Computing 2-isogenies on Kummer lines

Nicolas Sarkis
Advisors: Razvan Barbulescu and Damien Robert

Institut de Mathématiques de Bordeaux

October 31st, 2023 – Isogeny Club

Outline

Montgomery curves

Elliptic curves (char $k \neq 2, 3$)

- Short Weierstrass (general case):

$$E : y^2 = x^3 + ax + b$$

- Montgomery curves:

$$E : By^2 = x(x^2 + Ax + 1)$$

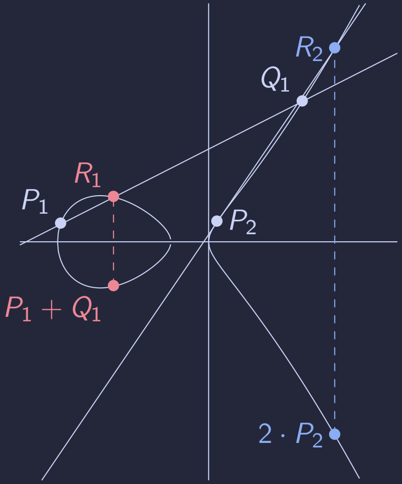

Figure: A Montgomery curve

Kummer lines

Focus on Montgomery curves:

$$E : By^2 = x(x^2 + Ax + 1)$$

If $P = (x : y : z)$, then $-P = (x : -y : z)$. If one forgets about the sign of y, we get a Kummer line $\mathcal{K} = E/\{\pm 1\}$.

Montgomery *xz*-coordinates

This map is a degree 2 covering ($\pi^{-1}(x : z) = \{(x : \pm y : z)\}$ except if $y = 0$):

$$E \xrightarrow{\pi} \mathbb{P}^1$$
$$(x : y : z) \mapsto \begin{cases} (0 : 1) & \text{if } (x : y : z) = (0 : 1 : 0) \\ (x : z) & \text{otherwise} \end{cases}$$

Notation: $\pi(P) = [P]$.

What about the addition law?

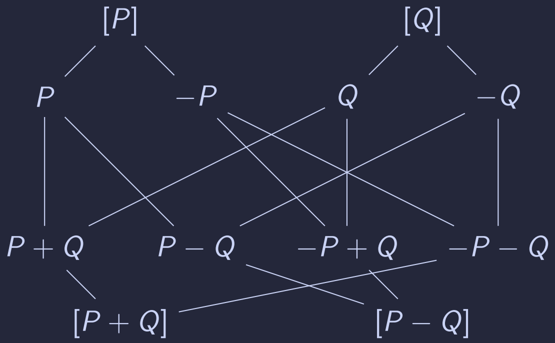

Figure: Two possible choices

What about the addition law?

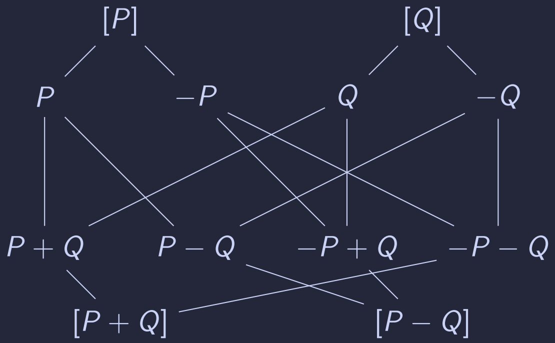

Figure: Two possible choices

However, if we know $[P]$, $[Q]$, $[P-Q]$, we can compute $[P+Q]$

Differential addition and doubling [Mon87]

- M is the cost of a multiplication in k, S the cost of a square in k.
- m_0 is the cost of a multiplication by a curve constant in k.

Differential addition $(3M + 2S)$

Set $u := (x_P + z_P)(x_Q - z_Q)$ and $v := (x_P - z_P)(x_Q + z_Q)$

$$x_{P+Q} = (u+v)^2 \qquad z_{P+Q} = \frac{x_{P-Q}}{z_{P-Q}}(u-v)^2$$

Doubling $(2M + 2S + 1m_0,\ d = \frac{A+2}{4})$

Set $u := (x_P + z_P)^2$, $v := (x_P - z_P)^2$ and $t := u - v$

$$x_{2.P} = uv \qquad z_{2.P} = t(v + dt)$$

Algorithm 1: Montgomery ladder

Input: $[R] = [m \cdot P]$, $[S] = [(m+1) \cdot P]$, b a bit
Output: $([2 \cdot R], [R+S])$ if $b = 0$ $([R+S], [2 \cdot S])$ if $b = 1$
Data: The point $[P]$

```
Function MontgomeryLadder([R], [S], b):
    if b = 0 then
        [S] ← DiffAdd([R], [S], [P]);
        [R] ← Doubling([R]);
    else if b = 1 then
        [R] ← DiffAdd([R], [S], [P]);
        [S] ← Doubling([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

P

Figure: Chaining ladder

Algorithm 1: Montgomery ladder

Input: $[R] = [m \cdot P]$, $[S] = [(m+1) \cdot P]$, b a bit
Output: $([2 \cdot R], [R+S])$ if $b = 0$ $([R+S], [2 \cdot S])$ if $b = 1$
Data: The point $[P]$

```
Function MontgomeryLadder([R], [S], b):
    if b = 0 then
        [S] ← DiffAdd([R], [S], [P]);
        [R] ← Doubling([R]);
    else if b = 1 then
        [R] ← DiffAdd([R], [S], [P]);
        [S] ← Doubling([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

$P \longrightarrow 2P$

Figure: Chaining ladder

Algorithm 1: Montgomery ladder

Input: $[R] = [m \cdot P]$, $[S] = [(m+1) \cdot P]$, b a bit
Output: $([2 \cdot R], [R+S])$ if $b = 0$ $([R+S], [2 \cdot S])$ if $b = 1$
Data: The point $[P]$

```
Function MontgomeryLadder([R], [S], b):
    if b = 0 then
        [S] ← DiffAdd([R], [S], [P]);
        [R] ← Doubling([R]);
    else if b = 1 then
        [R] ← DiffAdd([R], [S], [P]);
        [S] ← Doubling([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

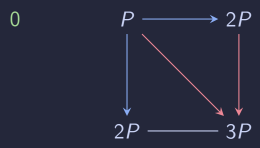

Figure: Chaining ladder

Algorithm 1: Montgomery ladder

Input: $[R] = [m \cdot P]$, $[S] = [(m+1) \cdot P]$, b a bit
Output: $([2 \cdot R], [R+S])$ if $b = 0$ $([R+S], [2 \cdot S])$ if $b = 1$
Data: The point $[P]$

```
Function MontgomeryLadder([R], [S], b):
    if b = 0 then
        [S] ← DiffAdd([R], [S], [P]);
        [R] ← Doubling([R]);
    else if b = 1 then
        [R] ← DiffAdd([R], [S], [P]);
        [S] ← Doubling([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

$$\begin{tikzcd}
0 & P \arrow[r] \arrow[d] \arrow[dr] & 2P \arrow[d] \\
1 & 2P \arrow[r, dash] \arrow[d] & 3P \arrow[dl] \arrow[d] \\
 & 5P \arrow[r, dash] & 6P
\end{tikzcd}$$

Figure: Chaining ladder

Algorithm 1: Montgomery ladder

Input: $[R] = [m \cdot P]$, $[S] = [(m+1) \cdot P]$, b a bit
Output: $([2 \cdot R], [R+S])$ if $b = 0$ $([R+S], [2 \cdot S])$ if $b = 1$
Data: The point $[P]$

```
Function MontgomeryLadder([R], [S], b):
    if b = 0 then
        [S] ← DiffAdd([R], [S], [P]);
        [R] ← Doubling([R]);
    else if b = 1 then
        [R] ← DiffAdd([R], [S], [P]);
        [S] ← Doubling([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

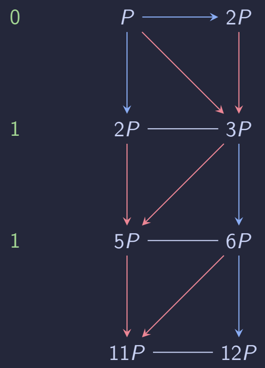

Figure: Chaining ladder

Algorithm 1: Montgomery ladder

Input: $[R] = [m \cdot P]$, $[S] = [(m+1) \cdot P]$, b a bit
Output: $([2 \cdot R], [R+S])$ if $b = 0$ $([R+S], [2 \cdot S])$ if $b = 1$
Data: The point $[P]$

```
Function MontgomeryLadder([R], [S], b):
    if b = 0 then
        [S] ← DiffAdd([R], [S], [P]);
        [R] ← Doubling([R]);
    else if b = 1 then
        [R] ← DiffAdd([R], [S], [P]);
        [S] ← Doubling([S]);
    end
    return ([R], [S]);
```

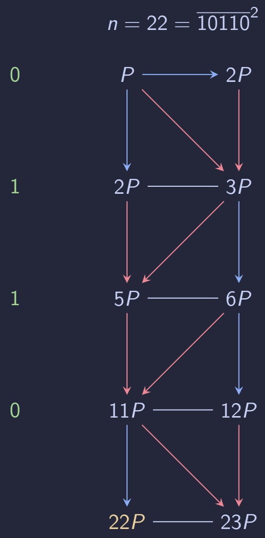

Figure: Chaining ladder

2-isogenies on Montgomery curves [Ren18]

Usage:

- Compute 2^n-isogenies: $E_1 = E \xrightarrow{f_1} E_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} E_{n+1} = E'$, $f = f_n \circ \cdots \circ f_1$.
- Compute $2 \cdot P$: $\hat{f} \circ f(P) = 2 \cdot P$.

2-isogenies with an additional 2-torsion point

Assume $T = (x_T : 0 : z_T)$ is a 2-torsion point with $x_T \neq 0$.
The 2-isogeny $f : E \to E'$ with kernel T is the following on the Kummer line:

$$f : (x : z) \mapsto (x(xx_T - zz_T) : z(xz_T - zx_T))$$

The co-domain $E' : B'y^2 = x(x^2 + A'x + 1)$ is given by:

$$(A' + 2 : 4) = (x_T^2 - z_T^2 : z_T^2)$$

Costs summary

2-isogenies on Montgomery curves

- Co-domain: $2S + 1a$.
- Image: $4M + 6a$ ($4M + 4a$ with a pre-computation).
- Doubling: $4M + 2S + 4a$.

Remark

We had earlier $2M + 2S + 1m_0$ for doubling. While chaining isogenies, we lose control on our constants, so $m_0 = 2M$ (given as numerator + denominator)

Costs summary

2-isogenies on Montgomery curves

- Co-domain: $2S + 1a$.
- Image: $4M + 6a$ ($4M + 4a$ with a pre-computation).
- Doubling: $4M + 2S + 4a$.

Remark

We had earlier $2M + 2S + 1m_0$ for doubling. While chaining isogenies, we lose control on our constants, so $m_0 = 2M$ (given as numerator + denominator)

For a 4-isogeny, we can chain two 2-isogenies (doubles the cost), or we can do better. . .

4-isogenies on Montgomery curves [CH17]

4-isogenies with an additional 4-torsion point

Assume $T = (x_T : * : z_T)$ is a 4-torsion point.
The 4-isogeny $f : E \to E'$ with kernel T is the following on the Kummer line:

$$\begin{aligned} f : (x : z) \mapsto & (x(2x_T z_T z - (x_T^2 + z_T^2)x)(x_T x - z_T z)^2 : \\ & z(2x_T z_T x - (x_T^2 + z_T^2)z)(z_T x - x_T z)^2) \end{aligned}$$

The co-domain $E' : B'y^2 = x(x^2 + A'x + 1)$ is given by:

$$(A' + 2 : 4) = (x_T^4 - z_T^4 : z_T^4)$$

The image can be computed in $6M + 2S + 6a$, better than $2 \times (4M + 4a)$.

Theta models

Motivation

Why are we doing that?

- We look for other maps $E \to \mathbb{P}^1$ with good arithmetic.
- Theta models provide that.
- They generalize to higher dimension.

Remark

Every elliptic curve E can be written in short Weierstrass form. Depending on the property of E and the field k, it can be put in different models (Montgomery, twisted Edwards, theta, ...). In ECC, we can choose a convenient curve with a convenient model, we won't discuss the classification here.

- Montgomery: one rational 4-torsion point on the Kummer line.
- Theta: two independent rational 4-torsion point on the Kummer line.

Motivation

Why are we doing that?

- We look for other maps $E \to \mathbb{P}^1$ with good arithmetic.
- Theta models provide that.
- They generalize to higher dimension.

Remark

Every elliptic curve E can be written in short Weierstrass form. Depending on the property of E and the field k, it can be put in different models (Montgomery, twisted Edwards, theta, ...). In ECC, we can choose a convenient curve with a convenient model, we won't discuss the classification here.

- Montgomery: one rational 4-torsion point on the Kummer line.
- Theta: two independent rational 4-torsion point on the Kummer line.

We will work on $\mathbb{C}$ (generalizes well thanks to Lefschetz principle).
An elliptic curve is then $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ with $\tau \in \mathbb{H}$ (upper half-plane).

Theta functions

Jacobi theta function

Let $\tau \in \mathbb{H}$, the Jacobi theta function is:

$$\vartheta(z;\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi n^2\tau + 2i\pi nz)$$

Theta functions

Jacobi theta function

Let $\tau \in \mathbb{H}$, the Jacobi theta function is:

$$\vartheta(z;\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi n^2\tau + 2i\pi nz)$$

Theta functions with characteristics

Let $a, b \in \mathbb{Z}$ (characteristics) and $\ell \in \mathbb{N}^*$ (the level), $\tau \in \mathbb{H}$:

$$\vartheta_\ell\left[a,b\right](z;\tau) = \sum_{n\in\mathbb{Z}} \exp\left(i\pi\left(n+\frac{a}{\ell}\right)^2\tau + 2i\pi\left(n+\frac{a}{\ell}\right)\left(z+\frac{b}{\ell}\right)\right)$$

Functions of level ℓ

Recall $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$.

Function of level ℓ

Let $\tau \in \mathbb{H}$, $\varphi : \mathbb{C} \to \mathbb{C}$ is of level ℓ (associated to τ) if:

$$\forall m \in \mathbb{Z}, \varphi(z+m) = \varphi(z) \text{ and } \varphi(z+m\tau) = \exp(-i\pi\ell m^2\tau - 2i\pi\ell mz)\varphi(z)$$

Denote by $R_{\tau,\ell}$ the vector space of level ℓ functions associated to τ.

Functions of level ℓ

Recall $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$.

Function of level ℓ

Let $\tau \in \mathbb{H}$, $\varphi : \mathbb{C} \to \mathbb{C}$ is of level ℓ (associated to τ) if:

$$\forall m \in \mathbb{Z}, \varphi(z+m) = \varphi(z) \text{ and } \varphi(z+m\tau) = \exp(-i\pi\ell m^2\tau - 2i\pi\ell mz)\varphi(z)$$

Denote by $R_{\tau,\ell}$ the vector space of level ℓ functions associated to τ.

Theorem

$\dim R_{\tau,\ell} = \ell$ (sketch of proof: exhibit bases derived from theta functions)

From now on, $\ell = 2$.

Theta models (finally!)

Examples of basis of $R_{\tau,2}$ and theta constants

- $\theta_0(z) = \vartheta_2[0;0](z;\tau/2)$ and $\theta_1(z) = \vartheta_2[0;1](z;\tau/2)$.
  We call $a = \theta_0(0)$ and $b = \theta_1(0)$ the theta constants.
- Montgomery xz: $x = \vartheta_2[0;1](u;\tau)^2$ and $z = \vartheta_2[1;1](u;\tau)^2$.

Theta models (finally!)

Examples of basis of $R_{\tau,2}$ and theta constants

- $\theta_0(z) = \vartheta_2[0;0](z;\tau/2)$ and $\theta_1(z) = \vartheta_2[0;1](z;\tau/2)$.
  We call $a = \theta_0(0)$ and $b = \theta_1(0)$ the theta constants.
- Montgomery xz: $x = \vartheta_2[0;1](u;\tau)^2$ and $z = \vartheta_2[1;1](u;\tau)^2$.

Theorem (Lefschetz)

Let $R_{\tau,2} = \mathrm{span}(f, g)$, the following map is an embedding:

$$\begin{aligned} \pi : E_\tau/\{\pm 1\} &\to \mathbb{P}^1(\mathbb{C}) \\ [z] &\mapsto (f(z) : g(z)) \end{aligned}$$

If $(f, g) = (\theta_0, \theta_1)$, the image is denoted by $\theta(a : b) \simeq \mathbb{P}^1(\mathbb{C})$ and is called the theta model with theta constants a and b.

Even more models

Theta model (on E_τ)

Constants: $a := \theta_0(0)$ and $b := \theta_1(0)$.
Notation: $\theta(a : b)$.

$$(x : z) := (\theta_0(u) : \theta_1(u)), u \in \mathbb{C}$$

Even more models

Theta model (on E_τ)

Constants: $a := \theta_0(0)$ and $b := \theta_1(0)$.
Notation: $\theta(a:b)$.

$$(x:z) := (\theta_0(u) : \theta_1(u)), u \in \mathbb{C}$$

Dual model (on E_τ)

Constants: $a' := a + b$ and $b' := a - b$.
Notation: $\theta'(a':b')$.

$$H : (x:z) \in \theta(a:b) \mapsto (x+z : x-z)$$

Even more models

Theta model (on E_τ)

Constants: $a := \theta_0(0)$ and $b := \theta_1(0)$.
Notation: $\theta(a : b)$.

$$(x : z) := (\theta_0(u) : \theta_1(u)), u \in \mathbb{C}$$

Dual model (on E_τ)

Constants: $a' := a + b$ and $b' := a - b$.
Notation: $\theta'(a' : b')$.

$$H : (x : z) \in \theta(a : b) \mapsto (x + z : x - z)$$

Theta twisted model (on E_τ)

Constants: a^2 and b^2.
Notation: $\theta_t(a^2 : b^2)$.

$$C : (x : z) \in \theta(a : b) \mapsto (ax : bz)$$

Even more models

Theta model (on E_τ)

Constants: $a := \theta_0(0)$ and $b := \theta_1(0)$.
Notation: $\theta(a : b)$.

$$(x : z) := (\theta_0(u) : \theta_1(u)), u \in \mathbb{C}$$

Dual model (on E_τ)

Constants: $a' := a + b$ and $b' := a - b$.
Notation: $\theta'(a' : b')$.

$$H : (x : z) \in \theta(a : b) \mapsto (x + z : x - z)$$

Theta twisted model (on E_τ)

Constants: a^2 and b^2.
Notation: $\theta_t(a^2 : b^2)$.

$$C : (x : z) \in \theta(a : b) \mapsto (ax : bz)$$

Theta squared model (on $E_{\tau/2}$)

Constants: a^2 and b^2.
Notation: $\theta_s(a^2 : b^2)$

$$S : (x : z) \in \theta(a : b) \mapsto (x^2 : z^2)$$

Relations between models

First two lines are theta models on E_τ.
The last two lines are theta models on the isogenous curve $E_{\tau/2}$.

$$
\begin{tikzcd}
\theta'(a' : b') \arrow[d, shift right] & & & \\
\theta(a : b) \arrow[u, shift right, "H"'] \arrow[r, shift left, "C"] \arrow[d, "S"'] & \theta_t(a^2 : b^2) \arrow[l, shift left, dotted, "\text{if } a/b \in k"] \arrow[r, shift left, "="] & ((\theta')_s)'(a^2 : b^2) \arrow[l, shift left] \arrow[r, shift right] & (\theta')_s(A'^2 : B'^2) \arrow[l, shift right, "H"'] \\
\theta_s(a^2 : b^2) \arrow[r, shift left, "H"] & (\theta_s)'(A'^2 : B'^2) \arrow[l, shift left] \arrow[r, shift left] & (\theta')_t(A'^2 : B'^2) \arrow[l, shift left, "="] \arrow[r, shift left, dotted, "\text{if } A'/B' \in k"] & \theta'(A' : B') \arrow[l, shift left, "C"] \arrow[u, "S"'] \arrow[d, shift left] \\
& & & \theta(A : B) \arrow[u, shift left, "H"]
\end{tikzcd}
$$

Figure: Relation between theta models

Differential addition and doubling on $\theta(a:b)$

We get these from duplication formulas.
We also have the relation $2A'^2 = a^2 + b^2$ and $2B'^2 = a^2 - b^2$.

Differential addition $(2M + 4S + 1m + 1m_0)$

Set $u := (x_P^2 + z_P^2)(x_Q^2 + z_Q^2)$ and $v := \frac{A'^2}{B'^2}(x_P^2 + z_P^2)(x_Q^2 + z_Q^2)$

$$x_{P+Q} = u + v \qquad z_{P+Q} = \frac{x_{P-Q}}{z_{P-Q}}(u - v)$$

Doubling $(4S + 2m_0)$

Set $u := (x_P^2 + z_P^2)^2$ and $v := \frac{A'^2}{B'^2}(x_P^2 + z_P^2)^2$

$$x_{2.P} = u + v \qquad z_{2.P} = \frac{a}{b}(u - v)$$

Differential addition and doubling on $\theta_s(a^2 : b^2)$

Set $X = x^2$ and $Z = z^2$.
We still have the relation $2A'^2 = a^2 + b^2$ and $2B'^2 = a^2 - b^2$.

Differential addition $(3M + 2S + 1m_0)$

Set $u := (X_P + Z_P)(X_Q + Z_Q)$ and $v := \frac{A'^2}{B'^2}(X_P + Z_P)(X_Q + Z_Q)$

$$X_{P+Q} = (u+v)^2 \qquad Z_{P+Q} = \frac{X_{P-Q}}{Z_{P-Q}}(u-v)^2$$

Doubling $(4S + 2m_0)$

Set $u := (X_P + Z_P)^2$ and $v := \frac{A'^2}{B'^2}(X_P + Z_P)^2$

$$X_{2.P} = (u+v)^2 \qquad Z_{2.P} = \frac{a^2}{b^2}(u-v)^2$$

Comparison to Montgomery xz-coordinates

	Montgomery	Theta squared
Diff. Add.	$3M + 2S$	$3M + 2S + 1m_0$
Doubling	$2M + 2S + 1m_0$	$4S + 2m_0$

Table: Comparison of arithmetic

- Differential addition is always slower.
- On $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$ with $p \equiv 3 \bmod 4$, we can reach $S = \frac{2}{3}M$, so doubling should be faster (if m_0 is small)

Relations between Montgomery and theta squared (1/2) [HR19]

Consider the theta squared model $\theta_s(a^2 : b^2)$, and the Montgomery Kummer line M associated to:

$$E : y^2 = x\left(x - \frac{a^2}{b^2}\right)\left(x - \frac{b^2}{a^2}\right)$$

Isomorphism

There is an isomorphism between $\theta_s(a^2 : b^2)$ and M given by:

$$\theta_s(a^2 : b^2) \xrightarrow{\varphi} M$$
$$P_\theta = (x : z) \mapsto P_M = (a^2x - b^2z : b^2x - a^2z)$$
$$P_\theta = (a^2x - b^2z : b^2x - a^2z) \leftarrow P_M = (x : z)$$

We have to spend some multiplications to convert...

Relations between Montgomery and theta squared (2/2) [KS20]

We use the same notations. The following points are of 2-torsion on their respective models:

$$T_\theta = (1:0) \qquad T_M = (a^2 : b^2)$$

Translation map

There is a bijection between $\theta_s(a^2 : b^2)$ and M given by:

$$\begin{aligned} \theta_s(a^2 : b^2) &\xrightarrow{\psi} M \\ P_\theta = (x:z) &\mapsto P_M + T_M = (x:z) \\ P_\theta + T_\theta = (x:z) &\leftarrow\!\shortmid P_M = (x:z) \end{aligned}$$

How can this improve doubling?

If T is a 2-torsion point, $2 \cdot T = \mathcal{O}$, one could do:

$$P_M \xmapsto{\psi^{-1}} P_\theta + T_\theta \xmapsto{[2]} 2 \cdot P_\theta \xmapsto{\psi} 2 \cdot P_M + T_M$$

We have to adapt the ladder to exploit the better doubling formulas of the theta model: hybrid ladder.

Algorithm 2: Hybrid ladder

Input: $[R]$, $[S]$ with $[R-S] \in \{[P], [P+T]\}$, b a bit

Output: $([2 \cdot R + T], [R+S])$ if $b = 0$
$([R+S], [2 \cdot S + T])$ if $b = 1$

Data: The point $[P]$

```
Function HybridLadder([R], [S], b):
    [D] ← [R − S];                              // pre-computed
    if b = 0 then
        [S] ← DiffAddMontgomery([R], [S], [D]);
        [R] ← DoublingTheta([R]);
    else if b = 1 then
        [R] ← DiffAddMontgomery([R], [S], [D]);
        [S] ← DoublingTheta([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

P

Figure: Chaining ladder

Algorithm 2: Hybrid ladder

Input: $[R]$, $[S]$ with $[R - S] \in \{[P], [P + T]\}$, b a bit

Output: $([2 \cdot R + T], [R + S])$ if $b = 0$

$([R + S], [2 \cdot S + T])$ if $b = 1$

Data: The point $[P]$

Function `HybridLadder`$([R], [S], b)$:

    $[D] \leftarrow [R - S]$; `// pre-computed`

    if $b = 0$ **then**

        $[S] \leftarrow$ `DiffAddMontgomery`$([R], [S], [D])$;

        $[R] \leftarrow$ `DoublingTheta`$([R])$;

    else if $b = 1$ **then**

        $[R] \leftarrow$ `DiffAddMontgomery`$([R], [S], [D])$;

        $[S] \leftarrow$ `DoublingTheta`$([S])$;

    end

    return $([R], [S])$;

$$n = 22 = \overline{10110}^2$$

$$P \longrightarrow 2P + T$$

Figure: Chaining ladder

Algorithm 2: Hybrid ladder

Input: $[R]$, $[S]$ with $[R-S] \in \{[P], [P+T]\}$, b a bit

Output: $([2 \cdot R + T], [R+S])$ if $b = 0$
$([R+S], [2 \cdot S + T])$ if $b = 1$

Data: The point $[P]$

```
Function HybridLadder([R], [S], b):
    [D] ← [R − S];                              // pre-computed
    if b = 0 then
        [S] ← DiffAddMontgomery([R], [S], [D]);
        [R] ← DoublingTheta([R]);
    else if b = 1 then
        [R] ← DiffAddMontgomery([R], [S], [D]);
        [S] ← DoublingTheta([S]);
    end
    return ([R], [S]);
```

$n = 22 = \overline{10110}^2$

$$\begin{tikzcd} 0 & P \arrow[r] \arrow[d] \arrow[dr] & 2P+T \arrow[d] \\ & 2P+T \arrow[r, dash] & 3P+T \end{tikzcd}$$

Figure: Chaining ladder

Algorithm 2: Hybrid ladder

Input: $[R]$, $[S]$ with $[R-S] \in \{[P],[P+T]\}$, b a bit

Output: $([2\cdot R+T],[R+S])$ if $b=0$
$([R+S],[2\cdot S+T])$ if $b=1$

Data: The point $[P]$

Function `HybridLadder`$([R],[S],b)$:
  $[D] \leftarrow [R-S]$; `// pre-computed`
  if $b=0$ **then**
    $[S] \leftarrow$ `DiffAddMontgomery`$([R],[S],[D])$;
    $[R] \leftarrow$ `DoublingTheta`$([R])$;
  else if $b=1$ **then**
    $[R] \leftarrow$ `DiffAddMontgomery`$([R],[S],[D])$;
    $[S] \leftarrow$ `DoublingTheta`$([S])$;
  end
  return $([R],[S])$;

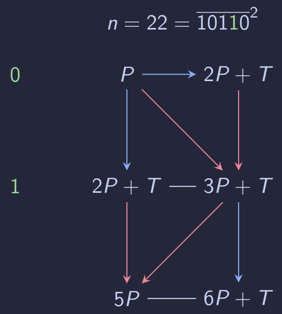

Figure: Chaining ladder

Algorithm 2: Hybrid ladder

Input: $[R]$, $[S]$ with $[R-S] \in \{[P],[P+T]\}$, b a bit
Output: $([2\cdot R+T],[R+S])$ if $b=0$
$([R+S],[2\cdot S+T])$ if $b=1$
Data: The point $[P]$

Function `HybridLadder`$([R],[S],b)$:
  $[D] \leftarrow [R-S]$; // pre-computed
  if $b=0$ **then**
    $[S] \leftarrow$ `DiffAddMontgomery`$([R],[S],[D])$;
    $[R] \leftarrow$ `DoublingTheta`$([R])$;
  else if $b=1$ **then**
    $[R] \leftarrow$ `DiffAddMontgomery`$([R],[S],[D])$;
    $[S] \leftarrow$ `DoublingTheta`$([S])$;
  end
  return $([R],[S])$;

$n = 22 = \overline{10110}^2$

$$\begin{tikzcd}
0 & P \arrow[r] \arrow[d] \arrow[dr] & 2P+T \arrow[d] \\
1 & 2P+T \arrow[r, dash] \arrow[d] & 3P+T \arrow[d] \arrow[dl] \\
1 & 5P \arrow[r, dash] \arrow[d] & 6P+T \arrow[d] \arrow[dl] \\
 & 11P+T \arrow[r, dash] & 12P+T
\end{tikzcd}$$

Figure: Chaining ladder

Algorithm 2: Hybrid ladder

Input: $[R]$, $[S]$ with $[R-S] \in \{[P], [P+T]\}$, b a bit

Output: $([2 \cdot R + T], [R+S])$ if $b = 0$
$([R+S], [2 \cdot S + T])$ if $b = 1$

Data: The point $[P]$

```
Function HybridLadder([R], [S], b):
    [D] ← [R − S];                          // pre-computed
    if b = 0 then
        [S] ← DiffAddMontgomery([R], [S], [D]);
        [R] ← DoublingTheta([R]);
    else if b = 1 then
        [R] ← DiffAddMontgomery([R], [S], [D]);
        [S] ← DoublingTheta([S]);
    end
    return ([R], [S]);
```

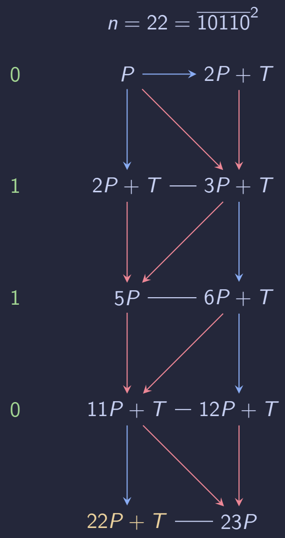

Figure: Chaining ladder

Hybrid ladder proof of concept

Context

- $\mathbb{F}_{p^{10}} = \mathbb{F}_{p^5}[i]$ and $\mathbb{F}_{p^5} = \mathbb{F}_p[u]$ with $i^2 = -1$, $u^5 = 2$.
- Small multiplications are elements of $\mathbb{F}_p$ times elements of $\mathbb{F}_{p^{10}}$.
- Curve constants: $\alpha = 1 + \mu i$, $d = \frac{2-\alpha-\alpha^{-1}}{4} = \nu + i$, $\mu, \nu \in \mathbb{F}_p$
- $x_P, z_P \in \mathbb{F}_{p^{10}}$, i.e. $m = M$.
- 100 random scalar multiplications, repeated 100 times.

TL;DR small constants behave as small constants.

	Montgomery ladder	Hybrid ladder
Average (s)	2.502 ± 0.039	2.348 ± 0.017 (6.2%)

Table: Timings on Intel Core i5-1145G7 @ 2.60GHz

2-isogenies in theta

We are interested in the following 2-isogeny:

$$f : z \in E_\tau \mapsto z \in E_{\tau/2} \qquad \hat{f} : z \in E_{\tau/2} \mapsto 2z \in E_\tau$$

This corresponds to the square operation $(x : z) \in \theta(a : b) \mapsto (x^2 : z^2) \in \theta_s(a^2 : b^2)$

$$\begin{tikzcd}
\theta(a : b) \arrow[d, "S"'] & \theta_t(a^2 : b^2) \arrow[l, "C"'] & (\theta')_s(A'^2 : B'^2) \arrow[l, "H"'] & \theta_s(A^2 : B^2) \\
\theta_s(a^2 : b^2) \arrow[r, "H"'] & (\theta_s)'(A'^2 : B'^2) \arrow[r, "C"'] & \theta'(A' : B') \arrow[u, "S"'] \arrow[r, "H"'] & \theta(A : B) \arrow[u, "S"']
\end{tikzcd}$$

Figure: 2-isogeny on the relation graph

2-isogenies in theta

We are interested in the following 2-isogeny:

$$f : z \in E_\tau \mapsto z \in E_{\tau/2} \qquad \hat{f} : z \in E_{\tau/2} \mapsto 2z \in E_\tau$$

This corresponds to the square operation $(x : z) \in \theta(a : b) \mapsto (x^2 : z^2) \in \theta_s(a^2 : b^2)$

$$\begin{tikzcd}
\theta(a : b) \arrow[d, "S"'] & \theta_t(a^2 : b^2) \arrow[l, "C"'] & (\theta')_s(A'^2 : B'^2) \arrow[l, "H"'] & \theta_s(A^2 : B^2) \\
\theta_s(a^2 : b^2) \arrow[r, "H"'] & (\theta_s)'(A'^2 : B'^2) \arrow[r, "C"'] & \theta'(A' : B') \arrow[r, "H"'] \arrow[u, "S"'] & \theta(A : B) \arrow[u, "S"']
\end{tikzcd}$$

Figure: 2-isogeny on the relation graph

2-isogeny cost (kernel $(-a : b) \in \theta(a : b)$): $2M + 2S + 4a$.

2-isogenies in theta

We are interested in the following 2-isogeny:

$$f : z \in E_\tau \mapsto z \in E_{\tau/2} \qquad \hat{f} : z \in E_{\tau/2} \mapsto 2z \in E_\tau$$

This corresponds to the square operation $(x : z) \in \theta(a : b) \mapsto (x^2 : z^2) \in \theta_s(a^2 : b^2)$

$$\begin{tikzcd}
\theta(a : b) \arrow[d, "S"'] & \theta_t(a^2 : b^2) \arrow[l, "C"'] & (\theta')_s(A'^2 : B'^2) \arrow[l, "H"'] & \theta_s(A^2 : B^2) \\
\theta_s(a^2 : b^2) \arrow[r, "H"'] & (\theta_s)'(A'^2 : B'^2) \arrow[r, "C"'] & \theta'(A' : B') \arrow[u, "S"'] \arrow[r, "H"'] & \theta(A : B) \arrow[u, "S"']
\end{tikzcd}$$

Figure: 2-isogeny on the relation graph

2-isogeny cost (kernel $(1 : 0) \in \theta_s(a^2 : b^2)$): $2M + 2S + 4a$.

2-isogenies in theta

We are interested in the following 2-isogeny:

$$f : z \in E_\tau \mapsto z \in E_{\tau/2} \qquad \hat{f} : z \in E_{\tau/2} \mapsto 2z \in E_\tau$$

This corresponds to the square operation $(x : z) \in \theta(a : b) \mapsto (x^2 : z^2) \in \theta_s(a^2 : b^2)$

$$\begin{tikzcd}
\theta(a : b) \arrow[d, "S"'] & \theta_t(a^2 : b^2) \arrow[l, "C"'] & (\theta')_s(A'^2 : B'^2) \arrow[l, "H"'] & \theta_s(A^2 : B^2) \\
\theta_s(a^2 : b^2) \arrow[r, "H"'] & (\theta_s)'(A'^2 : B'^2) \arrow[r, "C"'] & \theta'(A' : B') \arrow[r, "H"'] \arrow[u, "S"'] & \theta(A : B) \arrow[u, "S"']
\end{tikzcd}$$

Figure: Doubling on the relation graph

Doubling cost: $4M + 4S + 8a$.

Costs summary and Montgomery comparison

2-isogenies on theta squared models

- Co-domain: $2S + 2a$ (not explained).
- Image: $2M + 2S + 4a$.
- Doubling: $4M + 4S + 8a$.

	Montgomery	Theta squared
Co-domain	$2S + 1a$	$2S + 2a$
Image	$4M + 6a$	$2M + 2S + 4a$
Doubling	$4M + 2S + 4a$	$4M + 4S + 8a$

Table: Comparison of 2-isogenies

Costs summary and Montgomery comparison

2-isogenies on theta squared models

- Co-domain: $2S + 2a$ (not explained).
- Image: $2M + 2S + 4a$.
- Doubling: $4M + 4S + 8a$.

	Montgomery	Theta squared
Co-domain	$2S + 1a$	$2S + 2a$
Image	$4M + 6a$	$2M + 2S + 4a$
Doubling	$4M + 2S + 4a$	$4M + 4S + 8a$

Table: Comparison of 2-isogenies

- Similarly to hybrid ladder, we can do hybrid 2-isogenies.
- We are interested in more general formulas with other kernels.

Kummer lines

Similarities in previous constructions

Montgomery curves

$E : By^2 = x(x-\alpha)(x-\alpha^{-1})$ a Montgomery curve.

$$E \xrightarrow{\pi} \mathbb{P}^1$$
$$(x : y : z) \mapsto (x : z) \quad \text{(except } (1:0))$$

This is a degree 2 covering, that is $\pi^{-1}(\pi(P)) = \{-P, P\}$, except for the ramification points:

$$(1:0)^* \qquad (0:1) \qquad (\alpha:1) \qquad (1:\alpha)$$

Similarities in previous constructions

Montgomery curves with extra 2-torsion $(\alpha : 0 : 1)$

2-torsion (ramification points): $(1:0)^*$, $(0:1)$, $(\alpha:1)$, $(1:\alpha)$

Theta model $\theta(a:b)$

Consider theta constants $a, b \in \mathbb{C}$.

$$\pi : E \to E/\{\pm 1\} \to \mathbb{P}^1 \simeq \theta(a:b)$$

This is a degree 2 covering, that is $\pi^{-1}(\pi(P)) = \{-P, P\}$, except for the ramification points:

$$(a:b)^* \qquad (-a:b) \qquad (b:a) \qquad (-b:a)$$

Similarities in previous constructions

Montgomery curves with extra 2-torsion $(\alpha : 0 : 1)$

2-torsion (ramification points): $(1:0)^*$, $(0:1)$, $(\alpha:1)$, $(1:\alpha)$

Theta model $\theta(a:b)$

2-torsion (ramification points): $(a:b)^*$, $(-a:b)$, $(b:a)$, $(-b:a)$

Theta squared model $\theta_s(a^2:b^2)$

2-torsion (ramification points): $(a^2:b^2)^*$, $(b^2:a^2)$, $(1:0)$, $(0:1)$

Kummer lines

Definition

Let E be an elliptic curve, a Kummer line is a degree 2 covering of $\mathbb{P}^1$ with exactly 4 ramification points, one of which is marked:

$$\pi : E \to \mathbb{P}^1$$

$\#\pi^{-1}(P) = 2$ except for 4 ramification points.

Kummer lines

Definition

Let E be an elliptic curve, a Kummer line is a degree 2 covering of $\mathbb{P}^1$ with exactly 4 ramification points, one of which is marked:

$$\pi : E \to \mathbb{P}^1$$

$\#\pi^{-1}(P) = 2$ except for 4 ramification points.

- The 4 ramification points are enough to describe the Kummer line.
- They always correspond to the 2-torsion.
- $\pi^{-1}(\pi(P)) = \{-P, P\}$.

Kummer lines

Definition

Let E be an elliptic curve, a Kummer line is a degree 2 covering of $\mathbb{P}^1$ with exactly 4 ramification points, one of which is marked:

$$\pi : E \to \mathbb{P}^1$$

$\#\pi^{-1}(P) = 2$ except for 4 ramification points.

- The 4 ramification points are enough to describe the Kummer line.
- They always correspond to the 2-torsion.
- $\pi^{-1}(\pi(P)) = \{-P, P\}$.

To study a map between Kummer lines, we only need to look at the 2-torsion.

Canonical example

We want to compute 2-isogenies, so assume we have a curve with a 2-torsion point:

$$E : y^2 = x(x^2 + Ax + \gamma) = x(x-\alpha)(x-\gamma\alpha^{-1}) \text{ (maybe } \alpha \notin k)$$

Notations

The 2-torsion on the Kummer line will be noted as follows:

$$\mathcal{O} = (1:0)^* \qquad T = (0:1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)(= R + T)$$

We have $A = -\alpha - \frac{\gamma}{\alpha} \in k$.

Canonical example

We want to compute 2-isogenies, so assume we have a curve with a 2-torsion point:

$$E : y^2 = x(x^2 + Ax + \gamma) = x(x-\alpha)(x-\gamma\alpha^{-1}) \text{ (maybe } \alpha \notin k)$$

Notations

The 2-torsion on the Kummer line will be noted as follows:

$$\mathcal{O} = (1:0)^* \qquad T = (0:1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)(= R + T)$$

We have $A = -\alpha - \frac{\gamma}{\alpha} \in k$.

We can multiply γ by a square without changing the 2-torsion, because the isomorphisms preserving $\mathcal{O}$ and T are of this shape:

$$(x : z) \mapsto (\lambda x : z) \qquad \lambda \in k$$

Therefore, R is sent to $(\lambda\alpha : 1) = (\alpha' : 1)$ and S to $(\lambda\gamma : \alpha) = (\lambda^2\gamma : \alpha')$.

Invariant maps

T is a 2-torsion point, the 2-isogeny f with kernel T verifies: $f(\cdot + T) = f$.
Conversely, if $f(\cdot + T) = f$ $(+\deg 2)$, the 2-isogeny with kernel T is $g = f - f(\mathcal{O})$.

Invariant maps

T is a 2-torsion point, the 2-isogeny f with kernel T verifies: $f(\cdot + T) = f$.
Conversely, if $f(\cdot + T) = f$ $(+\deg 2)$, the 2-isogeny with kernel T is $g = f - f(\mathcal{O})$.

Step 1

What is the map $\tau : P \mapsto P + T$ on the Kummer line?

It is a homography (isomorphism of $\mathbb{P}^1$).

Step 1: example

$$E : y^2 = x(x^2 + Ax + \gamma)$$

$$\mathcal{O} = (1:0)^* \qquad T = (0:1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)(= R + T)$$

If $\tau : P \mapsto P + T$, we know that $\tau : (x : z) \mapsto (ax + bz : cx + dz)$.
We want $\tau(\mathcal{O}) = T$, $\tau(T) = \mathcal{O}$, $\tau(R) = S$ and $\tau(S) = R$, this yields:

$$\tau : (x : z) \mapsto (\gamma z : x) \text{ with } M_T = \begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}_2(k)$$

Type of a point

M_T: associated matrix to $\tau : P \mapsto P + T$.

By construction, $M_T^2 = I_2 \in \mathrm{PGL}_2(k)$, so with a lift: $\widetilde{M_T}^2 = \lambda_T I_2 \in \mathrm{GL}_2(k)$.

Definition

λ_T is the type of T, well-defined up to a square.

Type of a point

M_T: associated matrix to $\tau : P \mapsto P + T$.
By construction, $M_T^2 = I_2 \in \mathrm{PGL}_2(k)$, so with a lift: $\widetilde{M_T}^2 = \lambda_T I_2 \in \mathrm{GL}_2(k)$.

Definition

λ_T is the type of T, well-defined up to a square.

In the previous example, $\widetilde{M_T}^2 = \gamma I_2$ so the type is γ.
Fact: $\widetilde{M_T}/\sqrt{\lambda_T}$ only depends on T.

Step 2

We want to build a map in x^2, xz, z^2 invariant by T.
In terms of a quadratic form q, if $M = \widetilde{M_T}/\sqrt{\lambda_T} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we want:

$$M \cdot q(x,z) = q(ax+bz, cx+dz) = q(x,z)$$

Step 2

We want to build a map in x^2, xz, z^2 invariant by T.
In terms of a quadratic form q, if $M = \widetilde{M_T}/\sqrt{\lambda_T} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we want:

$$M \cdot q(x, z) = q(ax + bz, cx + dz) = q(x, z)$$

Step 2

We compute $M \cdot x^2$, $M \cdot z^2$ and $M \cdot xz$ and build invariant quadratic forms from that.

We need two of these, for the two isogenous coordinates.

Step 2: example

$$E : y^2 = x(x^2 + Ax + \gamma)$$

$$\mathcal{O} = (1 : 0)^* \qquad T = (0 : 1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)$$

We have $\lambda_T = \gamma$, we take $M = \begin{pmatrix} 0 & \sqrt{\gamma} \\ \sqrt{\gamma}^{-1} & 0 \end{pmatrix}$. Then:

$$M \cdot x^2 = \gamma z^2 \qquad M \cdot z^2 = \frac{1}{\gamma} x^2 \qquad M \cdot xz = xz$$

Step 2: example

$$E : y^2 = x(x^2 + Ax + \gamma)$$

$$\mathcal{O} = (1:0)^* \qquad T = (0:1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)$$

We have $\lambda_T = \gamma$, we take $M = \begin{pmatrix} 0 & \sqrt{\gamma} \\ \sqrt{\gamma}^{-1} & 0 \end{pmatrix}$. Then:

$$M \cdot x^2 = \gamma z^2 \qquad M \cdot z^2 = \frac{1}{\gamma} x^2 \qquad M \cdot xz = xz$$

xz is already invariant, for the other one we can consider (okay because $M^2 = I_2$):

$$x^2 + M \cdot x^2 = x^2 + \gamma z^2$$

The end?

Consider two invariant quadratic forms u, v, not co-linear. Set:

$$f : (x : z) \mapsto (u(x, z) : v(x, z))$$

By construction, $f(\cdot + T) = f$. That's it?

The end?

Consider two invariant quadratic forms u, v, not co-linear. Set:

$$f : (x : z) \mapsto (u(x,z) : v(x,z))$$

By construction, $f(\cdot + T) = f$. That's it?
Let's try with $u(x,z) = x^2 + \gamma z^2$ and $v(x,z) = xz$:

$$f(1:0) = (1:0) = f(0:1) \qquad f(\alpha : 1) = (-A : 1) = f(\gamma : \alpha)$$

The end?

Consider two invariant quadratic forms u, v, not co-linear. Set:

$$f : (x : z) \mapsto (u(x,z) : v(x,z))$$

By construction, $f(\cdot + T) = f$. That's it?
Let's try with $u(x,z) = x^2 + \gamma z^2$ and $v(x,z) = xz$:

$$f(1:0) = (1:0) = f(0:1) \qquad f(\alpha : 1) = (-A : 1) = f(\gamma : \alpha)$$

- Where is the remaining 2-torsion? Via 4-torsion
- How do I recover a good shaped Kummer line? Case-by-case

4-torsion on the Kummer line

$$E : y^2 = x(x^2 + Ax + \gamma)$$

$$\mathcal{O} = (1 : 0)^* \qquad T = (0 : 1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)$$

Assume T' is a 4-torsion point above T: $T = 2T'$.
Because we are on a Kummer line: $3T' = T' + T = -T' = T'$.
If $T' = (x : z)$, we then have:

$$T' + T = (\gamma z : x) = (x : z) \text{ iff } \left(\frac{x}{z}\right)^2 = \gamma$$

4-torsion on the Kummer line

$$E : y^2 = x(x^2 + Ax + \gamma)$$

$$\mathcal{O} = (1:0)^* \qquad T = (0:1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)$$

Assume T' is a 4-torsion point above T: $T = 2T'$.
Because we are on a Kummer line: $3T' = T' + T = -T' = T'$.
If $T' = (x : z)$, we then have:

$$T' + T = (\gamma z : x) = (x : z) \text{ iff } \left(\frac{x}{z}\right)^2 = \gamma$$

The 4-torsion points are (maybe in a quadratic extension):

$$T' = (\sqrt{\gamma} : 1) \qquad T'' = (-\sqrt{\gamma} : 1)$$

4-torsion on the Kummer line

$$E : y^2 = x(x^2 + Ax + \gamma)$$

$$\mathcal{O} = (1:0)^* \qquad T = (0:1) \qquad R = (\alpha : 1) \qquad S = (\gamma : \alpha)$$

Assume T' is a 4-torsion point above T: $T = 2T'$.
Because we are on a Kummer line: $3T' = T' + T = -T' = T'$.
If $T' = (x : z)$, we then have:

$$T' + T = (\gamma z : x) = (x : z) \text{ iff } \left(\frac{x}{z}\right)^2 = \gamma$$

The 4-torsion points are (maybe in a quadratic extension):

$$T' = (\sqrt{\gamma} : 1) \qquad T'' = (-\sqrt{\gamma} : 1)$$

$f(T')$ and $f(T'')$ are the remaining 2-torsion points on the image (always rational by construction)

Montgomery with full 2-torsion (1/2)

Montgomery: $\gamma = 1$.
We want to compute $f : E_1 \to E_1/T_1 = E_2$ where ($\alpha = A_1/B_1$):

$$\mathcal{O}_1 = (1:0)^* \quad T_1 = (0:1) \quad R_1 = (\alpha:1) = (A_1:B_1) \quad S_1 = (1:\alpha) = (B_1:A_1)$$

4-torsion above T_1: $T_1' = (1:1)$ and $T_1'' = (-1:1)$.

Montgomery with full 2-torsion (1/2)

Montgomery: $\gamma = 1$.
We want to compute $f : E_1 \to E_1/T_1 = E_2$ where ($\alpha = A_1/B_1$):

$$\mathcal{O}_1 = (1:0)^* \quad T_1 = (0:1) \quad R_1 = (\alpha:1) = (A_1:B_1) \quad S_1 = (1:\alpha) = (B_1:A_1)$$

4-torsion above T_1: $T_1' = (1:1)$ and $T_1'' = (-1:1)$.

1. Translation by T_1: $\tau : (x:z) \mapsto (z:x)$ (type of T_1: 1)

Montgomery with full 2-torsion (1/2)

Montgomery: $\gamma = 1$.
We want to compute $f : E_1 \to E_1/T_1 = E_2$ where ($\alpha = A_1/B_1$):

$$\mathcal{O}_1 = (1:0)^* \quad T_1 = (0:1) \quad R_1 = (\alpha : 1) = (A_1 : B_1) \quad S_1 = (1:\alpha) = (B_1 : A_1)$$

4-torsion above T_1: $T_1' = (1:1)$ and $T_1'' = (-1:1)$.

1. Translation by T_1: $\tau : (x : z) \mapsto (z : x)$ (type of T_1: 1)
2. Invariant quadratic forms: $u(x,z) = (x+z)^2$ and $v(x,z) = (x-z)^2$

Montgomery with full 2-torsion (1/2)

Montgomery: $\gamma = 1$.
We want to compute $f : E_1 \to E_1/T_1 = E_2$ where $(\alpha = A_1/B_1)$:

$$\mathcal{O}_1 = (1:0)^* \quad T_1 = (0:1) \quad R_1 = (\alpha : 1) = (A_1 : B_1) \quad S_1 = (1:\alpha) = (B_1 : A_1)$$

4-torsion above T_1: $T_1' = (1:1)$ and $T_1'' = (-1:1)$.

1. Translation by T_1: $\tau : (x : z) \mapsto (z : x)$ (type of T_1: 1)
2. Invariant quadratic forms: $u(x,z) = (x+z)^2$ and $v(x,z) = (x-z)^2$
3. Images of the special points by $f : (x:z) \mapsto (u(x,z) : v(x,z))$

$$f(\mathcal{O}_1) = f(T_1) = (1:1)^* \qquad f(T_1') = (1:0) \qquad f(T_1'') = (0:1)$$

$$f(A_1 : B_1) = f(B_1 : A_1) = ((A_1+B_1)^2 : (A_1 - B_1)^2) = (A_2^2 : B_2^2)$$

Montgomery with full 2-torsion (1/2)

Montgomery: $\gamma = 1$.
We want to compute $f : E_1 \to E_1/T_1 = E_2$ where ($\alpha = A_1/B_1$):

$$\mathcal{O}_1 = (1:0)^* \quad T_1 = (0:1) \quad R_1 = (\alpha:1) = (A_1:B_1) \quad S_1 = (1:\alpha) = (B_1:A_1)$$

4-torsion above T_1: $T_1' = (1:1)$ and $T_1'' = (-1:1)$.

1. Translation by T_1: $\tau : (x:z) \mapsto (z:x)$ (type of T_1: 1)
2. Invariant quadratic forms: $u(x,z) = (x+z)^2$ and $v(x,z) = (x-z)^2$
3. Images of the special points by $f : (x:z) \mapsto (u(x,z) : v(x,z))$

$$f(\mathcal{O}_1) = f(T_1) = (1:1)^* \qquad f(T_1') = (1:0) \qquad f(T_1'') = (0:1)$$

$$f(A_1:B_1) = f(B_1:A_1) = ((A_1+B_1)^2 : (A_1-B_1)^2) = (A_2^2 : B_2^2)$$

4. To get a convenient Kummer line, compose by $C : (x:z) \mapsto (B_2 x : A_2 z)$

$$\mathcal{O}_2 = (1:0) \qquad T_2 = (0:1) \qquad R_2 = (A_2:B_2) \qquad S_2 = (B_2:A_2)^*$$

Montgomery with full 2-torsion (2/2)

$$\mathcal{O}_1 = (1:0)^* \qquad T_1 = (0:1) \qquad R_1 = (A_1 : B_1) \qquad S_1 = (B_1 : A_1)$$

We set $A_2 = A_1 + B_1$ and $B_2 = A_1 - B_1$.

$$\mathcal{O}_2 = (1:0) \qquad T_2 = (0:1) \qquad R_2 = (A_2 : B_2) \qquad S_2 = (B_2 : A_2)^*$$

Translated 2-isogeny with kernel T_1

$g = f + S_2$, where $f : (x:z) \mapsto (B_2(x+z)^2 : A_2(x-z)^2)$.
f can be computed in $2S + 2M + 2a$. The co-domain is given by $\frac{\mathcal{A}_2+2}{4}$ where $\mathcal{A}_2 = -\frac{A_2}{B_2} - \frac{B_2}{A_2}$ and is computed in $2S + 5a$.

Translated dual isogeny

If $\hat{f} : (x:z) \mapsto (B_1(x+z)^2 : A_1(x-z)^2)$, then $\hat{f} \circ f(P) = 2 \cdot P + R_1$.
This quasi-doubling can be computed in $4M + 4S$.

Montgomery with an additional 4-torsion point

$$\mathcal{O}_1 = (1:0)^* \qquad T_1 = (0:1) \qquad R_1 = (A_1 : B_1) \qquad S_1 = (B_1 : A_1)$$

Assume we know $R_1' = (a' : b')$ above R_1.
Set $a = a' + b'$, $b = a' - b'$ (fact: $(A_1 : B_1) = (a^2 + b^2 : a^2 - b^2)$).

$$\mathcal{O}_2 = (1:0) \qquad T_2 = (0:1) \qquad R_2 = (a'^2 : b'^2)^* \qquad S_2 = (b'^2 : a'^2)$$

Montgomery with an additional 4-torsion point

$$\mathcal{O}_1 = (1:0)^* \qquad T_1 = (0:1) \qquad R_1 = (A_1 : B_1) \qquad S_1 = (B_1 : A_1)$$

Assume we know $R_1' = (a' : b')$ above R_1.
Set $a = a' + b'$, $b = a' - b'$ (fact: $(A_1 : B_1) = (a^2 + b^2 : a^2 - b^2)$).

$$\mathcal{O}_2 = (1:0) \qquad T_2 = (0:1) \qquad R_2 = (a'^2 : b'^2)^* \qquad S_2 = (b'^2 : a'^2)$$

Translated 2-isogeny with kernel R_1

$g = f + R_2$, with $f : (x : z) \mapsto \left((a(x+z) + b(x-z))^2 : (a(x+z) - b(x-z))^2\right)$
f can be computed in $2S + 2M$. The co-domain can be computed in $2S$.

Montgomery with an additional 4-torsion point

$$\mathcal{O}_1 = (1:0)^* \qquad T_1 = (0:1) \qquad R_1 = (A_1 : B_1) \qquad S_1 = (B_1 : A_1)$$

Assume we know $R_1' = (a' : b')$ above R_1.
Set $a = a' + b'$, $b = a' - b'$ (fact: $(A_1 : B_1) = (a^2 + b^2 : a^2 - b^2)$).

$$\mathcal{O}_2 = (1:0) \qquad T_2 = (0:1) \qquad R_2 = (a'^2 : b'^2)^* \qquad S_2 = (b'^2 : a'^2)$$

Translated 2-isogeny with kernel R_1

$g = f + R_2$, with $f : (x:z) \mapsto \left((a(x+z) + b(x-z))^2 : (a(x+z) - b(x-z))^2\right)$
f can be computed in $2S + 2M$. The co-domain can be computed in $2S$.

- Similarly, with the dual isogeny, we recover alternative formulas for $2 \cdot P + R_1$.
- If the next kernel is R_2, then we can easily chain isogenies.

Montgomery with an 8-torsion point [DJP14]

$$\mathcal{O}_1 = (1:0)^* \qquad T_1 = (0:1) \qquad \cancel{R_1 = (A_1 : B_1)} \qquad \cancel{S_1 = (B_1 : A_1)}$$

Recall $T_1' = (1:1)$ and $T_1'' = (-1:1)$ are 4-torsion points above T_1.
Assume we know $\widetilde{T_1} = (r:s)$ a 8-torsion point above T_1'.

$$\mathcal{O}_2 = (1:0)^* \qquad T_2 = (1:-\delta) \qquad R_2 = (1:0) \qquad S_2 = (-\delta:1)$$

Montgomery with an 8-torsion point [DJP14]

$$\mathcal{O}_1 = (1:0)^* \qquad T_1 = (0:1) \qquad \cancel{R_1 = (A_1 : B_1)} \qquad \cancel{S_1 = (B_1 : A_1)}$$

Recall $T_1' = (1:1)$ and $T_1'' = (-1:1)$ are 4-torsion points above T_1.
Assume we know $\widetilde{T_1} = (r:s)$ a 8-torsion point above T_1'.

$$\mathcal{O}_2 = (1:0)^* \qquad T_2 = (1:-\delta) \qquad R_2 = (1:0) \qquad S_2 = (-\delta:1)$$

2-isogeny with kernel T_1

Set $\delta = (4rs : (r-s)^2)$, then $f : (x:z) \mapsto (\delta(x-z)^2 : 4xz)$.
f can be computed in $2S + 2M + 3a$.
We may need a permutation of 2-torsion afterwards.

Future work and research direction

What's new?

- General framework to compute 2-isogenies on Kummer lines: new isogeny formulas.
- Hybrid ladder which provides better doubling (under specific circumstances).

Work in progress

- Classification of elliptic curves given torsion properties on their Kummer line (via Galois representation).
- Choices of good curves for ECC and ECM to use hybrid ladder.

References I

[CH17] Craig Costello and Huseyin Hisil. "A simple and compact algorithm for SIDH with arbitrary degree isogenies". English. In: *Advances in cryptology – ASIACRYPT 2017. 23rd international conference on the theory and applications of cryptology and information security, Hong Kong, China, December 3–7, 2017. Proceedings. Part II*. Cham: Springer, 2017, pp. 303–329. ISBN: 978-3-319-70696-2; 978-3-319-70697-9. DOI: 10.1007/978-3-319-70697-9_11.

[DJP14] Luca De Feo, David Jao, and Jérôme Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". English. In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247. ISSN: 1862-2976. DOI: 10.1515/jmc-2012-0015.

References II

[HR19] Huseyin Hisil and Joost Renes. "On Kummer lines with full rational 2-torsion and their usage in cryptography". English. In: *ACM Transactions on Mathematical Software* 45.4 (2019). Id/No 39, p. 17. ISSN: 0098-3500. DOI: 10.1145/3361680.

[KS20] Sabyasachi Karati and Palash Sarkar. "Kummer for genus one over prime-order fields". English. In: *Journal of Cryptology* 33.1 (2020), pp. 92–129. ISSN: 0933-2790. DOI: 10.1007/s00145-019-09320-4.

[Mon87] Peter L. Montgomery. "Speeding the Pollard and elliptic curve methods of factorization". English. In: *Mathematics of Computation* 48 (1987), pp. 243–264. ISSN: 0025-5718. DOI: 10.2307/2007888.

References III

[Ren18] Joost Renes. "Computing isogenies between Montgomery curves using the action of $(0, 0)$". English. In: *Post-quantum cryptography. 9th international conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9–11, 2018. Proceedings*. Cham: Springer, 2018, pp. 229–247. ISBN: 978-3-319-79062-6; 978-3-319-79063-3. DOI: 10.1007/978-3-319-79063-3_11.