Note that in Y_3 ~~(or…)~~ formula we divide by 2. We have two options to avoid multiplication by $2^{-1} \pmod p$.

1) Instead of (X_3, Y_3, Z_3) we output $(2X_3, 2Y_3, 2Z_3)$, and this trick removes the divisor 2 in formula for Y_3.

2) If operations are performed in the prime field $\mathbb{F}_p$, then if the formula in square brackets [ ] yields an even number then we simply make a shift to the right, if it yields an odd value then we can assign

$$Y_3 := (\underbrace{[\ldots] + p}_{\text{even number if } [\ldots] \text{ is odd}})/2$$

Let us calculate the number of multiplications and squarings in both formulas: For multiplication we use M, S for squaring. The cost of squaring is lower, e.g. $S \approx 0{,}8 \cdot M$ (but depends on the architecture).

Point doubling:

$$
\begin{array}{l|l}
1M \rightarrow & S = 2Y_1Z_1 \\
2M \rightarrow & B = 2SX_1Y_1 = 2X_1(SY_1) \\
1M+2S \rightarrow & W = 3X_1^2 + aZ_1^2 \\
1S \rightarrow & h = W^2 - 2B \\
1M \rightarrow & X_3 = h \cdot S \\
1M+1S \rightarrow & Y_3 = W(B-h) - 2(SY_1)^2 \\
1S+1M \rightarrow & Z_3 = S^3
\end{array}
$$

$7M + 5S$

we do not count as multiplications the operations of type: $2 \cdot y$, $3 \cdot y$

we utilize the same value

Point addition:

$$
\left\{
\begin{array}{ll}
1M \rightarrow & U_1 = X_1 Z_2 \\
1M \rightarrow & U_2 = X_2 Z_1 \\
1M \rightarrow & S_1 = Y_1 Z_2 \\
1M \rightarrow & S_2 = Y_2 Z_1 \\
1M \rightarrow & W = Z_1 Z_2 \\
 & P = U_2 - U_1 \\
 & R = S_2 - S_1 \\
1S + 2M \rightarrow & Z_3 = ((P^2) \cdot P) \cdot W \\
1S + 4M \rightarrow & Y_3 = [\underbrace{R \cdot}_{1M} (\underbrace{-2WR^2}_{1S+1M} + \overbrace{3(U_1 + U_2)P^2}^{1M}) - \underbrace{(S_1 + S_2) \cdot P^3}_{1M}]/2 \\
1M & X_3 = \underbrace{P \cdot}_{1M} (WR^2 - (U_1 + U_2) \cdot P^2)
\end{array}
\right.
$$

$2S + 12M$

Let us check, how the formulas behave if we use "zero at infinity" $(0, Y_1, 0)$ as an ordinary point:

Doubling - border cases in projective coordinates:

1) $2 \cdot (0, Y_1, 0)$:

$$
\left\{
\begin{array}{l}
S = 0 \\
B = 0 \\
W = 0 \\
h = 0 \\
X_3 = 0 \\
Y_3 = 0 - 0 = \underline{\underline{0}} \\
Z_3 = 0
\end{array}
\right.
$$

wrong!

so unfortunately $\mathcal{O}$ must be handled separately!

2) Note that the negative of point (X_1, Y_1, Z_1) is $(X_1, -Y_1, Z_1)$ because the two points map to affine coordinates;

$\left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right)$ and $\left(\frac{X_1}{Z_1}, \frac{-Y_1}{Z_1}\right)$ correspondingly

Hence $(X_1, 0, Z_1) = -(X_1, 0, Z_1)$ and

consequently

$$2(X_1, 0, Z_1) = \Theta$$

"zero at infinity"

Let us check ~~how~~ this is reflected in the projective formula for point doubling:

$$Y_1 = 0$$

$$\begin{cases} S = 0 \\ B = 0 \\ W = 3X_1^2 + aZ_1^2 \\ h = W^2 \\ X_3 = 0 \\ Y_3 = W(B - h) = -W^3 \\ Z_3 = 0 \end{cases}$$

So we have Θ as a result, correct?

Point addition - border cases in projective coordinates:

1) (X_1, Y_1, Z_1), $(0, Y_2, 0)$

$$\begin{cases} u_1 = 0 \\ u_2 = 0 \\ S_1 = 0 \\ S_2 = Y_2 Z_1 \\ P = 0 \\ R = Y_2 Z_1 \end{cases}$$

$$\begin{cases} W = 0 \\ Z_3 = 0 \\ Y_3 = [R \cdot (0 + 3 \cdot 0 \cdot 0) - (0 + S_2) \cdot 0]/2 = 0 \\ X_3 = 0 \end{cases}$$

$Z_3 = 0$ - wrong for $Z_1 \neq 0$

again, Θ must be handled separately as an argument

2) (X_1, Y_1, Z_1), $(X_1, -Y_1, Z_1)$ or rather (X_1, Y_1, Z_1), $(\lambda X_1, -\lambda Y_1, \lambda Z_1)$: $\lambda \neq 0$

$$\begin{cases} U_1 = \lambda X_1 Z_1 \\ U_2 = \lambda X_1 Z_1 \\ S_1 = \lambda Y_1 Z_1 \\ S_2 = -\lambda Y_1 Z_1 \\ W = \lambda \cdot Z_1^2 \\ P = 0 \\ R = S_2 - S_1 = 2\lambda Y_1 Z_1 \\ Z_3 = 0 \\ Y_3 = [-2WR^3]/2 = -W \cdot R^3 = \\ \quad = \lambda Z_1^2 \cdot (2\lambda Y_1 Z_1)^3 = \\ \quad = 8 \cdot \lambda^4 Y_1^3 Z_1^5 \neq 0 \quad \text{if } Y_1 \neq 0 \\ X_3 = 0 \end{cases}$$

so the result is correct if $Y_1 \neq 0$. For $Y_1 = 0$ point doubling must be applied.

Doubling is detected by checking if $U_1 = U_2$ and $S_1 = S_2$

because in the affine coordinates we have $x_1 = x_2$ AND $y_1 = y_2$

$$\frac{X_1}{Z_1} = \frac{X_2}{Z_2} \quad \text{AND} \quad \frac{Y_1}{Z_1} = \frac{Y_2}{Z_2}$$

so we get

$$\underbrace{X_1 Z_2}_{U_1} = \underbrace{X_2 Z_1}_{U_2} \text{ AND } \underbrace{Y_1 Z_2}_{S_1} = \underbrace{Y_2 Z_1}_{S_2}.$$

In fact, so far we discussed standard projective coordinates. In general consider the following relation:

Let F be a field, and let $c, d \in \mathbb{N} \setminus \{0\}$

Define an equivalence relation on the set $F^3 \setminus \{(0,0,0)\}$ by:

$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ if $(X_1 = \lambda^c X_2 \wedge$

$\wedge\ Y_1 = \lambda^d Y_2 \wedge$

$\wedge\ Z_1 = \lambda Z_2$

for some $\lambda \in F \setminus \{0\})$

The equivalence class containing $(X, Y, Z) \in F^3 \setminus \{(0,0,0)\}$ is

$$(X : Y : Z) = \{(\lambda^c X, \lambda^d Y, \lambda Z) : \lambda \in K^*\}$$

colons for indicating that this is an equivalence class, not an ordinary point in $F^3 \setminus \{(0,0,0)\}$

$(X : Y : Z)$ is a projective point

(X, Y, Z) is a representative of $(X : Y : Z)$.

Recall that if two equivalence classes share a single element then they are equal (different equivalence classes are disjoint).

The set of all projective points is called a (weighted) projective space and is denoted by $\mathbb{P}(F)$.

If $Z \neq 0$ then $(x, y, 1)$ is a representative of the projective point $(X : Y : Z)$, where $x = \lambda^c \cdot X$

$y = \lambda^d \cdot Y$, for $\lambda = \frac{1}{Z}$

That is $x = X / Z^c$

$y = Y / Z^d$

Denote

$\mathbb{P}(F)^* = \{(X : Y : Z) : X, Y, Z \in F, Z \neq 0\}$

Thus for $Z \neq 0$ we have a one-to-one correspondence between the set of projective points $\mathbb{P}(F)^*$ and the set of affine points $\mathbb{A}(F) = \{(x, y) : x, y \in F\}$