Point doubling:

Let $P = (X_1, Y_1, Z_1) \in E$, and let $P \neq -P$,

(as a result $P \neq \Theta$ because $\Theta = -\Theta$).

Consequently $P \sim \left(\frac{X_1}{Z_1^2}, \frac{Y_1}{Z_1^3}, 1 \right)$

We shall utilize the doubling formula on affine coordinates:

let $2P = \underbrace{(X_3' : Y_3' : 1)}_{\text{abstraction class}}$

$$X_3' = \left(\frac{3\frac{X_1^2}{Z_1^4} + a}{2\frac{Y_1}{Z_1^3}}\right)^2 - 2\frac{X_1}{Z_1^2} = \left(\frac{3\frac{X_1^2}{Z_1^4} + a}{2\frac{Y_1 Z_1}{Z_1^4}}\right)^2 - 2\frac{X_1}{Z_1^2} =$$

$$= \left(\frac{3X_1^2 + aZ_1^4}{2Y_1 Z_1}\right)^2 - 2\frac{X_1 Y_1^2}{Y_1^2 Z_1^2} =$$

$Y_1 \neq 0$ for $P \neq -P$

$$= \frac{(3X_1^2 + aZ_1^4)^2 - 8X_1 Y_1^2}{4Y_1^2 Z_1^2}$$

$$Y_3' = \left(\frac{3\frac{X_1^2}{Z_1^4} + a}{2\frac{Y_1}{Z_1^3}}\right) \cdot \left(\frac{X_1}{Z_1^2} - X_3'\right) - \frac{Y_1}{Z_1^3} =$$

similar step

$$= \left(\frac{3X_1^2 + aZ_1^4}{2Y_1 Z_1}\right)\left(\frac{X_1}{Z_1^2} - X_3'\right) - \frac{Y_1}{Z_1^3}$$

If we ~~(introduce $Z_3 =$)~~ are going to assign $Z_3 = 2Y_1Z_1$ (note that the denominator in X_3' is $(2Y_1Z_1)^2$ – ~~we may look~~ cf. the relation $(x,y,1) \sim (xt^2, yt^3, t)$ for $t \in F\setminus\{0\}$)

then we ~~need~~ may have $(2Y_1Z_1)^3$ in the denominator of Y_3':

$$Y_3' = \left(\frac{3X_1^2 + aZ_1^4}{2Y_1Z_1}\right)\left(\frac{X_1}{Z_1^2} - X_3'\right) \cdot \frac{4Y_1^2Z_1^2}{4Y_1^2Z_1^2} - \frac{Y_1}{Z_1^3} \cdot \frac{8Y_1^3Z_1^3}{8Y_1^3Z_1^3}$$

$$= \frac{1}{8Y_1^3Z_1^3} \cdot \left[(3X_1^2 + aZ_1^4) \cdot (4X_1Y_1^2 - X_3' \cdot 4Y_1^2Z_1^2) - 8Y_1^4\right]$$

Hence using $t = 2Y_1Z_1$ we get:

$$\begin{cases} X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2 \\ Y_3 = (3X_1^2 + aZ_1^4) \cdot (4X_1Y_1^2 - X_3) - 8Y_1^4 \\ Z_3 = 2Y_1Z_1 \end{cases}$$

We can re-arrange the process (see "Guide to Elliptic Curve Cryptography")

in the following way:

$$\begin{cases} A := Y_1^2 & \\ B := 4X_1 \cdot A & = 4X_1 \cdot Y_1^2 \\ C := 8A^2 & = 8Y_1^4 \end{cases}$$

$$\begin{cases} D := 3X_1^2 + aZ_1^4 \\ X_3 := D^2 - 2B & \{= (3X_1^2 + aZ_1^4)^2 - 2\cdot(4X_1Y_1^2) \\ Y_3 := D\cdot(B - X_3) - C & \{= \underbrace{(3X_1^2 + aZ_1^4)}_{D}\cdot(\underbrace{4X_1\cdot Y_1^2}_{B} - X_3) - \underbrace{8Y_1^4}_{C} \\ Z_3 := 2Y_1\cdot Z_1 \end{cases}$$

Cost: 6 squarings and 4 multiplications in F.

Point addition:

Let $P = (X_1 : Y_1 : Z_1)$, $Z_1 \neq 0$

$Q = (X_2 : Y_2 : Z_2)$, $Z_2 \neq 0$

Then $P+Q = (X_3 : Y_3 : Z_3)$ ~~such that~~ can be derived as follows:

$$\left.\begin{aligned} x_3' &= \frac{X_3}{Z_3^2} \\ y_3' &= \frac{Y_3}{Z_3^3} \end{aligned}\right\} \text{ in affine coordinates:}$$

$$x_3' = \underbrace{\left(\frac{\frac{Y_2}{Z_2^3} - \frac{Y_1}{Z_1^3}}{\frac{X_2}{Z_2^2} - \frac{X_1}{Z_1^2}}\right)^2}_{\lambda^2} - \frac{X_1}{Z_1^2} - \frac{X_2}{Z_2^2} = \left(\frac{Y_2Z_1^3 - Y_1Z_2^3}{Z_1Z_2(X_2Z_1^2 - X_1Z_2^2)}\right)^2 - \frac{X_1Z_2^2 + X_2Z_1^2}{Z_1^2Z_2^2}$$

$$\cancel{= \frac{1}{Z_1^2Z_2^2(X_2Z_1^2 - X_1Z_2^2)^2}\left[(Y_2Z_1^3 - Y_1Z_2^3)^2 - (X_1Z_2^2 + X_2Z_1^2)(X_2Z_1^2 - X_2Z_2^2)^2\right]}$$

$$= \frac{1}{Z_1^2Z_2^2(X_2Z_1^2 - X_1Z_2^2)^2}\left[(Y_2Z_1^3 - Y_1Z_2^3)^2 - (X_1Z_2^2 + X_2Z_1^2)(X_2Z_1^2 - X_1Z_2^2)^2\right]$$

Substitute:

$$U_1 := X_1 Z_2^2 \qquad P := U_2 - U_1$$
$$U_2 := X_2 Z_1^2 \qquad R := S_2 - S_1$$
$$S_1 := Y_1 Z_2^3$$
$$S_2 := Y_2 Z_1^3$$
$$W := Z_1 Z_2$$

$$x_3' = \frac{1}{W^2 (U_1 - U_2)^2}\left[(S_1 - S_2)^2 - (U_1+U_2)(U_2-U_1)^2\right] = \frac{1}{W^2P^2}\left[R^2 - (U_1+U_2)P^2\right]$$

$$\left.\begin{aligned} y_3' &= -y_1 + \alpha(x_1 - x_3') \\ y_3' &= -y_2 + \alpha(x_2 - x_3') \end{aligned}\right\}$$ similarly like in the projective coordinates

$$y_3' = \Big[-(y_1+y_2) + \underbrace{\cancel{\alpha(x_1 - x_3)}}_{\alpha\cdot(x_1+x_2-2x_3')}\Big]/2 = \Big[-\left(\frac{Y_1}{Z_1^3} + \frac{Y_2}{Z_2^3}\right) + \left(\frac{Y_2Z_1^3 - Y_1Z_2^3}{Z_1Z_2(X_2Z_1^2 - X_1Z_2^2)}\right)\cdot$$

$$\cdot\left(\frac{X_1}{Z_1^2} + \frac{X_2}{Z_2^2} - 2x_3'\right)\Big]/2 =$$

$$= \frac{1}{Z_1^3Z_2^3(X_2Z_1^2 - X_1Z_2^2)^3}\Big[-(Y_1Z_2^3 + Y_2Z_1^3)\cdot(X_2Z_1^2 - X_1Z_2^2)^3 +$$

$$+ (Y_2Z_1^3 - Y_1Z_2^3)(X_2Z_1^2 - X_1Z_2^2)^2\big(X_1Z_2^2 + X_2Z_1^2 -$$

third power was consumed

$$-2Z_1^2Z_1^2x_3'\big)\Big]/2 =$$

$$= \frac{1}{W^3P^3}\left[-(S_1+S_2)\cdot P^3 + (S_2 - S_1)(U_2-U_1)^2(U_1+U_2-2W^2x_3')\right]/2$$

$$= \frac{1}{W^3P^3}\left[-(S_1+S_2)P^3 + R\cdot P^2\cdot(U_1+U_2) - 2R\cdot P^2\cdot W^2x_3'\right]/2 =$$

$$= \frac{1}{W^3 P^3}\left[-(S_1+S_2)\cdot P^3 + R\left(P^2\cdot(U_1+U_2) - 2\cdot\left(R^2-(U_1+U_2)\cdot P^2\right)\right)\right]/2 =$$

$$= \frac{1}{W^3 P^3}\left[-(S_1+S_2)P^3 + R\left(-2R^2+3\cdot(U_1+U_2)P^2\right)\right]/2$$

Hence using $t = W\cdot P$ in $(x,y,1) \sim (xt^2, yt^3, t)$ for $t\in F\setminus\{0\}$

we get:

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

Cost: $\underbrace{12M}_{\text{multiplications}} + \underbrace{4S}_{\text{squaring}}$ in F, because

U_1: $1M + 1S$

U_2: $1M + 1S$

S_1: $2M$

S_2: $2M$

W: $1M$

Z_3: $1M$

X_3: $1S + (1M + 1S) = 2S + M$

Y_3: $(U_1+U_2)\cdot P^2$ is ~~…~~ ready from X_3, R^2 is ready from X_3

$3\cdot(\ )$ is not counted because 3 is very small

$-P^3(S_1+S_2)$ requires $2M$, $+1M$ for $\left[R\cdot(\quad)\ \cancel{-}\ (\ )\right]/2$

$= 3M$

~~As we see~~

The cost is smaller if we are sure that $Q = (X_2 : Y_2 : 1)$

$Z_2 = 1$

– cf. ~~…~~ the square and multiply algorithm: the same point is added ~~to~~ the accumulator if the corresponding bit of the scalar is set to 1.

In such a case the cost of addition is reduced to $8M + 3S$. – see pages 88-89 of the "Guide to Elliptic Curve Cryptography".

In a general case, however, we have the following situation:

	Standard projective coordinates	Jacobian coordinates
Point addition	$12M+2S$ (14M in total)	$12M+4S$ (16M in total)
Point doubling	$7M+5S$ (12M in total)	$4M+6S$ (10M in total)

In the paper

(*) "Sequences of Numbers 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 ~~noted that~~ pointed at the discrepancy above:

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

As a 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

$$P = (X_1, Y_1, Z_1, Z_1^2, Z_1^3)$$
$$Q = (X_2, Y_2, Z_2, Z_2^2, Z_2^3)$$

which in fact are tuples of 5 variables:

$$P = (X_1, Y_1, Z_1, Z_{1,2}, Z_{1,3})$$

$$Q = (X_2, Y_2, Z_2, Z_{2,2}, Z_{2,3})$$

And for point addition

$$P+Q = (X_3, Y_3, Z_3, Z_{3,2}, Z_{3,3})$$

we utilize the point addition formula for Jacobian coordinates:

$$U_1 := X_1 \cdot Z_{2,2} \quad = X_1 \cdot Z_2^2$$

$$U_2 := X_2 \cdot Z_{1,2} \quad = X_2 \cdot X_1^2$$

$$S_1 := Y_1 \cdot Z_{2,3} \quad = Y_1 \cdot Z_2^3$$

$$S_2 := Y_2 \cdot Z_{1,3} \quad = Y_2 \cdot Z_1^3$$

$$W := Z_1 \cdot Z_2$$

$$P := U_2 - U_1$$

$$R := S_2 - S_1$$

, we can assume that $P \neq 0 \wedge R \neq 0$, otherwise we have the same points (so point doubling formula to utilize) or the opposite points

$$X_3 := R^2 - (U_1 + U_2) P^2$$

$$Y_3 := \left[R \cdot \left(-2R^2 + 3P^2 (U_1 + U_2)\right) - P^3 \cdot (S_1 + S_2) \right] / 2$$

$$Z_3 := W \cdot P$$

$$Z_{3,2} = Z_3^2$$

$$Z_{3,3} = Z_{3,2} \cdot Z_3$$

For point doubling, that is when $U_1 = U_2$ and $S_1 = S_2$, we utilize point doubling formula for Jacobian coordinates as well, ~~rearranging~~ reformulating it slightly:

Define:

$$M := 3X_1^2 + a(Z_{1,2})^2 \quad \Big\} = 3X_1^2 + a(Z_1^2)^2 = 3X_1^2 + aZ_1^4$$

$$S := 4X_1 \cdot Y_1^2$$

$$X_3 := -2S + M^2$$

$$Y_3 := -8Y_1^4 + M(3S - M^2) \quad \Big\} = M(S - \underbrace{(-2S + M^2)}_{X_3}) - 8Y_1^4$$

$$Z_3 := 2Y_1 Z_1$$

$$Z_{3,2} := Z_3^2$$

$$Z_{3,3} := Z_{3,2} \cdot Z_3$$

The cost of the operations above:

Point addition: $\underbrace{12M + 4S}_{\text{cost of } P+Q \text{ in Jacobian}} - \underbrace{2S - 2M}_{\text{cheaper } U_1, U_2, S_1, S_2} + 1S + 1M = \underline{11M + 3S}$

Point doubling: $\underbrace{4M + 6S}_{\text{cost of } 2P \text{ in Jacobian}} - 1S + 1S + 1M = \underline{5M + 6S}$

Hence on average we gain (in scalar multiplication we need both doubling and point addition formulas).

The coordinate system is mixed in the sense that affine

$x = X/Z_2$

$y = Y/Z_3$

so we divide by the 1st power of some other coordinate like in the ~~projed~~ standard projective coordinates.

However, the formulas used for point addition and point doubling are borrowed from Jacobian coordinates. Hence the ~~coordi~~ last coordinate ~~Hence~~ system is (~~sometimes~~) called:

- cached Jacobian coordinates (for caching Z^2, Z^3)
- or Chudnovsky Jacobian coordinates,
- or Chudnovsky coordinates
- or Jacobian Chudnovsky coordinates

There are many different coordinate systems.

The next question is how fast can we multiply a point by a scalar.