Group law on an elliptic curve: Explicit addition formulas.

Elliptic curve E given over some field k by a general Weierstrass equation:

$$(*) \qquad E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ .$$

As usual $E(k)$ denotes the set of points on E that are defined over k. The set $E(k)$ is endowed with a structure of an abelian group. We give here explicit formulas for the composition of points in $E(k)$.

(I). When viewing $(*)$ projevtively we have 'the point at infinity' $O := (0,1,0)$ in projective coordinates (x,y,z). This is the neutral element in the group structure on $E(k)$.

Now let $P_i = (x_i, y_i)$, $i = 1,2$ be 2 points in $E(k)$.

(II). Notice, that if $x_1 = x_2$ then

$$y_1^2 + a_1x_1y_1 + a_3y_1 = y_2^2 + a_1x_1y_2 + a_3y_2 \ ,$$

and hence *either*

$$y_1 = y_2$$

or

$$y_2 = -y_1 - a_1x_1 - a_3 \ .$$

(III). Define the inverse $-P_1$ of the point P_1 thus:

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3) \ .$$

(IV). Now we give the coordinates (x_3, y_3) of the point $P_3 := P_1 + P_2$ in case $P_2 \neq -P_1$ (if $P_2 = -P_1$ then $P_1 + P_2 = O$).

Suppose first that $x_1 \neq x_2$. In that case define

$$\lambda := \frac{y_2 - y_1}{x_2 - x_1} \ , \qquad \nu := \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \ .$$

Suppose then that $x_1 = x_2$. Since $P_2 \neq -P_1$ it follows from **(II)** and **(III)** that we must have $P_2 = P_1$. Then again from **(II)**, and because we now know that $P_1 \neq -P_1$, we have $y_1 \neq -y_1 - a_1x_1 - a_3$. We may then define:

$$\lambda := \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \ , \qquad \nu := \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \ .$$

One checks that $y = \lambda x + \nu$ is precisely the equation for the line through P_1 and P_2, if $P_1 \neq P_2$, and is the equation for the tangent to E at the point P_1, if $P_1 = P_2$.

In any case the formulas for x_3 and y_3 are:

$$x_3 := \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \ , \quad y_3 := -(\lambda + a_1)x_3 - \nu - a_3 \ .$$

If one takes the above as *definition* of the addition in $E(k)$, one can in principle check by machine (Maple) that $(E(k), +)$ thus becomes an abelian group.