Formula Sheet

Let E be the elliptic curve over a field $\mathbf{F}$ defined by the Weierstrass equation

$$E: \ y^2 = x^3 + ax + b, \qquad \text{where } \Delta = -16(4a^3 + 27b^2) \neq 0.$$

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points in $E(\mathbf{F})$.

Addition Formula: If $x_1 \neq x_2$ then $P + Q = (x_3, y_3)$, where

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= -(mx_3 + n) \\ m &= \frac{y_2 - y_1}{x_2 - x_1} \\ n &= y_1 - mx_1 = y_2 - mx_2. \end{aligned}$$

Duplication Formula: If $[2]P \neq \mathcal{O}$ then $[2]P = (x_2, y_2)$, where

$$\begin{aligned} x_2 &= m^2 - 2x_1 \\ y_2 &= -(mx_2 + n) \\ m &= \frac{3x_1^2 + a}{2y_1} \\ n &= y_1 - mx_1. \end{aligned}$$