Ex: 10.15 $P=(4,2)$ Prime $=13$

$Q=(10,6)$

Find $R=P+Q$

Since $P \neq Q$, case (i) will be applied.

$$\lambda = \left(\frac{y_2-y_1}{x_2-x_1}\right) \text{MOD prime}$$

$$= \left(\frac{6-2}{10-4}\right) \text{MOD } 13$$

$$= \left(\frac{4}{6}\right) \text{MOD } 13$$

$$= (4 \times 6^{-1} \text{ MOD } 13) \text{ MOD } 13$$

$$= (4 \times 11) \text{ MOD } 13 \quad (\because 6^{-1} = 11 \text{ MOD } 13)$$

$$= 44 \text{ MOD } 13$$

$$= 5$$

$\therefore \boxed{\lambda = 5}$

$$x_3 = (\lambda^2 - x_1 - x_2) \text{ MOD Prime}$$

$$= (25 - 4 - 10) \text{ MOD } 13$$

$$= 11$$

$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod \text{prime}$

$= (5(4-11) - 2) \bmod 13$

$= -37 \bmod 13$

$= 2$

$$13 \overline{)-37} \quad -3$$
$$-39$$
$$+$$
$$2$$

$\therefore R = (x_3, y_3)$

$\therefore \boxed{R = (11, 2)}$

Ex 2

$E_{13}(1,1)$: curve

$P = (1,4)$

Find $2P$?

$2P = P + P$

Case (II) can be applied

$$\lambda = \left(\frac{3x_1^2 + a}{2y_1}\right) \bmod \text{prime}$$

$$= \left(\frac{3 \cdot 1^2 + 1}{2 \cdot 4}\right) \bmod 13$$

$$= (4 \times 8^{-1} \bmod 13)$$

$= (4 \times 5) \bmod 13 \quad (\because 8^{-1} = 5 \bmod 13)$

$= 7$

$\therefore \boxed{\lambda = 7}$

$x_3 = (\lambda^2 - x_1 - x_2) \bmod \text{prime}$

$= (49 - 1 - 1) \bmod 13$

$= 47 \% 13$

$= 8$

$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod \text{prime}$

$= (7(11 - 8) - 4) \bmod 13$

$= -53 \bmod 13$

$= 12$

$$13 \overline{)-53} \quad -5, \quad -65, \quad +12$$

$\therefore 2P = P + P = (x_3, y_3)$

$= (8, 12)$

Ex 3 From Ex (2) $2P = (8, 12)$

Find $4P$

$4P = 2P + 2P$

Case (II) can be applied

$$\lambda = \left(\frac{3x_1^2 + a}{2y_1}\right) \text{MOD prime}$$

$$= \left(\frac{3 \cdot 8^2 + 1}{2 \cdot 12}\right) \text{MOD } 13$$

$$= (193 \times 24^{-1} \text{ MOD } 13) \text{ MOD } 13$$

$$= (193 \times 11^{-1} \text{ MOD } 13) \text{ MOD } 13$$

$$= (193 \times 6) \% 13$$

$$= 1$$

$$x_3 = (\lambda^2 - x_1 - x_2) \text{ MOD prime}$$

$$= (1^2 - 8 - 8) \text{ MOD } 13$$

$$= -15 \text{ MOD } 13$$

$$= 11$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \text{ MOD prime}$$

$$= (1(8 - 11) - 12) \text{ MOD } 13$$

$$= -15 \text{ MOD } 13$$

$$= 11$$

$\therefore 4P = (x_3, y_3) = (11, 11)$

Ex 4 For the curve $E_{13}(1,1)$

$P = (1,4)$

Find $3P$.

$3P = 2P + P$

$= (8,12) + (1,4)$ (from Ex ②)

$\lambda = \left(\frac{4-12}{1-8}\right) \text{MOD } 13$

$= \frac{-8}{-7} \text{ MOD } 13$

$= 8 \times 7^{-1} \text{ MOD } 13$

$= (8 \times 2) \text{ MOD } 13$

$= 3$

$x_3 = (\lambda^2 - x_1 - x_2) \text{ MOD } 13$

$= (3^2 - 8 - 1) \text{ MOD } 13$

$= 0$

$y_3 = (\lambda(x_1 - x_3) - y_1) \% 13$

$= (3(1-0) - 4) \% 13$

$= -1 \% 13$

$= 12$

$\therefore \boxed{(x_3, y_3) = (0, 12)}$

Ex 5

$P = (8, 1)$

$$\lambda = \left(\frac{3 \cdot 8^2 + 1}{2 \cdot 1}\right) \text{MOD } 13$$

$$= 193 \times 2^{-1} \text{ MOD } 13$$

$$= 193 \times 7 \text{ MOD } 13$$

$$= 12$$

$$x_3 = (\lambda^2 - x_1 - x_2) \text{ MOD } 13$$

$$= (144 - 8 - 8) \text{ MOD } 13$$

$$= 128 \text{ MOD } 13$$

$$= 11$$

$$Y_3 = (\lambda(x_1 - x_3) - Y_1) \text{ MOD } 13$$

$$= (12(8 - 11) - 1) \text{ MOD } 13$$

$$= -37 \% 13$$

$$= 2$$

$\therefore 2P = (x_3, Y_3) = (11, 2)$

$\rightarrow 3P = 2P + P$

$= (11, 2) + (8, 1)$

$$\lambda = \left(\frac{1 - 2}{8 - 11}\right) \text{MOD } 13 = 3^{-1} \text{ MOD } 13$$

$$= 9$$

$x_3 = (\lambda^2 - x_1 - x_2) \text{ MOD Prime}$

$$\therefore x_3 = (9^2 - 11 - 8) \% 13$$
$$= 62 \% 13$$
$$= 10$$
$$y_3 = (\lambda(x_4 - x_3) - y_1) \% 13$$
$$= (9(11 - 10) - 2) \% 13$$
$$= 7 \% 13$$
$$= 7$$
$$\therefore \boxed{3P = (x_3, y_3) = (10, 7)}$$