TUTORIAL-4
COL 759

2019SIY7580
AMAN · BHARDWAJ

Q1 Periodic Sequence S = 011001000111101 of Period n = 15 is a PN-Sequence? Justify.

Soln For a periodic sequence to be a PN Sequence must satisfy :-

(a) In every period no. of 0's ≈ no. of 1's

(b) half the runs have length = 1, one 4th have length = 2 one eighth have length 3 and so on..

(c) Out of Phase autocorrelation is constant.

$$C(\tau) = \frac{A-D}{P}, \quad 0 \le \tau < P$$

Check for above properties to be true -

(a) # 0's = 7 & # 1's = 8

$\Rightarrow$ #0's ≈ #1's ——— (I)

(b) Runs of length 1 = 4
Runs of length 2 = 2
Runs of length 3 = 1
Runs of length 4 = 1
} Total Runs = 8 ——— (II)

(c)

St = 011001000111101	C(0) = 15−0/15 = 1
St+1 = 110010001111010	C(1) = (7−8)/15 = −1/15
St+2 = 100100011110101	C(2) = (7−8)/15 = −1/15
St+3 = 001000111101011	C(3) = (7−8)/15 = −1/15
St+4 = 010001111010110	C(4) = (7−8)/15 = −1/15
St+5 = 100011110101100	C(5) = (7−8)/15 = −1/15
St+6 = 000111101011001	C(6) = (7−8)/15 = −1/15
St+7 = 001111010110010	C(7) = −1/15
St+8 = 011110101100100	C(8) = −1/15

St+9 = 1 1 1 1 0 1 0 1 1 0 0 1 0 0 0

St+10 = 1 1 1 0 1 0 1 1 0 0 1 0 0 0 1

St+11 = 1 1 0 1 0 1 1 0 0 1 0 0 0 1 1

St+12 = 1 0 1 0 1 1 0 0 1 0 0 0 1 1 1

St+13 = 0 1 0 1 1 0 0 1 0 0 0 1 1 1 1

St+14 = 1 0 1 1 0 0 1 0 0 0 1 1 1 1 0

C(9) = (7-8)/15 = -1/15

C(10) = (7-8)/15 = -1/15

C(11) = (7-8)/15 = -1/15

C(12) = (7-8)/15 = -1/15

C(13) = (7-8)/15 = -1/15

C(14) = (7-8)/15 = -1/15

$\Rightarrow$ **C(0) = 1 & C(τ) = $-1/15$ = constant** — (iii)

∴ From (i), (ii) & (iii) Proved that Sequence S is PN Sequence YES

Q2 S-Boxes in AES uses 16 S box in each round are identical. They implement inverse fn in GF(2^8) with mapping $S: \{0,1\}^8 \rightarrow \{0,1\}^8$ so that

$x \in GF(2^8) \rightarrow x^{-1} \in GF(2^8)$

Find total no. of possible mappings.

Solution 2

$S: GF(2^8) \rightarrow GF(2^8)$ can be written as

$$S(x) = x^{2^8-1} a_{2^8-1} + a_{2^8-2} \cdot x^{2^8-2} - - - + a_1 x + a_0$$

It has total 2^8 terms — (i)

Each term can have coeff. a_i: 2^8 Possible values — (ii)

∴ Total no. of Possible mappings over GF(2^8)

$$\underbrace{2^8 \cdot 2^8 \cdot \dots \cdot 2^8}_{2^8 \text{ times}} = (2^8)^{2^8}$$

∴ # Possible mappings = $(2^8)^{2^8}$ Ans

Q3 Man In the Middle Attack on WiFi Network.

- How it is performed ?
- What are its consequences ?
- How to prevent or defeat it ?

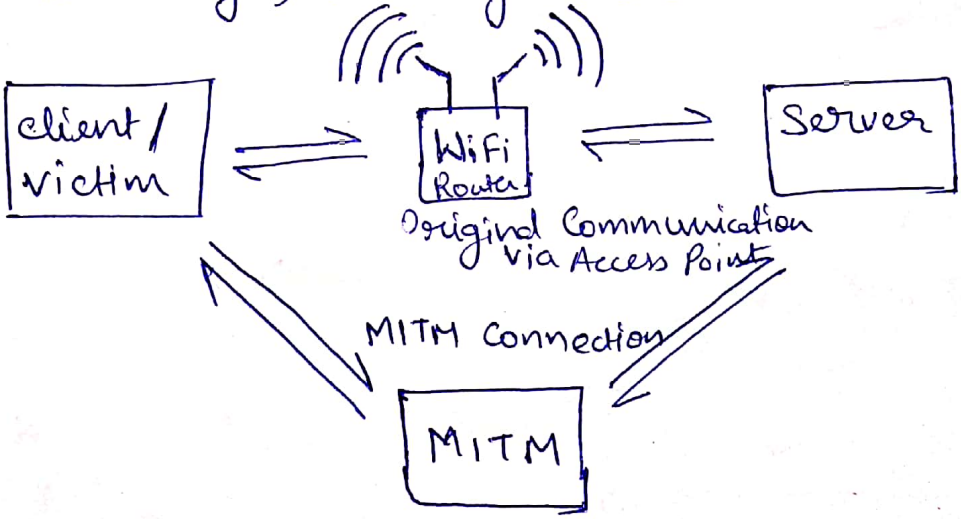
Soln Man In The Middle :-

MITM attack is the one where the attacker secretly captures and relays communication between two parties who believe they are directly communicating with each other.

WiFi Network MITM -

In this, the attacker searches for weakness in the network communication protocols, persuades their hosts that all the traffic should actually go through attacker rather than the regular router.

The captured wifi traffic includes potentially sensitive material such as login credentials, private web browsing, banking details etc.



Next we are going to discuss How this is carried out in wifi Networks.

Contd. on Next Page

How MITM is performed on WiFi Networks.

(A) ARP Spoofing :- Attacker sends Address Resolution Protocol messages onto a local wireless N/w Eg Free WiFi in coffee shops etc.

→ The idea is to convince the end user to update the routing data which enables the attacker to instruct the user's machine that the appropriate MAC address for the given IP address will from now be the MAC address of the attacker machine. This enables attacker to divert all the traffic from the user's machine to his machine.

→ Now the ARP spoofing is done on router, instructing the router to send all the user's data to his machine. Now attacker can monitor all the traffic to and from the user and can store, transmit, change the data and can perform N-number of tasks. Very harmful from user's perspective.

(B) Packet Sniffing :- Applications like wireshark enables to sniff all the packets going through a WiFi router. The data of all the users connected to the router. This may directly reveals login credentials and other sensitive information through unsafe protocols.

Consequences of the above two attacks :-

(a) Leak of Credentials - This may directly reveal login details which are unsecured. Weak encryptions can be broken.

(b) Session Hijacking - By stealing active session's cookie the attacker can replicate any active session on his machine. This can be dangerous for Banking websites.

(c) Private Browsing Data - can be revealed to the attacker

Continued...

(d) User's machine's data - It can be accessed by secretly deploying monitoring tools on the user's machine.

(e) Attack on weakly encrypted data can be done.

(f) There are several network and transport layer attacks which could be carried out after above two attacks. Eg.

- IP hijacking
- Surf Attack
- TCP Flooding
- UDP Flooding
- Malware attack
- FTP Bounce
- DOS - Denial of Service

etc.

How to Prevent/Defeat MITM on WiFi –

(i) Use VPN to secure the connection
(ii) Donot auto connect to public WiFi.
(iii) Disable wifi adapter when not in use.
(iv) While sharing files over wifi encrypt them.
(v) Enable Strong Firewall on your device.
(vi) Beware of any unusual network activity.
(vii) Beware of Pishing URLs.
(viii) Enable HTTPS everywhere in browser to force an SSL connection whenever possible
(ix) Avoid using public WiFi.

Q4 Plain Text Size = 1024 bits. has probability of 0's = 0.7. LFSR has 60% 0's. Find approximate no. of 0's in cipher

Soln P → Plain Text S → LFSR Sequence. C → Cipher Text

$Pr(P_0) = 0.7$ $Pr(P_1) = 0.3$

$Pr(S_0) = 0.6$ $Pr(S_1) = 0.4$

Cipher is produced by P XOR S = C.

Truth Table of XOR.

	P	S	C
(i)	0	0	0
(ii)	0	1	1
(iii)	1	0	1
(iv)	1	1	0

∴ Probability of occuring 0 is given by (i) & (iv)

(i) $0 \oplus 0 = 0$ Put values of Pr

$\Rightarrow 0.7 \times 0.6 = \underline{0.42}$ ①

(iv) $1 \oplus 1 = 0$

$0.3 \times 0.4 = \underline{0.12}$ ②

From ① & ② Total Probability of generating 0's in cipher $Pr(C_0) = 0.42 + 0.12 = \underline{0.54}$

Total Bits in cipher = 1024 bits

∴ Total 0 bits in the cipher

$\Rightarrow Pr(C_0) \times$ Total bits

$\Rightarrow 0.54 \times 1024 = 552.96$

∴ Total Approx 0's = 553 Ans

Q5 Show that any m-sequence is G1-random.

Proof (i) For an LFSR generator - Total possible 2^n tuples $2^n - 1$ are non zero tuples = Period of sequence. Out of these $2^n - 1$ tuples 2^{n-1} starts with 1 and $2^{n-1} - 1$ start with 0's. ∴ the number of 0's and 1's generated by LFSR differ by 1. [Balance Property]

∴ Golumb's Randomness 1st Postulate is satisfied.

(ii) The count of runs of 0's and 1's of length K for $K < n-1$ there are 2^{n-k-2} runs of each 0 & 1

∵ the remaining $n-k-2$ are arbitrary. The total runs of length K is thus 2^{n-k-1}

→ This number halves each time we increase K by 1

⇒ run of 1 of length 1 = $2^n/2$

⇒ " " " " 2 = $2^n/4$ so on [Run Distribution Property]

This fulfills the 2nd Postulate Golumb's Randomness.

(iii) The circular autocorrelation of m-sequence is a Kornecker delta fn. (P) Period ↳ S(K)

$$R(\tau) = \sum_{K=0}^{P-1} (-1)^{S(K)+S(K-\tau)} \qquad \tau = 0, 1, 2 \cdots P-1$$

bit value 1 is assigned $S = +1$ and the bit value 0 is assigned $S = -1$.

∴ $$R(\tau) = \frac{1}{P} \sum_{K=0}^{P-1} S(K) + S(K-\tau)$$

$$R(\tau) = \begin{cases} 1 & \tau = 0 \\ -1/P & 1 \le \tau < P \end{cases}$$ [Correlation Property]

∴ It satisfies Golomb Randomness 3rd Postulate

∴ Above three properties satisfies Golomb's Postulates of Randomness ∴ All m-Seq. are G1-Random Hence Proved

Q6 Prove that out of Phase correlation of m-seq. with Period 2^n-1 is $-1/2^n-1$.

Soln In Q5 we have proved that every m-Sequence is a PN Sequence. ∴ It follows properties of Golom's Randomness — (1)

⇒ Autocorrelation $C(\tau) = \begin{cases} 1 & \tau = 0 \\ \frac{A-D}{P} & 1 \le \tau < P \end{cases}$

⇒ out of Phase autocorrelation for msequence

$$\boxed{C(\tau) = \frac{A-D}{P}} \quad \text{—— (11)}$$

Property 1:- Let S_t = Unshifted PN Sequence and $S_{t+\tau}$ be the shifted PN Sequence.

Shift and Add:- When a PN Sequence is shifted and the shifted PN Sequence is added to unshifted Sequence modulo 2 with XOR. The result is the same PN Sequence with some other shift.

Property 2 - Any PN Sequence S contains 2^{n-1} ones and $2^{n-1}-1$ zeros.

∴ From Property 2 $A = 2^{n-1}$ and $D = 2^{n-1}-1$ — (3!)

Put values in eq (11)

$$C(\tau) = \frac{A-D}{P} = \frac{(2^{n-1}) - (2^{n-1}-1)}{2^n - 1} = \frac{-1}{2^n-1}$$

∴ Out of Phase Autocorrelation of m Sequence

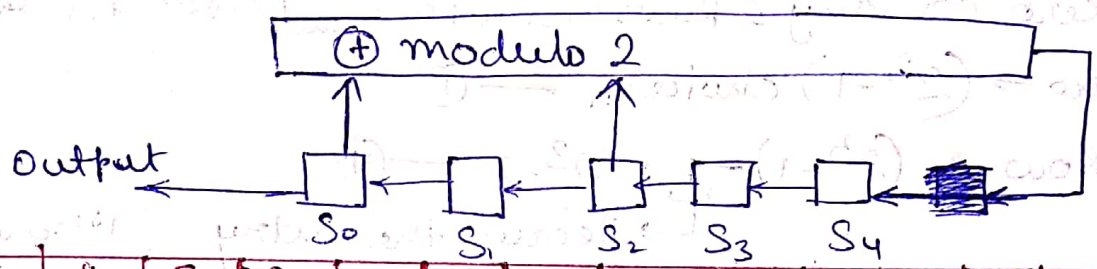
$$\boxed{C(\tau) = \frac{-1}{2^n-1}}$$

Hence Proved

Q7 We wish to construct m sequence of length 31 using Polynomial 45 (octal). Write resulting m-sequence by LSFR with initial sequence (1 0 0 0 0).

Solution Polynomial 45 in octal = (100101) in Binary

∴ Tap connections = $S_0=1$ $S_1=0$ $S_2=1$ $S_3=0$ $S_4=0$



	S_0	S_1	S_2	S_3	S_4	OUT		S_0	S_1	S_2	S_3	S_4	OUT
t=0	0	0	0	0	1		t=16	1	1	0	0	0	1
t=1	0	0	0	1	0	0	t=17	1	0	0	0	1	1
t=2	0	0	1	0	0	0	t=18	0	0	0	1	1	1
t=3	0	1	0	0	1	0	t=19	0	0	1	1	0	0
t=4	1	0	0	1	0	0	t=20	0	1	1	0	1	0
t=5	0	0	1	0	1	1	t=21	1	1	0	1	1	0
t=6	0	1	0	1	1	0	t=22	1	0	1	1	1	1
t=7	1	0	1	1	0	0	t=23	0	1	1	1	0	1
t=8	0	1	1	0	0	1	t=24	1	1	1	0	1	0
t=9	1	1	0	0	1	0	t=25	1	1	0	1	0	1
t=10	1	0	0	1	1	1	t=26	1	0	1	0	1	1
t=11	0	0	1	1	1	1	t=27	0	1	0	1	0	1
t=12	0	1	1	1	1	0	t=28	1	0	1	0	0	0
t=13	1	1	1	1	1	0	t=29	0	1	0	0	0	1
t=14	1	1	1	1	0	1	t=30	1	0	0	0	0	0
t=15	1	1	1	0	0	1	t=31	0	0	0	0	1	1

∴ Resulting m-sequence =

Ans → 0 0 0 0 1 0 0 1 0 1 1 0 0 1 1 1 1 1 0 0 0 1 1 0 1 1 1 0 1 0 1

Q8 Prove for Periodic Sequence with Period P

$$C(\tau) = 1 - \frac{4(K-u)}{P}$$

Soln for Periodic Sequence

$$C(\tau) = \sum_{i=0}^{P-1} \frac{(2S_i - 1)(2S_{i+\tau} - 1)}{P} \quad \text{---(I)}$$

$$= \sum_{i=0}^{P-1} \frac{(4 S_i S_{i+\tau} - 2S_i - 2S_{i+\tau} + 1)}{P}$$

$$= \sum_{i=0}^{P-1} \frac{1}{P} + \sum_{i=0}^{P-1} \frac{(4 S_i S_{i+\tau} - 2S_i - 2S_{i+\tau})}{P} \quad \text{---(II)}$$

given $\Sigma S_i S_{i+\tau} = u$

and $\Sigma S_i = \Sigma S_{i+\tau} = K$ } ---(III)

(we know that $S_i = S_{i+\tau}$ from properties of periodic binary seq.)

Put (III) in (II)

$$= \frac{P}{P} + \frac{(4u - 2K - 2K)}{P}$$

$$= 1 + \frac{(4u - 4K)}{P}$$

$$= 1 - \frac{4(K-u)}{P}$$

$$\Rightarrow \boxed{C(\tau) = 1 - \frac{4(K-u)}{P}}$$

Hence Proved

Q9 Find total possible Affine Block Ciphers.

$C = Am + t$ $\quad A \rightarrow 3\times3$ Matrix (Non singular)
$t \rightarrow$ tuple of 3

Solution

Matrix A → Non Singular Matrix

Each element $\in \{0,1\}$ $\quad A = \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}_{3\times3}$

∴ 2 Possibilities but any row cannot be zero or any 2 Rows cannot be same

∴ Ist Row → (2^3-1) choices — (I)

IInd Row → $(2^3-1)-1 = 2^3-2$ — (II)

↳ Because the entry of 1st row can not be used again.

IIIrd Row → $(2^3-1)-2-1$. we have removed 2 vectors from top 2 rows and 1 more vector as linear comb. of the two — (III)

∴ Total Non Singular 3×3 Matrix A $= (2^3-1)(2^3-2)(2^3-2^2)$

$= 7\times6\times4$

$\boxed{\text{Possibilities of A} = 168}$ — (IV)

t = tuple of 3. each entry can have 2 values $\in \{0,1\}$

$t = \begin{bmatrix} t_0 \\ t_1 \\ t_2 \end{bmatrix}$ $t \in \{0,1\}$

⇒ Possibilities of t

$= 2 \cdot 2 \cdot 2 = \boxed{8}$ — (V)

∴ Total possible Number of Affine Block cipher

$= 168 \times 8$

$= 1344$ Ans

Q10 Find order of P

(a) $P = (0, 16)$ on $y^2 = x^3 + 256$

Formula used :- class slides : Elliptic curve

Slide No :- 8 — (A)

Let $P = (0, 16) \equiv (x, y)$

$\therefore x = 0 \quad y = 16$ and $a = 0$

$2P \equiv (x_1, y_1)$ Put values in formula of $2P$

$\Rightarrow x_1 = \left(\frac{3 \cdot 0 + 0}{2 \cdot 16}\right)^2 - 0 \qquad y_1 = \left(\frac{3 \cdot 0 + 0}{2 \cdot 16}\right)^2 (0 - 0) - 16$

$\boxed{x_1 = 0}$ $\qquad$ $\boxed{y_1 = -16}$

$\Rightarrow 2P = (0, -16)$ — (1)

$3P = P + 2P = (x_3, y_3)$

$\Rightarrow x_3 = \left(\frac{-16 - 16}{0 - 0}\right)^2 - x_1 - x_2 = \infty$

$\therefore y_3 = \infty$

$\Rightarrow \boxed{3P = 0}$ $\qquad$ $\therefore$ $\boxed{\text{order of } P = 3}$ Answer

(b) $P = (1/2, 1/2) \equiv (x_1, y_1)$ on $y^2 = x^3 + (1/4)x$

$2P \equiv (x_3, y_3)$ Put values in formula — (A)

$x_3 = \left(\frac{3/4 + 1/4}{1}\right)^2 - 1/2 \times 2 = 0 \qquad \Rightarrow \boxed{2P = (0, 0)}$

$y_3 = (1)(1/2 - 0) - 1/2 = 0$

Now $4P \equiv (x_3, y_3) = 2(2P)$

$y = \infty$

$\Rightarrow x_3 = \infty$

$\Rightarrow \boxed{4P = 0}$ $\qquad$ $\therefore$ $\boxed{\text{order of } P = 4}$ Ans

(c) $P = (3,8) = (x_1, y_1)$ on $y^3 = x^3 - 43x + 166$

$x_1 = 3 \quad y_1 = 8 \quad a = -43$

$2P = (x_3, y_3)$ Put values in formula

$x_3 = \left(\frac{27-43}{16}\right)^2 - 2 \cdot 3 = 1 - 6 = -5$

$y_3 = (-1)(3-(-5)) - 8 = -16$

$2P = (-5, -16)$ —— (1)

Calculate $4P = (x_3\ y_3) = 2(2P)$

$x_3 = \left(\frac{785 - 43}{-32}\right)^2 + 10 = 11$

$y_3 = (1)(+16) + 16 = 32$

$\Rightarrow 4P = (11, 32)$

calculate $8P = 2(4P)$

$x_3 = \left(\frac{363 - 43}{64}\right)^2 - 22 = (5)^2 - 22 = 3$

$y_3 = (5)(11-3) - 32 = 40 - 32 = 8$

$\Rightarrow 8P = (3,8)$

$\Rightarrow \boxed{7P = O}$ $\therefore \boxed{\text{order} = 7}$ Answer

(d) $P = (0,0) \quad y^2 + y = x^3 - x^2$

$y^2 + y = x^3 - x^2$

$y^2 + y + \frac{1}{4} - \frac{1}{4} = x^3 - x^2 + \frac{x}{3} - \frac{1}{27} + \frac{x}{3} + \frac{1}{27}$

$(y + \frac{1}{2})^2 = (x - \frac{1}{3})^3 - \frac{1}{3}x + c$

$(y')^2 = (x')^3 - \frac{1}{3}(x') + c$

$\therefore Px' = Px + \frac{1}{3} \quad Py' = Py - \frac{1}{2} \Rightarrow P(\frac{1}{3}, -\frac{1}{2}) \quad a = -\frac{1}{3}$

$2P = (x_3, y_3)$

$x_3 = \left(\frac{1}{3} + \left(-\frac{1}{3}\right)\right) - \frac{2}{3} = -\frac{2}{3}$

$y_3 = 0 + \frac{1}{2} = \frac{1}{2}$

$2P = \left(-\frac{2}{3}, \frac{1}{2}\right)$ — ①

$3P = P + 2P = (x_3, y_3)$

$x_3 = \left(\frac{-\frac{1}{2} - \frac{1}{2}}{\frac{2}{3} + \frac{1}{3}}\right)^2 + \frac{1}{3} - \frac{2}{3} = \frac{2}{3}$

$y_3 = (-1)\left(-\frac{1}{3} - \frac{2}{3}\right) - \frac{1}{2} = 1 - \frac{1}{2} = -\frac{1}{2}$

$3P = \left(\frac{2}{3}, -\frac{1}{2}\right)$

$2P = -3P$

$\Rightarrow \boxed{5P = O}$ $\therefore \boxed{\text{order of } P = 5}$ Answer

Next Q on Next Page

Q11 Consider elliptic curve over f_{2^4}

$E: y^2 + xy = x^3 + g^4 x^2 + 1$ $g = (0010)$ generator of F_{2^4}

Primitive Poly $f(x) = x^4 + x + 1$

Soln $g = (0010)$ = generator

Let us find all elements in terms of g of f_{2^4}.

Primitive Poly $x^4 + x + 1$ must satisfy g.

$\Rightarrow g^4 + g + 1 = 0 \Rightarrow g^4 = -(g+1)$ since 2

$$\boxed{g^4 = g + 1} \quad -(1)$$

$F_2 = \{0, 1\}$

$f_{2^4} = \{ ax^3 + bx^2 + cx + d : a, b, c, d \in F_2 \}$ α is gen.

$g^0 = (0001)$

$g^1 = (0010)$

$g^2 = g(g) = g^2 = (0100)$

$g^3 = g(g^2) = g^3 = (1000)$

$g^4 = g(g^3) = g^4 = g + 1 = (0011)$

$g^5 = g(g+1) = g^2 + g = (0110)$

$g^6 = g(g^2+g) = g^3 + g^2 = (1100)$

$g^7 = g(g^3+g^2) = g^4 + g^3 = g^3 + g + 1 = (1011)$

$g^8 = g(g^3+g+1) = (g^4 + g^2 + g) = g^2 + 2g + 1 = (0101)$ (g^2+1)

$g^9 = g(g^2+1) = g^3 + g = (1010)$

$g^{10} = g(g^3+g) = g^4 + g^2 = g^2 + g + 1 = (0111)$

$g^{11} = g(g^2+g+1) = g^3 + g^2 + g = (1110)$

$g^{12} = g(g^3+g^2+g) = g^4 + g^3 + g^2 = (1111)$

$g^{13} = g(g^3+g^2+g+1) = (1101)$

$g^{14} = g(g^3+g^2+1) = (1001)$ (g^3+1)

$g^{15} = (0001)$

Continued on next Page

Now we need to check for the points which satisfy the E.

$E \rightarrow y^2 + xy = x^3 + g^4 x^2 + 1$

(i) $x = 0$ in E

$y^2 + 0 = 0 + 0 + 1 \Rightarrow y^2 = 1 \Rightarrow y = \pm 1 \bmod 2 \Rightarrow \boxed{y = 1}$

$\boxed{(0,1)}$

(ii) $x = g^0 = 1$

E: $y^2 + y = 1 + g^4 + 1 = g^4 = g + 1$ —①

→ Put $y = g^6$

$g^{12} + g^6 = (g^3 + g^2 + g + 1) + (g^3 + g^2) = g + 1 = RHS$

$\Rightarrow \boxed{(g^0, g^6)}$ satisfies

→ Put $y = g^{13}$ in ①

$g^{26} + g^{13} = g^{11} + g^{13} = (g^3 + g^2 + g) + (g^3 + g^2 + 1) = g + 1 = RHS$

$\Rightarrow \boxed{(g^0, g^{13})}$

(iii) $x = g^3$ Put in E

$y^2 + g^3 \cdot y = g^9 + g^{10} + 1$ —②

$RHS = (g^3 + g) + (g^2 + g + 1) + 1 = g^3 + g^2$

→ Put $y = g^8$ in ②

$g^{16} + g^{11} = g + g^{11} = g + g^3 + g^2 + g = g^3 + g^2 = RHS$

$\Rightarrow \boxed{(g^3, g^8)}$

→ Put $y = g^{13}$

$g^{26} + g^{16} = g^{11} + g = g^5 + g^2 = RHS$

$\Rightarrow \boxed{(g^3, g^{13})}$

continued on next Page

(iv) Let $x = g^5$

$RHS = g^{15} + g^{14} + 1 = 1 + g^3 + 1 + 1 = g^3 + 1$

→ Put $y = g^3$

$LHS = g^6 + g^8 = (g^3 + g^2) + (g^2 + 1) = g^3 + 1 = RHS$

$\Rightarrow \boxed{(g^5, g^3)}$

→ Put $y = g^{11}$

$LHS = g^{22} + g^{16} = g^7 + g = (g^3 + g + 1) + g = g^3 + 1 = RHS$

$\Rightarrow \boxed{(g^5, g^{11})}$

(v) Let $x = g^6$

$RHS = g^{18} + g^{10} + 1 = g^3 + g^{10} + 1 = g^3 + (g^2 + g + 1) =$

$= g^3 + g^2 + g + 1 = RHS$

→ $y = g^8$ Put.

$LHS = g^{16} + g^{20} = g + g^5 = g^3 + g^2 + g + 1 = RHS$

$= g^2$

$\Rightarrow \boxed{(g^6, g^8)}$

→ $y = g^{14}$

$LHS = g^{28} + g^{22} = g^{13} + g^7 = (g^3 + g^2 + 1) + (g^3 + g + 1) = g^2 = RHS$

$\Rightarrow \boxed{(g^6, g^{14})}$

(vi) Put $x = g^9$

$RHS = g^{27} + g^{22} + 1 = g^{12} + g^7 + 1 = (g^3 + g^2 + g + 1) + (g^3 + g + 1) = g^2$

→ $y = g^{10}$

$LHS = g^{20} + g^{19} = g^5 + g^4 = (g^2 + g + 1) + (g + 1) = g^2 = RHS$

$\Rightarrow \boxed{(g^9, g^{10})}$

→ $y = g^{13}$

$LHS = g^{26} + g^{22} = g^{11} + g^7 = (g^3 + g^2 + g) + (g^3 + g) = g^2 = RHS$

$\Rightarrow \boxed{(g^9, g^{13})}$

continued on next Page

(vii) Put $x = g^{10}$

$RHS = g^{30} + g^{24} + 1 = g^0 + g^9 + 1 = g^3 + g$

$\rightarrow y = g$

$LHS = g^2 + g^{11} = g^2 + g^3 + g^2 + g = g^3 + g = RHS$

$\Rightarrow \boxed{(g^{10}, g)}$

$\rightarrow$ Put $y = g^8$

$LHS = g^{16} + g^{18} = g + g^3 = RHS$

$\Rightarrow \boxed{(g^{10}, g^8)}$

(viii) Put $x = g^{12}$

$RHS = g^{36} + g^{24} + 1 = g^6 + g^{13} + 1 = (g^3 + g^2) + (g^3 + g^2 + 1) + 1$

$= 0$

$\rightarrow y = 0$ must satisfy

$\Rightarrow \boxed{(g^{12}, 0)}$

$\rightarrow y = g^{12}$

$LHS = g^{24} + g^{24} = g^9 + g^9 = 0$

$\Rightarrow \boxed{(g^{12}, g^{12})}$

$\therefore$ Points satisfying elliptic curve are

$(0, 1)$ (g^3, g^8) (g^3, g^{13}) (g^5, g^3) (g^5, g^{11})

(g^6, g^8) (g^6, g^{14}) (g^9, g^{10}) (g^9, g^{13}) (g^{10}, g)

(g^{10}, g^8) $(g^{12}, 0)$ (g^{12}, g^{12}) (g^0, g^6) (g^0, g^{13})

Total 15 Points satisfy E ——— Ans

END