Divison Polynomials for Alternate Models of Elliptic Curves

Dustin Moody *

December 10, 2010

Abstract

In this paper we find division polynomials for Huff curves, Jacobi quartics, and Jacobi intersections. These curves are alternate models for elliptic curves to the more common Weierstrass curve. Division polynomials for Weierstrass curves are well known, and the division polynomials we find are analogues for these alternate models. Using the division polynomials, we show recursive formulas for the n-th multiple of a point on each curve. As an application, we prove a type of mean-value theorem for Huff curves, Jacobi quartics and Jacobi intersections.

1 Introduction

Elliptic curves have been an object of study in mathematics for well over a century. Recently elliptic curves have proven useful in applications such as factoring [18], cryptography [17],[20], and in the proof of Fermat's last theorem [5], [25]. The traditional way of writing the equation of an elliptic curve is to use its Weierstrass form:

$$y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

In the past several years, other models of elliptic curves have been studied. Such models include Edwards curves [2], [7], Jacobi intersections and Jacobi quartics [3], [4],[13], Hessian curves [12], and Huff curves [9], [16], among others. These models sometimes allow for more efficient computation on elliptic curves or provide other features of interest to cryptographers, such as resistance to side-channel attacks.

In this paper we find division polynomials for Huff curves, Jacobi quartics, and Jacobi intersections. Division polynomials for Weierstrass curves are well known, and play a key role in the theory of elliptic curves. They can be used to find a formula for the n-th multiple of (x, y) in terms of x and y, as well as determing when a point is an n-torsion point on a Weierstrass curve. Division

*Computer Security Division, NIST, email: dbmoody25@gmail.com

polynomials are also a crucial ingredient in Schoof's algorithm to count points on an elliptic curve over a finite field [22]. In addition, they have been used to efficiently compute multiples of points, see for example [6], [10].

Hitt, McGuire, and Moloney recently have found formulas for division polynomials of twisted Edwards curves [14], [19]. The division polynomials we find are the analogues for Huff curves, Jacobi quartics, and Jacobi intersections. We illustrate a a recursive formula for the n-th multiple of a point using these division polynomials. We are also able to prove some properties of these division polynomials. As an application, we show how they can be used to find the mean value of a certain collection of points.

This paper is organized as follows. In section 2 we review Huff curves, Jacobi quartics, and Jacobi intersections. In section 3 we examine division polynomials for each of these models. As an application, in section 4 we look at a mean value theorem for the three curves. We conclude in section 5 with some remarks and open questions.

2 Alternate models of elliptic curves

2.1 Huff curves

Joye, Tibouchi, and Vergnaud re-introduced the Huff model ([15]) for elliptic curves in [16]. They showed that common elliptic curve computations, including point multiplications and pairings, can be efficiently performed on Huff curves. In addition, they allow for complete addition formulas, which Weierstrass curves do not. Complete addition formulas are formulas which are valid for all inputs. Throughout the remainder of this paper, let K be a field whose characteristic is not 2. The equation given in [16] for a Huff curve is $ax(y^2-1) = by(x^2-1)$. Wu and Feng in [9] generalized this form to curves given by the equation

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

which includes the previous model as a special case. The curve $H_{a,b}$ is an elliptic curve provided $ab(a-b) \neq 0$. Given a point $P = (x, y)$ on the curve $H_{a,b}$, its inverse is the point $-P = (-x, -y)$. The additive identity is the point $(0, 0)$. There are three points at infinity, given by $(1, 0, 0)$, $(0, 1, 0)$, and $(a, b, 0)$ in projective coordinates. These points at infinity are the three non-trivial points of order 2. Addition for points which are not these points of order 2 is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{(x_1+x_2)(1+ay_1y_2)}{(1+bx_1x_2)(1-ay_1y_2)}, \frac{(y_1+y_2)(1+bx_1x_2)}{(1-bx_1x_2)(1+ay_1y_2)} \right).$$

For adding a non-trivial point (x, y) to a point of order 2 we have, $(x, y) + (1, 0, 0) = (1/bx, -y)$, $(x, y) + (0, 1, 0) = (-x, 1/ay)$, and $(x, y) + (a, b, 0) = (-1/bx, -1/ay)$.

There is also a simple birational transformation from a curve in Huff form to the Weierstrass curve

$$s^2 = r^3 + (a+b)r^2 + abr.$$

The transformation is given by

$$(r, s) = \left(\frac{bx - ay}{y - x}, \frac{b - a}{y - x} \right),$$

for points with $x \neq y$. The only point on $H_{a,b}$ with $x = y$ is $(0, 0)$ which is mapped to ∞. The inverse transformation is given by

$$(x, y) = \left(\frac{r + a}{s}, \frac{r + b}{s} \right),$$

for points (r, s) with $s \neq 0$. The points with $s = 0$ are the points of order 2 which get sent to the points at infinity on $H_{a,b}$.

2.2 Jacobi quartics

There is another model of elliptic curves known as Jacobi quartics. For a background on these curves, see [3], [4], [13]. We recall only the basic facts. Any elliptic curve with a point of order 2 can be put into Jacobi quartic form, with equation

$$J_{d,e} : y^2 = ex^4 - 2dx^2 + 1,$$

where we require $e(d^2 - e) \neq 0$. The identity element is $(0, 1)$, and the point $(0, -1)$ has order 2. The inverse of the point (x, y) is $(-x, y)$. The addition formula on $J_{d,e}$ is given by

$$\begin{aligned}&(x_1, y_1) + (x_2, y_2)\\ &\qquad = \left(\frac{x_1 y_2 + y_1 x_2}{1 - e(x_1 x_2)^2}, \frac{(1 + e(x_1 x_2)^2)(y_1 y_2 - 2d x_1 x_2) + 2e x_1 x_2 ({x_1}^2 + {x_2}^2)}{(1 - e(x_1 x_2)^2)^2} \right).\end{aligned}$$

This addition formula can be efficiently implemented, which is one of the primary advantages of writing an elliptic curve in this form [11]. Another is that this addition formula protects against side-channel attacks [3], [13]. There is a birational transformation from a Jacobi quartic curve to a curve in Weierstrass form with point of order 2. For points with $x \neq 0$, the map

$$(r, s) = \left(2\frac{3(y + 1) - dx^2}{3x^2}, 4\frac{(y + 1) - dx^2}{x^3} \right),$$

sends the curve $J_{d,e}$ to the Weierstrass curve

$$s^2 = r^3 - 4\frac{3e + d^2}{3} r - \frac{16}{27} d(d^2 - 9e).$$

The point $(0, 1)$ corresponds to ∞, and the point of order 2 $(0, -1)$ goes to the point $(4d/3, 0)$. The inverse from the Weierstrass curve $s^2 = r^3 + ar + b$, with point of order 2 $(p, 0)$ is given by

$$(x, y) = \left(\frac{2(r - p)}{s}, \frac{(2r + p)(r - p)^2 - s^2}{s^2} \right),$$

with the image being the Jacobi quartic $J_{d,e}$ with $d = 3p/4$, and $e = -(3p^2 + 4a)/16$. The points $\infty, (p, 0)$ are exceptional, and get sent to $(0, 1)$ and $(0, -1)$ respectively.

2.3 Jacobi intersections

Representing elliptic curves as the intersection of two quadratic surfaces was first introduced in [4]. This model is known as Jacobi intersections. In [4], Chudnovsky and Chudnovsky showed that common elliptic curve computations can be efficiently performed on Jacobi intersections. Since then, more efficient ways to implement these computations have been found. See for instance [3], [11], and [13]. The equation for a curve given as a Jacobi intersection is

$$J_b : \begin{aligned} u^2 + v^2 &= 1 \\ bu^2 + w^2 &= 1. \end{aligned}$$

The curve J_b is an elliptic curve provided $b(1-b) \neq 0$. Given a point $P = (u, v, w)$ on the curve J_b, its inverse is the point $-P = (-u, v, w)$. The additive identity is the point $(0, 1, 1)$. On any Jacobi intersection curve, there are always three points of order 2, given by $(0, 1, -1), (0, -1, 1)$, and $(0, -1, -1)$. The addition law is given by

$$(u_1, v_1, w_1) + (u_2, v_2, w_2) = \left(\frac{u_1 v_2 w_2 + u_2 v_1 w_1}{v_2^2 + u_2^2 w_1^2}, \frac{v_1 v_2 - u_1 u_2 w_1 w_2}{v_2^2 + u_2^2 w_1^2}, \frac{w_1 w_2 - b u_1 u_2 v_1 v_2}{v_2^2 + u_2^2 w_1^2} \right).$$

There is also a simple birational transformation from a Jacobi intersection curve to the Weierstrass curve

$$y^2 = x(x+1)(x+1-b).$$

The transformation is given by

$$(u, v, w) = \left(\frac{-2y}{x^2 + 2x + 1 - b}, \frac{x^2 + b - 1}{x^2 + 2x + 1 - b}, \frac{x^2 + 2(1-b)x + 1 - b}{x^2 + 2x + 1 - b} \right),$$

with ∞ going to $(0, 1, 1)$. The inverse transformation is given by

$$(x, y) = \left(\frac{(1-b)(w-1)}{bv - w + 1 - b}, \frac{b(1-b)u}{bv - w + 1 - b} \right),$$

for points $(u, v, w) \neq (0, 1, 1)$. The point $(0, 1, 1)$ is mapped to ∞.

3 Division polynomials

3.1 Division polynomials for Weierstrass curves

We begin by recalling the standard division polynomials for Weierstrass curves. We write $[n](x, y)$ to denote the n-th multiple of a point (x, y).

Theorem 1 *Let E be given by $y^2 = x^3+ax+b$, over a field whose characteristic is not 2. Then for any point (x, y)*

$$[n](x,y) = \left(\frac{\phi_n(x,y)}{\psi_n^2(x,y)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right).$$

The functions ϕ_n, ω_n, and ψ_n in $\mathbb{Z}[x, y]$ are defined recursively by

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2 \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \text{ for } n \geq 2 \\
\psi_{2n} &= \frac{\psi_n}{2y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right) \text{ for } n \geq 3,
\end{aligned}$$

and

$$\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1} \\
\omega_n &= \frac{1}{4y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right).
\end{aligned}$$

Proof These formulas are well-known. For example, see [23] or [24] for details. □

The polynomial ψ_n is called the *n-th division polynomial* of E. It is easy to see that a point $P = (x, y)$ satisfies $[n]P = \infty$ if and only if $\psi_n(x) = 0$. Divison polynomials are an important tool for computing multiples of points. They also play a key role in Schoof's algorithm for counting the number of points on an elliptic curve over a finite field [22]. In addition, they have been used to efficiently compute multiples of points, see for example [6], [10].

3.2 Division polynomials for Huff curves

We now look at division polynomials for Huff curves. Again we write the coordinates of $[n](x, y)$ as (x_n, y_n). In particular, let (x_2, y_2) be the coordinates of $[2](x, y)$. As the defining equation for the Huff curve $H_{a,b}$ is symmetric with regards to x and y when a and b are interchanged, we only look at the x-coordinates. By symmetry, all our results are valid for the y-coordinates if we replace y for x, and a for b.

Theorem 2 *Let $F_1(x) = 1, F_2(x) = 1, G_1(x) = 1$, and $G_2(x) = 1$. Define polynomials $h_1(x) = 4b^2x^4 - 8bx^2 + 16ax^2 + 4$, and $h_2(x) = b^2x^4 - 1$. Then we* *have*

$$x_{2n} = x_2 \frac{F_{2n}(x)}{G_{2n}(x)}$$
$$x_{2n+1} = x \frac{F_{2n+1}(x)}{G_{2n+1}(x)},$$

where the F_i and G_i are polynomials defined recursively for $n > 1$ by

$$\begin{aligned} F_{2n+1} &= G_{2n-1}\left(h_1 F_{2n}^2 - h_2^2 G_{2n}^2\right), \\ G_{2n+1} &= F_{2n-1}\left(h_2^2 G_{2n}^2 - b^2 x^4 h_1 F_{2n}^2\right), \\ F_{2n+2} &= h_2^2 G_{2n}\left(F_{2n+1}^2 - G_{2n+1}^2\right), \\ G_{2n+2} &= h_1 F_{2n}\left(G_{2n+1}^2 - b^2 x^4 F_{2n+1}^2\right). \end{aligned}$$

Proof The following proof comes from a similar approach in [19] to calculate division polynomials for Edwards curves. They in turn were motivated by the polynomials Abel studied in proving his theorem on the n-division points of the lemniscate [1]. Let $(r_+, s_+) = (r_1, s_1) + (r_2, s_2)$ and $(r_-, s_-) = (r_1, s_1) - (r_2, s_2)$. Then using the addition law for Huff curves, we have

$$r_+ r_- = \frac{r_1^2 - r_2^2}{1 - b^2 r_1^2 r_2^2}.$$

Setting $r_1 = x_n$ and $r_2 = x$, we see that

$$x_{n+1} = \frac{1}{x_{n-1}} \frac{x_n^2 - x^2}{1 - b^2 x^2 x_n^2}.$$

Now note that

$$[2](x, y) = (x_2, y_2) = \left(\frac{2x(1 + ay^2)}{(1 + bx^2)(1 - ay^2)}, \frac{2y(1 + bx^2)}{(1 - bx^2)(1 + ay^2)} \right).$$

Replacing y^2 by $\left(y(bx^2 - 1) + x\right)/(ax)$ and simplifying the expression, we find that

$$x_2^2 = x^2 \frac{4b^2x^4 - 8bx^2 + 16ax^2 + 4}{(b^2x^4 - 1)^2} = x^2 \frac{h_1(x)}{h_2(x)^2}. \tag{3.1}$$

We will now use induction to prove the recursion formulas given above. For x_1 and x_2 the theorem is trivially true. We assume the result holds for all n, and show it is true for $n + 1$. There are two cases depending on whether n is even or odd. For odd $n = 2k + 1$ we calculate

$$
\begin{aligned}
x_{n+1} = x_{2k+2} &= \frac{1}{x_{2k}} \frac{x_{2k+1}^2 - x^2}{1 - b^2 x^2 x_{2k+1}^2}, \\
&= \frac{G_{2k}}{x_2 F_{2k}} \frac{x^2 \frac{F_{2k+1}^2}{G_{2k+1}^2} - x^2}{1 - b^2 x^4 \frac{F_{2k+1}^2}{G_{2k+1}^2}}, \\
&= x_2 \frac{x^2 G_{2k}}{x_2^2 F_{2k}} \frac{F_{2k+1}^2 - G_{2k+1}^2}{G_{2k+1}^2 - b^2 x^4 F_{2k+1}^2}, \\
&= x_2 \frac{h_2^2 G_{2k}}{h_1 F_{2k}} \frac{F_{2k+1}^2 - G_{2k+1}^2}{G_{2k+1}^2 - b^2 x^4 F_{2k+1}^2}, \\
&= x_2 \frac{F_{n+1}}{G_{n+1}}.
\end{aligned}
$$

Similarly, when $n = 2k$ is even,

$$
\begin{aligned}
x_{n+1} = x_{2k+1} &= \frac{1}{x_{2k-1}} \frac{x_{2k}^2 - x^2}{1 - b^2 x^2 x_{2k}^2}, \\
&= \frac{G_{2k-1}}{x F_{2k-1}} \frac{x_2^2 \frac{F_{2k}^2}{G_{2k}^2} - x^2}{1 - b^2 x^2 x_2^2 \frac{F_{2k}^2}{G_{2k}^2}}, \\
&= x \frac{G_{2k-1}}{F_{2k-1}} \frac{h_1 F_{2k}^2 - h_2^2 G_{2k}^2}{h_2^2 G_{2k}^2 - b^2 x^4 h_1 F_{2k}^2}, \\
&= x \frac{F_{n+1}}{G_{n+1}}.
\end{aligned}
$$

This proves the theorem. □

The recursive formulas given above lead to the polynomials F_n and G_n having high degree in x. Furthermore, the rational function $\frac{F_n}{G_n}$ can be simplified by removing common factors. The following theorem is important as it eliminates these common factors, thus reducing the degrees of the division polynomials. For example, the degree in x of F_9 is 2304, while the degree of the reduced polynomial f_9 is 80. In fact, the degrees of the F_n and G_n grow exponentially while it will be shown that the degrees of the f_n and g_n only grow quadratically.

Theorem 3 *Define $f_1 = 1, f_2 = 1, g_1 = 1,$ and $g_2 = 1$. For $n > 1$, let*

$$
f_{2n+1} = \begin{cases} \dfrac{h_1 f_{2n}^2 - h_2^2 g_{2n}^2}{h_2^2 f_{2n-1}}, & \text{if } 2n+1 \equiv 1 \text{ mod } 4 \\[2ex] \dfrac{h_1 f_{2n}^2 - h_2^2 g_{2n}^2}{f_{2n-1}}, & \text{if } 2n+1 \equiv 3 \text{ mod } 4 \end{cases}
$$

$$g_{2n+1} = \begin{cases} \dfrac{h_2^2 g_{2n}^2 - b^2 x^4 h_1 f_{2n}^2}{h_2^2 g_{2n-1}}, & \text{if } 2n+1 \equiv 1 \ mod\ 4 \\ \\ \dfrac{h_2^2 g_{2n}^2 - b^2 x^4 h_1 f_{2n}^2}{g_{2n-1}}, & \text{if } 2n+1 \equiv 3 \ mod\ 4 \end{cases}$$

and

$$f_{2n+2} = \frac{h_2(f_{2n+1}^2 - g_{2n+1}^2)}{h_1 f_{2n}},$$
$$g_{2n+2} = \frac{(g_{2n+1}^2 - b^2 x^4 f_{2n+1}^2)}{h_2 g_{2n}}.$$

The functions $f_n(x)$ and $g_n(x)$ are polynomials in x satisfying $x_{2n} = x_2 \frac{f_{2n}(x)}{g_{2n}(x)}$, and $x_{2n+1} = x \frac{f_{2n+1}(x)}{g_{2n+1}(x)}$.

Proof Note the similarities in the definitions of F_n and f_n and also between G_n and g_n. Since the f_n and g_n are just the F_n and G_n with their common factors cancelled then $F_n/G_n = f_n/g_n$, and we immediately have that $x_{2n} = x_2 \frac{f_{2n}(x)}{g_{2n}(x)}$, and $x_{2n+1} = x \frac{f_{2n+1}(x)}{g_{2n+1}(x)}$. All we need to show is that the f_n, and g_n are polynomials in x. We do this on a case by case basis.

We begin by showing $f_{2n-1} | (h_1 f_{2n}^2 - h_2^2 g_{2n}^2)$. Let $\gamma \in \overline{K}, \gamma \neq 0$ be a root of f_{2n-1}. Then for some $\delta \in \overline{K}$, we have (γ, δ) is a point of order $2n-1$ on $H_{a,b}$. It follows that $[2n](\gamma, \delta) = (\gamma, \delta)$, so $x_{2n}(\gamma) = \gamma$. Squaring this equation, we find that by Theorem 2 and (3.1)

$$\begin{aligned} \gamma^2 &= x_{2n}^2(\gamma), \\ &= x_2^2(\gamma) \frac{f_{2n}^2(\gamma)}{g_{2n}^2(\gamma)}, \\ &= \gamma^2 \frac{h_1(\gamma) f_{2n}^2(\gamma)}{h_2^2(\gamma) g_{2n}^2(\gamma)} \end{aligned}$$

so $h_1(\gamma) f_{2n}^2(\gamma) - h_2^2(\gamma) g_{2n}^2(\gamma) = 0$. As γ was an arbitrary root, then we've shown that f_{2n-1} divides $h_1 f_{2n}^2 - h_2^2 g_{2n}^2$.

We similarly see that f_{2n-2} divides $f_{2n-1}^2 - g_{2n-1}^2$. Let γ be a root of f_{2n-2}. Then it follows that $x_{2n-1}(\gamma) = \gamma$ and squaring this yields

$$\gamma^2 = \gamma^2 \frac{f_{2n-1}^2(\gamma)}{g_{2n-1}^2(\gamma)}.$$

So γ is a root of $f_{2n-1}^2 - g_{2n-1}^2$, which proves f_{2n-2} divides $f_{2n-1}^2 - g_{2n-1}^2$.

Next we check that g_{2n-1} is a factor of $h_2^2 g_{2n}^2 - b^2 x^4 h_1 f_{2n}^2$. If γ is a root of g_{2n-1}, then for some δ, the point $P = (\gamma, \delta)$ is on $H_{a,b}$, and $[2n-1]P$ is a point at infinity of order 2. As $[2n]P = [2n-1]P + P$, by the addition law for adding points at infinity we know that $x_{2n}(\gamma)$ must equal $-\gamma$ or $\pm 1/b\gamma$. We claim that it is not $-\gamma$. If $x_{2n}(\gamma) = -\gamma$ then the point $[2n-1]P = (0, 1, 0)$, and $[2n-2]P = -P + (0, 1, 0)$. We have that $[4n-1]P = -P$, so

$[2n+1]P = [4n-1]P - [2n-2]P = -P + P - (0,1,0) = (0,1,0)$. But $[2n+1]P = (0,1,0) = [2n-1]P$ implies that P is a point of order 2, which is contrary to P being an affine point. So $x_{2n}^2(\gamma) = 1/b^2\gamma^2$ or

$$\frac{1}{b^2\gamma^2} = \gamma^2 \frac{h_1(\gamma) f_{2n}^2(\gamma)}{h_2^2(\gamma) g_{2n}^2(\gamma)}.$$

We see γ is a root of $h_2^2 g_{2n}^2 - b^2 x^4 h_1 f_{2n}^2$. As γ was an arbitrary root then g_{2n-1} divides $h_2^2 g_{2n}^2 - b^2 x^4 h_1 f_{2n}^2$. By an analogous argument (which we omit for brevity) it can be shown that g_{2n-2} givides $g_{2n-1}^2 - b^2 x^4 f_{2n-1}^2$.

We now verify that h_1 and h_2 divide the numerators of f_{2n} and g_{2n} respectively. For this we use induction. The base case is $n = 2$, and we calculate

$$f_3^2 - g_3^2 = -8h_1h_2\left(b^4x^8 + 8\,ab^2x^6 - 4\,b^3x^6 + 6\,b^2x^4 + 8\,ax^2 - 4\,bx^2 + 1\right)$$

and

$$\begin{aligned} g_3^2 - b^2x^4f_3^2 = h_2(&b^4x^8 + 4\,b^3x^6 + 16\,abx^4 - 10\,b^2x^4 + 4\,bx^2 + 1) \\ &(-b^4x^8 + 4\,b^3x^6 + 16\,abx^4 - 6\,b^2x^4 + 4\,bx^2 - 1). \end{aligned}$$

Assume now that h_1 divides $f_{2n-1}^2 - g_{2n-1}^2$ and h_2 divides $g_{2n-1}^2 - b^2x^4f_{2n-1}^2$. The numerator of $f_{2n+1}^2 - g_{2n+1}^2$ is

$$\begin{aligned} &= g_{2n-1}^2(h_1 f_{2n}^2 - h_2^2 g_{2n}^2)^2 - f_{2n-1}^2(h_2^2 g_{2n}^2 - b^2x^4h_1f_{2n}^2)^2 \\ &= h_1 j(x) - h_2^4 g_{2n}^4 (f_{2n-1}^2 - g_{2n-1}^2), \end{aligned} \tag{3.2}$$

where $j = g_{2n-3}^2(h_1 f_{2n-2}^4 - 2h_2^2 f_{2n-2}^2 g_{2n-2}^2) - f_{2n-3}^2(-2b^2x^4h_2^2 f_{2n-2}^2 g_{2n-2}^2 + b^4x^8h_1f_{2n-2}^4)$. By the induction hypothesis, we see the expression for $f_{2n+1}^2 - g_{2n+1}^2$ in (3.2) is divisble by h_1. Similarly, the numerator of $g_{2n+1}^2 - b^2x^4f_{2n+1}^2$ is

$$\begin{aligned} &= f_{2n-1}^2(h_2^2 g_{2n}^2 - b^2x^4h_1f_{2n}^2)^2 - b^2x^4g_{2n-1}^2(h_1f_{2n}^2 - h_2^2g_{2n}^2)^2 \\ &= h_2 k(x) - b^2x^4h_1^2f_{2n}^4(g_{2n-1}^2 - b^2x^4f_{2n-1}^2) \end{aligned},$$

for a certain polynomial $k(x)$ (which we do not display). By the induction hypothesis, this is divisible by h_2.

Lastly, we need to show that $h_2^2 | f_{4n}^2$, but $h_2^2 \not| f_{4n-2}^2$. It is clearly true for $n = 1$ by a straightforward check: $f_2 = 1$ and $f_4 = -2h_2^2(b^4x^8 - 4b^3x^6 + 8b^2x^6a + 6b^2x^4 - 4bx^2 + 8ax^2 + 1)$. Now we use induction to prove it. We have

$$f_{4n}^2 = \frac{h_2^2(f_{4n-1}^2 - g_{4n-1}^2)^2}{h_1^2 f_{4n-2}^2}.$$

We see h_2^2 divides f_{4n}^2 as there is no cancellation in the denominator by the induction hypothesis. For our other case,

$$f_{4n+2}^2 = \frac{h_2^2(f_{4n+1}^2 - g_{4n+1}^2)^2}{h_1^2 f_{4n}^2}.$$

But by the induction hypothesis, we have that f_{4n}^2 has a factor of h_2^2 which cancels the h_2^2 in the numerator. This is as desired.

$\square$

We list the first few non-trivial division polynomials:

$$f_3 = -b^4x^8 + 6b^2x^4 + (16a - 8b)x^2 + 3, \tag{3.3}$$

$$g_3 = -3b^4x^8 - b^2(16a - 8b)x^6 - 6b^2x^4 + 1,$$

$$f_4 = -2(b^2x^4 - 1)^2(b^4x^8 + b^2(8a - 4b)x^6 + 6b^2x^4 + (8a - 4b)x^2 + 1,$$

$$g_4 = (b^4x^8+4b^3x^6+b(16a-b)x^4+4bx^2+1)(-b^4x^8+4b^2x^6+b(16a-6b)x^4+4bx^2-1).$$

We call the f_n and g_n *the Huff division polynomials*. An advantage of our division polynomials is that n-th one can be computed from the previous two rounds, i.e., f_n only depends on $f_{n-1}, g_{n-1}, f_{n-2}$, and g_{n-2}. The division polynomials for Weierstrass curves given in Theorem 1 require the previous $n/2$ rounds of computation. Just as with the Weierstrass division polynomials, we have an easy criterion for finding n-torsion points.

Corollary 1 *For $n > 2$, the point $(x, y) \neq (0, 0)$ on a Huff curve is an n-torsion point if and only if $f_n(x) = 0$.*

Proof This follows immediately from the previous theorem and the observation that the only point on a Huff curve with x-coordinate 0 is the identity point $(0, 0)$. $\square$

We are able to describe some properties of the f_i and g_i in the following propositions.

Proposition 1 *For $n \geq 1$ the functions f_n and g_n are even functions of x. When n is odd,*

$$\begin{aligned} f_n(x) &= (-1)^{(n-1)/2}b^{(n^2-1)/2}x^{n^2-1} + ... \\ g_n(x) &= (-1)^{(n-1)/2}nb^{(n^2-1)/2}x^{n^2-1} + ..., \end{aligned} \tag{3.4}$$

and for even n,,

$$\begin{aligned} f_n(x) &= (-1)^{(n+2)/2}\frac{n}{2}b^{e_n}x^{2e_n} + ... \\ g_n(x) &= (-1)^{(n+2)/2}b^{e_n}x^{2e_n} + ... \end{aligned} \tag{3.5}$$

where $e_n = n^2/2$ if $n \equiv 0$ mod 4 and $e_n = n^2/2 - 2$ if $n \equiv 2$ mod 4.

Proof As f_1, f_2, g_1, g_2, h_1, and h_2 are all even functions of x, then it follows from the recursive formulas that the f_n and g_n are even functions of x.

To prove (3.4) and (3.5) we use induction. Trivially f_1, f_2, g_1, and g_2 satisfy the claim and by (3.3) we see the proposition holds for f_3, f_4, g_3, and g_4.

Now

$$f_{2n} = \frac{h_2\left(f_{2n-1}^2 - g_{2n-1}^2\right)}{h_1 f_{2n-2}}$$

$$= \frac{(b^2x^4+..)\left((b^{4n^2-4n}x^{8n^2-8n}+...)-((2n-1)^2b^{4k^2-4k}x^{8k^2-8k}+...)\right)}{(4b^2x^4+...)((-1)^n(n-1)b^{e_{2n-2}}x^{2e_{2n-2}}+...)}$$

$$= (-1)^n\frac{(b^2x^4+...)(-4n(n-1)b^{4n^2-4n}x^{8n^2-8n}+...)}{(4b^2x^4+...)((n-1)b^{e_{2n-2}}x^{2e_{2n-2}}+...)}$$

$$= (-1)^{n+1}nb^{4n^2-4n-e_{2n-2}}x^{8n^2-8n-2e_{2n-2}}+...$$

We want this to equal $(-1)^{(2n+2)/2}nb^{e_{2n}}x^{2e_{2n}}$, so it remains to be seen that $e_{2n} = 4n^2 - 4n - e_{2n-2}$. By the definition of e_{2n}, we have $e_{2n-2} + e_{2n}$ equals either $2(n-1)^2 + 2n^2 - 2$ or $2(n-1)^2 - 2 + 2n^2$ depending on $2n$ mod 4. In either case, they both are $4n^2 - 4n$. Thus the claim has been proved for f_{2n}. The proof for g_{2n} is analogous, and we omit the details.

To verify the claim for the odd case, we again analyze the leading coefficients. We first assume that $2n+1 \equiv 3$ mod 4. Thus

$$f_{2n+1} = \frac{(b^2x^4+...)(n^2b^{2e_{2n}}x^{4e_{2n}}+...)-(b^4x^8+...)(b^{2e_{2n}}x^{4e_{2n}}+...)}{(-1)^{n-1}b^{2n^2-2n}x^{4n^2-4n}+...}$$

$$= (-1)^n b^{4+2e_{2n}-2n^2+2n}x^{8+4e_{2n}-4n^2+4n}+...$$

The claim is true if $4 + 2e_{2n} - 2n^2 + 2n = \left((2n+1)^2 - 1\right)/2 = 2n^2 + 2n$. As $2n+1 \equiv 3$ mod 4, then $2n \equiv 2$ mod 4, so $e_{2n} = 2n^2 - 2$. Substituting this in, we see everything is as desired. If instead we have $2n+1 \equiv 1$ mod 4, then we need to divide f_{2n+1} by $h_2^2 = (b^4x^8 + ...)$. So for this case

$$f_{2n+1} = (-1)^n b^{2e_{2n}-2n^2+2n}x^{4e_{2n}-4n^2+4n}+... \tag{3.6}$$

As $e_{2n} = 2n^2$ in this case then (3.6) is equal to $(-1)^n b^{2n^2+2n}x^{4n^2+4n}$ as claimed. This finishes the proof of the leading term for f_n, n odd. As before, the case g_{2n+1} is similar to the calculation for f_{2n+1}, so we leave it to the reader. □

The following proposition gives some functional equations for the Huff division polynomials.

Proposition 2 *For n odd*

$$g_n(x) = (-1)^{(n-1)/2}b^{(n^2-1)/2}x^{n^2-1}f_n\left(\frac{1}{bx}\right), \tag{3.7}$$

and for n even

$$f_n(x)^2 = b^{2e_n}x^{4e_n}f_n\left(\frac{1}{bx}\right)^2,$$

$$g_n(x)^2 = b^{2e_n} x^{4e_n} g_n\left(\frac{1}{bx}\right)^2.$$

Proof Looking at the first few f_n and g_n listed in (3.3), we see the result holds for $n = 1, 2, 3,$ and 4. We again use induction. The first case is when $n = 2k$. Then

$$f_{2k}^2\left(\frac{1}{bx}\right) = \frac{h_2^2(\frac{1}{bx})\left(f_{2k-1}^2(\frac{1}{bx}) - g_{2k-1}^2(\frac{1}{bx})\right)^2}{h_1^2(\frac{1}{bx})f_{2k-2}^2(\frac{1}{bx})}.$$

We know that $h_1\left(\frac{1}{bx}\right) = h_1(x)/b^2x^4$ and $h_2\left(\frac{1}{bx}\right) = -h_2(x)/b^2x^4$. By the induction hypothesis

$$f_{2k-1}^2\left(\frac{1}{bx}\right) = \frac{1}{b^{4k^2-4k}x^{8k^2-8k}} g_{2k-1}^2(x),$$

and

$$g_{2k-1}^2\left(\frac{1}{bx}\right) = \frac{1}{b^{4k^2-4k}x^{8k^2-8k}} f_{2k-1}^2(x),$$

so

$$\begin{aligned} f_{2k}\left(\frac{1}{bx}\right) &= \frac{h_2^2(x)\left(g_{2k-1}^2(x) - f_{2k-1}^2(x)\right)^2}{h_1^2(x)b^{8k^2-8k-2e_{2k-2}}x^{16k^2-16k-4e_{2k-2}}f_{2k-2}^2(x)} \\ &= \frac{f_{2k}^2(x)}{b^{2e_{2k}}x^{4e_{2k}}}. \end{aligned}$$

For the last step we again used the fact that $e_{2k-2} + e_{2k} = 4k^2 - 4k$. The proof for $g_{2k}^2\left(\frac{1}{bx}\right)$ follows in the same way and we omit the details.

For $n = 2k+1$, $n \equiv 3 \bmod 4$, we have

$$\begin{aligned} f_{2k+1}\left(\frac{1}{bx}\right) &= \frac{h_1\left(\frac{1}{bx}\right)f_{2k}^2\left(\frac{1}{bx}\right) - h_2^2\left(\frac{1}{bx}\right)g_{2k}\left(\frac{1}{bx}\right)}{f_{2k-1}\left(\frac{1}{bx}\right)}, \\ &= (-1)^k\frac{h_2^2(x)g_{2k}^2(x) - b^2x^4h_1(x)f_{2k}^2(x)}{b^{4+2e_{2k}-2k^2+2k}x^{8+4e_{2k}-4k^2+4k}g_{2k-1}(x)} \\ &= (-1)^k\frac{g_{2k+1}(x)}{b^{2k^2+2k}x^{4k^2+4k}}, \end{aligned}$$

as $e_{2k} = 2k^2 - 2$ in this case. For the case when $n \equiv 1 \bmod 4$ then we need to put an h_2^2 in the denominator. Recall also that now $e_{2k} = 2k^2$ as $2k \equiv 0 \bmod 4$. Thus

$$\begin{aligned} f_{2k+1}\left(\frac{1}{bx}\right) &= \frac{h_1\left(\frac{1}{bx}\right)f_{2k}^2\left(\frac{1}{bx}\right) - h_2^2\left(\frac{1}{bx}\right)g_{2k}\left(\frac{1}{bx}\right)}{h_2^2\left(\frac{1}{bx}\right)f_{2k-1}\left(\frac{1}{bx}\right)}, \\ &= (-1)^k\frac{h_2^2(x)g_{2k}^2(x) - b^2x^4h_1(x)f_{2k}^2(x)}{b^{2e_{2k}-2k^2+2k}x^{4e_{2k}-4k^2+4k}h_2^2(x)g_{2k-1}(x)} \\ &= (-1)^k\frac{g_{2k+1}(x)}{b^{2k^2+2k}x^{4k^2+4k}}. \end{aligned}$$

This establishes that (3.7) is true for odd n.

□

3.3 Division polynomials for Jacobi quartics

We do a similar calculation for Jacobi quartics. The division polynomials we find allow us to perform arithmetic on the Jacobi quartic with only the x-coordinate along with one multiplication by the y-coordinate. We only list the results and omit the proofs as the techniques are very similar to what was done for Huff curves in the last subsection.

Theorem 4 *Let $F_1 = 1, G_1 = 1, F_2 = -2$, and $G_2 = ex^4 - 1$. Let $P_1 = 1, Q_1 = 1, P_2 = e^2x^8 - 4dex^6 + 6ex^4 - 4dx^2 + 1$, and $Q_2 = (ex^4 - 1)^2$. For convenience, let $h(x) = ex^4 - 2dx^2 + 1$, so the curve equation is $y^2 = h(x)$. Write $[n](x, y) = (x_n, y_n)$. Then there are polynomials $F_n(x), G_n(x), P_n(x), Q_n(x)$ such that*

$$(x_{2n}, y_{2n}) = \left(xy \frac{F_{2n}(x)}{G_{2n}(x)}, \frac{P_{2n}(x)}{Q_{2n}(x)} \right),$$
$$(x_{2n+1}, y_{2n+1}) = \left(x \frac{F_{2n+1}(x)}{G_{2n+1}(x)}, y \frac{P_{2n+1}(x)}{Q_{2n+1}(x)} \right).$$

For $n > 1$ the F_n, G_n, P_n, and Q_n can be calculated recursively:

$$F_{2n+1} = 2hF_{2n}G_{2n-1}G_{2n} - F_{2n-1}(G_{2n}^2 - ex^4hF_{2n}^2),$$
$$G_{2n+1} = G_{2n-1}(G_{2n}^2 - ex^4hF_{2n}^2),$$

$$F_{2n+2} = 2F_{2n+1}G_{2n}G_{2n+1} - F_{2n}(G_{2n+1}^2 - ex^4F_{2n+1}^2),$$
$$G_{2n+2} = G_{2n}(G_{2n+1}^2 - ex^4F_{2n+1}^2),$$

and

$$P_{2n+1} = 2G_{2n}^2P_{2n}Q_{2n-1}(G_{2n}^2 + ex^4hF_{2n}^2) - P_{2n-1}Q_{2n}(G_{2n}^2 - ex^4hF_{2n}^2)^2,$$
$$Q_{2n+1} = Q_{2n-1}Q_{2n}(G_{2n}^2 - ex^4hF_{2n}^2)^2,$$

$$P_{2n+2} = 2hG_{2n+1}^2P_{2n+1}Q_{2n}(G_{2n+1}^2 + ex^4F_{2n+1}^2) - P_{2n}Q_{2n+1}(G_{2n+1}^2 - ex^4F_{2n+1}^2)^2,$$
$$Q_{2n+2} = Q_{2n}Q_{2n+1}(G_{2n+1}^2 - ex^4F_{2n+1}^2)^2.$$

As before, there are some common factors that can be cancelled in F_n/G_n and P_n/Q_n. The degrees of the F_n, G_n, P_n, and Q_n grow exponentially, and by removing these common factors our new division polynomials will have degrees that only grow quadratically. The next proposition shows what these are.

Theorem 5 *Let $f_1 = 1, g_1 = 1, f_2 = -2$, and $g_2 = ex^4 - 1$, as well as $p_1 = 1, p_2 = e^2x^8 - 4dex^6 + 6ex^4 - 4dx^2 + 1$. For $n > 2$, define*

$$f_{2n} = \frac{f_{2n-1}^2 - g_{2n-1}^2}{hf_{2n-2}},$$
$$f_{2n+1} = \frac{hf_{2n}^2 - g_{2n}^2}{f_{2n-1}},$$

$$g_{2n} = \frac{g_{2n-1}^2 - ex^4 f_{2n-1}^2}{g_{2n-2}},$$
$$g_{2n+1} = \frac{g_{2n}^2 - ex^4 h f_{2n}^2}{g_{2n-1}},$$

and

$$p_{2n} = \frac{2hp_{2n-1}(g_{2n-1}^2 + ex^4 f_{2n-1}^2) - p_{2n-2} g_{2n}^2}{g_{2n-2}^2},$$
$$p_{2n+1} = \frac{2p_{2n}(g_{2n}^2 + ex^4 h f_{2n}^2) - p_{2n-1} g_{2n+1}^2}{g_{2n-1}^2}.$$

Then the f_n, g_n, p_n and q_n are even polynomials in x satisfying

$$(x_{2n}, y_{2n}) = \left(xy \frac{f_{2n}(x)}{g_{2n}(x)}, \frac{p_{2n}(x)}{g_{2n}(x)^2} \right),$$

$$(x_{2n+1}, y_{2n+1}) = \left(x \frac{f_{2n+1}(x)}{g_{2n+1}(x)}, y \frac{p_{2n+1}(x)}{g_{2n+1}(x)^2} \right).$$

We list the division polynomials for $n = 3$:

$$f_3 = -e^2 x^8 + 6ex^4 - 8dx^2 + 3,$$

$$g_3 = -3e^2 x^9 + 8dex^6 - 6ex^4 + 1,$$

$$p_3 = e^4 x^{16} - 8de^3 x^{14} + 28e^3 x^{12} - 56de^2 x^{10} + (64d^2 e + 6e^2) x^8 - 56dex^6 + 28ex^4 - 8dx^2 + 1.$$

We call the f_n the Jacobi quartic division polynomials, as they satisfy the following corollary.

Corollary 2 *For $n > 2$, the point (x, y), with $xy \neq 0$, satisfies $[n](x, y) = (0, \pm 1)$ if and only if we have $f_n(x) = 0$.*

We see some of the properties of the Jacobi division polynomials.

Proposition 3 *For odd n we have*

$$f_n = (-1)^{(n-1)/2} e^{(n^2-1)/4} x^{n^2-1} + ...,$$

$$g_n = (-1)^{(n-1)/2} n e^{(n^2-1)/4} x^{n^2-1} + ...,$$

while for even n

$$f_n = (-1)^{n/2} n e^{(n^2-4)/4} x^{n^2-4} + ...,$$
$$g_n = (-1)^{n/2+1} e^{n^2/4} x^{n^2} + ...$$

Proposition 4 *For odd n,*

$$g_n(x) = (-1)^{(n-1)/2} e^{(n^2-1)/4} x^{n^2-1} f_n \left(\frac{1}{\sqrt{e} x} \right),$$

while for even n,

$$f_n(x) = (-1)^{(n+2)/2} e^{(n^2-4)/4} x^{n^2-4} f_n\left(\frac{1}{\sqrt{e}x}\right),$$

$$g_n(x) = (-1)^{n/2} e^{n^2/4} x^{n^2} g_n\left(\frac{1}{\sqrt{e}x}\right).$$

We also have

$$p_n(x) = e^{(n^2-1)/2} x^{2(n^2-1)} p_n\left(\frac{1}{\sqrt{e}x}\right),$$

for odd n, and for even n

$$p_n(x) = e^{n^2/2} x^{2n^2} p_n\left(\frac{1}{\sqrt{e}x}\right).$$

3.4 Division polynomials for Jacobi intersections

We now look at division polynomials for Jacobi intersections. Write the coordinates of $[n](u, v, w)$ as (u_n, v_n, w_n). The division polynomials we find allow us to perform arithmetic on the Jacobi intersection curve using mostly the coordinate u, as seen in the following theorem. Again, we omit the proofs in this subsection as they are analagous to the ones in section 3.2.

Theorem 6 *Let* $F_1(u) = 1, F_2(u) = 2, G_1(u) = 1, G_2(u) = bu^4 - 2u^2 + 1, H_1(u) = 1, H_2(u) = bu^4 - 2bu^2 + 1, D_1(u) = 1,$ *and* $D_2(u) = -bu^4 + 1$. *Then we have*

$$\begin{aligned}(u_{2n+1}, v_{2n+1}, w_{2n+1}) &= \left(u\frac{F_{2n+1}(u)}{D_{2n+1}(u)}, v\frac{G_{2n+1}(u)}{D_{2n+1}(u)}, w\frac{H_{2n+1}(u)}{D_{2n+1}(u)}\right)\\ (u_{2n+2}, v_{2n+2}, w_{2n+2}) &= \left(uvw\frac{F_{2n+2}(u)}{D_{2n+2}(u)}, \frac{G_{2n+2}(u)}{D_{2n+2}(u)}, \frac{H_{2n+2}(u)}{D_{2n+2}(u)}\right),\end{aligned}$$

where the $F_n, G_n, H_n,$ *and* D_n *are defined recursively for* $n > 1$ *by*

$$F_{2n+1} = 2(1-u^2)(1-bu^2)F_{2n}D_{2n-1}D_{2n} - F_{2n-1}((1-u^2)D_{2n}^2 + u^2H_{2n}^2),$$

$$\begin{aligned}G_{2n+1} &= 2G_{2n}D_{2n-1}D_{2n} - G_{2n-1}((1-u^2)D_{2n}^2 + u^2H_{2n}^2),\\ H_{2n+1} &= 2H_{2n}D_{2n-1}D_{2n} - H_{2n-1}((1-u^2)D_{2n}^2 + u^2H_{2n}^2),\\ D_{2n+1} &= D_{2n-1}((1-u^2)D_{2n}^2 + u^2H_{2n}^2),\end{aligned}$$

and

$$F_{2n+2} = 2F_{2n+1}D_{2n}D_{2n+1} - F_{2n}((1-u^2)D_{2n+1}^2 + u^2(1-bu^2)H_{2n+1}^2),$$

$$\begin{aligned}G_{2n+2} &= 2(1-u^2)G_{2n+1}D_{2n}D_{2n+1} - G_{2n}((1-u^2)D_{2n+1}^2 + u^2(1-bu^2)H_{2n+1}^2),\\ H_{2n+2} &= 2(1-bu^2)H_{2n+1}D_{2n}D_{2n+1} - H_{2n}((1-u^2)D_{2n+1}^2 + u^2(1-bu^2)H_{2n+1}^2),\\ D_{2n+2} &= D_{2n}((1-u^2)D_{2n+1}^2 + u^2(1-bu^2)H_{2n+1}^2).\end{aligned}$$

Again, the recursive formulas given above lead to the polynomials F_n, G_n, H_n, and D_n having high degree. Furthermore, the rational functions $\frac{F_n}{D_n}, \frac{G_n}{D_n}$, and $\frac{H_n}{D_n}$ can be simplified by removing common factors. Theorem 7 eliminates these common factors, thus reducing the degrees of the division polynomials.

Theorem 7 *Let $f_1(u) = 1, f_2(u) = 2, g_1(u) = 1, g_2(u) = bu^4 - 2u^2 + 1, h_1(u) = 1, h_2(u) = bu^4 - 2bu^2 + 1, d_1(u) = 1,$ and $d_2(u) = -bu^4 + 1$. For $n \geq 1$, define $f_n, g_n, h_n,$ and d_n recursively by:*

$$f_{2n+1} = \frac{(1-u^2)(1-bu^2)f_{2n}^2 - d_{2n}^2}{f_{2n-1}},$$

$$g_{2n+1} = \frac{(1-bu^2)g_{2n}^2 - (1-b)u^2 d_{2n}^2}{(1-u^2)g_{2n-1}},$$

$$h_{2n+1} = \frac{(1-u^2)h_{2n}^2 - (b-1)u^2 d_{2n}^2}{(1-bu^2)h_{2n-1}},$$

$$d_{2n+1} = \frac{((1-u^2)d_{2n}^2 + u^2 h_{2n}^2)}{d_{2n-1}},$$

and

$$f_{2n+2} = \frac{f_{2n+1}^2 - d_{2n+1}^2}{(1-u^2)(1-bu^2)f_{2n}},$$

$$g_{2n+2} = \frac{(1-u^2)(1-bu^2)g_{2n+1}^2 - (1-b)u^2 d_{2n+1}^2}{g_{2n}},$$

$$h_{2n+2} = \frac{(1-u^2)(1-bu^2)h_{2n+1}^2 - (b-1)u^2 d_{2n+1}^2}{h_{2n}},$$

$$d_{2n+2} = \frac{((1-u^2)d_{2n+1}^2 + u^2(1-bu^2)h_{2n+1}^2)}{d_{2n}}.$$

The functions $f_n(u), g_n(u), h_n(u),$ and $d_n(u)$ are even polynomials and

$$(u_{2n+1}, v_{2n+2}, w_{2n+1}) = \left(u\frac{f_{2n+1}}{d_{2n+1}}, v\frac{g_{2n+1}}{d_{2n+1}}, w\frac{h_{2n+1}}{d_{2n+1}}\right),$$

$$(u_{2n+2}, v_{2n+2}, w_{2n+2}) = \left(uvw\frac{f_{2n+2}}{d_{2n+2}}, \frac{g_{2n+2}}{d_{2n+2}}, \frac{h_{2n+2}}{d_{2n+2}}\right).$$

If desired, all the functions in Theorem 7 can be expressed in terms of h_n and d_n by using the curve equation of J_b. We list the division polynomials for $n = 3$:

$$\begin{aligned} f_3 &= -b^2u^8 + 6bu^4 - 4(b+1)u^2 + 3, \\ g_3 &= b^2u^8 - 4b^2u^6 + 6bu^4 - 4u^2 + 1, \\ h_3 &= b^2u^8 - 4bu^6 + 6bu^4 - 4bu^2 + 1, \\ d_3 &= -3b^2u^8 + 4b(b+1)u^6 - 6bu^4 + 1, \end{aligned} \tag{3.8}$$

We call the $f_n, g_n, h_n,$ and d_n *the Jacobi intersection division polynomials.* Just as with the Weierstrass, Huff, and Jacobi quartic division polynomials, we have a simple criterion to help find n-torsion points.

Corollary 3 *For $n > 2$, the point $(u, v, w) \neq (0, \pm 1, \pm 1)$ on a Jacobi intersection curve satisfies $[n](u, v, w) = (0, \pm 1, \pm 1)$ if and only if $f_n(u) = 0$.*

Notice that if the curve is defined over a finite field $\mathbb{F}_q$, and the number of points on $J_b(\mathbb{F}_q)$ is odd, then the corollary states that a point (u, v, w) is n-torsion if and only if $f_n(u) = 0$. We now describe some properties of the f_n, g_n, h_n and d_n in the following propositions.

Proposition 5 *For $n \geq 1$, the functions f_n, g_n, h_n and d_n have leading coefficients as described here. For n odd,*

$$f_n = (-1)^{(n-1)/2} b^{(n^2-1)/4} u^{(n^2-1)} + \ldots,$$

$$g_n = b^{(n^2-1)/4} u^{(n^2-1)} + \ldots,$$

$$h_n = b^{(n^2-1)/4} u^{(n^2-1)} + \ldots,$$

$$d_n = (-1)^{(n-1)/2} n b^{(n^2-1)/4} u^{(n^2-1)} + \ldots,$$

and for n even,

$$f_n = (-1)^{n/2+1} n b^{(n^2-4)/4} u^{n^2-4} + \ldots,$$

$$g_n = b^{n^2/4} u^{n^2} + \ldots,$$

$$h_n = b^{n^2/4} u^{n^2} + \ldots,$$

$$d_n = (-1)^{n/2} b^{n^2/4} u^{n^2} + \ldots.$$

Proposition 6 *For n odd,*

$$f_n(u) = (-1)^{(n-1)/2} b^{(n^2-1)/4} u^{n^2-1} d_n\left(\frac{1}{\sqrt{b}u}\right),$$

$$d_n(u) = (-1)^{(n-1)/2} b^{(n^2-1)/4} u^{n^2-1} f_n\left(\frac{1}{\sqrt{b}u}\right),$$

$$g_n(u) = b^{(n^2-1)/4} u^{n^2-1} h_n\left(\frac{1}{\sqrt{b}u}\right),$$

$$h_n(u) = b^{(n^2-1)/4} u^{n^2-1} g_n\left(\frac{1}{\sqrt{b}u}\right),$$

and for n even,

$$f_n(u) = (-1)^{n/2+1} b^{n^2/4-1} u^{n^2-4} f_n\left(\frac{1}{\sqrt{b}u}\right),$$

$$g_n(u) = b^{n^2/4} u^{n^2} g_n\left(\frac{1}{\sqrt{b}u}\right),$$

$$h_n(u) = b^{n^2/4} u^{n^2} h_n\left(\frac{1}{\sqrt{b}u}\right),$$

$$d_n(u) = (-1)^{n/2} b^{n^2/4} u^{n^2} d_n\left(\frac{1}{\sqrt{b}u}\right).$$

If we regard g_n and h_n as functions of u and b, then for n even

$$g_n(b,u) = b^{n^2/4} u^{n^2} h_n\left(\frac{1}{b}, \frac{1}{u}\right),$$

$$h_n(b,u) = b^{n^2/4} u^{n^2} g_n\left(\frac{1}{b}, \frac{1}{u}\right).$$

4 Mean value theorems

4.1 Weierstrass and Edwards mean value theorems

Let K be an algebraically closed field of characteristic not equal to 2 or 3. Let $E : y^2 = x^3+Ax+B$ be an elliptic curve defined over K, and $Q = (x_Q, y_Q) \neq \infty$ a point on E. Let $P_i = (x_i, y_i)$ be the n^2 points such that $[n]P_i = Q$, where $n \in \mathbb{Z}$, (char (K),n)=1. The P_i are known as the n-division points of Q. In [8], Feng and Wu showed that

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = x_Q, \qquad \frac{1}{n^2}\sum_{i=1}^{n^2} y_i = n y_Q.$$

This shows the mean value of the x-coordinates of the n-division points of Q is equal to x_Q, and ny_Q for the y-coordinates.

In [21] a similar formula was established for elliptic curves in twisted Edwards form. Let $Q \neq (0, \pm 1)$ be a point on a twisted Edwards curve. Let P_i be the n-division points of Q. If n is odd, then

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = \frac{1}{n} x_Q, \qquad \frac{1}{n^2}\sum_{i=1}^{n^2} y_i = \frac{(-1)^{(n-1)/2}}{n} y_Q.$$

If n is even, then $\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = 0$, and $\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = 0$.

4.2 Huff mean value theorem

We are able to prove the following mean value formula for Huff curves

Theorem 8 *Let $Q \neq (0,0)$ be a point on a Huff curve. Let $P_i = (x_i, y_i)$ be the n^2 points such that $[n]P_i = Q$.*

If n is odd, then

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = \frac{1}{n} x_Q, \qquad \frac{1}{n^2}\sum_{i=1}^{n^2} y_i = \frac{1}{n} y_Q.$$

If n is even, then both $\frac{1}{n^2}\sum_{i=1}^{n^2} x_i$ and $\frac{1}{n^2}\sum_{i=1}^{n^2} y_i$ equal 0.

Before giving the proof, we establish some results that will be needed in the proof. The first shows the theorem is true for $n = 2$.

Lemma 1 *Let P_1, P_2, P_3, and P_4 be the 4 distinct points on $H_{a,b}$ such that $[2]P_i = Q$, where $Q \neq (0,0)$. Then*

$$\sum_{i=1}^{4} x_i = 0 = \sum_{i=1}^{4} y_i.$$

Proof Let $P_1 = (x, y)$ be a point such that $[2](x, y) = Q$. If $Q \neq (0,0)$ then it follows that neither x nor y equals 0. Using the addition law, it can be checked that the points $P_2 = (-x, 1/ay), P_3 = (1/bx, -y)$, and $P_4 = (-1/bx, -1/ay)$ also satisfy $[2]P_i = Q$. For example,

$$\begin{aligned} P_2 &= \left(\frac{-2x(1+1/ay^2)}{(1+bx^2)(1-1/ay^2)}, \frac{2/ay(1+bx^2)}{(1-bx^2)(1+1/ay^2)} \right), \\ &= \left(\frac{2x(1+ay^2)}{(1+bx^2)(1-ay^2}, \frac{2y(1+bx^2)}{(1-bx^2)(1+ay^2)} \right) \\ &= Q. \end{aligned}$$

The points P_i, $i = 2, 3, 4$ arise by adding the three points at infinity to P_1. If we sum the x and y-coordinates of P_1, P_2, P_3, and P_4, the result is clear. $\square$

We look at how we can combine mean value results for n-division points and m-division points to obtain one for the mn-division points.

Proposition 7 *Fix m and n. Suppose we have that $\sum_{i=1}^{m^2} x_{P_i} = c_m x_Q$ and $\sum_{i=1}^{m^2} y_{P_i} = d_m y_Q$ for some constants c_m, d_m which depend only on m, whenever the P_i, $i = 1, 2, ..., m^2$ are points such that $[m]P_i = Q$, for some Q. Similarly, suppose we have that $\sum_{i=1}^{n^2} x_{R_i} = e_n x_S$ and $\sum_{i=1}^{n^2} y_{R_i} = f_n y_S$ for some constants e_n, f_n which depend only on n, where the R_i, $i = 1, 2, ..., n^2$ are points such that $[n]R_i = S$, for some S.*

Then given $(mn)^2$ points $T_1, T_2, ..., T_{(mn)^2}$ on $H_{a,b}$ such that $[mn]T_i = U$ for some $U \neq (0,0)$, we have that $\sum_{i=1}^{(mn)^2} x_{T_i} = c_m e_n x_U$ and $\sum_{i=1}^{(mn)^2} y_{T_i} = d_m f_n y_U$.

Proof Consider the set of points $\{[m]T_1, [m]T_2, ..., [m]T_{(mn)^2}\}$. Each element $[m]T_i$ satisfies $[n]([m]T_i) = U$. So this set must be equal to the same set of n^2 points V that satisfy $[n]V = U$. Call this set $\{V_1, V_2, ..., V_{n^2}\}$. For each V_j, there must be m^2 elements of the T_i which satisfy $[m]T_i = V_j$. This partitions our original set of the $(mn)^2$ points T_i into n^2 subsets of m^2 points. Then by assumption, we have

$$\sum_{i=1}^{(mn)^2} x_{T_i} = \sum_{i=1}^{n^2} c_m x_{V_i} = c_m e_n x_U,$$

and

$$\sum_{i=1}^{(mn)^2} y_{T_i} = \sum_{i=1}^{n^2} d_m y_{V_i} = d_m f_n y_U.$$

□

For example, fix an elliptic curve and suppose we know the mean value of the x-coordinates of the 3-division points, or $\sum_{i=1}^{9} x_i = 3x_Q$. Similary if know the same for the 5-division points, $\sum_{i=1}^{25} x_i = 5x_Q$, then by Proposition 7 we know the mean value for the 15-division points. It will be $\sum_{i=1}^{225} x_i = 15x_Q$.

We now give the proof of the mean value theorem for Huff's curves.

Proof By the obvious symmetry, we need only prove the result for the x-coordinates. We begin with the case when n is odd. By Theorem 3, we know that

$$x\frac{f_n(x)}{g_n(x)} - x_Q = 0$$

has the x_i as roots. By Proposition 1 this can be rewritten as

$$b^{(n^2-1)/2}x^{n^2} - nx_Q b^{(n^2-1)/2}x^{n^2-1} + ... = 0.$$

As the x_i are the n^2 roots, then this must be the same as

$$b^{(n^2-1)/2}\prod_{i=1}^{n^2}(x - x_i) = 0.$$

If we compare the coefficients of x^{n^2-1}, we see that $\sum_{i=1}^{n^2} x_i = nx_Q$, which proves the mean value theorem for the x-coordinates where n is odd.

We conclude (by induction) that whenever $n = 2^k$ we have $\sum_{i=1}^{n^2} x_{P_i} = 0 = \sum_{i=1}^{n^2} y_{P_i}$ by combining Lemma 1 and Proposition 7. So using proposition 7 again combined with our proof for odd n, we can conclude that whenever n is even the mean value theorem for x-coordinates holds as well. □

We remark that Theorem 8 was proved for points $Q \neq (0,0)$. For $Q = (0,0)$, recall that $(x_i, y_i) \neq (0,0)$ is an n-torsion point if and only if $f_n(x_i) = 0$. Note that for odd n, f_n is an even function of x and so

$$f_n(x) = \prod_{i=1}^{n^2-1}(x - x_i) = x^{n^2-1} + 0x^{n^2-2} + ...,$$

and hence $\sum_{i=1}^{n^2-1} x_i = 0$. When we consider $(0,0)$ as the last n-torsion point, then we have $\sum_{i=1}^{n^2} x_i = 0$. By symmetry, the same is true for the mean value of the y-coordinates when $Q = (0,0)$.

4.3 Jacobi quartic mean value theorem

We have a similar mean value theorem for the x-coordinates of Jacobi quartics.

Theorem 9 *Let Q be a point on $J_{d,e}$. Let $P_i = (x_i, y_i)$ be the n^2 points such that $[n]P_i = Q$. Then if n is odd*

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = \frac{1}{n}x_Q,$$

and $\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = 0$, if n is even.

Proof When $n = 2$, the addition formula shows that if $[2](x, y) = Q$, then $[2](-x, -y) = Q$ as well. So the four points P_i with $[2]P_i = Q$ can be written as $(x_1, y_1), (x_2, y_2), (-x_1, -y_1)$, and $(-x_2, -y_2)$. The rest of the proof is identical to the proof of the Huff mean value theorem. □

We are unable to prove, but conjecture the following mean-value theorem for the y-coordinates of the n-division points on a Jacobian quartic:

$$\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = y_Q, \tag{4.1}$$

for n odd, and $\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = 0$, for n even. Note that in our proof above, we showed it is true for $n = 2$. Thus, by Propositon 7, it suffices to show (4.1) for odd n.

4.4 Jacobi intersection mean value theorem

Finally, we have

Theorem 10 *Let Q be a point on the Jacobi intersection curve J_b. Let $P_i = (u_i, v_i, w_i)$ be the n^2 points such that $[n]P_i = Q$. Then*

$$\frac{1}{n^2}\sum_{i=1}^{n^2} u_i = \frac{u_Q}{n},$$

for n odd, and $\frac{1}{n^2}\sum_{i=1}^{n^2} u_i = 0$, for n even.

Proof Let P_1, P_2, P_3, and P_4 be the 4 distinct points on J_b such that $[2]P_i = Q$, where Q is a point on J_b. If we add the three non-trivial points of order 2 to P_1, we find that the other P_i are $(-u, -v, w), (u, -v, -w)$, and $(-u, v, -w)$. If we sum the coordinates, the result is immediate for $n = 2$. The remainder of the proof is identical to the proof of the Huff mean value theorem. □

We also conjecture the following mean-value theorem for the v and w-coordinates of the n-division points on a Jacobi intersection curve:

$$\frac{1}{n^2}\sum_{i=1}^{n^2} v_i = -\frac{v_Q}{n}, \qquad \frac{1}{n^2}\sum_{i=1}^{n^2} w_i = -\frac{w_Q}{n},$$

for n odd, and $\frac{1}{n^2}\sum_{i=1}^{n^2} v_i = 0$, $\frac{1}{n^2}\sum_{i=1}^{n^2} w_i = 0$, for n even. By Propositon 7, the even result follows immediately once this is shown to be true for odd n.

5 Conclusion

In this paper we looked at division polynomials for Huff curves, Jacobi quartics, and Jacobi intersections. Using them we were able to find a formula for the n-th multiple of a point. We also proved some of the properties of these division polynomials, and some mean-value theorems for some alternate models of elliptic curves. Some directions for future study would be to find division polynomials for other models of elliptic curves, such as Hessian curves. It would also be interesting to see if the formulas derived in this paper could be used to perform efficient scalar multiplication, as has been done in some cases with Weierstrass curves. This is the most important computation in elliptic curve cryptography and the subject of much research. We leave this for a future project.

Based on numerical evidence, we conjecture the following formula for the mean values of the coordinates for Hessian curves. If (x_i, y_i) are the n^2 points on a Hessian curve with $[n](x_i, y_i) = Q = (x_Q, y_Q)$, then

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = \begin{cases} \frac{1}{n}x_Q & n \equiv 1 \bmod 3 \\ 0 & n \equiv 0 \bmod 3, \end{cases}$$

and

$$\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = \begin{cases} \frac{1}{n}y_Q & n \equiv 1 \bmod 3 \\ 0 & n \equiv 0 \bmod 3. \end{cases}$$

It is an open problem to prove these formulas. We have not been able to adapt the technique used in this paper to prove the mean value results for Hessian curves. Also note, we are unable to conjecture the mean value for these points when $n \equiv 2 \bmod 3$. Based on numerical examples, we do know it is not a constant times the corresponding coordinate of Q.

References

[1] N. Abel, Oeuvres Completes, Nouvelle Edition, Oslo, 1881.

[2] D. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves, in Progress in cryptology—AFRICACRYPT 2008, first interna-

tional conference on cryptology in Africa, Casablanca, Morocco, June 11–14, 2008, proceedings, edited by S. Vaudenay, Lecture Notes in Computer Science 5023, Springer, pp. 389–405, 2008.

[3] O. Billet, and M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, AAECC 2003, LNCS 2643, 34-42, Springer-Verlag, 2003.

[4] D. Chudnovsky, and G. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Advances in Applied Mathematics 7, 385-434, 1986.

[5] H. Darmon, F. Diamond, and R. Taylor, Fermat's last theorem. In Current developments in mathematics, 1995 (Cambridge, MA), p1-154. Internat. Press, Cambridge, MAT, 1994

[6] V.S. Dimitrov, and P.K. Mishra, *Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication Using Multibase Number Representation*, in: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.) International Conference on Information Security 2007. Lecture Notes in Comput. Sci. 4779, Springer, Heidelberg, 2007, pp. 390406.

[7] H. Edwards, A normal form for elliptic curves, Bulletin of the American Mathematical Society **44** , pp. 393422, 2007.

[8] R. Feng, and H. Wu, A mean value formula for elliptic curves, Available at `http://eprint.iacr.org/2009/586.pdf`, 2009.

[9] R. Feng, and H. Wu, Elliptic curves in Huff's model, Available at `http://eprint.iacr.org/2010/390.pdf`, 2010.

[10] P. Giorgi, L. Imbert and T. Izard, *Optimizing elliptic curve scalar multiplication for small scalars*, in: Proc. Mathematics for Signal and Information Processing in SPIE'09, Volume 7444, 2009, pp. 74440N.

[11] H. Hisil, K. Wong, G. Carter, and E. Dawson, Faster group operations on elliptic curves, Australasian Information Security Conference (AISC 2009), Wellington, New Zealand, Conferences in Research and Practice in Information Technology (CRPIT), vol 98, p7-19, 2009.

[12] M. Joye, and J. Quisquater, Hessian elliptic curves and side-channel attacks, proceedings of the 3rd international workshop on cryptographic hardware and embedded systems, p402-410, 2001.

[13] P. Liardet, and N. Smart, Preventing SPA/DPA in ECC systems using the Jacobi form. In C.K. Koc, D. Naccache, and C. Paar, eds. Cryptographic Hardware and Embedded Systems -CHES 2001, volume 2162 of LNCS p. 391-401. Springer-Verlag, 2001.

[14] L. Hitt, G. Mcguire, and R. Moloney, Division polynomials for twisted Edwards curves, Available at `http://arxiv.org/PS_cache/arxiv/pdf/0907/0907.4347v1.pdf`, 2008.

[15] G. Huff, Diophantine problems in geometry and elliptic ternary forms. Duke Math. J., 15:443-453, 1948.

[16] M. Joye, M. Tibouchi, and D. Vergnaurd, Huff's model for elliptic curves, In 9th Algorithmic Number Theory Symposium (ANTS-IX), 2010, to appear.

[17] N. Koblitz, Elliptic curve cryptosystems, Math. Comp., 48:203-209, 1987.

[18] H. Lenstra, Factoring integers with elliptic curves, Ann. Math., 126 (2), 649-673, 1987.

[19] G. McGuire, and R. Moloney, Two Kinds of Division Polynomials For Twisted Edwards Curves, Available at `http://arxiv.org/PS_cache/arxiv/pdf/0907/0907.4347v1.pdf`, 2010.

[20] V. Miller, Use of elliptic curves in cryptography, In H.C. Williams, ed. Advances in Cryptology - CRYPTO '85, volume 218 of LNCS p417-426, Springer 1986.

[21] D. Moody, Mean value formulas for twisted Edwards curves, Available at `eprint.iacr.org/2010/142.pdf`, 2010.

[22] R. Schoof, Counting points on elliptic curves over finite fields, J. Théor. Nombres Bordeaux 7 (1995). p219-254.

[23] J. Silverman, The arithmetic of elliptic curves, Springer-Verlag, 1986.

[24] L. Washington, Elliptic curves (Number theory and cryptography), 2nd edition, Chapman & Hall, 2008.

[25] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2), 141 (3): 443-551, 1995.