Advanced Studies in Contemporary Mathematics
27 (2017), No. 1, pp. 73 – 83

www.jangjeon.or.kr
http://dx.doi.org/10.23001/ascm2017.27.1.73

DIVISION POLYNOMIALS FOR TWISTED JACOBI INTERSECTIONS CURVES

GYOYONG SOHN

Abstract. This paper presents two types of the division polynomials for twisted Jacobi intersections curves proposed by R. Feng et al. [7]. The division polynomials are important role for determining the n-torsion points of a given twisted Jacobi intersections curves. We also present the basic properties and the specific formulae for the division polynomials of a twisted Jacobi intersections curves.

2010 Mathematics Subject Classification. 14G50, 11T71.

Keywords and phrases. Division Polynomials, Twisted Jacobi Intersections Curves.

1. Introduction

Elliptic curves have been extensively studied in number theory and algebraic geometry for over 100 years. Recently, elliptic curves have been utilized in devising algorithms for factoring large integers [12, 16], primality proving [2, 8], and in cryptography [11, 15]. In particular, the elliptic curve cryptosystems depends on the presumed intractability of the discrete logarithm problem in the group of rational points on an elliptic curve.

In recent year, there are several models of elliptic curves to provide the efficient computation, such as Edwards curves [6], Huff curves [9], Jacobi quartics[4], Hessian curve [10], and Jacobi intersections [5]. Chudnovsky and Chudnovsky [5] presented the Jacobi intersections curve $u^2 + v^2 = 1$, $bu^2 + w^2 = 1$ and efficient doubling and addition formulae in projective coordinates. The Jacobi intersection is the intersection of two quadratic surfaces in three dimensional space with a point on it. R. Feng et al.[7] introduced the twisted Jacobi intersection curve $au^2 + v^2 = 1$, $bu^2 + w^2 = 1$ for $a, b \in K$ with $ab(a - b) \neq 0$.

In this paper, we present the division polynomials for twisted jacobi intersections curves. Division polynomials were introduced to compute scalar multiplications of points of elliptic curves. They enable us to investigate properties of multiplications without direct multiplication. They are also used to compute n-torsion points and to derive their properties. In [14], they presented two kinds of division polynomials for twised Edward curves. One is the induced the transformation between the elliptic curve and twisted Edward curve. The other is Abel methods to find the division polynomials of the lemniscate. Moody illustrated the division polynomials of alternated model of elliptic curve using by Abel methods [17]. In this paper, we present

This work was supported by the research fund of Daegu National University of Education.

the explicit forms of division polynomials for twisted jacobi intersections curve using by transformation between them. Using the division polynomials, we find a recursive formula for the n-torsion point on twisted Jacobi intersections curve.

This paper is organized as follows. Section 1 illustrate definition of twisted Jacobi intersections curve. Second section describe division polynomials for curve and some basic properties of division polynomials.

2. Twisted Jacobi Intersections Curve

Let K be a field with $\mathrm{char}(K) \neq 2$ and $\overline{K}$ its algebraic closure. In this section we briefly introduce the basic facts for twisted Jacobi intersections curve.

A Jacobi intersections curve is defined by $u^2 + v^2 = 1$, $bu^2 + w^2 = 1$ where $b \in K$ and $b(1-b) \neq 0$. The Jacobi intersection is the intersection of two quadratic surfaces in three dimensional space with a point on it. The point $(0, 1, 1)$ is the neutral element of the addition law. The negative of the point (u, v, w) is $(-u, v, w)$. The addition and doubling formula for Jacobi intersection can be found in [5].

An elliptic curve in twisted Jacobi intersections curve is an elliptic curve over a field K defined by

$$J_{a,b} : \begin{cases} au^2 + v^2 = 1 \\ bu^2 + w^2 = 1 \end{cases}$$

for $a, b \in K$ with $ab(a-b) \neq 0$. A Jacobi intersection elliptic curve is a twisted Jacobi intersection curve with $a = 1$. This curve is non-singular if and only if $ab(a-b) \neq 0$. The j-invariant is given by $j = 2^8 \frac{(a^2-ab+b^2)^3}{a^2b^2(a-b)^2}$.

Every twisted Jacobi intersections curve is birationally equivalent to an elliptic curve in Weierstrass form

$$E_{a,b} \ : \ y^2 = x(x-a)(x-b) \tag{1}$$

under the transformation

$$x = -\frac{a(w+1)}{v-1} \text{ and } y = \frac{au}{v-1}(x-b). \tag{2}$$

The inverse transformation is given by

$$u = -\frac{2y}{x^2-ab}, \ v = \frac{x^2-2ax+ab}{x^2-ab}, \ w = \frac{x^2-2bx+ab}{x^2-ab}.$$

Moreover, every elliptic curve over a field K with three points of order 2 is isomorphic to a twisted Jacobi intersections curve.

Let $P = (u_1, v_1, w_1)$ and $Q = (u_2, v_2, w_2)$ be two finite points on the twisted Jacobi intersections curve $J_{a,b}$. The addition formula denoted by $P + Q = (u_3, v_3, w_3)$ with

$$u_3 = \frac{u_1v_2w_2 + u_2v_1w_1}{v_2^2 + au_2^2w_1^2}, \ v_3 = \frac{v_1v_2 - au_1w_1u_2w_2}{v_2^2 + au_2^2w_1^2}, \ w_3 = \frac{w_1w_2 - bu_1v_1u_2v_2}{v_2^2 + au_2^2w_1^2}.$$

If $P = Q$ and $[2]P = (u_3, v_3, w_3)$, then

$$u_3 = \frac{2u_1v_1w_1}{v_1^2 + au_1^2w_1^2}, \ v_3 = \frac{v_1^2 - au_1^2w_1^2}{v_1^2 + au_1^2w_1^2}, \ w_3 = \frac{w_1^2 - bu_1^2v_1^2}{v_1^2 + au_1^2w_1^2}.$$

The identity element is $(0, 1, 1)$. The additive inverse of a point $P = (u, v, w)$ is the point $-P = (-u, v, w)$.

3. Division Polynomials

3.1. **Division Polynomials for Elliptic Curves.** In this section, we briefly describe the division polynomials for the elliptic curve in Weierstrass form over a field K.

Consider the elliptic curve $E_{a,b}$ over K given in (1),

$$E_{a,b} \ : \ y^2 = x(x-a)(x-b), \ a, b \in K$$

with identity O. The *n-th division polynomial* $\Psi_n(x, y)$, $n \geq 0$, of the elliptic curve $E_{a,b}$ with coefficients $\mathbb{Z}[a, b]$ is defined by the following recursion:

$$\begin{aligned}
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 2y,\\
\Psi_3 &= 3x^4 - 4(a+b)x^3 + 6abx^2 - a^2b^2,\\
\Psi_4 &= 4y(x^6 - 2(a+b)x^5 + 5abx^4 - 5a^2b^2x^2 + 2(a+b)a^2b^2x - a^3b^3),\\
\Psi_{2n+1} &= \Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3, \ n \geq 2,\\
\Psi_{2n} &= \frac{(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)\Psi_n}{\Psi_2}, \ n > 2.
\end{aligned}$$

The basic properties of the division polynomials are that $\Psi_n(P) = 0$ when P is an n-torsion point of $E_{a,b}$, and that the multiplication-by-n map $(x, y) \mapsto [n](x, y)$ can be expressed in terms of rational functions in x and y.

Theorem 3.1. *Let $E_{a,b}$ be an Elliptic curve defined over a field K, and let n be a positive integer. For $P = (x, y) \in E_{a,b}(\overline{K})$ such that $[n]P \neq O$, we have*

$$[n](x, y) = \Big(\frac{x\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4y\Psi_n^3}\Big),$$

where $\Psi_n = \Psi_n(x, y)$.

Proof. See [3] and [18] for details. □

Theorem 3.2. *Let P be a point in $E_{a,b}(\overline{K}) \setminus \{O\}$, and let $n \geq 1$. Then $P \in E_{a,b}[n]$ (P is n-torsion point of $E_{a,b}$) if and only if $\Psi_n(P) = 0$.*

If n is odd then $\Psi_n \in \mathbb{Z}[x, y, a, b]$, and Ψ_n has degree $(n^2 - 1)/2$ in x. If n is even then $\Psi_n \in 2y\mathbb{Z}[x, y^2, a, b]$ with degree $(n^2 - 4)/2$ in x.

3.2. **Division polynomials for twisted Jacobi intersections.** In this section, we present the division polynomials for the twisted Jacobi intersections over a field K. We consider that the transformation from twisted Jacobi intersection $J_{a,b}$ to elliptic curve $E_{a,b}$ over K given in (1) and the division polynomials Ψ_n of $E_{a,b}$. The division polynomials ψ_n, $n \geq 0$, for the twisted Jacobi intersection $J_{a,b}$ is defined by following recursion:

$$
\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= \frac{2au}{(v-1)^2}(aw+bv+a-b),\\
\psi_3 &= \frac{a^2}{(v-1)^4}(3a(w+1)^4 - b^2(v-1)^4\\
&\quad + 2a(w+1)^2(v-1)(2(a+b)(w+1)+3b(v-1))),\\
\psi_4 &= \frac{4a^4u}{(v-1)^8}(aw+bv+a-b)(a^3(w+1)^6 - b^3(v-1)^6\\
&\quad + 2(a+b)(w+1)(v-1)(a^2(w+1)^4 - b^2(v-1)^4)\\
&\quad + 5ab(w+1)^2(v-1)^2(a(w+1)^2 + b(v-1)^2)),
\end{aligned}
$$

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3,\ n \geq 2, \tag{3}$$

$$\psi_{2n} = \frac{(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)\psi_n}{\psi_2},\ n > 2. \tag{4}$$

The polynomial $\psi_n(u,v,w)$ is *n-th division polynomial* for the twisted Jacobi intersection $J_{a,b}$ with coefficients in $\mathbb{Z}[a,b]$. These polynomials are not defined at the point $(0,1,1)$.

We now consider that an n-torsion point of $J_{a,b}$ is characterized by the division polynomials.

Theorem 3.3. *Let $P=(u,v,w)$ be a point in $J_{a,b}$ and $[n]P=(u_n,v_n,w_n)$ an n-torsion point in $J_{a,b}[n]$. Then*

$$
\begin{aligned}
u_n &= -\frac{\psi_{2n}}{(x^4-ab)\psi_n^4 - 2x\psi_n^2\psi_{n-1}\psi_{n+1} + \psi_{n-1}^2\psi_{n+1}^2}\\
v_n &= \frac{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - 2a(x\psi_n^2 - \psi_{n-1}\psi_{n+1})\psi_n^2 + ab\psi_n^4}{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - ab\psi_n^4}\\
w_n &= \frac{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - 2b(x\psi_n^2 - \psi_{n-1}\psi_{n+1})\psi_n^2 + ab\psi_n^4}{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - ab\psi_n^4}
\end{aligned}
$$

Proof. Let $[n](u,v,w)=(u_n,v_n,w_n)$ for $(u,v,w)\in J_{a,b}(\overline{K})$ and $[n](x,y)=(x_n,y_n)$ for $(x,y)\in E_{a,b}(\overline{K})$. From Theorem 3.1 and $\Psi_i=\psi_i$ for all i,

$$x_n = x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2},\ y_n = \frac{\psi_{2n}}{2\psi_n^4},$$

and applying the birational equivalence gives

$$u_n = -\frac{2y_n}{x_n^2-ab},\ v_n = \frac{x_n^2-2ax_n+ab}{x_n^2-ab},\ w_n = \frac{x_n^2-2bx_n+ab}{x_n^2-ab}.$$

Then we have that

$$
\begin{aligned}
u_n &= 2\Big(\frac{\psi_{2n}}{2\psi_n^4}\Big)\Big/\Big(\Big(x-\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 - ab\Big)\\
&= -\frac{\psi_{2n}}{(x^4-ab)\psi_n^4 - 2x\psi_n^2\psi_{n-1}\psi_{n+1} + \psi_{n-1}^2\psi_{n+1}^2}
\end{aligned}
$$

$$v_n = \Big(\Big(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 - 2a\Big(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 + ab\Big) \Big/ \Big(\Big(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 - ab\Big)$$
$$= \frac{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - 2a(x\psi_n^2 - \psi_{n-1}\psi_{n+1})\psi_n^2 + ab\psi_n^4}{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - ab\psi_n^4}$$

and

$$w_n = \Big(\Big(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 - 2b\Big(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 + ab\Big) \Big/ \Big(\Big(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\Big)^2 - ab\Big)$$
$$= \frac{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - 2b(x\psi_n^2 - \psi_{n-1}\psi_{n+1})\psi_n^2 + ab\psi_n^4}{(x\psi_n^2 - \psi_{n-1}\psi_{n+1})^2 - ab\psi_n^4}$$

□

Corollary 3.4. *Let $P = (u, v, w)$ be in $J_{a,b}(\overline{K}) \setminus \{(0, 1, 1)\}$ and let $n \geq 1$. Then P is an n-torsion point of $J_{a,b}$ if and only if $\psi_n(P) = 0$.*

Proof. Since the identity is $(0, 1, 1)$, the result is clear from Theorem 3.3. □

Next we find explicit forms of the division polynomials for twisted Jacobi intersections curve. In the following Theorem 3.5, the division polynomials ψ_n are represented by the rational functions $\widetilde{\psi}_n$ which are also called the division polynomials for twisted Jacobi intersection curve.

Theorem 3.5. *The n-th division polynomial $\psi_n(u, v, w)$, $n \geq 0$, for $J_{a,b}$ is defined by the following n-th division polynomial $\widetilde{\psi}_n(v, w)$:*

$$\psi_n = \begin{cases} \frac{a^{t(n)}}{(v-1)^{m(n)}}\widetilde{\psi}_n(v, w) & \text{if } n \text{ odd} \\ \frac{ka^{t(n)}u}{(v-1)^{m(n)}}(aw + bv + a - b)\widetilde{\psi}_n(v, w) & \text{if } n \text{ even} \end{cases}$$

where

$$m(n) = \begin{cases} \frac{n^2-1}{2} & \text{if } n \text{ odd} \\ \frac{n^2}{2} & \text{if } n \text{ even} \end{cases}, \quad k = \begin{cases} 4 & \text{if } n \equiv 0 \pmod 4 \\ 2 & \text{if } n \equiv 2 \pmod 4, \end{cases}$$

and

$$t(n) = \begin{cases} \frac{n^2+16}{8} & \text{if } n \equiv 0 \pmod 4 \\ \frac{n^2+4}{8} & \text{if } n \equiv 2 \pmod 4 \\ \frac{n^2-1}{8} & \text{if } n \equiv 1, 3 \pmod 4. \end{cases}$$

For a positive integer r, the division polynomial, $\widetilde{\psi}_n$, is defined by the following recursion:

$$\widetilde{\psi}_0 = 0,$$
$$\widetilde{\psi}_1 = \widetilde{\psi}_2 = 1,$$
$$\widetilde{\psi}_3 = 3a^3(w+1)^4 + ab^2(v-1)^4 + 2a^2(w+1)^2(v-1)(2(a+b)(w+1) + 3b(v-1)),$$
$$\widetilde{\psi}_4 = a^3(w+1)^6 - b^3(v-1)^6 + 2(a+b)(w+1)(v-1)(a^2(w+1)^4 - b^2(v-1)^4)$$
$$+ 5ab(w+1)^2(v-1)^2(a(w+1)^2 - b(v-1)^2),$$

where

$$\widetilde{\psi}_{2r} = \begin{cases} (\widetilde{\psi}_{r+2}\widetilde{\psi}_{r-1}^2 - \widetilde{\psi}_{r-2}\widetilde{\psi}_{r+1}^2)\widetilde{\psi}_r & \text{if } r \equiv 0, 2 \pmod 4,\ r \geq 4 \\ (4a^3\widetilde{\psi}_{r+2}\widetilde{\psi}_{r-1}^2 - \widetilde{\psi}_{r-2}\widetilde{\psi}_{r+1}^2)\widetilde{\psi}_r & \text{if } r \equiv 1 \pmod 4,\ r \geq 6 \\ (\widetilde{\psi}_{r+2}\widetilde{\psi}_{r-1}^2 - 4a^3\widetilde{\psi}_{r-2}\widetilde{\psi}_{r+1}^2)\widetilde{\psi}_r & \text{if } r \equiv 3 \pmod 4,\ r \geq 3 \end{cases}$$

and

$$\widetilde{\psi}_{2r+1} = \begin{cases} 8a^3\mu^2\widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - \widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3 & \text{if } r \equiv 0 \pmod 4,\ r \geq 4 \\ \widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - 2\mu^2\widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3 & \text{if } r \equiv 1 \pmod 4,\ r \geq 5 \\ 2\mu^2\widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - \widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3 & \text{if } r \equiv 2 \pmod 4,\ r \geq 2 \\ \widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - 8a^3\mu^2\widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3 & \text{if } r \equiv 3 \pmod 4,\ r \geq 3 \end{cases}$$

where $\mu(v,w) = 4a(v^{-1}-v)(aw+bv+a-b)^2$.

Proof. The following proof comes from a similar approach in [14] to calculate division polynomials for Edward curves. The proof is by induction. The claim is true for $n = 0, \ldots, 4$. Assume true for $0, \ldots, n-1$. First observe for all $t \in \mathbb{Z}$, $t > 0$.

$$\begin{aligned} m(4l) &= \frac{(4l)^2}{2} = 8l^2 \\ m(4l \pm 1) &= \frac{(4l \pm 1)^2 - 1}{2} = \frac{16l^2 \pm 8l}{2} = 8l^2 \pm 4l \\ m(4l \pm 2) &= \frac{(4l \pm 2)^2}{2} = \frac{16l^2 \pm 16l + 4}{2} = 8l^2 \pm 8l + 2 \\ m(4l \pm 3) &= \frac{(4l \pm 3)^2 - 1}{2} = \frac{16l^2 \pm 24l + 8}{2} = 8l^2 \pm 12l + 4 \end{aligned}$$

and

$$\begin{aligned} t(4l) &= \frac{(4l)^2 + 16}{8} = 2l^2 + 2 \\ t(4l \pm 1) &= \frac{(4l \pm 1)^2 - 1}{8} = \frac{16l^2 \pm 8l}{8} = 2l^2 \pm l \\ t(4l \pm 2) &= \frac{(4l \pm 2)^2 + 4}{8} = \frac{16l^2 \pm 16l + 8}{8} = 2l^2 \pm 2l + 1 \\ t(4l \pm 3) &= \frac{4l \pm 3)^2 - 1}{8} = \frac{16l^2 \pm 24l + 8}{8} = 2l^2 \pm 3l + 1 \end{aligned}$$

CASE 1 : Consider $n \equiv 0 \pmod 8$ i.e. $n = 8l$ for some $l \in \mathbb{Z}$. Let $r = 4l$. From (4), the n-th division polynomial is

$$\begin{aligned} \psi_n &= \frac{\psi_r}{\psi_2}(\psi_{r+2}\psi_{r-1}^2 - \psi_{r-2}\psi_{r+1}^2) \\ &= \frac{4a^{t(r)-1}(aw+bv+a-b)u}{v^{m(r)-2}}\Big(\frac{a^{t(r+2)+2t(r-1)}}{v^{m(r+2)+2m(r-1)}}\widetilde{\psi}_{r+2}\widetilde{\psi}_{r-1}^2 \\ &\quad - \frac{a^{t(r-2)+2t(r+1)}}{v^{m(r-2)+2m(r+1)}}\psi_{r-2}\psi_{r+1}^2\Big)\widetilde{\psi}_r \end{aligned}$$

We verified that

$$\begin{aligned} t(r+2) + 2t(r-1) &= t(r-2) + 2t(r+1), \\ m(r+2) + 2m(r-1) &= m(r-2) + 2m(r+1) \end{aligned}$$

and

$$\begin{aligned} t(r) - 1 + t(r+2) + 2t(r-1) &= t(2r), \\ m(r) - 2 + m(r+2) + 2m(r-1) &= m(2r). \end{aligned}$$

So,

$$\begin{aligned}\psi_n &= \frac{4a^{t(n)}u}{(v-1)^{m(n)}}(aw+bv+a-b)(\widetilde{\psi}_{r+2}\widetilde{\psi}_{r-1}^2 - \widetilde{\psi}_{r-2}\widetilde{\psi}_{r+1}^2)\widetilde{\psi}_r \\ &= \frac{4a^{t(n)}u}{(v-1)^{m(n)}}(aw+bv+a-b)\widetilde{\psi}_n\end{aligned}$$

CASE 2 : Consider $n \equiv 1 \pmod 8$ i.e. $n = 8l+1$ for some $l \in \mathbb{Z}$. Let $r = 4l$. From (3), the n-th division polynomial is

$$\begin{aligned}\psi_n &= \psi_{r+2}\psi_r^3 - \psi_{r-1}\psi_{r+1}^3 \\ &= \frac{128a^{t(r+2)+3t(r)}}{(v-1)^{m(r+2)+3m(r)}}(aw+bv+a-b)^4u^4\widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 \\ &\quad - \frac{a^{t(r-1)+3t(r+1)}}{v^{m(r-1)+3m(r+1)}}\widetilde{\psi}_{r-1}\psi_{r+1}^3\end{aligned}$$

We verified that

$$\begin{aligned}(t(r+2)+3t(r)) - (t(r-1)+3t(r+1)) &= 7, \\ (m(r+2)+3m(r)) - (m(r-1)+3m(r+1)) &= 2,\end{aligned}$$

and

$$t(r-1)+3t(r+1) = t(2r+1),\ \ m(r-1)+3m(r+1) = m(2r+1).$$

So,

$$\begin{aligned}\psi_n &= \frac{a^{t(n)}}{(v-1)^{m(n)}}(128a^7u^4(aw+bv+a-b)^4v^{-2}\widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - \widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3) \\ &= \frac{a^{m(n)}}{v^{m(n)}}\widetilde{\psi}_n\end{aligned}$$

From the curve equation $au^2+v^2=1$, we have

$$\begin{aligned}\widetilde{\psi}_n &= 128a^5(1-v^2)^3(aw+bv+a-b)^4v^{-2}\widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - \widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3 \\ &= 8a^3(4a(v^{-1}-v)(aw+bv+a-b)^2)^2\widetilde{\psi}_{r+2}\widetilde{\psi}_r^3 - \widetilde{\psi}_{r-1}\widetilde{\psi}_{r+1}^3\end{aligned}$$

Cases $3,\ldots,8$: $n \equiv 2,\ldots,7 \pmod 8$. Similar. □

Corollary 3.6. *Let $P=(u,v,w)$ be in $J_{a,b}(\overline{K}) \setminus (0,1,1)$ and let $n \geq 1$. Then P is an n-torsion point of $J_{a,b}$ if and only if $\widetilde{\psi}(v,w)=0$.*

Proof. The result follows form Corollary 3.4 and Theorem 3.5. □

Corollary 3.7. *For a positive integer n, $\widetilde{\psi}_n$ be a polynomial in $\mathbb{Z}[u,v,w,a,b]$. If n is odd, then the degree of $\widetilde{\psi}_n$ is $\frac{n^2-1}{2}$ as a polynomial v with coefficients in $\mathbb{Z}[v,a,b]$. If n is even, the degree of $\widetilde{\psi}_n$ is $\frac{n^2-4}{2}$ as a polynomial v with coefficients in $Z[v,a,b]$.*

Proof. All polynomials appearing in the definition of the division polynomials $\widetilde{\psi}_{2n}$ and $\widetilde{\psi}_{2n+1}$ satisfy the induction assumptions in Theorem 3.5. So, $\widetilde{\psi}_n$ is a polynomial in $\mathbb{Z}[v,w,a,b]$ for a positive integer n. Also, the degree of $\widetilde{\psi}_n$ is clearly derived by induction rule. □

We now look at another kind of division polynomials for twisted Jacobi intersections curves. We denote the coordinates of $[n](u,v,w)$ by (u_n,v_n,w_n).

Theorem 3.8. *Let $P_1(t)=1$, $Q_1(t)=1$, $P_2(t)=2$, $Q_2(t)=1-abt^4$, $G_1(t)=1$, $G_2(t)=1-2at^2+abt^4$, $H_1(t)=1$, and $H_2(t)=1-2bt^2+abt^4$. Then we have*

$$(u_{2n},v_{2n},w_{2n})=\Big(uvw\frac{P_{2n}(u)}{Q_{2n}(u)},\frac{G_{2n}(u)}{Q_{2n}(u)},\frac{H_{2n}(u)}{Q_{2n}(u)}\Big)$$
$$(u_{2n+1},v_{2n+1},w_{2n+1})=\Big(u\frac{P_{2n+1}(u)}{Q_{2n+1}(u)},v\frac{G_{2n+1}(u)}{Q_{2n+1}(u)},w\frac{H_{2n+1}(u)}{Q_{2n+1}(u)}\Big)$$

where $P_n(t)$, $Q_n(t)$, $G_n(t)$, and $H_n(t)\in\mathbb{Z}[t]$ are defined by

$$\begin{aligned}
P_{2n+2}(t)&=2P_{2n+1}Q_{2n+1}Q_{2n}-P_{2n}(Q_{2n+1}^2-abt^4P_{2n+1}^2)\\
Q_{2n+2}(t)&=Q_{2n}(Q_{2n+1}^2-abt^4P_{2n+1}^2)\\
G_{2n+2}(t)&=2(1-at^2)G_{2n+1}Q_{2n+1}Q_{2n}-G_{2n}(Q_{2n+1}^2-abt^4P_{2n+1}^2)\\
H_{2n+2}(t)&=2(1-at^2)H_{2n+1}Q_{2n+1}Q_{2n}-H_{2n}(Q_{2n+1}^2-abt^4P_{2n+1}^2)
\end{aligned}$$

and

$$\begin{aligned}
P_{2n+1}(t)&=(1-at^2)(1-bt^2)P_{2n}(2Q_{2n}Q_{2n-1}+abt^4P_{2n}P_{2n-1})-P_{2n-1}Q_{2n}^2\\
Q_{2n+1}(t)&=Q_{2n-1}(Q_{2n}^2-abt^4(1-at^2)(1-bt^2)P_{2n}^2)\\
G_{2n+1}&=2G_{2n}Q_{2n}Q_{2n-1}-G_{2n-1}(Q_{2n}^2-abt^4(1-at^2)(1-bt^2)P_{2n}^2)\\
H_{2n+1}&=2H_{2n}Q_{2n}Q_{2n-1}-H_{2n-1}(Q_{2n}^2-abt^4(1-at^2)(1-bt^2)P_{2n}^2)
\end{aligned}$$

Proof. The proof follows in the similar way to compute division polynomials for Edwards curves[14]. They take Abel's way to find the n-division points of leminiscate [1].

We use induction on n. The claim is true for $n=1$,

$$(u_1,v_1,w_1)=\Big(u\frac{P_1(u)}{Q_1(u)},v\frac{G_1(u)}{Q_1(u)},w\frac{H_1(u)}{Q_1(u)}\Big).$$

For $n=2$, the doubling formula yields

$$(u_2,v_2,w_2)=\Big(\frac{2uvw}{v^2+au^2w^2},\frac{v^2-au^2w^2}{v^2+au^2w^2},\frac{w^2-bu^2v^2}{v^2+au^2w^2}\Big).$$

By the defining curve equation, we have that $au^2+v^2=1$ and $bu^2+w^2=1$, so

$$(u_2,v_2,w_2)=\Big(uvw\frac{P_2(u)}{Q_2(u)},\frac{G_2(u)}{Q_2(u)},\frac{H_2(u)}{Q_2(u)}\Big).$$

Given two points (u_1,v_1,w_1) and (u_2,v_2,w_2) on $J_{a,b}$, let $(u_+,v_+,w_+)=(u_1,v_1,w_1)+(u_2,v_2,w_2)$ and $(u_-,v_-,w_-)=(u_1,v_1,w_1)-(u_2,v_2,w_2)$. Then using the addition law for twisted Jacobi intersection, we have

$$u_++u_-=\frac{2u_1v_2w_2}{v_2^2+au_2^2w_1^2},\ v_++v_-=\frac{2v_1v_2}{v_2^2+au_2^2w_1^2},\ \text{and}\ w_++w_-=\frac{2w_1w_2}{v_2^2+au_2^2w_1^2}.$$

Setting $(u_1, v_1, w_1) = (u_n, v_n, w_n)$ and $(u_2, v_2, w_2) = (u, v, w)$. we see that

$$\begin{aligned} u_{n+1} &= \frac{2u_nvw}{v^2 + au^2w_n^2} - u_{n-1} = \frac{2u_nvw}{v^2 + au^2 - abuu_n^2} - u_{n-1} \\ &= \frac{2u_nvw}{1 - abu^2u_n^2} - u_{n-1}, \\ v_{n+1} &= \frac{2vv_n}{1 - abu^2u_n^2} - v_{n-1}, \text{ and } w_{n+1} = \frac{2vw_n}{1 - abu^2u_n^2} - w_{n-1}. \end{aligned}$$

Consider the two cases that n is odd or even. Assume that n is odd ($n = 2k + 1$), we have

$$\begin{aligned} u_{n+1} &= \frac{2vw\Big(u\frac{P_{2k+1}}{Q_{2k+1}}\Big)}{1 - abu^2\Big(u\frac{P_{2k+1}}{Q_{2k+1}}\Big)^2} - uvw\frac{P_{2k}}{Q_{2k}} \\ &= \frac{2uvwP_{2k+1}Q_{2k+1}}{Q_{2k+1}^2 - abu^4P_{2k+1}^2} - uvw\frac{P_{2k}}{Q_{2k}} \\ &= uvw\Big(\frac{2P_{2k+1}Q_{2k+1}Q_{2k} - P_{2k}(Q_{2k+1}^2 - abu^4P_{2k+1}^2)}{Q_{2k}(Q_{2k+1}^2 - abu^4P_{2k+1}^2)}\Big) = uvw\frac{P_{n+1}}{Q_{n+1}}, \end{aligned}$$

$$\begin{aligned} v_{n+1} &= \frac{2v\Big(v\frac{G_{2k+1}}{Q_{2k+1}}\Big)}{1 - abu^2\Big(u\frac{P_{2k+1}}{Q_{2k+1}}\Big)^2} - \frac{G_{2k}}{Q_{2k}} \\ &= \frac{2v^2G_{2k+1}Q_{2k+1}}{Q_{2k+1}^2 - abu^4P_{2k+1}^2} - \frac{G_{2k}}{Q_{2k}} \\ &= \frac{2v^2G_{2k+1}Q_{2k+1}Q_{2k} - G_{2k}(Q_{2k+1}^2 - abu^4P_{2k+1}^2)}{Q_{2k}(Q_{2k+1}^2 - abu^4P_{2k+1}^2)} = \frac{G_{n+1}}{Q_{n+1}} \end{aligned}$$

When $n = 2k$ is even, we have

$$\begin{aligned} u_{n+1} &= \frac{2vw(uvw\frac{P_{2k}}{Q_{2k}})}{1 - abu^2(uvw\frac{P_{2k}}{Q_{2k}})^2} - u\frac{P_{2k-1}}{Q_{2k-1}} \\ &= \frac{2uv^2w^2P_{2k}Q_{2k}}{Q_{2k}^2 - abu^4v^2w^2P_{2k}^2} - u\frac{P_{2k-1}}{Q_{2k-1}} \\ &= \frac{2uv^2w^2P_{2k}Q_{2k}Q_{2k-1} - uP_{2k-1}(Q_{2k}^2 - abu^4v^2w^2P_{2k}^2)}{Q_{2k-1}(Q_{2k}^2 - abu^4v^2w^2P_{2k}^2)} \\ &= u\Big(\frac{(1 - au^2)(1 - bu^2)P_{2k}(2Q_{2k}Q_{2k-1} + abu^4P_{2k}P_{2k-1}) - P_{2k-1}Q_{2k}^2}{Q_{2k-1}(Q_{2k}^2 - abu^4(1 - au^2)(1 - bu^2)P_{2k}^2)}\Big) \\ &= u\frac{P_{n+1}}{Q_{n+1}}, \end{aligned}$$

$$\begin{aligned} v_{n+1} &= \frac{2v(\frac{G_{2k}}{Q_{2k}})}{1-abu^2(uvw\frac{P_{2k}}{Q_{2k}})^2} - v\frac{G_{2k-1}}{Q_{2k-1}} \\ &= \frac{2vG_{2k}Q_{2k}}{Q_{2k}^2 - abu^4v^2w^2P_{2k}^2} - v\frac{G_{2k-1}}{Q_{2k-1}} \\ &= \frac{2vG_{2k}Q_{2k}Q_{2k-1} - G_{2k-1}(Q_{2k}^2 - abu^4v^2w^2P_{2k}^2)}{Q_{2k-1}(Q_{2k}^2 - abu^4v^2w^2P_{2k}^2)} = v\frac{G_{n+1}}{Q_{n+1}} \end{aligned}$$

Similarly, we can compute the w_{n+1} for n odd and even. □

Acknoledgements

This paper is dedicated to Professor Dae San Kim who will get an honorable retirement form Sogang University in Seoul, August of 2016.

References

[1] N. Abel, Oeuvres Completes, Nouvelle Edition, Oslo, 1881.
[2] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. 61(203) (1993), 29–68.
[3] I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series 265, 1999.
[4] O. Billet, and M. Joye, *The Jacobi model of an elliptic curve and side-channel analysis*, In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 2003 proceedings, LNCS vol 2643, pages 34–42, Springer, 2003.
[5] D. V. Chudnovsky, and G. V. Chudnovsky, Sequences of numbers gnerated by addition in formal groups and new primality and factorization tests, Advances in Applied Mathematics 7(1986), 385–434.
[6] H. M. Edwards, *A normal form for elliptic curves*, Bull. Am. Math. Soc., New Ser. 44(3) (2007), 393–422.
[7] R.Q. Feng, M.L. Nie, H.F. Wu, Twisted Jacobi Intersections Curves, Theory and applications of models of computation, Lecture Notes in Computer Science, 2010, Volume 6108/2010, 199–210.
[8] S. Goldwaser and J. Kilian, *Primality testing using elliptic curves*, J. ACM 46(4) (1999), 450–472.
[9] G. B. Huff, *Diophantine problems in geometry and elliptic ternary forms*, Duke Math. J. 15 (1948), 443–453.
[10] M. Joye, and J. Quisquater, *Hessian elliptic curves and side-channel attacks*, In Workshop on Cryptographic Hardware and Embedded systems proceedings, LNCS vol 2162, pages 402–410, springer, 2001.
[11] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. 48 (1987), 203–209.
[12] H. W. Lenstra, Jr. *Factoring integers with elliptic curves*, Ann. Math. 126(2) (1987), 649–673.
[13] G. McGuire, and R. Moloney, *Two Kinds of Division Polynomials For Twisted Edward Curves*, Available at
[14] G. McGuire and R. Moloney, *Two Kinds of Division Polynomials For Twisted Edward Curves*, Applicable Algebra in Engineering, Communication and Computing, vol. 22, no. 5-6, pp. 321–345, 2011.
[15] V. S. Miller, *Use of elliptic curves in cryptography*, In H. C. Williams, editor, Advances in Cryptology-CRYPTO'85, Lect. Notes Comput. Sci. 218 (1986), 417–426.
[16] P. L. Mongomery, *Speeding up the Pollard and elliptic curve methods of factorization*, Mathematics of Computation 48(177) (1987), 243-264.
[17] D. Moody, *Division Polynomials for Alternate Models of Elliptic Curves*, 2010.
[18] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, 2003.

Department of Mathematics Education, Daegu National University of Education, Daemyung 2-dong, Daegu, Republic of Korea
E-mail address: gysohn@dnue.ac.kr