## 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

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

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

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

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

1. Show $P$ and $Q$ lie on $E(\mathbb{Z}_{59}^*)$ but do not lie on the curve if we do not reduce mod 59

2. Find $P + Q$ by applying Theorem 6.6

3. Find $2P$ by applying Theorem 6.6

4. How could you use a "double-and-add" algorithm to compute $37P$?

# Elliptic Curve Diffie-Hellman Key Exchange

### *Trusted Party*

- Generate $E(\mathbb{F}_p) : Y^2 = X^3 + AX + B$ and $P \in E(\mathbb{F}_p)$ of large prime order $q$
- Publish $(p, A, B, P, q)$

### *Alice*

- Select $n_A$ where $1 < n_A < q$
- Compute $Q_A = n_A P \in E(\mathbb{F}_p)$
- Send $Q_A$ to Bob

### *Bob*

- Select $n_B$ where $1 < n_B < q$
- Compute $Q_B = n_B P \in E(\mathbb{F}_p)$
- Send $Q_B$ to Alice

Shared key is $Q = n_A n_B P = n_B n_A P$