Mean value formulas for twisted Edwards curves

Dustin Moody

February 23, 2010

Abstract

R. Feng, and H. Wu recently established a certain mean-value formula for the x-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 both the x and y-coordinates on a twisted Edwards elliptic curve.

1 Introduction

Let K be a 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 $n \in \mathbb{Z}$, (n,char (K))=1. The P_i are known as the n-division points of Q. In [3], Feng and Wu showed that

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

This shows the mean value of the x-coordinates of the n-division points of Q is equal to x_Q. In this paper we establish a similar formula for elliptic curves in twisted Edwards form. We are able to give the mean value for both the x and y-coordinates of the n-division points. Our main result is given in Theorem 1.

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

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

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 [4], [5], 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 [2]. These Edwards curves are of the form

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

with $d \neq 1, d \in K$. 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

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

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 $x(1 - y) \neq 0$. 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 the following results from [4], [5], concerning division polynomials for twisted Edwards curves. These 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 given in the last section. Standard facts about the classical division polynomials can be found in [6] or [7].

Theorem 2 *Let (x, y) be a point on the twisted Edwards curve $E_{a,d}$, with $(x, y) \neq (0, \pm 1)$. 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

$$\psi_0(x,y) = 0,$$

$$\psi_1(x,y) = 1,$$

$$\psi_2(x,y) = \frac{(a-d)(y+1)}{x(2(1-y))},$$

$$\psi_3(x,y) = \frac{(a-d)^3(-dy^4 - 2dy^3 + 2ay + a)}{(2(1-y))^4},$$

$$\psi_4(x,y) = \frac{2(a-d)^6 y(1+y)(a-dy^4)}{x(2(1-y))^7},$$

$$\psi_{2k+1}(x,y) = \psi_{k+2}(x,y)\psi_k^3(x,y) - \psi_{k-1}(x,y)\psi_{k+1}^3(x,y) \text{ for } k \geq 2,$$

$$\psi_{2k}(x,y) = \frac{\psi_k(x,y)}{\psi_2(x,y)}(\psi_{k+2}(x,y)\psi_{k-1}^2(x,y) - \psi_{k-2}(x,y)\psi_{k+1}^2(x,y)) \text{ for } k \geq 3,$$

and

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

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

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 [4], [5], Hitt, Moloney, and McGuire showed that

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

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 in y, and not x. There is a recurrence relation they satisfy, which we will use below. Hitt, Moloney, and McGuire proved a formula for their first coefficient, and we will establish a formula for the second leading coefficient. As we will see, the second leading coefficient directly determines the mean value of the n-division points.

Proposition 1 *We have*

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

and

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

where

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

Proof As the result for the leading coefficient was shown in [4], [5], 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 relation 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 [4], [5] is

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

Theorem 8.1 of [5] 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. Let $j = k/2 \in \mathbb{Z}$, since k is even. By the induction hypothesis, we have

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

This proves 2. 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

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

We now show 3. Again let $k = 2j = 4i$ and define $e_j = 2j^2 - 1 - \lfloor 3j^2/2 \rfloor$. The recurrence from [4], [5] 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

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

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

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

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

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

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

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

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. 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.

Corollary 1 *We have*

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

and

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

Proof Using the previous lemma, and looking only at the leading coefficients we see

$$\psi_{2k+1}(x,y) = \frac{(a-d)^{3/2(k^2+k)}d^{(k^2+k)/2}}{(2(1-y))^{2(k^2+k)}}\Big((-1)^k y^{2(k^2+k)} - 2\left\lfloor \frac{k+1}{2} \right\rfloor y^{2(k^2+k)-1} + ...\Big),$$

and consequently

$$\psi_{2k+1}^2(x,y) = \frac{(a-d)^{3(k^2+k)}d^{(k^2+k)}}{(2(1-y))^{4(k^2+k)}}\Big(y^{4(k^2+k)}-(-1)^k 4\left\lfloor\frac{k+1}{2}\right\rfloor y^{4(k^2+k)-1}+...\Big).$$

Also,

$$\psi_{2k}(x,y) = \frac{(a-d)^{\lfloor 3k^2/2\rfloor}d^{2k^2-1-\lfloor 3k^2/2\rfloor}}{x(2(1-y))^{2k^2-1}}\Big(b_k y^{2k^2-1} + b_k y^{2k^2-2} + ...\Big),$$

where b_k is as defined above. Thus,

$$\psi_{2k}(x,y)\psi_{2k+2}(x,y) = \frac{(a-d)^{3(k^2+k)+1}d^{k^2+k}}{2^{4(k^2+k)-1}(1-y)^{4(k^2+k)+1}}\Big((-1)^{k+1}\left\lfloor\frac{k+1}{2}\right\rfloor(y^{4(k^2+k)}+y^{4(k^2+k)-1})+...\Big).$$

By definition, $\phi_{2k+1}(x,y) = \frac{1+y}{1-y}\psi_{2k+1}^2(x,y) - \frac{4}{a-d}\psi_{2k}(x,y)\psi_{2k+2}(x,y)$. So

$$\begin{aligned}
\phi_{2k+1}(x,y) &= \frac{1+y}{1-y}\frac{(a-d)^{3k^2+3k}d^{k^2+k}}{(2(1-y))^{4k^2+4k}}(y^{4k^2+4k} - (-1)^k 4\left\lfloor\frac{k+1}{2}\right\rfloor y^{4k^2+4k-1} + ...) \\
&\quad - \frac{4}{a-d}\frac{(a-d)^{\lfloor 3k^2/2\rfloor}d^{e(k)}}{x(2(1-y))^{2k^2-1}}(b_k y^{2k^2-1} + b_k y^{2k^2-2}...) \\
&\quad \cdot \frac{(a-d)^{\lfloor 3(k+1)^2/2\rfloor}d^{e(k+1)}}{x(2(1-y))^{2(k+1)^2-1}}(b_{k+1}y^{2(k+1)^2-1} + b_{k+1}y^{2(k+1)^2-2}...) \\
&= \frac{(a-d)^{3k^2+3k}d^{k^2+k}}{2^{4k^2+4k}(1-y)^{4k^2+4k+1}}(y^{4k^2+4k+1} + (1-(-1)^k 4\lfloor\frac{k+1}{2}\rfloor)y^{4k^2+4k} + ...) \\
&\quad - \frac{(a-d)^{3k^2+3k}d^{k^2+k}}{2^{4k^2+4k-3}(1-y)^{4k^2+4k+1}}(((-1)^k\lfloor\frac{k+1}{2}\rfloor)(y^{4k^2+4k} + y^{rk^2+4k-1}) + ...) \\
&= \frac{(a-d)^{3k^2+3k}d^{k^2+k}}{2^{4k^2+4k}(1-y)^{4k^2+4k+1}}(y^{4k^2+4k+1} + (1+(-1)^k 4\left\lfloor\frac{k+1}{2}\right\rfloor y^{4k^2+4k}) + ...) \\
&= \frac{(a-d)^{3k^2+3k}d^{k^2+k}}{2^{4k^2+4k}(1-y)^{4k^2+4k+1}}(y^{4k^2+4k+1} + (-1)^k(2k+1)y^{4k^2+4k}) + ...).
\end{aligned}$$

In the last line, we used the identity $1+(-1)^k 4\left\lfloor\frac{k+1}{2}\right\rfloor = (-1)^k(2k+1)$. This is easily seen to be true by considering k to be even, then odd. Hence

$$\phi_{2k+1}(x,y)-\psi_{2k+1}^2(x,y) = \frac{(a-d)^{3(k^2+k)}d^{k^2+k}}{2^{4(k^2+k)-1}(1-y)^{4(k^2+k)+1}}\Big(y^{4(k^2+k)+1}+0y^{4(k^2+k)}+...\Big),$$

and

$$\phi_{2k+1}(x,y)+\psi_{2k+1}^2(x,y) = \frac{(a-d)^{3(k^2+k)}d^{k^2+k}}{2^{4(k^2+k)-1}(1-y)^{4(k^2+k)+1}}\Big((-1)^k(2k+1)y^{4(k^2+k)}+...\Big).$$

The corollary for odd n is clear from these last two lines. We omit the analagous calculation to show the result for even n. $\square$

4 Mean Value Theorem

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

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

$$\frac{1}{n^2}\sum_{i=1}^{n^2} x_i = \frac{1}{n} x_Q, \tag{4}$$

$$\frac{1}{n^2}\sum_{i=1}^{n^2} y_i = \frac{(-1)^{(n-1)/2}}{n} y_Q. \tag{5}$$

If n is even, then

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

Proof For odd n, the approach is similar to that used by Feng and Wu in [3]. From the above results about twisted Edwards division polynomials, we see $[n](x,y) = Q$ if and only if

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

In other words,

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

As seen in Proposition 1, 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 $Q \neq (0,1)$). 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, the result for the y-coordinates follows immediately.

The result for the x-coordinates 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

$$(\sqrt{a}x_Q, y_Q) = [n]((y_i, -\sqrt{a}x_i) + (-1, 0)) = [n](y_i, -\sqrt{a}x_i) + [n](-1, 0).$$

It is not hard to see that for odd n,

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

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

$$[n](y_i, -\sqrt{a}x_i) = (\sqrt{a}x_Q, y_Q)+((-1)^{(n-1)/2}, 0) = ((-1)^{(n-1)/2}y_Q, \sqrt{a}(-1)^{(n+1)/2}x_Q).$$

By our result for the y-coordinates, we then have

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

The result for the x-coordinates follows immediately.

We now show that if n is even, then $\sum_{i=1}^{n^2} y_i = 0$. Assuming this, by repeating our 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 1 again to see $\sum_{i=1}^{n^2} y_i = 0$, but we will a different technique.

Lemma 1 *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 $Q \neq (0, 1)$. Then*

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

Proof The points of order 4 on $E_{a,d}$ are the identity $(0, 1)$, the point $(0, -1)$ of order 2, and the points $(\frac{1}{\sqrt{a}}, 0)$ and $(-\frac{1}{\sqrt{a}}, 0)$. From this it is clear that the x and y-coordinates both sum to zero. □

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 2 *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 $[m]P = Q$, for some $Q \neq (0, 1)$. 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 $[n]R = S$, for some $S \neq (0, 1)$.*

Then given $(mn)^2$ points $T_1, T_2, ..., T_{(mn)^2}$ on $E_{a,d}$ such that $[mn]T_i = U$ for some $U \neq (0, 1)$. 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 2 we know the mean value for the 15-division points. It will be $\sum_{i=1}^{225} x_i = (15x_Q)$.

Combining Proposition 2 and Lemma 1 we can conclude by induction that whenever $n = 2^k$ we have $\sum_{i=1}^{n^2} x_{P_i} = 0 = \sum_{i=1}^{n^2} y_{P_i}$. The earlier results (4) and (5) for odd n can now be combined with Lemma 1 and Proposition 2 which shows our mean value theorem is true whenever n is even.

□

We remark that Theorem 1 was proved for points $Q \neq (0, 1)$. When $Q = (0, 1)$ then we claim $\sum_{i=1}^{n^2} x_i = 0 = \sum_{i=1}^{n^2} y_i = 0$. Let P_i be the n^2 points which satisfy $[n]P_i = (0, 1)$. 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. In this paper we showed similar results hold for both the x and y-coordinates on twisted Edwards curves.

Based on numerical examples, we conjecture 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), for $i = 1, .., n^2$, are the points such that $[n]P = Q \neq \infty$ on $E : y^2 = x^3 + Ax + B$, then

$$\frac{1}{n^2} \sum_{i=1}^{n^2} y_i = n y_Q. \tag{6}$$

We have been unable to prove this in general, although Wu [8] has proved it for $n = 2$. Feng and Wu's technique of using division polynomials fails in general 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 $\prod_{i=1}^{n^2}(y - y_i)$. However, by Proposition 2, the result (6) is true for n a power of 2. Thus to prove it in general requires establishing the case where n is an odd prime. This is an open problem. It would be interesting to see if mean value theorems can be found for other models of elliptic curves, such as Hessian curves or Jacobi intersections.

References

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

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

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

[4] 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.

[5] 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.

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

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

[8] H. Wu, Personal correspondence with the author, 2010.