Name: Muhammad Iaraib Akhtar

Section: BCS-6A

Roll no: 21L-5294

Question 1

$$A = \begin{bmatrix} 3 & 1 & -1 \\ 1 & 2 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

$$|A - \lambda I| = 0$$

$$\begin{vmatrix} 3-\lambda & 1 & -1 \\ 1 & 2-\lambda & 1 \\ -1 & 0 & 1-\lambda \end{vmatrix} = 0$$

$$(3-\lambda)((2-\lambda)(1-\lambda)-(1\times 0)) - 1((1-\lambda)+1) + (-1)((1\times 0)-(-1)(2-\lambda)) = 0$$

$$(3-\lambda)(2-3\lambda+\lambda^2) - 1(2-\lambda) - 1(2-\lambda) = 0$$

$$6 - 11\lambda + 6\lambda^2 - \lambda^3 - (2-\lambda) - (2-\lambda) = 0$$

$$(-\lambda^3 + 6\lambda^2 - 9\lambda + 2) = 0$$

$$\therefore (\lambda - 2)(a\lambda^2 + b\lambda + c) = -\lambda^3 + 6\lambda^2 - 9\lambda + 2$$

$$a\lambda^3 + b\lambda^2 + c\lambda - 2a\lambda^2 - 2b\lambda - 2c = -\lambda^3 + 6\lambda^2 - 9\lambda + 2$$

$$a = -1$$

$$b - 2a = 6$$

$$b + 2 = 6$$

$$b = 4$$

$$c - 2b = -9$$

$$c - 8 = -9$$

$$c = -1$$

$(\lambda-2)(-\lambda^2+4\lambda^*-1)$

$\lambda = 0.26 \qquad \lambda = 3.73 \qquad \lambda = 2$

for $\lambda = 0.26$

$$\left[\begin{array}{ccc|c} 2.74 & 1 & -1 & 0 \\ 1 & 1.74 & 1 & 0 \\ -1 & 0 & 0.74 & 0 \end{array}\right] \quad R_1/2.74$$

$$\left[\begin{array}{ccc|c} 1 & 0.366 & -0.366 & 0 \\ 1 & 1.74 & 1 & 0 \\ -1 & 0 & 0.73 & 0 \end{array}\right] \quad \begin{array}{l} R_2 \leftarrow R_2 - R_1 \\ R_3 \leftarrow R_3 + R_1 \end{array}$$

$$\left[\begin{array}{ccc|c} 1 & 0.366 & -0.366 & 0 \\ 0 & 1.366 & 1.366 & 0 \\ 0 & 0.366 & 0.366 & 0 \end{array}\right] \quad R_2/1.366$$

$$\left[\begin{array}{ccc|c} 1 & 0.366 & -0.366 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0.366 & 0.366 & 0 \end{array}\right] \quad \begin{array}{l} R_1 \leftarrow R_1 - 0.366 \times R_2 \\ R_3 \leftarrow R_3 - 0.366 R_2 \end{array}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & -0.732 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$$V_1 = \begin{bmatrix} 0.732 \\ -1 \\ 1 \end{bmatrix}$$

for $\lambda = 2$

$$\left[\begin{array}{ccc|c} 1 & 1 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 \end{array}\right] \quad \begin{matrix} R_2 - R_1 \\ R_3 + R_1 \end{matrix}$$

$$\left[\begin{array}{ccc|c} 1 & 1 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 1 & -2 & 0 \end{array}\right] \quad R_2 / -1$$

$$\left[\begin{array}{ccc|c} 1 & 1 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 1 & -2 & 0 \end{array}\right] \quad \begin{matrix} R_1 - R_2 \\ R_3 - R_2 \end{matrix}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$x_1 + x_3 = 0$

$x_2 - 2x_3 = 0$

$x_1 = -x_3$

$x_2 = 2x_3$

$$V_2 = \begin{bmatrix} -x_3 \\ 2x_3 \\ x_3 \end{bmatrix} \qquad V_2 = \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix}$$

for $\lambda = 3.73$

$$\left[\begin{array}{ccc|c} -0.73 & 1 & -1 & 0 \\ 1 & -1.73 & 1 & 0 \\ -1 & 0 & -2.73 & 0 \end{array}\right] \quad R_1 \leftrightarrow R_2$$

$$\left[\begin{array}{ccc|c} 1 & -1.73 & 1 & 0 \\ -0.73 & 1 & -1 & 0 \\ -1 & 0 & -2.73 & 0 \end{array}\right] \quad \begin{array}{l} R_2 + 0.73R_1 \\ R_3 + 1R_1 \end{array}$$

$$\left[\begin{array}{ccc|c} 1 & -1.73 & 1 & 0 \\ 0 & -0.26 & -0.26 & 0 \\ 0 & -1.73 & -1.73 & 0 \end{array}\right] \quad R_2 \longleftrightarrow R_3$$

$$\left[\begin{array}{ccc|c} 1 & -1.73 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -0.26 & -0.26 & 0 \end{array}\right] \quad R_2 / -1.73$$

$$\left[\begin{array}{ccc|c} 1 & -1.73 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -0.26 & -0.26 & 0 \end{array}\right] \quad \begin{array}{l} R_1 + 1.73R_2 \\ R_3 + 0.26R_2 \end{array}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & 2.73 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$x_1 + 2.73x_3 = 0$

$x_2 + x_3 = 0$

$x_2 = -x_3$

$x_1 = -2.73x_3$

$x_3 = x_3$

$$V_3 = \begin{bmatrix} -2.73 \\ -1 \\ 1 \end{bmatrix}$$

2. a) $\begin{pmatrix} 7 & 0 \\ 0 & -1 \end{pmatrix}$

$\lambda_1 = 7 \qquad x_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$\lambda_2 = -1 \qquad x_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

(7) Diagonal rule

b) $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 3 \\ 0 & 0 & 5 \end{pmatrix}$

$\lambda_1 = 1 \qquad X_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ (7) Diagonal rule

$\lambda_2 = 2 \qquad X_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ (7) Diagonal rule

$\lambda_3 = 5 \qquad X_3 = ?$ from (7) Diagonal rule

$$\left[\begin{array}{ccc|c} -4 & 0 & 2 & 0 \\ 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \quad R_1/-4$$

$$\left[\begin{array}{ccc|c} 1 & 0 & -\frac{1}{2} & 0 \\ 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \quad R_2/-3$$

$$\left[\begin{array}{ccc|c} 1 & 0 & -1/2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$x_1 = \frac{1}{2}x_3$

$x_2 = x_3$

$x_3 = x_3$

$$X_3 = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}$$

c) $\begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$

$\lambda_1 = 1 \quad X_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ⑦ Diagonal rule

$\lambda_2 = 4 \quad X_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ ⑫ All row have same sum.

3. N=437

1. $x = 2$

2. $\gcd(2, 437) = 1$

3. $2^r \bmod 437 \equiv 1$ ~~gcd(2,~~

$2^{10} \bmod 437 \equiv 150$

$2^{12} \bmod 437 \equiv 163$

$2^{14} \bmod 437 \equiv 215$

3. $3^r \bmod 437 \equiv 1$ $\gcd(3, 437) = 1$

$3^6 \bmod 437 \equiv 292$

$3^8 \bmod 437 \equiv 6$

$3^{10} \bmod 437 \equiv 54$

3. $5^r \bmod 437 \equiv$ ~~188~~ 1 $\gcd(5, 437) = 1$

$5^4 \bmod 437 =$ ~~330~~ 188

$5^6 \bmod 437 \equiv 530$

3. $7^r \bmod 437 \equiv 1$ $\gcd(7, 437) = 1$

$7^4 \bmod 437$ 216

$7^6 \bmod 437$ 96

2. $\gcd(11, 437) = 1$

3. $11^r \bmod 437 \equiv 1$

$11^4 \bmod 437 \equiv 220$

2. $\gcd(13, 437) \equiv 1$

3. $13^r \bmod 437 \equiv$ ~~186~~ 1

$13^4 \bmod 437 \equiv 220$

2. $\gcd(17, 437) = 1$

3. $17^r \bmod 437 = 1$

$17^4 \bmod 437 = 54$

2. gcd(19, 437) = 19

$\frac{437}{19} = 23$

return 19, 23

4. eigen value = λ

eigen vector = $|\psi\rangle$

$U|\psi\rangle = \lambda|\psi\rangle$ (By definition

unitary matrices preserve norm

$\| |\psi\rangle \| = \| U|\psi\rangle \|$

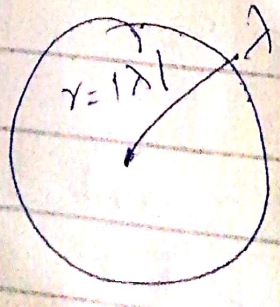
$= \| \lambda |\psi\rangle \|$

$\sqrt{\langle\psi|\psi\rangle} = \sqrt{(\lambda|\psi\rangle)^{+}(\lambda|\psi\rangle)}$

$= \sqrt{\langle\psi|\lambda^{*}\lambda|\psi\rangle}$

$\sqrt{\langle\psi|\psi\rangle} = |\lambda| \sqrt{\langle\psi|\psi\rangle}$

$\therefore |\lambda| = 1$



hence proven.

Question 5

$p = 13 \quad q = 7$

$n = 91$

$\phi(n) = 72$

public key $\quad \gcd(e, \phi(n)) = 1$

$e = 5$

private key d

$de = 1 \bmod \phi(n)$

~~$de \bmod \phi(n) = 1$~~

$de \bmod \phi(n) = 1$

$5 \times 2 \bmod \phi(n) = 7$

$5 \times 21 \bmod \phi(n) = 11$

$5 \times 22 \bmod \phi(n) = 19$

$5 \times 23 \bmod \phi(n) = 43$

$5 \times 24 \bmod \phi(n) = 2$

$5 \times 25 \bmod \phi(n) = 53$

$5 \times 26 \bmod \phi(n) = 29$

$5 \times 27 \bmod \phi(n) = 7$

$5 \times 28 \bmod \phi(n) = 17$

$5 \times 29 \bmod \phi(n) = 1$

$d = 29$

$x = 3$

$3^5 \bmod 91 = 61$

$$61^{29} \bmod 91 = 3$$