Complete Addition Formulae for Elliptic Curves

Marc Joye
Technicolor
marc.joye@technicolor.com

Consider the elliptic curve \( E \) over a field \( \mathbb{K} \) (with \( \text{Char} \mathbb{K} \neq 2, 3 \)) given by a Weierstraß equation

\[
Y^2Z = X^3 + aXZ^2 + bZ^3
\]

where \( a, b \in \mathbb{K} \) are constants, \( 4a^3 + 27b^2 \neq 0 \). The set \( E(\mathbb{K}) \) of points \( (X : Y : Z) \in \mathbb{P}^2(\mathbb{K}) \) forms an abelian group under the chord-and-tangent rule, with neutral element \( O = (0 : 1 : 0) \). The addition law is written additively. The negative of a point \( P_1 = (X_1 : Y_1 : Z_1) \) is \( (X_1 : -Y_1 : Z_1) \). Given two points \( P_1 = (X_1 : Y_1 : Z_1) \) and \( P_2 = (X_2 : Y_2 : Z_2) \), we let \( P_3 := P_1 + P_2 = (X_3 : Y_3 : Z_3) \).

**Addition Algorithm.** The usual algorithm (e.g., see [6, Chapter III, §2]) for adding two points on \( E(\mathbb{K}) \) distinguishes several cases:

1. If \( P_1 = O \) then \( P_3 = (X_2 : Y_2 : Z_2) \);
2. If \( P_2 = O \) then \( P_3 = (X_1 : Y_1 : Z_1) \);
3. If \( P_1 = -P_2 \) then \( P_3 = (0 : 1 : 0) \);
4. If \( P_1 \neq \pm P_2 \) and \( P_1, P_2 \neq O \) then \( P_3 = (X_3 : Y_3 : Z_3) \) where

\[
\begin{align*}
X_3 &= (X_1Z_2 - X_2Z_1)X'_3, \\
Y_3 &= (Y_1Z_2 - Y_2Z_1)\left[(X_1Z_2 - X_2Z_1)^2X_1Z_2 - X'_3\right] - (X_1Z_2 - X_2Z_1)^3Y_1Z_2, \\
Z_3 &= (X_1Z_2 - X_2Z_1)^3Z_1Z_2
\end{align*}
\]  

(1)

with \( X'_3 = (Y_1Z_2 - Y_2Z_1)^2Z_1Z_2 + (X_1Z_2 - X_2Z_1)^3 - 2(X_1Z_2 - X_2Z_1)^2X_1Z_2 \).

5. If \( P_1 = P_2 \neq O \) then \( P_3 = (X_3 : Y_3 : Z_3) \) where

\[
\begin{align*}
X_3 &= 2Y_1Z_1\left[(3X_1^2 + aZ_1^2)^2 - 8X_1Y_1^2Z_1\right], \\
Y_3 &= (3X_1^2 + aZ_1^2)\left[12X_1Y_1^2Z_1 - (3X_1^2 + aZ_1^2)^2\right] - 2(2Y_1^2Z_1)^2, \\
Z_3 &= (2Y_1Z_1)^3
\end{align*}
\]  

(2)

Borrowing the notation of [1], \( M, S, \) and \( \text{add} \) will respectively stand for the cost of a field multiplication, a field squaring, and a field addition (in \( \mathbb{K} \)), and \( *c \) will stand for the cost of the multiplication by some given constant \( c \in \mathbb{K} \).

A careful operation count shows that the addition operation (1) costs \( 12M + 2S + 6\text{add} + 1*2 \) and that the doubling operation (2) costs \( 5M + 6S + 1*a + 7\text{add} + 3*2 + 1*3 \) [1,3].

A complete addition law. It is worth noting that formulae (1) and (2) are not valid for the point at infinity \( O \). We present below a formula that is valid for \( O \), as well as for the case \( P_1 = P_2 \). It is adapted from Formula III in [4, Section 3] and optimized.
Let \( P_1 = (X_1 : Y_1 : Z_1) \) and \( P_2 = (X_2 : Y_2 : Z_2) \). We assume that \( P_1 - P_2 \) is not a finite\(^1\) point of order 2. Then \( P_3 := P_1 + P_2 = (X_3 : Y_3 : Z_3) \) is given by

\[
\begin{align*}
X_3 &= (X_1 Y_2 + X_2 Y_1)[Y_1 Y_2 - 3b Z_1 Z_2 - a(X_1 Z_2 + X_2 Z_1)] - \\
&\quad (Y_1 Z_2 + Y_2 Z_1)[a(X_1 X_2 - a Z_1 Z_2) + 3b(X_1 Z_2 + X_2 Z_1)] \\
Y_3 &= (Y_1 Y_2 + 3b Z_1 Z_2)(Y_1 Y_2 - 3b Z_1 Z_2) + a(X_1 X_2 - a Z_1 Z_2)(3X_1 X_2 + a Z_1 Z_2) + \\
&\quad (X_1 Z_2 + X_2 Z_1)[3b(X_1 X_2 - a Z_1 Z_2) - a^2(X_1 Z_2 + X_2 Z_1)] \\
Z_3 &= (Y_1 Z_2 + Y_2 Z_1)[Y_1 Y_2 + 3b Z_1 Z_2 + a(X_1 Z_2 + X_2 Z_1)] + (X_1 Y_2 + X_2 Y_1)(3X_1 X_2 + a Z_1 Z_2)
\end{align*}
\]

**Remark 1.** If \( P_1 - P_2 = (\xi : 0 : 1) \) for some \( \xi \in \mathbb{K} \) (i.e., it is a finite point of order 2) then \( P_3 = P_1 + P_2 = (X_3 : Y_3 : Z_3) \) is given by the usual addition algorithm; namely, \( P_3 \) is given by Eq. (1) if \( P_1, P_2 \neq O \), and by \( P_3 = (\xi : 0 : 1) \) if \( P_1 \) or \( P_2 = O \). As demonstrated in [2], the case \( P_1 - P_2 = (\xi : 0 : 1) \) for some \( \xi \in \mathbb{K} \) can also be handled by a single addition formula.

**Remark 2.** Reference [4] produces two other addition formulas that can handle \( O \). However, they do not fit our needs. The same formulas, extended to the long Weierstraß equations, can be found in [5,2].

**Detailed algorithm and complexity.**

\[
\begin{align*}
X_1 X_2 &= X_1 \ast X_2 \\
Y_1 Y_2 &= Y_1 \ast Y_2 \\
Z_1 Z_2 &= Z_1 \ast Z_2 \\
u &= (X_1 + Y_1) \ast (X_2 + Y_2) - X_1 X_2 - Y_1 Y_2 \\
v &= (X_1 + Z_1) \ast (X_2 + Z_2) - X_1 X_2 - Z_1 Z_2 \\
w &= (Y_1 + Z_1) \ast (Y_2 + Z_2) - Y_1 Y_2 - Z_1 Z_2 \\
Q_a &= a \ast Q \\
Z_a &= 3b \ast Z_1 Z_2 \\
Z_b &= 3b \ast Z_1 Z_2 \\
va &= a \ast v \\
P &= X_1 X_2 + Z_a \\
Q &= X_1 X_2 - Z_a \\
Q_a &= a \ast Q \\
M &= 2 \ast X_1 X_2 + P \\
R &= Y_1 Y_2 + Z_b \\
S &= Y_1 Y_2 - Z_b \\
X_3 &= u \ast (S - va) - w \ast (Q_a + 3b \ast v) \\
Y_3 &= R \ast S + Q_a \ast M + v \ast (3b \ast Q - a \ast va) \\
Z_3 &= w \ast (R + va) + u \ast M
\end{align*}
\]

Cost: \( 13M + 4a + 3 \ast 3b + 25add + 1 \ast 2 \).

**References**


\(^1\) By finite point, we mean a point with a \( Z \)-coordinate different from 0.

