Elligator

Chris Anto Fröschl

August 8, 2026

Chapter 1

Elligator 1

Definition 1 (The quadratic character χ)**.** Fix a prime power $q \equiv 3 \pmod 4$. Define $\chi : \mathbb{F}_q \to \mathbb{F}_q$ as the quadratic character of $\mathbb{F}_q$, with its values $0, \pm 1$ read inside $\mathbb{F}_q$; equivalently

$$\chi(a) = a^{(q-1)/2}.$$

If a is a nonzero square then $\chi(a) = 1$; if a is a non-square then $\chi(a) = -1$; if $a = 0$ then $\chi(a) = 0$.

Definition 2 (The curve parameter c)**.** Let q be a prime power congruent to 3 modulo 4, and let s be a nonzero element of $\mathbb{F}_q$ with $(s^2 - 2)(s^2 + 2) \neq 0$. Define

$$c = 2/s^2.$$

Definition 3 (The curve parameter r)**.** With $c = 2/s^2$ as above, define

$$r = c + 1/c.$$

Definition 4 (The Edwards curve coefficient d)**.** With $c = 2/s^2$ as above, define

$$d = -(c + 1)^2/(c - 1)^2,$$

the coefficient of the complete Edwards curve $E : x^2 + y^2 = 1 + dx^2y^2$.

Definition 5 (The auxiliary quantity u)**.** For $t \in \mathbb{F}_q \setminus \{\pm 1\}$ define

$$u = (1 - t)/(1 + t).$$

Definition 6 (The auxiliary quantity v)**.** For $t \in \mathbb{F}_q \setminus \{\pm 1\}$, with u and r as above, define

$$v = u^5 + (r^2 - 2)u^3 + u.$$

Definition 7 (The auxiliary coordinate X)**.** For $t \in \mathbb{F}_q \setminus \{\pm 1\}$, with u and v as above and χ the quadratic character of $\mathbb{F}_q$, define

$$X = \chi(v)u.$$

Definition 8 (The auxiliary coordinate Y)**.** For $t \in \mathbb{F}_q \setminus \{\pm 1\}$, with u, v and c as above, define

$$Y = (\chi(v)v)^{(q+1)/4}\chi(v)\chi(u^2 + 1/c^2).$$

Definition 9 (The curve coordinate x)**.** For $t \in \mathbb{F}_q \setminus \{\pm 1\}$, with c, X and Y as above, define

$$x = (c-1)sX(1+X)/Y.$$

Definition 10 (The curve coordinate y)**.** For $t \in \mathbb{F}_q \setminus \{\pm 1\}$, with r and X as above, define

$$y = (rX - (1+X)^2)/(rX + (1+X)^2).$$

Definition 11 (The inversion quantity η)**.** For a point (x, y) of $E(\mathbb{F}_q)$ with $y + 1 \neq 0$, define

$$\eta = \frac{y-1}{2(y+1)}.$$

Definition 12 (The reconstructed coordinate $\bar{X}$)**.** For a point $(x, y) \in \varphi(\mathbb{F}_q)$, with η as above, define

$$\bar{X} = -(1+\eta r) + ((1+\eta r)^2 - 1)^{(q+1)/4}.$$

Definition 13 (The inversion sign z)**.** For a point $(x, y) \in \varphi(\mathbb{F}_q)$, with $\bar{X}$ as above, define

$$z = \chi((c-1)s\bar{X}(1+\bar{X})x(\bar{X}^2 + 1/c^2)).$$

Definition 14 (The reconstructed quantity $\bar{u}$)**.** For a point $(x, y) \in \varphi(\mathbb{F}_q)$, with z and $\bar{X}$ as above, define

$$\bar{u} = z\bar{X}.$$

Definition 15 (The reconstructed preimage $\bar{t}$)**.** For a point $(x, y) \in \varphi(\mathbb{F}_q)$, with $\bar{u}$ as above, define

$$\bar{t} = (1-\bar{u})/(1+\bar{u}).$$

Definition 16 (The string length b)**.** For a prime q, define the length of the encoded bit strings as

$$b = \lfloor \log_2 q \rfloor.$$

Definition 17 (Binary value of a bit string)**.** A bit string $(\tau_0, \tau_1, \ldots, \tau_{n-1}) \in \{0,1\}^n$ has binary value

$$\sum_i \tau_i 2^i \in \mathbb{Z}_{\geq 0}.$$

Definition 18 (The string-to-field map σ)**.** Define $\sigma : \{0,1\}^b \to \mathbb{F}_q$ by

$$\sigma(\tau_0, \tau_1, \ldots, \tau_{b-1}) = \sum_i \tau_i 2^i.$$

Definition 19 (The admissible string set S)**.** Define the set of admissible bit strings as

$$S = \sigma^{-1}(\{0, 1, 2, \ldots, (q-1)/2\}),$$

i.e. the strings whose binary value lies in the lower half of $\mathbb{F}_q$.

Theorem 20 ($c(c-1)(c+1) \neq 0$)**.** *In the situation of Theorem 1, $c = 2/s^2$ satisfies*

$$c(c-1)(c+1) \neq 0.$$

Proof. □

Theorem 21 ($r \neq 0$)**.** *In the situation of Theorem 1, $r = c + 1/c \neq 0$: if $r = 0$ then $c = -1/c$, so $c^2 = -1$, a contradiction since -1 is not a square in $\mathbb{F}_q$.*

Proof. □

Theorem 22 (d is not a square)**.** *In the situation of Theorem 1, $d = -(c+1)^2/(c-1)^2$ is not a square in $\mathbb{F}_q$: otherwise $-1 = d(c-1)^2/(c+1)^2$ would be a square, a contradiction.*

Proof. □

Definition 23 (The complete Edwards curve equation)**.** For a coefficient $d \notin \{0, 1\}$, the complete Edwards curve E over $\mathbb{F}_q$ is given by the equation

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

Definition 24 (The point set $E(\mathbb{F}_q)$)**.** With $d = -(c+1)^2/(c-1)^2$ as in Theorem 1, let

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : x^2 + y^2 = 1 + dx^2y^2\}$$

be the set of affine points of the complete Edwards curve E.

Theorem 25 ($(0, 1)$ is a point of E)**.** *The neutral point $(0, 1)$, which is the value of $\varphi(\pm 1)$ in Definition 2, lies on the complete Edwards curve $E : x^2 + y^2 = 1 + dx^2y^2$.*

Proof. □

Theorem 26 ($u \neq 0$)**.** *In the situation of Theorem 1, $u = (1-t)/(1+t) \neq 0$ for $t \in \mathbb{F}_q \setminus \{\pm 1\}$, since $1 - t \neq 0$ and $1 + t \neq 0$.*

Proof. □

Theorem 27 ($v \neq 0$)**.** *In the situation of Theorem 1, $v \neq 0$.*

Proof. □

Theorem 28 ($X \neq 0$)**.** *In the situation of Theorem 1, $X = \chi(v)u \neq 0$, since $u \neq 0$ and $\chi(v) \neq 0$.*

Proof. □

Theorem 29 ($XY \neq 0$, so x is defined)**.** *In the situation of Theorem 1, $XY \neq 0$; in particular $Y \neq 0$, so $x = (c-1)sX(1+X)/Y$ is defined.*

Proof. □

Theorem 30 ($1 + X \neq 0$, so $x \neq 0$)**.** *In the situation of Theorem 1, $1 + X \neq 0$: if $X = -1$ then $u = -\chi(v)$, so $v = -\chi(v)r^2$ and hence $\chi(v) = -\chi(v)$, a contradiction.*

Proof. □

Theorem 31 ($x \neq 0$)**.** *In the situation of Theorem 1, $x = (c-1)sX(1+X)/Y \neq 0$, since $c \neq 1$, $s \neq 0$, $X \neq 0$ and $1 + X \neq 0$.*

Proof. □

Theorem 32 (u is defined)**.** *In the situation of Theorem 1, for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$ the denominator of*

$$u = (1-t)/(1+t)$$

is nonzero, i.e. $1 + t \neq 0$.

Proof. □

Theorem 33 (Y is defined)**.** *In the situation of Theorem 1, the quantity*

$$Y = (\chi(v)v)^{(q+1)/4}\chi(v)\chi(u^2 + 1/c^2)$$

is defined for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$, since $c^2 \neq 0$.

Proof. □

Theorem 34 (x is defined)**.** *In the situation of Theorem 1, $Y \neq 0$ for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$, so that*

$$x = (c-1)sX(1+X)/Y$$

is defined.

Proof. □

Theorem 35 (y is defined)**.** *In the situation of Theorem 1, $rX + (1+X)^2 \neq 0$ for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$, so that*

$$y = (rX - (1+X)^2)/(rX + (1+X)^2)$$

is defined.

Proof. □

Theorem 36 ((X, Y) lies on the auxiliary curve)**.** *In the situation of Theorem 1, let $t \in \mathbb{F}_q \setminus \{\pm 1\}$ and let r, X, Y be as above. Then*

$$Y^2 = X^5 + (r^2 - 2)X^3 + X$$

Proof. □

Theorem 37 (Nonvanishing of the auxiliary quantities)**.** *In the situation of Theorem 1, let $t \in \mathbb{F}_q \setminus \{\pm 1\}$ and let u, v, X, Y, x, y be as above. Then*

$$uvXYx(y+1) \neq 0.$$

Proof. □

Theorem 38 ((x, y) lies on the Edwards curve)**.** *In the situation of Theorem 1, let $t \in \mathbb{F}_q \setminus \{\pm 1\}$ and let x, y be as above. Then (x, y) is a point of the complete Edwards curve $E : x^2 + y^2 = 1 + dx^2y^2$, i.e.*

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

Proof. □

Definition 39 (The decoding function φ)**.** In the situation of Theorem 1, the decoding function for the complete Edwards curve $E : x^2 + y^2 = 1 + dx^2y^2$ is the function $\varphi : \mathbb{F}_q \to E(\mathbb{F}_q)$ defined as follows:

$$\varphi(\pm 1) = (0, 1);$$

if $t \notin \{\pm 1\}$ then $\varphi(t) = (x, y)$.

Definition 40 (Image condition 1: $y + 1 \neq 0$)**.** The first of the three conditions characterizing $\varphi(\mathbb{F}_q)$ inside $E(\mathbb{F}_q)$ in Theorem 3: a point (x, y) satisfies

$$y + 1 \neq 0.$$

Definition 41 (Image condition 2: $(1+\eta r)^2-1$ is a square)**.** The second of the three conditions characterizing $\varphi(\mathbb{F}_q)$ inside $E(\mathbb{F}_q)$ in Theorem 3: a point (x, y) satisfies that

$$(1 + \eta r)^2 - 1$$

is a square, where $\eta = (y - 1)/(2(y + 1))$.

Definition 42 (Image condition 3: the exceptional case $\eta r = -2$)**.** The third of the three conditions characterizing $\varphi(\mathbb{F}_q)$ inside $E(\mathbb{F}_q)$ in Theorem 3: a point (x, y) satisfies that if $\eta r = -2$ then

$$x = 2s(c - 1)\chi(c)/r.$$

Definition 43 (The image conditions of Theorem 3)**.** The conjunction of the three conditions of Theorem 3 for a point $(x, y) \in E(\mathbb{F}_q)$: $y + 1 \neq 0$; $(1 + \eta r)^2 - 1$ is a square, where $\eta = (y - 1)/(2(y + 1))$; and if $\eta r = -2$ then $x = 2s(c - 1)\chi(c)/r$.

Definition 44 (The image $\varphi(\mathbb{F}_q)$)**.** The image of the decoding function of Definition 2,

$$\varphi(\mathbb{F}_q) = \{\varphi(t) : t \in \mathbb{F}_q\} \subseteq E(\mathbb{F}_q).$$

Theorem 45 (Points of $\varphi(\mathbb{F}_q)$ satisfy the image conditions)**.** *The forward part of statement 2 of Theorem 3: every $(x, y) \in \varphi(\mathbb{F}_q)$ satisfies $y + 1 \neq 0$; $(1 + \eta r)^2 - 1$ is a square, where $\eta = (y - 1)/(2(y + 1))$; and if $\eta r = -2$ then $x = 2s(c - 1)\chi(c)/r$.*

Proof. □

Definition 46 (Coordinates of the decoding function)**.** In the situation of Theorem 1, the decoding function for the complete Edwards curve $E : x^2 + y^2 = 1 + dx^2y^2$ is the function $\varphi : \mathbb{F}_q \to E(\mathbb{F}_q)$ with

$$\varphi(\pm 1) = (0, 1), \qquad \varphi(t) = (x, y) \text{ for } t \notin \{\pm 1\}.$$

Here φ is regarded as a map $\mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q$, forgetting the proof that the image lies on E.

Theorem 47 ($2^b \leq q$)**.** *With $b = \lfloor \log_2 q \rfloor$ we have $2^b \leq q$; hence the integers $0, 1, \ldots, 2^b - 1$ are distinct in $\mathbb{F}_q$.*

Proof. □

Theorem 48 (Binary evaluation is injective)**.** *Distinct bit strings of length n have distinct binary values $\sum_i \tau_i 2^i$.*

Proof. □

Theorem 49 (Binary evaluation is onto $\{0, \dots, 2^n - 1\}$)**.** *Every integer m with $0 \le m < 2^n$ is the binary value of some bit string of length n.*

Proof. □

Theorem 50 (The lower half contains no pair of negatives)**.** *Let q be prime and let $a, b \in \{0, 1, \dots, (q-1)/2\}$ with $a = -b$ in $\mathbb{F}_q$. Then $a = b$. This is the step of Theorem 4 that removes the sign ambiguity of φ.*

Proof. □

Theorem 51 (σ is injective)**.** *Since $2^b \le q$, the integers $0, 1, \dots, 2^b - 1$ are distinct in $\mathbb{F}_q$; hence σ is injective.*

Proof. □

Theorem 52 (Preimages under σ of the lower half)**.** *Since $2^b > q/2$, the set $\{0, 1, \dots, (q-1)/2\}$ is a subset of $\{0, 1, \dots, 2^b - 1\}$; hence each of $0, 1, \dots, (q-1)/2$ has a preimage under σ, lying in S.*

Proof. □

Theorem 53 (Every field element is $\pm\sigma(\tau)$ for some $\tau \in S$)**.** *For every $t \in \mathbb{F}_q$, at least one of $t, -t$ lies in $\{0, 1, \dots, (q-1)/2\} = \sigma(S)$; that is, there is $\tau \in S$ with $\sigma(\tau) = t$ or $\sigma(\tau) = -t$.*

Proof. □

Theorem 54 ($\bar{t} = \pm t$)**.** *For $t \in \mathbb{F}_q$, the parameter $\bar{t}$ reconstructed from $\varphi(t)$ in Theorem 3.3 satisfies $\bar{t} = t$ or $\bar{t} = -t$. This is the key step showing that $\varphi(t)$ has no preimages besides t and $-t$.*

Proof. □

Theorem 55 ($\varphi(t) = \varphi(-t)$)**.** *The forward part of statement 1 of Theorem 3: for every $t \in \mathbb{F}_q$,*

$$\varphi(t) = \varphi(-t).$$

Proof. □

Theorem 56 (φ has no preimages besides t and $-t$)**.** *The reverse part of statement 1 of Theorem 3: for $t \in \mathbb{F}_q$, no element of $\mathbb{F}_q$ other than t and $-t$ is a preimage of $\varphi(t)$ under φ.*

Proof. □

Theorem 57 (The image conditions characterize $\varphi(\mathbb{F}_q)$)**.** *The reverse part of statement 2 of Theorem 3: every $(x, y) \in E(\mathbb{F}_q)$ such that $y + 1 \neq 0$; $(1 + \eta r)^2 - 1$ is a square, where $\eta = (y-1)/(2(y+1))$; and $x = 2s(c-1)\chi(c)/r$ whenever $\eta r = -2$, lies in $\varphi(\mathbb{F}_q)$.*

Proof. □

Theorem 58 (Theorem 3.1: the fibers of φ)**.** *In the situation of Definition 2: if $t \in \mathbb{F}_q$ then the set of preimages of $\varphi(t)$ under φ is $\{t, -t\}$. Equivalently, $\varphi(t) = \varphi(-t)$ if and only if no element of $\mathbb{F}_q$ other than t and $-t$ maps to $\varphi(t)$.*

Proof. □

Theorem 59 (Theorem 3.2: the image of φ)**.** *In the situation of Definition 2:* $\varphi(\mathbb{F}_q)$ *is the set of* $(x, y) \in E(\mathbb{F}_q)$ *such that*

- $y + 1 \neq 0$*;*
- $(1 + \eta r)^2 - 1$ *is a square, where* $\eta = \frac{y-1}{2(y+1)}$*; and*
- *if* $\eta r = -2$ *then* $x = 2s(c-1)\chi(c)/r$*.*

Proof. □

Theorem 60 (Theorem 3.3: inverting φ)**.** *In the situation of Definition 2: if* $(x, y) \in \varphi(\mathbb{F}_q)$ *then the following elements* $\bar{X}, z, \bar{u}, \bar{t}$ *of* $\mathbb{F}_q$ *are defined and* $\varphi(\bar{t}) = (x, y)$*:*

$$\begin{aligned} \bar{X} &= -(1 + \eta r) + ((1 + \eta r)^2 - 1)^{(q+1)/4}, \\ z &= \chi((c-1)s\bar{X}(1 + \bar{X})x(\bar{X}^2 + 1/c^2)), \\ \bar{u} &= z\bar{X}, \\ \bar{t} &= (1 - \bar{u})/(1 + \bar{u}). \end{aligned}$$

Proof. □

Theorem 61 ($\bar{X}$ is defined)**.** *For* $(x, y) \in \varphi(\mathbb{F}_q)$ *the denominator* $2(y + 1)$ *of* η *is nonzero, so* η *and hence* $\bar{X}$ *of Theorem 3.3 are defined.*

Proof. □

Theorem 62 (z is defined)**.** *The denominator* c^2 *occurring in* z *of Theorem 3.3 is nonzero, so* z *is defined.*

Proof. □

Theorem 63 ($\bar{t}$ is defined)**.** *For* $(x, y) \in \varphi(\mathbb{F}_q)$ *the denominator* $1 + \bar{u}$ *of* $\bar{t}$ *in Theorem 3.3 is nonzero, so* $\bar{t}$ *is defined.*

Proof. □

Theorem 64 (Binary values of the admissible strings)**.** *Since* $2^b \leq q$ *and* $2^b > q/2$*, each of* $0, 1, \ldots, (q-1)/2$ *has a preimage under* σ*, and the binary values of the strings in* S *are exactly*

$$\{0, 1, \ldots, (q-1)/2\}.$$

Proof. □

Theorem 65 ($\#S$ equals the size of the lower half)**.** *Binary evaluation is injective, hence*

$$\#S = \#\{0, 1, \ldots, (q-1)/2\}.$$

Proof. □

Theorem 66 ($\#S = (q+1)/2$)**.** *For* $q \equiv 3 \pmod 4$*, the set* S *has exactly*

$$\#S = (q + 1)/2$$

elements.

Proof. □

Definition 67 (The string encoding ι)**.** In the situation of Definition 2, assume that q is prime, and let b, σ and S be as above. Define

$$\iota : S \to E(\mathbb{F}_q)$$

by $\iota(\tau) = \varphi(\sigma(\tau))$.

Theorem 68 (Theorem 4.1: cardinality of S)**.** *In the situation of Theorem 4, the set of admissible strings satisfies*

$$\#S = (q+1)/2.$$

Proof. □

Theorem 69 (Theorem 4.2: injectivity of ι)**.** *In the situation of Theorem 4, ι is an injective map from S to $E(\mathbb{F}_q)$.*

Proof. □

Definition 70 (The image $\iota(S)$)**.** The set of curve points produced by the string encoding,

$$\iota(S) = \{\varphi(\sigma(\tau)) : \tau \in S\} \subseteq E(\mathbb{F}_q).$$

Theorem 71 (Theorem 4.3: $\iota(S) = \varphi(\mathbb{F}_q)$)**.** *In the situation of Theorem 4, $\iota(S) = \varphi(\mathbb{F}_q)$.*

Proof. □

Definition 72 (The encoding ι as a map onto $\varphi(\mathbb{F}_q)$)**.** The string encoding of Theorem 4, viewed as a map

$$\iota : S \to \varphi(\mathbb{F}_q)$$

with codomain the image of φ rather than all of $E(\mathbb{F}_q)$.

Theorem 73 (ι is a bijection from S onto $\varphi(\mathbb{F}_q)$)**.** *Combining the injectivity of ι with $\iota(S) = \varphi(\mathbb{F}_q)$: the map*

$$\iota : S \to \varphi(\mathbb{F}_q)$$

is a bijection.

Proof. □

Definition 74 (Binary modular exponentiation)**.** For a modulus m, a fuel bound $fuel$, a base b and an exponent e define powMod by binary exponentiation, so that $\mathrm{powMod}(m, fuel, b, e) = b^e \bmod m$ whenever $e < 2^{fuel}$.

Theorem 75 (The Pratt primality criterion)**.** *Let p be a natural number and let L be a list of primes with $\prod_{r \in L} r = p - 1$. If there is an a with $a^{p-1} \equiv 1 \pmod{p}$ and $a^{(p-1)/r} \not\equiv 1 \pmod{p}$ for every $r \in L$, then p is prime.*

Proof. □

Definition 76 (The Curve1174 characteristic q)**.** Curve1174 is defined over $\mathbb{F}_q$ with

$$q = 2^{251} - 9.$$

Theorem 77 (q is prime)**.** *The number $q = 2^{251} - 9$ is prime.*

Proof. □

Definition 78 (The Curve1174 base field)**.** Let $\mathbb{F}_q$ be the prime field with $q = 2^{251} - 9$ elements.

Theorem 79 ($q \equiv 3 \pmod 4$)**.** *The characteristic satisfies $q \equiv 3 \pmod 4$, so the standing hypotheses of Elligator 1 are met by $\mathbb{F}_q$.*

Proof. □

Definition 80 (The Curve1174 parameter s)**.** Define $s \in \mathbb{F}_q$ to be

$$s = 1806494121122717992522804053500797229648438766985538871240722010849934886421.$$

Theorem 81 (s satisfies the hypotheses of Theorem 1)**.** *The element s is nonzero and satisfies $(s^2 - 2)(s^2 + 2) \neq 0$.*

Proof. □

Theorem 82 (The value of c for Curve1174)**.** *With s as above, $c = 2/s^2$ equals*

$$2179648967284864129978754827181620133949030013113193603783078030367640144353.$$

Proof. □

Theorem 83 (The value of r for Curve1174)**.** *With c as above, $r = c + 1/c$ equals*

$$1696655186501596000718351496024572392351302524672376124832205648027286373 15.$$

Proof. □

Theorem 84 (The Elligator 1 curve for (q, s) is Curve1174)**.** *With $c = 2/s^2$ as above,*

$$d = -(c+1)^2/(c-1)^2 = -1174,$$

so the complete Edwards curve of Theorem 1 and Definition 2 for this choice of (q, s) is exactly Curve1174, $x^2 + y^2 = 1 - 1174x^2y^2$.

Proof. □

Theorem 85 ($\chi(-1174) = -1$)**.** *The quadratic character of the Edwards coefficient satisfies $\chi(d) = -1$.*

Proof. □

Theorem 86 (-1174 is a non-square)**.** *The coefficient -1174 is a non-square in $\mathbb{F}_q$; this is the criterion of [bernstein2013a, Theorem 3.3] making Curve1174 a complete Edwards curve.*

Proof. □

Definition 87 (Curve1174)**.** Curve1174 is the complete Edwards curve

$$x^2 + y^2 = 1 - 1174x^2y^2$$

over $\mathbb{F}_q$, obtained from the Elligator 1 construction with the parameter s.

Definition 88 (The Curve1174 decoding function)**.** The map $\varphi : \mathbb{F}_q \to E(\mathbb{F}_q)$ of Definition 2, specialised to Curve1174.

Theorem 89 (Theorem 1 for Curve1174)**.** *For every $t \in \mathbb{F}_q$ the point $\varphi(t)$ lies on Curve1174.*

Proof. □

Theorem 90 (Curve1174 encodes to 250-bit strings)**.** *For Curve1174 the string length of Theorem 4 is $b = \lfloor \log_2 q \rfloor = 250$.*

Proof. □

Theorem 91 (Theorem 4 for Curve1174)**.** *For Curve1174 the string encoding ι is a bijection from S onto $\varphi(\mathbb{F}_q)$.*

Proof. □

Definition 92 (The Curve1174 base point)**.** The base point of [bernstein2013a], Section 4.1 is $(x, y) = (4/V, 3/5)$, where V is the V-coordinate of the point of order $4p_1$ on the Montgomery model at $U = 4$.

Theorem 93 (The Montgomery base point)**.** *The point $(U, V) = (4, V)$ lies on the Montgomery curve*

$$(4/1175)V^2 = U^3 + (4/1175 - 2)U^2 + U.$$

Proof. □

Theorem 94 (The base point lies on Curve1174)**.** *The point $(4/V, 3/5)$ satisfies the Curve1174 equation.*

Proof. □