MEAN VALUE FORMULAS FOR TWISTED EDWARDS CURVES

Dustin Moody*
National Institute of Standards and Technology (NIST)
100 Bureau Drive Stop 8930, Gaithersburg, MD 20899-8930, USA

September 29, 2010

Abstract

R. Feng and H. Wu recently established a certain mean-value formula for the coordinates of the n-division points on an elliptic curve given in Weierstrass form (A mean value formula for elliptic curves, 2010, available at http://eprint.iacr.org/2009/586.pdf). We prove a similar result for the x and y-coordinates on a twisted Edwards elliptic curve.

Key Words: elliptic curves, Edwards curves, division polynomials **A**MS Subject Classification: 11G05, 14H52.

*E-mail address: dustin.moody@nist.gov
This work was done while the author was a postdoctoral researcher at the University of Calgary

1. Introduction

Let K be an algebraically closed field of characteristic greater than 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 [4], Feng and Wu showed that

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

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

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 this paper we establish a similar formula for elliptic curves in twisted Edwards form. Our main result is given below.

Theorem 1. *Let $Q \neq (0, \pm 1)$ 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

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

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

If n is even, then

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

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

Edwards curves are a new model for elliptic curves which have been shown to have uses in cryptography [1],[2],[5]. They have not been studied nearly as well in comparison to the more commonly used Weierstrass curves. While this paper has no direct applications in cryptography, a better understanding of Edwards curves could lead to improvements in future cryptographic uses. For example, given points P and $Q = [n]P$ on an elliptic curve, the discrete log problem is to find n. It is crucial for elliptic curve cryptography that this problem is computationally infeasible. Theorem 1.1 provides us with some information about the value n.

This paper is organized as follows. In section 2 we review twisted Edwards curves, and in section 3 we look at their division polynomials. The twisted Edwards division polynomials, introduced in [6], [7], are an analogue to the classical division polynomials and a key ingredient of the proof of Theorem 1. We prove Thereom 1 in section 4. Section 5 concludes with a look at some open questions.

2. Twisted Edwards curves

H. Edwards recently proposed a new parameterization for elliptic curves [3]. These Edwards curves are of the form

$$E_d : x^2 + y^2 = 1 + dx^2y^2,$$

with $d = 1, d \in K$. In [1], Bernstein et al. generalized this definition to twisted Edwards curves. These curves are given by the equation

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where a and d are distinct, non-zero elements of K. Edwards curves are simply twisted Edwards curves with $a = 1$. The addition law for points on $E_{a,d}$ is given by:

$$(x_1, y_1) + (x_2, y_2) = \Big(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\Big).$$

If a is a square and d is not a square in K, then the addition law is complete. This means that the addition formula is valid for all points, with no exceptions. The addition law for Weierstrass curves is not complete, which is one of the advantages of Edwards curves. The additive identity on $E_{a,d}$ is the point $(0, 1)$, and the inverse of the point (x, y) is $(-x, y)$.

There is a birational transformation from $E_{a,d}$ to change it to a curve in Weierstrass form. The map

$$\phi : (x, y) \to \left(\frac{(5a - d) + (a - 5d)y}{12(1 - y)}, \frac{(a - d)(1 + y)}{4x(1 - y)}\right) \tag{1}$$

maps the curve $E_{a,d}$ to the curve

$$E : y^2 = x^3 - \frac{a^2 + 14ad + d^2}{48}x - \frac{a^3 - 33a^2d - 33ad^2 + d^3}{864}.$$

This map holds for all points (x, y), with $x(1-y) = 0$. For these points, we have $\phi(0, 1) = \infty$, and $\phi(0, -1) = (\frac{a+d}{6}, 0)$.

3. Division polynomials for twisted Edwards curves

We will need some results from [6], [7], concerning division polynomials for twisted Edwards curves. These polynomials are the analogue of the classical division polynomials associated to Weierstrass curves. In fact, the twisted Edwards division polynomials are the image of the classical division polynomials under the birational transformation (1) given in the last section. Standard facts about the classical division polynomials can be found in [8] or [9].

Theorem 2. *Let (x, y) be a point on the twisted Edwards curve $E_{a,d}$, with $(x, y) = (0, \pm 1)$. Then for positive integers $n \geq 1$ we have*

$$[n](x, y) = \Big(\frac{\phi_n(x, y)\psi_n(x, y)}{\omega_n(x, y)}, \frac{\phi_n(x, y) - \psi_n^2(x, y)}{\phi_n(x, y) + \psi_n^2(x, y)}\Big),$$

where

$$\psi_0(x,y) = 0,$$
$$\psi_1(x,y) = 1,$$
$$\psi_2(x,y) = \frac{(a-d)(y+1)}{x(2(1-y))},$$
$$\psi_3(x,y) = \frac{(a-d)^3(-dy^4-2dy^3+2ay+a)}{(2(1-y))^4},$$
$$\psi_4(x,y) = \frac{2(a-d)^6 y(1+y)(a-dy^4)}{x(2(1-y))^7},$$
$$\psi_{2k+1}(x,y) = \psi_{k+2}(x,y)\psi_k^3(x,y) - \psi_{k-1}(x,y)\psi_{k+1}^3(x,y) \textit{ for } k \geq 2,$$
$$\psi_{2k}(x,y) = \frac{\psi_k(x,y)}{\psi_2(x,y)}(\psi_{k+2}(x,y)\psi_{k-1}^2(x,y) - \psi_{k-2}(x,y)\psi_{k+1}^2(x,y)) \textit{ for } k \geq 3,$$

and

$$\phi_n(x,y) = \frac{(1+y)\psi_n^2(x,y)}{1-y} - \frac{4\psi_{n-1}(x,y)\psi_{n+1}(x,y)}{a-d},$$
$$\omega_n(x,y) = \frac{2\psi_{2n}(x,y)}{(a-d)\psi_n(x,y)}.$$

Proof. See Theorem 5.1 in [6] or [7]. □

It is a bit of a misnomer to refer to $\psi_n(x,y)$ as a division polynomial since it is not a polynomial. However, their behavior is largely shaped by a certain polynomial $\tilde{\psi}_n(y)$ in their numerator. In [6], [7], Hitt, Moloney, and McGuire showed that $\tilde{\psi}_n(x,y)$ can be written

$$\psi_n(x,y) = \begin{cases} \frac{(a-d)^{\lfloor 3n^2/8 \rfloor}\tilde{\psi}_n(y)}{(2(1-y))^{(n^2-1)/2}} & \text{if } n \text{ is odd,} \\ \frac{(a-d)^{\lfloor 3n^2/8 \rfloor}\tilde{\psi}_n(y)}{x(2(1-y))^{(n^2-2)/2}} & \text{if } n \text{ is even.} \end{cases} \tag{2}$$

The first few $\tilde{\psi}_n(y)$ are

$$\tilde{\psi}_0(y) = 0,$$
$$\tilde{\psi}_1(y) = 1,$$
$$\tilde{\psi}_2(y) = y+1,$$
$$\tilde{\psi}_3(y) = -dy^4 - 2dy^3 + 2ay + a,$$
$$\tilde{\psi}_4(y) = -2dy^6 - 2dy^5 + ...,$$
$$\tilde{\psi}_5(y) = d^3y^{12} - 2d^3y^{11} + ...$$

Note that $\tilde{\psi}_n(y)$ is a polynomial solely in y (and not x). We will use the recurrence relation they satisfy. Hitt, Moloney, and McGuire also proved a formula for their first coefficient, and we will establish a formula for the second leading coefficient. As will be shown, the second leading coefficient directly determines the mean value of the n-division points.

Proposition 3. *We have*

$$\tilde{\psi}_{2k+1}(y) = d^{(k^2+k)/2} \ \ (-1)^k y^{2k^2+2k} - 2\left\lfloor \frac{k+1}{2} \right\rfloor y^{2k^2+2k-1} + ... \tag{3}$$

and

$$\tilde{\psi}_{2k}(y) = d^{2k^2-1-\lfloor 3k^2/2 \rfloor} \ \ b_k y^{2k^2-1} + b_k y^{2k^2-2} + ... \tag{4}$$

where

$$b_k = \begin{cases} k/y, & \text{if } k \equiv 0 \mod 4 \\ 1, & \text{if } k \equiv 1 \mod 4 \\ -k/y, & \text{if } k \equiv 2 \mod 4 \\ -1, & \text{if } k \equiv 3 \mod 4. \end{cases} \tag{5}$$

Proof. As the result for the leading coefficient was shown in [6], [7], all that remains to be seen is that the second leading coefficient is as claimed. There are several cases to be considered, depending on k mod 4, since the recurrence relations for the $\tilde{\psi}_n(y)$ depends on n mod 4. We prove the lemma for the case when $k \equiv 0$ mod 4, and leave the other cases, which can be similarly treated. The proof is by induction. Looking at the first few $\tilde{\psi}_n$ it can be seen the result is true for $n = 0, 1, 2, 3, 4$ and 5.

We begin with the case of n odd, $n = 2k + 1$. For $k \equiv 0$ mod 4, then the recurrence relation given in [6], [7] is

$$\tilde{\psi}_{2k+1}(y) = \frac{4(a-d)(a-dy^2)}{(y+1)^2}\tilde{\psi}_{k+2}(y)\tilde{\psi}_k^3(y) - \tilde{\psi}_{k-1}(y)\tilde{\psi}_{k+1}^3(y). \tag{6}$$

Theorem 8.1 of [7] shows that when n is even, then $y + 1$ evenly divides into $\tilde{\psi}_n(y)$, so the first term is a polynomial in y. Examining degrees, we see that the degree of $\frac{4(a-d)(a-dy^2)}{(y+1)^2}\tilde{\psi}_{k+2}\tilde{\psi}_k^3$ in y is $2k^2 + 2k - 2$, while the degree of $\tilde{\psi}_{k-1}\tilde{\psi}_{k+1}^3$ is $2k^2 + 2k$. As we are only concerned with the first two leading coefficients, we can ignore the first term in (6). Let $j = k/2$, an integer since k is even. By the induction hypothesis, we have

$$\begin{aligned} \tilde{\psi}_{k-1}\tilde{\psi}_{k+1}^3 &= -d^{(j^2-j)/2} \ \ - y^{2j^2-2j} - 2\left\lfloor \frac{j}{2} \right\rfloor y^{2j^2-2j-1} + ... \\ &\qquad \cdot d^{3(j^2+j)/2} \ \ y^{2j^2+2j} - 2\left\lfloor \frac{j+1}{2} \right\rfloor y^{2j^2+2j-1} + ... \ \ ^3 \\ &= -d^{2j^2+2j} \ \ - y^{8j^2+4j} - (2\left\lfloor \frac{j}{2} \right\rfloor - 6\left\lfloor \frac{j+1}{2} \right\rfloor) y^{8j^2+4j-1} + ... \\ &= d^{(k^2+k)/2} \ \ y^{2k^2+2k} - 2\left\lfloor \frac{k+1}{2} \right\rfloor y^{2k^2+2k-1} + ... \ \ . \end{aligned}$$

This proves (3). Note that in the last lines, we used the fact that $2\left\lfloor \frac{j}{2} \right\rfloor - 6\left\lfloor \frac{j+1}{2} \right\rfloor =$

$-2\left\lfloor\frac{k+1}{2}\right\rfloor$. This is easy to see by writing $j = 2i$, as

$$\begin{aligned} 2\ \frac{j}{2}\ -6\ \frac{j+1}{2} &= 2\ \frac{2i}{2}\ -6\ \frac{2i+1}{2} \\ &= -4i \\ &= -k \\ &= -2\ \frac{k+1}{2}\ . \end{aligned}$$

We now show (4). Again let $k = 2j = 4i$ and define $e_j = 2j^2 - 1 - \left\lfloor 3j^2/2\right\rfloor$. The recurrence from [6], [7] shows that when $k \equiv 0 \bmod 4$,

$$\tilde{\psi}_{2k}(y) = \frac{\tilde{\psi}_k(y)}{y+1}\ \tilde{\psi}_{k+2}(y)\tilde{\psi}_{k-1}^3(y) - \tilde{\psi}_{k-2}(y)\tilde{\psi}_{k+1}^3(y)\ .$$

By the induction hypothesis and the results for $\tilde{\psi}_{2k+1}$, we see that

$$\begin{aligned} \tilde{\psi}_{2k}(y) = \frac{d^{e_j}}{y+1}\ & b_j y^{2j^2-1} + b_j y^{2j^2-2} + ... \\ & \cdot \Big[d^{e_{j+1}+j^2-j}\ c_{j+1} y^{2j^2+4j+1} + c_{j+1} y^{2j^2+4j} + ... \\ & \cdot\ \ - y^{2j^2-2j} - 2\lfloor j/2 \rfloor y^{2j^2-2j-1} + ...\ \Big]^2 \\ & - d^{e_{j-1}+j^2+j}\ c_{j-1} y^{2j^2-4j+1} + c_{j-1} y^{2j^2-4j} + ... \\ & \cdot\ \ y^{2j^2+2j} - 2\ \frac{j+1}{2}\ y^{2j^2+2j-1} + ...\ \Big]^2 \Big]. \end{aligned}$$

Looking at the degrees (in y) of the terms of the binomial, we see they are both equal to $6j^2 + 1$, so we cannot ignore either. Observe that

$$\begin{aligned} e_{j+1} + j^2 - j &= 3j^2 + 3j + 1 - \ \frac{3(j+1)^2}{2} \\ &= 3j^2 + 3j + 1 - \lfloor 6i^2 + 6i + 3/2 \rfloor \\ &= 3j^2 + 3j + 1 - 3/2j^2 - 3j - 1 \\ &= \lfloor 3j^2/2 \rfloor. \end{aligned}$$

Similarly, it is easy to check that $e_{j-1} + j^2 + j = \left\lfloor 3j^2/2\right\rfloor$ and $e_j + \left\lfloor 3j^2/2\right\rfloor = 2j^2 - 1$. Also $e(k) = e(2j) = 8j^2 - 1 - \lfloor 6j^2 \rfloor = 2j^2 - 1$. Using these identities to further simplify, we find

$$\begin{aligned} \tilde{\psi}_{2k}(y) = \frac{d^{e_j}}{y+1}\ & b_j y^{2j^2-1} + b_j y^{2j^2-2} + ...\ \ d^{\lfloor 3j^2/2 \rfloor}\ \ (b_{j+1} - b_{j-1}) y^{6j^2+1} \\ & +\ \ b_{j+1} - b_{j-1} + 4\ \ \frac{j}{2}\ \ b_{j+1} + 4\ \ \frac{j+1}{2}\ \ b_{j-1}\ \ y^{6j^2} + ...\ \ . \end{aligned}$$

From the definition of b_j we see that $4 \ \frac{j}{2} \ b_{j+1} + 4 \ \frac{j+1}{2} \ b_{j-1} = 0$, so

$$\begin{aligned}\tilde{\psi}_{2k}(y) &= \frac{d^{e(k)}}{y+1} \ b_j y^{2j^2-1} + b_j y^{2j^2-2} + ... \quad 2b_{j+1} y^{6j^2+1} + 2b_{j+1} y^{6j^2} + ... \\ &= \frac{d^{e(k)}}{y+1} \ 2b_j b_{j+1} y^{8j^2} + 4b_j b_{j+1} y^{8j^2-1} + ... \ .\end{aligned}$$

Recall that if we know $y+1$ divides a polynomial of the form $ay^r + by^{r-1} + ...$, then their quotient is $ay^{r-1} + (b-a)y^{r-2} + ...$ So

$$\begin{aligned}\tilde{\psi}_{2k}(y) &= d^{e(k)} \ 2b_j b_{j+1} y^{8j^2-1} + 2b_j b_{j+1} y^{8j^2-2} + ... \\ &= d^{e(k)} \ b_k y^{2k^2-1} + b_k y^{2k^2-2} + ...\end{aligned}$$

as desired, proving (4). As mentioned before, the cases $k \equiv 1, 2, 3 \bmod 4$ can be similarly handled, and we omit the details. □

The following is an easy consequence. We leave the proof to the reader.

Corollary 4. *We have*

$$\begin{aligned}&\phi_{2k+1}(y) - \psi_{2k+1}^2(y) - y_Q(\phi_{2k+1}(y) + \psi_{2k+1}^2(y)) \\ &\quad = \frac{(a-d)^{3(k^2+k)} d^{k^2+k}}{2^{4(k^2+k)-1}(1-y)^{4(k^2+k)+1}} \ y^{(2k+1)^2} - y_Q(-1)^k(2k+1)y^{4(k^2+k)} + ... \ ,\end{aligned}$$

and

$$\begin{aligned}&\phi_{2k}(x,y) - \psi_{2k}^2(x,y) - y_Q \ \phi_{2k}(x,y) + \psi_{2k}^2(x,y) \\ &\quad = (-1)^k \frac{(a-d)^{3k^2-1} d^{k^2}}{2^{4k^2-2}(1-y)^{4k^2}} \ (1-(-1)^k)y^{4k^2} + 0y^{4k^2-1} + ...\end{aligned}$$

4. Mean Value Theorem

We now state and prove our mean-value theorem for twisted Edwards curves.

Theorem 5. *Let $Q = (0, \pm 1)$ be a point on the Edwards curve $E_{a,d}$. Let $P_i = (x_i, y_i)$ be the n^2 points such that $[n]P_i = Q$.*

If n is odd, then

$$\frac{1}{n^2} \sum_{i=1}^{n^2} x_i = \frac{1}{n} x_Q, \tag{7}$$

$$\frac{1}{n^2} \sum_{i=1}^{n^2} y_i = \frac{(-1)^{(n-1)/2}}{n} y_Q. \tag{8}$$

If n is even, then

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = 0, \tag{9}$$

$$\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = 0. \tag{10}$$

Proof. For odd n, the approach is similar to that used by Feng and Wu in [4]. By Theorem 2, we see $[n](x,y) = Q$ if and only if

$$\frac{\phi_n(x,y)\psi_n(x,y)}{\omega_n(x,y)}, \frac{\phi_n(x,y) - \psi_n^2(x,y)}{\phi_n(x,y) - \psi_n^2(x,y)} \quad = (x_Q, y_Q).$$

In other words,

$$\phi_n(x,y) - \psi_n^2(x,y) - y_Q \quad \phi_n(x,y) - \psi_n^2(x,y) \quad = 0.$$

From Corollary 4, for odd n this is equivalent to

$$y^{n^2} - (-1)^{(n-1)/2} n y_Q y^{n^2-1} + ... = 0,$$

(we need not worry about when $y = 1$ since $Q = (0,1)$). This polynomial has as roots the n^2 y_i. So it must also be equal to the polynomial

$$\prod_{i=1}^{n^2}(y - y_i).$$

Comparing the y^{n^2-1} coefficients of these two equal polynomials, equation (8) follows immediately.

The result for the x-coordinates in (7) could be established by rewriting the division polynomials in terms of x, however we prefer the following approach. Define a map $\Phi : E_{a,d} \to E_{1,d/a}$ by $\Phi(x,y) = (\sqrt{a}x, y)$. Using the addition law it is easily verified that Φ is a homomorphism. So if $[n](x,y) = (x_Q, y_Q)$, then $[n](\sqrt{a}x, y) = [n]\Phi(x,y) = \Phi([n](x,y)) = \Phi(Q) = (\sqrt{a}x_Q, y_Q)$ on $E_{1,d/a}$. Observe also that $(\sqrt{a}x, y) = (-y, \sqrt{a}x) + (1,0)$ on $E_{1,d/a}$.

By what we just noted the $(\sqrt{a}x_i, y_i)$ are the n^2 points on $E_{1,d/a}$ which satisfy $[n]P = (\sqrt{a}x_Q, y_Q)$. So then

$$\begin{aligned}(\sqrt{a}x_Q, y_Q) &= [n] \quad (y_i, -\sqrt{a}x_i) + (-1,0) \\ &= [n](y_i, -\sqrt{a}x_i) + [n](-1,0).\end{aligned} \tag{11}$$

It is not hard to see that for odd n,

$$[n](-1,0) = \quad (-1)^{(n+1)/2}, 0$$

on $E_{1,a/d}$. Rewriting (11), we see that

$$\begin{aligned} y_i, -\sqrt{a}x_i &= \sqrt{a}x_Q, y_Q \ + \ (-1)^{(n-1)/2}, 0 \\ &= (-1)^{(n-1)/2} y_Q, \sqrt{a}(-1)^{(n+1)/2} x_Q \ . \end{aligned}$$

By the result for the y-coordinates (8) (which we already showed), we then have

$$\sum_{i=1}^{n^2} -\sqrt{a}x_i = (-1)^{(n-1)/2} n \ \ \sqrt{a}(-1)^{(n+1)/2} x_Q \ .$$

Thus (7) follows immediately.

We now show that if n is even, then $\sum_{i=1}^{n^2} y_i = 0$. Assuming this, by repeating the above argument to swap the x and y-coordinates it follows that $\sum_{i=1}^{n^2} x_i = 0$ as well. We could use Corollary 4 again to show $\sum_{i=1}^{n^2} y_i = 0$, but we illustrate a different technique.

Lemma 6. *Let P_1, P_2, P_3, and P_4 be the 4 distinct points on $E_{a,d}$ such that $[2]P_i = Q$, where $Q = (0, \pm 1)$. Then*

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

Proof. Note that if $[2](x_i, y_i) = Q$ then necessarily $[2](-x_i, -y_i) = Q$, as $[2](x_i, y_i) = [2](-x_i, -y_i)$ directly from the addition formula for Edwards curves. From this the result follows immediately. □

We now show how 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 $Q = (0, \pm 1)$. 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 $S = (0, \pm 1)$.*

Then given $(mn)^2$ points $T_1, T_2, ..., T_{(mn)^2}$ on $E_{a,d}$ such that $[mn]T_i = U$ for some $U = (0, 1)$. Then $\sum_{i=1}^{(mn)^2} x_{T_i} = c_m e_n x_U$ 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 $\sum_{i=1}^{225} x_i = 15x_Q$.

Combining Proposition 7 and Lemma 6 we can conclude by induction that whenever $n = 2^k$ we have $\sum_{i=1}^{n^2} x_{P_i} = 0 = \sum_{i=1}^{n^2} y_{P_i}$. Together with the earlier results (7) and (8) for odd n, this shows (9) and (10).

□

We remark that Theorem 5 was proved for points $Q = (0, \pm 1)$. When $Q = (0, \pm 1)$ then we claim $\sum_{i=1}^{n^2} x_i = 0 = \sum_{i=1}^{n^2} y_i$. Let P_i be the n^2 points which satisfy $[n]P_i = (0, \pm 1)$. If P_i is one of our n^2 points, then $-P_i$ is also. The only time $P_i = -P_i$ are the points $(0, \pm 1)$. Then clearly $\sum_{i=1}^{n^2} x_i = 0$. Then we repeat our trick of switching the x and y coordinates to get the same result for the sum of the y_i.

5. Conclusion

Feng and Wu proved a mean value theorem for the x-coordinates of the division points on an elliptic curve in Weierstrass form using division polynomials. In this paper we showed similar results hold for both the x and y-coordinates on twisted Edwards curves.

Based on numerical examples, we conjectured the following mean value formula for the y-coordinate of the n-division points on an elliptic curve in Weierstrass form. If (x_i, y_i) are the n^2 points such that $[n]P = Q = \infty$ on $E : y^2 = x^3 + Ax + B$, then

$$\frac{1}{n^2} \sum_{i=1}^{n^2} y_i = n y_Q. \tag{12}$$

Feng and Wu have since been able to prove this [4], although not with their technique of using division polynomials. It fails as the polynomial satisfied by the n^2 y-coordinates is a polynomial in x and y, not just y. Thus we cannot set it equal to $\prod_{i=1}^{n^2}(y - y_i)$. It would be interesting to see if the argument can somehow be modified to prove (12) with division polynomials. It is an open problem to see if mean value theorems can be found for other models of elliptic curves, such as Hessian curves, Jacobi intersections, and Huff curves.

References

[1] Bernstein, D.; Birkner, P.; Joye, M.; Lange, T.; Peters C. *Twisted Edwards curves* In *Progress in cryptology—AFRICACRYPT 2008 proceedings*; editor Vaudenay, S.; Ed.; Lecture Notes in Comput. Sci. 5023, Springer: New York, NY, 2008, pp. 389–405.

[2] Bernstein, D.; Lange, T. *Faster addition and doubling on elliptic curves* In *Advances in cryptology— ASIACRYPT 2007 proceedings*; editor Kurosawa, K.; Ed.; Lecture Notes in Comput. Sci. 4833, Springer: New York, NY, 2007 pp. 29-50.

[3] Edwards, H. *A normal form for elliptic curves.* Bull. Amer. Math. Soc. 2007, 44, pp. 393-422.

[4] Feng R.; Wu, H. (2009). *A mean value formula for elliptic curves*. Available at `http://eprint.iacr.org/2009/586.pdf`

[5] Hisil, H.; Carter, G.; Dawson, E. *New formulae for efficient elliptic curve arithmetic* In *Proceedings of INDOCRYPT 2007*; editor by Srinathan, K.; Pandu Rangan, C.; Yung, M.; Eds.; Lecture Notes in Comput. Sci. 4859, Springer: New York, NY, 2007, pp. 138–151.

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

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

[8] Silverman, J. *The arithmetic of elliptic curves;* Springer-Verlag: New York, NY, 1986;

[9] Washington, L. *Elliptic curves (Number theory and cryptography);* Second edition. Chapman & Hall: Boca Raton, LA, 2008;