1, Degree of a vertex (看 vertex 有几个 edges)

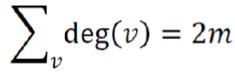
2, Simple path: path such that all its vertices and edges are distinct.

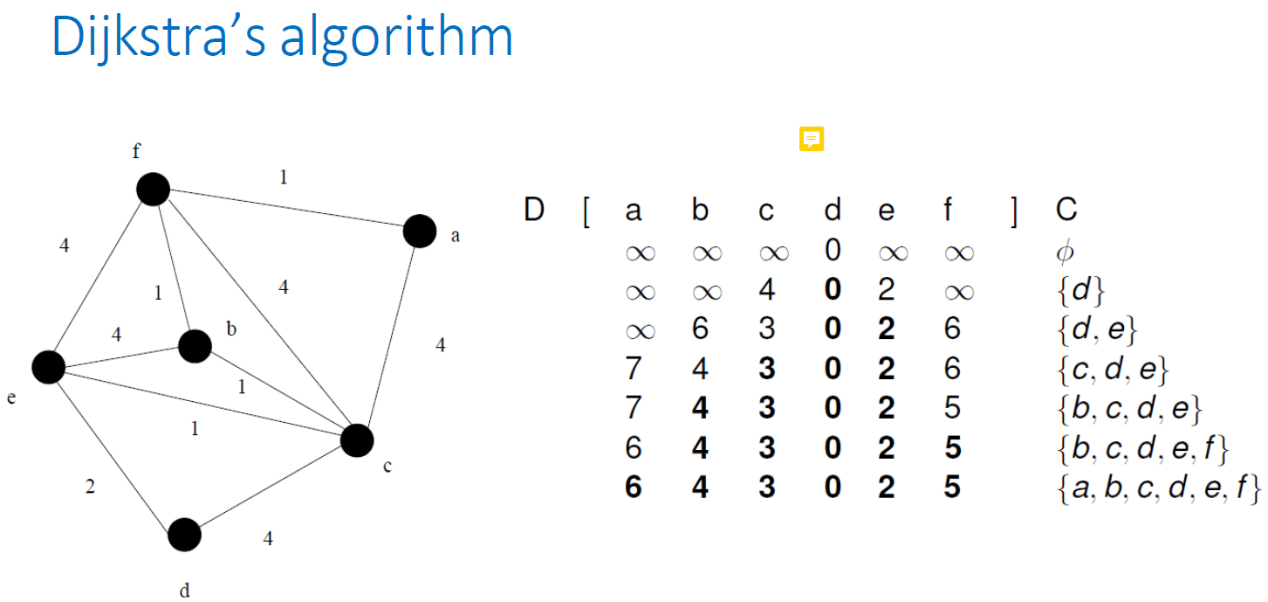
3, A walk in a graph is a sequence of alternating vertices and edges, starting at a vertex and ending at a vertex.

A trail: a walk with no repeated edge.

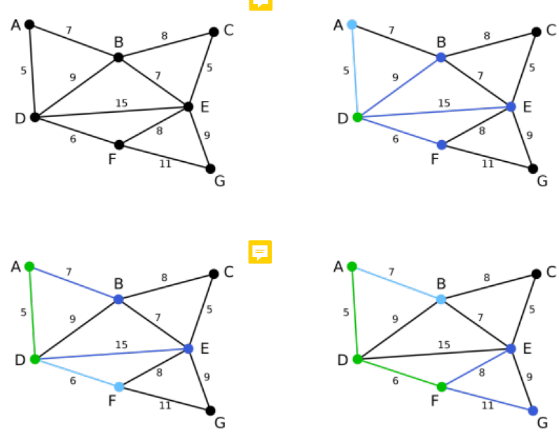
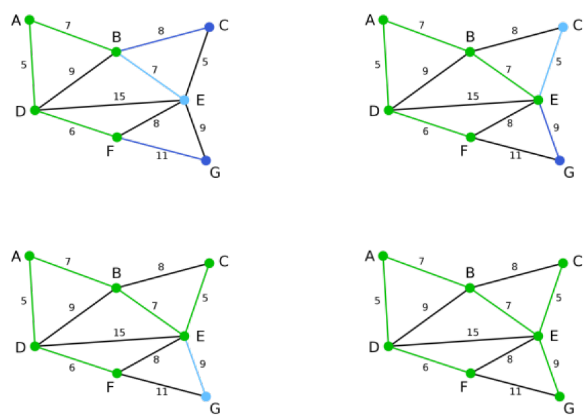
A circuit is a walk with the same start and end vertex.

A cycle is a circuit where each vertex in the circuit is distinct (except for first and last vertex).

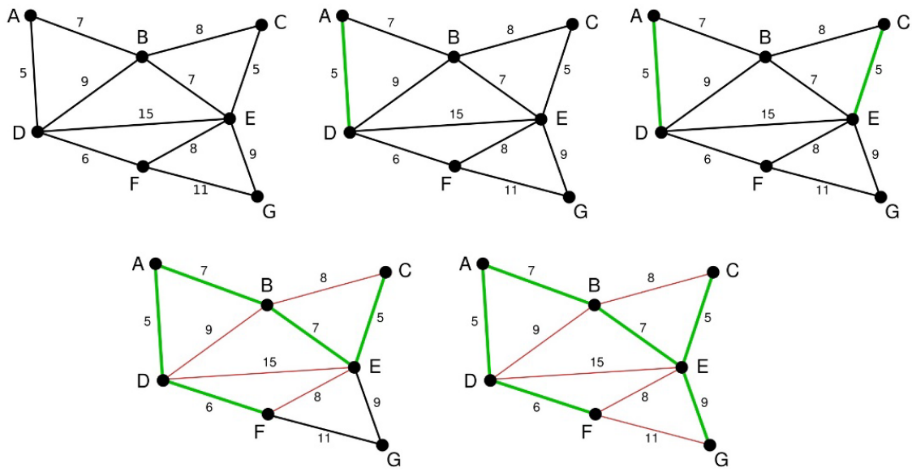
4, 

5, 

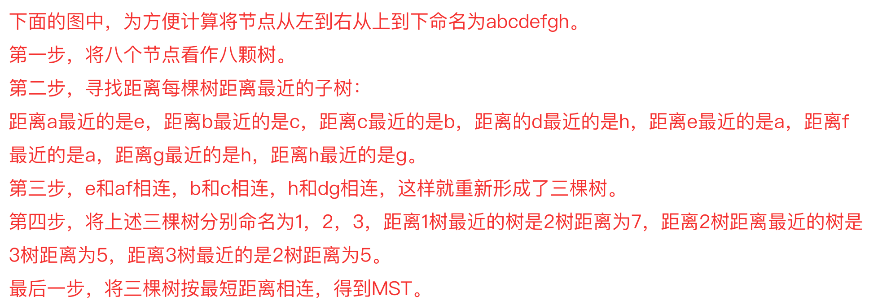
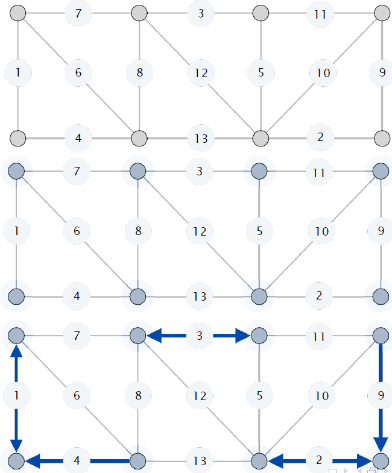
6, Prim’s Algorithm

7, Kruskal’s Algorithm for MST



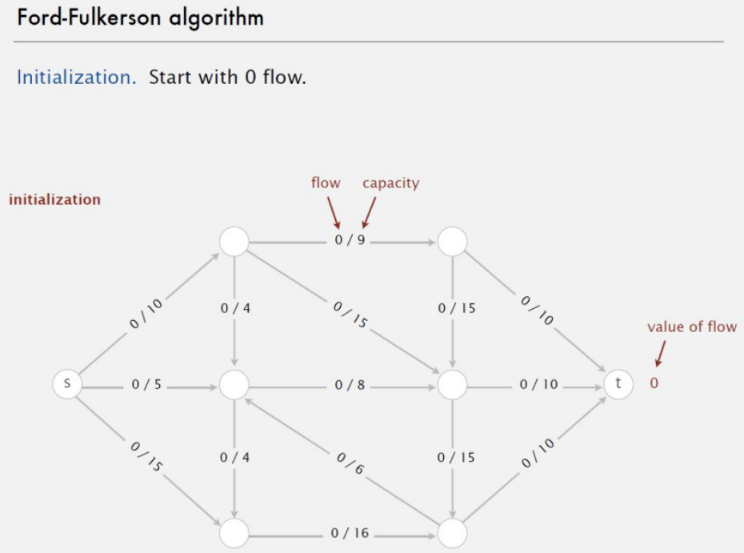
8, Borůvka's algorithm



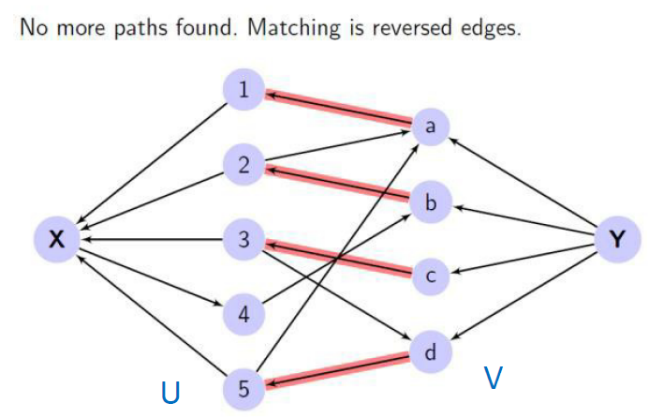
9, Flow f (χ) across a cut χ: total flow of forward edges minus total flow of backward edges

Capacity c(χ) of a cut χ: total capacity of forward edges

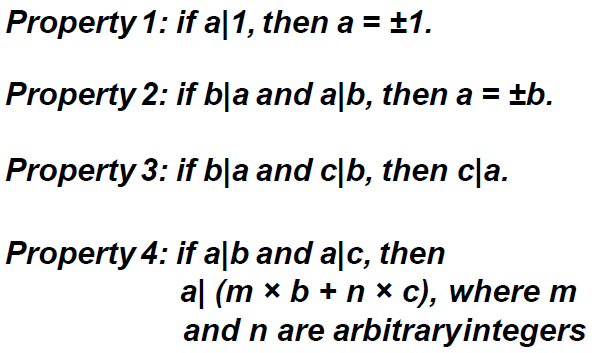
10, The Ford-Fulkerson Algorithm

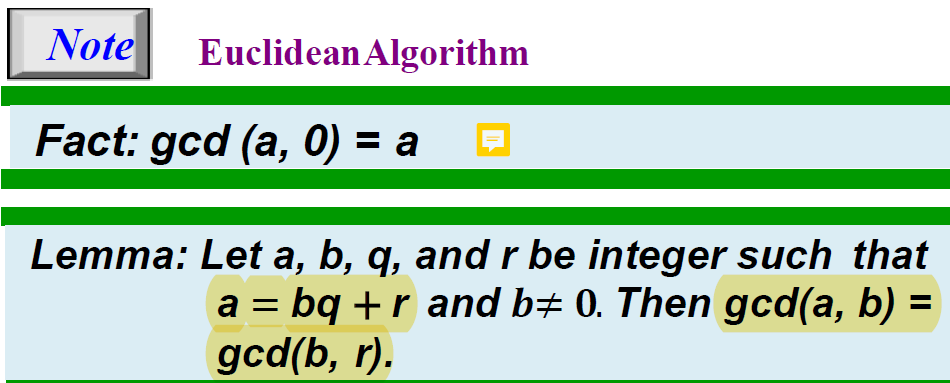


11, Maximum Bipartite Matching

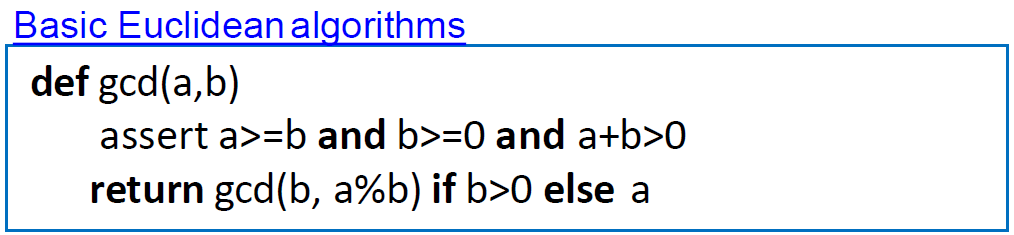


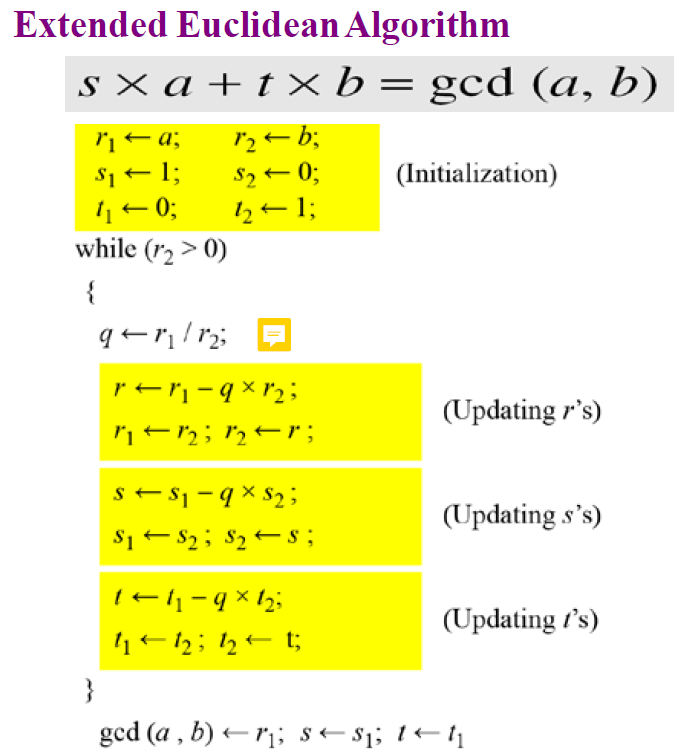
12, 整除：n | a, 不能整除：𝒏∤𝒂

13, 

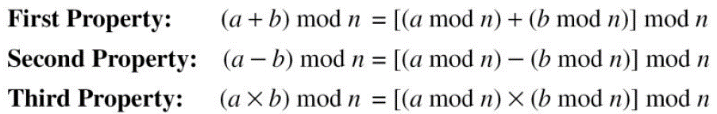
14, 

15, When gcd (a, b) = 1, we say that a and b are relatively prim.

16, 

17, 

18, Zn, Z6 = {0, 1, 2, 3, 4, 5}

19,  

10^n mod x = (10 mode x)^n mod x

20, Inverse:

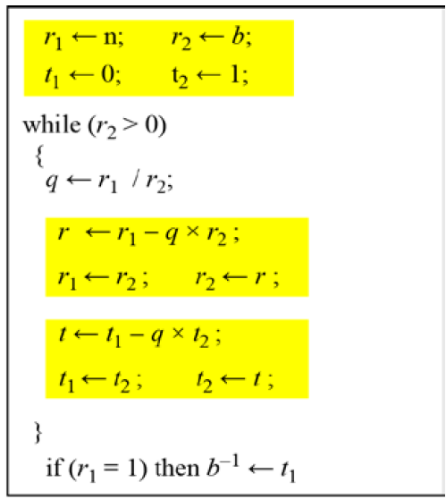
Additive Inverse:

In Zn, two numbers a and b are additive inverses of each other if: a + b ≡ 0 (mod n)

Multiplicative Inverse:

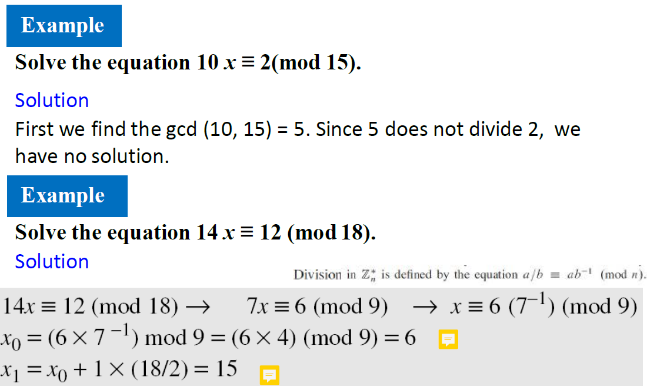
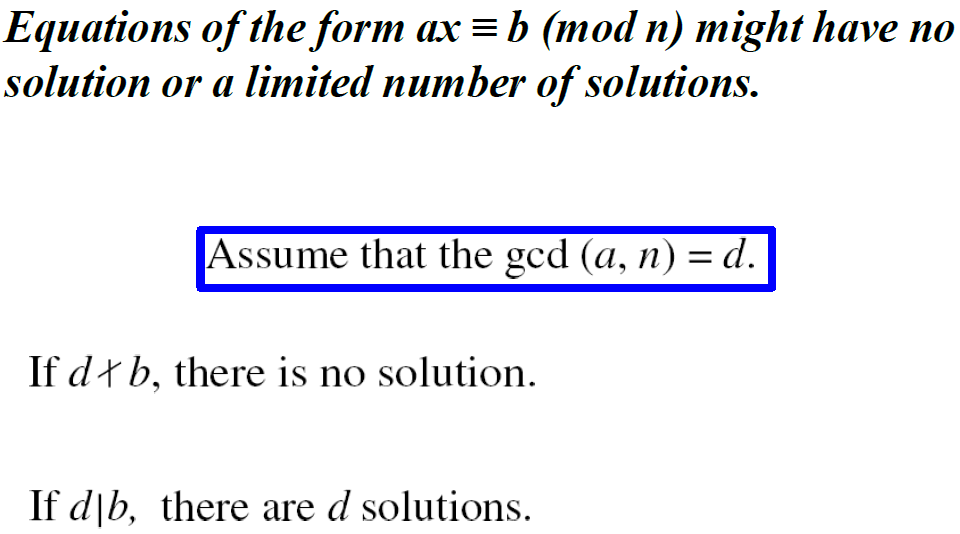
In Zn, two numbers a and b are the multiplicative inverse of each other if: a x b ≡ 1 (mod n), a = b-1

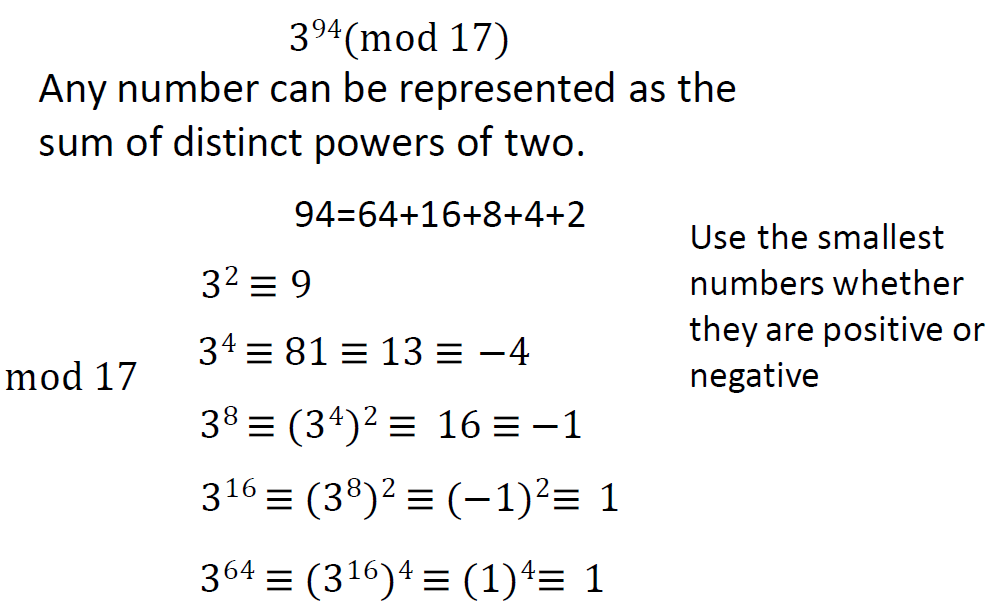
no multiplicative inverse if gcd (10, 8) = 2 ≠ 1.

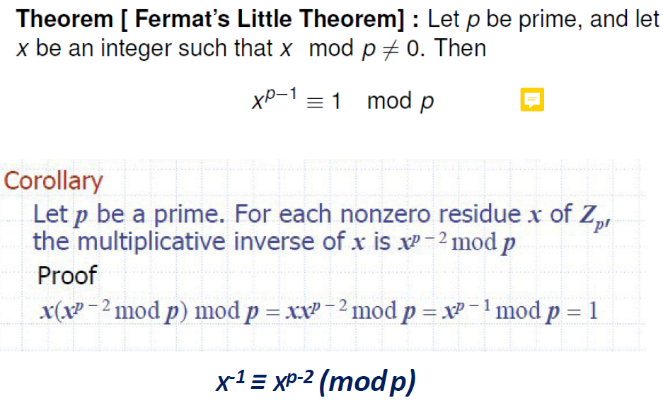
21, 

22, Zn\*: Zn 中所有和 n 互质的数 (gcd(a,n)=1)

23, single-Variable Linear Equations

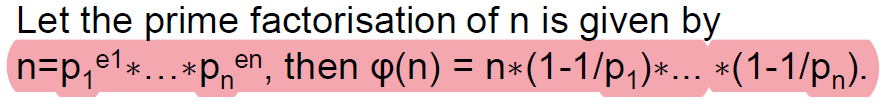


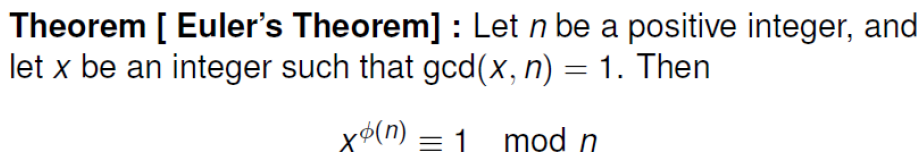
24, 

25, 

26, Euler’s function

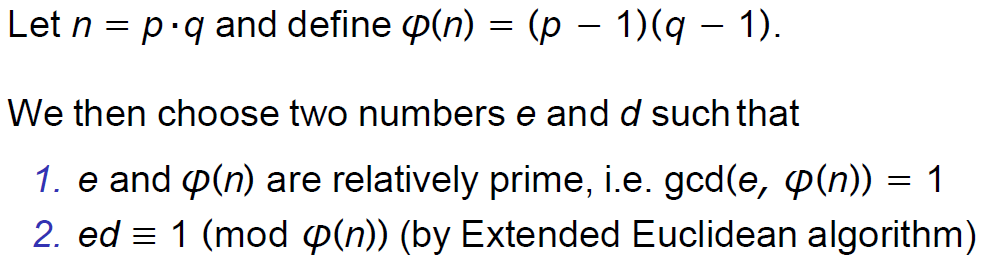
φ(n) 是 Zn\* 的长度

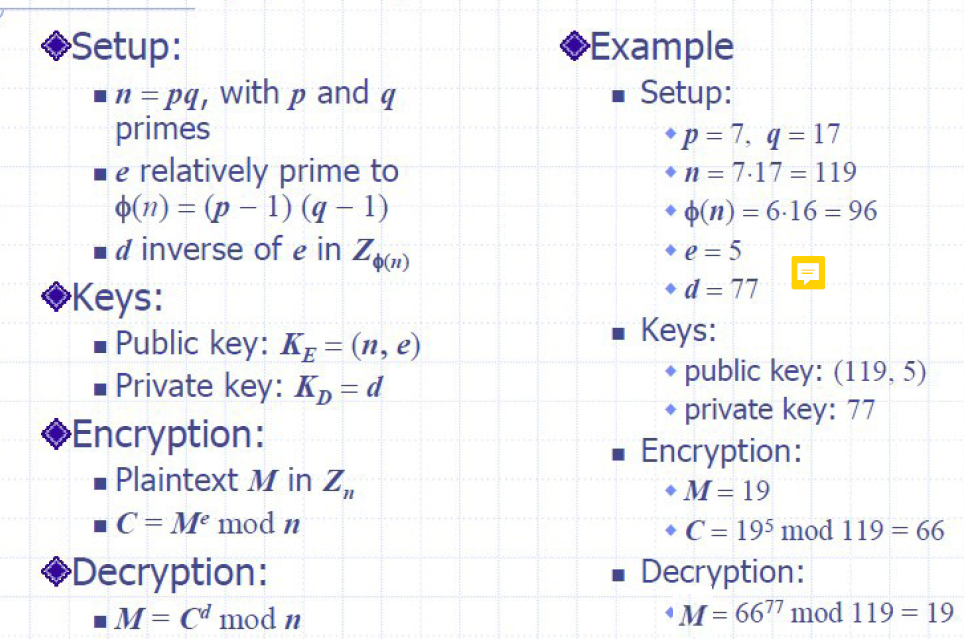




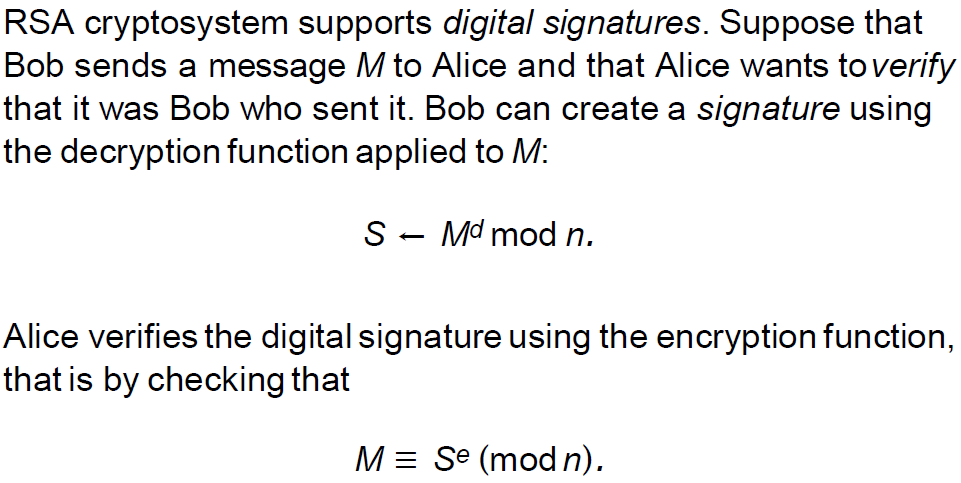
27, plaintext: 明文, ciphertext: 加密文

28, RSA encryption scheme:





29, Digital signatures:



30, NPC 问题：存在这样一个 NP 问题，所有的 NP 问题都可以约化成它。换句话说，只要解决了这个问题，那么所有的NP问题都解决了。

其定义要满足2个条件：

首先，它得是一个NP问题；

然后，所有的NP问题都可以约化到它。

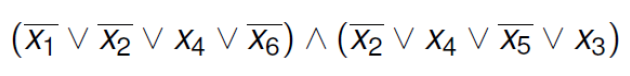
要证明npc问题的思路就是： 先证明它至少是一个NP问题，再证明其中一个已知的NP 问题能约化到它。

31, 如果 L 可以在多项式时间内解出来，并且 L 里的 s 可以通过一个函数 f(s) 转变到 M 里，那么 L 就可以被约化到 M



32, NP-Hard问题是这样一种问题，它满足NPC问题定义的第二条但不一定要满足第一条（就是说，NP-Hard问题要比 NPC问题的范围广，NP-Hard问题没有限定属于NP），即所有的NP问题都能约化到它，但是它不一定是一个NP问题。

33, Conjunctive Normal Form:



3-SAT is CNF-SAT in which each clause has exactly three literals.

34, Approximation Ratios:

T is a k-approximation to the optimal solution OPT if c(T)/c(OPT) ≤ k (assuming a min. problem)

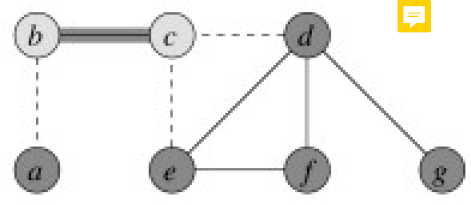
T is a k-approximation to the optimal solution OPT if c(OPT)/c(T) ≤k (assuming a max. problem)

The value of k is never less than 1.

34, Polynomial-Time Approximation Schemes: PTAS 的运行时间必须是 n 的多项式，但是它可以是 ε 的指数。

fully polynomial-time approximation scheme: fully PTAS 的运行时间不但要是是 n 的多项式，也要是 1 / Є 的多项式。

35, Approx-Vertex-Cover:



随便找个边，把两个顶点都加进结果集，将与这两个顶点相连的边都从候选边中移除。

36, Triangle Inequality TSP:

The algorithm finds a minimum spanning tree, and then apply pre-order traversal

