

Approche géométrique de la loi de la sécante-tangente

Soit E une courbe elliptique définie sur $\mathbb{P}^2(\mathbb{K})$ par :

$$E : Y^2 Z = X^3 + aXZ^2 + b \quad (1)$$

soit encore en coordonnées non homogènes (en posant $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$) :

$$E : y^2 = x^3 + ax + b \cup \mathcal{O} = (0, 1, 0) \quad (2)$$

On peut alors définir sur E une loi de composition $*$ dite *loi de composition de la sécante-tangente* :

- si $(P, Q) \in E^2$ avec $P \neq Q$, on définit $P * Q$ comme étant le troisième point d'intersection de la droite D passant par P et Q avec E

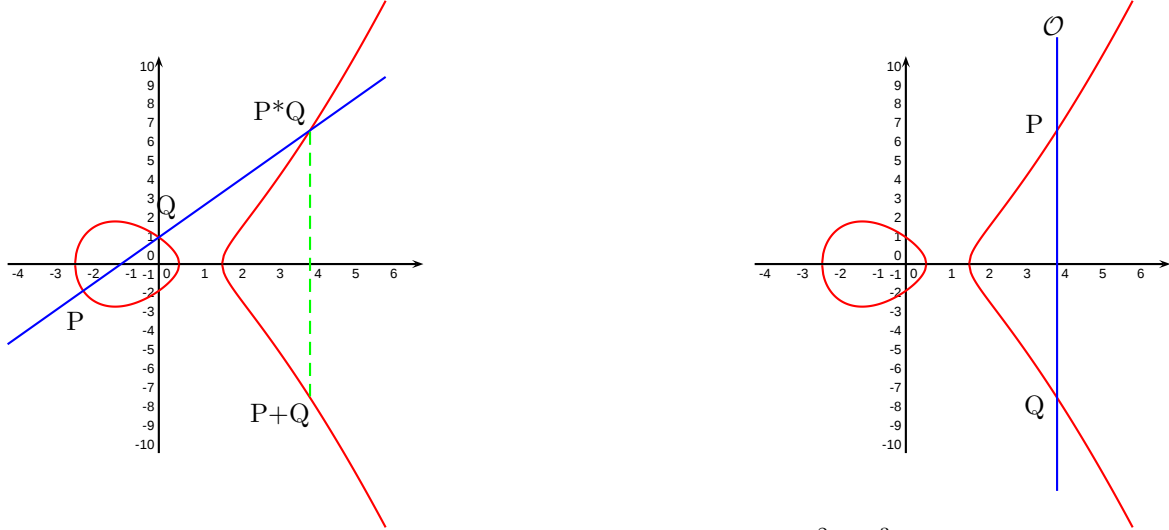


FIG. 1 – Calcul de $P * Q$ dans la courbe elliptique $E : y^2 = x^3 - 4x + 2 \cup \mathcal{O}$

- si $P \in E$, on définit $P * P$ comme étant le troisième point d'intersection de la droite D tangente à la courbe en P avec E (P est alors considéré comme un point double d'intersection)

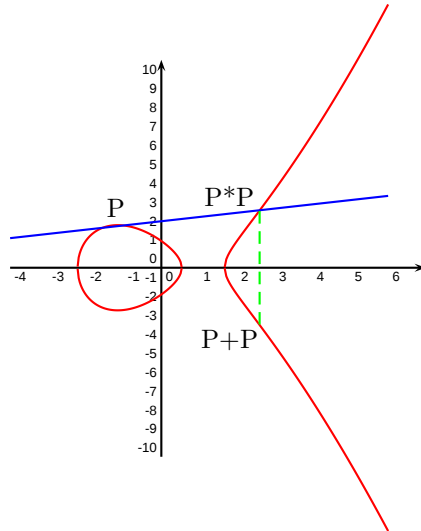


FIG. 2 – Calcul de $P * P$ dans la courbe elliptique $E : y^2 = x^3 - 4x + 2 \cup \mathcal{O}$

Remarque 1. On a aussi représenté $P + Q = \mathcal{O} * (P * Q)$.