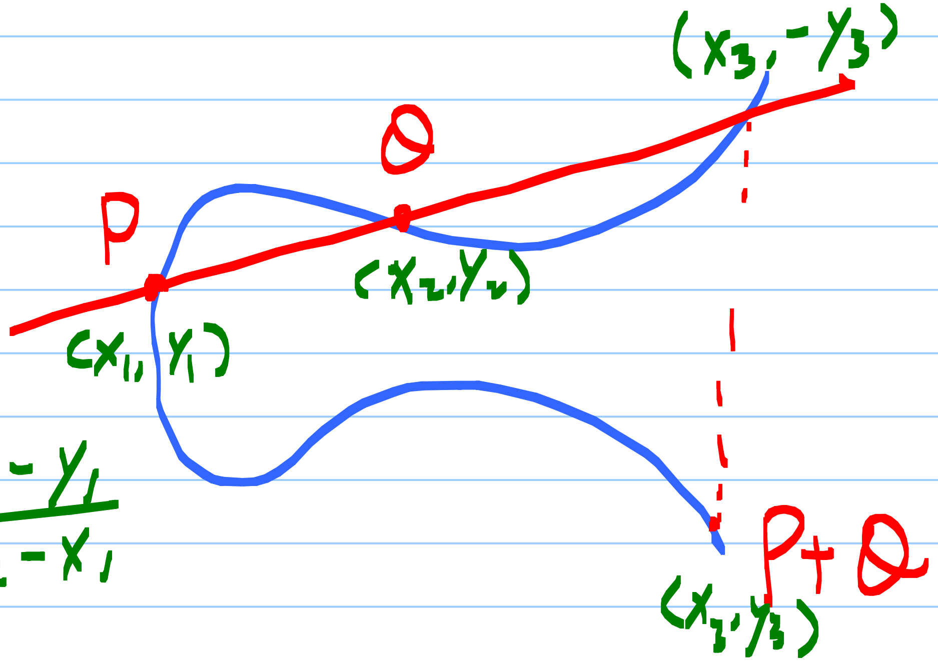
$P + Q$

$2P$

$P = (x_1, y_1) \quad Q = (x_2, y_2)$

[1] $P + Q$



斜率

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

令直线方程式为

$$\lambda = \frac{y - y_1}{x - x_1} \Rightarrow y = \lambda(x - x_1) + y_1$$

代入 $y^2 = x^3 + ax + b$

$$(\lambda(x - x_1) + y_1)^2 = x^3 + ax + b$$

x_1, x_2, x_3 为其解 $\Rightarrow (x - x_1)(x - x_2)(x - x_3) = 0$

根與係數關係

$$x_1+x_2+x_3=-c_2$$

where $x^3+c_2x^2+c_1x+c_0=0$

$$(\lambda(x-x_1)+y_1)^2=x^3+ax+b$$

$$c_2=-\lambda^2$$

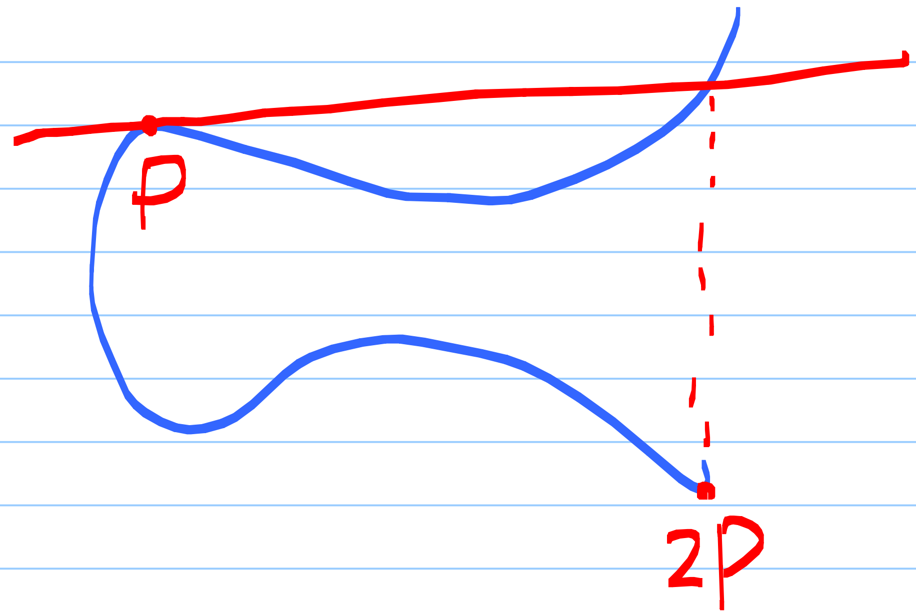
$$\therefore x_1+x_2+x_3=\lambda^2$$

$$\therefore\ x_3 = \lambda^2 - x_1 - x_2$$

$$\lambda = \frac{(-y_3) - y_1}{x_3 - x_1}$$

$$\therefore\ y_3 = \lambda(x_1 - x_3) - y_1$$

[2] $2P = P + P$



$P = (x_1, y_1)$

线方程式

$$\lambda = \frac{y - y_1}{x - x_1}$$

$\lambda = ?$

$$y^2 = x^3 + ax + b$$

对 x 微分

$$2y\,y' = 3x^2 + a$$

$$\therefore\ y' = \frac{3x^2 + a}{2y}$$

$$\lambda = y'\Big|_{\substack{y=y_1 \\ x=x_1}} = \frac{3x_1^2 + a}{2y_1}$$

Same as in [ ]

直线代入曲线方程式解 x_3

$$(\lambda(x-x_1)+y_1)^2 = x^3+ax+b$$

$$\Rightarrow x^3+c_2x^2+c_1x+c_0=0$$

$$2x_1+x_3=-c_2=\lambda^2$$

$$\therefore\ x_3 = \lambda^2 - 2x_1$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$\boxed{\diagup\!\!\diagup}$