Cavell Tang
Make-Up Exam

10-12. $E_{11}(1,6)$ $\quad y^2 = x^3 + x + 6$ $\quad p = 11$

Y	Y^2	$Y^2 \bmod 11$	X	$x^3 + x + 6$	$\bmod 11$	Y_1	Y_2
0	0	0	0	6	6		
1	1	1	1	8	8		
2	4	4	2	16	5	7	4
3	9	9	3	36	3	5	6
4	16	5	4	79	8		
5	25	3	5	136	4	2	9
6	36	3	6	224	8		
7	49	5	7	356	4	2	9
8	64	9	8	526	9	3	8
9	81	4	9	744	7		
10	100	1	10	1016	4	2	9

All pts: $(2,4)\ (2,7)$, $(3,5)\ (3,6)$, $(5,2)\ (5,9)$ } Points of $E_{11}(1,6)$
$(7,2)\ (7,9)$
$(8,3)\ (8,8)$
$(10,2)\ (10,9)$

10-13: $P = (5,8)$ $\quad Q = (3,0)$ $\quad R = (0,6)$ $\quad p = 17$

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

$-P = (5,9)$, $-Q = (3,0)$, $-R = (0,11)$

10-14: $E_{11}(1,6)$ $\quad G = (2,7)$

$2G = G + G \rightarrow P = (x_p, y_p)$, $Q = (x_q, y_q) \rightarrow P + Q = R$

$$\lambda = [(3x_p^2 + a)/2y_p] \bmod p$$

$$\begin{cases} x_R = (\lambda^2 - x_p - x_q) \bmod p \\ y_R = (\lambda(x_p - x_R) - y_p) \bmod p \end{cases}$$

$\lambda = (3(2)^2 + 1)/14) \bmod 11 = \frac{13}{14} \bmod 11$.

↳ $\left(\frac{13 \bmod 11}{14 \bmod 11}\right) \bmod 11 = \frac{2}{3} \bmod 11 = 8$

$x_R = 8^2 - 2 - 2 \mod 11 = 5$

$y_R = 8(2-5) - 7 \mod 11 = 2$

$2G = (5,2)$

$2G + G \Rightarrow \lambda = \frac{y_Q - y_P}{x_Q - x_P} \mod p = 5 \cdot 8^{-1} \mod 11 \rightarrow 5 \cdot 7 \mod 11 = 2$

$x_R = (2^2 - 5 - 2) \mod 11 = -3 \mod 11 = 8$

$3G = (8,3)$ $\quad y_R = [2(5-8) - 2] \mod 11 = -8 \mod 11 = 3$

$2G + 2G \Rightarrow \lambda = 8$

$x_R = (8^2 - 5 - 5) \mod 11 = 54 \mod 11 = 10$

$4G = (10,2)$ $\quad y_R = [8(5-10) - 2] \mod 11 = -42 \mod 11 = 2$

$3G + 2G \Rightarrow \lambda = 4$

$x_R = (16 - 8 - 5) \mod 11 = 3$

$5G = (3,6)$ $\quad y_R = [4(8-3) - 3] \mod 11 = 6$

$3G + 3G \Rightarrow \lambda = 1$

$6G = (7,9)$

$4G + 3G \Rightarrow \lambda = 5$

$7G = (7,2)$

$4G + 4G \Rightarrow \lambda = 1$

$8G = (3,5)$

$5G + 4G \Rightarrow \lambda = 1$

$9G = (10,2)$

$5G + 5G \Rightarrow \lambda = 6$

$10G = (8,8)$

$6G + 5G \Rightarrow \lambda = 9$

$11G = (5,9)$

$6G + 6G \Rightarrow \lambda = 7$

$12G = (2,4)$

$7G + 6G \Rightarrow \lambda = 1$

$13G = (3,5)$

10-15: $E_{11}(1,6)$ $G=(2,7)$ $n_B = 7$ ← B's private key.

(a) $P_B = n_B \times G \Rightarrow P_B = 7G = (7,2)$

(b) $P_m = (10,9)$ $k=3$

$C_m = \{kG,\ P_m + kP_B\}$

$= \{3G,\ (10,9) + 3P_B\}$

$P_B + P_B \rightarrow \lambda = 4 \rightarrow (2,7) = 2P_B$

$2P_B + P_B \rightarrow \lambda = 10 \rightarrow (3,5) = 3P_B$

$(10,9) + (3,5) \rightarrow \lambda = 10 \rightarrow (10,2)$

$C_m = \{(8,3),\ (10,2)\}$

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

$P_m = (10,2) - 7 * (3 * (2,7))$

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

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

$21G = (3,5)$

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

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

$-P = (3,-5) = (3,6)$

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

$\lambda = 1 \rightarrow (10,9)$

P_m