Let K be a field, E be an elliptic curve defined by Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{0.1}$$

For any integer n, let $[n] : E \to E$ be the multiply-by-n isogeny.

Let's state some motivation; they are not exact definitions. Let $\psi_2 = 2y + a_1x + a_3$ as a function on E, then $\psi_2^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. We have the double formula

$$\begin{aligned} x \circ [2] &= \frac{x^4 - b_4x^2 - 2b_6x - b_8}{\psi_2^2}, \\ \psi_2 \circ [2] &= \frac{2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)}{\psi_2^3}, \end{aligned} \tag{0.2}$$

where the first formula can be proved by Vieta's formulas. For the second formula, when the characteristic of K is not 2 it can also be proved by Vieta's formulas (in this case we use $\psi_2^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$), when the characteristic of K is 2 it's a consequence of the first formula. As for the double formula for y-coordinate, it's complicated when a_1, a_3 are not zero:

$$\begin{aligned} y \circ [2] = \psi_2^{-3} \Big[& \\ & - a_3^4 + a_2a_3^2a_4 - a_1a_3a_4^2 - a_4^3 - 6a_3^2a_6 + a_1^2a_4a_6 + 4a_2a_4a_6 - 8a_6^2 \\ & + \big(2a_2^2a_3^2 - 4a_1a_3^3 - 2a_1a_2a_3a_4 - 3a_3^2a_4 - 2a_2a_4^2 + 2a_1^2a_2a_6 \\ & \quad + 8a_2^2a_6 - 12a_1a_3a_6 - 4a_4a_6\big)\, x \\ & + \big(-6a_1^2a_3^2 + 3a_2a_3^2 - 12a_1a_3a_4 - 5a_4^2 - 3a_1^2a_6 + 20a_2a_6\big)\, x^2 \\ & + \big(-4a_1^3a_3 - 6a_1a_2a_3 + 3a_3^2 - 5a_1^2a_4 + 20a_6\big)\, x^3 \\ & + \big(-a_1^4 - 4a_1^2a_2 - 3a_1a_3 + 5a_4\big)\, x^4 \\ & + \big(-3a_1^2 + 2a_2\big)\, x^5 + x^6 + \Big(\\ & \quad - a_1a_2a_3^2 - a_3^3 + a_1^2a_3a_4 + a_1a_4^2 - a_1^3a_6 - 4a_1a_2a_6 - 4a_3a_6 \\ & \quad + \big(-6a_1a_3^2 - 4a_3a_4 - 16a_1a_6\big)\, x \\ & \quad + \big(-6a_1^2a_3 - 4a_2a_3 - 10a_1a_4\big)\, x^2 \\ & \quad + \big(-2a_1^3 - 8a_1a_2 - 4a_3\big)\, x^3 - 7a_1x^4\Big) y \Big]. \end{aligned}$$

Note that x is an even function and ψ_2 is an odd function, namely $x \circ [-1] = x$ and $\psi_2 \circ [-1] = -\psi_2$. Hence for any $m \in \mathbb{Z}$, $x \circ [m]$ and $\frac{\psi_2 \circ [m]}{\psi_2}$ are all even function, they are in $K(x)$. We are going to find out their explicit formula. First we have the following result.

Proposition 0.1. *Let $(x_i, y_i), i = 1, 2, 3, 4$ be the affine coordinate of points $P, Q, P+Q, P-Q$ on E, respectively, and $Y_i, i = 1, 2, 3, 4$ be the ψ_2 evaluated at these points. Then if $x_1 \neq x_2$, we have*

$$\begin{aligned} x_3 + x_4 &= \frac{2x_1x_2(x_1 + x_2) + b_2x_1x_2 + b_4(x_1 + x_2) + b_6}{(x_2 - x_1)^2} \\ x_3x_4 &= \frac{x_1^2x_2^2 - b_4x_1x_2 - b_6(x_1 + x_2) - b_8}{(x_2 - x_1)^2} \end{aligned} \tag{0.3}$$

and

$$\begin{aligned} Y_3 + Y_4 &= Y_1 \frac{2x_2^2(3x_1 + x_2) + b_2x_2(x_1 + x_2) + b_4(x_1 + 3x_2) + 2b_6}{(x_2 - x_1)^3} \\ Y_3Y_4 &= \Big(4x_1^3x_2^3 + b_2x_1^2x_2^2\,(x_1 + x_2) + 2b_4x_1x_2\,\big(x_1^2 + 3x_1x_2 + x_2^2\big) \\ & \quad + b_6\,(x_1 + x_2)\,\big(x_1^2 + 8x_1x_2 + x_2^2\big) + 4b_8\,\big(x_1^2 + 3x_1x_2 + x_2^2\big) \\ & \quad + (b_2b_8 - b_4b_6)\,(x_1 + x_2) + 2\,\big(b_4b_8 - b_6^2\big)\Big)/(x_2 - x_1)^3 \end{aligned} \tag{0.4}$$

Proof. The first two can be obtained via

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2$$
$$x_4 = \left(\frac{-y_2 - a_1x_2 - a_3 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{-y_2 - a_1x_2 - a_3 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2$$

and lengthy computation. As for the last two, when the characteristic of K is not 2, they can be obtained via

$$\psi_2(P \pm Q) = Y_1 \pm Y_2 + \frac{1}{4}\left[12\left(\frac{\pm Y_2 - Y_1}{x_2 - x_1}x_2 \mp Y_2\right) + b_2\frac{\pm Y_2 - Y_1}{x_2 - x_1} - \left(\frac{\pm Y_2 - Y_1}{x_2 - x_1}\right)^3\right]$$

and lengthy computation. When the characteristic of K is 2, they are consequences of the first two. □

In particular, changing the rule of P and Q in (0.4), we obtain

$$Y_3 - Y_4 = Y_2\frac{2x_1^2(x_1 + 3x_2) + b_2x_1(x_1 + x_2) + b_4(3x_1 + x_2) + 2b_6}{(x_1 - x_2)^3}. \tag{0.5}$$

Now we can formally give the definition of division polynomials ([GTM106], Exercise 3.7). Define the commutative ring $R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]/(f)$, where $a_1, a_2, a_3, a_4, a_6, x, y$ are all formal variables, $f = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ be the polynomial defined by the Weierstrass equation (0.1). For $m \in \mathbb{Z}$, define the division polynomials $\psi_m, \phi_m, \omega_m \in R$ as

$$\begin{aligned}
\psi_0 &= 0, \quad \psi_1 = 1, \quad \psi_{-m} = -\psi_m,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4 &= \psi_2 \cdot \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\right),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\\
\psi_{2m} &= \psi_m \cdot \left(\psi_{m-1}^2\psi_{m+2} - \psi_{m+1}^2\psi_{m-2}\right)/\psi_2,\\
\phi_m &= x\psi_m^2 - \psi_{m-1}\psi_{m+1},\\
\omega_m &= \left(\psi_{m-1}^2\psi_{m+2} - \psi_{m+1}^2\psi_{m-2}\right)/\psi_2 = \psi_{2m}/\psi_m.
\end{aligned}$$

Note that $\psi_2^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \in \mathbb{Z}[b_2, b_4, b_6, b_8, x] \subset R$, by induction we know that ψ_{2m+1} and ψ_{2m}/ψ_2 are contained in this subring, so ϕ_m, ω_{2m+1}/ψ_2 and ω_{2m} are also contained in this subring.

For E/K defined by (0.1), there is a natural ring homomorphism $R \to K(E)$. Note that the image of ψ_2 in $K(E)$ is not zero (since when the characteristic of K is 2, not all the a_1, a_3 are zero), so the images of ψ_m, ϕ_m, ω_m in $K(E)$ are also uniquely determined by the above recursion formulas. When there is no risk of confusion, we also denote their images by ψ_m, ϕ_m, ω_m. Note that if these polynomials satisfy polynomial equations of R-coefficients in R, then their images in $K(E)$ also satisfies the same polynomial equations.

By induction it's easy to see that the leading terms of ψ_{2m+1} and ψ_{2m}/ψ_2 are $(2m+1)x^{2m^2+2m}$ and mx^{2m^2-2}, respectively, so the leading terms of ϕ_m and ψ_m^2 are x^{m^2} and $m^2x^{m^2-1}$, respectively.

We claim that the images of ϕ_n and ψ_n^2 in $K[x] \subset K(E)$ are coprime (since R is not PID, we don't talk about them being coprime in R). This is clear when $n = 0, 1$. When $n = 2$ we should prove $x^4 - b_4x^2 - 2b_6x - b_8$ and $4x^3 + b_2x^2 + 2b_4x + b_6$ are coprime in $K[x]$ ([GTM106], Exercise 3.1). We need to use that the discriminant of E is not zero, and we need to divide the characteristic of K by three cases: 2, 3, or other; for the last case by linear change of variable we may assume $b_2 = 0$. The details are omitted. For general $n \geq 3$ we only need to show that in $K[x]$, for any $m \geq 0$ we have (a) $(\psi_{2m+1}, \psi_2^2) = 1$, (b) $(\psi_{2m+1}, \frac{\psi_{2m+2}}{\psi_2}) = 1$, and (c) $(\psi_{2m+1}, \frac{\psi_{2m}}{\psi_2}) = 1$. The (a) holds when $m = 0, 1$, (b) holds when $m = 0, 1$, utilizing the fact $\frac{\psi_4}{\psi_2} = \psi_3(6x^2 + b_2x + b4) - \psi_2^4$, and the (c) holds when $m = 0, 1, 2$. For the general m they are proved by induction.

We claim that

$$x \circ [m] = \frac{\phi_m}{\psi_m^2} = x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2} \tag{0.6}$$

holds in $K(E)$. We should also show that for any $m \neq 0$, the image of ψ_m in $K(E)$ is not zero; this is true when $m = 1, 2$. Suppose $m \geq 2$ is such that the image of ψ_m in $K(E)$ is not zero, and (0.6) holds for m, then the image of ψ_{m+1} in $K(E)$ must be not zero. Suppose otherwise, namely the image of ψ_{m+1}

in $K(E)$ is zero, then we have $x \circ [m] = x$, therefore for any $P \in E(\overline{K})$, either $[m]P = P$ or $[m]P = -P$, hence either $[m-1]P = O$ or $[m+1]P = O$. But since $m \geq 2$, the $[m-1]$ and $[m+1]$ are all finite morphisms, a contradiction. Starting from this, in the following we prove that (0.6) holds for $m+1$.

It can be shown directly that (0.6) holds for $m = 1, 2$. When $m \geq 3$ we use induction. From the first formula in (0.3), we only need to show that when $n \geq 2$,

$$\frac{\phi_{n+1}}{\psi_{n+1}^2} + \frac{\phi_{n-1}}{\psi_{n-1}^2} = \frac{2\left(\phi_n/\psi_n^2\right) x \left(\phi_n/\psi_n^2 + x\right) + b_2 \left(\phi_n/\psi_n^2\right) x + b_4 \left(\phi_n/\psi_n^2 + x\right) + b_6}{\left(\phi_n/\psi_n^2 - x\right)^2}$$

holds in R. This is equivalent to

$$\psi_n^3\psi_2^2 - \psi_{n-1}\psi_n\psi_{n+1}\left(6x^2 + b_2x + b_4\right) + \psi_{n+2}\psi_{n-1}^2 + \psi_{n-2}\psi_{n+1}^2 = 0. \tag{0.7}$$

It can be checked directly when $n = 2$. To do induction from $n-1$ case to n case, we only need to show

$$\frac{\psi_{n+1}}{\psi_{n-2}}\left(\psi_{n-3}\psi_n^2 + \psi_{n-1}^3\psi_2^2\right) = \psi_{n+2}\psi_{n-1}^2 + \psi_n^3\psi_2^2,$$

which can be derived from the $n-1$ and n case of the following formula

$$\psi_{n+2}\psi_{n-2} = \psi_{n+1}\psi_{n-1}\psi_2^2 - \psi_3\psi_n^2 \tag{0.8}$$

(which is the special case of the general recursion formula (0.10) at $(n, m, r) = (n, 2, 1)$). Therefore we only need to show that (0.8) holds when $n \geq 2$.

By direct computation, the (0.8) is true for $n = 2, 3, 4$. When $n \geq 5$, there are two cases. The first case is $n = 2m$ is even with $m \geq 3$. In this case we have

$$\begin{aligned}
-\psi_2^2 \cdot \mathrm{LHS} &= \psi_{m-1}\psi_{m+1}\left(\psi_{m-2}^2\psi_{m+1} - \psi_{m-3}\psi_m^2\right)\left(\psi_{m+2}^2\psi_{m-1} - \psi_{m+3}\psi_m^2\right) \\
&= \left(\psi_{m-2}^2\psi_{m+1}^2 - \psi_{m-3}\psi_{m+1}\psi_m^2\right)\left(\psi_{m+2}^2\psi_{m-1}^2 - \psi_{m+3}\psi_{m-1}\psi_m^2\right) \\
&= \left(\psi_3\psi_{m-1}^2\psi_m^2 + \psi_{m-2}^2\psi_{m+1}^2 - \psi_{m-2}\psi_m^3\psi_2^2\right)\left(\psi_3\psi_{m+1}^2\psi_m^2 + \psi_{m+2}^2\psi_{m-1}^2\right. \\
&\qquad \left. - \psi_{m+2}\psi_m^3\psi_2^2\right) \qquad \text{because (0.8) holds for } m-1 \text{ and } m+1 \\
&=: (A_1 + A_2 - A_3)(A_4 + A_5 - A_6), \\
-\psi_2^2 \cdot \mathrm{RHS} &= \psi_2^4\left(\psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3\right)\left(\psi_{m-2}\psi_m^3 - \psi_{m+1}\psi_{m-1}^3\right) \\
&\qquad + \psi_3\psi_m^2\left(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2\right)^2 \\
&=: \psi_2^4(B_1 - B_2)(B_3 - B_4) + \psi_3\psi_m^2(B_5 - B_6)^2,
\end{aligned}$$

here A_1A_5, A_2A_4, A_3A_6 cancels with B_5^2, B_6^2, B_1B_3, respectively. Since (0.8) holds for m, it's easy to see that in the remaining terms, $A_1A_6 + A_3A_4, A_2A_6 + A_3A_5, B_1B_4 + B_2B_3$ all contains $\psi_{m-1}^2\psi_{m+2} + \psi_{m+1}^2\psi_{m-2}$ as a factor, and they canceled; the remaining four terms $A_1A_4, A_2A_5, B_2B_4, 2B_5B_6$ doesn't contain that factor, and they also canceled.

The second case is $n = 2m+1$ is odd with $m \geq 2$. In this case we have

$$\begin{aligned}
\mathrm{LHS} &= \left(\psi_{m+3}\psi_{m+1}^3 - \psi_m\psi_{m+2}^3\right)\left(\psi_{m+1}\psi_{m-1}^3 - \psi_{m-2}\psi_m^3\right) =: (A_1 - A_2)(A_3 - A_4), \\
\mathrm{RHS} &= \psi_m\psi_{m+1}\left(\psi_{m-1}^2\psi_{m+2} - \psi_{m+1}^2\psi_{m-2}\right)\left(\psi_m^2\psi_{m+3} - \psi_{m+2}^2\psi_{m-1}\right) \\
&\qquad - \psi_3\left(\psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3\right) =: \psi_m\psi_{m+1}(B_1 - B_2)(B_3 - B_4) - \psi_3(B_5 - B_6)^2,
\end{aligned}$$

here A_1A_4, A_2A_3 cancels with B_2B_3, B_1B_4, respectively. Apply the formula (0.8) for m and $m+1$ case to A_2A_4, A_1A_3, we may eliminate ψ_{m-2} and ψ_{m+3}, the terms containing ψ_3 cancels with B_5^2, B_6^2. Similarly, we can eliminate ψ_{m-2} and ψ_{m+3} inside B_2B_4, B_1B_3, the terms containing ψ_3 cancels with $2B_5B_6$. At last, the four remaining terms containing ψ_2^2 also cancels.

We claim that

$$\psi_2 \circ [m] = \frac{\omega_m}{\psi_m^3} = \frac{\psi_{2m}}{\psi_m^4} \tag{0.9}$$

holds in $K(E)$. When $m = 1, 2$ it can be computed directly. By (0.5), we only need to show that when $n \geq 2$ the

$$\frac{\omega_{n+1}}{\psi_{n+1}^3} - \frac{\omega_{n-1}}{\psi_{n-1}^3} = \psi_2\frac{2x_n^2(x_n + 3x) + b_2x_n(x_n + x) + b_4(3x_n + x) + 2b_6}{(x_n - x)^3}$$

holds in R, where $x_n = \phi_n/\psi_n^2 = x - \psi_{n-1}\psi_{n+1}/\psi_n^2$. We have

$$
\begin{aligned}
&\left(\psi_2\psi_{n-1}^3\psi_{n+1}^3\right)\cdot \mathrm{LHS} = \psi_{n-1}^3\left(\psi_n^2\psi_{n+3} - \psi_{n-1}\psi_{n+2}^2\right) - \psi_{n+1}^3\left(\psi_{n-2}^2\psi_{n+1} - \psi_{n-3}\psi_n^2\right)\\
&= \psi_n^2\left(\psi_{n-1}^3\psi_{n+3} + \psi_{n+1}^3\psi_{n-3}\right) - \left(\psi_{n-1}^2\psi_{n+2} + \psi_{n+1}^2\psi_{n-2}\right)^2 + 2\psi_{n+1}^2\psi_{n-1}^2\psi_{n+2}\psi_{n-2}\\
&= \psi_n^2\left[\psi_{n-1}^2\left(\psi_n\psi_{n+2}\psi_2^2 - \psi_3\psi_{n+1}^2\right) + \psi_{n+1}^2\left(\psi_n\psi_{n-2}\psi_2^2 - \psi_3\psi_{n-1}^2\right)\right]\\
&\quad - \left(\psi_{n-1}^2\psi_{n+2} + \psi_{n+1}^2\psi_{n-2}\right)^2 + 2\psi_{n+1}^2\psi_{n-1}^2\left(\psi_{n+1}\psi_{n-1}\psi_2^2 - \psi_3\psi_n^2\right) \qquad \text{by (0.8)}\\
&= \psi_2^2\psi_n^3\left(\psi_{n-1}^2\psi_{n+2} + \psi_{n+1}^2\psi_{n-2}\right) - 2\psi_3\psi_{n-1}^2\psi_n^2\psi_{n+1}^2\\
&\quad - \left(\psi_{n-1}^2\psi_{n+2} + \psi_{n+1}^2\psi_{n-2}\right)^2 + 2\psi_{n+1}^2\psi_{n-1}^2\left(\psi_{n+1}\psi_{n-1}\psi_2^2 - \psi_3\psi_n^2\right)\\
&= \left(2\psi_2^2\psi_n^3 - (6x^2+b_2x+b_4)\psi_{n-1}\psi_n\psi_{n+1}\right)\left((6x^2+b_2x+b_4)\psi_{n-1}\psi_n\psi_{n+1} - \psi_2^2\psi_n^3\right)\\
&\quad - 2\psi_3\psi_{n-1}^2\psi_n^2\psi_{n+1}^2 + 2\psi_{n+1}^2\psi_{n-1}^2\left(\psi_{n+1}\psi_{n-1}\psi_2^2 - \psi_3\psi_n^2\right) \qquad \text{by (0.7)}\\
&= 2\psi_2^2\psi_{n-1}^3\psi_{n+1}^3 - \left((6x^2+b_2x+b_4)^2 + 4\psi_3\right)\psi_{n-1}^2\psi_n^2\psi_{n+1}^2\\
&\quad + 3(6x^2+b_2x+b_4)\psi_2^2\psi_n^4\psi_{n-1}\psi_{n+1} - 2\psi_2^4\psi_n^6,
\end{aligned}
$$

note that $(6x^2+b_2x+b_4)^2 + 4\psi_3 = (12x+b_2)\psi_2^2$, by expanding the right hand side, it's easy to check that both sides are equal.

We claim that

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2, \qquad \forall n \geq m \geq r \geq 0 \tag{0.10}$$

holds. It's clear when one of the "$\geq$" is "$=$". Note that we only need to show (0.10) for $(n,m,r) = (n,m,1)$ case, namely

$$\psi_{n+m}\psi_{n-m} = \psi_{n+1}\psi_{n-1}\psi_m^2 - \psi_{m+1}\psi_{m-1}\psi_n^2, \qquad \forall n \geq m \geq 1. \tag{0.11}$$

This is because the (n,m,r) case can be obtained from linear combinations of $(n,m,1)\cdot\psi_r^2$, $(n,r,1)\cdot\psi_m^2$ and $(m,r,1)\cdot\psi_n^2$ case. We already proved that (0.11) holds when $m=2$. When $m=1$ or $n-m=0,1,2$ the (0.11) can be checked directly. Therefore in the following we assume $m\geq 3$, $n-m\geq 3$. In this case we have $\psi_{n+m}\psi_{n-m} = (\psi_{n+m}\psi_{n-m+2})(\psi_{n+m-2}\psi_{n-m})/(\psi_{n+m-2}\psi_{n-m+2})$, Applying $(n+1,m-1,1)$, $(n-1,m-1,1)$, $(n,m-2,1)$ cases, we only need to show

$$
\begin{aligned}
&\left(\psi_{n+2}\psi_n\psi_{m-1}^2 - \psi_m\psi_{m-2}\psi_{n+1}^2\right)\left(\psi_{n-2}\psi_n\psi_{m-1}^2 - \psi_m\psi_{m-2}\psi_{n-1}^2\right)\\
&= \left(\psi_{n+1}\psi_{n-1}\psi_{m-2}^2 - \psi_{m-1}\psi_{m-3}\psi_n^2\right)\left(\psi_{n+1}\psi_{n-1}\psi_m^2 - \psi_{m+1}\psi_{m-1}\psi_n^2\right).
\end{aligned}
$$

By (0.7) and (0.8) we may eliminate all the ψ_{n-2}, ψ_{n+2} in the left hand side, and the remaining terms are of three types: $\psi_{n-1}^2\psi_{n+1}^2$, $\psi_n^2\psi_{n-1}\psi_{n+1}$ and ψ_n^4. It's easy to see that first type terms canceled. The coefficients of the last two types are also canceled, utilizing (0.7) and (0.8).

In conclusion, we have

Proposition 0.2 ([GTM106], Exercise 3.7)**.** *The division polynomials satisfy:*

(1) ψ_2^2, ψ_{2m+1}, ψ_{2m}/ψ_2, ϕ_m, ω_{2m+1}/ψ_2, $\omega_{2m} \in \mathbb{Z}[b_2,b_4,b_6,b_8,x]$;

(2) *The leading terms of* ψ_{2m+1}, ψ_{2m}/ψ_2, ϕ_m *and* ψ_m^2 *are* $(2m+1)x^{2m^2+2m}$, mx^{2m^2-2}, x^{m^2} *and* $m^2x^{m^2-1}$, *respectively;*

(3) *In* $K[x]\subset K(E)$ *we have* $(\psi_{2m+1},\psi_2^2) = (\psi_{2m+1},\frac{\psi_{2m+2}}{\psi_2}) = (\psi_{2m+1},\frac{\psi_{2m}}{\psi_2}) = (\phi_n,\psi_n^2) = 1$;

(4) *When* $m\neq 0$, *the image of* ψ_m *in* $K(E)$ *is not zero, and we have* $(x,\psi_2)\circ[m] = \left(\frac{\phi_m}{\psi_m^2},\frac{\omega_m}{\psi_m^3}\right)$ *in* $K(E)$, *in particular, multiply-by-m isogeny* $[m]$ *is of degree* m^2;

(5) *the recursion formula* (0.10);

(6) *(???) the image of* ψ_n *in* $K(E)$ *has divisor* $\sum_{T\in E[n]}(T) - \#E[n]\cdot(O)$.

In the following we consider elliptic divisibility sequence (EDS for short), which is a sequence $(W_n)_{n=0}^\infty$ in K, satisfying $W_0=0$ and the following recursion formula

$$W_{n+m}W_{n-m}W_1^2 = W_{n+1}W_{n-1}W_m^2 - W_{m+1}W_{m-1}W_n^2, \qquad \forall n\geq m\geq 1. \tag{0.12}$$

If $W_1\neq 0$, then the sequence (W_n/W_1) is also EDS, hence in this case we usually assume $W_1=1$. When $W_1\neq 0$ the following recursion formula also holds (which is not always true when $W_1=0$):

$$W_{n+m}W_{n-m}W_r^2 = W_{n+r}W_{n-r}W_m^2 - W_{m+r}W_{m-r}W_n^2, \qquad \forall n\geq m\geq r\geq 0, \tag{0.13}$$

whose proof is similar to that of (0.10). Therefore if $W_1\neq 0, W_m\neq 0$, then the sequence (W_{nm}/W_n) is also EDS. It's easy to see that for any $c\in K^\times$, the sequence $(c^{n^2-1}W_n)$ is also EDS. The following is some examples of EDS: (1) $W_n = n$; (2) $W_n = F_{2n}$, where $F_1 = F_2 = 1, F_{n+1} = F_n + F_{n-1}$ is Fibonacci sequence, which has closed formula $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, here $\alpha, \beta = \frac{1 \pm \sqrt{5}}{2}$ are roots of $x^2 - x - 1 = 0$; more generally, $W_n = L_{2n}$, where $L_1 = 1, L_2 = A, L_{n+1} = AL_n - L_{n-1}$, which has closed formula $L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, where α, β are roots of $x^2 - Ax + 1 = 0$; (3) $W_n = \left(\frac{n}{3}\right)$, and $W_n = \left(\frac{-2}{n}\right)$, where $\left(\frac{\cdot}{\cdot}\right)$ is Kronecker symbol; (4) $W_n = \psi_n$ is division polynomial, or its image in $K(E)$, or it evaluated at a fixed point $P \in E(\overline{K})$.

We claim that, when $W_1 W_2 \neq 0$, the recursion formula (0.12) is equivalent to the following recursion formula:

$$
\begin{aligned}
W_{2m+1} W_1^3 &= W_{m+2} W_m^3 - W_{m-1} W_{m+1}^3 \\
W_{2m} W_2 W_1^2 &= W_m \left(W_{m-1}^2 W_{m+2} - W_{m+1}^2 W_{m-2} \right)
\end{aligned} \tag{0.14}
$$

We only need to show that they can derive (0.12). We may assume $W_1 = 1$. Note that (0.14) and the initial conditions W_1, W_2, W_3, W_4 determines the sequence uniquely. Suppose all of W_i are not zero, then we can prove formulas similar to (0.7) and (0.8), hence the proof is similar to that of (0.11). For the general case we consider the sequence (V_n) in the ring $R = \mathbb{Z}[X, Y, Z]$, where $V_1 = 1$, $V_2 = X$, $V_3 = Y$, $V_4 = XZ$, and the remaining terms are determined by (0.14) uniquely. Similar to the proof of division polynomial, we can deduce that V_i is indeed contained in that polynomial ring. Note that all of V_i are not zero, since we have ring homomorphism $R \to \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]/(f)$, $X \mapsto \psi_2$, $Y \mapsto \psi_3$, $Z \mapsto \psi_4/\psi_2$, which makes the image of V_i is ψ_i, which is not zero. From this, similar to the proof of division polynomial, we can prove the recursion formula similar to (0.7), (0.8) and (0.11). Finally, consider the ring homomorphism $R \to K$, $X \mapsto W_2$, $Y \mapsto W_3$, $Z \mapsto W_4/W_2$, then (W_n) is the image of (V_n), hence (W_n) satisfies (0.12).