edge: $\sum d_i = 2e \Rightarrow e = \sum d / 2$.

isomorphic: 同构: check the sequence of degrees.

bipartite: 二分体: Assume it is a bipartite.

Then first color one node, then color all nodes which connect to the previous node with another color, until all nodes are colo

Euler path: a simple path that containing all every edge of G.

Euler circuit: a simple circuit that ..... => check if there's node with odd degree, if yes no Euler circuit.

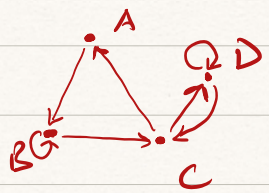
circuit: a path that start & end at a same node

Connected: there is a path between every nodes => no node left unconnected.

it is a path, not an edge!

Adjcency List:

A	B
B	B -> C
C	A -> D
D	C -> D



Simple graph: 1 edge between vertexes

multi graph: allow 2 or more edges between each pair of vertexes

Strongly connected: a directed graph that is connected.

Weakly connected: the underlying undirected graph is connected

Strong component: maximal connected subgraphs in a directed graph.

Weak component: minimal ..... => every vertexes.

a divides b <=> a|b <=> b = ac

a is a factor/divisor of b / b is a multiple of a

$n = d \cdot q + r$

dividend divisor quotient remainder

Sieve of Eratosthenes: removes all multiples except itself till $\sqrt{n}$

Mersenne prime: prime in form of $2^k - 1$.

- $a = b \cdot q_0 + r_0$
- $b = r_0 \cdot q_1 + r_1$
- $r_0 = r_1 \cdot q_2 + r_2$
- $r_1 = r_2 \cdot q_3 + r_3$
- ...
- $r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$ with $r_{k+1} = 0$

Euclidean algorithm: finding gcd

cute theorem: $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

Bézout's Theorem: $\gcd(a,b) = sa + tb$ (Bézout's identity)

Bézout coefficients.

Bézout coeffients can be computed by working backwards Euclid's Algorithm.

- Gcd(135,145)
- 145 = 135·1 + 10
- 135 = 10·13 + 5
- 10 = 5·2 + 0
- Gcd(135,145) = 5

=>

- 5 = 135 – 10·13
- 5 = 135 – (145-135·1)·13
- 5 = 14·135-13·145

Linear congruence: $ax \equiv b \bmod m$.

z is an inverse of x modulo m: $xz \equiv 1 \bmod m$

an inverse of a modulo m exist iff $\gcd(a,m) = 1$

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases} \Rightarrow x \equiv c \bmod mn$$

if Bézout identity $sm+tn=1$ is known, then

$c = (b-a)sm + a = (a-b)tn + b$

RSA cryptosystem: Large prime a, b.

cryptosystem: $\varphi(N) = (a-1)(b-1)$ where $N = ab$

$k = \text{Lcm}(a-1, b-1)$ ← secret

public ↓

pick random int e such that $e \in (1,k)$, $\gcd(e,k) = 1$

let $d \equiv e^{-1} \bmod k$ ($de \,\%\, \varphi = 1$) ← secret

to encrypt message x: $x^e \bmod a.b$

decrypt y: $y^d \bmod a.b$.

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

$n = pq$

1. $\varphi = (p-1)(q-1)$
2. $k = \text{lcm}(p, q)$
3. e. $\gcd(e, k) = 1$
4. d. $de \% \varphi = 1$

en: $x^e \% n$

de: $y^d \% n$.

injective: one-to-one => distinct element in the domain has distinct image

surjective: onto => :77 every element in the codomain has an image

bijective: both injective and surjective

All these properties only applies to a function!