Es 1

Let $E: y^2 \equiv x^3+2x+2 \bmod 17$ 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 $\lambda=\dfrac{y_2-y_1}{x_2-x_1}$ if $P\neq Q$

$\nu=y_1-\lambda x_1$

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

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

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

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

$R'=(10,6)$

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

Es 1 other version

Let $E: y^2 \equiv x^3+2x+2 \bmod 17$ an elliptic curve and let $P=(6,3)$ and $Q=(10,6)$ and $R=(x,y)$ such that $P+Q+R=\emptyset$

a) $R=(9,16)$
b) $R=(9,1)$ ✓
c) $R=(9,14)$
d) $R=(9,12)$

Solution: $P+Q=R'$
$R=-R'$

$P \neq Q \Rightarrow \lambda = \frac{y_2-y_1}{x_2-x_1} = 3\cdot 4^{-1} \bmod 17 = 3\cdot 13 = 5$

$\nu = y_1 - \lambda x_1 = 3-5\times 6 = 7$

$x_3 = \lambda^2 - x_1 - x_2 = 5^2-6-10 \equiv 9$

$y_3 = -(\lambda x_3+\nu) = -(5\cdot 9+7) = 16$

$R'=(9,16)$

$R=(9,-16)=(9,1)$

Es 2

Let $GF(8)$ be the Galois field defined by the polynomial

$G(x) = x^3+x+1 \in \mathbb{Z}_2[x]$

Let $a(x) \in GF(8)$ be $a(x) = x+1$. The multiplicative inverse of $a(x)$ is

a) x^2+1

b) x^2

c) x^2+x+1

d) x^2+x ✓

Solution:

Step 1: compute the remainder of the division between $G(x)$ and $a(x)$

$$
\begin{array}{llll|l}
x^3 & +\,0x^2 & +\,x & +\,1 & x+1 \\
\cline{5-5}
x^3 & +\,x^2 & & & x^2+x \\
\cline{1-4}
\emptyset & x^2 & +\,x & +\,1 & \\
 & x^2 & +\,x & & \\
\cline{2-4}
 & \emptyset & \emptyset & +\,1 &
\end{array}
$$

"Send" the pair (remainder, divisor) $\xrightarrow[\text{quotient}]{}$ until reach $(0,1)$

$$(x+1,\, x^3+x+1) \xrightarrow[x^2+x]{} (1,\, x+1) \xrightarrow[x+1]{} (0,1)$$

Step 2: "reverse" to obtain the multiplicative inverse

Rule: $(y+qx,\, x) \longleftarrow (x,y)$

$$\overset{x\ \ y}{(0,1)} \xrightarrow[\substack{x+1\\ q}]{} (1,0) \xrightarrow[x^2+x]{} (x^2+x,\, 1)$$

The multiplicative inverse is the last x-coordinate

Es 2 other version

Let $GF(8)$ be the Galois field defined by the polynomial

$G(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$

Let $a(x) \in GF(8)$ be $a(x) = x^2 + x$. The multiplicative inverse of $a(x)$ is

a) $x + 1$ ✓

b) x

c) $x^2 + x + 1$

d) $x^2 + x$

Solution

$$
\begin{array}{l|l}
x^3 + 0x^2 + x + 1 & x^2 + x \\
x^3 \quad x^2 & \hline x + 1 \\
\hline
\quad x^2 + x + 1 & \\
\quad x^2 + x & \\
\cline{1-1}
\end{array}
$$

Es. 3

Find $x \in \mathbb{Z}_{401}$ such that

$x \cdot 56 \equiv 1 \bmod 401$ and
$5 \cdot x \equiv 308 \bmod 401$

Solution: we have to find the inverse of 56

Extended Euclidean Algorithm

$401 = 56 \times 7 + 9$
$56 = 9 \times 6 + 2$
$9 = 2 \times 4 + 1$
$2 = 1 \times 2 + \emptyset$

$p_0 = 0$
$p_1 = 1$

$p_i = p_{i-2} - q_{i-2} p_{i-1} \bmod N$

$p_2 = 0 - 7 \times 1 \bmod 401 = 394$

$p_3 = 1 - 6 \times 394 \bmod 401 = 1 - 359 \equiv 43 \bmod 401$

$p_4 = 394 - 43 \times 4 \bmod 401 = 222$

Try: $5 \times 222 = 1110 \equiv 308$ OK!

So $x \equiv 222 \bmod 401$

Es 3 other version

Find $x \in 401$ such that

$x \cdot 29 \equiv 1 \bmod 401$
$5x \equiv 14 \bmod 401$

$x = 29^{-1} \bmod 401$

$401 = 29 \times 13 + 24$
$29 = 24 \times 1 + 5$
$24 = 5 \times 4 + 4$
$5 = 4 \times 1 + 1$
$4 = 1 \times 4 + 0$

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 13 = 388$
$p_3 = 1 - 388 = 14$
$p_4 = 388 - 14 \times 4 = 332$
$p_5 = 14 - 332 = 83$

$5 \times 83 = 415 \equiv 14 \bmod 401$

$x = 83$