Problem 5.5

a) E: $Y^2 = X^3 + 3X + 2$ over F_7

$E(F_7) = \{0, (0,3), (0,4), (2,3), (2,4), (4,1), (4,6), (5,3), (5,4)\}$

$0^3 + 3(0) + 2 = 2 \pmod 7$

$3^2 = 2 \pmod 7$

$4^2 = 2 \pmod 7$

$2^3 + 3(2) + 2 = 2 \pmod 7$

$3^2 = 2 \pmod 7$

$4^2 = 2 \pmod 7$

$4^3 + 3(4) + 2 = 1 \pmod 7$

$1^2 = 1 \pmod 7$

$6^2 = 1 \pmod 7$

$5^3 + 3(5) + 2 = 2 \pmod 7$

$3^2 = 2 \pmod 7$

$4^2 = 2 \pmod 7$

b) E: $Y^2 = X^3 + 2X + 7$ over F_{11}

$E(F_{11}) = \{0, (6,2), (6,9), (7,1), (7,10), (10,2), (10,9)\}$

$6^2 + 2(6) + 7 = 4 \pmod{11}$

$2^2 = 4 \pmod{11}$

$9^2 = 4 \pmod{11}$

$7^2 + 2(7) + 7 = 1 \pmod{11}$

$1^2 = 1 \pmod{11}$

$10^2 = 1 \pmod{11}$

$6^2 + 2(6) + 7 = 4 \pmod{11}$

$2^2 = 4 \pmod{11}$

$9^2 = 4 \pmod{11}$

c) E: $Y^2 = X^3 + 4X + 5$ over F_{11}

$E(F_{11}) = \{0, (0,4), (0,7), (3,0), (6,5), (6,6), (9,0), (10,0)\}$

$0^3 + 4(0) + 5 = 5 \pmod{11}$

$4^2 = 5 \pmod{11}$

$7^2 = 5 \pmod{11}$

$3^3 + 4(3) + 5 = 0 \pmod{11}$

$0^2 = 0 \pmod{11}$

$6^3 + 4(6) + 5 = 3 \pmod{11}$

$5^2 = 3 \pmod{11}$

$6^2 = 3 \pmod{11}$

$9^3 + 4(9) + 5 = 0 \pmod{11}$

$0^2 = 0 \pmod{11}$

$10^3 + 4(10) + 5 = 0 \pmod{11}$

$0^2 = 0 \pmod{11}$

d) E: $Y^2 = X^3 + 9X + 5$ over F_{11}

$E(F_{11}) = \{0, (0,4), (0,7), (1,2), (1,9), (2,3), (2,8), (3,2), (3,9), (6,0), (7,2), (7,9), (9,1), (9,10)\}$

$0^3 + 9(0) + 5 = 5 \pmod{11}$

$4^2 = 5 \pmod{11}$

$7^2 = 5 \pmod{11}$

$1^3 + 9(1) + 5 = 4 \pmod{11}$

$2^2 = 4 \pmod{11}$

$9^2 = 4 \pmod{11}$

$2^3 + 9(2) + 5 = 9 \pmod{11}$

$3^2 = 9 \pmod{11}$

$8^2 = 9 \pmod{11}$

$3^3 + 9(3) + 5 = 4 \pmod{11}$

$2^2 = 4 \pmod{11}$

$9^2 = 4 \pmod{11}$

$6^3 + 9(6) + 5 = 0 \pmod{11}$

$0^2 = 0 \pmod{11}$

$7^3 + 9(7) + 5 = 4 \pmod{11}$

$2^2 = 4 \pmod{11}$

$9^2 = 4 \pmod{11}$

$9^3 + 9(9) + 5 = 1 \pmod{11}$

$1^2 = 1 \pmod{11}$

$10^2 = 1 \pmod{11}$

e) E: $Y^2 = X^3 + 9X + 5$ over F_{13}

$E(F_{13}) = \{0, (4,1), (4,12), (8,2), (8,11), (9,3), (9,10), (10,4), (10,9)\}$

$4^3 + 9(4) + 5 = 1 \pmod{13}$

$1^2 = 1 \pmod{13}$

$12^2 = 1 \pmod{13}$

$8^3 + 9(8) + 5 = 4 \pmod{13}$

$2^2 = 4 \pmod{13}$

$11^2 = 4 \pmod{13}$

$9^3 + 9(9) + 5 = 9 \pmod{13}$

$3^2 = 9 \pmod{13}$

$10^2 = 9 \pmod{13}$

$10^3 + 9(10) + 5 = 3 \pmod{13}$

$4^2 = 3 \pmod{13}$

$9^2 = 3 \pmod{13}$

5.6 Make an addition table for E over $\mathbb{F}_p$, as we did in table 5.1

a) $E: Y^2 = X^3 + X + 2$ over $\mathbb{F}_5$

$1^2 \equiv 1 \mod 5$
$2^2 \equiv 4 \mod 5$
$3^2 \equiv 4 \mod 5$
$4^2 \equiv 1 \mod 5$

(0) $Y^2 = 0^3 + 0 + 2$
$Y^2 = 2$ ✗

(1) $Y^2 = 1^3 + 1 + 2$
$Y = 3$ ✗

(2) $Y^2 = 2^3 + 2 + 2$
$Y^2 = 12 \mod 5$
$= 2$ ✗

(3) $Y^2 = 3^3 + 3 + 2$
$Y^2 = 32 \mod 5$
$= 2$ ✗

(4) $Y^2 = 4^3 + 4 + 2$
$Y^2 = 70 \mod 5$
$= 0$ ✗

no table

b) $E: Y^2 = X^3 + 2X + 3$ over $\mathbb{F}_7$

$1^2 = 1$
$2^2 \equiv 4$
$3^2 \equiv 2$
$4^2 \equiv 2$
$5^2 \equiv 4$
$6^2 \equiv 1$

(0) $Y^2 = 0 + 0 + 3$
$= 3$

(1) $Y^2 = 1 + 2 + 3$
$= 5$

(2) $Y^2 = 2^3 + 2(2) + 3$
$Y^2 = 15 \mod 7$
$= 1$ ✓ $(2,1), (2,6)$

(3) $Y^2 = 3^3 + 2(3) + 3$
$= 36 \mod 7$
$= 1$ ✓ $(3,1), (3,6)$

(4) $Y^2 = 4^3 + 2(4) + 3$
$= 75 \mod 7$
$= 5$ ✗

(5) $Y^2 = 5^3 + 2(5) + 3$
$= 138 \mod 7$
$= 5$ ✗

(6) $Y^2 = 6^3 + 2(6) + 3$
$= 231 \mod 7$
$= 0$ ✗

$E(\mathbb{F}_7) = \{\mathcal{O}, (2,1), (2,6), (3,1), (3,6)\}$

$\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

$v = y_1 - \lambda x_1$

$x_3 = \lambda^2 - x_1 - x_2$
$y_3 = -(\lambda x_3 + v)$

	$\mathcal{O}$	(2,1)	(2,6)	(3,1)	(3,6)
$\mathcal{O}$	$\mathcal{O}$	(2,1)	(2,6)	(3,1)	(3,6)
(2,1)	(2,1)	(0,1)	$\mathcal{O}$	(3,0)	(2,1)
(2,6)	(2,6)	$\mathcal{O}$	(0,1)	(2,1)	(1,3)
(3,1)	(3,1)	(1,1)	(2,0)	(1,0)	$\mathcal{O}$
(3,6)	(3,6)	(0,0)	(0,0)	$\mathcal{O}$	$\mathcal{O}$

work on next page
↓

b) $P+P = (2,1)+(2,1) = (0,1)$

$Y^2 = X^3+2x+3$ over $\mathbb{F}_3$

$\lambda = \frac{3x_1^2+A}{2y_1} = \frac{3(2)^2+2}{2(1)} = 7 \bmod 3 = 1$

$V = y_1 - \lambda x_1 = 1 - 1(2) = -1 \bmod 3 = 2$

$X_3 = \lambda^2 - x_1 - x_2 = 1-2-2 = -3 \bmod 3 = 0$

$Y_3 = -(\lambda x_3 + v) = -(1(0)+2) = -2 \bmod 3 = 1$

$(2,6)+(2,6) = (0,1)$

$\lambda = \frac{3(2)^2+2}{2(1)} = 1$

$V = y_1 - \lambda x_1 = 1 - 1(2) = 2$

$X_3 = \lambda^2 - x_1 - x_2 = 1-2-2 = 0$

$Y_3 = -(\lambda x_3 + v) = -(2(0)+2) = -2 \bmod 3 = 1$

$(3,6)+(3,6) = \mathcal{O}$

$\lambda = \frac{3(3)+2}{2(6)} = \frac{11 \bmod 3}{12 \bmod 3} = \frac{2}{0}$

$(3,1)+(3,1) = (1,0)$

$\lambda = \frac{3(3)+2}{2(3)} = 2$

$V = y_1 - \lambda x_1 = 1 - 2(3) = -5 \bmod 3 = 1$

$X_3 = \lambda^2 - x_1 - x_2 = 2^2-3-3 = -2 \bmod 3 = 1$

$Y_3 = -(\lambda x_3 + v) = -(2(1)+1) = -3 \bmod 3 = 0$

$(2,1)+(2,3) = \mathcal{O}$

$\lambda = \frac{y_2-y_1}{x_2-x_1} = \frac{3-2}{2-2}$

$(2,1)+(3,1) = (1,1)$

$\lambda = \frac{1-1}{3-2} = 0$

$V = y_1 - \lambda x_1 = 1 - 0(2) = 1$

$X_3 = \lambda^2 - x_1 - x_2 = 0-2-3 = -5 \bmod 3 = 1$

$Y_3 = -(\lambda x_3 + v) = -(0(1)+1) = 1$

$(3,6)+(2,6) = (1,3)$

$\lambda = \frac{6-6}{2-3} = 0$

$V = y_1 - \lambda x_1 = 3-(0)(6) = 3 \bmod 3 = 0$

$X_3 = \lambda^2 - x_1 - x_2 = 0-3-2 = -5 \bmod 3 = 1$

$Y_3 = -(\lambda x_3 + v) = -(0(1)+0) = 0 \bmod 3 = 0$

$(3,1)+(2,1) = (3,0)$

$\lambda = \frac{y_2-y_1}{x_2-x_1} = \frac{1-1}{2-3} = 0$

$V = y_1 - \lambda x_1 = 3-0 = 3 \bmod 3 = 0$

$x_3 = \lambda^2 - x_1 - x_2 = 0^2-3-2 = -5 \bmod 3 = 1$

$Y_3 = -(\lambda x_3 + v) = -(0(1)+0) = 0 \bmod 3 = 0$

$(2,6)+(3,6) = (0,0)$

$\lambda = 0$

$V = y_1 - \lambda x_1 = 6-(0)(2) = 6 \bmod 3 = 0$

$X_3 = \lambda^2 - x_1 - x_2 = 0-3-2 = -5 = 1$

$Y_3 = -(0(1)+0) = 0$

$(3,6)+(2,1) = (2,1)$

$\lambda = \frac{y_2-y_1}{x_2-x_1} = \frac{1-6}{2-3} = \frac{-5}{1} = -5$

$V = y_1 - \lambda x_1 = 6-(-5)(3) = 21 \bmod 3 = 0$ ✓

$x_3 = \lambda^2 - x_1 - x_2 = (-5)^2-3-2 = 20 \bmod 3 = 2$

$Y_3 = -(\lambda x_3 + v) = -(-5(2)+0) = 10 \bmod 3 = 1$

$(3,1)+(2,6) = (2,1)$

$\lambda = \frac{6-1}{2-3} = \frac{5}{-1} = -5$

$V = y_1 - \lambda x_1 = 3-(-5)(3) = 18 \bmod 3 = 0$

$X_3 = \lambda^2 - x_1 - x_2 = (-5)^2-3-2 = 20 \bmod 3 = 2$

$Y_3 = -(\lambda x_3 + v) = -(-5(2)+0) = 10 \bmod 3 = 1$

$(2,1)+(3,6) = (0,0)$

$\lambda = \frac{6-1}{3-2} = \frac{5}{1} = 5$

$V = 1-(5)(2) = 9 \bmod 3 = 0$ ✓

$X_3 = \lambda^2 - x_1 - x_2 = (5)-2-3 = 0$

$Y_3 = -(\lambda x_3 + v) = -(5(0)+0) = 0$

$(2,6)+(3,1) = (2,0)$

$\lambda = \frac{1-2}{3-2} = \frac{-1}{1} = -1$

$V = y_1 - \lambda x_1 = 6-(-1)(2) = 8 \bmod 3 = 2$

$X_3 = \lambda^2 - x_1 - x_2 = (-1)^2-2-3 = -4 \bmod 3 = 2$

$Y_3 = -(\lambda x_3 + v) = -(-1(2)+2) = -0 \bmod 3 = 0$

c) $E : Y^2 = X^3 + 2X + 5$ over $\mathbb{F}_{11}$

$1^2 \equiv 1 \mod 11$
$2^2 \equiv 4$
$3^2 \equiv 9$
$4^2 \equiv 5$
$5^2 \equiv 3$
$6^2 \equiv 3$
$7^2 \equiv 5$
$8^2 \equiv 9$
$9^2 \equiv 4$
$10^2 \equiv 1$

(0) $Y^2 = 0 * 0 + 5$
$Y_2 = 5$ ✓
$(0,4),(0,7)$

(1) $Y^2 = 1 + 2 + 5$
$Y = 8$ ×

(2) $Y^2 = 2^3 + 2(2) + 5$
$= 17 \mod 11$
$= 6$ ×

(3) $Y^2 = 3^3 + 2(3) + 5$
$= 38 \mod 11$
$= 5$ ✓ $(3,4),(3,7)$

(4) $Y^2 = 4^3 + 2(4) + 5$
$= 77 \mod 11$
$= 0$ ×

(5) $Y^2 = 5^3 + 2(5) + 5$
$= 140 \mod 11$
$= 8$ ×

(6) $Y^2 = 6^3 + 2(6) + 5$
$= 233 \mod 11$
$= 2$ ×

(7) $Y^2 = 7^3 + 2(7) + 5$
$= 362 \mod 11$
$= 10$ ×

(8) $Y^2 = 8^3 + 2(8) + 5$
$= 533 \mod 11$
$= 5$ ✓ $(8,4),(8,7)$

(9) $Y^2 = 9^3 + 2(9) + 5$
$= 752 \mod 11$
$= 4$ ✓ $(9,2),(9,9)$

(10) $Y^2 = 10^3 + 2(10) + 5$
$= 1025 \mod 11$
$= 2$ ×

$E(\mathbb{F}_{11}) = \{ \mathcal{O}, (0,4), (0,7), (3,4), (3,7), (8,4), (8,7), (9,2), (9,9) \}$

	$\mathcal{O}$	(0,4)	(0,7)	(3,4)	(3,7)	(8,4)	(8,7)	(9,2)	(9,9)
$\mathcal{O}$	$\mathcal{O}$	(0,4)	(0,7)	(3,4)	(3,7)	(8,4)	(8,7)	(9,2)	(9,9)
(0,4)	(0,4)	$(\frac{1}{5}, \frac{4}{9})$	$\mathcal{O}$	(8,8)	(9,9)	(3,0)	$(\frac{3}{4}, \frac{1}{2})$	$(\frac{1}{7}, \frac{1}{4})$	(0,3)
(0,7)	(0,7)	$\mathcal{O}$	$(\frac{4}{9}, \frac{8}{5})$	(9,2)	.	$(\frac{3}{2}, \frac{3}{5})$	$\mathcal{O}$		
(3,4)	(3,4)			$(\frac{6}{2}, \frac{6}{9})$	$\mathcal{O}$				
(3,7)	(3,7)			$\mathcal{O}$					
(8,4)	(8,4)						$\mathcal{O}$		
(8,7)	(8,7)					$\mathcal{O}$			
(9,2)	(9,2)								$\mathcal{O}$
(9,9)	(9,9)							$\mathcal{O}$	

5.7

5.7

	p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$	
a)	3	4	0	3.464	$\lvert 0\rvert \leq 2\sqrt{p}$
b)	5	9	-3	4.47	$\lvert -3\rvert \leq 2\sqrt{p}$
c)	7	5	3	5.29	$\lvert 3\rvert \leq 2\sqrt{p}$
d)	11	14	-2	6.633	$\lvert -2\rvert \leq 2\sqrt{p}$

5.13

a) $Q_B = (1432, 667)$

b) $n_B Q_A = (2424, 911)$

secret value $= 2424$

c) $n_a = 726 \Rightarrow 726P = Q_A$

takes

$O(\sqrt{P})$

d) Bob sends $\boxed{X_b = 161}$

Shared value

$y_A^2 = X_A^3 + 171 X_A + 853 = (2)^3 + 171(2) + 853 = 1203$

$Y_A = 1203^{(2671+1)/4} = 1203^{(668)} \equiv 2575$

$Q_A' = (2, 2575)$

$n_B Q_A' = 875(2, 2575) = (1708, 1419)$

$\therefore$ the secret shared value is $\boxed{1708}$