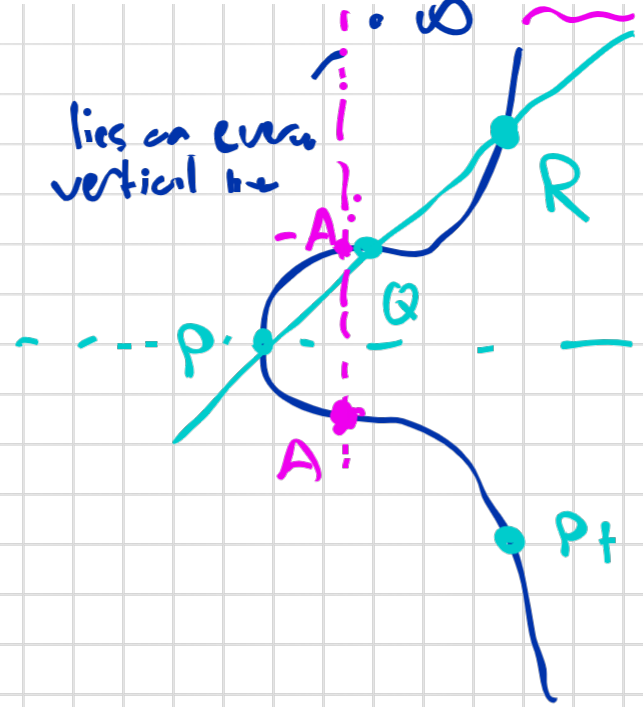
$y^2 = x^3 + B$



when flip ∞ about the x-axis, get ∞ back.

Solutions in $\mathbb{R}^2$ (x, y).

To add P, Q —

1. Draw the line between them
2. Find the 3rd point of intersection (R)
3. Flip it about the x-axis to get P+Q.

This really is a group law (commutative) — hard thing to check.

- ∞ is the identity element
- $P = (x, y)$ $-P = (x, -y)$.
- $P + Q = Q + P$ } easy

$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ ← Hard to verify.

Some complicated geometric statement about lines intersecting the curve.

Today: Give Formula for adding two points.

Exercise 1.-(1).

Need to 1) parametrize $\ell = PQ$ (variable is t)

2) plug in your parameterization to $y^2 = x^3 + 8$

get degree 3 polynomial in t

$t^3 + at^2 + bt + c$.

roots $\leftrightarrow$ points of intersection

Use that you already know 2 roots

roots $t = \underbrace{\alpha_P \quad \alpha_Q}_{\text{know}} \quad \underbrace{\alpha_R}_{\text{want}}$

$$t^3 + at^2 + bt + c = (t-\alpha_P)(t-\alpha_Q)(t-\alpha_R)$$

$$a = -\alpha_P - \alpha_Q - \alpha_R$$

expand coefficient of t^2

$$-a - \alpha_P - \alpha_Q = \alpha_R$$

$P = (x_P, y_P)$
$Q = (x_Q, y_Q)$

$\vec{v} = Q - P = (v_1, v_2) = (x_Q - x_P, y_Q - y_P)$

$l = PQ$ parameterised as $\gamma(t) = P + t\vec{v}$

$\gamma(0) = P \qquad \gamma(1) = P + (Q-P) = Q$

$$\gamma(t) = (x(t), y(t)) = (x_P + t(x_Q - x_P), y_P + t(y_Q - y_P))$$

Intersection values of t are solutions to

$$y(t)^2 = x(t)^3 + 8$$

$$\Leftrightarrow$$

$$y(t)^2 - x(t)^3 - 8 = 0$$

Know roots $t = 0, 1$ corresponding to P, Q.

Need to expand out to get coeff. of t^2 to apply trick for 3rd root.

$$0 = (y_P + t(y_Q - y_P))^2 - (x_P + t(x_Q - x_P))^3 + 8.$$

$$0 = -(x_Q - x_P)^3 t^3 + ((y_Q - y_P)^2 - 3x_P(x_Q - x_P)^2)\, t^2 + \dots$$

Divide by $-(x_Q - x_P)^3$

$$0 = t^3 + \left(\frac{-(y_Q - y_P)^2}{(x_Q - x_P)^3} + \frac{3x_P}{(x_Q - x_P)} \right) t^2 + \ldots$$

So third root is

$$t_R = \frac{(y_Q - y_P)^2}{(x_Q - x_P)^3} - \frac{3x_P}{x_Q - x_P} - 1 - 0.$$

So $R = \gamma(t_R) =$

$$\left(x_P + \frac{(y_Q - y_P)}{(x_Q - x_P)^2} - 3x_P - (x_Q - x_P), \right.$$

$$\left. y_P + \frac{(y_Q - y_P)^3}{(x_Q - x_P)^3} - 3x_P \frac{(y_Q - y_P)}{x_Q - x_P} - (y_Q - y_P) \right)$$

$$= \left(-x_P - x_Q + \frac{(y_Q - y_P)^2}{(x_Q - x_P)^2},\ 2y_P - y_Q + \frac{(y_Q - y_P)^3}{(x_Q - x_P)^3} - 3x_P\left(\frac{y_Q - y_P}{x_Q - x_P}\right)\right).$$

$$= \left(-x_P - x_Q + m^2,\ 2y_P - y_Q + m^3 - 3x_P m\right).$$

$\hat{\Sigma}$ Intersection R

$$P + Q = \left(-x_P - x_Q + m^2,\ 2y_P - y_Q + m^3 - 3x_P m\right).$$