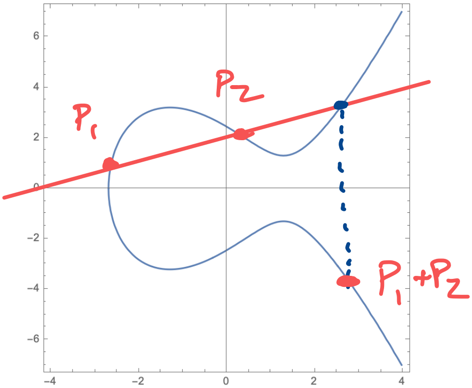
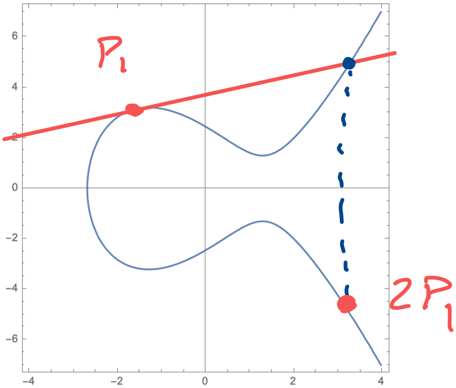
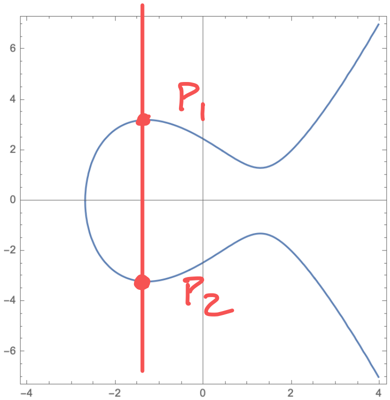
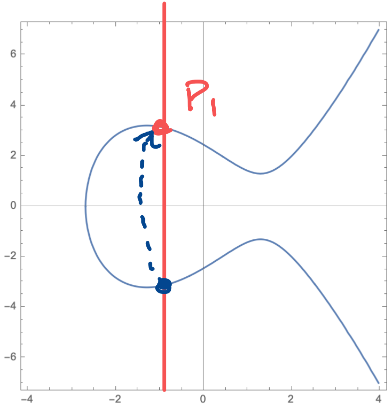
Addition on Elliptic Curve $E : Y^2 = X^3 + AX + B, \quad 4A^3 + 27B^2 \neq 0$





Note: The first 7 slides are from
Advanced Crypto in Spring 2021



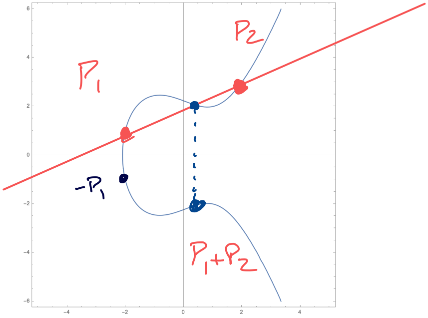


why need point $\mathcal{O}$ at ∞
(y = infinity)

$P_1 + \mathcal{O} = P_1$

Example: $E : Y^2 = X^3 - 2X + 5$, $P_1 = (-2, 1)$ and $P_2 = (2, 3)$

Find $P_1 + P_2$



what is $-P_1$?

$-P_1 = (-2, -1)$

Line thru P_1 and P_2

$$\text{slope} = \frac{\text{rise}}{\text{run}} = \frac{3-1}{2-(-2)} = \frac{1}{2}$$

$$y - 1 = \frac{1}{2}(x - (-2))$$

$$y = \frac{1}{2}x + 2$$

To find 3rd point:

$$\left(\frac{1}{2}x + 2\right)^2 = x^3 - 2x + 5$$

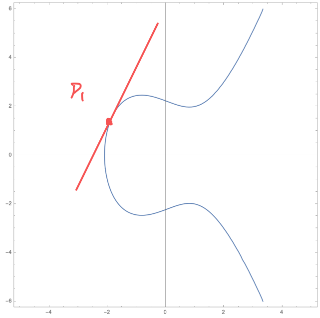
Multiply out, then $(x+2)$ and $(x-3)$ must be factors

$x = \frac{1}{4}$ $\quad y = \frac{17}{8}$

$$\boxed{P_1 + P_2 = \left(\frac{1}{4}, -\frac{17}{8}\right)}$$

Example: $E : Y^2 = X^3 - 2X + 5$, $P_1 = (-2, 1)$ **and** $P_2 = (2, 3)$

Find $2P_1$



Form tangent line

Slope of tangent line $\frac{dY}{dX}$

$$\frac{d}{dx} Y^2 = \frac{d}{dx}(x^3 - 2x + 5)$$

$$2Y \frac{dY}{dx} = 3x^2 - 2$$

$$\frac{dY}{dx} = \frac{3x^2 - 2}{2Y}$$

At $P_1 = (-2, 1)$,

$$\frac{dY}{dX} = 5$$

$$Y - 1 = 5(X + 2)$$

$$y = 5X + 11$$

$$(5x + 11)^2 = x^3 - 2x + 5$$

$x = 29$ $Y = 156$

$$\boxed{2P_1 = (29, -156)}$$

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

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

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

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

$E : Y^2 = X^3 - 2X + 5,\quad P_1 = (-2, 1)$ **and** $P_2 = (2, 3)$.

Find $P_1 + P_2$

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

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \frac{3-1}{2-(-2)} = \frac{1}{2}$$

$$x_3 = \left(\frac{1}{2}\right)^2 - \cancel{(-2)} - \cancel{2}$$

$$= \frac{1}{4}$$

$$y_3 = \frac{1}{2}\left(-2 - \frac{1}{4}\right) - 1$$

$$= \frac{1}{2}\left(-\frac{9}{4}\right) - 1$$

$$= -\frac{9}{8} - 1$$

$$= -\frac{17}{8}$$

$E: Y^2 = X^3 - 2X + 5$, $\boxed{P_1 = (-2, 1)}$

Find $2P_1$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases} \qquad x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \frac{3(-2)^2 + (-2)}{2(1)} = 5$$

$$x_3 = 5^2 - (-2) + 2 = 29$$

$-(-2)$

$$y_3 = 5(-2 - 29) - 1 = -155 - 1 = -156$$

NOTE: If P_1 and P_2 are rational, then $P_1 + P_2$ is rational!!

ECDLP: Solve $ng = h$ where $g, h \in E$

1. Use Mathematica to draw the following elliptic curves

(a) Let $E : Y^2 = X^3 - 5X + 6$
Verify $4A^3 + 27B^2 \neq 0$
How many points on E are their own additive inverse?
i.e. How many points on E satisfy $P = -P$?

(b) $E : Y^2 = X^3 - 4X + 1$
Verify $4A^3 + 27B^2 \neq 0$
How many points on E are their own additive inverse?

(c) $E : Y^2 = X^3 - 3X + 2$
Verify $4A^3 + 27B^2 = 0$
By looking at the graph, why is this a problem for defining addition on E?

(d) $E : Y^2 = X^3$
Verify $4A^3 + 27B^2 = 0$
By looking at the graph, why is this a problem for defining addition on E?

2. Consider the elliptic curve $E : Y^2 = X^3 - 6X + 5$

(a) Verify that $P_1 = (-2, 3)$ and $P_2 = (2, 1)$ lie on E

(b) Use the geometric description of addition on E to find $P_1 + P_2$

(c) Use the geometric description of addition on E to find $2P_1$

(d) Use Theorem 6.6 to verify your answers to (b) and (c)

(e) Verify that $Q_1 = \left(\frac{1}{4}, -\frac{15}{8}\right)$ and $Q_2 = \left(\frac{58}{9}, \frac{413}{27}\right)$ lie on E

(f) Use Theorem 6.6 to find $Q_2 + Q_1$ and $Q_1 - Q_1$

Note: $-Q_1$ means the additive inverse of Q_1 in E