Swissogeny Day 2, 20th of March 2025

PEGASIS
Practical Efficient Class Group Action using 4-dimensional isogenies

Joint with Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herledan Le Merdy, Riccardo Invernizzi, Damien Robert, Frederik Vercauteren and Benjamin Wesolowski

https://eprint.iacr.org/2025/401

Ryan Rueger
IBM Research Zurich & Technical University of Munich

PEGASIS

Practically Efficient Class Group Action using 4-dimensional isogenies

PEGASIS

Practically Efficient Class Group Action using 4-dimensional isogenies

Practically Efficient Class Group Action using 4-dimensional isogenies

Practically Efficient Class Group Action using 4-dimensional isogenies

Results

	Lang.	500	1000	1500	2000	4000
SCALLOP*	C++	35s	750s			
SCALLOP-HD*	Sage	88s	1140s			
PEARL-SCALLOP*	C++	30s	58s	710s		
KLaPoTi	Sage	207s				
	Rust	1.95s				
PEGASIS	Sage	1.53s	4.21s	10.5s	21.3s	121s

Table: Time measured in wall-clock time. Stars indicate different measuring hardware.

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties* $\quad E, E'$ Elliptic curves

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties*

$f : A \to B$ *isogeny*

E, E' Elliptic curves

$\varphi : E \to E'$ isogeny

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties*

$f : A \to B$ *isogeny*

$\tilde{f} : B \to A$ *polarised dual*

E, E' Elliptic curves

$\varphi : E \to E'$ isogeny

$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties*

$f: A \to B$ *isogeny*

$\tilde{f}: B \to A$ *polarised dual*

f is *polarised isogeny* if $\tilde{f}f = [d]_A$

E, E' Elliptic curves

$\varphi: E \to E'$ isogeny

$\hat{\varphi} = \tilde{\varphi}: E' \to E$ dual

(They all are)

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties*

$f : A \to B$ *isogeny*

$\tilde{f} : B \to A$ *polarised dual*

f is *polarised isogeny* if $\tilde{f} f = [d]_A$

...it has *polarised degree* $\deg_{\mathrm{p}}(f) = d$

E, E' Elliptic curves

$\varphi : E \to E'$ isogeny

$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual

(They all are)

$\deg_{\mathrm{p}}(\varphi) = \deg(\varphi)$

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties*
$f : A \to B$ *isogeny*
$\tilde{f} : B \to A$ *polarised dual*
f is *polarised isogeny* if $\tilde{f} f = [d]_A$
...it has *polarised degree* $\deg_p(f) = d$

E, E' Elliptic curves
$\varphi : E \to E'$ isogeny
$\hat{\varphi} = \tilde{\varphi} : E' \to E$ dual
(They all are)
$\deg_p(\varphi) = \deg(\varphi)$

Important fact

$f : A \to B$ a polarised isogeny

$$\mathrm{diag}_d(f) = \begin{pmatrix} f & & 0 \\ & \ddots & \\ 0 & & f \end{pmatrix} : A^d \to B^d$$

Higher dimensional isogenies

A, B *Principally Polarised Abelian Varieties*
$f: A \to B$ *isogeny*
$\tilde{f}: B \to A$ *polarised dual*
f is *polarised isogeny* if $\tilde{f}f = [d]_A$
...it has *polarised degree* $\deg_{\mathrm{p}}(f) = d$

E, E' Elliptic curves
$\varphi: E \to E'$ isogeny
$\hat{\varphi} = \tilde{\varphi}: E' \to E$ dual
(They all are)
$\deg_{\mathrm{p}}(\varphi) = \deg(\varphi)$

Important fact

$f: A \to B$ a polarised isogeny

$$\mathrm{diag}_d(f) = \begin{pmatrix} f & & 0 \\ & \ddots & \\ 0 & & f \end{pmatrix} : A^d \to B^d$$

$\deg_{\mathrm{p}}(\mathrm{diag}_d(f)) = \deg_{\mathrm{p}}(f)$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_\mathrm{p}(\varphi_{ij})$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_p(\varphi_{ij})$

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} : A_1 \times A_2 \to B_1 \times B_2$$

is a polarised isogeny

$$\iff$$

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi_{11}} & B_1 \\ {\scriptstyle -\varphi_{12}}\big\downarrow & & \big\downarrow{\scriptstyle \widetilde{\varphi_{21}}} \\ B_2 & \xrightarrow[\widetilde{\varphi_{22}}]{} & A_2 \end{array}$$

$$\deg_p(\varphi_{11}) = \deg_p(\varphi_{22})$$
$$\deg_p(\varphi_{12}) = \deg_p(\varphi_{21})$$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_p(\varphi_{ij})$

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} : A_1 \times A_2 \to B_1 \times B_2$$

is a polarised isogeny

$$\iff$$

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi_{11}} & B_1 \\ {\scriptstyle -\varphi_{12}}\downarrow & & \downarrow{\scriptstyle \widetilde{\varphi_{21}}} \\ B_2 & \xrightarrow[\widetilde{\varphi_{22}}]{} & A_2 \end{array}$$

$$\deg_p(\varphi_{11}) = \deg_p(\varphi_{22})$$
$$\deg_p(\varphi_{12}) = \deg_p(\varphi_{21})$$

Then $\deg_p(\Phi) = \deg_p(\varphi_{11}) + \deg_p(\varphi_{21})$

Kani's Lemma

A_i, B_j PPAVs over k, $\varphi_{ij} : A_i \to B_j$ polarised isogenies, $\mathrm{char}(k) \nmid \deg_p(\varphi_{ij})$

$$\Phi = \begin{pmatrix} \varphi_{11} & \varphi_{21} \\ \varphi_{12} & \varphi_{22} \end{pmatrix} : A_1 \times A_2 \to B_1 \times B_2$$

is a polarised isogeny

$$\iff$$

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi_{11}} & B_1 \\ {\scriptstyle -\varphi_{12}}\downarrow & & \downarrow{\scriptstyle \widetilde{\varphi_{21}}} \\ B_2 & \xrightarrow[\widetilde{\varphi_{22}}]{} & A_2 \end{array}$$

$$\deg_p(\varphi_{11}) = \deg_p(\varphi_{22})$$
$$\deg_p(\varphi_{12}) = \deg_p(\varphi_{21})$$

Then $\deg_p(\Phi) = \deg_p(\varphi_{11}) + \deg_p(\varphi_{21})$

If additionally $\deg_p(\varphi_{11}), \deg_p(\varphi_{21})$ coprime and $\mathrm{char}(k) \nmid \deg_p(\Phi)$ then

$$\ker(\Phi) = \left\{ \left(\deg_p(\varphi_{11})x, \widetilde{\varphi_{21}}\varphi_{11}(x) \right) \mid x \in A_1[\deg_p(\Phi)] \right\} \subseteq A_1 \times A_2$$

Factoring Lemma

Factoring Lemma

$f\colon A \to B$ polarised isogeny between PPAVs

Let (d_1, d_2) coprime positive integers such that $\deg_p(f) = d_1 d_2$

Factoring Lemma

$f: A \to B$ polarised isogeny between PPAVs

Let (d_1, d_2) coprime positive integers such that $\deg_p(f) = d_1 d_2$

There exists a PPAV C and isogenies $f_1: A \to C$, $f_2: C \to B$ such that

1. $\deg_p(f_1) = d_1$
2. $\deg_p(f_2) = d_2$
3. $f = f_2 f_1$

Factoring Lemma

$f : A \to B$ polarised isogeny between PPAVs

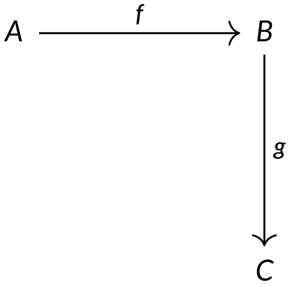
Let (d_1, d_2) coprime positive integers such that $\deg_p(f) = d_1 d_2$

There exists a PPAV C and isogenies $f_1 : A \to C$, $f_2 : C \to B$ such that

1. $\deg_p(f_1) = d_1$
2. $\deg_p(f_2) = d_2$
3. $f = f_2 f_1$

Corollary

$f : A \to B$, $g : B \to C$ polarised isogenies with $\deg_p(f), \deg_p(g)$ coprime



Factoring Lemma

$f : A \to B$ polarised isogeny between PPAVs

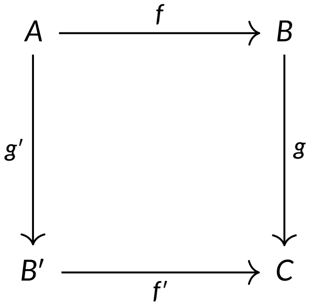
Let (d_1, d_2) coprime positive integers such that $\deg_p(f) = d_1 d_2$

There exists a PPAV C and isogenies $f_1 : A \to C$, $f_2 : C \to B$ such that

1. $\deg_p(f_1) = d_1$
2. $\deg_p(f_2) = d_2$
3. $f = f_2 f_1$

Corollary

$f : A \to B$, $g : B \to C$ polarised isogenies with $\deg_p(f), \deg_p(g)$ coprime



Factoring Lemma

$f\colon A \to B$ polarised isogeny between PPAVs

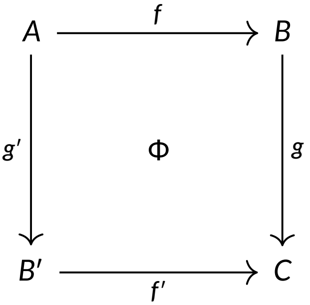
Let (d_1, d_2) coprime positive integers such that $\deg_p(f) = d_1 d_2$

There exists a PPAV C and isogenies $f_1 : A \to C$, $f_2 : C \to B$ such that

1. $\deg_p(f_1) = d_1$ 2. $\deg_p(f_2) = d_2$ 3. $f = f_2 f_1$

Corollary

$f\colon A \to B$, $g\colon B \to C$ polarised isogenies with $\deg_p(f), \deg_p(g)$ coprime



$\rightsquigarrow$

$$\Phi = \begin{pmatrix} f & \tilde{g} \\ -g' & \tilde{f'} \end{pmatrix} : A \times C \to B \times B'$$

The Ideal2Isogeny Construction

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

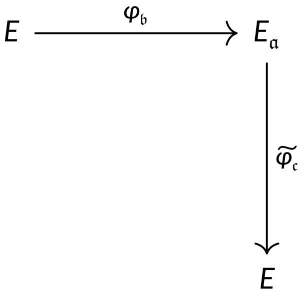
Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

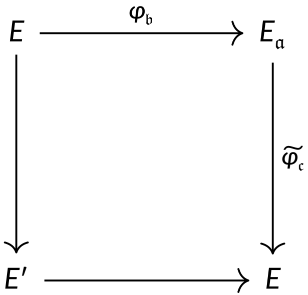


The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

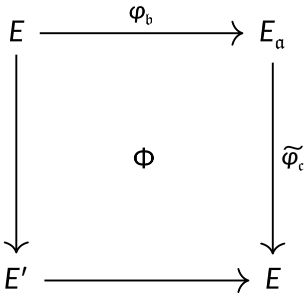


The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

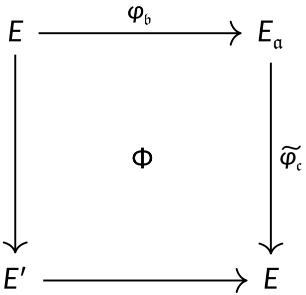


The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime



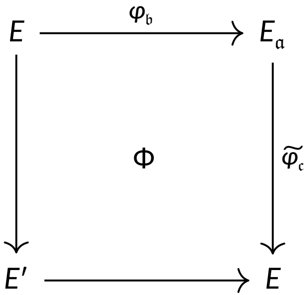
$$\begin{aligned}\ker(\Phi) &= \left\{\left(\mathrm{N}(\mathfrak{b})x, \widetilde{\varphi}_{\mathfrak{c}}\varphi_{\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)]\right\} \\ &= \left\{\left(\mathrm{N}(\mathfrak{b})x, \varphi_{\bar{\mathfrak{c}}\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)]\right\}\end{aligned}$$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime



$$\ker(\Phi) = \left\{\left(\mathrm{N}(\mathfrak{b})x, \widetilde{\varphi}_{\mathfrak{c}}\varphi_{\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)]\right\}$$
$$= \left\{\left(\mathrm{N}(\mathfrak{b})x, \varphi_{\bar{\mathfrak{c}}\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)]\right\}$$

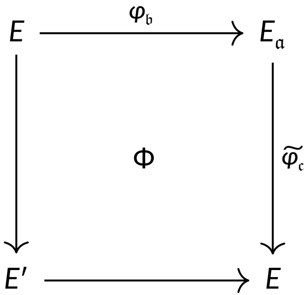
Norm equation $\deg_{\mathrm{p}}(\Phi) = \mathrm{N}(\mathfrak{b}) + \mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

The Ideal2Isogeny Construction

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

Assume $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime



$$\begin{aligned}\ker(\Phi) &= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)] \right\} \\ &= \left\{ \left(\mathrm{N}(\mathfrak{b})x, \varphi_{\bar{\mathfrak{c}}\mathfrak{b}}(x)\right) \mid x \in E[\deg_{\mathrm{p}}(\Phi)] \right\}\end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = \mathrm{N}(\mathfrak{b}) + \mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

Requirements

1. $f \leq v_2(p+1) - 3$
2. $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

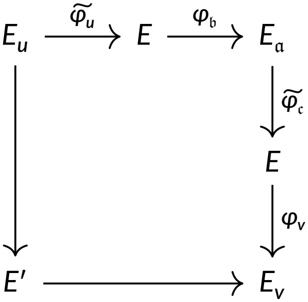
$$\begin{array}{ccccc} E_u & \xrightarrow{\widetilde{\varphi_u}} & E & \xrightarrow{\varphi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ & & & & \downarrow \widetilde{\varphi_{\mathfrak{c}}} \\ & & & & E \\ & & & & \downarrow \varphi_v \\ & & & & E_v \end{array}$$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

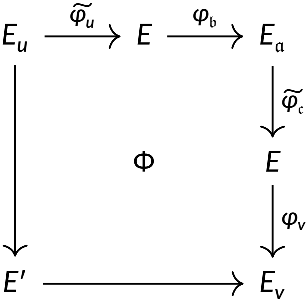


The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

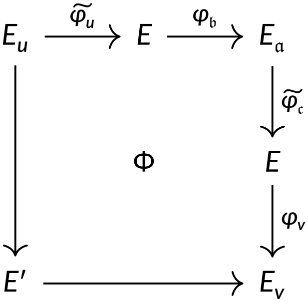


The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime



$$\ker(\Phi)$$

$$= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \widetilde{\varphi}_{\mathfrak{c}} \varphi_{\mathfrak{b}} \widetilde{\varphi}_u(x) \right) \mid x \in E_u[\deg_p(\Phi)] \right\}$$

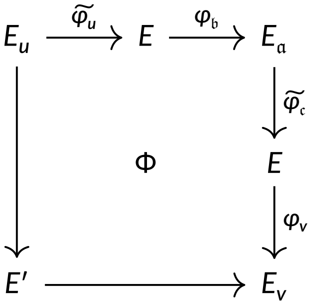
$$= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \varphi_{\bar{\mathfrak{c}}\mathfrak{b}} \widetilde{\varphi}_u(x) \right) \mid x \in E_u[\deg_p(\Phi)] \right\}$$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime



$$\begin{aligned}&\ker(\Phi)\\ &= \left\{\left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \widetilde{\varphi}_{\mathfrak{c}} \varphi_{\mathfrak{b}} \widetilde{\varphi}_u(x)\right) \mid x \in E_u[\deg_p(\Phi)]\right\}\\ &= \left\{\left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \varphi_{\bar{\mathfrak{c}}\mathfrak{b}} \widetilde{\varphi}_u(x)\right) \mid x \in E_u[\deg_p(\Phi)]\right\}\end{aligned}$$

Norm equation $\deg_p(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

The Ideal2Isogeny Construction: Iteration #2

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E \to E_u$, $\varphi_v : E \to E_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{array}{ccccc} E_u & \xrightarrow{\widetilde{\varphi_u}} & E & \xrightarrow{\varphi_{\mathfrak{b}}} & E_{\mathfrak{a}} \\ \big\downarrow & & & & \big\downarrow \widetilde{\varphi_{\mathfrak{c}}} \\ & & \Phi & & E \\ \big\downarrow & & & & \big\downarrow \varphi_v \\ E' & & \longrightarrow & & E_v \end{array}$$

$$\begin{aligned} &\ker(\Phi) \\ &= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \widetilde{\varphi_{\mathfrak{c}}} \varphi_{\mathfrak{b}} \widetilde{\varphi_u}(x) \right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\ &= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \varphi_{\bar{\mathfrak{c}}\mathfrak{b}} \widetilde{\varphi_u}(x) \right) \mid x \in E_u[\deg_{\mathrm{p}}(\Phi)] \right\} \end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

Requirements

1. $f \leq v_2(p+1) - 3$ 2. $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime 3. $u = \deg_{\mathrm{p}}(\varphi_u), v = \deg_{\mathrm{p}}(\varphi_v)$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

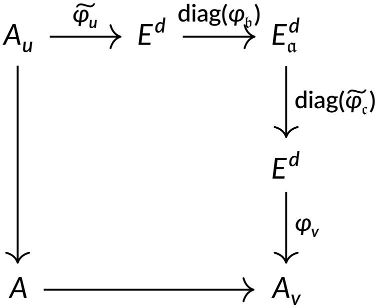
$$
\begin{array}{ccccc}
A_u & \xrightarrow{\widetilde{\varphi_u}} & E^d & \xrightarrow{\mathrm{diag}(\varphi_{\mathfrak{b}})} & E_{\mathfrak{a}}^d \\
 & & & & \big\downarrow \mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}}}) \\
 & & & & E^d \\
 & & & & \big\downarrow \varphi_v \\
 & & & & A_v
\end{array}
$$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime



The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$
\begin{array}{ccccc}
A_u & \xrightarrow{\widetilde{\varphi}_u} & E^d & \xrightarrow{\mathrm{diag}(\varphi_{\mathfrak{b}})} & E_{\mathfrak{a}}^d \\
\downarrow & & & & \downarrow \mathrm{diag}(\widetilde{\varphi}_{\mathfrak{c}}) \\
 & & \Phi & & E^d \\
\downarrow & & & & \downarrow \varphi_v \\
A & & \longrightarrow & & A_v
\end{array}
$$

$$
\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\widetilde{\varphi}_{\mathfrak{c}} \varphi_{\mathfrak{b}}) \widetilde{\varphi}_u(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\varphi_{\bar{\mathfrak{c}}\mathfrak{b}}) \widetilde{\varphi}_u(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}
$$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime

$$\begin{array}{ccccc}
A_u & \xrightarrow{\widetilde{\varphi}_u} & E^d & \xrightarrow{\mathrm{diag}(\varphi_{\mathfrak{b}})} & E^d_{\mathfrak{a}} \\
\big\downarrow & & & & \big\downarrow \mathrm{diag}(\widetilde{\varphi}_{\mathfrak{c}}) \\
 & & \Phi & & E^d \\
\big\downarrow & & & & \big\downarrow \varphi_v \\
A & & \longrightarrow & & A_v
\end{array}$$

$$\begin{aligned}
&\ker(\Phi) \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\widetilde{\varphi}_{\mathfrak{c}} \varphi_{\mathfrak{b}}) \widetilde{\varphi}_u(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\
&= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\varphi_{\bar{\mathfrak{c}}\mathfrak{b}}) \widetilde{\varphi}_u(x) \right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\}
\end{aligned}$$

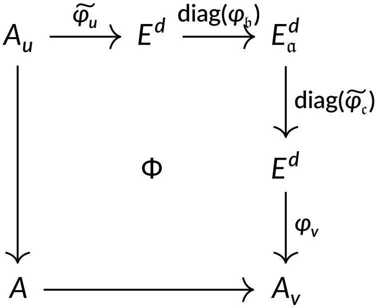
Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

The Ideal2Isogeny Construction: Iteration #3

Want to compute $[\mathfrak{a}] \cdot E = E_{\mathfrak{a}}$

Let $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$, $\varphi_u : E^d \to A_u$, $\varphi_v : E^d \to A_v$

Assume $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime



$$\begin{aligned} &\ker(\Phi) \\ &= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\widetilde{\varphi}_{\mathfrak{c}}\varphi_{\mathfrak{b}})\widetilde{\varphi}_u(x)\right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \\ &= \left\{ \left(u\mathrm{N}(\mathfrak{b})x, \varphi_v \mathrm{diag}(\varphi_{\bar{\mathfrak{c}}\mathfrak{b}})\widetilde{\varphi}_u(x)\right) \mid x \in A_u[\deg_{\mathrm{p}}(\Phi)] \right\} \end{aligned}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) \overset{!}{=} 2^f$

Requirements

1. $f \leq v_2(p+1) - 3$
2. $u\mathrm{N}(\mathfrak{b}), v\mathrm{N}(\mathfrak{c})$ coprime
3. $u = \deg_{\mathrm{p}}(\varphi_u), v = \deg_{\mathrm{p}}(\varphi_v)$

Solvability of the norm equation

Solvability of the norm equation

Frobenius Coin Problem

$u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^f$ has a solution if $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Solvability of the norm equation

Frobenius Coin Problem

$u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^f$ has a solution if $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Minkowski Bound

Every class in $\mathrm{Cl}(\mathcal{O})$ has a representative of norm at most $\sqrt{\mathrm{Disc}(\mathcal{O})}$

Solvability of the norm equation

Frobenius Coin Problem

$u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^f$ has a solution if $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Minkowski Bound

Every class in $\mathrm{Cl}(\mathcal{O})$ has a representative of norm at most $\sqrt{\mathrm{Disc}(\mathcal{O})}$

Heuristic

Every class in $\mathrm{Cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$ has two representatives $\mathfrak{b}, \mathfrak{c}$, with $\mathfrak{b} \neq \lambda\mathfrak{c}$, such that $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

Solvability of the norm equation

Frobenius Coin Problem

$u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^f$ has a solution if $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Minkowski Bound

Every class in $\mathrm{Cl}(\mathcal{O})$ has a representative of norm at most $\sqrt{\mathrm{Disc}(\mathcal{O})}$

Heuristic

Every class in $\mathrm{Cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$ has two representatives $\mathfrak{b}, \mathfrak{c}$, with $\mathfrak{b} \neq \lambda\mathfrak{c}$, such that $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

Tension

We only permit $f < e$, but $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \approx p = c2^e - 1 \not\lesssim 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Solvability of the norm equation

Frobenius Coin Problem

$u\mathrm{N}(\mathfrak{b}) + v\mathrm{N}(\mathfrak{c}) = 2^f$ has a solution if $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Minkowski Bound

Every class in $\mathrm{Cl}(\mathcal{O})$ has a representative of norm at most $\sqrt{\mathrm{Disc}(\mathcal{O})}$

Heuristic

Every class in $\mathrm{Cl}(\mathbb{Z}[(1+\sqrt{-p})/2])$ has two representatives $\mathfrak{b}, \mathfrak{c}$, with $\mathfrak{b} \neq \lambda\mathfrak{c}$, such that $p \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \leq 2p$

Tension

We only permit $f < e$, but $\mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c}) \approx p = c2^e - 1 \not\leq 2^f - \mathrm{N}(\mathfrak{b}) - \mathrm{N}(\mathfrak{c})$

Conclusion The norms $\mathrm{N}(\mathfrak{b}), \mathrm{N}(\mathfrak{c})$ are too big!

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Idea

Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$ with action of $\mathfrak{b}_e, \mathfrak{c}_e$ “easy”

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Idea

Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e\mathfrak{c}_k$ with action of $\mathfrak{b}_e, \mathfrak{c}_e$ “easy”

Compute easy part first.

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Idea

Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$ with action of $\mathfrak{b}_e, \mathfrak{c}_e$ "easy"

Compute easy part first. Then norm equation for "hard" part $\mathfrak{b}_k, \mathfrak{c}_k$

$$u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f$$

easier to solve because $\mathrm{N}(\mathfrak{b}_k)\mathrm{N}(\mathfrak{c}_k) \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Idea

Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$ with action of $\mathfrak{b}_e, \mathfrak{c}_e$ "easy"

Compute easy part first. Then norm equation for "hard" part $\mathfrak{b}_k, \mathfrak{c}_k$

$$u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f$$

easier to solve because $\mathrm{N}(\mathfrak{b}_k)\mathrm{N}(\mathfrak{c}_k) \leq \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{c})$

Maybe $\mathrm{N}(\mathfrak{b}_k)\mathrm{N}(\mathfrak{c}_k) \leq 2^f - \mathrm{N}(\mathfrak{b}_k) - \mathrm{N}(\mathfrak{c}_k)$

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Idea

Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$ with action of $\mathfrak{b}_e, \mathfrak{c}_e$ "easy"

Compute easy part first. Then norm equation for "hard" part $\mathfrak{b}_k, \mathfrak{c}_k$

$$uN(\mathfrak{b}_k) + vN(\mathfrak{c}_k) = 2^f$$

easier to solve because $N(\mathfrak{b}_k)N(\mathfrak{c}_k) \leq N(\mathfrak{b})N(\mathfrak{c})$

Maybe $N(\mathfrak{b}_k)N(\mathfrak{c}_k) \leq 2^f - N(\mathfrak{b}_k) - N(\mathfrak{c}_k)$

"Easy" In practice

Ensure $N(\mathfrak{b}_e), N(\mathfrak{c}_e)$ are products of small primes split in $\mathcal{O}$

Solvability of the norm equation: An idea

Recall

Ideals of $\mathcal{O}$ prime to the conductor factorise uniquely as product of prime ideals

Idea

Factor the ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$ with action of $\mathfrak{b}_e, \mathfrak{c}_e$ “easy”

Compute easy part first. Then norm equation for “hard” part $\mathfrak{b}_k, \mathfrak{c}_k$

$$uN(\mathfrak{b}_k) + vN(\mathfrak{c}_k) = 2^f$$

easier to solve because $N(\mathfrak{b}_k)N(\mathfrak{c}_k) \leq N(\mathfrak{b})N(\mathfrak{c})$

Maybe $N(\mathfrak{b}_k)N(\mathfrak{c}_k) \leq 2^f - N(\mathfrak{b}_k) - N(\mathfrak{c}_k)$

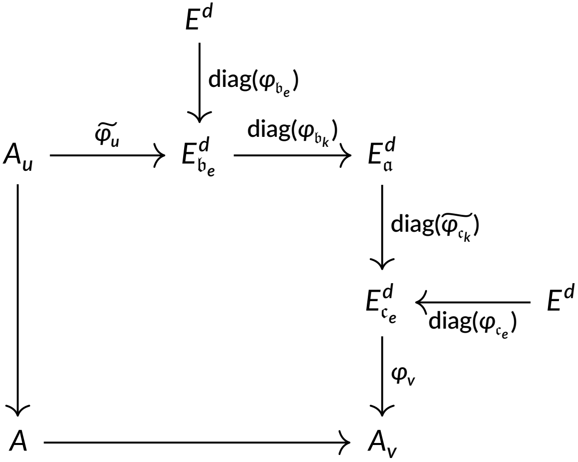
“Easy” In practice

Ensure $N(\mathfrak{b}_e), N(\mathfrak{c}_e)$ are products of small primes split in $\mathcal{O}$

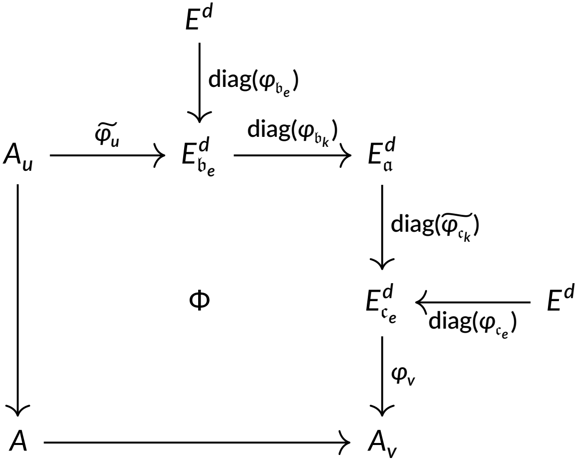
Concretely $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-p})/2]$

Compute $[\mathfrak{b}_e] \cdot E$ with successive Elkies isogenies defined over F_p

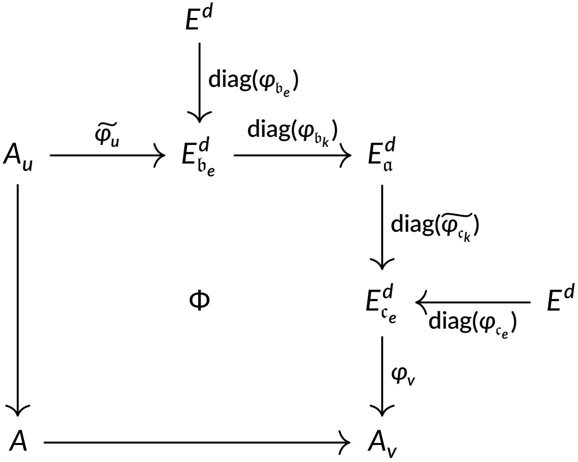
Solvability of the norm equation: The diagram



Solvability of the norm equation: The diagram

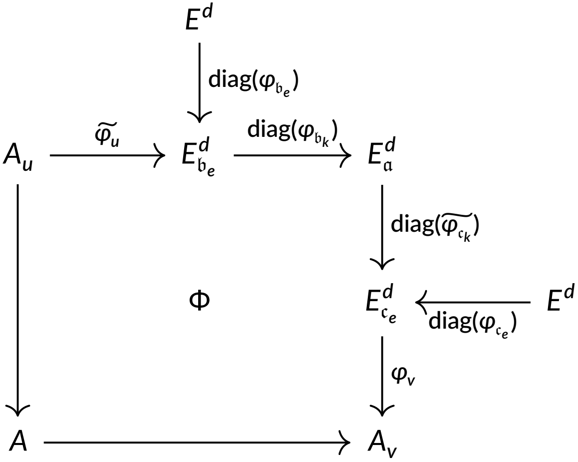


Solvability of the norm equation: The diagram



Norm equation $\deg_p(\Phi) = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) \stackrel{!}{=} 2^f$

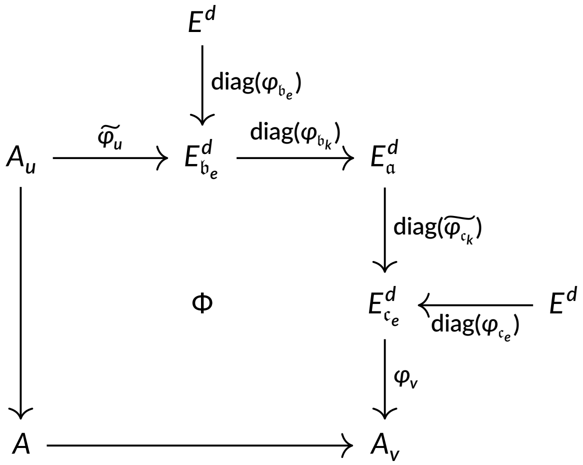
Solvability of the norm equation: The diagram



Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) \overset{!}{=} 2^f$

$$\ker(\Phi) = \left\{(u\mathrm{N}(\mathfrak{b}_e)x, \varphi_v \mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k})\widetilde{\varphi_u}(x)) \mid x \in A_u[2^f]\right\} \quad \text{and} \quad \widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k} = \frac{1}{\mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)}\widetilde{\varphi_{\mathfrak{c}_e}}\varphi_{\bar{\mathfrak{c}}\mathfrak{b}}\varphi_{\mathfrak{b}_e}$$

Solvability of the norm equation: The diagram



$$\varphi_{\bar{\mathfrak{c}}\mathfrak{b}} = \widetilde{\varphi_{\mathfrak{c}}}\varphi_{\mathfrak{b}} = \widetilde{\varphi_{\mathfrak{c}_e}}\varphi_{\mathfrak{c}_k}\varphi_{\mathfrak{b}_k}\widetilde{\varphi_{\mathfrak{b}_e}}$$

Norm equation $\deg_{\mathrm{p}}(\Phi) = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) \overset{!}{=} 2^f$

$$\ker(\Phi) = \left\{(u\mathrm{N}(\mathfrak{b}_e)x, \varphi_v\mathrm{diag}(\widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k})\widetilde{\varphi_u}(x)) \mid x \in A_u[2^f]\right\} \quad \text{and} \quad \widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k} \overset{(*)}{=} \frac{1}{\mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)}\widetilde{\varphi_{\mathfrak{c}_e}}\varphi_{\bar{\mathfrak{c}}\mathfrak{b}}\varphi_{\mathfrak{b}_e}$$

Solvability of the norm equation: Some data

	Avg	Med	Min	Max
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.285	4	0	19
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.297	2	0	10
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.768	2	0	8
13-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.612	1	0	8

Table: Elkies steps required for $\log_2(p) = 33 \cdot 2^{503} - 1$.

Solvability of the norm equation: Some data

	Avg	Med	Min	Max
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.574	4	0	24
5-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	3.011	3	0	12
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.482	2	0	10
13-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.908	2	0	9

Table: Elkies steps required for $p = 15 \cdot 2^{1004} - 1$.

Solvability of the norm equation: Some data

	Avg	Med	Min	Max
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	5.582	5	0	18
5-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	3.746	4	0	11
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.402	2	0	8

Table: Elkies steps required for $p = 9 \cdot 2^{1551} - 1$.

Solvability of the norm equation: Some data

	Avg	Med	Min	Max
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.891	4	0	22
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.733	3	0	9
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.172	2	0	9
17-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.785	2	0	9

Table: Elkies steps required for $p = 51 \cdot 2^{2026} - 1$.

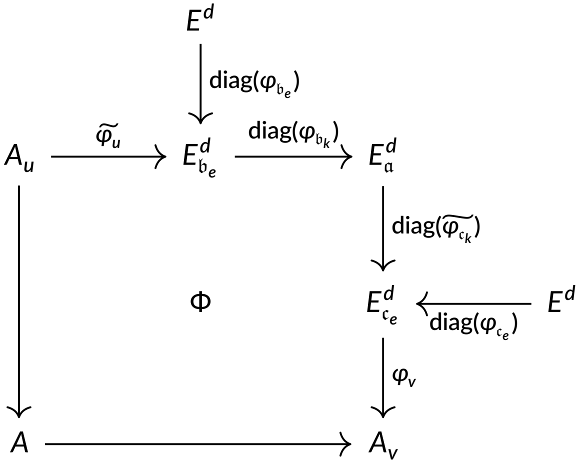
Solvability of the norm equation: Some data

	Avg	Med	Min	Max
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.950	4	0	17
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.658	2	0	9
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.010	2	0	9
17-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.691	1	0	7
19-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.567	1	0	6

Table: Elkies steps required for $p = 63 \cdot 2^{4084} - 1$.

Reminder of the diagram

$[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}] \quad \mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e \mathfrak{c}_k$



Problem Need to construct φ_u, φ_v

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

Dimension 1 $\rightsquigarrow$ Dimension 2 Kani-isogeny Φ

Requires knowledge of the endomorphism ring (SQISign2D)

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

Dimension 1 $\rightsquigarrow$ Dimension 2 Kani-isogeny Φ

Requires knowledge of the endomorphism ring (SQISign2D)

Dimension 2 $\rightsquigarrow$ Dimension 4 Kani-isogeny Φ

Sums of squares (or QFESTA-style splitting using 4-dimensional isogenies)

Constructing isogenies of prescribed degree

The isogenies φ_u, φ_v

Dimension 1 $\rightsquigarrow$ Dimension 2 Kani-isogeny Φ

Requires knowledge of the endomorphism ring (SQISign2D)

Dimension 2 $\rightsquigarrow$ Dimension 4 Kani-isogeny Φ

Sums of squares (or QFESTA-style splitting using 4-dimensional isogenies)

Dimension 4 $\rightsquigarrow$ Dimension 8 Kani-isogeny Φ

Zahrin's trick

Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$u = x_u^2 + y_u^2 \qquad M_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \to E^2 \qquad \deg_{\mathrm{p}}(\varphi_u) = u$$

Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$u = x_u^2 + y_u^2 \qquad M_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \to E^2 \qquad \deg_{\mathrm{p}}(\varphi_u) = u$$

Theorem

$u = p_1^{k_1} \cdots p_n^{k_n} = x_u^2 + y_u^2$ if and only if k_i even when $p_i \equiv 3 \pmod 4$

Constructing isogenies of prescribed degree

In dimension 2 with sum of two squares

$$u = x_u^2 + y_u^2 \qquad M_u = \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix} : E^2 \to E^2 \qquad \deg_{\mathrm{p}}(\varphi_u) = u$$

Theorem

$u = p_1^{k_1} \cdots p_n^{k_n} = x_u^2 + y_u^2$ if and only if k_i even when $p_i \equiv 3 \pmod 4$

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity
4. Then $u/g_u = x_u^2 + y_u^2$.

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity
4. Then $u/g_u = x_u^2 + y_u^2$.
5. Let ψ_u be isogeny of degree g_u, computed by sequence of p_i-isogenies using Elkies' algorithm

An Algorithm for constructing isogenies

of prescribed degree in dimension 2

Input: Integer u, Bound B, Set of small split primes $\mathcal{S}$

Output: Isogeny φ_u with degree u

1. Attempt factorisation of u with trial divisions up to B
2. Reject if prime $p_i \equiv 3 \pmod 4$, $p_i \notin \mathcal{S}$ divides u with odd multiplicity
3. Let g_u product of primes $p_i \equiv 3 \pmod 4$ and $p_i \in \mathcal{S}$ that divide u with odd multiplicity
4. Then $u/g_u = x_u^2 + y_u^2$.
5. Let ψ_u be isogeny of degree g_u, computed by sequence of p_i-isogenies using Elkies' algorithm
6. Return

$$\varphi_u = \begin{pmatrix} \psi_u & 0 \\ 0 & \psi_u \end{pmatrix} \begin{pmatrix} x_u & y_u \\ -y_u & x_u \end{pmatrix}$$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$
4. Choosing pairs $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e\mathfrak{c}_k$, try to solve $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f < 2^{e-3}$

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$
4. Choosing pairs $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e\mathfrak{c}_k$, try to solve $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f < 2^{e-3}$
5. Use previous algorithm to construct φ_u, φ_v

An algorithm for solving the norm equation

Input: $\mathfrak{a} \subset \mathcal{O}$, $p = c2^e - 1$, Set of small split primes $\mathfrak{B}$

Output: Return $\mathfrak{b}_e, \mathfrak{b}_k, \mathfrak{c}_e, \mathfrak{c}_k, \varphi_u, \varphi_v$ such that $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f \leq 2^{e-3}$

1. Perform lattice reduction on $\mathfrak{a}$ to obtain small basis b_1, b_2
2. Use b_1, b_2 to iterate over small ideals $\mathrm{N}(\mathfrak{b})$ equivalent to $\mathfrak{a}$
3. Factor the ideals $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k$ so that $\mathrm{N}(\mathfrak{b}_e)$ is a product of primes in $\mathfrak{B}$
4. Choosing pairs $\mathfrak{b} = \mathfrak{b}_e\mathfrak{b}_k, \mathfrak{c} = \mathfrak{c}_e\mathfrak{c}_k$, try to solve $u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k) = 2^f < 2^{e-3}$
5. Use previous algorithm to construct φ_u, φ_v
6. Return $\mathfrak{b}_e, \mathfrak{b}_k, \varphi_u, \varphi_v$

Rerandomisation

If we cannot solve the norm equation for $[\mathfrak{a}]$ we can rerandomise

Rerandomisation

If we cannot solve the norm equation for $[\mathfrak{a}]$ we can rerandomise

Pick small ideal $[\mathfrak{l}]$ and compute $[\mathfrak{a}\mathfrak{l}] \cdot ([\mathfrak{l}]^{-1}E)$

Rerandomisation

If we cannot solve the norm equation for $[\mathfrak{a}]$ we can rerandomise

Pick small ideal $[\mathfrak{l}]$ and compute $[\mathfrak{a}\mathfrak{l}] \cdot ([\mathfrak{l}]^{-1}E)$

Let's look at some data ...

Some data for the solvability of the norm equation

	Avg	Med	Min	Max
Time:	0.149	0.111	0.043	2.286
Rerandomisations:	0.119	0	0	11
$\log(2^f = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k))$	494.284	495	476	500
UV solutions tried:	845.562	480	0	11020
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.285	4	0	19
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.297	2	0	10
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.768	2	0	8
13-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.612	1	0	8
3-Elkies steps for φ_u, φ_v:	0.496	0	0	1
7-Elkies steps for φ_u, φ_v:	0.256	0	0	1
11-Elkies steps for φ_u, φ_v:	0.165	0	0	1
13-Elkies steps for φ_u, φ_v:	0.000	0	0	0

Table: Times, rerandomisations and elkies steps required for $\log_2(p) = 33 \cdot 2^{503} - 1$.

Some data for the solvability of the norm equation

	Avg	Med	Min	Max
Time:	0.364	0.286	0.067	3.935
Rerandomisations:	0.061	0	0	7
$\log(2^f = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k))$	994.723	995	974	1001
UV solutions tried:	3810.389	2305	0	43378
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.574	4	0	24
5-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	3.011	3	0	12
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.482	2	0	10
13-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.908	2	0	9
3-Elkies steps for φ_u, φ_v:	0.505	1	0	1
5-Elkies steps for φ_u, φ_v:	0.000	0	0	0
7-Elkies steps for φ_u, φ_v:	0.250	0	0	1
13-Elkies steps for φ_u, φ_v:	0.173	0	0	1

Table: Times, rerandomisations and elkies steps required for $p = 15 \cdot 2^{1004} - 1$.

Some data for the solvability of the norm equation

	Avg	Med	Min	Max
Time:	2.396	1.268	0.135	25.267
Rerandomisations:	1.588	0	0	29
$\log(2^f = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k))$	1544.054	1545	1531	1548
UV solutions tried:	5436.683	1991	1	87007
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	5.582	5	0	18
5-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	3.746	4	0	11
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.402	2	0	8
3-Elkies steps for φ_u, φ_v:	0.513	1	0	1
5-Elkies steps for φ_u, φ_v:	0.000	0	0	0
11-Elkies steps for φ_u, φ_v:	0.181	0	0	1

Table: Times, rerandomisations and elkies steps required for $p = 9 \cdot 2^{1551} - 1$.

Some data for the solvability of the norm equation

	Avg	Med	Min	Max
Time:	4.148	2.181	0.163	57.346
Rerandomisations:	1.489	0	0	26
$\log(2^f = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k))$	2018.792	2019	1998	2023
UV solutions tried:	6873.200	2816	0	72885
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.891	4	0	22
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.733	3	0	9
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.172	2	0	9
17-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.785	2	0	9
3-Elkies steps for φ_u, φ_v:	0.520	1	0	1
7-Elkies steps for φ_u, φ_v:	0.260	0	0	1
11-Elkies steps for φ_u, φ_v:	0.162	0	0	1
17-Elkies steps for φ_u, φ_v:	0.000	0	0	0

Table: Times, rerandomisations and elkies steps required for $p = 51 \cdot 2^{2026} - 1$.

Some data for the solvability of the norm equation

	Avg	Med	Min	Max
Time:	37.137	24.506	0.968	542.416
Rerandomisations:	0.499	0	0	11
$\log(2^f = u\mathrm{N}(\mathfrak{b}_k) + v\mathrm{N}(\mathfrak{c}_k))$	4076.080	4077	4058	4081
UV solutions tried:	38952.563	19701	10	548118
3-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	4.950	4	0	17
7-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.658	2	0	9
11-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	2.010	2	0	9
17-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.691	1	0	7
19-Elkies steps for $\varphi_{\mathfrak{b}_e}, \varphi_{\mathfrak{c}_e}$:	1.567	1	0	6
3-Elkies steps for φ_u, φ_v:	0.496	0	0	1
7-Elkies steps for φ_u, φ_v:	0.259	0	0	1
11-Elkies steps for φ_u, φ_v:	0.160	0	0	1
17-Elkies steps for φ_u, φ_v:	0.000	0	0	0
19-Elkies steps for φ_u, φ_v:	0.106	0	0	1

Table: Times, rerandomisations and elkies steps required for $p = 63 \cdot 2^{4084} - 1$.

Our algorithm

What we implemented

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Step 2: Computing $\ker(\Phi)$ with Elkies steps

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Step 2: Computing ker(Φ) with Elkies steps

Evaluate the isogeny $\varphi_{\mathfrak{b}_e}$

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Step 2: Computing $\ker(\Phi)$ with Elkies steps

Evaluate the isogeny φ_{b_e}

Evaluate the isogeny $\widetilde{\varphi_{\mathfrak{c}_k}} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi_{\mathfrak{b}_e}} \varphi_{\mathfrak{c}_e} / \mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)$

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Step 2: Computing ker(Φ) with Elkies steps

Evaluate the isogeny φ_{b_e}

Evaluate the isogeny $\widetilde{\varphi_{\mathfrak{c}_k}} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi_{\mathfrak{b}_e}} \varphi_{\mathfrak{c}_e} / \mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)$

Step 3: Compute the 4d-isogeny

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Step 2: Computing ker(Φ) with Elkies steps

Evaluate the isogeny φ_{b_e}

Evaluate the isogeny $\widetilde{\varphi_{\mathfrak{c}_k}}\varphi_{\mathfrak{b}_k} = \widetilde{\varphi_{\mathfrak{b}_e}}\varphi_{\mathfrak{c}_e}/\mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)$

Step 3: Compute the 4d-isogeny

Pass the kernel to 4d-library

Our algorithm

What we implemented

Step 1: Finding UV

Do (easy) Lagrange lattice reduction on the input ideal $\mathfrak{a}$

Iterate small equivalent representatives

Factor out all small ideals $\mathfrak{b} = \mathfrak{b}_e \mathfrak{b}_k$

Try to solve the norm equation for the non-smooth part $\mathfrak{b}_k, \mathfrak{c}_k$

Step 2: Computing ker(Φ) with Elkies steps

Evaluate the isogeny φ_{b_e}

Evaluate the isogeny $\widetilde{\varphi_{\mathfrak{c}_k}} \varphi_{\mathfrak{b}_k} = \widetilde{\varphi_{\mathfrak{b}_e}} \varphi_{\mathfrak{c}_e} / \mathrm{N}(\mathfrak{b}_e)\mathrm{N}(\mathfrak{c}_e)$

Step 3: Compute the 4d-isogeny

Pass the kernel to 4d-library

Solve the twisting problem

Timings of the steps

Parameter	Find UV	Elkies	4D	Tot. Time
500	0.097s	0.48s	0.96s	1.53s
1000	0.21s	1.16s	2.84s	4.21s
1500	1.19s	2.85s	6.49s	10.5s
2000	1.68s	8.34s	11.3s	21.3s
4000	15.6s	52.8s	53.5s	122s

Table: SageMath 10.5 timings on Intel Core i5-1235U at 4.0 GHz, in wall-clock time.

Thank you

Paper https://eprint.iacr.org/2025/401

Implementation https://github.com/pegasis4d

Slides https://rueg.re/pegasis-swissogeny

Ask me anything (I have bonus slides!)

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider $\gamma_1 = x_1 + y_1\sqrt{\Delta}$ and $\gamma_2 = x_2 + y_2\sqrt{\Delta}$ in $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider $\gamma_1 = x_1 + y_1\sqrt{\Delta}$ and $\gamma_2 = x_2 + y_2\sqrt{\Delta}$ in $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Then

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \to E^2 \qquad \text{has} \qquad \deg_p(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider $\gamma_1 = x_1 + y_1\sqrt{\Delta}$ and $\gamma_2 = x_2 + y_2\sqrt{\Delta}$ in $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Then

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \to E^2 \qquad \text{has} \qquad \deg_p(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

Idea If $N \gg |\Delta|$ then $m = N - |\Delta|(y_1^2 + y_2^2) \geq 0$ often enough that we find $m = x_1^2 + x_2^2$ as sum of squares

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Consider $\gamma_1 = x_1 + y_1\sqrt{\Delta}$ and $\gamma_2 = x_2 + y_2\sqrt{\Delta}$ in $\mathcal{O} = \mathbb{Z} + \sqrt{\Delta}\mathbb{Z}$

Then

$$\gamma = \begin{pmatrix} \gamma_1 & \overline{\gamma_1} \\ -\gamma_2 & \overline{\gamma_2} \end{pmatrix} : E^2 \to E^2 \qquad \text{has} \qquad \deg_p(\gamma) = (x_1^2 + x_2^2) + \Delta(y_1^2 + y_2^2)$$

Idea If $N \gg |\Delta|$ then $m = N - |\Delta|(y_1^2 + y_2^2) \geq 0$ often enough that we find $m = x_1^2 + x_2^2$ as sum of squares

Heuristic If $N \gg |\Delta|$, we can find endomorphism of E^2 with polarised degree N

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1 \mu_2 = \nu_2 \nu_1$ with $\deg_{\mathrm{p}}(\mu_1) = N_1$ and $\deg_{\mathrm{p}}(\nu_1) = N_2$

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_p(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1\mu_2 = \nu_2\nu_1$ with $\deg_p(\mu_1) = N_1$ and $\deg_p(\nu_1) = N_2$

Then the 4-dimensional isogeny

$$\Gamma = \begin{pmatrix} \mu_1 & \widetilde{\mu_2} \\ -\nu_1 & \widetilde{\nu_2} \end{pmatrix}$$

has polarised degree $N = N_1 + N_2$ and kernel $\left\{(\deg_p(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\right\}$

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_p(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1\mu_2 = \nu_2\nu_1$ with $\deg_p(\mu_1) = N_1$ and $\deg_p(\nu_1) = N_2$

Then the 4-dimensional isogeny

$$\Gamma = \begin{pmatrix} \mu_1 & \widetilde{\mu_2} \\ -\nu_1 & \widetilde{\nu_2} \end{pmatrix}$$

has polarised degree $N = N_1 + N_2$ and kernel $\left\{(\deg_p(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\right\}$

Idea (Specific to Frobenius orientation)

Constructing isogenies of prescribed degree

In dimension 2 with QFESTA splitting via 4-dimensional isogeny

Moreover

Let $\deg_{\mathrm{p}}(\gamma) = N_1 N_2$ with N_i coprime

Then $\gamma = \mu_1\mu_2 = \nu_2\nu_1$ with $\deg_{\mathrm{p}}(\mu_1) = N_1$ and $\deg_{\mathrm{p}}(\nu_1) = N_2$

Then the 4-dimensional isogeny

$$\Gamma = \begin{pmatrix} \mu_1 & \widetilde{\mu_2} \\ -\nu_1 & \widetilde{\nu_2} \end{pmatrix}$$

has polarised degree $N = N_1 + N_2$ and kernel $\left\{(\deg_{\mathrm{p}}(\mu_1)x, \gamma(x)) \mid x \in E^2[N]\right\}$

Idea (Specific to Frobenius orientation)

Our $u \approx \sqrt{\Delta} = \sqrt{p}$

Set $N = u(2^{e/2} - u) \gg |\Delta| = p$ to get 4-dimensional isogeny Γ of degree $2^{e/2}$

Obtain u-isogeny $\mu_i : E^2 \to A_u$ as component of Γ

Improved timings

Parameter	Find UV	Elkies	Exp. Total time	Prev. Total time	N. Rerand.
2000	0.49 s	3.83 s	21.57 s	21.3 s	0.70
4000	3.25 s	22.8 s	106.25 s	122 s	1.25

Table: Step 1 and Step 2 when solving the norm equation with single sum of squares, in wall-clock seconds.

Working over F_p: Fast basis sampling

Let $p \equiv 7 \pmod 8$ and E/F_p oriented by $\mathbb{Z}\left[\left(\sqrt{-p}+1\right)/2\right]$

Working over F_p: Fast basis sampling

Let $p \equiv 7 \pmod 8$ and E/F_p oriented by $\mathbb{Z}\left[\left(\sqrt{-p}+1\right)/2\right]$

Then for $2^e \,||\, p+1$ we have

$$E[2^e] \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} + {}^{\mathbb{Z}}/_{2^{e-1}\mathbb{Z}}$$

Working over F_p: Fast basis sampling

Let $p \equiv 7 \pmod 8$ and E/F_p oriented by $\mathbb{Z}\left[\left(\sqrt{-p}+1\right)/2\right]$

Then for $2^e \,||\, p+1$ we have

$$E[2^e] \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} + {}^{\mathbb{Z}}/_{2^{e-1}\mathbb{Z}}$$

Let $T_{\text{desc}}, T_{\text{horiz},1}, T_{\text{horiz},2}$ points of 2-torsion

Working over F_p: Fast basis sampling

Let $p \equiv 7 \pmod 8$ and E/F_p oriented by $\mathbb{Z}\left[\left(\sqrt{-p}+1\right)/2\right]$

Then for $2^e \,||\, p+1$ we have

$$E[2^e] \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} + {}^{\mathbb{Z}}\!/_{2^{e-1}\mathbb{Z}}$$

Let $T_{\text{desc}}, T_{\text{horiz},1}, T_{\text{horiz},2}$ points of 2-torsion

Lemma

Let $E : y^2 = g(x)$

An element x_p in F_p lifts to $P = (x_p, y_p)$

(i) on E with $\text{ord}(P) = 2^{e-1}$ iff $x_p - x(T_{\text{desc},1})$ a non-zero non-square (and $g(x_p)$ non-zero square)

(ii) on E^t with $\text{ord}(P) = 2^{e-1}$ iff $x_p - x(T_{\text{desc},2})$ non-zero square (and $g(x_p)$ a non-zero non-square)