Note: Please cite any resources used, and mention any classmates that you worked with on this assignment. If you worked alone, please also say so. We will start taking points off if this is missing.

Problem 1. Elliptic Curve Important Points

(a) On an elliptic curve, what is the negative of a point A?

(b) What is zero on an elliptic curve, and why is it important from a group theory perspective?

In answering both questions, consider the case where x and y vary over the real numbers.

Problem 2. Elliptic Curve Addition

When computing $A \bigoplus B = C$, we take the straight line through A and B and find the point it intersects the elliptic curve. We then reflect that point through the x-axis. If we don't do this reflection, this breaks something about elliptic curve addition. What have we broken?

Recall the rules for adding points together on an Elliptic Curve modulo p:
Rule 1: $P \bigoplus \mathcal{O} = P$
Rule 2: $(x, y) \bigoplus (x, -y) = \mathcal{O}$
Rule 3: Otherwise, first calculate:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P = Q \end{cases} \tag{1}$$

and then $P \bigoplus Q = (x_3, y_3)$, where $x_3 = (\lambda^2 - x_1 - x_2)$ and $y_3 = \lambda(x_1 - x_3) - y_1$.

For the remaining problems, we will be using the following Elliptic Curve: $y^2 \equiv x^3 + 4x + 3 \ (mod\ 7)$.
Below is the complete addition table for this Elliptic Curve. You can use it for reference.

$\bigoplus$	$\mathcal{O}$	**(1,1)**	**(1,6)**	**(3,0)**	**(5,1)**	**(5,6)**
$\mathcal{O}$	$\mathcal{O}$	$(1,1)$	$(1,6)$	$(3,0)$	$(5,1)$	$(5,6)$
(1,1)	$(1,1)$	$(5,6)$	$\mathcal{O}$	$(5,1)$	$(1,6)$	$(3,0)$
(1,6)	$(1,6)$	$\mathcal{O}$	$(5,1)$	$(5,6)$	$(3,0)$	$(1,1)$
(3,0)	$(3,0)$	$(5,1)$	$(5,6)$	$\mathcal{O}$	$(1,1)$	$(1,6)$
(5,1)	$(5,1)$	$(1,6)$	$(3,0)$	$(1,1)$	$(5,6)$	$\mathcal{O}$
(5,6)	$(5,6)$	$(3,0)$	$(1,1)$	$(1,6)$	$\mathcal{O}$	$(5,1)$

Problem 3. Elliptic Curve Points

Prove that the only points on the Elliptic Curve $y^2 \equiv x^3 + 4x + 3 \ (mod\ 7)$ are the following:

$$\{\mathcal{O}, (1,1), (1,6), (3,0), (5,1), (5,6)\}$$

Problem 4. Elliptic Curve Addition rules

(a) Which rule above justifies the following calculations? (Just name which Rule)
$\mathcal{O} \bigoplus \mathcal{O} = \mathcal{O}; \mathcal{O} \bigoplus (1,1) = (1,1); \mathcal{O} \bigoplus (1,6) = (1,6); \mathcal{O} \bigoplus (3,0) = (3,0); \mathcal{O} \bigoplus (5,1) = (5,1); \mathcal{O} \bigoplus (5,6) = (5,6)$

(b) Which rule above justifies the following calculations? (Just name which Rule)
$(1,1) \bigoplus (1,6) = \mathcal{O}; (3,0) \bigoplus (3,0) = \mathcal{O}; (5,1) \bigoplus (5,6) = \mathcal{O}.$

Problem 5. Elliptic Curve Point Additions

(a) Show that $(1,1) \bigoplus (1,1) = (5,6)$. Write out your work.

(b) Show that $(5,1) \bigoplus (5,1) = (5,6)$. Write out your work.

(c) Show that $(1,1) \bigoplus (3,0) = (5,1)$. Write out your work.

(d) Show that $(1,1) \bigoplus (5,6) = (3,0)$. Write out your work.

(e) Show that $(1,6) \bigoplus (5,1) = (3,0)$. Write out your work.