eigenvalue 不一定存在，

ex. $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \Rightarrow$ 特徵多項式

為 $p(x) = x^2+1$，

不具實根，因此 A 不

具有 eigenvalues.

RSA:

1. RSA is built on top of Fermat's little theorem.

2. The two primes p and q chosen initially should be large enough.

3. The encryption key e is co-prime to $(p-1)(q-1)$.

4. The decryption key d is inverse of e modulo $(p-1)(q-1)$

5. encryption key 是 public key.
decryption key 是 private key.

對角化和可逆無關 (不是對稱矩陣不能對角化)

1. 對角化 → 太少 eigenvector → 無法對角化

(方正矩陣才能對角化)

(對稱矩陣必可對角化)

2. 可逆 → λ ~~為~~ 有 0 → 無法可逆

A為方正矩陣 → 可 SVD → $A = U\Sigma V^T$

(對稱矩陣)才可以作(頻譜分解)

$$A = \lambda_1 u_1 u_1^T + \lambda_2 u_2 u_2^T + \cdots + \lambda_n u_n u_n^T.$$

(有獨立的 eigenvectors)

$$\binom{r+s}{n} = \sum_{0\le k\le n}\binom{r}{k}\binom{s}{n-k}$$

⇓

r+s 件裡取 n 件

⇒ 分二堆討論：r 件一堆、s 件一堆

⇒ 討論

1. 在 r 裡挑 0 件，s 裡挑 n 件
2. 〃 1 件 n-1 件

⋮

n. 〃 n 件 〃 0 件

sum rule ⇒ $\sum_{0\le k\le n}\binom{r}{n}\binom{s}{n-k} = \binom{r+s}{n}$

$$\frac{1}{(1-ax)^2} = \sum_{r=0}^{\infty}\binom{2+r-1}{r}(ax)^r$$

$\binom{r+n+1}{n}$ ⇒ 在 r+n+1 裡挑 n 件

⇒ 討論 r+n，1 二堆

A. 不挑 1 的條件下，

在 r+n 裡挑 n 件

⇒ $\binom{r+n}{n}$

B. 挑 1 的條件下，

在 r+n 裡挑 n-1 件

$\binom{r+n}{n-1}$

⇒ sum rule = $\binom{r+n}{n}+\binom{r+n}{n-1}$

$$\sum_{n=2}^{\infty} 2z^n = 2\sum_{n=2}^{\infty} z^n = 2z^2\sum_{n=0}^{\infty} z^n$$

$$2z^2\cdot\frac{1}{1-z}$$

$$\sum_{n=2}^{\infty} 2^{n-2} z^n = \frac{2z^2}{1-z}$$

$\sum_{0\le k\le n}\binom{r+k}{k} = \binom{r+n+1}{n}$，$\sum_{0\le k\le n}\binom{k}{m} = \binom{k+1}{m+1}$

$$\sum_{n=1}^{\infty} nx^n = \frac{x}{(1-x)^2}$$