Division Polynomials for Jacobi Quartic Curves *

Dustin Moody
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD, 20899-8930, USA
dbmoody25@gmail.com

ABSTRACT

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

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*Algebraic Algorithms*

General Terms

Algorithms, Theory

Keywords

Algorithms, Elliptic Curves, Division Polynomials

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 [16] and cryptography [15],[19]. The traditional way of writing the equation of an elliptic curve is to use its Weierstrass form:

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

In the past several years, other models of elliptic curves have been introduced. Such models include Edwards curves [2], [6], Jacobi intersections and Jacobi quartics [3], [4],[17], Hessian curves [13], and Huff curves [8], [14], among others. These models sometimes allow for more efficient computation on elliptic curves or provide other features of interest to cryptographers. In particular, Jacobi quartics provide resistance to side channel attacks, and they also have the most efficient unified point addition formulae [3], [10].

In this paper we find division polynomials for Jacobi quartics, although the ideas can be extended to Jacobi intersections and Huff curves. 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 the point (x, y) in terms of x and y, as well as determining when a point is an n-torsion point on a Weierstrass curve. Division 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 perform efficient computations on elliptic curves, see for example [5], [9].

Hitt, McGuire, and Moloney recently have found formulas for division polynomials of twisted Edwards curves [11], [18]. The division polynomials we find are the analogues for Jacobi quartic curves. We illustrate 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 illustration, we show how they can be used to find the mean value of a certain collection of points related to the discrete logarithm problem.

This paper is organized as follows. In section 2 we review Jacobi quartics, and in section 3 we examine their division polynomials. As an application, in section 4 we look at a certain mean value theorem. We conclude in section 5 with some remarks and open questions.

2. THE JACOBI QUARTIC

One model for elliptic curves is known as Jacobi quartics. For a background on these curves, see [3], [4], [17]. We recall only the basic facts. For the remainder of this paper, let K be a field whose characteristic is not 2 or 3. 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 $e(d^2 - e) \neq 0$, with $d, e \in K$. The identity element is $(0, 1)$, and the point $(0, -1)$ has order 2. The inverse of a point (x, y) is $(-x, y)$. There are two points at infinity, whose coordinates can be written in projective coordinates (with $z = 0$). The addition formula on $J_{d,e}$ is

*A full version of this paper is available as *Divison Polynomials for Alternate Models of Elliptic Curves* at `http://eprint.iacr.org/2010/630`

ISSAC'11, June 8–11, 2011, San Jose, California, USA.

given by

$$(x_1,y_1)+(x_2,y_2)=\Big(\frac{x_1y_2+y_1x_2}{1-e(x_1x_2)^2},$$
$$\frac{(1+e(x_1x_2)^2)(y_1y_2-2dx_1x_2)+2ex_1x_2({x_1}^2+{x_2}^2)}{(1-e(x_1x_2)^2)^2}\Big).$$

This addition formula can be efficiently implemented, which is one of the primary advantages of writing an elliptic curve in this form [10]. Another is that this addition formula protects against side-channel attacks [3], [17]. There is a birational transformation from a Jacobi quartic curve to a curve in Weierstrass form with a point of order 2. 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 points of the curve $J_{d,e}$ with $x=0$ to the Weierstrass curve

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

Under this transformation, the identity point $(0,1)$ corresponds to ∞, and the point of order two $(0,-1)$ 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.

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) and $n\geq 2$*

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

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 $\psi_n(x)=0$. Division polynomials are an important tool for finding multiples of points. In fact, they have been used to speed up computation of point multiplication in some cases (see for example [5], [9]). 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].

3.2 Division polynomials for Jacobi quartics

We now perform 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. For convenience, let $h(x)=ex^4-2dx^2+1$, so the curve equation for $J_{d,e}$ is $y^2=h(x)$.

THEOREM 2. *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 $Q_2=(ex^4-1)^2$. Write $[n](x,y)=(x_n,y_n)$. Then there are polynomials $F_n(x)$, $G_n(x)$, $P_n(x)$, and $Q_n(x)$ such that*

$$(x_{2k},y_{2k})=\left(xy\frac{F_{2k}(x)}{G_{2k}(x)},\frac{P_{2k}(x)}{Q_{2k}(x)}\right),$$

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

The F_n,G_n,P_n, and Q_n can all be calculated recursively:

$$\begin{aligned}F_{2k+1}&=2hF_{2k}G_{2k-1}G_{2k}-F_{2k-1}(G_{2k}^2-ex^4hF_{2k}^2),\\ G_{2k+1}&=G_{2k-1}(G_{2k}^2-ex^4hF_{2k}^2),\\ F_{2k+2}&=2F_{2k+1}G_{2k}G_{2k+1}-F_{2k}(G_{2k+1}^2-ex^4F_{2k+1}^2),\\ G_{2k+2}&=G_{2k}(G_{2k+1}^2-ex^4F_{2k+1}^2),\end{aligned}$$

and

$$\begin{aligned}P_{2k+1}&=2G_{2k}^2P_{2k}Q_{2k-1}(G_{2k}^2+ex^4hF_{2k}^2)\\ &\quad-P_{2k-1}Q_{2k}(G_{2k}^2-ex^4hF_{2k}^2)^2,\\ Q_{2n+1}&=Q_{2k-1}Q_{2k}(G_{2k}^2-ex^4hF_{2k}^2)^2,\\ P_{2k+2}&=2hG_{2k+1}^2P_{2k+1}Q_{2k}(G_{2k+1}^2+ex^4F_{2k+1}^2)\\ &\quad-P_{2k}Q_{2k+1}(G_{2k+1}^2-ex^4F_{2k+1}^2)^2,\\ Q_{2k+2}&=Q_{2k}Q_{2k+1}(G_{2k+1}^2-ex^4F_{2k+1}^2)^2,\end{aligned}$$

for $k\geq 1$.

PROOF. The proof is along the same lines as what was done for Edwards curves in [11],[18]. In turn, these authors credit Abel [1]. We use induction on n. For $n=1$ the claim is trivially true,

$$(x_1,y_1)=\left(x\frac{F_1(x)}{G_1(x)},y\frac{P_1(x)}{Q_1(x)}\right).$$

For $n=2$, the addition formula yields

$$(x_2,y_2)=\left(-\frac{2xy}{ex^4-1},\frac{(1+ex^4)(y^2-2dx^2)+4ex^4}{(ex^4-1)^2}\right).$$

By the defining curve equation, we have that $y^2 = ex^4 - 2dx^2 + 1$, so y_2 can be rewritten as

$$y_2 = \frac{e^2x^8 - 4dex^6 + 6ex^4 - 4dx^2 + 1}{(ex^4 - 1)^2}.$$

Thus $(x_2, y_2) = (xyF_2/G_2, P_2/Q_2)$. We now assume the result holds true for all n.

Given two points (r_1, s_1) and (r_2, s_2) on $J_{d,e}$, let $(r_+, s_+) = (r_1, s_1) + (r_2, s_2)$ and $(r_-, s_-) = (r_1, s_1) - (r_2, s_2)$. Then by the addition formula, we have

$$r_+ + r_- = \frac{2r_1s_2}{1 - e(r_1r_2)^2}$$

and

$$s_+ + s_- = \frac{2s_1s_2(1 + e(r_1r_2)^2)}{(1 - e(r_1r_2)^2)^2}.$$

If we substitute in $(r_1, s_1) = (x_n, y_n)$, and $(r_2, s_2) = (x, y)$ we obtain

$$x_{n+1} = \frac{2x_ny}{1 - e(xx_n)^2} - x_{n-1},$$

and

$$y_{n+1} = \frac{2y_ny(1 + e(xx_n)^2)}{(1 - e(xx_n)^2)^2} - y_{n-1}.$$

Assume first that $n = 2k$ is even, so then

$$\begin{aligned} x_{2k+1} &= \frac{2xh\frac{F_{2k}}{G_{2k}}}{1 - ex^4h\frac{F_{2k}^2}{G_{2k}^2}} - x\frac{F_{2k-1}}{G_{2k-1}} \\ &= x \quad \frac{2hF_{2k}G_{2k-1}G_{2k} - F_{2k-1}(G_{2k}^2 - ex^4hF_{2k}^2)}{G_{2k-1}(G_{2k}^2 - ex^4hF_{2k}^2)} \quad , \end{aligned}$$

and

$$\begin{aligned} y_{2k+1} &= \frac{2y\frac{P_{2k}}{Q_{2k}}(1 + ex^4h\frac{F_{2k}^2}{G_{2k}^2})}{(1 - ex^4h\frac{F_{2k}^2}{G_{2k}^2})^2} - y\frac{P_{2k-1}}{Q_{2k-1}} \\ &= y \quad \frac{2G_{2k}^2P_{2k}Q_{2k-1}(G_{2k}^2 + ex^4hF_{2k}^2)}{Q_{2k-1}Q_{2k}(G_{2k}^2 - ex^4hF_{2k}^2)^2} \\ &\qquad - \frac{P_{2k-1}Q_{2k}(G_{2k}^2 - ex^4hF_{2k}^2)^2}{Q_{2k-1}Q_{2k}(G_{2k}^2 - ex^4hF_{2k}^2)^2} \quad . \end{aligned}$$

When $n = 2k + 1$ is odd

$$\begin{aligned} x_{2k+2} &= \frac{2xy\frac{F_{2k+1}}{G_{2k+1}}}{1 - ex^4\frac{F_{2k+1}^2}{G_{2k+1}^2}} - xy\frac{F_{2k}}{G_{2k}} \\ &= xy \quad \frac{2F_{2k+1}G_{2k}G_{2k+1} - F_{2k}(G_{2k+1}^2 - ex^4F_{2k+1}^2)}{G_{2k}(G_{2k+1}^2 - ex^4F_{2k+1}^2)} \quad , \end{aligned}$$

and

$$\begin{aligned} y_{2k+2} &= \frac{2y^2\frac{P_{2k+1}}{Q_{2k+1}}(1 + ex^4\frac{F_{2k+1}^2}{G_{2k+1}^2})}{(1 - ex^4\frac{F_{2k+1}^2}{G_{2k+1}^2})^2} - \frac{P_{2k}}{Q_{2k}} \\ &= \frac{2hG_{2k+1}^2P_{2k+1}Q_{2k}(G_{2k+1}^2 + ex^4F_{2k+1}^2)}{Q_{2k+1}Q_{2k}(G_{2k+1}^2 - ex^4F_{2k+1}^2)^2} \\ &\qquad - \frac{P_{2k}Q_{2k+1}(G_{2k+1}^2 - ex^4F_{2k+1}^2)^2}{Q_{2k+1}Q_{2k}(G_{2k+1}^2 - ex^4F_{2k+1}^2)^2}. \end{aligned}$$

This proves the recurrence relations given in the statement of the theorem hold.

Alternatively, if we let $\alpha_n = F_n/G_n$ and $\beta_n = P_n/Q_n$, then the above can be rewritten as follows: for n odd,

$$x_{n+1} = xy \quad \frac{2\alpha_n}{1 - ex^4\alpha_n^2} - \alpha_{n-1} \quad ,$$

$$y_{n+1} = \frac{2h\beta_n(1 + ex^4\alpha_n^2)}{(1 - ex^4\alpha_n^2)^2} - \beta_{n-1}.$$

When n is even,

$$x_{n+1} = x \quad \frac{2h\alpha_n}{1 - ex^4h\alpha_n^2} - \alpha_{n-1} \quad ,$$

and

$$y_{n+1} = y \quad \frac{2\beta_n(1 + ex^4h\alpha_n^2)}{(1 - ex^4h\alpha_n^2)^2} - \beta_{n-1} \quad .$$

□

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

THEOREM 3. *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 $n > 2$, define f_n, g_n, p_n, and q_n by*

$$f_{2k} = \frac{2f_{2k-1}g_{2k-2}g_{2k-1} - f_{2k-2}(g_{2k-1}^2 - ex^4f_{2k-1}^2)}{g_{2k-2}^2},$$

$$f_{2k+1} = \frac{2hf_{2k}g_{2k-1}g_{2k} - f_{2k-1}(g_{2k}^2 - ex^4hf_{2k}^2)}{g_{2k-1}^2},$$

$$g_{2k} = \frac{g_{2k-1}^2 - ex^4f_{2k-1}^2}{g_{2k-2}},$$

$$g_{2k+1} = \frac{g_{2k}^2 - ex^4hf_{2k}^2}{g_{2k-1}},$$

and

$$\begin{aligned} p_{2k} &= \frac{2hg_{2k-1}^2p_{2k-1}q_{2k-2}(g_{2k-1}^2 + ex^4f_{2k-1}^2)}{q_{2k-2}^2q_{2k-1}} \\ &\qquad - \frac{p_{2k-2}q_{2k-1}(g_{2k-1}^2 - ex^4f_{2k-1}^2)^2}{q_{2k-2}^2q_{2k-1}}, \\ p_{2k+1} &= \frac{2g_{2k}^2p_{2k}q_{2k-1}(g_{2k}^2 + ex^4hf_{2k}^2)}{q_{2k-1}^2q_{2k}} \\ &\qquad - \frac{p_{2k-1}q_{2k}(g_{2k}^2 - ex^4hf_{2k}^2)^2}{q_{2k-1}^2q_{2k}}, \end{aligned}$$

$$q_{2k} = \frac{(g_{2k-1}^2 - ex^4f_{2k-1}^2)^2}{q_{2k-2}},$$

$$q_{2k+1} = \frac{(g_{2k}^2 - ex^4hf_{2k}^2)^2}{q_{2k-1}}.$$

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

$$(x_{2k}, y_{2k}) = \quad xy\frac{f_{2k}(x)}{g_{2k}(x)}, \frac{p_{2k}(x)}{q_{2k}(x)} \quad ,$$

$$(x_{2k+1}, y_{2k+1}) = \quad x\frac{f_{2k+1}(x)}{g_{2k+1}(x)}, y\frac{p_{2k+1}(x)}{q_{2k+1}(x)} \quad .$$

Before we give the proof, we prove a lemma. It will be needed in the proof of Theorem 3 as well as for some of the identities of the Jacobi division polynomials. Most importantly, it gives a simpler recurrence for the f_n (and p_n).

LEMMA 1. *For $n \geq 1$, the functions f_n, g_n, p_n, and q_n from Theorem 3 satisfy*

$$g_{2k}^2 - hf_{2k}^2 = -f_{2k-1}f_{2k+1}, \tag{1}$$

and as a result

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

and for $n > 1$

$$f_{2k-1}^2 - g_{2k-1}^2 = hf_{2k-2}f_{2k}, \tag{2}$$

so therefore

$$f_{2k} = \frac{f_{2k-1}^2 - g_{2k-1}^2}{hf_{2k-2}}.$$

Also $q_n = g_n^2$ and

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

$$p_{2k+1} = \frac{2p_{2k}(g_{2k}^2 + ex^4hf_{2k}^2) - p_{2k-1}g_{2k+1}^2}{q_{kn-1}}.$$

PROOF. First note that by definition, we have

$$\begin{aligned} f_{2k+1}g_{2k-1} &= \frac{2hf_{2k}g_{2k-1}g_{2k} - f_{2k-1}(g_{2k}^2 - ex^4hf_{2k}^2)}{g_{2k-1}}, \\ &= \frac{2hf_{2k}g_{2k-1}g_{2k} - f_{2k-1}g_{2k-1}g_{2k+1}}{g_{2k-1}}, \\ &= 2hf_{2k}g_{2k} - f_{2k-1}g_{2k+1}. \end{aligned} \tag{3}$$

We now use induction. For $k = 1$, a direct computation checks that both sides of (1) are equal to $e^2x^8 - 6ex^4 + 8dx^2 - 3$. The expression $g_{2k}^2 - hf_{2k}^2 + f_{2k-1}f_{2k+1}$ can be rewritten as

$$\begin{aligned} \frac{g_{2k}^2}{g_{2k-2}^2g_{2k-1}^2} \quad & - f_{2k-1}^2(g_{2k-2}^2 - ex^4hf_{2k-2}^2) \\ & + g_{2k-1}^2(g_{2k-2}^2 - hf_{2k-2}^2) \\ & + 2hf_{2k-2}f_{2k-1}g_{2k-2}g_{2k-1} \quad . \end{aligned}$$

By the induction hypothesis, $g_{2k-2}^2 - hf_{2k-2}^2 = -f_{2k-3}f_{2k-1}$, and we also have $g_{2k-2}^2 - ex^4hf_{2k-2}^2 = g_{2k-3}g_{2k-1}$ so this last expression becomes

$$\frac{f_{2k-1}g_{2k}^2}{g_{2k-2}^2g_{2k-1}} \quad 2hf_{2k-2}g_{2k-2} - f_{2k-1}g_{2k-3} - g_{2k-1}f_{2k-3} \quad .$$

By (3) (with $k-1$ in place of k), we see that this is equal to 0. This shows $g_{2k}^2 - hf_{2k}^2 + f_{2k-1}f_{2k+1} = 0$, which was to be proved.

To prove (2) we also use induction. For $k = 2$ both sides are equal to $8(ex^4 - 2dx^2 + 1)(ex^4 - 1)(-e^2x^8 + 4dex^6 - 6ex^4 + 4dx^2 - 1)$. We can rewrite $f_{2k-1}^2 - g_{2k-1}^2 - hf_{2k-2}f_{2k}$ as

$$\begin{aligned} \frac{g_{2k-1}^2}{g_{2k-3}^2g_{2k-2}^2} \quad & g_{2k-2}^2(f_{2k-3}^2 - g_{2k-3}^2) \\ & - 2hf_{2k-3}f_{2k-2}g_{2k-3}g_{2k-2} \\ & + hf_{2k-2}^2(g_{2k-3}^2 - ex^4f_{2k-3}^2) \quad . \end{aligned} \tag{4}$$

Using the induction hypothesis and the identity $g_{2k-3}^2 - ex^4f_{2k-3}^2 = g_{2k-4}g_{2k-2}$ then equation (4) becomes

$$\frac{hf_{2k-2}g_{2k-1}^2}{g_{2k-3}^2g_{2k-2}} \quad f_{2k-4}g_{2k-2} - 2f_{2k-3}g_{2k-3} + f_{2k-2}g_{2k-4} \quad . \tag{5}$$

But

$$\begin{aligned} f_{2k-2}g_{2k-4} &= \frac{2f_{2k-3}g_{2k-4}g_{2k-3} - f_{2k-4}(g_{2k-3}^2 - ex^4f_{2k-3}^2)}{g_{2k-4}} \\ &= 2f_{2k-3}g_{2k-3} - f_{2k-4}g_{2k-2}, \end{aligned}$$

so (5) is equal to 0, showing $f_{2k-1}^2 - g_{2k-1}^2 - hf_{2k-2}f_{2k} = 0$.

Finally, we verify that $q_n = g_n^2$. For $n = 1$ and 2, this is clearly true. Now assume that $q_n = g_n^2$. Then by definition $q_{n+1} = g_{n+1}^2g_{n-2}^2/q_{n-2}$. By the induction hypothesis, $g_{n-2}^2 = q_{n-2}$ which proves $q_{n+1} = g_{n+1}^2$. Using this, combined with the definition of the g_n, the formulas for the p_n are straightforward and we omit the details. □

We now give the proof of Theorem 3.

PROOF. Note the similarities in the definitions of F_n and f_n, G_n and g_n, P_n and p_n, and finally between Q_n and q_n. Since the f_n and g_n are just the F_n and G_n with their common factors canceled then $F_n/G_n = f_n/g_n$. Likewise $P_n/Q_n = p_n/q_n$. It is clear that f_n, g_n, p_n, and q_n are all even using the recursion formulas combined with the fact that $f_1, f_2, g_1, g_2, p_1, p_2, q_1$, and q_2 are all even.

We first show that the g_n are polynomials. Let γ be a root of g_{2k-2}, and $\delta \in \overline{K}$ such that (γ, δ) is a point on $J_{d,e}$. It follows that $[2k-2](\gamma, \delta)$ is a point at infinity R. Using the addition law for projective coordinates (given in [3]), $(x, y) + R = (\pm 1/\sqrt{e}x, \pm y/\sqrt{e})$. As a result, we see

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

This is equivalent to γ being a root of $g_{2k-1}^2 - ex^4f_{2k-1}^2$. As γ was arbitrary, then this shows $g_{2k-2} | g_{2k-1}^2 - ex^4f_{2k-1}^2$. Similarly, if $g_{2k-1}(\gamma) = 0$ then by the same reasoning we have

$$x_{2k}^2(\gamma) = \frac{1}{e\gamma^2} = \gamma^2h(\gamma)\frac{f_{2k}^2(\gamma)}{g_{2k}^2(\gamma)}.$$

Thus γ is a root of $g_{2k}^2 - ex^4hf_{2k}^2$ as desired. We conclude that the g_n are polynomials in x.

We now show that the f_n are polynomials in x. By Lemma 1, $f_{2k+1} = (hf_{2k}^2 - g_{2k}^2)/f_{2k-1}$. Let γ be a root of f_{2k-1}. Then by the addition law, we have $x_{2k}(\gamma) = \pm\gamma$. Squaring this relation yields

$$\gamma^2 = \gamma^2h(\gamma)\frac{f_{2k}^2(\gamma)}{g_{2k}^2(\gamma)},$$

which shows γ is a root of $g_{2k}^2 - hf_{2k}^2$, and hence f_{2k+1} is a polynomial.

Similarly, by Lemma 1 we have that $f_{2k} = \frac{f_{2k-1}^2 - g_{2k-1}^2}{h f_{2k-2}}$. Now if $f_{2k-2}(\gamma) = 0$ for some $\gamma = 0$, then $x_{2k-1}(\gamma) = \pm\gamma$. Squaring this yields

$$\gamma^2 = \gamma^2 \frac{f_{2k-1}^2(\gamma)}{g_{2k-1}^2(\gamma)},$$

and we see that γ is a root of $f_{2k-1}^2 - g_{2k-1}^2$, so f_{2k-2} divides $f_{2k-1}^2 - g_{2k-1}^2$.

If γ is a root of $h = ex^4 - 2dx^2 + 1$, then $(\gamma, 0)$ is a point on the curve $J_{d,e}$, and it is easy to check that $[2](\gamma, 0) = (0, -1), [3](\gamma, 0) = (-\gamma, 0)$, and $[4](\gamma, 0) = (0, 1)$. So then

$$x_{2k-1}^2(\gamma) = \gamma^2 = \gamma^2 \frac{f_{2k-1}^2(\gamma)}{g_{2k-1}^2(\gamma)},$$

so γ is a root of $f_{2k-1}^2 - g_{2k-1}^2$, and hence h divides $f_{2k-1}^2 - g_{2k-1}^2$. This shows that f_{2k} is a polynomial in x.

To see q_n is a polynomial in x, we appeal to Lemma 1. As g_n is a polynomial, and $q_n = g_n^2$, then q_n is a polynomial as well. The proof that p_n is a polynomial is much more cumbersome to write down, although the technique is the same. Consequently, we omit it. □

We list the division polynomials for $n = 3$ and 4:

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

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

$$\begin{aligned} p_3 = {} & e^4x^{16} - 8de^3x^{14} + 28e^3x^{12} - 56de^2x^{10} \\ & + 2e(32d^2 + 3e)x^8 - 56dex^6 + 28ex^4 - 8dx^2 + 1, \end{aligned}$$

$$q_3 = (-3e^2x^8 + 8dex^6 - 6ex^4 + 1)^2,$$

$$f_4 = -4(ex^4 - 1)(-e^2x^8 + 4dex^6 - 6ex^4 + 4dx^2 - 1),$$

$$\begin{aligned} g_4 = {} & -e^4x^{16} + 20e^3x^{12} - 64de^2x^{10} + (64d^2 + 26e^2)ex^8 \\ & - 64dex^6 + 20ex^4 - 1, \end{aligned}$$

$$p_4 = e^8x^{32} - 16\,de^7x^{30} - 560\,de^6x^{26} + \cdots - 16\,dx^2 + 1,$$

$$q_4 = {g_4}^2.$$

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

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

Proof. This is immediate from Theorems 2 and 3. Note that $[n](x, y) = (0, 1)$ if and only if $[n](x, -y) = (0, -1)$. □

An advantage of our division polynomials is that the n-th one can be computed from the previous two rounds, i.e., f_n and g_n only depend 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. We now show some of the properties of these latter Jacobi division polynomials, beginning with their degrees.

Proposition 1. *For odd n,*

$$\frac{f_n(x)}{g_n(x)} = \frac{e^{(n^2-1)/4}x^{n^2-1} + \cdots}{ne^{(n^2-1)/4}x^{n^2-1} + \cdots},$$

$$\frac{p_n(x)}{q_n(x)} = \frac{e^{(n^2-1)/2}x^{2(n^2-1)+\cdots}}{(ne^{(n^2-1)/4}x^{n^2-1} + \cdots)^2},$$

where $+\cdots$ indicates lower powers of x. For even n, we have

$$\frac{f_n(x)}{g_n(x)} = -n\frac{e^{(n^2-4)/4}x^{n^2-4} + \cdots}{e^{n^2/4}x^{n^2} + \cdots},$$

$$\frac{p_n(x)}{q_n(x)} = \frac{e^{n^2/2}x^{2n^2} + \cdots}{(e^{n^2/4}x^{n^2} + \cdots)^2}.$$

Proof. The proof of the leading terms of the quotient f_n/g_n and p_n/q_n is a straightforward exercise in induction. We only give the proof for f_n/g_n, and skip the proof for p_n/q_n. We first establish that for odd n,

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

$$g_n = (-1)^{(n-1)/2}ne^{(n^2-1)/4}x^{n^2-1} + \cdots,$$

while for even n

$$f_n = (-1)^{n/2}ne^{(n^2-4)/4}x^{n^2-4} + \cdots,$$

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

Note that for $n = 1$ and 2 this is clearly true. For even n, if we include only the leading terms we have

$$\begin{aligned} f_{n+1} &= \frac{(ex^4)(n^2e^{(n^2-4)/2}x^{2(n^2-4)}) - (e^{n^2/2}x^{2n^2})}{(-1)^{(n-2)/2}e^{(n^2-2n)/4}x^{n^2-2n}} \\ &= -(-1)^{n/2}e^{(n^2+2n)/4}x^{n^2+2n} + \cdots \\ &= (-1)^{(n+1-1)/2}e^{((n+1)^2-1)/4}x^{(n+1)^2-1} + \cdots. \end{aligned}$$

Similarly, when n is odd we have

$$\begin{aligned} f_{n+1} &= \frac{(e^{(n^2-1)/2}x^{2(n^2-1)}) - (n^2e^{(n^2-1)/2}x^{2(n^2-1)})}{(ex^4)((-1)^{(n-1)/2}(n-1)e^{(n^2-2n-3)/4}x^{n^2-2n-3})} \\ &= (n+1)(-1)^{(n+1)/2}e^{((n+1)^2-4)/4}x^{(n+1)^2-4} + \cdots. \end{aligned}$$

This shows the leading term of f_n is as desired for n even or odd. Now for $n = 2k$, we have

$$\begin{aligned} g_{n+1} &= \frac{e^{2k^2}x^{8k^2} - ex^4(ex^4)(4k^2)e^{2k^2-2}x^{8k^2-8}}{(-1)^{k-1}(2k-1)e^{k^2-k}x^{4k^2-4k}} \\ &= (-1)^k(2k+1)e^{k^2+k}x^{4k^2+4k} + \cdots \\ &= (-1)^{(n+1-1)/2}(n+1)e^{((n+1)^2-1)/4}x^{(n+1)^2-1} + \cdots. \end{aligned}$$

Also for $n = 2k + 1$,

$$\begin{aligned} g_{n+1} &= \frac{(2k+1)^2e^{2k^2+2k}x^{8k^2+8k} - ex^4e^{2k^2+2k}x^{8k^2+8k}}{(-1)^{k+1}e^{k^2}x^{4k^2}} \\ &= (-1)^ke^{k^2+2k+1}x^{4k^2+8k+4} + \cdots \\ &= -(-1)^{(n+1)/2}e^{n^2/4}x^{n^2} + \cdots, \end{aligned}$$

which shows the leading term of g_n is as claimed. □

We include some functional equations for the Jacobi division polynomials.

Proposition 2. *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,

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

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

We also have

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

for odd n, and

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

for even n.

PROOF. Recall that f_n, g_n, and p_n are even, so the square roots in the formulae make sense. We use induction to prove Proposition 2. The results are all easily verified for $n = 1, 2$. We first verify the functional equation for g_n when $n = 2k$ is even:

$$\begin{aligned}
&(-1)^k e^{k^2} x^{4k^2} g_{2k} \quad \left(\frac{1}{\sqrt{e}x}\right) \\
&\quad = (-1)^k e^{k^2} x^{4k^2} \frac{g_{2k-1}^2 - e x^4 f_{2k-1}^2}{g_{2k-2}} \quad \left(\frac{1}{\sqrt{e}x}\right) \quad , \\
&\quad = (-1)^k e^{k^2} x^{4k^2} \frac{\frac{f_{2k-1}^2}{e^{2k^2-2k} x^{8k^2-8k}} - \frac{g_{2k-1}^2}{e^{2k^2-2k+1} x^{8k^2-8k+4}}}{\frac{(-1)^{k-1} g_{2k-2}}{e^{(k-1)^2} x^{4(k-1)^2}}}, \\
&\quad = \frac{g_{2k-1}^2 - e x^4 f_{2k-1}^2}{g_{2k-2}},
\end{aligned}$$

which is $g_{2k}(x)$ as desired.

Also for $n = 2k$,

$$\begin{aligned}
&(-1)^{k+1} e^{k^2-1} x^{4k^2-4} f_{2k} \quad \left(\frac{1}{\sqrt{e}x}\right) \\
&\quad = (-1)^{k+1} e^{k^2-1} x^{4k^2-4} \frac{f_{2k-1}^2 - g_{2k-1}^2}{h f_{2k-2}} \quad \left(\frac{1}{\sqrt{e}x}\right) \quad , \\
&\quad = (-1)^{k+1} e^{k^2-1} x^{4k^2-4} \frac{\frac{g_{2k-1}^2}{e^{2k^2-2k} x^{8k^2-8k}} - \frac{f_{2k-1}^2}{e^{2k^2-2k} x^{8k^2-8k}}}{\frac{h}{ex^4} \frac{f_{2k-2}}{(-1)^k e^{k^2-2k} x^{4k^2-8k}}}, \\
&\quad = \frac{g_{2k-1}^2 - f_{2k-1}^2}{h f_{2k-2}}, \\
&\quad = f_{2k}.
\end{aligned}$$

Finally, we show the functional equation relating f_n and g_n for odd $n = 2k + 1$. We leave the proof of the functional equation for p_n to the reader. We have

$$\begin{aligned}
&(-1)^k e^{k^2+k} x^{4k^2+4k} f_{2k+1} \quad \left(\frac{1}{\sqrt{e}x}\right) \\
&\quad = (-1)^k e^{k^2+k} x^{4k^2+4k} \frac{h f_{2k}^2 - g_{2k}^2}{f_{2k-1}} \quad \left(\frac{1}{\sqrt{e}x}\right) \quad , \\
&\quad = (-1)^k e^{k^2+k} x^{4k^2+4k} \frac{\frac{h}{ex^4} \frac{f_{2k}^2}{e^{2k^2-2} x^{8k^2-8}} - \frac{g_{2k}^2}{e^{2k^2} x^{8k^2}}}{\frac{g_{2k-1}}{(-1)^{k-1} e^{k^2-k} x^{4k^2-4k}}}, \\
&\quad = \frac{g_{2k}^2 - e x^4 h f_{2k}^2}{g_{2k-1}}, \\
&\quad = g_{2k+1},
\end{aligned}$$

which was to be proved. Note these functional equations impose certain symmetries on the coefficients of the Jacobi division polynomials. □

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 $Q = (x_Q, y_Q) = \infty$ 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 [7], 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 be a point on a twisted Edwards curve. Let $P_i = (x_i, y_i)$ be the n^2 points such that $[n]P_i = Q$. If n is odd, then

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

If n is even, then

$$\frac{1}{n^2} \sum_{i=1}^{n^2} x_i = 0 = \frac{1}{n^2} \sum_{i=1}^{n^2} y_i.$$

4.2 Jacobi quartic mean value theorem

We now give a mean value theorem for the x-coordinates of Jacobi quartics.

THEOREM 4. *Let $Q = (0, \pm 1)$ 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*

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

if n is odd and

$$\frac{1}{n^2} \sum_{i=1}^{n^2} x_i = 0,$$

if n is even.

We first need a result showing how we can combine mean value results for n-division points and m-division points to obtain one for the mn-division points.

PROPOSITION 3. *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, $i = 1, 2, \cdots, m^2$ are points such that $[m]P_i = Q$, for some $Q = (0, 0)$. 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, $i = 1, 2, \cdots, n^2$ are points such that $[n]R_i = S$, for some $S = (0, 0)$.

Then given $(mn)^2$ points $T_1, T_2, \cdots, T_{(mn)^2}$ on $J_{d,e}$ such that $[mn]T_i = U$ for some $U = (0, 0)$, 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 $\{[m]T_1, [m]T_2, \cdots, [m]T_{(mn)^2}\}$. 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 $\{V_1, V_2, \cdots, V_{n^2}\}$. For each V_j, there are at most m^2 elements of the T_i which satisfy $[m]T_i = V_j$. As each T_i must satisfy $[m]T_i = V_j$ for some 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 $\sum_{i=1}^{9} x_i = 3x_Q$. Similarly if know the same for the 5-division points, $\sum_{i=1}^{25} x_i = 5x_Q$, then by Proposition 3 we know the mean value for the 15-division points. It will be $\sum_{i=1}^{225} x_i = 15x_Q$.

Now we give the proof of Theorem 4.

PROOF. We first examine the case when n is odd. By definition, the solutions of $x\frac{f_n(x)}{g_n(x)}, y\frac{p_n(x)}{q_n(x)} = (x_Q, y_Q)$ are exactly the (x_i, y_i). By proposition 1, we can rewrite this x-coordinate relation as

$$x\ \ e^{(n^2-1)/4}x^{n^2-1} + 0x^{n^2-2} + \cdots\ \ = x_Q(ne^{(n^2-1)/4x^{n^2-1}} + \cdots)$$

or

$$e^{(n^2-1)/4}\ \ x^{n^2} - nx_Q x^{n^2-1} + \cdots\ \ = 0.$$

This must be equal to the polynomial $e^{(n^2-1)/4}\prod_{i=1}^{n^2}(x - x_i)$, so we can conclude that

$$\sum_{i=1}^{n^2} x_i = nx_Q.$$

This proves the mean value of the x-coordinate is as claimed when n is odd.

We now look at the case when $n = 2$. By the addition formula it is clear 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 result for $n = 2$ is immediate. Now by Proposition 3, and the result for odd n, Theorem 4 is true for even n as well. □

We remark that Theorem 4 was proved for points $Q = (0, \pm 1)$. For $Q = (0, \pm 1)$, recall that $(x_i, y_i) = (0, \pm 1)$ is an n-division point of Q if and only if $f_n(x_i) = 0$. Recall that for odd n, f_n is an even function of x and so

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

and hence $\sum_{i=1}^{n^2-1} x_i = 0$. When we consider Q as the last n-division point of Q, then we have $\sum_{i=1}^{n^2} x_i = 0$.

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:

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

for n odd, and

$$\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = 0,$$

for n even. The proof techniques in [7], [21] do not work for Jacobi quartic curves. The Weierstrass result uses properties of the Weierstrass $\wp(z)$ function, which we do not have a Jacobi quartic analogue for. In the Edwards case, the result is obtained by the obvious symmetry of x and y in the defining curve equation.

Note that in our proof above, we showed the conjecture is true for $n = 2$. Hence, by Proposition 3, the even result follows immediately once it is true for odd n. Also note that the y-coordinate mean value theorem is equivalent to showing

$$\sum_{i=1}^{n^2} \frac{g_n(x_i)}{f_n(x_i)} = n^2,$$

for odd n because $y_i\frac{f_n(x_i)}{g_n(x_i)} = y_Q$.

5. CONCLUSION

In this paper we looked at division polynomials for Jacobi quartics. 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 a type of mean-value theorem. In the extended version of this paper ([20]) we show how to extend these results to other models of elliptic curves, namely, Huff curves and Jacobi intersections. This includes results for the division polynomials and related mean-value theorems.

Some directions for future study would be to find division polynomials for the remaining 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.

6. ACKNOWLEDGMENTS

The author would like to thank Hongfeng Wu for his thoughtful discussions which helped improve this paper.

7. REFERENCES

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

[2] D. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In *Progress in cryptology—AFRICACRYPT 2008 proceedings*, LNCS vol 5023, pages 389–405. Springer, 2008.

[3] 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.

[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] V.S. Dimitrov, and P.K. Mishra. Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication Using Multibase Number Representation. In *International Conference on Information Security 2007 proceedings*, LNCS vol 4779, pages 390–406. Springer, 2007.

[6] H. Edwards. A normal form for elliptic curves. *Bulletin of the AMS*, 44: 393–422, 2007.

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

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

[9] P. Giorgi, L. Imbert and T. Izard. Optimizing elliptic curve scalar multiplication for small scalars. In *Mathematics for Signal and Information Processing proceedings*, SPIE vol 7444, page 7444N. 2009.

[10] H. Hisil, K. Wong, G. Carter, and E. Dawson. Faster group operations on elliptic curves. In *Australasian Information Security Conference proceedings*, 98:7–19, 2009.

[11] L. Hitt, G. Mcguire, and R. Moloney. Division polynomials for twisted Edwards curves. Available at `http://arxiv.org/abs/0809.2182`, 2008.

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

[13] 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.

[14] M. Joye, M. Tibouchi, and D. Vergnaurd. Huff's model for elliptic curves. In *Algorithmic Number Theory Symposium (ANTS-IX) proceedings*, LNCS vol 6197, pages 234–250. Springer, 2010.

[15] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.

[16] H. Lenstra. Factoring integers with elliptic curves. *Ann. Math.*, 126 (2): 649–673, 1987.

[17] P. Liardet, and N. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In *Workshop on Cryptographic Hardware and Embedded Systems*, LNCS vol 2162, pages 391–401. Springer, 2001.

[18] G. McGuire, and R. Moloney. Two Kinds of Division Polynomials For Twisted Edwards Curves. Available at `http://arxiv.org/abs/0907.4347`, 2009.

[19] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO '85 proceedings*, 218: 417–426, Springer, 1986.

[20] D. Moody. Division Polynomials for Alternate Models of Elliptic Curves. Available at `eprint.iacr.org/2010/630.pdf`

[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: 219–254, 1995.

[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.