Math 4981 Spring 2021
Cryptography HW 9
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?

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.

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.)

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 $\mathbb{F}_{11}$.

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.

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?

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?