Es 1 Domanda identica a Es1-Exam020721 con stessi valori

Let $E: y^2 \equiv x^3+2x+2 \mod 17$ an elliptic curve and let $P=(5,1)$ and $Q=(6,3)$ and $R=(x,y)$ such that $P+Q+R=\phi$

Then R is

a) $R=(10,12)$

b) $R=(10,1)$

c) $R=(10,11)$ ✓

d) $R=(10,6)$

Solution: $P+Q=R'=(x_3,y_3)$; $R=-R'=(x_3,-y_3)$

$P(x_1,y_1)+Q(x_2,y_2)=R(x_3,y_3)$

$x_3=\lambda^2-x_1-x_2$

$y_3=-(\lambda x_3+\nu)$

where $\lambda=\frac{y_2-y_1}{x_2-x_1}$ if $P\neq Q$

$\nu=y_1-\lambda x_1$

$\lambda=\frac{3-1}{6-5} \mod 17 = 2\cdot 1^{-1} \mod 17 \equiv 2$

$\nu = 1-2\times 5 \equiv 8$

$x_3 = 2^2-5-6 = 4-5-6 = -7 \equiv 10 \mod 17$

$y_3 = -(2\times 10+8) = -(11) \equiv 6 \mod 17$

$R'=(10,6)$

$R=(10,-6)=(10,11)$

Es 2

Let $f: \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$ be the isomorphism of CRT, then

a) $f(x,y) = 7x + 9y$

b) $f(x,y) = 6x + 10y$

c) $f(x,y) = 10x + 6y$ ✓

d) $f(x,y) = 12x + 4y$

Solution:

CRT: Assume n_1, n_2 coprime, i.e $\gcd(n_1, n_2) = 1$. Let x be the solution to the following systems of modulo identities

$x \equiv a_1 \bmod n_1$
$x \equiv a_2 \bmod n_2$

Then $x = (X_2 n_2 a_1 + X_1 n_1 a_2) \bmod N$, where $N = n_1 \times n_2$ and $X_1 n_1 + X_2 n_2 = 1$

$\Rightarrow$ bijection between $\mathbb{Z}_p \times \mathbb{Z}_q$

$\left.\begin{matrix} n_1 = 3 \\ n_2 = 5 \end{matrix}\right\} N = 15$

Example : $9 \bmod 15 \Rightarrow (0,4)$

$\mathbb{Z}_{15} = \underset{x}{\mathbb{Z}_3} \times \underset{y}{\mathbb{Z}_5}$

$7 \times 0 + 9 \times 4 = 36 \equiv 6 \bmod 15$ NO
$6 \times 0 + 10 \times 4 = 40 \equiv 10 \bmod 15$ NO

$10x + 6y = 24 \equiv 9 \bmod 15$

Another method

$f(a,b) = a f(1,0) + b f(0,1)$ Linear Combination

$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 0 \bmod 5 \end{cases}$

If $x \equiv 0 \bmod 5$, then $x = 5y$

$5y \equiv 1 \bmod 3$

$\Rightarrow y = 5^{-1} \bmod 3 = 2$

$x = 5y = 10$

Es 2

Let $f: \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$ be the isomorphism of CRT, then

a) $f(x,y) = 7x + 9y$

b) $f(x,y) = 6x + 10y$

c) $f(x,y) = 10x + 6y$ ✓

d) $f(x,y) = 12x + 4y$

Solution:

$\mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$ $\Rightarrow f(a,b) = af(1,0) + bf(0,1)$

$\mathbb{Z}_3$ (x)	$\mathbb{Z}_5$ (y)	$\mathbb{Z}_{15}$
0	0	0
1	1	1
2	2	2
0	3	3
1	4	4
2	0	5
0	1	6 $\leftarrow$ b $\to f(0,1)$
1	2	7
2	3	8
0	4	9
1	0	10 $\leftarrow$ a $\to f(1,0)$
2	1	11
0	2	12
1	3	13
2	4	14

$\to 10x + 6y$

See other possible methods at Exam 03072020, Exercise 2

Exercise 3

Let $Enc^1_k(P) = k \oplus P$ be the Vernam or XOR cipher of 3-bit blocks.
Let $Enc^2_k(P) = k \boxtimes P$ be the multiplication cipher modulo $8 = 2^3$ where k, P are the binary expression of elements of $\mathbb{Z}_8$ i.e. [011] is 3.

Let

$$Enc_k(P) = Enc^2_{k2}(Enc^1_{k1}(P))$$

be the 3-bit double-encryption.

Knowing that $Enc_k(3) = 4$ and $Enc_k(4) = 7$

find the pair $(k2, k1)$.

$$\begin{cases} (3 \oplus K_1) \boxtimes K_2 = 4 \pmod 8 \\ (4 \oplus K_1) \boxtimes K_2 = 7 \pmod 8 \end{cases} \quad \begin{cases} 3 \boxtimes K_2 \oplus K_1 \boxtimes K_2 = 4 \\ 4 \boxtimes K_2 \oplus K_1 \boxtimes K_2 = 7 \end{cases}$$

$$\begin{cases} K_1 \boxtimes K_2 = 4 \oplus 3 \boxtimes K_2 \\ K_1 \boxtimes K_2 = 7 \oplus 4 \boxtimes K_2 \end{cases} \Rightarrow 4 \oplus 3 \boxtimes K_2 = 7 \oplus 4 \boxtimes K_2 \Rightarrow$$

$$\Rightarrow \underbrace{7 \oplus 4}_{3} \oplus 3 \boxtimes K_2 = 4 \boxtimes K_2 \Rightarrow 3 \oplus 3 \boxtimes K_2 = 4 \boxtimes K_2$$

$$\Rightarrow 3 \oplus 3 \boxtimes K_2 \oplus 4 \boxtimes K_2 = 0 \Rightarrow 3 \oplus K_2 \boxtimes \overbrace{(3 \oplus 4)}^{7} = 0$$

$$\Rightarrow 3 \oplus K_2 \boxtimes 7 = 0 \Rightarrow 7 \boxtimes K_2 = 3 \Rightarrow K_2 = 3 \boxtimes 7^{-1}$$

$$\Rightarrow K_2 = 3 \boxtimes 7 = 5 \pmod 8$$

$$(3 \oplus K_1) \boxtimes 5 = 4 \pmod 8$$

$$\underbrace{3 \boxtimes 5}_{7} \oplus K_1 \boxtimes 5 = 4$$

$$7 \oplus K_1 \boxtimes 5 = 4$$

$$K_1 \boxtimes 5 = \underbrace{4 \oplus 7}_{3}$$

$$K_1 \boxtimes 5 = 3$$

$$K_1 = 3 \boxtimes 5^{-1} = 3 \boxtimes 5 = 7 \pmod 8$$

$$(K_1, K_2) = (7, 5)$$