10.12 Determine all the points in $E_{11}(1, 6)$

①

Y	Y^2	$y^2 \bmod 11$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

②

X	x^3+x+6	$X \bmod 11$	Y_1	Y_2
0	6	6	—	—
1	8	8	—	—
2	16	5	7	4
3	36	3	5	6
4	74	8	—	—
5	136	4	2	9
6	228	8	~~2~~	~~9~~
7	356	4	~~2~~	~~9~~
8	526	9	3	8
9	744	7	—	—
10	1016	4	2	9

no vals

Points of $E_{11}(1, 6)$ at (X, Y)

$(2, 4)$, $(2, 7)$, $(3, 5)$, $(3, 6)$, $(5, 2)$, $(5, 9)$

$-P = (x_p, -y_p \bmod p)$

10.13 What are the negatives of the following elliptic curve points over Z_{17}? $P = (5, 8)$;

for $P = (5, 8)$ negative $P = (5, -8)$ $P = (5, 9)$
$Q = (3, 0)$ negative $Q = (3, 0)$ $Q(3, 0)$
$R = (9, 6)$ negative $R = (9, -6)$ $R = (0, 11)$

10.14 For $E_{11}(1, 6)$ consider the point $G = (0, 1)$. Compute the multiples of G from $2G$ through $13G$

Solve for $\lambda = (3x^2 + a)/2y_p \bmod p$

$2G$ is: $\lambda = (3 \cdot 0^2 + 1)/(2 \cdot 1) \bmod 11$

$= 1/2 \bmod 11 = 2^{-1} \bmod 11 = 6$

$x_3 = 6^2 - 0 - 0 \bmod 11 = 36 \bmod 11 = 3$

$y_3 = 6(0 - 3) - 1 \bmod 11 = -19 \bmod 11 = 3$

pts $2G = (3, 3)$
$3G = (8, 3)$
$4G = (10, 1)$
$5G = (3, 6)$
$6G = (7, 9)$
$7G = (7, 2)$
$8G = (3, 5)$
$9G = (10, 9)$
$10G = (8, 8)$
$11G = (0, 10)$
$12G = (2, 4)$
$13G = (1, 7)$

10.4

$2G = P + P = (2,7) + (2,7)$

$\lambda = \frac{3(x_p^2 + a)}{2y_p} \bmod p$

$= \frac{3(2^2)+1}{2(7)} \bmod 11 = 2 \cdot 3^{-1} \bmod 11 = 2 \cdot 4 \bmod 11 = 8$

$x_r = (\lambda^2 - x_p - x_p) \bmod p = (8^2 - 2 - 2) \bmod p = 60 \bmod 11 = 5$
$y_r = (\lambda(x_p - x_r) - y_p) \bmod p = (8(2-5) - 7) \bmod p = -31 \bmod 11 = 2$

$2G = (5,2)$

$3G = 2G + G = (5,2) + (2,7)$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$

$\lambda = \frac{7-2}{2-5} \bmod 11 = 5 \cdot 8^{-1} \bmod 11 = 5 \cdot 7 \bmod 11 = 2$

$x_r = (\lambda^2 - x_p - x_q) \bmod p = (2^2 - 5 - 2) \bmod 11 = -3 \bmod 11 = 8$
$y_r = (\lambda(x_p - x_r) - y_p) \bmod p = (2(5-8) - 2) \bmod 11 = -9 \bmod$
$= 3$

$3G = (8,3)$

$4G = (10, 2)$

$5G = 3G + 1G = (8, 3) + (3, 2)$

$\lambda = \frac{3-3}{5-9} \bmod 11 = 10 \cdot 8^{-1} \bmod 11 = 10 \cdot 7 \bmod 11 = 4$

$x_r = (4^2 - 8 - 5) \bmod 11 = 3 \bmod 11 = 3$
$y_r = (4(8-3) - 3) \bmod 11 = 17 \bmod 11 = 6$

$5G = (3, 6)$

$6G = (6, 3) + (8, 3)$

$\lambda = 3(8^2) + 1) \bmod 11 = 4 \cdot 6^{-1} \bmod 11 = 4 \cdot 2 \bmod 11 = 8$

$7G = 3G + 4G = (8,3) + (10,2)$

$\lambda = \frac{2-3}{10-8} \bmod 11 = 10 \cdot 2^{-1} \bmod 11 = 10 \cdot 6 \bmod 11 = 5$

$x_R = (5^2 - 8 - 10) \bmod 11 = 7 \bmod 11 = 7$
$y_R = (5(8-7) - 3) \bmod 11 = 2 \bmod 11 = 2$

$7G = (7,2)$

$8G = 4G + 4G = (10,2) + (10,2)$

$\lambda = \frac{3(10^2)+1}{2(2)} \bmod 11 = 4 \cdot 4^{-1} \bmod 11 = 4 \cdot 3 \bmod 11$

$x_R = (1^2 - 10 - 10) \bmod 11 = -15 \bmod 11 = 3$
$y_R = (1(10-3) - 2) \bmod 11 = 5 \bmod 11 = 5$

$8G = (3,5)$

$9G = 5G + 4G = (3,6) + (10,2)$

$\lambda = \frac{2-6}{10-3} \bmod 11 = 7 \cdot 7^{-1} \bmod 11 = 7 \cdot 8 \bmod 11 = 1$

$x_R = (1^2 - 3 - 10) \bmod 11 = -12 \bmod 11 = 10$
$y_R = (1(3-10) - 6) \bmod 11 = -13 \bmod 11 = 2$

$9G = (10,2)$

$10G = 5G + 5G = (3,6) + (3,6)$

$\lambda = \frac{3(3^2)+1}{2(6)} \bmod 11 = 6 \cdot 1^{-1} \bmod 11 = 6 \cdot 1 \bmod 11 = 6$

$x_r = (6^2 - 3 - 3) \bmod 11 = 30 \bmod 11 = 8$
$y_r = (6(3-8) - 6) \bmod 11 = -36 \bmod 11 = 8$

$10G = (8,8)$

$11G = 5G + 6G = (3,6) + (7,9)$

$\lambda = \frac{9-6}{7-3} \bmod 11 = 3 \cdot 4^{-1} \bmod 11 = 3 \cdot 3 \bmod 11 = 9$

$x_r = (9^2 - 3 - 7) \bmod 11 = 71 \bmod 11 = 5$
$y_r = (9(3-8) - 6) \bmod 11 = -51 \bmod 11 = 9$

$11G = (5,9)$

$12G = 6G + 6G = (7,9) + (7,9)$

$\lambda = \frac{3(7^2)+1}{2(9)} \bmod 11 = 5 \cdot 7^{-1} \bmod 11 = 5 \cdot 8 \bmod 11 =$

$x_r = (7^2 - 7 - 7) \bmod 11 = 35 \bmod 11 = 2$
$y_r = (7(7-2) - 9) \bmod 11 = 26 \bmod 11 = 4$

$12(G) = (8,8)$

$3G = 9G + 4G = (10, 2) + (10, 8)$

$\lambda = \frac{3(10)^2 + 1}{2(2)} \bmod 11 = 4 \cdot 4^{-1} \bmod 11 =$

$4 \cdot 3 \bmod 11 = 1$

$x_r = (1^2 - 10 - 10) \bmod 11 = -19 \bmod 11 = 3$

$y_r = (1(10 - 3) - 2) \bmod 11 = 5 \bmod 11 = 5$

$3G = (3, 5)$

10.15

a) To find public key use $P_B = n_B * G$

$= 7\,(2,7) = (7,2)$ $\quad P_B = (7,2)$

b) encryption of $P_M = (10,5)$ for $k = 3$

$C_M = \{kG,\ P_M + kP_B\}$

$= \{3(2,7),\ (10,5) + 3(7,2)\}$

$2(7,2) =$

$\lambda = \frac{3(x_1^2 + a)}{2y_1} \bmod p$

$= \frac{3(49)+1}{2 \cdot 2} \bmod 11 = 5 \cdot 4^{-1} \bmod 11$

$= 5 \cdot 3 \bmod 11 = 4$

$x_r = (\lambda^2 - x_q - x_q) \bmod p = (4^2 - 7 - 7) \bmod 11$

$= 2 \bmod 11 = 2$

$y_r = (\lambda(x_q - x_r) - y_q) \bmod p = (4(5) - 2) \bmod 11$

$= 18 \bmod 11 = 7$

$3 * (7,2) = 2 * (7,2) + (7,2) = (2,7) + (7,2)$

$$\lambda = \frac{y_q - y_p}{x_q - x_p} \bmod p$$

$$\lambda = \frac{2-7}{7-2} \bmod 11 = 6 \cdot 5^{-1} \bmod 11 = \cancel{6^{54}} \bmod 11 = 10$$

$x_r = (10^2 - 2 - 7) \bmod 11 = 91 \bmod 11 = 3.$
$y_r = (\lambda(x_p - x_r) - y_p) \bmod p = (10(2-3) - 7) \bmod 11$
$= -17 \bmod 11 = 5$

$3(7,2) = (3,5)$

$C_m = \{3(2,7), (10,9) + 3 \cdot (7,2)) = \{(8,3), (10,9) + (3,5$

$(10,9) + (3,5) = P + Q$

$$\lambda = \frac{5-9}{3-10} \bmod 11 = 7 \cdot 4^{-1} \bmod 11 = 7 \cdot 3 \bmod 11 = 10$$

$x_r = (10^2 - 10 - 3) \bmod 11 = 87 \bmod 11 = 10$
$y_r = (10(10-10) - 9) \bmod 11 = -9 \bmod 11 = 2$

$(10,9) + (3,5) = (10,2)$

Thus $C_M = \{(8,3), ((10,9) + (3,5)) = \{(8,3), (10,2)$

4. Calculate the B which recovers P_m from C_m

$P_m + kP_B - n_B(kG) = P_m$

$= (10,2) - 7 \cdot (3 \cdot (8,7)) = (10,2) - 7 \cdot (8,3)$

$\lambda = \frac{3(x_g^2 + a)}{2y_g} \mod p$

$\lambda = \frac{3(64)+1}{2 \cdot 3} \mod 11 = 6 \cdot 6^{-1} \mod 11 = 1$

$x_r = (1^2 - 8 - 8) \mod 11 = -15 \mod 11 = 7$
$y_r = (1(8-7) - 3) \mod 11 = -2 \mod 11 = 9$

$3 \cdot (8,3) = 2 \cdot (8,3) + (8,3) = (7,9) + (8,3)$

$\lambda = \frac{3-9}{8-7} \mod 11 = 5 \cdot 1^{-1} \mod 11 = 5 \cdot 1 \mod 11 = 5$

$x_r = (5^2 - 7 - 8) \mod 11 = 10 \mod 11 = 10$
$y_r = (5(7-10) - 9) \mod 11 = -24 \mod 11 = 9$

$3 \cdot (8,3) = (10,9)$

$4 \cdot (8,3)$

$\lambda = \frac{3(7^2)+1}{2(9)} \mod 11 = 5 \cdot 7^{-1} \mod 11 = 5 \cdot 8 \mod 11$

$x_r = (7^2 - 7 - 7) \mod 11 = 2$
$y_r = (7(7-2) - 9) \mod 11 = 26 \mod 11 = 4$

$7 \cdot (8,3) = 4 \cdot (8,3) + 3 \cdot (8,3) = (2,4) + (19,9)$

$\lambda = \frac{9-4}{10-2} \bmod 11 = 5 \cdot 8^{-1} \bmod 11 = 5 \cdot 7 \bmod 11 = 2$

$x_r = (2^2 - 2 - 10) \bmod 11 = -8 \bmod 11 = 3$
$y_r = (2(2-3) - 4) \bmod 11 = -6 \bmod 11 = 5$

$7 \cdot (8,3) = (3,5)$

$P_m = (10,2) - (3,5) = (10,2) + (-(3,5))$

$\downarrow$

$(3,6)$ at $p = 11$

$P_m = (10,2) + (3,6) =$

$\lambda = \frac{6-2}{3-10} \bmod 11 = 4 \cdot 4^{-1} \bmod 11 = 12 \bmod 11 = 1$

$x_r = (1^2 - 10 - 3) \bmod 11 = -12 \bmod 11 = 10$
$y_r = (1(10-10) - 2) \bmod 11 = -2 \bmod 11 = 9$

$P_m = (10,2) + (3,6) = (10,9)$ which is the original plaintext