AGC^{2}T 2023

Split Jacobians with isogenous components

Curves of genus two induced by isogenies

Martin Djukanović

8 June 2023

Gluing two elliptic curves

- K is a fixed base field with $\mathrm{char}(K) \neq 2$
- $n \geq 2$ is coprime to $\mathrm{char}(K)$
- E and E' are elliptic curves

Gluing two elliptic curves

- K is a fixed base field with $\mathrm{char}(K) \neq 2$
- $n \geq 2$ is coprime to $\mathrm{char}(K)$
- E and E' are elliptic curves
- $\alpha : E[n] \xrightarrow{\sim} E'[n]$ is an *anti-isometry*, i.e. $e_n(P, Q) = e_n(\alpha(P), \alpha(Q))^{-1}$

Gluing two elliptic curves

- K is a fixed base field with $\mathrm{char}(K) \neq 2$
- $n \geq 2$ is coprime to $\mathrm{char}(K)$
- E and E' are elliptic curves
- $\alpha : E[n] \xrightarrow{\sim} E'[n]$ is an *anti-isometry*, i.e. $e_n(P, Q) = e_n(\alpha(P), \alpha(Q))^{-1}$
- Γ_α is the graph of α, a subgroup of $(E \times E')[n]$

Gluing two elliptic curves

- K is a fixed base field with $\mathrm{char}(K) \neq 2$
- $n \geq 2$ is coprime to $\mathrm{char}(K)$
- E and E' are elliptic curves
- $\alpha : E[n] \xrightarrow{\sim} E'[n]$ is an *anti-isometry*, i.e. $e_n(P, Q) = e_n(\alpha(P), \alpha(Q))^{-1}$
- Γ_α is the graph of α, a subgroup of $(E \times E')[n]$
- $\varphi : E \times E' \to (E \times E')/\Gamma_\alpha =: \mathfrak{J}$ is the isogeny with kernel Γ_α

Gluing two elliptic curves

- K is a fixed base field with $\mathrm{char}(K) \neq 2$
- $n \geq 2$ is coprime to $\mathrm{char}(K)$
- E and E' are elliptic curves
- $\alpha : E[n] \xrightarrow{\sim} E'[n]$ is an *anti-isometry*, i.e. $e_n(P, Q) = e_n(\alpha(P), \alpha(Q))^{-1}$
- Γ_α is the graph of α, a subgroup of $(E \times E')[n]$
- $\varphi : E \times E' \to (E \times E')/\Gamma_\alpha =: \mathfrak{J}$ is the isogeny with kernel Γ_α

Lemma

The principal polarization on $E \times E'$ defined by $\Theta = E \times \{O\} + \{O\} \times E'$ descends to a principal polarization on the quotient $\mathfrak{J}$, defined by a divisor C such that $\varphi^*(C) \sim n\Theta$, making φ a polarized isogeny.

Gluing two elliptic curves along the n-torsion

Additional facts:

- $\mathfrak{J}$ is a p.p.a.s. that is a Jacobian if and only if C is geometrically irreducible.

Gluing two elliptic curves along the n-torsion

Additional facts:

- $\mathfrak{J}$ is a p.p.a.s. that is a Jacobian if and only if C is geometrically irreducible.
- Isomorphism α is said to be *irreducible* if $\mathfrak{J}$ is a Jacobian, otherwise it is said to be *reducible*.

Gluing two elliptic curves along the n-torsion

Additional facts:

- $\mathfrak{J}$ is a p.p.a.s. that is a Jacobian if and only if C is geometrically irreducible.
- Isomorphism α is said to be *irreducible* if $\mathfrak{J}$ is a Jacobian, otherwise it is said to be *reducible*.
- If $\mathfrak{J} = \mathrm{Jac}(C)$ then geometrically C admits a pair of *minimal* coverings $\phi : C \to E$ and $\phi' : C \to E'$ of degree n, such that under embeddings

$$E \xhookrightarrow{\phi^*} \mathrm{Jac}(C) \xhookleftarrow{\phi'^*} E'$$

  the elliptic curves E and E' have common n-torsion.

Kani's reducibility criterion

Lemma (Kani)

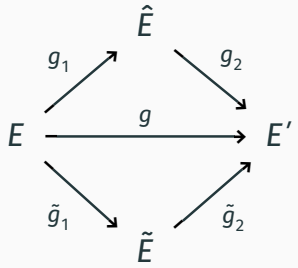
Suppose that $K = \bar{K}$. Let $g : E \to E'$ be an isogeny such that $g = g_2 \circ g_1 = \tilde{g}_2 \circ \tilde{g}_1$, where $g_1, g_2, \tilde{g}_1, \tilde{g}_2$ are suitable isogenies satisfying:

1) $\deg(g_1) + \deg(g_2) = n$,
2) $\deg(g_1) = \deg(\tilde{g}_2)$,
3) $\mathrm{Ker}(g_1) \cap \mathrm{Ker}(\tilde{g}_1) = \{0\}$.

Then there exists a unique reducible anti-isometry $\alpha : E[n] \xrightarrow{\sim} E'[n]$ such that $g_2^\vee \circ \alpha = g_1|_{E[n]}$ and $\tilde{g}_2^\vee \circ \alpha = -\tilde{g}_1|_{E[n]}$. Moreover, every reducible anti-isometry arises in this way.

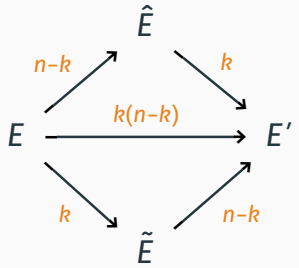
Kani's reducibility criterion – in short

Obstacles to irreducibility are isogenies $g : E \to E'$ of degree $k(n-k)$ with two distinct factorizations:



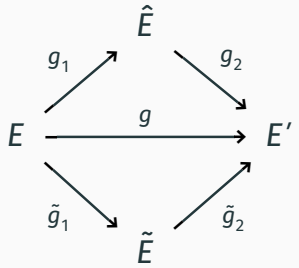
Kani's reducibility criterion – in short

Obstacles to irreducibility are isogenies $g : E \to E'$ of degree $k(n-k)$ with two distinct factorizations, such that:



Kani's reducibility criterion – in short

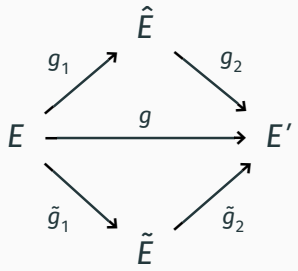
Obstacles to irreducibility are isogenies $g : E \to E'$ of degree $k(n-k)$ with two distinct factorizations, such that:

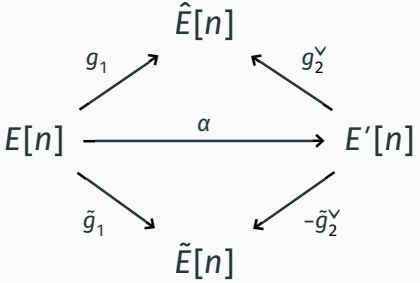


$\mathrm{Ker}(g_1) \cap \mathrm{Ker}(\tilde{g}_1) = \{0\}$

Kani's reducibility criterion – in short

Obstacles to irreducibility are isogenies $g : E \to E'$ of degree $k(n-k)$ with two distinct factorizations, such that:

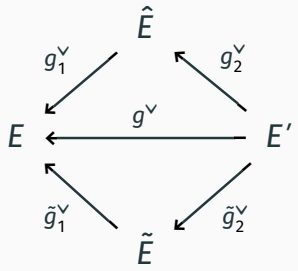


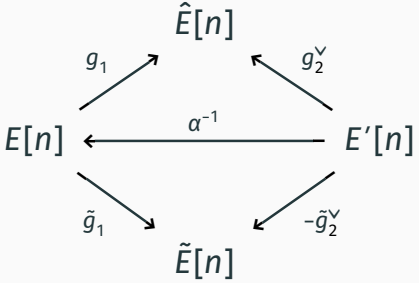


$\mathrm{Ker}(g_1) \cap \mathrm{Ker}(\tilde{g}_1) = \{0\}$

Kani's reducibility criterion – in short

Obstacles to irreducibility are isogenies $g : E \to E'$ of degree $k(n-k)$ with two distinct factorizations, such that:





$\mathrm{Ker}(g_1^\vee) \cap \mathrm{Ker}(\tilde{g}_1^\vee) = \{0\}$

Gluing curves via isogenies

- Let $f : E \to E'$ be a cyclic isogeny of degree D.

Gluing curves via isogenies

- Let $f : E \to E'$ be a cyclic isogeny of degree D.
- Let $(D, n) = 1$ so that the restriction $f|_{E[n]}$ is an isomorphism.

Gluing curves via isogenies

- Let $f : E \to E'$ be a cyclic isogeny of degree D.
- Let $(D, n) = 1$ so that the restriction $f|_{E[n]}$ is an isomorphism.
- Suppose $m \in \mathbb{Z}$ is such that $Dm^2 \equiv -1 \pmod{n}$.

Gluing curves via isogenies

- Let $f : E \to E'$ be a cyclic isogeny of degree D.
- Let $(D, n) = 1$ so that the restriction $f|_{E[n]}$ is an isomorphism.
- Suppose $m \in \mathbb{Z}$ is such that $Dm^2 \equiv -1 \pmod{n}$.
- Then $\alpha = [m] \circ f|_{E[n]}$ is an anti-isometry.

Gluing curves via isogenies

- Let $f : E \to E'$ be a cyclic isogeny of degree D.
- Let $(D, n) = 1$ so that the restriction $f|_{E[n]}$ is an isomorphism.
- Suppose $m \in \mathbb{Z}$ is such that $Dm^2 \equiv -1 \pmod{n}$.
- Then $\alpha = [m] \circ f|_{E[n]}$ is an anti-isometry.

Question

When is $\mathfrak{J} = (E \times E')/\Gamma_\alpha$ a Jacobian?

The main observation

Proposition (Dj.)

Suppose:

- $\mathrm{char}(K) = 0$
- $\mathrm{End}_{\bar{K}}(E) \cong \mathrm{End}_{\bar{K}}(E') \cong \mathbb{Z}$
- $f \in \mathrm{Hom}(E, E')$ cyclic
- $\deg(f) = D \ \ \& \ \ (D, n) = 1$
- $Dm^2 \equiv -1 \pmod{n}$
- $\alpha = [m] \circ f|_{E[n]}$

The main observation

Proposition (Dj.)

Suppose:

- $\mathrm{char}(K) = 0$
- $\mathrm{End}_{\bar{K}}(E) \cong \mathrm{End}_{\bar{K}}(E') \cong \mathbb{Z}$
- $f \in \mathrm{Hom}(E, E')$ cyclic
- $\deg(f) = D \ \ \& \ \ (D, n) = 1$
- $Dm^2 \equiv -1 \pmod{n}$
- $\alpha = [m] \circ f|_{E[n]}$

Then $\mathfrak{J} = (E \times E')/\Gamma_\alpha$ is *NOT* a Jacobian if and only if the following holds:

The main observation

Proposition (Dj.)

Suppose:

- $\mathrm{char}(K) = 0$
- $\mathrm{End}_{\bar{K}}(E) \cong \mathrm{End}_{\bar{K}}(E') \cong \mathbb{Z}$
- $f \in \mathrm{Hom}(E, E')$ cyclic
- $\deg(f) = D$ & $(D, n) = 1$
- $Dm^2 \equiv -1 \pmod{n}$
- $\alpha = [m] \circ f|_{E[n]}$

Then $\mathfrak{J} = (E \times E')/\Gamma_\alpha$ is *NOT* a Jacobian if and only if the following holds:

$\exists a, b, r, s \in \mathbb{Z}$ such that $D = rs$ and $ra^2 + sb^2 = n$ and $(a, b) = 1$ and $r < s$ and $a \equiv \pm mbs \pmod{n}$.

A classical result on binary quadratic forms

Lemma

An integer n is representable by a binary quadratic form of discriminant Δ if and only if $\Delta \equiv u^2 \pmod{4n}$. In particular, the (classes of) forms representing n are

$$nx^2 \pm uxy + \star y^2$$

via $(x, y) = (\pm 1, 0)$.

The main observation

Corollary

If $n = 2^k \prod p_i^{e_i}$ and $-D \equiv \square \pmod{n}$ then an D-isogeny $E \to E'$ induces a genus-two curve C with an (n, n)-split Jacobian if and only if there exist more roots of $-D$ modulo n than there are proper representations of n by (reduced) primitive diagonal forms of discriminant $-4D$, i.e. if and only if one of the following hold:

1) n is properly representable by non-diagonal forms with $\Delta = -4D$;
2) n (or 2^k) is not properly representable by a form with $\Delta = -4D$;
3) $D \equiv 7 \pmod{8}$ and $n \equiv 0 \pmod{8}$.

Genus-zero families: $D \in \{1, \dots, 10, 12, 13, 16, 18, 25\}$

For integers D such that $g(X_0(D)) = 0$, the class group of $\mathbb{Z}(\sqrt{-D})$ is either $\{0\}$ or $\mathbb{Z}/2\mathbb{Z}$, so the irreducibility condition can be expressed in terms of congruences.

Genus-zero families: $D \in \{1, \dots, 10, 12, 13, 16, 18, 25\}$

Theorem (Dj.)

If $n = 2^k \prod p_i^{e_i}$ and $g(X_0(D)) = 0$ then there is a suitable m such that the anti-isometry $[m] \circ f : E[n] \xrightarrow{\sim} E[n]$ is irreducible if and only if:

(1) $D = 3$ and $p_i \equiv 1 \pmod 3$ and $n \equiv 2, 6 \pmod 8$;

(2) $D = 5$ and $p_i \equiv 1, 3, 7, 9 \pmod{20}$ and $n \equiv 2, 3, 7, 18 \pmod{20}$;

(3) $D = 7$ and $p_i \equiv 1, 2, 4 \pmod 7$ and $n \equiv 0 \pmod 2$;

(4) $D = 8$ and $p_i \equiv 1, 3 \pmod 8$ and $n \equiv 3 \pmod 8$;

(5) $D = 9$ and $p_i \equiv 1 \pmod 4$ and $n \equiv 2, 5 \pmod{12}$;

(6) $D = 13$ and $p_i \equiv 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \pmod{52}$ and $n \equiv 2, 6, 7, 11, 15, 18, 19, 31, 34, 46, 47, 50 \pmod{52}$;

Genus-zero families: $D \in \{1, \dots, 10, 12, 13, 16, 18, 25\}$

Theorem (Dj.)

If $n = 2^k \prod p_i^{e_i}$ and $g(X_0(D)) = 0$ then there is a suitable m such that the anti-isometry $[m] \circ f : E[n] \xrightarrow{\sim} E[n]$ is irreducible if and only if:

(1) $D = 3$ and $p_i \equiv 1 \pmod 3$ and $n \equiv 2, 6 \pmod 8$;

(2) $D = 5$ and $p_i \equiv 1, 3, 7, 9 \pmod{20}$ and $n \equiv 2, 3, 7, 18 \pmod{20}$;

$\vdots$

(7) $D = 16$ and $p_i \equiv 1 \pmod 4$ and $n \equiv 5 \pmod 8$;

(8) $D = 25$ and $5 \neq p_i \equiv 1 \pmod 4$ and $n \equiv 2, 13, 17, 18 \pmod{20}$.

Genus-zero families: $D \in \{1, \dots, 10, 12, 13, 16, 18, 25\}$

Theorem (Dj.)

If $n = 2^k \prod p_i^{e_i}$ and $g(X_0(D)) = 0$ then there is a suitable m such that the anti-isometry $[m] \circ f : E[n] \xrightarrow{\sim} E[n]$ is irreducible if and only if:

(1) $D = 3$ and $p_i \equiv 1 \pmod 3$ and $n \equiv 2, 6 \pmod 8$;

(2) $D = 5$ and $p_i \equiv 1, 3, 7, 9 \pmod{20}$ and $n \equiv 2, 3, 7, 18 \pmod{20}$;

$\vdots$

(7) $D = 16$ and $p_i \equiv 1 \pmod 4$ and $n \equiv 5 \pmod 8$;

(8) $D = 25$ and $5 \neq p_i \equiv 1 \pmod 4$ and $n \equiv 2, 13, 17, 18 \pmod{20}$.

A similar result holds if $g(X_0(D)) = 1$, but congruences do not suffice.

Genus-zero and genus-one families for $n \leq 13$

n	D
2	3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 49
3	5, 8, 11, 14, 17, 20, 32
4	7, 11, 15, 19, 27
5	9, 11, 14, 16, 19, 21, 24, 36, 49
6	11, 17
7	5, 13, 17, 19, 20, 24, 27
8	7, 15
9	7, 11, 17, 32
10	11, 19, 49
11	8, 13, 17, 19, 21, 32
12	11
13	14, 16, 17, 25, 27, 49

Genus-zero families for $n \in \{2, 3\}$

Since a complete description of the minimal coverings $\phi : C \to E$ and $\phi' : C \to E'$ is known for $n = 2, 3$, explicit families can be obtained by imposing $\Phi_D(j(E), j(E')) = 0$.

The family defined by $n = 2$ and $D = 3$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t + 18$

$b = 2t + 81$

$c = t$

The family defined by $n = 2$ and $D = 3$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t + 18$

$b = 2t + 81$

$c = t$

These are precisely the curves with $D_6 \subset \mathrm{Aut}(C)$.

The family defined by $n = 2$ and $D = 5$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t^2 + 16t + 50$

$b = 2t^2 + 80t + 625$

$c = t^2$

The family defined by $n = 2$ and $D = 5$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t^2 + 16t + 50$

$b = 2t^2 + 80t + 625$

$c = t^2$

These are precisely the curves that I will show you again in a minute :)

The family defined by $n = 2$ and $D = 7$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t^3 + 16t^2 + 80t + 98$

$b = 2t^3 + 80t^2 + 784t + 2401$

$c = t^3$

The family defined by $n = 2$ and $D = 9$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t^4 + 16t^3 + 96t^2 + 240t + 162$

$b = 2t^4 + 80t^3 + 864t^2 + 3888t + 6561$

$c = t^4$

The family defined by $n = 2$ and $D = 13$

$$C : y^2 = x^6 - ax^4 + bx^2 - c$$

$$a = t^6 + 16t^5 + 112t^4 + 432t^3 + 944t^2 + 1040t + 338$$

$$b = 2t^6 + 80t^5 + 944t^4 + 5616t^3 + 18928t^2 + 35152t + 28561$$

$$c = t^6$$

The family defined by $n = 2$ and $D = 25$

$$C : y^2 = x^6 - ax^4 + bx^2 - c$$

$$a = t^{12} + 16t^{11} + 128t^{10} + 672t^9 + 2560t^8 + 7408t^7 + 16608t^6 + 28912t^5 + 38528t^4 + 37920t^3 + 25600t^2 + 10000t + 1250$$

$$b = 2t^{12} + 80t^{11} + 1024t^{10} + 7584t^9 + 38528t^8 + 144560t^7 + 415200t^6 + 926000t^5 + 1600000t^4 + 2100000t^3 + 2000000t^2 + 1250000t + 390625$$

$$c = t^{12}$$

The family defined by $n = 3$ and $D = 5$

$C : y^2 = x^6 - ax^4 + bx^2 - c$

$a = t^2 + 16t + 50$

$b = 2t^2 + 80t + 625$

$c = t^2$

The family defined by $n = 3$ and $D = 5$

$$C : y^2 = x^6 - ax^4 + bx^2 - c$$

$$a = t^2 + 16t + 50$$

$$b = 2t^2 + 80t + 625$$

$$c = t^2$$

The curve

$$C : y^2 = \left(x^3 + (t + 10)x^2 + (2t + 25)x + t\right) \cdot \left(x^3 - (t + 10)x^2 + (2t + 25)x - t\right)$$

has a Jacobian that is both $(2, 2)$-split and $(3, 3)$-split as $E \times E'$.

The family defined by $n = 3$ and $D = 5$

$$C : y^2 = x^6 - ax^4 + bx^2 - c$$

$$a = t^2 + 16t + 50$$

$$b = 2t^2 + 80t + 625$$

$$c = t^2$$

The curve

$$C : y^2 = \left(x^3 + (t+10)x^2 + (2t+25)x + t\right) \cdot \left(x^3 - (t+10)x^2 + (2t+25)x - t\right)$$

has a Jacobian that is both $(2,2)$-split and $(3,3)$-split as $E \times E'$. In fact, the anti-isometries $E[2] \xrightarrow{\sim} E'[2]$ and $E[3] \xrightarrow{\sim} E'[3]$ are both obtained by restricting the 5-isogeny $E \to E'$.

The family defined by $n = 3$ and $D = 8$

The curve

$$C : y^2 = \left(x^2 - t^2\right) \cdot \left(tx^2 + t + 2\right) \cdot \left((t+1)x^2 + 4\right)$$

has a Jacobian that is $(3,3)$-split as $E \times E'$ and $(2,2)$-split as $\tilde{E} \times \tilde{E}'$, where the elliptic curves admit a chain of 2-isogenies

$$E \to \tilde{E} \to \tilde{E}' \to E',$$

that restricts to the anti-isometry $E[3] \xrightarrow{\sim} E'[3]$.

Je vous remercie de votre attention!