Math 4981 Spring 2021
Cryptography HW 9 Solutions
Due Thursday, March 25

1. Consider the following curves:

   (i) $y^2 = x^3 - 7x + 3$

   (ii) $y^2 = x^3 - 7x + 9$

   (iii) $y^2 = x^3 - 7x - 12$

   (iv) $y^2 = x^3 - 3x + 2$

   (v) $y^2 = x^3$.

   (a) Compute the discriminant of each curve. Which of these are elliptic curves?

   (b) Sketch a graph of each curve (you may use a computer for this step). How can you visually tell which of these curves was an elliptic curve?

   Solution:

   (a) The discriminants are:

   (i) -1129

   (ii) 815

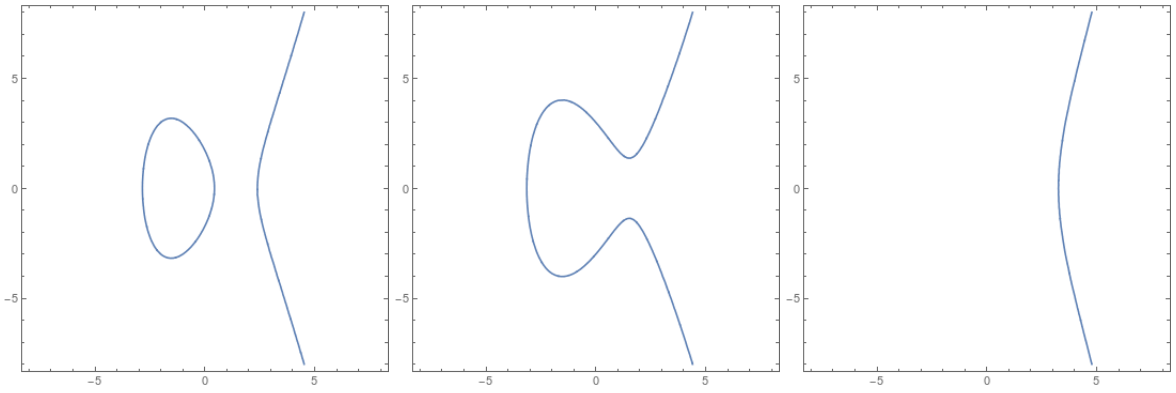
   (iii) 2516

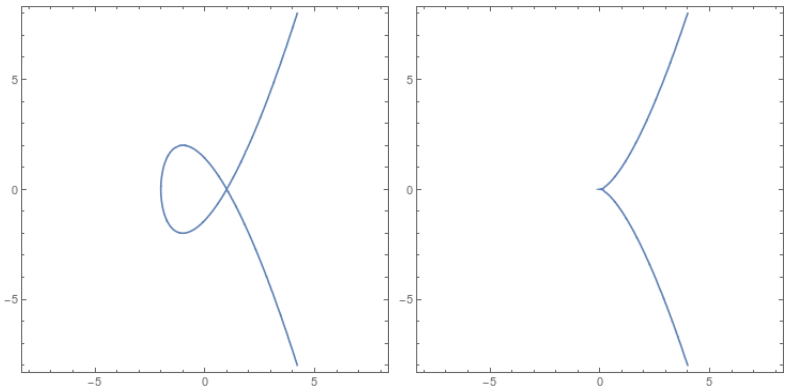
   (iv) 0

   (v) 0

   So the first three are elliptic curves, and the last two are not.

   (b)





We see the first three are smooth curves, and thus are reasonable elliptic curves. The fourth has a self-intersection and the fifth has a cusp, so are not differentiable everywhere, and so the elliptic curve addition isn't always well-defined.

2. (20 pts) Let $E : y^2 = x^3 - 2x + 4$, and let $P = (0, 2)$ and $Q = (3, -5)$.

   (a) Check that $P, Q \in E(\mathbb{Q})$.

   (b) Compute Δ to confirm that this is an elliptic curve.

   (c) Explicitly using the geometric definition, compute $P \oplus Q$. Sketch a picture of all the lines involved.

   (d) Explicitly using the geometric definition, ompute $P \oplus P$ and $Q \oplus Q$. Sketch a picture of all the lines involved.

   (e) Compute $3P = P \oplus P \oplus P$ and $3Q = Q \oplus Q \oplus Q$. You can use the explicit algorithm here.

Solution:

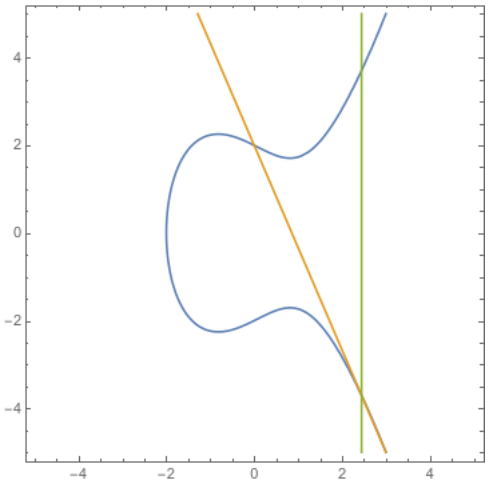
(a) $0^3 - 2 \cdot 0 + 4 = 4 = 2^2$ and $3^3 - 2 \cdot 3 + 4 = 25 = 5^2$ so these are on the curve.

(b) $\Delta = 4A^3 + 27B^2 = 4 \cdot (-2)^3 + 27 \cdot 4^2 = -32 + 432 = 400 \neq 0$ so this is an elliptic curve.

(c) The line through P and Q is given by $y = \frac{-5-2}{3-0}(x - 0) + 2 = -\frac{7}{3}x + 2$.
We plug this into the cubic and get

$$\begin{aligned} (2 - 7x/3)^2 &= x^3 - 2x + 4 \\ 4 - 28x/3 + 49x^2/9 &= x^3 - 2x + 4 \\ 0 &= x^3 - 49x^2/9 + 22x/3 \end{aligned}$$

and we know that $-49/9 = -x_1 - x_2 - x_3 = -0 - 3 - x_3$ so $-22/9 = x_3$ and $x_3 = 22/9$.
Plugging this back into the equation for the line, we get $y_3 = -154/27 + 2 = -100/27$, so $\mathbf{P \oplus Q = (22/9, 100/27)}$.



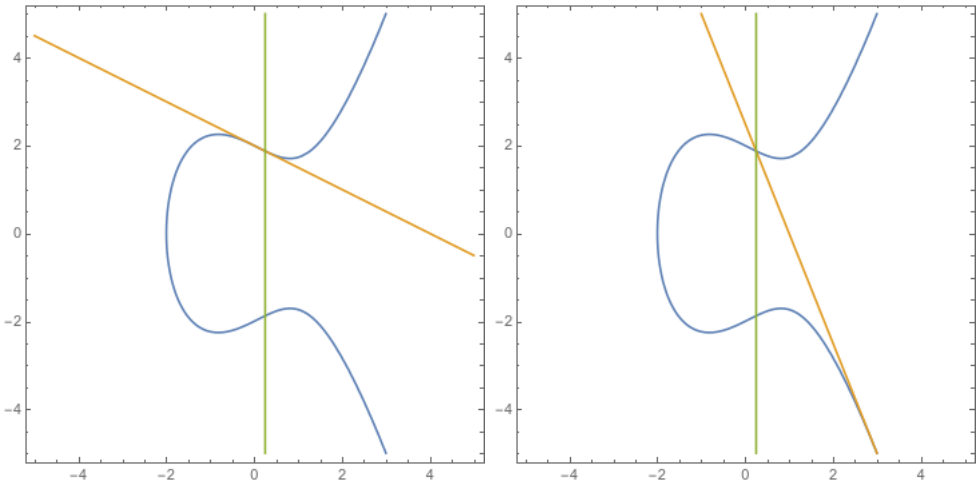
(d) We have $2yy' = 3x^2 - 2$, so at the point P we have $2 \cdot 2 \cdot y' = 3 \cdot 0^2 - 2$ or $y' = -1/2$. Thus the tangent line is $y = -x/2 + 2$.

Plugging this into the cubic gives

$$\begin{aligned}(-x/2+2)^2 &= x^3 - 2x + 4\\ x^2/4 - 2x + 4 &= x^3 - 2x + 4\\ 0 &= x^3 - x^2/4\end{aligned}$$

and we have $-1/4 = -x_1 - x_2 - x_3 = -0 - 0 - x_3$ so $x_3 = 1/4$.

Plugging this into the line gives $y_3 = -1/8+2 = 15/8$. Thus we have $\mathbf{P} \oplus \mathbf{P} = (\mathbf{1/4}, \mathbf{-15/8})$



Similarly, at the point Q we have $2 \cdot (-5) \cdot y' = 3 \cdot 3^2 - 2$ or $-10y' = 25$, so $y' = -5/2$. Thus the tangent line is $y = -5/2(x-3) - 5 = -5x/2 + 5/2$.

Plugging this into the cubic gives

$$\begin{aligned}(-5x/2+5/2)^2 &= x^3 - 2x + 4\\ 25x^2/4 - 25x/2 + 25/4 &= x^3 - 2x + 4\\ 0 &= x^3 - 25x^2/4 + 21x/2 - 9/4\end{aligned}$$

and we have $-25/4 = -x_1 - x_2 - x_3 = -3 - 3 - x_3$ so $-1/4 = -x_3$ and $x_3 = 1/4$.

Plugging this into the line gives $y_3 = -5/8+5/2 = 15/8$, so $\mathbf{Q} \oplus \mathbf{Q} = (\mathbf{1/4}, \mathbf{-15/8})$.

(e) We have $3P = (1/4, -15/8) \oplus (0, 2)$. Then

$$\lambda = \frac{1/2 - 0}{-15/8 - 2} = \frac{-31}{2}$$
$$x_3 = \lambda^2 - x_1 - x_2 = \frac{31^2}{4} - 1/4 - 0 = 240$$
$$y_3 = \lambda(0 - 240) - 2 = 3718$$

so $\mathbf{3P} = (\mathbf{240}, \mathbf{3718})$.
Similarly, $3Q = (1/4, -15/8) \oplus (3, -5)$. Then

$$\lambda = \frac{-15/8 + 5}{1/4 - 3} = \frac{-25}{22}$$
$$x_3 = \lambda^2 - x_1 - x_2 = \frac{25^2}{22^2} - 1/4 - 3 = -237/121$$
$$y_3 = (-25/22)(3 + 237/121) + 5 = -845/1331$$

so $\mathbf{3Q} = (\mathbf{-237/121}, \mathbf{-845/1331})$.

3. Let $E : y^2 = x^3 + 17$. Let $P = (-1, 4)$ and let $Q = (2, 5)$.

(a) Confirm that $P, Q \in E(\mathbb{Q})$.
(b) Compute Δ to confirm that this is an elliptic curve.
(c) Compute $P \oplus Q$ and $P - Q$. (You can use the explicit algorithm.)
(d) Compute $2P = P \oplus P$ and $2Q = Q \oplus Q$. (You can use the explicit algorithm.)

Solution:

(a) $(-1)^3 + 17 = 15 = 4^2$ so $P \in E(\mathbb{Q})$, and $2^3 + 17 = 25 = 5^2$ so $Q \in E(\mathbb{Q})$.
(b) $\Delta = 4A^3 + 27B^2 = 27 \cdot 17^2 = 7803 \neq 0$ so this is an elliptic curve.
(c) We have $P \oplus Q = (-1, 4) \oplus (2, 5)$. Then

$$\lambda = \frac{5 - 4}{2 + 1} = \frac{1}{3}$$
$$x_3 = \frac{1}{9} + 1 - 2 = -8/9$$
$$y_3 = 1/3(-1 + 8/9) - 4 = -109/27$$

so $\mathbf{P} \oplus \mathbf{Q} = (\mathbf{-8/9}, \mathbf{-109/27})$.
We have $P - Q = (-1, 4) \oplus (2, -5)$. Then

$$\lambda = \frac{-5 - 4}{2 + 1} = -3$$
$$x_3 == 9 + 1 - 2 = 8$$
$$y_3 = -3(-1 - 8) - 4 = 23$$

so $\mathbf{P - Q} = (\mathbf{8}, \mathbf{23})$.

(d) We have $2P = (-1, 4) \oplus (-1, 4)$. Then

$$\lambda = \frac{3+0}{8} = 3/8$$
$$x_3 == 9/64 + 1 + 1 = 137/64$$
$$y_3 = 3/8(-1 - 137/64) - 4 = -2651/512$$

so $\mathbf{2P} = (\mathbf{137/64}, \mathbf{-2651/512})$.
We have $2P = (2, 5) \oplus (2, 5)$. Then

$$\lambda = \frac{12+0}{10} = 6/5$$
$$x_3 == 36/25 - 2 - 2 = -64/25$$
$$y_3 = 6/5(2 + 64/25) - 5 = 59/125$$

so $\mathbf{2Q} = (\mathbf{-64/25}, \mathbf{59/125})$.

4. Find every point, and sketch a picture, of:

(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.

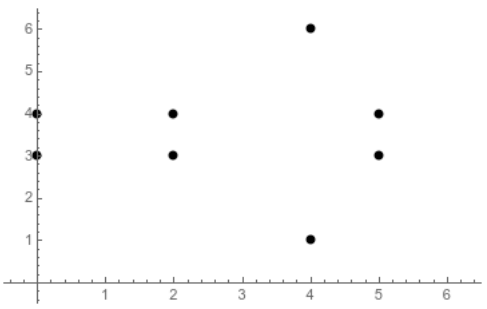
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$
$6^2 \equiv 1$	$5^2 \equiv 4$	$4^2 \equiv 2$

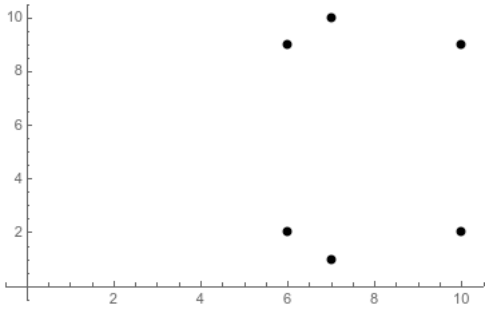
So our squares are $0, 1, 2, 4$.
Now we compute

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

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:

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

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

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

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

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

   (b) 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

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

6. 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

$$\begin{aligned} 2P &= (34, 33) \\ 4P &= (26, 33) \\ 8P &= (62, 48) \\ 16P &= (67, 60) \end{aligned}$$

   (a) Bob sends $n_B P = 10(3, 21) = (62, 48) \oplus (34, 33) = (20, 16)$.

   (b) Bob computes

$$\begin{aligned} 2Q_A &= (9, 6) \\ 4Q_A &= (33, 43) \\ 8Q_A &= (34, 50) \\ 10Q_A &= (1, 28) \end{aligned}$$

   and thus $n_b Q_A = 10(71, 82) = (1, 28)$.

7. 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 $Q_A = n_A P = 16P \oplus P = (67, 60) \oplus (3, 21) = (54, 40)$.

   (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 $C_2 - n_A C_1 = (71, 82) - 17(30, 8)$. We have $17(30, 8) = (24, 69)$, so the message is $M = (17, 82) - (24, 69) = (51, 37)$.