-ary tree there are at most m^k vertices at level k. If the height is h, there are at most m^h leaves.