International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 1, (2025), 291–305
DOI: https://doi.org/10.69793/ijmcs/01.2025/genesis

The Multi-Variable Division Polynomials for the Holm Curve

Genesis Alberto

Department of Mathematics and Computer Science
Faculty of Mathematics
CUNY John Jay College of Criminal Justice
New York, NY, USA

email: galberto@jjay.cuny.edu

(Received May 28, 2024, Revised August 3, 2024,
Accepted August 5, 2024, Published October 24, 2024)

Abstract

This paper presents the division polynomials for the Holm curve and a few of their properties. One of the main properties being the n torsion points for a given Holm curve.

1 Introduction

Let p be a prime number and $\mathbb{K} = \mathbb{F}_p$ be the finite field with p elements not of characteristic 2 or 3. It is well known that an elliptic curve can be defined by using its Weierstrass equation:

$$W : Y^2 = X^3 + aX + b$$

where $a, b \in \mathbb{K}$, and there is an extra point $\mathcal{O}$ at infinity. The division polynomials $\Psi_n \in \mathbb{Z}[X, Y, a, b]$ for the curve are defined recursively, for $n, m \in \mathbb{N}$ as shown:

Key words and phrases: Elliptic curve, Division polynomial, Holm.
AMS (MOS) Subject Classifications: 11G07, 14H52.
ISSN 1814-0432, 2025, https://future-in-tech.net

$$\begin{aligned}
\Psi_0(X,Y) &= 0\\
\Psi_1(X,Y) &= 1\\
\Psi_2(X,Y) &= 2Y\\
\Psi_3(X,Y) &= 3X^4+6aX^2+12bX-a^2\\
\Psi_4(X,Y) &= 4Y(X^6+5aX^4+20bX^3-5a^2X^2-4abX-a^3-8b^2)\\
\Psi_{2m+1}(X,Y) &= \Psi_{m+2}\Psi_m^3-\Psi_{m-1}\Psi_{m+1}^3 \text{ for m} \geq 2\\
\Psi_{2m}(X,Y) &= \frac{\Psi_m}{\Psi_2}\left(\Psi_{m+2}\Psi_{m-1}^2-\Psi_{m-2}\Psi_{m+1}^2\right) \text{ for m} \geq 3.
\end{aligned}$$

We abbreviate the notation so that $\Psi_n = \Psi_n(x,y)$. The curve itself has group properties with the point at infinity, $\mathcal{O}$, as the identity element. Here, we can use these division polynomials to find the coordinates of the point nP for an $n \in \mathbb{N}$ and $P=(x,y)\in W$ by using the multiplication-by-n map $[n]: W \to W$.

$$[n](X,Y) = \left(\frac{X\Psi_n^2-\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{2n}}{2\Psi_n^4}\right)$$

Using the division polynomials we have that (X,Y) is an n-torsion point of W (i.e. $[n](X,Y)=\mathcal{O}$) if and only if $\Psi_n(X,Y)=0$. (see [6], Chapter 1 of [2], Chapter 3 of [8], and Chapter 3 of [10])

In this paper, we will show analogous results for the Holm Curve. We will use (X,Y) to refer to an equation in Weierstrass form and reserve (x,y) when we are referring to the Holm curve.

2 The Holm Curve

The Holm curve is defined by:

$$H_{a,b}: by(y^2-1) = ax(x^2-1)$$

where $a,b\in\mathbb{K}$, $ab\neq 0, a\neq \pm b$. Putting $\lambda = \dfrac{a}{b}$ we rewrite the curve as

$$H_\lambda: y^3-y=\lambda(x^3-x)$$

where $\lambda \neq 0, \pm 1$. This is the form we will use when referring to the Holm curve.

Investigating the points at infinity, we see they occur when $z = 0$ in the projective space. The points at infinity are $(1, \sqrt[3]{\lambda}, 0)$. If $\rho = \sqrt[3]{1}$ and $\sqrt[3]{\lambda} \in \mathbb{K}$, then the three points at infinity are $(1 : \rho\sqrt[3]{\lambda} : 0), (1 : \rho^2\sqrt[3]{\lambda} : 0)$ and $(1 : \sqrt[3]{\lambda} : 0)$. Furthermore, the curve is an elliptic curve and the points $(0,0), (0,\pm 1), (\pm 1, 0)$ and $(\pm 1, \pm 1)$ are contained in H_λ for all possible λ.

2.1 Group structure

The points on the curve can be added under the following operation: Let $P = (x_1, y_1)$, $Q = (x_2, y_2) \in H_\lambda$ where $P \neq Q$. Then we define $P + Q = R$ and $R = (x_3, y_3)$ where

$$\begin{aligned} x_3 &= \frac{3(x_2 - x_1)(y_2 - y_1)^2 y_1 - 3(y_2 - y_1)^3 x_1}{(y_2 - y_1)^3 - (x_2 - x_1)^3 \lambda} + x_1 + x_2 \\ y_3 &= \frac{3\lambda(x_2 - x_1)^3 y_1 - 3\lambda(x_2 - x_1)^2 (y_2 - y_1) x_1}{(y_2 - y_1)^3 - (x_2 - x_1)^3 \lambda} + y_1 + y_2 \end{aligned}$$

Under this operation the curve forms an abelian group with the point $\mathcal{O} = (0,0)$ as its identity. The additive inverse of the point $(x, y) \in H_\lambda$ is $(-x, -y)$.

2.2 Bi-rational mapping

The curve is also bi-rationally equivalent to the elliptic curve with Weierstrass equation

$$E_\lambda : Y^2 - X^3 + 3\lambda^2 X - \lambda^2(\lambda^2 + 1) = 0$$

under the rational mapping

$$(x, y) \mapsto \left(\frac{\lambda(x - \lambda y)}{\lambda x - y}, \frac{\lambda(1 - \lambda^2)}{\lambda x - y} \right) = (X, Y)$$

$$(X, Y) \mapsto \left(\frac{X - \lambda^2}{Y}, \frac{\lambda(X - 1)}{Y} \right) = (x, y)$$

with the addition of mapping origin $(0,0) \in H_\lambda$ to origin $(0,1,0) \in E_\lambda$ where $\lambda \in \mathbb{K}$ and $\lambda \neq 0, \pm 1$.

2.3 Function Fields

Theorem 1. *Consider the Holm curve*

$$H_\lambda : y^3 - y = \lambda \left(x^3 - x\right).$$

Let the function field $K(H_\lambda) = K(x, y)$. *Then*

a. $[K(x, y) : K(x)] = 3$,

b. every element $f(x, y) \in K(x, y)$ *can be written uniquely as*

$$f(x, y) = A_1(x) + yB_1(x) + y^2 C_1(x)$$

where $A_1(x)$, $B_1(x)$, $C_1(x)$ *are rational functions in* $K(x)$.

Proof. It is enough to show that in $K(x)[T]$, T indeterminate, the polynomial

$$T^3 - T - \lambda x^3 + \lambda x$$

is irreducible. If it were not irreducible, it would have a factor of degree one, hence, it would have a root in $K(x)$. Let $\frac{f(x)}{g(x)}$ be such a root, where $f(x)$ and $g(x)$ are in $K[x]$ and we may assume that their GCD in $K[x]$ is 1. Plugging in the root forces $g(x) = 1$, the polynomial $f(x)$ satisfies

$$(f(x))^3 - f(x) = \lambda x (x-1)(x+1).$$

In $K[x]$, this equation gives the expansion of $(f(x))^3 - f(x)$ as a product of irreducible polynomials. Since $char(K) \neq 2$, the three factors on the right hand side are distinct.

Looking at the degrees of both sides leads to

$$\deg(f(x)) = 1$$

hence

$$f(x) = ax + b$$

for $a, b \in \mathbb{K}$. We find

$$(ax+b)(ax+b-1)(ax+b+1) = \lambda x (x-1)(x+1).$$

By uniqueness of the decomposition into a product of irreducible factors we obtain

$$\{ax+b, ax+b-1, ax+b+1\} = \{\lambda x, x-1, x+1\}.$$

Taking into consideration all the possibilities will lead to a contradiction in each case. Hence $T^3 - T - \lambda x^3 + \lambda x$ is irreducible in $K(x)[T]$.

As y is a root of this polynomial, $[K(x,y) : K(x)] = 3$ and $\{1, y, y^2\}$ is a basis for $K(x,y)$ over $K(x)$.

□

Theorem 2. *Consider the Weierstrass model*

$$E_\lambda : Y^2 = X^3 - 3\lambda^2 X + \lambda^2(\lambda^2+1)$$

Let the function field $K(E_\lambda) = K(X,Y)$. Then

a. $[K(X,Y) : K(X)] = 2$,

b. every element $g(X,Y) \in K(X,Y)$ can be written uniquely as

$$g(X,Y) = A_2(X) + YB_2(X)$$

where $A_2(X)$, $B_2(X)$ are rational function in $K(X)$.

Proof. It is enough to show that in $K(X)[T]$, T indeterminate, the polynomial

$$T^2 - X^3 + 3\lambda^2 X - \lambda^2(\lambda^2+1)$$

is irreducible. If it were not, then $X^3 - 3\lambda^2 X + \lambda^2(\lambda^2+1)$ would be a square in $K[X]$. A degree consideration leads to a contradiction.

As Y is a root of this polynomial, $[K(X,Y) : K(X)] = 2$ and $\{1, Y\}$ is a basis for $K(X,Y)$ over $K(X)$.

□

3 Multi-Variable Division Rational Functions

In order to form the division polynomials for H_λ we need to use the division polynomials for an Elliptic curve in the Weierstrass form, and the bi-rational correspondence between the curve E_λ and H_λ. We define the following rational functions $\psi_n(x,y)$ recursively for $n \geq 0$:

$$\begin{aligned}
\psi_0(x,y) &:= 0\\
\psi_1(x,y) &:= 1\\
\psi_2(x,y) &:= \frac{2\lambda(1-\lambda^2)}{\lambda x - y}\\
\psi_3(x,y) &:= \frac{3\lambda^4(x-\lambda y)^4}{(\lambda x - y)^4} - \frac{18\lambda^4(x-\lambda y)^2}{(\lambda x - y)^2}\\
&\quad + \frac{12\lambda^3(\lambda^2+1)(x-\lambda y)}{\lambda x - y} - 9\lambda^4\\
\psi_4(x,y) &:= \frac{4\lambda^7(1-\lambda^2)(x-\lambda y)^6}{(\lambda x - y)^7} - \frac{60\lambda^7(1-\lambda^2)(x-\lambda y)^4}{(\lambda x - y)^5}\\
&\quad + \frac{80\lambda^6(1-\lambda^4)(x-\lambda y)^3}{(\lambda x - y)^4} - \frac{180\lambda^7(1-\lambda^2)(x-\lambda y)^2}{(\lambda x - y)^3}\\
&\quad + \frac{48\lambda^6(1-\lambda^4)(x-\lambda y)}{(\lambda x - y)^2} + \frac{108\lambda^7(1-\lambda^2)}{\lambda x - y}\\
&\quad - \frac{32\lambda^5(\lambda^2+1)^2(1-\lambda^2)}{\lambda x - y}
\end{aligned}$$

$$\begin{aligned}
\psi_{2m+1}(x,y) &:= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for m} \geq 2\\
\psi_{2m}(x,y) &:= \frac{\psi_m}{\psi_2}\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \text{ for m} \geq 3.
\end{aligned}$$

Let's call these functions the division rational functions. The notation can be abbreviated just as with Ψ_n, by letting $\psi_n = \psi_n(x,y)$. Notice these functions are not defined at the point $(0,0)$).

We can factor the division rational functions. Doing so we obtain a quotient multiplied by a polynomial in terms of x and y. Let's call these polynomials the multi-variable division polynomials, as defined in the following theorem.

Theorem 3. *The multi-variable division polynomials, denoted $\tilde{\psi}_n$, are defined by*

$$\psi_n = \frac{\lambda^{k(n)}\tilde{\psi}_n}{(\lambda x - y)^{m(n)}}$$

where

$$m(n) = \begin{cases} \dfrac{n^2-2}{2} & \textit{if } n \textit{ is even} \\ \dfrac{n^2-1}{2} & \textit{if } n \textit{ is odd} \end{cases} \qquad k(n) = \left\lceil \frac{n^2-1}{3} \right\rceil$$

and

$$\begin{aligned}
\tilde{\psi}_0(x,y) &= 0 \\
\tilde{\psi}_1(x,y) &= 1 \\
\tilde{\psi}_2(x,y) &= 2(1-\lambda^2) \\
\tilde{\psi}_3(x,y) &= 3\lambda(x-\lambda y)^4 - 18\lambda(x-\lambda y)^2(\lambda x - y)^2 \\
&\quad +12(\lambda^2+1)(x-\lambda y)(\lambda x - y)^3 - 9\lambda(\lambda x - y)^4 \\
\tilde{\psi}_4(x,y) &= 4\lambda^2(1-\lambda^2)(x-\lambda y)^6 - 60\lambda^2(1-\lambda^2)(x-\lambda y)^4(\lambda x - y)^2 \\
&\quad +80\lambda(1-\lambda^4)(x-\lambda y)^3(\lambda x - y)^3 \\
&\quad -180\lambda^2(1-\lambda^2)(x-\lambda y)^2(\lambda x - y)^4 \\
&\quad +48\lambda(1-\lambda^4)(x-\lambda y)(\lambda x - y)^5 \\
&\quad +108\lambda^2(1-\lambda^2)(\lambda x - y)^6 - 32(\lambda^2+1)^2(1-\lambda^2)(\lambda x - y)^6
\end{aligned}$$

and

$$\tilde{\psi}_{2r} = \begin{cases} \frac{\tilde{\psi}_r}{\tilde{\psi}_2}(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2) & \textit{if } r \equiv 0,3 \mod 6, r \geq 3 \\ \frac{\tilde{\psi}_r}{\tilde{\psi}_2}(\lambda\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2) & \textit{if } r \equiv 1,4 \mod 6, r \geq 4 \\ \frac{\tilde{\psi}_r}{\tilde{\psi}_2}(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \lambda\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2) & \textit{if } r \equiv 2,5 \mod 6, r \geq 5 \end{cases}$$

and

$$\tilde{\psi}_{2r+1} = \begin{cases} \lambda(\lambda x - y)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & \textit{if } r \equiv 0 \mod 6, r \geq 6 \\ \tilde{\psi}_{r+2}\tilde{\psi}_r^3 - (\lambda x - y)^2\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & \textit{if } r \equiv 1 \mod 6, r \geq 7 \\ (\lambda x - y)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \lambda\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & \textit{if } r \equiv 2 \mod 6, r \geq 2 \\ \lambda\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - (\lambda x - y)^2\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & \textit{if } r \equiv 3 \mod 6, r \geq 3 \\ (\lambda x - y)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & \textit{if } r \equiv 4 \mod 6, r \geq 4 \\ \tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \lambda(\lambda x - y)^2\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3 & \textit{if } r \equiv 5 \mod 6, r \geq 5 \end{cases}$$

Proof. First observe that for all $t \in \mathbb{Z}, t > 0$,

$$\begin{aligned} m(6t) &= 18t^2 - 1 \\ m(6t \pm 1) &= 18t^2 \pm 6t \\ m(6t \pm 2) &= 18t^2 \pm 12t + 1 \\ m(6t \pm 3) &= 18t^2 \pm 18t + 4 \end{aligned}$$

$$\begin{aligned} k(6t) &= 12t^2 \\ k(6t \pm 1) &= 12t^2 \pm 4t \\ k(6t \pm 2) &= 12t^2 \pm 8t + 1 \\ k(6t \pm 3) &= 12t^2 \pm 12t + 3 \end{aligned}$$

$$\begin{aligned} m(12t) &= = 72t^2 - 1 & k(12t) &= 48t^2 \\ m(12t \pm 1) &= 72t^2 \pm 12t & k(12t \pm 1) &= 48t^2 \pm 8t \\ m(12t \pm 2) &= 72t^2 \pm 24t + 1 & k(12t \pm 2) &= 48t^2 \pm 16t + 1 \\ m(12t \pm 3) &= 72t^2 \pm 36t + 4 & k(12t \pm 3) &= 48t^2 \pm 24t + 3 \\ m(12t \pm 4) &= 72t^2 \pm 48t + 7 & k(12t \pm 4) &= 48t^2 \pm 32t + 5 \\ m(12t \pm 5) &= 72t^2 \pm 60t + 12 & k(12t \pm 5) &= 48t^2 \pm 40t + 8 \\ m(12t + 6) &= 72t^2 + 72t + 17 & k(12t + 6) &= 48t^2 + 48t + 12 \end{aligned}$$

This proof is by induction. We see that it is true for $n = 1, 2, 3, 4$. Assume it is true for all values up to the $n - 1$ case.

Case 1: Let $n \equiv 0 \mod 12$, $n = 12l$ for some $l \in \mathbb{Z}$, and $r = 6l$. By definition we have:

$$\begin{aligned} \psi_n &= \frac{\psi_r}{\psi_2}\left(\psi_{r+2}\psi_{r-1}^2 - \psi_{r-2}\psi_{r+1}^2\right) \\ &= \frac{\lambda^{k(r)-1}\tilde{\psi}_r}{(\lambda x - y)^{m(r)-1}\tilde{\psi}_2}\left(\frac{\lambda^{k(r+2)+2k(r-1)}\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2}{(\lambda x - y)^{m(r+2)+2m(r-1)}} - \frac{\lambda^{k(r-2)+2k(r+1)}\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2}{(\lambda x - y)^{m(r-2)+2m(r+1)}}\right) \\ &= \frac{\tilde{\psi}_r}{\tilde{\psi}_2}\left(\frac{\lambda^{k(r)-1+k(r+2)+2k(r-1)}\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2}{(\lambda x - y)^{m(r)-1+m(r+2)+2m(r-1)}} - \frac{\lambda^{k(r)-1+k(r-2)+2k(r+1)}\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2}{(\lambda x - y)^{m(r)-1+m(r-2)+2m(r+1)}}\right) \end{aligned}$$

Notice,

$$\begin{aligned} k(6l)-1+k(6l+2)+2k(6l-1) &= 12l^2-1+12l^2+8l+1+24l^2-8l \\ &= 48l^2 = k(12l) = k(n) \\ k(6l)-1+k(6l-2)+2k(6l+1) &= 12l^2-1+12l^2-8l+1+24l^2+8l \\ &= 48l^2 = k(12l) = k(n) \end{aligned}$$

and

$$\begin{aligned} m(6l)-1+m(6l+2)+2m(6l-1) &= 18l^2-1-1+18l^2+12l+1+36l^2-12l \\ &= 72l^2-1 = m(12l) = m(n) \\ m(6l)-1+m(6l-2)+2m(6l+1) &= 18l^2-1-1+18l^2-12l+1+36l^2+12l \\ &= 72l^2-1 = m(12l) = m(n) \end{aligned}$$

Thus,

$$\begin{aligned} \psi_n(x,y) &= \frac{\lambda^{k(n)}}{(\lambda x-y)^{m(n)}}\left[\frac{\tilde{\psi}_r}{\tilde{\psi}_2}(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2-\tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2)\right] \\ &= \frac{\lambda^{k(n)}\tilde{\psi}_{2r}}{(\lambda x-y)^{m(n)}} = \frac{\lambda^{k(n)}\tilde{\psi}_n}{(\lambda x-y)^{m(n)}} \end{aligned}$$

<u>Case 2:</u> Let $n \equiv 1 \mod 12$, $n = 12l+1$ for some $l \in \mathbb{Z}$, and $r = 6l$. By definition we have:

$$\begin{aligned} \psi_n(x,y) &= \psi_{r+2}\psi_r^3-\psi_{r-1}\psi_{r+1}^3 \\ &= \frac{\lambda^{k(r+2)+3k(r)}\tilde{\psi}_{r+2}\tilde{\psi}_r^3}{(\lambda x-y)^{m(r+2)+3m(r)}} - \frac{\lambda^{k(r-1)+3k(r+1)}\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3}{(\lambda x-y)^{m(r-1)+3m(r+1)}} \end{aligned}$$

Notice,

$$\begin{aligned} k(6l+2)+3k(6l) &= 12l^2+8l+1+36l^2 \\ &= 48l^2+8l+1 = k(12l+1)+1 = k(n)+1 \\ k(6l-1)+3k(6l+1) &= 12l^2-4l+36l^2+12l \\ &= 48l^2+8l = k(12l+1) = k(n) \end{aligned}$$

and

$$\begin{aligned} m(6l+2)+3m(6l) &= 18l^2+12l+1+54l^2-3 \\ &= 72l^2+12l-2 = m(12l+1)-2 = m(n)-2 \\ m(6l-1)+3m(6l+1) &= 18l^2-6l+54l^2+18l \\ &= 72l^2+12l = m(12l+1) = m(n) \end{aligned}$$

Thus,

$$\begin{aligned} \psi_n(x,y) &= \frac{\lambda^{k(n)}}{(\lambda x-y)^{m(n)}}\left(\lambda(\lambda x-y)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3-\tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3\right) \\ &= \frac{\lambda^{k(n)}\tilde{\psi}_{2r+1}}{(\lambda x-y)^{m(n)}} = \frac{\lambda^{k(n)}\tilde{\psi}_n}{(\lambda x-y)^{m(n)}} \end{aligned}$$

Case 3, ... 12: $n \equiv 2, \ldots 11 \mod 12$. Similar. □

Also, these equations are in fact, polynomials.

Theorem 4. *$\tilde{\psi}_n(x,y) \in \mathbb{Z}[\lambda,x,y]$, $\forall n \geq 0$ and $2(1-\lambda^2)$ divides $\tilde{\psi}_n(x,y)$ if n is even.*

Proof. Here notice

$$\begin{aligned} \tilde{\psi}_0 &= 0 \\ \tilde{\psi}_1 &= 1 \\ \tilde{\psi}_2 &= 2(1-\lambda^2) \\ \tilde{\psi}_3 &= 3\lambda(x-\lambda y)^4-18\lambda(x-\lambda y)^2(\lambda x-y)^2 \\ &\quad +12(\lambda^2+1)(x-\lambda y)(\lambda x-y)^3-9\lambda(\lambda x-y)^4 \\ \tilde{\psi}_4 &= 2(1-\lambda^2)\begin{bmatrix} 2\lambda^2(x-\lambda y)^6-30\lambda^2(x-\lambda y)^4(\lambda x-y)^2 \\ +40\lambda(1+\lambda^2)(x-\lambda y)^3(\lambda x-y)^3 \\ -90\lambda^2(x-\lambda y)^2(\lambda x-y)^4 \\ +24\lambda(1+\lambda^2)(x-\lambda y)(\lambda x-y)^5 \\ +54\lambda^2(\lambda x-y)^6-16(\lambda^2+1)^2(\lambda x-y)^6 \end{bmatrix} \end{aligned}$$

Thus the statement is true for $n = 0,1,2,3,4$. Suppose it is true for values up to $n-1$.

Case 1: Let $n \equiv 0 \mod 12$, $n = 12l$ for some $l \in \mathbb{Z}$, and $r = 6l$.

Thus, $\tilde{\psi}_n = \frac{\tilde{\psi}_r}{2(1-\lambda^2)}(\tilde{\psi}_{r+2}\tilde{\psi}_{r-1}^2 - \tilde{\psi}_{r-2}\tilde{\psi}_{r+1}^2)$.

By hypothesis $\tilde{\psi}_r, \tilde{\psi}_{r+2}, \tilde{\psi}_{r-1}, \tilde{\psi}_{r-2}, \tilde{\psi}_{r+1} \in \mathbb{Z}[\lambda, x, y]$ and $2(1-\lambda^2)$ divides $\tilde{\psi}_r, \tilde{\psi}_{r+2}$ and $\tilde{\psi}_{r-2}$. Thus $\tilde{\psi}_n \in \mathbb{Z}[\lambda, x, y]$ and is divisible by $2(1-\lambda^2)$.

Case 2: Let $n \equiv 1 \mod 12$, $n = 12l + 1$ for some $l \in \mathbb{Z}$, and $r = 6l$.

Thus, $\tilde{\psi}_n = \lambda(\lambda x - y)^2\tilde{\psi}_{r+2}\tilde{\psi}_r^3 - \tilde{\psi}_{r-1}\tilde{\psi}_{r+1}^3$.

By hypothesis $\tilde{\psi}_{r+2}, \tilde{\psi}_r, \tilde{\psi}_{r-1}, \tilde{\psi}_{r+1} \in \mathbb{Z}[\lambda, x, y]$. Thus, $\tilde{\psi}_n \in \mathbb{Z}[\lambda, x, y]$.

Case 3, ... 12: $n \equiv 2, \dots 11 \mod 12$. Similar. □

4 Properties of Multi-Variable Division Rational Functions

Using the multi-variable division rational functions, we can find what nP equals for a point $P \in H_\lambda$ and $n \in \mathbb{N}$.

Theorem 5. *Let (x,y) be a point in $H_\lambda(\mathbb{F}_p)\backslash\{(0,0)\}$ and $n \geq 1$ be an integer. Then*

$$[n](x, y) = (x\alpha - \omega, y\alpha - \lambda\omega)$$

where:

$$\alpha = \frac{2\lambda(1-\lambda^2)\psi_n^4}{(\lambda x - y)\psi_{2n}} \qquad \omega = \frac{2\psi_{n-1}\psi_n^2\psi_{n+1}}{\psi_{2n}}$$

Proof. We know for an elliptic curve of Weierstrass form: $Y^2 = X^3 + aX + b$,

$$[n](X, Y) = \left(\frac{X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{2n}}{2\Psi_n^4}\right)$$

Here Ψ_n are the division polynomials. Let $[n](X, Y) = (X_n, Y_n)$. Once again we can use our bi-rational correspondence to determine the coordinates of $[n](x, y) = (x_n, y_n)$ in our Holm curve. We know that E_λ is bi-rationally equivalent to H_λ. As we substituted our values for a, b, X and Y in the division polynomials for the Weierstrass equation, we have that $\Psi_i(X, Y) = \psi_i(x, y)$ for $i = 0, 1, 2, 3, 4$. Also as they have the same recursion formulas for $i \geq 5$, we have that $\Psi_n(X, Y) = \psi(x, y)$. Thus,

$$X_n = X - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \qquad Y_n = \frac{\Psi_{2n}}{2\Psi_n^4}$$

is equivalent to

$$X_n = X - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \qquad Y_n = \frac{\psi_{2n}}{2\psi_n^4}$$

We apply this to our substitution equations from H_λ to E_λ;

$$x = \frac{X - \lambda^2}{Y} \qquad y = \frac{\lambda(X-1)}{Y}$$

and from E_λ to H_λ;

$$X = \frac{\lambda(x - \lambda y)}{\lambda x - y} \qquad Y = \frac{\lambda(1-\lambda^2)}{\lambda x - y}$$

to obtain:

$$\begin{aligned}
x_n &= \frac{X_n - \lambda^2}{Y_n} = \frac{2\psi_n^4}{\psi_{2n}}\left[\frac{\lambda(x-\lambda y)}{\lambda x - y} - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2} - \lambda^2\right] \\
&= \frac{2\psi_n^4}{\psi_{2n}}\left[\frac{\lambda x - \lambda^3 x}{\lambda x - y} - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}\right] \\
&= \frac{2\psi_n^2}{\psi_{2n}}\left[\frac{(\lambda - \lambda^3)x\psi_n^2}{\lambda x - y} - \psi_{n-1}\psi_{n+1}\right] \\
&= x\left(\frac{2\lambda(1-\lambda^2)\psi_n^4}{(\lambda x - y)\psi_{2n}}\right) - \frac{2\psi_{n-1}\psi_n^2\psi_{n+1}}{\psi_{2n}} \\
&= x\alpha - \omega
\end{aligned}$$

$$\begin{aligned}
y_n &= \frac{\lambda(X_n - 1)}{Y_n} = \frac{2\psi_n^4}{\psi_{2n}}\left[\frac{\lambda^2(x-\lambda y)}{\lambda x - y} - \frac{\lambda\psi_{n-1}\psi_{n+1}}{\psi_n^2} - \lambda\right] \\
&= \frac{2\psi_n^4}{\psi_{2n}}\left[\frac{-\lambda^3 y + \lambda y}{\lambda x - y} - \frac{\lambda\psi_{n-1}\psi_{n+1}}{\psi_n^2}\right] \\
&= \frac{2\psi_n^4}{\psi_{2n}}\left[\frac{(\lambda - \lambda^3)y}{\lambda x - y} - \frac{\lambda\psi_{n-1}\psi_{n+1}}{\psi_n^2}\right] \\
&= y\left(\frac{2\lambda(1-\lambda^2)\psi_n^4}{(\lambda x - y)\psi_{2n}}\right) - \lambda\left(\frac{2\psi_{n-1}\psi_n^2\psi_{n+1}}{\psi_{2n}}\right) \\
&= y\alpha - \lambda\omega
\end{aligned}$$

Finally showing,

$$[n](x,y) = (x\alpha - \omega, y\alpha - \lambda\omega).$$

□

Corollary 1. *Let $P = (x, y)$ be in $H_\lambda(\mathbb{F}_p)\backslash\{(0,0)\}$ and let $n \geq 3$. P is an n-torsion point of H_λ if and only if $\psi_n(P) = 0$.*

Proof. We use:

$$\begin{aligned}
\psi_{2n}(x,y) &= \frac{\psi_n}{\psi_2}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right) \text{ for n} \geq 3 \\
x_n &= \frac{2\psi_n^2}{\psi_{2n}}\left[\frac{(\lambda-\lambda^3)x\psi_n^2}{\lambda x - y} - \psi_{n-1}\psi_{n+1}\right] \\
y_n &= \frac{2\psi_n^2}{\psi_{2n}}\left[\frac{(\lambda-\lambda^3)y\psi_n^2}{\lambda x - y} - \lambda\psi_{n-1}\psi_{n+1}\right]
\end{aligned}$$

Suppose $\psi_n(P) = 0$. Plugging in ψ_{2n} into x_n and y_n, we obtain:

$$\begin{aligned}
x_n &= \frac{2\psi_2\psi_n}{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}\left[\frac{(\lambda-\lambda^3)x\psi_n^2}{\lambda x - y} - \psi_{n-1}\psi_{n+1}\right] \\
y_n &= \frac{2\psi_2\psi_n}{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}\left[\frac{(\lambda-\lambda^3)y\psi_n^2}{\lambda x - y} - \lambda\psi_{n-1}\psi_{n+1}\right]
\end{aligned}$$

Thus as $\psi_n = 0$ we have that $n[x,y] = (x_n, y_n) = (0,0)$.

Now let $[n](x,y) = (x_n, y_n) = (0,0)$. Investigating ψ_2 we know that $\lambda x - y \neq 0$ as $(x,y) \neq (0,0)$. Also as $\lambda \neq 0, \pm 1$; ψ_2 is non-zero.

Suppose $\psi_n \neq 0$. We have that:

$$\begin{aligned}
0 &= \frac{(\lambda-\lambda^3)x\psi_n^2}{\lambda x - y} - \psi_{n-1}\psi_{n+1} \\
0 &= \frac{(\lambda-\lambda^3)y\psi_n^2}{\lambda x - y} - \lambda\psi_{n-1}\psi_{n+1}
\end{aligned}$$

Solving for $\psi_{n-1}\psi_{n+1}$ in the second equation we obtain:

$$\psi_{n-1}\psi_{n+1} = \frac{(\lambda-\lambda^3)y\psi_n^2}{\lambda(\lambda x - y)}$$

Plugging this into the first equation we obtain:

$$\begin{aligned} 0 &= \frac{(\lambda-\lambda^3)x\psi_n^2}{\lambda x - y} - \frac{(\lambda-\lambda^3)y\psi_n^2}{\lambda(\lambda x - y)} \\ &= \psi_n^2\left(\frac{(\lambda-\lambda^3)x}{\lambda x - y} - \frac{(\lambda-\lambda^3)y}{\lambda(\lambda x - y)}\right) \\ &= \psi_n^2\left(\frac{\lambda-\lambda^3}{\lambda x - y}\right)\left(x - \frac{y}{\lambda}\right) \end{aligned}$$

Now

$$\psi_n^2 \neq 0, \frac{\lambda-\lambda^3}{\lambda x - y} \neq 0 \implies \left(x - \frac{y}{\lambda}\right) = 0$$

If $\left(x - \frac{y}{\lambda}\right) = 0$ we have $x = \frac{y}{\lambda}$. Plugging this into $H_\lambda : 0 = y^3 - y - \lambda x^3 + \lambda x$ we obtain $(1 - \frac{1}{\lambda^2})y^3 = 0$ and $y = 0$. We obtain that $(x, y) = (0, 0)$, a contradiction.

We must have that $\psi_n = 0$. Thus $[n](x, y) = (0, 0)$ if and only if $\psi_n = 0$. □

Using these multi-variable division polynomials we can once again find the torsion points.

Corollary 2. *Let $P = (x, y)$ be in $H_\lambda(\mathbb{F}_p)\backslash\{(0, 0)\}$ and let $n \geq 3$. P is an n-torsion point of H_λ if and only if $\tilde{\psi}_n(P) = 0$.*

Proof. This result follows from Corollary 1 and Theorem 3. □

References

[1] J. Cheon, S. Hahn, Division Polynomials of Elliptic Curves Over Finite Fields, Proc. Japan Acad., (1996).

[2] I. Connell, *Elliptic Curve Handbook*, Universidad Complutense Madrid, 2009, 542 pp.

[3] H. M. Edwards, A Normal Form For Elliptic Curves, American Mathematical Society, 2007.

[4] B. Foster, Rational points and isogenies of the Holm curves over a finite field, Dissertation, Howard University, (2013), 69 pp.

[5] A. Holm, Some points in Diophantine analysis, *Proc. Edinburgh Math. Soc.*, **22**, (1903), 40–48.

[6] G. McGuire, R. Moloney, Two Kinds of Division Polynomials For Twisted Edwards Curves, Springer-Verlag, 2011.

[7] F. Ramaroson, A. Rajan, Ratios of congruent numbers, *Acta Arithmetica*, **128,** no. 2, (2007).

[8] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009, 513 pp.

[9] M. Ulas, On torsion Points on an Elliptic Curves via Division Polynomials, *Universiatis Iagellonicae Actica Mathematica*, 2005.

[10] L. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., Chapman & Hall/CRC, 2008, 536 pp.