$2\cdot(X_1, 0, Z_1)$ doubling in the standard projective coordinates can be expressed as:

$$(X_1, 0, Z_1) + (X_2, 0, Z_2)$$

where $X_2 = \lambda X_1$

$Z_2 = \lambda \cdot Z_1$ for $\lambda \in F \setminus \{0\}$

For such a case we enter point addition formula. But in such a case we detect that we have doubling of the entry point by checking $U_1 = U_2$ and $S_1 = S_2$.

In such a case we call the doubling subroutine.

So we enter the case $2\cdot(X_1, 0, Z_1)$ we have analyzed.

So let us return to projective coordinates.

The set of projective points $\{(X:Y:Z) : X, Y, Z \in F, Z = 0\}$ is called a <u>line at infinity</u>:

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

So we distinguish:

1) Standard projective coordinates: $c=1, d=1$

2) Jacobian coordinates: $c=2, d=3$.

So in Jacobian coordinates the projective point

$(X:Y:Z) \in \mathbb{P}(F)^*$ corresponds to the affine point (x, y) such that:

$$x = \frac{X}{Z^2}, \quad y = \frac{Y}{Z^3}.$$

Hence for an elliptic curve $E_{a,b}(F)$ we have:

$$E: \quad y^2 = x^3 + ax + b, \quad a, b \in F, \quad 4a^3 + 27b^2 \neq 0$$

$$\left(\frac{Y}{Z^3}\right)^2 = \left(\frac{X}{Z^2}\right)^3 + a\left(\frac{X}{Z^2}\right) + b \quad / \cdot Z^6$$

$$(*) \qquad Y^2 = X^3 + aXZ^4 + bZ^6$$

Formula (*) is the elliptic curve equation in the Jacobian coordinates.

Let us deduce how many points from the line at infinity $\mathbb{P}(E)^0$ we have.

If we assign $Z = 0$ in (*) then we get

$$(**) \qquad Y^2 = X^3 \quad / \cdot (Y^2)^{-1}$$

$$1 = X^3 \cdot (Y^2)^{-1}$$

Note that $\sqrt[3]{(Y^2)^{-1}}$ must exist in F, because

$$(Y^2)^{-1} = (X^{-1})^3, \text{ so finally}$$

$$1 = \left(\underbrace{X \cdot \sqrt[3]{(Y^2)^{-1}}}_{x'}\right)^3$$

So x' is a cubic root from 1. In F there are at most 3 such roots,

1) there is one root if $3 \nmid |F| - 1$ (unimodality of the multiplicative group F^* because in such a case $(3, |F^*|) = 1$ and operation $(\ )^3$ is a permutation in that group.

2) there are 3 roots if $3 \mid |F| - 1$ because then there is a subgroup $H < F^*$, such that $|H| = 3$

and $\forall h \in H \quad h^3 = 1$ in F.

For example in $\mathbb{F}_7$ we have:

$$H = \{1, 2, 4\} = \langle 2 \rangle$$

$$1^3 = 1$$
$$2^3 = 1 \quad \text{in } \mathbb{F}_7$$
$$4^3 = 64 = 63 + 1 = 1 \quad \text{in } \mathbb{F}_7$$

To get 1 on the left-hand side of (**) it suffices to take $Y = 1$ or $Y = -1$.

Let $\alpha_1, \ldots, \alpha_k$ $k \in \{1, 3\}$ be a set of cube roots from 1 in F. Then the following triples satisfy (**):

$$\begin{cases} (\alpha_1, 1, 0) \sim (1, 1, 0) & \text{for } \lambda = \alpha_1 : (\underbrace{\alpha_1^2 \alpha_1}_{1}, \underbrace{\alpha_1^3 \cdot 1}_{1 \cdot 1}, \underbrace{\alpha_1 \cdot 0}_{0}) \\ (\alpha_1, -1, 0) \sim (1, 1, 0) & \text{for } \lambda = -\alpha_1 \\ (\alpha_2, 1, 0) \sim (1, 1, 0) & \text{for } \lambda = \alpha_2 \\ (\alpha_2, -1, 0) \sim (1, 1, 0) & \text{for } \lambda = -\alpha_2 : (\underbrace{(-\alpha_2)^2 \cdot \alpha_2}_{\alpha_2^3 = 1}, \underbrace{(-\alpha_2)^3 \cdot (-1)}_{1}, 0) \\ (\alpha_3, 1, 0) \sim (1, 1, 0) & \text{for } \lambda = \alpha_3 \end{cases}$$

$(\alpha_3, -1, 0) \sim (1, 1, 0)$ for $\lambda = -\alpha_3$.

Hence $(1:1:0)$ is the projective point Θ in Jacobian coordinates.

Negative of $(X:Y:Z)$ is derived from negative in affine coordinates:

If $Z \neq 0$ $(X:Y:Z) \xrightarrow[x = \frac{X}{Z^2}]{} (x, y)$

$y = \frac{Y}{Z^3}$

negative

$(x, -y) \longrightarrow \left(\frac{X}{Z^2}, \frac{-Y}{Z^3}\right) \rightarrow$

$\rightarrow (X:-Y:Z)$

If $Z = 0$ then $(X:Y:Z)$ satisfying the elliptic curve equation is the as $(1:1:0)$ (zero at infinity) and $(1:-1:0) \sim (1:1:0)$ for $\lambda = -1$, hence

$(1:-1:0)$ is still zero at infinity.

All in all, negative of $(X:Y:Z)$ is $(X:-Y,Z)$ in Jacobian coordinates (exactly as in the standard projective coordinates).

Point doubling (we skip the derivation process):

$$2\cdot(X_1,Y_1,Z_1)$$

We apply the following formulas:

$$\begin{cases} A := Y_1^2 \\ B := 4X_1 \cdot A \\ C = 8A^2 \\ D = 3X_1^2 + aZ_1^4 \\ X_3 = D^2 - 2B \\ Y_3 = D(B - X_3) - C \\ Z_3 = 2 \cdot Y_1 Z_1 \end{cases}$$

the cost is 6 squaring and 4 multiplications in F.

Point addition:

$$\begin{cases} U_1 := X_1 \cdot Z_2^2 \\ U_2 := X_2 \cdot Z_1^2 \\ S_1 := Y_1 \cdot Z_2^3 \\ S_2 := Y_2 \cdot Z_1^3 \\ W := Z_1 Z_2 \\ P := U_2 - U_1 \\ R := S_2 - S_1 \\ X_3 := R^2 - (U_1 + U_2)P^2 \\ Y_3 := \left[R \cdot (-2R^2 + 3(U_1+U_2)P^2) - P^3(S_1+S_2) \right]/2 \\ Z_3 := W \cdot P \end{cases}$$

cost: $12M + 4S$ in F

	Standard projective coor.	Jacobian coor.
Point addition	12M+2S	12M+4S
Point doubling	7M+5S	4M+6S

In the paper

(*) "Sequences of Number Generated by Addition in Formal Groups and New Primality and Factorization Tests" by D.V. Chudnovski and G.V. Chudnovski (in Advances in Applied Mathematics 7, 385-434, 1986) the authors pointed at the discrepancy above:

- for point doubling Jacobian coordinates are better,
- for point addition the better ones are the standard projective coordinates.

As the result the authors of (*) proposed to mix both the representations above. To do so they proposed to keep track on Z, Z^2, Z^3 separately, that is

$$P = (X_1, Y_1, Z_1, Z_1^2, Z_1^3)$$

$$Q = (X_2, Y_2, Z_2, Z_2^2, Z_2^3).$$

Finally, the cost of

point addition: 11M+3S

point doubling: 5M+6S.

The coordinate system above is called:

- cached Jacobian coordinates
- or Chudnovsky Jacobian coordinates
- or Chudnovsky coordinates
- or Jacobian Chudnovski coordinates.