Theorem 6.6: $E : Y^2 = X^3 + AX + B, \quad 4A^3 + 27B^2 \neq 0$

Let P_1 and P_2 be two points on E

- If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$
  If $P_2 = \mathcal{O}$, then $P_1 + P_2 = P_1$
- Otherwise, write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$
  - If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 = -P_2$ in E and $P_1 + P_2 = \mathcal{O}$
  - Otherwise, define

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } P_1 \neq P_2 \\ \\ (3x_1^2 + A)(2y_1)^{-1} & \text{if } P_1 = P_2 \end{cases}$$

  Then $P_1 + P_2 = (x_3, y_3)$ where

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

Let $E: Y^2 = X^3 + 17X + 3$ over $\mathbb{F}_{59}$ and let $P = (3, 50)$ and $Q = (41, 1)$

1. Show P and Q lie on $E(\mathbb{F}_{59})$ but do not lie on the curve if we do not reduce mod 59
2. Find $P + Q$ by applying Theorem 6.6 by hand
3. Find $2P$ by applying Theorem 6.6 by hand
4. Use the double and add algorithm to compute $37P$
   For this problem, you may use
   `https://andrea.corbellini.name/ecc/interactive/modk-add.html`
   to add two points or to double a point.
5. According to Hasse's Theorem, what is the minimum number of points that an elliptic curve over $\mathbb{F}_{59}$ can have? What is the maximum number?
   Is this consistent with the information from the website for our particular curve?