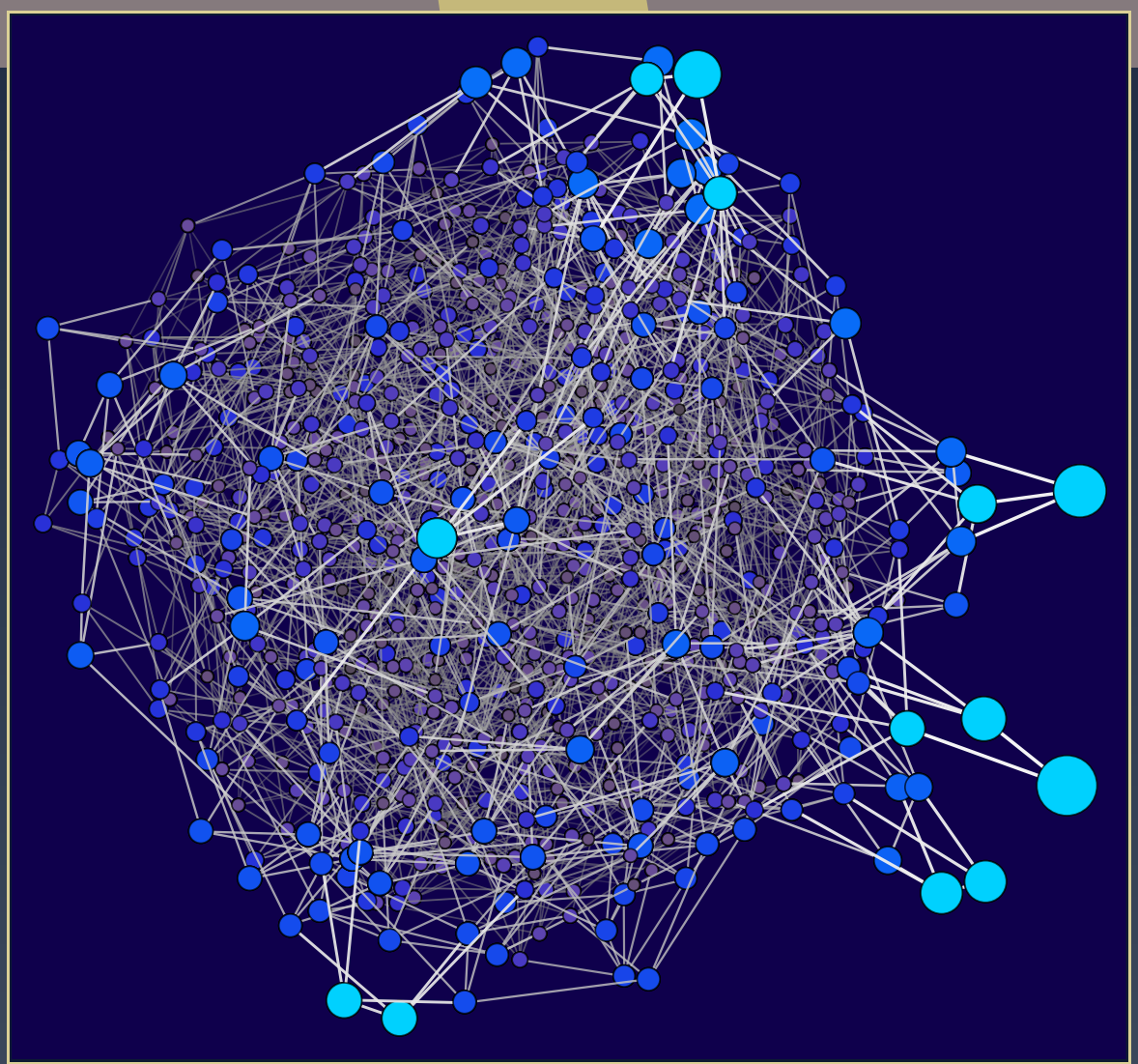
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Counting Richelot isogenies between superspecial abelian surfaces

Toshiyuki Katsura and Katsuyuki Takashima



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.283

Counting Richelot isogenies between superspecial abelian surfaces

Toshiyuki Katsura and Katsuyuki Takashima

Castryck, Decru, and Smith used superspecial genus-2 curves and their Richelot isogeny graph for basing genus-2 isogeny cryptography, and recently, Costello and Smith devised an improved isogeny path-finding algorithm in the genus-2 setting. In order to establish a firm ground for the cryptographic construction and analysis, we give a new characterization of *decomposed Richelot isogenies* in terms of *involutive reduced automorphisms* of genus-2 curves over a finite field, and explicitly count such decomposed (and nondecomposed) Richelot isogenies between *superspecial* principally polarized abelian surfaces. As a corollary, we give another algebraic geometric proof of Theorem 2 in the paper of Castryck et al.

1. Introduction

Isogenies of supersingular elliptic curves are widely studied as one candidate for postquantum cryptography, e.g., [3; 5; 10; 2]. Recently, several authors have extended the cryptosystems to higher genus isogenies, especially the genus-2 case [17; 6; 1; 4].

Castryck, Decru, and Smith [1] showed that *superspecial* genus-2 curves and their isogeny graphs give a correct foundation for constructing genus-2 isogeny cryptography. The recent cryptanalysis by Costello and Smith [4] employed the subgraph whose vertices consist of decomposed principally polarized abelian varieties, hence it is important to study the subgraph in cryptography.

Castryck et al. also presented concrete algebraic formulas for computing $(2, 2)$-isogenies by using the Richelot construction. In the genus-2 case, the isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed isogenies. In [1], the authors gave explicit formulas for the decomposed isogenies and a theorem stating that the number of decomposed Richelot isogenies outgoing from the Jacobian $J(C)$ of a superspecial curve C of genus 2 is *at most six* [1, Theorem 2], but they *do not precisely determine* this number. Moreover, their proof is *computer-aided*, that is, using the Gröbner basis computation.

Therefore, we revisit the isogeny counting based on an intrinsic algebraic geometric characterization. In 1960, Igusa [9] classified the curves of genus 2 with given reduced groups of automorphisms,

MSC2010: primary 14K02; secondary 14G50, 14H37, 14H40.
Keywords: Richelot isogenies, superspecial abelian surfaces, reduced group of automorphisms, genus-2 isogeny cryptography.

and in 1986, Ibukiyama, Katsura, and Oort [7] explicitly counted such superspecial curves according to the classification. Based on the classical results, we first count the number of Richelot isogenies from a superspecial Jacobian to decomposed surfaces (Cases (0)–(6) in Section 5) in terms of *involutive* (*i.e., of order 2*) *reduced automorphisms* which are called long elements. As a corollary, we give an algebraic geometric proof of Theorem 2 in [1] together with a *precise count of decomposed Richelot isogenies* (Remark 5.1). Moreover, by extending the method, we also count the total number of (decomposed) Richelot isogenies up to isomorphism outgoing from irreducible superspecial curves of genus 2 (resp. decomposed principally polarized superspecial abelian surfaces) in Theorem 6.2 (resp. Theorem 6.4).

Our paper is organized as follows: Section 2 gives mathematical preliminaries including the Igusa classification and the Ibukiyama–Katsura–Oort curve counting. Section 3 presents an abstract description of Richelot isogenies and Section 4 gives the main characterization of decomposed Richelot isogenies in terms of reduced groups of automorphisms. Section 5 counts the number of long elements of order 2 in reduced groups of automorphisms based on the results in Section 4. Section 6 gives the total numbers of (decomposed) Richelot isogenies outgoing from the irreducible superspecial curves of genus 2 and products of two elliptic curves, respectively. Section 7 gives some examples in small characteristic. Finally, Section 8 gives a concluding remark.

We use the following notation: For an abelian surface A, $A[n]$ denotes the group of n-torsion points of A, A^t the dual of A, $\mathrm{NS}(A)$ the Néron–Severi group of A, and T_v the translation by an element v of A. For a nonsingular projective variety X, $D \sim D'$ (resp. $D \approx D'$) denotes linear equivalence (resp. numerical equivalence) for divisors D and D' on X, and id_X the identity morphism of X.

2. Preliminaries

Let k be an algebraically closed field of characteristic $p > 5$. An abelian surface A defined over k is said to be superspecial if A is isomorphic to $E_1 \times E_2$ with E_i supersingular elliptic curves ($i = 1, 2$). Since for any supersingular elliptic curves E_i ($i = 1, 2, 3, 4$) we have an isomorphism $E_1 \times E_2 \cong E_3 \times E_4$ (see Shioda [15, Theorem 3.5], for instance), this notion does not depend on the choice of supersingular elliptic curves. For a nonsingular projective curve C of genus 2, we denote by $(J(C), C)$ the canonically polarized Jacobian variety of C. The curve C is said to be superspecial if $J(C)$ is superspecial as an abelian surface. We denote by $\mathrm{Aut}(C)$ the group of automorphisms of C. Since C is hyperelliptic, C has the hyperelliptic involution ι such that the quotient curve $C/\langle\iota\rangle$ is isomorphic to the projective line $\mathbb{P}^1$:

$$\psi : C \to \mathbb{P}^1.$$

There exist 6 ramification points on C. We denote them by P_i ($1 \le i \le 6$). Then, the $Q_i = \psi(P_i)$ are the branch points of ψ on $\mathbb{P}^1$. The group $\langle\iota\rangle$ is a normal subgroup of $\mathrm{Aut}(C)$. We put $\mathrm{RA}(C) \cong \mathrm{Aut}(C)/\langle\iota\rangle$ and we call it the reduced group of automorphisms of C. We call an element of $\mathrm{RA}(C)$ a reduced automorphism of C. For $\sigma \in \mathrm{RA}(C)$, $\tilde{\sigma}$ is an element of $\mathrm{Aut}(C)$ such that $\tilde{\sigma} \bmod \langle\iota\rangle = \sigma$.

Definition 2.1. An element $\sigma \in \mathrm{RA}(C)$ of order 2 is said to be long if $\tilde{\sigma}$ is of order 2. Otherwise, an element $\sigma \in \mathrm{RA}(C)$ of order 2 is said to be short (see [12, Definition 7.15]).

This definition does not depend on the choice of $\tilde{\sigma}$.

Lemma 2.2. *If an element $\sigma \in \mathrm{RA}(C)$ of order 2 acts freely on 6 branch points, then σ is long.*

Proof. By a suitable choice of coordinate x of $\mathbb{A}^1 \subset \mathbb{P}^1$, taking 0 as a fixed point of σ, we may assume $\sigma(x) = -x$, and $Q_1 = 1$, $Q_2 = -1$, $Q_3 = a$, $Q_4 = -a$, $Q_5 = b$, $Q_6 = -b$ ($a \neq 0, \pm 1$; $b \neq 0, \pm 1$; $a \neq \pm b$). Then, the curve is defined by

$$y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2),$$

and $\tilde{\sigma}$ is given by $x \mapsto -x$, $y \mapsto \pm y$. Therefore, $\tilde{\sigma}$ is of order 2. □

Lemma 2.3. *If $\mathrm{RA}(C)$ has an element σ of order 2, then there exists a long element $\tau \in \mathrm{RA}(C)$ of order 2.*

Proof. If σ acts freely on 6 branch points, then by Lemma 2.2, σ itself is a long element of order 2. We assume that the branch point $Q_1 = \psi(P_1)$ is a fixed point of σ. Since σ is of order 2, it must have one more fixed point among the branch points, say $Q_2 = \psi(P_2)$. By a suitable choice of coordinate x of $\mathbb{A}^1 \subset \mathbb{P}^1$, we may assume $Q_1 = 0$ and $Q_2 = \infty$. We may also assume $Q_3 = 1$. Then, σ is given by $x \mapsto -x$ and the six branch points are 0, 1, -1, a, $-a$, ∞ ($a \neq \pm 1$). The curve C is given by

$$y^2 = x(x^2 - 1)(x^2 - a^2) \quad (a \neq 0, \pm 1).$$

We consider an element $\tau \in \mathrm{Aut}(\mathbb{P}^1)$ defined by $x \mapsto a/x$. Then, we have an automorphisms $\tilde{\tau}$ of C defined by $x \mapsto a/x$, $y \mapsto a\sqrt{a}y/x^3$. Therefore, we see $\tau \in \mathrm{RA}(C)$. Since $\tilde{\tau}$ is of order 2, τ is long. □

$\mathrm{RA}(C)$ acts on the projective line $\mathbb{P}^1$ as a subgroup of $\mathrm{PGL}_2(k)$. The structure of $\mathrm{RA}(C)$ is classified as follows (see [9, page 644] and [7, page 130]):

$$(0)\ 0, \quad (1)\ \mathbb{Z}/2\mathbb{Z}, \quad (2)\ S_3, \quad (3)\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (4)\ D_{12}, \quad (5)\ S_4, \quad (6)\ \mathbb{Z}/5\mathbb{Z}.$$

We denote by n_i the number of superspecial curves of genus 2 whose reduced group of automorphisms is isomorphic to the group (i). Then, the n_i are given as follows (see [7, Theorem 3.3]):

$$(0)\ n_0 = \frac{(p-1)(p^2-35p+346)}{2880} - \frac{\left\{1-\left(\frac{-1}{p}\right)\right\}}{32} - \frac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{8} - \frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{9} + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod 5, \\ -\frac{1}{5} & \text{if } p \equiv 4 \pmod 5. \end{cases}$$

$$(1)\ n_1 = \frac{(p-1)(p-17)}{48} + \frac{\left\{1-\left(\frac{-1}{p}\right)\right\}}{8} + \frac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{2} + \frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{2}.$$

$$(2)\ n_2 = \frac{(p-1)}{6} - \frac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{2} - \frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{3}.$$

$$(3)\ n_3 = \frac{(p-1)}{8} - \frac{\left\{1-\left(\frac{-1}{p}\right)\right\}}{8} - \frac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{4} - \frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{2}.$$

$$(4)\ n_4 = \frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{2}.$$

(5) $n_5 = \dfrac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{2}$.

(6) $n_6 = \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod 5, \\ 1 & \text{if } p \equiv 4 \pmod 5. \end{cases}$

Here, for a prime number q and an integer a, $\left(\frac{a}{q}\right)$ is the Legendre symbol. The total number n of superspecial curves of genus 2 is given by

$$\begin{aligned} n &= n_0+n_1+n_2+n_3+n_4+n_5+n_6 \\ &= \frac{(p-1)(p^2+25p+166)}{2880} - \frac{\left\{1-\left(\frac{-1}{p}\right)\right\}}{32} + \frac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{8} + \frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{18} + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod 5, \\ \frac{4}{5} & \text{if } p \equiv 4 \pmod 5. \end{cases} \end{aligned}$$

For an abelian surface A, we have $A^t = \mathrm{Pic}^0(A)$ (Picard variety of A), and for a divisor D on A, there exists a homomorphism

$$\begin{aligned} \varphi_D : A &\to A^t \\ v &\mapsto T_v^* D - D. \end{aligned}$$

If D is ample, then φ_D is surjective, i.e., an isogeny. We know $(D \cdot D)^2 = 4 \deg \varphi_D$. We set $K(D) = \mathrm{Ker}\, \varphi_D$. If D is ample, then $K(D)$ is finite and there is a nondegenerate alternating bilinear form $e^D(v, w)$ on $K(D)$ (see Mumford [14, Section 23]). Let G be an isotropic subgroup scheme of $K(D)$ with respect to $e^D(v, w)$. In case D is ample, G is finite and we have an isogeny

$$\pi : A \to A/G.$$

The following theorem is due to Mumford [14, Section 23, Theorem 2, Corollary]:

Theorem 2.4. *Let G be an isotropic subgroup scheme of $K(D)$. Then, there exists a divisor D' on A/G such that $\pi^* D' \sim D$.*

Let n be a positive integer which is prime to p. Then, we have the Weil pairing $e_n : A[n] \times A^t[n] \to \mu_n$. Here, μ_n is the multiplicative group of order n. By Mumford [14, Section 23 "Functorial properties of e^L (5)"], we have the following.

Lemma 2.5. *For $v \in A[n]$ and $w \in \varphi_D^{-1}(A^t[n])$, we have*

$$e_n(v, \varphi_D(w)) = e^{nD}(v, w).$$

If D is a principal polarization, the homomorphism $\varphi_D : A \to A^t$ is an isomorphism. Therefore, by this identification we can identify the pairing e^{nD} with the Weil pairing e_n.

3. Richelot isogenies

We recall the abstract description of Richelot isogenies. (For the concrete construction of Richelot isogenies, see Smith [16] or Castryck, Decru and Smith [1, Section 3], for instance.)

Let A be an abelian surface with a principal polarization C. Then, we may assume that C is effective, and we have the self-intersection number $C^2 = 2$. It is easy to show (or as was shown by A. Weil) that there are two cases for effective divisors with self-intersection 2 on an abelian surface A:

(1) There exists a nonsingular curve C of genus 2 such that A is isomorphic to the Jacobian variety $J(C)$ of C and that C is the divisor with self-intersection 2. In this case, $(J(C), C)$ is said to be nondecomposed.

(2) There exist two elliptic curves E_1, E_2 with $(E_1 \cdot E_2) = 1$ such that $E_1 \times \{0\} + \{0\} \times E_2$ is a divisor with self-intersection 2 and that $A \cong E_1 \times E_2$. In this case, $(A, E_1 \times \{0\} + \{0\} \times E_2)$ is said to be decomposed.

Since φ_C is an isomorphism by the fact that C is a principal polarization, we have $K(2C) = \operatorname{Ker} \varphi_{2C} = \operatorname{Ker} 2\varphi_C = A[2]$. Let G be a maximal isotropic subgroup of $K(2C) = A[2]$ with respect to the pairing e^{2C}. Since we have $|G|^2 = |A[2]| = 2^4$ (see Mumford [14, Section 23, Theorem 4]), we have $|G| = 4$ and $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We have a quotient homomorphism

$$\pi : A \to A/G.$$

By Theorem 2.4, there exists a divisor C' on A/G such that $2C \sim \pi^* C'$. Since π is a finite morphism and $2C$ is ample, we see that C' is also ample. We have the self-intersection number $(2C \cdot 2C) = 8$, and we have

$$8 = (2C \cdot 2C) = (\pi^* C' \cdot \pi^* C') = \deg \pi (C' \cdot C') = 4(C' \cdot C').$$

Therefore, we have $(C' \cdot C') = 2$, that is, C' is a principal polarization on A/G. By the Riemann–Roch theorem of an abelian surface for ample divisors, we have

$$\dim \mathrm{H}^0(A/G, \mathcal{O}_{A/G}(C')) = (C' \cdot C')/2 = 1.$$

Therefore, we may assume C' is an effective divisor.

Using these facts, we see that C' is either a nonsingular curve of genus 2 or $E_1 \cup E_2$ with elliptic curves E_i $(i = 1, 2)$ which intersect each other transversely. In this situation, the correspondence from (A, C) to $(A/G, C')$ is called a Richelot isogeny. We consider a triple (A, C, G) with maximal isotropic subgroup $G \subset A[2]$ with respect to the pairing e^{2C}, and the corresponding Richelot isogeny π from (A, C, G) to $(A/G, C', G')$ with maximal isotropic subgroup $G' = \pi(A[2])$. Then, it is easy to see that for the Richelot isogeny $\pi' : (A/G, C') \to ((A/G)/G', C'')$, the principally polarized abelian surface $((A/G)/G', C'', G'')$ with maximal isotropic subgroup $G'' = \pi'((A/G)[2])$ is isomorphic to the original (A, C, G).

Now, we consider the case where A is a superspecial abelian surface. Then, since π is separable, A/G is also a superspecial abelian surface. We will use this fact freely.

From here on, for abelian surface $E_1 \times E_2$ with elliptic curves E_i $(i = 1, 2)$ we denote by $E_1 + E_2$ the divisor $E_1 \times \{0\} + \{0\} \times E_2$, if no confusion occurs. We sometimes call $E_1 \times E_2$ a principally polarized abelian surface. In this case, the principal polarization on $E_1 \times E_2$ is given by $E_1 + E_2$.

Definition 3.1. Let (A, C), (A', C') and (A'', C'') be principally polarized abelian surfaces with principal polarizations C, C', C'', respectively. The Richelot isogeny $\pi : A \to A'$ is said to be isomorphic to the Richelot isogeny $\varpi : A \to A''$ if there exist an automorphism $\sigma \in A$ with $\sigma^* C \approx C$ and an isomorphism $g : A' \to A''$ with $g^* C'' \approx C'$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\varpi} \\ A' & \xrightarrow{g} & A'' \end{array}$$

4. Decomposed Richelot isogenies

In this section, we use the same notation as in Section 3.

Definition 4.1. Let A and A' be abelian surfaces with principal polarizations C, C', respectively. A Richelot isogeny $A \to A'$ is said to be decomposed if C' consists of two elliptic curves. Otherwise, the Richelot isogeny is said to be nondecomposed.

Example 4.2. Let $C_{a,b}$ be a nonsingular projective model of the curve of genus 2 defined by the equation

$$y^2 = (x^2 - 1)(x^2 - a)(x^2 - b) \quad (a \neq 0, 1; b \neq 0, 1; a \neq b).$$

Let ι be the hyperelliptic involution defined by $x \mapsto x$, $y \mapsto -y$. $\mathrm{RA}(C_{a,b})$ has an element of order 2 defined by

$$\sigma : x \mapsto -x, y \mapsto y.$$

We put $\tau = \iota \circ \sigma$. We have two elliptic curves $E_\sigma = C_{a,b}/\langle\sigma\rangle$ and $E_\tau = C_{a,b}/\langle\tau\rangle$. The elliptic curve E_σ is isomorphic to an elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ with

$$\lambda = (b - a)/(1 - a) \tag{4-1}$$

and the elliptic curve E_τ is isomorphic to an elliptic curve $E_\mu : y^2 = x(x-1)(x-\mu)$ with

$$\mu = (b - a)/b(1 - a). \tag{4-2}$$

The map given by (4-1) and (4-2) yields a bijection

$$\{(a, b) \mid a, b \in k; a \neq 0, 1; b \neq 0, 1; a \neq b, \text{ and } J(C_{a,b}) \text{ is superspecial}\}$$
$$\to \{(\lambda, \mu) \mid \lambda, \mu \in k; \lambda \neq \mu; E_\lambda, E_\mu \text{ are supersingular}\}$$

(for the details, see Katsura and Oort [13, page 259]). We have a natural morphism $C_{a,b} \to E_\sigma \times E_\tau$ and this morphism induces an isogeny

$$\pi : J(C_{a,b}) \to E_\sigma \times E_\tau.$$

By [9, page 648], we know $\operatorname{Ker}\pi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\operatorname{Ker}\pi$ consists of $P_1 - \sigma(P_1)$, $P_3 - \sigma(P_3)$, $P_5 - \sigma(P_5)$ and the zero point. Here, $P_1 = (1, 0)$, $P_3 = (a, 0)$, $P_5 = (b, 0)$. Since $P_i - \sigma(P_i)$ is a divisor of order 2, we have $P_i - \sigma(P_i) \sim \sigma(P_i) - P_i$.

Comparing the calculation in [1, Proposition 1(2)] with the one in [13, Lemma 2.4], we see that $\pi : J(C_{a,b}) \to E_\sigma \times E_\tau$ is a decomposed Richelot isogeny with $C'_{a,b} = E_\sigma + E_\tau$ (also see [12, Proof of Proposition 7.18 (iii)]). We will use the bijection above to calculate decomposed Richelot isogenies.

Proposition 4.3. *Let C be a nonsingular projective curve of genus 2. Then, the following three conditions are equivalent*:

(i) *C has a decomposed Richelot isogeny outgoing from $J(C)$.*

(ii) *$\mathrm{RA}(C)$ has an element of order 2.*

(iii) *$\mathrm{RA}(C)$ has a long element of order 2.*

Proof. (i) $\Rightarrow$ (ii). By assumption, we have a Richelot isogeny

$$\pi : J(C) \to J(C)/G \tag{4-3}$$

such that G is an isotropic subgroup of $J(C)[2]$ with respect to $2C$, and that C' is a principal polarization consisting of two elliptic curves E_i $(i = 1, 2)$ on $J(C)/G$ with $2C \sim \pi^*(E_1 + E_2)$. Since C is a principal polarization, we have an isomorphism $\varphi_C : J(C) \cong J(C)^t$. In a similar way, we have $J(C)/G \cong (J(C)/G)^t$. Dualizing (4-3), we have

$$\eta = \pi^t : J(C)/G \to J(C)$$

with $J(C)/G \cong E_1 \times E_2$, $C' = E_1 + E_2$ and $\eta^*(C) \sim 2(E_1 + E_2)$. The kernel $\operatorname{Ker}\eta$ is an isotropic subgroup of $(E_1 \times E_2)[2]$ with respect to the divisor $2(E_1 + E_2)$.

Denoting by ι_{E_1} the inversion of E_1, we set

$$\bar{\tau} = \iota_{E_1} \times \mathrm{id}_{E_2}.$$

Then, $\bar{\tau}$ is an automorphism of order 2 which is not the inversion of $E_1 \times E_2$. By the definition, we have

$$\bar{\tau}^*(E_1 + E_2) = E_1 + E_2.$$

Moreover, since $\operatorname{Ker}\eta$ consists of elements of order 2 and $\bar{\tau}$ fixes the elements of order 2, $\bar{\tau}$ preserves $\operatorname{Ker}\eta$. Therefore, $\bar{\tau}$ induces an automorphism τ of $J(C) \cong (J(C)/G)/\operatorname{Ker}\eta \cong (E_1 \times E_2)/\operatorname{Ker}\eta$. Therefore, we have the following diagram:

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\bar{\tau}} & E_1 \times E_2 \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta} \\ J(C) & \xrightarrow{\tau} & J(C) \end{array}$$

We have

$$\eta^*\tau^*C = \bar{\tau}^*\eta^*C \sim \bar{\tau}^*(2(E_1+E_2)) = 2(E_1+E_2).$$

On the other hand, we have

$$\eta^*C \sim 2(E_1+E_2).$$

Since η^* is an injective homomorphism from $\mathrm{NS}(J(C))$ to $\mathrm{NS}(E_1\times E_2)$, we have $C \approx \tau^*C$. Therefore, $\tau^*C - C$ is an element of $\mathrm{Pic}^0(J(C)) = J(C)^t$. Since C is ample, the homomorphism

$$\begin{aligned}\varphi_C : J(C) &\to J(C)^t\\ v &\mapsto T_v^*C - C\end{aligned}$$

is surjective. Therefore, there exists an element $v \in J(C)$ such that

$$T_v^*C - C \sim \tau^*C - C,$$

that is, $T_v^*C \sim \tau^*C$. Since T_v^*C is a principal polarization, we see

$$\dim \mathrm{H}^0(J(C), \mathcal{O}_{J(C)}(T_v^*C)) = 1.$$

Therefore, we have $T_v^*C = \tau^*C$, that is, $T_{-v}^*\tau^*C = C$. Since τ is of order 2, we have $(\tau\circ T_{-v})^2 = T_{-v-\tau(v)}$, a translation. Therefore, we have $T_{-v-\tau(v)}^*C = C$. However, since C is a principal polarization, we have $\mathrm{Ker}\,\varphi_C = \{0\}$. Therefore, we have $T_{-v-\tau(v)} = \mathrm{id}$. This means $\tau\circ T_{-v}$ is an automorphism of order 2 of C. By definition, this is not the inversion ι. Hence, this gives an element of order 2 in $\mathrm{RA}(C)$.

(ii) $\Rightarrow$ (iii) This follows from Lemma 2.3.

(iii) $\Rightarrow$ (i) This follows from Lemma 2.2 and Example 4.2. □

Remark 4.4. In the proof of the proposition, the automorphism $\tau\circ T_{-v}$ really gives a long element of order 2 in $\mathrm{RA}(C)$.

By [1, Section 3.3], if the curve C of genus 2 is obtained from a decomposed principally polarized abelian surface by a Richelot isogeny, then the curve C has a long reduced automorphism of order 2. As is well-known, for a curve C of genus 2, the Jacobian variety $J(C)$ has 15 Richelot isogenies (see [1, Section 3.2], for instance). If we have a Richelot isogeny $(A, C) \to (A', C')$, then we also have a Richelot isogeny $(A', C') \to (A, C)$. Therefore, we have the following proposition.

Proposition 4.5. *Let C be a nonsingular projective curve of genus 2. Among the 15 Richelot isogenies outgoing from $J(C)$, the number of decomposed Richelot isogenies is equal to the number of long elements of order 2 in $\mathrm{RA}(C)$.*

In this proposition, we consider that a different isotropic subgroup gives a different Richelot isogeny. However, two different Richelot isogenies may be isomorphic to each other by a suitable automorphism (see Definition 3.1). From the next section, we will compute the number of Richelot isogenies up to isomorphism.

5. The number of long elements of order 2

In this section, we count the number of long elements of order 2 in $\mathrm{RA}(C)$. For an element $f \in \mathrm{RA}(C)$, we express the reduced automorphism by

$$f : x \mapsto f(x)$$

with a suitable coordinate x of $\mathbb{A}^1 \subset \mathbb{P}^1$. We will give the list of $f(x)$ corresponding to elements of order 2. Here, we denote by ω a primitive cube root of unity, by i a primitive fourth root of unity, and by ζ a primitive sixth root of unity:

Case 0: $\mathrm{RA}(C) \cong \{0\}$.

- There exist no long elements of order 2.

Case 1: $\mathrm{RA}(C) \cong \mathbb{Z}/2\mathbb{Z}$.

- The curve C is given by $y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)$.
- There exists only one long element of order 2 given by $f(x) = -x$.

Case 2: $\mathrm{RA}(C) \cong S_3$.

- The curve C is given by $y^2 = (x^3-1)(x^3-a^3)$.
- There exist three long elements of order 2 given by $f(x) = a/x,\ \omega a/x,\ \omega^2 a/x$.

Case 3: $\mathrm{RA}(C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- The curve C is given by $y^2 = x(x^2-1)(x^2-a^2)$.
- There exist two long elements of order 2 given by $f(x) = a/x,\ -a/x$.
- There exists one short element of order 2 given by $f(x) = -x$.

Case 4: $\mathrm{RA}(C) \cong D_{12}$.

- The curve is given by $y^2 = x^6 - 1$.
- There exist four long elements of order 2 given by $f(x) = -x,\ \zeta/x,\ \zeta^3/x,\ \zeta^5/x$.
- There exist three short elements of order 2 given by $f(x) = 1/x,\ \zeta^2/x,\ \zeta^4/x$.

Case 5: $\mathrm{RA}(C) \cong S_4$.

- The curve C is given by $y^2 = x(x^4-1)$.
- There exist six long elements of order 2 given by $f(x) = (x+1)/(x-1),\ -(x-1)/(x+1),\ i(x+i)/(x-i),\ i/x,\ -i/x,\ -i(x-i)/(x+i)$.
- There exist three short elements of order 2 given by $f(x) = -x,\ 1/x,\ -1/x$.

Case 6: $\mathrm{RA}(C) \cong \mathbb{Z}/5\mathbb{Z}$.

- The curve is given by $y^2 = x^5 - 1$.
- There exist no long elements of order 2.

Remark 5.1. By Proposition 4.5 and the calculation above, we see that for a curve C of genus 2, the number of outgoing decomposed Richelot isogenies from $J(C)$ is at most six. This result coincides with the one given in [1, Theorem 2].

6. Counting Richelot isogenies

6A. ***Richelot isogenies from Jacobians of irreducible genus-2 curves.*** Let C be a nonsingular projective curve of genus 2, and let $J(C)$ be the Jacobian variety of C. For a fixed C, we consider the set $\{(J(C), G)\}$ of pairs of $J(C)$ and an isotropic subgroup G for the polarization $2C$. The group $\mathrm{Aut}(C)$ acts on the ramification points of $C \to \mathbb{P}^1$. Using this action, $\mathrm{Aut}(C)$ induces the action on the set $\{(J(C), G)\}$. Since the inversion ι of C acts on $J(C)[2]$ trivially, the reduced group $\mathrm{RA}(C)$ of automorphisms acts on the set $\{(J(C), G)\}$ which consists of 15 elements.

Let P_i $(i = 1, 2, \ldots, 6)$ be the ramification points of $\psi : C \to \mathbb{P}^1$. A division into the sets of 3 pairs of these 6 points gives an isotropic subgroup G, that is,

$$\{P_{i_1} - P_{i_2},\ P_{i_3} - P_{i_4},\ P_{i_5} - P_{i_6},\ \text{the identity}\}$$

gives an isotropic subgroup of $J(C)[2]$. The action of $\mathrm{RA}(C)$ on the set $\{(J(C), G)\}$ is given by the action of $\mathrm{RA}(C)$ on the set

$$\{\langle (P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6})\rangle\},$$

which contains 15 sets. Here, the pair (P_i, P_j) is unordered. In this section, we count the number of orbits of this action for each case.

Let C be a curve of genus 2 with $\mathrm{RA}(C) \cong \mathbb{Z}/2\mathbb{Z}$. Such a curve is given by the equation

$$y^2 = (x^2 - 1)(x^2 - a)(x^2 - b)$$

with suitable conditions for a and b. The branch points $Q_i = \psi(P_i)$ are given by

$$Q_1 = 1, \quad Q_2 = -1, \quad Q_3 = \sqrt{a}, \quad Q_4 = -\sqrt{a}, \quad Q_5 = \sqrt{b}, \quad Q_6 = -\sqrt{b}.$$

The generator of the reduced group $\mathrm{RA}(C)$ of automorphisms is given by

$$\sigma : x \mapsto -x.$$

Since the inversion ι acts trivially on the ramification points, $\mathrm{RA}(C)$ acts on the set of the ramification points $\{P_1, P_2, P_3, P_4, P_5, P_6\}$, and the action of σ on the ramification points is given by

$$P_{2i-1} \mapsto P_{2i},\ P_{2i} \mapsto P_{2i-1} \quad (i = 1, 2, 3).$$

The isotropic subgroup which corresponds to $\langle (P_1, P_2), (P_3, P_4), (P_5, P_6)\rangle$ gives a decomposed Richelot isogeny and the other isotropic subgroups give nondecomposed isogenies. Moreover, $\langle (\sigma(P_{i_1}), \sigma(P_{i_2})), (\sigma(P_{i_3}), \sigma(P_{i_4})), (\sigma(P_{i_5}), \sigma(P_{i_6}))\rangle$ gives the Richelot isogeny isomorphic to the one given by $\langle (P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6})\rangle$. We denote P_i by i for the sake of simplicity. Then, the action σ is given by the

permutation $(1,2)(3,4)(5,6)$, and by the action of $\mathrm{RA}(C)$, the set $\{\langle (P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6})\rangle\}$ of 15 elements is divided into the following 11 loci:

$$\{[(1,2),(3,4),(5,6)]\},\ \{[(1,2),(3,5),(4,6)]\},\ \{[(1,2),(3,6),(4,5)]\},$$
$$\{[(1,3),(2,4),(5,6)]\},\ \{[(1,3),(2,5),(4,6)],[(1,6),(2,4),(3,5)]\},$$
$$\{[(1,3),(2,6),(4,5)],[(1,5),(2,4),(3,6)]\},\ \{[(1,4),(2,3),(5,6)]\},$$
$$\{[(1,4),(2,5),(3,6)],[(1,6),(2,3),(4,5)]\},\ \{[(1,4),(2,6),(3,5)],[(1,5),(2,3),(4,6)]\},$$
$$\{[(1,5),(2,6),(3,4)]\},\ \{[(1,6),(2,5),(3,4)]\}.$$

The reduced automorphism σ is a long one of order 2 and the element $[(1,2),(3,4),(5,6)]$ is fixed by σ. Therefore, the element $[(1,2),(3,4),(5,6)]$ gives a decomposed isogeny. The other 10 loci give nondecomposed isogenies. In the same way, we have the following proposition.

Proposition 6.1. *Under the notation above, the number of Richelot isogenies up to isomorphism in each case and the number of elements in each orbit are listed as follows. Here, in the list, for example,* $(1\times 6, 2\times 4)(1\times 1)$ *means that there exist* 6 *orbits which contain* 1 *element and* 4 *orbits which contain* 2 *elements for nondecomposed Richelot isogenies, and there exists* 1 *orbit which contains* 1 *element for decomposed Richelot isogenies*:

(0) $\underline{\mathrm{RA}(C)\cong\{0\}}$ 15 *Richelot isogenies, no decomposed ones*: $(1\times 15)(0)$.

(1) $\underline{\mathrm{RA}(C)\cong\mathbb{Z}/2\mathbb{Z}}$ 11 *Richelot isogenies*, 1 *decomposed one*: $(1\times 6, 2\times 4)(1\times 1)$.

(2) $\underline{\mathrm{RA}(C)\cong S_3}$ 7 *Richelot isogenies*, 1 *decomposed one*: $(1\times 3, 3\times 3)(3\times 1)$.

(3) $\underline{\mathrm{RA}(C)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}}$ 8 *Richelot isogenies*, 2 *decomposed ones*: $(1\times 1, 2\times 4, 4\times 1)(1\times 2)$.

(4) $\underline{\mathrm{RA}(C)\cong D_{12}}$ 5 *Richelot isogenies*, 2 *decomposed ones*: $(2\times 1, 3\times 1, 6\times 1)(1\times 1, 3\times 1)$.

(5) $\underline{\mathrm{RA}(C)\cong S_4}$ 4 *Richelot isogenies*, 1 *decomposed one*: $(1\times 1, 4\times 2)(6\times 1)$.

(6) $\underline{\mathrm{RA}(C)\cong\mathbb{Z}/5\mathbb{Z}}$ 3 *Richelot isogenies, no decomposed ones*: $(5\times 3)(0)$.

Theorem 6.2. *The total number of Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus* 2 *is equal to*

$$\frac{(p-1)(p+2)(p+7)}{192}-\frac{3\left\{1-\left(\frac{-1}{p}\right)\right\}}{32}+\frac{\left\{1-\left(\frac{-2}{p}\right)\right\}}{8}.$$

The total number of decomposed Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 *is equal to*

$$\frac{(p-1)(p+3)}{48}-\frac{\left\{1-\left(\frac{-1}{p}\right)\right\}}{8}+\frac{\left\{1-\left(\frac{-3}{p}\right)\right\}}{6}. \tag{6-1}$$

Proof. The total number of Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to

$$15n_0+11n_1+7n_2+8n_3+5n_4+4n_5+3n_6$$

and the total number of decomposed Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to

$$n_1 + n_2 + 2n_3 + 2n_4 + n_5.$$

The results follow from these facts. □

6B. ***Richelot isogenies from elliptic curve products.*** Let E, E' be supersingular elliptic curves, and we consider a decomposed principal polarization $E + E'$ and a Richelot isogeny $(E \times E', E + E') \to (J(C), C)$. For a principally polarized abelian surface $(E \times E', E + E')$, we denote by $\mathrm{Aut}(E \times E')$ the group of automorphisms of $E \times E'$ which preserve the polarization $E + E'$. Let $\{P_1, P_2, P_3\}$ (resp. $\{P_4, P_5, P_6\}$) be the 2-torsion points of E' (resp. E). Then, the six points P_i $(1 \le i \le 6)$ on $E \times E'$ play the role of ramification points of irreducible curves of genus 2, and $\mathrm{Aut}(E \times E')$ acts on the set $\{P_1, P_2, P_3, P_4, P_5, P_6\}$. The subgroup $\langle \iota_E \times \mathrm{id}_{E'}, \mathrm{id}_E \times \iota_{E'} \rangle$ acts on the set $\{P_1, P_2, P_3, P_4, P_5, P_6\}$ trivially. In this section, let E_2 be the elliptic curve defined by $y^2 = x^3 - x$ and E_3 the elliptic curve defined by $y^2 = x^3 - 1$. We know $\mathrm{Aut}\, E_2 \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{Aut}\, E_3 \cong \mathbb{Z}/6\mathbb{Z}$. The elliptic curve E_2 is supersingular if and only if $p \equiv 3 \pmod 4$ and E_3 is supersingular if and only if $p \equiv 2 \pmod 3$. In this section, the abelian surface $E \times E'$ means an abelian surface $E \times E'$ with principal polarization $E + E'$.

Now, let E, E' be supersingular elliptic curves which are neither isomorphic to E_2 nor to E_3. We also assume E is not isomorphic to E'. Using these notations, we have the following list of orders of the groups of automorphisms:

$$|\mathrm{Aut}(E \times E')| = 4, \quad |\mathrm{Aut}(E \times E) = 8, \quad |\mathrm{Aut}(E \times E_2)| = 8, \quad |\mathrm{Aut}(E \times E_3)| = 12,$$
$$|\mathrm{Aut}(E_2 \times E_2)| = 32, \quad |\mathrm{Aut}(E_3 \times E_3)| = 72, \quad |\mathrm{Aut}(E_2 \times E_3)| = 24.$$

The isotropic subgroups for the polarization $2(E + E')$ are determined in [1, Section 3.3]. Using their results and the same method as in Section 6A, we have the following proposition.

Proposition 6.3. *Let E, E' be supersingular elliptic curves which are neither isomorphic to E_2 nor to E_3 with E_2 and E_3 defined as above. We also assume that E is not isomorphic to E'. The number of Richelot isogenies up to isomorphism outgoing from a decomposed principally polarized superspecial abelian surface in each case and the number of elements in each orbit are listed as follows. Here, in the list, for example, $(1 \times 3, 2 \times 1)(1 \times 4, 2 \times 3)$ means that there exist 3 orbits which contain 1 element and 1 orbit which contains 2 elements for nondecomposed Richelot isogenies, and there exist 4 orbits which contain 1 element and 3 orbits which contain 2 elements for decomposed Richelot isogenies*:

(i) $\underline{E \times E'}$ 15 *Richelot isogenies*, 6 *nondecomposed ones*: $(1 \times 6)(1 \times 9)$.

(ii) $\underline{E \times E}$ 11 *Richelot isogenies*, 4 *nondecomposed ones*: $(1 \times 3, 2 \times 1)(1 \times 4, 2 \times 3)$.

(iii) $\underline{E \times E_2}$ 9 *Richelot isogenies*, 3 *nondecomposed ones* $(p \equiv 3 \pmod 4)$: $(2 \times 3)(1 \times 3, 2 \times 3)$.

(iv) $\underline{E \times E_3}$ 5 *Richelot isogenies*, 2 *nondecomposed ones* $(p \equiv 2 \pmod 3)$: $(3 \times 2)(3 \times 3)$.

(v) $\underline{E_2 \times E_2}$ 5 *Richelot isogenies*, 1 *nondecomposed one* $(p \equiv 3 \pmod 4)$: $(4 \times 1)(1 \times 1, 2 \times 1, 4 \times 2)$.

(vi) $\underline{E_3 \times E_3}$ 3 *Richelot isogenies*, 1 *nondecomposed one* ($p \equiv 2 \pmod 3$): $(3 \times 1)(3 \times 1, 9 \times 1)$.

(vii) $\underline{E_2 \times E_3}$ 3 *Richelot isogenies*, 1 *nondecomposed one* ($p \equiv 11 \pmod{12}$): $(6 \times 1)(3 \times 1, 6 \times 1)$.

Proof. We give a proof for the case (iv). For the other cases, the arguments are quite similar. Since the elliptic curve E_3 is defined by $y^2 = x^3 - 1$, the 2-torsion points (x, y) of E_3 are given by $P_1 = (1, 0)$, $P_2 = (\omega, 0)$ and $P_3 = (\omega^2, 0)$. Here, ω is a primitive cube root of unity. We denote by P_4, P_5 and P_6 the 2-torsion points of E. We have an automorphism σ of order 3 of E_3 defined by $\sigma : x \mapsto \omega x$, $y \mapsto y$. As in the case of Section 6A, we describe the isotropic subgroups G. We know that a division into the sets of 3 pairs of these 6 points P_i $(1 \le i \le 6)$ on $E \times E_3$ gives an isotropic subgroup G, that is, $\{P_{i_1} - P_{i_2}, P_{i_3} - P_{i_4}, P_{i_5} - P_{i_6},$ the identity$\}$ gives an isotropic subgroup of $(E \times E_3)[2]$. Here, we consider P_i $(1 \le i \le 3)$ as the point $(0, P_i)$ on $E \times E_3$, and P_i $(4 \le i \le 6)$ as the point $(P_i, 0)$ on $E \times E_3$. This set contains 15 elements. In the case (iv), we have $E \ncong E_3$. Therefore, by [1, Section 3.3], among the 15 isotropic subgroups the 9 cases such that $P_{i_1}, P_{i_2}, P_{i_3} \in E$ and $P_{i_4}, P_{i_5}, P_{i_6} \in E_3$ give the decomposed Richelot isogenies and the rest gives the nondecomposed Richelot isogenies. For the abbreviation, we denote by P_i by i. Then, on the set $\{1, 2, 3, 4, 5, 6\}$, $\mathrm{id}_E \times \sigma$ acts as the cyclic permutation $(1, 2, 3)$. The isotropic subgroup G is determined by the set of 3 pairs of 2-torsion points:

$$\{(i_1, i_2), (i_3, i_4), (i_5, i_6)\},$$

and the group $\mathrm{Aut}(E \times E_3)$ induces the action on the set of the 15 isotropic subgroups. Since the action of the subgroup $\langle \iota_E \times \mathrm{id}_{E_3}, \mathrm{id}_E \times \iota_{E_3} \rangle$ is trivial on the set of the 15 isotropic subgroups, we see that the action is given by the group $\mathrm{Aut}(E \times E_3)/\langle \iota_E \times \mathrm{id}_{E_3}, \mathrm{id}_E \times \iota_{E_3} \rangle \cong \langle \mathrm{id}_E \times \sigma \rangle$. By this action, the set of the 15 isotropic subgroups is divided into the following 5 orbits:

$$\{[(1, 2), (3, 4), (5, 6)], [(2, 3), (1, 4), (5, 6)], [(1, 3), (2, 4), (5, 6)]\},$$
$$\{[(1, 2), (3, 5), (4, 6)], [(2, 3), (1, 5), (4, 6)], [(1, 3), (2, 5), (4, 6)]\},$$
$$\{[(1, 2), (3, 6), (4, 5)], [(2, 3), (1, 6), (4, 5)], [(1, 3), (2, 6), (4, 5)]\},$$
$$\{[(1, 4), (2, 5), (3, 6)], [(1, 6), (2, 4), (3, 5)], [(1, 5), (2, 6), (3, 5)]\},$$
$$\{[(1, 4), (2, 6), (3, 5)], [(1, 5), (2, 4), (3, 6)], [(1, 6), (2, 5), (3, 4)]\}.$$

By the criterion above, the first 3 sets correspond with the decomposed Richelot isogenies, and the last 2 sets correspond with the nondecomposed Richelot isogenies. □

We denote by h the number of supersingular elliptic curves defined over k. Then, we know

$$h = \frac{p-1}{12} + \frac{\left\{1 - \left(\frac{-3}{p}\right)\right\}}{3} + \frac{\left\{1 - \left(\frac{-1}{p}\right)\right\}}{4}$$

(see Igusa [8], for instance). We denote by h_1 the number of supersingular elliptic curves E with $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$, h_2 the number of supersingular elliptic curves E_2 with $\mathrm{Aut}(E_2) \cong \mathbb{Z}/4\mathbb{Z}$, h_3 the number of supersingular elliptic curves E_3 with $\mathrm{Aut}(E_3) \cong \mathbb{Z}/6\mathbb{Z}$. We have $h = h_1 + h_2 + h_3$ and $h_2 = \left\{1 - \left(\frac{-1}{p}\right)\right\}/2$ and $h_3 = \left\{1 - \left(\frac{-3}{p}\right)\right\}/2$.

Theorem 6.4. *The total number of nondecomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to*

$$\frac{(p-1)(p+3)}{48} - \frac{\{1-(\frac{-1}{p})\}}{8} + \frac{\{1-(\frac{-3}{p})\}}{6}. \tag{6-2}$$

The total number of decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$\frac{(p-1)(3p+17)}{96} + \frac{(p+6)\{1-(\frac{-1}{p})\}}{16} + \frac{\{1-(\frac{-3}{p})\}}{3}.$$

Proof. The total number of nondecomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$6\left\{\frac{h_1(h_1-1)}{2}\right\} + 4h_1 + 3h_2h_1 + 2h_3h_1 + h_2 + h_3 + h_2h_3.$$

The total number of decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$9\left\{\frac{h_1(h_1-1)}{2}\right\} + 7h_1 + 6h_2h_1 + 3h_3h_1 + 4h_2 + 2h_3 + 2h_2h_3.$$

Since $\{1-(\frac{-1}{p})\}^2 = 2\{1-(\frac{-1}{p})\}$ and $\{1-(\frac{-3}{p})\}^2 = 2\{1-(\frac{-3}{p})\}$, the result follows from these facts. □

Remark 6.5. Since the total number of *decomposed* Richelot isogenies up to isomorphism outgoing from the *irreducible* superspecial curves of genus 2 is equal to the total number of *nondecomposed* Richelot isogenies up to isomorphism outgoing from *decomposed* principally polarized superspecial abelian surfaces, (6-1) and (6-2) give the same number.

7. Examples

By [7, Section 1.3], we have the following normal forms of curves C of genus 2 with given reduced group $\mathrm{RA}(C)$ of automorphisms:

(1) For $S_3 \subset \mathrm{RA}(C)$, the normal form is $y^2 = (x^3-1)(x^3-\alpha)$. This curve is superspecial if and only if α is a zero of the polynomial

$$g(z) = \sum_{l=0}^{[p/3]} \binom{(p-1)/2}{((p+1)/6)+l} \binom{(p-1)/2}{l} z^l.$$

(2) For $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{RA}(C)$, the normal form is $y^2 = x(x^2-1)(x^2-\beta)$. This curve is superspecial if and only if β is a zero of the polynomial

$$h(z) = \sum_{l=0}^{[p/4]} \binom{(p-1)/2}{((p+1)/4)+l} \binom{(p-1)/2}{l} z^l.$$

(3) For $\mathrm{RA}(C) \cong D_{12}$, the normal form is $y^2 = x^6 - 1$. This curve is superspecial if and only if $p \equiv 5 \pmod 6$ (see [7, Proposition 1.11]).

(4) For $\mathrm{RA}(C) \cong S_4$, the normal form is $y^2 = x(x^4 - 1)$. This is superspecial if and only if $p \equiv 5$ or $7 \pmod 8$ (see [7, Proposition 1.12]).

Finally, the elliptic curve E defined by $y^2 = x(x-1)(x-\lambda)$ is supersingular if and only if λ is a zero of the Legendre polynomial

$$\Phi(z) = \sum_{l=0}^{(p-1)/2} \binom{(p-1)/2}{l}^2 z^l.$$

Using these results, we construct some examples.

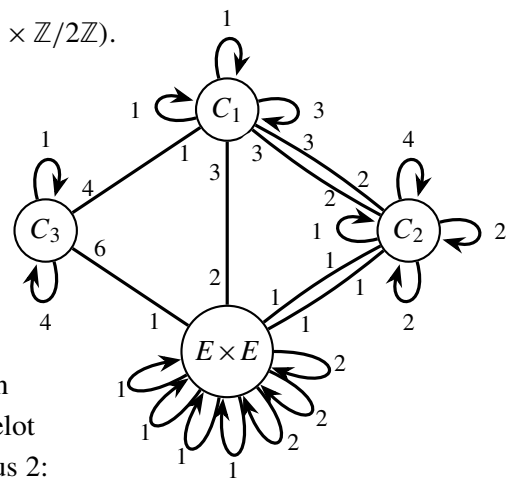
7A. ***Examples in characteristic 13.*** Assume the characteristic is $p = 13$. Over k we have only one supersingular elliptic curve E, and three superspecial curves C_1, C_2 and C_3 of genus 2 with $\mathrm{RA}(C_1) \cong S_3$, $\mathrm{RA}(C_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{RA}(C_3) = S_4$, respectively (see [7, Remark 3.4]). In characteristic 13, we know $h(z) = 7z^3 + 12z^2 + 12z + 7$, and the zeros are -1 and $-5 \pm \sqrt{6}$. We also know $g(z) = 2z^4 + 3z^3 + 4z^2 + 3z + 2$, and one of the zeros is $-4 + \sqrt{2}$. The Legendre polynomial is given by $\Phi(z) = z^6 + 10z^5 + 4z^4 + 10z^3 + 4z^2 + 10z + 1$, and one of the zeros is $3 - 2\sqrt{2}$. Using these facts, we know that the curves above are given by the following equations:

(1) E: $y^2 = x(x-1)(x-3+2\sqrt{2})$ $\quad (\mathrm{RA}(E) = \mathrm{Aut}(E)/\langle \iota_E \rangle \cong \{0\})$.

(2) C_1: $y^2 = (x^3-1)(x^3+4-\sqrt{2})$ $\quad (\mathrm{RA}(C_1) \cong S_3)$.

(3) C_2: $y^2 = x(x^2-1)(x^2+5+2\sqrt{6})$ $\quad (\mathrm{RA}(C_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

(4) C_3: $y^2 = x(x^4-1)$ $\quad (\mathrm{RA}(C_3) \cong S_4)$.



Therefore, outgoing from superspecial curves of genus 2, we have, in total, $1 + 2 + 1 = 4$ decomposed Richelot isogenies up to isomorphism by Proposition 6.1. On the other hand, outgoing from the unique decomposed principally polarized abelian surface $(E \times E, E + E)$, we have 5 nondecomposed Richelot isogenies (not up to isomorphism) (see [8] and [1, Figure 1]). Using the method in [1, Section 3.3], as the images of 5 nondecomposed Richelot isogenies, we have the following superspecial curves of genus 2:

(a) C_a: $y^2 = (x^2-1)(x^2-4+7\sqrt{2})(x^2-6+6\sqrt{2})$ $\quad (\mathrm{RA}\,(C_a) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

(b) C_b: $y^2 = (x^2-1)(x^2+3-2\sqrt{2})(x^2-4-\sqrt{2})$ $\quad (\mathrm{RA}\,(C_b) \cong S_4)$.

(c) C_c: $y^2 = (x^2-1)(x^2+3-4\sqrt{2})(x^2+1+3\sqrt{2})$ $\quad (\mathrm{RA}\,(C_c) \cong S_3)$.

(d) C_d: $y^2 = (x^2-1)(x^2-3)(x^2+3-4\sqrt{2})$ $\quad (\mathrm{RA}\,(C_d) \cong S_3)$.

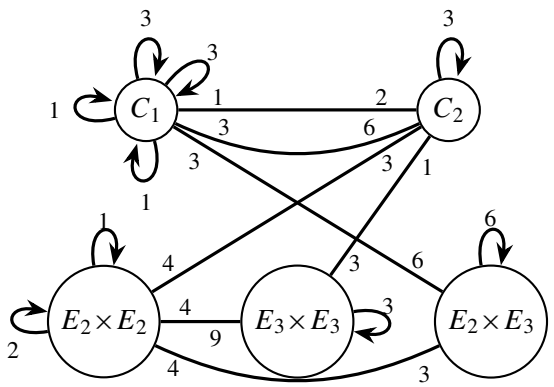
(e) C_e: $y^2 = (x^2-1)(x^2-6-6\sqrt{2})(x^2-2+2\sqrt{2})$ $\quad (\mathrm{RA}\,(C_e) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

We see that $C_a \cong C_e \cong C_2$, $C_c \cong C_d \cong C_1$ and $C_b \cong C_3$. As Richelot isogenies, $(E \times E, E + E) \to (J(C_c), C_c)$ is isomorphic to $(E \times E, E + E) \to (J(C_d), C_d)$, but $(E \times E, E + E) \to (J(C_a), C_a)$ is not isomorphic to $(E \times E, E + E) \to (J(C_e), C_e)$. Compare our graph with Figure 1 of [1]. In the graph the numbers along the edges are the multiplicities of Richelot isogenies outgoing from the nodes.

7B. ***Examples in characteristic 11.*** Assume the characteristic is $p = 11$. Over k we have two supersingular elliptic curves E_2,E_3 and two superspecial curves C_1, C_2 of genus 2 with $\mathrm{RA}(C_1) \cong S_3$, $\mathrm{RA}(C_2) \cong D_{12}$, respectively (see [7, Remark 3.4]). In characteristic 11, we know

$$g(z) = 10(z^3 + 5z^2 + 5z + 1),$$

and the roots are -1, 3 and 4. Using this fact, we know that the curves above are given by the following equations:



(1) E_2: $y^2 = x^3 - x$ $\quad (\mathrm{RA}(E_2) \cong \mathbb{Z}/2\mathbb{Z})$.

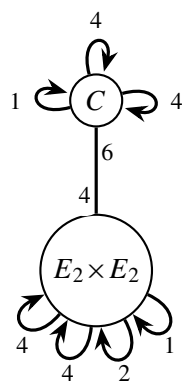
(2) E_3: $y^2 = x^3 - 1$ $\quad (\mathrm{RA}(E_3) \cong \mathbb{Z}/3\mathbb{Z})$.

(3) C_1: $y^2 = (x^3 - 1)(x^3 - 3)$ $\quad (\mathrm{RA}(C_1) \cong S_3)$.

(4) C_2: $y^2 = x^6 - 1$ $\quad (\mathrm{RA}(C_2) \cong D_{12})$.

We have three decomposed principally polarized abelian surfaces: $E_2 \times E_2$, $E_3 \times E_3$, $E_2 \times E_3$. Therefore, from the superspecial curves of genus 2 we have, in total, $1 + 2 = 3$ decomposed Richelot isogenies up to isomorphism by Proposition 6.1. On the other hand, from the decomposed principally polarized abelian surfaces, we have $1 + 1 + 1 = 3$ nondecomposed Richelot isogenies up to isomorphism by Proposition 6.3. For the decomposed principally polarized abelian surface $E_2 \times E_2$ the image of the only one nondecomposed Richelot isogeny is given by C_2. For the decomposed principally polarized abelian surface $E_3 \times E_3$ the image of the only one nondecomposed Richelot isogeny is also given by C_2. For the decomposed principally polarized abelian surface $E_2 \times E_3$ the image of the only one nondecomposed Richelot isogeny is given by C_1. See also Jordan and Zaytman [11, Section 5.1].

7C. ***Examples in characteristic 7.*** Assume the characteristic is $p = 7$. Over k we have only one supersingular elliptic curve E_2 and only one superspecial curves C of genus 2, which has $\mathrm{RA}(C) \cong S_4$ (see [7, Remark 3.4]). They are given by the following equations:



(1) E_2: $y^2 = x^3 - x$ $\quad (\mathrm{RA}(E_2) \cong \mathbb{Z}/2\mathbb{Z})$.

(2) C: $y^2 = x(x^4 - 1)$ $\quad (\mathrm{RA}(C) \cong S_4)$.

We have only one decomposed principally polarized abelian surface $E_2 \times E_2$. Therefore, outgoing from the superspecial curves of genus 2 we have only one decomposed Richelot isogeny up to isomorphism. From the decomposed principally polarized abelian surface, we also have only one nondecomposed Richelot isogeny up to isomorphism

(see [1, Sections 3.2 and 3.3]). For the decomposed principally polarized abelian surface $E_2 \times E_2$ the image of the only one nondecomposed Richelot isogeny is given by C.

8. Concluding remark

Our results answered a question about the number of decomposed Richelot isogenies and improved our understanding of the isogeny graph for genus-2 isogeny cryptography. Further applications (or implications) of our results to cryptography are left as an open problem.

For example, a very recent cryptanalytic algorithm by Costello and Smith [4] is considered as an interesting target. They reduced the isogeny path-finding algorithm in the superspecial Richelot isogeny graph to the elliptic curve path-finding problem, thus improving the complexity. A key ingredient of the reduction is a subalgorithm for finding a path connecting a given irreducible genus-2 curve and the (connected) subgraph consisting of elliptic curve products.

Proposition 4.3 showed the equivalence of existence of a decomposed Richelot isogeny outgoing from $J(C)$ and that of a (long) element of order 2 in the reduced group of automorphisms of C. It implies that the subgraph of elliptic curve products are adjacent to genus-2 curves having involutive reduced automorphisms in the superspecial graph. We hope that this new characterization can be applied to analyzing and/or improving the Costello–Smith attack.

Acknowledgements

The authors would like to thank anonymous reviewers of ANTS-XIV for their careful reading and useful suggestions for revising our paper, and E. Florit and B. Smith for their useful comments, in particular, for the correction of the figure in the case of $p = 11$ in Section 7B. Research of Katsura is partially supported by JSPS Grant-in-Aid for Scientific Research (C) No. 20K03530. Research of Takashima is partially supported by JST CREST Grant Number JPMJCR14D6, Japan.

References

[1] Wouter Castryck, Thomas Decru, and Benjamin Smith, *Hash functions from superspecial genus-2 curves using Richelot isogenies*, NutMiC 2019: Number-Theoretic Methods in Cryptology, 2019, To appear in J. of Math. Crypt.

[2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, *CSIDH: an efficient post-quantum commutative group action*, ASIACRYPT 2018, Part III, 2018, pp. 395–427.

[3] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Crypt. **22** (2009), no. 1, 93–113.

[4] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, PQCrypto 2020, 2020, pp. 151–168.

[5] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Crypt. **8** (2014), no. 3, 209–247.

[6] E. Victor Flynn and Yan Bo Ti, *Genus two isogeny cryptography*, PQCrypto 2019, 2019, pp. 286–306.

[7] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127–152.

[8] Jun-Ichi Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.

[9] Jun-Ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann of Math. **72** (1960), 612–649.

[10] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik, *SIKE: supersingular isogeny key encapsulation*, submission to the NIST's PQC standardization, round 2, updated version (2020).

[11] Bruce W. Jordan and Yevgeny Zaytman, *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*, preprint, 2020. arXiv 2005.09031

[12] Toshiyuki Katsura and Frans Oort, *Families of supersingular abelian surfaces*, Compositio Math. **62** (1987), 107–167.

[13] Toshiyuki Katsura and Frans Oort, *Supersingular abelian varieties of dimension two or three and class numbers*, Advanced Studies in Pure Math. **10** (1987), 253–281.

[14] David Mumford, *Abelian varieties*, Oxford Univ. Press, 1970.

[15] Tetsuji Shioda, *Supersingular K3 surfaces*, Algebraic Geometry, Proc. Copenhagen 1978 (K. Lønsted, ed.), Lecture Notes in Math. **732**, Springer-Verlag, 1979, pp. 563–591.

[16] Benjamin Smith, *Explicit endomorphisms and correspondences*, Ph.D. thesis, The University of Sydney, 2005.

[17] Katsuyuki Takashima, *Efficient algorithms for isogeny sequences and their cryptographic applications*, Mathematical modelling for next-generation cryptography: CREST crypto-math project, Springer-Verlag, 2017, pp. 97–114.

Received 20 Feb 2020. Revised 27 Jul 2020.

TOSHIYUKI KATSURA: tkatsura@ms.u-tokyo.ac.jp
Graduate School of Mathematical Sciences, The University of Tokyo, Japan

KATSUYUKI TAKASHIMA: takashima.katsuyuki@aj.mitsubishielectric.co.jp
Information Technology R&D Center, Mitsubishi Electric, Ofuna, Japan

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS

Commitment schemes and diophantine equations — José Felipe Voloch 1

Supersingular curves with small noninteger endomorphisms — Jonathan Love and Dan Boneh 7

Cubic post-critically finite polynomials defined over $\mathbb{Q}$ — Jacqueline Anderson, Michelle Manes and Bella Tobin 23

Faster computation of isogenies of large prime degree — Daniel J. Bernstein, Luca De Feo, Antonin Leroux and Benjamin Smith 39

On the security of the multivariate ring learning with errors problem — Carl Bootland, Wouter Castryck and Frederik Vercauteren 57

Two-cover descent on plane quartics with rational bitangents — Nils Bruin and Daniel Lewis 73

Abelian surfaces with fixed 3-torsion — Frank Calegari, Shiva Chidambaram and David P. Roberts 91

Lifting low-gonal curves for use in Tuitman's algorithm — Wouter Castryck and Floris Vermeulen 109

Simultaneous diagonalization of incomplete matrices and applications — Jean-Sébastien Coron, Luca Notarnicola and Gabor Wiese 127

Hypergeometric L-functions in average polynomial time — Edgar Costa, Kiran S. Kedlaya and David Roe 143

Genus 3 hyperelliptic curves with CM via Shimura reciprocity — Bogdan Adrian Dina and Sorina Ionica 161

A canonical form for positive definite matrices — Mathieu Dutour Sikirić, Anna Haensch, John Voight and Wessel P.J. van Woerden 179

Computing Igusa's local zeta function of univariates in deterministic polynomial-time — Ashish Dwivedi and Nitin Saxena 197

Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs — Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison and Jennifer Park 215

New rank records for elliptic curves having rational torsion — Noam D. Elkies and Zev Klagsbrun 233

The nearest-colattice algorithm: Time-approximation tradeoff for approx-CVP — Thomas Espitau and Paul Kirchner 251

Cryptanalysis of the generalised Legendre pseudorandom function — Novak Kaluđerović, Thorsten Kleinjung and Dušan Kostić 267

Counting Richelot isogenies between superspecial abelian surfaces — Toshiyuki Katsura and Katsuyuki Takashima 283

Algorithms to enumerate superspecial Howe curves of genus 4 — Momonari Kudo, Shushi Harashita and Everett W. Howe 301

Divisor class group arithmetic on $C_{3,4}$ curves — Evan MacNeil, Michael J. Jacobson Jr. and Renate Scheidler 317

Reductions between short vector problems and simultaneous approximation — Daniel E. Martin 335

Computation of paramodular forms — Gustavo Rama and Gonzalo Tornaría 353

An algorithm and estimates for the Erdős–Selfridge function — Brianna Sorenson, Jonathan Sorenson and Jonathan Webster 371

Totally p-adic numbers of degree 3 — Emerald Stacy 387

Counting points on superelliptic curves in average polynomial time — Andrew V. Sutherland 403