12

1

Verify that the order of the point $P=(1,0)$ in the curve $E_8: y^2+xy=x^3+\alpha^2x^2+\alpha^6$ is 12 over the field $\mathbb{F}_8=\mathbb{Z}_2[X]/X^3+X+1$. The class of X is denoted as α.

Answer

Derivation of μ:

$y+x\mu=x^2$

$\mu=x+\frac{y}{x}$

$$\mu=\begin{cases}\frac{y_2+y_1}{x_2+x_1} & P\neq Q\\ x+\frac{y}{x} & P=Q\end{cases}$$

$x_3=\mu^2+\mu+\alpha^2+x_1+x_2$

$y_3=y_1+\mu(x_3+x_1)+x_3$

$P=(1,0)$

$2P=P+P$

$\mu=1$

$x_3=1+1+\alpha^2+1+1=\alpha^2$

$y_3=0+1(\alpha^2+1)+\alpha^2=1$

$2P=(\alpha^2,1)$

$3P=2P+P$

$\mu=\frac{1}{\alpha^2+1}=\alpha$

$x_3=\alpha^2+\alpha+\alpha^2+1+\alpha^2=\alpha^2+\alpha+1$

$y_3=0+\alpha(1+\alpha^2+\alpha+1)+\alpha^2+\alpha+1=0$

$y_3=1+\alpha(\alpha^2+\alpha+1+\alpha^2)+\alpha^2+\alpha+1=0$

$3P=(\alpha^2+\alpha+1,0)$

$4P=2P+2P$

$\mu=\alpha^2+\frac{1}{\alpha^2}=\alpha+1$

$x_3=\alpha^2+1+\alpha+1+\alpha^2+\alpha^2+\alpha^2=\alpha$

$y_3=1+(\alpha+1)(\alpha+\alpha^2)+\alpha=\alpha$

$4P=(\alpha,\alpha)$

$6P=4P+2P$

$\mu=\frac{\alpha}{\alpha^2+\alpha}=\alpha^2+\alpha$

$x_3=\alpha+\alpha^2+\alpha+\alpha^2+\alpha^2+\alpha=\alpha^2+\alpha$

$y_3=1+(\alpha^2+\alpha)(\alpha^2+\alpha+\alpha^2)+\alpha^2+\alpha=0$

$6P = 3P + 3P$
$\mu = \alpha^2 + \alpha + 1 + \frac{0}{\alpha^2+\alpha+1} = \alpha^2 + \alpha + 1$
$x_3 = \alpha^2 + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha$
$y_3 = 0 + (\alpha^2 + \alpha)(\alpha^2 + \alpha + \alpha^2 + \alpha + 1) + \alpha^2 + \alpha = 0$
$6P = (\alpha^2 + \alpha, 0)$

$12P = 6P + 6P$
$\mu = \alpha^2 + \alpha + \frac{0}{\alpha^2+\alpha} = \alpha^2 + \alpha$
$x_3 = \alpha + \alpha^2 + \alpha + \alpha^2 = 0$
$y_3 = 0 + (\alpha^2 + \alpha)(0 + \alpha^2 + \alpha) + 0 = \alpha$
$12P = \mathscr{O}$

Therefore the order is 12

2

Solve the equation $Q = nP$ with $P = (1, 0)$ and $Q = (\alpha + 1, \alpha^2 + 1)$.

✓ **Answer**
$5P = 4P + P$
$\mu = \frac{\alpha}{\alpha+1} = \alpha^2 + \alpha + 1$
$x_3 = \alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + 1 = \alpha + 1$
$y_3 = 0 + (\alpha^2 + \alpha + 1)(\alpha + 1 + 1) + \alpha + 1 = \alpha^2 + \alpha$
$5P = (\alpha + 1, \alpha^2 + \alpha)$

$7P = 4P + 3P$
$\mu = \frac{\alpha}{\alpha^2+\alpha+1+\alpha} = \alpha^2$
$x_3 = \alpha^2 + \alpha + \alpha^2 + \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = \alpha + 1$
$y_3 = 0 + \alpha^2(\alpha + 1 + \alpha^2 + \alpha + 1) + \alpha + 1 = \alpha^2 + 1$
$7P = (\alpha + 1, \alpha^2 + 1)$

$Q = 7P$

3

For the curve $E : y^2 + xy = x^3 + 1$, determine the number of points over the field $\mathbb{F}_2$, and then over the field $\mathbb{F}_{2^{13}}$.

✓ **Answer**
For $\mathbb{F}_2$

With $x = 0$
$y^2 = 1 \pmod 2$

$y \in \{1\} | x = 0$

With $x = 1$
$y^2 + y = 0 \pmod 2$
$y \in \{0, 1\} | x = 1$

$\{(0,1), (1,0), (1,1), \mathscr{O}\} \in \mathbb{P}$

For $\mathbb{F}_{2^{13}}$

$t_0 = 2$
$N_1 = 4$
$t_1 = 2 + 1 - 4 = -1$

$X^2 - t_1 X + q = 0$
$X^2 + X + 2 = 0$
$X = -0.5 \pm \sqrt{1.75} i$

$t_{13} = (0.5 + \sqrt{1.75} i)^{13} + (0.5 - \sqrt{1.75} i)^{13}$
$= -181$

$N_{13} = 2^{13} + 1 + 181 = 8374$