Elliptic Curve Cryptography: Theory for EdDSA

Lukas Prokop

July 2014 to April 2016

Contents

This article sums up research results from the field of Elliptic Curve Cryptography I needed for my implementation of EdDSA. An ECDH implementation was given, but I extended it for Curve25519. If you start working in that field, check out the Explicit Formula Database (maintained by Tanja Lange) and its referenced papers.

My main goal is to get an overview over parameters and cite them thoroughly.

Until 24th of June 2016, the birational equivalence formula $E_{E,a,d}$ to $E_{M,A,B}$ was incorrect as pointed out by Theo Fanuela Prabowo. I fixed it now. Thanks!

1 Theoretical background

The theoretical background of ECC lies in group theory and number theory.

1.1 Group

A *group* $(G, +)$ is a set of elements G associated with a binary operation creating a new element denoted $+$. The following axioms hold for the operation (with $a, b, c, e \in G$):

- closure: $\forall\, a, b : (a + b) \in G$
- associativity: $\forall\, a, b, c : (a + b) + c = a + (b + c)$
- identity: $\exists\, e\, \forall\, a : a + e = e + a = a$
- invertibility: $\forall\, a\, \exists\, b : a + b = b + a = e$

e is called *identity* element (eg. in integer groups, it's 0). An *abelian* group is a group satisfying

- commutativity: $\forall\, a, b : a + b = b + a$

Let $\cdot$ be multiplication resulting from repeated application of addition a variable number of times. Let $(G, \cdot)$ be a group itself and x^n is defined as follows:

$$\begin{aligned} x^0 &= \infty \\ x^{n+1} &= x^n \cdot x \quad \text{with } n \in \mathbb{N} \end{aligned}$$

∞ is the multiplicative identity element. The *order r of an element x* is defined as smallest integer $r > 0$ such that $x^r = \infty$. It holds that: If the group has one element g such that $\{g^n | n \in \mathbb{Z}\}$ yields all elements of the group, g is called *generator* of the cyclic group.

1.2 Ring

A *ring* is an abelian group with a second binary operation that is associative and distributive over the abelian group operation:

$$\forall\, a, b, c \in G : a \cdot (b + c) = a \cdot b + a \cdot c$$

The ring $\mathbb{Z}/n\mathbb{Z}$ of integers has *characteristic n.*

1.3 Field

A field is a non-zero commutative ring that contains a multiplicative inverse for every nonzero element. As a ring the nonzero elements form an abelian group under multiplication.

Example fields:

- real numbers ($\mathbb{R}$)

- complex numbers ($\mathbb{C}$)
- rational numbers ($\mathbb{Q}$)

Finite fields are fields with a finite number of elements. This includes integer modulo fields, which we will look at. Because the elements are enumerated 0 to $n-1$, you only need to specify the field size n to specify some field. Hence GF$(2^{255}-19)$ specifies a (Galois) field with field size $2^{255}-19$.

1.4 Elliptic curves

An elliptic curve is specified by a curve equation and some underlying fields for coordinates.

All coordinates satisfying the curve equation constitute a curve C. Coordinates are tuples with elements of the finite field. The equation of a curve depends on the selected coordinate system (per default: affine coordinate system). An addition law allows to add two points on a curve. A doubling law allows to double points on a curve. Scalar multiplication allows to multiply some point on a curve a variable number of times with itself. Every curve has a neutral point denoted ∞. It is specific for an addition law.

E(GF(p^k)) is the set of points which satisfy the curve equation (and the point at infinity). The cardinality $\left|\text{E}(\text{GF}(p^k))\right|$ defines the *order* of the curve. If you specify some element of E(GF(p^k)) as generator, this induces another subgroup where the following law holds:

$$h = \frac{\left|\text{E}(\text{GF}(p^k))\right|}{o}$$

h is called cofactor and o is the order of the generator[1].

The number of generators in a finite field GF(n) is $\varphi(n-1)$ where φ is Euler's totient function. This follows from the fact that the multiplicative group is cyclic [13]. In ECC mostly groups with n ($n=p$) being prime or n being binary ($n=2^k$) are considered. Recall that $\varphi(p) = p-1$ and $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$ holds. As far as the number of points on an elliptic curve are concerned, Hasse's theorem [15] provides an lower and upper bound. Even though there are multiple generators on a curve, we always talk about *the generator*, because negotiation about the generator point is required in all protocols. The specific generator is chosen in terms of performance.

If this stuff still sounds very strange to you, Elliptic curves are also nicely explained on openssl.org.

1.5 Coordinate systems

In general curve equations consider two coordinates x and y. For example consider Montgomery curve over field F defined by

$$By^2 = x^3 + Ax^2 + x \qquad A, B \in F \text{ and } B(A^2-4) \neq 0$$

A and B are constant for a specific curve. Elements on the curve are tuples (x, y). However, this representation can be extended as shown in Table 1.

The field size $2^{255}-19$ in binary is given as: `111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111`

[1] Recall the definition of *order of an element* from section 1.1

(x, y)	affine	
(X, Y, Z, ZZ)	standard	with $x = X/Z$ and $y = Y/Z$ and $ZZ = Z^2$
(X, Y, Z)	projective	with $x = X/Z$ and $y = Y/Z$
(X, Y, Z)	Lopez-Dahab	with $x = X/Z$ and $y = Y/Z^2$
(X, Y, Z)	Jacobian	with $x = X/Z^2$ and $y = Y/Z^3$
(X, Y, Z, Z^2, XZ)	Extended Lopez-Dahab	with $x = X/Z$ and $y = Y/Z^2$
(X, Y, Z, Z^2)	Extended Jacobian	with $x = X/Z^2$ and $y = Y/Z^3$
(X, Y, Z, T)	Extended Twisted Edwards	with $x = X/Z$ and $Y = Y/Z$ with $T = X \cdot Y$

Table 1: Coordinate systems

`1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111`
`1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111`
`1111 1111 1111 1111 1111 1110 1101`$_2$ hence it gives a very high hamming weight[2]. This can be used for optimizations when reducing numbers. It follows the convention to use prime fields with size $p = b^k + c$ with $b = 2$. The other values are set here to $k = 255$ and $c = -2^4 - 2^1 - 2^0 = -19$.

Furthermore $p^k = q = 2^{255} - 19 \equiv 1 \pmod 4$ holds which is a requirement for EdDSA.

h	8
o	$2^{252} + 27742317777372353535851937790883648493$

Given $+$ as addition of points on an elliptic curve. It holds that for any arbitrary point $P \in C$,

$$\infty + P = P + \infty = P$$

whereas $\infty + P_2 \neq \infty \,\forall\, P_2 \neq \infty \in C$

Let r be the group order of the underlying field. Given an additive group (hence $+$ is the group's operation), then it holds that for any arbitrary point $P \in C$,

$$r \cdot P = \infty$$

Correspondingly in a multiplicative group it holds that

$$P^r = \infty$$

1.6 Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod p \\ 1 & \text{if } a \text{ is quadratic residue mod } p \\ -1 & \text{if } a \text{ is quadratic non-residue mod } p \end{cases}$$

[2]The hamming weight of a number is defined as number of nonzero elements; hence 1s in binary representation.

1.7 Extended euclidean algorithm

Given. two integers a and b
Find. compute the greatest common divisor (gcd) g and integers s and t such that $g = sa + tb$

A python implementation [19] is given in Appendix A.

In *Sagemath* you can use `xgcd(a, b)`.

1.8 Multiplicative inverse

Given. an integer e and a field F
Find. the inverse element of e in F, e^{-1}

For an inverse element e^{-1} it holds that $e \cdot e^{-1} = \infty$ where ∞ denotes the identity element.

In *Sagemath* you can use `inverse_mod(e, m)` to compute the inverse element, where m is the field size. In general you can use `xgcd(e, m)`. If the gcd is not one, a multiplicative inverse does not exist. The returned factor applied to e is the multiplicative element.

2 Curves

$E_{M,a,b}$	Montgomery curve with coefficients a and b
$E_{E,c,d}$	Edwards curve with coefficients c and d
$E_{E,d}$	Edwards curve with coefficients $c = 1$ and d
E_{E_B,d_1,d_2}	Binary Edwards curve with d_1 and d_2
$E_{E_T,a,d}$	Twisted Edwards curvce with a and d
$E(K)$	Set of points of curve E over field $K + \infty$

2.1 Simple Weierstrass curve

$$E/\mathbb{F}: \quad y^2 = x^3 + ax + b$$

Special case of the more general Weierstrass curve:

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

Precondition for parameters: [14]

- The curve must be non-singular (hence, no cusps or self-intersections). The discriminant is zero if and only if the curve is singular.
- Weierstrass curves are the default EllipticCurve instances in *Sagemath* [10][17].

2.2 Montgomery curve

Given a field K, a Montgomery curve is defined as [22, section Definition]:

$$M_{A,B}: \quad By^2 = x^3 + Ax^2 + x$$

denoted as $M_{A,B}$ [22] or $E_{M,a,b}$ [8].

$$\begin{aligned}\text{montgomery}(\infty) &= (0,1)\\ \text{montgomery}(0,0) &= (0,-1)\\ \text{montgomery}(p_1+p_2) &\widehat{=} \text{edwards}(p_1+p_2)\end{aligned}$$

Precondition for parameters:

- $A, B \in K$
- $B(A^2-4) \neq 0 \Rightarrow B \neq 0, A \neq -2, A \neq 2$

Let $P=(x,y)$, $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$ be points on a Montgomery-form elliptic curve. Assume that $P_2 = P_1 + P$ and $y \neq 0$. Then [18, page 129]

$$y_1 = \frac{(x_1x+1)(x_1+x+2A)-2A-(x_1-x)^2x_2}{2By}$$

2.3 Edwards curve

Given a field K with characteristic $2 \neq 0$, an Edwards curve is defined as [6, page 2]

$$x^2+y^2 = 1+dx^2y^2$$

or as

$$x^2+y^2 = c^2(1+dx^2y^2)$$

Properties and preconditions for parameters:

- Field K must not have characteristic 2 [6, page 2]
- $d \notin \{0,1\}$
- $c, d \in K$ with $cd(1\text{-}c^4 \cdot d) \neq 0$ hence $c \neq 0$, $d \neq 0$ and $dc^4 \neq 1$ [5, page 5]
- If d is not a square in k then the Edwards addition law is complete[3] [6, page 3].
- Daniel J. Bernstein and Tanja Lange suggest to represent coordinates as Inverted Edwards Coordinates [6, page 3].

Edwards curves use the strongly unified[4] [6, page 3] addition law [4, page 10]

$$(x_1,y_1)+(x_2+y_2) = \left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right)$$

The neutral element is given as $(0,1)$.

The parameter c is respected in the denominator [5, page 5]

$$(x_1,y_1)+(x_2+y_2) = \left(\frac{x_1y_2+y_1x_2}{c(1+dx_1x_2y_1y_2)}, \frac{y_1y_2-x_1x_2}{c(1-dx_1x_2y_1y_2)}\right)$$

[3] This means that there are no points $(x_1,y_1),(x_2,y_2)$ on the curve where the denominators vanish; the Edwards addition law produces the correct output for every pair of input points.

[4] i.e. it can also be used to double a point. Unlike the Weierstrass group law.

2.4 Twisted Edwards curve

Given a field K with characteristic $2 \neq 0$, an Twisted Edwards curve is defined as [8, page 3]

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

In Inverted Edwards Coordinates, the curve is given as (compare Appendix C):

$$aY^2Z^2 + X^2Z^2 = X^2Y^2 + dZ^4$$

Properties and preconditions for parameters:

- Field K must not have characteristic 2 [8, page 3]
- $a \neq 0$ and $b \neq 0$ and $a \neq b$ [8, page 3]
- An Edwards curve is a twisted Edwards curve with $a = 1$ [8, page 3].
- X, Y and Z must be non-zero [8, page 12].

The addition law is given as [8, page 11]

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

- The neutral element is given as $(0, 1)$ [8, page 11].
- The negation of a point (x_1, y_1) is $(-x_1, y_1)$ [8, page 11].
- The formula is complete, if a is a square in K and d is a non-square in K [8, page 11].

Retrieving x, given y:

$$\begin{aligned} ax^2 + y^2 &= 1 + dx^2y^2 \\ ax^2 - dx^2y^2 &= 1 - y^2 \\ x^2(a - dy^2) &= 1 - y^2 \\ x^2 &= \frac{1 - y^2}{a - dy^2} \end{aligned}$$

Retrieving y, given x:

$$\begin{aligned} ax^2 + y^2 &= 1 + dx^2y^2 \\ dx^2y^2 - y^2 &= ax^2 - 1 \\ y^2(dx^2 - 1) &= ax^2 - 1 \\ y^2 &= \frac{ax^2 - 1}{dx^2 - 1} \end{aligned}$$

2.5 Binary Edwards curves

$$d_1 \cdot (x + y) + d_2 \cdot (x^2 + y^2) = (x + x^2) \cdot (y + y^2)$$

3 Birational equivalences

3.1 Weierstrass Curve to Montgomery Curve

1. Find r with $r^3 + ar + b = 0$
2. Find s with $s^2 = 3r^2 + a$
3. $u = \frac{x-r}{s}, B = \frac{1}{s^3}, A = \frac{3r}{s}$

3.2 Montgomery Curve to Weierstrass Curve

Given a Montgomery curve [22]:

$$
\begin{aligned}
By^2 &= x^3 + Ax^2 + x && \text{[divide by } B^3\text{]} \\
\frac{y^2}{B^2} &= \frac{x^3}{B^3} + \frac{Ax^2}{B^3} + \frac{x}{B^3} && [y = Bv, x = Bu] \\
\frac{(Bv)^2}{B^2} &= \frac{(Bu)^3}{B^3} + \frac{A(Bu)^2}{B^3} + \frac{Bu}{B^3} \\
v^2 &= u^3 + \frac{A}{B}u^2 + \frac{1}{B^2}u && \left[u = t - \frac{A}{3B}\right] \\
v^2 &= \left(t - \frac{A}{3B}\right)^3 + \frac{A}{B}\left(t - \frac{A}{3B}\right)^2 + \frac{1}{B^2}\left(t - \frac{A}{3B}\right) && \text{[common divisor]} \\
v^2 &= \frac{(3Bt - A)^3}{27B^3} + \frac{3A(A - 3Bt)^2}{27B^3} + \frac{27Bt - 9A}{27B^3} \\
&= \frac{-A^3 + 9A^2Bt - 27AB^2t^2 + 27B^3t^3 + 3A^3 - 18A^2Bt + 27AB^2t^2 + 27Bt - 9A}{27B^3} \\
&= \frac{2A^3 - 9A^2Bt + 27B^3t^3 + 27Bt - 9A}{27B^3} \\
&= t^3 + \frac{(27 - 9A^2)t}{27B^2} + (2A^2 - 9)\frac{A}{27B^3} \\
&= t^3 + \frac{3 - A^2}{3B^2}t + \frac{2A^3 - 9A}{27B^3}
\end{aligned}
$$

This is equivalent to the Weierstrass form:

$$E/\mathbb{F} : y^2 = x^3 + ax + b$$

with

$$a = \frac{3 - A^2}{3B^2} \qquad b = \frac{2A^3 - 9A}{27B^3}$$

In conclusion, the map is given as

$$\psi : M_{A,B} \to E/\mathbb{F}$$

$$(x, y) \mapsto (u, v) = \left(\frac{x}{B} + \frac{A}{3B}, \frac{y}{B}\right), \quad a = \frac{3 - A^2}{3B^2}, \quad b = \frac{2A^3 - 9A}{27B^3}$$

3.3 Edwards Curve to smooth Weierstrass Curve

Edwards curve:

$$x^2 + y^2 = 1 + dx^2y^2$$

Smooth Weierstrass curve:

$$y^2 = x^3 + a_2x^2 + a_4x$$

$$a_2 = 2\frac{(1+d)}{(1-d)^2} \qquad a_4 = \frac{1}{(1-d)^2}$$

3.4 Montgomery Curve to Edwards Curve

$u = (1 + x)/(1 - y)$ and $v = \sqrt{486664}\frac{u}{x}$

$x = \sqrt{486664}\frac{u}{v}$ and $y = (u - 1)/(u + 1)$

3.5 Edwards Curve to Montgomery Curve

3.6 Montgomery Curve to Twisted Edwards Curve

[22, section 6]

$$a = \frac{A+2}{B} \qquad d = \frac{A-2}{B}$$
$$x = \frac{x}{y} \qquad y = \frac{x-1}{x+1}$$

3.7 Twisted Edwards Curve to Montgomery Curve

$$A = \frac{2(a+d)}{a-d} \qquad B = \frac{4}{a-d}$$
$$x_M = \frac{1+y}{1-y} \qquad y_M = \frac{1+y}{(1-y)\cdot x}$$

3.8 Twisted Edwards Curve to Weierstrass Curve

For the parameters, from 3.2 it follows that

$$(a_{\text{weier}}, b_{\text{weier}}) \mapsto \left(\frac{3 - A_{\text{mont}}^2}{3B_{\text{mont}}^2}, \frac{2A_{\text{mont}}^3 - 9A_{\text{mont}}}{27B_{\text{mont}}^3} \right)$$

From 3.7 it follows that

$$(a_{\text{weier}}, b_{\text{weier}}) \mapsto \left(\frac{3 - \left(\frac{2(a_{\text{TEC}}+d_{\text{TEC}})}{a_{\text{TEC}}-d_{\text{TEC}}}\right)^2}{3\left(\frac{4}{a_{\text{TEC}}-d_{\text{TEC}}}\right)^2}, \frac{2\left(\frac{2(a_{\text{TEC}}+d_{\text{TEC}})}{a_{\text{TEC}}-d_{\text{TEC}}}\right)^3 - 9\left(\frac{2(a_{\text{TEC}}+d_{\text{TEC}})}{a_{\text{TEC}}-d_{\text{TEC}}}\right)}{27\left(\frac{4}{a_{\text{TEC}}-d_{\text{TEC}}}\right)^3} \right)$$

$$\begin{aligned}
(a_{\text{weier}}, b_{\text{weier}}) &= \left(\frac{3 - \left(\frac{4(a+d)^2}{(a-d)^2}\right)}{\frac{48}{(a-d)^2}}, \frac{2\left(\frac{8(a+d)^3}{(a-d)^3}\right) - \left(\frac{18(a+d)}{a-d}\right)}{\frac{1728}{(a-d)^3}} \right) \\
&= \left(\frac{\frac{3(a-d)^2}{(a-d)^2} - \frac{4(a+d)^2}{(a-d)^2}}{\frac{48}{(a-d)^2}}, \frac{\frac{16(a+d)^3}{(a-d)^3} - \frac{18(a+d)(a-d)^2}{(a-d)^3}}{\frac{1728}{(a-d)^3}} \right) \\
&= \left(\frac{\left(3(a-d)^2 - 4(a+d)^2\right)(a-d)^2}{48(a-d)^2}, \frac{\left(16(a+d)^3 - 18(a+d)(a-d)^2\right)(a-d)^3}{1728(a-d)^3} \right) \\
&= \left(\frac{3(a-d)^2 - 4(a+d)^2}{48}, \frac{16(a+d)^3 - 18(a+d)(a-d)^2}{1728} \right) \\
&= \left(-\frac{1}{48}\left(a^2 + 14ad + d^2\right), \frac{1}{864}(a+d)(-a^2 + 34ad - d^2) \right)
\end{aligned}$$

For affine coordinates with 3.2 it holds that

$$\begin{aligned}
(x_w, y_w) &= \left(\frac{x_{\text{mont}}}{B_{\text{mont}}} + \frac{A_{\text{mont}}}{3B_{\text{mont}}}, \frac{y_{\text{mont}}}{B_{\text{mont}}} \right) \\
&= \left(\frac{\frac{1+y}{1-y}}{\frac{4}{a-d}} + \frac{\frac{2(a+d)}{a-d}}{3\frac{4}{a-d}}, \frac{\frac{1+y}{(1-y)x}}{\frac{4}{a-d}} \right) \\
&= \left(\frac{(1+y)(a-d)}{4(1-y)} + \frac{2(a+d)(a-d)}{12(a-d)}, \frac{(1+y)(a-d)}{4x \cdot (1-y)} \right) \\
&= \left(\frac{3a + 3ay - 3d - 3dy}{12 - 12y} + \frac{2a + 2d - 2ay - 2dy}{12 - 12y}, \frac{a + ay - dy - d}{4x - 4xy} \right) \\
&= \left(\frac{5a + ay - 5dy - d}{12 - 12y}, \frac{a + ay - dy - d}{4x - 4xy} \right)
\end{aligned}$$

In conclusion, the map is given as

$$(x, y) \mapsto (u, v) = \left(\frac{5a + ay - 5dy - d}{12 - 12y}, \frac{a + ay - dy - d}{4x - 4xy} \right)$$

$$a \mapsto -\frac{1}{48}\left(a^2 + 14ad + d^2\right)$$
$$b \mapsto \frac{1}{864}(a+d)(-a^2 + 34ad - d^2)$$

In Inverted Edwards Coordinates, the map is given as

$$\begin{aligned}(x,y,z) \mapsto (u,v) &= \left(\frac{-a(\frac{z}{y}+5) + 5d\frac{z}{y} + d}{12(\frac{z}{y}-1)}, \frac{\frac{z}{x}(\frac{z}{y}+1)(a-d)}{4(1-\frac{z}{y})}\right) \\ &= \left(\frac{-5ay - az + dy + 5dz}{12(z-y)}, \frac{z(a-d)(y+z)}{4x(y-z)}\right)\end{aligned}$$

In Extended Twisted Edwards Coordinates, the map is given as

$$\begin{aligned}(x,y,z,t) \mapsto (u,v) &= \left(\frac{-a(\frac{y}{z}+5) + 5d\frac{y}{z} + d}{12(\frac{y}{z}-1)}, \frac{\frac{x}{z}(\frac{y}{z}+1)(a-d)}{4(1-\frac{y}{z})}\right) \\ &= \left(\frac{-ay - 5az + 5dy + dz}{12(y-z)}, \frac{x(a-d)(y+z)}{4z(z-y)}\right) \\ &= \left(\frac{-ay - 5az + 5dy + dz}{12(y-z)}, \frac{(a-d)(t+xz)}{4z(z-y)}\right)\end{aligned}$$

3.9 Weierstrass Curve to Twisted Edwards Curve

4 ECDH

4.1 Montgomery ladder

The Montgomery ladder is a side-channel attack resistant algorithm for scalar multiplication. Given a scalar n and a point P, it returns $[n]P$. However, Yuval Yarom and Naomi Benger attacked it successfully using `FLUSH+RELOAD`. For the algorithm, m is the number of bits of the binary representation of n and d_i all the individual bits.

1. $R_0 = 0$
2. $R_1 = P$
3. for $i = m \to 0$
   (a) if $d_i = 0$
      i. $R_1 = R_0 + R_1$
      ii. $R_0 = 2 \cdot R_0$
   (b) else
      i. $R_0 = R_0 + R_1$
      ii. $R_1 = 2 \cdot R_1$
4. return R_0

5 EdDSA

Public key: 32 bytes = 256 bits
Private key: 32 bytes = 256 bits

5.1 Curve25519 is a Montgomery Curve

$$M_{A,B}: \quad By^2 = x^3 + Ax^2 + x$$

with $B = 1$ and $A = 486662_{10} = \texttt{76D06}_{16} = 1110110110100000110_2$ giving

$$M_{A,B}: \quad y^2 = x^3 + 486662x^2 + x$$

over $\mathbb{F}_{2^{255}-19}$.

Sources: [5, page 3]

5.2 Curve25519 as Weierstrass Curve

$$E/\mathbb{F}_{a,b} : y^2 = x^3 + ax + b$$

over the prime field of size $2^{255} - 19$.

Sources: converted to Weierstrass curve using 3.2

5.3 Curve25519 as Edwards Curve

$$x^2 + y^2 = 1 + \frac{121665}{121666}x^2y^2$$

where $\frac{121665}{121666} \pmod{2^{255} - 19}$

$= 20800338683988658368647408995589388737092878452977063003340006470870624536394_{10}$
$= \texttt{2DFC9311D490018C7338BF8688861767FF8FF5B2BEBE27548A14B235ECA6874A}_{16}$

Sources: [5, page 4]

5.4 Curve25519 as Twisted Edwards Curve (namely Ed25519)

$$E_{E,a,d} : -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$$

over the prime field of size $2^{255} - 19$.

Field size:	$2^{255} - 19$ [20]
A:	486662 [20]
B:	1 [20]
Generator:	$x = 9$, compute y with curve equation [1, section Computing public keys], see appendix O
Group order:	$2^{252} + 27742317777372353535851937790883648493$ [11] [7, parameter l] [12, section 5]
Cofactor:	8 [3, page 8]

Table 2: Symbolic values

Field size:	$\texttt{7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF}\texttt{ED}_{16}$
A:	$\texttt{76D06}_{16}$
B:	$\texttt{1}_{16}$
Generator:	$x = \texttt{9}_{16}$
	$y_1 = \texttt{20AE19A1B8A086B4E01EDD2C7748D14C923D4D7E6D7C61B229E9C5A27ECED3D9}_{16}$
	$y_2 = \texttt{5F51E65E475F794B1FE122D388B72EB36DC2B28192839E4DD6163A5D81312C14}_{16}$
Group order:	$\texttt{1000000000000000000000000000000014DEF9DEA2F79CD65812631A5CF5D3ED}_{16}$

Table 3: Values in hexadecimal notation

Field size:	$57896044618658097711785492504343953926634992332820282019728792003956564819949_{10}$
A:	48666210
B:	110
Generator:	$x = 910$
	$y_1 = 14781619447589544791020593568409986887264606134616475288964881837755586237401_{10}$
	$y_2 = 43114425171068552920764898935933967039370386198203806730763910166200978582548_{10}$
Group order:	$72370055773322622139731865630429942408571163593799076060019509382854542509 89_{10}$

Table 4: Values in decimal notation

Field size:	$2^{255} - 19$ [20, field size stays the same]
a:	N/A
b:	N/A
Generator:	N/A
Group order:	N/A
Cofactor:	N/A

Table 5: Symbolic values

Field size:	$\texttt{7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFED}_{16}$
a:	$\texttt{2AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA984914A144}_{16}$
b:	$\texttt{7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864}_{16}$
Generator:	$x = \texttt{2AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD245A}_{16}$
	$y_1 = \texttt{20AE19A1B8A086B4E01EDD2C7748D14C923D4D7E6D7C61B229E9C5A27ECED3D9}_{16}$
	$y_2 = \texttt{5F51E65E475F794B1FE122D388B72EB36DC2B28192839E4DD6163A5D81312C14}_{16}$
Group order:	**TODO** determine, might stay the same: hence $\texttt{100..014DEF9DEA2F79CD65812631A5CF5D3ED}$

Table 6: Values in hexadecimal notation

Field size:	$57896044618658097711785492504343953926634992332820282019728792003956564819949_{10}$
a:	$19298681539552699237261830834781317975544997444273427339909597334573241639236_{10}$
b:	$55751746669818908907645289078257140818241103727901012315294400837956729358436_{10}$
Generator:	$x = 19298681539552699237261830834781317975544997444273427339909597334652188435546_{10}$
	$y_1 = 14781619447589544791020593568409986887264606134616475288964881837755586237401_{10}$
	$y_2 = 43114425171068552920764898935933967039370386198203806730763910166200978582548_{10}$
Group order:	**TODO** determine

Table 7: Values in decimal notation

Field size:	N/A
a:	N/A
d:	N/A
Generator:	N/A
Group order:	N/A
Cofactor:	4 [3, page 8]

Table 8: Symbolic values

Sources: [21, section Ed25519], [2, variable d and function isoncurve], [7, page 8]

$$E_{E,a,d} : 121666x^2 + y^2 = 1 + 121665x^2y^2$$

over the prime field of size $2^{255} - 19$.

Sources: [8, page 15]

Field size:	$2^{255} - 19$ [20]
a:	N/A
d:	N/A
Generator:	$y = 4/5$, compute x with curve equation [2, variable B]
Group order:	$2^{252} + 27742317777372353535851937790883648493$ [11] [7, parameter l]
Cofactor:	8 **TODO** verification needed

Table 9: Symbolic values

Field size:	$\texttt{7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF}\texttt{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFED}_{16}$
a:	$\texttt{7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF}\texttt{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEC}_{16}$
d:	$\texttt{52036CEE2B6FFE738CC740797779E89800700A4D4141D8AB75EB4DCA135978A3}_{16}$
Generator:	$x = \texttt{216936D3CD6E53FEC0A4E231FDD6DC5C692CC7609525A7B2C9562D608F25D51A}_{16}$
	$y = \texttt{6666666666666666666666666666666666666666666666666666666666666658}_{16}$
Group order:	$\texttt{1000000000000000000000000000000014DEF9DEA2F79CD65812631A5CF5D3ED}_{16}$

Table 10: Values in hexadecimal notation

Field size:	$57896044618658097711785492504343953926634992332820282019728792003956564819949_{10}$
a:	$57896044618658097711785492504343953926634992332820282019728792003956564819948_{10}$
d:	$37095705934669439343138083508754565189542113879843219016388785533085940283555_{10}$
Generator:	$x = 15112221349535400772501151409588531511454012693041857206046113283949847762202_{10}$
	$y = 46316835694926478169428394003475163141307993866256225615783033603165251855960_{10}$ [12, section 5]
Group order:	$72370055773322622139731865630429942408571163593799076060019509382854542509 89_{10}$

Table 11: Values in decimal notation

5.5 Edwards Digital Signature Scheme (EdDSA)

Parameters you need to prepare:

b An arbitrary integer greater-equal 10 (EdDSA with SHA512: $b = 256$)

H A hash algorithm providing output of size $2b$ (EdDSA with SHA512: H =SHA512)

B The generator point of the elliptic curve used (EdDSA with SHA512: see Ed25519 5.4)

l The group order (EdDSA with SHA512: see Table 9)

$\underline{X}$ The underline denotes a b-bit encoding for values modulo l or points on Ed25519 (EdDSA with SHA512: Little endian)

The signature consists of two encoded values of length b. Signatures have size $2b = 2 \cdot 256 = 512$ bits $= 64$ bytes in case of EdDSA with SHA512. The public key is a point on the curve and can be encoded with b bits giving $b = 256$ bits $= 32$ bytes encodings for EdDSA with SHA512.

Key Pair generation *Input:* k as b random bits
Output: $H(k)$ as secret key and A as public key.

$$
\begin{aligned}
H_k = H(k) &= (h_0, h_1, \ldots, h_{2b-1}) \text{ where } k \text{ is a } b\text{-bit string with output of size } 2b \\
a &= 2^{b-2} + \sum_{3 \le i \le b-3} 2^i h_i \in \left\{2^{b-2}, 2^{b-2}+8, \ldots, 2^{b-1}-8\right\} \\
A &= aB
\end{aligned}
$$

$H(k)$ is our private key[5]. A is the public key.

Signing *Output:* $(\underline{R}, \underline{S})$ as signature

$$
\begin{aligned}
r &= H(h_b, \ldots, h_{2b-1}, M) \text{ with output of size } 2b \\
R &= rB \\
S &= (r + H(\underline{R}, \underline{A}, M)a) \bmod l
\end{aligned}
$$

Just for the sake of completeness: S is an integer of size 253 bits.

Verification *Output:* Does signature $(\underline{R}, \underline{S})$ fit to the given message M?

$$8SB \stackrel{?}{=} 8R + 8H(\underline{R}, \underline{A}, M)$$

The encoding in detail Given the affine coordinate (x, y), the encoding specified for EdDSA with SHA512 is defined as $b - 1$ bit little endian encoding of y concatenated with the distinguishing bit of x. You can retrieve the affine representation using the equation:

$$x = \pm\sqrt{(y^2 - 1)(dy^2 + 1)^{-1}}$$

Given the encoded representation of (x, y) as byte array b, the byte index 0 contains the LSB of y. Hence $b[0]\&1$ returns 1 iff y is an odd integer. In contrast byte index -1 (for EdDSA with SHA512 this is 31) contains the MSB of y. Bit 7 is discarded. Bit 7 is set to 1 if $x\&1$ yields 1. Otherwise it yields 0.

If you are curious about djb's test vectors[6], Table 12 shows the x-bits of the first test vectors.

[5] Here $H(k)$ and a constitute the secret key. a is technically considered the secret key, because the scalar for A is the secret key in comparable protocols like ECDSA, but actually $H(k)$ is required in the signing process and a can be derived from $H(k)$. Hence $H(k)$ should be considered as secret value.

[6] See `sign.input` at `http://ed25519.cr.yp.to/software.html`

vector number	EdDSA variable	x-bit when encoded
1	A	0
1	R	0
2	A	0
2	R	1
3	A	0
3	R	1
4	A	0
4	R	1
5	A	1
5	R	0

Table 12: x-bits of djb's test vectors

6 Coordinate systems

6.1 Affine coordinates

$$(x, y)$$

The well-known cartesian coordinates.

6.2 Projective coordinates

$$(x, y) \to \left(\frac{X}{Z}, \frac{Y}{Z}\right)$$
$$\forall \lambda : (X, Y, Z) = (\lambda X, \lambda Y, \lambda Z) \qquad \text{if } \lambda \neq 0$$
$$-(X : Y : Z) = (X : -Y : Z)$$

6.3 Jacobian coordinates

$$(x, y) \to \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$$

6.4 Extended Jacobian coordinates

$$(x, y) \to \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$$

store z^2 internally for speedup as well.

6.5 López-Dahab coordinates

$$(x, y) \to \left(\frac{X}{Z}, \frac{Y}{Z^2}\right)$$

6.6 Extended López-Dahab coordinates

$$(x, y) \to \left(\frac{X}{Z}, \frac{Y}{Z^2}\right)$$

store z^2 internally for speedup as well.

6.7 Inverted Edwards coordinates [6]

$$(x, y) \to \left(\frac{Z}{X}, \frac{Z}{Y}\right)$$

Special treatment for $xy = 0$. Has 4 special points:

$$\begin{aligned}
(1 : 0 : 0) &\to (0, 1) \text{ neutral point, identity} \\
(-1 : 0 : 0) &\to (0, -1) \text{ order 2} \\
(0 : -1 : 0) &\to (1, 0) \text{ order 4} \\
(0 : 1 : 0) &\to (-1, 0) \text{ order 4}
\end{aligned}$$

Let (x, y) be affine coordinates satisfying $ax^2 + y^2 = 1 + dx^2y^2$ (compare with Twisted Edwards curves 2.4) with $xy \neq 0$, then $(X : Y : Z)$ from $(x^{-1} : y^{-1} : 1)$ satisfies $Z^2(aY^2+X^2) = X^2Y^2+dZ^4$ where $(X_1 : Y_1 : Z_1) = (X_2 \cdot \lambda : Y_2 \cdot \lambda : Z_2 \cdot \lambda) \quad \forall \lambda \neq 0$ with $XYZ \neq 0$.

6.8 YZ coordinates with square d [Edwards curves]

$$(x, y) \to \left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

like projective coordinates, with $c = 1$ and $d = r^2$ and $(x, y) \to (Y, Z)$ with $ry = \frac{Y}{Z}$.

6.9 Squared YZ coordinates with square d [Edwards curves]

$$(x, y) \to \left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

with $c = 1$ and $d = r^2$ and $(x, y) \to (Y, Z)$ with $ry^2 = \frac{Y}{Z}$.

6.10 XZ coordinates [Montgomery curves]

$$(x, y) \to \left(\frac{X}{Z}\right)$$

Loses one coordinates, which is expected to be computable by other means [4, page 8, section Montgomery coordinates]. For Montgomery curve, the y-coordinate can be retrieved using the formula [9, page 286]

$$y_n = \frac{(x_1 x_n + 1)(x_1 + x_n + 2A) - 2A - (x_1 - x_n)^2 x_{n+1}}{2By_1}$$

where $P = (x_1, y_1)$ is the basepoint (difference) for the Montgomery ladder and x_n and x_{n+1} are affine coordinates of $[n]P$ and $[n+1]P$.

6.11 Extended Twisted Edwards coordinates

$$(x, y) \to (x, y, 1, xy)$$

7 Addition and doubling laws

The addition law for Twisted Edwards curves (2.4) in Extended Twisted Edwards coordinates (6.11) is given as [16, 3.2 Dedicated Addition in ε^e]:

$$A \leftarrow X_1 \cdot X_2, \quad B \leftarrow Y_1 \cdot Y_2, \quad C \leftarrow Z_1 \cdot T_2, \quad D \leftarrow T_1 \cdot Z_2, \quad E \leftarrow D + C$$

$$F \leftarrow (X_1 - Y_1) \cdot (X_2 + Y_2) + B - A, \quad G \leftarrow B + aA, \quad H \leftarrow D - C$$

$$X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \quad Z_3 \leftarrow F \cdot G, \quad T_3 \leftarrow E \cdot H$$

with $9\mathbf{M} + 1\mathbf{D}$.

The addition law for Twisted Edwards curves (2.4) in Extended Twisted Edwards coordinates (6.11) with $Z_1 = Z_2 = 1$ based on the addition law above is given as:

$$A \leftarrow X_1 \cdot X_2, \quad B \leftarrow Y_1 \cdot Y_2, \quad E \leftarrow T_1 + T_2$$

$$F \leftarrow (X_1 - Y_1) \cdot (X_2 + Y_2) + B - A, \quad G \leftarrow B + aA, \quad H \leftarrow T_1 - T_2$$

$$X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \quad Z_3 \leftarrow F \cdot G, \quad T_3 \leftarrow E \cdot H$$

with $7\mathbf{M} + 1\mathbf{D}$.

The addition law for Twisted Edwards curves (2.4) in Extended Twisted Edwards coordinates (6.11) with $Z_2 = 1$ based on the addition law above is given as:

$$A \leftarrow X_1 \cdot X_2, \quad B \leftarrow Y_1 \cdot Y_2, \quad C \leftarrow Z_1 \cdot T_2, \quad E \leftarrow T_1 + C$$

$$F \leftarrow (X_1 - Y_1) \cdot (X_2 + Y_2) + B - A, \quad G \leftarrow B + aA, \quad H \leftarrow T_1 - C$$

$$X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \quad Z_3 \leftarrow F \cdot G, \quad T_3 \leftarrow E \cdot H$$

with $8\mathbf{M} + 1\mathbf{D}$.

The doubling law for Twisted Edwards curves (2.4) in Extended Twisted Edwards coordinates (6.11) is given as [16, 3.3 Dedicated Doubling in ε^e]:

$$A \leftarrow X^2, \quad B \leftarrow Y^2, \quad C \leftarrow 2Z^2, \quad D \leftarrow aA, \quad E \leftarrow (X+Y)^2 - A - B$$
$$G \leftarrow D + B, \quad F \leftarrow G - C, \quad H \leftarrow D - B$$
$$X \leftarrow E \cdot F, \quad Y \leftarrow G \cdot H, \quad Z \leftarrow F \cdot G, \quad T \leftarrow E \cdot H$$

with $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$.

The doubling law for Twisted Edwards curves (2.4) in Extended Twisted Edwards coordinates (6.11) with $Z = 1$ based on the doubling law above is given as:

$$A \leftarrow X^2, \quad B \leftarrow Y^2, \quad D \leftarrow aA, \quad E \leftarrow (X+Y)^2 - A - B$$
$$G \leftarrow D + B, \quad F \leftarrow G - 2, \quad H \leftarrow D - B$$
$$X \leftarrow E \cdot F, \quad Y \leftarrow G \cdot H, \quad Z \leftarrow F \cdot G, \quad T \leftarrow E \cdot H$$

with $3\mathbf{M} + 3\mathbf{S} + 1\mathbf{D}$.

If you want to use a unified addition law which is also complete given that d is a non-square in K and a is a square in K, then you can use

$$\begin{aligned} X_3 &= (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2) \\ Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2) \\ T_3 &= (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2) \\ Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2) \end{aligned}$$

procedurally as

$$A \leftarrow X_1 \cdot X_2, \quad B \leftarrow Y_1 \cdot Y_2, \quad C \leftarrow dT_1T_2, \quad D \leftarrow Z_1Z_2, \quad E \leftarrow (X_1+Y_1)(X_2+Y_2) - A - B$$
$$F \leftarrow D - C, \quad G \leftarrow D + C, \quad H \leftarrow B - aA$$
$$X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \quad Z_3 \leftarrow F \cdot G, \quad T_3 \leftarrow E \cdot H$$

with $9\mathbf{M} + 2\mathbf{D}$. Assuming that $Z_2 = 1$ we have

$$A \leftarrow X_1 \cdot X_2, \quad B \leftarrow Y_1 \cdot Y_2, \quad C \leftarrow dT_1T_2, \quad E \leftarrow (X_1+Y_1)(X_2+Y_2) - A - B$$
$$F \leftarrow Z_1 - C, \quad G \leftarrow Z_1 + C, \quad H \leftarrow B - aA$$
$$X_3 \leftarrow E \cdot F, \quad Y_3 \leftarrow G \cdot H, \quad Z_3 \leftarrow F \cdot G, \quad T_3 \leftarrow E \cdot H$$

with $8\mathbf{M} + 2\mathbf{D}$.

Appendices

A Extended euclidean algorithm and multiplicative inverse in python

```
def xgcd(a, b):
    x, y, u, v = 0, 1, 1, 0
```

```
    while a != 0:
        q, r = b // a, b % a
        m, n = x - u * q, y - v * q
        b, a, x, y, u, v = a, r, u, v, m, n
    gcd = b
    return gcd, x, y

def mult_inverse(a, m):
    gcd, x, y = xgcd(a, m)
    if gcd != 1:
        raise ValueError("Inverse does not exist")
    else:
        return x % m
```

With the following output:

```
>>> print(xgcd(244, 46))
(2, 10, -53)
>>> print(mult_inverse(244, 269))
43
>>> print(xgcd(244, 269))
(1, 43, -39)
```

B Montgomery Curve to Weierstrass Curve in Inverted Edwards Coordinates

$$\left(\frac{Z}{X}, \frac{Z}{Y}\right) \mapsto (u, v) = \left(\frac{Z}{XB} + \frac{A}{3B}, \frac{Z}{yB}\right)$$

C Twisted Edwards Curve in Inverted Edwards Coordinates

$$\begin{gathered}
ax^2 + y^2 = 1 + dx^2y^2 \\
a\left(\frac{Z}{X}\right)^2 + \left(\frac{Z}{Y}\right)^2 = 1 + d\left(\frac{Z}{X}\right)^2\left(\frac{Z}{Y}\right)^2 \\
a\frac{Z^2}{X^2} + \frac{Z^2}{Y^2} = 1 + d\frac{Z^4}{X^2Y^2} \\
\frac{aY^2Z^2}{X^2Y^2} + \frac{X^2Z^2}{X^2Y^2} = \frac{X^2Y^2}{X^2Y^2} + \frac{dZ^4}{X^2Y^2} \\
aY^2Z^2 + X^2Z^2 = X^2Y^2 + dZ^4
\end{gathered}$$

See also [16, page 5].

D Twisted Edwards Curve in Extended Twisted Edwards Coordinates

$$
\begin{aligned}
ax^2 + y^2 &= 1 + dx^2y^2 \\
a\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 &= 1 + d\left(\frac{X}{Z}\right)^2\left(\frac{Y}{Z}\right)^2 \\
a\frac{X^2}{Z^2} + \frac{Y^2}{Z^2} &= 1 + d\frac{X^2Y^2}{Z^4} \\
aX^2 + Y^2 &= Z^2 + d\frac{X^2Y^2}{Z^2} && \left[T = \frac{XY}{Z}\right] \\
aX^2 + Y^2 &= Z^2 + dT^2
\end{aligned}
$$

The identity element is given as $(0 : 1 : 0 : 1)$ and the negative of $(X : Y : T : Z)$ is $(-X : Y : -T : Z)$.

E Does the neutral element satisfy the Twisted Edwards Curve equation?

The neutral element in affine coordinates is given as $(0, 1)$ [6, page 4]:

$$
\begin{aligned}
ax^2 + y^2 &= 1 + dx^2y^2 \\
a0^2 + 1^2 &= 1 + d0^21^2 \\
1 &= 1
\end{aligned}
$$

Answer: Yes.

F Assuming the neutral element is $(0 : 1 : 0)$ in Inverted Edwards Coordinates, does the Twisted Edwards Curve equation hold?

$$
\begin{aligned}
aY^2Z^2 + X^2Z^2 &= X^2Y^2 + dZ^4 \\
a1^20^2 + 0^20^2 &= 0^21^2 + d0^4 \\
0 + 0 &= 0 + 0
\end{aligned}
$$

```
>>> a, d = var('a'), var('d')
>>> X, Y, Z = 0, 1, 0

>>> print(a * Y**2 * Z**2 + X**2 * Z**2 - X**2 * Y**2 - d * Z**4)
```

```
0
>>> print(a * Y**2 * Z**2 + X**2 * Z**2 - X**2 * Y**2 - d * Z**4 == 0)
True
```

Answer: Yes.

G Does $\infty + p = p$ with $\infty = (0 : 1 : 0 : 1)$ as Extended Twisted Edwards Coordinates and the Dedicated Addition Law on Twisted Edwards Curve Ed25519 hold?

```
>>> X_1, Y_1, T_1, Z_1 = 0, 1, 0, 1
>>> X_2, Y_2, T_2, Z_2 = var("x2"), var("y2"), var("t2"), var("z2")
>>> C = GF(2^255-19)
>>> # a = 0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEC
>>> a = C(-1)

>>> A = X_1 * X_2
>>> B = Y_1 * Y_2
>>> C = Z_1 * T_2
>>> D = T_1 * Z_2
>>> E = D + C
>>> F = (X_1 - Y_1) * (X_2 + Y_2) + B - A
>>> G = B + a * A
>>> H = D - C
>>> X_3 = E * F
>>> Y_3 = G * H
>>> Z_3 = F * G
>>> T_3 = E * H

>>> print(X_3, Y_3, T_3, Z_3)
(-t2*x2, -t2*y2, -t2**2, -x2*y2)
```

Answer: No.

H Does $\infty + \infty = \infty$ with $\infty = (0 : 1 : 0 : 1)$ in Extended Twisted Edwards Coordinates and the Dedicated Addition Law on Twisted Edwards Curve Ed25519 hold?

```
>>> X_1, Y_1, T_1, Z_1 = 0, 1, 0, 1
>>> X_2, Y_2, T_2, Z_2 = 0, 1, 0, 1
>>> C = GF(2^255-19)
>>> a = C(-1)
```

```
>>> A = X_1 * X_2
>>> B = Y_1 * Y_2
>>> C = Z_1 * T_2
>>> D = T_1 * Z_2
>>> E = D + C
>>> F = (X_1 - Y_1) * (X_2 + Y_2) + B - A
>>> G = B + a * A
>>> H = D - C
>>> X_3 = E * F
>>> Y_3 = G * H
>>> Z_3 = F * G
>>> T_3 = E * H

>>> print(X_3, Y_3, T_3, Z_3)
(0, SymmetricModularIntegerMod238(0), 0, SymmetricModularIntegerMod238(0))
```

Answer: Yes.

I Does $\infty + \infty = \infty$ with $\infty = (0 : 1 : 0 : 1)$ in Extended Twisted Edwards Coordinates and the Unified non-procedural Addition Law on Twisted Edwards Curve Ed25519 hold?

```
>>> X_1, Y_1, T_1, Z_1 = 0, 1, 0, 1
>>> X_2, Y_2, T_2, Z_2 = 0, 1, 0, 1
>>> C = GF(2^255-19)
>>> a = C(-1)
>>> # d = C(-121665) / C(121666)
>>> d = 0x52036cee2b6ffe738cc740797779e89800700a4d4141d8ab75eb4dca135978a3

>>> X_3 = (X_1 * Y_2 + Y_1 * X_2) * (Z_1 * Z_2 - d * T_1 * T_2)
>>> Y_3 = (Y_1 * Y_2 - a * X_1 * X_2) * (Z_1 * Z_2 + d * T_1 * T_2)
>>> T_3 = (Y_1 * Y_2 - a * X_1 * X_2) * (X_1 * Y_2 + Y_1 * X_2)
>>> Z_3 = (Z_1 * Z_2 - d * T_1 * T_2) * (Z_1 * Z_2 + d * T_1 * T_2)

>>> print(X_3, Y_3, T_3, Z_3)
(0L, SymmetricModularIntegerMod238(1), SymmetricModularIntegerMod238(0), 1L)
```

Answer: Yes.

J Does $\infty + p = p$ hold for the neutral element on Twisted Edwards Curves?

The addition law is given as [8, page 11]:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

The neutral element in affine coordinates is given as $(0, 1)$ [6, page 4]:

$$\begin{aligned}
(0, 1) + (p_x, p_y) &= \left(\frac{0 \cdot p_y + 1 \cdot p_x}{1 + d \cdot 0 \cdot p_x \cdot 1 \cdot p_y}, \frac{1 \cdot p_y - a \cdot 0 \cdot p_x}{1 - d \cdot 0 \cdot p_x \cdot 1 \cdot p_y} \right) \\
&= \left(\frac{1 \cdot p_x}{1}, \frac{1 \cdot p_y}{1} \right) \\
&= (p_x, p_y)
\end{aligned}$$

Answer: Yes.

K Assuming the neutral element is $(0 : 1 : 0)$ in Inverted Edwards Coordinates, does $\infty + p = p$ hold?

We use the procedural addition law given in [8, page 13]

$$\begin{aligned}
A &= Z_1 \cdot Z_2 && = 0 \cdot p_z \\
B &= dA^2 && = 0 \\
C &= X_1 \cdot X_2 && = 0 \cdot p_x \\
D &= Y_1 \cdot Y_2 && = 1 \cdot p_y \\
E &= C \cdot D && = 0 \\
H &= C - aD && = 0 - a p_y \\
I &= (X_1 + X_2) \cdot (X_2 + Y_2) - C - D && = (0 + 1) \cdot (p_x + p_y) - 0 - p_y = p_x \\
X_3 &= (E + B) \cdot H && = (0 + 0) \cdot (-a p_y) = 0 \\
Y_3 &= (E - B) \cdot I && = (0 - 0) \cdot p_x = 0 \\
Z_3 &= A \cdot H \cdot I && = 0 \cdot -a p_y \cdot p_x = 0
\end{aligned}$$

Giving us

$$(0, 0, 0)$$

which might be considered as neutral point?

```
>>> X1, Y1, Z1 = 1, 0, 1
>>> X2, Y2, Z2 = var('X2'), var('Y2'), var('Z2')
>>> a, d = var('a'), var('d')
```

```
>>> A = Z1 * Z2
>>> B = d * A**2
>>> C = X1 * X2
>>> D = Y1 * Y2
>>> E = C * D
>>> H = C - a * D
>>> I = (X1 + Y1) * (X2 + Y2) - C - D
>>> X3 = (E + B) * H
>>> Y3 = (E - B) * I
>>> Z3 = A * H * I
>>> print(X3, Y3, Z3)
(X2*Z2**2*d, -Y2*Z2**2*d, X2*Y2*Z2)
```

L $2^{256} \equiv 38 \bmod 2^{255} - 19$

M Is $a = -1$ a square in $\mathrm{GF}_{2^{255}-19}$?

```
>>> import math

>>> fieldsize = 2**255-19
>>> a = -1 % fieldsize
>>> a_alt = 2**255-20 % fieldsize

>>> assert(a == a_alt)

>>> # technically, we should start with 0, but this is a better value
>>> lower_limit = 0x2B8324804FC1DF0B2B4D00993DFBD7A72F431806AD2FE478C4EE1B274A0EA0B0
>>> upper_limit = a_alt / 2
>>> i = lower_limit

>>> while i < upper_limit:
...     if (i**2 % fieldsize) == a_alt:
...         print("0x%X ^ 2 == -1" % i)
...         break
...     i += 1
...
0x2B8324804FC1DF0B2B4D00993DFBD7A72F431806AD2FE478C4EE1B274A0EA0B0 ^ 2 == -1
>>> d = 37095705934669439343138083508754565189542113879843219016388785533085940283555
```

N Is $d = -\frac{121665}{121666}$ a square in $\mathbb{F}_{2^{255}-19}$?

A python program without fancy algorithms would take too long to compute. So only a sage math program is given here:

```
C = GF(2**255-19)
d = C(0x52036CEE2B6FFE738CC740797779E89800700A4D4141D8AB75EB4DCA135978A3)

print d.is_square()
```

This script returns "False".

O What's the base point of Curve25519?

> ...and it uses the base point $x = 9$. [20]

Given the x-coordinate, what are the y-coordinates?

```
fieldsize = 2^255-19
field = GF(fieldsize)
x = field(9)

# curve equation
y_squared = x^3 + field(486662)*x^2 + x

for root in y_squared.nth_root(2, all=True):
    print(root)
    print(bin(int(root)))
    print(hex(int(root)))
```

The results are represented in table 7. Is the base point on the curve?

```
>>> field = 2**255-19
>>> x, y = 0x9, 0x20ae19a1b8a086b4e01edd2c7748d14c923d4d7e6d7c61b229e9c5a27eced3d9

>>> right = (x**3 + 486662*x**2 + x) % field
>>> left = (y**2) % field
>>> print(left == right)
True
```

References

[1] Daniel J Bernstein. *Curve25519: high-speed elliptic-curve cryptography*. URL: `http://cr.yp.to/ecdh.html#use` (visited on 04/10/2015).

[2] Daniel J Bernstein. *Ed25519 python reference implementation*. URL: `http://ed25519.cr.yp.to/python/ed25519.py` (visited on 04/10/2015).

[3] Daniel J Bernstein, Chitchanok Chuengsatiansup, and Tanja Lange. "Curve41417: Karatsuba revisited". In: *Cryptographic Hardware and Embedded Systems–CHES 2014*. Springer, 2014, pp. 316–334.

[4] Daniel J Bernstein and Tanja Lange. "Analysis and optimization of elliptic-curve single-scalar multiplication". In: *IACR Cryptology ePrint Archive* 2007 (2007), p. 455.

[5] Daniel J Bernstein and Tanja Lange. "Faster addition and doubling on elliptic curves". In: *Advances in cryptology–ASIACRYPT 2007*. Springer, 2007, pp. 29–50.

[6] Daniel J Bernstein and Tanja Lange. "Inverted edwards coordinates". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Springer, 2007, pp. 20–27.

[7] Daniel J Bernstein et al. "High-speed high-security signatures". In: *Journal of Cryptographic Engineering* 2.2 (2012), pp. 77–89.

[8] Daniel J Bernstein et al. "Twisted edwards curves". In: *Progress in Cryptology–AFRICACRYPT 2008*. Springer, 2008, pp. 389–405.

[9] Henri Cohen et al. *Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition*. 2nd. Chapman & Hall/CRC, 2012. ISBN: 1439840008, 9781439840009.

[10] William Stein John Cremona. *Elliptic curve constructor*. URL: http://www.sagemath.org/doc/reference/plane_curves/sage/schemes/elliptic_curves/constructor.html (visited on 04/27/2015).

[11] user Samuel Neves Cryptography Stack Exchange. *Why are the lower 3 bits of curve25519/ed25519 secret keys cleared during creation?* URL: http://crypto.stackexchange.com/a/12614 (visited on 04/10/2015).

[12] Internet Engineering Task Force. *EdDSA and Ed25519*. URL: http://tools.ietf.org/html/draft-josefsson-eddsa-ed25519-02#section-5 (visited on 04/15/2015).

[13] Groupprops. *Multiplicative group of a finite field is cyclic*. URL: http://groupprops.subwiki.org/wiki/Multiplicative_group_of_a_finite_field_is_cyclic (visited on 04/07/2016).

[14] Christian Hanser. "New Trends in Elliptic Curve Cryptography". masthesis. Institute of Applied Information Processing and Communications, 2010. URL: https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=51075 (visited on 04/10/2015).

[15] Helmut Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung." In: *Journal für die reine und angewandte Mathematik* 175 (1936), pp. 55–62.

[16] Huseyin Hisil et al. "Twisted Edwards curves revisited". In: *Advances in Cryptology-ASIACRYPT 2008*. Springer, 2008, pp. 326–343.

[17] Tanja Lange. *Explicit-Formulas Database / Weierstrass curves*. URL: https://hyperelliptic.org/EFD/oldefd/weierstrass.html (visited on 04/27/2015).

[18] Katsuyuki Okeya and Kouichi Sakurai. "Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve". In: *CHES*. Vol. 2162. Springer. 2001, pp. 126–141.

[19] open books for an open world Wikibooks. *Algorithm Implementation/Mathematics/Extended Euclidean algorithm*. URL: http://en.wikibooks.org/wiki/Algorithm_Implementation/Mathematics/Extended_Euclidean_algorithm#Python (visited on 04/10/2015).

[20] the free encyclopedia Wikipedia. *Curve25519*. URL: https://en.wikipedia.org/wiki/Curve25519 (visited on 04/10/2015).

[21] the free encyclopedia Wikipedia. *EdDSA*. URL: https://en.wikipedia.org/wiki/EdDSA (visited on 04/10/2015).

[22] the free encyclopedia Wikipedia. *Montgomery curve*. URL: http://en.wikipedia.org/wiki/Montgomery_curve#Equivalence_with_twisted_Edwards_curves (visited on 04/10/2015).