KLPT^2: Algebraic pathfinding in dimension two and applications

徐铮

2025.10.31

目录

1 Principally Polarized Abelian Surfaces

Defintion 1 (Principally Polarized Abelian Varieties) Let A be an abelian variety defined over k. Then a divisor D determines an isogeny

$$\begin{aligned}\lambda_D : A \to \hat{A} &= \mathrm{Pic}^0(A)\\ P \to &[t_{-P}(D) - D]\end{aligned}$$

where t_{-P} denotes point-wise translation by $-P$.

If D is an ample divisor, then λ_D is a polarization on A.

If moreover $\deg(\lambda_D) = 1$, then λ_D is a principally polarization of A and (A, D) is called a principally polarized abelian variety. Here we haven't defined the degree of isogeny, the origin definition can be obtained from intersection number: $\deg(\lambda_D) = \left(\frac{(D \bullet D)}{g!}\right)^2$.

Defintion 2 (Superspecial Abelian Varieties) Let A be an abelian variety of dimension g, if A is isomorphic to a product of g supersingular elliptic curves, then we say A is a superspecial abelian variety.

Theorem 1 There are two types of principally polarized superspecial abelian surface over $\bar{\mathbb{F}}_p$:

1. Jacobian type $\mathrm{Jac}(C)$: consisting of Jacobians of superspecial hyperelliptic curve C of genus 2 with the canonical principal polarization C, whose number (isomorphism classes) is

$$\begin{cases} 0, & \text{if } p = 2, 3,\\ 1, & \text{if } p = 5,\\ \dfrac{p^3 + 24p^2 + 141p - 346}{2880}, & \text{if } p > 5. \end{cases}$$

2. Product type $E_1 \times E_2$: consisting of products of two supersingular elliptic curves E_1, E_2 with the principal polarization $E_1 \times \{0\} + \{0\} \times E_2$, whose number is

$$\begin{cases} 1, & \text{if } p = 2, 3, 5,\\ \frac{1}{2} S_{p^2}(S_{p^2} + 1), & \text{if } p > 5, \end{cases}$$

where S_{p^2} is the number of isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$.

2 Isogenies Between Abelian Surfaces

Defintion 3 (Isogenies) Let A, B be two abelian varieties over k, $\varphi : A \to B$ be a morphism, if two of the following conditions holds:

- φ is surjective
- $\ker(\varphi)$ is finite
- $\dim(A) = \dim(B)$

we say φ is an isogeny between A and B.

Defintion 4 (Isogenies between Principally Polarized Abelian Surfaces) A (polarized) isogeny between two principally polarized abelian surfaces (A, λ_A) and (B, λ_B) is an isogeny $\varphi : A \to B$ that respects the polarizations, i.e., there exists a positive integer N for which the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "{[N]\lambda_A}"'] & B \arrow[d, "\lambda_B"] \\ \hat{A} & \hat{B} \arrow[l, "\hat{\varphi}"] \end{tikzcd}$$

Here, $\hat{\varphi}$ is the dual isogeny, defined by taking inverse image divisors under φ, and $\deg(\varphi) = N^2$. (We simplify denote the reduced degree of φ as $\mathrm{degrd}(\varphi) = N$.)

If $N = 1$, then φ is called a (polarized) isomorphism.

Remark 1 From above, we define $\tilde{\varphi} = \lambda_A^{-1} \circ \hat{\varphi} \circ \lambda_B : B \to A$ as adjoint isogeny(dual isogeny) of φ.

It is easily to see that if φ is polarized, we have $\varphi \circ \tilde{\varphi} = [N]$ and $\tilde{\varphi} \circ \varphi = [N]$.

If the isogeny φ is an endomorphism of A, the adjoint isogeny of φ is also called Rosati involution of φ, denoted by $\varphi^\dagger$, i.e. $\varphi^\dagger = \lambda_A^{-1} \circ \hat{\varphi} \circ \lambda_A$.

Defintion 5 (Maximal Weil Isotropic Subgroups) If m is prime to p, a subgroup S of $A[m]$ is called maximal m-isotropic if it is maximal among subgroups T of $A[m]$ such that the restriction of the Weil pairing $e_m : A[m] \times A[m] \to \mu_m$ on $T \times T$ is trivial.

Theorem 2 Let (A, D) be a principal polarized abelian surface, $\phi : A \to A' = A/S$ be the isogeny with kernel S. If S is a maximal m-isotropic subgroup of $A[m]$, then exists a divisor D' on A' such that (A', D') is also a principally polarized abelian variety, i.e. $[m]\lambda_D = \hat{\varphi} \circ \lambda_{D'} \circ \varphi$ or $\varphi^* D' \sim mD$.

3 Relationship Between Isogenies and Matrices (Ibukiyama-Katsura-Oort Correspondence)

3.1 Endomorphsims of E^2

Let E be a fixed supersingular elliptic curve, $\mathcal{O} := \mathrm{End}(E)$.

Then E^2 is a superspecial abelian variety of dimension 2, equipped with the principal polarization $\{0\} \times E + E \times \{0\}$. We have $\mathrm{End}(E^2) = M_2(\mathcal{O})$ and

$$\mathrm{Aut}(E^2) = \mathrm{GL}_2(\mathcal{O}) = \{M \in M_2(\mathcal{O}) \mid M \text{ is invertible}\}.$$

The reduced norm $\mathrm{Nrd} : \mathcal{O} \to \mathbb{Z}$ induces the reduced norm $\mathrm{Nrd} : M_2(\mathcal{O}) \to \mathbb{Z}$.

Remark 2 Moreover, if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O})$, the reduced norm of M can be defined as $\mathrm{Nrd}(M) = \mathrm{Nrd}(\Delta(M))$, where $\Delta(M) = \begin{cases} -bc & \text{if } a = 0 \\ ad - aca^{-1}b & \text{if } a \neq 0 \end{cases}$. The above definition of reduced norm of matrix is also called Dieudonne determinant. By computation, we have $\mathrm{Nrd}(M) = \det(M^+ M)$.

By computation, we have the degree of φ equals to the redced norm of matrix M.

For $M \in M_g(\mathcal{O})$, let M^+ denote the conjugate transpose of M. If M is associated to the endomorphism $\alpha \in \mathrm{End}(A)$, then M^+ is the matrix associated to the Rosati involution $\alpha^\dagger$.

3.2 IKO Correspondence

Let A be a superspecial abelian variety of dimension 2. E^2 and A are isomorphic. Let $\iota_A : A \to E^2$ be a fixed isomorphism which induces $\iota_A : \mathrm{End}(A) \cong M_2(\mathcal{O})$. Note that another isomorphism ι'_A is uniquely determined by $\iota'_A \iota_A^{-1} \in \mathrm{GL}_2(\mathcal{O})$.

Ibukiyama, Katsura and Oort leverage matrices to represent principal polarizations as following:

Suppose X is a (fixed) principal polarized divisor of A. The map

$$\mu : \mathrm{Pic}(A) \to \mathrm{End}(A), \quad L \mapsto \lambda_X^{-1} \circ \lambda_L$$

factors through the Néron-Severi group $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$. Denote the quotient map by

$$j : NS(A) \to \mathrm{End}(A) \cong M_g(\mathcal{O}); \qquad \overline{L} \to \iota_A(\lambda_X^{-1} \circ \lambda_L). \tag{1}$$

This map extends to $j : NS(A) \otimes \mathbb{Q} \to \mathrm{End}(A) \otimes \mathbb{Q} \cong M_g(\mathcal{O}) \otimes \mathbb{Q}$.

Proposition 1 The map j is invariant under the Rosati involution, which implies that

$$j(\bar{L}) = j(\bar{L})^+.$$

The following result allows us to determine whether a divisor of an abelian variety corresponds to a (principal) polarization.

Proposition 2 Let L be a divisor of an abelian variety A of dimension g. Then

1. L is associated to a polarization (i.e. L is an ample divisor) if and only if $j(\bar{L})$ is positive definite;
2. L is associated to a principal polarization if and only if $j(\bar{L})$ is positive definite with reduced norm 1.

Overall, j is injective and the image of j are $\left\{ \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \in M_2(\mathscr{O}) \mid a, c \in \mathbb{Z}_+, ac - b\bar{b} = 1 \right\}$

Defintion 6 (Equivalent of Principally Polarizations) Two principal polarizations λ_1 and λ_2 on an abelian variety A are said to be equivalent if $(A, \lambda_1) \cong (A, \lambda_2)$, i.e. there exists an automorphism α of A such that $\hat{\alpha}\lambda_1\,\alpha = \lambda_2$.

We write $\mathrm{PPol}^0(A)$ for the set of principal polarizations on A up to equivalence.

Let

$$\mathscr{H} = \{H \in M_n(\mathscr{O}) \mid H \text{ is positive-definite Hermitian of reduced norm } 1\},$$

if we write principal polarizations as matrices in $\mathscr{H}$, automorphim α as matrix in $\mathrm{GL}_2(\mathscr{O})$, we have the following result corresponding to above definition:

Proposition 3 Two matrices H and H' in $\mathscr{H}$ correspond to the same polarized divisor if and only if they are in the same orbit under the action of $\mathrm{GL}_2(\mathscr{O})$ on the set $\mathscr{H}$:

$$\mathrm{GL}_2(\mathscr{O}) \times \mathscr{H} \to \mathscr{H}; \quad (M, H) \mapsto M^+HM.$$

Moreover, there is a one-to-one correspondence between $\mathscr{H} \,/\, \mathrm{GL}_g(\mathscr{O})$ and the set of isomorphism classes of principal polarized abelian surfaces of dimension 2.

4 The (ℓ, ℓ)-isogeny graph of principal polarized abelian surfaces

Suppose $p > 3$ and ℓ is a prime different from p.

Let (A, D_1) and (A, D_2) be two principally polarized abelian surfaces over $\overline{\mathbb{F}}_p$. An (ℓ, ℓ)-isogeny is an isogeny $\phi : A_1 \to A_2$ such that $\ker(\phi) \cong \mathbb{Z}\,/\ell\,\mathbb{Z} \times \mathbb{Z}\,/\ell\,\mathbb{Z}$.

We can describe (ℓ, ℓ) isogenies using matrices in $M_2(\mathscr{O})$ in the following proposition.

Proposition 4 Let A be a superspecial abelian surface, P_1 and P_2 be two principal polarizations of A. Let $H_1 = j(\bar{P}_1)$ and $H_2 = j(\bar{P}_2)$. If $\alpha : A \to A$ is an isogeny of degree ℓ^{2m} associated to $M \in M_2(\mathscr{O})$, then $\alpha^*(P_2) = \ell^m P_1$ if and only if $M^+H_2M = \ell^m H_1$, and in this case, α is an isogeny from (A, P_1) to (A, P_2).

Proof. For α is an isogeny from (A, λ_1) to (A, λ_2), where λ_i corresponds to P_i, $i = 1, 2$, we have $[\ell^m]\lambda_1 = \hat{\varphi}\lambda_2\,\varphi$.

Then $[\ell^m]\lambda_0^{-1}\lambda_1 = \lambda_0^{-1}\hat{\varphi}\lambda_0\lambda_0^{-1}\lambda_2\,\varphi$, φ(endomorphism of A without polarization) corresponds to matrix M, $\lambda_0^{-1}\hat{\varphi}\lambda_0$ is the Rosati involution of endomorphism φ, hence $\lambda_0^{-1}\hat{\varphi}\lambda_0$ corresponds to matrix M^+. Moreover, by the map j, $\lambda_0^{-1}\lambda_i$ corresponds to matrix H_i, $i = 1, 2$. Therefore, we have $[\ell^m]H_1 = M^+H_2M$. $\square$

5 Pathfinding in Dimension 2

Lemma 1 Let $h_1, h_2 \in M_2(\mathscr{O}_0)$ be Hermitian matrices with equal upper-left entries and equal determinants, i.e. we have $h_1 = \begin{pmatrix} D & r_1 \\ \bar{r}_1 & t_1 \end{pmatrix}, h_2 = \begin{pmatrix} D & r_2 \\ \bar{r}_2 & t_2 \end{pmatrix}$ for $D, t_1, t_2 \in \mathbb{Z}$, $r_1, r_2 \in \mathscr{O}_0$ such that $Dt_1 - \mathrm{Nrd}(r_1) = Dt_2 - \mathrm{Nrd}(r_2)$. Then for $\tau = \begin{pmatrix} D & r_1 - r_2 \\ 0 & D \end{pmatrix}$, we have $\tau^+h_2\tau = D^2h_1$.

Lemma 2 Assume that $\delta^+ g_2 \delta = N u^+ g_1 u$ with $N \in \mathbb{Z}$, $u, \delta \in M_2(\mathscr{O}_0)$. Then there exists $\gamma \in M_2(\mathscr{O}_0)$ such that $\gamma^+ g_2 \gamma = N \operatorname{Nrd}(u)^2 g_1$.

Proof. $\gamma = \delta u^{-1} \operatorname{Nrd}(u)$. For any Hermite matrix g, we have $g^{-1}\det(g) \in M_2(\mathscr{O}_0)$, therefore, $(u^+u)^{-1}\det(u^+u) \in M_2(\mathscr{O}_0)$. Hence, $u^{-1}\operatorname{Nrd}(u) \in M_2(\mathscr{O}_0)$, and $\gamma \in M_2(\mathscr{O}_0)$. □

Now we want to solve the problem: finding $\gamma \in M_2(\mathscr{O}_0)$ such that $\gamma^+ g_2 \gamma = \ell^e g_1$?

5.1 First Step

For any $g = \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}$ corresponds to principally polarization, how to find $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathscr{O}_0)$ such that the upper left entry of u^+gu is ℓ^{e_2} for fixed e_2 and $\operatorname{Nrd}(u)$ is another fixed power of ℓ?

By computation, we have the upper left entry of u^+gu is

$$s' = s\operatorname{Nrd}(a) + t\operatorname{Nrd}(c) + \operatorname{Trd}(\bar{c}\bar{r}a)$$

and the bottom right entry is

$$t' = s\operatorname{Nrd}(b) + t\operatorname{Nrd}(d) + \operatorname{Trd}(\bar{b}\bar{r}d)$$

Now we need solve the new problem: find a, c such that s' is ℓ^{e_2} and find b, d such that $\operatorname{Nrd}(u)$ is ℓ^{e_0}.

5.2 Second Step

The second step is to find s'.

For finding a, c, we choose $a = a_1 + a_2 i \in \mathbb{Z}[i]$, $c = c_1\bar{r}j + c_2\bar{r}k \in \bar{r}j\,\mathbb{Z}[i]$. Since $\operatorname{Trd}(\bar{c}\bar{r}a) = 0$, then we only solve:

$$\ell^{e_2} = s(a_1^2 + a_2^2) + tp\operatorname{Nrd}(r)(c_1^2 + c_2^2)$$

As in KLPT's algorithm, by module s, we compute c_1, c_2. After Cornacchia's algorithm, we obtain a_1, a_2.

5.3 Third Step

After obtaining a, c, we will find b, d. i.e. find u.

Since $\operatorname{Nrd}\left(\begin{pmatrix} a & x \\ c & y \end{pmatrix}\right) = \operatorname{Nrd}(a)\operatorname{Nrd}(y) + \operatorname{Nrd}(c)\operatorname{Nrd}(x) - \operatorname{Trd}(\bar{a}x\bar{y}c) = \ell^{e_0}$, we define a quadratic form $Q(x, y) = \operatorname{Nrd}(a)\operatorname{Nrd}(y) + \operatorname{Nrd}(c)\operatorname{Nrd}(x) - \operatorname{Trd}(\bar{a}x\bar{y}c)$.

Then we have:

Lemma 3 Let $M_1 = (a, c)\,\mathscr{O}_0$. Furthermore, let α, β be integers such that $\alpha\operatorname{Nrd}(a) + \beta\operatorname{Nrd}(c) = 1$. Let $M_2 = (\beta\operatorname{Nrd}(c)a, -\alpha\operatorname{Nrd}(a)c)B_{p,\infty} \cap \mathscr{O}_0^2$. Then M_2 is a right $\mathscr{O}_0$-module and $M_1 \oplus M_2 = \mathscr{O}_0^2$.

Proof. It is easily to see that M_2 is a right $\mathscr{O}_0$-module since M_2 is the intersection of two right $\mathscr{O}_0$-modules.

For any element $w = (\beta\operatorname{Nrd}(c)a, -\alpha\operatorname{Nrd}(a)c)z \in M_2$, where $z \in B_{p,\infty}$, then

$$\begin{aligned}
Q(w) &= \operatorname{Nrd}(a)\operatorname{Nrd}(-\alpha\operatorname{Nrd}(a)cz) + \operatorname{Nrd}(c)\operatorname{Nrd}(\beta\operatorname{Nrd}(c)az) - \operatorname{Trd}(\bar{a}\,\beta\operatorname{Nrd}(c)az\overline{(-\alpha\operatorname{Nrd}(a)cz)}c) \\
&= \alpha^2\operatorname{Nrd}(a)^3\operatorname{Nrd}(c)\operatorname{Nrd}(z) + \beta^2\operatorname{Nrd}(c)^3\operatorname{Nrd}(a)\operatorname{Nrd}(z) + 2\,\alpha\,\beta\operatorname{Nrd}(c)^2\operatorname{Nrd}(a)^2\operatorname{Nrd}(z) \\
&= \operatorname{Nrd}(a)\operatorname{Nrd}(c)\operatorname{Nrd}(z)(\alpha^2\operatorname{Nrd}(a)^2 + \beta^2\operatorname{Nrd}(c)^2 + 2\,\alpha\,\beta\operatorname{Nrd}(a)\operatorname{Nrd}(c)) \\
&= \operatorname{Nrd}(a)\operatorname{Nrd}(c)\operatorname{Nrd}(z)(\alpha\operatorname{Nrd}(a) + \beta\operatorname{Nrd}(c))^2 \\
&= \operatorname{Nrd}(a)\operatorname{Nrd}(c)\operatorname{Nrd}(z)
\end{aligned}$$

Since every element in M_1 with $Q(x,y)$-norm 0, and $a, c, z \neq 0$, then we have $M_1 \cap M_2 = \{0\}$.

Moreover, by computation, we have:

$$(a,c)\,\alpha\,\bar{a} + (\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)\frac{1}{\mathrm{Nrd}(a)}\bar{a} = (1,0)$$

$$(a,c)\,\beta\,\bar{c} - (\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)\frac{1}{\mathrm{Nrd}(c)}\bar{c} = (0,1)$$

It implies $M_1 \oplus M_2 = \mathscr{O}_0^2$. □

Proposition 5 The module M_2 is $\mathrm{Nrd}(c)$-homothetic to the right $\mathscr{O}_0$-ideal $I = \mathrm{Nrd}(c)\,\mathscr{O}_0 + a\bar{c}\,\mathscr{O}_0$. More precisely, the map

$$\tau : M_2 \to I$$

$$(\beta\,\mathrm{Nrd}(c), -\alpha\,c\bar{a})o_1 + (\beta\,a\bar{c}, -\alpha\,\mathrm{Nrd}(a))o_2 \to \mathrm{Nrd}(c)o_1 + a\bar{c}o_2,\ \ o_1, o_2 \in \mathscr{O}_0$$

is a well-defined isomorphism of right $\mathscr{O}_0$-modules such that $Q(\tau(m)) = \mathrm{Nrd}(c)Q(m)$ for all $m \in M_2$.

Proof. Note that $(\beta\,\mathrm{Nrd}(c), -\alpha\,c\bar{a}) = (\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)\frac{1}{a}$, $(\beta\,a\bar{c}, -\alpha\,\mathrm{Nrd}(a)) = (\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)\frac{1}{c}$ are in M_2.

Next, observe that

$$\begin{aligned}
Q((\beta\,\mathrm{Nrd}(c), -\alpha\,c\bar{a})o_1 + (\beta\,a\bar{c}, -\alpha\,\mathrm{Nrd}(a))o_2) &= Q((\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)(a^{-1}o_1 + c^{-1}o_2)) \\
&= \mathrm{Nrd}(a)\,\mathrm{Nrd}(c)\,\mathrm{Nrd}(a^{-1}o_1 + c^{-1}o_2) \\
&= \frac{1}{\mathrm{Nrd}(c)}\,\mathrm{Nrd}(a\,\mathrm{Nrd}(c)(a^{-1}o_1 + c^{-1}o_2)) \\
&= \frac{1}{\mathrm{Nrd}(c)}\,\mathrm{Nrd}(\mathrm{Nrd}(c)o_1 + a\bar{c}o_2)
\end{aligned}$$

It shows the map τ satisfied $Q(\tau(m)) = \mathrm{Nrd}(c)\,\mathrm{Nrd}(m)$.

It is easily to see that τ from $M_2' = \langle(\beta\,\mathrm{Nrd}(c), -\alpha\,c\bar{a}), (\beta\,a\bar{c}, -\alpha\,\mathrm{Nrd}(a))\,\rangle$ to I is bijective.

It remains to argue that $M_2' = M_2$.

As the proof in Lemma 3, we have:

$$(a,c)\,\alpha\,\bar{a} + (\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)\frac{1}{\mathrm{Nrd}(a)}\bar{a} = (a,c)\,\alpha\,\bar{a} + (\beta\,\mathrm{Nrd}(c), -\alpha\,c\bar{a}) = (1,0)$$

$$(a,c)\,\beta\,\bar{c} - (\beta\,\mathrm{Nrd}(c)a, -\alpha\,\mathrm{Nrd}(a)c)\frac{1}{\mathrm{Nrd}(c)}\bar{c} = (a,c)\,\beta\,\bar{c} - (\beta\,a\bar{c}, -\alpha\,\mathrm{Nrd}(a)) = (0,1)$$

It means $M_1 \oplus M_2' = \mathscr{O}_0^2$, and then $M_2 = M_2'$. □

We use KLPT's algorithm to generate an element in I with reduced norm $\mathrm{Nrd}(c)\ell^{e_0}$. Then this element can be written as $\mathrm{Nrd}(c)o_1 + a\bar{c}o_2$, and $(\beta\,\mathrm{Nrd}(c), -\alpha\,c\bar{a})o_1 + (\beta\,a\bar{c}, -\alpha\,\mathrm{Nrd}(a))o_2$ has $Q(x,y)$-norm ℓ^{e_0}. Hence, we choose $b = \beta\,\mathrm{Nrd}(c)o_1 + \beta\,a\bar{c}o_2$, $d = -\alpha\,c\bar{a}o_1 - \alpha\,\mathrm{Nrd}(a)o_2$, and the reduced norm of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is ℓ^{e_0}.

5.4 Fourth Step

However, when we find a, c, we need to solve the Diophantine equation by module s. To decrease the size of outputs, we should choose a small s.

The method to solve this problem is finding a transformation matrix u' making s as small as possible.

Since after the action of $u' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have $s' = s\,\mathrm{Nrd}(a) + t\,\mathrm{Nrd}(c) + \mathrm{Trd}(\bar{c}\bar{r}a)$. It shows s' only depends on a, c, we can also choose b, d as above to make sure the reduced norm of u' is power of ℓ.

We first define the quadratic form $K(x,y) = s\,\mathrm{Nrd}(x) + t\,\mathrm{Nrd}(y) + \mathrm{Trd}(\bar{y}\bar{r}x)$, then we have:

Proposition 6 The quadratic form $K(x,y)$ is positive definite and has determinant $\left(\frac{p}{4}\right)^4$.

Proof. It is easily to see that $K(x,y)$ is semi-positive definite. If there exists $(a,c) \neq (0,0)$ such that $s' = K(a,c) = 0$, then the matrix $u'^{+}gu'$ has form $\begin{pmatrix} 0 & r' \\ \bar{r}' & t' \end{pmatrix}$. The reduced norm of $u'^{+}gu'$ is $-\operatorname{Nrd}(r') \leq 0$, which is a contradiction. Hence K is positive definite.

Writing $r = r_1 + r_2 i + r_3 j + r_4 k$, then we have the matrix of K under basis $\{(1,0),(i,0)\cdots,(0,k)\}$ is

$$\begin{pmatrix} s & 0 & 0 & 0 & r_1 & -r_2 & -pr_3 & -pr_4 \\ 0 & s & 0 & 0 & r_2 & r_1 & -pr_4 & pr_3 \\ 0 & 0 & sp & 0 & pr_3 & pr_4 & pr_1 & -pr_2 \\ 0 & 0 & 0 & sp & pr_4 & -pr_3 & pr_2 & pr_1 \\ r_1 & -r_2 & pr_3 & pr_4 & t & 0 & 0 & 0 \\ -r_2 & r_1 & pr_4 & -pr_3 & 0 & t & 0 & 0 \\ -pr_3 & -pr_4 & pr_1 & pr_2 & 0 & 0 & tp & 0 \\ -pr_4 & pr_3 & -pr_2 & pr_1 & 0 & 0 & 0 & tp \end{pmatrix}$$

where the entry of this matrix is the inner product(induced by $K(x,y)$) of two elements in basis, for example $\langle (1,0),(0,k) \rangle = \frac{K((1,k))-K((1,0))-K((0,k))}{2} = \frac{s+pt-2r_4p-s-tp}{2} = -r_4 p$.

The determinant of this matrix is $p^4(st - \operatorname{Nrd}(r))^4 = p^4$. Any matrix of base change between a $\mathbb{Z}$-basis of $\mathscr{O}_0^2$ and the above basis has determinant $1/16$, leading to the desired result. $\square$

From the Minkowski bound, we have there exists at least one vector with $s' < 4\left(\frac{(p/4)^2}{v_8}\right)^{1/4} < \frac{3}{2}\sqrt{p}$, where $v_8 = \frac{\pi^4}{24}$ is the volume of an 8-dimension unit ball.

Moreover, since $\alpha \operatorname{Nrd}(a) + \beta \operatorname{Nrd}(c) = 1$, it should be required $\operatorname{Nrd}(a), \operatorname{Nrd}(c)$ are coprime. To simplify this case, we require s' is a prime different from $2, \ell$. Hence, we will enlarge the above bound.

For we have $\#\{(a,c) \in \mathscr{O}_0^2 \mid K(a,c) < R\} \approx v_8 \frac{R^4}{(p/4)^2}$, and if we require $K(a,c)$ is a prime (coprime to $2,\ell$), we have $v_8 \frac{R^4}{(p/4)^2} \geq \frac{\pi^2}{6}\frac{2\ell}{\varphi(2\ell)} \ln(R)$. We choose $R = \sqrt{p}(\ln(p))^{1/4}$, then there exists such (a,c).

From above, we assume the matrix $u'^{+}gu'$ also has the form $\begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}$, where $s,t \in \mathbb{Z}_+$ and $r \in \mathscr{O}_0$, $st - \operatorname{Nrd}(r) > 0$. Since after transformation of u', the determinant of $\begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix}$ is ℓ^{2e_0}, $s \leq \sqrt{p}(\ln(p))^{1/4}$ is a prime not dividing $2\ell t$. For r, we use matrix $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ to make sure $|r_i| \leq \frac{s}{2}$, then $\operatorname{Nrd}(r) \leq s^2 p$.

6 The Size of KLPT^2

To find new s as small as possible, we compute a,c to obtain and set $g' = u'^{+}gu'$. To ensure the reduced norm of u' is power of ℓ, we use the method mentioned in Third Step to compute b,d.

Note that the output of KLPT's algorithm is $O(p^3)$, then the reduced norm of u' is $O(p^3)$.

After that, since $s \approx \sqrt{p}$, in

$$\ell^{e_2} = s(a_1^2 + a_2^2) + tp \operatorname{Nrd}(r)(c_1^2 + c_2^2)$$

$c_1, c_2 \approx s$, then $tp \operatorname{Nrd}(r)(c_1^2 + c_2^2) = O(\frac{p^3}{s} \cdot p \cdot s^2 p \cdot 2s^2) = O(p^{6.5})$.

It means the reduced norm of u'' is also $O(p^3)$.

We use first u' to obtain a small s, and use another u'' to obtain the matrix we needed.

Overall, the matrix $(u'u'')^+ g_1 u'u''$ has reduced norm $O(p^6)$ and the upper-left entry of this matrix is $\ell^{e_2} = O(p^{6.5})$. Similarly to $g_2((u_1'u_1'')^+ g_2 u_1'u_1''$ has reduced norm $O(p^6)$ and the upper-left entry of this matrix is $\ell^{e_2} = O(p^{6.5})$.).

From Lemma 1, 2, there exists τ with reduced norm ℓ^{e_2} such that

$$\tau^+(u'u'')^+ g_1 u'u''\tau = \ell^{2e_2}(u_1'u_1'')^+ g_2 u_1'u_1''$$

Overall, we have there exists $\gamma = u'u''\tau(u_1'u_1'')^{-1}\operatorname{Nrd}(u_1'u_1'')$ such that $\gamma^+ g_1 \gamma = \ell^{2e_2}\operatorname{Nrd}(u_1'u_1'')^2 g_2$, where $\ell^{2e_2}\operatorname{Nrd}(u_1'u_1'')^2 = O(p^{13}\cdot p^{12}) = O(p^{25})$.

7 Translating Between Matrices and Isogenies

7.1 Matrices to Isogenies

For any $\gamma \in M_2(\mathscr{O}_0)$ of reduced norm N^2, $N = N_1 N_2 \cdots N_r$, then the isogeny corresponds to γ can be written as $\varphi_r \circ \cdots \circ \varphi_2 \circ \varphi_1$, and the codomain of every step is either a product of elliptic curves or the Jacobian of genus 2 curve.

For every N_i, we choose a basis P_i, Q_i of $E_0[N_i]$, and $(P_i, 0), (0, P_i), (Q_i, 0), (0, Q_i)$ is a basis of E_0^2. By acting γ on $(xP_i + zQ_i, yP_i + wQ_i)$, one obtain x, y, z, w by solving discrete logarithm(Another simpler method is to evaluate the adjoint isogeny $N\gamma^{-1}$ on N_i-torsion points).

From above, we obtain $\ker(\gamma)[N_i]$. For computing the i-th step, we send $\ker(\gamma)[N_i]$ by $\varphi_{i-1} \circ \cdots \circ \varphi_1$ and denote it by S_i. After that, we compute the isogeny from $A_{i-1} \to A_i$ with kernel S_i, then we get the i-th step. Overall, we obtain the isogeny step by step.

algorithm 1 MatrixToIsogeny

INPUT: $\gamma \in M_2(\mathscr{O}_0)$ with $\operatorname{Nrd}(\gamma) = (N_1 \cdots N_r)^2$ powersmooth.

OUTPUT: polarized isogeny $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$ with $\deg(\varphi_i) = N_i^2$ corrsponds to γ.

$\tilde{\gamma} = N\gamma^{-1}$, $\varphi_0 = 1$;
for $i = 1, \cdots r$ **do**
  $\langle P_i, Q_i \rangle = E_0[N_i]$;
  $S_i \leftarrow \tilde{\gamma}((P_i, 0), (0, P_i), (Q_i, 0), (0, Q_i))$;
end for
for $i = 1, \cdots, r$ **do**
  $S_i \leftarrow (\varphi_{r-1} \circ \cdots \circ \varphi_0)(S_i)$;
  $\varphi_i \leftarrow A_{i-1} \to A_i$ with kernel S_i;
end for
return $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$.

7.2 Isogenies to Matrices

For the powersmooth case:

algorithm 2 IsogenyToMatrix1

INPUT: polarized isogeny $\varphi_r \circ \cdots \circ \varphi_1 : A_0 \to A_r$ with $\deg(\varphi_i) = N_i^2$.

OUTPUT: $\gamma \in M_2(\mathscr{O}_0)$ with $\mathrm{Nrd}(\gamma) = (N_1 \cdots N_r)^2$, $\ker(\gamma) = \ker(\varphi_r \circ \cdots \circ \varphi_1)$.

1: $\gamma \leftarrow I_2$;
2: **for** $i = 1, \cdots r$ **do**
3: $\quad G_i \leftarrow (\tilde{\varphi}_{i-1} \circ \cdots \circ \tilde{\varphi}_2 \circ \tilde{\varphi}_1)(\ker(\varphi_i))$;
4: $\quad K_i \leftarrow \gamma(G_i)$;
5: $\quad$ Find $\Gamma_i \in M_2(\mathscr{O}_0)$ such that $\ker(\Gamma_i) \cap A_0[N_i] = K_i$ (Exhaustive search);
6: $\quad \gamma_i$ is a generator of left ideal $M_2(\mathscr{O}_0)\Gamma_i + M_2(\mathscr{O}_0)N_i$;
7: $\quad \gamma \leftarrow \gamma_i \gamma$;
8: **end for**
9: **return** γ.

For the power of 2 case:

algorithm 3 IsogenyToMatrix2

INPUT: polarized isogeny with kernel $K \cong (\mathbb{Z}/2^r\mathbb{Z})^2$.

OUTPUT: $\gamma \in M_2(\mathscr{O}_0)$ with $\ker(\gamma) = K$.

1: $\gamma \leftarrow I_2$, $K_1 \leftarrow K$;
2: **for** $i = 1, \cdots r$ **do**
3: $\quad G_i \leftarrow 2^{r-i} K_i$;
4: $\quad$ Compute γ_i which is the matrix with kernel G_i;
5: $\quad \gamma \leftarrow \gamma_i \gamma$, $K_{i+1} \leftarrow \gamma_i(K_i)$;
6: **end for**
7: **return** γ.

Compared to powersmoothness case, in the case of power of 2, one can search the table instead of solving PIP(Principal Ideal Problem). The cost of powersmoothness case is sub-exponential and that of power of 2 case is polynomial.

8 Applications of KLPT^2

8.1 Constructive IKO Correspondence

Theorem 3 There exists a (heuristic) polynomial-time algorithm which upon input $g \in Mat(A_0)$, finds product of elliptic curves A or Jacobian A with principally polarization λ such that the $(A, \lambda) \cong (A_0, \mu^{-1}(g))$.

Proof. By KLPT^2, we find $\gamma \in M_2(\mathscr{O}_0)$ such that $\gamma^+ g \gamma = NI_2$ with N powersmooth.

After MatrixToIsogeny, the image of isogeny corresponds to γ is (A, λ). $\square$

8.2 Relaxing Smoothness Assumptions in Translating Between Matrices and Isogenies

Let $\gamma \in M_2\mathscr{O}_0$ be a matrix corresponds to isogeny φ of degree N^2. Recall that a matrix g representing the codomain of φ, we have $\gamma^+ g \gamma = NI_2$.

From KLPT^2, there exist another matrix $\gamma_1 \in M_2(\mathscr{O}_0)$ and powersmooth integer N_1 such that $\gamma_1^+ g \gamma_1 = N_1 I_2$. We denote the isogeny corresponds to γ_1 by φ_1. Then we have the degree of φ_1 is N_1^2.

Since $N_1\,\varphi = \varphi_1\,\tilde{\varphi}_1\,\varphi$, and $\tilde{\varphi}_1\,\varphi = \lambda_0^{-1}\hat{\varphi}_1\lambda\,\varphi = \lambda_0^{-1}\hat{\varphi}_1\lambda_0\lambda_0^{-1}\lambda\,\varphi \in \mathrm{End}(A_0)$, the isogeny φ corresponds to matrix γ, $\lambda_0^{-1}\hat{\varphi}_1\lambda_0$ corresponds to matrix γ_1^+, then we have $\tilde{\varphi}_1\,\varphi$ corresponds to matrix $\gamma_1^+ g\gamma$.

After above computation, we have $\varphi(P) = \frac{1}{N_1}\,\varphi_1(\gamma_1^+ g\gamma(P))$.

8.3 Translating Between Matrices and Isogenies From Any surface

Matrices to Isogenies: Let us be given a matrix g_1 corresponds to principal polarization λ_1 and a matrix $\gamma \in M_2(\mathscr{O}_0)$ of reduced norm N^2, where γ defines a polarized isogeny emanating from (A_0, λ_1). We want to translate γ to isogeny.

If N is powersmooth, we can compute $\gamma_1 \in M_2(\mathscr{O}_0)$ such that $\gamma_1^+ g_1\gamma_1 = N_1 I_2$. Assume the matrix of principal polarization of codomain of φ is g_2, we have $\gamma^+ g_2\gamma = Ng_1$. Overall, $(\gamma\gamma_1)^+ g_2\gamma\gamma_1 = NN_1 I_2$. Then we translate the matrix $\gamma\gamma_1$ to isogeny and obtain N-isogeny from decomposition of this isogeny.

If N is not powersmooth, we use the method in the above subsection to obtain another smooth isogeny.

Isogenies to Matrices: Let $\gamma \in M_2(\mathscr{O})$ be a matrix corresponds to $\varphi : (A, \lambda_1) \to (A, \lambda_2)$, we can use KLPT^2 to find $\gamma_1 \in M_2(\mathscr{O}_0)$ which corresponds to an isogeny φ' from (A, λ_0) to (A, λ_1) with powersmooth degree. Since $\varphi \circ \varphi'$ is an isogeny from (A, λ_0) to (A, λ_2), then we first translate $\varphi \circ \varphi'$ to matrix, by multiplying the inverse of γ_1, we obtain the matrix corresponds to φ.