

Math 400 Fall 2017  
 Cryptology HW 8 Solutions  
 Due Thursday, October 26

1. Find every point :

(a)  $E : y^2 = x^3 + 3x + 2$  over  $\mathbb{F}_7$ .

(b)  $E : y^2 = x^3 + 2x + 7$  over  $\mathbb{F}_{11}$ .

**Solution:**

(a) First we form our multiplication table.

$$\begin{array}{lll} 1^2 \equiv 1 & 2^2 \equiv 4 & 3^2 \equiv 2 \\ 6^2 \equiv 1 & 5^2 \equiv 4 & 4^2 \equiv 2 \end{array}$$

So our squares are 0, 1, 2, 4.

Now we compute

$$\begin{array}{lll} x = 0 & y^2 \equiv 2 & y \equiv \pm 3 \\ x = 1 & y^2 \equiv 6 & \text{no solutions} \\ x = 2 & y^2 \equiv 2 & y \equiv \pm 3 \\ x = 3 & y^2 \equiv 3 & \text{no solutions} \\ x = 4 & y^2 \equiv 1 & y \equiv \pm 1 \\ x = 5 & y^2 \equiv 2 & y \equiv \pm 3 \\ x = 6 & y^2 \equiv 5 & \text{no solutions} \end{array}$$

Thus we have the points

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0, 3), (0, 4), (2, 3), (2, 4), (4, 1), (4, 6), (5, 3), (5, 4)\}.$$

(b) First we form a multiplication table:

$$1^2 \equiv 1 \quad 2^2 \equiv 4 \quad 3^2 \equiv 9 \quad 4^2 \equiv 5 \quad 5^2 \equiv 3$$

So our squares are 0, 1, 3, 4, 5, 9.

Now we compute

$x = 0$	$y^2 \equiv 7$	no solutions
$x = 1$	$y^2 \equiv 10$	no solutions
$x = 2$	$y^2 \equiv 8$	no solutions
$x = 3$	$y^2 \equiv 7$	no solutions
$x = 4$	$y^2 \equiv 2$	no solutions
$x = 5$	$y^2 \equiv 10$	no solutions
$x = 6$	$y^2 \equiv 4$	$y \equiv \pm 2$
$x = 7$	$y^2 \equiv 1$	$y \equiv \pm 1$
$x = 8$	$y^2 \equiv 7$	no solutions
$x = 9$	$y^2 \equiv 6$	no solutions
$x = 10$	$y^2 \equiv 4$	$y \equiv \pm 2$

Thus we have the points

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (6, 2), (6, 9), (7, 1), (7, 10), (10, 2), (10, 9)\}.$$

2. Let  $E : y^2 = x^3 + x + 1$  over  $\mathbb{F}_{23}$  and let  $P = (0, 22)$ .

- Compute  $\log_P(18, 20)$ . Show the results of each point addition you compute.
- Compute  $17P$ . Show the results of each point addition you compute.

**Solution:**

(a) We compute

$$\begin{aligned} P &= (0, 22) \\ 2P &= (6, 4) \\ 3P &= (3, 10) \\ 4P &= (13, 7) \\ 5P &= (18, 20) \end{aligned}$$

(b) We compute

$$\begin{aligned} P &= (0, 22) \\ 2P &= (6, 4) \\ 4P &= (13, 7) \\ 8P &= (5, 4) \\ 16P &= (17, 20) \\ 17P &= 16P \oplus P = (17, 20) \oplus (0, 22) = (1, 16). \end{aligned}$$

3. Suppose Alice and Bob want to communicate using a Elliptic Curve Diffie-Hellman scheme. They have chosen the curve  $E : y^2 = x^3 + 23x + 13$ , the field  $\mathbb{F}_{83}$ , and the point  $P = (3, 21)$ .

- (a) Bob chooses a secret number  $n_B = 10$ . What information should he send to Alice?
- (b) Bob receives the point  $Q_A = (71, 82)$  from Alice. What is the shared secret key?

**Solution:** We have

$$2P = (34, 33)$$

$$4P = (26, 33)$$

$$8P = (62, 48)$$

$$16P = (67, 60)$$

- (a) Bob sends  $n_BP = 9(3, 21) = (62, 48) \oplus (34, 33) = (20, 16)$ .
  - (b) Bob computes  $n_bQ_A = 10(71, 82) = (1, 28)$ .
4. Now Alice and Bob communicate using an Elliptic Curve ElGamal scheme. They use the same curve and point as in the previous problem.
- (a) Alice chooses a private key  $n_A = 17$ . What is her public key?
  - (b) Suppose Bob's public key is  $Q_B = (68, 32)$ . Alice wishes to send the message  $M = (75, 8)$  using the ephemeral key  $k = 5$ . What ciphertext does Alice send?
  - (c) Alice receives the ciphertext  $(C_1, C_2) = ((30, 8), (71, 82))$  from Bob. What message does she decrypt?

**Solution:**

- (a) Her public key is  $Q_A = n_AP = 16P \oplus P = (67, 60) \oplus (3, 21) = (54, 40)$ .
- (b) We have  $C_1 = kP = 5(3, 21) = (26, 33) \oplus (3, 21) = (64, 41)$ , and we have  $C_2 = M \oplus kQ_B = (75, 8) \oplus 5(68, 32) = (75, 8) \oplus (64, 41) = (36, 41)$ . So Alice sends  $((64, 41), (36, 41))$ .
- (c) Alice computes  $C_2 - n_AC_1 = (71, 82) - 17(30, 8)$ . We have  $17(30, 8) = (24, 69)$ , so the message is  $M = (71, 82) - (24, 69) = (51, 37)$ .