EDWARDS COORDINATES

RAYMOND FRIEND

Abstract. A normal form for elliptic curves, introduced by Harold M. Edwards in 2007, quickly became well-known because of its convenient and complete addition formula, as well as its interesting parametric form. Every elliptic curve over a field of characteristic greater than 2 is birationally equivalent to a curve in Edwards form over an appropriate extension of the field. Bernstein and Lange introduced a broader analysis of this form, while also comparing multiple operations in Edwards form to other coordinate systems, concluding Edwards form could outperform many of the leading algorithms of the time. The application to cryptography is emphasized in Section 5.

Contents

1. Introduction

There exists a broad field of study on cryptography that has embraced the varied use of elliptic curve mathematics partly for its improved efficiency in forward encryption over other methods. Harold Edwards, in 2007, published results on a particular family of curves over finite fields that is of particular interest in elliptic curve cryptography. Bernstein and Lange developed many of their applications in the same year, providing algorithms for many types of calculations used in these applications, and compared their algorithms to the fastest algorithms associated with other coordinate systems for elliptic curves. Their algorithms bested the majority of the previously known algorithms, providing a new wave of efficiency to elliptic curve cryptography.

Edwards curves are powerful because over some sufficiently extended field, every elliptic curve is birationally equivalent to a curve in Edwards form. Moreover, the addition formula for elliptic curves translated to the language of Edwards coordinates is complete, meaning it has the same form no matter the parameters. Doubling, general addition, etc. are all treated equally.

Finally, Edwards curve admit a relatively natural parameterization, and analyzing

Date: December 14, 2017.

the parameterization gives a succinct, numerical method for classifying all elliptic curves by Edwards curves.

2. Elliptic Curves

Definition 2.1. An *elliptic curve* over field k is presented with k along with a curve of the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 3 or 4 with distinct roots that has coefficients in an algebraic number field.

Definition 2.2. An *elliptic function field* is the field of rational functions on a specified elliptic curve. Elements are represented by expressions of the form $r(x) + s(x)z$, where $r(x)$ and $s(x)$ are rational functions of x with coefficients in k.

We define two curves to be birationally equivalent if their fields of rational functions are isomorphic. I.e. we could construct rational transformations in one coordinate system to the other, as well as the inverse transformation.

Our study of elliptic curves may be realized over any field of characteristic not 2 or 3, and we wish to have some group structure over these curves. The following operation is natural for any smooth, irreducible cubic curve $F \subset \mathbb{CP}^2$.

Definition 2.3. Let $F \subset \mathbb{CP}^2$ be an irreducible curve, and let k be a field. For $P \neq Q \in F$ over k, denote by $\overline{PQ}$ the line in $\mathbb{CP}^2$ passing through P and Q. Define $P \star Q$ as follows

- If $\overline{PQ}$ is not tangent at either P nor Q to F, then since lines intersect cubics at 3 points, counting multiplicity, there exists a third point $R \in F \cap \overline{PQ} \setminus \{P, Q\}$. Then
$$P \star Q := R.$$
- When $\overline{PQ}$ is tangent to F at P (or Q) and $P \neq Q$, then define
$$P \star Q := P \text{ (or } Q)$$
- If $P = Q$, then $\overline{PQ}$ is definitely tangent to F at P. Treat this point as a tangent point of multiplicity 2 and find the third intersection point R on F and define $P \star P := R$, as in the first case.

One can prove the following properties of this binary operation easily.

Proposition 2.4. *$\star$ satisfies the properties. For any P, Q, R, S on the curve F,*

(i) $P \star Q = Q \star P$,
(ii) $(P \star Q) \star P = Q$,
(iii) $((P \star Q) \star R) \star S = P \star ((Q \star S) \star R)$.

Now we will define the addition operation on the curve F over field k and prove that $(F(k), +)$ is an abelian group.

Definition 2.5. Let $\infty = [0 : 1 : 0]$ be the infinite point in $\mathbb{CP}^2$. Then define the operation $+$ on F by $P + Q = (P \star Q) \star \infty$.

Lemma 2.6. *The points of F form an abelian group under the operation $+$. The identity element of the group is ∞, and an element P has inverse $-P = P \star (\infty \star \infty)$.*

Proof. We verify that $(F, +)$ satisfies the axioms for an abelian group. Commutativity easily follows from the commutativity of $\star$ in 2.4(i), and commutativity of $\star$ also implies ∞ is the identity element. Associativity follows from 2.4(iii):

$$\begin{aligned}(P+Q)+R &= (((P\star Q)\star\infty)\star R)\star\infty \\ &= (P\star((Q\star R)\star\infty))\star\infty \\ &= (P\star(Q+R))\star\infty = P+(Q+R).\end{aligned}$$

Finally, each element P has an inverse $-P = P\star(\infty\star\infty)$ since

$$\begin{aligned}P+(-P) &= P+(P\star(\infty\star\infty)) \\ &= (P\star(P\star(\infty\star\infty)))\star\infty \\ &= ((P\star(\infty\star\infty))\star P)\star\infty = (\infty\star\infty)\star\infty = \infty.\end{aligned}$$

□

Geometrically, general addition on an elliptic curve follows the procedure: pick summands P and Q; draw $\overline{PQ}$ and find its third intersection with F, point $-R$; then take the vertical line passing through R and find the second intersection with F: point $-R$. Then $P+Q = -R$. This method of addition on elliptic curves composes the Weierstrass form for addition on elliptic curves. Obviously there are multiple cases for addition depending on the choice of $P, Q \in F$. Algebraically, and without proof, this type of addition can be described on the curve $y^2 = x^3 - px - q$ over the field k whose characteristic is neither 2 nor 3, points $P = (x_P, y_P), Q = (x_Q, y_Q)$, slope of $\overline{PQ}$ being s, and $R = -(P+Q)$ by

$$x_R = s^2 - x_P - x_Q, \qquad y_R = y_P + s(x_R - x_P).$$

3. Edwards Coordinates

Definition 3.1. The equation of an *Edwards curve* over a field k which does not have characteristic 2 is

$$\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$$

for some scalar $\overline{d} \in K \setminus \{0, 1\}$. Alternatively, one may define an Edwards curve by the form

$$u^2 + v^2 = c^2(1 + du^2v^2)$$

where $c, d \in k$ with $cd(1 - d \cdot c^4) \neq 0$.

It is possible to restrict our attention to the $c = 1$ case without any loss of generality by reparameterizing: if $\overline{d} = dc^4$, then define $\overline{u} = u/c$ and $\overline{v} = v/c$. It is easy to check the isomorphism/birational equivalence. Bernstein and Lange remark that for computational purposes, minimizing c is often much more useful than minimizing d; moreover, despite an Edwards curve being easily transformable to an isomorphic Edwards curve having $c = 1$, there may be applications in which $c \neq 1$. This could occur, for example, for a curve with a fairly small c and $d = 1$ having smaller computational steps in the costs of multiplying by c and multiplications by d than those on the curve with $\overline{c} = 1$ and $\overline{d} = c^4$.
Now we wish to find which elliptic curves may be represented by an Edwards curve. Bernstein and Lange propose the following:

Theorem 3.2. *Let k be a field with characteristic not 2. Let E be an elliptic curve over k such that the group $E(k)$ has an element of order 4. Then*

(i) *there exists* $d \in k \setminus \{0,1\}$ *such that the curve* $u^2+v^2 = 1+du^2v^2$ *is birationally equivalent over* k *to a quadratic twist of* E.
(ii) *If* $E(k)$ *has a unique element of order* 2, *then there is a nonsquare* $d \in k$ *such that the curve* $u^2+v^2 = 1+du^2v^2$ *is birationally equivalent over* k *to a quadratic twist of* E.
(iii) *If* k *is finite and* $E(k)$ *has a unique element of order* 2, *then there is a nonsquare* $d \in k$ *such that the curve* $u^2+v^2 = 1+du^2v^2$ *is birationally equivalent over* k *to* E.

Proof. Write E in "long Weierstrass form" $\bar{s}^2 + \bar{a}_1\bar{r}\bar{s} + \bar{a}_3\bar{s} = \bar{r}^3 + \bar{a}_2\bar{r}^2\bar{a}_4\bar{r}\bar{a}_6$. We reduce this by defining $s = \bar{s} + (\bar{a}_1\bar{r} + \bar{a}_3)/2$. Moreover, let $P = (r_1, s_1)$ be an element of order 4 on $E(k)$. Let $2P = (r_2, 0)$. Then define $r = \bar{r} - r_2$, making $s = \bar{s} + (\bar{a}_1(r+r_2) + \bar{a}_3)/2$. Then we obtain a curve of the form

$$s^2 = r^3 + a_2r^2 + a_4r,$$

where $a_1 = a_3 = a_6 = 0$, $a_2 = \bar{a}_2 + \bar{a}_1^2/4 + 3r_1, a_4 = \bar{a}_4 + \bar{a}_1\bar{a}_3/2 + 2(\bar{a}_2 + \bar{a}_1^2/4 + 3r_1) + 3r_1^2$, and $2P = (0,0)$. Next, we wish to express a_2, a_4 in terms of r_1, s_1. Note that $s_1 \neq 0$ or else P has a lesser order of 2. Thus, $r_1 \neq 0$. The equation $2P = (0,0)$ means that the tangent line to E at P passes through $(0,0)$, i.e. $s_1 - 0 = (r_1 - 0)\lambda$, with λ being the tangent slope $(3r_1^2 + 2a_2r_1 + a_4)/2s_1$. Therefore,

$$s_1 = r_1\lambda = \frac{r_1(3r_1^2 + 2a_2r + a_4)}{2s_1},$$

$$\therefore r_1^2 = a_4.$$

Furthermore, $a_2 = \frac{s_1^2 - r_1^3 - a_4r_1}{r_1^2} = s_1^2/r_1^2 - 2r_1$. Let $d = 1 - r_1^3/s_1^2$. Then $a_2 = 2(1+d)/(1-d)r_1$, where $d \neq 0, 1$, since if $d = 0$ then $4r_1^3 = s_1^2$ implies

$$r^3 + a_2r^2 + a_4r = r^3 + 2r_1r^2 + 2r_1^2r = r(r+r_1)^2,$$

a contradiction to E being elliptic and having distinct roots. If d is a square, then the point $\left(r_1(\sqrt{d}+1)/(\sqrt{d}-1), 0\right)$ is another point of order 2 on $E(k)$. Now consider the two quadratic twists of E:

$$E' : \left(\frac{r_1}{1-d}\right)s^2 = r^3 + a_2r^2 + a_4r, \qquad E'' : \left(\frac{dr_1}{1-d}\right)s^2 = r^3 + a_2r^2 + a_4r.$$

If k is finite, and if d is not a square in k, then either $\frac{r_1}{1-d}$ or $\frac{dr_1}{1-d}$ is a square in k, since the product of non-squares (e.g. d and $\frac{r_1}{1-d}$) in a finite field is a square in the field. So E is equivalent to either E' or E''.
Now substitute $x = r/r_1$ and $y = s/r_1$. Then we see

$$E' \cong \frac{1}{1-d}y^2 = x^3 + 2\frac{1+d}{1-d}x^2 + x$$
$$E'' \cong \frac{d}{1-d}y^2 = x^3 + 2\frac{1+d}{1-d}x^2 + x.$$

We will show that $u^2+v^2 = 1+du^2v^2$ is equivalent to $\frac{1}{1-d}y^2 = x^3 + 2\frac{1+d}{1-d}x^2 + x$, which is equivalent to E'. Define the rational map $(x,y) \mapsto (u,v)$, $u = 2x/y$, $v = (x-1)/(x+1)$. There are finitely many exception points to this map, satisfying

$(x+1)y = 0$. We will show one of the directions for birational equivalence:

$$\begin{aligned}\left(2\frac{x}{y}\right)^2 + \left(\frac{x-1}{x+1}\right)^2 &= 1 + d\left(2\frac{x}{y}\right)^2\left(\frac{x-1}{x+1}\right)^2 \\ \implies 0 &= 4x^2(x+1)^2 + y^2(x-1)^2 - (x+1)^2y^2 - 4dx^2(x-1)^2 \\ &= 4(1-d)x^4 + 8(1+d)x^3 - 4xy^2 + 4x^2(1-d) \\ \therefore \frac{1}{1-d}y^2 &= x^3 + 2\frac{1+d}{1-d}x^2 + x(1-d).\end{aligned}$$

The inverse map $x = (1+v)(1-v), y = 2(1+v)/u(1-v)$ also gives us the backwards equivalence, with finitely many exceptions satisfying $u(1-v) = 0$. Now, substituting $d \mapsto 1/d$ and $x \mapsto -x$, then $u^2 + v^2 = 1 + (1/d)u^2v^2$ is birationally equivalent to $d/(1-d)y^2 = x^3 + 2(1+d)/(1-d)x^2 + x$, which is equivalent to E''. In summary, the curve $u^2 + v^2 = 1 + du^2v^2$ is equivalent to a quadratic twist E' of E. If E has a unique point of order 2 then d is a nonsquare and $u^2+v^2 = 1+du^2v^2$ is equivalent to a quadratic twist E' of E. Lastly, if k is finite and E has a unique point of order 2 then d is a nonsquare so E is isomorphic to E' or to E''; thus E is birationally equivalent to $u^2 + v^2 = 1 + du^2v^2$ or to $u^2 + v^2 = 1 + (1/d)u^2v^2$. □

As will be discussed in a further section, elliptic curves are very popular in cryptographic applications. Cryptography involves performing operations over finite fields, and every finite field of characteristic not 2 contains a nonsquare element, so part (iii) of the previous theorem applies to any cryptographic application. In Edwards' original paper, he showed the following:

Proposition 3.3. *An elliptic function field is birationally equivalent to the field of rational functions on $x^2 + y^2 = a^2 + a^2x^2y^2$ for some $a \in k$ such that $a^5 \neq a$.*

As seen, Edwards' original "Edwards" curve is of a slightly different form (namely, $c = a, d = 1$). We wonder whether this form is equivalent to either of the two forms $u^2 + v^2 = c^2(1 + du^2v^2)$ or $\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$. Recall we were able to show the equivalence of the two Edwards forms introduced in 3 by means of the birational equivalence $\overline{u} = u/c, \overline{v} = v/c, \overline{d} = dc^4$. The inverse transformation does not require any field extensions either. However, let us try to produce a map between $u^2 + v^2 = c^2(1 + du^2v^2)$ and $x^2 + y^2 = a^2 + a^2x^2y^2$. Notice $u = x/d^{1/4}$, $v = y/d^{1/4}, c = a/d^{1/4}$ produces the correct mapping, but requires a field extension of to $k\left(\sqrt[4]{d}\right)$. We can construct the map between the remaining pair $\overline{u}^2 + \overline{v}^2 = 1 + \overline{d}\overline{u}^2\overline{v}^2$ and $x^2 + y^2 = a^2 + a^2x^2y^2$ is $\overline{u} = x/(cd^{1/4})$, $\overline{v} = y/(cd^{1/4})$, $\overline{d} = a^4$, which still requires the same field extension.

4. Addition on an Edwards Curve

The following is the addition formula originally posed by Edwards, which applies to an Edwards curve with $d = 1$ and $c = a$.

Theorem 4.1. *If a is a constant for which $a^4 \neq 1$, then the addition formula for the elliptic curve $x^2 + y^2 = a^2 + a^2x^2y^2$ is*

$$X = \frac{1}{a} \cdot \frac{x_1y_2 + x_2y_1}{1 + x_1y_1x_2y_2}, \qquad Y = \frac{1}{a} \cdot \frac{y_1y_2 - x_1x_2}{1 - x_1y_1x_2y_2}.$$

What makes the above formula so special is its almost symmetric treatment of x and y, as well as its admission of a simple identity element: $(0, c)$. Moreover, Edwards goes on to show that all elliptic curves over a non-binary finite field may be transformed to Edwards form. Some require a field extension for the transformation, but some elliptic curves have transformations defined over the original field. Bernstein and Lange broadened Edwards' addition formula to the general Edwards curve with $cd(1 - dc^4) \neq 0$.

Theorem 4.2. *For a fixed field k of characteristic different than 2, fix $c, d \in k$ such that $cd(1 - dc^4) \neq 0$. Then the Edwards addition law is*

$$(u_1, v_1), (u_2, v_2) \mapsto \left(\frac{u_1v_2 + v_1u_2}{c(1 + du_1u_2v_1v_2)}, \frac{v_1v_2 - u_1u_2}{c(1 - du_1u_2v_1v_2)} \right) = (u_3, v_3).$$

on the Edwards curve $u^2 + v^2 = c^2(1 + du^2v^2)$ over k. We claim (u_3, v_3) lies on the curve $u^2 + v^2 = c^2(1 + du^2v^2)$. We are under the assumption that $du_1u_2v_1v_2 \notin \{-1, 1\}$.

Proof. Define $T = (u_1v_2+v_1u_2)^2(1-du_1u_2v_1v_2)^2+(v_1v_2-u_1u_2)^2(1+du_1u_2v_1v_2)^2-d(u_1v_2 + v_1u_2)^2(v_1v_2 - u_1u_2)^2$. We claim that

$$T = (u_1^2 + v_1^2 - (u_2^2 + v_2^2)du_1^2v_1^2) \cdot (u_2^2 + v_2^2 - (u_1^2 + v_1^2)du_2^2v_2^2).$$

This can be checked by direct calculation. Next, combine the two conditions on $(u_1, v_1), (u_2, v_2)$:

$$\begin{aligned} u_1^2 + v_1^2 &= c^2(1 + du_1^2v_1^2) \\ - \quad [(u_2^2 + v_2^2)du_1^2v_1^2 &= c^2(1 + du_2^2v_2^2)du_1^2v_1^2] \\ \hline u_1^2 + v_1^2 - (u_2^2 + v_2^2)du_1^2v_1^2 &= c^2(1 - d^2u_1^2u_2^2v_1^2v_2^2) \\ &= u_2^2 + v_2^2 - (u_1^2 + v_1^2)du_2^2v_2^2. \end{aligned}$$

The final equality follows by similar combination of equations using a different factor: $du_2^2v_2^2$. It follows that $T = c^4(1 - d^2u_1^2u_2^2v_1^2v_2^2)^2$. Finally, we if $(u_1, v_1) + (u_2, v_2) = (u_3, v_3)$, we have

$$\begin{aligned} &u_3^2 + v_3^2 - c^2du_3^2v_3^2 \\ &= \frac{(u_1v_2 + v_1u_2)^2}{c^2(1 + du_1u_2v_1v_2)^2} + \frac{(v_1v_2 - u_1u_2)^2}{c^2(1 - du_1u_2v_1v_2)^2} - \frac{c^2d(u_1v_2 + v_1v_2)^2(v_1v_2 - u_1u_2)^2}{c^4(1 + du_1u_2v_1v_2)^2)(1 - du_1u_2v_1v_2)^2} \\ &= \frac{T}{c^2(1 + du_1u_2v_1u_2)^2(1 - du_1u_2v_1v_2)^2} = \frac{T}{c^2(1 - d^2u_1^2u_2^2v_1^2v_2^2)^2} = c^2. \end{aligned}$$

Thus, $(u_3, v_3) \in F(k)$. □

Remark 4.3. Notice, as in Edwards' original formula, $(0, c)$ is the neutral element of the more general addition law. Notice also that $(0, -c)$ has order 2, while $(c, 0)$ and $(-c, 0)$ have order 4.

Theorem 4.4. *For a fixed field k of characteristic different than 2, fix $c, d \in k$ such that $cd(1 - dc^4) \neq 0$. Let $e = 1 - dc^4$, and E be the elliptic curve*

$$E : \frac{1}{e}x^2 = y^3 = \left(\frac{4}{e} - 2 \right) x^2 + x.$$

Let $(u_3, v_3) = (u_1, v_1) + (u_2, v_2)$. *For each* $i \in \{1, 2, 3\}$ *define* P_i *as follows:*

$$P_i := \begin{cases} \infty & \text{if } (u_i, v_i) = (0, c) \\ (0, 0) & \text{if } (u_i, v_i) = (0, -c) \\ (x_i, y_i) & \text{if } u_i \neq 0, \end{cases}$$

where $x_i = (c + v_i)/(c - v_i)$ *and* $y_i = 2c(c + v_i)/(c - v_i)u_i$. *Then* $P_i \in E(k)$ *and* $P_1 + P_2 = P_3$.

A full proof of this fact exists in Bernstein and Lange's work. The proof is split into many cases, but below is a partial look into it; specifically, under the assumption that $x_1 \neq x_2$.

Partial Proof of Thm 4.4. If $x_1 \neq x_2$, then the standard addition formula says

$$(x_1, y_1) + (x_2, y_2) = (r, s),$$

where $\lambda = (3x_1^2 + 2(4/e - 2)x_1 + 1)/((2/e)y_1)$, $r = (1/e)\lambda^2 - (4/e - 2) - 2x_1$, and $s = \lambda(x_1 - r) - y_1$. It is left to check that $(r, s) = (x_3, y_3)$. The left side has a relatively complicated dependence on (u_1, v_1), and (u_2, v_2), so it takes a lot of algebraic manipulation to show their equality. Nevertheless, addition matches between standard formulas and Edwards formulas, showing that Edwards coordinates provide a unique opportunity to perform addition on elliptic curves. Notice that the only chance of this formula being incomplete is when the denominator of either coordinate is zero, or $du_1u_2v_1v_2 \in \{-1, 1\}$. □

What more, if d is not a square, it can be shown that there are no exceptional points in Edwards' addition formula, i.e. the Edwards addition law is complete.

Theorem 4.5. *Let* k *be a field in which* $2 \neq 0$. *Let* c, d, e *be nonzero elements of* k *with* $e = 1 - dc^4$. *Assume that* d *is not a square in* k. *Let* u_1, v_1, u_2, v_2 *be elements of* k *for which* $u_1^2 + v_1^2 = c^2(1 + du_1^2v_1^2)$ *and* $u_2^2 + v_2^2 = c^2(1 + du_2^2v_2^2)$. *Then* $du_1u_2v_1v_2 \neq \pm 1$.

Proof. Let $\epsilon = du_1u_2v_1v_2$, and suppose $\epsilon \in \{-1, 1\}$. then $u_1, u_2, v_1, v_2 \neq 0$. Furthermore,

$$du_1^2v_1^2(u_2^2+v_2^2) = c^2(du_1^2v_1^2+d^2u_1^2u_2^2v_1^2v_2^2) = c^2(du_1^2v_1^2+\epsilon^2) = c^2(1+du_1^2v_1^2) = u_1^2+v_1^2.$$

Thus,

$$\begin{aligned}(u_1 + \epsilon v_1)^2 = u_1^2 + v_1^2 + 2\epsilon u - 1v_1 &= du_1^2v_1^2(u_1^2 + v_1^2) + 2u_1v_1du_1u_2v_1v_2 \\ &= du_1^2v_1^2(u_1^2 + 2u_2v_2 + v_1^2) = du_1^2v_1^2(u_2 + v_2)^2.\end{aligned}$$

With this, if $u_2 + v_2 \neq 0$, then $d = ((u_1 + \epsilon v_1)/(u_1v_1(u_2 + v_2)))^2$, meaning d is a square. This is a contradiction. Similarly, if $u_2 - v_2 \neq 0$, then $d = ((u_1 - \epsilon v_1)/(u_1v_1(u_2 - v_2)))^2$, meaning d is a square, again a contradiction. However, if both $u_1 + v_1 = 0 = u_1 - v_1$, then both are zero, which is another contradiction. □

5. Applications

For assessing the efficiency of the following algorithms, I will use the same notation as Bernstein and Lange, as I believe it is standard to count different operations with as much detail as possible in order to be able to discern computational-time differences between algorithms for different computing systems. Separate tallies of the number of general multiplications (costing **M**), squarings (each costing **S**),

multiplications by c (each costing $\mathbf{C}$), multiplications by d (each costing $\mathbf{D}$), and additions/subtractions (each costing $\mathbf{A}$). Each of these costs depend on the computing platform, the choice of a finite field, and on the choice of c and d.

We are specifically interested in analyzing the algorithm for Edwards addition. Using the affine formula introduced in the previous section is not suitable for cryptographic purposes due to side-channel attacks (or physical indications of private information). Notice also that in the Edwards addition law, two inversion operations appear. Inversion typically runs one to two orders of magnitude slower than multiplication for a computing system, so it is undesirable to have such operations. Luckily, expressing Edwards addition in projective coordinates eliminates inversions. Let's use the projective coordinates $(X : Y : Z)$ to represent the affine coordinate $(x, y) = (X/Z, Y/Z)$. Other systems have different relations, such as the Jacobian system with $(x, y) = (X/Z^2, Y/Z^3)$.

In projective homogeneous coordinates, we homogenize the affine Edwards curve equation $x^2 + y^2 = c^2(1 + dx^2y^2)$ to $(X^2 + Y^2)Z^2 = c^2(Z^4 + dX^2Y^2)$. The neutral element is $(0 : c : 1)$, while the inverse of an element $(X : Y : Z)$ is $(-X : Y : Z)$. In projective homogeneous coordinates, addition is given by $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$, where

$$\begin{aligned}
X_3 &= Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)\left((X_1 + Y_1)(X_2 + Y_2) - X_1X_2 - Y_1Y_2\right),\\
Y_3 &= Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2),\\
Z_3 &= c \cdot (Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2).
\end{aligned}$$

One can check that $x_3 = X_3/Z_3$ and $y_3 = Y_3/Z_3$ to verify the addition formula in projective coordinates matches the definition of that on the affine curve. Obviously, for the sake of mathematical simplicity,

$$X_3 = Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)\left(X_1Y_2 + Y_1X_2\right).$$

However, because the quantities X_1Y_1, X_2Y_2, $X_1 + Y_1$, and $X_2 + Y_2$ are already computed for Y_3 and Z_3, we do not need to perform X_1Y_2 nor Y_1X_2. We may observe the full procedure by explicitly providing the sequence of operations and registers involved with a general addition calculation.

Addition Algorithm: Let R_1, R_2, R_3 hold X_1, Y_1, Z_1 initially, R_4, R_5, R_6 hold X_2, Y_2, Z_2 initially, and let R_7, R_8 be temporary registers, with c and d being constants. Perform

$$\begin{gathered}
R_3 \cdot R_6 \to R_3; R_1 + R_2 \to R_7; R_4 + R_5 \to R_8; R_1 \cdot R_4 \to R_1; R_2 \cdot R_5 \to R_2;\\
R_7 \cdot R_8 \to R_7; R_7 - R_1 \to R_7; R_7 - R_2 \to R_7; R_7 \cdot R_3 \to R_7; R_1 \cdot R_2 \to R_8;\\
d \cdot R_8 \to R_8; R_2 - R_1 \to R_2; R_2 \cdot R_3 \to R_2; R_3^2 \to R_3; R_3 - R_8 \to R_1;\\
R_3 + R_8 \to R_3; R_2 \cdot R_3 \to R_2; R_3 \cdot R_1 \to R_3; R_1 \cdot R_7 \to R_1; c \cdot R_3 \to R_3.
\end{gathered}$$

Registers R_1, R_2, R_3 end containing X_3, Y_3, Z_3, respectively. One may count this algorithm uses $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{C} + 1\mathbf{D} + 7\mathbf{A}$.

A similar algorithm slightly changes the operations involved, obtaining

$$\begin{gathered}
Z_1Z_2(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2),\ Z_1Z_2(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2),\ \text{and}\\
(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)
\end{gathered}$$

as linear combinations of $(Z_1Z_2)^2, (Z_1^2Z_2^2)^2, (dX_1X_2Y_1Y_2)^2, (Z_1Z_2 + Z_1^2Z_2^2)^2$, and $(Z_1Z_2 + dX_1X_2Y_1Y_2)^2$. This changes $10\mathbf{M} + 1\mathbf{S}$ to $7\mathbf{M} + 5\mathbf{S}$. In many systems, the ratio $\mathbf{S}/\mathbf{M} < 3/4$, meaning this change is favorable for running time. More algorithms exist for mixed addition (where $Z_2 = 1$), and doubling (where $(X_1 : Y_1 : Z_1) = (X_2 : Y_2 : Z_2)$). For instance, an algorithm for doubling can be reduced to $3\mathbf{M} + 4\mathbf{S} + 5\mathbf{C} + 6\mathbf{A}$ with two temporary registers; if temporary registers are expensive, a variation using only one increases the number of additions to seven: $7\mathbf{A}$.

Coordinate systems on elliptic curves is a game of applying various "trivial" manipulations to formulas until finding an efficient algorithm for performing a desired operation. For instance, Edwards coordinates would not be so revolutionary (in cryptography) without the addition algorithm given above for its projective coordinate representation. A decade ago, Bernstein and Lange compared their Edwards addition algorithm to those of previously developed representations. Below is a subset of their analysis.

System	ADD	(1,1)	(0.8,0.5)	(0.8,0)
Jacobian	$11\mathbf{M} + 5\mathbf{S}$	$16\mathbf{M}$	$15\mathbf{M}$	$15\mathbf{M}$
Projective	$12\mathbf{M} + 2\mathbf{S}$	$14\mathbf{M}$	$13.6\mathbf{M}$	$13.6\mathbf{M}$
Jacobi Quartic	$10\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$	$14\mathbf{M}$	$12.9\mathbf{M}$	$12.4\mathbf{M}$
Hessian	$12\mathbf{M}$	$12\mathbf{M}$	$12\mathbf{M}$	$12\mathbf{M}$
Edwards	$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$	$12\mathbf{M}$	$11.3\mathbf{M}$	$10.8\mathbf{M}$

The ordered pairs in the last few columns represent possible values for the ratios $(\mathbf{S}/\mathbf{M}, \mathbf{D}/\mathbf{M})$. Regardless, Edwards addition will always perform at least as well as any of the other addition algorithms for elliptic curves in this chart.

Elliptic curves are generally used for cryptography due to their group structure, which immediately implies the Discrete Logarithm problem on the set. A public observer can be aware of a curve being generated by point $P \in E(k)$ and aware of a point $Q \in E(k)$ (i.e. a multiple of P). Information is leaked if the observer can find the positive integer n such that $Q = nP$. However, this is a nontrivial task that is very hard to compute outside of a few specific, degenerate curves. The discrete logarithm problem applies to any finite field. Another popular example is finding the factors of a very large product of two large primes. Cryptography relies on processes which can be computed efficiently in one direction and ability of choice, but may not be undone efficiently or all too methodically. Authors of elliptic curve algorithms on $E(k)$ wish to make this forward process as efficient as possible, while also ensuring the chosen elliptic curves or representations are not vulnerable for attacks that compromise the security of the discrete logarithm problem.

Since 2007, mathematicians have developed inverted Edwards coordinates (which do not offer complete, but strongly unified, addition formulas), and extended coordinates for Edwards curves. The coordinates in inverted Edwards are of the form $(x, y) = (Z/X, Z/Y)$, and offer a slightly faster set of operations than the standard coordinates. Extended Edwards coordinates are even faster than inverted coordinates, and are of the form $ax^2 + y^2 = 1 + dx^2y^2$, and are all twists of Edwards curves, whose $a = 1$.

6. Parameterization

Another application to Edwards form requires some more theory. Parameterizations of elliptic curves are of particular interest for calculations on and classifications of them. Edwards proposes a particular function given one parameter τ that parameterizes elliptic curves in Edwards form over $t \in \mathbb{C}$. Because Edwards form treats x and y identically, they may be parameterized by meromorphic functions only different by some phase shift, similar to how $\sin(t)$ and $\cos(t) = \sin(t + \pi/2)$ are essentially the same function, only off by some phase shift, that parameterize ellipses.

Theorem 6.1. *Given a complex $\tau \in \mathcal{H}$, where $\mathcal{H}$ is the upper half plane, then*

$$\psi(t) = \frac{\sum_{n\ odd} e^{i\pi\left(\frac{n^2}{2}\cdot\tau + nt\right)}}{\sum_{n\ even} e^{i\pi\left(\frac{n^2}{2}\cdot\tau + nt\right)}}$$

defines a meromorphic function of a complex variable t with the following properties:

- *(i)* $\psi(t+1) = -\psi(t)$.
- *(ii)* $\psi(t+\tau) = 1/\psi(t)$.
- *(iii) The periods 2 and 2τ form a period basis of ψ.*
- *(iv) The only zeros of $\psi(t)$ in the period parallelogram $\{r + s\tau : \leq r < 2, 0 \leq s < 2\}$ are at $1/2$ and $3/2$, meaning the only poles in this parallelogram are at $1/2 + \tau$ and $3/2 + \tau$.*
- *(v)* $\psi(\tau/2) = 1$.
- *(vi)* $\psi(\tau/2 - 1/2) = i$.
- *(vii) Properties (i)-(v) uniquely determine $\psi(t)$.*

The proof of this theorem is very straightforward and only requires a few substitutions and extraneous multiplications by $e^{i\pi\tau/2+t}$ to the numerator and denominator in the proof of (i). The final item requires an argument about the quotient of two doubly periodic meromorphic functions with the same poles and zeros being constant.

If τ is given, let $\phi(t) = \psi(t - 1/2)$. Notice $\phi(t)^2 + \psi(t)^2$ and $1 + \phi(t)^2\psi(t)^2$ are doubly periodic functions with periods $2, 2\tau$, and same singularities. This means their quotient is constant. At $t = 0$, we have this constant is $\psi(0)^2$. Therefore, $\phi(t)^2 + \psi(t)^2 = \psi(0)^2 + \psi(0)^2\phi(t)^2\psi(t)^2$, meaning the map $t \mapsto (\phi(t), \psi(t))$ for a given τ maps the complex t-plane in a doubly periodic way onto the Riemann surface $x^2 + y^2 = a^2 + a^2x^2y^2$ for $a = \psi(0)$. We have reduced the problem of parameterizing $x^2 + y^2 = a^2 + a^2x^2y^2$ to finding τ for given a such that

$$a = \frac{\sum_{n\ \text{odd}} e^{\frac{i\pi n^2}{2}\cdot\tau}}{\sum_{n\ \text{even}} e^{\frac{i\pi n^2}{2}\cdot\tau}}.$$

Without going too much further into the analysis, I will present some results. It is possible to make sense of a fundamental domain of a under the modular group $\mathrm{PSL}(2, \mathbb{Z})$. In fact,

Proposition 6.2. *The elliptic function field determined by $x^2 + y^2 = a^2 + a^2x^2y^2$ is equivalent to the one determined by $x^2 + y^2 = b^2 + b^2x^2y^2$ whenever b has one of the 24 values*

$$i^\epsilon a, \qquad \frac{i^\epsilon}{a}, \qquad i^\epsilon \cdot \frac{a-1}{a+1}, \qquad i^\epsilon \cdot \frac{a+1}{a-1}, \qquad i^\epsilon \cdot \frac{a-i}{a+i}, \qquad i^\epsilon \cdot \frac{a+i}{a-i},$$

where i is a square root of -1 that is to be adjoined, if necessary, to the field of constants, and where $\epsilon \in \{0, 1, 2, 3\}$.

Proof. The values listed for b are the orbit of a under the group of fractional linear transformations of the Riemann sphere generated by the two transformations $a \mapsto ia$ and $a \mapsto \frac{a-1}{a+1}$. This group is actually isomorphic to the group of the cube; the first map permutes $1 \mapsto i \mapsto -1 \mapsto -i \mapsto 1$ cyclically, leaving $0, \infty$ fixed, while the second permutes $1 \mapsto 0 \mapsto -1 \mapsto \infty \mapsto 1$ cyclically, leaving $\pm i$ fixed. The proposition will be proved if the function field of $x^2 + y^2 = a^2 + a^2x^2y^2$ is shown to be equivalent to the two function fields obtained by replacing a with its image under the two generators $a \mapsto ia$ and $a \mapsto \frac{a-1}{a+1}$. For this, it will suffice to show that there exists a fractional linear transformation that carries $(a, -a, 1/a, -1/a)$ to the set $(b, -b, 1/b, -1/b)$, which is true since $x \mapsto ix$ is such a fractional linear transformation in the first case, and $x \mapsto \frac{x-1}{x+1}$ is so in the second. □

The homomorphism from the modular group to the 24 fractional linear transformations of a has kernel which is a normal subgroup of index 24. We can show that $\phi'(t) = \mu \cdot \psi(t)(1 - a^2\phi(t)^2)$ for some constant $\mu \in \mathbb{C}$. Then

$$\tau = \frac{\int_0^i \frac{dx}{y(1-a^2x^2)}}{\int_0^a \frac{dx}{y(1-a^2x^2)}}.$$

This quotient of path integrals in the domain of a is evaluated by means of some bisection method which follows by the doubling formula obtained from 4.1:

$$\phi(2t) = \frac{1}{a} \cdot \frac{2\phi(t)\psi(t)}{1 + \phi(t)^2\psi(t)^2}, \qquad \psi(2t) = \frac{1}{a} \cdot \frac{\psi(t)^2 - \phi(t)^2}{1 - \phi(t)^2\psi(t)^2}.$$

The bisection method relies on gathering $(\phi(t), \psi(t))$ from $(\phi(2t), \psi(2t))$.
Let $(\phi(2t), \psi(2t)) = (X, Y)$, and $(\phi(t), \psi(t)) = (x, y)$. Then $a(1-x^2y^2)Y = y^2 - x^2$, and multiplication of this equation by $1 - a^2x^2$ and use of $y^2(1 - a^2x^2) = a^2 - x^2$ gives

$$\begin{aligned} aY(1 - a^2x^2) - aYx^2(a^2 - x^2) &= a^2 - x^2 - x^2(1 - a^2x^2), \\ \iff (aY - a^2)x^4 + 2(1 - a^3Y)x^2 + (aY - a^2) &= 0. \end{aligned}$$

It follows that if x is a known solution to this equation, then so too will $-x, \pm 1/x$. Moreover, once x is known, $y^2 = (a^2 - x^2)/(1 - a^2x^2)$ is uniquely determined, with $X = \frac{1}{a}\frac{2xy}{1+x^2y^2}$ determining the sign of y. So knowledge of $(\phi(2t), \psi(2t))$ actually reduces to four possible values of $(\phi(t), \psi(t))$. Since we may take relatively small steps while traversing the integrals' paths, one can use distance information to choose the most likely value for the next step along the path. We have seen our method for parameterizing a given Edwards curve, and hence, any elliptic curve, over sufficiently extended fields.

References

[1] D. J. Bernstein, T. Lange. *Faster Addition and Doubling on Elliptic Curves*. 2007.
[2] H. M. Edwards. *A Normal Form for Elliptic Curves*. 2007.
[3] J. Hisel. *Addition Law on Elliptic Curves*. 2014.
[4] L. C. Washington. *Elliptic curves: Number Theory and Cryptography*. 2nd ed. Chapter 2, Section 6. 2008.