**Due Aug 11, 2025**

**MATH 173B: Cryptology II**
**Homework 1: Elliptic Curves**

**Instructions:** Please answer the following questions carefully. Show all your work to receive full credit. Write your answers clearly and justify each step.

# 1 Problem 1 (15pts)

Below is the the textbook page 305. Chapter 6.1. Theorem 6.6

**Theorem 6.6** (Elliptic Curve Addition Algorithm). *Let*

$$E : Y^2 = X^3 + AX + B$$

*be an elliptic curve and let $P_1$ and $P_2$ be points on $E$.*
(a) *If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$.*
(b) *Otherwise, if $P_2 = \mathcal{O}$, then $P_1 + P_2 = P_1$.*
(c) *Otherwise, write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.*
(d) *If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \mathcal{O}$.*
(e) *Otherwise, define $\lambda$ by*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2, \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2, \end{cases}$$

*and let*

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \text{and} \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

*Then $P_1 + P_2 = (x_3, y_3)$.*

1. Let $P_1 = P_2$. Briefly explain what $\lambda$ means geometrically in this case. Prove in part (e) that
$$\lambda = \frac{3x_1^2 + A}{2y_1}.$$
2. **Fact 1:** Any line intersects a cubic curve exactly three times (counting multiplicity). Use this fact to explain why an inverse always exists under the addtion law. That is, let $P \in E$ be a point on the elliptic curve. Show that there exists a point $Q \in E$ such that $P + Q = \mathcal{O}$.
3. This is an alternative proof for part (2). Use Theorem 6.6 to show that the additive inverse exists. *Hint:* Start with $P = (x_1, y_1)$, and let $Q = (x_1, -y_1)$. Think about what needs to be checked.

# 2 Problem 2 (20pts)

**Exercise 6.2 from the textbook**
Here is a Visualization help; Desmos Elliptic Grapher:https://www.desmos.com/calculator/jzkq2soxyf
Let$P = (-1, 4)$ and $Q = (2, 5)$. Let E be the elliptic curve defined as follow:

$$E : Y^2 = X^3 + 17.$$

Please answer the following questions:

(0) Check that the points $P = (-1, 4)$ and $Q = (2, 5)$ lie on the elliptic curve E.

(a) Compute the points $P \oplus Q$ and $P \ominus Q$.

(b) Compute the points $2P$ and $2Q$.

(c) How many points with integer coordinates can you find on $E$? Explaine your answer.

# 3 Problem 3 (20pts)

**Exercise 6.5.** For each of the following elliptic curves $E$ over finite fields $\mathbb{F}_p$, list all the points $E(\mathbb{F}_p)$. That is, find all pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ that satisfy the curve equation, and include the point at infinity $\mathcal{O}$.

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

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

# 4 Problem 4 (10pts)

**Exercise 6.6.** Make an addition table for the elliptic curve $E$ over $\mathbb{F}_5$, as shown in Table 6.1.

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

*hint:* First, determine all points $(x, y) \in \mathbb{F}_5 \times \mathbb{F}_5$ that lie on the curve. Don't forget to include the point at infinity $\mathcal{O}$. Then construct the group addition table, listing all these points along both the top row and left column. Fill in each entry with the result of adding the two points according to the elliptic curve group law over $\mathbb{F}_5$.

# 5 Problem 5 (15pts)

**Exercise 6.8.** Let $E$ be the elliptic curve

$$E : y^2 = x^3 + x + 1$$

over $\mathbb{F}_5$. Let $P = (4, 2)$ and $Q = (0, 1)$ be points on $E(\mathbb{F}_5)$.

Solve the elliptic curve discrete logarithm problem (ECDLP) for $P$ and $Q$; that is, find the smallest positive integer $n$ such that

$$Q = nP.$$

# 6 Problem 6 (20pts)

**Exercise 6.9.** Let $E$ be an elliptic curve over $\mathbb{F}_p$, and let $P, Q \in E(\mathbb{F}_p)$ such that $Q$ is a multiple of $P$. Let $n_0 > 0$ be the smallest positive integer such that $Q = n_0 P$. Also, let $s > 0$ be the smallest positive integer such that

$$sP = \mathcal{O},$$

where $\mathcal{O}$ is the point at infinity.

Prove that every solution $n$ to the equation $Q = nP$ is of the form

$$n = n_0 + is \quad \text{for some } i \in \mathbb{Z}.$$

*Hint:* Write $n = is + r$ with $0 \le r < s$, and analyze the value of $r$.