Assignment

4)) a) a must be invertible so $\gcd(a, m) = 0$

b can be 0 to m-1.

Total possibilities = $\phi(m) \times m$

b)) Value of

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix}$$ in $\mathbb{F}_{2^8}$

→ Polynomial of max degree 8.

Let $1 = 1$, $2 = x$, $3 = x+1$

This is like Binary $11 = (1011) = x^3 + x + 1$

So calculating the det

$$\Delta = \begin{vmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & 1 & x+1 \\ x+1 & 1 & 1 & x \end{vmatrix}$$

$\Delta = x^3 + x^2 + x + 1 \Rightarrow (1111) = (15)$

5)) $R_0 \equiv \dfrac{\mathbb{Z}_n[x]}{x^2}$

Since x^2 is not irreducible we can't directly use results.

CI → $\Psi(x) \equiv 0$ {obvi}

CII → $\Psi(x) = ax + b$

Note → if I take any higher power of x it will just become 0.

a)) $\Psi(0) = 0 \Rightarrow b = 0$

b)) ONE-ONE $(v_1 + v_1 x) \neq (v_2 + v_2 x)$

Let $\Psi(v_1 + v_1 x) = \Psi(v_2 + v_2 x)$

$a v_1 x + a v_1 x^2 = a v_2 x + a v_2 x^2$

$a v_1 = a v_2 \Rightarrow v_1 = v_2$

if a is invertible

$\gcd(a, n) = 1$

↓

$\phi(n)$ possibilities.

Now $N = pq$

$$\phi(N) = (p-1)(q-1) = pq - p - q + 1$$

this will form a quadratic equation which is solvable.