Complete Addition Formulæ for Elliptic Curves

Marc Joye

Technicolor
marc.joye@technicolor.com

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

$$Y^2 Z = X^3 + aXZ^2 + bZ^3$$

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 $\boldsymbol{O} = (0 : 1 : 0)$. The addition law is written additively. The negative of a point $\boldsymbol{P_1} = (X_1 : Y_1 : Z_1)$ is $(X_1 : -Y_1 : Z_1)$. Given two points $\boldsymbol{P_1} = (X_1 : Y_1 : Z_1)$ and $\boldsymbol{P_2} = (X_2 : Y_2 : Z_2)$, we let $\boldsymbol{P_3} := \boldsymbol{P_1} + \boldsymbol{P_2} = (X_3 : Y_3 : Z_3)$.

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

$$\begin{cases} X_3 = (X_1Z_2 - X_2Z_1)X_3' \\ Y_3 = (Y_1Z_2 - Y_2Z_1)\big[(X_1Z_2 - X_2Z_1)^2\, X_1Z_2 - X_3'\big] - (X_1Z_2 - X_2Z_1)^3\, Y_1Z_2 \\ Z_3 = (X_1Z_2 - X_2Z_1)^3\, Z_1Z_2 \end{cases} \tag{1}$$

with $X_3' = (Y_1Z_2 - Y_2Z_1)^2\, Z_1Z_2 + (X_1Z_2 - X_2Z_1)^3 - 2(X_1Z_2 - X_2Z_1)^2\, X_1Z_2$.

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

$$\begin{cases} X_3 = 2Y_1Z_1\big[(3{X_1}^2 + a{Z_1}^2)^2 - 8X_1{Y_1}^2Z_1\big] \\ Y_3 = (3{X_1}^2 + a{Z_1}^2)\big[12X_1{Y_1}^2Z_1 - (3{X_1}^2 + a{Z_1}^2)^2\big] - 2(2{Y_1}^2Z_1)^2 \\ Z_3 = (2Y_1Z_1)^3 \end{cases} . \tag{2}$$

Borrowing the notation of [1], M, S, and add will respectively stand for the cost of a field multiplication, a field squaring, and a field addition (in $\mathbb{K}$), and $*\mathsf{c}$ 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 $\underline{12\mathsf{M} + 2\mathsf{S} + 6\mathsf{add} + 1{*}\mathsf{2}}$ and that the doubling operation (2) costs $\underline{5\mathsf{M} + 6\mathsf{S} + 1{*}\mathsf{a} + 7\mathsf{add} + 3{*}\mathsf{2} + 1{*}\mathsf{3}}$ [1,3].

A complete addition law. It is worth noting that formulæ (1) and (2) are not valid for the point at infinity $\boldsymbol{O}$. We present below a formula that is valid for $\boldsymbol{O}$, as well as for the case $\boldsymbol{P_1} = \boldsymbol{P_2}$. It is adapted from Formula III in [4, Section 3] and optimized.

Let $\boldsymbol{P_1} = (X_1 : Y_1 : Z_1)$ and $\boldsymbol{P_2} = (X_2 : Y_2 : Z_2)$. *We assume that* $\boldsymbol{P_1} - \boldsymbol{P_2}$ *is not a finite*[1] *point of order* 2. Then $\boldsymbol{P_3} := \boldsymbol{P_1} + \boldsymbol{P_2} = (X_3 : Y_3 : Z_3)$ is given by

$$\begin{cases} X_3 = (X_1Y_2 + X_2Y_1)\big[Y_1Y_2 - 3bZ_1Z_2 - a(X_1Z_2 + X_2Z_1)\big] - \\ \qquad\qquad (Y_1Z_2 + Y_2Z_1)\big[a(X_1X_2 - aZ_1Z_2) + 3b(X_1Z_2 + X_2Z_1)\big] \\ Y_3 = (Y_1Y_2 + 3bZ_1Z_2)(Y_1Y_2 - 3bZ_1Z_2) + a(X_1X_2 - aZ_1Z_2)(3X_1X_2 + aZ_1Z_2) + \\ \qquad\qquad (X_1Z_2 + X_2Z_1)\big[3b(X_1X_2 - aZ_1Z_2) - a^2(X_1Z_2 + X_2Z_1)\big] \\ Z_3 = (Y_1Z_2 + Y_2Z_1)\big[Y_1Y_2 + 3bZ_1Z_2 + a(X_1Z_2 + X_2Z_1)\big] + (X_1Y_2 + X_2Y_1)(3X_1X_2 + aZ_1Z_2) \end{cases} . \tag{3}$$

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

```
X1X2 = X1*X2
Y1Y2 = Y1*Y2
Z1Z2 = Z1*Z2
u = (X1+Y1)*(X2+Y2) - X1X2 - Y1Y2
v = (X1+Z1)*(X2+Z2) - X1X2 - Z1Z2
w = (Y1+Z1)*(Y2+Z2) - Y1Y2 - Z1Z2
Za = a*Z1Z2
Zb = 3b*Z1Z2
va = a*v
P = X1X2 + Za
Q = X1X2 - Za
Qa = a*Q
M = 2*X1X2 + P
R = Y1Y2 + Zb
S = Y1Y2 - Zb
X3 = u*(S - va) - w*(Qa + 3b*v)
Y3 = R*S + Qa*M + v*(3b*Q - a*va)
Z3 = w*(R + va) + u*M
```

Cost: 13M + 4∗a + 3∗3b + 25add + 1∗2.

References

1. Daniel J. Bernstein and Tanja Lange. Explicit-formulas database. http://www.hyperelliptic.org/EFD/.
2. Wieb Bosma and Hendrik W. Lenstra Jr. Complete systems of two addition laws for elliptic curves. *Journal of Number Theory*, 53(2):229–240, 1995.

[1] By finite point, we mean a point with a Z-coordinate different from 0.

3. Henri Cohen, Atsuko Miyaji, and Takatoshi Ono. Efficient elliptic curve exponentiation using mixed coordinates. In K. Ohta and D. Pei, editors, *Advances in Cryptology – ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 51–65. Springer, 1998.
4. Herbert Lange and Wolfgang Ruppert. Complete systems of addition laws on abelian varieties. *Inventiones mathematicae*, 79(3):603–610, 1985.
5. Herbert Lange and Wolfgang Ruppert. Addition laws on elliptic curves in arbitrary characteristics. *Journal of Algebra*, 107(1):106–116, 1987.
6. Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.